(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2005-500740
(P2005-500740A)
(43)公表日　平成17年1月6日(2005.1.6)

(51)Int.Cl.[7]	F I			テーマコード（参考）
H04L 9/08	H04L	9/00	601C	5J104
	H04L	9/00	601F	

審査請求 未請求　予備審査請求 有　（全 134 頁）

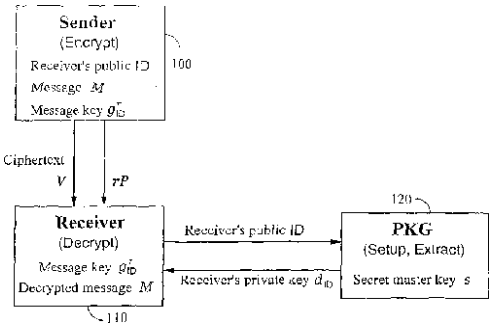
(21)出願番号	特願2003-521528(P2003-521528)
(86)(22)出願日	平成14年8月13日(2002.8.13)
(85)翻訳文提出日	平成16年2月13日(2004.2.13)
(86)国際出願番号	PCT/US2002/027155
(87)国際公開番号	WO2003/017559
(87)国際公開日	平成15年2月27日(2003.2.27)
(31)優先権主張番号	60/311,946
(32)優先日	平成13年8月13日(2001.8.13)
(33)優先権主張国	米国(US)

(71)出願人　591036321
ザ　ボード　オブ　トラスティーズ　オブ　ザ　リーランド　スタンフォード　ジュニア　ユニバーシティ
アメリカ合衆国　９４３０６－１１０６　カリフォルニア州　パロ・アルト　エル　カミノ　リール　１７０５
(74)代理人　100068755
弁理士　恩田　博宣
(74)代理人　100105957
弁理士　恩田　誠
(72)発明者　ボネ、ダン
アメリカ合衆国　９４３０５－９０４５　カリフォルニア州　スタンフォード　ゲイツ　４７５

最終頁に続く

(54)【発明の名称】ＩＤベース暗号化および関連する暗号手法のシステムおよび方法

(57)【要約】
送信者（１００）によって受信者（１１０）に送信される第１の情報Ｍを暗号化する方法およびシステムを利用することにより、送信者と受信者は両方とも、ＩＤベース情報および双線形写像を使用して秘密メッセージ鍵を計算することができる。一実施形態では、送信者（１００）は受信者（１１０）に関連付けられている識別子ＩＤからＩＤベース暗号鍵を計算する。識別子ＩＤには、受信者の電子メール・アドレス、受信者信任状、メッセージ識別子、または日付などのさまざまな種類の情報を入れることができる。送信者は、双線形写像および暗号鍵を使用して、秘密メッセージ鍵g^{r}_{ID}を計算し、これを使用して、メッセージＭを暗号化し、暗号文Ｖを出力して、送信者（１００）から受信者（１１０）に要素ｒＰとともに送信する。ＩＤベース解読鍵d_{ID}は、受信者に関連付けられたＩＤおよび秘密マスター鍵ｓに基づいて個人鍵作成器（１２０）により計算される。鍵作成器（１２０）から秘密解読鍵を取得した後、受信者（１１０）はそれを要素ｒＰおよび双線形写像とともに使用して、秘密メッセージ鍵g^{r}_{ID}を計算し、それを使



【特許請求の範囲】
【請求項１】
暗号システムにおいて、送信者と受信者との間でＩＤベース秘密メッセージ鍵を共有する方法であって、
（ａ）個人鍵作成器では：受信者のＩＤベース公開暗号鍵を表す、第１の代数群の要素Ｑを取得し；ｓを秘密マスター鍵を表す整数として、該受信者の個人解読鍵を表すｓＱを計算して、ｓＱを該受信者に送信し；第２の代数群の要素Ｐを取得して、ｓＰを計算し、ｓＰを該送信者に送信する工程と；
（ｂ）送信者側では、該要素Ｑを取得し；該要素Ｐを取得し；該個人鍵作成器から要素ｓＰを取得し；秘密ｒ∈★Ｚを選択し；ｒＰを計算し；ｒ、ｓＰ、Ｑ、および双線形写像から秘密メッセージ鍵を計算し；ｒＰを該受信者に送信する工程と、
（ｃ）受信者側では、送信者からｒＰを取得し；該個人鍵作成器からｓＱを取得し、ｒＰ、ｓＱ、および双線形写像から該秘密メッセージ鍵を計算する工程と、からなる方法。
【請求項２】
ｓＰおよびＰは前記個人鍵作成器により公開されたシステム・パラメータである請求項１に記載の方法。
【請求項３】
前記双線形写像は許容写像である請求項１に記載の方法。
【請求項４】
前記双線形写像は対称写像であり、前記第１の代数群は前記第２の代数群に等しい請求項１に記載の方法。
【請求項５】
前記双線形写像は非対称写像である請求項１に記載の方法。
【請求項６】
前記受信者側で前記要素Ｑを取得する工程は、前記受信者に関連付けられている公開識別子ＩＤを取得し、該ＩＤからＱを計算する工程からなる請求項１に記載の方法。
【請求項７】
公開識別子ＩＤに基づいて解読鍵を作成する方法であって、
（ａ）マスター鍵およびＩＤベース暗号システムに関連付けられている１組のシステム・パラメータを取得する工程と、
（ｂ）該公開識別子ＩＤから導かれる、代数群の要素Q_{ID}を取得する工程と、
（ｃ）Q_{ID}上の該マスター鍵の作用を使用して該マスター鍵およびQ_{ID}から、該代数群に属す該解読鍵d_{ID}を計算する工程と、
からなる方法。
【請求項８】
前記代数群は楕円曲線群の素数位数の部分群である請求項７に記載の方法。
【請求項９】
前記解読鍵を計算する工程は、ｓが前記マスター鍵を表すものとして、$d_{ID} = sQ_{ID}$を計算する工程からなる請求項７に記載の方法。
【請求項１０】
前記要素Q_{ID}を取得する工程は、前記公開識別子ＩＤを取得し、該公開識別子ＩＤから該要素Q_{ID}を計算する工程からなる請求項７に記載の方法。
【請求項１１】
前記公開識別子ＩＤは、個人名、エンティティの名前、ドメイン名、ＩＰアドレス、電子メール・アドレス、社会保障番号、パスポート番号、ライセンス番号、連続番号、郵便番号、住所、電話番号、ＵＲＬ、日付、時刻、件名、事例、管轄区、州、国、信任状、機密取扱資格レベル、および肩書きからなる有限の組み合わせからなるグループから選択された識別子である請求項７に記載の方法。
【請求項１２】
ＩＤベース暗号システムでメッセージを暗号化し、対応する暗号文を出力する方法であっ

て、
（ａ）★G_0、★G_1、および★G_2を（必ずしも異ならない）代数群とする双線形写像ｅ＾：★G_0×★G_1→★G_2からなる、暗号システムに関連付けられている１組のパラメータを取得する工程と、
（ｂ）該メッセージの宛先受信者を識別する情報からなる公開識別子ＩＤを選択する工程と、
（ｃ）該公開識別子ＩＤから要素Q_{ID}∈★G_0を計算する工程と、
（ｄ）ｅ＾およびQ_{ID}を使用して、秘密メッセージ鍵ｇ∈★G_2を計算する工程と、
（ｅ）該メッセージ鍵ｇを使用して該メッセージから該暗号文を計算する工程と、からなる方法。
【請求項１３】
前記暗号文を計算する工程は、前記メッセージ鍵ｇからビット・マスクを計算する工程と、同ビット・マスクを使用して前記メッセージをマスクする工程と、からなる請求項１２に記載の方法。
【請求項１４】
前記暗号文を計算する工程は、ランダム・ビット列σのハッシュからビット・マスクを計算する工程と、該ビット・マスクを使用して前記メッセージをマスクする工程と、前記秘密メッセージ鍵のハッシュを使用して該ランダム・ビット列σをマスクする工程と、からなる請求項１２に記載の方法。
【請求項１５】
前記暗号文を計算する工程は、ｒ∈★Ｚをランダムに選択した秘密とし、Ｐ∈★G_1として、要素ｒＰ∈★G_1を計算する工程からなる請求項１２に記載の方法。
【請求項１６】
前記メッセージ鍵を計算する工程は又、ｒをランダムに選択した秘密として、ｒ∈★Ｚを使用する請求項１２に記載の方法。
【請求項１７】
前記メッセージ鍵を計算する工程は、ｓを秘密マスター鍵として、要素ｓＰ∈★G_1を使用する請求項１２に記載の方法。
【請求項１８】
前記メッセージ鍵ｇ∈★G_2を計算する工程は、s_iを秘密マスター鍵の割符として、複数の要素s_iＰ∈★G_1を使用する請求項１２に記載の方法。
【請求項１９】
前記要素Q_{ID}を計算する工程は、文字コード体系を使用して前記公開識別子ＩＤを２進数列に写像する工程と、該２進数列を★G_0の該要素Q_{ID}にハッシュする工程と、からなる請求項１２に記載の方法。
【請求項２０】
★G_0および★G_1は場上で定義された楕円曲線から導かれる請求項１２に記載の方法。
【請求項２１】
ｅ＾は、楕円曲線上のＷｅｉｌペアリングから導かれる請求項２０に記載の方法。
【請求項２２】
ｅ＾は、楕円曲線上のＴａｔｅペアリングから導かれる請求項２０に記載の方法。
【請求項２３】
前記公開識別子ＩＤは、個人名、エンティティの名前、ドメイン名、ＩＰアドレス、電子メール・アドレス、社会保障番号、パスポート番号、ライセンス番号、連続番号、郵便番号、住所、電話番号、ＵＲＬ、日付、時刻、件名、事例、管轄区、州、国、信任状、機密取扱資格レベル、および肩書きからなる有限の組み合わせからなるグループから選択された識別子である請求項１２に記載の方法。
【請求項２４】
ＩＤベース暗号システムでメッセージを解読し、オリジナルのメッセージを出力する方法であって、

（ａ）★G_0、★G_1、および★G_2を（必ずしも異ならない）代数群とする双線形写像ｅ＾：★G_0×★G_1→★G_2からなる、暗号システムに関連付けられている１組のパラメータを取得する工程と、
（ｂ）該メッセージの宛先受信者を識別する情報からなる公開識別子ＩＤを選択する工程と、
（ｃ）該公開識別子ＩＤに対応する秘密鍵d_{ID}∈★G_0を取得する工程と、
（ｄ）ｅ＾および秘密鍵d_{ID}を使用して、秘密メッセージ鍵ｇ∈★G_2を計算する工程と、
（ｅ）該メッセージ鍵ｇを使用して該暗号文から該オリジナルのメッセージを計算する工程と、
からなる方法。
【請求項２５】
前記オリジナルのメッセージを計算する工程は、前記メッセージ鍵からビット・マスクを計算する工程と、該ビット・マスクを使用して該暗号文のマスクを外す工程と、からなる請求項２４に記載の方法。
【請求項２６】
前記オリジナルのメッセージを計算する工程は、前記メッセージ鍵のハッシュを使用してランダム・ビット列σのマスクを外す工程と、該ランダム・ビット列σのハッシュを使用して該メッセージのマスクを外す工程と、からなる請求項２４に記載の方法。
【請求項２７】
前記秘密鍵d_{ID}∈★G_1は、Q_{ID}および秘密マスター鍵ｓから導かれる請求項２４に記載の方法。
【請求項２８】
前記個人鍵d_{ID}∈★G_1を取得する工程は、ＩＤの認証を個人鍵作成器に与える工程と、該個人鍵作成器から該個人鍵を受信する工程と、からなる請求項２４に記載の方法。
【請求項２９】
前記公開識別子ＩＤに対応する前記個人鍵d_{ID}∈★G_0を取得する工程は、複数の対応する個人鍵作成器から複数の個人鍵部分d_i∈★G_0を取得する工程からなる請求項２４に記載の方法。
【請求項３０】
★G_0、★G_1、および★G_2は素数ｑで割り切れる位数を持つ巡回群である請求項２４に記載の方法。
【請求項３１】
★G_0および★G_1は場上で定義された楕円曲線の（必ずしも真部分群でない）部分群である請求項２４に記載の方法。
【請求項３２】
ｅ＾は、楕円曲線上のＷｅｉｌペアリングから導かれる請求項３１に記載の方法。
【請求項３３】
ｅ＾は、楕円曲線上のＴａｔｅペアリングから導かれる請求項３１に記載の方法。
【請求項３４】
前記公開識別子ＩＤは、個人名、エンティティの名前、ドメイン名、ＩＰアドレス、電子メール・アドレス、社会保障番号、パスポート番号、ライセンス番号、連続番号、郵便番号、住所、電話番号、ＵＲＬ、日付、時刻、時間間隔、件名、事例、管轄区、州、国、信任状、機密取扱資格レベル、および肩書きからなる有限の組み合わせからなるグループから選択された識別子である請求項２４に記載の方法。
【請求項３５】
メッセージを暗号化し、暗号文を出力する方法であって、
（ａ）★G_1および★G_2を代数群とする双線形写像ｅ＾：★G_1×★G_1→★G_2からなる、暗号システムに関連付けられている１組のパラメータと、ｓ∈★Ｚを秘密マスター鍵とする要素Ｐ、ｓＰ∈★G_1と、を取得する工程と、

（ｂ）ｘ∈★Ｚを宛先受信者の秘密として、該宛先受信者に対応する公開鍵ｘＰ∈★$Ｇ_1$を取得する工程と、
（ｃ）ｅ＾、ｓＰ、該公開鍵ｘＰ、およびランダムに選択したｒ∈★Ｚを使用して、メッセージ鍵ｇ∈★$Ｇ_2$を計算する工程と、
（ｄ）該メッセージ鍵ｇを使用して該メッセージから該暗号文を計算する工程と、からなる方法。
【請求項３６】
暗号文を解読し、メッセージを出力する方法であって、
（ａ）★$Ｇ_1$および★$Ｇ_2$を代数群とする双線形写像ｅ＾：★$Ｇ_1$×★$Ｇ_1$→★$Ｇ_2$からなる、暗号システムに関連付けられている１組のパラメータと、ｓ∈★Ｚを秘密マスター鍵とする要素Ｐ、ｓＰ∈★$Ｇ_1$と、を取得する工程と、
（ｂ）ｒ∈★Ｚを該送信者の秘密としてｅ＾、ｓＰ、個人鍵ｘ、および送信者から受信した要素ｒＰ∈★$Ｇ_1$を使用してメッセージ鍵ｇ∈★$Ｇ_2$を計算する工程と、
（ｃ）該メッセージ鍵ｇを使用して該暗号文から該メッセージを計算する工程と、からなる方法。
【請求項３７】
暗号文を解読し、メッセージを出力する方法であって、
（ａ）秘密マスター鍵ｓ∈★Ｚ、および★$Ｇ_1$および★$Ｇ_2$を代数群とする認容写像ｅ＾：★$Ｇ_0$×★$Ｇ_1$→★$Ｇ_2$からなる、暗号システムに関連付けられている１組のパラメータを取得する工程と、
（ｂ）ｘ∈★Ｚを宛先受信者の秘密として該メッセージの該宛先受信者に対応する公開鍵ｘＰ∈★$Ｇ_1$を取得する工程と、
（ｃ）ｒ∈★Ｚを該送信者の秘密として、ｅ＾、公開鍵ｘＰ、秘密マスター鍵ｓ、および送信者から受信した要素ｒＰ∈★$Ｇ_1$を使用して、メッセージ鍵ｇ∈★$Ｇ_2$を計算する工程と、
（ｄ）該メッセージ鍵ｇを使用して該暗号文からメッセージを計算する工程と、からなる方法。
【請求項３８】
受信者を宛先とする電子メール・メッセージを暗号化する方法であって、
（ａ）★$Ｇ_0$、★$Ｇ_1$、および★$Ｇ_2$を代数群とする双線形写像ｅ＾：★$Ｇ_0$×★$Ｇ_1$→★$Ｇ_2$からなる、暗号システムに関連付けられている１組のパラメータを取得する工程と、
（ｂ）該受信者の電子メール・アドレスからなる公開識別子ＩＤを選択する工程と、
（ｃ）該公開識別子ＩＤに対応する要素$Ｑ_{ＩＤ}$∈★$Ｇ_0$を計算する工程と、
（ｄ）ｅ＾、$Ｑ_{ＩＤ}$、およびランダムに選択した秘密ｒ∈★Ｚを使用して、メッセージ鍵ｇ∈★$Ｇ_2$を計算する工程と、
（ｅ）該メッセージ鍵ｇを使用して該メッセージから暗号化されているメッセージを計算する工程と、からなる方法。
【請求項３９】
前記公開識別子ＩＤはさらに、個人名、エンティティの名前、ドメイン名、ＩＰアドレス、社会保障番号、パスポート番号、ライセンス番号、シリアル番号、郵便番号、住所、電話番号、ＵＲＬ、日付、時刻、件名、事例、管轄区、州、国、信任状、機密取扱資格レベル、および肩書きからなるグループから選択された識別子からなる請求項３８に記載の方法。
【請求項４０】
暗号文を格納するコンピュータ読み込み可能記憶媒体であって、秘密メッセージ鍵は双線形写像、秘密整数、および宛先受信者のＩＤベース公開鍵を使用して送信者により計算され、該送信者のランダムに選択された秘密整数から計算された要素を表す第１の構成要素、および該秘密メッセージ鍵を使用して、送信者によって暗号化されたメッセージを表す第２の構成要素からなる記憶媒体。

【請求項４１】
送信者により受信者へ送信される第１の情報を暗号化する方法であって、第２の情報を供給する工程と、該第２の情報から暗号鍵を作成する工程と、双線形写像および該暗号鍵を使用して該送信者から該受信者に送信すべき該第１の情報の少なくとも一部を暗号化する工程からなる方法。
【請求項４２】
前記双線形写像は対称写像である請求項４１に記載の方法。
【請求項４３】
前記双線形写像は認容写像である請求項４１に記載の方法。
【請求項４４】
前記双線形写像はＷｅｉｌペアリングに基づく請求項４１に記載の方法。
【請求項４５】
前記双線形写像はＴａｔｅペアリングに基づく請求項４１に記載の方法。
【請求項４６】
前記第２の情報は前記受信者に関連付けられた情報を含む請求項４１に記載の方法。
【請求項４７】
前記第２の情報は電子メール・アドレスからなる請求項４１に記載の方法。
【請求項４８】
前記第２の情報は時刻に対応する情報を含む請求項４１に記載の方法。
【請求項４９】
前記第２の情報はメッセージ識別子を含む請求項４１に記載の方法。
【請求項５０】
前記第２の情報は信任状識別子を含む請求項４１に記載の方法。
【請求項５１】
前記第２の情報は前記メッセージの件名識別子を含む請求項４１に記載の方法。
【請求項５２】
受信者に関連付けられたＩＤベース暗号鍵で送信者により暗号化された暗号文を解読する方法であって、
該暗号鍵から誘導される解読鍵を取得する工程と、双線形写像および該解読鍵を使用して該暗号文の少なくとも一部を解読する工程からなる方法。
【請求項５３】
前記双線形写像は対称写像である請求項５２に記載の方法。
【請求項５４】
前記双線形写像は認容写像である請求項５２に記載の方法。
【請求項５５】
前記双線形写像はＷｅｉｌペアリングに基づく請求項５２に記載の方法。
【請求項５６】
前記双線形写像はＴａｔｅペアリングに基づく請求項５２に記載の方法。
【請求項５７】
さらに、前記解読鍵を取得する前に前記暗号文を取得する工程からなる請求項５２に記載の方法。
【請求項５８】
前記解読鍵を取得する工程は、個人鍵作成器に要求を送信する工程からなり、該要求は該暗号文とともに送信者により送信された情報からなる請求項５２に記載の方法。
【請求項５９】
暗号鍵に対応する解読鍵を作成する方法であって、該暗号鍵は第１の情報に基づいており、
群作用を持つ代数群を与える工程と、マスター鍵を与える工程と、該第１の情報に基づき暗号鍵を作成する工程と、該マスター鍵および該暗号鍵に適用される群作用に基づき解読鍵を作成する工程と、

からなる方法。
【請求項６０】
前記代数群は楕円曲線の少なくとも一部で定義される請求項５９に記載の方法。
【請求項６１】
前記第１の情報はエンティティに関連付けられた情報からなる請求項５９に記載の方法。
【請求項６２】
前記第１の情報は電子メール・アドレスからなる請求項５９に記載の方法。
【請求項６３】
前記解読鍵は、暗号化されたメッセージの受信者からの要求への応答として作成され、前記第１の情報はメッセージ識別子を含む請求項５９に記載の方法。
【請求項６４】
前記解読鍵は、受信者からの要求への応答として作成され、前記第１の情報は該受信者に関連付けられた属性を含む請求項５９に記載の方法。
【請求項６５】
前記第１の情報は時刻に対応する情報を含む請求項５９に記載の方法。
【請求項６６】
前記第１の情報は時刻に対応する情報を含み、前記解読鍵はユーザ・システム上で作成され、さらにターゲット・システム上に該解読鍵を格納する工程からなる請求項５９に記載の方法。
【請求項６７】
前記第１の情報は責任に対応する情報を含み、さらに、該責任に関連付けられたそれぞれの解読鍵をエンティティに与える工程からなる請求項５９に記載の方法。
【請求項６８】
さらに、受信者から前記解読鍵の要求を受信する工程と、該受信者が認証された場合に該受信者に該鍵を与える工程からなる請求項５９に記載の方法。
【請求項６９】
前記マスター鍵は共有マスター鍵の割符である請求項５９に記載の方法。
【請求項７０】
暗号システムのシステム・パラメータを与える方法であって、
代数群★G_1および代数群★G_2を表すシステム・パラメータを与える工程と、★G_1の要素の対を★G_2の要素に対応させる双線形写像ｅ＾を表すシステム・パラメータを与える工程からなる方法。
【請求項７１】
前記双線形写像は対称写像である請求項７０に記載の方法。
【請求項７２】
前記双線形写像はＷｅｉｌペアリングに基づく請求項７０に記載の方法。
【請求項７３】
前記双線形写像はＴａｔｅペアリングに基づく請求項７０に記載の方法。
【請求項７４】
前記代数群★G_1は楕円曲線の少なくとも一部から導かれる請求項７０に記載の方法。
【請求項７５】
前記代数群★G_1は楕円曲線$y^2 = x^3 + 1$の少なくとも一部から導かれる請求項７０に記載の方法。
【請求項７６】
送信者と受信者との間で通信を行う方法であって、
一部はメッセージ識別子から導かれる暗号鍵を使用して該送信者から該受信者に送信されるメッセージを暗号化する工程と、
該暗号化されたメッセージを送信者から受信者に送信する工程と、
該メッセージ識別子を含む、解読鍵の要求を受信者から受信する工程と、
解読鍵の要求を受信した後、受信者がメッセージを受信したことを示す受信情報を作成

する工程と、
該解読鍵を受信者に与える工程と、
からなる方法。
【請求項７７】
送信者に、作成された受信情報を送信する工程からなる請求項７６に記載の方法。
【請求項７８】
前記暗号鍵は前記送信者に関連付けられた識別子から一部は導かれる請求項７６に記載の方法。
【請求項７９】
前記暗号鍵は前記受信者に関連付けられた識別子から一部は導かれる請求項７６に記載の方法。
【請求項８０】
送信者と受信者との間で通信を行う方法であって、
受信者の識別情報を取得する工程と、
受信者が解読鍵を取得するために必要な該信任状を指定する工程と、
受信者の該識別情報および該信任状から暗号鍵を導く工程と、
該暗号鍵および双線形写像を使用してメッセージを暗号化する工程と、
該暗号化されたメッセージを送信者から該受信者に送信する工程と、
該メッセージの受信者からの解読鍵の要求を受信する工程と、
該受信者は信任状を保有しているかどうか調べる工程と、
該受信者が該信任状を保有している場合に、該解読鍵を受信者に与える工程と、
該解読鍵および該双線形写像を使用して該暗号化されているメッセージを解読する工程と、
からなる方法。
【請求項８１】
ＩＤベース暗号システムでメッセージを暗号化し、対応する暗号文を出力するシステムであって、
（ａ）★G_0、★G_1、および★G_2を（必ずしも異ならない）代数群とする双線形写像ｅ＾：★G_0×★G_1→★G_2からなる、暗号システムに関連付けられている１組のパラメータを取得するリソースと、
（ｂ）該メッセージの宛先受信者を識別する情報からなる公開識別子ＩＤを選択するリソースと、
（ｃ）該公開識別子ＩＤから要素Q_{ID}∈★G_0を計算するリソースと、
（ｄ）ｅ＾およびQ_{ID}を使用して、秘密メッセージ鍵ｇ∈★G_2を計算するリソースと、
（ｅ）該メッセージ鍵ｇを使用して該メッセージから暗号文を計算するリソースと、
からなるシステム。
【請求項８２】
メッセージとメッセージ鍵ｇから計算された暗号文からなる電子メッセージであって、
（ａ）★G_0、★G_1、および★G_2を（必ずしも異ならない）代数群とする双線形写像ｅ＾：★G_0×★G_1→★G_2からなる、暗号システムに関連付けられている１組のパラメータを取得する工程と、
（ｂ）該メッセージの宛先受信者を識別する情報からなる公開識別子ＩＤを選択する工程と、
（ｃ）該公開識別子ＩＤからQ_{ID}∈★G_0を計算する工程と、
（ｄ）ｅ＾およびQ_{ID}を使用して該メッセージ鍵ｇ∈★G_2を計算する工程により、ｇが作成される、電子メッセージ。
【発明の詳細な説明】
【技術分野】
【０００１】

本発明の分野は一般的に暗号システムに関する。
【背景技術】
【０００２】
公開鍵暗号システムでは、当事者２人がプライベートな認証されたメッセージを交換するのに、秘密鍵を共有するための秘匿性のある通信チャネルを最初に確保する必要がない。最も広く使用されている公開鍵暗号システムの１つは、（特許文献２）で開示されているＲＳＡ暗号システムである。ＲＳＡ暗号システムは、現在、多くの商用システムに搭載されている。この暗号システムは、Ｗｅｂトラフィックの秘匿性保護のためＷｅｂサーバおよびブラウザによって使用され、電子メールのプライバシーと認証の保護、およびリモート・ログイン・セッションの秘匿性保護を目的としても使用され、さらに電子クレジット・カード決済システムの心臓部に配置されている。つまり、ＲＳＡは、デジタル・データの秘匿性が懸念されるアプリケーションで使用されることが多い。
【０００３】
ＲＳＡ暗号システムなどの公開鍵暗号システムによれば、各個人は、秘密にしておく秘密鍵と公開されている公開鍵からなる特定の１対の鍵を持つ。この鍵の対は、（１）公開鍵だけがわかっても、秘密鍵を推論できず、（２）この２つの鍵は相補的である、つまりこの対の一方の鍵で暗号化されたメッセージは、相補的な鍵でしか解読できないという２つの重要な特性を有する。これらのシステムでは、一対の公開鍵と秘密鍵は両方とも、入力として乱数シードを受け取る鍵作成アルゴリズムの出力として一緒に作成される。そのため、これらの暗号システムでは、ユーザが望むような公開鍵または秘密鍵を選択できず、鍵作成アルゴリズムによってユーザ向けに作成された鍵をそのまま使用するしかない。このような方法は、他の人がある人へのメッセージを暗号化しようにも、その人が公開鍵を作成し公開していないと暗号化できないという欠点を有する。このタイプの暗号システムには、ほかに、悪意ある人が公開鍵を公開し、その鍵が誰か他の人のものだと主張することが可能だという問題がある。このような課題を解決するために、信頼できる公開鍵証明書発行機関（ＣＡ）を利用して、個人を認証し、その個人の公開鍵が真正の鍵であることを他の人に証明する。しかし残念なことに、このような対策だと、送信者がすべての受信者の証明書を取得しなければならず、既存の証明書の有効期限が切れる毎に新規証明書を取得する必要があるため、暗号システムの複雑さが増す。さらに、受信者側で、公開鍵を作成し、公開し、証明書をＣＡに登録し、期限が切れる場合にそのような証明書を更新する必要がある。
【０００４】
１９８４年に、シャミール（Ｓｈａｍｉｒ）は、新しいタイプの公開鍵暗号化方式を考えた（（非特許文献１）で説明されている）。シャミール（Ｓｈａｍｉｒ）の方式によれば、ユーザの公開鍵は、ユーザの名前とネットワーク・アドレス、または、名前と電子メール・アドレス、社会保障番号、住所、電話番号、または勤先住所との組み合わせ、などの公開識別子からなる。公開鍵はユーザの既存の公開識別子（ＩＤ）であって、乱数シードから作成された鍵ではないため、この種の公開鍵暗号システムはＩＤベース暗号（ＩＢＥ）方式と呼ばれる。しかし、シャミール（Ｓｈａｍｉｒ）は、具体的な実用的ＩＢＥ暗号システムを提示していなかった。実際、シャミール（Ｓｈａｍｉｒ）は、既存の暗号システム（ＲＳＡなど）は、秘匿性ＩＢＥ暗号システムを実現するのに適さないだろうと主張していた。
【特許文献１】
米国仮出願第６０／３１１９４６号
【特許文献２】
米国特許第４，４０５，８２９号
【非特許文献１】
エー・シャミール（Ａ．Ｓｈａｍｉｒ）“Ｉｄｅｎｔｉｔｙ－ｂａｓｅｄ ｃｒｙｐｔｏ ｓｙｓｔｅｍｓ ａｎｄ ｓｉｇｎａｔｕｒｅ ｓｃｈｅｍｅｓ”、Ａｄｖａｎｃｅｓ ｉｎ Ｃｒｙｐｔｏｌｏｇｙ － Ｃｒｙｐｔｏ ’８４、Ｌｅｃｔｕｒｅ Ｎｏｔｅｓ

in Computer Science、Vol.196、Springer Verlag、47－53ページ、1984年
【非特許文献2】
ディー・ボネ（D. Boneh），エム・フランクリン（M. Franklin），“Identity based encryption from the Weil pairing”，extended abstract in Advances in Cryptology－Crypto 2001，Lecture Notes in Computer Science，第2139巻、Springer－Verlag，pp. 231－229、2001年
【非特許文献3】
イー・フジサキ（E. Fujisaki）およびティー・オカモト（T. Okamoto）“Secure integration of asymmetric and symmetric encryption schemes”，in Advances in Cryptology － Crypto ’99，Lecture Notes in Computer Science，第1666巻，Springer－Verlag，pp. 537－554、1999年
【非特許文献4】
エー・ミヤジ（A. Miyaji）、エム・ナカバヤシ（M. Nakabayashi）、エス・タカノ（S. Takano）“New explicit condition of elliptic curve trace for FR－reduction”，IEICE Trans. Fundamentals，第E84A巻，No. 5，2001年5月
【非特許文献5】
アール・ゲナロ（R. Gennaro）、エス・ジャレッキ（S. Jarecki）、エイチ・クラウチク（H. Krawczyk）、ティー・レービン（T. Rabin）“Secure Distributed Key Generation for Discrete－Log Based Cryptosystems”，Advances in Cryptology － Eurocrypt ’99，Lecture Notes in Computer Science，第1592巻，Springer－Verlag，pp. 295－310，1999年
【非特許文献6】
ディー・ボネ（D. Boneh），ビー・リン（B. Lynn），エイチ・シャッチャム（H. Shacham），“Short signatures from the Weil pairing”，in Advances in Cryptology － AsiaCrypt 2001，Lecture Notes in Computer Science，第2248巻，Springer－Verlag，pp. 514－532，2001年）
【0005】
本出願特許の英語原文には、特許出願に使用できない符号が多数使用されているので、翻訳文においては表1の対照表に示す符号を使用した。また、上付きと下付きが上下になっているものは、「A^{b}_{c}」のようにずらして入力した。
【表1】

原文の符号	翻訳文の符号
$\hat{e}$	ｅ＾
$\mathbb{G}$	★Ｇ
$\mathbb{Z}$	★Ｚ
$\mathbb{F}$	★Ｆ
$\mathbb{F}_{p^2}$	★Ｆ■
$\mathbb{F}_{p^r}$	★Ｆ△
$\mathbb{F}_{p^6}$	★Ｆ□
$\mathcal{A}$ 、 $\mathcal{M}$	＄Ａ、＄Ｍ
$\notin$	∈／
$\oplus$	○＋
$\sum$	Σ
$g_{ID} = \prod_i g_i^{\lambda_i}$	ｇＩＤ＝Πｉｇｉ▲

【発明の開示】
【発明が解決しようとする課題】
【０００６】
シャミール（Ｓｈａｍｉｒ）がＩＢＥ方式を提案してから数年の間に、ＩＤベース暗号システムを実現する試みがいくつか行われた。いくつかの提案では、ユーザ同士が共謀しないことが必要である。また他の提案では、個人鍵作成器（ＰＫＧ）がそれぞれの個人鍵作成要求を処理するのに非現実的な時間がかかる。また別の提案では、不正操作防止ハードウェアを必要とする。
【０００７】
つまり、改善された暗号化の方法およびシステムが必要とされているということである。
【課題を解決するための手段】
【０００８】
本発明の一実施形態によれば、送信者によって受信者に送信される第１の情報を暗号化する方法は、第２の情報から作成された暗号化鍵を使用する。送信者から受信者に送信される第１の情報の少なくとも一部を暗号化するために、双線形写像および暗号化鍵を使用する。双線形写像は対称でも非対称でもよい。双線形写像は、楕円曲線から導かれる代数群上で定義されたＷｅｉｌペアリングまたはＴａｔｅペアリングに基づく。より一般的には、双線形写像は、代数多様体上で定義されたペアリングに基づいていてよい。
【０００９】
本発明の一実施形態によれば、第１の情報の一部の暗号化は、暗号化鍵に対応する解読鍵を作成する前に完了することが可能である。
本発明の他の実施形態によれば、第２の情報は、暗号化鍵に対応する解読鍵を作成する前に受信者に公開されている。第２の情報は、本発明の異なる実施形態により、受信者に関連付けられた電子メール・アドレス、名前またはその他の識別子を含むことができる。第２の情報はさらに、さまざまな実施形態によれば、１つ以上の時間間隔を定義する日付または一連の日付など、１つ以上の時刻に対応する受信者または情報に関連付けられた属性

を含むこともできる。解読鍵は、時刻に対応する情報に関して解読鍵の要求が受信された時刻に基づいて提供され得る。本発明の他の実施形態によれば、第２の情報は、メッセージ識別子、信任状識別子、メッセージ・サブジェクト識別子を含むことができる。

【００１０】

本発明の他の実施形態によれば、双線形写像を使用してメッセージ鍵を暗号化鍵から作成し、暗号ハッシュ関数をそのメッセージ鍵に適用する。

本発明の他の実施形態によれば、第１の情報の一部の暗号化は、双線形写像を使用して第２の情報からマスクを作成することを含む。マスクは、第２の情報の一部に適用される。

【００１１】

本発明の一実施形態は、受信者に関連付けられたＩＤベース暗号化鍵を使用して送信者によって暗号化された暗号文を解読する方法を対象とする。暗号化鍵から導かれる解読鍵が得られる。暗号文の少なくとも一部は、双線形写像および解読鍵を使用して解読される。双線形写像は対称でも非対称でもよい。双線形マップは、楕円曲線から導かれる代数群上で定義されたＷｅｉｌペアリングまたはＴａｔｅペアリングに基づく。

【００１２】

本発明の他の実施形態によれば、暗号文は解読鍵を作成する前に得られる。本発明の他の実施形態によれば、第１の情報は、暗号文を得る前に、また解読鍵を得る前に受信者に公開されている。解読鍵を得るには、暗号文とともに送信された情報も含めて、要求を個人鍵作成器に送る。

【００１３】

本発明の一実施形態は、暗号化鍵に対応する解読鍵を作成する方法を対象とする。代数群、群作用、およびマスター鍵が与えられる。暗号化鍵は、第１の情報に基づいて作成される。解読鍵は、群作用、マスター鍵、および暗号化鍵に基づいて作成される。本発明の一実施形態によれば、群作用を多項式時間内で計算し得る。本発明の他の態様によれば、マスター鍵がない場合、解読鍵を作成するには多項式時間よりも長い時間を要する。

【００１４】

本発明の他の実施形態は、暗号システムのシステム・パラメータを与える方法を対象とする。位数ｑの代数群★G_1および★G_2は、関連する群作用とともに与えられる。さらに、★G_1内の点の対を★G_2の点に対応させる双線形マップが与えられる。他の実施形態では、G_1の要素Ｐを表すシステム・パラメータおよびG_1の要素P_{pub}を表すシステム・パラメータが与えられるが、ただし、P_{pub}はＰに適用されるマスター鍵ｓの群作用に基づく。本発明の他の実施形態では、１つ以上のハッシュ関数H_1、H_2、H_3、またはH_4からなる関数群を表すシステム・パラメータが与えられる。本発明の他の実施形態では、メッセージ空間のサイズｎを表すシステム・パラメータが与えられる。

【００１５】

本発明の他の実施形態によれば、双線形写像は非対称でも対称でもよい。他の実施形態では、双線形写像は、楕円曲線の一部の上で定義されたＷｅｉｌペアリングまたはＴａｔｅペアリングに基づく。

【００１６】

本発明の他の実施形態によれば、代数群G_1は、位数ｐの場上で定義された楕円曲線により定義され、位数ｑは位数ｐよりも小さい。本発明の他の態様によれば、ｐの長さは少なくとも１０２４ビットであり、ｑの長さは１６０ビット以下である。

【００１７】

本発明の他の実施形態は、マスター鍵の割符を作成することを含む暗号通信を管理する方法を対象とする。割符は、別のシステム内に格納される。秘密鍵を取得する受信者からの要求に対して、別のシステムでマスター鍵のそれぞれの割符から秘密鍵の対応するそれぞれの割符を作成することにより応答する。受信者は秘密鍵の割符から秘密鍵を構成し、その秘密鍵は受信者の識別情報に対応する。

【００１８】

本発明の他の実施形態は、送信者と受信者との間で通信を行うための方法を対象とする。

送信者から受信者に送信されるメッセージが暗号化され、メッセージが送信者から受信者に送信される。メッセージの受信者からの解読鍵の要求が受信される。解読鍵の要求を受信した後、受信者がメッセージを受信したことを示す情報が作成され、受信者に解読鍵が与えられる。本発明の実施形態によれば、送信者の返信アドレスがメッセージに含まれ、メッセージを受信したことを示す確認通知が返信アドレスに送信される。本発明の他の態様によれば、メッセージの識別が確認通知に含まれ、その確認通知は送信者に送信される。本発明の他の態様によれば、暗号化鍵は送信者の返信アドレスに基づいて導出される。

【００１９】

本発明の他の実施形態は、送信者と信任状を有する受信者との間で通信を行うための方法を対象とする。受信者の識別情報を取得する。受信者が解読鍵を取得するために必要な信任状を指定すると、受信者の識別情報と信任状から暗号化鍵が導かれる。送信者から受信者に送信されるメッセージは、暗号化鍵および双線形写像を使用して暗号化され、メッセージが、送信者から受信者に送信される。メッセージの受信者からの解読鍵の要求を受信する。受信者が信任状を持っているかどうかが調べられ、受信者が信任状を持っていれば、解読鍵が受信者に与えられる。そこで、受信者は解読鍵と双線形写像を使用してメッセージを解読できる。

【００２０】

本発明の他の実施形態は、送信者と、ターゲット・システム上で解読鍵を格納することにかかわる受信者と、の間で通信を行う方法を対象とする。メッセージを解読する時刻に関連付けられている解読鍵の集まりを導出することができ、解読鍵はターゲット・システムに格納される。暗号化鍵は、メッセージが解読される時刻に関連付けられている文字列から導出される。暗号化鍵を使用してメッセージを暗号化する。ターゲット・システム上でメッセージを受信すると、そのメッセージは、双線形写像および対応する解読鍵を使用して解読される。

【００２１】

本発明の他の実施形態は、責任関係の異なる実体（エンティティ）に関わる送信者と受信者との間で通信を行う方法を対象とする。１組の解読鍵を、マスター鍵および異なる責任関係に関連付けられている１組の文字列から導出する。それぞれの責任関係のあるエンティティに解読鍵が与えられる。暗号化鍵は、異なる責任関係のうちの１つに関連付けられている文字列から導出される。暗号化鍵および双線形写像を使用して、送信者から受信者に送信されるメッセージが暗号化される。特定の責任を有するエンティティが、メッセージを受信し、それぞれの解読鍵および双線形写像を使用してメッセージを解読する。本発明の一実施形態によれば、特定の責任に対応する文字列として、電子メールの件名行がある。

【発明を実施するための最良の形態】

【００２２】

以下の説明では、本発明の暗号化手法のいくつかの実施例の詳細を述べ、またシステムの秘匿性の技術的内容についても解説する。

概要

現代の暗号システムでは普通のことであるが、本発明でも、その手法は一般的に、通信媒体に接続されたコンピュータ上に実装される。通常、コンピュータはインターネットまたは他のコンピュータ・ネットワークにより接続されるが、通信媒体も使用され得る。

【００２３】

本発明の一実施形態は、ＩＤベース情報から導かれる秘密メッセージ鍵を使用するＩＤベース暗号化システムを含む。送信者側はメッセージ鍵を使用してメッセージを暗号化し、受信者側はそのメッセージを解読することができる。秘密メッセージ鍵は、受信者のＩＤベース公開鍵から送信者により計算される。受信者側では、受信者のＩＤベース公開鍵から導かれる受信者の秘密鍵から同じメッセージ鍵を計算することができる。送信者および受信者は両方とも、双線形写像を使用して同じ秘密鍵を計算する。例えば、一実施形態では、非対称または対称双線形写像$e\hat{}：★G_0 \times ★G_1 \rightarrow ★G_2$を使用するが、ただし、

★G_0、★G_1、★G_2は（必ずしも異なるものではない）代数群である。★G_0が★G_1に等しい場合、双線形写像は対称であるといい、ｅ＾：★G_1×★G_1→★G_2と表すことが多い。非退化で、効率よく計算できる双線形写像ｅ＾は、認容写像と呼ぶ。本発明のいくつかの実施形態では、双線形写像は認容的であるのが好ましい。

【００２４】

この説明全体の規約として、★G_0および★G_1の群演算を加法で表し、★G_2の群演算を乗法で表す。素数位数の群★Ｇについては、★G^*で集合★G^*＝★Ｇ＼｛Ｏ｝を表すが、ただしＯは群★Ｇの単位要素とする。任意の長さの２進数列の集合を、｛０，１｝*で表す。★Z_qで、ｑを法とする加法による群｛０，．．．，ｑ－１｝を表し、★Z^+で、正の整数の集合を表す。加法の繰り返しにより★Ｇ上に★Z_qの自然な群作用が与えられること、および要素Ｐ∈★Ｇに対する要素ａ∈★Z_qの作用の結果をａＰと表すことに注意されたい。

【００２５】

本発明の他の実施形態によれば、ある種の計算Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎ問題（写像ｅ＾を伴う）は難しい問題である。一実装では、写像ｅ＾は認容的であり、★G_0、★G_1、★G_2の位数の素因数ｑは非常に大きい。。★G_0、★G_1、★G_2の位数は互いに等しくてもよい。以下の説明では、簡単にするため、一般性を失うことなく、★G_0、★G_1、★G_2の位数はすべて素数位数ｑであると仮定する。

【００２６】

実施例では、認容写像ｅ＾：★G_1×★G_1→★G_2を使用して、以下のようにＩＤベース暗号システムを実現している。メッセージを暗号化するために、送信者は、送り先である受信者の公開識別子ＩＤと関連付けられた公開鍵Q_{ID}∈★G_1を使用する。暗号化されたメッセージを解読するために、受信者は相補的な秘密鍵d_{ID}∈★G_1を使用する。秘密鍵は、公開鍵Q_{ID}、秘密マスター鍵ｓ∈★Z^*_q、および★G_1上の★Z^*_qの群作用から計算される。一実施形態では、例えば、$d_{ID}=sQ_{ID}$である。秘密マスター鍵ｓは信頼できるＰＫＧにのみ公開されているため、ユーザは通常、自分自身で秘密鍵を計算することは可能でない。秘密鍵を取得するには、個人が認証の済んだ後にＰＫＧから取得するのが好ましい。しかし、対応する秘密鍵が決定される前であっても、誰でも任意の公開識別子ＩＤに関連付けられた公開鍵Q_{ID}をいつでも計算することが可能である。例えば、一実施形態では、公開鍵Q_{ID}は、（１）従来の指標符号化方式を使用して公開識別子ＩＤを｛０，１｝*の対応する２進数列に写像し、（２）ハッシュ関数H_1：｛０，１｝*→★G^*_1を使用して２進数列を★G^*_1の要素Q_{ID}にハッシュすることで得られるが、ただし、Q_{ID}の位数はｑとする。

【００２７】

この実施形態では、公開識別子ＩＤを有する受信者を宛先とするメッセージの暗号化および解読を以下のように行うことができる。送信者は認容写像ｅ＾を使用して、秘密メッセージ鍵を決定することができる。送信者および受信者は同じ情報をすべて共有するわけではないが、写像ｅ＾が双線形であるという事実を使用することで、異なる情報を使って同じメッセージ鍵を計算することが可能である。それぞれプライベートの情報を使用するため、メッセージ鍵は秘密である。

【００２８】

このアプローチの実装方法を説明するため、送信者は★G_1の要素ＰおよびｓＰを知っていると仮定する。一実施形態では、例えば、★G_1の要素ＰおよびP_{pub}＝ｓＰは公開されたシステム・パラメータである。そこでさらに、送信者は非公開で、乱数ｒ∈★Z^*_qを選択し、受信者のＩＤベース公開鍵Q_{ID}を使用してg^r_{ID}＝ｅ＾（ｒQ_{ID}，ｓＰ）を使用する。要素g^r_{ID}はＩＤベースの秘密であり、送信者はこれを秘密メッセージ鍵として使用し、受信者へのメッセージのＩＤベース暗号化を実行する。次に、送信者は、暗号化されたメッセージをｒＰとともに受信者に送信することができる。すると受信者は、ｒＰを受信し、それを秘密鍵sQ_{ID}とともに使用して、秘密メッセージ鍵g^r_{ID}＝ｅ＾（sQ_{ID}，ｒＰ）を計算する。この秘密メッセージ鍵は、ｅ＾写像の双線形性

より、送信者によって計算される秘密メッセージ鍵に等しい。この計算された要素$g^{r}{}_{ID} \in \bigstar G_2$は、したがって、受信者が要素ｒＰおよび秘密鍵$sQ_{ID}$を使用して計算することができる送信者のＩＤベース秘密鍵である。この秘密鍵は、送信者と受信者との間の暗号化された通信を行うためのメッセージ鍵として使用することができる。

【００２９】

ＰＫＧはさらに、受信者の秘密鍵も知っているため、さらに秘密メッセージ鍵を計算し、メッセージを解読することが可能であることに注意されたい。送信者、受信者、およびＰＫＧすべてに、秘密メッセージ鍵を計算するための十分な情報がすべて用意されている。しかし、他のエンティティにはいっさい、通常、送信者の秘密鍵ｒまたは受信者の秘密sQ_{ID}は公開されない。この実施形態の秘匿性は、ｒが公開されていない、またはsQ_{ID}が公開されていないと、双線形写像を使用しｒ、ｓ、およびQ_{ID}の組み合わせに基づいて秘密メッセージ鍵を計算することの困難さに関係している。

【００３０】

一実施形態では、メッセージ鍵$g^{r}{}_{ID}$を使用し、ＸＯＲ演算（「○＋」で表される）を使用してメッセージのビットの暗号化および解読を行うのに使用されるマスクを決定する。特に、メッセージＭの暗号文Ｖは、$H_2 : \bigstar G_2 \rightarrow \{0, 1\}^{n}$をハッシュ関数とし、ｎをメッセージのビット長として、$V = M \bigcirc + H_2 (g^{r}{}_{ID})$を計算して得られる。逆に、メッセージＭは、$M = V \bigcirc + H_2 (g^{r}{}_{ID})$を計算することにより暗号文Ｖから復元される。

【００３１】

他の実施形態では、上で概要を述べた一方向暗号化方式は、選択暗号文秘匿システムに変換することにより秘匿性を高められる。本発明の一実施形態では、例えば、Ｆｕｊｉｓａｋｉ－Ｏｋａｍｏｔｏの一般的手法を使用する。

【００３２】

他の実施形態では、マスター鍵は、分散ＰＫＧの複数の個人鍵作成器に分散させた成分s_iに分割される。識別子ＩＤに基づく公開鍵Q_{ID}を持つユーザが与えられた場合、分散ＰＫＧ内の個人鍵作成器のそれぞれがＱおよびマスター鍵の公開鍵部分s_iを使用して秘密鍵部分d_iを計算する。これらの秘密鍵部分は、Q_{ID}で暗号化されたメッセージを解読するため、ユーザによって組み合わされ、単一の秘密鍵d_{ID}として使用される可能性がある。

【００３３】

他の実施形態では、ＥｌＧａｍａｌ暗号化方式に鍵エスクローが組み込まれる、つまり任意の公開鍵で暗号化された暗号文を１つの大域的なエスクロー鍵で解読することが可能である。この実施形態では、上述のシステム例は以下のように適合される。受信者はさらに、要素ＰおよびｓＰも知っていると想定する。受信者は、ＰＫＧから秘密鍵を取得するのではなく、乱数$x \in \bigstar Z^{*}_{q}$を選択し、群作用を使用してｘＰを計算し、計算結果に基づいて公開鍵を公開することにより公開／秘密鍵の対を作成する。一実施形態では、公開鍵はｘＰであり、相補的秘密鍵はｄ＝ｘ（ｓＰ）である。（したがって、ｘＰは、Q_{ID}の役割を担い、ｄ＝ｘ（ｓＰ）＝ｓ（ｘＰ）は$d_{ID} = sQ_{ID}$の役割を担う。）受信者へのメッセージを暗号化するには、送信者は前のように、乱数ｒを選択して、ｒＰを受信者に送信する。次に、ｘ（ｓＰ）＝ｄは秘密であるとして、受信者は対（ｒＰ，ｘ（ｓＰ））を知り、ｒ（ｘＰ）は秘密であるとして、送信者は対（ｓＰ，ｒ（ｘＰ））を知る。そのため、送信者および受信者は両用とも、ｇ＝ｅ＾（ｒＰ，ｘ（ｓＰ））＝ｅ＾（ｓＰ，ｒ（ｘＰ））を計算し、ただし、第２の等式はｅ＾の双線形性から導かれる。しかし、この秘密も、マスター鍵の情報ｓからを調べることが可能である。送信者からの要素ｒＰ、受信者の公開鍵ｘＰ、およびマスター鍵ｓを使用し、ｇ＝ｅ＾（ｒＰ，ｓ（ｘＰ））を評価することよりメッセージ鍵を計算することが可能である。この実施形態では、対称双線形写像$e\hat{} : \bigstar G_1 \times \bigstar G_1 \rightarrow \bigstar G_2$を使用することに注意されたい。

【００３４】

本発明のいくつかの実施形態では、$\bigstar G_1$は楕円曲線の部分群であり、認容写像ｅ＾は楕

円曲線上のＷｅｉｌペアリング（またはＴａｔｅペアリング）から構成される。（ただし、定義より、部分群は、必ずしも、群よりも小さいわけではないことに留意されたい。つまり、★$Ｇ_1$は楕円曲線全体の場合もあるということである。）より一般的には、★$Ｇ_1$をアーベル多様体とし、ｅ＾を★$Ｇ_1$の要素の認容的ペアリングとすることができる。★$Ｇ_0$および★$Ｇ_1$が異なるものとして写像ｅ＾：★$Ｇ_0$×★$Ｇ_1$→★$Ｇ_2$を使用するいくつかの実施形態では、★$Ｇ_0$はさらに、楕円曲線の部分群、つまりアーベル多様体であってもよい。

【００３５】

他の実施形態では、ＩＤベース暗号化のさまざまな新規性のある応用が考えられる。他の種類の公開識別子、または機能強化された公開識別子を使用することによりＩＢＥシステムの新しい有用な応用が可能である。例えば、公開識別子ＩＤは個人に関連付けられた識別子に限られず、個人だけでなく組織、政府機関、企業などのあらゆる種類のエンティティと関連付けられた識別子であってもよい。また、グループを形成する個々のアイデンティティから自然の組み合わせにより、対応するグループ秘密鍵を備えるグループのジョイント・アイデンティティが得られることにも注意されたい。グループの秘密鍵は、ＰＫＧによって発行される必要はなく、単に、グループを構成する別々の秘密鍵の組み合わせである。エンティティのアイデンティティを指定する基本ＩＤは、名前、電子メール・アドレス、住所、またはエンティティの社会保障番号に限られず、ドメイン名、ＵＲＬ、９ケタ郵便番号、納税者番号など他の種類の情報を含めることもできることにも注意しなければならない。多くの応用では、公開識別子ＩＤは、特定のエンティティまたはエンティティの集まりに一意に関連付けられる一般に知られている何らかの文字列を含む。しかし、一般的に、公開識別子ＩＤは、任意の文字列またはその他の任意の情報とすることが可能である。

【００３６】

ＩＢＥのさまざまな有用な応用では、機能強化された公開識別子を利用する。機能強化された識別子は、必ずしも、特定のエンティティの独自性を指定する情報に限られない情報を含む一種の識別子とすることができる。例えば、ＩＤは、エンティティに関連付けられたライセンス番号、肩書き、または機密取扱資格などの信任状記述子を含めることが可能である。機関は、機関が証明するエンティティにのみ秘密鍵を与えることにより信任状を管理することが可能である。一実施例では、ＩＤに、連続番号、車両識別番号、特許番号などの所有物記述子を含めることが可能である。資産所有者の登録および所有者の認証を担当する機関は、その機関によって真の所有者であるとして登録されるエンティティにのみ秘密鍵を与えることにより資産登録を管理することが可能である。より一般的に、２つまたはそれ以上の物事の間の関連は、ＩＤにその識別子を含めることにより管理することが可能である。その後、ＰＫＧは、物事の間の関連付けに対する管理権限を有するものとして機能する。

【００３７】

他の種類の機能強化されたＩＤとして、時刻、時間間隔、または１組の時間間隔を含む識別子がある。このような識別子に対する秘密鍵は、ある時刻になると自動的に期限切れになるように、ある時間の経過後にのみ自動的にアクティブ状態になるように、または１つ以上の指定された時間間隔についてのみ有効となるように構成することが可能である。この手法を信任状および所有権管理と組み合わせることにより、アクティブ化および／または期限切れの時間を制御することが可能である。

【００３８】

上記の例から、本発明によるＩＤベース暗号化システムは特定の種類の識別子に限られないことは明白である。したがって、「ＩＤベース」という用語は、任意の文字列またはその他の任意の情報を基盤として使用できることを示すものとして一般的に理解すべきである。

【００３９】

他の実施形態によれば、ＩＢＥシステムを使用することで解読機能を委託することができ

る。エンティティは、自分の秘密マスター鍵を使って自分のＩＢＥシステムを設定し、このＩＢＥシステムに対してＰＫＧの役割を担うことが可能である。エンティティにはマスター鍵があるため、エンティティは鍵を発行することで、解読機能を他のエンティティに委託することが可能である。例えば、エンティティが企業であれば、その従業員は企業ＰＫＧから秘密鍵を取得することが可能である。個人に対し、その名前、肩書き、責務、プロジェクト、事例、または職務関係の識別子と一致する秘密鍵を発行することが可能である。他の例では、個人が業務出張時のみ有効な秘密鍵をラップトップに対して発行することが可能である。ラップトップの紛失または盗難が発生した場合でも、その期間の鍵しか損なわれない。マスター鍵は、家に保存しておくため、損なわれることはない。

【００４０】

また、通信の媒体は電子メールまたはインターネットに限られる必要はなく、印刷された刊行物、デジタル記録媒体、ラジオ放送、無線通信などの通信媒体も考えられる。

定義

ＩＤベース暗号化。ＩＤベース暗号化システムおよびその方法＄ｅの実施例では、Ｓｅｔｕｐ、Ｅｘｔｒａｃｔ、Ｅｎｃｒｙｐｔ、Ｄｅｃｒｙｐｔの４つのランダム・アルゴリズムを使用する。

【００４１】

Ｓｅｔｕｐ：秘匿性パラメータｋが与えられた場合、ｐａｒａｍｓ（システム・パラメータ）およびｍａｓｔｅｒ－ｋｅｙを返す。このシステム・パラメータは、有限メッセージ空間＄Ｍの説明および有限暗号文空間＄Ｃの説明を含む。通常、システム・パラメータは、周知であるが、ｍａｓｔｅｒ－ｋｅｙは個人鍵作成器（ＰＫＧ）にのみ公開される。

【００４２】

Ｅｘｔｒａｃｔ：入力として、ｐａｒａｍｓ、ｍａｓｔｅｒ－ｋｅｙ、および任意のＩＤ∈｛０，１｝*を受け取り、秘密鍵ｄを返す。ここで、ＩＤは公開鍵として使用される任意の文字列であり、ｄは対応する秘密解読鍵である。Ｅｘｔｒａｃｔアルゴリズムは、与えられた公開鍵から秘密鍵を抽出する。抽出にはｍａｓｔｅｒ－ｋｅｙが必要なため、通常は、ＰＫＧによって抽出が実行される。

【００４３】

Ｅｎｃｒｙｐｔ：入力として、ｐａｒａｍｓ、ＩＤ、およびＭ∈＄Ｍを受け取る。暗号文Ｃ∈＄Ｃを返す。

Ｄｅｃｒｙｐｔ：入力として、ｐａｒａｍｓ、Ｃ∈＄Ｃ、および秘密鍵ｄを受け取る。Ｍ∈＄Ｍを返す。

【００４４】

本発明の一実施形態によれば、これらのアルゴリズムは、暗号化されたメッセージが解読により忠実に復元されることを保証する標準の一貫性制約を充足する。より具体的には、ｄがアルゴリズムＥｘｔｒａｃｔによって作成された秘密鍵である場合、公開鍵としてＩＤが与えられると以下の式が成り立つ。

【００４５】

∀Ｍ∈＄Ｍ：Ｄｅｃｒｙｐｔ（ｐａｒａｍｓ，Ｃ，ｄ）＝Ｍ　ただし、Ｃ＝Ｅｎｃｒｙｐｔ（ｐａｒａｍｓ，ＩＤ，Ｍ）。

本発明の一実施形態によるＩＤベース暗号システムでは、図１に示されているように、上記のアルゴリズムが一緒に使用される。送信者１００はＥｎｃｒｙｐｔを使用し、受信者１１０はＤｅｃｒｙｐｔを使用し、ＰＫＧ　１２０はＳｅｔｕｐとＥｘｔｒａｃｔを使用する。メッセージＭを受信者１１０に送信するために、送信者１００は受信者のＩＤ（例えば、受信者の電子メール・アドレス）を取得し、無作為に選択した整数ｒと組み合わせて秘密メッセージ鍵$g^{r}{}_{ID}$を計算する。要素ｒＰが受信者１１０に送信されると、受信者１１０はその要素を秘密鍵d_{ID}と組み合わせて、同じメッセージ鍵$g^{r}{}_{ID}$を決定する。送信者および受信者は秘密メッセージ鍵を共有しているため、送信者によりこの鍵で暗号化されたメッセージは、受信者側で解読することが可能である。特に、送信者はＭをメッセージ鍵で暗号化し、暗号文Ｖを作成して、ｒＰとともに受信者に伝達する。そこで

、受信者は、秘密メッセージ鍵を使用して、暗号文を解読し、元のメッセージを復元する。しかし、メッセージを解読するために、受信者１１０は最初に、ＰＫＧ　１２０から秘密鍵d_{ID}を取得しておかなければならない。ＰＫＧが受信者のアイデンティティを認証した後、受信者に、受信者のＩＤに対応する秘密鍵を供給する。（ただし、この実施形態では、ＰＫＧはシステム内で任意の秘密鍵を計算することが可能であり、したがって、システム内で任意のユーザへの任意のメッセージを解読することが可能であることに注意されたい。）

選択暗号文の秘匿性。選択暗号文の秘匿性（ＩＮＤ－ＣＣＡ）は、公開鍵暗号化方式の秘匿性の標準的な受け入れられる概念である。ＩＤベース暗号化システムおよび方法の実施形態は、この秘匿性という強力な概念を充足するように実装することができる。さらに、選択暗号文の秘匿性の選択されたレベルを少し強化することができる。なぜなら、敵対者がＩＤベース・システム内の公開鍵ＩＤに攻撃をしかけたときに、敵対者はすでに自分が選択したユーザ$ID_1, \ldots, ID_n$の秘密鍵を所有しているおそれがあるからである。本発明の一実施形態では、システムはこのような攻撃にさらされても秘匿性を保持する。つまり、本システムは、敵対者が自分の選択したアイデンティティID_iに関連する秘密鍵（攻撃されている公開鍵ＩＤ以外）を取得することが可能な場合であっても秘匿性を保持するということである。このようなクエリを秘密鍵抽出クエリと呼ぶ。さらにこの実施形態のシステムは、敵対者が自分の選んだ公開鍵ＩＤについてチャレンジを受けたとしても、秘匿性を保持する（ランダム公開鍵とは反対に）。

【００４６】

以下のＩＮＤ－ＩＤ－ＣＣＡゲームにおいてチャレンジャに対する無視できない優位性を持つ多項式有界敵対者＄Ａがいない場合、ＩＤベース暗号化システムまたは方法＄ｅの実施形態は、適応的選択暗号文攻撃に対する意味秘匿性（ＩＮＤ－ＩＤ－ＣＣＡ）があるという。

【００４７】

Ｓｅｔｕｐ：チャレンジャは、秘匿性パラメータｋを受け取り、Ｓｅｔｕｐアルゴリズムを実行する。これにより、敵対者は、その結果のシステム・パラメータｐａｒａｍｓが与えられる。このアルゴリズムは、マスターキー（ｍａｓｔｅｒ－ｋｅｙ）をそれ自身に保持する。

【００４８】

段階１：敵対者は、クエリ$q_1, \ldots, q_m$を発行するが、クエリq_iは以下のうちの１つである。

－　抽出クエリ＜ID_i＞。チャレンジャは、アルゴリズムＥｘｔｒａｃｔを実行し公開鍵＜ID_i＞に対応する秘密鍵d_iを作成することにより応答する。d_iを敵対者に送信する。

【００４９】

－解読クエリ＜ID_i, C_i＞。チャレンジャは、アルゴリズムＥｘｔｒａｃｔを実行しID_iに対応する秘密鍵d_iを作成することにより応答する。次に、アルゴリズムＤｅｃｒｙｐｔを実行し、秘密鍵d_iを使用して暗号文C_iを解読する。これは、その結果の平文を敵対者に送信する。

【００５０】

これらのクエリは状況に応じて行われる、つまり、各クエリq_iは$q_1, \ldots, q_{i-1}$への返信に依存する。

チャレンジ：敵対者は、段階１が終了したと判断すると、長さの等しい２つの平文M_0、$M_1 \in \$M$、およびチャレンジの際のアイデンティティＩＤを出力する。唯一の制約は、ＩＤが段階１で秘密鍵抽出クエリ内に出現していなかったという点である。

【００５１】

チャレンジャは、ランダム・ビット$b \in \{0, 1\}$を選択し、Ｃ＝Ｅｎｃｒｙｐｔ（ｐａｒａｍｓ、ＩＤ，M_b）を設定する。敵対者へのチャレンジとしてＣを送信する。

段階２：敵対者は、さらにクエリ$q_{m+1}, \ldots, q_n$を発行し、クエリq_iは以下の

うちの１つである。
【００５２】
－　抽出クエリ＜ＩＤ$_i$＞、ただし、ＩＤ$_i$≠ＩＤ。チャレンジャは、段階１と同じように応答する。
－　解読クエリ＜ＩＤ$_i$，Ｃ$_i$＞≠＜ＩＤ，Ｃ＞。チャレンジャは、段階１と同じように応答する。
【００５３】
これらのクエリは、段階１のように状況に応じて行うことができる。
推測：最後に、敵対者は推測ｂ’∈｛０，１｝を出力する。ｂ＝ｂ’であれば、敵対者がゲームの勝利者である。
【００５４】
このような敵対者＄ＡをＩＮＤ－ＩＤ－ＣＣＡ敵対者と呼ぶ。方式＄Ｅを攻撃する際の敵対者＄Ａの優位性を秘匿性パラメータｋの以下のような関数として定義する（ｋは、チャレンジャへの入力として与えられる）。
【００５５】
【数１】

$$\mathrm{Adv}_{\mathcal{E},\mathcal{A}}(k) = \left|\Pr[b = b'] - \frac{1}{2}\right|.$$

この確率は、チャレンジャと敵対者によって使用されるランダム・ビット上の確率である。
【００５６】
ＩＮＤ－ＩＤ－ＣＣＡゲームを使用して、ＩＢＥ方式の選択暗号文秘匿性を定義することが可能である。通常のように、関数ｇ：★Ｒ→★Ｒは、ｇ（ｋ）が任意の多項式ｆについて１／ｆ（ｋ）よりも小さい場合に、無視できるという。
【００５７】
定義１　ＩＢＥシステム＄ｅは、任意の多項式時間ＩＮＤ－ＩＤ－ＣＣＡ敵対者＄Ａについて関数Ａｄｖ＄ｅ，＄Ａ（ｋ）が無視できる場合に、適応的選択暗号文攻撃に対する意味秘匿性を有するという。簡単に、＄ｅはＩＮＤ－ＩＤ－ＣＣＡ秘匿性があるという。
【００５８】
ただし、選択暗号文秘匿性（ＩＮＤ－ＣＣＡ）の標準的定義は、秘密鍵抽出クエリがないことを除き上述と同じであり、敵対者はランダム公開鍵（自分の選択した公開鍵ではなく）に基づいてチャレンジを受けることに注意されたい。秘密鍵抽出クエリは、マルチユーザ設定での選択暗号文秘匿性の定義に関係している。結局、この定義は、複数ユーザに属す複数の公開鍵を必要とする。マルチユーザＩＮＤ－ＣＣＡは、標準ハイブリッド引数を使用してシングル・ユーザＩＮＤ－ＣＣＡに簡約可能と考えられる。これは、ＩＤベース設定ＩＮＤ－ＩＤ－ＣＣＡでは成立しないが、それは、敵対者が攻撃中に壊れる公開鍵を選択するようになるからである。秘密鍵抽出クエリが重要であることを強調するために、開示されているＩＢＥシステムの１実装を（ハッシュ関数の１つを除去することにより）修正して、秘密鍵抽出クエリが禁止される場合に選択暗号文秘匿性を有するシステムに導入することが可能であることを指摘しておく。しかし、この実装は、抽出クエリが許される場合には秘匿性がない。
【００５９】
意味秘匿ＩＤベース暗号化。このＩＢＥシステムの実装の秘匿性の証明では、意味（ｓｅｍａｎｔｉｃ）秘匿（選択平文攻撃に対する意味秘匿性とも呼ばれる）と呼ばれる秘匿性の弱い概念を利用する。意味秘匿は、敵対者に対する制限が強いことを除いて選択暗号文秘匿（ＩＮＤ－ＩＤ－ＣＣＡ）に類似しており、チャレンジ公開鍵を攻撃している間は、解読クエリを発行し得ない。標準公開鍵システム（ＩＤベース・システムではなく）では、意味秘匿は、（１）チャレンジャによって作成されたランダム公開鍵を敵対者に与え、

（２）敵対者は長さの等しい２つのメッセージM_0およびM_1を出力し、｛０，１｝でランダムに選択したｂについてチャレンジャからM_bの暗号化を受け取り、（３）敵対者はｂ’を出力し、ｂ＝ｂ’であれば敵対者が勝利するというゲームを使用して定義される。公開鍵システムは、多項式時間の敵対者が無視できない優位性でゲームに勝利する可能性がない場合に意味秘匿であるという。簡単に、意味秘匿公開鍵はＩＮＤ－ＣＰＡ秘匿性があるという。意味秘匿性には、暗号文が与えられると、敵対者は対応する平文に関して何も情報を得られないという我々の直観に訴えかけるところがある。

【００６０】

ＩＤベース・システムの意味秘匿（ＩＮＤ－ＩＤ－ＣＰＡと表す）を定義するために、敵対者が選択秘密鍵抽出クエリを発行することを許すことにより、標準定義を強化する。同様に、敵対者は、自分の選択した公開鍵ＩＤに関してチャレンジを受ける。ここで、ＩＮＤ－ＩＤ－ＣＰＡゲームを使用してＩＤベース暗号化方式の意味秘匿を定義する。ゲームは、敵対者は解読クエリを実行し得ないという点を除き上で定義したＩＮＤ－ＩＤ－ＣＣＡゲームと同じである。敵対者は、秘密鍵抽出クエリを実行するしかない。以下のＩＮＤ－ＩＤ－ＣＰＡゲームにおいてチャレンジャに対する無視できない優位性を持つ多項式制限敵対者＄Ａがいない場合、ＩＤベース暗号化方式＄ｅは、意味秘匿性（ＩＮＤ－ＩＤ－ＣＰＡ）があるという。

【００６１】

Ｓｅｔｕｐ：チャレンジャは、秘匿性パラメータｋを受け取り、Ｓｅｔｕｐアルゴリズムを実行する。これにより、敵対者は、その結果のシステム・パラメータｐａｒａｍｓが与えられる。このアルゴリズムは、ｍａｓｔｅｒ－ｋｅｙをそれ自身に留める。

【００６２】

段階１：敵対者は、秘密鍵抽出クエリID_1，．．．，ID_mを発行する。チャレンジャは、アルゴリズムＥｘｔｒａｃｔを実行し公開鍵ID_iに対応する秘密鍵d_iを作成することにより応答する。d_iを敵対者に送信する。これらのクエリは状況に応じて実行することができる。

【００６３】

チャレンジ：敵対者は、段階１が終了したと判断すると、長さの等しい２つの平文M_0、$M_1 \in$＄Ｍ、およびチャレンジの際の公開鍵ＩＤを出力する。唯一の制約は、ＩＤが段階１で秘密鍵抽出クエリ内に出現していなかったという点である。チャレンジャは、ランダム・ビットｂ∈｛０，１｝を選択し、Ｃ＝Ｅｎｃｒｙｐｔ（ｐａｒａｍｓ、ＩＤ，M_b）を設定する。敵対者へのチャレンジとしてＣを送信する。

【００６４】

段階２：敵対者は、さらに抽出クエリID_{m+1}，．．．，ID_nを発行する。唯一の制約は、ＩＤｉ≠ＩＤである。チャレンジャは、段階１と同じように応答する。

推測：最後に、敵対者は推測ｂ’∈｛０，１｝を出力する。ｂ＝ｂ’であれば、敵対者がゲームの勝利者である。

【００６５】

このような敵対者＄ＡをＩＮＤ－ＩＤ－ＣＰＡ敵対者と呼ぶ。上で行ったように、方式＄ｅに対するＩＮＤ－ＩＤ－ＣＰＡ敵対者＄Ａの優位性は、秘匿性パラメータｋの以下の関数である。

【００６６】

【数２】

$$\mathrm{Adv}_{\mathcal{E},\mathcal{A}}(k) = \left|\Pr[b = b'] - \frac{1}{2}\right|.$$

この確率は、チャレンジャと敵対者によって使用されるランダム・ビット上の確率である。

【００６７】

定義２　ＩＢＥシステム＄ｅは、任意の多項式時間ＩＮＤ－ＩＤ－ＣＰＡ敵対者＄Ａについて関数Ａｄｖ＄ｅ，＄Ａ（ｋ）が無視できる場合に、意味秘匿であるという。簡単に、＄ｅはＩＮＤ－ＩＤ－ＣＰＡ秘匿性があるという。

【００６８】

一方向ＩＤベース暗号化。一方向暗号化（ＯＷＥ）と呼ばれる秘匿性の更に弱い概念を定義することが可能である。大まかにいうと、公開鍵暗号化方式は、ランダム平文の暗号化が与えられたときに、敵対者がその平文をそのまま出力し得ない場合に一方向暗号化である。敵対者が例えば平文のビットの半分を学習するのを妨げるものがないため、一方向暗号化は秘匿性の弱い概念である。したがって、一方向暗号化方式は、一般的に秘匿性のある暗号化を実現しない。ランダム・オラクル・モデルでは、セッション鍵の暗号化に一方向暗号化方式を使用することが可能である（セッション鍵は、平文のハッシュとみなされる）。秘密鍵抽出クエリを定義に加えることにより一方向暗号化の概念をＩＤベース・システムに拡張することが可能であることを注意しておく。秘匿性の最も弱い概念として意味秘匿を使用するため、ここでは完全な定義を掲載しない。

【００６９】

双線形写像および双線形ＤＩＦＦＩＥ－ＨＥＬＭＡＮ仮定

本発明の一実施形態は、ある大きな素数ｑについて位数ｑの群$★G_1$と$★G_2$との間の写像ｅ＾：$★G_1 \times ★G_1 \rightarrow ★G_2$を使用するＩＢＥシステムを対象とする。写像ｅ＾は、以下の特性を満たす場合に認容写像と呼ぶことができる。

【００７０】

１．双線形：写像ｅ＾：$★G_1 \times ★G_1 \rightarrow ★G_2$は、すべての（Ｐ，Ｑ）$\in ★G_1 \times ★G_1$およびすべてのａ，ｂ$\in ★Z$について、ｅ＾（ａＰ，ｂＱ）＝ｅ＾（Ｐ，Ｑ）^{ab}を満たす。

【００７１】

２．非退化：この写像は、$★G_1 \times ★G_1$内のすべての対を$★G_2$内の単位要素に対応させない。$★G_1$、$★G_1$、$★G_2$は素数位数の群なので、これは、$★G_1 = ★G_1$およびＰが$★G_1 = ★G_1$の作成要素であれば、ｅ＾（Ｐ，Ｐ）は$★G_2$の作成要素であることを意味していることがわかる。

【００７２】

３．計算可能：任意の（Ｐ，Ｑ）$\in ★G_1 \times ★G_1$についてｅ＾（Ｐ，Ｑ）を計算する効率のよいアルゴリズムが存在する。

実施形態の多くは、写像ｅ＾：$★G_1 \times ★G_1 \rightarrow ★G_2$を参照して説明されているが、これは、本発明の実施形態で使用されている双線形写像の特定の場合にすぎない。より一般的には、写像ｅ＾：$★G_0 \times ★G_1 \rightarrow ★G_2$を使用することができ、$★G_0$および$★G_1$は異なっていてもよい。しかし、説明を簡単にするため、実施形態の多くは、$★G_1$および$★G_1$が同じである場合について主に詳述しており、この群は両方とも$★G_1$で表される。以下では、群$★G_1$、$★G_2$およびそれらの間の認容写像を使用する詳細な実施例を取りあげる。この実施例では、群$★G_1$は、楕円曲線Ｅ／$★F_p$の点の加法群の部分群であり、群$★G_2$は、有限体$★F^*$■の乗法群の部分群である。以下のＩＢＥシステムの詳細な例からわかるように、Ｗｅｉｌペアリング（それ自体は認容写像でない）を使用して、これら２つの群の間の認容写像を構成することが可能である。

【００７３】

上で述べたように認容写像ｅ＾：$★G_1 \times ★G_1 \rightarrow ★G_2$が存在することで、これらの群に対し２通りの意味が生じる。

ＭＯＶ帰着：$★G_1$における離散対数問題は$★G_2$における離散対数問題よりも困難ではない。これを見るために、Ｐ，Ｑ$\in ★G_1$を$★G_1$における離散対数問題の実例とし、Ｐ、Ｑは両方とも位数ｑであるとする。Ｑ＝αＰとなるような$\alpha \in ★Z_q$を見つけたい。ｇ＝ｅ＾（Ｐ，Ｐ）およびｈ＝ｅ＾（Ｑ，Ｐ）とする。そこで、ｅ＾の双線形性により、$h = g^{\alpha}$であることがわかる。ｅ＾が非退化であることから、ｇ、ｈは両方とも$★G_2$において位数ｑである。したがって、$★G_1$における離散対数問題は、$★G_2$における離散対

数問題に帰着した。よって、離散対数が★G_1において困難であるためには、離散対数が★G_2において困難であるように秘匿性パラメータを選択しなければならない。

【００７４】

決定Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎは容易である：★G_1における決定Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎ問題（ＤＤＨ）は、分布＜Ｐ，ａＰ，ｂＰ，ａｂＰ＞と＜Ｐ，ａＰ，ｂＰ，ｃＰ＞とを区別する問題であり、ａ、ｂ、ｃは★Z_qにおいてランダムであり、Ｐは★G_1においてランダムである。★G_1におけるＤＤＨが容易であることを見るために、Ｐ、ａＰ、ｂＰ、ｃＰ∈★G^*_1が与えられた場合、以下の式が成り立つことに注意する。

【００７５】

ｃ＝ａｂ　ｍｏｄ　ｑ　＜＝＝＞　ｅ＾（Ｐ，ｃＰ）＝ｅ＾（ａＰ，ｂＰ）

★G_1における計算Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎ問題（ＣＤＨ）は、それでも、困難である可能性がある（★G_1におけるＣＤＨはランダムな＜Ｐ，ａＰ，ｂＰ＞が与えられた場合にａｂＰを見つけることである）。実施例では、★G_1におけるＤＤＨが容易であるとしても★G_1におけるＣＤＨは困難であると考えられる場合に、写像ｅ＾：★G_1×★G_1→★G_2を使用することができる。

【００７６】

双線形Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎ仮定（ＢＤＨ）

★G_1における決定Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎ問題（ＤＤＨ）は容易なので、本発明の実施形態ではその群で暗号システムを構築するのにＤＤＨを使用しない。その代わりに、このＩＢＥシステムの実施形態の秘匿性は、双線形Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎ仮定（ＢＤＨ）と呼ばれる計算Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎ仮定の新規性のある変種に基づく。

【００７７】

双線形Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎ問題。★G_1、★G_2を素数位数ｑの２つの群とする。ｅ＾：★G_1×★G_1→★G_2を認容写像とし、Ｐを★G_1の作成要素とする。＜★G_1，★G_2，ｅ＾＞のＢＤＨ問題は以下のとおりである。あるａ、ｂ、ｃ∈★Z^*_qについて＜Ｐ，ａＰ，ｂＰ，ｃＰ＞が与えられたとして、Ｗ＝ｅ＾（Ｐ，Ｐ）^{abc}∈★G_2を計算する。アルゴリズム＄Ａには、以下の場合に、＜★G_1，★G_2，ｅ＾＞におけるＢＤＨを解く上で優位性＄ｅがある。

【００７８】

Ｐｒ［＄Ａ（Ｐ，ａＰ，ｂＰ，ｃＰ）＝ｅ＾（Ｐ，Ｐ）^{abc}］≧ε

ただし、この確率は★Z^*_qにおけるａ，ｂ，ｃのランダムな選択、Ｐ∈★G^*_1のランダムな選択、および＄Ａのランダム・ビットについてのものである。

【００７９】

ＢＤＨパラメータ作成要素。ランダム・アルゴリズム＄ｇは、（１）＄ｇが秘匿性パラメータｋ∈★Z^+を受け取り、（２）＄ｇがｋの多項式時間で実行され、（３）＄ｇは素数ｑ、位数ｑの２つの群★G_1、★G_2の説明および許容写像ｅ＾：★G_1×★G_1→★G_2の説明を出力する場合に、ＢＤＨパラメータ作成要素であるという。＄ｇの出力を＄ｇ（１ｋ）＝＜ｑ，★G_1，★G_2，ｅ＾＞で表す。秘匿性パラメータｋは、ｑのサイズを決定する場合に使用され、例えば、ｑをランダムなｋビット素数とみなすことも可能である。ｉ＝１，２について、群★G_iの説明に、★G_iにおける群作用を計算するための多項式時間（ｋにおける）アルゴリズムが含まれる、★G_iの作成要素が含まれると仮定する。★G_iの作成要素により、★G_iに一様にランダムな要素を作成することができる。同様に、ｅ＾の説明に、ｅ＾を計算するための多項式時間アルゴリズムが含まれると仮定する。Ｗｅｉｌペアリングを使用するＩＢＥシステムの以下の詳細な例では、ＢＤＨパラメータ作成要素の例を挙げる。

【００８０】

双線形Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎ仮定。＄ｇをＢＤＨパラメータ作成要素とする。アルゴリズム＄Ａは、十分に大きなｋについて以下の式が成り立つ場合に、ＢＤＨ問題を解く際に優位性ε（ｋ）を有するという。

【００８１】
【数３】

$$\mathrm{Adv}_{\mathcal{G},\mathcal{A}}(k) = \Pr\left[\mathcal{A}(q,\mathbb{G}_1,\mathbb{G}_2,\hat{e},P,aP,bP,cP) = \hat{e}(P,P)^{abc} \;\middle|\; \begin{array}{l}\langle q,\mathbb{G}_1,\mathbb{G}_2,\hat{e}\rangle \leftarrow \mathcal{G}(1^k),\\ P \leftarrow \mathbb{G}_1^*,\ a,b,c \leftarrow \mathbb{Z}_q^*\end{array}\right] > \epsilon(k$$

任意のランダム多項式時間（ｋにおいて）アルゴリズムおよび任意の多項式ｆ∈★Ｚ［ｘ］アルゴリズムについて＄Ａは高々１／ｆ（ｋ）の優位性でＢＤＨ問題を解く場合に、＄ｇはＢＤＨ仮定を満たすという。＄ｇがＢＤＨ仮定を満たす場合、ＢＤＨは、＄ｇによって作成された群において困難であるという。

【００８２】
ＩＢＥシステムの以下の詳細な例の説明では、ＢＤＨ仮定を満たすと思われるＢＤＨパラメータ作成要素の例をいくつか挙げる。
ＢＤＨの困難さ。ＢＤＨ問題と暗号で使用される他の困難な問題との関係を調べると興味深いことがわかる。現在、いえるのは、＜★Ｇ$_1$，★Ｇ$_2$，ｅ＾＞のＢＤＨ問題は★Ｇ$_1$または★Ｇ$_2$におけるＣＤＨ問題よりも困難ではないということである。つまり、★Ｇ$_1$または★Ｇ$_2$のＣＤＨのアルゴリズムは＜★Ｇ$_1$，★Ｇ$_2$，ｅ＾＞のＢＤＨを解くのに十分であるということである。今のところ、この逆、つまり、★Ｇ$_1$または★Ｇ$_2$でＣＤＨを解くのにＢＤＨのアルゴリズムは十分かという問題は未解決である。

【００８３】
以下のＩＢＥシステムの詳細な例では、認容写像によって誘導された★Ｇ$_1$から★Ｇ$_2$への同型写像は、一方向関数であると考えられることを注意しておく。より具体的には、点Ｑ∈★Ｇ$^*_1$について、ｆ$_Q$（Ｐ）＝ｅ＾（Ｐ，Ｑ）により同型写像ｆ$_Q$：★Ｇ$_1$→★Ｇ$_2$を定義する。これらの同型写像のどれか１つでも不可逆であることは判明すれば、ＢＤＨは＜★Ｇ$_1$，★Ｇ$_2$，ｅ＾＞において容易である。幸運なことに、ｆ$_Q$の逆を求める効率のよいアルゴリズムがあれば、群★Ｇ$_2$においてＤＤＨを決定する効率のよいアルゴリズムがあることがいえる。実施例では、ＤＤＨは群★Ｇ$_2$において困難であると考えられる。したがって、認容写像によって誘導された同型写像ｆ$_Q$：★Ｇ$_1$→★Ｇ$_2$は一方向関数であると考えられる。

【００８４】
ＩＤベース暗号化方式の例
以下の実施例について段階を追って説明する。まず、適応的選択暗号文攻撃に対して秘匿性がない基本的なＩＤベース暗号化システムと方法について説明する。後述の他の実施形態では、基本的な方式を拡張し、ランダム・オラクル・モデルにおいて適応的選択暗号文攻撃に対する秘匿性（ＩＮＤ－ＩＤ－ＣＣＡ）を有するようにする。後で、ハッシュ関数に対する要求条件を一部弱めて、他の実施形態を提示する。これらの実施形態については、ＢＤＨ仮定を満たすジェネリックなＢＤＨパラメータ作成要素を参照して説明する。後で、Ｗｅｉｌペアリングを使用するＩＢＥシステムの詳細な例を説明する。

【００８５】
ＢａｓｉｃＩｄｅｎｔ
ここでは、ＢａｓｉｃＩｄｅｎｔと呼ばれる基本的な実施形態について説明する。実施形態の説明では、Ｓｅｔｕｐ、Ｅｘｔｒａｃｔ、Ｅｎｃｒｙｐｔ、Ｄｅｃｒｙｐｔという４つのアルゴリズムを取りあげる。ｋをセットアップ・アルゴリズムに与えられる秘匿性パラメータとする。＄ｇをあるＢＤＨパラメータ作成要素とする。

【００８６】
Ｓｅｔｕｐ：秘匿性パラメータｋ∈★Ｚ$^+$が与えられると、基本的な実施形態のアルゴリズムは以下のようになる。
工程１：入力ｋに対して＄ｇを実行し、素数ｑ、位数ｑの２つの群★Ｇ$_1$、★Ｇ$_2$、および認容写像ｅ＾：★Ｇ$_1$×★Ｇ$_1$→★Ｇ$_2$を作成する。任意の作成要素Ｐ∈★Ｇ$_1$を選択

する。
【００８７】
工程２：ランダムなｓ∈★Ｚ$^{*}_{q}$を選び、P_{pub}＝ｓＰと設定する。
工程３：暗号ハッシュ関数H_1：｛０，１｝*→★Ｇ$^{*}_{1}$を選択する。あるｎについて、暗号ハッシュ関数H_2：★Ｇ$^{*}_{2}$→｛０，１｝^{n}を選択する。秘匿性解析により、H_1、H_2はランダム・オラクルとみなされる。
【００８８】
メッセージ空間は、＄Ｍ＝｛０，１｝^{n}である。暗号文空間は、＄Ｃ＝★Ｇ$^{*}_{1}$×｛０，１｝^{n}である。システム・パラメータは、ｐａｒａｍｓ＝＜ｑ，★G_1，★G_2，ｅ＾，ｎ，Ｐ，P_{pub}，H_1，H_2＞である。ｍａｓｔｅｒ－ｋｅｙは、ｓ∈★Ｚ$^{*}_{q}$である。
【００８９】
ＩＢＥシステムの実施形態を使用して、対称鍵を暗号化できるが、その場合、ｎを、例えば、１２８または２５６とすることができる。ｋについては、例えば、５１２または１０２４または２０４８を使用できる。
【００９０】
Ｅｘｔｒａｃｔ：与えられた２進数列ＩＤ∈｛０，１｝*について、基本的な実施形態のアルゴリズムは、（１）Q_{ID}＝H_1（ＩＤ）∈★Ｇ$^{*}_{1}$を計算し、（２）ｓをマスター鍵として、秘密鍵d_{ID}をd_{ID}＝ｓQ_{ID}となるように設定する。
【００９１】
Ｅｘｔｒａｃｔは、図２に示されているように、さまざまな実施形態におけるＰＫＧにより実行することができる。ＰＫＧは、ブロック２００でマスター鍵を取得し、ブロック２１０で公開識別子ＩＤを取得し、ブロック２２０でＩＤから公開鍵を計算し、ブロック２３０でマスター鍵と公開鍵から秘密鍵を計算する。ブロック２４０で、秘密鍵が、公開識別子ＩＤに関連付けられているエンティティに送られるが、これは通常、エンティティの素性が識別された後に行われる。
【００９２】
Ｅｎｃｒｙｐｔ：公開鍵ＩＤのもとでＭ∈＄Ｍを暗号化するために、（１）Q_{ID}＝H_1（ＩＤ）∈★Ｇ$^{*}_{1}$を計算し、（２）ランダムなｒ∈★Ｚ$^{*}_{q}$を選択し、（３）暗号文を以下のように設定する。
【００９３】
Ｃ＝＜ｒＰ，Ｍ○＋H_2（g^{r}_{ID}）＞　ただし、g_{ID}＝ｅ＾（Q_{ID}，P_{pub}）∈★Ｇ$^{*}_{2}$
基本的な実施形態では、メッセージの送信者は図３に示されているようにＥｎｃｒｙｐｔを実行することができる。ブロック３００で、システム・パラメータが取得される（ＰＫＧなどの外部リソース、またはすでに取得されていればローカルの記憶媒体から）。ブロック３１０で、受信者のＩＤが決定され、ブロック３２０で、対応する公開鍵がＩＤから計算される。その後、ブロック３３０で、秘密メッセージ鍵が計算され、ブロック３４０で、メッセージ鍵を使用して、メッセージが暗号化される。
【００９４】
Ｄｅｃｒｙｐｔ：Ｃ＝＜Ｕ，Ｖ＞∈＄Ｃを、公開鍵ＩＤを使用して暗号化された暗号文であるとする。秘密鍵d_{ID}∈★Ｇ$^{*}_{1}$を使用してＣを暗号化するために、以下を計算する。
【００９５】
Ｖ○＋H_2（ｅ＾（d_{ID}，Ｕ））＝Ｍ
基本的な実施形態では、受信者は、図４に示されているようにＤｅｃｒｙｐｔを実行することができる。ブロック４００で、システム・パラメータが取得される（ＰＫＧなどの外部リソース、またはすでに取得されていればローカルの記憶媒体から）。ブロック４１０で、送信者から暗号文Ｖおよび要素ｒＰを取得する。要素ｒＰは、送信者から得られた暗号文全体の一部と考えることができる。ブロック４２０で、受信者は、メッセージを暗号

化するために使用された公開識別子ＩＤに対応する秘密鍵d_{ID}を取得する。秘密鍵は、通常、ＰＫＧなどの外部リソース、またはすでに取得されていればローカルの記憶媒体から取得される。その後、ブロック４３０で、秘密メッセージ鍵が計算され、ブロック４４０で、これを使用して、メッセージが解読される。

【００９６】

これで、基本的な実施形態のＢａｓｉｃＩｄｅｎｔの説明は完了する。最初に整合性を確認する。すべてが上のように計算されると、

１．暗号化時に、Ｍとg^{r}_{ID}のハッシュとのビット排他ＯＲが計算される。

【００９７】

２．解読時に、Ｖとｅ＾（d_{ID}，Ｕ）のハッシュとのビット排他ＯＲが計算される。暗号化および解読時に使用されるこれらのマスクは、以下の式が成り立つため同じである。

【００９８】

ｅ＾（d_{ID}，Ｕ）＝ｅ＾（ｓQ_{ID}，ｒＰ）＝ｅ＾（Q_{ID}，Ｐ）^{sr}＝ｅ＾（Q_{ID}，P_{pub}）^{r}＝g^{r}_{ID}

したがって、暗号化の後に解読を適用すると、必要に応じてオリジナルのメッセージＭが出力される。ＢａｓｉｃＩｄｅｎｔの性能上の考慮事項については後述する。

【００９９】

秘匿性。次に、この基本的な実施形態の秘匿性について調べる。

システムの例の秘匿性は、★G_1における計算Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎ問題の一変種が困難であるという仮定に基づいている。暗号化方式の秘匿性の技術面の詳細については、発明者が（非特許文献２）で解説しており、本願明細書に援用する。

【０１００】

実施例では、システムの性能は★F^{*}_{p}におけるＥｌＧａｍａｌ暗号化の性能に匹敵している。システムの例の秘匿性は、計算Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎ仮定の一変種に基づいている。この仮定に基づき、システム例がランダム・オラクル・モデルにおいて選択暗号文秘匿性を有することを示す。分散ＰＫＧ実施形態によれば、閾値暗号化手法を使用することで、ＰＫＧを分散させ、ｍａｓｔｅｒ－ｋｅｙを１カ所だけで利用することをできなくすることが可能である。普通の閾値システムとは異なり、分散ＰＫＧ実施形態の堅牢性は免除されることを示す。

【０１０１】

システム例の秘匿性について論じるため、ＩＤベース暗号化の選択暗号文秘匿性を定義する。このモデルでは、敵対者に、選択暗号文秘匿性の標準モデルよりも大きな権限を与える。最初に、攻撃者が自分の選択した任意の公開鍵ＩＤを攻撃することを許す。次に、ＩＤに対し選択暗号文攻撃がしかけられている間に、攻撃者がＩＤの秘密鍵以外の、自分の選択した公開鍵をＰＫＧから取得することを許す。これにより、自分の選択したいくつかのＩＤに対応する複数の秘密鍵を取得し、自分の選択した他の何らかの公開鍵ＩＤを攻撃しようとする攻撃者のモデルが作成される。このようなクエリの手助けがあっても、システムの意味秘匿を破るという点での攻撃者の優位性がいぜんとして無視できるくらい小さいことが望ましい。

【０１０２】

以下の定理では、ＢＤＨが＄ｇによって作成される群において困難であると仮定して、ＢａｓｉｃＩｄｅｎｔが意味秘匿ＩＤベース暗号化方式（ＩＮＤ－ＩＤ－ＣＰＡ）であることを証明する。

【０１０３】

定理１　ハッシュ関数H_1、H_2はランダム・オラクルであると仮定する。そこで、ＢＤＨが＄ｇによって作成される群において困難であると仮定すると、ＢａｓｉｃＩｄｅｎｔは意味秘匿ＩＤベース暗号化方式（ＩＮＤ－ＩＤ－ＣＰＡ）である。具体的には、方式ＢａｓｉｃＩｄｅｎｔに対し優位性得ε（ｋ）を有するＩＮＤ－ＩＤ－ＣＰＡ敵対者＄Ａが存在すると仮定する。また、＄Ａが高々q_E＞０個の秘密鍵抽出クエリとH_2へのq_{H_2}＞０個のハッシュ・クエリを作成すると仮定する。すると、少なくとも以下の優位性を持

つ＄ｇによって作成された群においてＢＤＨを解くアルゴリズム＄Ｂが存在する。
【０１０４】
【数４】

$$Adv_{G,\mathcal{B}}(k) \geq \frac{2\epsilon(k)}{e(1+q_E)\cdot q_{H_2}}$$

ここで、ｅ～～２．７１は自然対数の底である。＄Ｂの実行時間のオーダーはＯ（ｔｉｍｅ（＄Ａ））である。
【０１０５】
この定理を証明するために、まずＢａｓｉｃＰｕｂと呼ばれる関連する公開鍵暗号化方式（ＩＤベース方式ではなく）を定義する。ＢａｓｉｃＰｕｂは、ｋｅｙｇｅｎ、ｅｎｃｒｙｐｔ、ｄｅｃｒｙｐｔの３つのアルゴリズムにより記述される。
【０１０６】
ｋｅｙｇｅｎ：秘匿性パラメータｋ∈★Z^+が与えられると、このアルゴリズムは以下のように実行される。
工程１：入力ｋに対して＄ｇを実行し、２つの素数位数の群★G_1、★G_2、および認容写像ｅ＾：★G_1×★G_1→★G_2を作成する。ｑを★G_1、★G_2の位数とする。任意の作成要素Ｐ∈★G_1を選択する。
【０１０７】
工程２：ランダムなｓ∈★Z^*_qを選び、P_{pub}＝ｓＰと設定する。ランダムなQ_{ID}∈★G^*_1を選ぶ。
工程３：あるｎについて、暗号ハッシュ関数H_2：★G_2→｛０，１｝^{n}を選択する。
【０１０８】
工程４：公開鍵は、＜ｑ，★G_1，★G_2，ｅ＾，ｎ，Ｐ，P_{pub}，H_1，H_2＞である。秘密鍵はd_{ID}＝ｓQ_{ID}∈★G^*_1である。
ｅｎｃｒｙｐｔ：Ｍ∈｛０，１｝^{n}を暗号化するために、ランダムなｒ∈★Z^*_qを選択し、暗号文を以下のように設定する。
【０１０９】
Ｃ＝＜ｒＰ，Ｍ○＋H_2（g^r）＞　ただし、ｇ＝ｅ＾（Q_{ID}，P_{pub}）∈★G^*_2
ｄｅｃｒｙｐｔ：Ｃ＝＜Ｕ，Ｖ＞を、公開鍵＜ｑ，★G_1，★G_2，ｅ＾，ｎ，Ｐ，P_{pub}，を使用して作成された暗号文であるとする。秘密鍵d_{ID}∈★G^*_1を使用してＣを解読するために、以下を計算する。
【０１１０】
Ｖ○＋H_2（ｅ＾（d_{ID}，Ｕ））＝Ｍ
これで、ＢａｓｉｃＰｕｂの説明は完了である。そこで、定理１を２段階で証明する。まず、ＢａｓｉｃＩｄｅｎｔに対するＩＮＤ－ＩＤ－ＣＰＡ攻撃はＢａｓｉｃＰｕｂに対するＩＮＤ－ＣＰＡ攻撃に変換することが可能であることを示す。この段階で、秘密鍵抽出クエリが敵対者を手助けしないことを示す。次に、ＢＤＨ仮定が成立する場合に、ＢａｓｉｃＰｕｂがＩＮＤ－ＣＰＡ秘匿性を有することを示す。これらの証明は略す。
【０１１１】
補助定理２　H_1を｛０，１｝*から★G^*_1へのランダム・オラクルとする。＄ＡをＢａｓｉｃＩｄｅｎｔに対し優位性得ε（ｋ）を有するＩＮＤ－ＩＤ－ＣＰＡ敵対者とする。＄Ａは高々q_E＞０個の秘密鍵抽出クエリを作成すると仮定する。すると、ＢａｓｉｃＰｕｂに対して少なくともε（ｋ）／ｅ（１＋q_E）の優位性を持つＩＮＤ－ＣＰＡ敵対者＄Ｂが存在する。この実行時間のオーダーはＯ（ｔｉｍｅ（＄Ａ））である。
【０１１２】
補助定理３　H_2を★G^*_2から｛０，１｝^{n}へのランダム・オラクルとする。＄ＡをＢａｓｉｃＰｕｂに対し優位性得ε（ｋ）を有するＩＮＤ－ＣＰＡ敵対者とする。＄ＡはＨ

$_{H2}$に対して合計$q_{H2}>0$個のクエリを作成する。すると、少なくとも$2\varepsilon(k)/q_{H2}$の優位性を有する$gに対するBDH問題を解くアルゴリズム$Bが存在し、実行時間のオーダーはO(time(A))である。

【0113】

定理1の証明。この定理は、直接補助定理3および補助定理3から導かれる。両方の帰結を書くと、優位性$\varepsilon(k)$を有するBasicIdentに対するIND-ID-CPA敵対者は、必要に応じて、少なくとも$2\varepsilon(k)/e(1+q_E)q_{H2}$の優位性を持つ$gに対するBDHアルゴリズムを与えることが示される。

【0114】

選択暗号文秘匿性のあるIDベース暗号化

本発明の一実施形態によれば、FujisakiおよびOkamotoの手法（本願明細書に援用する（非特許文献3）を参照）を適宜適合させ、前節のBasicIdent実施形態をランダム・オラクル・モデルにおけるIBEシステム（前で定義した意味において）の選択暗号文秘匿性実施形態に転換することができる。$eを確率論的公開的暗号方式とする。公開鍵pkのもとでランダム・ビットrを使用するMの暗号化を$$e_{pk}(M;r)$$で表す。Fujisaki-Okamotoは、ハイブリッド方式を以下のように定義する。

【0115】

$$e^{hy}{}_{pk}(M)=<e_{pk}(\sigma;H_3(\sigma,M)),H_4(\sigma)\bigcirc+M>$$

ここで、σはランダムに作成され、H_3、H_4は暗号ハッシュ関数である。Fujisaki-Okamotoは、$eが一方向暗号化方式であれば、$e^{hy}$はランダム・オラクル・モデルにおいて選択暗号秘匿性システム（IND-CCA）であることを示している（e_{pk}がいくつかの自然な制約を満たしていると仮定して）。ここで、意味秘匿は一方向暗号化を意味し、したがって、$eが意味秘匿（IND-CPA）であれば、Fujisaki-Okamotoの結果も適用されることを注意する。

【0116】

Fujisaki-Okamoto変換をBasicIdentに適用し、IBEシステムのその結果の実施形態がIND-ID-CCA秘匿性を有することを示す。FullIdentという以下のIBE実施形態を得る。ただし、nは暗号化するメッセージの長さであることに留意されたい。

【0117】

Setup：BasicIdent方式の場合と同様。さらに、ハッシュ関数$H_3:\{0,1\}^n\times\{0,1\}^n\rightarrow\bigstar Z^*_q$およびハッシュ関数$H_4:\{0,1\}^n\rightarrow\{0,1\}^n$を選ぶ。

【0118】

Extract：BasicIdent方式の場合と同様。

Encrypt：公開鍵IDのもとで$M\in\{0,1\}^n$を暗号化するために、（1）$Q_{ID}=H_1(ID)\in\bigstar G^*_1$を計算し、（2）ランダムな$\sigma\in\{0,1\}^n$を選択し、（3）$r=H_3(\sigma,M)$と設定し、（4）暗号文を以下のように設定する。

【0119】

$$C=<rP,\sigma\bigcirc+H_2(g^r{}_{ID}),M\bigcirc+H_4(\sigma)>$$ ただし、$g_{ID}=e\hat{}(Q_{ID},P_{pub})\in\bigstar G_2$

Decrypt：$C=<U,V,W>$を、公開鍵IDを使用して暗号化された暗号文であるとする。$U\in/\bigstar G^*_1$であればその暗号文を却下する。秘密鍵$d_{ID}\in\bigstar G^*_1$を使用してCを暗号化するために、以下を実行する。

【0120】

1．$V\bigcirc+H_2(e\hat{}(d_{ID},U))=\sigma$を計算する。

2．$W\bigcirc+H_4(\sigma))=M$を計算する。

3．$r=H_3(\sigma,M)$と設定する。$U=rP$であることを検査する。そうでなければ、その暗号文を却下する。

【０１２１】
４．ＭをＣの解読として出力する。
これで、ＦｕｌｌＩｎｄｅｎｔの説明は完了である。この実装は、図２、３、４に示されているＢａｓｉｃＩｄｅｎｔと同じ基本パターンに従う。Ｍは、Ｗ＝Ｍ○＋H_4（σ）として暗号化されることに注意されたい。これは、Ｗ＝E_{H4}（σ）（Ｍ）で置き換えられるが、ただし、Ｅは意味秘匿対称暗号化方式である。
【０１２２】
秘匿性。以下の定理では、ＢＤＨは＄ｇによって作成される群において困難であると仮定して、ＦｕｌｌＩｎｄｅｎｔは選択暗号文秘匿性のあるＩＢＥ（つまり、ＩＮＤ－ＩＤ－ＣＣＡ）であることを証明する。
【０１２３】
定理４　ハッシュ関数H_1、H_2、H_3、H_4はランダム・オラクルであるとする。すると、ＢＤＨが＄ｇによって作成される群において困難であると仮定すると、ＦｕｌｌＩｄｅｎｔは選択暗号文秘匿ＩＢＥ（ＩＮＤ－ＩＤ－ＣＣＡ）である。
【０１２４】
具体的には、方式ＦｕｌｌＩｄｅｎｔに対し優位性得ε（ｋ）を有するＩＮＤ－ＩＤ－ＣＣＡ敵対者＄Ａが存在すると仮定すると、＄Ａは高々ｔ（ｋ）の時間で実行される。また、＄Ａは高々q_E個の抽出クエリ、高々q_D個の解読クエリ、および高々q_{H2}、q_{H3}、q_{H4}個のクエリをハッシュ関数H_2、H_3、H_4に対してそれぞれ作成すると仮定する。すると、以下のような、実行時間がt_1（ｋ）である＄ｇに対するＢＤＨアルゴリズム＄Ｂが存在する。
【０１２５】
【数５】

$$Adv_{g,\mathcal{B}}(k) \geq 2FO_{adv}(\tfrac{\epsilon(k)}{e(1+q_E+q_D)}, q_{H_4}, q_{H_3}, q_D)/q_{H_2}$$
$$t_1(k) \leq FO_{time}(t(k), q_{H_4}, q_{H_3})$$

ただし、関数FO_{time}およびFO_{adv}は、定理５で定義されている。
定理４の証明は、ＦｕｊｉｓａｋｉとＯｋａｍｏｔｏの以下の結果に基づいている。ＢａｓｉｃＰｕｂ^{hy}は、Ｆｕｊｉｓａｋｉ－Ｏｋａｍｏｔｏ変換をＢａｓｉｃＰｕｂに適用した結果とする。
【０１２６】
定理５（Ｆｕｊｉｓａｋｉ－Ｏｋａｍｏｔｏ）　＄Ａは、ＢａｓｉｃＰｕｂ^{hy}を攻撃したときに優位性ε（ｋ）を得るＩＮＤ－ＣＣＡ敵対者であるものとする。＄Ａは実行時間ｔ（ｋ）が設定され、高々q_D個の解読クエリを作成し、および高々q_{H3}、q_{H4}個のクエリをハッシュ関数H_3、H_4に対して作成すると仮定する。すると、以下が成り立てば、実行時間t_1（ｋ）、優位性ε_1（ｋ）のＢａｓｉｃＰｕｂに対するＩＮＤ－ＣＰＡ敵対者＄Ｂが存在する。
【０１２７】
【数６】

$$\epsilon_1(k) \geq FO_{adv}(\epsilon(k), q_{H_4}, q_{H_3}, q_D) = \frac{1}{2(q_{H_4}+q_{H_3})}[(\epsilon(k)+1)(1-2/q)^{q_D}-1]$$
$$t_1(k) \leq FO_{time}(t(k), q_{H_4}, q_{H_3}) = t(k) + O((q_{H_4}+q_{H_3})\cdot n), \quad and$$

ここで、ｑは、群★G_1、★G_2のサイズであり、ｎはσの長さである。
実際には、Ｆｕｊｉｓａｋｉ－Ｏｋａｍｏｔｏは次のさらに強い結果を証明している。定理４の仮説のもとでは、ＢａｓｉｃＰｕｂ^{hy}は一方向暗号化方式ですらない。本発明の

目的に関しては、定理５の結果で十分である。定理４を証明するために、さらに、ＦｕｌｌＩｄｅｎｔに対するＩＮＤ－ＩＤ－ＣＣＡ選択暗号文攻撃とＢａｓｉｃＰｕｂ^{hy}に対するＩＮＤ－ＣＣＡ選択暗号文攻撃との間の変換に以下の補助定理が必要である。

【０１２８】

補助定理６　＄ＡをＦｕｌｌＩｄｅｎｔに対し優位性得ε（ｋ）を有するＩＮＤ－ＩＤ－ＣＣＡ敵対者とする。また、＄Ａが高々$q_E > 0$個の秘密鍵抽出クエリと$q_D > 0$個の解読クエリを作成すると仮定する。すると、ＢａｓｉｃＰｕｂ^{hy}に対し少なくとも

【０１２９】

【数７】

$$\frac{\epsilon(k)}{e(1+q_E+q_D)}$$

の優位性得を有するＩＮＤ－ＣＣＡ敵対者が存在する。この実行時間のオーダーはＯ（ｔｉｍｅ（＄Ａ））である。

【０１３０】

定理４の証明。補助定理６により、ＦｕｌｌＩｄｅｎｔに対するＩＮＤ－ＩＤ－ＣＣＡ敵対者ならば、ＢａｓｉｃＰｕｂ^{hy}に対するＩＮＤ－ＣＣＡ敵対者である。定理５から、ＢａｓｉｃＰｕｂ^{hy}に対するＩＮＤ－ＣＣＡ敵対者ならば、ＢａｓｉｃＰｕｂに対するＩＮＤ－ＣＰＡ敵対者である。補助定理３から、ＢａｓｉｃＰｕｂに対するＩＮＤ－ＣＰＡ敵対者ならば、ＢＤＨのアルゴリズムである。よって、必要条件が得られた。

【０１３１】

ハッシングの要求条件の緩和

前節のＩＢＥシステムは、ハッシュ関数$H_1 : \{0,1\}^* \rightarrow ★G^*_1$を使用していることに留意されたい。次節で述べるＩＢＥシステムの詳細な例では、$★G_1$を楕円曲線上の点のなす群の部分群として使用する。実際、このような群に直接ハッシュするハッシュ関数を構築することが困難な場合がある。１実施例では、したがって、$★G^*_1$の上へのハッシュの要求条件を緩和する方法を示す。$★G^*_1$の上へのハッシュではなく、ある集合$A \subseteq \{0,1\}^*$の上へのハッシュを行い、決定論的符号化関数を使用してＡを$★G^*_1$に写像する。

【０１３２】

認容符号化：$★G_1$を群とし、$A \in \{0,1\}^*$を有限集合とする。符号化関数Ｌ：Ａ→$★G^*_1$が以下の特性を満たす場合、この符号化関数は認容的であるという。

１．計算可能：任意のｘ∈Ａに対しＬ（ｘ）を計算する効率のよい決定論的アルゴリズムが存在する。

【０１３３】

２．＄ｌ対１：任意のｙ∈$★G^*_1$について、Ｌのもとでのｙのプリイメージのサイズはちょうど＄ｌである。つまり、すべてのｙ∈$★G^*_1$について｜L^{-1}（ｙ）｜＝＄ｌが成り立つ。これが成り立てば、｜Ａ｜＝＄ｌ・｜$★G^*_1$｜であることに注意されたい。

【０１３４】

３．サンプリング可能：＄Ｌ（ｓ）から任意のｙ∈$★G^*_1$に対するL^{-1}（ｙ）上の一様分布が得られるような効率のよいランダム・アルゴリズム$\$L_S$が存在する。つまり、＄Ｌ（ｓ）は$L^{-1}$（ｙ）の一様ランダム要素である。

【０１３５】

ＦｕｌｌＩｄｅｎｔを修正し、H_1をある集合Ａの中へのハッシュ関数で置き換えたＩＢＥシステムのＩＮＤ－ＩＤ－ＣＣＡ秘匿実施形態を得る。変更は比較的小さいため、この新しい方式をＦｕｌｌＩｄｅｎｔ’と呼ぶ。

【０１３６】

Ｓｅｔｕｐ：ＦｕｌｌＩｄｅｎｔ方式の場合と同様。唯一の違いは、H_1がハッシュ関数$H'_1：\{0,1\}^* \rightarrow$Ａで置き換えられていることである。システム・パラメータはさらに、認容的符号化関数Ｌ：Ａ→★G^*_1の記述も含む。

【０１３７】

Ｅｘｔｒａｃｔ，Ｅｎｃｒｙｐｔ：ＦｕｌｌＩｄｅｎｔ方式の場合と同様。唯一の違いは、工程１では、これらのアルゴリズムは$Q_{ID}=L(H'_1(ID))\in$★G^*_1を計算する点である。

【０１３８】

Ｄｅｃｒｙｐｔ：ＦｕｌｌＩｄｅｎｔ方式の場合と同様。

これで、ＦｕｌｌＩｎｄｅｎｔ’説明は完了である。以下の定理では、ＦｕｌｌＩｄｅｎｔを仮定して、ＦｕｌｌＩｎｄｅｎｔ’は選択暗号文秘匿性のあるＩＢＥ（つまり、ＩＮＤ－ＩＤ－ＣＣＡ）であることを証明する。

【０１３９】

定理７　$Ａを優位性得ε（ｋ）を満たすＦｕｌｌＩｄｅｎｔ’に対するＩＮＤ－ＩＤ－ＣＣＡ敵対者とする。$Ａは、ハッシュ関数$H'_1$への高々$q_{H_1}$個のクエリを作成するとする。そこで、同じ優位性ε（ｋ）が得られ、ｔｉｍｅ（$Ｂ）＝ｔｉｍｅ（$Ａ）＋q_{H_1}・ｔｉｍｅ（L_S）となるＦｕｌｌＩｄｅｎｔに対するＩＮＤ－ＩＤ－ＣＣＡ敵対者$Ｂが存在する。

【０１４０】

証明の概略　アルゴリズム$Ｂはアルゴリズム$Ａを実行することによりＦｕｌｌＩｄｅｎｔを攻撃する。これは、すべての解読クエリ、抽出クエリ、およびハッシュ・クエリを直接$Ａからチャレンジャに中継し、チャレンジャの応答を$Ａに中継して戻す。これは、$Ａがハッシュ・クエリを$H'_1$に発行した場合にのみ異なる挙動を示す。ただし、$Ｂは、ハッシュ関数$H_1：\{0,1\}^* \rightarrow$★$G^*_1$にのみアクセスできることに留意されたい。$H'_1$クエリに応答するため、後述のように、アルゴリズム$Ｂはタプル＜ID_j，y_j＞のリストを保持する。このリストを$(H'_1)^{list}$と呼ぶ。このリストは、最初は空である。$Ａが点$ID_i$でオラクル$H'_1$にクエリを実行すると、アルゴリズム$Ｂは以下のように応答する。

【０１４１】

１．クエリID_iがすでにタプル＜ID_i，y_i＞の$(H'_1)^{list}$上に出現していれば、$H'_1(ID_i)=y_i\in$Ａで応答する。

２．そうでなければ、$Ｂは$H_1(ID_i)$のクエリを発行する。例えば、$H_1(ID_i)=\alpha\in$★$G^*_1$である。

【０１４２】

３．$Ｂはサンプリング関数$$L_S(\alpha)$を実行して、ランダム要素$y\in L^{-1}(\alpha)$を作成する。

４．$Ｂは、タプル＜$ID_i$，ｙ＞を$(H')^{list}$に加え、$H'_1(ID_i)=y\in$Ａで$Ａに応答する。αは★G^*_1内に一様分布し、Ｌは$ｌ対１写像であるため、ｙは必要に応じてＡ内に一様分布することに注意されたい。

【０１４３】

Ｈ’１クエリを含む、$Ａのすべてのクエリへのアルゴリズム$Ｂの応答は、実際の攻撃における$Ａの見解と同じである。したがって、$Ｂは、チャレンジャでゲームに勝利する際のと同じ優位性ε（ｋ）を有する

Ｗｅｉｌペアリングを使用するＩＢＥシステムの詳細例

この節では、ＦｕｌｌＩｄｅｎｔ’を使用して、ＩＢＥシステムの一実施形態の詳細な例を説明する。この実施形態は、Ｗｅｉｌペアリングに基づく。実際にはＴａｔｅペアリングは計算量に関しては有利であり、さまざまな実施形態においてＷｅｉｌペアリングの代わりに使用できるが、比較すると単純なのでＷｅｉｌペアリングを使用する実装について最初に説明する。その後、Ｔａｔｅペアリングについて説明する。

【０１４４】

Ｗｅｉｌペアリングの特性
ｐ＞３を、ｐ＝２　ｍｏｄ　３を満たす素数とし、ｑをｐ＋１のある素因数とする。Ｅを、★Ｆ$_{p}$上の方程式ｙ^{2}＝ｘ^{3}＋１によって定義された楕円曲線とする。この曲線Ｅに関する初等的な事実をいくつか述べる。これ以降、Ｅ（★Ｆ△）は★Ｆ△上で定義されたＥの点からなる群を表すものとする。
【０１４５】
事実１：ｘ^{3}＋１は★Ｆ$_{p}$上の順列なので、したがって群Ｅ（★Ｆ$_{p}$）はｐ＋１個の点を含む。Ｏで無限遠の点を表す。Ｐ∈Ｅ（★Ｆ$_{p}$）を位数ｑの点とし、★Ｇ$_{1}$をＰによって作成される点のなす部分群とする。
【０１４６】
事実２：任意のｙ$_{0}$∈★Ｆ$_{p}$について、Ｅ（★Ｅ$_{p}$）上に一意の点（ｘ$_{0}$，ｙ$_{0}$）が存在する、つまり、ｘ$_{0}$＝（ｙ$_{0}$^{2}－１）$^{1/3}$∈★Ｆ$_{p}$である。したがって、（ｘ，ｙ）がＥ（★Ｆ$_{p}$）上のランダムなゼロでない点であれば、ｙは★Ｆ$_{p}$上で一様である。この特性を使って、単純な認容的符号化関数を作成する。
【０１４７】
事実３：１≠ζ∈★Ｆ■をｘ^{3}－１＝０　ｍｏｄ　ｐの解とする。すると、写像φ（ｘ，ｙ）＝（ζｘ，ｙ）は、曲線Ｅ上の点のなす群の自己同型写像となる。任意の点Ｑ＝（ｘ，ｙ）∈Ｅ（★Ｆ$_{p}$）について、φ（Ｑ）∈Ｅ（★Ｆ■）であるが、φ（Ｑ）∈＼Ｅ（★Ｆ$_{p}$）であることに注意されたい。したがって、Ｑ∈Ｅ（★Ｆ$_{p}$）はφ（Ｑ）∈Ｅ（★Ｆ■）に関して一次独立である。
【０１４８】
事実４：点Ｐ∈★Ｇ$_{1}$およびφ（Ｐ）は一次独立なので、これらは、★Ｚ$_{q}$×★Ｚ$_{q}$に同型な群を作成する。この点のなす群をＥ［ｑ］で表す。
★Ｇ$_{2}$を位数ｑの★Ｆ*■の部分群とする。曲線Ｅ（★Ｆ■）上のＷｅｉｌペアリングは、写像ｅ：Ｅ［ｑ］×Ｅ［ｑ］→★Ｇ$_{2}$である。（この写像は、「Ｗｅｉｌペアリングの説明」という表題の節で定義し、説明されている。）任意のＱ、Ｒ∈Ｅ（★Ｆ$_{p}$）について、Ｗｅｉｌペアリングはｅ（Ｑ，Ｒ）＝１を満たす。つまり、Ｗｅｉｌペアリングは、Ｅ（★Ｆ$_{p}$）上で退化し、したがって、群★Ｇ$_{1}$上で退化する。非退化写像を得るために、修正したＷｅｉｌペアリングｅ＾：★Ｇ$_{1}$×★Ｇ$_{1}$→★Ｇ$_{2}$を次のように定義する。
【０１４９】
ｅ＾（Ｐ，Ｑ）＝ｅ（Ｐ，φ（Ｑ））
修正したＷｅｉｌペアリングは、以下の特性を満たす。
１．双線形：すべてのＰ、Ｑ∈★Ｇ$_{1}$について、およびすべてのａ、ｂ∈★Ｚについて、ｅ＾（ａＰ，ｂＱ）＝ｅ＾（Ｐ，Ｑ）^{ab}となる。
【０１５０】
２．非退化：もしＰが★Ｇ$_{1}$の作成要素ならば、ｅ＾（Ｐ，Ｐ）∈★Ｆ＊■は★Ｇ$_{2}$の作成要素である。
３．計算可能：Ｐ、Ｑ∈★Ｇ$_{1}$が与えられた場合、ｅ＾（Ｐ，Ｑ）∈★Ｇ$_{2}$を計算する効率のよいアルゴリズムが存在する。（このアルゴリズムは、「Ｗｅｉｌペアリングの説明」という表題の以下の節で説明されている。）実行時間は、★Ｆ$_{p}$の指数に比較しうる。
【０１５１】
計算Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎ問題（ＣＤＨ）は群★Ｇ$_{1}$の中では困難であるように見えるが、決定Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎ問題（ＤＤＨ）は★Ｇ$_{1}$の中では容易である。
【０１５２】
ＢＤＨパラメータ作成要素＄ｇ$_{1}$：秘匿性パラメータ２＜ｋ∈★Ｚが与えられたとすると、ＢＤＨパラメータ作成要素によりランダムなｋビットの素数ｑを選び、（１）ｐ＝２　ｍｏｄ　３、（２）ｑはｐ＋１を割り切り、（３）ｑ^{2}はｐ＋１を割り切らないような最小の素数ｐを求める。ｐ＝＄ｌｑ＋１と書く。群★Ｇ$_{1}$は、★Ｆ$_{p}$上の曲線ｙ^{2}＝ｘ^{3}＋１の点のなす群の位数ｑの部分群である。★Ｇ$_{2}$は★Ｆ＊■の位数ｑの部分群である。双

線形写像ｅ＾：★Ｇ$_1$×★Ｇ$_1$→★Ｇ$_2$は、上で定義した修正されたＷｅｉｌペアリングである。

【０１５３】

ＢＤＨパラメータ作成要素＄ｇ$_1$は、漸近的にＢＤＨ仮定を満たすと考えられる。しかし、それでも、ＢＤＨ問題を十分に困難できる実際に使用可能なｐおよびｑの値には問題がある。最低でも、★Ｇ$_1$における離散対数問題は十分に困難であることを保証することが可能であるのが望ましい。前のほうで指摘したように、★Ｇ$_1$の離散対数問題は、★Ｇ$_2$における離散対数に効率よく帰着できる。したがって、★Ｆ*■における離散対数を計算することで、十分に★Ｇ$_1$における離散対数を計算できる。実際、★Ｆ*■の離散対数の固有の秘匿性については、少なくとも５１２ビット長の素数ｐを使用するのが望ましい（したがって、群のサイズは少なくとも１０２４ビット長である）。その結果、実施形態によっては、このＢＤＨパラメータ作成要素は、５１２ビット長以上になりそうな素数ｐで使用される。

【０１５４】

認容的符号化関数：ＭａｐＴｏＰｏｉｎｔ

上で定義したように、★Ｇ$_1$、★Ｇ$_2$を＄ｇ$_1$により作成された２つの群とする。前のほうで説明したＩＢＥシステムは、ハッシュ関数Ｈ$_1$：｛０，１｝*→★Ｇ$^*_1$を使用していることに留意されたい。ある集合Ａに対するハッシュ関数Ｈ$_1$：｛０，１｝*→Ａと認容的符号化関数Ｌ：Ａ→★Ｇ$^*_1$を用意するだけで十分である。以下では、集合Ａは★Ｆ$_p$となり、認容的符号化関数ＬはＭａｐＴｏＰｏｉｎｔと呼ばれ、本発明のさまざまの実施形態で使用することができる。

【０１５５】

この例では、ｐを、ある素数ｑ＞３についてｐ＝２　ｍｏｄ　３およびｐ＝＄ｌｑ－１を満たす素数とする。この実施例では、ｑは＄ｌを割り切らない（つまり、ｑ^{2}はｐ＋１を割り切らない）。Ｅを★Ｆ$_p$上の楕円曲線ｙ^2＝ｘ^3＋１とする。★Ｇ$_1$を位数ｑのＥ上の点のなす部分群とする。さらに、ハッシュ関数Ｈ$_1$：｛０，１｝*→★Ｆ$_p$を与える。

【０１５６】

この実施例では、アルゴリズムＭａｐＴｏＰｏｉｎｔは入力ｙ$_0$∈★Ｆ$_p$上で以下のように動作する。

１．ｘ$_0$＝（ｙ$_0$^{2}－１）$^{1/3}$＝（ｙ$_0$^{2}－１）$^{(2p-1)/3}$∈★Ｆ$_p$

２．Ｑ＝（ｘ$_0$，ｙ$_0$）∈Ｅ（★Ｆ$_p$）とし、Ｑ$_{ID}$＝＄ｌＱ∈★Ｇ$_1$と設定する。

【０１５７】

３．ＭａｐＴｏＰｏｉｎｔ（ｙ$_0$）＝Ｑ$_{ID}$を出力する。

これで、ＭａｐＴｏＰｏｉｎｔの説明は完了である。

＄ｌＱ＝＄ｌ（ｘ$_0$，ｙ$_0$）＝Ｏとなるｙ$_0$∈★Ｆ$_p$の＄ｌ－１個の値が存在することに注意されたい（これらは＄ｌを割り切る位数の非Ｏ点である）。Ｂ⊂★Ｆ$_p$をこれらのｙ$_0$の集合とする。Ｈ$_1$（ＩＤ）がこれら＄ｌ－１個の値の１つであれば、Ｑ$_{ID}$は★Ｇ$_1$の単位要素である。Ｈ^1（ＩＤ）がこれらの点の１つに当たる可能性はほとんどなく、その確率は１／ｑ＜１／２^{k}である。したがって、簡単にするため、Ｈ$_1$（ＩＤ）は★Ｆ$_p$＼Ｂの要素を出力するだけである、つまりＨ$_1$：｛０，１｝*→★Ｆ$_p$＼Ｂである。他の実施形態では、異なるハッシュ関数を使用してＩＤを複数回ハッシュすることにより、アルゴリズムＭａｐＴｏＰｏｉｎｔを拡張して値ｙ$_0$∈Ｂを扱えるようにすることが可能である。

【０１５８】

命題８　ＭａｐＴｏＰｏｉｎｔ：★Ｆ$_p$＼Ｂ→★Ｇ$^*_1$は認容的符号化関数である。

証明　この写像は、明らかに計算可能であり、＄ｌ対１写像である。Ｌがサンプリング可能であることを証明する必要がある。ＰをＥ（★Ｆ$_p$）の作成要素とする。Ｑ∈★Ｇ$^*_1$が与えられると、サンプリング・アルゴリズム＄Ｌ$_S$は、（１）ランダムなｂ∈｛０，．．．，＄ｌ－１｝を選び、（２）Ｑ’＝＄ｌ$^{-1}$・Ｑ＋ｂｑＰ＝（ｘ，ｙ）を計算し、（３）＄Ｌ$_S$（Ｑ）＝ｙ∈★Ｆ$_p$を出力する。ここで、＄ｌ$^{-1}$は、★Ｚ$^*_q$における＄ｌ

の逆要素である。このアルゴリズムは、必要に応じて、ＭａｐＴｏＰｏｉｎｔ内の＄ｌ個の要素からランダムな要素を出力する。

【０１５９】

ＩＢＥシステムの詳細な例

ＢＤＨパラメータ作成要素$$g_1$$および認容的符号化関数ＭａｐＴｏＰｏｉｎｔを使用して、ＩＢＥシステムの一実施形態の以下の詳細の例を得る。

【０１６０】

Ｓｅｔｕｐ：秘匿性パラメータｋ∈★$$Z^+$$が与えられると、このアルゴリズムは以下のように実行する。

工程１：入力ｋでｇを実行し、ｑがｐ＋１を割り切るようなｋビットの素数ｑおよび素数ｐ＝２　ｍｏｄ　３を作成する。Ｅを、★$$F_p$$上の方程式$$y^2 = x^3 + 1$$によって定義された楕円曲線とする。位数ｑの任意のＰ∈Ｅ（★$$F_p$$）を選択する。

【０１６１】

工程２：ランダムなｓ∈★$$Z^*_q$$を選び、$$P_{pub} = sP$$と設定する。

工程３：４つのハッシュ関数$$H_1 : \{0, 1\}^* \rightarrow$$★$$F_q$$、あるｎに対する$$H_2$$：★Ｆ■$$\rightarrow \{0, 1\}^n$$、$$H_3 : \{0, 1\}^n \times \{0, 1\}^n \rightarrow$$★$$Z^*_q$$、およびハッシュ関数$$H_4 : \{0, 1\}^n \rightarrow \{0, 1\}^n$$を選ぶ。メッセージ空間は、$Ｍ＝｛０，１｝^{n}である。暗号文空間は、$Ｃ＝Ｅ（★$$F_p$$）×｛０，１｝^{n}である。システム・パラメータは、ｐａｒａｍｓ＝＜ｐ，ｑ，ｎ，Ｐ，$$P_{pub}$$，$$H_1$$，．．．，$$H_4$$＞である。ｍａｓｔｅｒ－ｋｅｙは、ｓ∈★$$Z^*_q$$である。

【０１６２】

Ｅｘｔｒａｃｔ：与えられた２進数列ＩＤ∈｛０，１｝$*$について、アルゴリズムは秘密鍵ｄを次のように作成する。

工程１：位数ｐのＭａｐＴｏＰｏｉｎｔ（$$H_1$$（ＩＤ））＝$$Q_{ID} \in$$Ｅ（★$$F_p$$）を計算する。

【０１６３】

工程２：秘密鍵$$d_{ID}$$を$$d_{ID} = sQ_{ID}$$となるように設定し、ｓはマスター鍵である。

Ｅｎｃｒｙｐｔ：公開鍵ＩＤのもとでＭ∈｛０，１｝^{n}を暗号化するには、以下を実行する。

【０１６４】

工程１：位数ｑのＭａｐＴｏＰｏｉｎｔ（$$H_1$$（ＩＤ））＝$$Q_{ID} \in$$Ｅ（★$$F_p$$）を計算する。

工程２：ランダムなσ∈｛０，１｝^{n}を選択する。

【０１６５】

工程３：ｒ＝$$H_3$$（σ，Ｍ）と設定する。

工程４：　暗号文を次のように設定する。

Ｃ＝＜ｒＰ，σ○＋$$H_2$$（$$g^r_{ID}$$），Ｍ○＋$$H_4$$（σ）＞　ただし、$$g_{ID} = e\hat{}(Q_{ID}, P_{pub}) \in$$★Ｆ■

【０１６６】

Ｄｅｃｒｙｐｔ：Ｃ＝＜Ｕ，Ｖ、Ｗ＞を、公開鍵ＩＤを使用して暗号化された暗号文であるとする。Ｕ∈Ｅ（★$$F_p$$）が位数ｑの点でない場合、その暗号文を拒絶する。秘密鍵$$d_{ID}$$を使用してＣを暗号化するために、以下を実行する。

【０１６７】

工程１．Ｖ○＋$$H_2$$（$$e\hat{}(d_{ID}, U)$$）＝σを計算する。

工程２．Ｗ○＋$$H_4$$（σ））＝Ｍを計算する。

工程３．ｒ＝$$H_3$$（σ，Ｍ）と設定する。Ｕ＝ｒＰであることを検査する。そうでなければ、その暗号文を却下する。

【０１６８】

工程４．ＭをＣの解読として出力する。

性能。この実施形態では、アルゴリズムＳｅｔｕｐおよびＥｘｔｒａｃｔは非常に単純で

ある。両方のアルゴリズムの中心にあるのは、曲線Ｅ（★$Ｆ_{p}$）上の標準の乗法である。アルゴリズムＥｎｃｒｙｐｔでは、エンクリプタが$Ｑ_{ＩＤ}$および$Ｐ_{ｐｕｂ}$のＷｅｉｌペアリングを計算する必要がある。この計算は、メッセージとは無関係であり、したがって、一度だけ実行することが可能であることに注意されたい。$ｇ_{ＩＤ}$が計算されてしまうと、この実施形態の性能は、標準ＥｌＧａｍａｌ暗号化とほとんど同じである。さらに、ＢａｓｉｃＩｄｅｎｔの実施例の暗号文長は★$Ｆ_{p}$の通常のＥｌｇａｍａｌの場合と同じであることにも注意されたい。解読は、単純なＷｅｉｌペアリング計算である。

【０１６９】

秘匿性。説明したばかりの詳細な実施例の秘匿性は、定理４と定理７から直接得られる。系９　上で説明した詳細な実施例は、ＢＤＨパラメータ作成要素$ｇ_{1}$がＢＤＨ仮定を満たしていると仮定した場合の選択暗号文秘匿ＩＢＥシステムである（つまり、ランダム・オラクル・モデルのＩＮＤ－ＩＤ－ＣＣＡ）。

【０１７０】

拡張と観察

Ｔａｔｅペアリングおよびその他の曲線。

このＩＢＥシステムの実施形態は、ＢＤＨ仮定が成立する場合に２つの群★$Ｇ_{1}$、★$Ｇ_{2}$の間の効率よく計算できる双線形写像ｅ＾：★$Ｇ_{1}$×★$Ｇ_{1}$→★$Ｇ_{2}$で動作する。多くの異なる楕円曲線から、このような写像が得られる。例えば、ｐ＝３　ｍｏｄ　４、$ｉ^{2}$＝－１、自己準同型写像φ：（ｘ，ｙ）→（－ｘ，ｉｙ）と定められた★$Ｆ_{p}$上の曲線$ｙ^{2}$＝$ｘ^{3}$＋ｘを使用することが可能である。

【０１７１】

他の実施形態では、ミヤジ他（Ｍｉｙａｊｉ　ｅｔ　ａｌ）（（非特許文献４）を参照）によって説明されている★$Ｆ_{p}$上の非超特異楕円曲線族を使用することができる。例えば、この曲線族の曲線Ｅ／★$Ｆ_{p}$を使用するには、★$Ｇ_{1}$をＥ（★Ｆ□）（Ｅ（★$Ｆ_{p}$）には含まれない）の巡回部分群とみなし、トレース写像を、ペアリングｅ＾を定義するのに使用した自己準同型写像φとして使用することが可能である。なお、ＦｕｌｌＩｄｅｎｔにおける暗号化と解読は両方とも、他の実施形態では、Ｗｅｉｌペアリングの代わりにＴａｔｅペアリングを楕円曲線上で使用することにより、高速化することが可能であることに注意されたい。他の実施形態では、アーベル多様体から適当な双線形写像を誘導することができる。

【０１７２】

非対称ペアリング

前述のように、このＩＢＥシステムの実施形態は、対称写像に限られず、非対称写像をも含むことができる。つまり、実施形態では一般に、★$Ｇ_{0}$、★$Ｇ_{1}$を素数位数ｑの群とした場合に、ｅ＾：★$Ｇ_{0}$×★$Ｇ_{1}$→★$Ｇ_{2}$の形式の写像を使用できる。★$Ｇ_{0}$および★$Ｇ_{1}$が等しい場合、写像は対称であるという。★$Ｇ_{0}$と★$Ｇ_{1}$が等しくない場合、写像は非対称であるという。

【０１７３】

非対称の場合の要素$Ｑ_{ＩＤ}$およびＰはそれぞれ★$Ｇ_{0}$および★$Ｇ_{1}$に属し（逆もまた同様）、ハッシュ関数$Ｈ_{1}$の対象となる群はそれに応じて選択される。しかし、秘匿性の証明を行うため（特に補助定理２）、ランダムなＰ、ａＰ、ｂＰ∈★$Ｇ_{1}$およびＱ、ａＱ、ｃＱ∈★$Ｇ_{0}$が与えられた場合に無視できない確率で$ｅ＾（Ｐ，Ｑ）^{ａｂｃ}$を計算することが可能な多項式時間アルゴリズムはないというｃｏ－ＢＤＨ仮定と呼ぶ見かけが少し変わっている複雑度仮定を使用する。この仮定を使用するのであれば、Ｍｉｙａｊｉ　ｅｔ　ａｌの曲線Ｅ／★$Ｆ_{p}$を使用する実施形態については（上で説明したように）、★$Ｇ_{1}$を位数ｑの巡回部分群Ｅ（★$Ｆ_{p}$）とみなし、★$Ｇ_{0}$を位数ｑのＥ（★Ｆ□）の別の巡回部分群とみなすことが可能である。これにより、これらの曲線を使用することについて前段落で説明した方法よりも効率的なシステムが得られる。

【０１７４】

分散ＰＫＧ

ＩＢＥシステムの実施例では、ＰＫＧに保管されるｍａｓｔｅｒ－ｋｅｙは保護されるのが望ましい。この鍵を保護する方法として、閾値暗号の手法を使用して異なる複数のサイトに分散させる方法がある。このＩＢＥシステムの実施形態では、これを非常に効率のよい、堅牢な方法でサポートしている。ただし、上述のいくつかの実施形態では、ｍａｓｔｅｒ－ｋｅｙはあるｓ∈★Z^{*}_{q}とすることができ、ＰＫＧは群作用を使用してｓおよびQ_{ID}から秘密鍵を計算し、Q_{ID}はユーザの公開鍵ＩＤから導かれる。例えば、$d_{ID}=sQ_{ID}$である。分散ＰＫＧ実施形態は、ｎ個のＰＫＧのそれぞれにｓ　ｍｏｄ　ｑのシャミール秘密分散の１つの割符s_iを与えることにより「ｎ個のうちのｔ個」方式で実装することが可能である。ｎ個のＰＫＧはそれぞれ、$d_i=s_iQ_{ID}$を計算することにより、マスター鍵のその割符を使用して、秘密鍵d_{ID}の対応する割符d_iを作成することが可能である。その後、ユーザは、ｎ個のうちのｔ個のＰＫＧに秘密鍵の割符d_iを要求し、λ_iを適切なラグランジュ補間係数として$d_{ID}=\Sigma_i\lambda_i d_i$を計算することにより割符を結合して秘密鍵全体を構成することが可能である。

【０１７５】

さらに、ＤＤＨは★G_1では容易であるという事実を利用してこの実施形態を堅牢なものにし不正なＰＫＧに対抗するようにすることが容易である。設定時に、ｎ個のＰＫＧのそれぞれ$P_i=s_iP$を公開する。鍵作成要求が出されたら、ユーザは、以下を検査して、ｉ番目のＰＫＧからの応答が有効であることを確認することが可能である。

【０１７６】

$e^{\wedge}(d_i, P)=e^{\wedge}(Q_{ID}, P_i)$

したがって、不正な動作をするＰＫＧは即座に捕捉される。通常の堅牢な閾値方式と同様、ゼロ知識証明の必要はない。ＰＫＧのｍａｓｔｅｒ－ｋｅｙは、Ｒ．ゲナロ他（Ｒ．Ｇｅｎｎａｒｏ　ｅｔ　ａｌ．）（（非特許文献５）を参照）の手法を使用して分散方式で作成することが可能である。また、この手法を使用することで、ＰＫＧは、マスター鍵がどこか１つの場所に存在していなくてもマスター鍵のそれぞれの割符を結合作成できる協調プロトコルを実行することが可能である。

【０１７７】

さらに分散ｍａｓｔｅｒ－ｋｅｙ実施形態を使用すると、メッセージ毎に閾値解読を実行することができ、しかも、対応する解読鍵を導く必要はないことにも注意されたい。例えば、各ＰＫＧが$e^{\wedge}(s_i, Q_{ID}, U)$で応答すれば、ＢａｓｉｃＩｄｅｎｔ暗号文（Ｕ，Ｖ）の閾値解読は簡単である。

【０１７８】

図５は、本発明の一実施形態による分散ＰＫＧシステムを説明するブロック図である。図５は、送信者システム５０１、受信者システム５０２、および３つのＰＫＧ（ＰＫＧ　Ａ　５０３、ＰＫＧ　Ｂ　５０４、ＰＫＧ　Ｃ　５０５）を含む。「３個のうちの２個」分散方式を説明する一実施形態では、３つのＰＫＧはそれぞれ、マスター鍵の異なる割符を含み、３つのうち２つでマスター鍵を誘導することができる。図に示されているように、ＰＫＧ　Ａ　５０３、ＰＫＧ　Ｂ　５０４、およびＰＫＧ　Ｃ　５０５は、それぞれマスター鍵割符s_1、５１１、マスター鍵割符s_2、５１２、およびマスター鍵割符s_3、５１３を含む。「３個の２個」分散方式では、３個のうち２個のＰＫＧにより割符を結合し、マスター鍵を決定することが可能であるが、この実施形態では、それぞれのＰＫＧは秘密のうちにそのマスター鍵割符を保持する。

【０１７９】

送信者システム５０１は、受信者５０２にメッセージを送信する。メッセージ５１４は、受信者の識別子ＩＤに基づく公開鍵を使用して暗号化することができる。対応する秘密鍵を取得するために、受信者システムは、例えば、受信者のＩＤまたは公開鍵を使用して３個のうち２個のＰＫＧにクエリを実行する。図に示されているように、受信者システム５０２は、クエリ５０６および５０７をそれぞれＰＫＧ　Ａ　５０３およびＰＫＧ　Ｂ　５０４に送り、秘密鍵の２つの割符を取得する。これらのクエリへの応答として、ＰＫＧ　Ａ　５０３およびＰＫＧ　Ｂ　５０４は、それぞれ、秘密鍵ｄ、５１０の割符d_1、５０

８、および割符d_2、５０９を返す。その後、受信者システム５０２は、対応する秘密鍵d_{ID}を構成することができるが、これは、メッセージ５１４の暗号化に使用された公開鍵に対応している。より一般的には、受信者は３個のうち任意の２個のＰＫＧにクエリを行うように選択しておくことが可能である。例えば、受信者システム５０２は、他の方法として、ＰＫＧ　ＢおよびＣにクエリを実行し、秘密鍵割符d_2およびd_3を結合して、秘密鍵５１０を作成しておくことが可能である。これらの手法は一般化をたやすく行うことができ、ｎ個のうちｔ個という分散方式を使用して類似の実施形態が得られる。

【０１８０】

送信者システム５０１、受信者システム５０２、さらにＰＫＧ　５０３、５０４、および５０５は、それぞれ、プロセッサおよびメモリおよび他の記憶デバイスなどのコンピュータ可読媒体などの要素を備えるコンピュータ・システムとして実装することができる。それぞれの要素間の通信は、データ・ネットワーク上で送信するデータ・パケットを使用して、または他のさまざまな形態の電子的およびデータ伝送および通信を使用して行うことができる。通信は、各種の有線、無線、およびその他の通信媒体を利用する、インターネットなどのコンピュータ・ネットワークなど、さまざま通信アーキテクチャを介して伝送することができる。

【０１８１】

部分群での動作

上述の詳細なＩＢＥシステムの他の実施形態では、曲線の比較的小さな部分群において動作させることにより性能を改善することができる。例えば、ある１６０ビットの素数ｑについてｐ＝ａｑ－１となる１０２４ビットの素数ｐ＝２　ｍｏｄ　３を選択する。そこで、点Ｐを、位数ｑの点となるように選択する。各公開鍵ＩＤを曲線Ｑ上の点にハッシュし、その後、ａをその点に掛けてＩＤを群の点に変換する。システムは、Ｐによって作成された群においてＢＤＨ仮定が成立する場合に秘匿性がある。この実施形態の利点は、Ｗｅｉｌ計算が小さな位数の点で実行され、したがってかなり高速であることである。

【０１８２】

ＩＢＥは署名を含む

上述のさまざまなＩＢＥ手法を使用して、公開鍵署名システムおよび方法を実現することが可能である。考え方は以下のとおりである。署名方式の秘密鍵は、ＩＢＥ方式のマスター鍵である。この署名方式の公開鍵は、ＩＢＥ方式の大域的システム・パラメータの集合である。メッセージＭの署名は、ＩＤ＝Ｍに対するＩＢＥ解読鍵である。署名を検証するために、ランダム・メッセージＭ’を選択し、公開鍵ＩＤ＝Ｍを使用してＭ’を暗号化し、それから、Ｍの指定された署名を解読鍵として使用して解読を試みる。ＩＢＥシステムがＩＮＤ－ＩＤ－ＣＣＡの場合、署名方式は選択メッセージ攻撃に対し存在的偽造不可である。ただし、たいていの署名方式とは異なり、この署名検証実施形態はランダム化されている。このことから、ここで説明しているＩＢＥ手法は公開鍵暗号化と電子署名の両方を包含することができる。これらのアプローチから派生する署名方式を使用して、興味深い特性を得ることが可能であるが、これについてはボネ他（Ｂｏｎｅｈ　ｅｔ　ａｌ．）（本願明細書に援用する（非特許文献６）で説明している。

【０１８３】

エスクローＥｌＧａｍａｌ暗号化

この節では、上述のさまざまなＩＢＥ手法を使用して、大域的エスクロー機能を持つＥｌＧａｍａｌ暗号化システムの実施形態を実現することが可能であることを示す。本実施形態では、単一のエスクロー鍵を使用して、任意の公開鍵で暗号化された暗号文の解読を行うことができる。

【０１８４】

１実施例では、ＥｌＧａｍａｌエスクロー・システムは以下のように動作する。ＳｅｔｕｐはＢａｓｉｃＩｄｅｎｔのと類似している。ＩＤベースＢａｓｉｃＩｄｅｎｔと異なり、それぞれのユーザが秘密乱数を選択し、それを使用して、公開鍵／秘密鍵のペアを作成する。こうして、送信者および受信者はＥｎｃｒｙｐｔとＤｅｃｒｙｐｔを使用して、暗

号化されたメッセージを伝達することが可能である。メッセージは、マスター鍵ｓをメッセージの解読に使用することが可能なエスクローを除き秘匿される。

【０１８５】

図６は、本発明の一実施形態によるエスクロー解読機能を備える暗号システム内の要素を説明するブロック図である。システムは、暗号化論理回路６１０を備える送信者システム６０１、解読論理回路６１１を備える受信者システム６０２、エスクロー・エージェント・システム６０４、およびブロードキャスト・システム６０５を含む。ブロードキャスト・システム６０５は、エスクロー・エージェント・システム６０４、受信者システム６０２、および送信者システム６０１などの参加者にシステム・パラメータを送信する。受信者システム６０２は、秘密鍵ｘ、６０７を選択し、それを使って、公開鍵$P_{pub}=xP$、６０６を作成し、その後、公開する。秘密鍵ｘおよび公開鍵P_{pub}は、相補的鍵の対を形成する。送信者システム６０１は、公開鍵$P_{pub}=xP$、６０６を使用し、暗号化論理回路６１０でメッセージＭを暗号化する。送信者システム６０１は、その結果得られた暗号化されたメッセージ６０３を受信者６０２に送信する。受信者システム６０２は、秘密鍵ｘ、６０７を使用して解読論理回路６１１でメッセージを解読する。エスクロー・エージェント・システム６０４は、メッセージ６０３を横取りし、エスクロー・エージェント鍵ｓ、６０９、公開鍵$P_{pub}=xP$、６０６を使用し、解読論理回路６１２でメッセージ６０３を解読する。他の実施形態では、ブロードキャスト・システム６０５およびエスクロー・エージェント６０４は、単一のエンティティであってもよい。さらに他の実施形態では、すでに述べている分散ＰＫＧ実施形態などの方法でエスクロー・エージェント鍵を共有することができる。

【０１８６】

さらに詳細には、この手法の実施例は以下の手順を含む。

Ｓｅｔｕｐ：$ｇをあるＢＤＨパラメータ作成要素とする。秘匿性パラメータ$k\in\bigstar Z^{+}$が与えられると、このアルゴリズムは以下のように実行する。

【０１８７】

工程１：入力ｋに対して$ｇを実行し、素数ｑ、位数ｑの２つの群$\bigstar G_1$、$\bigstar G_2$、および認容写像ｅ＾：$\bigstar G_1\times\bigstar G_1\rightarrow\bigstar G_2$を作成する。Ｐを$\bigstar G_1$のある作成要素とする。

【０１８８】

工程２：ランダムな$s\in\bigstar Z^{*}_{q}$を選び、Ｑ＝ｓＰと設定する。

工程３：暗号ハッシュ関数Ｈ：$\bigstar G_2\rightarrow\{0,1\}^{n}$を選択する。

メッセージ空間は、$M=\{0,1\}^{n}$である。暗号文空間は、$C=\bigstar G_1\times\{0,1\}^{n}$である。システム・パラメータは、ｐａｒａｍｓ＝＜ｐ，$\bigstar G_1$，$\bigstar G_2$，ｅ＾，ｎ，Ｐ，Ｑ，Ｈ＞である。エスクロー鍵は、$s\in\bigstar Z^{*}_{q}$である。

【０１８９】

ｋｅｙｇｅｎ：ユーザは、ランダムな$x\in\bigstar Z^{*}_{q}$を選び、$P_{pub}=xP\in\bigstar G_1$を計算して、自分自身の公開鍵／秘密鍵の対を作成する。ユーザの秘密鍵はｘ（またはｘＱ）であり、ユーザの公開鍵はP_{pub}である。

【０１９０】

Ｅｎｃｒｙｐｔ：公開鍵P_{pub}のもとで$M\in\{0,1\}^{n}$を暗号化するために、（１）ランダムな$r\in\bigstar Z^{*}_{q}$を選び、（２）暗号文を以下のように設定する。

$C=\langle rP,\ M\bigcirc+H(g^{r})\rangle$　ただし、$g=e\hat{}(P_{pub},Q)\in\bigstar G_2$。

【０１９１】

こと暗号化手法はさらに、図７でも説明されており、そこで、送信者は、ブロック７００で、システム・パラメータおよび要素ＰおよびＱ＝ｓＰを取得し、ブロック７１０で、受信者の公開鍵$P_{pub}=xP$を取得する。その後、ブロック７２０で、送信者は乱数ｒを選択し、メッセージ鍵を計算する。その後、ブロック７３０で、メッセージ鍵を使用してメッセージを暗号化する。次に、送信者は、カプセル化された鍵ｒＰおよび暗号化されたメッセージＶを受信者に送信する。

【０１９２】
Ｄｅｃｒｙｐｔ：Ｃ＝＜Ｕ，Ｖ＞を、P_{pub}を使用して暗号化された暗号文であるとする。すると、Ｕ∈★G_1である。秘密鍵ｘを使用してＣを解読するために、以下を実行する。
【０１９３】
Ｖ○＋Ｈ（ｅ＾（Ｕ，ｘＱ））＝Ｍ
図８で説明されているように、受信者は、ブロック８００で、システム・パラメータおよび要素ＰおよびＱ＝ｓＰを取得し、ブロック８１０で、暗号化されたメッセージＶおよびカプセル化された鍵ｒＰを送信者から取得する。その後、ブロック８２０で、受信者はメッセージ鍵を計算し、ブロック８３０で、これを使用してメッセージを解読する。
【０１９４】
送信者および受信者によって計算されたメッセージ鍵が同じであることを見るためには、送信者は秘密ｒだけでなく公開Ｑ＝ｓＰおよびP_{pub}＝ｘＰも知り、これらを使用して、ｅ＾（ｓＰ，ｘＰ）^{r}から鍵を計算することに注意されたい。一方、受信者は、秘密ｘだけでなく公開Ｑ＝ｓＰおよびｒＰを知り、これらを使用して、ｅ＾（ｒＰ，ｘ（ｓＰ））からメッセージ鍵を計算する。ｅ＾の双線形性から、ｅ＾（ｓＰ，ｘＰ）^{r}＝ｅ＾（ｒＰ，ｘ（ｓＰ））が成り立ち、ゆえに、送信者および受信者は同じメッセージ鍵を計算する。
【０１９５】
Ｅｓｃｒｏｗ－ｄｅｃｒｙｐｔ：この実施形態の目的は、他の方法で秘匿性のある通信のエスクロー解読を行えるようにすることである。エスクロー鍵ｓを使用してＣ＝＜Ｕ，Ｖ＞を解読するために、以下を計算する。
【０１９６】
Ｖ○＋Ｈ（ｅ＾（Ｕ，ｓP_{pub}））＝Ｍ
図９に示されているように、エスクローは、ブロック９００で、システム・パラメータおよび要素Ｐを取得し、ブロック９１０で、受信者の公開鍵ｘＰを取得し、送信者から暗号化されたメッセージＶおよびカプセル化された鍵ｒＰを取得する。その後、ブロック９２０で、エスクローはメッセージ鍵を計算し、ブロック９３０で、これを使用してメッセージを解読する。エスクローは、ｓ、ｒＰ、およびｘＰを知ってメッセージを計算することが可能である。
【０１９７】
標準的な議論から、ＢＤＨが＄ｇで作成され群に対し困難であると仮定すると、この実施形態のシステムは、ランダム・オラクル・モデルにおいて意味秘匿性を有することがわかる（ＤＤＨは容易であるため、ＤＤＨに基づいて意味秘匿性を証明することはできないことに留意されたい）。それでも、エスクロー・エージェントは、ユーザの公開鍵を使用して暗号化した暗号文を解読することが可能である。エスクロー・エージェントの解読機能は、前に述べたＰＫＧ分散手法を使用して分散させることが可能である。
【０１９８】
他の実施形態では、非大域的エスクローを使用するＥｌＧａｍａｌ暗号化システムとともに類似の困難さ仮定を使用する。この実施形態では、それぞれのユーザが２つの対応する秘密鍵を使って公開鍵を構成し、その秘密鍵の一方を信頼できる第三者に与える。信頼できる第三者は、さまざまなユーザから与えられたすべての秘密鍵のデータベースを保持する。秘密鍵は両方とも、解読に使用可能であるが、ユーザの秘密鍵のみ、離散対数ベースの署名方式の署名鍵として同時に使用することが可能である。
【０１９９】
他のさまざまな暗号システムを、上記の実施形態に示されている原理に考案することが可能である。例えば、３つのエンティティＡ、Ｂ、およびＣは、個人として乱数整数ａ、ｂ、ｃを選択し、公開鍵ａＰ、ｂＰ、ｃＰを公開することにより１つのグループとして安全に通信することが可能である。そのうちの１つ、例えばＡはメッセージ鍵ｅ＾（ｂＰ，ｃＰ）^{r}を使用してメッセージを暗号化し、ｒＰとともに送信することが可能である。次に

Ｂが、ｅ＾（ｃＰ，ｒＰ）^{r}を計算してメッセージを解読し、Ｃは、ｅ＾（ｂＰ，ｒＰ）^{c}を計算してそのメッセージを解読することが可能である。同様、Ｂがメッセージを ＡおよびＣに送信するか、またはＣがメッセージをＡおよびＢに送信することが可能である。

【０２００】

他の考えられる実施形態では、３つのエンティティのうち２つ、例えばＡとＢは、共有公開鍵ａｂＰを公開することが可能である。次に、Ｃはメッセージ鍵ｅ＾（ａｂＰ，ｃＰ）^{r}を使用してメッセージを暗号化し、ｒＰとともに送信することが可能である。すると、ＡもＢも単独ではメッセージを解読しえないが、ＡとＢの両方が一緒にｅ＾（ｃＰ，ｒＰ）^{ab}を計算し、共同でメッセージを解読することは可能である。この手法は、任意の数のエンティティに一般化される。例えば、Ｃは、ａｂＰを使用して三者共有公開鍵ａｂｃＰを計算し公開することにより、ＡおよびＢを参加させることが可能である。その後は、誰でも、メッセージ鍵ｅ＾（ａｂｃＰ，ｘＰ）^{r}を使用してメッセージを暗号化し、ｒＰとともに送信することが可能になる。その後、ＡおよびＢおよびＣのみが一緒に、ｅ＾（ｘＰ，ｒＰ）^{abc}を計算し、共同で、メッセージを解読することが可能である。

【０２０１】

しきい値解読

本発明の実施形態では、ｎ個のエンティティが与えられた公開鍵ＩＤに対応する秘密鍵d_{ID}の割符を所有し、ｎ個のｔ個のエンティティが共同する場合にのみ、そのＩＤを使用して暗号化されたメッセージを解読するようにすることが可能である。秘密鍵d_{ID}は、決して、単一の場所では再構成されない。このＩＢＥシステムの実施形態ではこれに以下のように対応できる。

【０２０２】

他の実施形態では、$s \in \bigstar Z^{*}_{q}$がマスター鍵であるとして秘密鍵$d_{ID} = sQ_{ID}$であることに留意されたい。その代わりに、$s_1, \ldots, s_n \in \bigstar Z^{*}_{q}$をマスター鍵ｓの「ｎ個のうちｔ個」シャミール秘密分散とする。ｎ人のユーザのそれぞれに$d_i = s_i Q_{ID}$を与える。鍵ＩＤを使用して暗号化された暗号文＜Ｕ，Ｖ＞を解読するために、各ユーザはローカルで$g_i = e\hat{}(U, d_i)$を計算し、解読工程を管理するユーザに$g_i \in \bigstar G_2$を送信する。そのユーザは、λ_iをシャミール秘密分散で使用される適切なラグランジュ補間係数として$g_{ID} = \Pi_i g_i^{\blacktriangle}$を計算することにより解読割符を結合する。その後、$H_2(g_{ID}) \bigcirc + V = M$を計算することによりメッセージを取得する。

【０２０３】

暗号法の当業者であれば、本発明の基本原理を使用する他の多くの方式を考案することができるであろう。

ＩＤベース暗号化の応用

ＩＤベース暗号化の実施形態の一応用として、公開鍵インフラストラクチャの配備の支援が考えられる。この節では、このような応用およびその他の応用のいくつかの実施形態を示す。

【０２０４】

公開鍵の取り消し

この本実施形態では、送信者は、年、日、またはその他の時刻表示などの時間要素を含む情報から誘導された公開鍵を使用して暗号化し、鍵の有効期限またはその他の形式の時間に関係する鍵管理の実現を補助することができる。例えば、一実施形態では、“ｂｏｂ＠ｃｏｍｐａｎｙ．ｃｏｍ ｜｜ ｃｕｒｒｅｎｔ－ｙｅａｒ”というように公開鍵を使用して、ボブに送信する電子メールをアリスに暗号化してもらうことで鍵の有効期限を定められる。そうすることで、ボブは今年のみ自分の秘密鍵を使用することが可能である。１年に一度、ボブはＰＫＧから新規の秘密鍵を取得する必要がある。こうして、秘密鍵有効期限を１年間に設定する効果が得られる。既存の公開鍵インフラストラクチャとは異なり、ボブが自分の秘密鍵を更新する毎に、アリスがボブから新規証明書を取得する必要はないことに注意されたい。

【０２０５】

他の実施形態において、“ｂｏｂ@ｃｏｍｐａｎｙ．ｃｏｍ ｜｜ ｃｕｒｒｅｎｔ－ｄａｔｅ”または他のタイムスタンプを使用してボブ宛の電子メールを暗号化することにより、このアプローチの設定を細かくできる。こうすることで、ボブはいやおうなく新規秘密鍵を毎日取得することになる。この実施形態は、ＰＫＧが企業によって維持されている場合に企業環境内で使用することができる。このアプローチでは、鍵の取り消しは非常に単純であり、ボブが退社し、その鍵を取り消す必要が生じたら、企業ＰＫＧに、ボブの電子メール・アドレスに対応する秘密鍵の発行を停止するよう指令するという形をとる。その結果、ボブは自分の電子メールを読めなくなる。興味深い特性として、アリスは、ボブの毎日の公開鍵を取得するために第三者の証明書ディレクトリとやりとりする必要がないという点が挙げられる。したがって、ＩＤベース暗号化の実施形態は、一日限りの公開鍵を実装する非常に効率のよいメカニズムを実現することが可能である。なお、この実施形態を使用すると、アリスが未来に向けてメッセージを送信することができる、つまりボブはアリスの指定した日付に限り電子メールを解読することができるようになる。

【０２０６】

ユーザ信任状の管理

本発明の一実施形態では、ＩＢＥシステムを使用してユーザ信任状を管理することができる。メッセージは、信任状識別子を含む文字列で暗号化される。例えば、アリスが公開鍵を使用して“ｂｏｂ@ｃｏｍｐａｎｙ．ｃｏｍ ｜｜ ｃｕｒｒｅｎｔ－ｙｅａｒ ｜｜ ｃｌｅａｒａｎｃｅ＝ｓｅｃｒｅｔ”というようボブへのメールを暗号化する。すると、ボブは、指定された日に機密取扱資格がある場合にのみその電子メールを読むことができる。したがって、ＰＫＧを使用するとユーザ信任状の付与および取り消しは非常に容易である。

【０２０７】

図１０は、本発明の一実施形態によりＩＤベース暗号化システムで信用状を管理するシステムを説明するブロック図である。システムは、送信者システム１００１、受信者システム１００２、およびＰＫＧ １００３を備える。このようなシステムはそれぞれ、コンピュータ・ネットワークに接続されたクライアントまたはサーバなどコンピュータ・システムとして実装することができる。そのため、送信者１００１、受信者１００２、およびＰＫＧ １００３は、それぞれ、プロセッサ１０１４、プロセッサ１０１３、およびプロセッサ１０１２などのプロセッサを備えることができる。さらに、これらのシステムは、コンピュータ・メモリなどのコンピュータ可読記憶媒体を備え、さらに、有線、無線、またはその他のネットワークとの通信に対応する技術を含む、コンピュータ・ネットワークとのインターフェイスを備えることができる。送信者システム１００１は、ソフトウェア・プラグイン１０１７を備えることができる。このようなプラグインは、暗号機能を実行するソフトウェア・モジュールを含むことができる。本発明の一実施形態によれば、プラグインには、暗号論理回路１００４などが含まれる。プラグイン１０１７は、ネットワーク経由で送信者システム１００１および受信者システム１００２などのさまざまなコンピュータに配布し、ＩＤベース暗号化と関連する機能およびその他の通信機能を展開することができる。ＰＫＧ １００３などのシステムからのパラメータ１０１５も、コンピュータ・ネットワークまたはその他の通信媒体経由で、送信者システム１００１および受信者システム１００２など送信者および受信者に配布し、これらのシステムでは、メッセージを暗号化または解読する際にプラグイン１０１７とともにそれらのパラメータを使用することができる。一実施形態では、プラグイン１０１７は、パラメータとともに配布される。他の実施形態では、パラメータ１０１５を別々に配布することもできる。

【０２０８】

送信者システム１００１は、プラグイン１０１７の暗号化論理回路１００４を使用してメッセージＭを暗号化する。暗号化論理回路１００４は、選択した信任状１００５およびメッセージの宛先受信者の識別１０１６に基づく暗号鍵１０１１を使用してメッセージを暗号化する。いくつかの実施形態では、この鍵は、他の情報にも基づくことができる。送信者システム１００１は、受信者システム１００２に情報１００６を、例えば、ネットワー

クまたはその他の通信媒体経由で送信されるデータ・パケットの形式で送信する。受信者システム１００２に送信された情報１００６には、暗号化されたメッセージが入っており、さらに、暗号鍵の基盤の一部として使用される信任状１００５に関する情報１００７も含めることができる。

【０２０９】

情報１００６の受信前であろうと受信後であろうと、受信者システム１００２は要求１００９をＰＫＧ　１００３に送信する。一実施形態では、要求１００９は、受信者のＩＤ　１０１６を含むことができ、さらに、選択した信任状１００５に関係する情報を入れることもできる。応答として、ＰＫＧ　１００３は信任状検査論理回路１００８を使用して受信者１００２の信任状を検証する。このような論理回路は、ソフトウェア、ハードウェア、またはその組み合わせで実装することができる。信任状が受信者に属するものとして検証された場合、ＰＫＧ　１００３は応答１０１０を受信者１００２に送るが、この応答は、暗号鍵１０１１に対応する秘密解読鍵１０１８を含む。次に、秘密解読鍵を使用することで、受信者は情報１００６に含まれる暗号化されたメッセージを解読し、オリジナルのメッセージＭを復要素することができる。したがって、このような実施形態では、暗号鍵の一部として信任状を含めることにより、送信者が受信者宛先のメッセージを暗号化することができ、受信者によるメッセージの解読を受信者の信任状の有効性を条件とするようにできる。

【０２１０】

解読鍵の委託

ＩＢＥシステムを実施形態の他の応用として、解読機能の委託がある。ＰＫＧの役割を果たすユーザであるボブについて説明した２つの実施例を用意する。ボブは、設定アルゴリズムを実行して、自分のＩＢＥシステム・パラメータｐａｒａｍｓおよび自分のｍａｓｔｅｒ－ｋｅｙを作成する。ここで、ｐａｒａｍｓをボブの公開鍵であるとみなす。ボブは、自分の公開鍵ｐａｒａｍｓ用にＣＡからの証明書を入れる。アリスは、ボブにメールを送信したい場合、最初にボブの公開鍵ｐａｒａｍｓをボブの公開鍵証明書から取得する。ボブは、自分のｍａｓｔｅｒ－ｋｅｙを知っている唯一の人物であり、したがって、この設定には鍵エスクローはないことに注意されたい。

【０２１１】

１．ラップトップへの委託。アリスがＩＢＥ暗号鍵として現在の日付を使用してボブへのメールを暗号化すると仮定する（アリスは、ボブのｐａｒａｍｓをＩＢＥシステム・パラメータとして使用する）。ボブはｍａｓｔｅｒ－ｋｅｙを持っているので、このＩＢＥ暗号鍵に対応する秘密鍵を抽出して、メッセージを解読することが可能である。そこで、ボブは７日間旅行に出るとする。通常であれば、ボブは自分の秘密鍵を自分のラップトップに入れる。ラップトップが盗まれると、秘密鍵は危険にさらされることになる。ＩＢＥシステムを使用すると、ボブは単に、自分のラップトップに７日間の旅行期間に対応する７日分の秘密鍵をインストールするだけよい。ラップトップが盗まれた場合でも、７日間の秘密鍵しか損なわれない。ｍａｓｔｅｒ－ｋｅｙは、無事である。

【０２１２】

図１１は、本発明の一実施形態による鍵委託機能を備えるシステムを説明するブロック図である。システムは、ユーザ・システム１１０１およびターゲット・システム１１０２を備える。ターゲット・システムは、ラップトップ・コンピュータなどのコンピュータを含むことができる。ユーザ・システム１１０１は、解読鍵１１０４を作成するために使用される、マスター鍵１１０３を含む。解読鍵１１０４は、ターゲット・システム１１０２にダウンロードされる。上述の鍵取り消しの手法を使用すると、これらの解読鍵は、限られた期間のみ有効にすることができ、したがって、ターゲット・システム１１０１が危険にさらされた場合でも秘匿性を高められる。ユーザ・システム１１０１およびターゲット・システム１１０２は、メモリ１１０６および１１０７さらにプロセッサ１１０５および１１０８などのコンピュータ・システムの要素を備えることができる。ユーザ・システム１１０１は、ユーザＩＤ　１１１３および１つ以上の日付１１１４またはその他のタイムス

タンプから導かれる情報に基づきマスター鍵１１０３およびシステム・パラメータ１１１０を使用して秘密解読鍵１１０４を作成する鍵作成器論理回路１１０９を備える。ターゲット・システム１１０２は、ユーザ・システム１１０１およびシステム・パラメータ１１１０から得られた秘密解読鍵１１０４を使用して受信した暗号化されたメッセージ１１１２を解読する、解読論理回路１１１１を備える。ＩＤ　１１１３および日付１１１４の１つに基づいて公開鍵を使用してメッセージ１１１２が暗号化されている場合、秘密解読鍵を使用して、それを解読することができる。したがって、ターゲット・システム１１０２の解読機能を、選択した日付１１１４と関連するメッセージに制限することができる。他の実施形態では、ターゲット・システムは、必要に応じて他のコンピュータ・システムに接続することが可能なデータ記憶媒体または携帯型データ記憶デバイスとすることができ、そのため、これらのシステム上の解読鍵を使用することができる。

【０２１３】

２．職務の委任。アリスが、件名をＩＢＥ暗号鍵として使用してボブへのメールを暗号化するものとする。ボブは、自分のｍａｓｔｅｒ－ｋｅｙを使用してメールを解読することが可能である。そこで、ボブには、複数のアシスタントがおり、それぞれ異なる職務を担当していると仮定する（例えば、「購買」担当、「人事」担当など）。この本実施形態では、ボブはアシスタントの責任に対応する秘密鍵を１つ、各アシスタントに与えることができる。そこで、各アシスタントは、自分の責任範囲内の件名が設定されているメッセージを解読することは可能であるが、他のアシスタントを宛先とするメッセージを解読することは可能でない。アリスは、ボブからの単一の公開鍵（ｐａｒａｍｓ）のみを取得し、その公開鍵を使用して自分の選択した件名が含まれるメールを送信することに注意されたい。メールは、その件名の担当であるアシスタントにとってのみ可読である。

【０２１４】

より一般的には、ＩＢＥの実施形態により、多数の公開鍵を管理するさまざまなシステムを簡素化することが可能である。システムでは、公開鍵の大きなデータベースを保管するのではなく、ユーザの名前からこれらの公開鍵を導くか、または単に、整数１，．．．，ｎを異なる公開鍵として使用することが可能である。例えば、企業では、各社員に一意の社員番号を割り当て、その番号を社員の公開鍵としても使用することができる。

【０２１５】

受信確認返信

図１２は、本発明の一実施形態による受信確認返信機能を備える暗号システムを説明するブロック図である。本発明の一実施形態によれば、送信者は受信者が暗号化されたメッセージを受信したという確認を受信することが可能である。より一般的には、受信者から解読鍵の要求を受信したときに、ＰＫＧは解読鍵を受信者に与えることとは別のアクションを実行する。このようなアクションは、一実施形態による、メッセージを受信したことを示す受信確認を送信者に送る動作を含む。

【０２１６】

受信確認返信機能を備えるシステムの一実施形態が図１２に示されている。システムは、送信者システム１２０１、受信者システム１２０２、およびＰＫＧシステム１２０３を備える。送信者システム１２０１、受信者システム１２０２、およびＰＫＧシステム１２０３は、コンピュータ・ネットワークに結合されたコンピュータ・システムとして実装することができる。例えば、ＰＫＧ　１２０３、送信者システム１２０１、および受信者システム１２０２は、プロセッサ１２１２、プロセッサ１２１３、およびプロセッサ１２１４をそれぞれ備えることができる。これらのコンピュータ・システムは、コンピュータ可読記憶媒体、コンピュータ・メモリ、およびその他の記憶デバイスなどの要素を備えることができる。さらに、これらのシステムは、有線、無線、またはその他のネットワークとの通信に対応する技術を含む、コンピュータ・ネットワークとのインターフェイスを備えることができる。さらに、本発明の一実施形態によれば、それぞれの要素間の通信は、コンピュータ・ネットワーク上で送信されるデータ・パケットを使用して、または他のさまざまな形態の電子的およびデータ伝送および通信を使用して行うことができる。

【０２１７】
送信者１２０１は、メッセージＭを暗号化し、その結果得られた暗号文を受信確認返信要求情報１２０９も含むことができるデータ・パッケージ１２０４で受信者１２０２に送信する。受信確認返信要求情報は、例えば、返信アドレスおよび、特定のメッセージ１２０４に対応するメッセージ識別子を含むことができる。メッセージＭは、送信者により、暗号化論理回路１２１１および暗号鍵１２１５を使用して、暗号化される。暗号鍵１２１５は、受信者ＩＤ（電子メール・アドレスなど）１２１６および受信確認返信要求情報１２０９に基づくことができる。暗号鍵１２１５の決定のため送信者により受信者ＩＤおよび受信確認返信要求情報１２０９が使用されるため、受信者１２０２は、そのメッセージを解読するために使用することができる対応する解読鍵を必要とする。したがって、受信者システム１２０２は、メッセージ１２０４を受信したことに対する応答として、ＰＫＧ　１２０３に要求１２０６を送信するが、これには、受信確認返信要求情報１２０９および受信者のＩＤ、１２１６が含まれる。応答として、ＰＫＧ　１２０３は受信者１２０２に、秘密解読鍵１２０５を送信し、その後受信者はその解読鍵を解読論理回路１２１７で使用してメッセージ１２０４の暗号文を解読し、オリジナルのメッセージＭを復元する。受信者１２０２に解読鍵１２０５を送信するほかに、ＰＫＧ　１２０３はさらに、受信確認返信１２０７を送信者１２０１に送信する。ＰＫＧ　１２０３は、それとは別に、受信確認返信を送信するのではなく、ログの一部として受信結果を記憶媒体上に格納することができる。受信確認返信１２０７は、メッセージ識別子などの情報を含むことができる。こうして、送信者１２０１は、受信者１２０２がメッセージ１２０４を受信したという証明を受信する。システムは、プラグイン・ソフトウェアを送信者システム１２０１および受信者システム１２０２などさまざまなシステムに置くことにより初期化することができる。このようなプラグイン・ソフトウェアに、システム・パラメータを含めることができ、その一部はシステム・マスター鍵から導くことができる。送信者１２０１および受信者１２０２などのローカル・デバイスに格納されているこのようなパラメータを使用して、暗号鍵の作成、暗号化の実行、解読の実行、およびその他の機能を、適宜行う。

【０２１８】
Ｗｅｉｌペアリングの説明
この節では、楕円曲線上のＷｅｉｌペアリングについて説明し、その後、アルゴリズムを使用して効率よく計算する方法を示す。具体的には、ｐ＞３の素体★Ｆ$_{p}$上で定義された超特異楕円曲線を使用する例を示す（ｐ＝２　ｍｏｄ　３の★Ｆ$_{p}$上の曲線$y^{2}=x^{3}+1$がこのような曲線の一例である）。以下の説明は、他の楕円曲線上のＷｅｉｌペアリングの計算に容易に一般化できる。

【０２１９】
楕円曲線とＷｅｉｌペアリング
ｐ＞３の素体★Ｆ$_{p}$上で定義された超特異楕円曲線に関する初等的な事実をいくつか述べる。

【０２２０】
事実１：超特異曲線Ｅ／★Ｆ$_{p}$（ｐ＞３）は★Ｆ$_{p}$内にｐ＋１個の点を含む。Ｏで無限遠の点を表す。★Ｆ$_{p}$上の点の群は、位数ｐ＋１の巡回群をなす。簡単にするため、Ｐをこの群の作成要素とし、ｎ＝ｐ＋１と設定する。

【０２２１】
事実２：点Ｅ（★Ｆ■）の群は、Ｅ（★Ｆ$_{p}$）内の点に関して一次独立である位数ｎの点Ｑを含む。したがって、Ｅ（★Ｆ■）は、群★$Z^{2}{}_{n}$に同型な部分群を含む。この群は、Ｐ∈Ｅ（★Ｆ$_{p}$）およびＱ∈Ｅ（★Ｆ■）によって作成される。この群をＥ［ｐ＋１］＝Ｅ［ｎ］で表す。

【０２２２】
Ｅ［ｎ］内の点の対を★$Ｆ^{*}$■に写像するＷｅｉｌペアリングｅ、つまりｅ：Ｅ［ｎ］×Ｅ［ｎ］→★$Ｆ^{*}$■を扱う。このペアリングを説明するために、以下の概念を復習する。

【０２２３】

因子　因子とは、曲線Ｅ（★Ｆ■）上の点の形式和のことである。ａＰ∈★Ｚ、Ｐ∈Ｅ（★Ｆ■）として、因子を＄Ａ＝Σ$_{Ｐ}$ａ$_{Ｐ}$（Ｐ）と書く。例えば、＄Ａ＝３（Ｐ$_{1}$）－２（Ｐ$_{2}$）－（Ｐ$_{3}$）は因子である。ここでは、Σ$_{Ｐ}$ａ$_{Ｐ}$＝０として、因子＄Ａ＝Σ$_{Ｐ}$ａ$_{Ｐ}$（Ｐ）のみを考える。

【０２２４】

関数　概して、曲線Ｅ（★Ｆ■）上の関数ｆは、有理関数ｆ（ｘ，ｙ）∈★Ｆ■（ｘ，ｙ）とみなすことができる。任意の点Ｐ＝（ｘ，ｙ）∈Ｅ（★Ｆ■）について、ｆ（Ｐ）＝ｆ（ｘ，ｙ）と定義する。

【０２２５】

関数の因子　ｆを曲線Ｅ（★Ｆ■）上の関数とする。この因子を（ｆ）＝Σ$_{Ｐ}$ｏｒｄ$_{Ｐ}$（ｆ）・Ｐで定義し、（ｆ）で表す。ここで、ｏｒｄ$_{Ｐ}$（ｆ）は点Ｐにおけるｆの零位数である。例えば、ａｘ＋ｂｙ＋ｃ＝０を、Ｐ$_{1}$≠±Ｐ$_{2}$となるような点Ｐ$_{1}$、Ｐ$_{2}$∈Ｅ（★Ｆ■）を通る直線とする。この直線は、第３の点Ｐ$_{3}$∈Ｅ（★Ｆ■）で曲線と交差する。そこで、関数ｆ（ｘ，ｙ）＝ａｘ＋ｂｙ＋ｃは３つの零点Ｐ$_{1}$、Ｐ$_{2}$、Ｐ$_{3}$を持ち、無限遠で位数３の極を持つ。ｆの因子は、（ｆ）＝（Ｐ$_{1}$）＋（Ｐ$_{2}$）＋（Ｐ$_{3}$）－３（Ｏ）となる。

【０２２６】

主因子　＄Ａを因子とする。（ｆ）＝＄Ａとなるような関数ｆが存在すれば、＄Ａは主因子であるという。因子＄Ａ＝Σ$_{Ｐ}$ａ$_{Ｐ}$（Ｐ）が主因子であるのは、Σ$_{Ｐ}$ａ$_{Ｐ}$＝０および＄Ａ＝Σ$_{Ｐ}$ａ$_{Ｐ}$Ｐ＝Ｏのときかつそのときに限ることが知られている。第２の和では、曲線上の群作用を使用していることに注意されたい。さらに、主因子＄Ａが与えられた場合、（＄Ａ）＝（ｆ）となるような一意的な関数ｆ（定数倍を除いて）が存在する。

【０２２７】

因子の同値性　２つの因子＄Ａ、＄Ｂは、差＄Ａ－＄Ｂが主因子であれば、同値であるという。任意の因子＄Ａ＝Σ$_{Ｐ}$ａ$_{Ｐ}$（Ｐ）（Σ$_{Ｐ}$ａ$_{Ｐ}$＝０の場合）は、あるＱ∈Ｅが存在して、＄Ａ’＝（Ｑ）－（Ｏ）の形式の因子に同値であることが知られている。Ｑ＝Σ$_{Ｐ}$ａ$_{Ｐ}$Ｐであることに注意されたい。

【０２２８】

表記　関数ｆおよび因子＄Ａ＝Σ$_{Ｐ}$ａ$_{Ｐ}$（Ｐ）が与えられたときに、ｆ（＄Ａ）をｆ（＄Ａ）＝Π$_{Ｐ}$ｆ（Ｐ）$^{ａ Ｐ}$と定義する。Σ$_{Ｐ}$ａ$_{Ｐ}$＝０なので、任意のｃ∈★Ｆ■についてｆの代わりにｃｆを使用してもｆ（＄Ａ）は変わらないことに注意されたい。

【０２２９】

これで、２つの点Ｐ、Ｑ∈Ｅ［ｎ］のＷｅｉｌペアリングを説明する準備ができた。＄Ａ$_{Ｐ}$を因子（Ｐ）－（Ｏ）に同値なある因子とする。ｎ＄Ａ$_{Ｐ}$は主因子であることが知られている（これは、明らかに主因子であるｎ（Ｐ）－ｎ（Ｏ）と同値である）。したがって、（ｆ$_{Ｐ}$）＝ｎ＄Ａ$_{Ｐ}$となるような関数ｆＰが存在する。＄Ａ$_{Ｑ}$およびｆ$_{Ｑ}$を同様に定義する。ＰおよびＱのＷｅｉｌペアリングは以下の式で与えられる。

【０２３０】

【数８】

$$e(P,Q)=\frac{f_P(\mathcal{A}_Q)}{f_Q(\mathcal{A}_P)}$$

この比が矛盾なく定義されている限り（つまり、零による除算が生じない限り）、この比からＰとＱのＷｅｉｌペアリングの値が求められる。この比が不確定の場合、別の因子＄Ａ$_{Ｐ}$、＄Ａ$_{Ｑ}$を使用して、ｅ（Ｐ，Ｑ）を定義する。Ｐ、Ｑ∈Ｅ（★Ｆ■）ならば、ｅ（Ｐ，Ｑ）∈★Ｆ■である。

【０２３１】

Ｗｅｉｌペアリングが矛盾なく定義されていることを簡単に証明する。つまり、ｅ（Ｐ，Ｑ）の値は、$Ａ$Ｐが（Ｐ）－（Ｏ）に同値である限り因子$Ａ$Ｐの選択とは無関係であり、$Ａ$Ｐから矛盾なく定義された値が得られる。同じことが$Ａ$Ｑについても成り立つ。$Ａ^$Ｐを$Ａ$Ｐと同値な因子とし、ｆ^Ｐを、（ｆ^Ｐ）＝ｎＡ^Ｐとなるような関数とする。すると、ある関数ｇが存在して$Ａ^Ｐ＝$Ａ$Ｐ＋（ｇ）、ｆ^Ｐ＝ｆ$Ｐ・ｇ^{n}となる。そこで、以下の式が得られた。

【０２３２】

【数９】

$$e(P,Q)=\frac{\hat{f}_P(\mathcal{A}_Q)}{f_Q(\hat{\mathcal{A}}_P)}=\frac{f_P(\mathcal{A}_Q)g(\mathcal{A}_Q)^n}{f_Q(\mathcal{A}_P)f_Q((g))}=\frac{f_P(\mathcal{A}_Q)}{f_Q(\mathcal{A}_P)}\cdot\frac{g(n\mathcal{A}_Q)}{f_Q((g))}=\frac{f_P(\mathcal{A}_Q)}{f_Q(\mathcal{A}_P)}\cdot\frac{g((f_Q))}{f_Q((g))}=\frac{f_P(\mathcal{A}_Q)}{f_Q(\mathcal{A}_P)}$$

最後の式は、任意の２つの関数ｆ、ｇについて、ｆ（（ｇ））＝ｇ（（ｆ））が成り立つというＷｅｉｌ相互律と呼ばれる事実から求められる。ゆえに、Ｗｅｉｌペアリングは矛盾なく定義されている。

【０２３３】

事実１０　Ｗｅｉｌペアリングは、以下の特性を持つ。

・　すべてのＰ∈Ｅ［ｎ］について、ｅ（Ｐ，Ｐ）＝１である。

・　双線形：　ｅ（Ｐ$_{1}$＋Ｐ$_{2}$，Ｑ）＝ｅ（Ｐ$_{1}$，Ｑ）・ｅ（Ｐ$_{2}$，Ｑ）およびｅ（Ｐ，Ｑ$_{1}$＋Ｑ$_{2}$）＝ｅ（Ｐ，Ｑ$_{1}$）・ｅ（Ｐ，Ｑ$_{2}$）が成り立つ。

【０２３４】

・　Ｐ，Ｑ∈Ｅ［ｎ］が共線形ならば、ｅ（Ｐ，Ｑ）＝１である。同様にｅ（Ｐ，Ｑ）＝ｅ（Ｑ，Ｐ）$^{-1}$である。

・　ｎ番目の根：すべてのＰ、Ｑ∈Ｅ［ｎ］について、ｅ（Ｐ，Ｑ）^{n}＝１である。

【０２３５】

・　非退化：すべてのすべてのＱ∈Ｅ［ｎ］についてＰがｅ（Ｐ，Ｑ）＝１を満たせば、Ｐ＝Ｏである。

すでに述べたように、ＩＢＥ方式の一実施形態のこの詳細な例では、修正したＷｅｉｌペアリングｅ^（Ｐ，Ｑ）＝ｅ（Ｐ，φ（Ｑ））を使用し、φはＥの点のなす群上の自己同型写像である。

【０２３６】

Ｔａｔｅペアリング。Ｔａｔｅペアリングは、このシステムの実施形態の必要な特性を有するもう１つの双線形ペアリングである。さまざまなを実施形態において、Ｔａｔｅペアリングのオリジナルの定義を少し修正して本明細書の目的に合わせる。ｆ$Ｐ$および$Ａ$Ｐを前のように定義して、２つの点Ｐ、Ｑ∈Ｅ［ｎ］のＴａｔｅペアリングを

【０２３７】

【数１０】

$$T(P,Q)=f_P(\mathcal{A}_Q)^{|\mathbf{F}_{p^2}^*|/n}$$

として定義する。この定義から、計算可能な双線形ペアリングＴ：Ｅ［ｎ］×Ｅ［ｎ］→★Ｇ$_{2}$が得られる。

【０２３８】

Ｗｅｉｌペアリングの計算

２つの点Ｐ、Ｑ∈Ｅ［ｎ］が与えられたとして、★Ｆ$_{p}$におけるＯ（ｌｏｇ　ｐ）の算術

演算を使用してｅ（Ｐ，Ｑ）∈★Ｆ＊■を計算する方法を示す。Ｐ≠Ｑと仮定する。次のように進める。２つのランダムな点Ｒ１、Ｒ２∈Ｅ［ｎ］を選ぶ。因子＄Ａｐ＝（Ｐ＋Ｒ１）－（Ｒ１）および＄ＡＱ＝（Ｑ＋Ｒ２）－（Ｒ２）を考える。これらの因子は、（Ｐ）－（Ｏ）および（Ｑ）－（Ｏ）とそれぞれ同値である。そこで、＄ＡＰおよび＄ＡＱを使用して、Ｗｅｉｌペアリングを以下のように計算することが可能である。

【０２３９】

【数１１】

$$e(P,Q) = \frac{f_P(\mathcal{A}_Q)}{f_Q(\mathcal{A}_P)} = \frac{f_P(Q+R_2)f_Q(R_1)}{f_P(R_2)f_Q(P+R_1)}$$

この式は、Ｒ１、Ｒ２の選択に関して非常に高い確率で矛盾なく定義されている（失敗の確率は、最大でＯ（ｌｏｇ　ｐ／ｐ）である。ｅ（Ｐ，Ｑ）の計算中に零除算が発生するまれなケースでは、単純に、新しいランダム点Ｒ１、Ｒ２を選んで、この工程を繰り返す。

【０２４０】

ｅ（Ｐ，Ｑ）を評価するために、＄ＡＱで関数ｆＰを評価する方法を示すだけで十分である。ｆＱ（＄ＡＰ）の評価も同様に行われる。倍するのを繰り返してｆＰ（＄ＡＰ）を評価する。正の整数ｂについて、因子を以下のように定義する。

【０２４１】

＄Ａｂ＝ｂ（Ｐ＋Ｒ１）－ｂ（Ｒ１）－（ｂＰ）＋（Ｏ）

これは主因子であり、したがって、（ｆｂ）＝＄Ａｂとなるような関数ｆｂが存在する。（ｆＰ）＝（ｆｎ）であり、したがって、ｆＰ（＄ＡＱ）＝ｆｎ（＄ＡＱ）であることに注意されたい。ｆｎ（＄ＡＱ）を評価する方法を示すので十分である。

【０２４２】

補助定理１１　あるｂ、ｃ＞０についてｆｂ（＄ＡＱ）、ｆｃ（＄ＡＱ）、およびｂＰ、ｃＰ、（ｂ＋ｃ）Ｐが与えられた場合に、ｆｂ＋ｃ（＄ＡＱ）を出力するアルゴリズム＄Ｄが存在する。このアルゴリズムは、★Ｆ■における（少ない）一定数の算術演算を使用するだけである。

【０２４３】

証明　まず、２つの補助線形関数ｇ１、ｇ２を定義する。

１．ａ１ｘ＋ｂ１ｙ＋ｃ１＝０が点ｂＰおよびｃＰを通過する直線とする（ｂ＝ｃであれば、ａ１ｘ＋ｂ１ｙ＋ｃ１＝０をｂＰでＥに接する直線とする）。ｇ１（ｘ，ｙ）＝ａ１ｘ＋ｂ１ｙ＋ｃ１を定義する。

【０２４４】

２．ｘ＋ｃ２＝０を、点（ｂ＋ｃ）Ｐを通過する垂直線とする。ｇ２（ｘ，ｙ）＝ｘ＋ｃ２を定義する。

これらの関数の因子は以下のとおりである。

【０２４５】

（ｇ１）＝（ｂＰ）＋（ｃＰ）＋（－（ｂ＋ｃ）Ｐ）－３（Ｏ）

（ｇ２）＝（（ｂ＋ｃ）Ｐ）＋（－（ｂ＋ｃ）Ｐ）－２（Ｏ）

定義から、以下の式が得られる。

【０２４６】

＄Ａｂ＝ｂ（Ｐ＋Ｒ１）－ｂ（Ｒ１）－（ｂＰ）＋（Ｏ）

＄Ａｃ＝ｃ（Ｐ＋Ｒ１）－ｃ（Ｒ１）－（ｃＰ）＋（Ｏ）

＄Ａ（ｂ＋ｃ）＝（ｂ＋ｃ）（Ｐ＋Ｒ１）－（ｂ＋ｃ）（Ｒ１）－（（ｂ＋ｃ）Ｐ）＋（Ｏ）

そこで、＄Ａ（ｂ＋ｃ）＝＄Ａｂ＋＄Ａｃ＋（ｇ１）－（ｇ２）が得られる。ゆえに、以

下の式が得られる。

【０２４７】

【数１２】

$$f_{b+c}(\mathcal{A}_Q) = f_b(\mathcal{A}_Q) \cdot f_c(\mathcal{A}_Q) \cdot \frac{g_1(\mathcal{A}_Q)}{g_2(\mathcal{A}_Q)} \qquad (1)$$

このことから、f_{b+c}（A_Q）を評価するには、すべてのｉ＝１，２についてg_i（A_Q）を評価し、その結果を式１に差し込むだけで十分である。したがって、f_b（A_Q）、ｆｃ（A_Q）、およびｂＰ、ｃＰ、（ｂ＋ｃ）Ｐが与えられると、一定数の算術演算を使用してf_{b+c}（A_Q）を計算することが可能である。

【０２４８】

補助定理１１のアルゴリズム＄Ｄの出力を、＄Ｄ（f_b（A_Q），f_c（A_Q），ｂＰ，ｃＰ，（ｂ＋ｃ）Ｐ）＝f_{b+c}（A_Q）により表す。次に、以下の標準の倍増手順を使用してf_P（A_Q）＝f_n（A_Q）を計算することが可能である。ｎ＝$b_m b_{m-1} \ldots b_1 b_0$をｎの２進数表現とする、つまり、$n = \Sigma^m_{i=0} b_i 2^i$である。

【０２４９】

開始：Ｚ＝Ｏ、Ｖ＝f_0（A_Q）＝１、およびｋ＝０と設定する。

反復：ｉ＝ｍ，ｍ－１，．．．，１，０について以下を実行する。

１：b_i＝１ならば、Ｖ＝＄Ｄ（Ｖ，f_1（A_Q），Ｚ，Ｐ，Ｚ＋Ｐ）を設定し、Ｚ＝Ｚ＋Ｐを設定し、ｋ＝ｋ＋１を設定する。

【０２５０】

２：ｉ＞０ならば、Ｖ＝＄Ｄ（Ｖ，Ｖ，Ｚ，Ｚ，２Ｚ）を設定し、Ｚ＝２Ｚを設定し、ｋ＝２ｋを設定する。

３：各反復の終わりに、ｚ＝ｋＰおよびＶ＝f_k（A_Q）となることに注意されたい。

【０２５１】

出力：最後の反復の後、ｋ＝ｎとなり、したがって、必要に応じてＶ＝f_n（$_{A_Q}$）である。

Ｗｅｉｌペアリングｅ（Ｐ，Ｑ）を評価するために、上記のアルゴリズムを１回実行し、f_P（A_Q）を計算し、１回実行してf_Q（A_P）を計算する。反復二乗アルゴリズムはf_1（A_Q）に評価する必要があることに注意されたい。関数f_1（ｘ，ｙ）（その因子は（f_1）＝（Ｐ＋R_1）－（R_1）－（Ｐ）＋（Ｏ））は以下のように明示的に書くことが可能なので、この作業は簡単に行える。

【０２５２】

１．$a_1 x + b_1 y + c_1 = 0$を、点ＰおよびR_1を通過する直線とする。関数g_1（ｘ，ｙ）＝$a_1 x + b_1 y + c_1$を定義する。

２．ｘ＋c_2＝０を、点Ｐ＋R_1を通過する垂直線とする。関数g_2（ｘ，ｙ）＝ｘ＋c_2を定義する。

【０２５３】

３．関数f_1（ｘ，ｙ）は単に、f_1（ｘ，ｙ）＝g_2（ｘ，ｙ）／g_1（ｘ，ｙ）であり、★Ｆ■において容易に評価できる。

【図面の簡単な説明】

【０２５４】

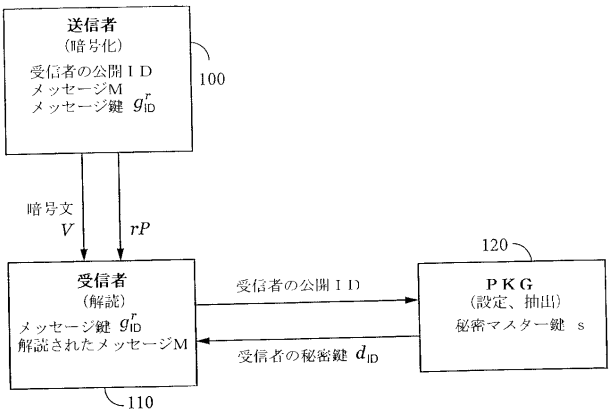
【図１】送信者、受信者、および個人鍵作成器（ＰＫＧ）によって実行される工程およびそれらの間でやり取りされる情報を示す、本発明の実施形態による暗号システムを説明するブロック図。

【図２】本発明の一実施形態により秘密鍵を作成するときにＰＫＧによって実行される工程を説明するブロック図。

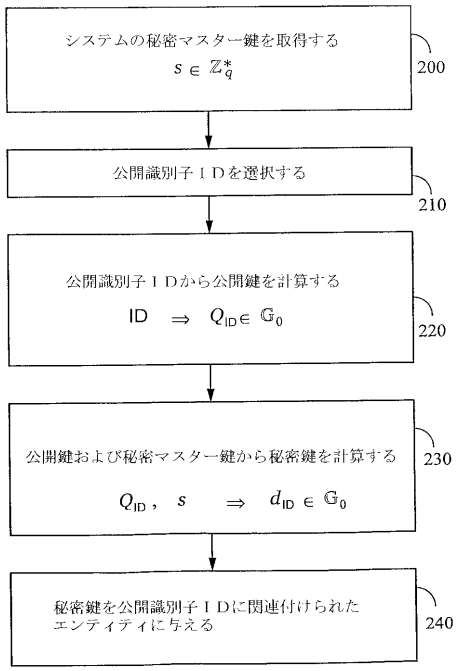
【図３】本発明の一実施形態により秘密メッセージ鍵を計算し、その鍵を使用して受信者

を送り先とするメッセージを暗号化する場合に送信者によって実行される工程を説明するブロック図。
【図４】本発明の一実施形態により秘密メッセージ鍵を計算し、その鍵を使用して送信者から受信した暗号文を解読する場合に受信者によって実行される工程を説明するブロック図。
【図５】本発明の一実施形態による分散ＰＫＧを説明するブロック図。
【図６】本発明の一実施形態によるエスクロー解読機能を備える暗号システム内の要素を説明するブロック図。
【図７】本発明の一実施形態によるエスクロー解読機能を備えるＥｌＧａｍａｌ暗号システムでメッセージを暗号化する場合に送信者によって実行される工程を説明するブロック図。
【図８】本発明の一実施形態によるエスクロー解読機能を備えるＥｌＧａｍａｌ暗号システムでメッセージを解読する場合に受信者によって実行される工程を説明するブロック図。
【図９】本発明の他の実施形態によるエスクロー解読機能を備えるＥｌＧａｍａｌ暗号システムでメッセージを解読する場合にエスクローによって実行される工程を説明するブロック図。
【図１０】本発明の一実施形態によりＩＤベース暗号化システムで信用状を管理するシステムを説明するブロック図。
【図１１】本発明の一実施形態による鍵委託機能を備えるシステムを説明するブロック図。
【図１２】本発明の一実施形態による受信確認返信機能を備える暗号システムを説明するブロック図。

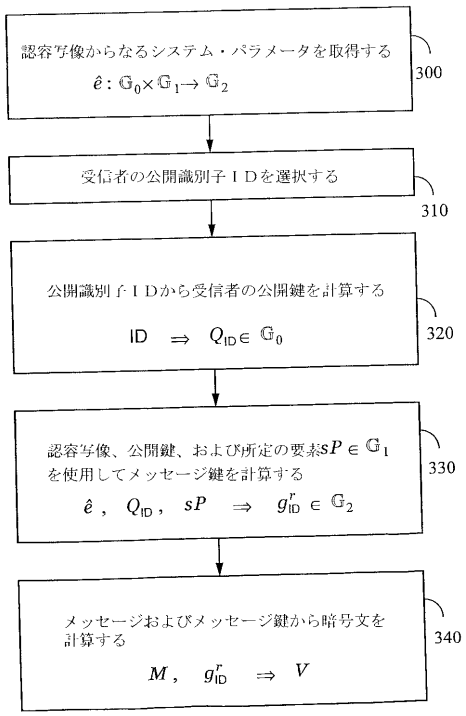
【図１】



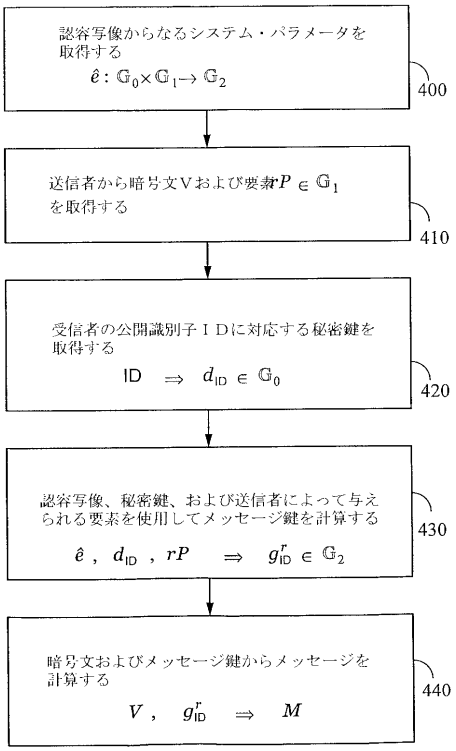
【図２】



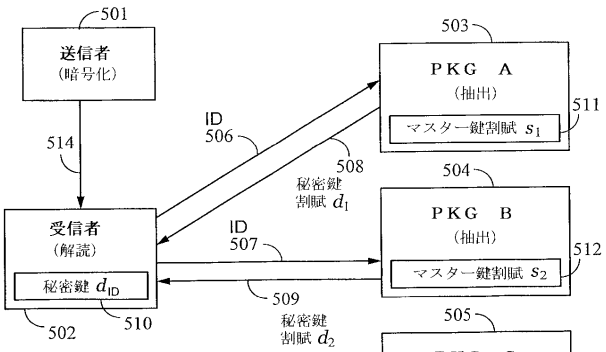
【図３】


認容写像からなるシステム・パラメータを取得する
$\hat{e}: \mathbb{G}_0 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$
300
受信者の公開識別子ＩＤを選択する
310
公開識別子ＩＤから受信者の公開鍵を計算する
ID $\Rightarrow$ $Q_{ID} \in \mathbb{G}_0$
320
認容写像、公開鍵、および所定の要素$sP \in \mathbb{G}_1$を使用してメッセージ鍵を計算する
$\hat{e}$, Q_{ID}, sP $\Rightarrow$ $g_{ID}^r \in \mathbb{G}_2$
330
メッセージおよびメッセージ鍵から暗号文を計算する
M, g_{ID}^r $\Rightarrow$ V
340

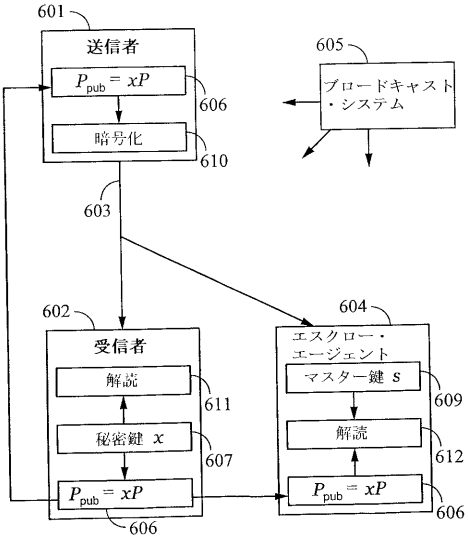
【図４】


認容写像からなるシステム・パラメータを取得する
$\hat{e}: \mathbb{G}_0 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$
400
送信者から暗号文Ｖおよび要素$rP \in \mathbb{G}_1$を取得する
410
受信者の公開識別子ＩＤに対応する秘密鍵を取得する
ID $\Rightarrow$ $d_{ID} \in \mathbb{G}_0$
420
認容写像、秘密鍵、および送信者によって与えられる要素を使用してメッセージ鍵を計算する
$\hat{e}$, d_{ID}, rP $\Rightarrow$ $g_{ID}^r \in \mathbb{G}_2$
430
暗号文およびメッセージ鍵からメッセージを計算する
V, g_{ID}^r $\Rightarrow$ M
440

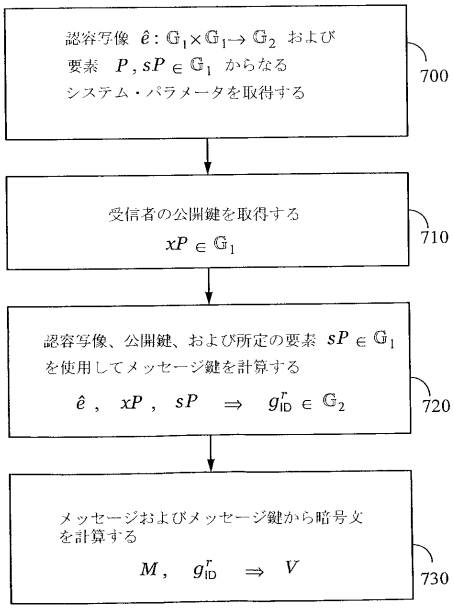
【図５】


501
送信者
（暗号化）
514
受信者
（解読）
秘密鍵 d_{ID}
502
510
ID
506
秘密鍵
割賦 d_1
508
ID
507
509
秘密鍵
割賦 d_2
503
ＰＫＧ Ａ
（抽出）
マスター鍵割賦 s_1
511
504
ＰＫＧ Ｂ
（抽出）
マスター鍵割賦 s_2
512
505
ＰＫＧ Ｃ
（抽出）
マスター鍵割賦 s_3
513

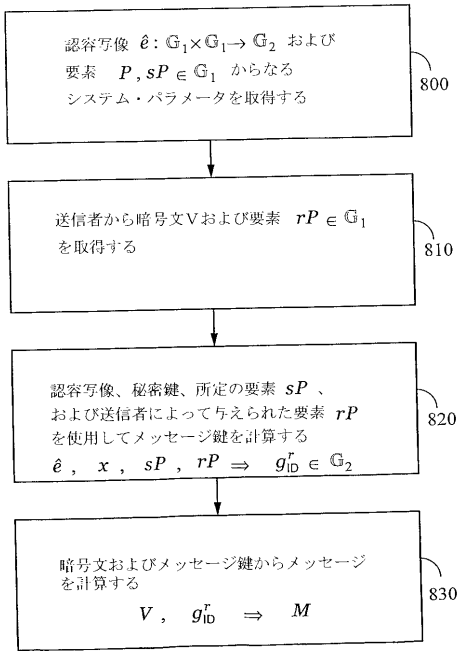
【図６】


601
送信者
$P_{pub} = xP$
606
暗号化
610
603
605
ブロードキャスト
・システム
602
受信者
解読
611
秘密鍵 x
607
$P_{pub} = xP$
606
604
エスクロー・
エージェント
マスター鍵 s
609
解読
612
$P_{pub} = xP$
606

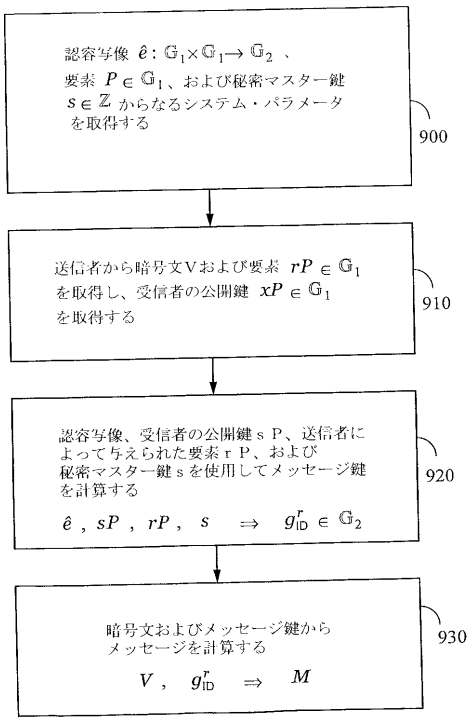
【図７】


認容写像 $\hat{e}: \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ および
要素 $P, sP \in \mathbb{G}_1$ からなる
システム・パラメータを取得する
700
受信者の公開鍵を取得する
$xP \in \mathbb{G}_1$
710
認容写像、公開鍵、および所定の要素 $sP \in \mathbb{G}_1$
を使用してメッセージ鍵を計算する
$\hat{e}$, xP , sP $\Rightarrow$ $g_{ID}^{r} \in \mathbb{G}_2$
720
メッセージおよびメッセージ鍵から暗号文
を計算する
M , g_{ID}^{r} $\Rightarrow$ V
730

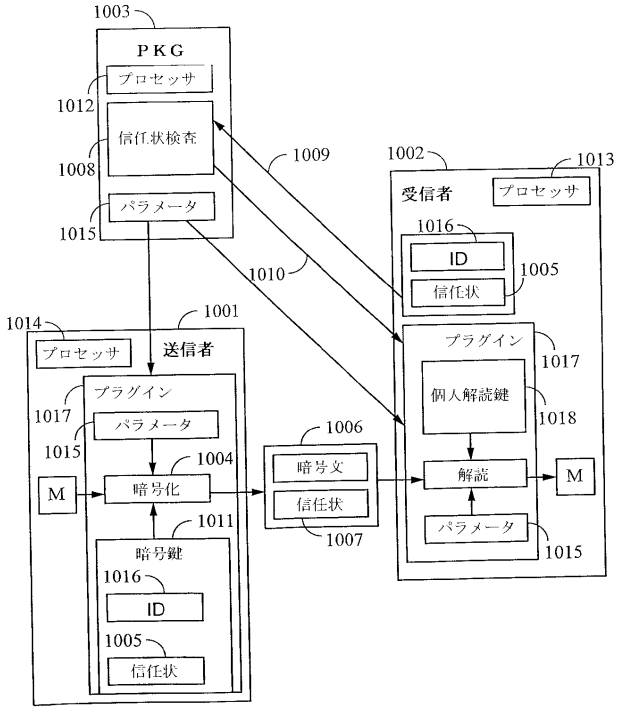
【図８】


認容写像 $\hat{e}: \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ および
要素 $P, sP \in \mathbb{G}_1$ からなる
システム・パラメータを取得する
800
送信者から暗号文Vおよび要素 $rP \in \mathbb{G}_1$
を取得する
810
認容写像、秘密鍵、所定の要素 sP 、
および送信者によって与えられた要素 rP
を使用してメッセージ鍵を計算する
$\hat{e}$, x , sP , rP $\Rightarrow$ $g_{ID}^{r} \in \mathbb{G}_2$
820
暗号文およびメッセージ鍵からメッセージ
を計算する
V , g_{ID}^{r} $\Rightarrow$ M
830

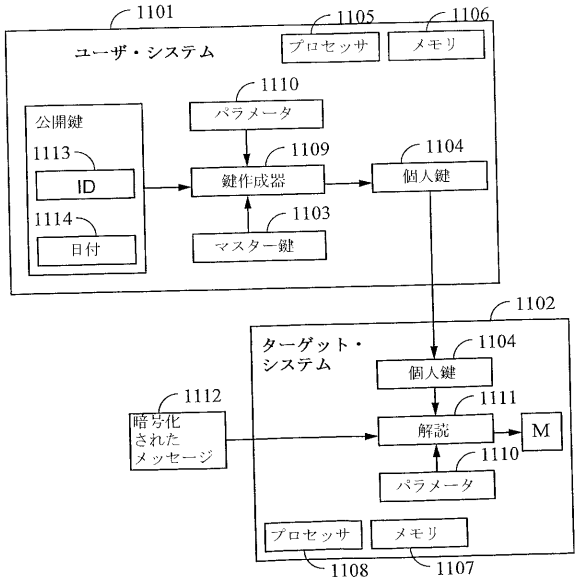
【図９】


認容写像 $\hat{e}: \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ 、
要素 $P \in \mathbb{G}_1$、および秘密マスター鍵
$s \in \mathbb{Z}$ からなるシステム・パラメータ
を取得する
900
送信者から暗号文Vおよび要素 $rP \in \mathbb{G}_1$
を取得し、受信者の公開鍵 $xP \in \mathbb{G}_1$
を取得する
910
認容写像、受信者の公開鍵ｓＰ、送信者に
よって与えられた要素ｒＰ、および
秘密マスター鍵ｓを使用してメッセージ鍵
を計算する
$\hat{e}$, sP , rP , s $\Rightarrow$ $g_{ID}^{r} \in \mathbb{G}_2$
920
暗号文およびメッセージ鍵から
メッセージを計算する
V , g_{ID}^{r} $\Rightarrow$ M
930

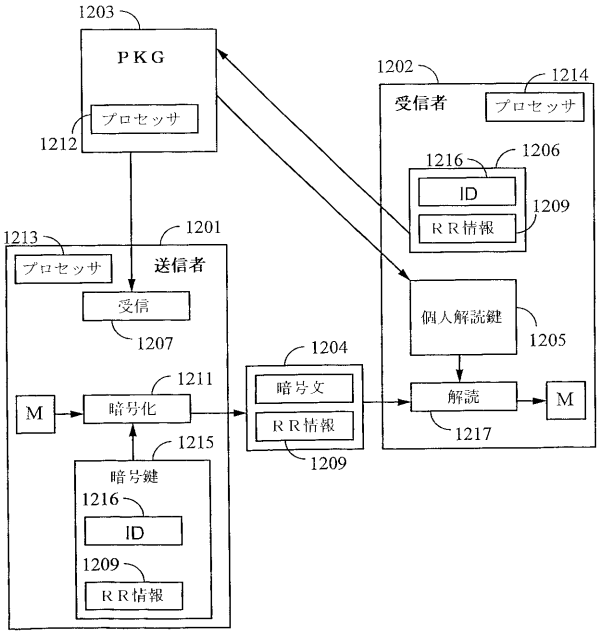
【図１０】


1003
PKG
プロセッサ
1012
信任状検査
1008
パラメータ
1015
1009
1010
1002
受信者
1013
プロセッサ
1016
ID
信任状
1005
1014
プロセッサ
1001
送信者
プラグイン
1017
パラメータ
1015
M
暗号化
1004
1011
暗号鍵
1016
ID
1005
信任状
1006
暗号文
信任状
1007
プラグイン
1017
個人解読鍵
1018
解読
M
パラメータ
1015

【図１１】


1101
ユーザ・システム
1105
プロセッサ
1106
メモリ
1110
パラメータ
公開鍵
1113
ID
1114
日付
1109
鍵作成器
1104
個人鍵
1103
マスター鍵
1102
ターゲット・システム
1104
個人鍵
1112
暗号化されたメッセージ
1111
解読
M
1110
パラメータ
プロセッサ
メモリ
1108
1107

【図１２】


1203
PKG
プロセッサ
1212
1202
受信者
1214
プロセッサ
1216
1206
ID
1209
RR情報
1213
プロセッサ
1201
送信者
受信
1207
個人解読鍵
1205
1204
暗号文
RR情報
1209
M
1211
暗号化
1215
暗号鍵
1216
ID
1209
RR情報
解読
M
1217

【国際公開パンフレット】

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
27 February 2003 (27.02.2003)

PCT

(10) International Publication Number
WO 03/017559 A2

(51) International Patent Classification⁷: H04L

(21) International Application Number: PCT/US02/27155

(22) International Filing Date: 13 August 2002 (13.08.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/311,946 13 August 2001 (13.08.2001) US

(71) Applicant: **BOARD OF TRUSTEES OF THE LELAND STANFORD JUNIOR UNIVERSITY** [US/US]; 900 Welch Road, Suite 350, Palo Alto, CA 94304 (US).

(72) Inventors: **BONEH, Dan**; Gates 475, Stanford, CA 94305-9045 (US). **FRANKLIN, Matthew**; 3021 Engineering II, Davis, CA 95616 (US).

(74) Agent: **ALBOSZTA, Marek**; 45 Cabot Ave., Suite 110, Santa Clara, CA 95051 (US).

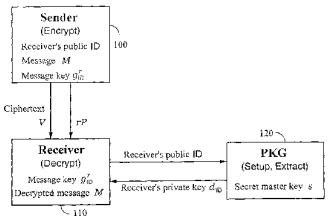
(81) Designated States *(national)*: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
without international search report and to be republished upon receipt of that report

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) **Title:** SYSTEMS AND METHODS FOR IDENTITY-BASED ENCRYPTION AND RELATED CRYPTOGRAPHIC TECHNIQUES



(57) **Abstract:** A method and system for encrypting a first piece of information *M* to be sent by a sender (100) to a receiver (110) allows both sender and receiver to compute a secret message key using identity-based information and a bilinear map. In a one embodiment, the sender (100) computes an identity-based encryption key from an identifier ID associated with the receiver (110). The identifier ID may include various types of information such as the receiver's e-mail address, a receiver credential, a message identifier, or a date. The sender uses a bilinear map and the encryption key to compute a secret message key g'_{ID}, which is then used to encrypt a message *M*, producing ciphertext *V* to be sent from the sender (100) to the receiver (110) together with an element *rP*. An identity-based decryption key d_{ID} is computed by a private key generator (120) based on the ID associated with the receiver and a secret master key *s*. After obtaining the private decryption key from the key generator (120), the receiver (110) uses it together with the element *rP* and the bilinear map to compute the secret message key g'_{ID}, which is then used to decrypt *V* and recover the original message *M*. According to one embodiment, the bilinear map is based on a Weil pairing or a Tate pairing defined on a subgroup of an elliptic curve. Also described are several applications of the techniques, including key revocation, credential management, and return receipt notification.

WO 03/017559 A2

SYSTEMS AND METHODS FOR IDENTITY-BASED ENCRYPTION AND RELATED CRYPTOGRAPHIC TECHNIQUES

CROSS-REFERENCE TO RELATED APPLICATIONS

This application claims the benefit of U.S. provisional application number 60/311946, filed 08/13/2001, which is incorporated herein by reference.

STATEMENT REGARDING FEDERALLY SPONSORED RESEARCH OR DEVELOPMENT

The present invention was made with the support of DARPA contract F30602-99-1-0530. The U.S. Government has certain rights in the invention.

REFERENCE TO COMPACT DISK APPENDIX

Not applicable.

BACKGROUND OF THE INVENTION

The field of the present invention relates generally to cryptographic systems.

Public-key cryptographic systems allow two people to exchange private and authenticated messages without requiring that they first have a secure communication channel for sharing private keys. One of the most widely used public-key cryptosystem is the RSA cryptosystem disclosed in U.S. Pat. No. 4,405,829. The RSA cryptosys-

tem is currently deployed in many commercial systems. It is used by web servers and browsers to secure web traffic, it is used to ensure privacy and authenticity of e-mail, it is used to secure remote login sessions, and it is at the heart of electronic credit-card payment systems. In short, RSA is frequently used in applications where security of digital data is a concern.

According to public-key cryptosystems such as the RSA cryptosystem, each person has a unique pair of keys: a private key that is a secret and a public key that is widely known. This pair of keys has two important properties: (1) the private key cannot be deduced from knowledge of the public key alone, and (2) the two keys are complementary, i.e., a message encrypted with one key of the pair can be decrypted only with the complementary key. In these systems, both the public key and the private key in a pair are generated together as the output of a key generation algorithm that takes as input a random seed. Consequently, in these cryptosystems, people cannot choose a desired public or private key, but must simply use the keys that are generated for them by a key generation algorithm. This has the disadvantage that others cannot encrypt messages to a person until that person generates and publishes a public key. Another problem with this type of cryptosystem is that an impostor can publish a public key and claim that it belongs to someone else. To address this issue, a trusted certificate authority (CA) is used to authenticate individuals and certify to others that the individual's public key is authentic. Unfortunately, this adds complexity to the cryptosystem since a sender must obtain a certificate for every receiver, and must obtain a new certificate every time an existing certificate expires. It also requires receivers to create public keys, publish them, register certificates with the CA, and renew such certificates when they expire.

In 1984 Shamir envisioned a new type of public key encryption scheme (described in A. Shamir, "Identity-based cryptosystems and signature schemes", in *Advances in Cryptology - Crypto '84*, Lecture Notes in Computer Science, Vol. 196, Springer-Verlag, pp. 47-53, 1984). According to Shamir's scheme, a person's public key consists of a public identifier, which may be the person's name and network address, or combination of name and e-mail address, social security number, street address, telephone number, or office address. Because the public key is the person's pre-existing public identifier (ID) rather than a key produced from a random seed, this kind of public key cryptosystem is called an identity-based encryption (IBE) scheme. Shamir, however,

did not provide a concrete, practical IBE cryptosystem. In fact, Shamir argued that existing cryposystems (such as RSA) could not be adapted to realize a secure IBE cryptosystem.

In the years since Shamir proposed his IBE scheme there have been several attempts to realize an identity-based cryptosystem. Some proposals require that users not collude. Other proposals require the private key generator (PKG) to spend an impractically long time for each private key generation request. Some proposals require tamper resistant hardware.

In short, there remains a need for improved cryptographic methods and systems.

SUMMARY OF THE INVENTION

According to one embodiment of the invention, a method of encrypting a first piece of information to be sent by a sender to a receiver uses an encryption key generated from a second piece of information. A bilinear map and the encryption key are used to encrypt at least a portion of the first piece of information to be sent from the sender to the receiver. The bilinear map may be symmetric or asymmetric. The bilinear map may be based on a Weil pairing or a Tate pairing defined on an algebraic group derived from an elliptic curve. More generally, the bilinear map may be based on a pairing defined on algebraic varieties.

According to one embodiment of the invention, encrypting the portion of the first piece of information can be completed prior to generating a decryption key corresponding to the encryption key.

According to another embodiment of the invention, the second piece of information is known to the receiver prior to the generation of a decryption key corresponding to the encryption key. The second piece of information may comprise a character string such as an e-mail address, name or other identifier associated with the receiver, according to different embodiments of the invention. The second piece of information may also include, according to various embodiments, an attribute associated with the receiver or information corresponding to a time or times, such as a date or series of dates defining one or more time intervals. A decryption key may be provided based on a time that a request for the decryption key is received relative to the information corresponding to a time. According to other embodiments of the invention, the

second piece of information may include a message identifier, a credential identifier or a message subject identifier.

According to another embodiment of the invention, a message key is generated from the encryption key using a bilinear map, and a cryptographic hash function is applied to the message key.

According to another embodiment of the invention, encrypting the portion of the first piece of information includes generating a mask from the second piece of information using a bilinear map. The mask is applied to the portion of the second piece of information.

An embodiment of the invention is directed to a method of decrypting ciphertext which has been encrypted by a sender using an identity-based encryption key associated with a receiver. A decryption key derived from the encryption key is obtained. At least a portion of the ciphertext is decrypted using a bilinear map and the decryption key. The bilinear map may be symmetric or asymmetric. The bilinear map may be based on a Weil pairing or a Tate pairing defined on an algebraic group derived from an elliptic curve.

According to another embodiment of the invention, the ciphertext is obtained prior to creating the decryption key. According to another embodiment of the invention, the first piece of information is known to the receiver prior to obtaining the ciphertext and prior to obtaining the decryption key. The decryption key may be obtained by sending a request to a private key generator, including information sent together with the ciphertext.

An embodiment of the invention is directed to a method of generating a decryption key corresponding to an encryption key. An algebraic group, a group action, and a master key are provided. The encryption key is generated based on a first piece of information. The decryption key is generated based on the group action, the master key and the encryption key. According to one embodiment of the invention, the group action is capable of being calculated in polynomial time. According to another aspect of the invention, generation of the decryption key in the absence of the master key would require greater than polynomial time.

Another embodiment of the invention is directed to a method of providing system

parameters for a cryptographic system. Algebraic groups $\mathbb{G}_1$ and $\mathbb{G}_2$ having an order q are provided, together with associated group actions. In addition, a bilinear map is provided that maps pairs of points in $\mathbb{G}_1$ to points in $\mathbb{G}_2$. In another embodiment, a system parameter representing a member P of G_1, and a system parameter representing a member P_{pub} of G_1 are provided, where P_{pub} is based on the group action of a master key s applied to P. According to other embodiments of the invention, a system parameter representing a set of one or more hash functions H_1, H_2, H_3, or H_4 are provided. According to another embodiment of the invention, a system parameter representing a size n of a message space is provided.

According to another embodiment of the invention, the bilinear map may be asymmetric or symmetric. In another embodiment the bilinear map is based on a Weil pairing or a Tate pairing defined on a portion of an elliptic curve.

According to another embodiment of the invention, the algebraic group G_1 is defined by an elliptic curve defined over a field of order p and the order q is less than the order p. According to another aspect of the invention, the length of p is at least 1024 bits and the length of q is no greater than 160 bits.

Another embodiment of the invention is directed to a method for managing cryptographic communication including generating shares of a master key. The shares are stored in separate systems. A request from a receiver to obtain a private key is responded to in the separate systems by generating from the respective shares of the master key, corresponding respective shares of the private key. The receiver constructs the private key from the shares of the private key, where the private key corresponds to identifying information of the receiver.

Another embodiment of the invention is directed to a method for communicating between a sender and a receiver. A message to be sent from the sender to the receiver is encrypted, and the message is sent from the sender to the receiver. A request for a decryption key is received from the receiver of the message. After receiving the request for the decryption key, information indicating that the receiver has received the message is generated, and the decryption key is provided to the receiver. According to an embodiment of the invention, a return address of the sender is included in the message, and an acknowledgment that the message has been received is sent to the return address. According to another aspect of the invention, an identification of

the message is included in an acknowledgment and the acknowledgment is sent to the sender. According to another aspect of the invention, the encryption key is derived based on a return address of the sender.

Another embodiment of the invention is directed to a method for communicating between a sender and a receiver having a credential. Identifying information of the receiver is obtained. A credential required for the receiver to gain a decryption key is specified, and an encryption key is derived from the identifying information of the receiver and the credential. A message to be sent from the sender to the receiver is encrypted using the encryption key and a bilinear map, and the message is sent from the sender to the receiver. A request for a decryption key is received from the receiver of the message. It is determined whether the receiver has the credential, and if the receiver has the credential, the decryption key is provided to the receiver. The receiver then may use the decryption key and the bilinear map to decrypt the message.

Another embodiment of the invention is directed to a method of communicating between a sender and a receiver involving storing a decryption key on a target system. Sets of decryption keys associated with times messages may be decrypted are derived, and the decryption keys are stored on the target system. An encryption key is derived from a string associated with a time a message is to be decrypted. A message is encrypted using the encryption key. The message is received on the target system, and the message is decrypted using a bilinear map and the corresponding decryption key.

Another embodiment of the invention is directed to a method of communicating between a sender and receiver involving entities having different responsibilities. A set of decryption keys is derived from a master key and a set of strings associated with different responsibilities. The decryption keys are provided to entities having the respective responsibilities. An encryption key is derived from a string associated with one of the different responsibilities. A message to be sent from the sender to the receiver is encrypted using the encryption key and a bilinear map. An entity having a particular responsibility receives the message and decrypts the message using the respective decryption key and the bilinear map. According to one embodiment of the invention, the string corresponding to the particular responsibility comprises a subject line of an e-mail.

BRIEF DESCRIPTION OF THE DRAWING FIGURES

FIG. 1 is a block diagram illustrating a cryptosystem according to an embodiment of the invention, showing steps taken by a sender, a receiver, and a private key generator (PKG), and information communicated between them.

FIG. 2 is a block diagram illustrating steps performed by a PKG when generating a private key according to an embodiment of the invention.

FIG. 3 is a block diagram illustrating steps performed by a sender when computing a secret message key and using it to encrypt a message intended for a receiver according to an embodiment of the invention.

FIG. 4 is a block diagram illustrating steps performed by a receiver when computing a secret message key and using it to decrypt ciphertext received from a sender according to an embodiment of the invention.

FIG. 5 is a block diagram illustrating a distributed PKG, according to an embodiment of the invention.

FIG. 6 is a block diagram illustrating elements in a cryptosystem with escrow decryption capability according to an embodiment of the invention.

FIG. 7 is a block diagram illustrating steps performed by a sender when encrypting messages in an ElGamal cryptosystem with escrow decryption capability according to an embodiment of the invention.

FIG. 8 is a block diagram illustrating steps performed by a receiver when decrypting messages in an ElGamal cryptosystem with escrow decryption capability according to an embodiment of the invention.

FIG. 9 is a block diagram illustrating steps performed by an escrow when decrypting messages in an ElGamal cryptosystem with escrow decryption capability according to an alternate embodiment of the invention.

FIG. 10 is a block diagram illustrating a system for managing credentials in an identity based encryption system according to an embodiment of the invention.

FIG. 11 is a block diagram illustrating a system with key delegation according to an embodiment of the invention.

FIG. 12 is a block diagram illustrating an encryption system with return receipt according to an embodiment of the invention.

DETAILED DESCRIPTION OF THE INVENTION

The following description provides details of several exemplary embodiments of the cryptographic techniques of the present invention, as well as a technical discussion of the security of the system.

OVERVIEW

As is normally the case with modern cryptosystems, the techniques of the present invention are generally implemented on computers connected by a communication medium. Although typically the computers are connected by the Internet or another computer network, any communication medium may be used.

One embodiment of the invention comprises an identity-based encryption system that uses a secret message key derived from identity-based information. The message key may be used by a sender to encrypt a message, and by a receiver to decrypt the message. The secret message key is computed by the sender from an identity-based public key of the receiver. The same message key may be computed by the receiver from the receiver's private key, which is derived from the receiver's identity-based public key. Both sender and receiver compute the same secret key using a bilinear map. For example, in one embodiment, an asymmetric or symmetric bilinear map $\hat{e} : \mathbb{G}_0 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ is used where $\mathbb{G}_0, \mathbb{G}_1, \mathbb{G}_2$ are (not necessarily distinct) algebraic groups. In the case where $\mathbb{G}_0$ is equal to $\mathbb{G}_1$, we say the bilinear map is symmetric and often denote it as $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$. A bilinear map $\hat{e}$ that is non-degenerate and efficiently computable will be referred to as an *admissible* map. It is preferable in some embodiments of the invention that the bilinear map be admissible.

The convention throughout this description will be to denote the group operations of $\mathbb{G}_0$ and $\mathbb{G}_1$ by addition, and the group operation of $\mathbb{G}_2$ by multiplication. For a group $\mathbb{G}$ of prime order we use $\mathbb{G}^*$ to denote the set $\mathbb{G}^* = \mathbb{G} \setminus \{O\}$ where O is the identity element in the group $\mathbb{G}$. The set of binary strings of arbitrary length is denoted by $\{0,1\}^*$. We use $\mathbb{Z}_q$ to denote the group $\{0, \ldots, q-1\}$ under addition modulo q, and we use $\mathbb{Z}^+$ to denote the set of positive integers. We note that there

is a natural group action of $\mathbb{Z}_q$ on $\mathbb{G}$ given by repeated addition, and we denote the result of the action of an element $a \in \mathbb{Z}_q$ on an element $P \in \mathbb{G}$ by aP.

According to another embodiment of the invention, a certain variant (involving the map $\hat{e}$) of the computational Diffie-Hellman problem is hard. In one implementation the map $\hat{e}$ is admissible and the orders of $\mathbb{G}_0, \mathbb{G}_1, \mathbb{G}_2$ have a very large prime factor q. The orders of $\mathbb{G}_0, \mathbb{G}_1$ and $\mathbb{G}_2$ may be equal to each other. Without loss of generality, the following description assumes for simplicity that the orders of $\mathbb{G}_0, \mathbb{G}_1$ and $\mathbb{G}_2$ are all of prime order q.

In an exemplary embodiment, an admissible map $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ is used to realize an identity-based cryptosystem, as follows. To encrypt a message, a sender uses a public key $Q_{\mathsf{ID}} \in \mathbb{G}_1$ associated with a public identifier ID for the intended receiver. To decrypt the encrypted message, the receiver uses a complementary private key $d_{\mathsf{ID}} \in \mathbb{G}_1$. The private key is computed from the public key Q_{ID}, a secret master key $s \in \mathbb{Z}_q^*$, and a group action of $\mathbb{Z}_q^*$ on $\mathbb{G}_1$. In one embodiment, for example, $d_{\mathsf{ID}} = sQ_{\mathsf{ID}}$. Since the secret master key s is known only by a trusted PKG, users normally cannot themselves compute private keys. To obtain a private key, an individual may obtain it from the PKG, preferably after being authenticated. At any time, however, anyone can compute the public key Q_{ID} associated with any public identifier ID even before the corresponding private key has been determined. For example, in one embodiment the public key Q_{ID} may be obtained by (1) using a conventional character encoding scheme to map the public identifier ID to a corresponding binary string in $\{0,1\}^*$, and (2) using a hash function $H_1 : \{0,1\}^* \rightarrow \mathbb{G}_1^*$ to hash the binary string to the element Q_{ID} of $\mathbb{G}_1^*$, where the order of Q_{ID} is q.

In this embodiment, a message intended for a receiver with public identifier ID may be encrypted and decrypted as follows. The admissible map $\hat{e}$ may be used by the sender to determine a secret message key. Although the sender and receiver do not share all the same information, using the fact that the map $\hat{e}$ is bilinear, they can use different information to compute the same message key. Since each uses information that is private, the message key is a secret.

To illustrate how this approach may be implemented, suppose that the sender has knowledge of elements P and sP in $\mathbb{G}_1$. In one embodiment, for example, elements P and $P_{pub} = sP$ in $\mathbb{G}_1$ are published system parameters. Now further suppose the

sender privately selects a random $r \in \mathbb{Z}_q^*$, and uses the receiver's identity-based public key Q_{ID} to compute $g_{ID}^r = \hat{e}(rQ_{ID}, sP)$. The element g_{ID}^r is an identity-based secret which the sender may use as a secret message key to perform identity-based encryption of a message to the receiver. The sender may then send an encrypted message together with rP to the receiver. The receiver then receives rP and uses it together with the private key sQ_{ID} to compute the secret message key $g_{ID}^r = \hat{e}(sQ_{ID}, rP)$. This secret message key is equal to the secret message key computed by the sender because of the bilinearity of the $\hat{e}$ map. This computed element $g_{ID}^r \in \mathbb{G}_2$ is thus an identity-based secret of the sender which the receiver may compute using the element rP and the private key sQ_{ID}. This secret may be used as a message key for cryptographic communication between the sender and receiver.

Note that the PKG also knows the receiver's private key, so can also compute the secret message key and decrypt the message. The sender, receiver and PKG all have sufficient information to compute the secret message key. No other entity, however, normally has knowledge of the sender's secret r or the receiver's secret sQ_{ID}. The security of this embodiment is related to the difficulty of computing the secret message key, which is based upon a combination of r, s, and Q_{ID} using a bilinear map, without knowledge of r or knowledge of sQ_{ID}.

In one embodiment, the message key g_{ID}^r is used to determine a mask which is used to encrypt and decrypt the bits of the message using an XOR operation (denoted by '$\oplus$'). Specifically, the ciphertext V of a message M is produced by computing $V = M \oplus H_2(g_{ID}^r)$, where $H_2 : \mathbb{G}_2 \rightarrow \{0,1\}^n$ is a hash function, and n is the bit length of the message. Conversely, the message M is recovered from the ciphertext V by computing $M = V \oplus H_2(g_{ID}^r)$.

In another embodiment, the one-way encryption scheme outlined above is made more secure by converting it into a chosen ciphertext secure system. In one embodiment of the invention, for example, a general technique of Fujisaki-Okamoto is used.

In another embodiment, the master key is broken into components s_i distributed among several private key generators in a distributed PKG. For a given user with a public key Q_{ID} based on an identifier ID, each of these private key generators in the distributed PKG computes a private key portion d_i using Q and its portion s_i of the

master key. These private key portions can be combined by the user and used as a single private key d_{ID} to decrypt messages encrypted with Q_{ID}.

In another embodiment, an ElGamal encryption scheme is provided with built-in key escrow, i.e., where one global escrow key can decrypt ciphertexts encrypted under any public key. In this embodiment, the exemplary system described above is adapted as follows. Suppose that the receiver also has knowledge of elements P and sP. Rather than obtaining a private key from the PKG, the receiver generates a public/private key pair by selecting a random $x \in \mathbb{Z}_q^*$, computing xP using a group action, and publishing a public key based on the result of the computation. In one embodiment, the public key is xP and the complementary private key is $d = x(sP)$. (Thus, xP plays the role of Q_{ID}, and $d = x(sP) = s(xP)$ plays the role of $d_{ID} = sQ_{ID}$.) To encrypt a message to the receiver, the sender as before selects a random r and sends rP to the receiver. Then the receiver knows the pair $(rP, x(sP))$, where $x(sP) = d$ is a secret, while the sender knows the pair $(sP, r(xP))$, where $r(xP)$ is a secret. Thus, the sender and receiver both can compute $g = \hat{e}(rP, x(sP)) = \hat{e}(sP, r(xP))$, where the second equality follows from the bilinearity of $\hat{e}$. This secret, however, can also be determined from knowledge of the master key s. Using the element rP from the sender, the receiver's public key xP, and the master key s, the message key can be computed by evaluating $g = \hat{e}(rP, s(xP))$. It should be noted that this embodiment makes use of a symmetric bilinear map $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$.

In several embodiments of the invention, $\mathbb{G}_1$ is a subgroup of an elliptic curve, and an admissible map $\hat{e}$ is constructed from the Weil pairing (or Tate pairing) on the elliptic curve. (Recall that, by definition, a subgroup is not necessarily smaller than the group, i.e., $\mathbb{G}_1$ may be the entire elliptic curve). More generally, $\mathbb{G}_1$ may be an abelian variety and $\hat{e}$ an admissible pairing of its elements. In embodiments using a map $\hat{e} : \mathbb{G}_0 \times \mathbb{G}_1 \to \mathbb{G}_2$ where $\mathbb{G}_0$ and $\mathbb{G}_1$ are distinct, $\mathbb{G}_0$ also may be a subgroup of an elliptic curve, or more generally, an abelian variety.

In other embodiments, various novel applications of identity-based encryption are provided. New and useful applications of IBE systems are possible by using other types of public identifiers, or enhanced public identifiers. For example, the public identifier ID is not limited to an identifier associated with an individual person, but may be an identifier associated with any type of entity including not just individuals but also organizations, governmental agencies, corporations and the like. It should

also be noted that individual identities forming a group may be naturally combined to produce a joint identity for the group with a corresponding group private key. The group's private key need not be issued by a PKG, but is simply the combination of the separate private keys of the entities composing the group. It should be noted that the basic ID specifying the identity of an entity is not limited to the name, e-mail address, address, or social security number of an entity, but could also include other types of information such as domain names, URLs, 9-digit zip codes, tax identification numbers, and so on. In many applications, the public identifier ID will contain some character string known to the public to be uniquely associated with a particular entity or collection of entities. In general, however, the public identifier ID can be any arbitrary character string or other arbitrary information.

Various useful applications of IBE make use of enhanced public identifiers. An *enhanced* identifier may comprise a type of identifier that contains information not necessarily limited to information specifying the identity of a particular entity. For example, an ID can contain a credential descriptor such as a license number, official title, or security clearance associated with an entity. An agency can then manage the credentials by providing private keys only to entities it certifies. In one exemplary embodiment, an ID can contain a property descriptor such as a serial number, vehicle identification number, patent number, or the like. An agency responsible for registering property owners and authenticating owners can manage property registration by providing private keys only to entities that it registers as true owners. More generally, an association between two or more things can be managed by including identifiers for them in an ID. The PKG then acts as the management authority for the associations between things.

Another type of enhanced ID is an identifier that includes a time, a time interval, or a set of time intervals. A private key for such an identifier can then be constructed to automatically expire at a certain time, to automatically activate only after a certain time, or to be valid only for one or more specified time intervals. This technique can be combined with the credential and ownership management to control the time of activation and/or expiration.

From the above examples, it is evident that an identity-based encryption systems according to the present invention are not limited to any particular type of identifier. Thus, the term 'identity-based' should be understood in general terms as indicating

that any arbitrary character string or other arbitrary information may be used as a basis.

According to another embodiment, an IBE system allows the delegation of decryption capabilities. An entity can set up its own IBE system with its own secret master key, and assume the role of PKG for this IBE system. Because the entity has the master key, it can issue keys to delegate decryption capabilities to others. For example, if the entity is a corporation, the employees can obtain private keys from the corporate PKG. Individuals can be issued private keys matching their names, titles, duties, projects, cases, or any other task-related identifier. In another example, an individual can issue to a laptop private keys that are valid only for the duration of a business trip. If the laptop is lost or stolen, only the keys for that time period are compromised. The master key, which remained at home, is uncompromised.

It should also be pointed out that the medium of communication need not be limited to e-mail or the Internet, but could include any communication medium such as printed publications, digital storage media, radio broadcasting, wireless communications, and so on.

DEFINITIONS

Identity-Based Encryption. An exemplary embodiment of an identity-based encryption system and method $\mathcal{E}$ uses four randomized algorithms: Setup, Extract, Encrypt, Decrypt:

Setup: Given a security parameter k, return params (system parameters) and master-key. The system parameters include a description of a finite message space $\mathcal{M}$, and a description of a finite ciphertext space $\mathcal{C}$. Normally, the system parameters will be publicly known, while the master-key will be known only to a Private Key Generator (PKG).

Extract: takes as input params, master-key, and an arbitrary $\mathsf{ID} \in \{0,1\}^*$, and returns a private key d. Here ID is an arbitrary string that will be used as a public key, and d is the corresponding private decryption key. The Extract algorithm extracts a private key from the given public key. Because the extraction requires the master-key, it is normally performed by the PKG.

Encrypt: takes as input params, ID, and $M \in \mathcal{M}$. It returns a ciphertext $C \in \mathcal{C}$.

Decrypt: takes as input params, $C \in \mathcal{C}$, and a private key d. It return $M \in \mathcal{M}$.

According to an embodiment of the invention, these algorithms satisfy the standard consistency constraint that ensures decryption will faithfully recover any encrypted message. More specifically, when d is the private key generated by algorithm Extract when it is given ID as the public key, then

$$\forall M \in \mathcal{M} : \mathsf{Decrypt}(\mathsf{params}, C, d) = M \quad \text{where} \quad C = \mathsf{Encrypt}(\mathsf{params}, \mathsf{ID}, M).$$

In an identity-based cryptosystem according to an embodiment of the invention, the above algorithms are used together as illustrated in FIG. 1. A sender 100 uses Encrypt, a receiver 110 uses Decrypt, and a PKG 120 uses Setup and Extract. To send a message M to receiver 110, the sender 100 obtains an ID of the receiver (e.g., the receiver's e-mail address) and combines it with a randomly selected integer r to compute a secret message key g_{ID}^{r}. The element rP is sent to receiver 110 who combines it with a private key d_{ID} to determine the same message key g_{ID}^{r}. Because the sender and receiver share the secret message key, a message encrypted with the key by the sender can be decrypted by the receiver. In particular, the sender encrypts M with the message key to produce ciphertext V which is communicated with rP to the receiver. The receiver then uses the secret message key to decrypt the ciphertext to recover the original message. In order to decrypt messages, however, the receiver 110 must first obtain the private key d_{ID} from the PKG 120. After the PKG authenticates the identity of the receiver, it provides the receiver with the private key corresponding to the receiver's ID. (Note that, in this embodiment, the PKG can compute any private key in the system, and can thus decrypt any message to any user in the system.)

Chosen ciphertext security. Chosen ciphertext security (IND-CCA) is the standard acceptable notion of security for a public key encryption scheme. An embodiment of an identity-based encryption system and method may be implemented to satisfy this strong notion of security. Additionally, the selected level of chosen ciphertext security may be strengthened a bit. The reason is that when an adversary attacks a public key ID in an identity-based system, the adversary might already possess the private keys of users $\mathsf{ID}_1, \ldots, \mathsf{ID}_n$ of her choice. In an embodiment of the invention, the system remains secure under such an attack. That is, the system remains secure

even when the adversary can obtain the private key associated with any identity ID_i of her choice (other than the public key ID being attacked). We refer to such queries as private key extraction queries. The system of this embodiment also remains secure even though the adversary is challenged on a public key ID of her choice (as opposed to a random public key).

We say that an embodiment of an identity-based encryption system or method $\mathcal{E}$ is semantically secure against an adaptive chosen ciphertext attack (IND-ID-CCA) if no polynomially bounded adversary $\mathcal{A}$ has a non-negligible advantage against the Challenger in the following IND-ID-CCA game:

Setup: The challenger takes a security parameter k and runs the Setup algorithm. It gives the adversary the resulting system parameters params. It keeps the master-key to itself.

Phase 1: The adversary issues queries $q_1, \ldots, q_m$ where query q_i is one of:

- Extraction query $\langle \mathsf{ID}_i \rangle$. The challenger responds by running algorithm Extract to generate the private key d_i corresponding to the public key $\langle \mathsf{ID}_i \rangle$. It sends d_i to the adversary.
- Decryption query $\langle \mathsf{ID}_i, C_i \rangle$. The challenger responds by running algorithm Extract to generate the private key d_i corresponding to ID_i. It then runs algorithm Decrypt to decrypt the ciphertext C_i using the private key d_i. It sends the resulting plain-text to the adversary.

These queries may be asked adaptively, that is, each query q_i may depend on the replies to $q_1, \ldots, q_{i-1}$.

Challenge: Once the adversary decides that Phase 1 is over it outputs two equal length plain-texts $M_0, M_1 \in \mathcal{M}$ and an identity ID on which it wishes to be challenged. The only constraint is that ID did not appear in any private key extraction query in Phase 1.

The challenger picks a random bit $b \in \{0, 1\}$ and sets $C = \mathsf{Encrypt}(\mathsf{params}, \mathsf{ID}, M_b)$. It sends C as the challenge to the adversary.

Phase 2: The adversary issues more queries $q_{m+1}, \ldots, q_n$ where query q_i is one of:

- Extraction query $\langle \mathsf{ID}_i \rangle$ where $\mathsf{ID}_i \neq \mathsf{ID}$. Challenger responds as in

Phase 1.

– Decryption query $\langle \mathsf{ID}_i, C_i \rangle \neq \langle \mathsf{ID}, C \rangle$. Challenger responds as in Phase 1.

These queries may be asked adaptively as in Phase 1.

Guess: Finally, the adversary outputs a guess $b' \in \{0,1\}$. The adversary wins the game if $b = b'$.

We refer to such an adversary $\mathcal{A}$ as an IND-ID-CCA adversary. We define adversary $\mathcal{A}$'s advantage in attacking the scheme $\mathcal{E}$ as the following function of the security parameter k (k is given as input to the challenger): $\mathrm{Adv}_{\mathcal{E},\mathcal{A}}(k) = \left|\Pr[b = b'] - \frac{1}{2}\right|$.
The probability is over the random bits used by the challenger and the adversary.

Using the IND-ID-CCA game we can define chosen ciphertext security for IBE schemes. As usual, we say that a function $g : \mathbb{R} \to \mathbb{R}$ is *negligible* if $g(k)$ is smaller than $1/f(k)$ for any polynomial f.

Definition 1 *We say that an IBE system $\mathcal{E}$ is semantically secure against an adaptive chosen ciphertext attack if for any polynomial time* IND-ID-CCA *adversary $\mathcal{A}$ the function $Adv_{\mathcal{E},\mathcal{A}}(k)$ is negligible. As shorthand, we say that $\mathcal{E}$ is* IND-ID-CCA *secure.*

Note that the standard definition of chosen ciphertext security (IND-CCA) is the same as above except that there are no private key extraction queries and the adversary is challenged on a random public key (rather than a public key of her choice). Private key extraction queries are related to the definition of chosen ciphertext security in the multiuser settings. After all, our definition involves multiple public keys belonging to multiple users. A multiuser IND-CCA may be reducible to single user IND-CCA using a standard hybrid argument. This does not hold in the identity-based settings, IND-ID-CCA, since the adversary gets to choose which public keys to corrupt during the attack. To emphasize the importance of private key extraction queries we note that one implementation of the disclosed IBE system can be modified (by removing one of the hash functions) into a system which has chosen ciphertext security when private extraction queries are disallowed. However, the implementation is insecure when extraction queries are allowed.

Semantically secure identity based encryption. The proof of security for an implementation of our IBE system makes use of a weaker notion of security known as semantic security (also known as semantic security against a chosen plain-text attack). Semantic security is similar to chosen ciphertext security (IND-ID-CCA) except that the adversary is more limited; it cannot issue decryption queries while attacking the challenge public key. For a standard public key system (not an identity based system) semantic security is defined using the following game: (1) the adversary is given a random public key generated by the challenger, (2) the adversary outputs two equal length messages M_0 and M_1 and receives the encryption of M_b from the challenger where b is chosen at random in $\{0,1\}$, (3) the adversary outputs b' and wins the game if $b = b'$. The public key system is said to be semantically secure if no polynomial time adversary can win the game with a non-negligible advantage. As shorthand we say that a semantically secure public key system is IND-CPA secure. Semantic security captures our intuition that given a ciphertext the adversary learns nothing about the corresponding plain-text.

To define semantic security for identity based systems (denoted IND-ID-CPA) we strengthen the standard definition by allowing the adversary to issue chosen private key extraction queries. Similarly, the adversary is challenged on a public key ID of her choice. We define semantic security for identity based encryption schemes using an IND-ID-CPA game. The game is identical to the IND-ID-CCA game defined above except that the adversary cannot make any decryption queries. The adversary can only make private key extraction queries. We say that an identity-based encryption scheme $\mathcal{E}$ is semantically secure (IND-ID-CPA) if no polynomially bounded adversary $\mathcal{A}$ has a non-negligible advantage against the Challenger in the following IND-ID-CPA game:

Setup: The challenger takes a security parameter k and runs the Setup algorithm. It gives the adversary the resulting system parameters params. It keeps the master-key to itself.

Phase 1: The adversary issues private key extraction queries $\mathsf{ID}_1, \ldots, \mathsf{ID}_m$. The challenger responds by running algorithm Extract to generate the private key d_i corresponding to the public key ID_i. It sends d_i to the adversary. These queries may be asked adaptively.

Challenge: Once the adversary decides that Phase 1 is over it outputs

two equal length plain-texts $M_0, M_1 \in \mathcal{M}$ and a public key ID on which it wishes to be challenged. The only constraint is that ID did not appear in any private key extraction query in Phase 1. The challenger picks a random bit $b \in \{0,1\}$ and sets $C = \mathsf{Encrypt}(\mathsf{params}, \mathsf{ID}, M_b)$. It sends C as the challenge to the adversary.

Phase 2: The adversary issues more extraction queries $\mathsf{ID}_{m+1}, \ldots, \mathsf{ID}_n$. The only constraint is that $\mathsf{ID}_i \neq \mathsf{ID}$. The challenger responds as in Phase 1.

Guess: Finally, the adversary outputs a guess $b' \in \{0,1\}$. The adversary wins the game if $b = b'$.

We refer to such an adversary $\mathcal{A}$ as an IND-ID-CPA adversary. As we did above, the advantage of an IND-ID-CPA adversary $\mathcal{A}$ against the scheme $\mathcal{E}$ is the following function of the security parameter k: $\mathrm{Adv}_{\mathcal{E},\mathcal{A}}(k) = \left|\Pr[b = b'] - \frac{1}{2}\right|$.

The probability is over the random bits used by the challenger and the adversary.

Definition 2 *We say that the IBE system $\mathcal{E}$ is semantically secure if for any polynomial time* IND-ID-CPA *adversary $\mathcal{A}$ the function $Adv_{\mathcal{E},\mathcal{A}}(k)$ is negligible. As shorthand, we say that $\mathcal{E}$ is* IND-ID-CPA *secure.*

One way identity-based encryption. One can define an even weaker notion of security called one-way encryption (OWE). Roughly speaking, a public key encryption scheme is a one-way encryption if given the encryption of a random plain-text the adversary cannot produce the plain-text in its entirety. One-way encryption is a weak notion of security since there is nothing preventing the adversary from, say, learning half the bits of the plain-text. Hence, one-way encryption schemes do not generally provide secure encryption. In the random oracle model one-way encryption schemes can be used for encrypting session-keys (the session-key is taken to be the hash of the plain-text). We note that one can extend the notion of one-way encryption to identity based systems by adding private key extraction queries to the definition. We do not give the full definition here since we use semantic security as the weakest notion of security.

Bilinear maps and the Bilinear Diffie-Hellman Assumption

One embodiment of the invention is directed to an IBE system that makes use of a map $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ between groups $\mathbb{G}_1$ and $\mathbb{G}_2$ of order q for some large prime q. A map $\hat{e}$ may be called an *admissible* map if it satisfies the following properties:

1. Bilinear: The map $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ satisfies $\hat{e}(aP, bQ) = \hat{e}(P, Q)^{ab}$ for all $(P, Q) \in \mathbb{G}_1 \times \mathbb{G}_1$ and all $a, b \in \mathbb{Z}$.
2. Non-degenerate: The map does not send all pairs in $\mathbb{G}_1 \times \mathbb{G}_1$ to the identity in $\mathbb{G}_2$. Observe that since $\mathbb{G}_1, \mathbb{G}_1, \mathbb{G}_2$ are groups of prime order this implies that if $\mathbb{G}_1 = \mathbb{G}_1$ and P is a generator of $\mathbb{G}_1 = \mathbb{G}_1$ then $\hat{e}(P, P)$ is a generator of $\mathbb{G}_2$.
3. Computable: There is an efficient algorithm to compute $\hat{e}(P, Q)$ for any $(P, Q) \in \mathbb{G}_1 \times \mathbb{G}_1$.

Although many of the embodiments are described with reference to a map $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$, this is only a specific case of bilinear maps used in embodiments of the invention. More generally, maps $\hat{e} : \mathbb{G}_0 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ may be used, where $\mathbb{G}_0$ and $\mathbb{G}_1$ may be distinct. For simplicity of description, however, the description of many of the embodiments focuses primarily on the case where $\mathbb{G}_1$ and $\mathbb{G}_1$ are the same, and both groups are then denoted $\mathbb{G}_1$. Below we present a detailed exemplary embodiment using groups $\mathbb{G}_1, \mathbb{G}_2$ and an admissible map between them. In this exemplary embodiment, the group $\mathbb{G}_1$ is a subgroup of the additive group of points of an elliptic curve $E/\mathbb{F}_p$, and the group $\mathbb{G}_2$ is a subgroup of the multiplicative group of a finite field $\mathbb{F}_{p^2}^*$. As we will see below in the detailed example of an IBE system, the Weil pairing (which is not itself an admissible map) can be used to construct an admissible map between these two groups.

The existence of the admissible map $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ as above has two direct implications to these groups.

The MOV reduction: The discrete log problem in $\mathbb{G}_1$ is no harder than the discrete log problem in $\mathbb{G}_2$. To see this, let $P, Q \in \mathbb{G}_1$ be an instance of the discrete log problem in $\mathbb{G}_1$ where both P, Q have order q. We wish to find an $\alpha \in \mathbb{Z}_q$ such that $Q = \alpha P$. Let $g = \hat{e}(P, P)$ and $h = \hat{e}(Q, P)$. Then, by bilinearity of $\hat{e}$ we know that $h = g^{\alpha}$. By non-degeneracy of $\hat{e}$ both g, h have order q in $\mathbb{G}_2$. Hence, we reduced the discrete log problem in $\mathbb{G}_1$ to a discrete log problem in

$\mathbb{G}_2$. It follows that for discrete log to be hard in $\mathbb{G}_1$ we must choose our security parameter so that discrete log is hard in $\mathbb{G}_2$.

Decision Diffie-Hellman is Easy: The Decision Diffie-Hellman problem (DDH) in $\mathbb{G}_1$ is the problem of distinguishing between the distributions $\langle P, aP, bP, abP\rangle$ and $\langle P, aP, bP, cP\rangle$ where a, b, c are random in $\mathbb{Z}_q$ and P is random in $\mathbb{G}_1$. To see that DDH in $\mathbb{G}_1$ is easy, observe that given $P, aP, bP, cP \in \mathbb{G}_1^*$ we have

$$c = ab \bmod q \iff \hat{e}(P, cP) = \hat{e}(aP, bP).$$

The Computational Diffie-Hellman problem (CDH) in $\mathbb{G}_1$ can still be hard (CDH in $\mathbb{G}_1$ is to find abP given random $\langle P, aP, bP\rangle$). Exemplary embodiments may use mappings $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$ where CDH in $\mathbb{G}_1$ is believed to be hard even though DDH in $\mathbb{G}_1$ is easy.

The Bilinear Diffie-Hellman Assumption (BDH)

Since the Decision Diffie-Hellman problem (DDH) in $\mathbb{G}_1$ is easy, embodiments of the invention do not use DDH to build cryptosystems in the group $\mathbb{G}_1$. Instead, the security in embodiments of our IBE system is based on a novel variant of the Computational Diffie-Hellman assumption called the Bilinear Diffie-Hellman Assumption (BDH).

Bilinear Diffie-Hellman Problem. Let $\mathbb{G}_1, \mathbb{G}_2$ be two groups of prime order q. Let $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$ be an admissible map and let P be a generator of $\mathbb{G}_1$. The BDH problem in $\langle \mathbb{G}_1, \mathbb{G}_2, \hat{e}\rangle$ is as follows: Given $\langle P, aP, bP, cP\rangle$ for some $a, b, c \in \mathbb{Z}_q^*$ compute $W = \hat{e}(P, P)^{abc} \in \mathbb{G}_2$. An algorithm $\mathcal{A}$ has advantage ϵ in solving BDH in $\langle \mathbb{G}_1, \mathbb{G}_2, \hat{e}\rangle$ if

$$\Pr\left[\mathcal{A}(P, aP, bP, cP) = \hat{e}(P, P)^{abc}\right] \geq \epsilon$$

where the probability is over the random choice of a, b, c in $\mathbb{Z}_q^*$, the random choice of $P \in \mathbb{G}_1^*$, and the random bits of $\mathcal{A}$.

BDH Parameter Generator. We say that a randomized algorithm $\mathcal{G}$ is a *BDH parameter generator* if (1) $\mathcal{G}$ takes a security parameter $k \in \mathbb{Z}^+$, (2) $\mathcal{G}$ runs in polynomial time in k, and (3) $\mathcal{G}$ outputs a prime number q, the description of two groups

$\mathbb{G}_1, \mathbb{G}_2$ of order q, and the description of an admissible map $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$. We denote the output of $\mathcal{G}$ by $\mathcal{G}(1^k) = \langle q, \mathbb{G}_1, \mathbb{G}_2, \hat{e} \rangle$. The security parameter k is used to determine the size of q; for example, one could take q to be a random k-bit prime. For $i = 1, 2$ we assume that the description of the group $\mathbb{G}_i$ contains polynomial time (in k) algorithms for computing the group action in $\mathbb{G}_i$ and contains a generator of $\mathbb{G}_i$. The generator of $\mathbb{G}_i$ enables us to generate uniformly random elements in $\mathbb{G}_i$. Similarly, we assume that the description of $\hat{e}$ contains a polynomial time algorithm for computing $\hat{e}$. We give an example of a BDH parameter generator below in the detailed example of an IBE system using the Weil pairing.

Bilinear Diffie-Hellman Assumption. Let $\mathcal{G}$ be a BDH parameter generator. We say that an algorithm $\mathcal{A}$ has advantage $\epsilon(k)$ in solving the BDH problem for $\mathcal{G}$ if for sufficiently large k:

$$\mathrm{Adv}_{\mathcal{G},\mathcal{A}}(k) = \Pr\left[\mathcal{A}(q, \mathbb{G}_1, \mathbb{G}_2, \hat{e}, P, aP, bP, cP) = \hat{e}(P,P)^{abc} \;\middle|\; \begin{array}{l} \langle q, \mathbb{G}_1, \mathbb{G}_2, \hat{e} \rangle \leftarrow \mathcal{G}(1^k), \\ P \leftarrow \mathbb{G}_1^*,\ a, b, c \leftarrow \mathbb{Z}_q^* \end{array}\right] > \epsilon(k$$

We say that $\mathcal{G}$ satisfies the BDH assumption if for any randomized polynomial time (in k) algorithm $\mathcal{A}$ and for any polynomial $f \in \mathbb{Z}[x]$ algorithm $\mathcal{A}$ solves the BDH problem with advantage at most $1/f(k)$. When $\mathcal{G}$ satisfies the BDH assumption we say that BDH is hard in groups generated by $\mathcal{G}$.

In the description below of a detailed example of an IBE system we give some examples of BDH parameter generators that are believed to satisfy the BDH assumption.

Hardness of BDH. It is interesting to study the relationship of the BDH problem to other hard problems used in cryptography. Currently, all we can say is that the BDH problem in $\langle \mathbb{G}_1, \mathbb{G}_2, \hat{e} \rangle$ is no harder than the CDH problem in $\mathbb{G}_1$ or $\mathbb{G}_2$. In other words, an algorithm for CDH in $\mathbb{G}_1$ or $\mathbb{G}_2$ is sufficient for solving BDH in $\langle \mathbb{G}_1, \mathbb{G}_2, \hat{e} \rangle$. The converse is currently an open problem: is an algorithm for BDH sufficient for solving CDH in $\mathbb{G}_1$ or in $\mathbb{G}_2$?

We note that in a detailed example of an IBE system below, the isomorphisms from $\mathbb{G}_1$ to $\mathbb{G}_2$ induced by the admissible map are believed to be one-way functions. More specifically, for a point $Q \in \mathbb{G}_1^*$ define the isomorphism $f_Q : \mathbb{G}_1 \to \mathbb{G}_2$ by

$f_Q(P) = \hat{e}(P,Q)$. If any one of these isomorphisms turns out to be invertible, then BDH is easy in $\langle \mathbb{G}_1, \mathbb{G}_2, \hat{e} \rangle$. Fortunately, an efficient algorithm for inverting f_Q would imply an efficient algorithm for deciding DDH in the group $\mathbb{G}_2$. In the exemplary embodiments DDH is believed to be hard in the group $\mathbb{G}_2$. Hence, the isomorphisms $f_Q : \mathbb{G}_1 \rightarrow \mathbb{G}_2$ induced by the admissible map are believed to be one-way functions.

Exemplary Identity-Based Encryption Scheme

We describe the following exemplary embodiments in stages. First we describe a basic identity-based encryption system and method which is not secure against an adaptive chosen ciphertext attack. Another embodiment described below extends the basic scheme to get security against an adaptive chosen ciphertext attack (IND-ID-CCA) in the random oracle model. We later relax some of the requirements on the hash functions to provide alternative embodiments. These embodiments are described with reference to a generic BDH parameter generator $\mathcal{G}$ satisfying the BDH assumption. Later we describe a detailed example of an IBE system using the Weil pairing.

BasicIdent

The following describes a basic embodiment, called BasicIdent. We present the embodiment by describing the four algorithms: Setup, Extract, Encrypt, Decrypt. We let k be the security parameter given to the setup algorithm. We let $\mathcal{G}$ be some BDH parameter generator.

Setup: Given a security parameter $k \in \mathbb{Z}^+$, the algorithm in the basic embodiment works as follows:

Step 1: Run $\mathcal{G}$ on input k to generate a prime q, two groups $\mathbb{G}_1, \mathbb{G}_2$ of order q, and an admissible map $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$. Choose an arbitrary generator $P \in \mathbb{G}_1$.

Step 2: Pick a random $s \in \mathbb{Z}_q^*$ and set $P_{pub} = sP$.

Step 3: Choose a cryptographic hash function $H_1 : \{0,1\}^* \rightarrow \mathbb{G}_1^*$. Choose a cryptographic hash function $H_2 : \mathbb{G}_2 \rightarrow \{0,1\}^n$ for some n. The security analysis will view H_1, H_2 as random oracles.

The message space is $\mathcal{M} = \{0,1\}^n$. The ciphertext space is $\mathcal{C} = \mathbb{G}_1^* \times \{0,1\}^n$. The system parameters are params $= \langle q, \mathbb{G}_1, \mathbb{G}_2, \hat{e}, n, P, P_{pub}, H_1, H_2 \rangle$. The master-key is $s \in \mathbb{Z}_q^*$.

Embodiments of the IBE system may be used to encrypt a symmetric key, in which

case one may take n to be, for example, 128 or 256. For k one may use, for example, 512 or 1024 or 2048.

Extract: For a given string $\mathsf{ID} \in \{0,1\}^*$ the algorithm in the basic embodiment does: (1) computes $Q_{\mathsf{ID}} = H_1(\mathsf{ID}) \in \mathbb{G}_1^*$, and (2) sets the private key d_{ID} to be $d_{\mathsf{ID}} = sQ_{\mathsf{ID}}$ where s is the master key.

Extract may be performed by a PKG in various embodiments as illustrated in FIG. 2. The PKG obtains the master key in block 200, obtains the public identifier ID in block 210, computes the public key from the ID in block 220, then computes the private key from the master key and the public key in block 230. In block 240 the private key is then sent to an entity associated with the public identifier ID, normally after the entity's identity has been authenticated.

Encrypt: To encrypt $M \in \mathcal{M}$ under the public key ID do the following: (1) compute $Q_{\mathsf{ID}} = H_1(\mathsf{ID}) \in \mathbb{G}_1^*$, (2) choose a random $r \in \mathbb{Z}_q^*$, and (3) set the ciphertext to be

$$C = \langle rP,\ M \oplus H_2(g_{\mathsf{ID}}^r) \rangle \quad \text{where} \quad g_{\mathsf{ID}} = \hat{e}(Q_{\mathsf{ID}}, P_{pub}) \in \mathbb{G}_2^*.$$

In the basic embodiment, the sender of a message may perform Encrypt as illustrated in FIG. 3. In block 300 the system parameters are obtained (from an external resource such as a PKG, or from a local storage medium if they were obtained previously). A receiver's ID is determined in block 310, and the corresponding public key is computed from the ID in block 320. Then the secret message key is computed in block 330, and the message key is used to encrypt the message in block 340.

Decrypt: Let $C = \langle U, V \rangle \in \mathcal{C}$ be a ciphertext encrypted using the public key ID. To decrypt C using the private key $d_{\mathsf{ID}} \in \mathbb{G}_1^*$ compute:

$$V \oplus H_2(\hat{e}(d_{\mathsf{ID}}, U)) = M.$$

In the basic embodiment, the receiver may perform Decrypt as illustrated in FIG. 4. In block 400, the system parameters are obtained (from an external resource such as a PKG, or from a local storage medium if they were obtained previously). The ciphertext V and an element rP are obtained from the sender in block 410. The element rP may be considered a portion of the total ciphertext obtained from the sender. In block 420 the receiver obtains the private key d_{ID} corresponding to the public identifier ID used to encrypt the message. The private key is normally

obtained from an external resource such as a PKG, or from a local storage medium if it was obtained previously. The secret message key is then computed in block 430, and used to decrypt the message in block 440.

This completes the description of BasicIdent for the basic embodiment. We first verify consistency. When everything is computed as above we have:
1. During encryption M is bitwise exclusive-ored with the hash of: g_{ID}^{r}.
2. During decryption V is bitwise exclusive-ored with the hash of: $\hat{e}(d_{\mathrm{ID}}, U)$.
These masks used during encryption and decryption are the same since:

$$\hat{e}(d_{\mathrm{ID}}, U) = \hat{e}(sQ_{\mathrm{ID}}, rP) = \hat{e}(Q_{\mathrm{ID}}, P)^{sr} = \hat{e}(Q_{\mathrm{ID}}, P_{pub})^{r} = g_{\mathrm{ID}}^{r}$$

Thus, applying decryption after encryption produces the original message M as required. Performance considerations of BasicIdent are discussed later.

Security. Next, we study the security of this basic embodiment.

The security of the exemplary system is based on the assumption that a variant of the Computational Diffie-Hellman problem in $\mathbb{G}_1$ is hard. The technical security details of the encryption scheme are discussed by the inventors in D. Boneh, M. Franklin, "Identity based encryption from the Weil pairing", extended abstract in *Advances in Cryptology – Crypto 2001*, Lecture Notes in Computer Science, Vol. 2139, Springer-Verlag, pp. 231–229, 2001, which is incorporated herein by reference.

In an exemplary embodiment, the performance of the system is comparable to the performance of ElGamal encryption in $\mathbb{F}_p^*$. The security of the exemplary system is based on a variant of the computational Diffie-Hellman assumption. Based on this assumption we show that the exemplary system has chosen ciphertext security in the random oracle model. In accordance with a distributed PKG embodiment, threshold cryptography techniques allow the PKG to be distributed so that the master-key is never available in a single location. Unlike common threshold systems, we show that robustness for the distributed PKG embodiment is free.

To argue about the security of the exemplary system, we define chosen ciphertext security for identity-based encryption. Our model gives the adversary more power than the standard model for chosen ciphertext security. First, we allow the attacker to attack an arbitrary public key ID of her choice. Second, while mounting a chosen

ciphertext attack on ID we allow the attacker to obtain from the PKG the private key for any public key of her choice, other than the private key for ID. This models an attacker who obtains a number of private keys corresponding to some identities of her choice and then tries to attack some other public key ID of her choice. Even with the help of such queries, it is desirable that the attacker still have negligible advantage in defeating the semantic security of the system.

The following theorem shows that BasicIdent is a semantically secure identity based encryption scheme (IND-ID-CPA) assuming BDH is hard in groups generated by $\mathcal{G}$.

Theorem 1 *Suppose the hash functions H_1, H_2 are random oracles. Then* BasicIdent *is a semantically secure identity based encryption scheme (*IND-ID-CPA*) assuming BDH is hard in groups generated by $\mathcal{G}$. Concretely, suppose there is an* IND-ID-CPA *adversary $\mathcal{A}$ that has advantage $\epsilon(k)$ against the scheme* BasicIdent. *Suppose $\mathcal{A}$ makes at most $q_E > 0$ private key extraction queries and $q_{H_2} > 0$ hash queries to H_2. Then there is an algorithm $\mathcal{B}$ that solves BDH in groups generated by $\mathcal{G}$ with advantage at least:*

$$Adv_{\mathcal{G},\mathcal{B}}(k) \geq \frac{2\epsilon(k)}{e(1+q_E)\cdot q_{H_2}}$$

Here $e \approx 2.71$ is the base of the natural logarithm. The running time of $\mathcal{B}$ is $O(time(\mathcal{A}))$.

To prove the theorem we first define a related Public Key Encryption scheme (not an identity based scheme), called BasicPub. BasicPub is described by three algorithms: keygen, encrypt, decrypt.

keygen: Given a security parameter $k \in \mathbb{Z}^+$, the algorithm works as follows:

Step 1: Run $\mathcal{G}$ on input k to generate two prime order groups $\mathbb{G}_1, \mathbb{G}_2$ and an admissible map $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$. Let q be the order of $\mathbb{G}_1, \mathbb{G}_2$. Choose an arbitrary generator $P \in \mathbb{G}_1$.

Step 2: Pick a random $s \in \mathbb{Z}_q^*$ and set $P_{pub} = sP$. Pick a random $Q_{\mathrm{ID}} \in \mathbb{G}_1^*$.

Step 3: Choose a cryptographic hash function $H_2 : \mathbb{G}_2 \rightarrow \{0,1\}^n$ for some n.

Step 4: The public key is $\langle q, \mathbb{G}_1, \mathbb{G}_2, \hat{e}, n, P, P_{pub}, Q_{\mathrm{ID}}, H_2 \rangle$. The private key is $d_{\mathrm{ID}} = sQ_{\mathrm{ID}} \in \mathbb{G}_1^*$.

encrypt: To encrypt $M \in \{0,1\}^n$ choose a random $r \in \mathbb{Z}_q^*$ and set the ciphertext to be:

$$C = \langle rP,\ M \oplus H_2(g^r) \rangle \quad \text{where} \quad g = \hat{e}(Q_{\text{ID}}, P_{pub}) \in \mathbb{G}_2^*$$

decrypt: Let $C = \langle U, V \rangle$ be a ciphertext created using the public key $\langle q, \mathbb{G}_1, \mathbb{G}_2, \hat{e}, n, P, P_{pub},$ To decrypt C using the private key $d_{\text{ID}} \in \mathbb{G}_1^*$ compute:

$$V \oplus H_2(\hat{e}(d_{\text{ID}}, U)) = M$$

This completes the description of BasicPub. We now prove Theorem 1 in two steps. We first show that an IND-ID-CPA attack on BasicIdent can be converted to a IND-CPA attack on BasicPub. This step shows that private key extraction queries do not help the adversary. We then show that BasicPub is IND-CPA secure if the BDH assumption holds. The proofs are omitted.

Lemma 2 *Let H_1 be a random oracle from $\{0,1\}^*$ to $\mathbb{G}_1^*$. Let $\mathcal{A}$ be an* IND-ID-CPA *adversary that has advantage $\epsilon(k)$ against* BasicIdent. *Suppose $\mathcal{A}$ makes at most $q_E > 0$ private key extraction queries. Then there is a* IND-CPA *adversary $\mathcal{B}$ that has advantage at least $\epsilon(k)/e(1+q_E)$ against* BasicPub. *Its running time is $O(time(\mathcal{A}))$.*

Lemma 3 *Let H_2 be a random oracle from $\mathbb{G}_2$ to $\{0,1\}^n$. Let $\mathcal{A}$ be an* IND-CPA *adversary that has advantage $\epsilon(k)$ against* BasicPub. *Suppose $\mathcal{A}$ makes a total of $q_{H_2} > 0$ queries to H_2. Then there is an algorithm $\mathcal{B}$ that solves the BDH problem for $\mathcal{G}$ with advantage at least $2\epsilon(k)/q_{H_2}$ and a running time $O(time(\mathcal{A}))$.*

Proof of Theorem 1. The theorem follows directly from Lemma 2 and Lemma 3. Composing both reductions shows that an IND-ID-CPA adversary on BasicIdent with advantage $\epsilon(k)$ gives a BDH algorithm for $\mathcal{G}$ with advantage at least $2\epsilon(k)/e(1+q_E)q_{H_2}$, as required. □

Identity-Based Encryption with Chosen Ciphertext Security

According to one embodiment of the invention, a technique of Fujisaki and Okamoto (described in E. Fujisaki and T. Okamoto, "Secure integration of asymmetric and symmetric encryption schemes", in *Advances in Cryptology – Crypto '99*, Lecture Notes

in Computer Science, Vol. 1666, Springer-Verlag, pp. 537–554, 1999, which is incorporated herein by reference) may be appropriately adapted to convert the BasicIdent embodiment of the previous section into a chosen ciphertext secure embodiment of an IBE system (in the sense defined earlier) in the random oracle model. Let $\mathcal{E}$ be a probabilistic public key encryption scheme. We denote by $\mathcal{E}_{pk}(M;r)$ the encryption of M using the random bits r under the public key pk. Fujisaki-Okamoto define the hybrid scheme $\mathcal{E}^{hy}$ as:

$$\mathcal{E}^{hy}_{pk}(M) \;=\; \langle\, \mathcal{E}_{pk}(\sigma; H_3(\sigma, M)),\;\; H_4(\sigma) \oplus M \,\rangle$$

Here σ is generated at random and H_3, H_4 are cryptographic hash functions. Fujisaki-Okamoto show that if $\mathcal{E}$ is a one-way encryption scheme then $\mathcal{E}^{hy}$ is a chosen ciphertext secure system (IND-CCA) in the random oracle model (assuming $\mathcal{E}_{pk}$ satisfies some natural constraints). We note that semantic security implies one-way encryption and hence the Fujisaki-Okamoto result also applies if $\mathcal{E}$ is semantically secure (IND-CPA).

We apply the Fujisaki-Okamoto transformation to BasicIdent and show that the resulting embodiment of an IBE system is IND-ID-CCA secure. We obtain the following IBE embodiment which we call FullIdent. Recall that n is the length of the message to be encrypted.

Setup: As in the BasicIdent scheme. In addition, we pick a hash function $H_3 : \{0,1\}^n \times \{0,1\}^n \to \mathbb{Z}_q^*$, and a hash function $H_4 : \{0,1\}^n \to \{0,1\}^n$.

Extract: As in the BasicIdent scheme.

Encrypt: To encrypt $M \in \{0,1\}^n$ under the public key ID do the following: (1) compute $Q_{\mathrm{ID}} = H_1(\mathrm{ID}) \in \mathbb{G}_1^*$, (2) choose a random $\sigma \in \{0,1\}^n$, (3) set $r = H_3(\sigma, M)$, and (4) set the ciphertext to be

$$C = \langle rP,\;\; \sigma \oplus H_2(g_{\mathrm{ID}}^r),\;\; M \oplus H_4(\sigma) \rangle \quad \text{where} \quad g_{\mathrm{ID}} = \hat{e}(Q_{\mathrm{ID}}, P_{pub}) \in \mathbb{G}_2$$

Decrypt: Let $C = \langle U, V, W \rangle$ be a ciphertext encrypted using the public key ID. If $U \notin \mathbb{G}_1^*$ reject the ciphertext. To decrypt C using the private key $d_{\mathrm{ID}} \in \mathbb{G}_1^*$ do:

1. Compute $V \oplus H_2(\hat{e}(d_{\mathrm{ID}}, U)) = \sigma$.
2. Compute $W \oplus H_4(\sigma) = M$.
3. Set $r = H_3(\sigma, M)$. Test that $U = rP$. If not, reject the ciphertext.
4. Output M as the decryption of C.

This completes the description of FullIdent. Its implementation follows the same basic pattern as BasicIdent shown in FIGS. 2, 3, 4. Note that M is encrypted as $W = M \oplus H_4(\sigma)$. This can be replaced by $W = E_{H_4(\sigma)}(M)$ where E is a semantically secure symmetric encryption scheme.

Security. The following theorem shows that FullIdent is a chosen ciphertext secure IBE (i.e. IND-ID-CCA), assuming BDH is hard in groups generated by $\mathcal{G}$.

Theorem 4 *Let the hash functions H_1, H_2, H_3, H_4 be random oracles. Then* FullIdent *is a chosen ciphertext secure IBE (*IND-ID-CCA*) assuming BDH is hard in groups generated by $\mathcal{G}$.*
Concretely, suppose there is an IND-ID-CCA *adversary $\mathcal{A}$ that has advantage $\epsilon(k)$ against the scheme* FullIdent *and $\mathcal{A}$ runs in time at most $t(k)$. Suppose $\mathcal{A}$ makes at most q_E extraction queries, at most q_D decryption queries, and at most $q_{H_2}, q_{H_3}, q_{H_4}$ queries to the hash functions H_2, H_3, H_4 respectively. Then there is a BDH algorithm $\mathcal{B}$ for $\mathcal{G}$ with running time $t_1(k)$ where:*

$$\begin{aligned} Adv_{\mathcal{G},\mathcal{B}}(k) &\geq 2FO_{adv}(\tfrac{\epsilon(k)}{e(1+q_E+q_D)}, q_{H_4}, q_{H_3}, q_D)/q_{H_2} \\ t_1(k) &\leq FO_{time}(t(k), q_{H_4}, q_{H_3}) \end{aligned}$$

where the functions FO_{time} and FO_{adv} are defined in Theorem 5.

The proof of Theorem 4 is based on the following result of Fujisaki and Okamoto. Let BasicPub^{hy} be the result of applying the Fujisaki-Okamoto transformation to BasicPub.

Theorem 5 (Fujisaki-Okamoto) *Suppose $\mathcal{A}$ is an* IND-CCA *adversary that achieves advantage $\epsilon(k)$ when attacking* BasicPub^{hy}. *Suppose $\mathcal{A}$ has running time $t(k)$, makes at most q_D decryption queries, and makes at most q_{H_3}, q_{H_4} queries to the hash functions H_3, H_4 respectively. Then there is an* IND-CPA *adversary $\mathcal{B}$ against* BasicPub *with running time $t_1(k)$ and advantage $\epsilon_1(k)$ where*

$$\begin{aligned} \epsilon_1(k) &\geq FO_{adv}(\epsilon(k), q_{H_4}, q_{H_3}, q_D) = \frac{1}{2(q_{H_4}+q_{H_3})}[(\epsilon(k)+1)(1-2/q)^{q_D}-1] \\ t_1(k) &\leq FO_{time}(t(k), q_{H_4}, q_{H_3}) = t(k) + O((q_{H_4}+q_{H_3})\cdot n), \quad \textit{and} \end{aligned}$$

Here q is the size of the groups $\mathbb{G}_1, \mathbb{G}_2$ and n is the length of σ.

In fact, Fujisaki-Okamoto prove a stronger result: Under the hypothesis of Theorem 5, BasicPub^{hy} would not even be a one-way encryption scheme. For our purposes the result in Theorem 5 is sufficient. To prove Theorem 4 we also need the following lemma to translate between an IND-ID-CCA chosen ciphertext attack on FullIdent and an IND-CCA chosen ciphertext attack on BasicPub^{hy}.

Lemma 6 *Let $\mathcal{A}$ be an* IND-ID-CCA *adversary that has advantage $\epsilon(k)$ against* FullIdent. *Suppose $\mathcal{A}$ makes at most $q_E > 0$ private key extraction queries and at most q_D decryption queries. Then there is an* IND-CCA *adversary $\mathcal{B}$ that has advantage at least $\frac{\epsilon(k)}{e(1+q_E+q_D)}$ against* BasicPub^{hy}. *Its running time is $O(time(\mathcal{A}))$.*

Proof of Theorem 4. By Lemma 6 an IND-ID-CCA adversary on FullIdent implies an IND-CCA adversary on BasicPub^{hy}. By Theorem 5 an IND-CCA adversary on BasicPub^{hy} implies an IND-CPA adversary on BasicPub. By Lemma 3 an IND-CPA adversary on BasicPub implies an algorithm for BDH. Composing all these reductions gives the required bounds. □

Relaxing the hashing requirements

Recall that an IBE system of Section uses a hash function $H_1 : \{0,1\}^* \rightarrow \mathbb{G}_1^*$. The detailed example of an IBE system presented in the next section uses $\mathbb{G}_1$ as a subgroup of the group of points on an elliptic curve. In practice, it sometimes can be difficult to build hash functions that hash directly onto such groups. In an exemplary embodiment, we therefore show how to relax the requirement of hashing directly onto $\mathbb{G}_1^*$. Rather than hash onto $\mathbb{G}_1^*$ we hash onto some set $A \subseteq \{0,1\}^*$ and then use a deterministic encoding function to map A onto $\mathbb{G}_1^*$.

Admissible encodings: Let $\mathbb{G}_1$ be a group and let $A \in \{0,1\}^*$ be a finite set. We say that an encoding function $L : A \rightarrow \mathbb{G}_1^*$ is *admissible* if it satisfies the following properties:

1. Computable: There is an efficient deterministic algorithm to compute $L(x)$ for any $x \in A$.
2. ℓ-to-1: For any $y \in \mathbb{G}_1^*$ the preimage of y under L has size exactly ℓ. In other words, $|L^{-1}(y)| = \ell$ for all $y \in \mathbb{G}_1^*$. Note that this implies that $|A| = \ell \cdot |\mathbb{G}_1^*|$.

3. Samplable: There is an efficient randomized algorithm $\mathcal{L}_S$ such that $\mathcal{L}_S(y)$ induces a uniform distribution on $L^{-1}(y)$ for any $y \in \mathbb{G}_1^*$. In other words, $\mathcal{L}_S(y)$ is a uniform random element in $L^{-1}(y)$.

We modify FullIdent to obtain an IND-ID-CCA secure embodiment of an IBE system where H_1 is replaced by a hash function into some set A. Since the change is relatively minor we refer to this new scheme as FullIdent':

Setup: As in the FullIdent embodiment. The only difference is that H_1 is replaced by a hash function $H_1' : \{0,1\}^* \rightarrow A$. The system parameters also include a description of an admissible encoding function $L : A \rightarrow \mathbb{G}_1^*$.

Extract, Encrypt: As in the FullIdent embodiment. The only difference is that in Step 1 these algorithms compute $Q_{\mathsf{ID}} = L(H_1'(\mathsf{ID})) \in \mathbb{G}_1^*$.

Decrypt: As in the FullIdent embodiment.

This completes the description of FullIdent'. The following theorem shows that FullIdent' is a chosen ciphertext secure IBE (i.e. IND-ID-CCA), assuming FullIdent is.

Theorem 7 *Let $\mathcal{A}$ be an* IND-ID-CCA *adversary on* FullIdent' *that achieves advantage $\epsilon(k)$. Suppose $\mathcal{A}$ makes at most q_{H_1} queries to the hash function H_1'. Then there is an* IND-ID-CCA *adversary $\mathcal{B}$ on* FullIdent *that achieves the same advantage $\epsilon(k)$ and $time(\mathcal{B}) = time(\mathcal{A}) + q_{H_1} \cdot time(L_S)$*

Proof Sketch Algorithm $\mathcal{B}$ attacks FullIdent by running algorithm $\mathcal{A}$. It relays all decryption queries, extraction queries, and hash queries from $\mathcal{A}$ directly to the challenger and relays the challenger's response back to $\mathcal{A}$. It only behaves differently when $\mathcal{A}$ issues a hash query to H_1'. Recall that $\mathcal{B}$ only has access to a hash function $H_1 : \{0,1\}^* \rightarrow \mathbb{G}_1^*$. To respond to H_1' queries algorithm $\mathcal{B}$ maintains a list of tuples $\langle \mathsf{ID}_j, y_j \rangle$ as explained below. We refer to this list as the $(H_1')^{list}$. The list is initially empty. When $\mathcal{A}$ queries the oracle H_1' at a point ID_i algorithm $\mathcal{B}$ responds as follows:

1. If the query ID_i already appears on the $(H_1')^{list}$ in a tuple $\langle \mathsf{ID}_i, y_i \rangle$ then respond with $H_1'(\mathsf{ID}_i) = y_i \in A$.
2. Otherwise, $\mathcal{B}$ issues a query for $H_1(\mathsf{ID}_i)$. Say, $H_1(\mathsf{ID}_i) = \alpha \in \mathbb{G}_1^*$.
3. $\mathcal{B}$ runs the sampling algorithm $\mathcal{L}_S(\alpha)$ to generate a random element $y \in L^{-1}(\alpha)$.

4. $\mathcal{B}$ adds the tuple $\langle \mathsf{ID}_i, y \rangle$ to the $(H_1^l)^{list}$ and responds to $\mathcal{A}$ with $H_1^l(\mathsf{ID}_i) = y \in A$. Note that y is uniformly distributed in A as required since α is uniformly distributed in $\mathbb{G}_1^*$ and L is an ℓ-to-1 map.

Algorithm $\mathcal{B}$'s responses to all of $\mathcal{A}$'s queries, including H_1^l queries, are identical to $\mathcal{A}$'s view in the real attack. Hence, $\mathcal{B}$ will have the same advantage $\epsilon(k)$ in winning the game with the challenger. □

A DETAILED EXAMPLE OF AN IBE SYSTEM USING THE WEIL PAIRING

In this section we use FullIdent' to describe a detailed example of an embodiment of an IBE system. This embodiment is based on the Weil pairing. Although in practice the Tate pairing has computational advantages and may be used instead of the Weil pairing in various embodiments, the implementation using the Weil pairing will be described first because it is simpler. Later, the Tate pairing will be discussed.

Properties of the Weil Pairing

Let $p > 3$ be a prime satisfying $p = 2 \bmod 3$ and let q be some prime factor of $p + 1$. Let E be the elliptic curve defined by the equation $y^2 = x^3 + 1$ over $\mathbb{F}_p$. We state a few elementary facts about this curve E. From here on we let $E(\mathbb{F}_{p^r})$ denote the group of points on E defined over $\mathbb{F}_{p^r}$.

Fact 1: Since $x^3 + 1$ is a permutation on $\mathbb{F}_p$ it follows that the group $E(\mathbb{F}_p)$ contains $p + 1$ points. We let O denote the point at infinity. Let $P \in E(\mathbb{F}_p)$ be a point of order q and let $\mathbb{G}_1$ be the subgroup of points generated by P.

Fact 2: For any $y_0 \in \mathbb{F}_p$ there is a unique point (x_0, y_0) on $E(\mathbb{F}_p)$, namely $x_0 = (y_0^2 - 1)^{1/3} \in \mathbb{F}_p$. Hence, if (x, y) is a random non-zero point on $E(\mathbb{F}_p)$ then y is uniform in $\mathbb{F}_p$. We use this property to build a simple admissible encoding function.

Fact 3: Let $1 \neq \zeta \in \mathbb{F}_{p^2}$ be a solution of $x^3 - 1 = 0 \bmod p$. Then the map $\phi(x, y) = (\zeta x, y)$ is an automorphism of the group of points on the curve E. Note that for any point $Q = (x, y) \in E(\mathbb{F}_p)$ we have that $\phi(Q) \in E(\mathbb{F}_{p^2})$, but $\phi(Q) \notin E(\mathbb{F}_p)$. Hence, $Q \in E(\mathbb{F}_p)$ is linearly independent of $\phi(Q) \in E(\mathbb{F}_{p^2})$.

Fact 4: Since the points $P \in \mathbb{G}_1$ and $\phi(P)$ are linearly independent they generate a group isomorphic to $\mathbb{Z}_q \times \mathbb{Z}_q$. We denote this group of points by $E[q]$.

Let $\mathbb{G}_2$ be the subgroup of $\mathbb{F}_{p^2}^*$ of order q. The Weil pairing on the curve $E(\mathbb{F}_{p^2})$ is a mapping $e : E[q] \times E[q] \rightarrow \mathbb{G}_2$. (This map is defined and discussed in the section below entitled Description of the Weil Pairing.) For any $Q, R \in E(\mathbb{F}_p)$ the Weil pairing satisfies $e(Q, R) = 1$. In other words, the Weil pairing is degenerate on $E(\mathbb{F}_p)$, and hence degenerate on the group $\mathbb{G}_1$. To get a non-degenerate map we define the modified Weil pairing $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ as follows:

$$\hat{e}(P, Q) = e(P, \phi(Q))$$

The modified Weil pairing satisfies the following properties:

1. Bilinear: For all $P, Q \in \mathbb{G}_1$ and for all $a, b \in \mathbb{Z}$ we have $\hat{e}(aP, bQ) = \hat{e}(P, Q)^{ab}$.
2. Non-degenerate: If P is a generator of $\mathbb{G}_1$ then $\hat{e}(P, P) \in \mathbb{F}_{p^2}^*$ is a generator of $\mathbb{G}_2$.
3. Computable: Given $P, Q \in \mathbb{G}_1$ there is an efficient algorithm to compute $\hat{e}(P, Q) \in \mathbb{G}_2$. (This algorithm is described in the section below entitled Description of the Weil Pairing.) Its running time is comparable to exponentiation in $\mathbb{F}_p$.

Although the the Computational Diffie-Hellman problem (CDH) appears to be hard in the group $\mathbb{G}_1$, the Decision Diffie-Hellman problem (DDH) is easy in $\mathbb{G}_1$.

BDH Parameter Generator $\mathcal{G}_1$: Given a security parameter $2 < k \in \mathbb{Z}$ the BDH parameter generator picks a random k-bit prime q and finds the smallest prime p such that (1) $p = 2 \bmod 3$, (2) q divides $p + 1$, and (3) q^2 does not divide $p + 1$. We write $p = \ell q + 1$. The group $\mathbb{G}_1$ is the subgroup of order q of the group of points on the curve $y^2 = x^3 + 1$ over $\mathbb{F}_p$. The group $\mathbb{G}_2$ is the subgroup of order q of $\mathbb{F}_{p^2}^*$. The bilinear map $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ is the modified Weil pairing defined above.

The BDH parameter generator $\mathcal{G}_1$ is believed to satisfy the BDH assumption asymptotically. However, there is still the question of what values of p and q can be used in practice to make the BDH problem sufficiently hard. It is desirable that we can ensure, at the very least, that the discrete log problem in $\mathbb{G}_1$ is sufficiently hard. As pointed out earlier, the discrete log problem in $\mathbb{G}_1$ is efficiently reducible to discrete log in $\mathbb{G}_2$. Hence, computing discrete log in $\mathbb{F}_{p^2}^*$ is sufficient for computing discrete log in $\mathbb{G}_1$. In practice, for proper security of discrete log in $\mathbb{F}_{p^2}^*$ it is desirable to use primes p that are at least 512-bits long (so that the group size is at least 1024-bits long). Consequently, in some embodiments, this BDH parameter generator is used with primes p that may be 512-bits long or more.

An admissible encoding function: MapToPoint

Let $\mathbb{G}_1, \mathbb{G}_2$ be two groups generated by $\mathcal{G}_1$ as defined above. Recall that an IBE system discussed earlier uses a hash function $H_1 : \{0,1\}^* \rightarrow \mathbb{G}_1^*$. It suffices to have a hash function $H_1 : \{0,1\}^* \rightarrow A$ for some set A, and an admissible encoding function $L : A \rightarrow \mathbb{G}_1^*$. In what follows the set A will be $\mathbb{F}_p$, and the admissible encoding function L will be called MapToPoint, which may be used in various embodiments of the present invention.

In this example, let p be a prime satisfying $p = 2 \bmod 3$ and $p = \ell q - 1$ for some prime $q > 3$. In this exemplary embodiment, q does not divide ℓ (i.e. q^2 does not divide $p+1$). Let E be the elliptic curve $y^2 = x^3 + 1$ over $\mathbb{F}_p$. Let $\mathbb{G}_1$ be the subgroup of points on E of order q. In addition, a hash function $H_1 : \{0,1\}^* \rightarrow \mathbb{F}_p$ is provided.

In this exemplary embodiment, algorithm MapToPoint works as follows on input $y_0 \in \mathbb{F}_p$:

1. Compute $x_0 = (y_0^2 - 1)^{1/3} = (y_0^2 - 1)^{(2p-1)/3} \in \mathbb{F}_p$.
2. Let $Q = (x_0, y_0) \in E(\mathbb{F}_p)$ and set $Q_{\text{ID}} = \ell Q \in \mathbb{G}_1$.
3. Output $\text{MapToPoint}(y_0) = Q_{\text{ID}}$.

This completes the description of MapToPoint.

We note that there are $\ell - 1$ values of $y_0 \in \mathbb{F}_p$ for which $\ell Q = \ell(x_0, y_0) = O$ (these are the non-O points of order dividing ℓ). Let $B \subset \mathbb{F}_p$ be the set of these y_0. When $H_1(\text{ID})$ is one of these $\ell - 1$ values Q_{ID} is the identity element of $\mathbb{G}_1$. It is extremely unlikely for $H_1(\text{ID})$ to hit one of these points – the probability is $1/q < 1/2^k$. Hence, for simplicity we say that $H_1(\text{ID})$ only outputs elements in $\mathbb{F}_p \setminus B$, i.e. $H_1 : \{0,1\}^* \rightarrow \mathbb{F}_p \setminus B$. In other embodiments, algorithm MapToPoint can be easily extended to handle the values $y_0 \in B$ by hashing ID multiple times using different hash functions.

Proposition 8 $\text{MapToPoint} : \mathbb{F}_p \setminus B \rightarrow \mathbb{G}_1^*$ *is an admissible encoding function.*

Proof The map is clearly computable and is a $\ell - to - 1$ mapping. It remains to show that L is samplable. Let P be a generator of $E(\mathbb{F}_p)$. Given a $Q \in \mathbb{G}_1^*$ the sampling algorithm $\mathcal{L}_S$ does the following: (1) pick a random $b \in \{0, \ldots, \ell - 1\}$, (2)

compute $Q' = \ell^{-1} \cdot Q + bqP = (x, y)$, and (3) output $\mathcal{L}_S(Q) = y \in \mathbb{F}_p$. Here ℓ^{-1} is the inverse of ℓ in $\mathbb{Z}_q^*$. This algorithm outputs a random element from the ℓ elements in $\mathsf{MapToPoint}^{-1}(Q)$ as required. □

A detailed example of an IBE system

Using the BDH parameter generator $\mathcal{G}_1$ and the admissible encoding function MapToPoint we obtain the following detailed example of an embodiment of an IBE system.

Setup: Given a security parameter $k \in \mathbb{Z}^+$, the algorithm works as follows:

Step 1: Run $\mathcal{G}_1$ on input k to generate a k-bit prime q and a prime $p = 2 \bmod 3$ such that q divides $p+1$. Let E be the elliptic curve defined by $y^2 = x^3 + 1$ over $\mathbb{F}_p$. Choose an arbitrary $P \in E(\mathbb{F}_p)$ of order q.

Step 2: Pick a random $s \in \mathbb{Z}_q^*$ and set $P_{pub} = sP$.

Step 3: Pick four hash functions: $H_1 : \{0,1\}^* \to \mathbb{F}_p$; $H_2 : \mathbb{F}_{p^2} \to \{0,1\}^n$ for some n ; $H_3 : \{0,1\}^n \times \{0,1\}^n \to \mathbb{Z}_q^*$, and a hash function $H_4 : \{0,1\}^n \to \{0,1\}^n$.

The message space is $\mathcal{M} = \{0,1\}^n$. The ciphertext space is $\mathcal{C} = E(\mathbb{F}_p) \times \{0,1\}^n$.

The system parameters are $\mathsf{params} = \langle p, q, n, P, P_{pub}, H_1, \ldots, H_4 \rangle$. The master-key is $s \in \mathbb{Z}_q^*$.

Extract: For a given string $\mathsf{ID} \in \{0,1\}^*$ the algorithm builds a private key d as follows:

Step 1: Compute $\mathsf{MapToPoint}(H_1(\mathsf{ID})) = Q_{\mathsf{ID}} \in E(\mathbb{F}_p)$ of order q.

Step 2: Set the private key d_{ID} to be $d_{\mathsf{ID}} = sQ_{\mathsf{ID}}$ where s is the master key.

Encrypt: To encrypt $M \in \{0,1\}^n$ under the public key ID do the following:

Step 1: Compute $\mathsf{MapToPoint}(H_1(\mathsf{ID})) = Q_{\mathsf{ID}} \in E(\mathbb{F}_p)$ of order q.

Step 2: Choose a random $\sigma \in \{0,1\}^n$.

Step 3: Set $r = H_3(\sigma, M)$.

Step 4: Set the ciphertext to be

$$C = \langle rP,\ \sigma \oplus H_2(g_{\mathsf{ID}}^r),\ M \oplus H_4(\sigma) \rangle \quad \text{where} \quad g_{\mathsf{ID}} = \hat{e}(Q_{\mathsf{ID}}, P_{pub}) \in \mathbb{F}_{p^2}$$

Decrypt: Let $C = \langle U, V, W \rangle \in \mathcal{C}$ be a ciphertext encrypted using the public key ID. If $U \in E(\mathbb{F}_p)$ is not a point of order q reject the ciphertext. To decrypt C using the

private key d_{ID} do:

Step 1. Compute $V \oplus H_2(\hat{e}(d_{\mathrm{ID}}, U)) = \sigma$.

Step 2. Compute $W \oplus H_4(\sigma) = M$.

Step 3. Set $r = H_3(\sigma, M)$. Test that $U = rP$. If not, reject the ciphertext.

Step 4. Output M as the decryption of C.

Performance. In this embodiment, algorithms Setup and Extract are very simple. At the heart of both algorithms is a standard multiplication on the curve $E(\mathbb{F}_p)$. Algorithm Encrypt requires that the encryptor compute the Weil pairing of Q_{ID} and P_{pub}. Note that this computation is independent of the message, and hence can be done once and for all. Once g_{ID} is computed the performance of this embodiment is almost identical to standard ElGamal encryption. We also note that the ciphertext length of the exemplary embodiment of BasicIdent is the same as in regular ElGamal encryption in $\mathbb{F}_p$. Decryption is a simple Weil pairing computation.

Security. The security of the detailed exemplary embodiment just described follows directly from Theorem 4 and Theorem 7.

Corollary 9 *The detailed exemplary embodiment described above is a chosen ciphertext secure IBE system (i.e.* IND-ID-CCA *in the random oracle model) assuming the BDH parameter generator $\mathcal{G}_1$ satisfies the BDH assumption.*

Extensions and Observations

Tate pairing and other curves.

Embodiments of our IBE system work with efficiently computable bilinear maps $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$ between two groups $\mathbb{G}_1, \mathbb{G}_2$ where the BDH assumption holds. Many different elliptic curves may give rise to such maps. For example, one could use the curve $y^2 = x^3 + x$ over $\mathbb{F}_p$ with $p = 3 \bmod 4$ and its endomorphism $\phi : (x, y) \to (-x, iy)$ where $i^2 = -1$.

In an alternative embodiment, one may use a family of nonsupersingular elliptic curves over $\mathbb{F}_p$ discussed by Miyaji et al. (A. Miyaji, M. Nakabayashi, S. Takano,

"New explicit condition of elliptic curve trace for FR-reduction", *IEICE Trans. Fundamentals*, Vol. E84 A, No. 5, May 2001). For example, to use a curve $E/\mathbb{F}_p$ in this family one can take $\mathbb{G}_1$ to be a cyclic subgroup of $E(\mathbb{F}_{p^6})$ (that is not contained in $E(\mathbb{F}_p)$) and then use the trace map on the curve E as the endomorphism ϕ used to define the pairing $\hat{e}$. We also note that both encryption and decryption in FullIdent can be made faster in alternate embodiments by using the Tate pairing on elliptic curves rather than the Weil pairing. In other embodiments, suitable bilinear maps may be derived from abelian varieties.

Asymmetric pairings

As mentioned earlier, embodiments of our IBE system are not limited to symmetric maps, but may include asymmetric maps as well. In other words, embodiments generally may use maps of the form $\hat{e} : \mathbb{G}_0 \times \mathbb{G}_1 \to \mathbb{G}_2$ where $\mathbb{G}_0, \mathbb{G}_1$ are groups of prime order q. When $\mathbb{G}_0$ and $\mathbb{G}_1$ are equal we say the map is symmetric. When$\mathbb{G}_0$ and $\mathbb{G}_1$ are not equal we say the map is asymmetric.

The elements Q_{ID} and P in the asymmetric case are members of $\mathbb{G}_0$ and $\mathbb{G}_1$, respectively (or vice versa), and the target group of the hash function H_1 is selected accordingly. However, to make the proof of security go through (Lemma 2 in particular) we use a slightly strange looking complexity assumption which we call the co-BDH assumption: given random $P, aP, bP \in \mathbb{G}_1$ and $Q, aQ, cQ \in \mathbb{G}_0$ no polynomial time algorithm can compute $\hat{e}(P, Q)^{abc}$ with non-negligible probability. If one is uses this assumption then for embodiments using a curve $E/\mathbb{F}_p$ from Miyaji et al. (as just described above) one can take $\mathbb{G}_1$ to be a cyclic subgroup of $E(\mathbb{F}_p)$ of order q and $\mathbb{G}_0$ to be a different cyclic subgroup of $E(\mathbb{F}_{p^6})$ of order q. This will result in a more efficient system than the method described in the preceding paragraph for using these curves.

Distributed PKG

In exemplary embodiments of an IBE system it is desirable that the master-key stored at the PKG be protected. One way of protecting this key is by distributing it among different sites using techniques of threshold cryptography. Embodiments of our IBE system support this in a very efficient and robust way. Recall that in some embodiments discussed above, the master-key may be some $s \in \mathbb{Z}_q^*$ and the PKG uses

the group action to compute a private key from s and Q_{ID}, where Q_{ID} is derived from the user's public key ID. For example, $d_{ID} = sQ_{ID}$. A distributed PKG embodiment can be implemented in a t-out-of-n fashion by giving each of the n PKGs one share s_i of a Shamir secret sharing of s mod q. Each of the n PKGs can use its share s_i of the master key to generate a corresponding share d_i of a private key d_{ID} by calculating $d_i = s_i Q_{ID}$. The user can then construct the entire private key d_{ID} by requesting from t of the n PKGs its share d_i of the private key, then combining the shares by calculating $d_{ID} = \sum_i \lambda_i d_i$, where the λ_i's are the appropriate Lagrange interpolation coefficients.

Furthermore, it is easy to make this embodiment robust against dishonest PKGs using the fact that DDH is easy in $\mathbb{G}_1$. During setup each of the n PKGs publishes $P_i = s_i P$. During a key generation request the user can verify that the response from the i'th PKG is valid by testing that:

$$\hat{e}(d_i, P) = \hat{e}(Q_{ID}, P_i)$$

Thus, a misbehaving PKG will be immediately caught. There is no need for zero-knowledge proofs as in regular robust threshold schemes. The PKG's master-key can be generated in a distributed fashion using the techniques of R. Gennaro et al. (R. Gennaro, S. Jarecki, H. Krawczyk, T. Rabin, "Secure Distributed Key Generation for Discrete-Log Based Cryptosystems", *Advances in Cryptology – Eurocrypt '99*, Lecture Notes in Computer Science, Vol. 1592, Springer-Verlag, pp. 295–310, 1999). Using this technique, the PKGs can execute a cooperative protocol that allows them to jointly generate their respective shares of the master key without the master key ever existing in any one place.

Note that a distributed master-key embodiment also enables threshold decryption on a *per-message* basis, without any need to derive the corresponding decryption key. For example, threshold decryption of BasicIdent ciphertext (U, V) is straightforward if each PKG responds with $\hat{e}(s_i Q_{ID}, U)$.

FIG. 5 is a block diagram illustrating a distributed PKG system, according to an embodiment of the invention. FIG. 5 includes a sender system 501, receiver system 502 and three PKGs (PKG A 503, PKG B 504 and PKG C 505). In one embodiment illustrating a 2-out-of-3 sharing, each of three PKGs contains a different share of a master key, and any two of the three are able to derive the master key. As shown in the figure, PKG A 503, PKG B 504, and PKG C 505 include, respectively, master key

share s_1, 511, master key share s_2, 512, and master key share s_3, 513. In 2-out-of-3 sharing, any two out of these three PKGs could combine their shares to determine the master key, although in this embodiment each PKG secretly holds its master key share.

Sender system 501 sends a message to receiver 502. The message 514 may be encrypted using a public key based on an identifier ID of the receiver. In order to obtain the corresponding private key, the receiver system queries two of the three PKGs using, for example, the receiver's identity or public key. As shown in the figure, receiver system 502 makes queries 506 and 507 to PKG A 503 and PKG B 504, respectively, in order to obtain two shares of the private key. In response to the queries, PKG A 503 and PKG B 504 return, respectively, share d_1, 508, and share d_2, 509, of private key d, 510. Receiver system 502 is then able to assemble the corresponding private key d_{ID}, which corresponds to the public key with which the message 514 was encrypted. More generally, the receiver could have selected to query any two of the three PKGs. For example, receiver system 502 alternatively could have queried PKGs B and C and combined private key shares d_2 and d_3 to produce the private key 510. These techniques easily generalize to provide similar embodiments using t-out-of$n$ sharing.

Sender system 501, receiver system 502 as well as PKGs 503, 504 and 505 may be each implemented as computer systems which include elements such as processors and computer-readable media such as memory and other storage devices. Communication between the respective elements may take place using data packets sent over data networks, or any of various other forms of electronic and data transmission and communication. The communication may transpire over various architectures of communication, such as a computer network, such as the Internet, with various wired, wireless and other communications media.

Working in subgroups

In an alternative embodiment of the detailed IBE system described above, performance may be improved by working in a comparatively small subgroup of the curve. For example, choose a 1024-bit prime $p = 2 \bmod 3$ with $p = aq - 1$ for some 160-bit prime q. The point P is then chosen to be a point of order q. Each public key ID is converted to a group point by hashing ID to a point Q on the curve and then multi-

plying the point by a. The system is secure if the BDH assumption holds in the group generated by P. The advantage of this embodiment is that the Weil computation is done on points of small order, and hence is much faster.

IBE implies signatures

Various IBE techniques described above can be used to provide public key signature systems and methods. The intuition is as follows. The private key for the signature scheme is the master key for the IBE scheme. The public key for the signature scheme is the set of global system parameters for the IBE scheme. The signature on a message M is the IBE decryption key for $\mathsf{ID} = M$. To verify a signature, choose a random message M', encrypt M' using the public key $\mathsf{ID} = M$, and then attempt to decrypt using the given signature on M as the decryption key. If the IBE system is IND-ID-CCA, then the signature scheme is existentially unforgeable against a chosen message attack. Note that, unlike most signature schemes, this signature verification embodiment is randomized. This shows that the IBE techniques described herein may encompass both public key encryption and digital signatures. Signature schemes derived from these approaches can be used to provide interesting properties, as described by Boneh et al. (D. Boneh, B. Lynn, H. Shacham, "Short signatures from the Weil pairing", in *Advances in Cryptology – AsiaCrypt 2001*, Lecture Notes in Computer Science, Vol. 2248, Springer-Verlag, pp. 514-532, 2001, which is incorporated herein by reference).

Escrow ElGamal encryption

In this section we show that various IBE techniques described above can be used to provide an ElGamal encryption system embodiment having global escrow capability. In this embodiment, a single escrow key enables the decryption of ciphertexts encrypted under any public key.

In one exemplary embodiment, the ElGamal escrow system works as follows. The Setup is similar to that for BasicIdent. Unlike the identity-based BasicIdent, each user selects a secret random number and uses it to generate a public/private key pair. A sender and receiver can then use Encrypt and Decrypt to communicate an encrypted message. The message is secure except for an escrow who can use a master key s to decrypt the message.

FIG. 6 is a block diagram illustrating elements in a cryptosystem with escrow decryption capability according to an embodiment of the invention. The system includes a sender system 601 with encryption logic 610, receiver system 602 with decryption logic 611, escrow agent system 604 and broadcasting system 605. Broadcast system 605 sends system parameters to participants such as escrow agent system 604, receiver system 602 and sender system 601. The receiver system 602 selects a private key x, 607, and uses it to generate a public key $P_{pub} = xP$, 606, which is then published. The private key x and the public key P_{pub} form a complementary key pair. Using the public key $P_{pub} = xP$, 606, sender system 601 encrypts a message M with encryption logic 610. Sender system 601 sends a resulting encrypted message 603 to receiver 602. Receiver system 602 decrypts the message with decryption logic 611 using the private key x, 607. Escrow agent system 604 may intercept message 603 and, using the escrow agent key s, 609, public key $P_{pub} = xP$, 606, and decrypt message 603 with decryption logic 612. In an alternate embodiment, broadcast system 605 and escrow agent 604 may be a single entity. In yet another embodiment, the escrow agent key s may be shared in a manner such as in the distributed PKG embodiments described earlier.

In more detail, an exemplary embodiment of the technique involves the following procedures:

Setup: Let $\mathcal{G}$ be some BDH parameter generator. Given a security parameter $k \in \mathbb{Z}^+$, the algorithm works as follows:

Step 1: Run $\mathcal{G}$ on input k to generate a prime q, two groups $\mathbb{G}_1, \mathbb{G}_2$ of order q, and an admissible map $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$. Let P be some generator of $\mathbb{G}_1$.

Step 2: Pick a random $s \in \mathbb{Z}_q^*$ and set $Q = sP$.

Step 3: Choose a cryptographic hash function $H : \mathbb{G}_2 \rightarrow \{0,1\}^n$.

The message space is $\mathcal{M} = \{0,1\}^n$. The ciphertext space is $\mathcal{C} = \mathbb{G}_1 \times \{0,1\}^n$. The system parameters are $\mathsf{params} = \langle q, \mathbb{G}_1, \mathbb{G}_2, \hat{e}, n, P, Q, H \rangle$. The escrow key is $s \in \mathbb{Z}_q^*$.

keygen: A user generates a public/private key pair for herself by picking a random $x \in \mathbb{Z}_q^*$ and computing $P_{pub} = xP \in \mathbb{G}_1$. Her private key is x (or xQ), her public key is P_{pub}.

Encrypt: To encrypt $M \in \{0,1\}^n$ under the public key P_{pub} do the following: (1) pick a random $r \in \mathbb{Z}_q^*$, and (2) set the ciphertext to be:

$$C = \langle rP,\ M \oplus H(g^r) \rangle \quad \text{where} \quad g = \hat{e}(P_{pub}, Q) \in \mathbb{G}_2.$$

This encryption technique is also illustrated in FIG. 7, where the sender obtains the system parameters and elements P and $Q = sP$ in block 700, and obtains the recipient's public key $P_{pub} = xP$ in block 710. The sender then selects a random r and computes a message key in block 720. The message key is then used to encrypt a message in block 730. The sender then transmits an encapsulated key rP and encrypted message V to the receiver.

Decrypt: Let $C = \langle U, V \rangle$ be a ciphertext encrypted using P_{pub}. Then $U \in \mathbb{G}_1$. To decrypt C using the private key x do:

$$V \oplus H(\hat{e}(U, xQ)) = M.$$

As illustrated in FIG. 8, the receiver obtains the system parameters and elements P and $Q = sP$ in block 800, then obtains the encrypted message V and encapsulated key rP from the sender in block 810. The receiver then computes the message key in block 820, and uses it to decrypt the message in block 830.

To see that the message keys computed by the sender and receiver are the same, note that the sender knows the secret r as well as the public $Q = sP$ and $P_{pub} = xP$, and uses these to compute a key from $\hat{e}(sP, xP)^r$. The receiver, on the other hand, knows the secret x as well as the public $Q = sP$ and rP, and uses these to compute a message key from $\hat{e}(rP, x(sP))$. The bilinearity of $\hat{e}$ implies that $\hat{e}(sP, xP)^r = \hat{e}(rP, x(sP))$, so the sender and receiver compute the same message key.

Escrow-decrypt: The purpose of this embodiment is to permit escrow decryption of otherwise secure communications. To decrypt $C = \langle U, V \rangle$ using the escrow key s, compute:

$$V \oplus H(\hat{e}(U, sP_{pub})) = M.$$

As shown in FIG. 9, the escrow obtains the system parameters and element P in block 900, then in block 910 obtains the recipient's public key xP, and obtains the encrypted message V and encapsulated key rP from the sender. The escrow then computes the message key in block 920, and uses it to decrypt the message in block 930. The escrow can compute the message key from the knowledge of s, rP, and xP.

A standard argument shows that assuming that BDH is hard for groups generated by $\mathcal{G}$ the system of this embodiment has semantic security in the random oracle model (recall that since DDH is easy we cannot prove semantic security based on DDH). Yet, the escrow agent can decrypt any ciphertext encrypted using any user's public key. The decryption capability of the escrow agent can be distributed using the PKG distribution techniques described earlier.

Another embodiment uses a similar hardness assumption, with an ElGamal encryption system with non-global escrow. In this embodiment, each user constructs a public key with two corresponding private keys, and gives one of the private keys to the trusted third party. The trusted third party maintains a database of all private keys given to it by the various users. Although both private keys can be used to decrypt, only the user's private key can be used simultaneously as the signing key for a discrete logarithm based signature scheme.

Various other cryptographic systems can be devised based on the principles illustrated in the above embodiments. For example, three entities A, B, and C can communicate securely as a group by privately selecting random integers a, b, c and publishing public keys aP, bP, cP. One of them, such as A, could encrypt a message using the message key $\hat{e}(bP, cP)^r$ and transmit it with rP. Then B could decrypt the message by calculating $\hat{e}(cP, rP)^b$ and C could decrypt it by calculating $\hat{e}(bP, rP)^c$. Similarly, B could send a message to A and C, or C could send a message to A and B.

In another possible embodiment, two of the three entities, say A and B, could publish a joint public key abP. Then C could encrypt a message using the message key $\hat{e}(abP, cP)^r$ and transmit it with rP. Then neither A nor B alone could decrypt the message, but both A and B together could compute $\hat{e}(cP, rP)^{ab}$ and jointly decrypt the message. This technique generalizes to any number of entities. For example, C could join A and B by using abP to compute and publish the three-way joint public key $abcP$. Then anyone could encrypt a message using the message key $\hat{e}(abcP, xP)^r$ and transmit it with rP. Then only A and B and C together could compute $\hat{e}(xP, rP)^{abc}$ and jointly decrypt the message.

Threshold decryption.

Embodiments of the invention enable n entities to have shares of a private key d_{ID} corresponding to a given public key ID, so that messages encrypted using ID can only be decrypted if t of the n entities collaborate. The private key d_{ID} is never reconstructed in a single location. Embodiments of our IBE system may support this as follows.

Recall that in other embodiments the private key $d_{\mathsf{ID}} = sQ_{\mathsf{ID}}$ where $s \in \mathbb{Z}_q^*$ is the master-key. Instead, let $s_1, \ldots, s_n \in \mathbb{Z}_q^*$ be a t-out-of-n Shamir secret sharing of the master-key s. Each of the n users is given $d_i = s_i Q_{\mathsf{ID}}$. To decrypt a ciphertext $\langle U, V \rangle$ encrypted using the key ID each user locally computes $g_i = \hat{e}(U, d_i)$ and sends $g_i \in \mathbb{G}_2$ to the user managing the decryption process. That user then combines the decryption shares by computing $g_{\mathsf{ID}} = \prod_i g_i^{\lambda_i}$ where λ_i are the appropriate Lagrange interpolation coefficients used in Shamir secret sharing. The message is then obtained by computing $H_2(g_{\mathsf{ID}}) \oplus V = M$.

Those skilled in the art of cryptography will be able to devise many other schemes that employ the basic principles of the present invention.

Applications of Identity-Based Encryption

One application for embodiments of identity-based encryption is to help the deployment of a public key infrastructure. In this section, we show several embodiments of this and other applications.

Revocation of Public Keys

In this embodiment, the sender may encrypt using a public key derived from a piece of information containing a time element, such as a year, date or other time, to help provide key expiration or other forms of temporal key management. For example, in one embodiment, key expiration can be done by having Alice encrypt e-mail sent to Bob using the public key: "`bob@company.com` $\|$ `current-year`". In doing so Bob can use his private key during the current year only. Once a year Bob needs to obtain a new private key from the PKG. Hence, we get the effect of annual private key expiration. Note that unlike the existing public key infrastructure, Alice does not need to obtain a new certificate from Bob every time Bob refreshes his private

key.

One may make this approach more granular in other embodiments by encrypting e-mail for Bob using "bob@company.com || current-date", or using another time stamp. This forces Bob to obtain a new private key every day. This embodiment may be used in a corporate context where the PKG is maintained by the corporation. With this approach key revocation is very simple: when Bob leaves the company and his key needs to be revoked, the corporate PKG is instructed to stop issuing private keys for Bob's e-mail address. As a result, Bob can no longer read his email. The interesting property is that Alice does not need to communicate with any third party certificate directory to obtain Bob's daily public key. Hence, embodiments of identity based encryption can provide a very efficient mechanism for implementing ephemeral public keys. Also note that this embodiment can be used to enable Alice to send messages into the future: Bob will only be able to decrypt the e-mail on the date specified by Alice.

Managing user credentials

An embodiment of the invention enables the management of user credentials using an IBE system. The message is encrypted with a string containing a credential identifier. For example, suppose Alice encrypts mail to Bob using the public key: "bob@company.com || current-year || clearance=secret". Then Bob will only be able to read the email if on the specified date he has secret clearance. Consequently, it is very easy to grant and revoke user credentials using the PKG.

FIG. 10 is a block diagram illustrating a system for managing credentials in an identity based encryption system according to an embodiment of the invention. The system includes sender system 1001, receiver system 1002 and PKG 1003. Each such system may be implemented as a computer system such as a client or server connected to a computer network. Accordingly, sender 1001, receiver 1002 and PKG 1003 may each contain processors, such as processor 1014, processor 1013 and processor 1012. Additionally, these systems may include computer-readable storage media, such as computer memory, and may additionally include interfaces to a computer network, including technology allowing for communication with a wired, wireless or other network. Sender system 1001 may include a software plug-in 1017. Such a plug-in may comprise a software module which performs cryptographic functions.

The plug-in includes, according to an embodiment of the invention, items such as cryptographic logic 1004. Plug-in 1017 may be distributed to various computers such as sender system 1001 and receiver system 1002 through a network in order to roll out functionality associated with identity-based encryption and other communication functionality. Parameters 1015 from a system such as PKG 1003 are also distributed over a computer network or other communications medium to senders and receivers, such as sender system 1001 and receiver system 1002, who may then use them in conjunction with plug-in 1017 when encrypting or decrypting messages. In one embodiment, plug-in 1017 is distributed together with parameters 1014. In an alternate embodiment, parameters 1015 may be distributed separately.

Sender system 1001 encrypts a message M using encryption logic 1004 in plug-in 1017. Encryption logic 1004 encrypts the message using encryption key 1011, which is based on selected credential 1005 and an identification 1016 of the intended receiver of the message. In some embodiments, the key may be based on other information as well. The sender system 1001 sends the receiver system 1002 information 1006, e.g., in the form of a data packet transmitted over a network or other communication medium. The information 1006 sent to receiver system 1002 contains the encrypted message and may also contain information 1007 regarding the credential 1005 used as part of the basis for the encryption key.

Either before or after receiving information 1006, receiver system 1002 sends a request 1009 to PKG 1003. In one embodiment, the request 1009 may include the receiver's identity 1016 and may also include information related to the selected credential 1005. In response, PKG 1003 verifies the credential of receiver 1002 using credential check logic 1008. Such logic may be implemented in software, hardware or a combination thereof. If the credential is verified as belonging to the receiver, then PKG 1003 provides a response 1010 to receiver 1002, which includes a private decryption key 1018 corresponding to the encryption key 1011. Using the private decryption key, the receiver then may decrypt the encrypted message contained in information 1006 to recover the original message M. Thus, by including a credential as part of an encryption key, embodiments such as this one allow a sender to encrypt a message intended for a receiver, where the decryption of the message by the receiver is contingent upon the validity of the receiver's credential.

Delegation of Decryption Keys

Another application for embodiments of IBE systems is delegation of decryption capabilities. We give two exemplary embodiments, described with reference to a user Bob who plays the role of the PKG. Bob runs the setup algorithm to generate his own IBE system parameters params and his own master-key. Here we view params as Bob's public key. Bob obtains a certificate from a CA for his public key params. When Alice wishes to send mail to Bob she first obtains Bob's public key params from Bob's public key certificate. Note that Bob is the only one who knows his master-key and hence there is no key-escrow with this setup.

1. **Delegation to a laptop.** Suppose Alice encrypts mail to Bob using the current date as the IBE encryption key (she uses Bob's params as the IBE system parameters). Since Bob has the master-key he can extract the private key corresponding to this IBE encryption key and then decrypt the message. Now, suppose Bob goes on a trip for seven days. Normally, Bob would put his private key on his laptop. If the laptop is stolen the private key is compromised. When using the IBE system Bob could simply install on his laptop the seven private keys corresponding to the seven days of the trip. If the laptop is stolen, only the private keys for those seven days are compromised. The master-key is unharmed.

FIG. 11 is a block diagram illustrating a system with key delegation according to an embodiment of the invention. The system includes user system 1101 and target system 1102. The target system may comprise a computer such as a laptop computer. User system 1101 includes a master key 1103, which is used to generate decryption keys 1104. The decryption keys 1104 are downloaded to the target system 1102. Using the techniques of key revocation described above, these decryption keys may be valid only for a limited time, thus providing additional security in the event that target system 1101 is compromised. User system 1101 and target system 1102 may include elements of computer systems such as memory 1106 and 1107 as well as processor 1105 and 1108. User system 1101 includes key generator logic 1109, which uses master key 1103 and system parameters 1110 to generate private decryption keys 1104 based on information derived from a user ID 1113 and one or more dates 1114 or other time stamps. Target system 1102 includes decryption logic 1111, which uses the private decryption keys 1104 obtained from user system 1101 and system parameters 1110 to decrypt an incoming encrypted message 1112.

If message 1112 is encrypted using public keys based on ID 1113 and one of the dates 1114, then private decryption keys may be used to decrypt it. Thus the decryption capabilities of target system 1102 may be limited to messages associated with selected dates 1114. In an alternate embodiment, the target system may be a data storage medium or portable data storage device which can be connected as desired to other computer systems, thereby enabling use of the decryption keys on those systems.

2. **Delegation of duties.** Suppose Alice encrypts mail to Bob using the subject line as the IBE encryption key. Bob can decrypt mail using his master-key. Now, suppose Bob has several assistants each responsible for a different task (e.g. one is 'purchasing', another is 'human-resources', etc.). In this embodiment, Bob may give one private key to each of his assistants corresponding to the assistant's responsibility. Each assistant can then decrypt messages whose subject line falls within its responsibilities, but it cannot decrypt messages intended for other assistants. Note that Alice only obtains a single public key from Bob (params), and she uses that public key to send mail with any subject line of her choice. The mail can only be read by the assistant responsible for that subject.

More generally, embodiments of IBE can simplify various systems that manage a large number of public keys. Rather than storing a big database of public keys the system can either derive these public keys from user names, or simply use the integers $1, \ldots, n$ as distinct public keys. For example, in a corporation, each employee might have a unique employee number, and that number may serve also as the employee's public key.

Return Receipt

FIG. 12 is a block diagram illustrating an encryption system with return receipt according to an embodiment of the invention. According to one embodiment of the invention, a sender can receive an confirmation that the recipient has received an encrypted message. More generally, upon receipt of a request for a decryption key from a receiver, the PKG takes an action separate from providing a decryption key to the receiver. Such an action comprises providing an acknowledgement to the sender that indicates that the message was received, according to one embodiment.

An embodiment of a system having return receipt capability is illustrated in FIG. 12. The system includes sender system 1201, recipient system 1202 and PKG system 1203. The sender system 1201, receiver system 1202 and PKG system 1203 may be implemented as computer systems coupled to a computer network. For example, PKG 1203, sender system 1201 and receiver system 1202 may include processor 1212, processor 1213 and processor and 1214, respectively. These computer systems may include elements such as computer readable storage media, computer memory and other storage devices. Additionally, these systems may include interfaces to a computer network, including technology allowing for communication from a wired, wireless or other network. Further, according an embodiment of the invention, communication between the respective elements may take place using data packets sent over a computer network, or using any of various other forms of electronic and data transmission and communication.

The sender 1201 encrypts a message M and sends the resulting ciphertext to receiver 1202 in a data package 1204 that also may include return receipt request information 1209. The return receipt request information may contain, for example, a return address and a message identifier corresponding to the particular message 1204. The message M is encrypted by the sender using encryption logic 1211 and an encryption key 1215. Encryption key 1215 may be based on a receiver ID (such as an e-mail address) 1216 and the return receipt request information 1209. Because the receiver ID and return receipt request information 1209 are used by the sender to determine the encryption key 1215, the receiver 1202 needs a corresponding decryption key that can be used to decrypt the message. Accordingly, recipient system 1202, in response to receiving message 1204, sends PKG 1203 a request 1206, which includes the return receipt request information 1209 and the receiver's ID, 1216. In response, PKG 1203 sends to receiver 1202 the private decryption key 1205, which receiver then uses with decryption logic 1217 to decrypt the ciphertext of message 1204 and recover the original message M. In addition to sending receiver 1202 the decryption key 1205, PKG 1203 also sends a return receipt 1207 to sender 1201. PKG 1203 may alternatively store the receipt on storage media as part of a log rather than send a return receipt. Return receipt 1207 may include information such as the message identifier. Thus, sender 1201 receives proof that recipient 1202 has received the message 1204. The system may be initialized by placing plug-in software in various systems, such as sender system 1201 and receiver system 1202. Such plug-in software may include

system parameters, some of which may be derived from a system master key. Such parameters, stored in local devices such as sender 1201 and receiver 1202 are then used to generate encryption keys, perform encryption, perform decryption, and other functions, as appropriate.

Description of the Weil pairing

In this section we describe the Weil pairing on elliptic curves and then show how to efficiently compute it using an algorithm. To be concrete we present an example using supersingular elliptic curves defined over a prime field $\mathbb{F}_p$ with $p > 3$ (the curve $y^2 = x^3 + 1$ over $\mathbb{F}_p$ with $p = 2 \bmod 3$ is an example of such a curve). The following discussion easily generalizes to computing the Weil pairing over other elliptic curves.

Elliptic curves and the Weil pairing

We state a few elementary facts about supersingular elliptic curves defined over a prime field $\mathbb{F}_p$ with $p > 3$:

Fact 1: A supersingular curve $E/\mathbb{F}_p$ (with $p > 3$) contains $p+1$ points in $\mathbb{F}_p$. We let O denote the point at infinity. The group of points over $\mathbb{F}_p$ forms a cyclic group of order $p+1$. For simplicity, let P be a generator of this group and set $n = p + 1$.

Fact 2: The group of points $E(\mathbb{F}_{p^2})$ contains a point Q of order n which is linearly independent of the points in $E(\mathbb{F}_p)$. Hence, $E(\mathbb{F}_{p^2})$ contains a subgroup which is isomorphic to the group $\mathbb{Z}_n^2$. The group is generated by $P \in E(\mathbb{F}_p)$ and $Q \in E(\mathbb{F}_{p^2})$. We denote this group by $E[p+1] = E[n]$.

We will be working with the Weil pairing e which maps pairs of points in $E[n]$ into $\mathbb{F}_{p^2}^*$, i.e. $e : E[n] \times E[n] \rightarrow \mathbb{F}_{p^2}^*$. To describe the pairing, we review the following concepts:

Divisors A divisor is a formal sum of points on the curve $E(\mathbb{F}_{p^2})$. We write divisors as $\mathcal{A} = \sum_P a_P(P)$ where $a_P \in \mathbb{Z}$ and $P \in E(\mathbb{F}_{p^2})$. For example, $\mathcal{A} = 3(P_1) - 2(P_2) - (P_3)$ is a divisor. We will only consider divisors $\mathcal{A} = \sum_P a_P(P)$ where $\sum_P a_P = 0$.

Functions Roughly speaking, a function f on the curve $E(\mathbb{F}_{p^2})$ can be viewed as a rational function $f(x, y) \in \mathbb{F}_{p^2}(x, y)$. For any point $P = (x, y) \in E(\mathbb{F}_{p^2})$ we

define $f(P) = f(x, y)$.

Divisors of functions Let f be a function on the curve $E(\mathbb{F}_{p^2})$. We define its divisor, denoted by (f), as $(f) = \sum_P \text{ord}_P(f) \cdot P$. Here $\text{ord}_P(f)$ is the order of the zero that f has at the point P. For example, let $ax + by + c = 0$ be the line passing through the points $P_1, P_2 \in E(\mathbb{F}_{p^2})$ with $P_1 \neq \pm P_2$. This line intersects the curve at third point $P_3 \in E(\mathbb{F}_{p^2})$. Then the function $f(x, y) = ax + by + c$ has three zeroes P_1, P_2, P_3 and a pole of order 3 at infinity. The divisor of f is $(f) = (P_1) + (P_2) + (P_3) - 3(O)$.

Principal divisors Let $\mathcal{A}$ be a divisor. If there exists a function f such that $(f) = \mathcal{A}$ then we say that $\mathcal{A}$ is a principal divisor. We know that a divisor $\mathcal{A} = \sum_P a_p(P)$ is principal if and only if $\sum_P a_p = 0$ and $\sum_P a_P P = O$. Note that the second summation is using the group action on the curve. Furthermore, given a principal divisor $\mathcal{A}$ there exists a *unique* function f (up to constant multiples) such that $(A) = (f)$.

Equivalence of divisors We say that two divisors $\mathcal{A}, \mathcal{B}$ are equivalent if their difference $\mathcal{A} - \mathcal{B}$ is a principal divisor. We know that any divisor $\mathcal{A} = \sum_P a_p(P)$ (with $\sum_P a_P = 0$) is equivalent to a divisor of the form $\mathcal{A}' = (Q) - (O)$ for some $Q \in E$. Observe that $Q = \sum_P a_P P$.

Notation Given a function f and a divisor $\mathcal{A} = \sum_P a_p(P)$ we define $f(\mathcal{A})$ as $f(\mathcal{A}) = \prod_P f(P)^{a_P}$. Note that since $\sum_P a_P = 0$ we have that $f(\mathcal{A})$ remains unchanged if instead of f we use cf for any $c \in \mathbb{F}_{p^2}$.

We are now ready to describe the Weil pairing of two points $P, Q \in E[n]$. Let $\mathcal{A}_P$ be some divisor equivalent to the divisor $(P) - (O)$. We know that $n\mathcal{A}_P$ is a principal divisor (it is equivalent to $n(P) - n(O)$ which is clearly a principal divisor). Hence, there exists a function f_P such that $(f_P) = n\mathcal{A}_P$. Define $\mathcal{A}_Q$ and f_Q analogously. The Weil pairing of P and Q is given by:

$$e(P, Q) = \frac{f_P(\mathcal{A}_Q)}{f_Q(\mathcal{A}_P)}$$

This ratio provides the value of the Weil pairing of P and Q whenever it is well defined (i.e., whenever no division by zero has occurred). If this ratio is undefined we use different divisors $\mathcal{A}_P, \mathcal{A}_Q$ to define $e(P, Q)$. When $P, Q \in E(\mathbb{F}_{p^2})$ we have that $e(P, Q) \in \mathbb{F}_{p^2}$.

We briefly show that the Weil pairing is well defined. That is, the value of $e(P,Q)$ is independent of the choice of the divisor $\mathcal{A}_P$ as long as $\mathcal{A}_P$ is equivalent to $(P)-(O)$ and $\mathcal{A}_P$ leads to a well defined value. The same holds for $\mathcal{A}_Q$. Let $\hat{\mathcal{A}}_P$ be a divisor equivalent to $\mathcal{A}_P$ and let $\hat{f}_P$ be a function so that $(\hat{f}_P) = n\hat{\mathcal{A}}_P$. Then $\hat{\mathcal{A}}_P = \mathcal{A}_P + (g)$ for some function g and $\hat{f}_P = f_P \cdot g^n$. We have that:

$$e(P,Q) = \frac{\hat{f}_P(\mathcal{A}_Q)}{f_Q(\hat{\mathcal{A}}_P)} = \frac{f_P(\mathcal{A}_Q)g(\mathcal{A}_Q)^n}{f_Q(\mathcal{A}_P)f_Q((g))} = \frac{f_P(\mathcal{A}_Q)}{f_Q(\mathcal{A}_P)}\frac{g(n\mathcal{A}_Q)}{f_Q((g))} = \frac{f_P(\mathcal{A}_Q)}{f_Q(\mathcal{A}_P)}\frac{g((f_Q))}{f_Q((g))} = \frac{f_P(\mathcal{A}_Q)}{f_Q(\mathcal{A}_P)}$$

The last equality follows from the following fact known as Weil reciprocity: for any two functions f, g we have that $f((g)) = g((f))$. Hence, the Weil pairing is well defined.

Fact 10 *The Weil pairing has the following properties:*

- *For all $P \in E[n]$ we have: $e(P,P) = 1$.*
- *Bilinear: $e(P_1+P_2,Q) = e(P_1,Q)\cdot e(P_2,Q)$ and $e(P,Q_1+Q_2) = e(P,Q_1)\cdot e(P,Q_2)$.*
- *When $P,Q \in E[n]$ are collinear then $e(P,Q) = 1$. Similarly, $e(P,Q) = e(Q,P)^{-1}$.*
- *n'th root: for all $P,Q \in E[n]$ we have $e(P,Q)^n = 1$.*
- *Non-degenerate: if P satisfies $e(P,Q) = 1$ for all $Q \in E[n]$ then $P = O$.*

As discussed earlier, our detailed example of an embodiment of an IBE scheme uses the modified Weil pairing $\hat{e}(P,Q) = e(P,\phi(Q))$, where ϕ is an automorphism on the group of points of E.

Tate pairing. The Tate pairing is another bilinear pairing that has the required properties for embodiments of our system. In various embodiments, we slightly modify the original definition of the Tate pairing to fit our purpose. Define the Tate pairing of two points $P,Q \in E[n]$ as $T(P,Q) = f_P(\mathcal{A}_Q)^{|\mathbb{F}_{p^2}^*|/n}$ where f_P and $\mathcal{A}_Q$ are defined as earlier. This definition gives a computable bilinear pairing $T : E[n] \times E[n] \to \mathbb{G}_2$.

Computing the Weil pairing

Given two points $P, Q \in E[n]$ we show how to compute $e(P,Q) \in \mathbb{F}_{p^2}^*$ using $O(\log p)$ arithmetic operations in $\mathbb{F}_p$. We assume $P \neq Q$. We proceed as follows: pick two random points $R_1, R_2 \in E[n]$. Consider the divisors $\mathcal{A}_P = (P + R_1) - (R_1)$ and $\mathcal{A}_Q = (Q + R_2) - (R_2)$. These divisors are equivalent to $(P) - (O)$ and $(Q) - (O)$ respectively. Hence, we can use $\mathcal{A}_P$ and $\mathcal{A}_Q$ to compute the Weil pairing as:

$$e(P,Q) = \frac{f_P(\mathcal{A}_Q)}{f_Q(\mathcal{A}_P)} = \frac{f_P(Q+R_2)f_Q(R_1)}{f_P(R_2)f_Q(P+R_1)}$$

This expression is well defined with very high probability over the choice of R_1, R_2 (the probability of failure is at most $O(\frac{\log p}{p})$). In the rare event that a division by zero occurs during the computation of $e(P,Q)$ we simply pick new random points R_1, R_2 and repeat the process.

To evaluate $e(P,Q)$ it suffices to show how to evaluate the function f_P at $\mathcal{A}_Q$. Evaluating $f_Q(\mathcal{A}_P)$ is done analogously. We evaluate $f_P(\mathcal{A}_Q)$ using repeated doubling. For a positive integer b define the divisor

$$\mathcal{A}_b = b(P + R_1) - b(R_1) - (bP) + (O)$$

It is a principal divisor and therefore there exists a function f_b such that $(f_b) = \mathcal{A}_b$. Observe that $(f_P) = (f_n)$ and hence, $f_P(\mathcal{A}_Q) = f_n(\mathcal{A}_Q)$. It suffices to show how to evaluate $f_n(\mathcal{A}_Q)$.

Lemma 11 *There is an algorithm $\mathcal{D}$ that given $f_b(\mathcal{A}_Q), f_c(\mathcal{A}_Q)$ and $bP, cP, (b+c)P$ for some $b, c > 0$ outputs $f_{b+c}(\mathcal{A}_Q)$. The algorithm only uses a (small) constant number of arithmetic operations in $\mathbb{F}_{p^2}$.*

Proof We first define two auxiliary linear functions g_1, g_2:

1. Let $a_1x + b_1y + c_1 = 0$ be the line passing through the points bP and cP (if $b = c$ then let $a_1x + b_1y + c_1 = 0$ be the line tangent to E at bP). Define $g_1(x,y) = a_1x + b_1y + c_1$.
2. Let $x + c_2 = 0$ be the vertical line passing through the point $(b+c)P$. Define $g_2(x,y) = x + c_2$

The divisors of these functions are:

$$\begin{aligned}(g_1) &= (bP) + (cP) + (-(b+c)P) - 3(O)\\ (g_2) &= ((b+c)P) + (-(b+c)P) - 2(O)\end{aligned}$$

By definition we have that:

$$\begin{aligned}\mathcal{A}_b &= b(P+R_1) - b(R_1) - (bP) + (O)\\ \mathcal{A}_c &= c(P+R_1) - c(R_1) - (cP) + (O)\\ \mathcal{A}_{b+c} &= (b+c)(P+R_1) - (b+c)(R_1) - ((b+c)P) + (O)\end{aligned}$$

It now follows that: $\mathcal{A}_{b+c} = \mathcal{A}_b + \mathcal{A}_c + (g_1) - (g_2)$. Hence:

$$f_{b+c}(\mathcal{A}_Q) = f_b(\mathcal{A}_Q) \cdot f_c(\mathcal{A}_Q) \cdot \frac{g_1(\mathcal{A}_Q)}{g_2(\mathcal{A}_Q)} \tag{1}$$

This shows that to evaluate $f_{b+c}(\mathcal{A}_Q)$ it suffices to evaluate $g_i(\mathcal{A}_Q)$ for all $i = 1, 2$ and plug the results into equation 1. Hence, given $f_b(\mathcal{A}_Q), f_c(\mathcal{A}_Q)$ and $bP, cP, (b+c)P$ one can compute $f_{b+c}(\mathcal{A}_Q)$ using a constant number of arithmetic operations. □

Denote the output of Algorithm $\mathcal{D}$ of Lemma 11 by $\mathcal{D}(f_b(\mathcal{A}_Q), f_c(\mathcal{A}_Q), bP, cP, (b+c)P) = f_{b+c}(\mathcal{A}_Q)$. Then one can compute $f_P(\mathcal{A}_Q) = f_n(\mathcal{A}_Q)$ using the following standard repeated doubling procedure. Let $n = b_m b_{m-1} \ldots b_1 b_0$ be the binary representation of n, i.e. $n = \sum_{i=0}^{m} b_i 2^i$.

Init: Set $Z = O$, $V = f_0(\mathcal{A}_Q) = 1$, and $k = 0$.

Iterate: For $i = m, m-1, \ldots, 1, 0$ do:

1: If $b_i = 1$ then do: Set $V = \mathcal{D}(V, f_1(\mathcal{A}_Q), Z, P, Z+P)$, set $Z = Z + P$, and set $k = k + 1$.

2: If $i > 0$ set $V = \mathcal{D}(V, V, Z, Z, 2Z)$, set $Z = 2Z$, and set $k = 2k$.

3: Observe that at the end of each iteration we have $z = kP$ and $V = f_k(\mathcal{A}_Q)$.

Output: After the last iteration we have $k = n$ and therefore $V = f_n(\mathcal{A}_Q)$ as required.

To evaluate the Weil pairing $e(P, Q)$ we run the above algorithm once to compute $f_P(\mathcal{A}_Q)$ and once to compute $f_Q(\mathcal{A}_P)$. Note that the repeated squaring algorithm

needs to evaluate $f_1(A_Q)$. This is easily done since the function $f_1(x,y)$ (whose divisor is $(f_1) = (P+R_1)-(R_1)-(P)+(O)$) can be written out explicitly as follows:

1. Let $a_1x + b_1y + c_1 = 0$ be the line passing through the points P and R_1. Define the function: $g_1(x,y) = a_1x + b_1y + c_1$.
2. Let $x + c_2 = 0$ be the vertical line passing through the point $P + R_1$. Define the function: $g_2(x,y) = x + c_2$.
3. The function $f_1(x,y)$ is simply $f_1(x,y) = g_2(x,y)/g_1(x,y)$ which is easy to evaluate in $\mathbb{F}_{p^2}$.

CLAIMS

The inventors claim:

1. In a cryptographic system, a method for sharing an identity-based secret message key between a sender and a receiver, the method comprising:

   (a) at a private key generator: obtaining an element Q of a first algebraic group, wherein Q represents an identity-based public encryption key of the receiver; computing sQ, where s is an integer representing a secret master key, and where sQ represents a private decryption key of the receiver; sending sQ to the receiver; obtaining an element P of a second algebraic group; computing sP; and sending sP to the sender;

   (b) at the sender: obtaining the element Q; obtaining the element P; obtaining an element sP from the private key generator; selecting a secret $r \in \mathbb{Z}$; computing rP; computing the secret message key from r, sP, Q, and a bilinear map; and sending rP to the receiver;

   (c) at the receiver: obtaining rP from the sender; obtaining sQ from the private key generator; and computing the secret message key from rP, sQ, and the bilinear map.

2. The method of claim 1 wherein sP and P are system parameters published by the private key generator.

3. The method of claim 1 wherein the bilinear map is an admissible map.

4. The method of claim 1 wherein the bilinear map is a symmetric map and the first algebraic group is equal to the second algebraic group.

5. The method of claim 1 wherein the bilinear map is an asymmetric map.

6. The method of claim 1 wherein obtaining the element Q at the receiver comprises obtaining a public identifier ID associated with the receiver and computing Q from the ID.

7. A method for generating a decryption key based on a public identifier ID, the method comprising:

(a) obtaining a master key and a set of system parameters associated with an identity-based encryption system;

(b) obtaining an element Q_{ID} of an algebraic group, wherein the element Q_{ID} is derived from the public identifier ID; and

(c) computing the decryption key d_{ID} from the master key and Q_{ID} using an action of the master key on Q_{ID}, wherein the decryption key d_{ID} is a member of the algebraic group.

8. The method of claim 7 wherein the algebraic group is a prime-order subgroup of an elliptic curve group.

9. The method of claim 7 wherein computing the decryption key comprises calculating $d_{ID} = sQ_{ID}$, where s represents the master key.

10. The method of claim 7 wherein obtaining the element Q_{ID} comprises: obtaining the public identifier ID; computing the element Q_{ID} from the public identifier ID.

11. The method of claim 7 wherein the public identifier ID is an identifier selected from the group consisting of the finite combinations of: a personal name, a name of an entity, a domain name, an IP address, an email address, a social security number, a passport number, a license number, a serial number, a zip code, an address, a telephone number, a URL, a date, a time, a subject, a case, a jurisdiction, a state, a country, a credential, a security clearance level, and a title.

12. A method for encrypting a message in an identity-based cryptosystem to produce corresponding ciphertext, the method comprising:

(a) obtaining a set of parameters associated with a cryptographic system, wherein the parameters comprise a bilinear map $\hat{e} : \mathbb{G}_0 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$, where $\mathbb{G}_0$, $\mathbb{G}_1$ and $\mathbb{G}_2$ are (not necessarily distinct) algebraic groups;

(b) selecting a public identifier ID comprising information identifying an intended receiver of the message;

(c) computing an element $Q_{ID} \in \mathbb{G}_0$ from the public identifier ID;

(d) computing a secret message key $g \in \mathbb{G}_2$ using $\hat{e}$ and Q_{ID}; and

(e) computing the ciphertext from the message using the message key g.

13. The method of claim 12 wherein computing the ciphertext comprises computing a bit mask from the message key g, and masking the message using the bit mask.

14. The method of claim 12 wherein computing the ciphertext comprises computing a bit mask from a hash of a random bit string σ, masking the message using the bit mask, and masking the random bit string σ using a hash of the secret message key.

15. The method of claim 12 wherein computing the ciphertext comprises computing an element $rP \in \mathbb{G}_1$, where $r \in \mathbb{Z}$ is a randomly selected secret, and where $P \in \mathbb{G}_1$.

16. The method of claim 12 wherein computing the message key also uses $r \in \mathbb{Z}$, where r is a randomly selected secret.

17. The method of claim 12 wherein computing the secret message key uses an element $sP \in \mathbb{G}_1$, where s is a secret master key.

18. The method of claim 12 wherein computing the message key $g \in \mathbb{G}_2$ uses multiple elements $s_i P \in \mathbb{G}_1$, where the s_i are shares of a secret master key.

19. The method of claim 12 wherein computing the element Q_{ID} comprises: using a character encoding scheme to map the public identifier ID to a binary string, and hashing the binary string to the element Q_{ID} of $\mathbb{G}_0$.

20. The method of claim 12 wherein $\mathbb{G}_0$ and $\mathbb{G}_1$ are derived from an elliptic curve defined over a field.

21. The method of claim 20 wherein $\hat{e}$ is derived from a Weil pairing on the elliptic curve.

22. The method of claim 20 wherein $\hat{e}$ is derived from a Tate pairing on the elliptic curve.

23. The method of claim 12 wherein the public identifier ID is an identifier selected from the group consisting of the finite combinations of: a personal name, a name of an entity, a domain name, an IP address, an email address, a social security number, a passport number, a license number, a serial number, a zip

code, an address, a telephone number, a URL, a date, a time, a subject, a case, a jurisdiction, a state, a country, a credential, a security clearance level, and a title.

24. A method for decrypting ciphertext in an identity-based cryptosystem to produce an original message, the method comprising:

(a) obtaining a set of parameters associated with a cryptographic system, wherein the parameters comprise a bilinear map $\hat{e} : \mathbb{G}_0 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$, where $\mathbb{G}_0$, $\mathbb{G}_1$ and $\mathbb{G}_2$ are (not necessarily distinct) algebraic groups;

(b) selecting a public identifier ID comprising information identifying an intended receiver of the message;

(c) obtaining a private key $d_{\text{ID}} \in \mathbb{G}_0$ corresponding to the public identifier ID;

(d) computing a secret message key $g \in \mathbb{G}_2$ using $\hat{e}$ and the private key d_{ID}; and

(e) computing the original message from the ciphertext using the message key g.

25. The method of claim 24 wherein computing the original message comprises computing a bit mask from the message key, and unmasking the ciphertext using the bit mask.

26. The method of claim 24 wherein computing the original message comprises unmasking a random bit string σ using a hash of the message key, and unmasking the message using a hash of the random bit string σ.

27. The method of claim 24 wherein the private key $d_{\text{ID}} \in \mathbb{G}_1$ is derived from Q_{ID} and a secret master key s.

28. The method of claim 24 wherein obtaining the private key $d_{\text{ID}} \in \mathbb{G}_1$ comprises providing authentication of identity to a private key generator and receiving the private key from the private key generator.

29. The method of claim 24 wherein obtaining the private key $d_{\text{ID}} \in \mathbb{G}_0$ corresponding to the public identifier ID comprises obtaining multiple private key portions $d_i \in \mathbb{G}_0$ from multiple corresponding private key generators.

30. The method of claim 24 wherein $\mathbb{G}_0$, $\mathbb{G}_1$ and $\mathbb{G}_2$ are cyclic groups having orders divisible by a prime number q.

31. The method of claim 24 wherein $\mathbb{G}_0$ and $\mathbb{G}_1$ are (not necessarily proper) subgroups of an elliptic curve defined over a field.

32. The method of claim 31 wherein $\hat{e}$ is derived from a Weil pairing on the elliptic curve.

33. The method of claim 31 wherein $\hat{e}$ is derived from a Tate pairing on the elliptic curve.

34. The method of claim 24 wherein the public identifier ID is an identifier selected from the group consisting of the finite combinations of: a personal name, a name of an entity, a domain name, an IP address, an email address, a social security number, a passport number, a license number, a serial number, a zip code, an address, a telephone number, a URL, a date, a time, a time interval, a subject, a case, a jurisdiction, a state, a country, a credential, a security clearance level, and a title.

35. A method for encrypting a message to produce ciphertext, the method comprising:

    (a) obtaining a set of parameters associated with a cryptographic system, wherein the parameters comprise a bilinear map $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$, where $\mathbb{G}_1$ and $\mathbb{G}_2$ are algebraic groups, and elements $P, sP \in \mathbb{G}_1$, where $s \in \mathbb{Z}$ is a secret master key;

    (b) obtaining a public key $xP \in \mathbb{G}_1$ corresponding to an intended receiver, where $x \in \mathbb{Z}$ is a secret of the intended receiver;

    (c) computing a message key $g \in \mathbb{G}_2$ using $\hat{e}$, sP, the public key xP, and a randomly selected $r \in \mathbb{Z}$; and

    (d) computing the ciphertext from the message using the message key g.

36. A method for decrypting a ciphertext to produce message, the method comprising:

    (a) obtaining a set of parameters associated with a cryptographic system, wherein the parameters comprise a bilinear map $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$, where

$\mathbb{G}_1$ and $\mathbb{G}_2$ are algebraic groups, and elements $P, sP \in \mathbb{G}_1$, where $s \in \mathbb{Z}$ is a secret master key;

(b) computing a message key $g \in \mathbb{G}_2$ using $\hat{e}$, sP, a private key x and an element $rP \in \mathbb{G}_1$ received from a sender, where $r \in \mathbb{Z}$ is a secret of the sender; and

(c) computing the message from the ciphertext using the message key g.

37. A method for decrypting a ciphertext to produce a message, the method comprising:

(a) obtaining a secret master key $s \in \mathbb{Z}$ and a set of parameters associated with a cryptographic system, wherein the parameters comprise an admissible map $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$, where $\mathbb{G}_1$ and $\mathbb{G}_2$ are algebraic groups;

(b) obtaining a public key $xP \in \mathbb{G}_1$ corresponding to an intended receiver of the message, where $x \in \mathbb{Z}$ is a secret of the intended receiver;

(c) computing a message key $g \in \mathbb{G}_2$ using $\hat{e}$, the public key xP, the secret master key s, and an element $rP \in \mathbb{G}_1$ received from a sender, where $r \in \mathbb{Z}$ is a secret of the sender; and

(d) computing the message from the ciphertext using the message key g.

38. A method for encrypting an e-mail message addressed to a receiver, the method comprising:

(a) obtaining a set of parameters associated with a cryptographic system, wherein the parameters comprise a bilinear map $\hat{e} : \mathbb{G}_0 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$, where $\mathbb{G}_0$, $\mathbb{G}_1$ and $\mathbb{G}_2$ are algebraic groups;

(b) selecting a public identifier ID comprising an e-mail address of the receiver;

(c) computing an element $Q_{\text{ID}} \in \mathbb{G}_0$ corresponding to the public identifier ID;

(d) computing a message key $g \in \mathbb{G}_2$ using $\hat{e}$, Q_{ID} and a randomly selected secret $r \in \mathbb{Z}$; and

(e) computing an encrypted message from the message using the message key g.

39. The method of claim 38 wherein the public identifier ID further comprises an identifier selected from the group consisting of: a personal name, a name of

an entity, a domain name, an IP address, a social security number, a passport number, a license number, a serial number, a zip code, an address, a telephone number, a URL, a date, a time, a subject, a case, a jurisdiction, a state, a country, a credential, a security clearance level, and a title.

40. A computer-readable storage medium having stored thereon ciphertext comprising: a first component representing an element computed from a randomly selected secret integer of a sender, and a second component representing a message encrypted by the sender using a secret message key, wherein the secret message key computed by the sender using a bilinear map, the secret integer, and an identity-based public key of an intended receiver.

41. A method of encrypting a first piece of information to be sent by a sender to a receiver, the method comprising: providing a second piece of information; generating an encryption key from the second piece of information; and using a bilinear map and the encryption key to encrypt at least a portion of the first piece of information to be sent from the sender to the receiver.

42. The method of claim 41 wherein the bilinear map is symmetric.

43. The method of claim 41 wherein the bilinear map is admissible.

44. The method of claim 41 wherein the bilinear map is based on a Weil pairing.

45. The method of claim 41 wherein the bilinear map is based on a Tate pairing.

46. The method of claim 41 wherein the second piece of information includes information associated with the receiver.

47. The method of claim 41 wherein the second piece of information comprises an e-mail address.

48. The method of claim 41 wherein the second piece of information includes information corresponding to a time.

49. The method of claim 41 wherein the second piece of information includes a message identifier.

50. The method of claim 41 wherein the second piece of information includes a credential identifier.

51. The method of claim 41 wherein the second piece of information includes a subject identifier for the message.

52. A method of decrypting ciphertext encrypted by a sender with an identity-based encryption key associated with a receiver, the method comprising: obtaining a decryption key derived from the encryption key; and using a bilinear map and the decryption key to decrypt at least a portion of the ciphertext.

53. The method of claim 52 wherein the bilinear map is symmetric.

54. The method of claim 52 wherein the bilinear map is admissible.

55. The method of claim 52 wherein the bilinear map is based on a Weil pairing.

56. The method of claim 52 wherein the bilinear map is based on a Tate pairing.

57. The method of 52 further comprising: obtaining the ciphertext prior to obtaining the decryption key.

58. The method of 52 wherein obtaining the decryption key comprises sending a request to a private key generator, wherein the request comprises information sent by a sender together with the ciphertext.

59. A method of generating a decryption key corresponding to an encryption key, wherein the encryption key is based on a first piece of information, the method comprising: providing an algebraic group having a group action; providing a master key; generating the encryption key based on the first piece of information; and generating the decryption key based on the group action applied to the master key and the encryption key.

60. The method of claim 59 wherein the algebraic group is defined by at least a portion of an elliptic curve.

61. The method of 59 wherein the first piece of information comprises information associated with an entity.

62. The method of 59 wherein the first piece of information comprises an e-mail address.

63. The method of 59 wherein the decryption key is generated in response to a request from a receiver of an encrypted message, and the first piece of information includes a message identifier.

64. The method of 59 wherein the decryption key is generated in response to a request from a receiver and the first piece of information includes an attribute associated with the receiver.

65. The method of 59 wherein the first piece of information includes information corresponding to a time.

66. The method of claim 59 wherein the first piece of information includes information corresponding to a time, wherein the decryption key is generated on a user system, and wherein the method further comprises storing the decryption key on a target system.

67. The method of claim 59 wherein the first piece of information includes information corresponding to a responsibility; and wherein the method further comprises providing respective decryption keys to an entity associated with the responsibility.

68. The method of claim 59 further comprising receiving a request for the decryption key from a receiver, and providing the key to the receiver if the receiver is authenticated.

69. The method of claim 59 wherein the master key is a share of a shared master key.

70. A method of providing system parameters for a cryptographic system comprising: providing a system parameter representing an algebraic group $\mathbb{G}_1$ and an algebraic group $\mathbb{G}_2$; and providing a system parameter representing a bilinear map $\hat{e}$ mapping pairs of elements of $\mathbb{G}_1$ to elements of $\mathbb{G}_2$.

71. The method of 70 wherein the bilinear map is symmetric.

72. The method of 70 wherein the bilinear map is based on a Weil pairing.

73. The method of 70 wherein the bilinear map is based on a Tate pairing.

74. The method of 70 wherein the algebraic group G_1 is derived from at least a portion of an elliptic curve.

75. The method of claim 70 wherein the algebraic group G_1 is derived from at least a portion of the elliptic curve $y^2 = x^3 + 1$.

76. A method for communicating between a sender and a receiver, the method comprising: encrypting a message to be sent from the sender to the receiver using an encryption key derived in part from a message identifier; sending the encrypted message from the sender to the receiver; receiving a request from the receiver for a decryption key, wherein the request includes the message identifier; after receiving the request for the decryption key, generating receipt information indicating that the receiver has received the message, and providing the decryption key to the receiver.

77. The method of claim 76 comprising: sending to the sender the generated receipt information.

78. The method of claim 76 wherein the encryption key is derived in part from an identifier associated with the sender.

79. The method of claim 76 wherein the encryption key is derived in part from an identifier associated with the receiver.

80. A method for communicating between a sender and a receiver, the method comprising: obtaining identifying information of the receiver; specifying a credential required for the receiver to gain a decryption key; deriving an encryption key from the identifying information of the receiver and the credential; encrypting a message using the encryption key and a bilinear map; sending the encrypted message from a sender to the receiver; receiving a request from the receiver of the message for a decryption key; determining whether the receiver has the credential; if the receiver has the credential, providing the decryption key to the receiver; decrypting the encrypted message using the decryption key and the bilinear map.

81. A system for encrypting a message in an identity-based cryptosystem to produce corresponding ciphertext, the system comprising:

(a) a resource that obtains a set of parameters associated with a cryptographic system, wherein the parameters comprise a bilinear map $\hat{e} : \mathbb{G}_0 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$, where $\mathbb{G}_0$, $\mathbb{G}_1$ and $\mathbb{G}_2$ are (not necessarily distinct) algebraic groups;

(b) a resource that selects a public identifier ID comprising information identifying an intended receiver of the message;

(c) a resource that computes an element $Q_{\text{ID}} \in \mathbb{G}_0$ from the public identifier ID;

(d) a resource that computes a secret message key $g \in \mathbb{G}_2$ using $\hat{e}$ and Q_{ID}; and

(e) a resource that computes the ciphertext from the message using the message key g.

82. An electronic message comprising ciphertext computed from a message and a message key g, wherein g is generated by:

(a) obtaining a set of parameters associated with a cryptographic system, wherein the parameters comprise a bilinear map $\hat{e} : \mathbb{G}_0 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$, where $\mathbb{G}_0$, $\mathbb{G}_1$ and $\mathbb{G}_2$ are (not necessarily distinct) algebraic groups;

(b) selecting a public identifier ID comprising information identifying an intended receiver of the message;

(c) computing an element $Q_{\text{ID}} \in \mathbb{G}_0$ from the public identifier ID; and

(d) computing the message key $g \in \mathbb{G}_2$ using $\hat{e}$ and Q_{ID}.

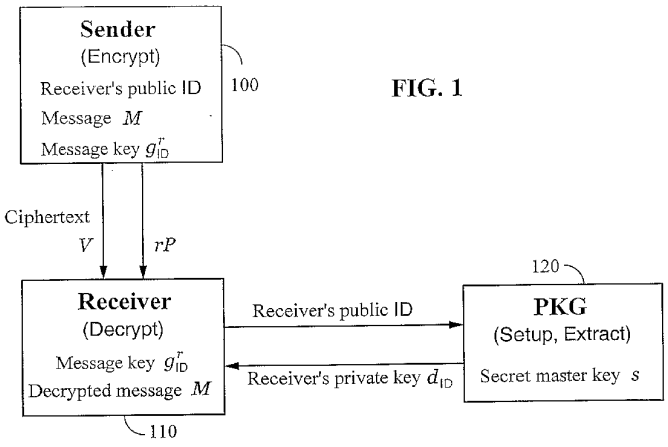

Sender
(Encrypt)
Receiver's public ID
Message M
Message key g_{ID}^{r}
100
Ciphertext
V
rP
120
Receiver
(Decrypt)
Message key g_{ID}^{r}
Decrypted message M
110
Receiver's public ID
Receiver's private key d_{ID}
PKG
(Setup, Extract)
Secret master key s

FIG. 1

FIG. 2

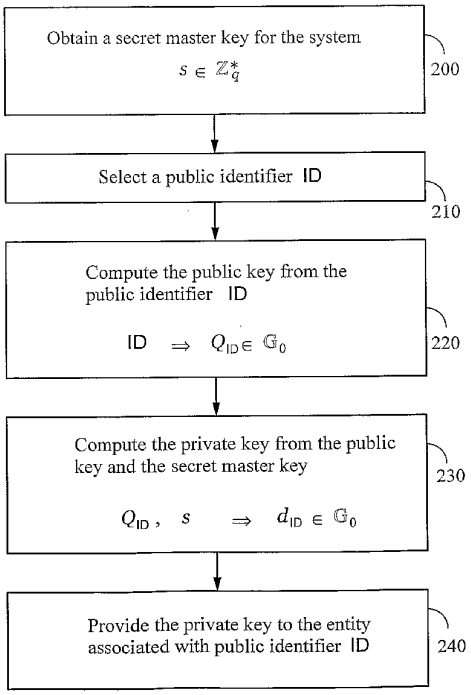

Obtain a secret master key for the system
$s \in \mathbb{Z}_q^*$
200
Select a public identifier ID
210
Compute the public key from the public identifier ID
ID $\Rightarrow$ $Q_{ID} \in \mathbb{G}_0$
220
Compute the private key from the public key and the secret master key
Q_{ID}, s $\Rightarrow$ $d_{ID} \in \mathbb{G}_0$
230
Provide the private key to the entity associated with public identifier ID
240

FIG. 3

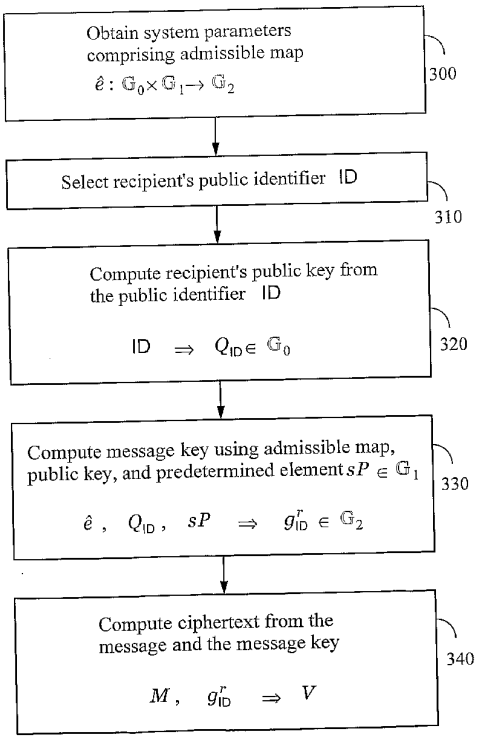
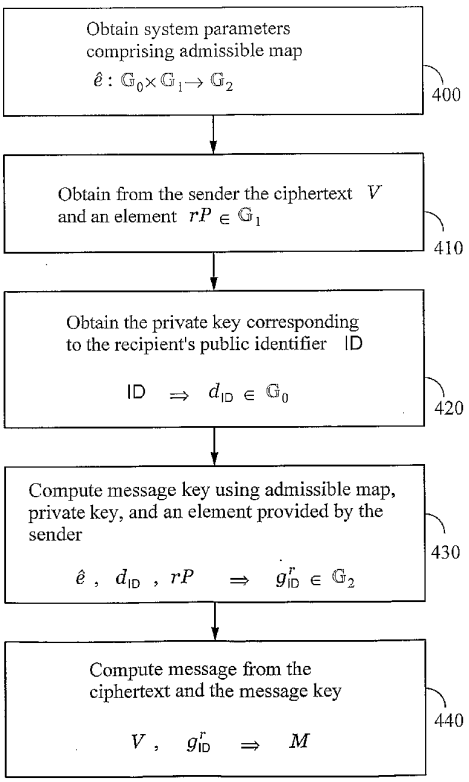

Obtain system parameters comprising admissible map
$\hat{e}: \mathbb{G}_0 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$
300
Select recipient's public identifier ID
310
Compute recipient's public key from the public identifier ID
ID $\Rightarrow$ $Q_{ID} \in \mathbb{G}_0$
320
Compute message key using admissible map, public key, and predetermined element $sP \in \mathbb{G}_1$
$\hat{e}$, Q_{ID} , sP $\Rightarrow$ $g_{ID}^r \in \mathbb{G}_2$
330
Compute ciphertext from the message and the message key
M , g_{ID}^r $\Rightarrow$ V
340

FIG. 4


Obtain system parameters comprising admissible map
$\hat{e} : \mathbb{G}_0 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$
400
Obtain from the sender the ciphertext V and an element $rP \in \mathbb{G}_1$
410
Obtain the private key corresponding to the recipient's public identifier ID
ID $\Rightarrow$ $d_{ID} \in \mathbb{G}_0$
420
Compute message key using admissible map, private key, and an element provided by the sender
$\hat{e}$, d_{ID} , rP $\Rightarrow$ $g_{ID}^r \in \mathbb{G}_2$
430
Compute message from the ciphertext and the message key
V , g_{ID}^r $\Rightarrow$ M
440

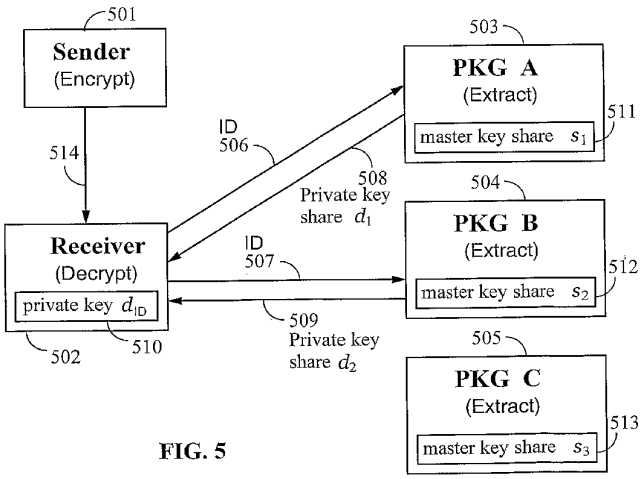

501
Sender
(Encrypt)
514
Receiver
(Decrypt)
private key d_{ID}
502
510
ID
506
508
Private key
share d_1
ID
507
509
Private key
share d_2
503
PKG A
(Extract)
master key share s_1
511
504
PKG B
(Extract)
master key share s_2
512
505
PKG C
(Extract)
master key share s_3
513

FIG. 5

FIG. 6

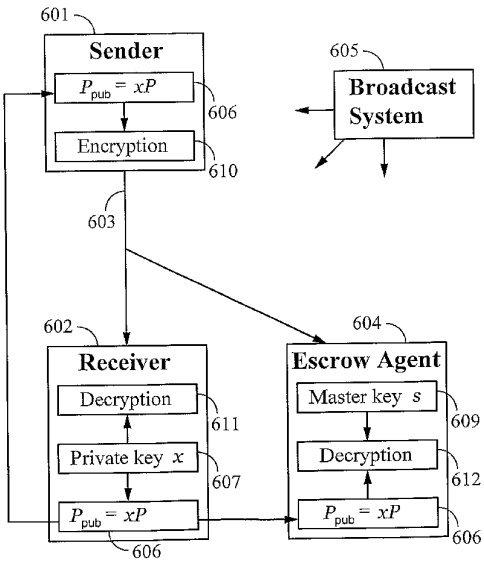

601
Sender
$P_{pub} = xP$
606
Encryption
610
603
605
Broadcast System
602
Receiver
Decryption
611
Private key x
607
$P_{pub} = xP$
606
604
Escrow Agent
Master key s
609
Decryption
612
$P_{pub} = xP$
606

FIG. 7

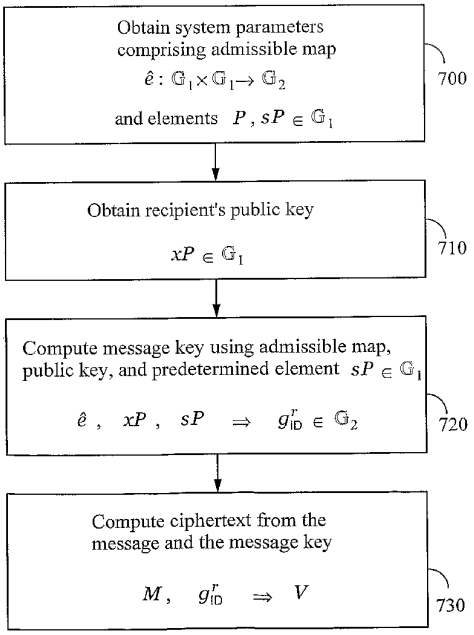

Obtain system parameters comprising admissible map
$\hat{e}: \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$
and elements $P, sP \in \mathbb{G}_1$
700
Obtain recipient's public key
$xP \in \mathbb{G}_1$
710
Compute message key using admissible map, public key, and predetermined element $sP \in \mathbb{G}_1$
$\hat{e}, xP, sP \Rightarrow g_{ID}^r \in \mathbb{G}_2$
720
Compute ciphertext from the message and the message key
$M, g_{ID}^r \Rightarrow V$
730

FIG. 8

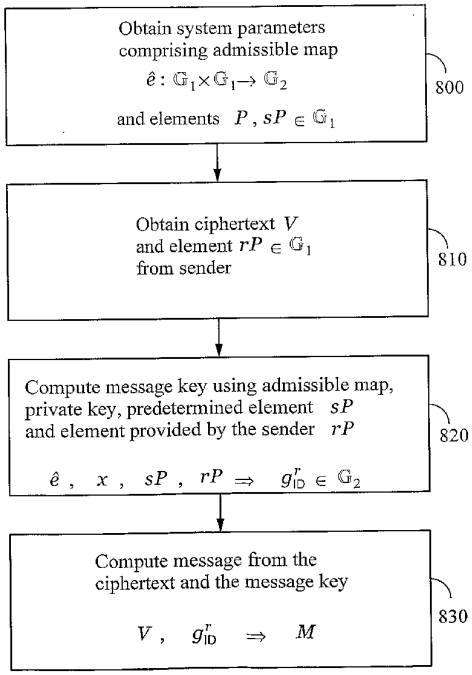

Obtain system parameters comprising admissible map
$\hat{e}: \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$
and elements $P, sP \in \mathbb{G}_1$
800
Obtain ciphertext V and element $rP \in \mathbb{G}_1$ from sender
810
Compute message key using admissible map, private key, predetermined element sP and element provided by the sender rP
$\hat{e}, x, sP, rP \Rightarrow g_{ID}^r \in \mathbb{G}_2$
820
Compute message from the ciphertext and the message key
$V, g_{ID}^r \Rightarrow M$
830

FIG. 9

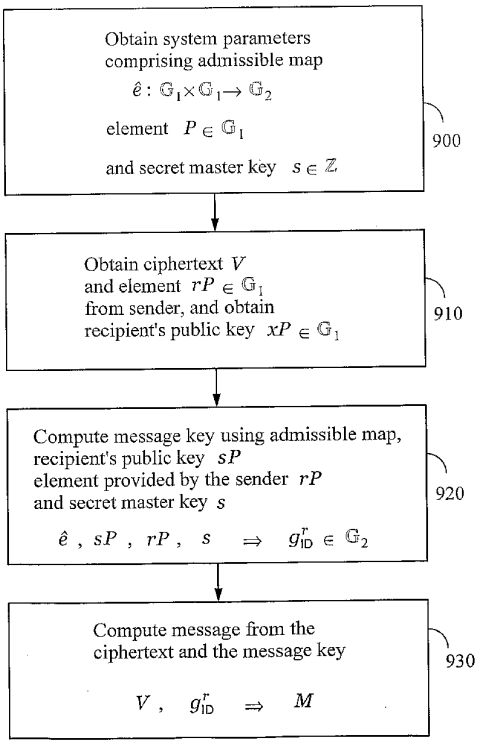

Obtain system parameters comprising admissible map
$\hat{e}: \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$
element $P \in \mathbb{G}_1$
and secret master key $s \in \mathbb{Z}$
900
Obtain ciphertext V and element $rP \in \mathbb{G}_1$ from sender, and obtain recipient's public key $xP \in \mathbb{G}_1$
910
Compute message key using admissible map, recipient's public key sP element provided by the sender rP and secret master key s
$\hat{e}$, sP , rP , s $\Rightarrow$ $g_{ID}^r \in \mathbb{G}_2$
920
Compute message from the ciphertext and the message key
V , g_{ID}^r $\Rightarrow$ M
930

FIG. 10

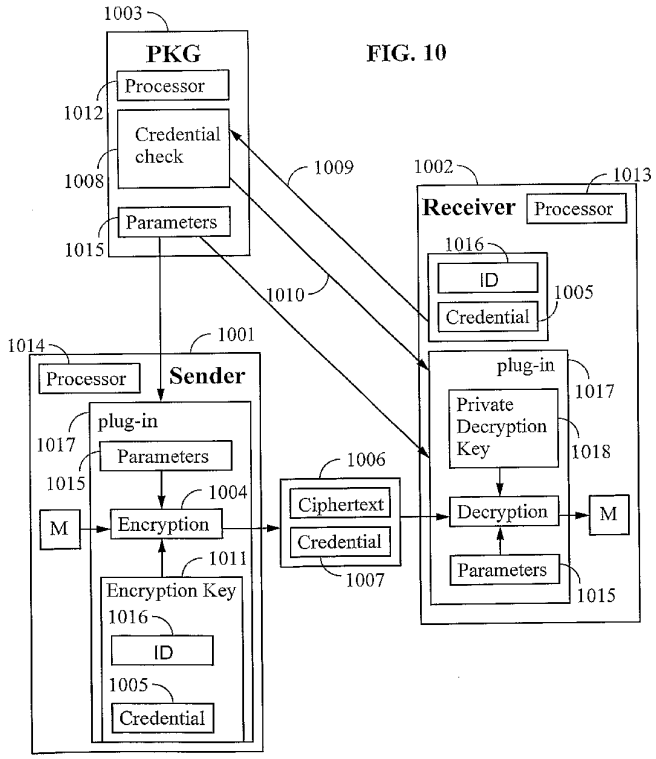
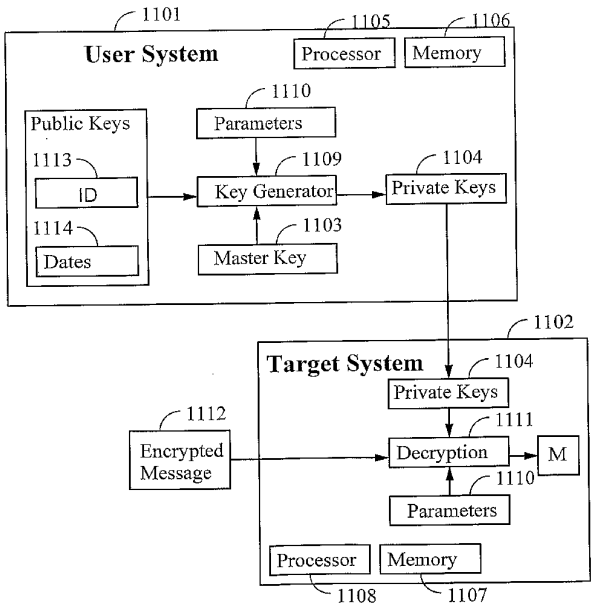

1003
PKG
Processor
1012
Credential check
1008
Parameters
1015
1009
1010
1002
Receiver
Processor
1013
1016
ID
Credential
1005
plug-in
1017
Private Decryption Key
1018
Decryption
M
Parameters
1015
1014
Processor
1001
Sender
plug-in
1017
Parameters
1015
M
Encryption
1004
1011
Encryption Key
1016
ID
1005
Credential
1006
Ciphertext
Credential
1007

FIG. 11


1101
User System
1105
Processor
1106
Memory
1110
Parameters
Public Keys
1113
ID
1114
Dates
1109
Key Generator
1104
Private Keys
1103
Master Key
1102
Target System
1104
Private Keys
1112
Encrypted Message
1111
Decryption
M
1110
Parameters
Processor
Memory
1108
1107

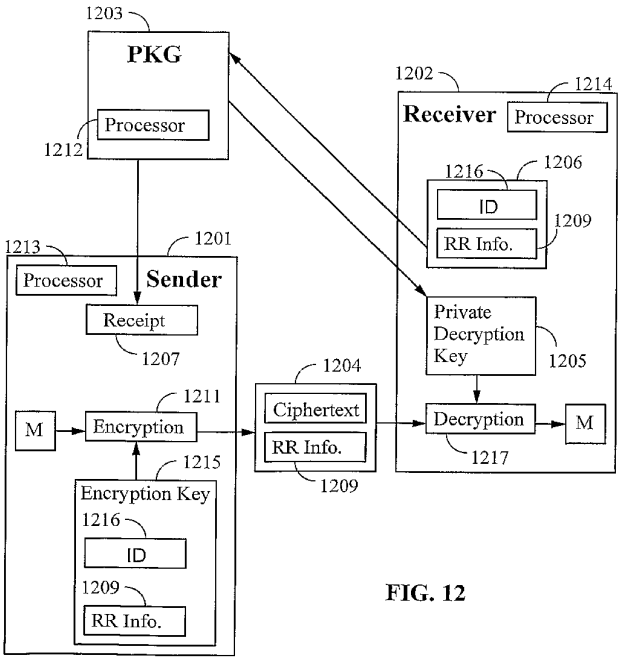

1203
PKG
Processor
1212
1202
1214
Receiver
Processor
1216
1206
ID
RR Info.
1209
1213
1201
Processor
Sender
Receipt
1207
Private
Decryption
Key
1205
1204
1211
M
Encryption
Ciphertext
RR Info.
1209
Decryption
M
1217
1215
Encryption Key
1216
ID
1209
RR Info.

FIG. 12

【国際公開パンフレット（コレクトバージョン）】

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
27 February 2003 (27.02.2003)

PCT

(10) International Publication Number
WO 03/017559 A3

(51) International Patent Classification[7]: H04L 9/00

(21) International Application Number: PCT/US02/27155

(22) International Filing Date: 13 August 2002 (13.08.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/311,946 13 August 2001 (13.08.2001) US

(71) Applicant: **BOARD OF TRUSTEES OF THE LELAND STANFORD JUNIOR UNIVERSITY** [US/US]; 900 Welch Road, Suite 350, Palo Alto, CA 94304 (US).

(72) Inventors: **BONEH, Dan**; Gates 475, Stanford, CA 94305-9045 (US). **FRANKLIN, Matthew**; 3021 Engineering II, Davis, CA 95616 (US).

(74) Agent: **ALBOSZTA, Marek**; 45 Cabot Ave., Suite 110, Santa Clara, CA 95051 (US).

(81) Designated States *(national)*: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

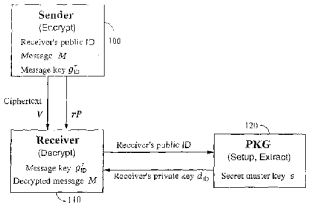
(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

(88) Date of publication of the international search report:
10 July 2003

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: SYSTEMS AND METHODS FOR IDENTITY-BASED ENCRYPTION AND RELATED CRYPTOGRAPHIC TECHNIQUES



(57) Abstract: A method and system for encrypting a first piece of information M to be sent by a sender (100) to a receiver (110) allows both sender and receiver to compute a secret message key using identity-based information and a bilinear map. In a one embodiment, the sender (100) computes an identity-based encryption key from an identifier ID associated with the receiver (110). The identifier ID may include various types of information such as the receiver's e-mail address, a receiver credential, a message identifier, or a date. The sender uses a bilinear map and the encryption key to compute a secret message key g^r_{ID}, which is then used to encrypt a message M, producing ciphertext V to be sent from the sender (100) to the receiver (110) together with an element rP. An identity-based decryption key d_{ID} is computed by a private key generator (120) based on the ID associated with the receiver and a secret master key s. After obtaining the private decryption key from the key generator (120), the receiver (110) uses it together with the element rP and the bilinear map to compute the secret message key g^r_{ID}, which is then used to decrypt V and recover the original message M. According to one embodiment, the bilinear map is based on a Weil pairing or a Tate pairing defined on a subgroup of an elliptic curve. Also described are several applications of the techniques, including key revocation, credential management, and return receipt notification.

WO 03/017559 A3

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US02/27155

A. CLASSIFICATION OF SUBJECT MATTER
IPC(7) : H04L 9/00
US CL : 713/171, 380,30
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 713/171

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
East

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5,150,411 A (MAURER et al) 22 September 1992 (22.09.92) Col. 3, line 30 - Col. 4, line 37 Col. 5, lines 52-65 Col. 6, lines 61-65 Col. 9, lines 19-24 Col. 2, lines 48-52	1, 2, 6-8, 10, 11, 40, 41, 46-52, 57-69, 76, 78-80
A	US 5,179,301 A (HUGHES et al) 12 January 1993 (12.01.93) Col. 7, line 6 - Col. 15, line 33	1-82
X	US 5,146,500 A (MAURER et al) 8 September 1992 (08.09.92) Col. 5, line 48 - Col. 10, line 43	1, 2, 6-8, 10, 11, 40, 41, 46-52, 57-69, 76, 78-80
A, P	US 6,307,935 B1 (CRANDALL et al) 23 October 2001 (23.10.01) Col. 1, line 20 - Col. 6, line 46	1-82

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
22 January 2003 (22.01.2003)	04 MAR 2003
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703)305-3230	Authorized officer Gilberto Barron Telephone No. 703-305-3900

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US02/27155

Box I Observations where certain claims were found unsearchable (Continuation of Item 1 of first sheet)

This international report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claim Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claim Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claim Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of Item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:
Please See Continuation Sheet

1. ☒ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest
☐ The additional search fees were accompanied by the applicant's protest.
☒ No protest accompanied the payment of additional search fees.

Form PCT/ISA/210 (continuation of first sheet(1)) (July 1998)

INTERNATIONAL SEARCH REPORT

PCT/US02/27155

BOX II. OBSERVATIONS WHERE UNITY OF INVENTION IS LACKING

Group I has the special technical feature of obtaining the public key of the receiver at the sender and creating the bilinear map which is not a technical feature of the other groups. Group II has the special technical feature of the parameters comprising a bilinear map e: G0 x G1 > G2 which is not a technical feature of the parameters comprising a bilinear map e: G1 x G1 > G2 which is not a technical feature of the other groups. Group IV has the special technical feature of generating an encryption key from an email address which is not a technical feature of the other groups. Group V has the special technical feature of generating an encryption key from information corresponding to time which is not a special technical feature of the other groups. Group VI has the special technical feature of system parameters representing a bilinear map e mapping pairs of elements of G1 to elements of G2 which is not a special technical feature of the other groups. Group VII has the special technical feature of sending the sender generated receipt information which is not a technical feature of the other groups. Group VIII has the special technical feature of generating an encryption key from the creditial information which is not a technical feature of the other groups. I. Claims 1-11, drawn to a for sharing an identity-based secret message key between a sender and a receiver

II. Claims 12-34, 38, 39, 81 and 82, drawn to a method of encrypting and decryting a message in an identity-based cryptosystem.

III. Claims 35-37, drawn to a method for encrypting and decrypting messages.

IV. Claims 40-51, drawn to a method for encrypting and decrypting information.

V. Claims 59-69, drawn to a method of generating a decryption key corresponding to an ecnryption key.

VI. Claims 70-75, drawn to a method of providing system parameters for a cryptographic system.

VII. Claims 76-79, drawn to a method for communicating between a sender and a receiver.

VIII. Claim 80, drawn to a method for communicating between a sender and a receiver.

フロントページの続き

(81)指定国 AP(GH,GM,KE,LS,MW,MZ,SD,SL,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,MD,RU,TJ,TM),EP(AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,IE,IT,LU,MC,NL,PT,SE,SK,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,ML,MR,NE,SN,TD,TG),AE,AL,AM,AT,AU,AZ,BA,BB,BG,BR,BY,CA,CH,CN,CU,CZ,DE,DK,EE,ES,FI,GB,GD,GE,GH,GM,HR,HU,ID,IL,IN,IS,JP,KE,KG,KP,KR,KZ,LC,LK,LR,LS,LT,LU,LV,MD,MG,MK,MN,MW,MX,NO,NZ,PL,PT,RO,RU,SD,SE,SG,SI,SK,SL,TJ,TM,TR,TT,TZ,UA,UG,UZ,VN,YU,ZA,ZW

(72)発明者 フランクリン、マシュー
アメリカ合衆国 ９５６１６ カリフォルニア州 デイビス エンジニアリング ザ セカンド ３０２１

Ｆターム(参考) 5J104 AA01 AA16 EA04 EA15 EA26 EA33 JA21 JA29 NA02 NA12 NA37

【要約の続き】
用して、暗号文Ｖを解読し、オリジナルのメッセージＭを復元する。一実施形態によれば、双線形写像は、楕円曲線の部分群上で定義されたＷｅｉｌペアリングまたはＴａｔｅペアリングに基づく。また、鍵の取り消し、信任状管理、および受信確認返信通知を含む、これらの手法の応用もいくつか説明されている。