

(19)日本国特許庁(JP)

(12)公表特許公報(A)

(11)公表番号
特表2024-514711
(P2024-514711A)

(43)公表日 令和6年4月2日(2024.4.2)

(51)国際特許分類

G 0 9 C 1/00 (2006.01)

F I

G 0 9 C 1/00 6 2 0 Z

審査請求 未請求 予備審査請求 未請求 (全63頁)

(21)出願番号	特願2023-565325(P2023-565325)	(71)出願人	523112138
(86)(22)出願日	令和4年4月25日(2022.4.25)		エヌティーティー リサーチ インコーポ レイテッド
(85)翻訳文提出日	令和5年12月19日(2023.12.19)		アメリカ合衆国 カリフォルニア州 9 4
(86)国際出願番号	PCT/US2022/026173		0 8 5 サニーバール スチュワート ド ライブ 9 4 0
(87)国際公開番号	WO2022/232042	(74)代理人	100107766
(87)国際公開日	令和4年11月3日(2022.11.3)		弁理士 伊東 忠重
(31)優先権主張番号	63/179,862	(74)代理人	100070150
(32)優先日	令和3年4月26日(2021.4.26)		弁理士 伊東 忠彦
(33)優先権主張国・地域又は機関	米国(US)	(74)代理人	100135079
(81)指定国・地域	AP(BW,GH,GM,KE,LR,LS,MW,MZ,NA ,RW,SD,SL,ST,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,RU,TJ,TM),EP(AL,A T,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR ,GB,GR,HR,HU,IE,IS,IT,LT,LU,LV,MC, 最終頁に続く	(72)発明者	ダッタ プラティッシュ アメリカ合衆国 カリフォルニア州 9 4 0 8 5 サニーバール スチュワート ド 最終頁に続く

(54)【発明の名称】 完全適応型セキュリティを有する分散型マルチオーソリティの属性ベース暗号化

(57)【要約】

本発明は、分散型マルチオーソリティの属性ベース暗号化(MA-ABE)スキームにおいてメッセージを暗号化及び復号するためのシステム、方法、ネットワークデバイス及び機械可読媒体に関する。MA-ABEスキームは、証明可能に完全に適応的に安全であり、具体的には、オーソリティの一部を破損し、システムの寿命を通じて適応的に鍵クエリを実行し得る攻撃者に対して安全である。

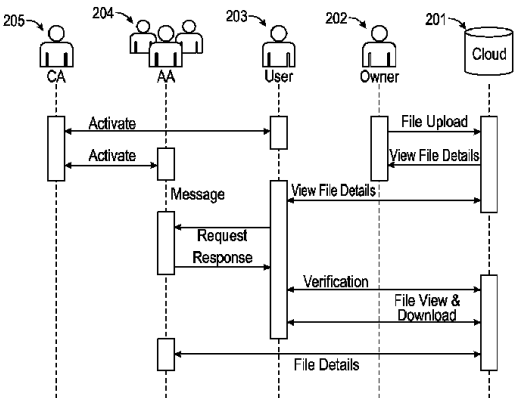


FIG. 2

【特許請求の範囲】

【請求項 1】

マルチオーソリティの属性ベース暗号化スキームに従ってメッセージを暗号化するためのコンピュータ化システムであって、

暗号化のために m_i ビットを含む電子メッセージ m を受信するステップと、

前記電子メッセージをコンピュータ化記憶媒体に記憶するステップと、

グローバル設定アルゴリズムを実行して、

グループ G を生成し、

G の2つの生成子として g 及び h をサンプリングし、

シード抽出器のための $seed$ をサンプリングする

ことによってグローバルパラメータを生成するステップと、

オーソリティ設定アルゴリズムを実行して、

2つの指数 y_A 及び y_B をサンプリングし、

公開鍵を $\{g^{y_A}, g^{y_B}\}$ として設定し、

秘密鍵を $\{y_A$ 及び $y_B\}$ として設定する

ことによって、公開及び秘密鍵ペアを生成するステップと、

s 、 r_A 、 r_B をサンプリングし、

$C_{\{1,A\}} = g^{r_A}$

$C_{\{1,B\}} = g^{r_B}$

$C_{\{2,A\}} = g^{y_A * r_A} g^s$

$C_{\{2,B\}} = g^{y_B * r_B} g^{-s}$

$C = m \text{ xor Ext}(e(g,h), seed)$

を計算し、

暗号化メッセージとして $(C, C_{\{1,A\}}, C_{\{1,B\}}, C_{\{2,A\}}, C_{\{2,B\}})$ をコンピュータ化記憶媒体に記憶する

ことによって、前記メッセージ m 及びアクセスポリシー M に対して暗号化アルゴリズムを実行するステップと、

$(H(GID) * h)^{y_A}$ 及び $(H(GID))^{y_B}$ を出力することによって、鍵生成アルゴリズムを実行するステップであり、 H はグループに写像するグローバル暗号ハッシュ関数である、ステップと

を行うように構成されたプロセッサを含むコンピュータ化システム。

【請求項 2】

任意の関係者が任意の時点でオーソリティとして参加でき、オーソリティの数に制限が存在しない、請求項 1 に記載のメッセージを暗号化するためのコンピュータ化システム。

【請求項 3】

当該方法は、完全に適応的に安全である、請求項 1 に記載のメッセージを暗号化するためのコンピュータ化システム。

【請求項 4】

当該方法は、オーソリティの一部を破損し、前記システムの寿命全体を通じて適応的に鍵クエリを実行し得る攻撃者に対して安全であるように、証明可能に完全に適応的に安全である、請求項 1 に記載のメッセージを暗号化するためのコンピュータ化システム。

【請求項 5】

敵対者は、アクセス構造に関して暗号化されたメッセージを復号するのに十分な秘密鍵又はオーソリティマスター鍵を保持しない、請求項 4 に記載のメッセージを暗号化するためのコンピュータ化システム。

【請求項 6】

前記コンピュータ化プロセッサは、

属性ベースの暗号化スキームに従って暗号化された前記メッセージをコンピュータ化記憶媒体に記憶するステップと、

$(K_{\{GID,A\}}, K_{\{GID,B\}})$ として生成された成分を含む鍵及び暗号文 $(C, C_{\{1,A\}}, C_{\{1,B\}}$

10

20

30

40

50

}、 $C_{\{2,A\}}$ 、 $C_{\{2,B\}}$ を受信し、

$D_A = e(C_{\{2,A\}}, H(GID) * h) / e(C_{\{1,A\}}, K_{\{GID,A\}})$ を計算し、

$D_B = e(C_{\{2,B\}}, H(GID)) / e(C_{\{1,B\}}, K_{\{GID,B\}})$ を計算し、

$C \text{ xor Ext}(D_A * D_B, \text{seed})$ を出力する

ことによって、復号アルゴリズムを実行するステップと

を行うことで、前記メッセージを復号するように更に構成される、請求項1に記載のメッセージを暗号化するためのコンピュータ化システム。

【請求項7】

マルチオーソリティの属性ベース暗号化スキームに従ってメッセージを暗号化するためのコンピュータ化方法であって、

暗号化のために m_i ビットを含む電子メッセージ m をコンピュータ化記憶媒体に記憶するステップと、

グローバル設定アルゴリズムを実行して、

グループ G を生成し、

G の2つの生成子として g 及び h をサンプリングし、

シード抽出器のための seed をサンプリングする

ことによってグローバルパラメータを生成するステップと、

オーソリティ設定アルゴリズムを実行して、

2つの指数 y_A 及び y_B をサンプリングし、

公開鍵を $\{g^{\{y_A\}}, g^{\{y_B\}}\}$ として設定し、

秘密鍵を $\{y_A$ 及び $y_B\}$ として設定する

ことによって、公開及び秘密鍵ペアを生成するステップと、

s 、 r_A 、 r_B をサンプリングし、

$C_{\{1,A\}} = g^{\{r_A\}}$

$C_{\{1,B\}} = g^{\{r_B\}}$

$C_{\{2,A\}} = g^{\{y_A * r_A\}} g^{\{s\}}$

$C_{\{2,B\}} = g^{\{y_B * r_A\}} g^{\{-s\}}$

$C = m \text{ xor Ext}(e(g, h), \text{seed})$

を計算し、

暗号化メッセージとして $(C, C_{\{1,A\}}, C_{\{1,B\}}, C_{\{2,A\}}, C_{\{2,B\}})$ をコンピュータ化記憶媒体に記憶する

ことによって、前記メッセージ m 及びアクセスポリシー M に対して暗号化アルゴリズムを実行するステップと、

$(H(GID) * h)^{\{y_A\}}$ 及び $(H(GID))^{\{y_B\}}$ を出力することによって、鍵生成アルゴリズムを実行するステップであり、 H はグループに写像するグローバル暗号ハッシュ関数である、ステップと

を含む方法。

【請求項8】

任意の関係者が任意の時点でオーソリティとして参加でき、オーソリティの数に制限が存在しない、請求項7に記載のメッセージを暗号化するためのコンピュータ化方法。

【請求項9】

当該方法は、完全に適応的に安全である、請求項7に記載のメッセージを暗号化するためのコンピュータ化方法。

【請求項10】

当該方法は、オーソリティの一部を破損し、システムの寿命全体を通じて適応的に鍵クエリを実行し得る攻撃者に対して安全であるように、証明可能に完全に適応的に安全である、請求項7に記載のメッセージを暗号化するためのコンピュータ化方法。

【請求項11】

敵対者は、アクセス構造に関して暗号化されたメッセージを復号するのに十分な秘密鍵又はオーソリティマスター鍵を保持しない、請求項10に記載のメッセージを暗号化する

10

20

30

40

50

ためのコンピュータ化方法。

【請求項 12】

当該方法は、前記マルチオーソリティの属性ベース暗号化スキームに従ってメッセージを復号するステップを更に含み、

当該方法は、

属性ベースの暗号化スキームに従って暗号化されたメッセージをコンピュータ化記憶媒体に記憶するステップと、

$(K_{\{GID,A\}}, K_{\{GID,B\}})$ として生成された成分を含む鍵及び暗号文 $(C, C_{\{1,A\}}, C_{\{1,B\}}, C_{\{2,A\}}, C_{\{2,B\}})$ を受信し、

$D_A = e(C_{\{2,A\}}, H(GID) * h) / e(C_{\{1,A\}}, K_{\{GID,A\}})$ を計算し、

$D_B = e(C_{\{2,B\}}, H(GID)) / e(C_{\{1,B\}}, K_{\{GID,B\}})$ を計算し、

$C \text{ xor } \text{Ext}(D_A * D_B, \text{seed})$ を出力する

ことによって、復号アルゴリズムを実行するステップと

を含む、請求項 7 に記載のメッセージを暗号化するためのコンピュータ化方法。

【発明の詳細な説明】

【技術分野】

【0001】

〔関連出願の相互参照〕

本出願は、2021年4月26日に出願された米国仮特許出願第63/179,862号の優先権を主張し、その全内容を参照により援用する。

【0002】

〔技術分野〕

本開示は、証明可能で完全に適応的に安全であり、具体的には、オーソリティ(authority)のうちいくつかを破損する可能性がある攻撃者に対して安全であり、且つ、システムの寿命全体を通じて適応的に鍵クエリを実行する、マルチオーソリティ(multi-authority)の属性ベース暗号化スキームに関する。

【背景技術】

【0003】

属性ベース暗号化(ABE, attribute-based encryption)スキームは、暗号化されたデータにアクセスするときに、きめの細かいアクセス制御を可能にする。このような暗号化スキームは、特定の証明書(又は属性)を有するユーザが、如何なる追加情報も漏洩することなく、特定のメッセージを復号することを可能にする、復号鍵をサポートする。長年にわたって、ABEスキームを設計するという課題は、非常に大きな注目を受けており、その結果、表現力、効率、セキュリティ及び基礎となる仮定の間の様々なトレードオフを達成する長い一連の研究がもたらされている。

【0004】

属性ベース暗号化は、受信者の証明書(又は属性)に基づいて暗号化データに対してきめの細かいアクセス制御を提供する従来の公開鍵暗号化の一般化である。ABEには、暗号文ポリシー及び鍵ポリシーの2つのアバターがある。暗号文ポリシーABE(CP-ABE, ciphertext-policy ABE)では、その名前が示唆するように、暗号文はアクセスポリシーに関連付けられ、鍵は属性に関連付けられる。鍵ポリシーABE(KP-ABE, key-policy ABE)では、アクセスポリシー及び属性セットの役割は反転し、すなわち、暗号文は、属性に関連付けられ、鍵はアクセスポリシーに関連付けられる。双方の場合、属性がアクセスポリシーを満たす場合にのみ復号が可能である。さらに、アクセスポリシーに関して作成されたいずれかの暗号文が与えられた場合、アクセスポリシーを満たす属性セットに対応する秘密鍵を個々に所有していない共謀ユーザのグループが、暗号化メッセージを復号できないことが必要である。この特性は、共謀耐性(collusion resistance)として知られている。

【0005】

Goyal、Pandey、Sahai及びWatersによるその発端以来、ABEは、潜在的なアプリ

ケーションの長いリストによる基本的な暗号プリミティブになっている。したがって、ABEスキームを設計するタスクは、暗号コミュニティによって非常に注目されており、その結果、表現力、効率、セキュリティ、及び基礎となる仮定の間のようなトレードオフを達成する長い作業シーケンスをもたらしている。

【0006】

マルチオーソリティABE

標準的なABEスキームには、以下のような1つの大きな制限がある。ABEスキームでは、各ユーザは、単一のマスタオーソリティに行き、これらの属性のそれぞれに対応する秘密鍵を受信するために、ユーザが特定のセットの属性を有することを証明しなければならない。これは、全ての属性、例えば、運転免許証、有権者登録及び大学入学を監視する1つの信頼できるオーソリティを有さなければならないことを意味する。しかし、実際には、異なる属性を発行して維持することを担う異なるエンティティが存在し、例えば、DMVは、運転免許証の管理者であり、同様に、他の2つの属性については、それぞれ、選挙管理委員会及び大学事務室である。したがって、属性のそれぞれを異なる(おそらく完全には信頼されていない)オーソリティに委ねることができることが望まれる。

【0007】

マルチオーソリティの属性ベース暗号化:ABEスキームでは、制限された復号鍵は、マスタ秘密鍵を所有する中央オーソリティによってのみ生成及び発行できる。Chaseは、マルチオーソリティABE(MA-ABE, multi-authority AB)の概念を導入しており、MA-ABEは、複数の関係者がオーソリティの役割を果たすことを可能にする。より正確にはMA-ABEでは、異なる属性を制御する複数のオーソリティが存在し、これらのそれぞれは、システム内の他のオーソリティとの如何なる相互作用もなしに、これらの制御下で属性を所有するユーザに秘密鍵を発行できる。何らかのアクセスポリシーに関して生成された暗号文が与えられると、アクセスポリシーを満たす属性のセットを所有するユーザは、これらの属性を制御する様々なオーソリティから取得した個々の秘密鍵を引き出すことによって暗号文を復号できる。

【0008】

上記の問題に対処するために、マルチオーソリティABE(MA-ABE, multi-authority ABE)スキームの概念が導入されている。MA-ABEでは、異なる属性を制御する複数のオーソリティが存在し、これらのそれぞれは、システム内の他のオーソリティとの如何なる相互作用もなしに、これらの制御下で属性を所有するユーザに秘密鍵を発行できる。何らかのアクセスポリシーに関して生成された暗号文が与えられると、アクセスポリシーを満たす属性のセットを所有するユーザは、これらの属性を制御する様々なオーソリティから取得した個々の秘密鍵を引き出すことによって暗号文を復号できる。上記のように、セキュリティは、オーソリティのないユーザに対する共謀防止を必要とするが、重要な違いは、属性オーソリティのいくつかが破損し、したがって、敵対ユーザと共謀する可能性があることである。

【0009】

様々な制限を有する少しの初期の試みの後に、Lewko及びWatersは、最初の真に分散型のMA-ABEスキームを設計できており、このスキームでは、任意の関係者がオーソリティになることができ、初期の信頼できる設定の作成以外には、如何なるグローバルな調整も必要としない。彼らのスキームでは、関係者は、単に、自分自身の公開鍵を発行し、異なるユーザに対してユーザの属性を反映する秘密鍵を発行することによって、オーソリティとして機能することができる。異なるオーソリティは、互いに認識する必要さえなく、任意の時点でシステムに参加できる。また、システムの寿命の間に関与できる属性オーソリティの数に制限は存在しない。これらのスキームは、 NC^1 回路によって計算可能な全てのアクセスポリシーをサポートする。さらに、強力なデュアルシステム技術を利用して、「サブグループ判定(subgroup decision)」型の仮定を用いて、ランダムオラクルモデル(random oracle model)において、合成数位数双線形群(composite order bilinear group)を仮定して、セキュリティが証明される。

【0010】

Lewko及びWatersに続いて、いくつかの拡張及び改善が存在する。Okamoto及びTakashimaは、判定線形(DLIN, decision-linear)仮定に依存する素数位数双線形群(prime order bilinear groups)に対する構成を提供している。Rouselakis及びWaters及びAmbroza及びGayは効率性の改善を提供しているが、標準よりも低い q -タイプ仮定及びジェネリックグループモデルをそれぞれ使用している。Dattaらは、アクセスポリシーの非自明なクラスをサポートする最初のLWE(Learning With Errors)ベースの構築を提供している。上記の全ては、ランダムオラクルモデルである。

【0011】

セキュリティ:自然なMA-ABEセキュリティの定義は、オーソリティのないユーザに対する通常の共謀耐性を必要とするが、ここでの重要な違いは、属性オーソリティのいくつかが破損する可能性があり、したがって、敵対するユーザと共謀する可能性があることである。いくつかの構成は適応的な鍵クエリをサポートするが、如何なる仮定の下でも、オーソリティの完全適応的な破損をサポートする既知の構成は存在しない。MA-ABEの分散型の性質を仮定すると、攻撃者が、セキュリティゲームの開始時に、たとえいずれかの秘密鍵を見る前であっても、破損したオーソリティのセットにコミットすると仮定することは、満足のいくものではないように思われる。実際には、現実的に全ての属性オーソリティがシステムに同時に参加することを期待することさえしない。したがって、以前の研究が考慮してきた「静的破損(static corruption)」モデルは、現実的な攻撃シナリオを捕捉せず、オーソリティの適応的な破損をサポートすることによってそれを改善することが望まれる。

【0012】

完全適応型セキュリティを得ることは、既存の構成におけるギャップである。これは、(準順指数的(sub-exponential)なセキュリティロスと認める場合であっても)一般的な複雑性レバレッジ/推測スタイルの引数(generic complexity leveraging/guessing style arguments)が失敗する稀なケースの1つである。実際に、これらの引数を発明者らの設定に適用すると、暗号文当たりのオーソリティの最大数に比例した指数的ロスが生じる。したがって、暗号文制限当たり所定の最大数のオーソリティが存在する必要があり、その場合、セキュリティパラメータは適切に選択される必要がある。さらに、任意の関係者が任意の時点でオーソリティとして参加でき、オーソリティの数に制限が存在しない、真に分散型のスキームを有することが望まれる。分散型マルチオーソリティの属性ベース暗号化(MA-ABE)は、信頼できる中央オーソリティが存在しない、標準的(暗号文ポリシー)属性ベース暗号化の分散型の一般化されたものであり、任意の関係者がオーソリティになって秘密鍵を発行でき、共通参照パラメータの初期セットの作成以外の如何なるグローバル調整も必要とされない。

【0013】

標準的な複雑さを活用するスタイルの引数は、マルチオーソリティ設定では機能しない。したがって、使用される仮定にかかわらず、オーソリティの適応的な破損に耐えることができる構成が必要である。

【発明の概要】

【0014】

本発明のいくつかの実施形態は、マルチオーソリティの属性ベース暗号化スキームに従ってメッセージを暗号化するためのシステム、方法、ネットワークデバイス及び機械可読媒体を提供する。当該システムは、

暗号化のために m_i ビットを含む電子メッセージ m を受信するステップと、

電子メッセージをコンピュータ化記憶媒体に記憶するステップと、

グローバル設定アルゴリズムを実行して、

グループ G を生成し、

G の2つの生成子として g 及び h をサンプリングし、

シード抽出器のためのseedをサンプリングする

ことによってグローバルパラメータを生成するステップと、
オーソリティ設定アルゴリズムを実行して、

2つの指数 y_A 及び y_B をサンプリングし、
公開鍵を $\{g^{y_A}, g^{y_B}\}$ として設定し、
秘密鍵を $\{y_A$ 及び $y_B\}$ として設定する

ことによって、公開及び秘密鍵ペアを生成するステップと、

s, r_A, r_B をサンプリングし、

$C_{\{1,A\}} = g^{r_A}$

$C_{\{1,B\}} = g^{r_B}$

$C_{\{2,A\}} = g^{y_A * r_A} g^s$

$C_{\{2,B\}} = g^{y_B * r_B} g^{-s}$

$C = m \text{ xor } \text{Ext}(e(g,h), \text{seed})$

を計算し、

暗号化メッセージとして $(C, C_{\{1,A\}}, C_{\{1,B\}}, C_{\{2,A\}}, C_{\{2,B\}})$ をコンピュータ化記憶媒体に記憶する

ことによって、メッセージ m 及びアクセスポリシー M に対して暗号化アルゴリズムを実行するステップと、

$(H(\text{GID}) * h)^{y_A}$ 及び $(H(\text{GID}))^{y_B}$ を出力することによって、鍵生成アルゴリズムを実行するステップであり、 H はグループに写像するグローバル暗号ハッシュ関数である、
ステップと

を行うように構成されたプロセッサを含む。

いくつかの更なる実施形態では、任意の関係者が任意の時点でオーソリティとして参加でき、オーソリティの数に制限が存在しない。いくつかの更なる実施形態では、当該方法は、完全に適応的に安全である。いくつかの更なる実施形態では、当該方法は、オーソリティの一部を破損し、システムの寿命全体を通じて適応的に鍵クエリを実行し得る攻撃者に対して安全であるように、証明可能に完全に適応的に安全である。いくつかの更なる実施形態では、敵対者は、アクセス構造に関して暗号化されたメッセージを復号するのに十分な秘密鍵又はオーソリティマスター鍵を保持しない。

いくつかの実施形態では、コンピュータ化プロセッサは、

属性ベースの暗号化スキームに従って暗号化されたメッセージをコンピュータ化記憶媒体に記憶するステップと、

$(K_{\{\text{GID},A\}}, K_{\{\text{GID},B\}})$ として生成された成分を含む鍵及び暗号文 $(C, C_{\{1,A\}}, C_{\{1,B\}}, C_{\{2,A\}}, C_{\{2,B\}})$ を受信し、

$D_A = e(C_{\{2,A\}}, H(\text{GID}) * h) / e(C_{\{1,A\}}, K_{\{\text{GID},A\}})$ を計算し、

$D_B = e(C_{\{2,B\}}, H(\text{GID})) / e(C_{\{1,B\}}, K_{\{\text{GID},B\}})$ を計算し、

$C \text{ xor } \text{Ext}(D_A * D_B, \text{seed})$ を出力する

ことによって、復号アルゴリズムを実行するステップと

を行うことで、メッセージを復号するように更に構成される。

【図面の簡単な説明】

【0015】

更なる理解を提供するために含まれており、本明細書に組み込まれており、その一部を構成する添付図面は、本開示の実施形態を例示し、詳細な説明とともに、本開示の実施形態の原理を説明する役目をする。

【図1】分散型マルチオーソリティの属性ベース暗号化スキームのためのシステムアーキテクチャの例を示す。

【図2】分散型マルチオーソリティの属性ベース暗号化スキームのシーケンス図の例を示す。

【図3】本発明のシステム及び方法を実装するためのコンピュータシステムアーキテクチャの例を示す。

【図4】本発明のシステム及び方法を実装するためのコンピュータシステムアーキテクチャ

10

20

30

40

50

ヤの例の更なる詳細を示す。

【発明を実施するための形態】

【0016】

発明者らは、完全適応的な鍵クエリに加えて、オーソリティの完全適応的な破損が許容される場合であっても証明可能に安全である、最初の真に分散型のMA-ABEスキームを構築する。本発明のスキームは、標準的な多項式の硬度(困難さ)の仮定を用いた双線形群に基づき、ランダムオラクルモデルにおけるものである。本発明の構成は、如何なる仮定の下でも、オーソリティの完全適応的な破損に対する最初の証明可能な安全なスキームであることを強調する。

【0017】

まず、(今までのところ)標準的なサブグループ判定の仮定を用いて、合成数位数の双線形群に基づく構成を提供し、次に、k-線形(k-Lin)又はより一般的には行列ディフィ・ヘルマン(MDDH, matrix Diffie-Hellman)が当てはまる素数位数双線形群における構成を提供する。

【0018】

定理(非公式):「標準的な(standard)」サブグループ判定の仮定が当てはまる合成数位数双線形群を仮定する。その場合、ランダムオラクルモデルにおいて完全適応型MA-ABEスキームが存在する。

【0019】

上記の定理において本発明が使用する仮定は、過去に複数回使用されており、これらは、一般的な双線形群モデルにおいて当てはまることが示されている。しかし、合成数位数ベースの構成は、より標準的な素数位数の設定と比較していくつかの欠点を有することを指摘しておく。第1に、素数位数群では、k-LIN又は双線形ディフィ・ヘルマン(BDH, bilinear Diffie-Hellman)仮定のようなより標準的な仮定の下でセキュリティを得ることができる。第2に、素数位数群では、同じセキュリティレベルについてはるかに効率的なシステムを達成することができる。これは、合成数位数群では、セキュリティは群の位数を因数分解することの困難さに典型的に依存するからである。次に、これは、大きい群の位数の使用を必要とし、その結果、グループ及びペアリング動作がかなり遅くなる。

【0020】

このために、Freeman及びLewkoから始まって、既存の合成数位数群の構成を素数位数の同様のものに変換するための複数のフレームワーク及びツールが開発されている。発明者らは、Chen、Gong、Kowalczyk及びWeeによる最近のツールのセットを使用し、セキュリティがより標準的なk-Lin又はMDDH仮定に基づく素数位数の(非対称)双線形群における構成を得ることに成功している。本発明の構成は、kの任意の選択に基づいて安全である。例えば、k=1を設定して、対称外部ディフィー・ヘルマン仮定(SXDH, Symmetric External Diffie-Hellman Assumption)の下でセキュリティを得ており、k=2の設定は、DLIN仮定の下でのセキュリティに対応する。

【0021】

定理(非公式):k-Lin又はMDDH仮定が当てはまる素数位数双線形群を仮定する。その場合、ランダムオラクルモデルにおける完全適応型MA-ABEスキームが存在する。

【0022】

技術的概要

本発明のMA-ABEは、(他の既知のMA-ABEスキームと同様に)システム内の各ユーザがグローバル識別子

【数1】

$$GID \subset \{0,1\}^*$$

10

20

30

40

50

の何らかの母集団から生じた一意のグローバル識別子を有するという仮定の下で設計されている。さらに、(一般性を失うことなく)各オーソリティは1つの属性のみを制御すると仮定する。したがって、「オーソリティ(authority)」及び「属性(attribute)」という用語を交換可能に使用できる。(この制限は、オーソリティ当たり先験的に制限された数の属性をサポートするように緩和できる点に留意する。)オーソリティ母集団(authority universe)を

【数 2】

$$\mathcal{AU}$$

10

で表す。

【0023】

ここで、NC¹アクセスポリシーについての分散型 MA-ABE のシンタックスを思い起こすと、これは(単調性)線形秘密分散法(LSSS, linear secret sharing scheme)によって実現可能であることがよく知られている。分散型 MA-ABE スキームは、GlobalSetup、AuthSetup、KeyGen、Enc及びDecの5つの手順からなる。GlobalSetup手順は、(単項符号化において)セキュリティパラメータを入力として取得し、グローバル公開パラメータを出力する。他の手順の全ては、これらのグローバルパラメータに依存する(文脈から明らかである場合には、これらを明示的に言及しない場合がある)。AuthSetup手順は、対応する公開鍵及びマスター秘密鍵のペア(PK_u, MSK_u)を生成するために、任意のオーソリティ

20

【数 3】

$$u \in \mathcal{AU}$$

によって実行できる。次いで、マスター秘密鍵 MSK_u を保持するオーソリティは、グローバル識別子 GID を有するユーザについて秘密鍵 $SK_{GID,u}$ を生成できる。任意の時点で、何らかのオーソリティの公開鍵 $\{PK_u\}$ を使用して、何らかの線形秘密分散ポリシー

30

【数 4】

$$(M, \rho)$$

に対してメッセージ msg を暗号化できる。ここで、

【数 5】

$$M$$

40

はポリシー行列であり、 ρ は、暗号文 CT を得るために、行列内の行インデックスをこれらのオーソリティによって制御される属性に割り当てる関数である。最後に、(同じ GID に対する)秘密鍵のセット $\{SK_{GID,u}\}$ を保持するユーザは、所有する秘密に対応する属性が、暗号文が生成されたアクセス構造を「満たす」場合にのみ、所与の暗号文 CT を復号できる。この文献の場合のように MA-ABE スキームがランダムオラクルモデルにおいて構築され、全ての以前の共謀体制 MA-ABE スキームにおいて構築される場合、

【数 6】

50

GID

におけるグローバル識別子を何らかの適切な空間に写像する公開ハッシュ関数 H の存在が考えられる。このハッシュ関数 H は、GlobalSetupによって生成され、セキュリティ証明においてランダムオラクルとしてモデル化される。

【0024】

完全適応型セキュリティ

標準的なABEと同様に、MA-ABEスキームのセキュリティは共謀耐性を要求し、すなわち、暗号文を復号することを個々に認可されていない共謀ユーザのグループは、彼らが彼らの秘密鍵の成分と一緒に引き出すとき、暗号文を復号できるべきではない。しかし、MA-ABEの場合、属性オースリティのいくつかが敵対するユーザと共謀し、それによって、これらのユーザが破損したオースリティによって制御される属性に対応する秘密鍵を自由に取得できる場合であっても、共謀耐性が保持されることが更に求められる。分散型MA-ABEは、破損したオースリティの公開鍵及び秘密鍵が悪意のある方法で生成されても、依然として共謀耐性を必要とすることを可能にする。これは、分散型MA-ABEスキームでは、システム内の他の全ての人からローカルに独立して公開鍵及び秘密鍵を生成することにより、誰もが属性オースリティとして機能することを許容されるため、重要である。発明者らは、以下のゲームによって大まかに定義される完全適応型セキュリティを目指している。

【0025】

グローバル設定: 挑戦者がグローバル公開パラメータを生成するためにGlobalSetupを実行する。

【0026】

クエリ段階1: 攻撃者は、以下の形式の多項式の数のクエリを適応的に行うことを許容される。

(a) オースリティ設定クエリ: 挑戦者が敵対者によって指定されたオースリティについての公開/マスター鍵ペアを作成するためにAuthSetupを実行する。

(b) 秘密鍵クエリ: 挑戦者が所与の属性についての秘密鍵を作成するためにKeyGenを実行する。

(c) オースリティマスター鍵クエリ: 挑戦者は、敵対者の選択の何らかのオースリティに対応するマスター秘密鍵を攻撃者に提供する。

【0027】

チャレンジ段階: 敵対者は、アクセス構造に含まれるオースリティの公開鍵のセットと共に、2つのメッセージ msg_0 、 msg_1 及びアクセス構造を提出する。これは、挑戦者から、アクセス構造に関するメッセージのうち1つ(ランダムに選択される)の暗号化を得る。敵対者が、アクセス構造に関して暗号化されたメッセージを復号するのに十分な秘密鍵/オースリティマスター鍵を保持しないことが重要である。

【0028】

クエリ段階2: クエリ段階1と同じである(チャレンジ段階からの制約が違反されていないことを確認しつつ行われる)。

【0029】

推測: 攻撃者は、どのメッセージがチャレンジ暗号文の基礎となるかについての推測を提出する。

【0030】

全ての以前のMA-ABEスキームは、敵対者が、グローバル設定段階中に、システム内のオースリティのセット及び破損したオースリティのサブセットに対してコミットしなければならない、はるかに弱い定義を考慮する。その時点で既に、全ての破損していないオースリティの秘密/公開鍵ペアが挑戦者によって作成されており、公開鍵が攻撃者に与え

られている。(すなわち、クエリ段階I及びIIの間に、形式2のクエリ(秘密鍵クエリ)のみが許可される。)本発明の完全適応型の定義は、MA-ABEの分散型の性質を考慮して、はるかに現実的である。

【0031】

以前の研究及び本発明のアプローチ

【0032】

いずれかのABEスキームのように、MA-ABEにおける課題は、共謀体制とすることである。通常では、ABEスキームは、ユーザに特有の新しいランダム性の助けを借りて、ユーザの異なる属性を表す異なる鍵成分と一緒に「結び付ける」ために、マスター秘密鍵を認識するシステムのオーソリティを使用することによって、共謀耐性を達成する。このようなランダム化は、ユーザの異なる鍵成分を互いに互換性のあるものにするが、別のユーザに発行された鍵の部分とは互換性のないものにする。

10

【0033】

しかし、マルチオーソリティ設定では、自律的な鍵生成及び共謀耐性の同時の目標を満たすことを望む。自律的な鍵生成の要件は、全ての部分と一緒にコンパイルする関係者が存在しないので、鍵ランダム化のための標準的な技術が適用できないことを意味する。さらに、分散型MA-ABEシステムにおいて、各コンポーネントは、異なるオーソリティからもたらされてよく、このようなオーソリティは、協調を有さず、場合によっては、互いに認識することさえしない。これを克服するために、従来の分散型MA-ABEスキームは、異なるオーソリティによって特定のユーザに発行された複数の鍵成分を結び付けるランダム性として、ユーザのグローバルアイデンティティGIDに適用される公開ハッシュ関数の出力を使用する。

20

【0034】

この課題を理解するために、Lewko及びWatersによる1つの特定の構成に焦点を当てる。これは、真の分散型MA-ABEスキームの最初のものであるが、全ての関連する後続の研究は、それに大きく依存し、したがって、同様の問題を被る。Lewko及びWatersの構成のセキュリティ証明は、Watersによって最初に開発されたデュアルシステム技術を使用する。デュアルシステムでは、暗号文及び鍵は、通常又は半機能的の2つの形式をとることができる。半機能的な暗号文及び鍵は、実際のシステムでは使用されず、これらはセキュリティ証明でのみ使用される。通常の鍵は、通常の暗号文又は半機能的な暗号文を復号でき、通常の暗号文は、通常の鍵又は半機能的な鍵によって復号できる。しかし、半機能的な暗号文を復号するために半機能的な鍵が使用されるとき、復号は失敗する。デュアルシステムのセキュリティは、一連の「区別できない(indistinguishable)」ゲームを使用して証明される。第1のゲームは、(通常の暗号文及び鍵を有する)実際のセキュリティゲームである。次のゲームでは、暗号文は半機能的であるが、全ての鍵は通常である。q個の秘密鍵の要求を行う攻撃者に対してq個のゲームを定義する。第kのゲームにおいて、最初のk個の鍵は半機能的であるが、残りの鍵は通常である。ゲームqにおいて、攻撃者に与えられる全ての鍵及びチャレンジ暗号文は半機能的である。したがって、与えられた鍵のいずれも、チャレンジ暗号文を復号するのに有用ではない。

30

【0035】

Lewko及びWatersの証明は、このハイレベルのアプローチに従うが、本質的に、破損したオーソリティが事前に指定されているという事実依存する。証明の終わりに向かって、全ての鍵は半機能的になり、チャレンジ暗号文も半機能的になる。最後のハイブリッドの目的は、半機能的なチャレンジ暗号文が(元のメッセージではなく)ランダムメッセージであるゲームに移行することである。これを区別できないようにするために、これらは、破損したオーソリティに対応するアクセスポリシーの行列内の行を「遮断する(shut off)」必要がある。これは、チャレンジ暗号文における行に直交するベクトルを選択する情報理論ツールを使用することによって行われる(破損したセットは許可されていないはずなので、このようなベクトルが存在するはずである)。事実上、これは、これらの行に対応するオーソリティマスター鍵の存在を完全に無視することを可能にし、一方、他の

40

50

行については、全ての鍵が半機能的であるゲームに移行したときに、秘密鍵の不在が既に対処されている。

【0036】

このアプローチは、オーソリティが適応的に破損され得る場合には、明らかに失敗する。第1に、チャレンジ暗号文が作成された後にオーソリティが破損される可能性があり、挑戦者が対応するマスター鍵を敵対者に与えることができるはずであるため、後者はチャレンジ暗号文が作成される時点では認識されていないことさえあるので、技術的には、破損したオーソリティに対応する行を「遮断する」ことは不可能である。しかし、Lewko及びWatersの(証明)アプローチでは、挑戦者は(その時点では)オーソリティにとって適切に形成されたマスター鍵さえも有していないので、これは不可能である。

10

【0037】

障壁の克服及び(合成数位数)スキーム

【0038】

この問題を解決するために、破損したオーソリティをどのようにしてデュアルシステム暗号化証明に統合するかを解明しなければならない。これは、Lewko及びWatersと同様に、本発明のオーソリティ鍵が、単に合成数位数の群 $N=p_1p_2p_3$ にわたる指数からなるので、困難である。これらのオーソリティ鍵は指数であり、群要素ではないので、典型的に証明が群ベースの秘密鍵を変更するように、これらを半機能的になるように移行させる明らかな方法は存在しない。

【0039】

本発明の証明では、このような鍵を利用するための新たな方法を考案する。証明の第1のステップは、 p_3 サブグループに対して暗号文を半機能的にすることである。この議論は以下の2つの重要な事実依存する。(1)攻撃者が侵害するオーソリティのいずれかのサブセットは、アクセス構造を満たさない。したがって、破損したオーソリティだけでは、チャレンジ暗号文が半機能的であるか否かを(情報理論的に)決定するのに十分ではない。(2)破損していないオーソリティによって与えられた鍵は、位数 p_3 サブグループの成分を有さないので、(このステップにおいて)このような攻撃者を助けることはない。まとめると、これは、オーソリティの適応的な破損を処理するために情報理論的ステップを活用する方法を提供する。本発明のアプローチは、異なるハイブリッドの実験の間を進むために、計算論的及び情報理論的引数の双方を使用する。重要な特徴は、アクセス構造を満たさない攻撃者の鍵に依存するいずれかのステップが情報理論的引数であり、したがって、どのオーソリティが破損しているかを推測することを中心に展開するいずれかの問題を回避することである。(当然、情報理論的引数の間及び情報理論的引数の設定に複数の計算上の引数が存在する)。敵対者が情報理論的引数においてのみ何を破損するかに関する情報を使用する同様のハイレベルのアプローチが、以前のいくつかのデュアルシステム証明において使用されているが、ここでは、(より困難な)分散型設定及び破損したオーソリティを取り囲むことにおいて、本技術を実装することが可能である。

20

30

【0040】

本発明のアプローチは、暗号システムの所与の部分空間において半機能的な鍵及び暗号文の双方を確立することを可能にする。しかし、これは大きい注意を伴う。半機能的な引数が p_3 サブグループで確立されるが、単に p_1 サブグループに存続するメッセージをブラインドする暗号文成分から分離した状態に保持しておかなければならない。したがって、この段階では、発明者らが行った全ての研究がメッセージを全く隠すことさえあることは、不明確である。したがって、本発明の証明の次の部分は、暗号文の半機能的な部分を、メッセージをブラインドする部分に「ブリードする(bleed)」必要がある。これを行うために、2つのサブシステム構成を確立する必要がある。ここで、本発明の構成は本質的にLewko及びWatersのマルチオーソリティABEスキームの2つのコピーのように見える。ここで、本発明では、最初に一方にブリードし、次いで他方にブリードすることを交代で行う。

40

【0041】

50

この新規な技術を、デュアルサブシステムを有するデュアルシステムと呼ぶ。この技術は、一方のサブシステム内の半機能性を利用して、他方のサブシステム内に半機能性を導入する。より具体的には、発明者らは、元々 p_1 サブグループ内に存続する公開パラメータ内に特別なグループ要素を導入する。本発明の目標は、最終的にこのグループ要素を p_1 及び p_2 サブグループの双方に存続させ、その p_1 及び p_2 セグメントでメッセージをブラインドすることである。次いで、この特別なグループ要素の p_2 セグメントが敵対者に対して情報理論的に隠されたままであり、暗号化メッセージを完全に隠すために適切なランダム性抽出器を使用してそのエントロピーが増幅され得るように、チャレンジ暗号文及び鍵を巧妙に変換する。

【0042】

2つのサブシステムのユーザ秘密鍵成分を非対称に設定し、すなわち、第1のサブシステムに対応するユーザ秘密鍵成分内の特別なグループ要素を乗算し、第2のサブシステムに対応するユーザ秘密鍵成分内のものを乗算しない。次いで、まず、第2のサブシステムの p_3 サブグループ内の半機能的な部分を同じものの p_2 サブグループにブリードして、半機能的にする。その後、第2のサブシステムのこの半機能性を利用して、特別なグループ要素を、第1のサブシステムのユーザ秘密鍵成分内に埋め込まれているものから、第2のサブシステムに対応するものに切り替える。このステップを終えると、次いで、第1のサブシステムの p_3 サブグループ内の反機能的な部分を同じものの p_2 部分にブリードする。この時点で、メッセージをブラインドする暗号文成分の p_2 セグメントは、全ての他の暗号文及び鍵成分の p_2 セグメントから完全に独立するようになり、それにより、そのエントロピーを利用して、メッセージを情報理論的にブラインドできる。

【0043】

デュアルシステム方法論の全てのアプリケーションが、これまで単一のシステムのみを扱い、このような2つのサブシステムの考えは、本発明の研究にとって完全に新しいことを強調したい。また、この研究で対処した問題は、メッセージをブラインドする暗号文成分に半機能的な部分をブリードし、単一システム内のその特別なグループ要素からユーザ鍵を独立させる方法が明らかでないので、標準的な単一システムデュアルシステム技術の範囲を超えるように思われる。長年の未解決の問題を解決する発明者らの研究から明らかのように、この新たな技術は非常に強力である。発明者らは、デュアルシステム暗号化方法の既存の変形の範囲を超えるように見える適応的セキュリティ問題に関連する更なる新たなアプリケーション、例えば、標準的なグループベースの仮定の下で線形関数を超える適応的にセキュアな関数型暗号化スキームを構築することを見出すことを想定する。

【0044】

構成:

【0045】

本発明のスキームは、合成数位数 N の双線形群

【数7】

$$\mathbb{G}$$

に依存することを思い起こす。これは3つの素数の積であり、すなわち、3つのサブグループ

【数8】

$$\mathbb{G}_{p_1}, \mathbb{G}_{p_2} \text{ 及び } \mathbb{G}_{p_3}$$

による $N=p_1p_2p_3$ である。また、シードランダム性抽出器 Ext も利用し、 seed をそのシ

ードとする。要素 g_1 及び h は、 $seed$ と共にグローバルパラメータ GP の一部であるサブグループ

【数 9】

$$\mathbb{G}_{p_1}$$

の一樣乱数発生器である。 H は、セキュリティ証明においてランダムオラクルとしてモデル化するグローバルハッシュ関数である。

【0046】

非常にハイレベルでは、構成から明らかなように、暗号化アルゴリズムはメッセージ m を項 $\text{Ext}(e(g_1, h)^s, seed)$ でブラインドする。ここで、 s は

【数 10】

$$\mathbb{Z}_N$$

におけるランダム要素である。セキュリティ証明における目標は、敵対者のビューを考慮して、 $e(g_1, h)^s$ に十分なエントロピーが残っていることを示し、それにより、メッセージが実際に隠されるようにすることである。一方の s 及び他方の $-s$ である 2 つの秘密分散法が関与する。 s のシェア (share) を $\sigma_{A,x}$ で表し、 $-s$ のシェアを $\sigma_{B,x}$ で表すものとする。

復号器は、属性及び暗号文成分のためのこれらの鍵を適切にペアにすることによって、

【数 11】

$$e(g_1, H(\text{GID}) \cdot h)^{\sigma_{A,x}} \text{ 及び } e(g_1, H(\text{GID}))^{\sigma_{B,x}}$$

を回復する。ユーザが暗号文を復号するのに十分な秘密鍵を保持している場合、2 つの項

【数 12】

$$e(g_1, H(\text{GID}) \cdot h)^{\sigma_{A,x}} \text{ 及び } e(g_1, H(\text{GID}))^{\sigma_{B,x}}$$

は、

【数 13】

$$e(g_1, H(\text{GID}) \cdot h)^s \text{ 及び } e(g_1, H(\text{GID}))^{-s}$$

を回復するために使用でき、これらは、乗算されると、必要に応じてブラインド係数 $e(g_1, h)^s$ を与える。

【0047】

$\text{AuthSetup}(GP, u)$: アルゴリズムは乱数値

【数 14】

$$y_{A,u}, y_{B,u} \in \mathbb{Z}_N$$

を選択し、

【数 15】

$$PK_u = (g_1^{y_{A,u}}, g_1^{y_{B,u}}) \quad MSK_u = (y_{A,u}, y_{B,u})$$

を出力する。

【数 1 6】

$Enc(GP, msg, (M, \rho), \{PK_u\})$: 最初に乱数値

【数 1 6】

10

$$S \leftarrow \mathbb{Z}_N$$

を選択する。次いで、LSSSアクセスポリシー

【数 1 7】

$$(M, \rho)$$

を使用して s の秘密分散を生成する。ここで、 $\sigma_{A,x}$ は、全ての $x \in [l]$ についてのシェアとし、すなわち、全ての $x \in [l]$ について、

20

【数 1 8】

$$\sigma_{A,x} = M_x \cdot v_A$$

とし、

【数 1 9】

$$v_A \leftarrow \mathbb{Z}_N^d$$

30

は、その第1エントリとして s を有するランダムベクトルであり、

【数 2 0】

$$M_x$$

は

【数 2 1】

40

$$M$$

の第 x 行である。アクセスポリシー

【数 2 2】

$$(M, \rho)$$

50

は、形式
【数 2 3】

$$\mathbf{M} = (M_{x,j})_{\ell \times d} = (\mathbf{M}_1, \dots, \mathbf{M}_\ell)^\top \in \mathbb{Z}_N^{\ell \times d}$$

となり、
【数 2 4】

$$\rho: [\ell] \rightarrow \mathcal{AU}$$

10

である。関数 ρ は
【数 2 5】

$$\mathbf{M}$$

の行をオーソリティに関連付ける。 ρ は単射関数であり、すなわち、オーソリティ / 属性
【数 2 6】

20

$$\mathbf{M}$$

の最大でも1つの行に関連付けられることを仮定する。これは、属性がアクセスポリシー
内で最大でも限られた回数だけ現れる設定に拡張できる。さらに、LSSSアクセスポリシ
ー
【数 2 7】

30

$$(\mathbf{M}, \rho)$$

に関して s の別の秘密分散を作成する。ここで、 $\sigma_{B,x}$ は全ての $x \in [l]$ についての $\rho(x)$ の
対応するシェアであり、すなわち、全ての $x \in [l]$ について、
【数 2 8】

$$\sigma_{B,x} = \mathbf{M}_x \cdot \mathbf{v}_B$$

40

であり、
【数 2 9】

$$\mathbf{v}_B \leftarrow \mathbb{Z}_N^d$$

は、その第1エントリとして s を有するランダムベクトルである。この手順は、暗号文を
以下のように生成する。各行 $x \in [l]$ について、ランダムな
【数 3 0】

50

$$r_{A,x}, r_{B,x} \leftarrow \mathbb{Z}_N$$

を選択し、暗号文
【数 3 1】

$$CT = ((M, \rho), C, \{C_{1,A,x}, C_{2,A,x}, C_{1,B,x}, C_{2,B,x}\}_{x \in [\ell]})$$

10

を出力する。ここで、
【数 3 2】

$$C = \text{msg} \oplus \text{Ext}(e(g_1, h)^s, \text{seed}), \quad C_{1,A,x} = g_1^{r_{A,x}} \quad C_{2,A,x} = g_1^{y_{A,\rho(x)} r_{A,x}} g_1^{\sigma_{A,x}}$$

$$C_{1,B,x} = g_1^{r_{B,x}} \quad C_{2,B,x} = g_1^{y_{B,\rho(x)} r_{B,x}} g_1^{\sigma_{B,x}}$$

20

である。

【0 0 4 9】

$\text{KeyGen}(\text{GP}, \text{GID}, \text{MSK}_u)$: オーソリティ属性 u は、 GID についての秘密鍵 $\text{SK}_{\text{GID},u}$ を $\text{SK}_{\text{GID},u} = (\text{K}_{\text{GID},A,u}, \text{K}_{\text{GID},B,u})$ として生成する。ここで、

【数 3 3】

$$K_{\text{GID},A,u} = (H(\text{GID}) \cdot h)^{y_{A,u}} \quad K_{\text{GID},B,u} = (H(\text{GID}))^{y_{B,u}}$$

30

である。

【0 0 5 0】

$\text{Dec}(\text{GP}, CT, \text{GID}, \{\text{SK}_{\text{GID},u}\})$: 復号は、グローバルパラメータ GP 、ハッシュ関数 H 、 L SSS アクセス構造

【数 3 4】

$$(M, \rho)$$

40

についての暗号文 CT (

【数 3 5】

$$M \in \mathbb{Z}_N^{\ell \times d} \text{ 且 } \rho: [\ell] \rightarrow \mathcal{AU}$$

)、ユーザのグローバル識別子

【数 3 6】

50

$$\text{GID} \in \mathcal{GID}$$

、及びインデックス $I \subseteq [l]$ を有する
【数 3 7】

$$M$$

10

の行のサブセットに対応する秘密鍵 $\{\text{SK}_{\text{GID}, \rho(x)}\}_{x \in I}$ を入力として取る。 $(1, 0, \dots, 0)$ が
これらの行のスパン
【数 3 8】

$$M_I$$

にない場合、復号は失敗する。そうでない場合、復号器は、
【数 3 9】

20

$$(1, 0, \dots, 0) = \sum_{x \in I} w_x \cdot M_x$$

となるような係数
【数 4 0】

$$\{w_x \in \mathbb{Z}_N\}_{x \in I}$$

30

を見つける。
【0 0 5 1】

全ての $x \in I$ について、復号アルゴリズムは、
【数 4 1】

$$D_{A,x} = e(C_{2,A,x}, H(\text{GID}) \cdot h) \cdot e(C_{1,A,x}, K_{\text{GID},A,\rho(x)})^{-1} = e(g_1, H(\text{GID}) \cdot h)^{\sigma_{A,x}}$$

40

$$D_{B,x} = e(C_{2,B,x}, H(\text{GID})) \cdot e(C_{1,B,x}, K_{\text{GID},B,\rho(x)})^{-1} = e(g_1, H(\text{GID}))^{\sigma_{B,x}}$$

を計算する。これは
【数 4 2】

50

$$D = \prod_{x \in I} (D_{A,x} \cdot D_{B,x})^{w_x} = e(g_1, h)^s$$

を計算し、
【数 4 3】

$$C \oplus \text{Ext}(D, \text{seed}) = \text{msg}$$

10

を出力する。

【0 0 5 2】

提案スキームは、検査によって正確である。

【0 0 5 3】

素数位数群へのポーティング

【0 0 5 4】

上記のように、既存の合成数位数群の構成を素数位数の同様のものに変換する方法を考え出そうとする多くの研究が行われてきた。これらのフレームワークの全ては異なり、様々なレベルの簡潔さ又は一般性を有する。発明者らは、最も効率的であり、(ほぼ間違いなく)使用するのが最も簡単であると思われるChenらの最近のフレームワークを使用し、合成数位数設定から素数位数設定への構成及び証明の適合に成功している。

20

【0 0 5 5】

このフレームワークは、ハイレベルで、様々なサブグループ判定スタイルの仮定の素数位数の同様のものを保証しつつ、素数位数群を使用して合成数位数群及びそのサブグループをシミュレートする方法を示す。これらの同様のものは、標準的なk-線形仮定(より一般的には、MDDH仮定)から得られる。ここで、変換プロセスは完全にブラックボックスではなく、当面のスキームに適合される必要があるので、本発明の特定の設定を扱うためにいくつかの追加の技術的概念を導入する必要がある。具体的には、本発明の素数位数構成のセキュリティの証明は、サブグループ判定スタイルの仮定だけでなく、いくつかの情報理論的引数及びランダムオラクルのセキュリティにも依存する。フレームワークを使用してこれを本発明のスキームに対して機能させることは、かなり技術的であり、系統的である。詳細については、技術セクションを参照する。それにもかかわらず、発明者らは、ハイレベルの概念及びハイブリッドのシーケンスが合成数位数の場合と同じであることを指摘する。

30

【0 0 5 6】

前置き

【0 0 5 7】

関数

【数 4 4】

40

$$\text{negl}: \mathbb{N} \rightarrow \mathbb{R}$$

は、任意の逆多項式関数よりも漸近的に小さい場合、すなわち、全ての定数 $c > 0$ について、全ての $\lambda > N_c$ について $\text{negl}(\lambda) \leq \lambda^{-c}$ となるような整数 N_c が存在する場合、無視可能である。[n]={1,...,n}とする。

【0 0 5 8】

50

ベクトルを表すために、
【数 4 5】

$$v$$

のような太字の小文字を使用し、行列については
【数 4 6】

$$M$$

10

のような太字の大文字を使用する。デフォルトでは、全てのベクトルが列ベクトルであると仮定する。行列の第 i 行は
【数 4 7】

$$M_i$$

で表され、同様に行インデックス I のセットについて、全ての $i \in I$ についての行
【数 4 8】

20

$$M_i$$

からなる
【数 4 9】

$$M$$

30

の部分行列について
【数 5 0】

$$M_I$$

で表す。整数 $q \geq 2$ について、
【数 5 1】

40

$$\mathbb{Z}_q$$

をモジュロ q の整数の環を表す。範囲 $(-q/2, q/2]$ 内の整数として
【数 5 2】

$$\mathbb{Z}_q$$

50

を表す。

【 0 0 5 9 】

区別不能性:確率変数の2つのシーケンス $X=\{X_\lambda\}_{\lambda \in \mathbb{N}}$ 及び $Y=\{Y_\lambda\}_{\lambda \in \mathbb{N}}$ は、任意の非均一PPT(non-uniform PPT)アルゴリズム

【数 5 3】

$\mathcal{A}$

10

について、全ての

【数 5 4】

$\lambda \in \mathbb{N}$

について

【数 5 5】

20

$$|\Pr[\mathcal{A}(1^\lambda, X_\lambda) = 1] - \Pr[\mathcal{A}(1^\lambda, Y_\lambda) = 1]| \leq \text{negl}(\lambda)$$

となるような無視可能関数 $\text{negl}(\cdot)$ が存在する場合、計算的に区別不能である。

【 0 0 6 0 】

離散ドメイン Ω 上での2つの分布 D 及び D' について、 D と D' との間の統計的距離は、 $SD(D, D') = (1/2) \cdot \sum_{\omega \in \Omega} |D(\omega) - D'(\omega)|$ として定義される。セキュリティパラメータ λ によってパラメータ化された分布 $D = \{D_\lambda\}_{\lambda \in \mathbb{N}}$ 及び $D' = \{D'_\lambda\}_{\lambda \in \mathbb{N}}$ のファミリーは、全ての

30

【数 5 6】

$\lambda \in \mathbb{N}$

について、 $SD(D_\lambda, D'_\lambda) \leq \text{negl}(\lambda)$ となるような無視可能関数 $\text{negl}(\cdot)$ が存在する場合、統計的に区別不能であると言われる。

【 0 0 6 1 】

アクセス構造及び線形秘密分散法

40

【 0 0 6 2 】

このサブセクションでは、アクセス構造及び線形秘密分散法の定義を提示する。

【 0 0 6 3 】

定義(アクセス構造):

【数 5 7】

$\mathbb{U}$

を属性母集団とする。

50

【数 5 8】

 $\mathbb{U}$

におけるアクセス構造は、空ではない属性セットの集合

【数 5 9】

$$\mathbb{A} \subseteq 2^{\mathbb{U}} \setminus \emptyset$$

10

である。

【数 6 0】

 $\mathbb{A}$

におけるセットは、有資格集合(authorized set)と呼ばれ、

【数 6 1】

20

 $\mathbb{A}$

にないセットは、無資格集合(unauthorized set)と呼ばれる。アクセス構造は、

【数 6 2】

$$\text{if } \forall B, C \in 2^{\mathbb{U}} \text{ if } B \in \mathbb{A} \text{ and } B \subseteq C, \text{ then } C \in \mathbb{A}$$

30

となる場合、単調性と呼ばれる。

【0 0 6 4】

定義(線形秘密分散法(LSSS, Linear Secret Sharing Scheme)): $q = q(\lambda)$ を素数とし、

【数 6 3】

 $\mathbb{U}$

40

を属性母集団とする。

【数 6 4】

 $\mathbb{U}$

上の単調性アクセス構造

【数 6 5】

50

$\mathbb{A}$

に対する秘密のドメイン
【数 6 6】

 $\mathbb{Z}_q$

10

を有する単調性秘密分散方式 Π (単調性秘密分散法 (monotone secret sharing scheme) と呼ばれる) は、入力時に秘密
【数 6 7】

 $z \in \mathbb{Z}_q$

が
【数 6 8】

20

 $|\mathbb{U}|$

個のシェア
【数 6 9】

 $sh_1, \dots, sh_{|\mathbb{U}|}$

30

を出力し、任意の集合
【数 7 0】

 $S \in \mathbb{A}$

について、シェア $\{sh_i\}_{i \in S}$ が z を決定し、他のセットのシェアが z から (確率変数として) 独立であるようなランダム化アルゴリズムである。
【数 7 1】

40

 $\mathbb{U}$

上で単調性アクセス構造を実現する秘密分散方式 Π は、以下の場合、
【数 7 2】

50

$$\mathbb{Z}_q$$

上で線形である。

【 0 0 6 5 】

1.

【 数 7 3 】

$$\mathbb{U}$$

10

における各属性に対する秘密

【 数 7 4 】

$$z \in \mathbb{Z}_q$$

のシェアが

【 数 7 5 】

20

$$\mathbb{Z}_q$$

上でベクトルを形成する。

【 0 0 6 6 】

2.

【 数 7 6 】

$$\mathbb{U}$$

30

上の各単調性アクセス構造

【 数 7 7 】

$$\mathbb{A}$$

について、シェア生成行列と呼ばれる行列

【 数 7 8 】

40

$$M \in \mathbb{Z}_q^{\ell \times s}$$

と、以下を満たす

【 数 7 9 】

$$\mathbb{U}$$

50

からの属性で
【数 8 0】

M

の行にラベルを付ける関数
【数 8 1】

$$\rho: [\ell] \rightarrow \mathbb{U}$$

10

が存在する。シェアの生成中に、ベクトル
【数 8 2】

$$v = (z, r_2, \dots, r_s)$$

を考える。ここで、
【数 8 3】

20

$$r_2, \dots, r_s \leftarrow \mathbb{Z}_q$$

である。次いで、 Π に従って秘密 z の l 個のシェアのベクトルは、
【数 8 4】

$$\mu = Mv^\top \in \mathbb{Z}_q^{\ell \times 1}$$

30

によって与えられる。ここで、全ての $j \in [l]$ について、シェア μ_j は属性 $\rho(j)$ に「属する」。
アクセス構造
【数 8 5】

$\mathbb{A}$

のLSSSポリシーとしてペア
【数 8 6】

40

$$(M, \rho)$$

を参照する。
【0 0 6 7】

単調性LSSSの正確性及びセキュリティは以下のように形式化される。 $S(S')$ を、何らかの単調性アクセス構造

【数 8 7】

50

$$\mathbb{A}$$

に従った属性の有資格(禁止)集合を表し、 $l(l')$ を、ラベルが $s(s')$ にある
【数 8 8】

$$\mathbb{A}$$

10

に関連付けられたLSSSポリシーペア
【数 8 9】

$$(M, \rho)$$

のシェア生成行列
【数 9 0】

$$M$$

20

の行のセットであるとする。正確性のために、
【数 9 1】

$$\mathbb{Z}_q$$

に定数 $\{w_i\}_{i \in I}$ が存在し、 Π に従った秘密
【数 9 2】

30

$$z \in \mathbb{Z}_q$$

の任意の有効なシェア
【数 9 3】

$$\{\mu_i = (Mv^T)_i\}_{i \in I}$$

40

について、
【数 9 4】

$$\sum_{i \in I} w_i \mu_i = z$$

(等価的に、
【数 9 5】

50

$$\sum_{i \in I} w_i M_i = \left(1, \overbrace{0, \dots, 0}^{s-1}\right)$$

ここで、
【数 9 6】

$$M_i$$

10

は
【数 9 7】

$$M$$

の第*i*行である)であることが当てはまる。健全性のために、行列
【数 9 8】

20

$$M$$

の行の如何なる部分集合*I*も存在せず、上記が当てはまる如何なる係数{*w_i*}*i* ∈ *I*も存在しない。

【0 0 6 8】

備考 1 (NC¹ 及び単調性 LSSS): NC¹ 回路で記述されるアクセス構造

【数 9 9】

$$\mathbb{A}$$

30

を考える。(fan-in 2) AND、OR 及び (fan-in 1) NOT ゲートで構成される対数深さのブール式にこの回路を変換するフォークロア変換 (folklore transformation) が存在する。さらに、ド・モルガンの法則を使用して NOT ゲートをリーフにプッシュし、内部ノードが OR 及び AND ゲートのみで構成され、リーフが属性又はその否定によってラベル付けされると仮定することができる。言い換えると、属性のセットに対する任意の NC¹ ポリシーを、その否定と共に同じ属性に対する対数深さの単調性ブール式で記述されるものに表現できる。Lewko 及び Waters は、単調性ブール式で記述されるアクセス構造について単調性 LSSS を提示している。これは、任意の NC¹ アクセスポリシーが単調性 LSSS で捕捉できることを意味する。

40

【0 0 6 9】

強力なランダム性抽出器

【0 0 7 0】

確率変数 *X* の最小エントロピーは、

【数 1 0 0】

$$H_{\infty}(X) = -\log(\max_x \Pr[X = x])$$

50

である。t-ソースは、
【数 1 0 1】

$$H_{\infty}(X) \geq t$$

での確率変数Xである。有限ドメインΩ上での2つの変数X及びYの間の統計的距離は、
【数 1 0 2】

$$SD(X, Y) = \frac{1}{2} \sum_{\omega \in \Omega} |\Pr[X = \omega] - \Pr[Y = \omega]| \quad 10$$

である。
【0 0 7 1】

定義(シードランダム性抽出器):関数 $\text{Ext}:\Omega \times S \rightarrow \Gamma$ は、Ω上のtソースXについて、
【数 1 0 3】

$$SD((\mathcal{U}_S, \text{Ext}(X, \mathcal{U}_S)), (\mathcal{U}_S, \mathcal{U}_{\Gamma})) < \epsilon \quad 20$$

である場合、強力な(t, ε)抽出器である。

【0 0 7 2】

定理:全ての
【数 1 0 4】

$$n, t \in \mathbb{N} \text{ 及び } \epsilon > 0$$

について、強力な(t, ε)抽出器 $\text{Ext}:\{0, 1\}^n \times \{0, 1\}^d \rightarrow \{0, 1\}^m$ が存在し、 $m=t-2\log(1/\epsilon)-O(1)$ 且つ $d=\log(n-t)+2\log(1/\epsilon)+O(1)$ である。

【0 0 7 3】

LSSSについての完全適応型分散型MA-ABE

【0 0 7 4】

分散型マルチオーソリティの属性ベース暗号化(MA-ABE, multi-authority attribute-based encryption)システムMA-ABE=(GlobalSetup, AuthSetup, KeyGen, Enc, Dec)は、構文が以下に与えられる5つの手順からなる。本発明が扱うサポートされるアクセス構造は、線形秘密分散法(LSSS, linear secret sharing schemes)によって捕捉されるアクセス構造である。オーソリティ母集団を

【数 1 0 5】

$$\mathcal{AU}$$

で表し、ユーザのグローバル識別子の母集団を

【数 1 0 6】

$$\mathcal{GID}$$

で表す。サポートされるメッセージ空間を
【数 1 0 7】

$$\mathbb{M}$$

で表す。さらに、各オーソリティは1つの属性のみを制御すると仮定し、したがって、「
オーソリティ」及び「属性」という用語を交換可能に使用する。この定義は、当然、各オ
ーソリティが潜在的に任意(有界又は非有界)の数の属性を制御できる状況に一般化される
。

10

【0 0 7 5】

$\text{GlobalSetup}(1^\lambda) \rightarrow \text{GP}$: グローバル設定アルゴリズムは、単項表現のセキュリティパ
ラメータ λ を取り込み、システムのためのグローバル公開パラメータGPを出力する。GP
が属性オーソリティの母集団

【数 1 0 8】

$$\mathcal{AU}$$

及びユーザのグローバル識別子の母集団

20

【数 1 0 9】

$$\mathcal{GID}$$

の記述を含むと仮定する。システム内のオーソリティ及びユーザの数の制限がない場合、
【数 1 1 0】

$$\mathcal{AU} \text{ 及び } \mathcal{GID}$$

30

の双方が $\{0, 1\}^\lambda$ によって与えられる点に留意する。

【0 0 7 6】

$\text{AuthSetup}(\text{GP}, u) \rightarrow (\text{PK}_u, \text{MSK}_u)$: オーソリティ

【数 1 1 1】

$$u \in \mathcal{AU}$$

40

は、グローバルパラメータGPを入力として用いて、その初期化中にオーソリティ設定ア
ルゴリズムを呼び出し、その公開鍵及びマスター秘密鍵のペア $\text{PK}_u, \text{MSK}_u$ を受信する。

【0 0 7 7】

$\text{KeyGen}(\text{GP}, \text{GID}, \text{MSK}_u) \rightarrow \text{SK}_{\text{GID}, u}$: 鍵生成アルゴリズムは、入力としてグローバル
パラメータGP、ユーザのグローバル識別子

【数 1 1 2】

$$\text{GID} \in \mathcal{GID}$$

50

及びオーソリティ
【数 1 1 3】

$$u \in \mathcal{AU}$$

のマスター秘密鍵 MSK_u を取り込む。これはユーザのための秘密鍵 $SK_{GID,u}$ を出力する。
【 0 0 7 8】
【数 1 1 4】

10

$$\text{Enc}(\text{GP}, \text{msg}, (\boldsymbol{M}, \rho), \{\text{PK}_u\}) \mapsto \text{CT}$$

: 暗号化アルゴリズムは、グローバルパラメータ GP、メッセージ
【数 1 1 5】

$$\text{msg} \in \mathbb{M}$$

20

、LSSS アクセスポリシー
【数 1 1 6】

$$(\boldsymbol{M}, \rho)$$

を取り込み、
【数 1 1 7】

$$\boldsymbol{M}$$

30

は
【数 1 1 8】

$$\mathbb{Z}_N$$

上の行列であり、 ρ は、
【数 1 1 9】

40

$$\boldsymbol{M}$$

の各行に割り当てる行ラベル付け関数であり、
【数 1 2 0】

$$\mathcal{AU}$$

50

における属性/オーソリティ及び全てのオーソリティについての公開鍵のセット $\{PK_u\}$ は ρ の範囲にある。これは暗号文CTを出力する。暗号文は、
【数 1 2 1】

$$(M, \rho)$$

を暗黙的に含むと仮定する。

【0 0 7 9】

$Dec(GP, CT, \{SK_{GID, u}\}) \rightarrow msg'$: 復号アルゴリズムは、グローバルパラメータGP、何
らかのLSSSアクセスポリシー 10

【数 1 2 2】

$$(M, \rho)$$

に関して生成された暗号文CT、及びグローバル識別子GIDを有するユーザによって所有
されるユーザID-属性ペア $\{(GID, u)\}$ に対応する鍵の集合 $\{SK_{GID, u}\}$ を取り込む。これは
、秘密鍵 $\{SK_{GID, u}\}$ に関連付けられた属性の集合がLSSSアクセスポリシー
【数 1 2 3】 20

$$(M, \rho)$$

を満たす場合、すなわち、秘密鍵 $\{SK_{GID, u}\}$ がグローバル識別子GIDを有するユーザによ
って所有されるように、ベクトル $(1, 0, \dots, 0)$ が ρ によって何らかの属性/オーソリティ
【数 1 2 4】

$$u \in \mathcal{AU}$$

30

に写像される

【数 1 2 5】

$$M$$

のこれらの行の線形スパンに含まれる場合、メッセージ msg' を出力する。そうでない場
合、復号は失敗する。

【0 0 8 0】

40

正確性:LSSSで実現可能なアクセス構造のためのMA-ABEスキームは、全ての

【数 1 2 6】

$$\lambda \in \mathbb{N}$$

、全てのメッセージ

【数 1 2 7】

50

$$\text{msg} \in \mathbb{M}$$

及び

【数 1 2 8】

$$\text{GID} \in \mathcal{GID}$$

10

、全てのLSSSアクセスポリシー

【数 1 2 9】

$$(\mathbf{M}, \rho)$$

、並びにアクセス構造を満たす属性を制御する全てのオーソリティのサブセット

【数 1 3 0】

20

$$U \subseteq \mathcal{AU}$$

について、

【数 1 3 1】

$$\Pr \left[\begin{array}{l} \text{GP} \leftarrow \text{GlobalSetup}(1^\lambda) \\ \forall u \in U: \text{PK}_u, \text{MSK}_u \leftarrow \text{AuthSetup}(\text{GP}, u) \\ \forall u \in U: \text{SK}_{\text{GID}, u} \leftarrow \text{KeyGen}(\text{GP}, \text{GID}, \text{MSK}_u) \\ \text{CT} \leftarrow \text{Enc}(\text{GP}, \text{msg}, (\mathbf{M}, \rho), \text{PK}_u) \\ \text{msg}' = \text{Dec}(\text{GP}, \text{CT}, \text{SK}_{\text{GID}, u_{u \in U}}) \end{array} \right] = 1$$

30

が当てはまる場合、正確であると言われる。

【0 0 8 1】

完全適応型セキュリティ:分散型MA-ABEスキームのための完全適応型の(選択された平文)セキュリティを定義する。すなわち、適応的な秘密鍵クエリ、適応的なオーソリティコラプションクエリ(corruption query)及び適応的なチャレンジ暗号文クエリが存在し得るセキュリティゲームを考える。これは、挑戦者と攻撃者との間の以下のゲームにおいて形式化される。2つのタイプのオーソリティ公開鍵、すなわち、挑戦者によって正当に生成されるものと、攻撃者自体によって供給されるものとを考慮し、前者のタイプのオーソリティ鍵はゲーム中の任意の時点で攻撃者によって破損される可能性があり、後者のタイプのオーソリティ鍵は潜在的に不正に形成される可能性がある点に留意する。

40

【0 0 8 2】

ゲームは、以下の段階からなる。

グローバル設定:挑戦者がグローバル公開パラメータGPを生成するためにGlobalSetupを実行し、攻撃者に与える。

クエリ段階1:攻撃者は、以下のタイプの多項式の数のクエリを適応的に行うことを許

50

容される。

オーソリティ設定クエリ:攻撃者は、その選択のオーソリティ

【数 1 3 2】

$$u \in \mathcal{AU}$$

を設定するように要求する。同じオーソリティ u についてオーソリティ設定クエリが以前に既に行われていた場合、挑戦者は中止する。そうでない場合、挑戦者はAuthSetupを実行して、オーソリティ u の公開/マスター鍵ペア (PK_u, MSK_u) を作成する。挑戦者は PK_u を攻撃者に提供し、 (PK_u, MSK_u) を記憶する。挑戦者は、生成された公開/マスター鍵ペアを攻撃者に返信しない点に留意する。

10

秘密鍵クエリ:攻撃者は、ペア (GID, u) を挑戦者に提示することによって秘密鍵クエリを作成する。ここで、

【数 1 3 3】

$$GID \in \mathcal{GID}$$

はグローバル識別子であり、

20

【数 1 3 4】

$$u \in \mathcal{AU}$$

は属性オーソリティである。オーソリティ u のオーソリティ設定クエリがまだ行われていない場合、挑戦者は中止する。そうでない場合、挑戦者は、 u のオーソリティ設定クエリに応じて既に生成されている公開/マスター鍵ペアを使用してKeyGenを実行し、 (GID, u) についての秘密鍵 $SK_{GID, u}$ を生成する。挑戦者は $SK_{GID, u}$ を攻撃者に提供する。

30

オーソリティマスター鍵クエリ:攻撃者は、オーソリティ

【数 1 3 5】

$$u \in \mathcal{AU}$$

のマスター秘密鍵を挑戦者に要求する。オーソリティ u のオーソリティ設定クエリが以前に行われていない場合、挑戦者は中止する。そうでない場合、挑戦者は、 u のオーソリティ設定クエリに応じて作成したオーソリティ u についてのマスター秘密鍵 MSK_u を攻撃者に提供する。

40

チャレンジ段階:攻撃者は2つのメッセージ

【数 1 3 6】

$$msg_0, msg_1 \in \mathcal{M}$$

及びLSSSアクセス構造

【数 1 3 7】

50

$$(M, \rho)$$

を提示する。攻撃者はまた、LSSSアクセス構造
【数 1 3 8】

$$(M, \rho)$$

10

に現れる属性オーソリティのサブセットについてオーソリティ公開鍵 $\{PK_u\}$ を提示する。
攻撃者によって供給されるオーソリティ公開鍵 $\{PK_u\}$ は、潜在的に不正に形成される可能性があり、すなわち、AuthSetupの範囲外になる可能性がある。LSSSアクセス構造
【数 1 3 9】

$$(M, \rho)$$

及びオーソリティ公開鍵 $\{PK_u\}$ は、以下の制約を満たさなければならない。

20

(a)

【数 1 4 0】

$$U_{\mathcal{A}}$$

を、攻撃者がオーソリティ公開鍵 $\{PK_u\}$ を供給した属性オーソリティのセットを表すものとする。また、
【数 1 4 1】

30

$$U_{\mathcal{B}}$$

を、挑戦者がこれまでに攻撃者のオーソリティ設定クエリに応じてマスタ公開鍵ペアを作成した属性オーソリティのセットを表す。その場合、
【数 1 4 2】

$$U_{\mathcal{A}} \cap U_{\mathcal{B}} = \emptyset$$

40

となることが必要とされる。

(b) Vを、攻撃者がこれまでにマスター鍵クエリを行ったオーソリティを加えた

【数 1 4 3】

$$U_{\mathcal{A}}$$

におけるオーソリティによってラベル付けされた
【数 1 4 4】

50

M

の行のサブセットを表すものとする。各グローバル識別子
【数 1 4 5】

$$GID \in \mathcal{GID}$$

10

について、 V_{GID} を、攻撃者がペア (GID, u) の秘密鍵をクエリしたオーソリティ u によってラベル付けされた
【数 1 4 6】

M

の行のサブセットを表すものとする。それぞれの
【数 1 4 7】

20

$$GID \in \mathcal{GID}$$

について、 $V \cup V_{GID}$ 内のオーソリティによってラベル付けされた
【数 1 4 8】

M

の行が $(1, 0, \dots, 0)$ に及ばないことが必要とされる。

30

挑戦者はランダムコイン $b \leftarrow \{0, 1\}$ を弾き、アクセス構造

【数 1 4 9】

$$(M, \rho)$$

の下で msg_b を暗号化する Enc アルゴリズムを実行することによって、暗号文 CT を生成する。

クエリ段階2: 攻撃者は、制約の特性 (a) 及び (b) に違反しない限り、クエリ段階1のように全てのタイプのクエリを行うことを許容される。

40

推測: 攻撃者は b に対する推測 b' を提示しなければならない。 $b = b'$ である場合、攻撃者の勝利である。このゲームにおける敵対者の優位性は、以下のように定義される。

【数 1 5 0】

$$\text{Adv}_{\mathcal{A}}^{\text{MA-ABE, fully-adaptive}}(\lambda) = |\Pr[b' = b] - 1/2|.$$

【0 0 8 3】

定義(LSSSについてのMA-ABEの完全適応型セキュリティ): LSSSで実現可能なアクセ

50

ス構造のためのMA-ABEスキームは、全ての
【数 1 5 1】

$$\lambda \in \mathbb{N}$$

について
【数 1 5 2】

$$\text{Adv}_{\mathcal{A}}^{\text{MA-ABE, fully-adaptive}}(\lambda) \leq \text{negl}(\lambda).$$

10

を有するような無視可能関数 $\text{negl}(\cdot)$ が任意のPPT敵対者
【数 1 5 3】

$$\mathcal{A}$$

について存在する場合、完全適応的に安全である。

20

【0 0 8 4】

備考(ランダムオラクルモデルにおけるLSSSについてのMA-ABEの完全適応型セキュリティ):さらに、ランダムオラクルモデルにおける完全適応型セキュリティの上記の概念を考える。この文脈では、グローバル公開パラメータの一部として公開され、攻撃者を含むシステム内の全ての関係者によってアクセス可能なグローバルハッシュ関数Hを仮定する。セキュリティ証明では、Hを確率関数としてモデル化し、挑戦者がこれをプログラムできるようにする。したがって、上記の完全適応型セキュリティゲームでは、さらに、チャレンジ暗号文クエリの前及び後の双方で行う鍵クエリと共に、攻撃者がHオラクルクエリを挑戦者に適応的に提示するようにさせる。

【0 0 8 5】

30

合成数位数群MA-ABEスキーム

【0 0 8 6】

以下に、合成数位数双線形群と、本発明の構成が依存する仮定とについて説明し、構成を与える。

【0 0 8 7】

合成数位数双線形群及び仮定

【0 0 8 8】

本発明のシステムは、合成数位数双線形群に依存する。特に、3つの素数の積である合成数位数N、すなわち、 $N = p_1 p_2 p_3$ の双線形群

【数 1 5 4】

40

$$\mathbb{G}$$

に依存する。このような群は、Nの全ての約数qについて位数qの固有のサブグループを有し、このようなサブグループを

【数 1 5 5】

$$\mathbb{G}_q$$

50

として表す。また、全ての要素
【数 1 5 6】

$$g \in \mathbb{G}$$

は、
【数 1 5 7】

10

$\mathbb{G}_{p_1}$ の要素、 $\mathbb{G}_{p_2}$ の要素及び $\mathbb{G}_{p_3}$ の要素

の積として(一意に)記述できる。これらの要素をそれぞれ
【数 1 5 8】

「 g の $\mathbb{G}_{p_1}$ 部分」、 g の $\mathbb{G}_{p_2}$ 部分」及び「 g の $\mathbb{G}_{p_3}$ 部分」

20

と呼ぶ。入力としてセキュリティパラメータ λ を得て、
【数 1 5 9】

$$G = (N = p_1 p_2 p_3, \mathbb{G}, \mathbb{G}_T, e)$$

を出力する手順
【数 1 6 0】

30

$$\mathcal{G}(1^\lambda)$$

が存在すると仮定し、ここで、
【数 1 6 1】

$$e: \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$$

はペアリングである。
【数 1 6 2】

40

$$\mathbb{G} \text{ 及び } \mathbb{G}_T$$

における群演算及び双線形写像 e が λ において多項式時間で計算可能であると仮定する。
さらに、 e が以下を満たすと仮定する。

1. (双線形)

【数 1 6 3】

50

$$\forall g, h \in \mathbb{G}, a, b \in \mathbb{Z}_N, e(g^a, h^b) = e(g, h)^{ab}$$

2. (非退化) $e(g, g)$ が

【数 1 6 4】

$$\mathbb{G}_T$$

10

において位数 N を有するような

【数 1 6 5】

$$\exists g \in \mathbb{G}$$

である。

【0 0 8 9】

構成

20

【0 0 9 0】

ここで、合成数位数双線形群における NC^1 構成のための MA-ABE を提示する。上記のように、各オーソリティは1つの属性のみを制御すると仮定し、したがって、「オーソリティ」及び「属性」という用語を交換可能に使用する。

【0 0 9 1】

$\text{GlobalSetup}(1^\lambda)$: グローバル設定アルゴリズムは、単項で符号化されたセキュリティパラメータ 1^λ を取り込む。この手順は、最初に素数 p_1 、 p_2 、 p_3 を選択し、 $N = p_1 p_2 p_3$ とする。次に、位数 N の双線形群

【数 1 6 6】

30

$$G = (N, \mathbb{G}, \mathbb{G}_T, e)$$

を生成する。

【数 1 6 7】

$$\mathbb{G}_{p_1}$$

を、位数 p_1 の

【数 1 6 8】

40

$$\mathbb{G}$$

のサブグループとし、 g_1 及び h を、サブグループ

【数 1 6 9】

$$\mathbb{G}_{p_1}$$

50

の一樣乱数生成子とする。強力なシードランダム性抽出器
【数 1 7 0】

$$\text{Ext}: \mathbb{G}_T \times S \rightarrow \mathbb{M}$$

を利用し、
【数 1 7 1】

$$\mathbb{M} \subset \{0,1\}^*$$

10

はメッセージ空間であり、 $S \subset \{0,1\}^*$ はシード空間である。アルゴリズムはシード $\text{seed} \leftarrow S$ をサンプリングする。これはグローバルパラメータ $\text{GP} = (G, g_1, h, \text{seed})$ を設定する。
さらに、
グローバル識別子
【数 1 7 2】

$$\text{GID} \in \mathcal{GID}$$

20

を
【数 1 7 3】

$$\mathbb{G}$$

における要素に写像するハッシュ関数
【数 1 7 4】

30

$$H : \{0,1\}^* \rightarrow \mathbb{G}$$

を利用する。
【0 0 9 2】

$\text{AuthSetup}(\text{GP}, H, u)$: グローバルパラメータ GP 、ハッシュ関数 H 及びオーソリティインデックス
【数 1 7 5】

$$u \in \mathcal{AU}$$

40

が与えられると、アルゴリズムは乱数値
【数 1 7 6】

$$y_{A,u}, y_{B,u} \in \mathbb{Z}_N$$

を選択し、
【数 1 7 7】

50

$$\text{PK}_u = (P_{A,u} = g_1^{y_{A,u}}, P_{B,u} = g_1^{y_{B,u}}) \quad \text{MSK}_u = (y_{A,u}, y_{B,u})$$

を出力する。

【 0 0 9 3 】

$\text{Enc}(\text{GP}, \text{H}, \text{msg}, (\text{M}, \rho), \{\text{PK}_u\})$: 暗号化アルゴリズムは、入力としてグローバルパラメータ GP、ハッシュ関数 H、暗号化するメッセージ

【 数 1 7 8 】

10

$$\text{msg} \in \mathbb{M}$$

、LSSSアクセス構造

【 数 1 7 9 】

$$(\mathbf{M}, \rho) \quad (\mathbf{M} = (M_{x,j})_{\ell \times d} = (\mathbf{M}_1, \dots, \mathbf{M}_\ell)^\top \in \mathbb{Z}_N^{\ell \times d} \text{ 且 } \rho: [\ell] \rightarrow \mathcal{AU})$$

20

、及び関連するオーソリティの公開鍵 $\{\text{PK}_u\}$ を取る。関数 ρ は

【 数 1 8 0 】

$$\mathbf{M}$$

の行をオーソリティに関連付ける (各オーソリティが単一の属性を制御すると仮定することを思い起こす)。 ρ は単射関数であり、すなわち、オーソリティ / 属性は

【 数 1 8 1 】

30

$$\mathbf{M}$$

の最大でも1つの行に関連付けられると仮定する。

【 0 0 9 4 】

最初に乱数値

【 数 1 8 2 】

$$s \leftarrow \mathbb{Z}_N$$

40

を選択する。次いで、LSSSアクセス構造

【 数 1 8 3 】

$$(\mathbf{M}, \rho)$$

を使用して s の秘密分散を生成する。ここで、 $\sigma_{A,x}$ は、全ての $x \in [l]$ についてのシェアとし、すなわち、全ての $x \in [l]$ について、

【 数 1 8 4 】

50

$$\sigma_{A,x} = \mathbf{M}_x \cdot \mathbf{v}_A$$

とし、

【数 1 8 5】

$$\mathbf{v}_A \leftarrow \mathbb{Z}_N^d$$

は、その第1エントリとしてsを有するランダムベクトルであり、

【数 1 8 6】

$$\mathbf{M}_x$$

は

【数 1 8 7】

$$\mathbf{M}$$

の第x行である。さらに、LSSSアクセスポリシー

【数 1 8 8】

$$(\mathbf{M}, \rho)$$

に関して-sの別の秘密分散を作成する。ここで、 $\sigma_{B,x}$ は全ての $x \in [l]$ についての $\rho(x)$ の対応するシェアであり、すなわち、全ての $x \in [l]$ について、

【数 1 8 9】

$$\sigma_{B,x} = \mathbf{M}_x \cdot \mathbf{v}_B$$

であり、

【数 1 9 0】

$$\mathbf{v}_B \leftarrow \mathbb{Z}_N^d$$

は、その第1エントリとして-sを有するランダムベクトルである。この手順は、暗号文を以下のように生成する。各行 $x \in [l]$ について、ランダムな

【数 1 9 1】

$$r_{A,x}, r_{B,x} \leftarrow \mathbb{Z}_N$$

を選択し、暗号文

【数 1 9 2】

$$CT = ((M, \rho), C, \{C_{1,A,x}, C_{2,A,x}, C_{1,B,x}, C_{2,B,x}\}_{x \in [\ell]})$$

を出力する。

【 0 0 9 5 】

ここで、

【 数 1 9 3 】

$$C = \text{msg} \oplus \text{Ext}(e(g_1, h)^s, \text{seed})$$

10

$$C_{1,A,x} = g_1^{r_{A,x}} \quad C_{2,A,x} = P_{A,\rho(x)}^{r_{A,x}} g_1^{\sigma_{A,x}} = g_1^{y_{A,\rho(x)} r_{A,x}} g_1^{\sigma_{A,x}}$$

$$C_{1,B,x} = g_1^{r_{B,x}} \quad C_{2,B,x} = P_{B,\rho(x)}^{r_{B,x}} g_1^{\sigma_{B,x}} = g_1^{y_{B,\rho(x)} r_{B,x}} g_1^{\sigma_{B,x}}$$

である。

【 0 0 9 6 】

KeyGen(GP, H, GID, MSK_u): 鍵生成アルゴリズムは、入力としてグローバルパラメータGP、ハッシュ関数H、ユーザのグローバル識別子

20

【 数 1 9 4 】

$$GID \in \mathcal{GID}$$

、及びオーソリティのマスター秘密鍵MSK_uを取る。これはGIDの秘密鍵SK_{GID,u}を以下のように生成する。

【 数 1 9 5 】

$$SK_{GID,u} = (K_{GID,A,u}, K_{GID,B,u})$$

30

ここで、

【 数 1 9 6 】

$$K_{GID,A,u} = (H(GID) \cdot h)^{y_{A,u}} \quad K_{GID,B,u} = (H(GID))^{y_{B,u}}$$

である。

40

【 0 0 9 7 】

Dec(GP, H, CT, GID, {SK_{GID,u}}): 復号は、グローバルパラメータGP、ハッシュ関数H、LSSSアクセス構造

【 数 1 9 7 】

$$(M, \rho)$$

についての暗号文CT(

【 数 1 9 8 】

50

$$M \in \mathbb{Z}_N^{\ell \times d} \text{ 且 } \rho: [\ell] \rightarrow \mathcal{AU} \text{ 単射}$$

)、ユーザのグローバル識別子
【数 1 9 9】

$$\text{GID} \in \mathcal{GID}$$

、及びインデックス $I \subseteq [l]$ を有する
【数 2 0 0】

$$M$$

の行のサブセットに対応する秘密鍵 $\{SK_{\text{GID},u}\}_{u \in \rho(I)}$ を入力として取る。 $(1, 0, \dots, 0)$ が
これらの行のスパン
【数 2 0 1】

$$M_I$$

にない場合、復号は失敗する。そうでない場合、復号器は、
【数 2 0 2】

$$(1, 0, \dots, 0) = \sum_{x \in I} w_x \cdot M_x$$

となるような $\{w_x \in \mathbb{N}\}_{x \in I}$ を見つける。
【0 0 9 8】
全ての $x \in I$ について、まず、復号アルゴリズムは、
【数 2 0 3】

$$D_{A,x} = e(C_{2,A,x}, H(\text{GID}) \cdot h) \cdot e(C_{1,A,x}, K_{\text{GID},A,\rho(x)})^{-1} = e(g_1, H(\text{GID}) \cdot h)^{\sigma_{A,x}}$$

$$D_{B,x} = e(C_{2,B,x}, H(\text{GID})) \cdot e(C_{1,B,x}, K_{\text{GID},B,\rho(x)})^{-1} = e(g_1, H(\text{GID}))^{\sigma_{B,x}}$$

を計算する。次いで、
【数 2 0 4】

$$D = \prod_{x \in I} (D_{A,x} \cdot D_{B,x})^{w_x} = e(g_1, h)^s$$

を計算し、最後に
【数 2 0 5】

10

20

30

40

50

$$C \oplus \text{Ext}(D, \text{seed}) = \text{msg}$$

を出力する。

【 0 0 9 9 】

素数位数群 MA-ABE スキーム

【 0 1 0 0 】

以下では、素数位数双線形群を思い起こし、関連する表記を与え、変換フレームワークの基本構造を与え、本発明の構成が依存する仮定を与え、構成を与える。

10

【 0 1 0 1 】

素数位数双線形群及び関連する表記

【 0 1 0 2 】

表記:

【 数 2 0 6 】

A

を、環(ring)

【 数 2 0 7 】

20

$\mathbb{Z}_q$

における行列とする。

【 数 2 0 8 】

A

30

の列スパンを表すために

【 数 2 0 9 】

$\text{span}(A)$

を使用し、幅 m の行列を表すために

【 数 2 1 0 】

$\text{span}^m(A)$

40

を使用する。これは、

【 数 2 1 1 】

$M \leftarrow \text{span}^m(A)$

が幅 m のランダム行列であり、各列が

【 数 2 1 2 】

50

$$\text{span}(A)$$

から一様に選択されることを意味する。

【数 2 1 3】

$$\text{span}(A)$$

10

の基底を表すために

【数 2 1 4】

$$\text{basis}(A)$$

を使用し、行列

【数 2 1 5】

$$A_1, A_2$$

20

の列に関する連結を表すために

【数 2 1 6】

$$(A_1 \parallel A_2)$$

を使用する。

【数 2 1 7】

30

$$I$$

を単位行列とし、

【数 2 1 8】

$$0$$

40

をゼロ行列とし、そのサイズは文脈から明らかになる。

【0 1 0 3】

任意の双線形群パラメータ

【数 2 1 9】

$$G = (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, g_1, g_2, e)$$

及び $g_T = e(g_1, g_2)$ での任意の $i=1, 2, T$ についてセキュリティパラメータを固定し、 g_i^M について

50

【数 2 2 0】

$$[[\mathbf{M}_i]]$$

と記述する。ここでし、累乗は要素毎である。括弧表記が使用される場合、群演算を
【数 2 2 1】

$$\boxplus$$

10

で表し、すなわち、行列
【数 2 2 2】

$$\mathbf{M}, \mathbf{N}$$

について
【数 2 2 3】

$$[[\mathbf{M}]]_i \boxplus [[\mathbf{N}]]_i = [[\mathbf{M} + \mathbf{N}]]_i$$

20

である。これらの負として
【数 2 2 4】

$$\boxminus$$

で表し、すなわち、
【数 2 2 5】

$$[[\mathbf{M}]]_i \boxminus [[\mathbf{N}]]_i = [[\mathbf{M} - \mathbf{N}]]_i$$

30

である。また、
【数 2 2 6】

$$\mathbf{N} \odot [[\mathbf{M}]]_i = [[\mathbf{NM}]]_i \text{ 及び } [[\mathbf{M}]]_i \odot \mathbf{N} = [[\mathbf{MN}]]_i$$

を定義する。また、表記をわずかに乱用し、グループ要素の行列の間のペアリングも示す
ために元のペアリング表記 e を使用する。すなわち、
【数 2 2 7】

40

$$e([[M]]_1, [[N]]_2) = [[MN]]_T$$

と記述する。
【0 1 0 4】
素数位数双線形群：
【数 2 2 8】

50

$$\mathbb{G}_1, \mathbb{G}_2 \text{ 及び } \mathbb{G}_T$$

を素数位数 $p = p(\lambda)$ の3つの巡回情報群とし、ここで、群演算は、セキュリティパラメータ λ において効率的に計算可能であり、 λ において効率的に計算できる

【数 2 2 9】

$$\mathbb{G}_1$$

10

と

【数 2 3 0】

$$\mathbb{G}_2$$

との間の同形は存在しない。 g_1 、 g_2 をそれぞれ

【数 2 3 1】

$$\mathbb{G}_1, \mathbb{G}_2$$

20

の生成子とし、

【数 2 3 2】

$$e: \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$$

を以下の特性を満たす効率的に計算可能なペアリング関数とする。

双線形性: 全ての

30

【数 2 3 3】

$$u \in \mathbb{G}_1, v \in \mathbb{G}_2 \text{ 及び } a, b \in \mathbb{Z}_p$$

について、 $e(u^a, v^b) = e(u, v)^{ab}$ が真である。

非退化:

【数 2 3 4】

$$e(g_1, g_2) \neq 1_{\mathbb{G}_T}$$

40

であり、

【数 2 3 5】

$$1_{\mathbb{G}_T}$$

は群

【数 2 3 6】

50

$$\mathbb{G}_T$$

の単位元である。

【0 1 0 5】

【数 2 3 7】

$$\mathcal{G}$$

10

を入力として 1^λ (セキュリティパラメータ λ の単項符号化) を取るアルゴリズムとし、非対称双線形群

【数 2 3 8】

$$G = (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, g_1, g_2, e)$$

の記述を出力する。

【0 1 0 6】

20

構成

【0 1 0 7】

ここで、素數位数双線形群における NC^1 構成のための MA-ABE を提示する。上記のように、各オーソリティは1つの属性のみを制御すると仮定し、したがって、「オーソリティ」及び「属性」という用語を交換可能に使用する。

【0 1 0 8】

$\text{GlobalSetup}(1^\lambda)$: グローバル設定アルゴリズムは、単項で符号化されたセキュリティパラメータ 1^λ を取り込む。この手順は、最初に素数 p を選択する。次に、位数 p の双線形群

【数 2 3 9】

30

$$G = (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, g_1, g_2, e)$$

を生成する。 g_1, g_2 をそれぞれ

【数 2 4 0】

$$\mathbb{G}_1, \mathbb{G}_2$$

40

の生成子とする。強力なシードランダム性抽出器

【数 2 4 1】

$$\text{Ext}: \mathbb{G}_T \times S \rightarrow \mathbb{M}$$

を利用し、

【数 2 4 2】

$$\mathbb{M} \subset \{0,1\}^*$$

50

はメッセージ空間であり、 $S \subset \{0, 1\}^*$ はシード空間である。アルゴリズムはシード $seed \leftarrow S$ をサンプリングする。次に、アルゴリズムは
【数 2 4 3】

$$\mathbf{A}_1, \mathbf{A}_2, \mathbf{A}_3 \leftarrow \mathbb{Z}_p^{3k \times k}, \mathbf{h} \leftarrow \mathbb{Z}_p^k$$

をサンプリングする。

【0 1 0 9】

【数 2 4 4】

10

$$(\mathbf{A}_1^* \parallel \mathbf{A}_2^* \parallel \mathbf{A}_3^*) = ((\mathbf{A}_1 \parallel \mathbf{A}_2 \parallel \mathbf{A}_3)^{-1})^\top$$

とし、ここで、

【数 2 4 5】

$$\mathbf{A}_1^*, \mathbf{A}_2^*, \mathbf{A}_3^* \leftarrow \mathbb{Z}_p^{3k \times k}$$

20

であり、全ての $i, j \in [3]$ について $i=j$ の場合、

【数 2 4 6】

$$\mathbf{A}_i^\top \mathbf{A}_j^* = \mathbf{I}$$

であり、 $i \neq j$ の場合、

【数 2 4 7】

$$\mathbf{0}$$

30

である。これはグローバルパラメータを

【数 2 4 8】

$$\text{GP} = (\mathbf{G}, [[\mathbf{A}_1]]_1, \mathbf{H} = [[\mathbf{A}_1^* \mathbf{h}]]_2, \text{seed})$$

として出力する。

【0 1 1 0】

さらに、全ての関係者がグローバル識別子

【数 2 4 9】

40

$$\text{GID} \in \mathcal{GID}$$

を

【数 2 5 0】

$$\mathbb{G}_2^{3k}$$

50

におけるランダムベクトルに写像するハッシュ関数
【数 2 5 1】

$$H : \{0,1\}^* \rightarrow \mathbb{G}_2^{3k}$$

にアクセスできると仮定する。すなわち、全ての
【数 2 5 2】

$$GID \in \mathcal{GID}$$

10

について、何らかの
【数 2 5 3】

$$\mathbf{h}_{GID} \leftarrow \mathbb{Z}_p^{3k}$$

に対して
【数 2 5 4】

20

$$H(GID) = [[\mathbf{h}_{GID}]]_2$$

を有する。

【0 1 1 1】

$\text{AuthSetup}(GP, u)$: グローバルパラメータ GP 及びオーソリティインデックス

【数 2 5 5】

$$u \in \mathcal{AU}$$

30

を与えると、アルゴリズムはランダム行列
【数 2 5 6】

$$\mathbf{W}_{A,u}, \mathbf{W}_{B,u} \in \mathbb{Z}_p^{3k \times 3k}$$

を選択し、

【数 2 5 7】

40

$$\text{PK}_u = (P_{A,u} = \mathbf{W}_{A,u}^\top \odot [[\mathbf{A}_1]]_1, P_{B,u} = \mathbf{W}_{B,u}^\top \odot [[\mathbf{A}_1]]_1)$$

$$= ([[\mathbf{W}_{A,u}^\top \mathbf{A}_1]], [[\mathbf{W}_{B,u}^\top \mathbf{A}_1]])_1$$

$$\text{MSK}_u = (\mathbf{W}_{A,u}, \mathbf{W}_{B,u})$$

50

を出力する。

【 0 1 1 2 】

$\text{Enc}(\text{GP}, \text{msg}, (\text{M}, \rho), \{\text{PK}_u\})$: 暗号化アルゴリズムは、入力としてグローバルパラメータ GP、暗号化するメッセージ

【数 2 5 8】

$$\text{msg} \in \mathbb{M}$$

、LSSSアクセス構造

10

【数 2 5 9】

$$(\mathbf{M}, \rho) \quad (\mathbf{M} = (M_{x,j})_{\ell \times d} = (\mathbf{M}_1, \dots, \mathbf{M}_\ell)^\top \in \mathbb{Z}_N^{\ell \times d} \text{ 且 } \rho: [\ell] \rightarrow \mathcal{AU})$$

、及び関連するオーソリティの公開鍵 $\{\text{PK}_u\}$ を取る。関数 ρ は

【数 2 6 0】

$$\mathbf{M}$$

20

(列ベクトルとして見なされる)の行をオーソリティに関連付ける(各オーソリティが単一の属性を制御すると仮定することを思い起こす)。 ρ は単射関数であり、すなわち、オーソリティ / 属性は

【数 2 6 1】

$$\mathbf{M}$$

の最大でも1つの行に関連付けられると仮定する。

【 0 1 1 3 】

30

最初にランダムベクトル

【数 2 6 2】

$$\mathbf{d} \leftarrow \mathbb{Z}_p^k$$

及びランダム行列

【数 2 6 3】

$$\mathbf{U}_A, \mathbf{U}_B \leftarrow \mathbb{Z}_p^{3k \times (d-1)}$$

40

をサンプリングする。この手順は、以下のように暗号文を生成する。各行 $x \in [l]$ について、ランダムベクトル

【数 2 6 4】

$$\mathbf{s}_{A,x}, \mathbf{s}_{B,x} \leftarrow \mathbb{Z}_p^k$$

を選択し、暗号文

50

【数 2 6 5】

$$CT = \left((M, \rho), C, \{C_{1,A,x}, C_{2,A,x}, C_{1,B,x}, C_{2,B,x}\}_{x \in [\ell]} \right)$$

を出力する。

【0 1 1 4】

ここで、

【数 2 6 6】

10

$$C = \text{msg} \oplus \text{Ext}(e([\mathbf{A}_1 \mathbf{d}]]_1, H), \text{seed})$$

であり、

【数 2 6 7】

$$C_{1,A,x} = [[\mathbf{A}_1]]_1 \odot \mathbf{s}_{A,x} = [[\mathbf{A}_1 \mathbf{s}_{A,x}]]_1$$

20

$$C_{2,A,x} = ([[\mathbf{A}_1]]_1 \odot \mathbf{d} \parallel [[\mathbf{U}_A]]_1) \odot \mathbf{M}_x + [[\mathbf{W}_{A,\rho(x)}^\top \mathbf{A}_1]]_1 \odot \mathbf{s}_{A,x}$$

$$= [[(\mathbf{A}_1 \mathbf{d} \parallel \mathbf{U}_A) \mathbf{M}_x + \mathbf{W}_{A,\rho(x)}^\top \mathbf{A}_1 \mathbf{s}_{A,x}]]_1$$

$$C_{1,B,x} = [[\mathbf{A}_1]]_1 \odot \mathbf{s}_{B,x} = [[\mathbf{A}_1 \mathbf{s}_{B,x}]]_1$$

$$C_{2,B,x} = ([[\mathbf{A}_1]]_1 \odot (-\mathbf{d}) \parallel [[\mathbf{U}_B]]_1) \odot \mathbf{M}_x + [[\mathbf{W}_{B,\rho(x)}^\top \mathbf{A}_1]]_1 \odot \mathbf{s}_{B,x}$$

30

$$= [[(-\mathbf{A}_1 \mathbf{d} \parallel \mathbf{U}_B) \mathbf{M}_x + \mathbf{W}_{B,\rho(x)}^\top \mathbf{A}_1 \mathbf{s}_{B,x}]]_1$$

である。

【0 1 1 5】

$\text{KeyGen}(\text{GP}, \text{GID}, \text{MSK}_u)$: 鍵生成アルゴリズムは、入力としてグローバルパラメータ G
 P 、ユーザのグローバル識別子

40

【数 2 6 8】

$$\text{GID} \in \mathcal{GID}$$

、及びオーソリティのマスター秘密鍵 MSK_u を取る。これは GID の秘密鍵 $\text{SK}_{\text{GID},u}$ を以下
 のように生成する。

【数 2 6 9】

50

$$\text{SK}_{\text{GID},u} = (K_{\text{GID},A,u}, K_{\text{GID},B,u})$$

ここで、

【数 2 7 0】

$$K_{\text{GID},A,u} = \mathbf{W}_{A,u} \odot (\text{H}(\text{GID}) \cdot H) = [[\mathbf{W}_{A,u} \cdot (\mathbf{h}_{\text{GID}} + \mathbf{A}_1^* \mathbf{h})]]_2$$

$$K_{\text{GID},B,u} = \mathbf{W}_{B,u} \odot \text{H}(\text{GID}) = [[\mathbf{W}_{B,u} \cdot \mathbf{h}_{\text{GID}}]]_2$$

10

である。

【0 1 1 6】

$\text{Dec}(\text{GP}, \text{CT}, \text{GID}, \{\text{SK}_{\text{GID},u}\})$: 復号は、グローバルパラメータ GP、LSSS アクセス構造

【数 2 7 1】

$$(\mathbf{M}, \rho)$$

20

についての暗号文 CT(

【数 2 7 2】

$$\mathbf{M} \in \mathbb{Z}_N^{\ell \times d} \text{ 且 } \rho: [\ell] \rightarrow \mathcal{AU} \text{ 単射}$$

)、ユーザのグローバル識別子

【数 2 7 3】

$$\text{GID} \in \mathcal{GID}$$

30

、及びインデックス $I \subseteq [l]$ を有する

【数 2 7 4】

$$\mathbf{M}$$

の行のサブセットに対応する秘密鍵 $\{\text{SK}_{\text{GID},u}\}_{u \in \rho(I)}$ を入力として取る。 $(1, 0, \dots, 0)$ が
これらの行のスパン

40

【数 2 7 5】

$$\mathbf{M}_I$$

にない場合、復号は失敗する。そうでない場合、復号器は、

【数 2 7 6】

50

$$(1,0,\dots,0) = \sum_{x \in I} w_x \cdot \mathbf{M}_x^\top$$

となるような $\{w_x \in \mathbb{N}\}_{x \in I}$ を見つける。

【 0 1 1 7 】

全ての $x \in I$ について、まず、復号アルゴリズムは、

【 数 2 7 7 】

$$D_{A,x} = e(C_{2,A,x}, [[\mathbf{h}_{\text{GID}} + \mathbf{A}_1^* \mathbf{h}]]_2) e(C_{1,A,x}, K_{\text{GID},A,\rho(x)})^{-1} \quad 10$$

$$= [[((\mathbf{A}_1 \mathbf{d} \parallel \mathbf{U}_A) \mathbf{M}_x)^\top \cdot (\mathbf{h}_{\text{GID}} + \mathbf{A}_1^* \mathbf{h})]]_2$$

$$D_{B,x} = e(C_{2,B,x}, [[\mathbf{h}_{\text{GID}}]]_2) e(C_{1,B,x}, K_{\text{GID},B,\rho(x)})^{-1} = [[((- \mathbf{A}_1 \mathbf{d} \parallel \mathbf{U}_B) \mathbf{M}_x)^\top \cdot \mathbf{h}_{\text{GID}}]]_2$$

を計算する。次いで、

【 数 2 7 8 】

20

$$D = \prod_{x \in I} (D_{A,x} \cdot D_{B,x})^{w_x} = e([[\mathbf{A}_1 \mathbf{d}]]_1, H)$$

を計算し、最後に

【 数 2 7 9 】

$$C \oplus \text{Ext}(D, \text{seed}) = \text{msg} \quad 30$$

を出力する。

【 0 1 1 8 】

システム実装

【 0 1 1 9 】

図 1 を参照すると、分散型マルチオーソリティの属性ベース暗号化スキームのシステムアーキテクチャの例が示されている。任意のデータのようなメッセージの所有者 105 は、ここで説明するようにメッセージを暗号化し、得られた暗号文をクラウドストレージ 110 に格納できる。アクセサ 115 として示されている他のユーザは、クラウドストレージ 110 からこの暗号文を取得してもよい。公開鍵及び秘密鍵を管理するために、複数のオーソリティ 120 がインスタンス化されてもよい。オーソリティ 120 は、秘密鍵をデータ所有者 105 に配布し、秘密鍵をアクセサ 115 に配布してもよい。ここで説明するように、ユーザは、必要なオーソリティから少なくとも所定数の属性を有する場合にのみ、暗号文を復号できる。

【 0 1 2 0 】

図 2 を参照すると、分散型マルチオーソリティの属性ベース暗号化スキームのシーケンス図の例が示されている。任意のデータがクラウド 201 に格納されてもよい。データ所有者 202 によって、データがクラウドにアップロードされていてもよい。その後、ユーザ 203 はクラウド 201 からデータを取得したいと考えてもよい。ユーザ 203 は最初にフ

40

50

ファイルの詳細を閲覧し、オーソリティ204から鍵を要求してもよい。ここでは単一のオーソリティ204のみが示されているが、複数のオーソリティがインスタンス化でき、ユーザは複数のオーソリティと通信してもよい。

【0121】

図3及び図4は、本開示に記載の様々な実施形態を実装するために有用なコンピュータシステムの例を示す。様々な実施形態は、例えば、図3に示すコンピュータシステム500のような1つ以上のコンピュータシステムを使用して実装されてもよい。1つ以上のコンピュータシステム500は、例えば、ここで議論されている実施形態のいずれか並びにこれらの組み合わせ及びサブコンビネーションを実装するために使用されてもよい。

【0122】

コンピュータシステム500は、プロセッサ504のような1つ以上のプロセッサ(中央処理装置、処理デバイス又はCPUとも呼ばれる)を含んでもよい。プロセッサ504は、通信インフラストラクチャ506(例えば、バス等)に接続されてもよい。

【0123】

コンピュータシステム500はまた、モニタ、キーボード、ポインティングデバイス等のようなユーザ入出力デバイス503を含んでもよく、これらはユーザ入出力インタフェース502を介して通信インフラ506と通信してもよい。プロセッサ504の1つ以上は、グラフィックス処理装置(GPU, graphics processing unit)でもよい。一実施形態では、GPUは、数学集約的なアプリケーションを処理するように設計された特殊な電子回路であるプロセッサでもよい。GPUは、コンピュータグラフィックスアプリケーション、画像、ビデオ等に共通の数学集約的なデータのように、大きいデータのブロックの並列処理に効率的となる並列構造を有してもよい。

【0124】

コンピュータシステム500はまた、ランダムアクセスメモリ(RAM, random-access memory)のようなメインメモリ508を含んでもよい。メインメモリ508は、1つ以上のレベルのキャッシュを含んでもよい。メインメモリ508は、制御ロジック(すなわち、コンピュータソフトウェア、命令等)及び/又はデータを格納しておいてもよい。コンピュータシステム500はまた、1つ以上の二次ストレージデバイス又は二次メモリ510を含んでもよい。二次メモリ510は、例えば、ハードディスクドライブ512及び/又は取り外し可能ストレージデバイス若しくは取り外し可能ストレージドライブ514を含んでもよい。取り外し可能ストレージドライブ514は、取り外し可能ストレージユニット518と相互作用してもよい。取り外し可能ストレージユニット518は、コンピュータソフトウェア(制御ロジック)及び/又はデータを格納したコンピュータ使用可能又は読み取り可能なストレージデバイスを含んでもよい。取り外し可能ストレージドライブ514は、取り外し可能ストレージユニット518に対して読み書きしてもよい。

【0125】

二次メモリ510は、コンピュータプログラム及び/又は他の命令及び/又はデータがコンピュータシステム500によってアクセスできるようにするための、他の手段、デバイス、コンポーネント、機器又は他のアプローチを含んでもよい。このような手段、デバイス、コンポーネント、機器又は他のアプローチは、例えば、取り外し可能ストレージユニット522及びインタフェース520を含んでもよい。取り外し可能ストレージユニット522及びインタフェース520の例は、プログラムカートリッジ及びカートリッジインタフェース、取り外し可能メモリチップ(EPROM又はPROM等)及び関連するソケット、メモリスティック及びUSBポート、メモリカード及び関連するメモリカードスロット、及び/又は他の取り外し可能ストレージユニット及び関連するインタフェースを含んでもよい。

【0126】

コンピュータシステム500は、通信インタフェース524(例えば、ネットワークインタフェース)を更にも含んでもよい。通信インタフェース524は、コンピュータシステム500が外部デバイス、外部ネットワーク、外部エンティティ等(個別に、また、まとめてリモートデバイス、ネットワーク、エンティティ528と呼ばれる)の任意の組み合わせと通信

10

20

30

40

50

して相互作用することを可能にしてもよい。例えば、通信インタフェース524は、コンピュータシステム500が通信経路526を介して外部又はリモートデバイス、ネットワーク、エンティティ528と通信することを可能にしてもよい。通信経路526は、有線及び/又は無線(又はこれらの組み合わせ)でもよく、LAN、WAN、インターネット等の任意の組み合わせを含んでもよい。制御ロジック及び/又はデータは、通信経路526を介してコンピュータシステム500との間で送受信されてもよい。

【0127】

コンピュータシステム500はまた、いくつかの非限定的な例を挙げると、携帯情報端末(PDA, personal digital assistant)、デスクトップワークステーション、ラップトップコンピュータ若しくはノートブックコンピュータ、ネットブック、タブレット、スマートフォン、スマートウォッチ若しくは他のウェアラブルデバイス、アプライアンス、モノのインターネットの一部及び/又は組み込みシステムのいずれかでもよく、或いは、これらの任意の組み合わせでもよい。

【0128】

コンピュータシステム500は、リモート又は分散クラウドコンピューティングソリューション、ローカル又はオンプレミスソフトウェア(「オンプレミス」クラウドベースソリューション)、「サービスとして」のモデル(例えば、サービスとしてのコンテンツ(CaaS, content as a service)、サービスとしてのデジタルコンテンツ(DCaaS, digital content as a service)、サービスとしてのソフトウェア(SaaS, software as a service)、サービスとしての管理ソフトウェア(MSaaS, managed software as a service)、サービスとしてのプラットフォーム(PaaS, platform as a service)、サービスとしてのデスクトップ(DaaS, desktop as a service)、サービスとしてのフレームワーク(FaaS, framework as a service)、サービスとしてのバックエンド(BaaS, backend as a service)、サービスとしてのモバイルバックエンド(MBaaS, mobile backend as a service)、サービスとしてのインフラストラクチャ(IaaS, infrastructure as a service)等)、及び/又は上記の例の任意の組み合わせを含むハイブリッドモデル又は他のサービス若しくは配信パラダイムを含むがこれらに限定されない、任意の配信パラダイムを通じて任意のアプリケーション及び/又はデータにアクセス又はホストする、クライアント又はサーバコンピューティングデバイスでもよい。

【0129】

図4は、コンピュータシステム900のマシンの例を示しており、その中で、ここで説明する操作のいずれか1つ以上をマシンに実行させるための命令のセットが実行されてもよい。別の実装では、マシンはLAN、イントラネット、エクストラネット及び/又はインターネット内の他のマシンに接続(例えば、ネットワーク接続)されてもよい。マシンは、クライアントサーバネットワーク環境におけるサーバ又はクライアントマシンとして動作してもよく、ピアツーピア(又は分散)ネットワーク環境におけるピアマシンとして動作してもよく、或いは、クラウドコンピューティングインフラストラクチャ又は環境におけるサーバ又はクライアントマシンとして動作してもよい。

【0130】

マシンは、パーソナルコンピュータ(PC, personal computer)、タブレットPC、セットトップボックス(STB, set-top box)、携帯情報端末(PDA)、携帯電話、ウェブアプライアンス、サーバ、ネットワークルータ、スイッチ若しくはブリッジ、専用アプリケーション若しくはネットワークセキュリティアプライアンス若しくはデバイス、又はそのマシンによって実行されるアクションを指定する命令のセット(シーケンシャル等)を実行できる任意のマシンでもよい。さらに、単一のマシンが例示されているが、「マシン」という用語はまた、ここで議論されている方法論のいずれか1つ以上を実行するための命令のセット(又は複数のセット)を個別に又は共同で実行するマシンの任意の集合を含むものとする。

【0131】

コンピュータシステム900の例は、バス930を介して通信する、処理デバイス902、メインメモリ904(例えば、読み取り専用メモリ(ROM, read-only memory)、フラッシュメモリ、シンクロナスDRAM(SDRAM, synchronous DRAMのようなダイナミックランダムアクセスメモリ(DRAM, dynamic random-access memory)等)、スタティックメモリ906(例えば、フラッシュメモリ、スタティックランダムアクセスメモリ(SRAM, static random-access memory)等)及びデータストレージデバイス918を含む。

【0132】

処理デバイス902は、マイクロプロセッサ、中央処理装置等のような1つ以上の処理デバイスを表す。より具体的には、処理デバイスは、複合命令セットコンピューティング(CISC, complex instruction set computing)マイクロプロセッサ、縮小命令セットコンピューティング(RISC, reduced instruction set computing)マイクロプロセッサ、超長命令語(VLIW, very long instruction word)マイクロプロセッサ、又は他の命令セットを実装するプロセッサ、又は命令セットの組み合わせを実装するプロセッサでもよい。処理デバイス902は、特定用途向け集積回路(ASIC, application-specific integrated circuit)、フィールドプログラマブルゲートアレイ(FPGA, field-programmable gate array)、デジタルシグナルプロセッサ(DSP, digital signal processor)、ネットワークプロセッサ等のような1つ以上の特殊用途の処理デバイスでもよい。処理デバイス902は、ここで説明する動作及びステップを実行するための命令926を実行するように構成される。

【0133】

コンピュータシステム900は、ネットワーク920を介して通信するためのネットワークインタフェースデバイス908を更に含んでもよい。コンピュータシステム900はまた、ビデオディスプレイユニット910、英数字入力デバイス912(例えば、キーボード)、カーソル制御デバイス914(例えば、マウス)、グラフィックス処理装置922、信号生成デバイス916(例えば、スピーカ)、グラフィックス処理装置922、ビデオ処理装置928及びオーディオ処理装置932を含んでもよい。

【0134】

データストレージデバイス918は、ここで説明する動作のいずれか1つ以上を具体化する1つ以上の命令のセット926(例えば、ソフトウェア命令)が格納される機械可読媒体924(コンピュータ可読記憶媒体としても知られる)を含んでもよい。命令926はまた、コンピュータシステム900による実行中に、完全に又は少なくとも部分的にメインメモリ904内及び/又は処理デバイス902内に存在してもよく、ここで、メインメモリ904及び処理デバイス902も機械可読記憶媒体を構成する。

【0135】

一例では、命令926は、本開示の主題に対応する動作及び機能を実装するための命令を含む。機械可読記憶媒体924は、実装例において単一の媒体であると示されているが、「機械可読記憶媒体」という用語は、1つ以上の命令のセット926を格納する単一の媒体又は複数の媒体(例えば、集中型若しくは分散型データベース及び/又は関連するキャッシュ及びサーバ)を含むものとして理解されるべきである。「機械可読記憶媒体」という用語は、マシンによる実行のために命令のセット926を格納又は符号化することができ、かつ、マシンに本開示の動作のいずれか1つ以上を実行させる媒体も含むものとして理解されるべきである。したがって、「機械可読記憶媒体」という用語は、固体メモリ、光媒体及び磁気媒体を含むが、これらに限定されないものとする。

【0136】

詳細な説明の一部は、コンピュータメモリ内のデータビットに対する操作のアルゴリズム及び記号表現の観点から提示されている。これらのアルゴリズム記述及び表現は、データ処理技術の当業者が、その分野の他の当業者に自分の研究の内容を最も効果的に伝えるために使用する方法である。ここでは一般的に、アルゴリズムは、所望の結果をもたらす首尾一貫した動作のシーケンスであると考えられる。動作は、物理量の物理的操作を必要

とするものである。必ずしもそうではないが、通常では、これらの量は、格納、結合、比較及び他の操作が可能な電気信号又は磁気信号の形式を取る。これらの信号をビット、値、要素、記号、文字、用語、数字等として参照することは、主に一般的な用法の理由から場合によっては便利であることが証明されている。

【0137】

しかし、これらの用語及び同様の用語の全ては適切な物理量に関連付けられており、これらの量に適用される単なる便宜的なラベルであることに留意する必要がある。特に明記されていない限り、上記の説明から明らかなように、説明の全体を通して、「識別する」、「決定する」、「実行する」、「行う」、「収集する」、「作成する」、「送信する」等のような用語を利用した説明は、コンピュータシステムのレジスタ及びメモリ内の物理(電子)量として表されるデータを、コンピュータシステムのメモリ若しくはレジスタ又は他のこのような情報ストレージデバイス内の物理量として同様に表される他のデータに操作して変換する、コンピュータシステム又は同様の電子計算デバイスのアクション及びプロセスを示すことが認識される。

10

【0138】

本開示はまた、ここでの動作を実行するための装置に関する。この装置は、意図した目的のために特別に構成されてもよく、或いは、コンピュータに格納されたコンピュータプログラムによって選択的に起動又は再構成されるコンピュータを含んでもよい。このようなコンピュータプログラムは、それぞれコンピュータシステムバスに結合された、フロッピーディスク、光ディスク、CD-ROM及び光磁気ディスクを含む任意の種類のディスク、読み取り専用メモリ(ROM)、ランダムアクセスメモリ(RAM)、EPROM、EEPROM、磁気カード若しくは光学カード、又は電子命令を格納するのに適した任意の種類の媒体のような、これらに限定されないコンピュータ可読記憶媒体に格納されてもよい。

20

【0139】

ここに示す動作及び例は、特定のコンピュータ又は他の装置に本質的に関連するものではない。様々な種類のシステムが、ここに示す教示に従ってプログラムとともに使用されてもよく、或いは、動作を実行するためのより特殊な装置を構築するのに便利であることが証明されてもよい。これらの様々なシステムの構造は、ここでの説明に記載されるように現れる。さらに、本開示は、特定のプログラミング言語を参照して記載されてない。ここで説明する本開示の教示を実装するために、様々なプログラミング言語が使用されてもよいことが認識される。

30

【0140】

本開示は、命令を格納した機械可読媒体を含んでもよいコンピュータプログラム製品又はソフトウェアとして提供されてもよく、本開示に従ったプロセスを実行するようにコンピュータシステム(又は他の電子デバイス)をプログラムするために使用されてもよい。機械可読媒体は、機械(例えば、コンピュータ)によって読み取り可能な形式で情報を格納する任意のメカニズムを含む。例えば、機械可読(例えば、コンピュータ可読)媒体は、読み取り専用メモリ(「ROM」)、ランダムアクセスメモリ(「RAM」)、磁気ディスク記憶媒体、光記憶媒体、フラッシュメモリデバイス等のような機械(例えば、コンピュータ)可読記憶媒体を含む。

40

【0141】

いくつかの実施形態では、制御ロジック(ソフトウェア)を格納した有形の非一時的なコンピュータ使用可能又は読み取り可能な媒体を含む有形の非一時的な装置又は製造物はまた、ここではコンピュータプログラム製品又はプログラム記憶デバイスとも呼ばれる。これは、コンピュータシステム500、メインメモリ508、二次メモリ510、取り外し可能ストレージユニット518及び522、並びに上記の任意の組み合わせを具体化する有形の製造物を含むが、これらに限定されない。このような制御ロジックは、1つ以上のデータ処理デバイス(コンピュータシステム500等)によって実行された場合、このようなデータ処理デバイスにここで説明するように動作させてもよい。

【0142】

50

本開示に含まれる教示に基づいて、図3及び図4に示すもの以外のデータ処理デバイス、コンピュータシステム及び/又はコンピュータアーキテクチャを使用して、どのように本開示の実施形態を作成して使用するかは、関連分野の当業者に明らかになる。特に、実施形態は、個々に記載しているもの以外のソフトウェア、ハードウェア及び/又はオペレーティングシステムの実装で動作させることができる。

【0143】

他の節ではなく、詳細な説明の節は、特許請求の範囲を解釈するために使用されることを意図していることが分かる。他の節は、発明者によって考案された1つ以上の実施形態を示すことができるが、全てを示すことはできない。したがって、本開示又は特許請求の範囲を限定することを意図するものではない。

10

【0144】

本開示は、例示的な分野及び用途のための例示的な実施形態を記載しているが、本開示がその内容に限定されないことが理解されるべきである。他の実施形態及びそれに対する修正は可能であり、本開示の範囲及び真意内にある。例えば、この段落の一般性を制限することなく、実施形態は、ここに記載の図に示すソフトウェア、ハードウェア、ファームウェア及び/又はエンティティに限定されない。さらに、実施形態は(ここに明示的に記載されているかどうかにかかわらず)、ここに記載の例以外の分野及び用途に対しても相当な有用性を有する。

【0145】

指定の機能及びその関係の実装を示す機能的な構成ブロックを用いて、ここに実施形態が記載されている。これらの機能的な構成ブロックの境界は、説明の便宜上でここでは任意に定義されている。指定の機能及び関係(又はそれに相当するもの)が適切に実行される限り、別の境界が定義できる。また、代替実施形態は、機能ブロック、ステップ、動作、方法等を、ここに記載の順序とは異なる順序を用いて実行できる。

20

【0146】

ここでの「一実施形態」、「実施形態」、「例示的な実施形態」又は同様の語句は、記載される実施形態が特定の特徴、構造又は特性を含むことができるが、全ての実施形態が特定の特徴、構造又は特性を含むとは限らないことを示す。さらに、このような語句は必ずしも同じ実施形態を示しているとは限らない。さらに、特定の特徴、構造、特性が実施形態に関連して記載される場合、このような特徴、構造又は特性を他の実施形態に組み込むことは、ここに明示的に言及又は記載されていなくても、関連分野の当業者の認識範囲内にある。さらに、いくつかの実施形態は、「結合される」及び「接続される」という表現をその派生語とともに使用して記述されることがある。これらの用語は、必ずしも互いに同義語を意図するものではない。例えば、いくつかの実施形態は、2つ以上の要素が互いに物理的又は電氣的に直接接触していることを示すために、「接続される」及び/又は「結合される」という用語を使用して記述することができる。しかし、「結合される」という用語は、2つ以上の要素が互いに直接接触していないが、それでも互いに協力又は相互作用することを意味することができる。

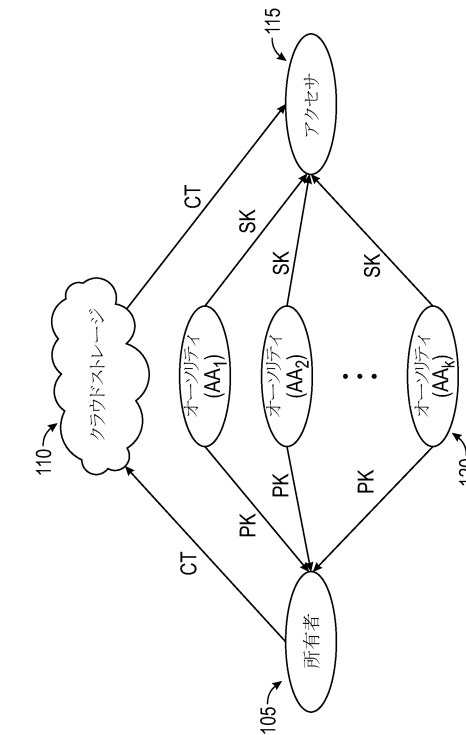
30

【0147】

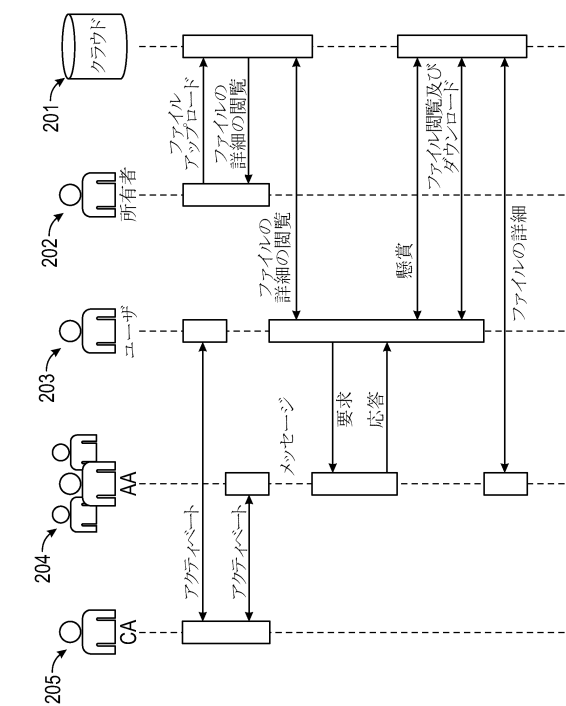
本開示の外延及び範囲は、上記の例示的な実施形態のいずれかによって限定されるべきではなく、以下の特許請求の範囲及びこれらの均等物に従ってのみ定義されるべきである。上記の明細書において、本開示の実装は、その具体的な実装例を参照して記載されている。以下の特許請求の範囲に記載のように、本開示のより広い真意及び範囲から逸脱することなく、様々な修正が加えられてもよいことは明らかである。したがって、明細書及び図面は、限定的な意味ではなく、例示的な意味で考慮されるべきである。

40

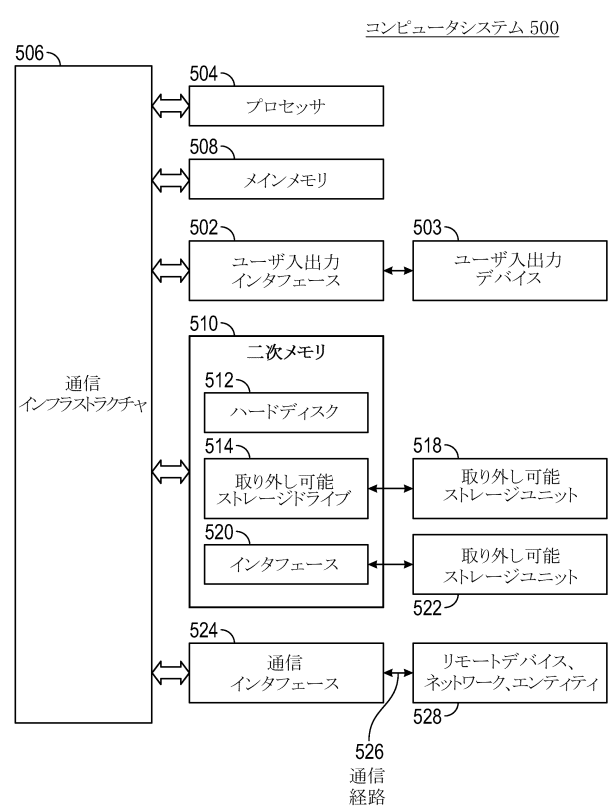
【図面】
【図 1】



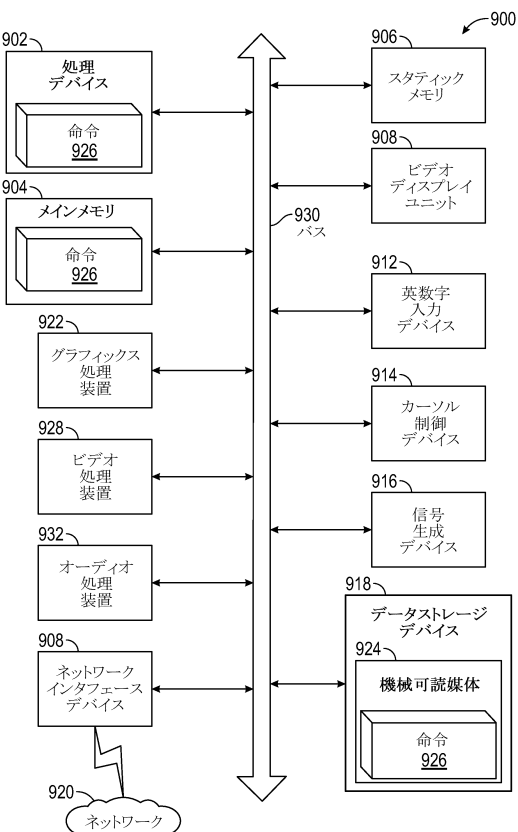
【図 2】



【図 3】



【図 4】



10

20

30

40

50

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US 22/28173

A. CLASSIFICATION OF SUBJECT MATTER

IPC - INV. H04L 9/08; ADD. H04L 9/30, H04L 9/08 (2022.01)

CPC - INV. H04L 9/085; ADD. H04L 9/30, H04L 9/088, H04L 2209/46

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)

See Search History document

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

See Search History document

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

See Search History document

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2013/0339754 A1 (Takashima et al.) 19 December 2013 (19.12.2013) entire document (especially para [0179], [0189]-[0194], [0255]-[0256])	1-12
A	US 2010/0185861 A1 (Chase et al.) 22 July 2010 (22.07.2010) entire document (especially para [0022])	1-12
A	US 2018/0054301 A1 (KING FAHD UNIVERSITY OF PETROLEUM AND MINERALS) 22 February 2018 (22.02.2018) entire document (especially para [0010])	1-12
A	US 2020/0336292 A1 (NEC Laboratories Europe GmbH) 22 October 2020 (22.10.2020) entire document (especially para [0020], [0022], [0070])	1-12
A	US 2019/0230094 A1 (KONINKLIJKE PHILIPS N.V.) 25 July 2019 (25.07.2019) entire document	1-12
A	US 9,209,974 B1 (Zeutro LLC) 08 December 2015 (08.12.2015) entire document	1-12

☒ 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

"D" document cited by the applicant in the international application

"E" earlier application or patent but 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

09 August 2022

Date of mailing of the international search report

SEP 08 2022

Name and mailing address of the ISA/US

Mail Stop PCT, Attn: ISA/US, Commissioner for Patents
P.O. Box 1450, Alexandria, Virginia 22313-1450
Facsimile No. 571-273-8300

Authorized officer

Karl Rodriguez

Telephone No. PCT Helpdesk: 571-272-4300

Form PCT/ISA/210 (second sheet) (July 2019)

INTERNATIONAL SEARCH REPORT		International application No. PCT/US 22/26173
C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	Shynu, P. G., and K. John Singh. "Privacy preserving secret key extraction protocol for multi-authority attribute-based encryption techniques in cloud computing." International Journal of Embedded Systems 10.4 (2018): 287-300. [Retrieved on 09 August 2022] Retrieved from the Internet<URL: https://www.researchgate.net/profile/K-Singh-8/publication/326593906_Privacy_preserving_secret_key_extraction_protocol_for_multi-authority_attribute-based_encryption_techniques_in_cloud_computing/links/5d3fd10d92851cd04691f57e/Privacy-preserving-secret-key-extraction-protocol-for-multi-authority-attribute-based-encryption-techniques-in-cloud-computing.pdf > entire document	1-12

Form PCT/ISA/210 (continuation of second sheet) (July 2019)

10

20

30

40

50

フロントページの続き

MK,MT,NL,NO,PL,PT,RO,RS,SE,SI,SK,SM,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,KM,ML,MR,N
E,SN,TD,TG),AE,AG,AL,AM,AO,AT,AU,AZ,BA,BB,BG,BH,BN,BR,BW,BY,BZ,CA,CH,CL,CN,CO,CR,CU,
CZ,DE,DJ,DK,DM,DO,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,GT,HN,HR,HU,ID,IL,IN,IR,IS,IT,JM,JO,J
P,KE,KG,KH,KN,KP,KR,KW,KZ,LA,LC,LK,LR,LS,LU,LY,MA,MD,ME,MG,MK,MN,MW,MX,MY,MZ,N
A,NG,NI,NO,NZ,OM,PA,PE,PG,PH,PL,PT,QA,RO,RS,RU,RW,SA,SC,SD,SE,SG,SK,SL,ST,SV,SY,TH,TJ,
TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC,VN,WS,ZA,ZM,ZW

ライブ 940

- (72)発明者 コマルゴドスキー イラン
アメリカ合衆国 カリフォルニア州 94085 サニーベール スチュワート ドライブ 940
- (72)発明者 ウォーターズ ブレント
アメリカ合衆国 カリフォルニア州 94085 サニーベール スチュワート ドライブ 940