(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4869824号
(P4869824)
(45)発行日　平成24年2月8日(2012.2.8)　(24)登録日　平成23年11月25日(2011.11.25)

(51)Int.Cl.　F I
H04L 9/08 (2006.01)　H04L 9/00 601D

請求項の数 16 (全 83 頁)

(21)出願番号　特願2006-215267(P2006-215267)
(22)出願日　平成18年8月8日(2006.8.8)
(65)公開番号　特開2008-42590(P2008-42590A)
(43)公開日　平成20年2月21日(2008.2.21)
審査請求日　平成21年5月20日(2009.5.20)

(73)特許権者　000006013
三菱電機株式会社
東京都千代田区丸の内二丁目７番３号
(74)代理人　100099461
弁理士　溝井　章司
(72)発明者　高島　克幸
東京都千代田区丸の内二丁目７番３号　三菱電機株式会社内

審査官　中里　裕正

最終頁に続く

(54)【発明の名称】受信者装置及び送信者装置及び暗号通信システム及びプログラム

(57)【特許請求の範囲】
【請求項１】
情報を記憶する記憶装置と、
情報を処理する処理装置と、
送信者装置が送信した情報を受信する受信装置と、
上記記憶装置を用いて、加法群G_2の要素d_{ID}を示す情報をユーザ秘密鍵情報として記憶する秘密鍵記憶部と、
上記受信装置を用いて、送信者装置が送信した暗号化セッション鍵を受信し、上記処理装置を用いて、受信した暗号化セッション鍵に含まれる加法群G_1の要素Ｒを示す情報を第四要素情報として出力する暗号化セッション鍵受信部と、
上記処理装置を用いて、上記秘密鍵記憶部が記憶したユーザ秘密鍵情報と上記暗号化セッション鍵受信部が出力した第四要素情報とを入力し、上記処理装置を用いて、入力したユーザ秘密鍵情報と第四要素情報とに基づいて、加法群G_1の要素Ｒと加法群G_2の要素d_{ID}とのペアリング値を算出して乗法群G_Tの要素ｗ’とし、上記処理装置を用いて、算出した乗法群G_Tの要素ｗ’を示す情報を受信ペアリング値情報として出力する受信ペアリング値算出部と、
上記処理装置を用いて、上記暗号化セッション鍵受信部が出力した第四要素情報と上記受信ペアリング値算出部が出力した受信ペアリング値情報とを入力し、上記処理装置を用いて、入力した第四要素情報と受信ペアリング値情報とに基づいて、ハッシュ値を算出し、上記処理装置を用いて、算出したハッシュ値に基づいて、送信者装置が生成したセッシ

ョン鍵と同一のセッション鍵を復元するセッション鍵復元部と、
を有することを特徴とする受信者装置。
【請求項２】
情報を記憶する記憶装置と、
情報を処理する処理装置と、
受信者装置に対して情報を送信する送信装置と、
上記記憶装置を用いて、加法群G_1の要素P_1を示す情報を第一要素情報として記憶する第一要素記憶部と、
上記記憶装置を用いて、加法群G_1の要素P_{pub}を示す情報を第二要素情報として記憶する第二要素記憶部と、
上記処理装置を用いて、上記第一要素記憶部が記憶した第一要素情報と自然数ｒを示す乱数情報とを入力し、上記処理装置を用いて、入力した第一要素情報と乱数情報とに基づいて、加法群G_1の要素Ｒを算出し、上記処理装置を用いて、算出した加法群G_1の要素Ｒを示す情報を第四要素情報として出力する第四要素算出部と、
上記処理装置を用いて、受信者装置を識別する識別情報を入力し、上記処理装置を用いて、入力した識別情報に対応する加法群G_2の要素Q_{ID}を算出し、上記処理装置を用いて、算出した加法群G_2の要素Q_{ID}を示す情報を第五要素情報として出力する第五要素算出部と、
上記処理装置を用いて、上記第二要素記憶部が記憶した第二要素情報と上記第五要素算出部が出力した第五要素情報と上記乱数情報とを入力し、上記処理装置を用いて、入力した第二要素情報と第五要素情報とに基づいて、加法群G_1の要素P_{pub}と加法群G_2の要素Q_{ID}とのペアリング値を算出し、上記処理装置を用いて、算出したペアリング値と入力した乱数情報とに基づいて、乗法群G_Tの要素ｗを算出し、上記処理装置を用いて、算出した乗法群G_Tの要素ｗを示す情報を送信ペアリング値情報として出力する送信ペアリング値算出部と、
上記処理装置を用いて、上記第四要素算出部が出力した第四要素情報と上記送信ペアリング値算出部が出力した送信ペアリング値情報とを入力し、上記処理装置を用いて、入力した第四要素情報と送信ペアリング値情報とに基づいて、ハッシュ値を算出し、上記処理装置を用いて、算出したハッシュ値に基づいて、セッション鍵を生成するセッション鍵生成部と、
上記処理装置を用いて、上記第四要素算出部が出力した第四要素情報を入力し、上記送信装置を用いて、入力した第四要素情報を含む情報を暗号化セッション鍵として受信者装置に対して送信する暗号化セッション鍵送信部と、
を有することを特徴とする送信者装置。
【請求項３】
情報を記憶する記憶装置と、
情報を処理する処理装置と、
受信者装置に対して情報を送信する送信装置と、
上記記憶装置を用いて、加法群G_1の要素P_1を示す情報を第一要素情報として記憶する第一要素記憶部と、
上記記憶装置を用いて、加法群G_1の要素P_{pub}を示す情報を第二要素情報として記憶する第二要素記憶部と、
上記処理装置を用いて、上記第一要素記憶部が記憶した第一要素情報と自然数ｒを示す乱数情報とを入力し、上記処理装置を用いて、入力した第一要素情報と乱数情報とに基づいて、加法群G_1の要素Ｒを算出し、上記処理装置を用いて、算出した加法群G_1の要素Ｒを示す情報を第四要素情報として出力する第四要素算出部と、
上記処理装置を用いて、受信者装置を識別する識別情報を入力し、上記処理装置を用いて、入力した識別情報に対応する加法群G_2の要素Q_{ID}を算出し、上記処理装置を用いて、算出した加法群G_2の要素Q_{ID}を示す情報を第五要素情報として出力する第五要素算出部と、

上記処理装置を用いて、上記第二要素記憶部が記憶した第二要素情報と上記第五要素算出部が出力した第五要素情報と上記乱数情報とを入力し、上記処理装置を用いて、入力した第二要素情報と第五要素情報とに基づいて、加法群G_1の要素P_{pub}と加法群G_2の要素Q_{ID}とのペアリング値を算出し、上記処理装置を用いて、算出したペアリング値と入力した乱数情報とに基づいて、乗法群G_Tの要素wを算出し、上記処理装置を用いて、算出した乗法群G_Tの要素wを示す情報を送信ペアリング値情報として出力する送信ペアリング値算出部と、

上記処理装置を用いて、上記第四要素算出部が出力した第四要素情報と上記送信ペアリング値算出部が出力した送信ペアリング値情報とを入力し、上記処理装置を用いて、入力した第四要素情報と送信ペアリング値情報とに基づいて、ハッシュ値を算出し、上記処理装置を用いて、算出したハッシュ値に基づいて、受信者装置がセッション鍵を復元するために用いるマスク情報を生成し、上記処理装置を用いて、生成したマスク情報を出力するセッション鍵生成部と、

上記処理装置を用いて、上記第四要素算出部が出力した第四要素情報と、上記セッション鍵生成部が出力したマスク情報とを入力し、上記送信装置を用いて、入力した第四要素情報とマスク情報とを含む情報を暗号化セッション鍵として受信者装置に対して送信する暗号化セッション鍵送信部と、

を有することを特徴とする送信者装置。

【請求項４】

情報を処理する処理装置と、

上記処理装置を用いて、加法群G_1の要素P_1を選択し、上記処理装置を用いて、選択した加法群G_1の要素P_1を示す情報を第一要素情報として出力する第一要素選択部と、

上記処理装置を用いて、自然数ｓを選択し、上記処理装置を用いて、選択した自然数ｓを示す情報をマスターキー情報として出力するマスターキー選択部と、

上記処理装置を用いて、上記第一要素選択部が出力した第一要素情報と上記マスターキー選択部が出力したマスターキー情報とを入力し、上記処理装置を用いて、入力した第一要素情報とマスターキー情報とに基づいて、加法群G_1の要素P_{pub}を算出し、上記処理装置を用いて、算出した加法群G_1の要素P_{pub}を示す情報を第二要素情報として出力する第二要素算出部と、

上記処理装置を用いて、上記第一要素選択部が出力した第一要素情報と上記第二要素算出部が出力した第二要素情報とを入力し、上記処理装置を用いて、入力した第一要素情報と第二要素情報とを含む情報をパラメータ情報として公開するパラメータ公開部と、

上記処理装置を用いて、受信者装置を識別する識別情報を入力し、上記処理装置を用いて、入力した識別情報に対応する加法群G_2の要素Q_{ID}を算出し、上記処理装置を用いて、算出した加法群G_2の要素Q_{ID}を示す情報を第三要素情報として出力する第三要素算出部と、

上記処理装置を用いて、上記第三要素算出部が出力した第三要素情報と上記マスターキー選択部が出力したマスターキー情報とを入力し、上記処理装置を用いて、入力した第三要素情報とマスターキー情報とに基づいて、加法群G_2の要素d_{ID}を算出し、上記処理装置を用いて、算出した加法群G_2の要素d_{ID}を示す情報をユーザ秘密鍵情報として出力する秘密鍵算出部と、

上記処理装置を用いて、上記秘密鍵算出部が出力したユーザ秘密鍵情報を入力し、上記処理装置を用いて、入力したユーザ秘密鍵情報を受信者装置に対して秘密裡に通知する秘密鍵通知部と、

を有する鍵生成装置と、

情報を記憶する記憶装置と、

情報を処理する処理装置と、

受信者装置に対して情報を送信する送信装置と、

上記処理装置を用いて、上記鍵生成装置が公開したパラメータ情報を取得し、上記処理装置を用いて、取得したパラメータ情報に含まれる第一要素情報と第二要素情報とを出力

するパラメータ取得部と、
上記処理装置を用いて、上記パラメータ取得部が出力した第一要素情報を入力し、上記記憶装置を用いて、入力した第一要素情報を記憶する第一要素記憶部と、
上記処理装置を用いて、上記パラメータ取得部が出力した第二要素情報を入力し、上記記憶装置を用いて、入力した第二要素情報を記憶する第二要素記憶部と、
上記処理装置を用いて、上記第一要素記憶部が記憶した第一要素情報と自然数ｒを示す乱数情報とを入力し、上記処理装置を用いて、入力した第一要素情報と乱数情報とに基づいて、加法群G_1の要素Ｒを算出し、上記処理装置を用いて、算出した加法群G_1の要素Ｒを示す情報を第四要素情報として出力する第四要素算出部と、
上記処理装置を用いて、受信者装置を識別する識別情報を入力し、上記処理装置を用いて、入力した識別情報に対応する加法群G_2の要素Q_{ID}を算出し、上記処理装置を用いて、算出した加法群G_2の要素Q_{ID}を示す情報を第五要素情報として出力する第五要素算出部と、
上記処理装置を用いて、上記第二要素記憶部が記憶した第二要素情報と上記第五要素算出部が出力した第五要素情報と上記乱数情報とを入力し、上記処理装置を用いて、入力した第二要素情報と第五要素情報とに基づいて、加法群G_1の要素P_{pub}と加法群G_2の要素Q_{ID}とのペアリング値を算出し、上記処理装置を用いて、算出したペアリング値と入力した乱数情報とに基づいて、乗法群G_Tの要素ｗを算出し、上記処理装置を用いて、算出した乗法群G_Tの要素ｗを示す情報を送信ペアリング値情報として出力する送信ペアリング値算出部と、
上記処理装置を用いて、上記第四要素算出部が出力した第四要素情報と上記送信ペアリング値算出部が出力した送信ペアリング値情報とを入力し、上記処理装置を用いて、入力した第四要素情報と送信ペアリング値情報とに基づいて、ハッシュ値を算出するセッション鍵生成部と、
上記処理装置を用いて、上記第四要素算出部が出力した第四要素情報を入力し、上記送信装置を用いて、入力した第四要素情報を含む情報を暗号化セッション鍵として受信者装置に対して送信する暗号化セッション鍵送信部と、
を有する送信者装置と、
情報を記憶する記憶装置と、
情報を処理する処理装置と、
送信者装置が送信した情報を受信する受信装置と、
上記処理装置を用いて、上記鍵生成装置が通知したユーザ秘密鍵情報を取得し、上記処理装置を用いて、取得したユーザ秘密鍵情報を出力する秘密鍵取得部と、
上記処理装置を用いて、上記秘密鍵取得部が出力したユーザ秘密鍵情報を入力し、上記記憶装置を用いて、入力したユーザ秘密鍵情報を記憶する秘密鍵記憶部と、
上記受信装置を用いて、送信者装置が送信した暗号化セッション鍵を受信し、上記処理装置を用いて、受信した暗号化セッション鍵に含まれる加法群G_1の要素Ｒを示す情報を第四要素情報として出力する暗号化セッション鍵受信部と、
上記処理装置を用いて、上記秘密鍵記憶部が記憶したユーザ秘密鍵情報と上記暗号化セッション鍵受信部が出力した第四要素情報とを入力し、上記処理装置を用いて、入力したユーザ秘密鍵情報と第四要素情報とに基づいて、加法群G_1の要素Ｒと加法群G_2の要素d_{ID}とのペアリング値を算出して乗法群G_Tの要素ｗ’とし、上記処理装置を用いて、算出した乗法群G_Tの要素ｗ’を示す情報を受信ペアリング値情報として出力する受信ペアリング値算出部と、
上記処理装置を用いて、上記暗号化セッション鍵受信部が出力した第四要素情報と上記受信ペアリング値算出部が出力した受信ペアリング値情報とを入力し、上記処理装置を用いて、入力した第四要素情報と受信ペアリング値情報とに基づいて、ハッシュ値を算出し、上記処理装置を用いて、算出したハッシュ値に基づいて、送信者装置が生成したセッション鍵と同一のセッション鍵を復元するセッション鍵復元部と、
を有する受信者装置と、

を備えることを特徴とする暗号通信システム。
【請求項５】
上記送信者装置は、更に、
上記処理装置を用いて、加法群G_1の位数より小さい自然数ｒをランダムに選択し、上記処理装置を用いて、選択した自然数ｒを示す情報を、上記第四要素算出部及び上記送信ペアリング値算出部が入力する乱数情報として出力する自然数選択部
を有し、
上記セッション鍵生成部は、
上記処理装置を用いて、第四要素情報と送信ペアリング値情報とを入力し、上記処理装置を用いて、入力した第四要素情報と送信ペアリング値情報とを結合してビット列情報を生成し、上記処理装置を用いて、生成したビット列情報に対応するハッシュ値を算出し、算出したハッシュ値をセッション鍵とする
ことを特徴とする請求項２に記載の送信者装置。
【請求項６】
上記セッション鍵復元部は、
上記処理装置を用いて、第四要素情報と受信ペアリング値情報とを入力し、上記処理装置を用いて、入力した第四要素情報と受信ペアリング値情報とを結合してビット列情報を生成し、上記処理装置を用いて、生成したビット列情報に対応するハッシュ値を算出し、算出したハッシュ値をセッション鍵とする
ことを特徴とする請求項１に記載の受信者装置。
【請求項７】
上記送信者装置は、更に、
上記処理装置を用いて、文字列ｍをランダムに選択し、上記処理装置を用いて、選択した文字列ｍを示す情報を文字列情報として出力する文字列選択部と、
上記処理装置を用いて、上記文字列選択部が出力した文字列情報を入力し、上記処理装置を用いて、入力した文字列情報に対応するハッシュ値を算出し、上記処理装置を用いて、算出したハッシュ値を示す情報を、上記第四要素算出部及び上記送信ペアリング値算出部が入力する乱数情報として出力する自然数算出部と、
を有し、
上記セッション鍵生成部は、
上記処理装置を用いて、第四要素情報と、送信ペアリング値情報と、上記文字列選択部が出力した文字列情報とを入力し、上記処理装置を用いて、入力した第四要素情報と送信ペアリング値情報とを結合してビット列情報を生成し、上記処理装置を用いて、生成したビット列情報に対応するハッシュ値を算出し、上記処理装置を用いて、算出したハッシュ値を示す情報と入力した文字列情報との排他的論理和を算出してマスク情報とし、上記処理装置を用いて、算出したマスク情報を出力し、上記処理装置を用いて、入力した文字列情報に対応するハッシュ値を算出し、算出したハッシュ値をセッション鍵として出力し、
上記暗号化セッション鍵送信部は、
上記処理装置を用いて、第四要素情報と、上記セッション鍵生成部が出力したマスク情報とを入力し、上記送信装置を用いて、入力した第四要素情報とマスク情報とを含む情報を暗号化セッション鍵として受信者装置に対して送信することを特徴とする請求項３に記載の送信者装置。
【請求項８】
上記暗号化セッション鍵受信部は、
上記受信装置を用いて、暗号化セッション鍵を受信し、上記処理装置を用いて、受信した暗号化セッション鍵に含まれる第四要素情報とマスク情報とを出力し、
上記セッション鍵復元部は、
上記処理装置を用いて、第四要素情報と、受信ペアリング値情報と、上記暗号化セッション鍵受信部が出力したマスク情報とを入力し、上記処理装置を用いて、入力した第四要素情報と受信ペアリング値情報とを結合してビット列情報を生成し、上記処理装置を用い

て、生成したビット列情報に対応するハッシュ値を算出し、上記処理装置を用いて、算出したハッシュ値を示す情報と入力したマスク情報との排他的論理和を算出して、復元文字列情報とし、上記処理装置を用いて、算出した復元文字列情報に対応するハッシュ値を算出し、算出したハッシュ値をセッション鍵とする
ことを特徴とする請求項１に記載の受信者装置。
【請求項９】
上記送信者装置は、更に、
上記処理装置を用いて、文字列ｍを示す文字列情報を入力し、上記処理装置を用いて、入力した文字列情報を、セッション鍵として出力するセッション鍵入力部と、
上記処理装置を用いて、上記セッション鍵入力部が出力したセッション鍵を入力し、上記処理装置を用いて、入力したセッション鍵に対応するハッシュ値を算出し、上記処理装置を用いて、算出したハッシュ値を示す情報を、上記第四要素算出部及び上記送信ペアリング値算出部が入力する乱数情報として出力する自然数算出部と、
を有し、
上記セッション鍵生成部は、
上記処理装置を用いて、第四要素情報と、送信ペアリング値情報と、上記セッション鍵入力部が出力したセッション鍵とを入力し、上記処理装置を用いて、入力した第四要素情報と送信ペアリング値情報とを結合してビット列情報を生成し、上記処理装置を用いて、生成したビット列情報に対応するハッシュ値を算出し、上記処理装置を用いて、算出したハッシュ値を示す情報と入力したセッション鍵との排他的論理和を算出してマスク情報とし、上記処理装置を用いて、算出したマスク情報を出力し、
上記暗号化セッション鍵送信部は、
上記処理装置を用いて、第四要素情報と、上記セッション鍵生成部が出力したマスク情報とを入力し、上記送信装置を用いて、入力した第四要素情報とマスク情報とを含む情報を暗号化セッション鍵として受信者装置に対して送信することを特徴とする請求項３に記載の送信者装置。
【請求項１０】
上記暗号化セッション鍵受信部は、
上記受信装置を用いて、暗号化セッション鍵を受信し、上記処理装置を用いて、受信した暗号化セッション鍵に含まれる第四要素情報とマスク情報とを出力し、
上記セッション鍵復元部は、
上記処理装置を用いて、第四要素情報と、受信ペアリング値情報と、上記暗号化セッション鍵受信部が出力したマスク情報とを入力し、上記処理装置を用いて、入力した第四要素情報と受信ペアリング値情報とを結合してビット列情報を生成し、上記処理装置を用いて、生成したビット列情報に対応するハッシュ値を算出し、上記処理装置を用いて、算出したハッシュ値を示す情報と入力したマスク情報との排他的論理和を算出して、セッション鍵とする
ことを特徴とする請求項１に記載の受信者装置。
【請求項１１】
上記第四要素算出部は、
上記処理装置を用いて、第一要素情報と乱数情報とを入力し、上記処理装置を用いて、入力した第一要素情報と乱数情報とに基づいて、加法群G_1の要素P_1をｒ回加算した要素を加法群G_1の要素Ｒとして算出し、上記処理装置を用いて、算出した加法群G_1の要素Ｒを示す情報を第四要素情報として出力し、
上記送信ペアリング値算出部は、
上記処理装置を用いて、第二要素情報と第五要素情報と乱数情報とを入力し、上記処理装置を用いて、入力した第二要素情報と第五要素情報と乱数情報とに基づいて、加法群G_1の要素P_{pub}と加法群G_2の要素Q_{ID}とのペアリング値のｒ乗を、乗法群G_Tの要素ｗとして算出し、上記処理装置を用いて、算出した乗法群G_Tの要素ｗを示す情報を送信ペアリング値情報として出力する

ことを特徴とする請求項２及び請求項３のいずれかに記載の送信者装置。
【請求項１２】
上記第二要素算出部は、
上記処理装置を用いて、第一要素情報とマスターキー情報とを入力し、上記処理装置を用いて、入力した第一要素情報とマスターキー情報とに基づいて、加法群G_1の要素P_1をｓ回加算した要素を加法群G_1の要素P_{pub}として算出し、上記処理装置を用いて、算出した加法群G_1の要素P_{pub}を示す情報を第二要素情報として出力し、
上記秘密鍵算出部は、
上記処理装置を用いて、第三要素情報とマスターキー情報とを入力し、上記処理装置を用いて、入力した第三要素情報とマスターキー情報とに基づいて、加法群G_2の要素Q_{ID}をｓ回加算した要素を加法群G_2の要素d_{ID}として算出し、上記処理装置を用いて、算出した加法群G_2の要素d_{ID}を示す情報をユーザ秘密鍵情報として出力する
ことを特徴とする請求項４に記載の暗号通信システム。
【請求項１３】
上記送信者装置は、更に、
上記処理装置を用いて、受信者装置に対して通知すべき情報を平文情報として入力し、上記処理装置を用いて、上記セッション鍵生成部が生成したセッション鍵を入力し、上記処理装置を用いて、入力した平文情報を、入力したセッション鍵で暗号化して暗号文情報を生成し、上記処理装置を用いて、生成した暗号文情報を出力する暗号文生成部と、
上記処理装置を用いて、上記暗号文生成部が出力した暗号文情報を入力し、上記送信装置を用いて、入力した暗号文情報を受信者装置に対して送信する暗号文送信部と、
を有することを特徴とする請求項２及び請求項３のいずれかに記載の送信者装置。
【請求項１４】
上記受信者装置は、更に、
上記受信装置を用いて、送信者装置が送信した暗号文情報を受信し、上記処理装置を用いて、受信した暗号文情報を出力する暗号文受信部と、
上記処理装置を用いて、上記暗号文受信部が出力した暗号文情報を入力し、上記処理装置を用いて、上記セッション鍵復元部が復元したセッション鍵を入力し、上記処理装置を用いて、入力した暗号文情報を、入力したセッション鍵で復号して、平文情報を生成し、
上記処理装置を用いて、生成した平文情報を出力する暗号文復号部と、
を有することを特徴とする請求項１に記載の受信者装置。
【請求項１５】
情報を記憶する記憶装置と、情報を処理する処理装置と、受信者装置に対して情報を送信する送信装置とを有するコンピュータを、請求項２及び請求項３のいずれかに記載の送信者装置として機能させることを特徴とするプログラム。
【請求項１６】
情報を記憶する記憶装置と、情報を処理する処理装置と、送信者装置が送信した情報を受信する受信装置とを有するコンピュータを、請求項１に記載の受信者装置として機能させることを特徴とするプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
この発明は、ＩＤベース公開鍵暗号方式の安全性を高める技術に関する。
【背景技術】
【０００２】
楕円暗号ペアリングを用いたＩＤベース公開鍵暗号を安全に行うためには、より良い安全性の証明を有する方式を用いることが重要である。これまでも安全性が数学的に証明された方法が提案されている。また、ペアリング応用技術は、超楕円曲線を含む一般の代数曲線を用いても実現できる。
【特許文献１】特開２００２－２６８９２号公報。

【特許文献２】特表２００５－５００７４０号公報。
【非特許文献１】境隆一、大岸聖史、笠原正雄「楕円曲線上のペアリングを用いた暗号方式」暗号と情報セキュリティシンポジウム（ＳＣＩＳ　２００１）、３６９～３７３ページ、２００１年。
【非特許文献２】Ｄａｎ　Ｂｏｎｅｈ、Ｍａｔｔ　Ｆｒａｎｋｌｉｎ「Ｉｄｅｎｔｉｔｙ－ｂａｓｅｄ　Ｅｎｃｒｙｐｔｉｏｎ　ｆｒｏｍ　ｔｈｅ　Ｗｅｉｌ　Ｐａｉｒｉｎｇ」Ｃｒｙｐｔｏ　２００１、２１３～２２９ページ、２００１年。
【非特許文献３】Ｂｅｎ　Ｌｙｎｎ「Ａｕｔｈｅｎｔｉｃａｔｅｄ　Ｉｄｅｎｔｉｔｙ－Ｂａｓｅｄ　Ｅｎｃｒｙｐｔｉｏｎ」ｈｔｔｐ：／／ｅｐｒｉｎｔ．ｉａｃｒ．ｏｒｇ、２００２年。
【非特許文献４】Ｖｉｃｔｏｒ　Ｓｈｏｕｐ「Ａ　Ｐｒｏｐｏｓａｌ　ｆｏｒ　ａｎ　ＩＳＯ　Ｓｔａｎｄａｒｄ　ｆｏｒ　Ｐｕｂｌｉｃ　Ｋｅｙ　Ｅｎｃｒｙｐｔｉｏｎ」ｈｔｔｐ：／／ｓｈｏｕｐ．ｎｅｔ／ｐａｐｅｒｓ／、２００１年。
【非特許文献５】Ｋ．Ｂｅｎｔａｈａｒ、Ｐ．Ｆａｒｓｈｉｍ、Ｊ．Ｍａｌｏｎｅ－Ｌｅｅ、Ｎ．Ｐ．Ｓｍａｒｔ「Ｇｅｎｅｒｉｃ　Ｃｏｎｓｔｒｕｃｔｉｏｎｓ　ｏｆ　Ｉｄｅｎｔｉｔｙ－Ｂａｓｅｄ　ａｎｄ　Ｃｅｒｔｉｆｉｃａｔｅｌｅｓｓ　ＫＥＭｓ”ｈｔｔｐ：／／ｅｐｒｉｎｔ．ｉａｃｒ．ｏｒｇ。
【非特許文献６】Ｒｏｎａｌｄ　Ｃｒａｍｅｒ、Ｖｉｃｔｏｒ　Ｓｈｏｕｐ「Ｄｅｓｉｇｎ　ａｎｄ　Ａｎａｌｙｓｉｓ　ｏｆ　Ｐｒａｃｔｉｃａｌ　Ｐｕｂｌｉｃ－Ｋｅｙ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｃｈｅｍｅｓ　Ｓｅｃｕｒｅ　ａｇａｉｎｓｔ　Ａｄａｐｔｉｖｅ　Ｃｈｏｓｅｎ　Ｃｉｐｈｅｒｔｅｘｔ　Ａｔｔａｃｋ」ＳＩＡＭ　Ｊｏｕｒｎａｌ　ｏｎ　Ｃｏｍｐｕｔｉｎｇ　３３、１６７～２２６ページ、２００３年。

【発明の開示】
【発明が解決しようとする課題】
【０００３】
近年の高度情報通信技術の実用化に伴い、楕円暗号を含む公開鍵暗号も既に実用化段階に入っているが、従来、公開鍵証明の必要性からＰＫＩ（Ｐｕｂｌｉｃ　Ｋｅｙ　Ｉｎｆｒａｓｔｒｕｃｔｕｒｅ）というインフラストラクチャが必要であり、それが公開鍵暗号技術の多方面への展開の妨げとなってきた。近年、名前や機器番号のような識別名（ＩＤ情報）を公開鍵に用いることでＰＫＩを不要化する公開鍵暗号が実現された。その実現には、（超）楕円曲線上のペアリング演算が本質的に重要である。
【０００４】
また、公開鍵暗号の安全性を数学的な問題の困難性に帰着させて示すことは、現在、暗号方式の安全性保証のために標準的に行われ、また、その帰着効率の評価が暗号方式の評価に繋がっている。それは、暗号解読によって得られる優位性と共に、その実行時間の評価も含む。即ち、ある公開鍵暗号を破ることがある数学的な問題を解くことに変換できたとしても（そして、その数学的な問題を解くには著しく時間がかかることがわかっていたとしても）、その変換後の数学問題解法アルゴリズム自身が著しく時間がかかることになってしまっては、元来の公開鍵暗号に対し、なんら安全性を保証することができなくなってしまうからである。
【０００５】
また、安全性証明を行う手法の一つとして、従来、ランダムオラクルモデルというものを用いれば効率的に安全な公開鍵暗号系を構成できることが知られており、公開鍵暗号の標準を定めたＩＳＯ　１８０３３－２等ではランダムオラクルモデルで安全性が保証された方式がいくつも採用されている。ＩＤベース暗号に関してもランダムオラクルモデルで安全性が証明された方式がいくつか存在する。
【０００６】
また、ＩＳＯ　１８０３３－２等では、公開鍵暗号は、鍵カプセル化（ＫＥＭ、Ｋｅｙ　Ｅｎｃａｐｓｕｌａｔｉｏｎ　Ｍｅｃｈａｎｉｓｍ）として規定されており、ＩＤベース暗号に関しても多くはＩＤベースＫＥＭの形で規定されている。例えば、非特許文献１

及び非特許文献２のＩＤベース暗号化方式をＩＤベースＫＥＭに変換した非特許文献３のＩＤベースＫＥＭなどが知られており、それの安全性はランダムオラクルモデルで与えられている。それらの安全性を更に高めることが課題とされている。

【０００７】

この発明は、上記のような課題を解決するためになされたものである。

【課題を解決するための手段】

【０００８】

この発明にかかる受信者装置は、

情報を記憶する記憶装置と、

情報を処理する処理装置と、

送信者装置が送信した情報を受信する受信装置と、

上記記憶装置を用いて、加法群G_2の要素d_{ID}を示す情報をユーザ秘密鍵情報として記憶する秘密鍵記憶部と、

上記受信装置を用いて、送信者装置が送信した暗号化セッション鍵を受信し、上記処理装置を用いて、受信した暗号化セッション鍵に含まれる加法群G_1の要素Ｒを示す情報を第四要素情報として出力する暗号化セッション鍵受信部と、

上記処理装置を用いて、上記秘密鍵記憶部が記憶したユーザ秘密鍵情報と上記暗号化セッション鍵受信部が出力した第四要素情報とを入力し、上記処理装置を用いて、入力したユーザ秘密鍵情報と第四要素情報とに基づいて、加法群G_1の要素Ｒと加法群G_2の要素d_{ID}とのペアリング値を算出して乗法群G_Tの要素ｗ’とし、上記処理装置を用いて、算出した乗法群G_Tの要素ｗ’を示す情報を受信ペアリング値情報として出力する受信ペアリング値算出部と、

上記処理装置を用いて、上記暗号化セッション鍵受信部が出力した第四要素情報と上記受信ペアリング値算出部が出力した受信ペアリング値情報とを入力し、上記処理装置を用いて、入力した第四要素情報と受信ペアリング値情報とに基づいて、ハッシュ値を算出し、上記処理装置を用いて、算出したハッシュ値に基づいて、送信者装置が生成したセッション鍵と同一のセッション鍵を復元するセッション鍵復元部と、

を有することを特徴とする。

【発明の効果】

【０００９】

この発明にかかる受信者装置によれば、セッション鍵復元部が、加法群G_1の要素Ｒを示す第四要素情報と、ペアリング値ｗ’を示す受信ペアリング値情報とに基づいてハッシュ値を算出し、算出したハッシュ値に基づいて、セッション鍵Ｋを復元するので、Ｇ－ＢＤＨ問題に効率良く帰着する安全性の高い暗号方式を実現することができるという効果を奏する。

【発明を実施するための最良の形態】

【００１０】

最初に、用語を定義する。

【００１１】

有限体ＧＦ（p^l）（ｐは、２でない素数。ｌは、自然数。）上の楕円曲線（以下、単に「楕円曲線」という。）とは、式$Y^2 = X^3 + aX + b$（Ｘ，Ｙ，ａ，ｂは、有限体ＧＦ（p^n）の要素。）を満たす点（Ｘ，Ｙ）の集合である。楕円曲線に含まれる点およびＹ軸方向の無限遠点Ｏを、楕円曲線上の点という。

なお、ここに示した楕円曲線の方程式は、標数が２でない場合の標準形であり、標数が２の場合の標準形は若干異なる。以下の説明は、すべての標数について適用可能であり、標数が２でない場合に限るものではない。

【００１２】

楕円曲線上の点の加算とは、楕円曲線上の点について定義された演算である。

楕円曲線上の点Ａ及び点Ｂが与えられたとき、点Ａと点Ｂとを通る直線が、楕円曲線と交わる点をＣ（X_C，Y_C）とすると、点（X_C，$-Y_C$）を点Ａと点Ｂとの和と定義す

る。なお、点Ａと点Ｂとが同一の点である場合は、点Ａ（＝点Ｂ）における楕円曲線の接線が楕円曲線と交わる点を点Ｃとする。また、点Ａと点Ｂとを通る直線が、点Ａ（または点Ｂ）で楕円曲線と接する場合は、点Ａ（または点Ｂ）を点Ｃとする。

楕円曲線上の点の加算は、コンピュータを用いて計算できることが知られている。

【００１３】

上述の定義より、楕円曲線上の点の和は楕円曲線上の点となる。すなわち、楕円曲線上の点は、加法について閉じている。楕円曲線上の点を要素とする加法群を、楕円曲線上の点がなす群という。

【００１４】

楕円曲線上の点のスカラー倍とは、楕円曲線上の点Ａをｎ回加算した点のことである。これを、ｎＡ（ｎは自然数。Ａは楕円曲線上の点。）と表記する。例えば、２Ａは、楕円曲線上の点Ａと点Ａとの和（Ａ＋Ａ）である。３Ａは、楕円曲線上の点２Ａと点Ａとの和（２Ａ＋Ａ）である。

楕円曲線上の点Ａのｎ倍が、ｎＡ＝Ｏ（Ｏは、Ｙ軸方向の無限遠点。）となるｎのうち、最小のものを楕円曲線上の点Ａの位数という。

また、楕円曲線上の点Ａの位数のうち最大のものを、楕円曲線上の点がなす群の位数という。

【００１５】

ここでは楕円曲線について説明したが、超楕円曲線やその他一般の代数曲線についても、代数曲線に基づく加法群を定義することができる。

以下の説明において「加法群」という場合、楕円曲線上の点がなす群だけでなく、一般の代数曲線に基づく加法群も含むものとする。

【００１６】

ペアリング（Ｐａｉｒｉｎｇ）とは、加法群G_1の要素Ｐと加法群G_2の要素Ｑとから、乗法群G_Tの要素ｗ＝ｅ（Ｐ，Ｑ）への写像$G_1 \times G_2 \rightarrow G_T$である。ここで、加法群$G_1$と加法群$G_2$とは、必ずしも同じ群である必要はない。特に、$G_1$と$G_2$が同じ群である場合を、対称的なペアリング（Ｓｙｍｍｅｔｒｉｃ　Ｐａｉｒｉｎｇ）といい、G_1とG_2が異なる群である場合を、非対称的なペアリング（Ａｓｙｍｍｅｔｒｉｃ　Ｐａｉｒｉｎｇ）という。

双線形ペアリング（Ｂｉｌｉｎｅａｒ　Ｐａｉｒｉｎｇ）とは、ｅ（ａＰ，ｂＱ）＝ｅ（Ｐ，Ｑ）^{ab}（ａ，ｂは、自然数。）を満たすペアリングをいう。コンピュータを用いてペアリングの値（乗法群G_Tの要素）を計算できる双線形ペアリングとして、楕円曲線上の点についてのヴェイユ（Ｗｅｉｌ）ペアリング、テイト（Ｔａｔｅ）ペアリングなどが知られている。

【００１７】

離散対数問題（Ｄｉｓｃｒｅｔｅ　Ｌｏｇａｒｉｔｈｍ　Ｐｒｏｂｌｅｍ）とは、「加法群Ｇの２つの要素g_1、g_2に対して、$g_1 = mg_2$を満たすようなｍを求めよ」という数学上の問題である。代数群Ｇの要素の数が大きい場合、多くの離散対数問題を解くことは、計算量的に非常に困難になることが知られている。この事実を利用して、公開鍵暗号を設計することができる。

【００１８】

楕円曲線ディフィー・ヘルマン問題（Ｅｌｌｉｐｔｉｃ　Ｃｕｒｖｅ　Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎ　Ｐｒｏｂｌｅｍ。以下、単に「ディフィー・ヘルマン問題」または「ＤＨ問題」という。）とは、「Ｐ、ａＰ及びｂＰ（ただし、Ｐは楕円曲線上の点。ａ及びｂは自然数。）が与えられたとき、ａｂＰを計算せよ。」という数学上の問題をいう。

【００１９】

双線形ディフィー・ヘルマン問題（Ｂｉｌｉｎｅａｒ　Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎ　Ｐｒｏｂｌｅｍ。以下「ＢＤＨ問題」という。）とは、「P_1、aP_1、bP_1、P_2、aP_2及びcP_2（ただし、P_1は加法群G_1（例えば楕円曲線上の点がなす群）の要素。P_2は加法群G_2（加法群G_1と同一の加法群でもよいし、異なる加法群でもよい）

の要素。ａ、ｂ及びｃは自然数。）が与えられたとき、ｅ（$Ｐ_1$，$Ｐ_2$）^{ａｂｃ}（ただし、ｅは双線形ペアリング）を計算せよ。」という数学上の問題をいう。ペアリングｅは、対称的なペアリングでもよいし、非対称的なペアリングでもよい。

多くのＩＤベース公開鍵暗号方式は、ＢＤＨ問題の困難性に基づく。

ＢＤＨ問題の困難性を確保するには、加法群$Ｇ_1$及び$Ｇ_2$における離散対数問題の困難性と、乗法群$Ｇ_T$における離散対数問題の困難性との双方を確保する必要がある。

【００２０】

双線形ディフィー・ヘルマン決定問題（Ｄｅｃｉｓｉｏｎａｌ　Ｂｉｌｉｎｅａｒ　Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎ　Ｐｒｏｂｌｅｍ。以下「ＢＤＨ決定問題」という。）とは、「$Ｐ_1$、$ａＰ_1$、$ｂＰ_1$、$Ｐ_2$、$ａＰ_2$、$ｃＰ_2$、ｚ（ただし、$Ｐ_1$は加法群$Ｇ_1$の要素。$Ｐ_2$は加法群$Ｇ_2$の要素。ａ、ｂ、ｃは自然数。ｚは乗法群$Ｇ_T$の要素。）が与えられたとき、ｚ＝ｅ（$Ｐ_1$，$Ｐ_2$）^{ａｂｃ}（ただし、ｅは双線形ペアリング）であるか否かを判定せよ。」という数学上の問題をいう。

【００２１】

ギャップ双線形ディフィー・ヘルマン問題（Ｇａｐ　Ｂｉｌｉｎｅａｒ　Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎ　Ｐｒｏｂｌｅｍ。以下「Ｇ－ＢＤＨ問題」という。）とは、「ＢＤＨ決定問題に答えるオラクルを利用できるという仮定のもとで、ＢＤＨ問題に答えよ。」という数学上の問題をいう。

なお、オラクルとは、特定の機能を有する入出力インターフェースのことをいう。すなわち、オラクルは、なんらかの値を入力し、入力した値に対してなんらかの処理を行い、その結果を出力する。ＢＤＨ決定問題に答えるオラクル（以下、「ＢＤＨ決定オラクル」という。）は、$Ｐ_1$、$ａＰ_1$、$ｂＰ_1$、$Ｐ_2$、$ａＰ_2$、$ｃＰ_2$、ｚを入力すると、ｚ＝ｅ（Ｐ，Ｑ）^{ａｂｃ}であるか否かを判定し、判定結果を（例えば「ＹＥＳ」「ＮＯ」として）出力する。

Ｇ－ＢＤＨ問題などのギャップ問題の困難性を仮定することで、多くの暗号方式の安全性を証明することができる。

【００２２】

公開鍵暗号技術は、上記のような数学上の問題を解くことが極めて困難であることに、安全性の根拠を持つ。

すなわち、攻撃者が、公開鍵や暗号文などの情報から秘密鍵や（暗号文を復号した）平文などの情報を得ることができると仮定すると、上記のような数学上の問題を解くことも可能となる。しかし、上記のような数学上の問題を解くことは極めて困難なので、背理法により、攻撃者が秘密鍵などの情報を得ることも極めて困難であるという結論に達する。

このように、暗号技術の安全性を、数学上の問題を解くことの困難性に基づいて証明することを、「安全性の帰着」という。

【００２３】

したがって、暗号技術の安全性は、それが帰着する数学上の問題を解くことがどれほど困難であるかによって決まる。

例えば、ある数学上の問題を理論上解くことができるとしても、その問題を解くアルゴリズムを現存するスーパーコンピュータに実行させて、答えを出すのに一万年かかるとすれば、その数学上の問題に帰着する暗号技術は安全であるといえる。

また、別の数学上の問題を解くアルゴリズムを現存するスーパーコンピュータに実行させて、答えを出すのに十万年かかるとすれば、その数学上の問題に帰着する暗号技術のほうが、更に安全であるといえる。

【００２４】

しかし、暗号を解読するために必要な計算量と、それが帰着する数学上の問題を解くために必要な計算量とは同一ではないので、例えば、数学上の問題を解くのには十万年かかるとしても、その問題に帰着する暗号を解読するには、千年しかかからない場合もあれば、一万年かかる場合もある。

暗号を解読するために必要な計算量と、それが帰着する数学上の問題を解くために必要

な計算量とが近い場合を、「帰着の効率が良い」という。
したがって、同じ数学上の問題に帰着する暗号方式であれば、帰着の効率が良い暗号方式のほうが、安全性が高いといえる。
【００２５】
ランダムオラクル（Ｒａｎｄｏｍ　Ｏｒａｃｌｅ）とは、例えば、文字列を入力して数値を出力するオラクルであって、同じ文字列を入力すると同じ数値を出力し、ある文字列に対する出力に基づいて他の文字列に対する出力を予想することができないものをいう。
対応する入力を知らなければ、出力から入力を求めることができないので、ランダムオラクルは、一方向性関数とも呼ばれる。
【００２６】
ＩＤベース公開鍵暗号方式とは、個人の名前や機器番号のような識別名（ＩＤ）を公開鍵として、データ暗号化である秘密鍵暗号用のセッション鍵を生成する暗号方式である。
【００２７】
鍵カプセル化方式（Ｋｅｙ　Ｅｎｃａｐｓｕｌａｔｉｏｎ　Ｍｅｃｈａｎｉｓｍ。以下「ＫＥＭ」という。）とは、セッション鍵を暗号化した暗号化セッション鍵を送信することにより、送信者と受信者とがセッション鍵を共有する暗号方式のうち、送信者がセッション鍵を選択することができないものをいう。
【００２８】
次に、ＫＥＭに対する安全性を定義する。
ＩＮＤ－ＩＤ－ＣＣＡ（Ｉｎｄｉｓｔｉｎｇｕｉｓｈａｂｌｉｔｙ　ｆｏｒ　ＩＤ－ｂａｓｅｄ　ＫＥＭ　ａｇａｉｎｓｔ　ａｄａｐｔｉｖｅ　ｃｈｏｓｅｎ　ｃｉｐｈｅｒｔｅｘｔ　ａｔｔａｃｋｓ：ＩＤベース暗号における適応的選択暗号文攻撃に対する暗号文識別不可能）安全性とは、攻撃者Ａが、以下の攻撃シナリオに基づく攻撃をした場合における安全性をいう。
【００２９】
（１）攻撃者Ａは、セットアップオラクルを呼び出す。
セットアップオラクルとは、ＩＤベース公開鍵暗号の鍵生成パラメータを出力するオラクルである。
実際のＩＤベース公開鍵暗号方式では、秘密鍵生成装置が鍵生成パラメータを生成し、公開するので、攻撃者Ａは、公開された情報から鍵生成パラメータを入手することが可能である。
【００３０】
（２）攻撃者Ａは、鍵漏洩オラクルに対する質問をする。
鍵漏洩オラクルとは、ＩＤを入力し、そのＩＤに対応するユーザ秘密鍵を出力するオラクルである。
実際のＩＤベース公開鍵暗号方式では、ユーザ秘密鍵は各ユーザが秘密裏に保管している。そこでは、複数の攻撃者が結託すれば、複数のＩＤについてのユーザ秘密鍵を入手することができる。したがって、攻撃者が任意のＩＤに対するユーザ秘密鍵を入手することができるという、もっとも厳しい条件での安全性を保証できれば、実際の環境での安全性はより高いものとなる。したがって、任意のＩＤに対するユーザ秘密鍵を入手できるという仮定での安全性を検討するものである。
【００３１】
（３）攻撃者Ａは、復号オラクルに対する質問をする。
復号オラクルとは、ＩＤと、そのＩＤが示すユーザに対して送信される暗号文とを入力し、その暗号文を復号した平文を出力するオラクルである。
実際のＩＤベース公開鍵暗号方式では、暗号文がインターネットなどを流れている。したがって、攻撃者は暗号文を入手できる。暗号文を受信したユーザが復号した結果を、なんらかの手段で攻撃者が入手したとすると、攻撃者は、暗号文とそれを復号した復号結果の組を入手可能である。したがって、そのような厳しい条件での安全性を検討するものである。

【００３２】
（４）攻撃者Ａは、（２）及び（３）を必要な回数だけ繰り返す。
【００３３】
（５）攻撃者Ａは、攻撃対象となるＩＤ（以下「攻撃対象ＩＤ」という）を選択する。
なお、攻撃対象ＩＤは、（２）でユーザ秘密鍵を入手したＩＤ以外のＩＤとする。
【００３４】
（６）攻撃者Ａは、暗号化オラクルを呼び出す。
暗号化オラクルとは、攻撃対象ＩＤを入力し、攻撃対象ＩＤが示す受信者に対して情報を送信しようとする送信者が生成するセッション鍵と、受信者がそのセッション鍵をユーザ秘密鍵を用いて復元するための情報（以下「暗号化セッション鍵」という。）とを出力するオラクルである。ただし、暗号化オラクルは、１／２の確率で、正しく対応するセッション鍵と暗号化セッション鍵の対を出力するが、１／２の確率で、正しく対応しないセッション鍵と暗号化セッション鍵の対を出力する。
実際のＩＤベース公開鍵暗号方式では、送信者と受信者とがセッション鍵を共有するため、送信者が受信者に対して暗号化セッション鍵を送信する。したがって、攻撃者は暗号化セッション鍵を入手可能である。もし、攻撃者が、セッション鍵と暗号化セッション鍵とが正しく対応しているか否かを（確率的に）判定できるならば、その暗号方式は安全でないことになる。
【００３５】
（７）攻撃者Ａは、必要に応じて、（２）及び（３）を必要な回数だけ繰り返してもよい。
ただし、鍵漏洩オラクルに対して、攻撃対象ＩＤを入力してはならない。また、復号オラクルに対して、攻撃対象ＩＤと（５）で暗号化オラクルが出力した暗号化セッション鍵との組を入力してもならない。そのような情報は、直接的な答えになってしまうからである。しかし、復号オラクルに対して、攻撃対象ＩＤと他の暗号文との組を入力したり、他のＩＤと暗号化セッション鍵との組を入力したりすることは許される。
【００３６】
（８）攻撃者Ａは、（６）で暗号化オラクルが出力したセッション鍵と暗号化セッション鍵とが、正しく対応するものであるか否かを判定する。
攻撃者Ａがまったく暗号を解読できないとすると、攻撃者Ａの判定した結果が正しい確率は１／２である。攻撃者Ａが暗号を解読できる場合があれば、攻撃者Ａの判定した結果が正しい確率は１／２を上回る。
そこで、攻撃者Ａの判定した結果が正しい確率から１／２を減算したものを、攻撃者Ａの優位性（Ａｄｖａｎｔａｇｅ）と呼ぶ。
【００３７】
一般的に、暗号方式が用いる有限体の要素の数が少なければ、その暗号は解読されやすく、多ければ、その暗号は解読されにくい傾向がある。したがって、暗号方式が用いる有限体の要素の数が多ければ、攻撃者Ａの優位性は低くなる。
【００３８】
そこで、攻撃者Ａの優位性εを、暗号方式が用いる有限体の要素の数の関数ε（ｎ）（ｎは、有限体の要素の数）と考える。
ε（ｎ）が、任意の多項式ｐ（ｎ）（ただし、最高次係数が正）に対して、$n > n_0$であるすべてのｎについてε（ｎ）＜１／ｐ（ｎ）となるn_0が存在する場合に、「ε（ｎ）は漸近的に無視できる（ｎｅｇｌｉｇｉｂｌｅ）」という。
【００３９】
攻撃者Ａの優位性が漸近的に無視できる値であれば、その暗号方式は安全であると考える。攻撃者Ａの優位性が漸近的に無視できる値でない場合、その暗号方式は安全でないと考える。
【００４０】
実施の形態１．

実施の形態１を、図１～図２３を用いて説明する。

【００４１】

図１は、この実施の形態におけるＩＤベース公開鍵暗号通信システム８００の全体構成の一例を示すシステム構成図である。

なお、ＩＤベース公開鍵暗号通信システム８００は、暗号通信システムの一例である。

【００４２】

ＩＤベース公開鍵暗号通信システム８００は、ユーザ秘密鍵生成センタ１００、送信者装置２００、受信者装置３００を有する。

なお、ユーザ秘密鍵生成センタ１００は、鍵生成装置の一例である。また、ユーザ秘密鍵生成センタ１００は、秘密鍵生成装置（Ｐｒｉｖａｔｅ　Ｋｅｙ　Ｇｅｎｅｒａｔｏｒ。ＰＫＧ）とも呼ばれる。

【００４３】

ユーザ秘密鍵生成センタ１００は、ＩＤベース公開鍵暗号通信システム８００で使用する暗号のパラメータを設定し、設定したパラメータを示すパラメータ情報を公開する。

また、ユーザ秘密鍵生成センタ１００は、受信者装置３００のＩＤに基づいて、ユーザ秘密鍵情報を生成し、受信者装置３００に対して秘密裡に通知する。

【００４４】

受信者装置３００のＩＤは、例えばメールアドレスなど、本人のものであることが明白なものを用いる。これにより、公開鍵証明書などを用いることなく、受信者装置３００だけが暗号文を復号できることを保証する。

【００４５】

送信者装置２００は、ユーザ秘密鍵生成センタ１００が公開したパラメータ情報と、受信者装置３００のＩＤとを入力し、受信者装置３００に対して送信すべき情報を暗号化するためのセッション鍵を生成する。

送信者装置２００は、セッション鍵についての情報を含む暗号化セッション鍵情報を、受信者装置３００に対して送信する。また、送信者装置２００は、セッション鍵により暗号化した暗号文情報を、受信者装置３００に対して送信する。

【００４６】

受信者装置３００は、送信者装置２００が送信した暗号化セッション鍵情報を受信する。受信者装置３００は、受信した暗号化セッション鍵情報と、ユーザ秘密鍵生成センタ１００が通知したユーザ秘密鍵情報とに基づいて、セッション鍵を復元する。受信者装置３００は、送信者装置２００が送信した暗号文情報を受信し、復元したセッション鍵で復号して、元の情報を取得する。

【００４７】

暗号化セッション鍵情報や暗号文情報は、インターネットなどオープンなネットワークを介して送受信されるので、攻撃者はこれらの情報を入手することができる。しかし、ユーザ秘密鍵情報は、秘密裡に通知されるので、攻撃者が入手することはできない。

【００４８】

攻撃者は、ユーザ秘密鍵情報がなければ、暗号化セッション鍵情報からセッション鍵を復元することができない。また、攻撃者は、セッション鍵がなければ、暗号文情報を復号することができない。したがって、送信者装置２００が受信者装置３００に対して通知した情報の秘密が守られる。

【００４９】

図２は、この実施の形態におけるユーザ秘密鍵生成センタ１００及び送信者装置２００及び受信者装置３００の外観の一例を示す図である。

ユーザ秘密鍵生成センタ１００及び送信者装置２００及び受信者装置３００は、システムユニット９１０、ＣＲＴ（Ｃａｔｈｏｄｅ・Ｒａｙ・Ｔｕｂｅ）やＬＣＤ（液晶）の表示画面を有する表示装置９０１、キーボード９０２（Ｋｅｙ・Ｂｏａｒｄ：Ｋ／Ｂ）、マウス９０３、ＦＤＤ９０４（Ｆｌｅｘｉｂｌｅ・Ｄｉｓｋ・Ｄｒｉｖｅ）、コンパクトディスク装置９０５（ＣＤＤ）、プリンタ装置９０６、スキャナ装置９０７などのハードウ

ェア資源を備え、これらはケーブルや信号線で接続されている。
システムユニット９１０は、コンピュータであり、ファクシミリ機９３２、電話器９３１とケーブルで接続され、また、ローカルエリアネットワーク９４２（ＬＡＮ）、ゲートウェイ９４１を介してインターネット９４０に接続されている。
【００５０】
図３は、この実施の形態におけるユーザ秘密鍵生成センタ１００及び送信者装置２００及び受信者装置３００のハードウェア資源の一例を示す図である。
ユーザ秘密鍵生成センタ１００及び送信者装置２００及び受信者装置３００は、プログラムを実行するＣＰＵ９１１（Ｃｅｎｔｒａｌ・Ｐｒｏｃｅｓｓｉｎｇ・Ｕｎｉｔ、中央処理装置、処理装置、演算装置、マイクロプロセッサ、マイクロコンピュータ、プロセッサともいう）を備えている。ＣＰＵ９１１は、バス９１２を介してＲＯＭ９１３、ＲＡＭ９１４、通信装置９１５、表示装置９０１、キーボード９０２、マウス９０３、ＦＤＤ９０４、ＣＤＤ９０５、プリンタ装置９０６、スキャナ装置９０７、磁気ディスク装置９２０と接続され、これらのハードウェアデバイスを制御する。磁気ディスク装置９２０の代わりに、光ディスク装置、メモリカード読み書き装置などの記憶装置でもよい。
ＲＡＭ９１４は、揮発性メモリの一例である。ＲＯＭ９１３、ＦＤＤ９０４、ＣＤＤ９０５、磁気ディスク装置９２０の記憶媒体は、不揮発性メモリの一例である。これらは、記憶装置あるいは記憶部の一例である。
通信装置９１５、キーボード９０２、スキャナ装置９０７、ＦＤＤ９０４などは、入力部、入力装置の一例である。
また、通信装置９１５、表示装置９０１、プリンタ装置９０６などは、出力部、出力装置の一例である。
通信装置９１５は、送信装置の一例である。また、通信装置９１５は、受信装置の一例である。
【００５１】
通信装置９１５は、ファクシミリ機９３２、電話器９３１、ＬＡＮ９４２等に接続されている。通信装置９１５は、ＬＡＮ９４２に限らず、インターネット９４０、ＩＳＤＮ等のＷＡＮ（ワイドエリアネットワーク）などに接続されていても構わない。インターネット９４０或いはＩＳＤＮ等のＷＡＮに接続されている場合、ゲートウェイ９４１は不要となる。
磁気ディスク装置９２０には、オペレーティングシステム９２１（ＯＳ）、ウィンドウシステム９２２、プログラム群９２３、ファイル群９２４が記憶されている。プログラム群９２３のプログラムは、ＣＰＵ９１１、オペレーティングシステム９２１、ウィンドウシステム９２２により実行される。
【００５２】
上記プログラム群９２３には、以下に述べる実施の形態の説明において「～部」、「～手段」として説明する機能を実行するプログラムが記憶されている。プログラムは、ＣＰＵ９１１により読み出され実行される。
ファイル群９２４には、以下に述べる実施の形態の説明において、「～の判定結果」、「～の計算結果」、「～の処理結果」として説明する情報やデータや信号値や変数値やパラメータが、「～ファイル」や「～データベース」の各項目として記憶されている。「～ファイル」や「～データベース」は、ディスクやメモリなどの記録媒体に記憶される。ディスクやメモリなどの記憶媒体に記憶された情報やデータや信号値や変数値やパラメータは、読み書き回路を介してＣＰＵ９１１によりメインメモリやキャッシュメモリに読み出され、抽出・検索・参照・比較・演算・計算・処理・出力・印刷・表示などのＣＰＵの動作に用いられる。抽出・検索・参照・比較・演算・計算・処理・出力・印刷・表示のＣＰＵの動作の間、情報やデータや信号値や変数値やパラメータは、メインメモリやキャッシュメモリやバッファメモリに一時的に記憶される。
また、以下に述べる実施の形態の説明において説明するフローチャートの矢印の部分は主としてデータや信号の入出力を示し、データや信号値は、ＲＡＭ９１４のメモリ、ＦＤ

Ｄ９０４のフレキシブルディスク、ＣＤＤ９０５のコンパクトディスク、磁気ディスク装置９２０の磁気ディスク、その他光ディスク、ミニディスク、ＤＶＤ（Ｄｉｇｉｔａｌ・Ｖｅｒｓａｔｉｌｅ・Ｄｉｓｃ）等の記録媒体に記録される。また、データや信号は、バス９１２や信号線やケーブルその他の伝送媒体によりオンライン伝送される。

【００５３】

また、以下に述べる実施の形態の説明において「～部」、「～手段」として説明するものは、「～回路」、「～装置」、「～機器」であってもよく、また、「～ステップ」、「～手順」、「～処理」であってもよい。すなわち、「～部」、「～手段」として説明するものは、ＲＯＭ９１３に記憶されたファームウェアで実現されていても構わない。或いは、ソフトウェアのみ、或いは、素子・デバイス・基板・配線などのハードウェアのみ、或いは、ソフトウェアとハードウェアとの組み合わせ、さらには、ファームウェアとの組み合わせで実施されても構わない。ファームウェアとソフトウェアは、プログラムとして、磁気ディスク、フレキシブルディスク、光ディスク、コンパクトディスク、ミニディスク、ＤＶＤ等の記録媒体に記憶される。プログラムはＣＰＵ９１１により読み出され、ＣＰＵ９１１により実行される。すなわち、プログラムは、以下に述べる「～部」、「～手段」としてコンピュータを機能させるものである。あるいは、以下に述べる「～部」、「～手段」の手順や方法をコンピュータに実行させるものである。

【００５４】

図４は、この実施の形態におけるユーザ秘密鍵生成センタ１００の機能ブロックの構成の一例を示すブロック構成図である。

【００５５】

ユーザ秘密鍵生成センタ１００は、公開パラメータ生成部１１０、ユーザ秘密鍵生成部１３０を有する。

公開パラメータ生成部１１０は、第一要素選択部１１１、マスターキー選択部１１２、マスターキー記憶部１１３、第二要素算出部１２１、パラメータ公開部１２２を有する。

ユーザ秘密鍵生成部１３０は、識別情報取得部１３１、第三要素算出部１３２、秘密鍵算出部１３３、秘密鍵通知部１３４を有する。

【００５６】

公開パラメータ生成部１１０とユーザ秘密鍵生成部１３０とは、異なる装置であってもよい。公開パラメータ生成部１１０とユーザ秘密鍵生成部１３０とを異なる装置とする場合、公開パラメータ生成部１１０を有する装置１つに対応して、ユーザ秘密鍵生成部１３０を有する装置が複数あってもよい。

【００５７】

ユーザ秘密鍵生成センタ１００は、ＣＰＵ９１１などの処理装置を用いて、ＩＤベース公開鍵暗号通信システム８００で使用する加法群G_1（例えば楕円曲線Ｅ上の点がなす群）、加法群G_2（例えば、加法群G_1と同一の群であってもよいし、加法群G_1と同一の楕円曲線Ｅ上の点がなす加法群G_1と異なる群であってもよい。）、乗法群G_T、ペアリング関数ｅ：$G_1 \times G_2 \rightarrow G_T$、鍵導出関数（Ｋｅｙ Ｄｅｒｉｖａｔｉｏｎ Ｆｕｎｃｔｉｏｎ）Ｇ、ＩＤを加法群G_2の要素に変換する変換関数Ｈなどのパラメータを決定しておく。

加法群G_1、加法群G_2及び乗法群G_Tは、位数が同一の素数であるものとする。

加法群G_1として、楕円曲線Ｅ上の点がなす群を用いる場合、楕円曲線Ｅには、ＤＨ問題を解くことが困難な楕円曲線を用いる。

ペアリング関数ｅには、例えば、テイトペアリングやヴェイユペアリングなど、双線形ペアリングを用いる。また、ペアリング関数ｅは、Ｇ－ＢＤＨ問題を解くことが困難であるものとする。

鍵導出関数Ｇは、任意のビット列を入力し、入力したビット列に対応する（所定のビット長を有する）ビット列を出力する関数である。例えば、現在一般に使用されているＳＨＡ（Ｓｅｃｕｒｅ Ｈａｓｈ Ａｌｇｏｒｉｔｈｍ）－１などのハッシュ関数を用いて、鍵導出関数Ｇを構成する。のちに説明する安全性証明は、ランダムオラクルモデルという

枠組みにおいて行われるものであり、鍵導出関数Ｇをランダムオラクルとみなして暗号方式の安全性を証明する。

変換関数Ｈは、任意のビット列を入力し、入力したビット列に対応する加法群$Ｇ_{2}$の要素を出力する関数である。のちに説明する安全性証明では、変換関数Ｈもランダムオラクルとみなして暗号方式の安全性を証明する。

【００５８】

第一要素選択部１１１は、ＣＰＵ９１１などの処理装置を用いて、加法群$Ｇ_{1}$の要素（例えば楕円曲線Ｅ上の点）$Ｐ_{1}$を選択する。このとき、第一要素選択部１１１は、加法群$Ｇ_{1}$の要素のなかから、任意の要素$Ｐ_{1}$をランダムに選択する。

第一要素選択部１１１は、ＣＰＵ９１１などの処理装置を用いて、選択した要素$Ｐ_{1}$を示す情報を、第一要素情報として出力する。

【００５９】

マスターキー選択部１１２は、ＣＰＵ９１１などの処理装置を用いて、自然数ｓを選択する。このとき、マスターキー選択部１１２は、加法群$Ｇ_{1}$の位数ｎより小さい自然数のなかから、自然数ｓをランダムに選択する。

マスターキー選択部１１２は、ＣＰＵ９１１などの処理装置を用いて、選択した自然数ｓを示す情報を、マスターキー情報として出力する。

【００６０】

マスターキー記憶部１１３は、ＣＰＵ９１１などの処理装置を用いて、マスターキー選択部１１２が出力したマスターキー情報を入力する。

マスターキー記憶部１１３は、磁気ディスク装置９２０などの記憶装置を用いて、入力したマスターキー情報を記憶する。マスターキー情報が外部に漏れると、第三者がユーザ秘密鍵を生成できてしまうので、ユーザ秘密鍵生成センタ１００は、マスターキー記憶部１１３が記憶したマスターキー情報が外部に漏れないよう、厳重に管理する。

【００６１】

なお、公開パラメータ生成部１１０とユーザ秘密鍵生成部１３０とを異なる装置とする場合、ユーザ秘密鍵生成部１３０を有する装置もマスターキー記憶部１１３を有し、公開パラメータ生成部１１０を有する装置から、秘密裡にマスターキー情報の通知を受け、通知されたマスターキー情報を記憶する。

【００６２】

第二要素算出部１２１は、ＣＰＵ９１１などの処理装置を用いて、第一要素選択部１１１が出力した第一要素情報を入力する。

第二要素算出部１２１は、ＣＰＵ９１１などの処理装置を用いて、マスターキー記憶部１１３が記憶したマスターキー情報を入力する。

第二要素算出部１２１は、ＣＰＵ９１１などの処理装置を用いて、入力した第一要素情報と、入力したマスターキー情報とに基づいて、加法群$Ｇ_{1}$の要素$Ｐ_{ｐｕｂ}$を算出する。このとき、第二要素算出部１２１は、第一要素情報が示す加法群$Ｇ_{1}$の要素$Ｐ_{1}$と、マスターキー情報が示す自然数ｓとから、要素$Ｐ_{1}$のｓ倍を計算し、加法群$Ｇ_{1}$の要素$Ｐ_{ｐｕｂ}$とする。

ここで、加法群$Ｇ_{1}$の要素Ｐのｓ倍とは、加法群$Ｇ_{1}$の要素Ｐをｓ回加算した要素のことである。

第二要素算出部１２１は、ＣＰＵ９１１などの処理装置を用いて、算出した加法群$Ｇ_{1}$の要素$Ｐ_{ｐｕｂ}$を示す情報を、第二要素情報として出力する。

【００６３】

パラメータ公開部１２２は、ＣＰＵ９１１などの処理装置を用いて、第一要素選択部１１１が出力した第一要素情報を入力する。

パラメータ公開部１２２は、ＣＰＵ９１１などの処理装置を用いて、第二要素算出部１２１が出力した第二要素情報を入力する。

パラメータ公開部１２２は、ＣＰＵ９１１などの処理装置を用いて、入力した第一要素情報と、入力した第二要素情報とを含む情報を、パラメータ情報として公開する。ここで

、「公開する」とは、例えば、インターネットに接続したサーバ装置にパラメータ情報を記憶し、送信者装置２００や受信者装置３００の要求に応じてダウンロードできるようにしたり、送信者装置２００や受信者装置３００に対して、パラメータ情報を含む電子メールなどを送信したりすることである。

なお、パラメータ公開部１２２が公開するパラメータ情報には、上記のほか、加法群G_1、加法群G_2、乗法群G_Tを示す情報（例えば、楕円曲線Ｅの係数や位数）、ペアリング関数$e：G_1 \times G_2 \rightarrow G_T$、鍵導出関数Ｇ、変換関数Ｈなどを示す情報が含まれる。

【００６４】

識別情報取得部１３１は、ＣＰＵ９１１などの処理装置を用いて、受信者装置３００のＩＤを示す情報（識別情報）を取得する。

識別情報取得部１３１は、ＣＰＵ９１１などの処理装置を用いて、取得したＩＤを示す情報を出力する。

受信者装置３００のＩＤは、公開された情報であり、受信者装置３００本人のものであることが明白なものであるから、識別情報取得部１３１は、必ずしも受信者装置３００のＩＤを、受信者装置３００自身から取得する必要はない。

【００６５】

第三要素算出部１３２は、ＣＰＵ９１１などの処理装置を用いて、識別情報取得部１３１が出力した受信者装置３００のＩＤを示す情報を入力する。

第三要素算出部１３２は、ＣＰＵ９１１などの処理装置を用いて、入力した受信者装置３００のＩＤを示す情報に対応する加法群G_2の要素Q_{ID}を算出する。このとき、第三要素算出部１３２は、パラメータ公開部１２２が公開した変換関数Ｈを用いて、受信者装置３００のＩＤを示す情報を、加法群G_2の要素Q_{ID}に変換する。

第三要素算出部１３２は、ＣＰＵ９１１などの処理装置を用いて、算出した加法群G_2の要素Q_{ID}を示す情報を、第三要素情報として出力する。

【００６６】

秘密鍵算出部１３３は、ＣＰＵ９１１などの処理装置を用いて、第三要素算出部１３２が出力した第三要素情報を入力する。

秘密鍵算出部１３３は、ＣＰＵ９１１などの処理装置を用いて、マスターキー記憶部１１３が記憶したマスターキー情報を入力する。

秘密鍵算出部１３３は、ＣＰＵ９１１などの処理装置を用いて、入力した第三要素情報と、入力したマスターキー情報とに基づいて、加法群G_2の要素d_{ID}を算出する。このとき、秘密鍵算出部１３３は、第三要素情報が示す加法群G_2の要素Q_{ID}と、マスターキー情報が示す自然数ｓとから、要素Q_{ID}のｓ倍を計算し、加法群G_2の要素d_{ID}とする。

秘密鍵算出部１３３は、ＣＰＵ９１１などの処理装置を用いて、算出した加法群G_2の要素d_{ID}を示す情報を、ユーザ秘密鍵情報として出力する。

【００６７】

秘密鍵通知部１３４は、ＣＰＵ９１１などの処理装置を用いて、秘密鍵算出部１３３が出力したユーザ秘密鍵情報を入力する。

秘密鍵通知部１３４は、ＣＰＵ９１１などの処理装置を用いて、入力したユーザ秘密鍵情報を、受信者装置３００に対して、秘密裡に通知する。

ユーザ秘密鍵情報が受信者装置３００以外の第三者に漏れると、その第三者は、暗号化セッション鍵からセッション鍵を復元できてしまうので、ユーザ秘密鍵生成センタ１００は、受信者装置３００以外の第三者にユーザ秘密鍵情報が漏れないよう、安全な方法で受信者装置３００にユーザ秘密鍵情報を通知する。

【００６８】

図５は、この実施の形態における送信者装置２００の機能ブロックの一例を示すブロック構成図である。

【００６９】

送信者装置２００は、パラメータ取得部２１１、第一要素記憶部２１２、第二要素記憶

部２１３、自然数選択部２２１、第四要素算出部２２２、暗号化セッション鍵送信部２２３、送信識別情報取得部２３１、第五要素算出部２３２、送信ペアリング値算出部２３３、セッション鍵生成部２３４、セッション鍵記憶部２３５、平文記憶部２４１、暗号文生成部２４２、暗号文送信部２４３を有する。

【００７０】

パラメータ取得部２１１は、ＣＰＵ９１１などの処理装置を用いて、ユーザ秘密鍵生成センタ１００が公開したパラメータ情報を取得する。例えば、ユーザ秘密鍵生成センタ１００がパラメータ情報を登録したサーバ装置に接続して、パラメータ情報をダウンロードしたり、ユーザ秘密鍵生成センタ１００からパラメータ情報を含む電子メールを受信したりする。

パラメータ取得部２１１は、ＣＰＵ９１１などの処理装置を用いて、取得したパラメータ情報に含まれる第一要素情報と、第二要素情報とを出力する。

第一要素情報は、ユーザ秘密鍵生成センタ１００が選択した加法群G_1の要素P_1を示す情報である。

第二要素情報は、ユーザ秘密鍵生成センタ１００が算出した加法群G_1の要素P_{pub}を示す情報である。

【００７１】

第一要素記憶部２１２は、ＣＰＵ９１１などの処理装置を用いて、パラメータ取得部２１１が出力した第一要素情報を入力する。

第一要素記憶部２１２は、磁気ディスク装置９２０などの記憶装置を用いて、入力した第一要素情報を記憶する。

【００７２】

第二要素記憶部２１３は、ＣＰＵ９１１などの処理装置を用いて、パラメータ取得部２１１が出力した第二要素情報を入力する。

第二要素記憶部２１３は、磁気ディスク装置９２０などの記憶装置を用いて、入力した第二要素情報を記憶する。

【００７３】

自然数選択部２２１は、ＣＰＵ９１１などの処理装置を用いて、自然数ｒを選択する。このとき、自然数選択部２２１は、加法群G_1の位数ｎ未満の自然数のなかから、自然数ｒをランダムに選択する。なお、加法群G_1の位数ｎを示す情報は、ユーザ秘密鍵生成センタ１００が公開したパラメータ情報に含まれている。自然数選択部２２１は、パラメータ取得部２１１が取得したパラメータ情報から、加法群G_1の位数ｎを示す情報を取得し、これに基づいて、自然数ｒを選択する。

自然数選択部２２１は、ＣＰＵ９１１などの処理装置を用いて、選択した自然数ｒを示す情報を、乱数情報として出力する。

自然数選択部２２１が選択する自然数ｒは、受信者装置３００との通信に用いるセッション鍵を生成する原料になるものである。

【００７４】

第四要素算出部２２２は、ＣＰＵ９１１などの処理装置を用いて、第一要素記憶部２１２が記憶した第一要素情報を入力する。

第四要素算出部２２２は、ＣＰＵ９１１などの処理装置を用いて、自然数選択部２２１が出力した乱数情報を入力する。

第四要素算出部２２２は、ＣＰＵ９１１などの処理装置を用いて、入力した第一要素情報と、入力した乱数情報とに基づいて、加法群G_1の要素Ｒを算出する。このとき、第四要素算出部２２２は、第一要素情報が示す加法群G_1の要素P_1と、乱数情報が示す自然数ｒとから、要素P_1のｒ倍を計算し、加法群G_1の要素Ｒとする。

第四要素算出部２２２は、ＣＰＵ９１１などの処理装置を用いて、算出した加法群G_1の要素Ｒを示す情報を、第四要素情報として出力する。

【００７５】

暗号化セッション鍵送信部２２３は、ＣＰＵ９１１などの処理装置を用いて、第四要素

算出部２２２が出力した第四要素情報を入力する。
暗号化セッション鍵送信部２２３は、通信装置９１５を用いて、入力した第四要素情報を、暗号化セッション鍵C_0として、受信者装置３００に対して送信する。
【００７６】
暗号化セッション鍵C_0は、インターネットなどのオープンなネットワークを介して送信する。したがって、攻撃者が暗号化セッション鍵C_0を入手する可能性がある。また、攻撃者は、ユーザ秘密鍵生成センタ１００が公開したパラメータ情報から、第一要素情報及び第二要素情報を入手することができる。
したがって、攻撃者は、加法群G_1の要素P_1、P_{pub}（＝sP_1）、R（＝rP_1）を知ることができる。しかし、例えば、加法群G_1が楕円曲線E上の点がなす群である場合、楕円曲線EはDH問題を解くことが困難な楕円曲線なので、攻撃者が、これらの情報から自然数sや自然数rを算出することは極めて困難である。
【００７７】
送信識別情報取得部２３１は、ＣＰＵ９１１などの処理装置を用いて、受信者装置３００のＩＤを示す情報（識別情報）を取得する。
送信識別情報取得部２３１は、ＣＰＵ９１１などの処理装置を用いて、取得した受信者装置３００のＩＤを示す情報を出力する。
【００７８】
第五要素算出部２３２は、ＣＰＵ９１１などの処理装置を用いて、送信識別情報取得部２３１が出力した受信者装置３００のＩＤを示す情報を入力する。
第五要素算出部２３２は、ＣＰＵ９１１などの処理装置を用いて、入力した受信者装置３００のＩＤを示す情報に対応する加法群G_2の要素Q_{ID}を算出する。このとき、第五要素算出部２３２は、ユーザ秘密鍵生成センタ１００が公開した変換関数Hを用いて、受信者装置３００のＩＤを示す情報を、加法群G_2の要素Q_{ID}に変換する。したがって、第五要素算出部２３２が算出する要素Q_{ID}は、ユーザ秘密鍵生成センタ１００の第三要素算出部１３２が算出する要素Q_{ID}と同一である。
第五要素算出部２３２は、ＣＰＵ９１１などの処理装置を用いて、算出した加法群G_2の要素Q_{ID}を示す情報を、第五要素情報として出力する。
【００７９】
送信ペアリング値算出部２３３は、ＣＰＵ９１１などの処理装置を用いて、第二要素記憶部２１３が記憶した第二要素情報を入力する。
送信ペアリング値算出部２３３は、ＣＰＵ９１１などの処理装置を用いて、第五要素算出部２３２が出力した第五要素情報を入力する。
送信ペアリング値算出部２３３は、ＣＰＵ９１１などの処理装置を用いて、自然数選択部２２１が出力した乱数情報を入力する。
送信ペアリング値算出部２３３は、ＣＰＵ９１１などの処理装置を用いて、入力した第二要素情報と、入力した第五要素情報と、入力した乱数情報とに基づいて、加法群G_1の要素P_{pub}と、加法群G_2の要素Q_{ID}とのペアリング値のｒ乗を算出して、乗法群G_Tの要素ｗとする。このとき、送信ペアリング値算出部２３３は、ユーザ秘密鍵生成センタ１００が公開したペアリング関数$e：G_1 \times G_2 \rightarrow G_T$を用いて、第二要素情報が示す加法群$G_1$の要素$P_{pub}$と、第五要素情報が示す加法群$G_2$の要素$Q_{ID}$と、乱数情報が示す自然数ｒとから、$e(P_{pub}, Q_{ID})^r$を計算し、ｗとする。
送信ペアリング値算出部２３３は、ＣＰＵ９１１などの処理装置を用いて、算出した乗法群G_Tの要素ｗを示す情報を、送信ペアリング値情報として出力する。
【００８０】
セッション鍵生成部２３４は、ＣＰＵ９１１などの処理装置を用いて、第四要素算出部２２２が出力した第四要素情報を入力する。
セッション鍵生成部２３４は、ＣＰＵ９１１などの処理装置を用いて、送信ペアリング値算出部２３３が出力した送信ペアリング値情報を入力する。
セッション鍵生成部２３４は、ＣＰＵ９１１などの処理装置を用いて、入力した第四要

素情報と、入力した送信ペアリング値情報とに基づいて、ハッシュ値を算出する。このとき、セッション鍵生成部２３４は、ユーザ秘密鍵生成センタ１００が公開した鍵導出関数Ｇを用いて、ハッシュ値を算出する。セッション鍵生成部２３４は、ＣＰＵ９１１などの処理装置を用いて、第四要素情報と送信ペアリング値情報とを結合してビット列情報を生成し、生成したビット列情報を鍵導出関数Ｇの入力とする。

ここで情報Ａと情報Ｂとの「結合」とは、情報Ａを構成するビット列（ビット長ａ）と情報Ｂを構成するビット列（ビット長ｂ）とをすべて含むビット列（ビット長ａ＋ｂ）を生成することである。例えば、情報Ａを構成するビット列のあとに、情報Ｂを構成するビット列をつなげて、全体として１つのビット列を構成する。情報Ａと情報Ｂの順序は逆でもよいし、情報Ａのビットと情報Ｂのビットとを交互に並べてもよい。

【００８１】

セッション鍵生成部２３４は、ＣＰＵ９１１などの処理装置を用いて、算出したハッシュ値に基づいて、セッション鍵Ｋを生成する。この例において、セッション鍵生成部２３４は、算出したハッシュ値を示す情報をそのままセッション鍵Ｋとする。

セッション鍵生成部２３４は、ＣＰＵ９１１などの処理装置を用いて、生成したセッション鍵Ｋを出力する。

セッション鍵生成部２３４が生成したセッション鍵Ｋは、受信者装置３００との通信を暗号化するために用いるものである。

【００８２】

セッション鍵記憶部２３５は、ＣＰＵ９１１などの処理装置を用いて、セッション鍵生成部２３４が出力したセッション鍵Ｋを入力する。

セッション鍵記憶部２３５は、磁気ディスク装置９２０などの記憶装置を用いて、入力したセッション鍵Ｋを記憶する。

【００８３】

平文記憶部２４１は、磁気ディスク装置９２０などの記憶装置を用いて、受信者装置３００に対して通知すべき平文情報を記憶している。

【００８４】

暗号文生成部２４２は、ＣＰＵ９１１などの処理装置を用いて、平文記憶部２４１が記憶した平文情報を入力する。

暗号文生成部２４２は、ＣＰＵ９１１などの処理装置を用いて、セッション鍵記憶部２３５が記憶したセッション鍵Ｋを入力する。

暗号文生成部２４２は、ＣＰＵ９１１などの処理装置を用いて、入力した平文情報を、入力したセッション鍵Ｋで暗号化して、暗号文情報を生成する。

なお、暗号文生成部２４２が平文情報を暗号化する際に使用する暗号方式は、共通鍵暗号方式とする。例えば、暗号文生成部２４２は、ＣＰＵ９１１などの処理装置を用いて、平文情報をセッション鍵Ｋと同じビット長のブロックに分割して平文ブロックとし、それぞれの平文ブロックとセッション鍵Ｋとのビットごとの排他的論理和を算出して暗号文ブロックとし、暗号文ブロックをすべて結合して暗号文情報を生成する。

暗号文生成部２４２は、ＣＰＵ９１１などの処理装置を用いて、生成した暗号文情報を出力する。

【００８５】

暗号文送信部２４３は、ＣＰＵ９１１などの処理装置を用いて、暗号文生成部２４２が出力した暗号文情報を入力する。

暗号文送信部２４３は、通信装置９１５を用いて、入力した暗号文情報を、受信者装置３００に対して送信する。

【００８６】

暗号文情報は、インターネットなどのオープンなネットワークを介して送信する。したがって、攻撃者が暗号文情報を入手する可能性がある。暗号文情報は、共通鍵暗号方式により暗号化されているので、暗号文情報を復号するには、暗号化に用いたセッション鍵Ｋと同一の鍵が必要である。

セッション鍵Ｋは、送信者装置２００が外部に漏れないよう、厳重に保管する。したがって、攻撃者がセッション鍵Ｋを入手することはできない。攻撃者は、暗号化セッション鍵$Ｃ_0$を入手することはできる。しかし、暗号化セッション鍵$Ｃ_0$からセッション鍵Ｋを復元するには、ユーザ秘密鍵情報が必要なので、攻撃者が暗号化セッション鍵$Ｃ_0$からセッション鍵Ｋを復元することもできない。したがって、攻撃者は暗号文を復号することができない。

【００８７】

図６は、この実施の形態における受信者装置３００の機能ブロックの一例を示すブロック構成図である。

【００８８】

受信者装置３００は、受信パラメータ取得部３１１、秘密鍵取得部３２１、秘密鍵記憶部３２２、暗号化セッション鍵受信部３３１、受信ペアリング値算出部３３３、セッション鍵復元部３３４、受信セッション鍵記憶部３３５、暗号文受信部３４１、暗号文復号部３４２を有する。

【００８９】

受信パラメータ取得部３１１は、ＣＰＵ９１１などの処理装置を用いて、ユーザ秘密鍵生成センタ１００が公開したパラメータ情報を取得する。

【００９０】

秘密鍵取得部３２１は、ＣＰＵ９１１などの処理装置を用いて、ユーザ秘密鍵生成センタ１００が秘密裡に通知したユーザ秘密鍵情報を取得する。

秘密鍵取得部３２１は、磁気ディスク装置９２０などの記憶装置を用いて、ユーザ秘密鍵情報を記憶する。

ユーザ秘密鍵情報は、加法群$Ｇ_2$の要素$ｄ_{ＩＤ}$を示す情報である。ユーザ秘密鍵情報は、暗号化セッション鍵$Ｃ_0$からセッション鍵Ｋを復元するための情報なので、受信者装置３００は、秘密鍵記憶部３２２が記憶したユーザ秘密鍵情報が外部に漏れないよう、厳重に保管する。

【００９１】

暗号化セッション鍵受信部３３１は、通信装置９１５を用いて、送信者装置２００が送信してきた暗号化セッション鍵$Ｃ_0$を受信する。

暗号化セッション鍵受信部３３１は、ＣＰＵ９１１などの処理装置を用いて、受信した暗号化セッション鍵$Ｃ_0$に含まれる第四要素情報を出力する。

第四要素情報は、加法群$Ｇ_1$の要素Ｒを示す情報である。

【００９２】

受信ペアリング値算出部３３３は、ＣＰＵ９１１などの処理装置を用いて、秘密鍵記憶部３２２が記憶したユーザ秘密鍵情報を入力する。

受信ペアリング値算出部３３３は、ＣＰＵ９１１などの処理装置を用いて、暗号化セッション鍵受信部３３１が出力した第四要素情報を入力する。

受信ペアリング値算出部３３３は、ＣＰＵ９１１などの処理装置を用いて、入力したユーザ秘密鍵情報と、入力した第四要素情報とに基づいて、楕円曲線Ｅ上の点Ｒと、楕円曲線Ｅ上の点$ｄ_{ＩＤ}$とのペアリング値を算出して、乗法群$Ｇ_Ｔ$の要素ｗ’とする。このとき、受信ペアリング値算出部３３３は、ユーザ秘密鍵生成センタ１００が公開したペアリング関数$ｅ：Ｇ_1 \times Ｇ_2 \rightarrow Ｇ_Ｔ$を用いて、第四要素情報が示す加法群$Ｇ_1$の要素Ｒと、ユーザ秘密鍵情報が示す加法群$Ｇ_2$の要素$ｄ_{ＩＤ}$とから、$ｅ（Ｒ，ｄ_{ＩＤ}）$を計算し、ｗ’とする。

受信ペアリング値算出部３３３は、ＣＰＵ９１１などの処理装置を用いて、算出した乗法群$Ｇ_Ｔ$の要素ｗ’を示す情報を、受信ペアリング値情報として出力する。

【００９３】

ここで、受信ペアリング値算出部３３３が算出した乗法群$Ｇ_Ｔ$の要素ｗ’は、送信者装置２００の送信ペアリング値算出部２３３が算出した乗法群$Ｇ_Ｔ$の要素ｗと等しい。

なぜなら、$Ｒ＝ｒＰ_1$、$ｄ_{ＩＤ}＝ｓＱ_{ＩＤ}$であるから、$ｗ’＝ｅ（Ｒ，ｄ_{ＩＤ}）＝ｅ（$

ｒＰ$_1$，ｓＱ$_{ID}$）である。ペアリング関数ｅ：Ｇ$_1$×Ｇ$_2$→Ｇ$_T$は双線形なので、ｗ’＝ｅ（Ｐ$_1$，Ｑ$_{ID}$）^{rs}である。

一方、Ｐ$_{pub}$＝ｓＰ$_1$であるから、ｗ＝ｅ（Ｐ$_{pub}$，Ｑ$_{ID}$）^{r}＝ｅ（ｓＰ$_1$，Ｑ$_{ID}$）^{r}＝ｅ（Ｐ$_1$，Ｑ$_{ID}$）^{rs}であり、ｗ＝ｗ’となる。

【００９４】

セッション鍵復元部３３４は、ＣＰＵ９１１などの処理装置を用いて、暗号化セッション鍵受信部３３１が出力した第四要素情報を入力する。

セッション鍵復元部３３４は、ＣＰＵ９１１などの処理装置を用いて、受信ペアリング値算出部３３３が出力した受信ペアリング値情報を入力する。

セッション鍵復元部３３４は、ＣＰＵ９１１などの処理装置を用いて、入力した第四要素情報と、入力した受信ペアリング値情報とに基づいて、ハッシュ値を算出する。このとき、セッション鍵復元部３３４は、ユーザ秘密鍵生成センタ１００が公開した鍵導出関数Ｇを用いて、ハッシュ値を算出する。セッション鍵生成部２３４は、ＣＰＵ９１１などの処理装置を用いて、第四要素情報と受信ペアリング情報とを結合してビット列情報を生成し、生成したビット列情報を鍵導出関数Ｇの入力とする。

【００９５】

受信ペアリング値算出部３３３が算出した乗法群Ｇ$_T$の要素ｗ’は、送信者装置２００の送信ペアリング値算出部２３３が算出した乗法群Ｇ$_T$の要素ｗと等しいので、受信ペアリング値算出部３３３が出力した受信ペアリング値情報は、送信者装置２００の送信ペアリング値算出部２３３が出力した送信ペアリング値情報と同一である。

したがって、セッション鍵復元部３３４が鍵導出関数Ｇの入力として生成したビット列情報は、送信者装置２００のセッション鍵生成部２３４が鍵導出関数Ｇの入力として生成したビット列情報と同一である。鍵導出関数Ｇは、同一の入力に対して常に同一の出力をする関数であるから、セッション鍵復元部３３４が算出したハッシュ値は、送信者装置２００のセッション鍵生成部２３４が算出したハッシュ値と同一となる。

【００９６】

セッション鍵復元部３３４は、ＣＰＵ９１１などの処理装置を用いて、算出したハッシュ値に基づいて、セッション鍵Ｋを復元する。この例において、セッション鍵復元部３３４は、算出したハッシュ値を示す情報を、そのままセッション鍵Ｋとする。

セッション鍵復元部３３４は、ＣＰＵ９１１などの処理装置を用いて、復元したセッション鍵Ｋを出力する。

【００９７】

セッション鍵復元部３３４が算出したハッシュ値は、送信者装置２００のセッション鍵生成部２３４が算出したハッシュ値と同一であるから、セッション鍵復元部３３４は、送信者装置２００のセッション鍵生成部２３４が生成したセッション鍵Ｋと同一のセッション鍵を復元する。

【００９８】

受信セッション鍵記憶部３３５は、ＣＰＵ９１１などの処理装置を用いて、セッション鍵復元部３３４が出力したセッション鍵Ｋを入力する。

受信セッション鍵記憶部３３５は、磁気ディスク装置９２０などの記憶装置を用いて、入力したセッション鍵Ｋを記憶する。

【００９９】

暗号文受信部３４１は、通信装置９１５を用いて、送信者装置２００が送信してきた暗号文情報を受信する。

暗号文受信部３４１は、ＣＰＵ９１１などの処理装置を用いて、受信した暗号文情報を出力する。

【０１００】

暗号文復号部３４２は、ＣＰＵ９１１などの処理装置を用いて、暗号文受信部３４１が出力した暗号文情報を入力する。

暗号文復号部３４２は、ＣＰＵ９１１などの処理装置を用いて、受信セッション鍵記憶

部３３５が記憶したセッション鍵Ｋを入力する。
暗号文復号部３４２は、ＣＰＵ９１１などの処理装置を用いて、入力した暗号文情報を、入力したセッション鍵Ｋで復号して、平文情報を生成する。例えば、暗号文復号部３４２は、ＣＰＵ９１１などの処理装置を用いて、暗号文情報をセッション鍵Ｋと同じビット長のブロックに分割して暗号文ブロックとし、それぞれの暗号文ブロックとセッション鍵Ｋとのビットごとの排他的論理和を算出して平文ブロックとし、平文ブロックをすべて結合して平文情報を生成する。
暗号文復号部３４２は、ＣＰＵ９１１などの処理装置を用いて、生成した平文情報を出力する。
【０１０１】
セッション鍵復元部３３４が復元したセッション鍵Ｋは、送信者装置２００の暗号文生成部２４２が暗号化に使用したセッション鍵と同一であるから、暗号文復号部３４２は、暗号文情報を正しく復号できる。
【０１０２】
図７は、この実施の形態におけるユーザ秘密鍵生成センタ１００がパラメータ情報を生成するパラメータ生成処理の流れの一例を示すフローチャート図である。
パラメータ生成処理は、セットアップ（Ｓｅｔｕｐ）処理とも呼ばれる。
【０１０３】
Ｓ１１において、第一要素選択部１１１は、ＣＰＵ９１１などの処理装置を用いて、加法群$Ｇ_{1}$の要素$Ｐ_{1}$をランダムに選択する。
第一要素選択部１１１は、ＣＰＵ９１１などの処理装置を用いて、選択した要素$Ｐ_{1}$を示す情報を第一要素情報として出力する。
【０１０４】
Ｓ１２において、マスターキー選択部１１２は、ＣＰＵ９１１などの処理装置を用いて、自然数ｓをランダムに選択する。
マスターキー選択部１１２は、ＣＰＵ９１１などの処理装置を用いて、選択した自然数ｓを示す情報をマスターキー情報として出力する。
マスターキー記憶部１１３は、ＣＰＵ９１１などの処理装置を用いて、マスターキー選択部１１２が出力したマスターキー情報を入力する。
マスターキー記憶部１１３は、磁気ディスク装置９２０などの記憶装置を用いて、入力したマスターキー情報を記憶する。
【０１０５】
Ｓ１３において、第二要素算出部１２１は、ＣＰＵ９１１などの処理装置を用いて、Ｓ１１で第一要素選択部１１１が出力した第一要素情報と、Ｓ１２でマスターキー記憶部１１３が記憶したマスターキー情報とを入力する。
第二要素算出部１２１は、ＣＰＵ９１１などの処理装置を用いて、入力した第一要素情報と、入力したマスターキー情報とに基づいて、要素Ｐのｓ倍を算出し、加法群$Ｇ_{1}$の要素$Ｐ_{ｐｕｂ}$とする。
第二要素算出部１２１は、ＣＰＵ９１１などの処理装置を用いて、算出した要素$Ｐ_{ｐｕｂ}$を示す情報を第二要素情報として出力する。
【０１０６】
Ｓ１４において、パラメータ公開部１２２は、ＣＰＵ９１１などの処理装置を用いて、Ｓ１１で第一要素選択部１１１が出力した第一要素情報と、Ｓ１３で第二要素算出部１２１が出力した第二要素情報とを入力する。
パラメータ公開部１２２は、ＣＰＵ９１１などの処理装置を用いて、入力した第一要素情報と、入力した第二要素情報とを含むパラメータ情報を公開する。
【０１０７】
図８は、この実施の形態におけるユーザ秘密鍵生成センタ１００がユーザ秘密鍵を生成する秘密鍵生成処理の流れの一例を示すフローチャート図である。
秘密鍵生成処理は、エクストラクト（Ｅｘｔｒａｃｔ）処理とも呼ばれる。

【０１０８】
Ｓ２１において、識別情報取得部１３１は、ＣＰＵ９１１などの処理装置を用いて、ユーザ秘密鍵を生成する受信者装置３００のＩＤを示す情報を取得する。
識別情報取得部１３１は、ＣＰＵ９１１などの処理装置を用いて、取得した受信者装置３００のＩＤを示す情報を出力する。
【０１０９】
Ｓ２２において、第三要素算出部１３２は、ＣＰＵ９１１などの処理装置を用いて、Ｓ２１で識別情報取得部１３１が出力した受信者装置３００のＩＤを示す情報を入力する。
第三要素算出部１３２は、ＣＰＵ９１１などの処理装置を用いて、入力した受信者装置３００のＩＤを示す情報に対応する加法群$Ｇ_{2}$の要素$Ｑ_{ＩＤ}$を算出する。
第三要素算出部１３２は、ＣＰＵ９１１などの処理装置を用いて、算出した加法群$Ｇ_{2}$の要素$Ｑ_{ＩＤ}$を示す情報を第三要素情報として出力する。
【０１１０】
Ｓ２３において、秘密鍵算出部１３３は、Ｓ２２で第三要素算出部１３２が出力した第三要素情報と、図７のＳ１２でマスターキー記憶部１１３が記憶したマスターキー情報とを入力する。
秘密鍵算出部１３３は、ＣＰＵ９１１などの処理装置を用いて、入力した第三要素情報とマスターキー情報とに基づいて、加法群$Ｇ_{2}$の要素$Ｑ_{ＩＤ}$のｓ倍を算出し、加法群$Ｇ_{2}$の要素$ｄ_{ＩＤ}$とする。
秘密鍵算出部１３３は、ＣＰＵ９１１などの処理装置を用いて、算出した加法群$Ｇ_{2}$の要素$ｄ_{ＩＤ}$を示す情報をユーザ秘密鍵情報として出力する。
【０１１１】
Ｓ２４において、秘密鍵通知部１３４は、ＣＰＵ９１１などの処理装置を用いて、Ｓ２３で秘密鍵算出部１３３が出力したユーザ秘密鍵情報を入力する。
秘密鍵通知部１３４は、ＣＰＵ９１１などの処理装置を用いて、入力したユーザ秘密鍵情報を、受信者装置３００に対して秘密裡に通知する。
【０１１２】
図９は、この実施の形態における送信者装置２００がセッション鍵Ｋを生成するセッション鍵生成処理の流れの一例を示すフローチャート図である。
セッション鍵生成処理は、エンカプスレイト（Ｅｎｃａｐｓｕｌａｔｅ）処理とも呼ばれる。
【０１１３】
Ｓ３１において、パラメータ取得部２１１は、ＣＰＵ９１１などの処理装置を用いて、図７のＳ１４でユーザ秘密鍵生成センタ１００が公開したパラメータ情報を取得する。
パラメータ取得部２１１は、ＣＰＵ９１１などの処理装置を用いて、取得したパラメータ情報に含まれる第一要素情報と第二要素情報とを出力する。
第一要素記憶部２１２は、ＣＰＵ９１１などの処理装置を用いて、パラメータ取得部２１１が出力した第一要素情報を入力する。
第一要素記憶部２１２は、磁気ディスク装置９２０などの記憶装置を用いて、入力した第一要素情報を記憶する。
第二要素記憶部２１３は、ＣＰＵ９１１などの処理装置を用いて、パラメータ取得部２１１が出力した第二要素情報を入力する。
第二要素記憶部２１３は、磁気ディスク装置９２０などの記憶装置を用いて、入力した第二要素情報を記憶する。
【０１１４】
Ｓ３２において、送信識別情報取得部２３１は、ＣＰＵ９１１などの処理装置を用いて、平文情報を通知したい相手である受信者装置３００のＩＤを示す情報を取得する。
送信識別情報取得部２３１は、ＣＰＵ９１１などの処理装置を用いて、取得した受信者装置３００のＩＤを示す情報を出力する。
【０１１５】

Ｓ３３において、自然数選択部２２１は、ＣＰＵ９１１などの処理装置を用いて、自然数ｒをランダムに選択する。

自然数選択部２２１は、ＣＰＵ９１１などの処理装置を用いて、選択した自然数ｒを示す情報を乱数情報として出力する。

【０１１６】

Ｓ３４において、第四要素算出部２２２は、ＣＰＵ９１１などの処理装置を用いて、Ｓ３１で第一要素記憶部２１２が記憶した第一要素情報と、Ｓ３３で自然数選択部２２１が出力した乱数情報とを入力する。

第四要素算出部２２２は、ＣＰＵ９１１などの処理装置を用いて、入力した第一要素情報と、入力した乱数情報とに基づいて、加法群G_1の要素P_1のｒ倍を算出し、加法群G_1の要素Ｒとする。

第四要素算出部２２２は、ＣＰＵ９１１などの処理装置を用いて、算出した加法群G_1の要素点Ｒを示す情報を第四要素情報として出力する。

【０１１７】

Ｓ３５において、第五要素算出部２３２は、ＣＰＵ９１１などの処理装置を用いて、Ｓ３２で送信識別情報取得部２３１が出力した受信者装置３００のＩＤを示す情報を入力する。

第五要素算出部２３２は、ＣＰＵ９１１などの処理装置を用いて、入力した受信者装置３００のＩＤを示す情報に対応する加法群G_2の要素Q_{ID}を算出する。

第五要素算出部２３２は、ＣＰＵ９１１などの処理装置を用いて、算出した加法群G_2の要素Q_{ID}を示す情報を第五要素情報として出力する。

【０１１８】

Ｓ３６において、送信ペアリング値算出部２３３は、ＣＰＵ９１１などの処理装置を用いて、Ｓ３１で第二要素記憶部２１３が記憶した第二要素情報と、Ｓ３５で第五要素算出部２３２が出力した第五要素情報と、Ｓ３３で自然数選択部２２１が出力した乱数情報とを入力する。

送信ペアリング値算出部２３３は、ＣＰＵ９１１などの処理装置を用いて、入力した第二要素情報と、入力した第五要素情報と、入力した乱数情報とに基づいて、加法群G_1の要素P_{pub}と加法群G_2の要素Q_{ID}とのペアリング値ｅ（P_{pub}，Q_{ID}）のｒ乗を算出し、乗法群G_Tの要素ｗとする。

送信ペアリング値算出部２３３は、ＣＰＵ９１１などの処理装置を用いて、算出した乗法群G_Tの要素ｗを示す情報を、送信ペアリング値情報として出力する。

【０１１９】

Ｓ３７において、セッション鍵生成部２３４は、ＣＰＵ９１１などの処理装置を用いて、Ｓ３４で第四要素算出部２２２が出力した第四要素情報と、Ｓ３６で送信ペアリング値算出部２３３が出力した送信ペアリング値情報とを入力する。

セッション鍵生成部２３４は、ＣＰＵ９１１などの処理装置を用いて、入力した第四要素情報と、入力した送信ペアリング値情報とを結合してビット列情報を生成する。

セッション鍵生成部２３４は、ＣＰＵ９１１などの処理装置を用いて、生成したビット列情報に対応するハッシュ値を算出し、セッション鍵Ｋとする。

セッション鍵生成部２３４は、ＣＰＵ９１１などの処理装置を用いて、生成したセッション鍵Ｋを出力する。

セッション鍵記憶部２３５は、ＣＰＵ９１１などの処理装置を用いて、セッション鍵生成部２３４が出力したセッション鍵Ｋを入力する。

セッション鍵記憶部２３５は、磁気ディスク装置９２０などの記憶装置を用いて、入力したセッション鍵Ｋを記憶する。

【０１２０】

Ｓ３８において、暗号化セッション鍵送信部２２３は、ＣＰＵ９１１などの処理装置を用いて、Ｓ３４で第四要素算出部２２２が出力した第四要素情報を入力する。

暗号化セッション鍵送信部２２３は、通信装置９１５を用いて、平文情報を通知したい

受信者装置３００に対して、入力した第四要素情報を、暗号化セッション鍵C_0として送信する。

【０１２１】

図１０は、この実施の形態における受信者装置３００がセッション鍵Ｋを復元するセッション鍵復元処理の流れの一例を示すフローチャート図である。

セッション鍵復元処理は、デカプスレイト（Ｄｅｃａｐｓｕｌａｔｅ）処理とも呼ばれる。

【０１２２】

Ｓ４１において、受信パラメータ取得部３１１は、ＣＰＵ９１１などの処理装置を用いて、図７のＳ１４でユーザ秘密鍵生成センタ１００が公開したパラメータ情報を取得する。

【０１２３】

Ｓ４２において、秘密鍵取得部３２１は、ＣＰＵ９１１などの処理装置を用いて、図８のＳ２４でユーザ秘密鍵生成センタ１００が通知したユーザ秘密鍵情報を取得する。

秘密鍵取得部３２１は、ＣＰＵ９１１などの処理装置を用いて、取得したユーザ秘密鍵情報を出力する。

秘密鍵記憶部３２２は、ＣＰＵ９１１などの処理装置を用いて、秘密鍵取得部３２１が出力したユーザ秘密鍵情報を入力する。

秘密鍵記憶部３２２は、磁気ディスク装置９２０などの記憶装置を用いて、入力したユーザ秘密鍵情報を記憶する。

【０１２４】

Ｓ４３において、暗号化セッション鍵受信部３３１は、通信装置９１５を用いて、図９のＳ３８で送信者装置２００が送信してきた暗号化セッション鍵C_0を受信する。

暗号化セッション鍵受信部３３１は、ＣＰＵ９１１などの処理装置を用いて、受信した暗号化セッション鍵C_0に含まれる第四要素情報を出力する。

【０１２５】

Ｓ４４において、受信ペアリング値算出部３３３は、ＣＰＵ９１１などの処理装置を用いて、Ｓ４３で暗号化セッション鍵受信部３３１が出力した第四要素情報と、Ｓ４２で秘密鍵記憶部３２２が記憶したユーザ秘密鍵情報とを入力する。

受信ペアリング値算出部３３３は、ＣＰＵ９１１などの処理装置を用いて、入力した第四要素情報と、入力したユーザ秘密鍵情報とに基づいて、加法群G_1の要素Ｒと、加法群G_2の要素d_{ID}とのペアリング値ｅ（Ｒ，d_{ID}）を算出し、乗法群G_Tの要素ｗ’とする。

受信ペアリング値算出部３３３は、ＣＰＵ９１１などの処理装置を用いて、算出した乗法群G_Tの要素ｗ’を示す情報を受信ペアリング値情報として出力する。

【０１２６】

なお、入力した第四要素情報が正しく加法群G_1の要素を示していない場合は、処理を続けることができないので、受信ペアリング値算出部３３３は、ＣＰＵ９１１などの処理装置を用いて、第四要素情報が加法群G_1の要素を示しているか否かを判断し、加法群G_1の要素を示していると判断した場合に、上述の処理を行う。

第四要素情報が加法群G_1の要素を示していないと判断した場合、受信ペアリング値算出部３３３は、ＣＰＵ９１１などの処理装置を用いて、セッション鍵の復元に失敗したことを示す情報を出力し、セッション鍵復元処理を中断する。

【０１２７】

Ｓ４５において、セッション鍵復元部３３４は、ＣＰＵ９１１などの処理装置を用いて、Ｓ４３で暗号化セッション鍵受信部３３１が出力した第四要素情報と、Ｓ４４で受信ペアリング値算出部３３３が出力した受信ペアリング値情報とを入力する。

セッション鍵復元部３３４は、ＣＰＵ９１１などの処理装置を用いて、入力した第四要素情報と、入力した受信ペアリング値情報とを結合して、ビット列情報を生成する。

セッション鍵復元部３３４は、ＣＰＵ９１１などの処理装置を用いて、生成したビット

列情報に対応するハッシュ値を算出し、セッション鍵Ｋとする。
セッション鍵復元部３３４は、ＣＰＵ９１１などの処理装置を用いて、復元したセッション鍵Ｋを出力する。
受信セッション鍵記憶部３３５は、ＣＰＵ９１１などの処理装置を用いて、セッション鍵復元部３３４が出力したセッション鍵Ｋを入力する。
受信セッション鍵記憶部３３５は、磁気ディスク装置９２０などの記憶装置を用いて、入力したセッション鍵Ｋを記憶する。
【０１２８】
次に、この実施の形態における暗号方式の安全性について説明する。
【０１２９】
図１１は、ここで議論するＫＥＭにおけるＩＮＤ－ＩＤ－ＣＣＡ安全性の定義に登場する攻撃者Ａを示す図である。
【０１３０】
攻撃者Ａは、セットアップオラクル、鍵漏洩オラクル、復号オラクル、ランダムオラクルを呼び出して、暗号を解読するために必要な情報を収集し、暗号化オラクルが出力したセッション鍵$K^{\dagger}$と暗号化セッション鍵c^{*}との組み合わせが正しいか否かを判定する。
【０１３１】
セットアップオラクルは、攻撃者Ａからの要求を入力し、パラメータ情報を出力するオラクルである。
【０１３２】
鍵漏洩オラクルは、ＩＤ（識別情報）を入力し、入力したＩＤに対応するユーザ秘密鍵情報（楕円曲線Ｅ上の点d_{ID}）を出力するオラクルである。
【０１３３】
復号オラクルは、ＩＤと暗号化セッション鍵ｃとを入力し、入力したＩＤに対応するユーザ秘密鍵を用いて、暗号化セッション鍵ｃから復元したセッション鍵Ｋを出力するオラクルである。なお、復元に失敗した場合は「拒否」を出力するものとする。
【０１３４】
ランダムオラクルは、暗号化セッション鍵ｃとペアリング値情報（自然数ｗ）とを入力し、暗号化セッション鍵ｃとペアリング値情報とを結合したビット列情報（ｃ‖ｗ）に対応するハッシュ値Ｇ（ｃ‖ｗ）を出力するオラクルである。
【０１３５】
暗号化オラクルは、攻撃対象ID^{*}を入力し、セッション鍵$K^{\dagger}$と暗号化セッション鍵c^{*}とを出力する。セッション鍵$K^{\dagger}$は、入力したID^{*}に対応するユーザ秘密鍵を用いて暗号化セッション鍵c^{*}から復元した（正しい）セッション鍵K^{*}である場合と、暗号化セッション鍵c^{*}とは無関係の（正しくない）セッション鍵である場合とがあり、それぞれ１／２の確率である。
【０１３６】
図１２は、ここで議論する攻撃者Ａの攻撃シナリオを示すフローチャート図である。
【０１３７】
Ａ０１において、攻撃者Ａは、セットアップオラクルを呼び出し、パラメータ情報を取得する。
【０１３８】
Ａ０２において、攻撃者Ａは、任意のＩＤを選択（生成）する。攻撃者Ａは、選択したＩＤを鍵漏洩オラクルの入力として、鍵漏洩オラクルを呼び出し、鍵漏洩オラクルが出力したユーザ秘密鍵情報を取得する。
攻撃者Ａは、必要な回数だけ鍵漏洩オラクルを呼び出してよい。
【０１３９】
Ａ０３において、攻撃者Ａは、任意のＩＤと任意の暗号化セッション鍵ｃとを選択（生成）する。攻撃者Ａは、選択したＩＤと暗号化セッション鍵ｃとを復号オラクルの入力として、復号オラクルを呼び出し、復号オラクルが出力したセッション鍵Ｋ（または「拒否

」）を取得する。
攻撃者Ａは、必要な回数だけ復号オラクルを呼び出してよい。
【０１４０】
次に、攻撃者Ａは、暗号解読に十分な情報を収集できたか否かを判断する。不十分と判断した場合には、更に、鍵漏洩オラクルや復号オラクルを呼び出して、更に、情報を収集する。
攻撃者Ａが十分な情報を収集したと判断した場合は、Ａ０４へ進む。
【０１４１】
Ａ０４において、攻撃者Ａは、攻撃対象となるＩＤ＊を選択（生成）する。なお、攻撃対象ＩＤ＊は、鍵漏洩オラクルによりユーザ秘密鍵を取得したＩＤ以外のＩＤとする。
攻撃者Ａは、攻撃対象ＩＤ＊を暗号化オラクルの入力として、暗号化オラクルを呼び出し、暗号化オラクルが出力したセッション鍵Ｋ†と暗号化セッション鍵ｃ＊とを取得する。
【０１４２】
攻撃者Ａは、更に情報が必要であれば、鍵漏洩オラクルや復号オラクルを呼び出して、情報を収集する（Ａ０５・Ａ０６）。
ただし、鍵漏洩オラクルに入力するＩＤは、攻撃対象ＩＤ＊以外のＩＤとする。ユーザ秘密鍵情報があればセッション鍵を復元できるので、暗号を解読したことにはならないからである。
また、復号オラクルに入力するＩＤと暗号化セッション鍵ｃとは、攻撃対象ＩＤ＊と暗号化セッション鍵ｃ＊との組み合わせ以外のものとする。復号オラクルが暗号化セッション鍵ｃ＊を復元したセッション鍵を取得したのでは、暗号を解読したことにならないからである。
ただし、攻撃対象ＩＤ＊と他の暗号化セッション鍵との組み合わせや、他のＩＤと暗号化セッション鍵ｃ＊との組み合わせであれば、復号オラクルに入力してよいものとする。
【０１４３】
Ａ０７において、攻撃者Ａは、Ａ０４で取得したセッション鍵Ｋ†と暗号化セッション鍵ｃ＊とが正しい組み合わせであるか否かを判定する。
【０１４４】
このように、攻撃者Ａは、直接的な答え以外のあらゆる情報を収集することができるものとする。このような仮想的な攻撃者でも暗号を解読できないのであれば、現実の攻撃者は、それよりも収集できる情報が少ないので、暗号の解読は不可能であり、安全性が保証される。
【０１４５】
次に、このような攻撃者Ａの優位性εについて検討する。
【０１４６】
図１３は、この実施の形態における暗号方式の安全性をＧ－ＢＤＨ問題に帰着させるために想定する（ＩＤベースではない）公開鍵暗号方式を説明する説明図である。
【０１４７】
鍵設定処理は、この実施の形態におけるユーザ秘密鍵生成センタ１００に相当する装置が行う処理である。
鍵設定処理において、加法群G_1の要素P_1、加法群G_1の位数ｎ未満の自然数ｓ、加法群G_2の要素P_2及びＱをランダムに選択する。
加法群G_1の要素$P_{pub}=sP_1$、加法群G_2の要素$Q_{pub}=sP_2$Ｑ及びｄ＝ｓＱを算出する。
加法群G_1の要素P_1及びP_{pub}、加法群G_2の要素P_2、Q_{pub}及びＱを公開する（パラメータ情報）。
加法群G_2の要素ｄを秘密鍵として、通知する。
【０１４８】
セッション鍵生成処理は、この実施の形態における送信者装置２００に相当する装置が

行う処理である。
セッション鍵生成処理において、公開された加法群G_1の要素P_1及びP_{pub}、加法群G_2の要素P_2、Q_{pub}及びQを取得する。
加法群G_1の位数n未満の自然数rをランダムに選択する。
加法群G_1の要素$R=rP_1$を算出し、暗号化セッション鍵cとして送信する。
加法群G_1の要素P_{pub}と加法群G_2の要素Qとのペアリング値$e(P_{pub}, Q)$のr乗を算出し、乗法群G_Tの要素wとする。
ハッシュ値$G(c \| w)$を算出し、セッション鍵Kとする。
【０１４９】
セッション鍵復元処理は、この実施の形態における受信者装置３００に相当する装置が行う処理である。
セッション鍵復元処理において、公開された加法群G_1の要素P_1及びP_{pub}、加法群G_2の要素P_2、Q_{pub}及びQと、秘密鍵（加法群G_2の要素d）とを取得する。
セッション鍵生成処理で送信された暗号化セッション鍵c（加法群G_1の要素Rを示す情報）を受信する。
加法群G_1の要素Rと加法群G_2の要素dとのペアリング値$e(R, d)$を算出し、乗法群G_Tの要素w’とする。
ハッシュ値$G(c \| w')$を算出し、セッション鍵Kとする。
【０１５０】
ここで、$P_{pub}=sP_1$、$d=sQ$、$R=rP_1$であるから、$w=e(P_{pub}, Q)^r=e(sP_1, Q)^r=e(P_1, Q)^{sr}$、$w'=e(R, d)=e(rP_1, sQ)=e(P_1, Q)^{sr}$となり、$w=w'$である。
したがって、セッション鍵生成処理で生成したセッション鍵と、セッション鍵復元処理で復元したセッション鍵とは同一である。
【０１５１】
次に、優位性εの攻撃者Aが存在すると仮定して、攻撃者Aを利用して、上述した非ＩＤベース公開鍵暗号方式を攻撃する攻撃者Ｂを想定する。
【０１５２】
図１４は、一般的な攻撃者Ｂの攻撃シナリオを示すフローチャート図である。
【０１５３】
Ｂ０１において、攻撃者Ｂは、セットアップオラクルを呼び出し、パラメータ情報を取得する。
この場合のセットアップオラクルは、攻撃者Ｂからの要求を入力し、図１３の非ＩＤベース公開鍵暗号方式におけるパラメータ情報を出力するオラクルである。
【０１５４】
Ｂ０２において、攻撃者Ｂは、任意の暗号化セッション鍵cを選択する。攻撃者Ｂは、選択した暗号化セッション鍵cを復号オラクルの入力として、復号オラクルを呼び出し、復号オラクルが出力したセッション鍵K（または「拒否」）を取得する。
この場合の復号オラクルは、暗号化セッション鍵cを入力し、秘密鍵dを用いて、入力した暗号化セッション鍵cから復元したセッション鍵Kを出力するオラクルである。
【０１５５】
攻撃者Ｂは、暗号解読に十分な情報を得るまで、何回でも復号オラクルを呼び出して、情報を収集する。
攻撃者Ｂが十分な情報を収集したと判断した場合は、Ｂ０３へ進む。
【０１５６】
Ｂ０３において、攻撃者Ｂは、暗号化オラクルを呼び出し、セッション鍵$K^{\dagger}$と暗号化セッション鍵c^{*}とを取得する。
この場合の暗号化オラクルは、攻撃者からの要求を入力し、図１３の非ＩＤベース公開鍵暗号方式におけるセッション鍵$K^{\dagger}$と暗号化セッション鍵c^{*}とを出力するオラクルである。暗号化オラクルは、やはり、１／２の確率で、正しい組み合わせのセッション鍵K

†と暗号化セッション鍵ｃ＊とを出力し、１／２の確率で、正しくない組み合わせのセッション鍵Ｋ†と暗号化セッション鍵ｃ＊とを出力する。

【０１５７】

攻撃者Ｂは、更に情報が必要であれば、復号オラクルを呼び出して、更に情報を収集する（Ｂ０４）。

ただし、復号オラクルに入力する暗号化セッション鍵ｃは、暗号化セッション鍵ｃ＊以外とする。

攻撃者Ｂが十分な情報を収集したと判断した場合は、Ｂ０５へ進む。

【０１５８】

Ｂ０５において、攻撃者Ｂは、セッション鍵Ｋ†と暗号化セッション鍵ｃ＊とが正しい組み合わせか否かを判定する。

【０１５９】

図１５は、攻撃者Ａを利用して非ＩＤベース公開鍵暗号方式を攻撃する攻撃者Ｂの構成を示す図である。

【０１６０】

攻撃者Ｂは、攻撃者Ａを利用するため、攻撃者Ａを呼び出す。

攻撃者Ａは、セットアップオラクルなどのオラクルを呼び出し、暗号の解読を試みる。ここで、攻撃者Ａがオラクルと思って呼び出すブラックボックスの中身は、実は攻撃者Ｂである。攻撃者Ｂは、自分が攻撃している非ＩＤベース公開鍵暗号方式の解読に必要な情報を攻撃者Ａから引き出すための問題を設定し、攻撃者Ａに攻撃される（この実施の形態における）暗号方式をシミュレートする。

攻撃者Ａが、攻撃者Ｂにとって望ましくない方向へ進んだ場合、攻撃者Ｂは、攻撃者Ａから情報を得るのを断念する。それ以外の場合は、攻撃者Ａが判定結果を出力し、攻撃者Ｂが取得する。

【０１６１】

攻撃者Ｂは、攻撃者Ａの判定結果や攻撃者Ａがオラクルに入力した情報などに基づいて、自身の攻撃対象である非ＩＤベース公開鍵暗号方式を解読し、セッション鍵Ｋ†と暗号化セッション鍵ｃ＊とが正しい組み合わせか否かを判定する。

【０１６２】

図１６は、攻撃者Ａを利用して非ＩＤベース公開鍵暗号方式を攻撃する攻撃者Ｂのアルゴリズムを示すフローチャート図である。

【０１６３】

Ｂ１１において、攻撃者Ｂは、非ＩＤベース公開鍵暗号方式のセットアップオラクルを呼び出し、パラメータ情報（加法群G_1の要素P_1及びP_{pub}、加法群G_2の要素P_2、Q_{pub}及びＱなど）を取得する（図１４の攻撃シナリオにおけるＢ０１）。

【０１６４】

Ｂ１２において、攻撃者Ｂは、非ＩＤベース公開鍵暗号方式の暗号化オラクルを呼び出し、セッション鍵Ｋ†と暗号化セッション鍵ｃ＊との組を取得する（図１４の攻撃シナリオにおけるＢ０３）。

【０１６５】

Ｂ１３において、攻撃者Ｂは、攻撃者Ａを呼び出す。

【０１６６】

Ｂ１４において、攻撃者Ｂは、攻撃者Ａから呼び出されたオラクルをシミュレートする。

攻撃者Ａは様々なオラクルを何回も呼び出すので、攻撃者Ｂは、それにしたがって、様々なオラクルのシミュレートを繰り返す。

【０１６７】

攻撃者Ａが判定結果を出力した場合など、攻撃者ＢがＢ１２で取得したセッション鍵Ｋ†と暗号化セッション鍵ｃ＊との組み合わせが正しいか否かを判定するために必要な情報を、攻撃者Ｂが攻撃者Ａから取得した場合、Ｂ１５へ進む。

攻撃者Ｂは、攻撃者Ａが呼び出したオラクルの入力に基づいて、攻撃者Ａの判定結果などが、攻撃者Ｂにとって必要な情報となり得るか否かを判断する。
攻撃者Ｂが攻撃者Ａから必要な情報を取得し得ないと判断した場合、Ｂ１６へ進む。
【０１６８】
Ｂ１５において、攻撃者Ｂは、攻撃者Ａから取得した情報に基づいて、Ｂ１２で取得した非ＩＤベース公開鍵暗号方式のセッション鍵$K^{\dagger}$と暗号化セッション鍵c^{*}との組が、正しいか否かを判定する。
その後、Ｂ１７へ進む。
【０１６９】
Ｂ１６において、攻撃者Ｂは、判定結果をランダムに生成する。攻撃者Ｂは、Ｂ１２で取得したセッション鍵$K^{\dagger}$と暗号化セッション鍵c^{*}との組み合わせが正しいか否かを判定するために必要な情報を、攻撃者Ａからの得ることができなかったので、ランダムに判定する。ランダムな判定が当たる確率は、１／２である。
【０１７０】
Ｂ１７において、攻撃者Ｂは、判定した判定結果を出力する。
【０１７１】
図１７は、攻撃者Ｂがオラクルをシミュレートするオラクルシミュレート処理の流れを示すフローチャート図（その１）である。
これは、図１６のＢ１４に相当する処理である。
【０１７２】
攻撃者Ａは、図１６のＢ１３で呼び出されると、最初に（攻撃者Ｂがシミュレートする）セットアップオラクルを呼び出す（図１２の攻撃シナリオにおけるＡ０１）。
攻撃者Ａが呼び出したオラクルが、セットアップオラクルである場合、Ｂ２１へ進む。
【０１７３】
Ｂ２１において、攻撃者Ｂは、セットアップオラクルの出力として、攻撃者Ａに対して、（この実施の形態の暗号方式の）パラメータ情報を出力する。
攻撃者Ｂは、非ＩＤベース公開鍵暗号方式を攻撃するために必要な情報を攻撃者Ａから取得できるように、攻撃者Ａが攻撃する（この実施の形態の）暗号方式のパラメータを設定する。
【０１７４】
Ｂ１１で攻撃者Ｂが取得した（非ＩＤベース公開鍵暗号方式の）パラメータ情報と、Ｂ２１で攻撃者Ａに対して出力する（この実施の形態の暗号方式の）パラメータ情報との間には、次のような関係がある。
攻撃者Ａが攻撃する暗号に使用する加法群G_1、加法群G_2、乗法群G_T、ペアリング関数$e：G_1 \times G_2 \rightarrow G_T$は、攻撃者Ｂが攻撃する非ＩＤベース公開鍵暗号方式で使用するものと同一のものである。
攻撃者Ａが攻撃する暗号に使用する加法群G_1の要素P_1及びP_{pub}は、攻撃者Ｂが Ｂ１１で取得したパラメータ情報が示す加法群G_1の要素P_1及びP_{pub}と同一である。
攻撃者Ａが攻撃する暗号に使用する鍵導出関数Ｇは、やはり、攻撃者Ｂが攻撃する非ＩＤベース公開鍵暗号方式で使用するものと同一のものである。
なお、以下の議論において、鍵導出関数Ｇ及び変換関数Ｈは、ランダムオラクルであるものとする。攻撃者Ａは、鍵導出関数Ｇ及び変換関数Ｈの値が必要な場合、攻撃者Ｂがシミュレートしているランダムオラクルを呼び出すことにより、鍵導出関数Ｇや変換関数Ｈの値を取得する。
【０１７５】
その後、セットアップオラクルのシミュレート処理を終了し、攻撃者Ａが次のオラクルを呼び出すのを待つ。
【０１７６】
攻撃者Ａが呼び出したオラクルが、鍵導出関数Ｇであるランダムオラクル（以下「ラン

ダムオラクルG」という。）である場合、Ｂ３１へ進む。

【０１７７】

Ｂ３１において、攻撃者Ｂは、ランダムオラクルGの入力として、攻撃者Ａから、暗号化セッション鍵ｃ（加法群G_1の要素Rを示す情報（第四要素情報）を含む）と、乗法群G_Tの要素wを示す情報（送信ペアリング値情報）とを入力する。

【０１７８】

Ｂ３２において、攻撃者Ｂは、入力した情報をそのまま非ＩＤベース公開鍵暗号方式のランダムオラクルの入力として、非ＩＤベース公開鍵暗号方式のランダムオラクルを呼び出す。

攻撃者Ｂは、非ＩＤベース公開鍵暗号方式のランダムオラクルの出力を取得する。

【０１７９】

Ｂ３３において、攻撃者Ｂは、Ｂ３２で取得した情報をそのまま、ランダムオラクルGの出力として、攻撃者Ａに対して出力する。

攻撃者Ａが攻撃する暗号方式の鍵導出関数Gは、攻撃者Ｂが攻撃する非ＩＤベース公開鍵暗号方式の鍵導出関数Gと同一なので、攻撃者Ｂは、非ＩＤベース公開鍵暗号方式のランダムオラクルを呼び出すことにより、ランダムオラクルGの出力を取得する。

【０１８０】

その後、ランダムオラクルGのシミュレート処理を終了し、攻撃者Ａが次のオラクルを呼び出すのを待つ。

【０１８１】

攻撃者Ａが呼び出したオラクルが、変換関数Hであるランダムオラクル（以下「ランダムオラクルH」という。）である場合、Ｂ４１へ進む。

【０１８２】

Ｂ４１において、攻撃者Ｂは、ランダムオラクルHの入力として、攻撃者Ａから、ＩＤを示す情報を入力する。

【０１８３】

Ｂ４２において、攻撃者Ｂは、Ｂ４１で入力した情報が示すＩＤが、攻撃者Ａから問い合わせを受けたことがない（新しい）ＩＤか、既に問い合わせを受けたことがある（古い）ＩＤかを判断する。

攻撃者Ｂは、攻撃者Ａに対してランダムオラクルHとして答えた出力をリストH_{list}に記憶しておく。攻撃者Ｂは、リストH_{list}に基づいて、Ｂ４１で入力した情報が示すＩＤが新しいか古いかを判断する。

古いＩＤであると判断した場合、Ｂ４３へ進む。

新しいＩＤであると判断した場合、Ｂ４４へ進む。

【０１８４】

Ｂ４３において、攻撃者Ｂは、リストH_{list}に基づいて、ランダムオラクルHの出力として、攻撃者Ａに対して、前の出力と同じ出力をする。

【０１８５】

その後、ランダムオラクルHのシミュレート処理を終了し、攻撃者Ａが次のオラクルを呼び出すのを待つ。

【０１８６】

Ｂ４４において、攻撃者Ｂは、ランダムオラクルHが呼ばれたのが何回目であるかを判断する。

攻撃者Ｂは、あらかじめ、ランダムオラクルHが呼ばれる回数の上限q_H以下の自然数ｊをランダムに選択しておく。

ランダムオラクルHが呼ばれたのがｊ回目でないと判断した場合、Ｂ４５へ進む。

ランダムオラクルHが呼ばれたのがｊ回目であると判断した場合、Ｂ４６へ進む。

【０１８７】

Ｂ４５において、攻撃者Ｂは、加法群G_1の位数ｎより小さい自然数のなかから、自然数b_iをランダムに選択する。

攻撃者Ｂは、Ｂ１１で取得したパラメータ情報が示す加法群$Ｇ_2$の要素$Ｐ_2$と、選択した自然数$ｂ_i$とから、加法群$Ｇ_2$の要素$Ｐ_2$の$ｂ_i$倍を算出し、加法群$Ｇ_2$の要素$Ｑ_i$（$＝ｂ_i Ｐ_2$）とする。

攻撃者Ｂは、ランダムオラクルＨの出力として、攻撃者Ａに対して、算出した加法群$Ｇ_2$の要素$Ｑ_i$を示す情報を出力する。

攻撃者Ｂは、Ｂ４１で入力した情報が示すＩＤ、算出した加法群$Ｇ_2$の要素$Ｑ_i$、選択した自然数$ｂ_i$の組（ＩＤ，$Ｑ_i$，$ｂ_i$）を示す情報をリスト$Ｈ_{list}$に追加して、記憶する。

なお、組（ＩＤ，$Ｑ_i$，$ｂ_i$）は、ランダムオラクルＨの入力として、一番目の値「ＩＤ」を入力した場合に、ランダムオラクルＨの出力として、二番目の値「$Ｑ_i$」を出力したことを示す。また、三番目の値「$ｂ_i$」は、二番目の値「$Ｑ_i$」が、Ｂ１１で取得したパラメータ情報が示す加法群$Ｇ_2$の要素$Ｐ_2$の$ｂ_i$倍であることを示す。

【０１８８】

その後、ランダムオラクルＨのシミュレート処理を終了し、攻撃者Ａが次のオラクルを呼び出すのを待つ。

【０１８９】

Ｂ４６において、攻撃者Ｂは、ランダムオラクルＨの出力として、攻撃者Ａに対して、Ｂ１１で取得したパラメータ情報が示す加法群$Ｇ_2$の要素Ｑを出力する。

攻撃者Ｂは、Ｂ４１で入力した情報が示すＩＤ、出力した加法群$Ｇ_2$の要素Ｑ、「＊」の組（ＩＤ，Ｑ，＊）を示す情報をリスト$Ｈ_{list}$に追加して、記憶する。

ここで、組（ＩＤ，Ｑ，＊）の三番目の値「＊」のところには、本来、二番目の値である加法群$Ｇ_2$の要素Ｑが、Ｂ１１で取得したパラメータ情報が示す加法群$Ｇ_2$の要素$Ｐ_2$の何倍であるかを示す自然数（Ｂ４５における$ｂ_i$）を記憶すべきである。しかし、攻撃者Ｂは、加法群$Ｇ_2$の要素Ｑが加法群$Ｇ_2$の要素$Ｐ_2$の何倍であるかを知らないので、不明であることを示す印として「＊」を記憶する。「＊」は、Ｂ４５で記憶する$ｂ_i$として有り得ない数値（例えば、０）であってもよい。

【０１９０】

その後、ランダムオラクルＨのシミュレート処理を終了し、攻撃者Ａが次のオラクルを呼び出すのを待つ。

【０１９１】

攻撃者Ａがこれ以外のオラクルを呼び出した場合については、図１８で説明する。

【０１９２】

図１８は、攻撃者Ｂがオラクルをシミュレートするオラクルシミュレート処理の流れを示すフローチャート図（その２）である。

これは、図１７と同様に、図１６のＢ１４に相当する処理である。

【０１９３】

攻撃者Ａが呼び出したオラクルが、鍵漏洩オラクルである場合（図１２の攻撃シナリオにおけるＡ０２・Ａ０５）、Ｂ５１へ進む。

【０１９４】

Ｂ５１において、攻撃者Ｂは、鍵漏洩オラクルの入力として、攻撃者Ａから、ＩＤを示す情報を入力する。

【０１９５】

Ｂ５２において、攻撃者Ｂは、ランダムオラクルＨについてのオラクルシミュレート処理（図１７のＢ４１～Ｂ４６）を呼び出す。ランダムオラクルＨの入力は、Ｂ５１で入力したＩＤを示す情報である。ランダムオラクルＨの出力は、攻撃者Ａではなく、攻撃者Ｂ自身に渡される。

攻撃者Ｂは、リスト$Ｈ_{list}$に基づいて、Ｂ５１で入力した情報が示すＩＤに対応する組（ＩＤ，$Ｑ_{ＩＤ}$，$ｂ_{ＩＤ}$）を取得する。

【０１９６】

Ｂ５３において、攻撃者Ｂは、Ｂ５２で取得した$ｂ_{ＩＤ}$が「＊」であるか否かを判断す

る。
b_{ID}が「＊」でないと判断した場合、Ｂ５４へ進む。
b_{ID}が「＊」であると判断した場合、オラクルシミュレート処理を中断し、図１６のＢ１６へ進む。
【０１９７】
Ｂ５４において、攻撃者Ｂは、Ｂ１１で取得したパラメータ情報が示す加法群G_2の要素Q_{pub}と、Ｂ５２で取得したＢＩＤとから、加法群G_2の要素Q_{pub}のb_{ID}倍を算出し、加法群G_2の要素d_{ID}（$=b_{ID}Q_{pub}$）とする。
攻撃者Ｂは、鍵漏洩オラクルの出力として、攻撃者Ａに対して、算出した加法群G_2の要素d_{ID}（ユーザ秘密鍵）を出力する。
その後、鍵漏洩オラクルのシミュレート処理を終了し、攻撃者Ａが次のオラクルを呼び出すのを待つ。
【０１９８】
非ＩＤベース公開鍵暗号方式のパラメータ情報が示す加法群G_2の要素P_2と加法群G_2の要素Q_{pub}との間には、$Q_{pub}=sP_2$という関係がある（図１３の鍵設定処理参照）。
したがって、攻撃者Ｂが、あるＩＤについて、ランダムオラクルＨとして出力した加法群G_2の要素Q_{ID}と、鍵漏洩オラクルとして出力した加法群G_2の要素d_{ID}との間には、$d_{ID}=sQ_{ID}$という関係がある（$\because Q_{ID}=b_{ID}P_2$、$d_{ID}=b_{ID}Q_{pub}=b_{ID}sP_2$）。
すなわち、攻撃者Ｂは、非ＩＤベース公開鍵暗号方式のマスターキーである自然数ｓを知らされていないが、攻撃者Ａが攻撃する暗号のマスターキーとして、攻撃者Ｂ自身が知らない自然数ｓを設定していることになる。
【０１９９】
なお、Ｂ５２で取得したb_{ID}が「＊」である場合には、攻撃者Ｂは、ユーザ秘密鍵d_{ID}を算出できないので、鍵漏洩オラクルをシミュレートすることができない。そのため、Ｂ５３でb_{ID}が「＊」であるか否かを判断し、b_{ID}が「＊」である場合には、シミュレート処理を中断する。
【０２００】
攻撃者Ａが呼び出したオラクルが、復号オラクルである場合（図１２の攻撃シナリオにおけるＡ０３・Ａ０６）、Ｂ６１へ進む。
【０２０１】
Ｂ６１において、攻撃者Ｂは、復号オラクルの入力として、攻撃者Ａから、ＩＤを示す情報と、暗号化セッション鍵ｃとを入力する。
【０２０２】
Ｂ６２において、攻撃者Ｂは、ランダムオラクルＨについてのオラクルシミュレート処理（図１７のＢ４１～Ｂ４６）を呼び出す。ランダムオラクルＨの入力は、Ｂ６１で入力したＩＤを示す情報である。ランダムオラクルＨの出力は、攻撃者Ａではなく、攻撃者Ｂ自身に渡される。
攻撃者Ｂは、リストH_{list}に基づいて、Ｂ６１で入力した情報が示すＩＤに対応する組（ＩＤ，Q_{ID}，b_{ID}）を取得する。
【０２０３】
Ｂ６３において、攻撃者Ｂは、Ｂ６２で取得したb_{ID}が「＊」であるか否かを判断する。
b_{ID}が「＊」でないと判断した場合、Ｂ６４へ進む。
b_{ID}が「＊」であると判断した場合、Ｂ６５へ進む。
【０２０４】
Ｂ６４において、攻撃者Ｂは、Ｂ６１で入力したＩＤに対応するユーザ秘密鍵d_{ID}を算出する。すなわち、攻撃者Ｂは、Ｂ１１で取得したパラメータ情報が示す加法群G_2の要素Q_{pub}と、Ｂ６２で取得した自然数b_{ID}とから、加法群G_2の要素Q_{pub}のb

$_{ID}$倍を算出し、ユーザ秘密鍵、d_{ID}とする。
攻撃者Ｂは、Ｂ６１で入力した暗号化セッション鍵ｃを、算出したユーザ秘密鍵d_{ID}で復号し、復号結果とする。
その後、Ｂ６６へ進む。
【０２０５】
Ｂ６５において、攻撃者Ｂは、Ｂ６１で入力した暗号化セッション鍵ｃを、そのまま非ＩＤベース公開鍵暗号方式の復号オラクルの入力として、非ＩＤベース公開鍵暗号方式の復号オラクルを呼び出す（図１４の攻撃シナリオにおけるＢ０２・Ｂ０４）。
攻撃者Ｂは、非ＩＤベース公開鍵暗号方式の復号オラクルの出力を取得し、復号結果とする。
【０２０６】
Ｂ６６において、攻撃者Ｂは、復号オラクルの出力として、攻撃者Ａに対して、Ｂ６４またはＢ６５で取得した復号結果を出力する。
【０２０７】
その後、復号オラクルのシミュレート処理を終了し、攻撃者Ａが次のオラクルを呼び出すのを待つ。
【０２０８】
鍵漏洩オラクルの説明で述べたように、攻撃者Ｂは、攻撃者Ａが攻撃する暗号のマスターキーとして、攻撃者Ｂが攻撃する非ＩＤベース公開鍵暗号方式のマスターキーである自然数ｓを設定している。
攻撃者Ｂは、自然数ｓを知らないが、b_{ID}が「＊」でない場合には、ユーザ秘密鍵d_{ID}を算出できるので、これを用いて、暗号化セッション鍵ｃを復号する。
b_{ID}が「＊」である場合、攻撃者Ｂは、ユーザ秘密鍵d_{ID}（＝ｓＱ）を算出できないが、この場合のユーザ秘密鍵d_{ID}は、攻撃者Ｂが攻撃する非ＩＤベース公開鍵暗号方式の秘密鍵ｄと同じである（図１３の鍵設定処理参照）。
したがって、攻撃者Ｂは、非ＩＤベース公開鍵暗号方式の復号オラクルを呼び出すことにより、暗号化セッション鍵ｃを復号した復号結果を取得し、攻撃者Ａに対して出力することができる。
【０２０９】
攻撃者Ａが呼び出したオラクルが、暗号化オラクルである場合（図１２の攻撃シナリオにおけるＡ０４）、Ｂ７１へ進む。
【０２１０】
Ｂ７１において、攻撃者Ｂは、暗号化オラクルの入力として、攻撃者Ａから、攻撃対象ＩＤ*を示す情報を入力する。
【０２１１】
Ｂ７２において、攻撃者Ｂは、ランダムオラクルＨについてのオラクルシミュレート処理（図１７のＢ４１～Ｂ４６）を呼び出す。ランダムオラクルＨの入力は、Ｂ７１で入力したＩＤ*を示す情報である。ランダムオラクルＨの出力は、攻撃者Ａではなく、攻撃者Ｂ自身に渡される。
攻撃者Ｂは、リストH_{list}に基づいて、Ｂ７１で入力した情報が示すＩＤ*に対応する組（ＩＤ*，$Q_{ID}{}^{*}$，$b_{ID}{}^{*}$）を取得する。
【０２１２】
Ｂ７３において、攻撃者Ｂは、Ｂ７２で取得した$b_{ID}{}^{*}$が「＊」であるか否かを判断する。
$b_{ID}{}^{*}$が「＊」であると判断した場合、Ｂ７４へ進む。
$b_{ID}{}^{*}$が「＊」でないと判断した場合、オラクルシミュレート処理を中断し、図１６のＢ１６へ進む。
【０２１３】
Ｂ７４において、攻撃者Ｂは、暗号化オラクルの出力として、攻撃者Ａに対して、図１６のＢ１２で取得したセッション鍵$K^{\dagger}$と暗号化セッション鍵ｃ*との組を出力する。

その後、暗号化オラクルのシミュレート処理を終了し、攻撃者Ａが次のオラクルを呼び出すのを待つ。

【０２１４】

図１２の攻撃シナリオによれば、攻撃者Ａは、暗号化オラクルを呼び出したあと、必要に応じて鍵漏洩オラクルや復号オラクルを呼び出す（Ａ０５、Ａ０６）。

攻撃者Ｂは、これに対しても同様に、オラクルシミュレート処理を行い、オラクルとしての出力を、攻撃者Ａに対して、出力する。

【０２１５】

その後、攻撃者Ａは、セッション鍵$K^{\dagger}$と暗号化セッション鍵c^{*}との組み合わせが正しいか否かを判定し（図１２のＡ０７）、判定結果を出力する。

【０２１６】

攻撃者Ｂは、攻撃者Ａが出力した判定結果を取得し、取得した判定結果をそのまま非ＩＤベース公開鍵暗号方式に対する判定結果とする。

攻撃者Ｂは、取得した判定結果をそのまま出力する（図１６のＢ１５）。

【０２１７】

非ＩＤベース公開鍵暗号方式において暗号化セッション鍵ｃを復号する秘密鍵ｄ＝ｓＱは、攻撃者Ｂに知らされていない。

攻撃者Ｂは、攻撃者ＡがランダムオラクルHや復号オラクルに入力した情報が示すＩＤに対応する加法群G_2の要素Q_{ID}のうちの１つに、非ＩＤベース公開鍵暗号方式のパラメータである加法群G_2の要素Ｑを割り当てる。

攻撃者Ｂは、攻撃者Ａが攻撃する暗号方式のマスターキーを、上述したように自然数ｓに設定しているので、点Ｑを割り当てたＩＤに対応するユーザ秘密鍵d_{ID}は、ｓＱである。

【０２１８】

したがって、攻撃者Ａが攻撃対象ＩＤ*として、点Ｑを割り当てたＩＤを選択した場合、攻撃者Ｂは、攻撃者Ａの判定結果を、そのまま、非ＩＤベース公開鍵暗号方式を攻撃する攻撃者Ｂの判定結果とすることができる。攻撃者Ａの判定結果が正しければ、攻撃者Ｂの判定結果も正しく、攻撃者Ａの判定結果が間違っていれば、攻撃者Ｂの判定結果も間違うこととなる。

【０２１９】

攻撃者Ｂは、攻撃者Ａが望ましくない方向へ進んだ場合に、オラクルシミュレート処理を中断し、ランダムな判定を行う（図１６のＢ１６）ので、攻撃者Ｂの優位性ε_Bは、攻撃者Ａの優位性εより低い。

【０２２０】

ここで、攻撃者Ｂがオラクルシミュレート処理を中断する確率について検討する。

【０２２１】

攻撃者Ｂは、ランダムオラクルHに尋ねられたＩＤのうちの１つに、加法群G_2の要素Ｑを割り当て、攻撃者Ａがそのｉｄを攻撃対象ＩＤ*として選択した場合に、攻撃者Ａの判定結果を、自身の判定結果とする。

【０２２２】

図１２の攻撃シナリオによれば、攻撃者Ａは、鍵漏洩オラクルによりユーザ秘密鍵を取得したＩＤを攻撃対象ＩＤ*とすることはない。したがって、攻撃者Ａが鍵漏洩オラクルに質問したＩＤが、攻撃者Ｂが点Ｑを割り当てたＩＤである場合、それ以上処理を続けても意味がない。

また、攻撃者Ｂは、点Ｑを割り当てたＩＤに対応するユーザ秘密鍵d_{ID}を算出することができないので、そもそもオラクルシミュレート処理を続けることができない。

そこで、攻撃者Ｂはオラクルシミュレート処理を中断する（図１８のＢ５３で「b_{ID}＝＊」の場合）。

【０２２３】

ここで、ランダムオラクルHが呼び出されて、対応する加法群G_2の要素Q_{ID}を答え

たＩＤの数を、q_H’とする。また、鍵漏洩オラクルが呼び出されて、対応するユーザ秘密鍵d_{ID}を答えたＩＤの数をq_E’とする。

【０２２４】

鍵漏洩オラクルが呼ばれた場合、攻撃者Ｂは、自分でランダムオラクルＨを呼び出すので、鍵漏洩オラクルに尋ねられたＩＤの集合は、必ずランダムオラクルＨに尋ねられたＩＤの集合の部分集合である。

【０２２５】

したがって、攻撃者Ａが鍵漏洩オラクルに質問したＩＤ（q_E’個）のなかに、攻撃者Ｂが点Ｑを割り当てたＩＤがある確率は、q_E’／q_H’である。

【０２２６】

攻撃者Ｂがオラクルシミュレート処理を中断せず、攻撃者Ａが図１２の攻撃シナリオにおけるＡ０４（暗号化オラクルの呼び出し）までたどり着く確率は、$1-q_E$’／q_H’である。

【０２２７】

攻撃者Ａが攻撃対象ＩＤ*として、攻撃者Ｂが点Ｑを割り当てたＩＤ以外のＩＤを選択した場合、攻撃者Ｂは、攻撃者Ａの判定結果を、自身の判定結果とすることができない。

そこで、この場合も、攻撃者Ｂはオラクルシミュレート処理を中断する（図１８のＢ７３で「$b_{ID}{}^* \neq *$」の場合）。

【０２２８】

攻撃者Ａが、攻撃者Ｂが点Ｑを割り当てたＩＤを攻撃対象ＩＤ*に選ぶ確率は、１／q_H’である。

【０２２９】

攻撃者Ｂがオラクルシミュレート処理を中断せず、暗号化オラクルに答えた場合、攻撃者Ａは、必要に応じて鍵漏洩オラクルを呼び出す場合がある（図１２のＡ０５）。

【０２３０】

しかし、図１２の攻撃シナリオによれば、Ａ０５における鍵漏洩オラクルの呼び出しにおいて、攻撃者Ａは、攻撃対象ＩＤ*については質問しないことになっているので、この段階で、攻撃者Ｂがオラクルシミュレート処理を中断することはない。

【０２３１】

以上より、攻撃者Ｂがオラクルシミュレート処理を中断せず、攻撃者Ａの判定結果を取得する確率σは、$\sigma = 1/q_H' \cdot (1-q_E'/q_H')$である。

【０２３２】

ここで、ランダムオラクルＨを呼び出す回数の上限をq_H、鍵漏洩オラクルを呼び出す回数の上限をq_Eとする。

攻撃者が実際の暗号システムを攻撃する場合について考えると、ランダムオラクルＨの出力を得る関数は、パラメータ情報として公開されているので、攻撃者は、何回でもランダムオラクルＨを呼び出すことができる。これに対し、鍵漏洩オラクルは、例えば、複数の攻撃者が結託して複数のユーザ秘密鍵を入手した場合に相当するものであるから、攻撃者が鍵漏洩オラクルを呼び出す回数は、ランダムオラクルＨを呼び出す回数と比較して、極めて少ない。

そこで、$q_E \ll q_H$であるものとする。

【０２３３】

ランダムオラクルＨを呼び出すにあたり、ランダムオラクルＨに同じＩＤを複数回入力してもよいので、$q_H' \leqq q_H$である。同様に、$q_E' \leqq q_E$である。

σは、q_E’が大きければ大きいほど小さくなる。また、$2q_E' < q_H'$である場合、σは、q_Hが大きければ大きいほど小さくなる。

したがって、$\sigma \geqq 1/q_H \cdot (1-q_E/q_H)$である。

【０２３４】

攻撃者Ｂが攻撃者Ａの判定結果を取得した場合（確率σ）、攻撃者Ｂの判定結果が正しい確率は、攻撃者Ａの判定結果が正しい確率と等しいので、ε＋１／２（εは、この実施

の形態の暗号方式に対する攻撃者Ａの優位性。）である。

【０２３５】

攻撃者Ｂがオラクルシミュレート処理を中断した場合（確率１－σ）、攻撃者Ｂは、ランダムに判定をするので、攻撃者Ｂの判定結果が正しい確率は、１／２である。

【０２３６】

したがって、攻撃者Ｂの判定結果が正しい確率は、全体で、（ε＋１／２）・σ＋１／２・（１－σ）＝ε・σ＋１／２である。

【０２３７】

以上より、ここで想定した非ＩＤベース公開鍵暗号方式に対する攻撃者Ｂの優位性ε_Bは、$\varepsilon_B = \varepsilon \cdot \sigma \geqq \varepsilon / q_H \cdot (1 - q_E / q_H)$である。

【０２３８】

ここまでで、この実施の形態における暗号方式に対する優位性εの攻撃者Ａが存在すると仮定すると、上述した非ＩＤベース公開鍵暗号方式に対する優位性がε／q_H・（１－q_E／q_H）以上の攻撃者Ｂが構成できることが示された。

【０２３９】

次に、上述した攻撃者Ｂを利用して、Ｇ－ＢＤＨ問題に解答する解答者Ｃを想定する。

【０２４０】

図１９は、攻撃者Ｂを利用してＧ－ＢＤＨ問題に解答する解答者Ｃの構成を示す図である。

【０２４１】

解答者Ｃは、Ｇ－ＢＤＨ問題を与えられる。

解答者Ｃは、与えられたＧ－ＢＤＨ問題のパラメータとして、加法群G_1の要素P_1、$P_1{}^*$（＝$a_0 P_1$）及び$P_1{}^{**}$（＝$b_0 P_1$）、加法群G_2の要素P_2、$P_2{}^*$（＝$a_0 P_2$）、Q_2（＝$c_0 P_2$）を取得する。ただし、解答者Ｃには、a_0、b_0、c_0は知らされない。

解答者Ｃの目標は、ペアリング値$e(P_1, P_2)^{a_0 b_0 c_0}$を出力することである。

【０２４２】

解答者Ｃは、ペアリング値$e(P_1, P_2)^{a_0 b_0 c_0}$の候補となる値を絞りこむため、攻撃者Ｂを呼び出す。

解答者Ｃは、攻撃者Ｂの攻撃を受ける非ＩＤベース公開鍵暗号方式のオラクルをシミュレートして、攻撃者Ｂから情報を収集する。

解答者Ｃは、ペアリング値$e(P_1, P_2)^{a_0 b_0 c_0}$の候補となる値が見つかった場合、ＢＤＨ決定オラクルを呼び出して、その候補値が正解であるか否かを判断させる。

解答者Ｃは、ＢＤＨ決定オラクルが正解であると判断した場合に、その候補値を、解答者Ｃに与えられたＧ－ＢＤＨ問題に対する解答として出力する。

【０２４３】

ここで、攻撃者Ｂは攻撃者Ａを利用して非ＩＤベース公開鍵暗号方式を攻撃する攻撃者であるから、解答者Ｃは、攻撃者Ａを利用してＧ－ＢＤＨ問題に解答する解答者であるということができる。

あるいは、攻撃者Ｂと解答者Ｃとを含む全体（図の破線で示したブロック）を、攻撃者Ａを利用してＧ－ＢＤＨ問題に回答する解答者と考えてもよい。

【０２４４】

図２０は、攻撃者Ｂを利用してＧ－ＢＤＨ問題に解答する解答者Ｃのアルゴリズムを示すフローチャート図である。

【０２４５】

Ｃ１１において、解答者Ｃは、加法群G_1の要素P_1、$P_1{}^*$、$P_1{}^{**}$、P_2、$P_2{}^*$、Q_2を取得する。

【０２４６】

Ｃ１２において、解答者Ｃは、攻撃者Ｂを呼び出す。

【０２４７】
Ｃ１３において、解答者Ｃは、攻撃者Ｂが呼び出した非ＩＤベース公開鍵暗号方式のオラクルをシミュレートする。
【０２４８】
Ｃ１４において、解答者Ｃは、攻撃者Ｂがオラクルに入力した情報に基づいて、ペアリング値$e(P_1, P_2)^{a_0 b_0 c_0}$の候補となる値ｗを取得する。
解答者Ｃは、ＢＤＨ決定オラクルを呼び出して、$w = e(P_1, P_2)^{a_0 b_0 c_0}$であるか否かの判定結果を取得する。
ＢＤＨ決定オラクルが、$w = e(P_1, P_2)^{a_0 b_0 c_0}$であると判定した場合は、Ｃ１５へ進む。
ＢＤＨ決定オラクルが、$w \neq e(P_1, P_2)^{a_0 b_0 c_0}$であると判定した場合は、Ｃ１３に戻る。
【０２４９】
Ｃ１５において、解答者Ｃは、与えられたＧ－ＢＤＨ問題に対する解答として、ペアリング値ｗを出力する。
【０２５０】
図２１は、解答者Ｃがオラクルをシミュレートするオラクルシミュレート処理の流れを示すフローチャート図（その１）である。
これは、図２０のＣ１３に相当する処理である。
【０２５１】
攻撃者Ｂは、最初に、非ＩＤベース公開鍵暗号方式のセットアップオラクルを呼び出す（図１４のＢ０１）。
攻撃者Ｂが呼び出したオラクルが、セットアップオラクルである場合、Ｃ２１へ進む。
【０２５２】
Ｃ２１において、解答者Ｃは、セットアップオラクルの出力として、攻撃者Ｂに対して、攻撃者Ｂが攻撃する非ＩＤベース公開鍵暗号方式のパラメータ情報を出力する。
解答者Ｃは、与えられたＧ－ＢＤＨ問題に解答するために必要な情報を攻撃者Ｂから取得できるように、攻撃者Ｂが攻撃する非ＩＤベース公開鍵暗号方式のパラメータを設定する。
【０２５３】
Ｃ２１で解答者Ｃが出力する非ＩＤベース公開鍵暗号方式のパラメータと、Ｃ１１で解答者Ｃが入力したＧ－ＢＤＨ問題のパラメータとの間には、以下のような関係がある。
【０２５４】
非ＩＤベース公開鍵暗号方式で使用する加法群G_1、加法群G_2、乗法群G_T、ペアリング関数$e : G_1 \times G_2 \rightarrow G_T$は、与えられたＧ－ＢＤＨ問題と同一のものを使用する。
非ＩＤベース公開鍵暗号方式のパラメータである加法群G_1の要素P_1は、与えられたＧ－ＢＤＨ問題における加法群G_1の要素P_1である。
非ＩＤベース公開鍵暗号方式のパラメータである加法群G_1の要素P_{pub}は、与えられたＧ－ＢＤＨ問題における加法群G_1の要素P_1^*である。
非ＩＤベース公開鍵暗号方式のパラメータである加法群G_2の要素P_2は、与えられたＧ－ＢＤＨ問題における加法群G_2の要素P_2である。
非ＩＤベース公開鍵暗号方式のパラメータである加法群G_2の要素Q_{pub}は、与えられたＧ－ＢＤＨ問題における加法群G_2の要素P_2^*である。
非ＩＤベース公開鍵暗号方式のパラメータである加法群G_2の要素Ｑは、与えられたＧ－ＢＤＨ問題における加法群G_2の要素Q_2である。
すなわち、解答者Ｃは、与えられたＧ－ＢＤＨ問題の６つのパラメータのうち５つを、非ＩＤベース公開鍵暗号方式のパラメータとして、攻撃者Ｂに渡す。
【０２５５】
その後、セットアップオラクルのシミュレート処理を終了し、攻撃者Ｂが次のオラクルを呼び出すのを待つ。

【０２５６】
攻撃者Ｂが呼び出したオラクルが、暗号化オラクルである場合（図１４のＢ０３）、Ｃ３１へ進む。
【０２５７】
Ｃ３１において、解答者Ｃは、セッション鍵$K^{\dagger}$をランダムに生成する。
【０２５８】
Ｃ３２において、解答者Ｃは、暗号化オラクルとして、攻撃者Ｂに対して、Ｃ３１で生成したセッション鍵$K^{\dagger}$と、暗号化セッション鍵ｃ＊とを出力する。
なお、解答者Ｃは、Ｃ１１で入力したＧ－ＢＤＨ問題のパラメータである加法群G_1の要素P_1＊＊を示す情報を含む情報を、暗号化セッション鍵ｃ＊として出力する。
【０２５９】
その後、暗号化オラクルのシミュレート処理を終了し、攻撃者Ｂが次のオラクルを呼び出すのを待つ。
【０２６０】
セッション鍵$K^{\dagger}$がランダムな値なのは、解答者Ｃは、攻撃者Ｂが判定した判定結果には興味がなく、攻撃者Ｂが呼び出すオラクルの入力から情報を得ようとしているからである。
【０２６１】
攻撃者Ｂが、これ以外のオラクルを呼び出した場合については、図２２で説明する。
【０２６２】
図２２は、解答者Ｃがオラクルをシミュレートするオラクルシミュレート処理の流れを示すフローチャート図（その２）である。
これは、図２０のＣ１３に相当する処理である。
【０２６３】
攻撃者Ｂが呼び出したオラクルが、ランダムオラクルである場合（図１７のＢ３２）、Ｃ４１へ進む。
【０２６４】
Ｃ４１において、解答者Ｃは、ランダムオラクルの入力として、攻撃者Ｂから、暗号化セッション鍵ｃと、ペアリング値ｗを示す情報とを入力する。
暗号化セッション鍵ｃは、加法群G_1の要素Ｒを示す情報（第四要素情報）を含む。また、ペアリング値ｗは、乗法群G_Tの要素である。
【０２６５】
Ｃ４２において、解答者Ｃは、リストν_1を検索する。リストν_1は、ｃ、ｗ、Ｋの組（ｃ，ｗ，Ｋ）のリストである。リストν_1は、解答者Ｃが、ランダムオラクルのシミュレート処理において、それまでに入力した（ｃ，ｗ）の組と、その入力（ｃ，ｗ）に対して出力したＫとの対応関係を示すものである。
解答者Ｃは、リストν_1を検索し、Ｃ４１で入力した（ｃ，ｗ）について、それまでに同じ（ｃ，ｗ）を入力したことがあるか否かを判断する。
同じ（ｃ，ｗ）を入力したことがある場合、リストν_1から、その入力（ｃ，ｗ）に対して出力したＫを取得し、Ｃ５０へ進む。
同じ（ｃ，ｗ）を入力したことがない場合、Ｃ４３へ進む。
【０２６６】
Ｃ４３において、解答者Ｃは、ＢＤＨ決定オラクルを呼び出す。解答者Ｃは、ＢＤＨ決定オラクルに対して、P_1、P_1＊、Ｒ、P_2、P_2＊、Q_2、ｗを入力する。
なお、P_1、P_1＊、P_2、P_2＊、Q_2は、図２０のＣ１１で解答者Ｃが入力したＧ－ＢＤＨ問題のパラメータである。Ｒは、Ｃ４１で入力した暗号化セッション鍵ｃに含まれる情報（第四要素情報）が示す加法群G_1の要素である。ｗは、Ｃ４１で入力した情報が示すペアリング値（乗法群G_Tの要素）である。
【０２６７】
ＢＤＨ決定オラクルは、入力したP_1、P_1＊、Ｒ、P_2、P_2＊、Q_2に対応するペ

アリング値がｗと等しいか否かを判定し、判定結果を出力する。
ここで、解答者Ｃに与えられたＧ－ＢＤＨ問題のパラメータと、解答者ＣがＢＤＨ決定オラクルに入力するパラメータとの違いは、P_1^{**}がＲになっている点である。したがって、$R=P_1^{**}$であれば、ＢＤＨ決定オラクルは、ｗが解答者Ｃが答えるべきペアリング値であるか否かを判定することになる。
また、$P_1^{*}=P_{pub}$（$=sP_1$）、$R=rP_1$、$P_2^{*}=Q_{pub}$（$=sP_2$）であるから、ＢＤＨ決定オラクルは、$w=e(P_1, Q)^{sr}$であるか否かを判定することになる（$\because Q=c_0P_2$だから、ペアリングｅの双線形より、$e(P_1, P_2)^{src_0}=e(P_1, c_0P_2)^{sr}=e(P_1, Q)^{sr}$）。
【０２６８】
ＢＤＨ決定オラクルは、$w=e(P_1, Q)^{sr}$か否かを判定し、判定結果を出力する。
解答者Ｃは、ＢＤＨ決定オラクルが出力した判定結果を取得する。
ＢＤＨ決定オラクルが、$w=e(P_1, Q)^{sr}$であると判定した場合には、Ｃ４４へ進む。
ＢＤＨ決定オラクルが、$w\neq e(P_1, Q)^{sr}$であると判定した場合には、Ｃ４８へ進む。
【０２６９】
Ｃ４４において、解答者Ｃは、Ｃ４１で入力した暗号化セッション鍵ｃが、Ｃ３２で出力した暗号化セッション鍵c^{*}であるか否かを判断する。
$c=c^{*}$であると判断した場合、Ｃ４５へ進む。
$c\neq c^{*}$であると判断した場合、Ｃ４６へ進む。
【０２７０】
Ｃ４５において、解答者Ｃは、Ｇ－ＢＤＨ問題に対する解答として、ｗを出力し、処理を終了する（図２０のＣ１５）。
【０２７１】
Ｃ４１で入力した暗号化セッション鍵ｃが、Ｃ３２で出力した暗号化セッション鍵c^{*}である場合、暗号化セッション鍵ｃに含まれる情報が示す加法群G_1の要素Ｒは、Ｃ１１で入力したＧＢＤＨ問題のパラメータである加法群G_1の要素P_1^{**}である。
したがって、ペアリング値ｗは、解答者Ｃに対して与えられたＧ－ＢＤＨ問題の解答となる。
【０２７２】
Ｃ４６において、解答者Ｃは、組（ｃ，ｗ）をリストν_2に追加する。リストν_2は、ＢＤＨ決定オラクルが$w=e(P_1, Q)^{sr}$であると判定した組（ｃ，ｗ）のリストである。
【０２７３】
Ｃ４７において、解答者Ｃは、リストν_3を検索する。リストν_3は、暗号化セッション鍵ｃ、セッション鍵Ｋの組（ｃ，Ｋ）のリストである。リストν_3は、解答者Ｃが、復号オラクルのシミュレート処理（Ｃ５１～Ｃ５８）において、入力した暗号化セッション鍵ｃと、その入力ｃに対して出力したセッション鍵Ｋとの対応関係を示すものである。
解答者Ｃは、リストν_3を検索し、Ｃ４１で入力した暗号化セッション鍵ｃについて、それまでに復号オラクルが同じ暗号化セッション鍵ｃを入力したことがあるか否かを判断する。
復号オラクルが同じ暗号化セッション鍵ｃを入力したことがあると判断した場合、解答者Ｃは、復号オラクルがその入力ｃに対して出力したセッション鍵Ｋを、リストν_3から取得し、Ｃ４９へ進む。
復号オラクルが同じ暗号化セッション鍵ｃを入力したことがないと判断した場合、Ｃ４８へ進む。
【０２７４】
Ｃ４８において、解答者Ｃは、セッション鍵Ｋをランダムに生成する。

【０２７５】
Ｃ４９において、解答者Ｃは、Ｃ４１で入力したｃ、ｗと、Ｃ４７で取得したＫあるいはＣ４８で生成したＫとの組（ｃ，ｗ，Ｋ）を、リストν_1に追加する。
【０２７６】
Ｃ５０において、解答者Ｃは、ランダムオラクルの出力として、攻撃者Ｂに対して、Ｃ４２あるいはＣ４７で取得したＫ、またはＣ４８で生成したＫを、出力する。
【０２７７】
その後、ランダムオラクルのシミュレート処理を終了し、攻撃者Ｂが次のオラクルを呼び出すのを待つ。
【０２７８】
ランダムオラクルは、ランダムな値を出力するが、同じ入力に対しては同じ出力をする。
したがって、以前に入力したことがある（ｃ，ｗ）の組については、それに対応して出力したセッション鍵Ｋをリストν_1に記憶しておき、同じセッション鍵Ｋを出力する。
【０２７９】
また、ｃ，ｗの組み合わせが正しい場合、ランダムオラクルが出力するＫは、暗号化セッション鍵ｃを復号したものになるはずなので、同じｃを入力した復号オラクルが出力するＫと等しい。
ここで、ｃ，ｗの組み合わせが正しい場合とは、暗号化セッション鍵ｃに含まれる情報が示す加法群G_1の要素Ｒに基づいて算出したペアリング値ｅ（Ｒ，ｄ）（ただし、ｄは非ＩＤベース公開鍵暗号方式の秘密鍵）がｗと等しい場合のことである。
【０２８０】
非ＩＤベース公開鍵暗号方式の構成によれば、$e(R,d)=e(P_{pub},Q)^r=e(P_1,Q)^{sr}$であるから、解答者Ｃは、ｃ，ｗの組み合わせが正しいか否かを、ＢＤＨ決定オラクルの判定結果によって知ることができる。
したがって、以前に復号オラクルが入力したことがある暗号化セッション鍵ｃについては、それに対応して復号オラクルが出力したＫをリストν_3に記憶しておき、ＢＤＨ決定オラクルが$w=e(P_1,Q)^{sr}$であると判定した場合、同じセッション鍵Ｋを出力する。
【０２８１】
それ以外の場合、すなわち、ｃ，ｗの組み合わせが正しくない場合や、同じｃや（ｃ，ｗ）を入力したことがない場合には、ランダムに生成したセッション鍵Ｋを出力する。
【０２８２】
このようにして、解答者Ｃは、攻撃者Ｂから見たランダムオラクルをシミュレートする。
【０２８３】
攻撃者Ｂが呼び出したオラクルが、復号オラクルである場合、Ｃ５１へ進む。
【０２８４】
Ｃ５１において、解答者Ｃは、復号オラクルの入力として、攻撃者Ｂから暗号化セッション鍵ｃを入力する。
暗号化セッション鍵ｃは、加法群G_1の要素Ｒを示す情報（第四要素情報）を含む。
【０２８５】
Ｃ５２において、解答者Ｃは、加法群G_1の要素Ｒが、Ｇ－ＢＤＨ問題における加法群G_1の要素P_1^{**}と等しいか否かを判断する。
等しい場合、解答者Ｃは、Ｇ－ＢＤＨ問題に対する解答に失敗したものとして、処理を打ち切る。
等しくない場合、Ｃ５３へ進む。
【０２８６】
これは、Ｇ－ＢＤＨ問題における加法群G_1の要素P_1^{**}を示す情報を含む暗号化セッション鍵ｃについての復号結果を攻撃者Ｂに知らせてしまうと、解答者Ｃは、暗号化オ

ラクルとして、加法群G_1の要素P_1^{**}を示す情報を含む暗号化セッション鍵を、暗号化セッション鍵c^*として、攻撃者Ｂに対して出力する（図２１のＣ３２）ことができなくなってしまうからである。

【０２８７】

Ｃ５３において、解答者Ｃは、リストν_2を検索する。

解答者Ｃは、リストν_2を検索し、Ｃ５１で入力した暗号化セッション鍵ｃについて、正しい組み合わせの（ｃ，ｗ）を、それまでにランダムオラクルが入力したことがあるか否かを判断する。

ランダムオラクルが正しい組み合わせの（ｃ，ｗ）を入力したことがある場合、解答者Ｃは、更にリストν_1を検索し、正しい組み合わせの（ｃ，ｗ）に対して、ランダムオラクルが出力したセッション鍵Ｋを取得し、Ｃ５７へ進む。

ランダムオラクルが正しい組み合わせの（ｃ，ｗ）を入力したことがない場合、Ｃ５４へ進む。

【０２８８】

Ｃ５４において、解答者Ｃは、リストν_3を検索する。

解答者Ｃは、リストν_3を検索し、Ｃ５１で入力した暗号化セッション鍵ｃについて、それまでに復号オラクルが同じ暗号化セッション鍵ｃを入力したことがあるか否かを判断する。

復号オラクルが同じ暗号化セッション鍵ｃを入力したことがない場合、Ｃ５５へ進む。

復号オラクルが同じ暗号化セッション鍵ｃを入力したことがある場合、解答者Ｃは、リストν_3から、その入力ｃに対応して出力したセッション鍵Ｋを取得し、Ｃ５７へ進む。

【０２８９】

Ｃ５５において、解答者Ｃは、セッション鍵Ｋをランダムに生成する。

【０２９０】

Ｃ５６において、解答者Ｃは、Ｃ５１で入力した暗号化セッション鍵ｃとＣ５５で生成したセッション鍵Ｋとの組（ｃ，Ｋ）を、リストν_3に追加する。

【０２９１】

Ｃ５７において、解答者Ｃは、復号オラクルの出力として、攻撃者Ｂに対して、Ｃ５４あるいはＣ５４で取得したＫ、またはＣ５５で生成したＫを、出力する。

【０２９２】

その後、復号オラクルのシミュレート処理を終了し、攻撃者Ｂが次のオラクルを呼び出すのを待つ。

【０２９３】

復号オラクルが出力するセッション鍵Ｋは、入力した暗号化セッション鍵ｃを復号したものであり、ランダムオラクルが正しい組み合わせの（ｃ，ｗ）を入力した場合に出力するセッション鍵Ｋと等しい。

そのため、ランダムオラクルが入力した正しい組み合わせの（ｃ，ｗ）をリストν_2に記憶しておく。それに対応してランダムオラクルが出力したセッション鍵Ｋはリストν_1に記憶しておき、同じセッション鍵Ｋを出力する。

【０２９４】

また、同じ暗号化セッション鍵ｃを復号すれば、当然同じセッション鍵Ｋになるはずなので、復号オラクルが以前に入力したことがある暗号化セッション鍵ｃについては、それに対応して出力したセッション鍵Ｋをリストν_3に記憶しておき、同じセッション鍵Ｋを出力する。

【０２９５】

それ以外の場合には、ランダムに生成したセッション鍵Ｋを出力する。

【０２９６】

このようにして、解答者Ｃは、攻撃者Ｂから見た復号オラクルをシミュレートする。

【０２９７】

攻撃者Ｂは、非ＩＤベース公開鍵暗号方式に対して優位性を有するので、暗号化オラク

ルが出力したセッション鍵Ｋ†と暗号化セッション鍵ｃ＊とが正しく対応するものであるか否かを、（少なくとも確率的に）判断できる。
攻撃者Ｂがこの判断をするためには、復号オラクルによらず、独自に暗号化セッション鍵ｃ＊を復号したセッション鍵Ｋ＊を、なんらかの形で入手する必要がある。
セッション鍵Ｋ＊は、鍵導出関数Ｇ（ランダムオラクル）の出力であるから、セッション鍵Ｋ＊を入手するためには、ランダムオラクルに正しい値を入力する必要がある。
ランダムオラクルには、暗号化セッション鍵ｃ＊と、ｃ＊に正しく対応するペアリング値ｗ＊とを入力する。
このうち、暗号化セッション鍵ｃ＊は、暗号化オラクルから与えられるものであるが、ペアリング値ｗ＊は、攻撃者Ｂが独自に生成する必要がある。

【０２９８】
したがって、非ＩＤベース公開鍵暗号方式に対する優位性を有する攻撃者Ｂは、暗号化セッション鍵ｃ＊に正しく対応するペアリング値ｗ＊を生成することができる。

【０２９９】
上述したように、解答者Ｃは、暗号化セッション鍵ｃ＊に正しく対応するペアリング値ｗ＊が、解答者Ｃに対して与えられたＧ－ＢＤＨ問題の解答となるように、非ＩＤベース公開鍵暗号方式のパラメータを設定する。
解答者Ｃは、攻撃者Ｂがランダムオラクルに入力するｃ、ｗを監視し、暗号化セッション鍵ｃ＊を入力した場合に、ｗがｃ＊に正しく対応するもの（＝ｗ＊）であるか否かを、ＢＤＨ決定オラクルを使って判断する。
解答者Ｃは、攻撃者Ｂがｃ＊に正しく対応するｗ＊をランダムオラクルに入力した場合に、それをＧ－ＢＤＨ問題に対する解答として出力する。

【０３００】
ここで、攻撃者Ｂは、セッション鍵Ｋ†と暗号化セッション鍵ｃ＊との対応を、常に正しく判断するとは限らないので、ｃ＊に正しく対応するｗをランダムオラクルに入力しない場合もある。
攻撃者Ｂがｃ＊に正しく対応するｗをランダムオラクルに入力せず、判定結果を出力した場合、解答者Ｃの目論見は失敗し、解答者Ｃは、与えられたＧ－ＢＤＨ問題に対する解答を、攻撃者Ｂから取得することができない。その場合、解答者Ｃは、攻撃者Ｂの助けなしで、与えられたＧ－ＢＤＨ問題に対する解答を見つける必要がある。

【０３０１】
攻撃者Ｂが、セッション鍵ｃ＊と、ｃ＊に正しく対応するペアリング値ｗ＊とをランダムオラクルに入力する事象を$Ｆ_{2}$とし、事象$Ｆ_{2}$が発生する確率を$Ｐｒ［Ｆ_{2}］$とする。
また、解答者Ｃが、攻撃者Ｂの助けなしで、正解を見つける確率を$ε_{0}$とする。
解答者Ｃが、与えられたＧ－ＢＤＨ問題に正しく解答する確率を、Ｇ－ＢＤＨ問題に対する解答者Ｃの優位性$Ａｄｖ_{C}^{Ｇ－ＢＤＨ}$と定義すると、$Ａｄｖ_{C}^{Ｇ－ＢＤＨ}＝Ｐｒ［Ｆ_{2}］＋ε_{0}≧Ｐｒ［Ｆ_{2}］$（$∵ε_{0}≧０$）である。

【０３０２】
事象$Ｆ_{2}$が発生せず、攻撃者Ｂが判定結果を出力した場合、攻撃者Ｂは、セッション鍵ｃ＊と、ｃ＊に正しく対応するペアリング値ｗ＊とをランダムオラクルに入力していないので、攻撃者Ｂは、セッション鍵Ｋ†と暗号化セッション鍵ｃ＊との対応を正しく判定することができない。したがって、攻撃者Ｂの判定結果が正解である事象$Ｔ_{2}$が発生する確率$Ｐｒ［Ｔ_{2}］$は、１／２である。

【０３０３】
一方、攻撃者Ｂが、セッション鍵ｃ＊と、ｃ＊に正しく対応するペアリング値ｗ＊とをランダムオラクルに入力した場合でも、そこで処理を終了するのではなく、攻撃者Ｂが判定結果を出力するまで処理を続けたとすると、攻撃者Ｂは、非ＩＤベース公開鍵暗号方式に対する優位性を有するので、攻撃者Ｂの判定結果が正解である事象$Ｔ_{1}$が発生する確率$Ｐｒ［Ｔ_{1}］$は、１／２より大きい。

【０３０４】

ここで、事象T_1が発生する場合には、事象F_2が発生した場合と、事象F_2が発生せしなかった場合とが含まれる。

したがって、事象T_1が発生する確率$Pr[T_1]$は、事象F_2が発生し、かつ、攻撃者Bの判定結果が正解である確率（$Pr[F_2 \wedge T_1]$）と、事象F_2が発生せず、攻撃者Bの判定結果が正解である確率（$Pr[\neg F_2 \wedge T_1] = Pr[T_2]$）との和である（$Pr[T_1] = Pr[F_2 \wedge T_1] + Pr[T_2]$）。

【０３０５】

また、事象F_2が発生した場合であっても、必ずしも攻撃者Bの判定結果が正解であるとは限らないので、事象F_2が発生し、かつ、攻撃者Bの判定結果が正解である確率$Pr[F_2 \wedge T_1]$は、事象F_2が発生する確率$Pr[F_2]$以下である（$Pr[F_2 \wedge T_1] \leqq Pr[F_2]$）。

【０３０６】

以上より、$Pr[T_1] \leqq Pr[F_2] + 1/2$であることがわかる。

【０３０７】

解答者Cが処理を打ち切るもう一つのケースとして、攻撃者Bが暗号化オラクルを呼び出す前に、解答者Cが暗号化オラクルの出力として攻撃者Bに対して出力しようとしていたセッション鍵c^*を、攻撃者Bが復号オラクルに対して入力した場合がある。

この事象をF_1とし、F_1が発生する確率を$Pr[F_1]$とする。

【０３０８】

攻撃者Bが、判定結果を出すまでに復号オラクルに対して入力する暗号化セッション鍵cの総数をq_D'とする。加法群G_1の位数をnとすると、攻撃者Bは、加法群G_1のn個の要素のなかから、暗号化セッション鍵に含まれる情報が示す加法群G_1の要素Rを選択するので、$Pr[F_1] = q_D'/n$である。

攻撃者Bが復号オラクルを呼び出すのは、攻撃者Aが復号オラクルを呼び出した場合のうち「$b_{ID} = *$」である場合（図１８のＢ６５）なので、攻撃者Aが復号オラクルを呼び出す回数の最大値をq_Dとすると、$q_D' \leqq q_D$である。したがって、$Pr[F_1] \leqq q_D/n$である。

【０３０９】

一方、F_1が発生した場合には、攻撃者Bに対して、異なる問題を与えて処理を続け、攻撃者Bが判定結果を出力したとすると、攻撃者Bの判定結果が正解である事象T_0が発生する確率$Pr[T_0]$は、$\varepsilon_B + 1/2$（ただし、ε_Bは、想定した非ＩＤベース公開鍵暗号方式に対する攻撃者Bの優位性。）である。

【０３１０】

ここで、事象T_0が発生する場合には、事象F_1が発生した場合と、事象F_1が発生せしなかった場合とが含まれる。

したがって、事象T_0が発生する確率$Pr[T_0]$は、事象F_1が発生し、かつ、攻撃者Bの判定結果が正解である確率（$Pr[F_1 \wedge T_0]$）と、事象F_1が発生せず、攻撃者Bの判定結果が正解である確率（$Pr[\neg F_1 \wedge T_0] = Pr[T_1]$）との和である（$Pr[T_0] = Pr[F_1 \wedge T_0] + Pr[T_1]$）。

【０３１１】

事象F_1が発生し、かつ、攻撃者Bの判定結果が正解である確率$Pr[F_1 \wedge T_0]$は、当然、事象F_1が発生する確率$Pr[F_1]$以下である（$Pr[F_1 \wedge T_0] \leqq Pr[F_1]$）。

【０３１２】

以上より、$\varepsilon_B + 1/2 \leqq Pr[F_1] + Pr[T_1] \leqq q_D/n + Pr[F_2] + 1/2$。すなわち、$\varepsilon_B \leqq q_D/n + Pr[F_2]$であることがわかる。

【０３１３】

ここで、$Pr[F_2] \leqq Adv_C^{G-BDH}$だから、$\varepsilon_B \leqq Adv_C^{G-BDH} + q_D/n$。

【０３１４】

前述したように、攻撃者Ｂの優位性ε_Bは、$\varepsilon_B \geqq \varepsilon / q_H \cdot (1 - q_E / q_H)$（ただし、εは、攻撃者Ａのこの実施の形態における暗号方式に対する優位性。q_Hは、攻撃者Ａがランダムオラクルを呼び出す回数の最大値。q_Eは、攻撃者Ａが鍵漏洩オラクルを呼び出す回数の最大値。）である。

【０３１５】

したがって、解答者Ｃの優位性Adv_C^{G-BDH}は、$Adv_C^{G-BDH} \geqq \varepsilon_B - q_D / n \geqq \varepsilon / q_H \cdot (1 - q_E / q_H) - q_D / n$である。

$q_E \ll q_H$なので、$Adv_C^{G-BDH} \geqq \varepsilon / q_H - q_D / n$。

【０３１６】

以上、この実施の形態における暗号方式のＩＮＤ－ＩＤ－ＣＣＡ安全性が、Ｇ－ＢＤＨ問題に帰着することを示した。

この実施の形態における暗号方式に対する攻撃者の優位性は、$q_H (Adv_C^{G-BDH} + q_D / n)$以下である。

【０３１７】

この実施の形態における暗号方式において、送信者装置２００のセッション鍵生成部２３４及び受信者装置３００のセッション鍵復元部３３４は、加法群G_1の要素Ｒを示す第四要素情報とペアリング値ｗを示す送信ペアリング値情報（またはペアリング値ｗ’（＝ｗ）を示す受信ペアリング値情報）とを結合したビット列情報を、鍵導出関数Ｇの入力としている。

【０３１８】

比較のため、鍵導出関数Ｇの入力が、ペアリング値ｗ（またはペアリング値ｗ’）を示す情報だけである場合について検討する。以下、この暗号方式を、「比較例の暗号方式」という。

【０３１９】

比較例の暗号方式について、上記説明したのと同様の安全性証明を行うため、比較例の暗号方式を攻撃する攻撃者Ａ’を想定する。

攻撃者Ａ’の構成・動作は、ランダムオラクルＧに入力するのが、ペアリング値ｗを示す情報だけである点を除けば、上述した攻撃者Ａと同様である。

【０３２０】

比較例の暗号方式に対応する非ＩＤベース公開鍵暗号方式として、鍵導出関数Ｇの入力がペアリング値ｗを示す情報だけである点を除いて、上述した非ＩＤベース公開鍵暗号方式と同じ暗号方式を想定し、攻撃者Ａ’を利用して、比較例の暗号方式に対応する非ＩＤベース公開鍵暗号方式を攻撃する攻撃者Ｂ’を想定する。

攻撃者Ｂ’の構成・動作は、ランダムオラクルＧのシミューレート処理において、攻撃者Ａ’から入力するのが、ペアリング値ｗを示す情報だけである点と、呼び出すランダムオラクルに入力するのが、ペアリング値ｗを示す情報だけである点との２つの点が、攻撃者Ｂと異なる。

しかし、攻撃者Ｂ（攻撃者Ｂ’）は、攻撃者Ａ（攻撃者Ａ’）が呼び出したランダムオラクルＧの入力をそのまま、ランダムオラクルの入力として呼び出し、ランダムオラクルの出力をそのまま、ランダムオラクルＧの出力として攻撃者Ａ（攻撃者Ａ’）に返すので、攻撃者Ｂと攻撃者Ｂ’との間に実質的な違いはない。

【０３２１】

次に、攻撃者Ｂ’を利用して、Ｇ－ＢＤＨ問題に解答する解答者Ｃ’を想定する。

解答者Ｃ’の構成・動作は、ランダムオラクルをシミュレートするオラクルシミュレート処理を除き、解答者Ｃと同様である。

【０３２２】

図２３は、解答者Ｃ’がランダムオラクルをシミュレートするオラクルシミュレート処理の流れを示すフローチャート図である。

【０３２３】

Ｃ４１’において、解答者Ｃ’は、ランダムオラクルの入力として、攻撃者Ｂから、ペ

アリング値ｗを示す情報を入力する。

【０３２４】

Ｃ４２’において、解答者Ｃ’は、リストν_1’を検索する。リストν_1は、組（ｗ，Ｋ）のリストである。リストν_1’は、解答者Ｃが、ランダムオラクルのシミュレート処理において、それまでに入力したペアリング値ｗと、その入力ｗに対して出力したセッション鍵Ｋとの対応関係を示すものである。

解答者Ｃ’は、リストν_1’を検索し、Ｃ４１’で入力したｗについて、それまでに同じｗを入力したことがあるか否かを判断する。

同じｗを入力したことがある場合、リストν_1から、その入力ｗに対して出力したＫを取得し、Ｃ４９’へ進む。

同じｗを入力したことがない場合、Ｃ４３’へ進む。

【０３２５】

Ｃ４３’において、解答者Ｃ’は、ＢＤＨ決定オラクルを呼び出す。解答者Ｃ’は、ＢＤＨ決定オラクルに対して、P_1、P_1^*、P_1^{**}、P_2、P_2^*、Q_2、ｗを入力する。

なお、P_1、P_1^*、P_1^{**}、P_2、P_2^*、Q_2は、解答者Ｃ’に与えられたＧ－ＢＤＨ問題のパラメータである。したがって、ＢＤＨ決定オラクルは、ｗが解答者Ｃの答えるべきペアリング値であるか否かを判定し、判定結果を出力する。

【０３２６】

解答者Ｃ’は、ＢＤＨ決定オラクルが出力した判定結果を取得する。

ＢＤＨ決定オラクルが、ｗが解答者Ｃ’の答えるべきペアリング値であると判定した場合、Ｃ４４’へ進む。

ＢＤＨ決定オラクルが、ｗが解答者Ｃ’の答えるべきペアリング値でないと判定した場合、Ｃ４５’へ進む。

【０３２７】

Ｃ４４’において、解答者Ｃ’は、Ｇ－ＢＤＨ問題に対する解答として、ｗを出力し、処理を終了する。

【０３２８】

Ｃ４５’において、解答者Ｃ’は、リストν_3’から、組（ｃ，Ｋ）を一つずつ取得し、Ｃ４６’の処理を繰り返す。

リストν_3’は、解答者Ｃ’が、復号オラクルのシミュレート処理において、それまでに入力した暗号化セッション鍵ｃと、その入力ｃに対して出力したセッション鍵Ｋとの対応関係を示すものである。

【０３２９】

Ｃ４６’において、解答者Ｃ’は、ＢＤＨ決定オラクルを呼び出す。解答者Ｃ’は、ＢＤＨ決定オラクルに対して、P_1、P_1^*、Ｒ、P_2、P_2^*、Q_2、ｗを入力する。

ここで、Ｒは、暗号化セッション鍵ｃに含まれる情報が示す加法群G_1の要素である。したがって、ＢＤＨ決定オラクルは、$w = e(P_1, Q)^{sr}$であるか否かを判定する。すなわち、ｃとｗとが正しく対応するものであるか否かを判定する。

ＢＤＨ決定オラクルは、判定結果を出力する。

【０３３０】

解答者Ｃ’は、ＢＤＨ決定オラクルが出力した判定結果を取得する。

ＢＤＨ決定オラクルが、$w = e(P_1, Q)^{sr}$であると判定した場合、解答者Ｃ’は、復号オラクルがその入力ｃに対して出力したセッション鍵Ｋを、リストν_3’から取得し、繰り返し処理から抜けて、Ｃ４８’へ進む。

ＢＤＨ決定オラクルが、$w \neq e(P_1, Q)^{sr}$であると判定した場合、Ｃ４５’に戻る。

なお、リストν_3に含まれるすべての組（ｃ，Ｋ）について処理した場合には、Ｃ４７’へ進む。

【０３３１】

Ｃ４７’において、解答者Ｃ’は、セッション鍵Ｋをランダムに生成する。

【０３３２】

Ｃ４８’において、解答者Ｃ’は、Ｃ４１’で入力したｗと、Ｃ４６’で取得したＫあるいはＣ４７’で生成したＫとの組（ｗ，Ｋ）を、リストν_1に追加する。

【０３３３】

Ｃ４９’において、解答者Ｃ’は、ランダムオラクルの出力として、攻撃者Ｂに対して、Ｃ４２’あるいはＣ４６’で取得したＫ、またはＣ４７’で生成したＫを、出力する。

【０３３４】

ランダムオラクルは、ランダムな値を出力するが、同じ入力に対しては同じ出力をする。

したがって、以前に入力したことがあるｗについては、それに対応して出力したセッション鍵Ｋをリストν_1’に記憶しておき、同じセッション鍵Ｋを出力する。

【０３３５】

また、ランダムオラクルの出力と、復号オラクルの出力との整合を保つため、復号オラクルに入力したｃと、ランダムオラクルに入力したｗとが正しい組み合わせである場合、復号オラクルが出力するセッション鍵Ｋと、ランダムオラクルが出力するセッション鍵Ｋとは、同一である必要がある。

そこで、それまでに復号オラクルに入力したことがあるｃについては、それに対応して復号オラクルが出力したＫを、リストν_3に記憶しておく。解答者Ｃ’は、ＢＤＨ決定オラクルを用いて、入力したｃと正しい組み合わせになるｗを、以前に復号オラクルが入力したことがあるか否かを判定し、ある場合には、復号オラクルが出力したセッション鍵Ｋと同一のセッション鍵Ｋを出力する。

【０３３６】

このようにして、解答者Ｃ’は、攻撃者Ｂ’から見たランダムオラクルをシミュレートする。

【０３３７】

ランダムオラクルのシミュレート処理以外の点では、解答者Ｃ’は解答者Ｃと同様なので、Ｇ－ＢＤＨ問題に対する解答者Ｃ’の優位性は、Ｇ－ＢＤＨ問題に対する解答者Ｃの優位性と等しい。

【０３３８】

したがって、比較例の暗号方式のＩＮＤ－ＩＤ－ＣＣＡ安全性は、Ｇ－ＢＤＨ問題に帰着する。比較例の暗号方式に対する攻撃者Ａ’の優位性は、q_H（$Adv_C^{G-BDH}+q_D/n$）以下であり、この実施の形態の暗号方式に対する攻撃者Ａの優位性と等しい。

【０３３９】

次に、解答者Ｃ及び解答者Ｃ’がＢＤＨ決定オラクルを呼び出す回数について検討する。

【０３４０】

解答者ＣがＢＤＨ決定オラクルを呼び出す（図２２のＣ４３）のは、攻撃者Ｂがランダムオラクルを呼び出した場合である。攻撃者Ｂがランダムオラクルを呼び出すのは、攻撃者Ａがランダムオラクルｇを呼び出した場合である。

したがって、解答者ＣがＢＤＨ決定オラクルを呼び出す回数q_Cは、$q_C \leqq q_G$（ただし、q_Gは、攻撃者Ａがランダムオラクルｇを呼び出す回数の最大値）である。

【０３４１】

解答者Ｃ’がＢＤＨ決定オラクルを呼び出す（図２３のＣ４３’及びＣ４６’）のは、攻撃者Ｂ’がランダムオラクルを呼び出した場合である。

解答者Ｃ’は、攻撃者Ｂ’がランダムオラクルを１回呼び出したのに対応して、ＢＤＨ決定オラクルを、最大q_D’回呼び出す。ここで、q_D’は、攻撃者Ｂ’が復号オラクルに対して入力する暗号化セッション鍵の総数であり、リストν_3に含まれる組（ｃ，Ｋ）の最大数である。

したがって、解答者Ｃ’がＢＤＨ決定オラクルを呼び出す回数$q_{C'}$は、$q_{C'} \leqq q_G$

・q_D（ただし、q_Gは、攻撃者ＡがランダムオラクルGを呼び出す回数の最大値。q_Dは、攻撃者Ａが復号オラクルを呼び出す回数の最大値であり、$q_D' \leqq q_D$。）である。

【０３４２】

この実施の形態における暗号方式の安全性と、比較例の暗号方式の安全性とを比較すると、帰着する数学上の問題は、Ｇ－ＢＤＨ問題であり、同一である。

また、攻撃者Ａの優位性と攻撃者Ａ’の優位性とは、等しい。

したがって、この点では、２つの暗号方式の安全性に差はない。

【０３４３】

しかし、解答者Ｃ’がＢＤＨ決定オラクルを呼び出す回数は、解答者ＣがＢＤＨ決定オラクルを呼び出す回数よりも多い（$\because q_D > 1$）。

【０３４４】

Ｇ－ＢＤＨ問題は、ＢＤＨ決定オラクルを利用することができるという仮定のもとで、ＢＤＨ問題に答える問題である。もし、ＢＤＨ決定オラクルを１回も利用しないでＢＤＨ問題に答えることができるならば、すなわち、Ｇ－ＢＤＨ問題よりも難しいＢＤＨ問題に答えたことになる。暗号方式が帰着する数学上の問題がＢＤＨ問題である場合、Ｇ－ＢＤＨ問題に帰着する暗号方式よりも、安全性が高いといえる。

【０３４５】

また、同じＧ－ＢＤＨ問題に帰着する暗号方式であれば、ＢＤＨ決定オラクルを利用する回数が少ないほうが、より難しい問題に帰着したことになるので、安全性が高いといえる。

【０３４６】

したがって、この実施の形態における暗号方式の安全性は、比較例の暗号方式よりも高いことが証明された。

【０３４７】

この実施の形態における受信者装置３００は、

情報を記憶する磁気ディスク装置９２０などの記憶装置と、

情報を処理するＣＰＵ９１１などの処理装置と、

送信者装置２００が送信した情報を受信する受信装置（通信装置９１５）と、

磁気ディスク装置９２０などの記憶装置を用いて、加法群G_2の要素d_{ID}を示す情報をユーザ秘密鍵情報として記憶する秘密鍵記憶部３２２と、

受信装置（通信装置９１５）を用いて、送信者装置２００が送信した暗号化セッション鍵C_0を受信し、ＣＰＵ９１１などの処理装置を用いて、受信した暗号化セッション鍵C_0に含まれる加法群G_1の要素Ｒを示す情報を第四要素情報として出力する暗号化セッション鍵受信部３３１と、

ＣＰＵ９１１などの処理装置を用いて、秘密鍵記憶部３２２が記憶したユーザ秘密鍵情報と暗号化セッション鍵受信部３３１が出力した第四要素情報とを入力し、ＣＰＵ９１１などの処理装置を用いて、入力したユーザ秘密鍵情報と第四要素情報とに基づいて、加法群G_1の要素Ｒと加法群G_2の要素d_{ID}とのペアリング値を算出して乗法群G_Tの要素ｗ’とし、ＣＰＵ９１１などの処理装置を用いて、算出した乗法群G_Tの要素ｗ’を示す情報を受信ペアリング値情報として出力する受信ペアリング値算出部３３３と、

ＣＰＵ９１１などの処理装置を用いて、暗号化セッション鍵受信部３３１が出力した第四要素情報と受信ペアリング値算出部３３３が出力した受信ペアリング値情報とを入力し、ＣＰＵ９１１などの処理装置を用いて、入力した第四要素情報と受信ペアリング値情報とに基づいて、ハッシュ値を算出し、ＣＰＵ９１１などの処理装置を用いて、算出したハッシュ値に基づいて、送信者装置２００が生成したセッション鍵Ｋと同一のセッション鍵を復元するセッション鍵復元部３３４と、

を有することを特徴とする。

【０３４８】

この実施の形態における受信者装置３００によれば、セッション鍵復元部３３４が、加法群G_1の要素Ｒを示す第四要素情報と、ペアリング値ｗ’を示す受信ペアリング値情報

とに基づいてハッシュ値を算出し、算出したハッシュ値に基づいて、セッション鍵Ｋを復元するので、Ｇ－ＢＤＨ問題に効率良く帰着する安全性の高い暗号方式を実現することができるという効果を奏する。

【０３４９】

この実施の形態における送信者装置２００は、

情報を記憶する磁気ディスク装置９２０などの記憶装置と、

情報を処理するＣＰＵ９１１などの処理装置と、

受信者装置３００に対して情報を送信する送信装置（通信装置９１５）と、

磁気ディスク装置９２０などの記憶装置を用いて、加法群G_1の要素P_1を示す情報を第一要素情報として記憶する第一要素記憶部２１２と、

磁気ディスク装置９２０などの記憶装置を用いて、加法群G_1の要素P_{pub}を示す情報を第二要素情報として記憶する第二要素記憶部２１３と、

ＣＰＵ９１１などの処理装置を用いて、第一要素記憶部２１２が記憶した第一要素情報と自然数ｒを示す乱数情報とを入力し、ＣＰＵ９１１などの処理装置を用いて、入力した第一要素情報と乱数情報とに基づいて、加法群G_1の要素Ｒを算出し、ＣＰＵ９１１などの処理装置を用いて、算出した加法群G_1の要素Ｒを示す情報を第四要素情報として出力する第四要素算出部２２２と、

ＣＰＵ９１１などの処理装置を用いて、受信者装置３００を識別する識別情報（受信者装置３００のＩＤを示す情報）を入力し、ＣＰＵ９１１などの処理装置を用いて、入力した識別情報に対応する加法群G_2の要素Q_{ID}を算出し、ＣＰＵ９１１などの処理装置を用いて、算出した加法群G_2の要素Q_{ID}を示す情報を第五要素情報として出力する第五要素算出部２３２と、

ＣＰＵ９１１などの処理装置を用いて、第二要素記憶部２１３が記憶した第二要素情報と第五要素算出部２３２が出力した第五要素情報と上記乱数情報とを入力し、ＣＰＵ９１１などの処理装置を用いて、入力した第二要素情報と第五要素情報とに基づいて、加法群G_1の要素P_{pub}と加法群G_2の要素Q_{ID}とのペアリング値を算出し、ＣＰＵ９１１などの処理装置を用いて、算出したペアリング値と入力した乱数情報とに基づいて、乗法群G_Tの要素ｗを算出し、ＣＰＵ９１１などの処理装置を用いて、算出した乗法群G_Tの要素ｗを示す情報を送信ペアリング値情報として出力する送信ペアリング値算出部２３３と、

ＣＰＵ９１１などの処理装置を用いて、第四要素算出部２２２が出力した第四要素情報を入力し、送信装置（通信装置９１５）を用いて、入力した第四要素情報を含む情報を暗号化セッション鍵C_0として受信者装置３００に対して送信する暗号化セッション鍵送信部２２３と、

ＣＰＵ９１１などの処理装置を用いて、第四要素算出部２２２が出力した第四要素情報と送信ペアリング値算出部２３３が出力した送信ペアリング値情報とを入力し、ＣＰＵ９１１などの処理装置を用いて、入力した第四要素情報と送信ペアリング値情報とに基づいて、ハッシュ値を算出し、ＣＰＵ９１１などの処理装置を用いて、算出したハッシュ値に基づいて、セッション鍵Ｋを生成するセッション鍵生成部２３４と、

を有することを特徴とする。

【０３５０】

この実施の形態における送信者装置２００によれば、セッション鍵生成部２３４が、加法群G_1の要素Ｒを示す第四要素情報と、ペアリング値ｗを示す送信ペアリング値情報とに基づいてハッシュ値を算出し、算出したハッシュ値に基づいて、セッション鍵Ｋを生成するので、Ｇ－ＢＤＨ問題に効率良く帰着する安全性の高い暗号方式を実現することができるという効果を奏する。

【０３５１】

この実施の形態における暗号通信システム（ＩＤベース公開鍵暗号通信システム８００）は、

鍵生成装置（ユーザ秘密鍵生成センタ１００）と、送信者装置２００と、受信者装置３

００とを備え、
鍵生成装置（ユーザ秘密鍵生成センタ１００）は、
情報を処理するＣＰＵ９１１などの処理装置と、
ＣＰＵ９１１などの処理装置を用いて、加法群G_1の要素P_1を選択し、ＣＰＵ９１１などの処理装置を用いて、選択した加法群G_1の要素P_1を示す情報を第一要素情報として出力する第一要素選択部１１１と、
ＣＰＵ９１１などの処理装置を用いて、自然数ｓを選択し、ＣＰＵ９１１などの処理装置を用いて、選択した自然数ｓを示す情報をマスターキー情報として出力するマスターキー選択部１１２と、
ＣＰＵ９１１などの処理装置を用いて、第一要素選択部１１１が出力した第一要素情報とマスターキー選択部１１２が出力したマスターキー情報とを入力し、ＣＰＵ９１１などの処理装置を用いて、入力した第一要素情報とマスターキー情報とに基づいて、加法群G_1の要素P_{pub}を算出し、ＣＰＵ９１１などの処理装置を用いて、算出した加法群G_1の要素P_{pub}を示す情報を第二要素情報として出力する第二要素算出部１２１と、
ＣＰＵ９１１などの処理装置を用いて、第一要素選択部１１１が出力した第一要素情報と第二要素算出部１２１が出力した第二要素情報とを入力し、ＣＰＵ９１１などの処理装置を用いて、入力した第一要素情報と第二要素情報とを含む情報をパラメータ情報として公開するパラメータ公開部１２２と、
ＣＰＵ９１１などの処理装置を用いて、受信者装置３００を識別する識別情報（受信者装置３００のＩＤを示す情報）を入力し、ＣＰＵ９１１などの処理装置を用いて、入力した識別情報に対応する加法群G_2の要素Q_{ID}を算出し、ＣＰＵ９１１などの処理装置を用いて、算出した加法群G_2の要素Q_{ID}を示す情報を第三要素情報として出力する第三要素算出部１３２と、
ＣＰＵ９１１などの処理装置を用いて、第三要素算出部１３２が出力した第三要素情報とマスターキー選択部１１２が出力したマスターキー情報とを入力し、ＣＰＵ９１１などの処理装置を用いて、入力した第三要素情報とマスターキー情報とに基づいて、加法群G_2の要素d_{ID}を算出し、ＣＰＵ９１１などの処理装置を用いて、算出した加法群G_2の要素d_{ID}を示す情報をユーザ秘密鍵情報として出力する秘密鍵算出部１３３と、
ＣＰＵ９１１などの処理装置を用いて、秘密鍵算出部１３３が出力したユーザ秘密鍵情報を入力し、ＣＰＵ９１１などの処理装置を用いて、入力したユーザ秘密鍵情報を受信者装置３００に対して秘密裡に通知する秘密鍵通知部１３４と、
を有し、
送信者装置２００は、
情報を記憶する磁気ディスク装置９２０などの記憶装置と、
情報を処理するＣＰＵ９１１などの処理装置と、
受信者装置３００に対して情報を送信する送信装置（通信装置９１５）と、
ＣＰＵ９１１などの処理装置を用いて、鍵生成装置（ユーザ秘密鍵生成センタ１００）が公開したパラメータ情報を取得し、ＣＰＵ９１１などの処理装置を用いて、取得したパラメータ情報に含まれる第一要素情報と第二要素情報とを出力するパラメータ取得部２１１と、
ＣＰＵ９１１などの処理装置を用いて、パラメータ取得部２１１が出力した第一要素情報を入力し、磁気ディスク装置９２０などの記憶装置を用いて、入力した第一要素情報を記憶する第一要素記憶部２１２と、
ＣＰＵ９１１などの処理装置を用いて、パラメータ取得部２１１が出力した第二要素情報を入力し、磁気ディスク装置９２０などの記憶装置を用いて、入力した第二要素情報を記憶する第二要素記憶部２１３と、
ＣＰＵ９１１などの処理装置を用いて、第一要素記憶部２１２が記憶した第一要素情報と自然数ｒを示す乱数情報とを入力し、ＣＰＵ９１１などの処理装置を用いて、入力した第一要素情報と乱数情報とに基づいて、加法群G_1の要素Ｒを算出し、ＣＰＵ９１１などの処理装置を用いて、算出した加法群G_1の要素Ｒを示す情報を第四要素情報として出力

する第四要素算出部２２２と、
ＣＰＵ９１１などの処理装置を用いて、受信者装置３００を識別する識別情報（受信者装置３００のＩＤを示す情報）を入力し、ＣＰＵ９１１などの処理装置を用いて、入力した識別情報に対応する加法群G_2の要素Q_{ID}を算出し、ＣＰＵ９１１などの処理装置を用いて、算出した加法群G_2の要素Q_{ID}を示す情報を第五要素情報として出力する第五要素算出部２３２と、
ＣＰＵ９１１などの処理装置を用いて、第二要素記憶部２１３が記憶した第二要素情報と第五要素算出部２３２が出力した第五要素情報と上記乱数情報とを入力し、ＣＰＵ９１１などの処理装置を用いて、入力した第二要素情報と第五要素情報とに基づいて、加法群G_1の要素P_{pub}と加法群G_2の要素Q_{ID}とのペアリング値を算出し、ＣＰＵ９１１などの処理装置を用いて、算出したペアリング値と入力した乱数情報とに基づいて、乗法群G_Tの要素ｗを算出し、ＣＰＵ９１１などの処理装置を用いて、算出した乗法群G_Tの要素ｗを示す情報を送信ペアリング値情報として出力する送信ペアリング値算出部２３３と、
ＣＰＵ９１１などの処理装置を用いて、第四要素算出部２２２が出力した第四要素情報を入力し、送信装置（通信装置９１５）を用いて、入力した第四要素情報を含む情報を暗号化セッション鍵C_0として受信者装置３００に対して送信する暗号化セッション鍵送信部２２３と、
ＣＰＵ９１１などの処理装置を用いて、第四要素算出部２２２が出力した第四要素情報と送信ペアリング値算出部２３３が出力した送信ペアリング値情報とを入力し、ＣＰＵ９１１などの処理装置を用いて、入力した第四要素情報と送信ペアリング値情報とに基づいて、ハッシュ値を算出し、ＣＰＵ９１１などの処理装置を用いて、算出したハッシュ値に基づいて、セッション鍵Ｋを生成するセッション鍵生成部２３４と、
を有し、
受信者装置３００は、
情報を記憶する磁気ディスク装置９２０などの記憶装置と、
情報を処理するＣＰＵ９１１などの処理装置と、
送信者装置２００が送信した情報を受信する受信装置（通信装置９１５）と、
ＣＰＵ９１１などの処理装置を用いて、鍵生成装置（ユーザ秘密鍵生成センタ１００）が通知したユーザ秘密鍵情報を取得し、ＣＰＵ９１１などの処理装置を用いて、取得したユーザ秘密鍵情報を出力する秘密鍵取得部３２１と、
ＣＰＵ９１１などの処理装置を用いて、秘密鍵取得部３２１が出力したユーザ秘密鍵情報を入力し、磁気ディスク装置９２０などの記憶装置を用いて、入力したユーザ秘密鍵情報を記憶する秘密鍵記憶部３２２と、
受信装置（通信装置９１５）を用いて、送信者装置２００が送信した暗号化セッション鍵C_0を受信し、ＣＰＵ９１１などの処理装置を用いて、受信した暗号化セッション鍵C_0に含まれる加法群G_1の要素Ｒを示す情報を第四要素情報として出力する暗号化セッション鍵受信部３３１と、
ＣＰＵ９１１などの処理装置を用いて、秘密鍵記憶部３２２が記憶したユーザ秘密鍵情報と暗号化セッション鍵受信部３３１が出力した第四要素情報とを入力し、ＣＰＵ９１１などの処理装置を用いて、入力したユーザ秘密鍵情報と第四要素情報とに基づいて、加法群G_1の要素Ｒと加法群G_2の要素d_{ID}とのペアリング値を算出して乗法群G_Tの要素ｗ’とし、ＣＰＵ９１１などの処理装置を用いて、算出した乗法群G_Tの要素ｗ’を示す情報を受信ペアリング値情報として出力する受信ペアリング値算出部３３３と、
ＣＰＵ９１１などの処理装置を用いて、暗号化セッション鍵受信部３３１が出力した第四要素情報と受信ペアリング値算出部３３３が出力した受信ペアリング値情報とを入力し、ＣＰＵ９１１などの処理装置を用いて、入力した第四要素情報と受信ペアリング値情報とに基づいて、ハッシュ値を算出し、ＣＰＵ９１１などの処理装置を用いて、算出したハッシュ値に基づいて、送信者装置２００が生成したセッション鍵Ｋと同一のセッション鍵を復元するセッション鍵復元部３３４と、

を有することを特徴とする。

【０３５２】

この実施の形態における暗号通信システム（ＩＤベース公開鍵暗号通信システム８００）によれば、送信者装置２００のセッション鍵生成部２３４が、加法群G_1の要素Ｒを示す第四要素情報と、ペアリング値ｗを示す送信ペアリング値情報とに基づいてハッシュ値を算出し、算出したハッシュ値に基づいて、セッション鍵Ｋを生成し、送信者装置２００の暗号化セッション鍵送信部２２３が、受信者装置３００に対して、加法群G_1の要素Ｒを示す第四要素情報を含む暗号化セッション鍵C_0を送信し、受信者装置３００の暗号化セッション鍵受信部３３１が、送信者装置２００から、加法群G_1の要素Ｒを示す第四要素情報を含む暗号化セッション鍵C_0を受信し、受信者装置３００のセッション鍵復元部３３４が、加法群G_1の要素Ｒを示す第四要素情報と、ペアリング値ｗ’を示す受信ペアリング値情報とに基づいてハッシュ値を算出し、算出したハッシュ値に基づいて、送信者装置２００が生成したセッション鍵Ｋと同一のセッション鍵を復元するので、Ｇ－ＢＤＨ問題に効率良く帰着する安全性の高い暗号方式により、送信者装置２００と受信者装置３００とが同一のセッション鍵Ｋを共有することができるという効果を奏する。

【０３５３】

この実施の形態における送信者装置２００は、更に、

ＣＰＵ９１１などの処理装置を用いて、加法群G_1の位数ｎより小さい自然数ｒをランダムに選択し、ＣＰＵ９１１などの処理装置を用いて、選択した自然数ｒを示す情報を、第四要素算出部２２２及び送信ペアリング値算出部２３３が入力する乱数情報として出力する自然数選択部２２１を有し、

セッション鍵生成部２３４が、

ＣＰＵ９１１などの処理装置を用いて、第四要素情報と送信ペアリング値情報とを入力し、ＣＰＵ９１１などの処理装置を用いて、入力した第四要素情報と送信ペアリング値情報とを結合してビット列情報を生成し、ＣＰＵ９１１などの処理装置を用いて、生成したビット列情報に対応するハッシュ値を算出し、算出したハッシュ値をセッション鍵Ｋとすることを特徴とする。

【０３５４】

この実施の形態における送信者装置２００によれば、セッション鍵生成部２３４が、加法群G_1の要素Ｒを示す第四要素情報と、ペアリング値ｗを示す送信ペアリング値情報とを結合してビット列情報を生成し、生成したビット列情報に対応するハッシュ値を算出して、セッション鍵Ｋとするので、Ｇ－ＢＤＨ問題に効率良く帰着する安全性の高い暗号方式により受信者装置３００と共有するセッション鍵Ｋを、効率的に生成することができるという効果を奏する。

【０３５５】

この実施の形態における受信者装置３００は、

セッション鍵復元部３３４が、

ＣＰＵ９１１などの処理装置を用いて、第四要素情報と受信ペアリング値情報とを入力し、ＣＰＵ９１１などの処理装置を用いて、入力した第四要素情報と受信ペアリング値情報とを結合してビット列情報を生成し、ＣＰＵ９１１などの処理装置を用いて、生成したビット列情報に対応するハッシュ値を算出し、算出したハッシュ値をセッション鍵Ｋとすることを特徴とする。

【０３５６】

この実施の形態における受信者装置３００によれば、セッション鍵復元部３３４が、加法群G_1の要素Ｒを示す第四要素情報と、ペアリング値ｗ’を示す受信ペアリング値情報とを結合してビット列情報を生成し、生成したビット列情報に対応するハッシュ値を算出して、セッション鍵Ｋとするので、Ｇ－ＢＤＨ問題に効率良く帰着する安全性の高い暗号方式により送信者装置２００と共有するセッション鍵Ｋを、効率的に復元することができるという効果を奏する。

【０３５７】

この実施の形態における送信者装置２００は、
第四要素算出部２２２が、
ＣＰＵ９１１などの処理装置を用いて、第一要素情報と乱数情報とを入力し、ＣＰＵ９１１などの処理装置を用いて、入力した第一要素情報と乱数情報とに基づいて、加法群G_1の要素P_1をｒ回加算した要素を加法群G_1の要素Ｒとして算出し、ＣＰＵ９１１などの処理装置を用いて、算出した加法群G_1の要素Ｒを示す情報を第四要素情報として出力し、
送信ペアリング値算出部２３３が、
ＣＰＵ９１１などの処理装置を用いて、第二要素情報と第五要素情報と乱数情報とを入力し、ＣＰＵ９１１などの処理装置を用いて、入力した第二要素情報と第五要素情報と乱数情報とに基づいて、加法群G_1の要素P_{pub}と加法群G_2の要素Q_{ID}とのペアリング値のｒ乗を、乗法群G_Tの要素ｗとして算出し、ＣＰＵ９１１などの処理装置を用いて、算出した乗法群G_Tの要素ｗを示す情報を送信ペアリング値情報として出力することを特徴とする。

【０３５８】

この実施の形態における送信者装置２００によれば、第四要素算出部２２２が、加法群G_1の要素$R = rP_1$を示す情報を第四要素情報として出力し、送信ペアリング値算出部２３３が、ペアリング値$w = e(P_{pub}, Q_{ID})^r$を示す情報を送信ペアリング値情報として出力するので、加法群G_1がＤＨ問題を解くことが困難な群であり、ペアリングｅがＧ－ＢＤＨ問題を解くことが困難な双線形ペアリングであれば、安全性の高い暗号方式を実現することができるという効果を奏する。

【０３５９】

この実施の形態における暗号通信システム（ＩＤベース公開鍵暗号通信システム８００）は、
鍵生成装置（ユーザ秘密鍵生成センタ１００）の第二要素算出部１２１が、
ＣＰＵ９１１などの処理装置を用いて、第一要素情報とマスターキー情報とを入力し、ＣＰＵ９１１などの処理装置を用いて、入力した第一要素情報とマスターキー情報とに基づいて、加法群G_1の要素P_1をｓ回加算した要素を加法群G_1の要素P_{pub}として算出し、ＣＰＵ９１１などの処理装置を用いて、算出した加法群G_1の要素P_{pub}を示す情報を第二要素情報として出力し、
鍵生成装置（ユーザ秘密鍵生成センタ１００）の秘密鍵算出部１３３が、
ＣＰＵ９１１などの処理装置を用いて、第三要素情報とマスターキー情報とを入力し、ＣＰＵ９１１などの処理装置を用いて、入力した第三要素情報とマスターキー情報とに基づいて、加法群G_2の要素Q_{ID}をｓ回加算した要素を加法群G_2の要素d_{ID}として算出し、ＣＰＵ９１１などの処理装置を用いて、算出した加法群G_2の要素d_{ID}を示す情報をユーザ秘密鍵情報として出力することを特徴とする。

【０３６０】

この実施の形態における暗号通信システム（ＩＤベース公開鍵暗号通信システム８００）によれば、鍵生成装置（ユーザ秘密鍵生成センタ１００）の第二要素算出部１２１が、加法群G_1の要素$P_{pub} = sP$を示す情報を第二要素情報として出力し、鍵生成装置（ユーザ秘密鍵生成センタ１００）の秘密鍵算出部１３３が、加法群G_2の要素$d_{ID} = sQ_{ID}$を示す情報をユーザ秘密鍵情報として出力するので、加法群G_1及び加法群G_2がＤＨ問題を解くことが困難な群であれば、安全性の高い暗号方式を実現することができるという効果を奏する。

【０３６１】

この実施の形態における送信者装置２００は、更に、
ＣＰＵ９１１などの処理装置を用いて、受信者装置３００に対して通知すべき情報を平文情報として入力し、ＣＰＵ９１１などの処理装置を用いて、セッション鍵生成部２３４が生成したセッション鍵Ｋを入力し、ＣＰＵ９１１などの処理装置を用いて、入力した平文情報を、入力したセッション鍵Ｋで暗号化して暗号文情報を生成し、ＣＰＵ９１１など

の処理装置を用いて、生成した暗号文情報を出力する暗号文生成部２４２と、
ＣＰＵ９１１などの処理装置を用いて、暗号文生成部２４２が出力した暗号文情報を入力し、送信装置（通信装置９１５）を用いて、入力した暗号文情報を受信者装置３００に対して送信する暗号文送信部２４３と、
を有することを特徴とする。
【０３６２】
この実施の形態における送信者装置２００によれば、安全性の高い暗号方式で受信者装置３００と共有したセッション鍵Ｋを用いて、平文情報を暗号化して、受信者装置３００に対して送信するので、第三者に秘密が漏洩することなく、平文情報を受信者装置３００に対して通知することができるという効果を奏する。
【０３６３】
この実施の形態における受信者装置３００は、更に、
受信装置（通信装置９１５）を用いて、送信者装置２００が送信した暗号文情報を受信し、ＣＰＵ９１１などの処理装置を用いて、受信した暗号文情報を出力する暗号文受信部３４１と、
ＣＰＵ９１１などの処理装置を用いて、暗号文受信部３４１が出力した暗号文情報を入力し、ＣＰＵ９１１などの処理装置を用いて、セッション鍵復元部３３４が復元したセッション鍵Ｋを入力し、ＣＰＵ９１１などの処理装置を用いて、入力した暗号文情報を、入力したセッション鍵Ｋで復号して、平文情報を生成し、ＣＰＵ９１１などの処理装置を用いて、生成した平文情報を出力する暗号文復号部３４２と、
を有することを特徴とする。
【０３６４】
この実施の形態における受信者装置３００によれば、安全性の高い暗号方式で送信者装置２００と共有したセッション鍵Ｋを用いて、送信者装置２００から受信した暗号文情報を復号するので、第三者に秘密が漏洩することなく、平文情報を送信者装置２００から取得することができるという効果を奏する。
【０３６５】
この実施の形態における送信者装置２００は、情報を記憶する磁気ディスク装置９２０などの記憶装置と、情報を処理するＣＰＵ９１１などの処理装置と、受信者装置３００に対して情報を送信する送信装置（通信装置９１５）とを有するコンピュータを送信者装置２００として機能させるプログラムを、コンピュータが実行することによって、実現することができる。
【０３６６】
この実施の形態におけるプログラムは、
情報を記憶する磁気ディスク装置９２０などの記憶装置と、情報を処理するＣＰＵ９１１などの処理装置と、受信者装置３００に対して情報を送信する送信装置（通信装置９１５）とを有するコンピュータを、この実施の形態における送信者装置２００として機能させることを特徴とする。
【０３６７】
この実施の形態におけるプログラムによれば、コンピュータが、加法群G_1の要素Ｒを示す第四要素情報と、ペアリング値ｗを示す送信ペアリング値情報とに基づいてハッシュ値を算出し、算出したハッシュ値に基づいて、セッション鍵Ｋを生成するので、Ｇ－ＢＤＨ問題に効率良く帰着する安全性の高い暗号方式を実現することができるという効果を奏する。
【０３６８】
この実施の形態における受信者装置３００は、情報を記憶する磁気ディスク装置９２０などの記憶装置と、情報を処理するＣＰＵ９１１などの処理装置と、送信者装置２００が送信した情報を受信する受信装置（通信装置９１５）とを有するコンピュータを受信者装置３００として機能させるプログラムを、コンピュータが実行することによって、実現することができる。

【０３６９】
この実施の形態におけるプログラムは、
情報を記憶する磁気ディスク装置９２０などの記憶装置と、情報を処理するＣＰＵ９１１などの処理装置と、送信者装置２００が送信した情報を受信する受信装置（通信装置９１５）とを有するコンピュータを、この実施の形態における受信者装置３００として機能させることを特徴とする。
【０３７０】
この実施の形態におけるプログラムによれば、コンピュータが、加法群G_1の要素Ｒを示す第四要素情報と、ペアリング値ｗ’を示す受信ペアリング値情報とに基づいてハッシュ値を算出し、算出したハッシュ値に基づいて、セッション鍵Ｋを復元するので、Ｇ－ＢＤＨ問題に効率良く帰着する安全性の高い暗号方式を実現することができるという効果を奏する。
【０３７１】
この実施の形態における送信者装置２００及び受信者装置３００は、セッション鍵共有装置ともいう。
【０３７２】
以上説明したセッション鍵共有装置は、
ペアリングを用いたＩＤベース公開鍵暗号を用いたセッション鍵共有装置において、ペアリング値をハッシュするのに用いる鍵導出関数への入力として、ペアリング値だけでなく、セッション鍵を暗号化した値も入力に加わっていることを特徴とする。
【０３７３】
以上説明したセッション鍵共有装置は、更に、
ペアリングを用いたＩＤベース鍵配送方式を用いたセッション鍵共有装置において、前記セッション鍵を暗号化するのに、
ＩＤ情報ＩＤから一意的に決まるQ_{ID}を計算し、
$1 \leqq r \leqq n$であるｒをランダムに生成し、
P_{pub}とQ_{ID}のペアリング値のｒ乗$w = e(P_{pub}, Q_{ID})^r$を計算し、
$C_0 = r \cdot P_1$を計算し、
鍵導出関数Ｇを用いて、セッション鍵$K = G(C_0, w)$を計算し、
セッション鍵Ｋと前記セッション鍵の暗号化C_0を出力することを特徴とする。
【０３７４】
以上説明したセッション鍵共有装置は、更に、
ペアリングを用いたＩＤベース鍵配送方式を用いたセッション鍵共有装置において、暗号化されたセッション鍵を復号するのに、
$C_0 \in G_1$であるかどうかをチェックし、
セッション鍵の暗号化C_0とユーザプライベート鍵d_{ID}のペアリング値$w = e(C_0, d_{ID})$を計算し、
鍵導出関数Ｇを用いて、セッション鍵$K = G(C_0, w)$を計算し、
セッション鍵Ｋを出力することを特徴とする。
【０３７５】
この実施の形態におけるプログラムは、セッション鍵共有プログラムともいう。
【０３７６】
以上説明したセッション鍵共有プログラムは、
ペアリングを用いたＩＤベース公開鍵暗号を用いたセッション鍵共有プログラムにおいて、ペアリング値をハッシュするのに用いる鍵導出関数への入力として、ペアリング値だけでなく、セッション鍵を暗号化した値も入力に加わっていることを特徴とする。
【０３７７】
以上説明したセッション鍵共有プログラムは、更に、
ペアリングを用いたＩＤベース鍵配送方式を用いたセッション鍵共有プログラムにおいて、前記セッション鍵を暗号化するのに、

ＩＤ情報ＩＤから一意的に決まるQ_{ID}を計算し、
１≦ｒ≦ｎであるｒをランダムに生成し、
P_{pub}とQ_{ID}のペアリング値のｒ乗ｗ＝ｅ（P_{pub}，Q_{ID}）^{r}を計算し、
C_0＝ｒ・P_1を計算し、
鍵導出関数Ｇを用いて、セッション鍵Ｋ＝Ｇ（C_0，ｗ）を計算し、
セッション鍵Ｋと前記セッション鍵の暗号化C_0を出力することを特徴とする。

【０３７８】

以上説明したセッション鍵共有プログラムは、更に、
ペアリングを用いたＩＤベース鍵配送方式を用いたセッション鍵共有プログラムにおいて、暗号化された鍵を復号するのに、
$C_0 \in G_1$であるかどうかをチェックし、
セッション鍵の暗号化C_0とユーザプライベート鍵d_{ID}のペアリング値ｗ＝ｅ（C_0、d_{ID}）を計算し、
鍵導出関数Ｇを用いて、セッション鍵Ｋ＝Ｇ（C_0、ｗ）を計算し、
セッション鍵Ｋを出力することを特徴とする。

【０３７９】

この実施の形態における送信者装置２００及び受信者装置３００は、ＩＤベース公開鍵暗号装置ともいう。

【０３８０】

以上説明したＩＤベース公開鍵暗号装置は、
ペアリングを用いたＩＤベース公開鍵暗号装置において、ペアリング値をハッシュするのに用いる鍵導出関数への入力として、ペアリング値だけでなく、セッション鍵を暗号化した値も入力に加わっていることを特徴とする。

【０３８１】

以上説明したＩＤベース公開鍵暗号装置は、更に、
ペアリングを用いたＩＤベース公開鍵暗号装置において、平文Ｍを暗号化するのに、
ＩＤ情報ＩＤから一意的に決まるQ_{ID}を計算し、
１≦ｒ≦ｎであるｒをランダムに生成し、
P_{pub}とQ_{ID}のペアリング値のｒ乗ｗ＝ｅ（P_{pub}、Q_{ID}）^{r}を計算し、
Ｕ＝ｒ・P_1を計算し、
鍵導出関数Ｇを用いて、Ｋ＝Ｇ（Ｕ、ｗ）を計算し、
鍵Ｋを用いて計算されたＭの暗号化を出力することを特徴とする。

【０３８２】

以上説明したＩＤベース公開鍵暗号装置は、更に、
ビット毎の排他的論理和ＸＯＲを用い、鍵Ｋを用いて計算されたＭの暗号化として、ＸＯＲ（Ｍ，Ｋ）を用いることを特徴とする。

【０３８３】

以上説明したＩＤベース公開鍵暗号装置は、更に、
ペアリングを用いたＩＤベース公開鍵暗号装置において、暗号文Ｃを復号するのに、
暗号文の成分Ｕとユーザプライベート鍵d_{ID}のペアリング値ｗ＝ｅ（Ｕ、d_{ID}）を計算し、
鍵導出関数Ｇを用いて、Ｋ＝Ｇ（Ｕ、ｗ）を計算し、
鍵Ｋを用いて計算されたＣの復号を出力することを特徴とする。

【０３８４】

以上説明したＩＤベース公開鍵暗号装置は、更に、
ビット毎の排他的論理和ＸＯＲを用い、鍵Ｋを用いて計算されたＣの復号として、ＸＯＲ（Ｃ，Ｋ）を用いることを特徴とする。

【０３８５】

この実施の形態におけるプログラムは、ＩＤベース公開鍵暗号プログラムともいう。

【０３８６】

以上説明したＩＤベース公開鍵暗号プログラムは、
ペアリングを用いたＩＤベース公開鍵暗号プログラムにおいて、ペアリング値をハッシュするのに用いる鍵導出関数への入力として、ペアリング値だけでなく、セッション鍵を暗号化した値も入力に加わっていることを特徴とする。

【０３８７】

以上説明したＩＤベース公開鍵暗号プログラムは、更に、
ペアリングを用いたＩＤベース公開鍵暗号プログラムにおいて、平文Ｍを暗号化するのに、
ＩＤ情報ＩＤから一意的に決まるQ_{ID}を計算し、
$1 \leqq r \leqq n$であるｒをランダムに生成し、
P_{pub}とQ_{ID}のペアリング値のｒ乗$w = e(P_{pub}, Q_{ID})^r$を計算し、
$U = r \cdot P_1$を計算し、
鍵導出関数Ｇを用いて、Ｋ＝Ｇ（Ｕ，ｗ）を計算し、
鍵Ｋを用いて計算されたＭの暗号化を出力することを特徴とする。

【０３８８】

以上説明したＩＤベース公開鍵暗号プログラムは、更に、
ビット毎の排他的論理和ＸＯＲを用い、鍵Ｋを用いて計算されたＭの暗号化として、ＸＯＲ（Ｍ，Ｋ）を用いることを特徴とする。

【０３８９】

以上説明したＩＤベース公開鍵暗号プログラムは、更に、
ペアリングを用いたＩＤベース公開鍵暗号プログラムにおいて、暗号文Ｃを復号するのに、
暗号文の成分Ｕとユーザプライベート鍵d_{ID}のペアリング値$w = e(U, d_{ID})$を計算し、
鍵導出関数Ｇを用いて、Ｋ＝Ｇ（Ｕ，ｗ）を計算し、
鍵Ｋを用いて計算されたＣの復号を出力することを特徴とする。

【０３９０】

以上説明したＩＤベース公開鍵暗号プログラムは、更に、
ビット毎の排他的論理和ＸＯＲを用い、鍵Ｋを用いて計算されたＣの復号として、ＸＯＲ（Ｃ，Ｋ）を用いることを特徴とする。

【０３９１】

以上説明したＩＤベース公開鍵暗号通信システム８００によれば、安全性が高められたＩＤベース暗号方式が実現される。それだけでなく、ペアリングを用い、ランダムオラクルモデルで安全性が保証されたいくつかの他の暗号、署名、認証法に対しても高い安全性を付与することができるようになる。

【０３９２】

実施の形態２．
実施の形態２について、図２４～図２７を用いて説明する。
この実施の形態におけるＩＤベース公開鍵暗号通信システム８００（暗号通信システム）の全体構成、ユーザ秘密鍵生成センタ１００・送信者装置２００・受信者装置３００のハードウェア構成は、実施の形態１で説明したものと同様なので、ここでは説明を省略する。
また、ユーザ秘密鍵生成センタ１００の機能ブロックの構成は、実施の形態１で説明したものと同様なので、ここでは説明を省略する。
なお、ユーザ秘密鍵生成センタ１００のパラメータ公開部１２２が公開するパラメータ情報には、実施の形態１で説明した情報のほか、マスク生成関数（Ｍａｓｋ　Ｇｅｎｅｒａｔｉｏｎ　Ｆｕｎｃｔｉｏｎ）H_2及びハッシュ関数H_3を示す情報が含まれている。
マスク生成関数H_2及びハッシュ関数H_3は、任意のビット列を入力し、入力したビット列に対応する（所定のビット長を有する）ビット列を出力する関数である。マスク生成関数H_2及びハッシュ関数H_3には、ランダムオラクルとみなせる関数を用いる。

【０３９３】
図２４は、この実施の形態における送信者装置２００の機能ブロックの構成の一例を示すブロック構成図である。
送信者装置２００は、パラメータ取得部２１１、第一要素記憶部２１２、第二要素記憶部２１３、第四要素算出部２２２、暗号化セッション鍵送信部２２３、文字列選択部２２４、自然数算出部２２５、送信識別情報取得部２３１、第五要素算出部２３２、送信ペアリング値算出部２３３、セッション鍵生成部２３４、セッション鍵記憶部２３５、平文記憶部２４１、暗号文生成部２４２、暗号文送信部２４３を有する。
【０３９４】
このうち、パラメータ取得部２１１、第一要素記憶部２１２、第二要素記憶部２１３、第四要素算出部２２２、送信識別情報取得部２３１、第五要素算出部２３２、送信ペアリング値算出部２３３、セッション鍵記憶部２３５、平文記憶部２４１、暗号文生成部２４２、暗号文送信部２４３は、実施の形態１で説明した機能ブロックと同様なので、ここでは説明を省略する。
【０３９５】
文字列選択部２２４は、ＣＰＵ９１１などの処理装置を用いて、文字列ｍをランダムに選択する。このとき、文字列選択部２２４は、所定のビット長を有する文字列のなかから、任意の文字列をランダムに選択する。
文字列選択部２２４は、ＣＰＵ９１１などの処理装置を用いて、選択した文字列ｍを示す情報を、文字列情報として出力する。
【０３９６】
自然数算出部２２５は、ＣＰＵ９１１などの処理装置を用いて、文字列選択部２２４が出力した文字列情報を入力する。
自然数算出部２２５は、ＣＰＵ９１１などの処理装置を用いて、入力した文字列情報に対応するハッシュ値を算出する。このとき、自然数算出部２２５は、ユーザ秘密鍵生成センタ１００が公開したハッシュ関数H_3を用いて、ハッシュ値を算出する。ハッシュ関数H_3は、文字列情報を入力し、入力した文字列情報に対応するハッシュ値として、加法群G_1の位数より小さい自然数ｒを出力する関数である。自然数算出部２２５は、入力した文字列情報を、ハッシュ関数H_3の入力とする。
自然数算出部２２５は、ＣＰＵ９１１などの処理装置を用いて、算出したハッシュ値（自然数ｒ）を示す情報を、第四要素算出部２２２及び送信ペアリング値算出部２３３が入力する乱数情報として出力する。
【０３９７】
セッション鍵生成部２３４は、ＣＰＵ９１１などの処理装置を用いて、第四要素算出部２２２が出力した第四要素情報を入力する。
セッション鍵生成部２３４は、ＣＰＵ９１１などの処理装置を用いて、送信ペアリング値算出部２３３が出力した送信ペアリング値情報を入力する。
セッション鍵生成部２３４は、ＣＰＵ９１１などの処理装置を用いて、文字列選択部２２４が出力した文字列情報を入力する。
セッション鍵生成部２３４は、ＣＰＵ９１１などの処理装置を用いて、入力した第四要素情報と、入力した送信ペアリング値情報とを結合して、ビット列情報を生成する。
セッション鍵生成部２３４は、ＣＰＵ９１１などの処理装置を用いて、生成したビット列情報に対応するハッシュ値を算出する。このとき、セッション鍵生成部２３４は、ユーザ秘密鍵生成センタ１００が公開したマスク生成関数H_2を用いて、ハッシュ値を算出する。マスク生成関数H_2は、ビット列情報を入力し、入力したビット列情報に対応するハッシュ値として、文字列選択部２２４が出力した文字列情報と同じビット長の文字列情報を出力する関数である。セッション鍵生成部２３４は、生成したビット列情報を、マスク生成関数H_2の入力とする。
セッション鍵生成部２３４は、ＣＰＵ９１１などの処理装置を用いて、算出したハッシュ値を示す情報と、入力した文字列情報との排他的論理和を算出してマスク情報ｖとする

。ここで、排他的論理和とは、ビットごとの排他的論理和のことである。
セッション鍵生成部２３４は、ＣＰＵ９１１などの処理装置を用いて、算出したマスク情報ｖを出力する。
【０３９８】
また、セッション鍵生成部２３４は、ＣＰＵ９１１などの処理装置を用いて、入力した文字列情報に対応するハッシュ値を算出する。このとき、セッション鍵生成部２３４は、ユーザ秘密鍵生成センタ１００が公開した鍵導出関数Ｇを用いて、ハッシュ値を算出する。セッション鍵生成部２３４は、入力した文字列情報を鍵導出関数Ｇの入力とする。
セッション鍵生成部２３４は、ＣＰＵ９１１などの処理装置を用いて、算出したハッシュ値を、セッション鍵Ｋとして出力する。
【０３９９】
暗号化セッション鍵送信部２２３は、ＣＰＵ９１１などの処理装置を用いて、第四要素算出部２２２が出力した第四要素情報を入力する。
暗号化セッション鍵送信部２２３は、ＣＰＵ９１１などの処理装置を用いて、セッション鍵生成部２３４が出力したマスク情報ｖを入力する。
暗号化セッション鍵送信部２２３は、通信装置９１５を用いて、受信者装置３００に対して、入力した第四要素情報と、入力したマスク情報ｖとを含む情報を、暗号化セッション鍵C_0として送信する。
【０４００】
図２５は、この実施の形態における受信者装置３００の機能ブロックの構成の一例を示すブロック構成図である。
受信者装置３００は、受信パラメータ取得部３１１、秘密鍵取得部３２１、秘密鍵記憶部３２２、暗号化セッション鍵受信部３３１、受信ペアリング値算出部３３３、セッション鍵復元部３３４、受信セッション鍵記憶部３３５、暗号文受信部３４１、暗号文復号部３４２を有する。
【０４０１】
このうち、受信パラメータ取得部３１１、秘密鍵取得部３２１、秘密鍵記憶部３２２、受信ペアリング値算出部３３３、受信セッション鍵記憶部３３５、暗号文受信部３４１、暗号文復号部３４２は、実施の形態１で説明したものと同様なので、ここでは説明を省略する。
【０４０２】
暗号化セッション鍵受信部３３１は、通信装置９１５を用いて、送信者装置２００が送信してきた暗号化セッション鍵C_0を受信する。
暗号化セッション鍵受信部３３１は、ＣＰＵ９１１などの処理装置を用いて、受信した暗号化セッション鍵C_0に含まれる第四要素情報と、マスク情報ｖとを出力する。
第四要素情報は、加法群G_1の要素Ｒを示す情報である。
【０４０３】
セッション鍵復元部３３４は、ＣＰＵ９１１などの処理装置を用いて、暗号化セッション鍵受信部３３１が出力した第四要素情報を入力する。
セッション鍵復元部３３４は、ＣＰＵ９１１などの処理装置を用いて、暗号化セッション鍵受信部３３１が出力したマスク情報ｖを入力する。
セッション鍵復元部３３４は、ＣＰＵ９１１などの処理装置を用いて、受信ペアリング値算出部３３３が出力した受信ペアリング値情報を入力する。
受信ペアリング値情報は、乗法群G_Tの要素ｗ’を示す情報である。
【０４０４】
セッション鍵復元部３３４は、ＣＰＵ９１１などの処理装置を用いて、入力した第四要素情報と、入力した受信ペアリング値情報とを結合して、ビット列情報を生成する。
セッション鍵復元部３３４は、ＣＰＵ９１１などの処理装置を用いて、生成したビット列情報に対応するハッシュ値を算出する。このとき、セッション鍵復元部３３４は、ユーザ秘密鍵生成センタ１００が公開したマスク生成関数H_2を用いて、ハッシュ値を算出す

る。セッション鍵復元部３３４は、生成したビット列情報を、マスク生成関数H_2の入力とする。

セッション鍵復元部３３４は、ＣＰＵ９１１などの処理装置を用いて、算出したハッシュ値を示す情報と、入力したマスク情報ｖとの排他的論理和を算出して、復元文字列情報とする。

【０４０５】

実施の形態１で説明したように、受信ペアリング値算出部３３３が算出したペアリング値ｗ’は、送信者装置２００の送信ペアリング値算出部２３３が算出したペアリング値ｗと等しい。

したがって、セッション鍵復元部３３４がマスク生成関数H_2を用いて算出したハッシュ値は、送信者装置２００のセッション鍵生成部２３４がマスク生成関数H_2を用いて算出したハッシュ値と等しい。

【０４０６】

マスク情報ｖは、文字列情報と、マスク生成関数H_2を用いて算出したハッシュ値を示す情報との排他的論理和であるから、セッション鍵復元部３３４が算出した復元文字列情報は、送信者装置２００の文字列選択部２２４が選択した文字列ｍを示す文字列情報と等しい。

【０４０７】

セッション鍵復元部３３４は、ＣＰＵ９１１などの処理装置を用いて、算出した復元文字列情報に対応するハッシュ値を算出して、自然数ｒ’とする。このとき、セッション鍵復元部３３４は、ユーザ秘密鍵生成センタ１００が公開したハッシュ関数H_3を用いて、ハッシュ値を算出する。セッション鍵復元部３３４は、算出した復元文字列情報を、ハッシュ関数H_3の入力とする。

セッション鍵復元部３３４は、ＣＰＵ９１１などの処理装置を用いて、受信パラメータ取得部３１１が取得したパラメータ情報に含まれる第一要素情報を入力する。

セッション鍵復元部３３４は、ＣＰＵ９１１などの処理装置を用いて、入力した第一要素情報が示す加法群G_1の要素P_1と、算出した自然数ｒ’とから、加法群G_1の要素P_1のｒ’倍を算出し、加法群G_1の要素Ｒ’とする。

セッション鍵復元部３３４は、入力した第四要素情報が示す加法群G_1の要素Ｒと、算出した加法群G_1の要素Ｒ’とを比較する。

セッション鍵復元部３３４は、加法群G_1の要素Ｒと加法群G_1の要素Ｒ’とが等しくない場合、復号に失敗したことを示す情報を出力して、処理を中断する。

【０４０８】

セッション鍵復元部３３４が復元した復元文字列情報と、送信者装置２００の文字列選択部２２４が出力した文字列情報とは等しいはずなので、自然数ｒと自然数ｒ’とは等しく、したがって、加法群G_1の要素ＲとＲ’とは等しいはずである。そのため、セッション鍵復元部３３４は、それを確認して、ＲとＲ’とが等しくない場合には、処理を中断する。

【０４０９】

セッション鍵復元部３３４は、ＣＰＵ９１１などの処理装置を用いて、算出した復元文字列情報に対応するハッシュ値を算出する。このとき、セッション鍵復元部３３４は、ユーザ秘密鍵生成センタ１００が公開した鍵導出関数Ｇを用いて、ハッシュ値を算出する。セッション鍵復元部３３４は、算出した復元文字列情報を、鍵導出関数Ｇの入力とする。

セッション鍵復元部３３４は、ＣＰＵ９１１などの処理装置を用いて、算出したハッシュ値を、セッション鍵Ｋとして出力する。

【０４１０】

上述したように、セッション鍵復元部３３４が算出した復元文字列情報は、元の文字列情報と同じであるから、セッション鍵復元部３３４は、送信者装置２００のセッション鍵生成部２３４が生成したセッション鍵Ｋと同一のセッション鍵を復元する。

【０４１１】

こうして、送信者装置２００と受信者装置３００とは、同一のセッション鍵Ｋを共有するので、セッション鍵Ｋを用いた共通鍵暗号方式による通信を行うことができる。

【０４１２】

図２６は、この実施の形態における送信者装置２００がセッション鍵Ｋを生成するセッション鍵生成処理の流れの一例を示すフローチャート図である。

なお、実施の形態１で図９を用いて説明した工程と共通する工程については、同一の符号を付し、説明を簡略化する。

【０４１３】

Ｓ３１において、パラメータ取得部２１１は、ＣＰＵ９１１などの処理装置を用いて、ユーザ秘密鍵生成センタ１００が公開したパラメータ情報を取得する。

Ｓ３２において、送信識別情報取得部２３１は、ＣＰＵ９１１などの処理装置を用いて、受信者装置３００のＩＤを示す情報（識別情報）を取得する。

【０４１４】

Ｓ５３において、文字列選択部２２４は、ＣＰＵ９１１などの処理装置を用いて、文字列ｍをランダムに選択する。

文字列選択部２２４は、ＣＰＵ９１１などの処理装置を用いて、選択した文字列ｍを示す文字列情報を出力する。

【０４１５】

Ｓ５４において、自然数算出部２２５は、ＣＰＵ９１１などの処理装置を用いて、Ｓ５３で文字列選択部２２４が出力した文字列情報を入力する。

自然数算出部２２５は、ＣＰＵ９１１などの処理装置を用いて、入力した文字列情報に対応するハッシュ値を算出し、自然数ｒとする。

自然数算出部２２５は、ＣＰＵ９１１などの処理装置を用いて、算出した自然数ｒを示す情報を、乱数情報として出力する。

【０４１６】

Ｓ３４において、第四要素算出部２２２は、ＣＰＵ９１１などの処理装置を用いて、第一要素記憶部２１２が記憶した第一要素情報が示す加法群G_1の要素P_1と、Ｓ５４で自然数算出部２２５が出力した乱数情報が示す自然数ｒとに基づいて、加法群G_1の要素P_1のｒ倍を算出し、加法群G_1の要素Ｒとする。

Ｓ３５において、第五要素算出部２３２は、ＣＰＵ９１１などの処理装置を用いて、受信者装置３００のＩＤを示す情報に対応する加法群G_2の要素Q_{ID}を算出する。

Ｓ３６において、送信ペアリング値算出部２３３は、ＣＰＵ９１１などの処理装置を用いて、第二要素記憶部２１３が記憶した第二要素情報が示す加法群G_1の要素P_{pub}と、Ｓ３５で第五要素算出部２３２が算出した加法群G_2の要素Q_{ID}と、Ｓ５４で自然数算出部２２５が出力した乱数情報が示す自然数ｒとに基づいて、ペアリング値$e(P_{pub}, Q_{ID})^r$を算出し、乗法群G_Tの要素ｗとする。

【０４１７】

Ｓ５８において、セッション鍵生成部２３４は、ＣＰＵ９１１などの処理装置を用いて、Ｓ３４で第四要素算出部２２２が算出した加法群G_1の要素Ｒを示す第四要素情報と、Ｓ３６で送信ペアリング値算出部２３３が算出した乗法群G_2の要素ｗを示す送信ペアリング値情報と、Ｓ５３で文字列選択部２２４が出力した文字列情報とを入力する。

セッション鍵生成部２３４は、ＣＰＵ９１１などの処理装置を用いて、入力した第四要素情報と、入力した送信ペアリング情報とを結合して、ビット列情報を生成する。

セッション鍵生成部２３４は、ＣＰＵ９１１などの処理装置を用いて、生成したビット列情報に対応するハッシュ値を算出する。

セッション鍵生成部２３４は、ＣＰＵ９１１などの処理装置を用いて、算出したハッシュ値と、入力した文字列情報との排他的論理和を算出し、マスク情報ｖとする。

セッション鍵生成部２３４は、ＣＰＵ９１１などの処理装置を用いて、算出したマスク情報ｖを出力する。

【０４１８】

Ｓ５９において、セッション鍵生成部２３４は、ＣＰＵ９１１などの処理装置を用いて、Ｓ５８で入力した文字列情報に対応するハッシュ値を算出し、セッション鍵Ｋとする。

セッション鍵生成部２３４は、算出したセッション鍵Ｋを出力する。

【０４１９】

Ｓ６０において、暗号化セッション鍵送信部２２３は、ＣＰＵ９１１などの処理装置を用いて、Ｓ３４で第四要素算出部２２２が算出した加法群$Ｇ_{1}$の要素Ｒを示す第四要素情報と、Ｓ５８でセッション鍵生成部２３４が出力したマスク情報ｖとを入力する。

暗号化セッション鍵送信部２２３は、通信装置９１５を用いて、受信者装置３００に対して、入力した第四要素情報と、入力したマスク情報ｖとを含む情報を、暗号化セッション鍵$Ｃ_{0}$として送信する。

【０４２０】

図２７は、この実施の形態における受信者装置３００がセッション鍵Ｋを復元するセッション鍵復元処理の流れの一例を示すフローチャート図である。

なお、実施の形態１で図１０を用いて説明した工程と共通する工程については、同一の符号を付し、説明を簡略化する。

【０４２１】

Ｓ４１において、受信パラメータ取得部３１１は、ＣＰＵ９１１などの処理装置を用いて、ユーザ秘密鍵生成センタ１００が公開したパラメータ情報を取得する。

Ｓ４２において、秘密鍵取得部３２１は、ＣＰＵ９１１などの処理装置を用いて、ユーザ秘密鍵生成センタ１００が秘密裡に通知したユーザ秘密鍵情報を取得する。

【０４２２】

Ｓ６３において、暗号化セッション鍵受信部３３１は、通信装置９１５を用いて、送信者装置２００から送信してきた暗号化セッション鍵$Ｃ_{0}$を受信する。

暗号化セッション鍵受信部３３１は、ＣＰＵ９１１などの処理装置を用いて、受信した暗号化セッション鍵$Ｃ_{0}$に含まれる第四要素情報とマスク情報ｖとを出力する。

【０４２３】

Ｓ４４において、受信ペアリング値算出部３３３は、ＣＰＵ９１１などの処理装置を用いて、Ｓ６３で暗号化セッション鍵受信部３３１が出力した第四要素情報が示す加法群$Ｇ_{1}$の要素Ｒと、秘密鍵記憶部３２２が記憶したユーザ秘密鍵情報が示す加法群$Ｇ_{2}$の要素$ｄ_{ＩＤ}$とに基づいて、ペアリング値ｅ（Ｒ，$ｄ_{ＩＤ}$）を算出し、乗法群$Ｇ_{Ｔ}$の要素ｗ’とする。

【０４２４】

Ｓ６５において、セッション鍵復元部３３４は、ＣＰＵ９１１などの処理装置を用いて、Ｓ６３で暗号化セッション鍵受信部３３１が出力した第四要素情報とマスク情報ｖと、Ｓ４４で受信ペアリング値算出部３３３が算出した乗法群$Ｇ_{Ｔ}$の要素ｗ’を示す受信ペアリング値情報と、受信パラメータ取得部３１１が取得したパラメータ情報に含まれる第一要素情報とを入力する。

セッション鍵復元部３３４は、ＣＰＵ９１１などの処理装置を用いて、入力した第四要素情報と、入力した受信ペアリング値情報とを結合して、ビット列情報を生成する。

セッション鍵復元部３３４は、ＣＰＵ９１１などの処理装置を用いて、生成したビット列情報に対応するハッシュ値を算出する。

セッション鍵復元部３３４は、ＣＰＵ９１１などの処理装置を用いて、算出したハッシュ値と、入力したマスク情報ｖとの排他的論理和を算出し、復元文字列情報とする。

セッション鍵復元部３３４は、ＣＰＵ９１１などの処理装置を用いて、算出した復元文字列情報に対応するハッシュ値を算出して、自然数ｒ’とする。

セッション鍵復元部３３４は、ＣＰＵ９１１などの処理装置を用いて、入力した第一要素情報が示す加法群$Ｇ_{1}$の要素$Ｐ_{1}$と、算出した自然数ｒ’とから、加法群$Ｇ_{1}$の要素$Ｐ_{1}$のｒ’倍を算出し、加法群$Ｇ_{1}$の要素Ｒ’とする。

セッション鍵復元部３３４は、ＣＰＵ９１１などの処理装置を用いて、入力した第四要素情報が示す加法群$Ｇ_{1}$の要素Ｒと、算出した加法群$Ｇ_{1}$の要素Ｒ’とを比較して、等し

いか否かを判断する。
　等しいと判断した場合、Ｓ６６へ進む。
　等しくないと判断した場合、セッション鍵復元処理を終了する。
【０４２５】
　Ｓ６６において、セッション鍵復元部３３４は、ＣＰＵ９１１などの処理装置を用いて、Ｓ６５で算出した復元文字列情報に対応するハッシュ値を算出し、セッション鍵Ｋとする。
　セッション鍵復元部３３４は、ＣＰＵ９１１などの処理装置を用いて、算出したセッション鍵Ｋを出力する。
【０４２６】
　次に、この実施の形態における暗号方式の安全性について説明する。
【０４２７】
　この実施の形態における暗号方式において、マスク生成関数H_2には、ランダムオラクルとみなすことができる関数を用いる。
　マスク生成関数H_2に入力するビット列情報は、加法群G_1の要素Ｒを示す情報（第四要素情報）と、ペアリング値ｗを示す情報（送信ペアリング値情報）とを結合したものである。
【０４２８】
　したがって、実施の形態１における暗号方式の安全性の議論において、鍵導出関数Ｇであるランダムオラクルを、ランダムオラクルＧとして議論したが、これを、マスク生成関数H_2であるランダムオラクルに置き換えれば、まったく同じように、この実施の形態における暗号方式の安全性が証明できる。
【０４２９】
　以上より、この実施の形態の暗号方式は、Ｇ－ＢＤＨ問題に効率良く帰着する安全性の高い暗号方式であることが証明された。
【０４３０】
　この実施の形態における送信者装置２００は、
　情報を記憶する磁気ディスク装置９２０などの記憶装置と、
　情報を処理するＣＰＵ９１１などの処理装置と、
　受信者装置に対して情報を送信する送信装置（通信装置９１５）と、
　磁気ディスク装置９２０などの記憶装置を用いて、加法群G_1の要素Ｐを示す情報を第一要素情報として記憶する第一要素記憶部２１２と、
　磁気ディスク装置９２０などの記憶装置を用いて、加法群G_1の要素P_{pub}を示す情報を第二要素情報として記憶する第二要素記憶部２１３と、
　ＣＰＵ９１１などの処理装置を用いて、第一要素記憶部２１２が記憶した第一要素情報と自然数ｒを示す乱数情報とを入力し、ＣＰＵ９１１などの処理装置を用いて、入力した第一要素情報と乱数情報とに基づいて、加法群G_1の要素Ｒを算出し、ＣＰＵ９１１などの処理装置を用いて、算出した加法群G_1の要素Ｒを示す情報を第四要素情報として出力する第四要素算出部２２２と、
　ＣＰＵ９１１などの処理装置を用いて、受信者装置３００を識別する識別情報（ＩＤを示す情報）を入力し、ＣＰＵ９１１などの処理装置を用いて、入力した識別情報に対応する加法群G_2の要素Q_{ID}を算出し、ＣＰＵ９１１などの処理装置を用いて、算出した加法群G_2の要素Q_{ID}を示す情報を第五要素情報として出力する第五要素算出部２３２と、
　ＣＰＵ９１１などの処理装置を用いて、第二要素記憶部２１３が記憶した第二要素情報と第五要素算出部２３２が出力した第五要素情報と上記乱数情報とを入力し、ＣＰＵ９１１などの処理装置を用いて、入力した第二要素情報と第五要素情報とに基づいて、加法群G_1の要素P_{pub}と加法群G_2の要素Q_{ID}とのペアリング値を算出し、ＣＰＵ９１１などの処理装置を用いて、算出したペアリング値と入力した乱数情報とに基づいて、乗法群G_Tの要素ｗを算出し、ＣＰＵ９１１などの処理装置を用いて、算出した乗法群G_Tの

要素ｗを示す情報を送信ペアリング値情報として出力する送信ペアリング値算出部２３３と、
ＣＰＵ９１１などの処理装置を用いて、第四要素算出部２２２が出力した第四要素情報と送信ペアリング値算出部２３３が出力した送信ペアリング値情報とを入力し、ＣＰＵ９１１などの処理装置を用いて、入力した第四要素情報と送信ペアリング値情報とに基づいて、ハッシュ値を算出し、ＣＰＵ９１１などの処理装置を用いて、算出したハッシュ値に基づいて、受信者装置３００がセッション鍵Ｋを復元するために用いるマスク情報ｖを生成し、ＣＰＵ９１１などの処理装置を用いて、生成したマスク情報ｖを出力するセッション鍵生成部２３４と、
ＣＰＵ９１１などの処理装置を用いて、第四要素算出部２２２が出力した第四要素情報と、セッション鍵生成部２３４が出力したマスク情報ｖとを入力し、送信装置（通信装置９１５）を用いて、入力した第四要素情報とマスク情報ｖとを含む情報を暗号化セッション鍵C_0として受信者装置３００に対して送信する暗号化セッション鍵送信部と、
を有することを特徴とする。
【０４３１】
この実施の形態における送信者装置２００によれば、セッション鍵生成部２３４が、加法群G_1の要素Ｒを示す第四要素情報と、ペアリング値ｗを示す送信ペアリング値情報とに基づいてハッシュ値を算出し、算出したハッシュ値に基づいて、受信者装置３００がセッション鍵Ｋを復元するために用いるマスク情報ｖを生成するので、Ｇ－ＢＤＨ問題に効率良く帰着する安全性の高い暗号方式を実現することができるという効果を奏する。
【０４３２】
この実施の形態における送信者装置２００は、更に、
ＣＰＵ９１１などの処理装置を用いて、文字列ｍをランダムに選択し、ＣＰＵ９１１などの処理装置を用いて、選択した文字列ｍを示す情報を文字列情報として出力する文字列選択部２２４と、
ＣＰＵ９１１などの処理装置を用いて、文字列選択部２２４が出力した文字列情報を入力し、ＣＰＵ９１１などの処理装置を用いて、入力した文字列情報に対応するハッシュ値を算出し、ＣＰＵ９１１などの処理装置を用いて、算出したハッシュ値を示す情報を、第四要素算出部２２２及び上記送信ペアリング値算出部２３３が入力する乱数情報として出力する自然数算出部２２５と、
を有し、
セッション鍵生成部２３４が、
ＣＰＵ９１１などの処理装置を用いて、第四要素情報と、送信ペアリング値情報と、文字列選択部２２４が出力した文字列情報とを入力し、ＣＰＵ９１１などの処理装置を用いて、入力した第四要素情報と送信ペアリング値情報とを結合してビット列情報を生成し、ＣＰＵ９１１などの処理装置を用いて、生成したビット列情報に対応するハッシュ値を算出し、ＣＰＵ９１１などの処理装置を用いて、算出したハッシュ値を示す情報と入力した文字列情報との排他的論理和を算出してマスク情報ｖとし、ＣＰＵ９１１などの処理装置を用いて、算出したマスク情報ｖを出力し、ＣＰＵ９１１などの処理装置を用いて、入力した文字列情報に対応するハッシュ値を算出し、算出したハッシュ値をセッション鍵Ｋとし、
暗号化セッション鍵送信部２２３が、
ＣＰＵ９１１などの処理装置を用いて、第四要素情報と、セッション鍵生成部２３４が出力したマスク情報ｖとを入力し、送信装置（通信装置９１５）を用いて、入力した第四要素情報とマスク情報ｖとを含む情報を暗号化セッション鍵C_0として受信者装置３００に対して送信することを特徴とする。
【０４３３】
この実施の形態における送信者装置２００によれば、セッション鍵生成部２３４が、加法群G_1の要素Ｒを示す第四要素情報と、ペアリング値ｗを示す送信ペアリング値情報とを結合してビット列情報を生成し、生成したビット列情報に対応するハッシュ値を算出し

、算出したハッシュ値を示す情報に基づいて、マスク情報ｖを生成するので、Ｇ－ＢＤＨ問題に効率良く帰着する安全性の高い暗号方式により受信者装置３００と共有するセッション鍵Ｋを、効率的に生成することができるという効果を奏する。

【０４３４】

この実施の形態における受信者装置３００は、

暗号化セッション鍵受信部３３１が、

受信装置（通信装置９１５）を用いて、暗号化セッション鍵C_0を受信し、ＣＰＵ９１１などの処理装置を用いて、受信した暗号化セッション鍵C_0に含まれる第四要素情報とマスク情報ｖとを出力し、

セッション鍵復元部３３４が、

ＣＰＵ９１１などの処理装置を用いて、第四要素情報と、受信ペアリング値情報と、暗号化セッション鍵受信部３３１が出力したマスク情報ｖとを入力し、ＣＰＵ９１１などの処理装置を用いて、入力した第四要素情報と受信ペアリング値情報とを結合してビット列情報を生成し、ＣＰＵ９１１などの処理装置を用いて、生成したビット列情報に対応するハッシュ値を算出し、ＣＰＵ９１１などの処理装置を用いて、算出したハッシュ値を示す情報と入力したマスク情報ｖとの排他的論理和を算出して、復元文字列情報とし、ＣＰＵ９１１などの処理装置を用いて、算出した復元文字列情報に対応するハッシュ値を算出し、算出したハッシュ値をセッション鍵Ｋとすることを特徴とする。

【０４３５】

この実施の形態における受信者装置３００によれば、セッション鍵復元部３３４が、加法群G_1の要素Ｒを示す第四要素情報と、ペアリング値ｗ’を示す受信ペアリング値情報とを結合してビット列情報を生成し、生成したビット列情報に対応するハッシュ値を算出し、算出したハッシュ値を示す情報に基づいて、セッション鍵Ｋを復元するので、Ｇ－ＢＤＨ問題に効率良く帰着する安全性の高い暗号方式により送信者装置２００と共有するセッション鍵Ｋを、効率的に復元することができるという効果を奏する。

【０４３６】

以上説明したセッション鍵共有装置は、

ペアリングを用いたＩＤベース公開鍵暗号を用いたセッション鍵共有装置において、ペアリング値をハッシュするのに用いるマスク生成関数への入力として、ペアリング値だけでなく、セッション鍵を暗号化した値も入力に加わっていることを特徴とする。

【０４３７】

以上説明したセッション鍵共有装置は、

ペアリングを用いたＩＤベース鍵配送方式を用いたセッション鍵共有装置において、前記セッション鍵を暗号化するのに、

ＩＤ情報ＩＤから一意的に決まるQ_{ID}を計算し、

データｍをランダムに生成し、ｍのハッシュ値$r = H_3(m)$を計算し、$R = rP_1$とし、

P_{pub}とQ_{ID}のペアリング値のｒ乗$w = e(P_{pub}, Q_{ID})^r$を計算し、

マスク生成関数H_2を用いて$v = XOR(m, H_2(R, w))$を計算し、

鍵導出関数Ｇを用いて、セッション鍵$K = G(m)$を計算し、

セッション鍵Ｋと前記セッション鍵の暗号化$C_0 = (R, v)$を出力することを特徴とする。

【０４３８】

以上説明したセッション鍵共有装置は、

ペアリングを用いたＩＤベース鍵配送方式を用いたセッション鍵共有装置において、暗号化された鍵$C_0 = (R, v)$を復号するのに、

Ｒとユーザプライベート鍵d_{ID}のペアリング値$w = e(R, d_{ID})$を計算し、

マスク生成関数H_2を用いて$m = XOR(v, H_2(R, w))$を計算し、

$r = H_3(m)$を計算し、

$R = rP_1$であるかどうかをチェックし、もし成立すれば、

鍵導出関数Ｇを用いて、セッション鍵Ｋ＝Ｇ（ｍ）を計算し、
セッション鍵Ｋを出力することを特徴とする。
【０４３９】
以上説明したセッション鍵共有プログラムは、
ペアリングを用いたＩＤベース公開鍵暗号を用いたセッション鍵共有プログラムにおいて、ペアリング値をハッシュするのに用いるマスク生成関数への入力として、ペアリング値だけでなく、セッション鍵を暗号化した値も入力に加わっていることを特徴とする。
【０４４０】
以上説明したセッション鍵共有プログラムは、
ペアリングを用いたＩＤベース鍵配送方式を用いたセッション鍵共有プログラムにおいて、前記セッション鍵を暗号化するのに、
ＩＤ情報ＩＤから一意的に決まるQ_{ID}を計算し、
データｍをランダムに生成し、ｍのハッシュ値ｒ＝H_3（ｍ）を計算し、Ｒ＝ｒP_1とし、
P_{pub}とQ_{ID}のペアリング値のｒ乗ｗ＝ｅ（P_{pub}，Q_{ID}）^{r}を計算し、
マスク生成関数H_2を用いてｖ＝ＸＯＲ（ｍ，H_2（Ｒ，ｗ））を計算し、
鍵導出関数Ｇを用いて、セッション鍵Ｋ＝Ｇ（ｍ）を計算し、
セッション鍵Ｋと前記セッション鍵の暗号化C_0＝（Ｒ，ｖ）を出力することを特徴とする。
【０４４１】
以上説明したセッション鍵共有プログラムは、
ペアリングを用いたＩＤベース鍵配送方式を用いたセッション鍵共有プログラムにおいて、暗号化された鍵C_0＝（Ｒ，ｖ）を復号するのに、
Ｒとユーザプライベート鍵d_{ID}のペアリング値ｗ＝ｅ（Ｒ，d_{ID}）を計算し、
マスク生成関数H_2を用いてｍ＝ＸＯＲ（ｖ，H_2（Ｒ，ｗ））を計算し、
ｒ＝H_3（ｍ）を計算し、
Ｒ＝ｒP_1であるかどうかをチェックし、もし成立すれば、
鍵導出関数Ｇを用いて、セッション鍵Ｋ＝Ｇ（ｍ）を計算し、
セッション鍵Ｋを出力することを特徴とする。
【０４４２】
以上説明したＩＤベース公開鍵暗号装置は、
ペアリングを用いたＩＤベース公開鍵暗号装置において、ペアリング値をハッシュするのに用いるマスク生成関数への入力として、ペアリング値だけでなく、セッション鍵を暗号化した値も入力に加わっていることを特徴とする。
【０４４３】
以上説明したＩＤベース公開鍵暗号装置は、
ペアリングを用いたＩＤベース公開鍵暗号装置において、平文Ｍを暗号化するのに、
ＩＤ情報ＩＤから一意的に決まるQ_{ID}を計算し、
データｍをランダムに生成し、ｍのハッシュ値ｒ＝H_3（ｍ）を計算し、Ｒ＝ｒP_1とし、
P_{pub}とQ_{ID}のペアリング値のｒ乗ｗ＝ｅ（P_{pub}，Q_{ID}）^{r}を計算し、
マスク生成関数H_2を用いてｖ＝ＸＯＲ（ｍ，H_2（Ｒ，ｗ））を計算し、
鍵導出関数Ｇを用いて、セッション鍵Ｋ＝Ｇ（ｍ）を計算し、
鍵Ｋを用いて計算されたＭの暗号化を出力することを特徴とする。
【０４４４】
以上説明したＩＤベース公開鍵暗号装置は、
ビット毎の排他的論理和ＸＯＲ（，）を用い、鍵Ｋを用いて計算されたＭの暗号化として、ＸＯＲ（Ｍ，Ｋ）を用いることを特徴とする。
【０４４５】
以上説明したＩＤベース公開鍵暗号装置は、

ペアリングを用いたＩＤベース公開鍵暗号装置において、暗号化された鍵C_0＝（Ｒ，ｖ）を復号するのに、
Ｒとユーザプライベート鍵d_{ID}のペアリング値ｗ＝ｅ（Ｒ、d_{ID}）を計算し、
マスク生成関数H_2を用いてｍ＝ＸＯＲ（ｖ，H_2（Ｒ，ｗ））を計算し、
ｒ＝H_3（ｍ）を計算し、
Ｒ＝ｒP_1であるかどうかをチェックし、もし成立すれば、
鍵導出関数Ｇを用いて、セッション鍵Ｋ＝Ｇ（ｍ）を計算し、
鍵Ｋを用いて計算された暗号文Ｃの復号を出力することを特徴とする。

【０４４６】

以上説明したＩＤベース公開鍵暗号装置は、
ビット毎の排他的論理和ＸＯＲ（，）を用い、鍵Ｋを用いて計算されたＣの復号として、ＸＯＲ（Ｃ，Ｋ）を用いることを特徴とする。

【０４４７】

以上説明したＩＤベース公開鍵暗号プログラムは、
ペアリングを用いたＩＤベース公開鍵暗号プログラムにおいて、ペアリング値をハッシュするのに用いるマスク生成関数への入力として、ペアリング値だけでなく、セッション鍵を暗号化した値も入力に加わっていることを特徴とする。

【０４４８】

以上説明したＩＤベース公開鍵暗号プログラムは、
ペアリングを用いたＩＤベース公開鍵暗号プログラムにおいて、平文Ｍを暗号化するのに、
ＩＤ情報ＩＤから一意的に決まるQ_{ID}を計算し、
データｍをランダムに生成し、ｍのハッシュ値ｒ＝H_3（ｍ）を計算し、Ｒ＝ｒP_1とし、
P_{pub}とQ_{ID}のペアリング値のｒ乗ｗ＝ｅ（P_{pub}，Q_{ID}）^{r}を計算し、
マスク生成関数H_2を用いてｖ＝ＸＯＲ（ｍ，H_2（Ｒ，ｗ））を計算し、
鍵導出関数Ｇを用いて、セッション鍵Ｋ＝Ｇ（ｍ）を計算し、
鍵Ｋを用いて計算されたＭの暗号化を出力することを特徴とする。

【０４４９】

以上説明したＩＤベース公開鍵暗号プログラムは、
ビット毎の排他的論理和ＸＯＲ（，）を用い、鍵Ｋを用いて計算されたＭの暗号化として、ＸＯＲ（Ｍ，Ｋ）を用いることを特徴とする。

【０４５０】

以上説明したＩＤベース公開鍵暗号プログラムは、
ペアリングを用いたＩＤベース公開鍵暗号プログラムにおいて、暗号化された鍵C_0＝（Ｒ，ｖ）を復号するのに、
Ｒとユーザプライベート鍵d_{ID}のペアリング値ｗ＝ｅ（Ｒ，d_{ID}）を計算し、
マスク生成関数H_2を用いてｍ＝ＸＯＲ（ｖ，H_2（Ｒ，ｗ））を計算し、
ｒ＝H_3（ｍ）を計算し、
Ｒ＝ｒP_1であるかどうかをチェックし、もし成立すれば、
鍵導出関数Ｇを用いて、セッション鍵Ｋ＝Ｇ（ｍ）を計算し、
鍵Ｋを用いて計算された暗号文Ｃの復号を出力することを特徴とする。

【０４５１】

以上説明したＩＤベース公開鍵暗号プログラムは、
ビット毎の排他的論理和ＸＯＲ（，）を用い、鍵Ｋを用いて計算されたＣの復号として、ＸＯＲ（Ｃ，Ｋ）を用いることを特徴とする。

【０４５２】

実施の形態３．
実施の形態３について、図２８～図２９を用いて説明する。
この実施の形態におけるＩＤベース公開鍵暗号通信システム８００（暗号通信システム

）の全体構成、ユーザ秘密鍵生成センタ１００・送信者装置２００・受信者装置３００のハードウェア構成は、実施の形態１で説明したものと同様なので、ここでは説明を省略する。

また、ユーザ秘密鍵生成センタ１００の機能ブロックの構成は、実施の形態１で説明したものと同様なので、ここでは説明を省略する。

なお、ユーザ秘密鍵生成センタ１００のパラメータ公開部１２２が公開するパラメータ情報には、実施の形態１で説明した情報のほか、マスク生成関数H_2及びハッシュ関数H_3を示す情報が含まれている。

マスク生成関数H_2及びハッシュ関数H_3には、ランダムオラクルとみなせる関数を用いる。

【０４５３】

図２８は、この実施の形態における送信者装置２００の機能ブロックの構成の一例を示すブロック構成図である。

送信者装置２００は、パラメータ取得部２１１、第一要素記憶部２１２、第二要素記憶部２１３、第四要素算出部２２２、暗号化セッション鍵送信部２２３、自然数算出部２２５、セッション鍵入力部２２６、送信識別情報取得部２３１、第五要素算出部２３２、送信ペアリング値算出部２３３、セッション鍵生成部２３４、セッション鍵記憶部２３５、平文記憶部２４１、暗号文生成部２４２、暗号文送信部２４３を有する。

【０４５４】

このうち、パラメータ取得部２１１、第一要素記憶部２１２、第二要素記憶部２１３、第四要素算出部２２２、暗号化セッション鍵送信部２２３、送信識別情報取得部２３１、第五要素算出部２３２、送信ペアリング値算出部２３３、平文記憶部２４１、暗号文生成部２４２、暗号文送信部２４３は、実施の形態２で説明したものと同様なので、ここでは説明を省略する。

【０４５５】

セッション鍵入力部２２６は、ＣＰＵ９１１などの処理装置を用いて、文字列ｍを入力する。

セッション鍵入力部２２６は、ＣＰＵ９１１などの処理装置を用いて、入力した文字列ｍを示す情報を、文字列情報（セッション鍵）として出力する。

【０４５６】

自然数算出部２２５は、ＣＰＵ９１１などの処理装置を用いて、セッション鍵入力部２２６が出力した文字列情報（セッション鍵）を入力し、ユーザ秘密鍵生成センタ１００が公開したハッシュ関数H_3を用いて、入力した文字列情報（セッション鍵）に対応するハッシュ値を算出し、自然数ｒとして出力する。

【０４５７】

セッション鍵生成部２３４は、ＣＰＵ９１１などの処理装置を用いて、第四要素算出部２２２が出力した第四要素情報と、送信ペアリング値算出部２３３が出力した送信ペアリング値情報と、セッション鍵入力部２２６が出力した文字列情報（セッション鍵）を入力し、入力した第四要素情報と、入力した送信ペアリング値情報とを結合して、ビット列情報を生成し、ユーザ秘密鍵生成センタ１００が公開したマスク生成関数H_2を用いて、生成したビット列情報に対応するハッシュ値を算出し、算出したハッシュ値と、入力した文字列情報（セッション鍵）との排他的論理和を算出して、マスク情報ｖとし、算出したマスク情報ｖを出力する。

【０４５８】

セッション鍵記憶部２３５は、ＣＰＵ９１１などの処理装置を用いて、セッション鍵入力部２２６が出力した文字列情報（セッション鍵）を入力する。

セッション鍵記憶部２３５は、磁気ディスク装置９２０などの記憶装置を用いて、入力した文字列情報（セッション鍵）を、セッション鍵Ｋとして記憶する。

【０４５９】

図２９は、この実施の形態における受信者装置３００の機能ブロックの構成の一例を示

すブロック構成図である。
受信者装置３００は、受信パラメータ取得部３１１、秘密鍵取得部３２１、秘密鍵記憶部３２２、暗号化セッション鍵受信部３３１、受信ペアリング値算出部３３３、セッション鍵復元部３３４、受信セッション鍵記憶部３３５、暗号文受信部３４１、暗号文復号部３４２を有する。
【０４６０】
このうち、受信パラメータ取得部３１１、秘密鍵取得部３２１、秘密鍵記憶部３２２、暗号化セッション鍵受信部３３１、受信ペアリング値算出部３３３、暗号文受信部３４１、暗号文復号部３４２は、実施の形態２で説明したものと同様なので、ここでは説明を省略する。
【０４６１】
セッション鍵復元部３３４は、ＣＰＵ９１１などの処理装置を用いて、暗号化セッション鍵受信部３３１が出力した第四要素情報及びマスク情報ｖと、受信ペアリング値算出部３３３が出力した受信ペアリング値情報とを入力する。
セッション鍵復元部３３４は、ＣＰＵ９１１などの処理装置を用いて、入力した第四要素情報と、入力した受信ペアリング値情報とを結合して、ビット列情報を生成する。
セッション鍵復元部３３４は、ＣＰＵ９１１などの処理装置を用いて、生成したビット列情報に対応するハッシュ値を、ユーザ秘密鍵生成センタ１００が公開したマスク生成関数H_2により、算出する。
セッション鍵復元部３３４は、ＣＰＵ９１１などの処理装置を用いて、算出したハッシュ値と、入力したマスク情報との排他的論理和を算出して、復元文字列情報（セッション鍵）とする。
セッション鍵復元部３３４は、ＣＰＵ９１１などの処理装置を用いて、算出した復元文字列情報（セッション鍵）を出力する。
【０４６２】
受信セッション鍵記憶部３３５は、ＣＰＵ９１１などの処理装置を用いて、セッション鍵復元部３３４が出力した復元文字列情報（セッション鍵）を入力する。
受信セッション鍵記憶部３３５は、磁気ディスク装置９２０などの記憶装置を用いて、入力した復元文字列情報（セッション鍵）を、セッション鍵Ｋとして記憶する。
【０４６３】
この実施の形態のＩＤベース公開鍵暗号通信システム８００は、実施の形態１及び実施の形態２で説明した鍵カプセル化方式によるセッション鍵共有方式と異なり、入力した文字列ｍを示す情報を、そのままセッション鍵として用いるものである。
【０４６４】
この実施の形態における暗号方式において、暗号化セッション鍵C_0から、セッション鍵Ｋを復元するためには、加法群G_1の要素Ｒを示す第四要素情報と、ペアリング値ｗ’を示す受信ペアリング値情報とを結合したビット列情報に対応するハッシュ値を、マスク生成関数H_2により算出する必要がある。
【０４６５】
マスク生成関数H_2には、ランダムオラクルとみなすことができる関数を用いるので、実施の形態１の暗号方式の安全性についての議論と、並行する議論により、この実施の形態における暗号方式の安全性を証明することができる。
【０４６６】
このように、鍵カプセル化方式でないセッション鍵共有方式であっても、加法群G_1の要素Ｒを示す第四要素情報と、ペアリング値ｗ’を示す受信ペアリング値情報とを結合したビット列情報を、マスク生成関数H_2の入力とすることにより、Ｇ－ＢＤＨ問題に効率良く帰着する安全性の高い暗号方式とすることができる。
【０４６７】
この実施の形態における送信者装置２００は、更に、
ＣＰＵ９１１などの処理装置を用いて、文字列ｍを示す情報を入力し、ＣＰＵ９１１な

どの処理装置を用いて、入力した文字列ｍを示す情報を、セッション鍵として出力するセッション鍵入力部２２６と、

ＣＰＵ９１１などの処理装置を用いて、セッション鍵入力部２２６が出力したセッション鍵を入力し、ＣＰＵ９１１などの処理装置を用いて、入力したセッション鍵に対応するハッシュ値を算出し、ＣＰＵ９１１などの処理装置を用いて、算出したハッシュ値を示す情報を、第四要素算出部２２２及び送信ペアリング値算出部２３３が入力する乱数情報として出力する自然数算出部２２５と、

を有し、

セッション鍵生成部２３４が、

ＣＰＵ９１１などの処理装置を用いて、第四要素情報と、送信ペアリング値情報と、セッション鍵入力部２２６が出力したセッション鍵とを入力し、ＣＰＵ９１１などの処理装置を用いて、入力した第四要素情報と送信ペアリング値情報とを結合してビット列情報を生成し、ＣＰＵ９１１などの処理装置を用いて、生成したビット列情報に対応するハッシュ値を算出し、ＣＰＵ９１１などの処理装置を用いて、算出したハッシュ値を示す情報と入力した文字列情報との排他的論理和を算出してマスク情報ｖとし、ＣＰＵ９１１などの処理装置を用いて、算出したマスク情報ｖを出力し、

暗号化セッション鍵送信部２２３が、

ＣＰＵ９１１などの処理装置を用いて、第四要素情報と、セッション鍵生成部２３４が出力したマスク情報ｖとを入力し、送信装置（通信装置９１５）を用いて、入力した第四要素情報とマスク情報ｖとを含む情報を暗号化セッション鍵C_0として受信者装置３００に対して送信することを特徴とする。

【０４６８】

この実施の形態における送信者装置２００によれば、セッション鍵生成部２３４が、加法群G_1の要素Ｒを示す第四要素情報と、ペアリング値ｗを示す送信ペアリング値情報とを結合してビット列情報を生成し、生成したビット列情報に対応するハッシュ値を算出し、算出したハッシュ値を示す情報に基づいて、マスク情報ｖを生成するので、Ｇ－ＢＤＨ問題に効率良く帰着する安全性の高い暗号方式により受信者装置３００と共有するセッション鍵Ｋを、効率的に生成することができるという効果を奏する。

【０４６９】

この実施の形態における受信者装置３００は、

暗号化セッション鍵受信部３３１が、

受信装置（通信装置９１５）を用いて、暗号化セッション鍵C_0を受信し、ＣＰＵ９１１などの処理装置を用いて、受信した暗号化セッション鍵C_0に含まれる第四要素情報とマスク情報ｖとを出力し、

セッション鍵復元部３３４が、

ＣＰＵ９１１などの処理装置を用いて、第四要素情報と、受信ペアリング値情報と、暗号化セッション鍵受信部３３１が出力したマスク情報ｖとを入力し、ＣＰＵ９１１などの処理装置を用いて、入力した第四要素情報と受信ペアリング値情報とを結合してビット列情報を生成し、ＣＰＵ９１１などの処理装置を用いて、生成したビット列情報に対応するハッシュ値を算出し、ＣＰＵ９１１などの処理装置を用いて、算出したハッシュ値を示す情報と入力したマスク情報ｖとの排他的論理和を算出して、セッション鍵Ｋとすることを特徴とする。

【０４７０】

この実施の形態における受信者装置３００によれば、セッション鍵復元部３３４が、加法群G_1の要素Ｒを示す第四要素情報と、ペアリング値ｗ’を示す受信ペアリング値情報とを結合してビット列情報を生成し、生成したビット列情報に対応するハッシュ値を算出し、算出したハッシュ値を示す情報に基づいて、セッション鍵Ｋを復元するので、Ｇ－ＢＤＨ問題に効率良く帰着する安全性の高い暗号方式により送信者装置２００と共有するセッション鍵Ｋを、効率的に復元することができるという効果を奏する。

【０４７１】

実施の形態４.

実施の形態１～実施の形態３では、特定の方式によるＩＤベース公開鍵暗号通信システム８００について説明したが、上記の説明から明らかなように、以下の条件を満たす構成のＩＤベース暗号方式についても適用が可能である。

【０４７２】

（１）Ｇ－ＢＤＨ問題に帰着する暗号方式であること。

（２）セッション鍵を復元するために、鍵導出関数Ｇやマスク生成関数H_2などのランダムオラクルとみなすことができる関数を用いる暗号方式であること。

（３）送信者装置２００が受信者装置３００に対して送信する情報（暗号化セッション鍵C_0）に、双線形ペアリング関数の一方の入力である加法群の要素を示す情報が含まれていること。

（４）受信者装置３００がセッション鍵を復元するために用いる秘密情報（ユーザ秘密鍵）に、双線形ペアリング関数の他方の入力である加法群の要素を示す情報が含まれていること。

【０４７３】

以上の条件を満たすＩＤベース暗号方式において、

（５）（３）で述べた双線形ペアリング関数の一方の入力である加法群の要素を示す情報と、双線形ペアリング関数の出力であるペアリング値を示す情報とを結合した情報を、（２）で述べたランダムオラクルとみなすことができる関数の入力とすること。

【０４７４】

これにより、Ｇ－ＢＤＨ問題に効率良く帰着する安全性の高い暗号方式とすることができる。

【図面の簡単な説明】

【０４７５】

【図１】実施の形態１におけるＩＤベース公開鍵暗号通信システム８００の全体構成の一例を示すシステム構成図。

【図２】実施の形態１におけるユーザ秘密鍵生成センタ１００及び送信者装置２００及び受信者装置３００の外観の一例を示す図。

【図３】実施の形態１におけるユーザ秘密鍵生成センタ１００及び送信者装置２００及び受信者装置３００のハードウェア資源の一例を示す図。

【図４】実施の形態１におけるユーザ秘密鍵生成センタ１００の機能ブロックの構成の一例を示すブロック構成図。

【図５】実施の形態１における送信者装置２００の機能ブロックの一例を示すブロック構成図。

【図６】実施の形態１における受信者装置３００の機能ブロックの一例を示すブロック構成図。

【図７】実施の形態１におけるユーザ秘密鍵生成センタ１００がパラメータ情報を生成するパラメータ生成処理の流れの一例を示すフローチャート図。

【図８】実施の形態１におけるユーザ秘密鍵生成センタ１００がユーザ秘密鍵を生成する秘密鍵生成処理の流れの一例を示すフローチャート図。

【図９】実施の形態１における送信者装置２００がセッション鍵Ｋを生成するセッション鍵生成処理の流れの一例を示すフローチャート図。

【図１０】実施の形態１における受信者装置３００がセッション鍵Ｋを復元するセッション鍵復元処理の流れの一例を示すフローチャート図。

【図１１】ここで議論するＫＥＭにおけるＩＮＤ－ＩＤ－ＣＣＡ安全性の定義に登場する攻撃者Ａを示す図。

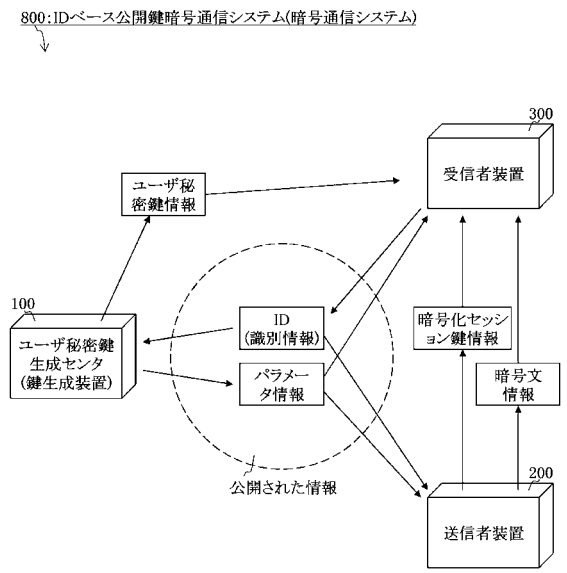
【図１２】ここで議論する攻撃者Ａの攻撃シナリオを示すフローチャート図。

【図１３】実施の形態１における暗号方式の安全性をＧ－ＢＤＨ問題に帰着させるために想定する（ＩＤベースではない）公開鍵暗号方式を説明する説明図。

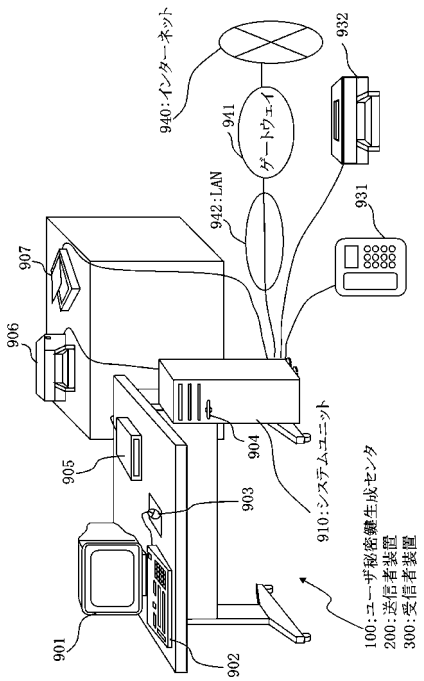
【図１４】一般的な攻撃者Ｂの攻撃シナリオを示すフローチャート図。

【図１５】攻撃者Ａを利用して非ＩＤベース公開鍵暗号方式を攻撃する攻撃者Ｂの構成を示す図。
【図１６】攻撃者Ａを利用して非ＩＤベース公開鍵暗号方式を攻撃する攻撃者Ｂのアルゴリズムを示すフローチャート図。
【図１７】攻撃者Ｂがオラクルをシミュレートするオラクルシミュレート処理の流れを示すフローチャート図（その１）。
【図１８】攻撃者Ｂがオラクルをシミュレートするオラクルシミュレート処理の流れを示すフローチャート図（その２）。
【図１９】攻撃者Ｂを利用してＧ－ＢＤＨ問題に解答する解答者Ｃの構成を示す図。
【図２０】攻撃者Ｂを利用してＧ－ＢＤＨ問題に解答する解答者Ｃのアルゴリズムを示すフローチャート図。
【図２１】解答者Ｃがオラクルをシミュレートするオラクルシミュレート処理の流れを示すフローチャート図（その１）。
【図２２】解答者Ｃがオラクルをシミュレートするオラクルシミュレート処理の流れを示すフローチャート図（その２）。
【図２３】解答者Ｃ’がランダムオラクルをシミュレートするオラクルシミュレート処理の流れを示すフローチャート図。
【図２４】実施の形態２における送信者装置２００の機能ブロックの構成の一例を示すブロック構成図。
【図２５】実施の形態２における受信者装置３００の機能ブロックの構成の一例を示すブロック構成図。
【図２６】実施の形態２における送信者装置２００がセッション鍵Ｋを生成するセッション鍵生成処理の流れの一例を示すフローチャート図。
【図２７】実施の形態２における受信者装置３００がセッション鍵Ｋを復元するセッション鍵復元処理の流れの一例を示すフローチャート図。
【図２８】実施の形態３における送信者装置２００の機能ブロックの構成の一例を示すブロック構成図。
【図２９】実施の形態３における受信者装置３００の機能ブロックの構成の一例を示すブロック構成図。
【符号の説明】
【０４７６】
１００　ユーザ秘密鍵生成センタ、１１０　公開パラメータ生成部、１１１　第一要素選択部、１１２　マスターキー選択部、１１３　マスターキー記憶部、１２１　第二要素算出部、１２２　パラメータ公開部、１３０　ユーザ秘密鍵生成部、１３１　識別情報取得部、１３２　第三要素算出部、１３３　秘密鍵算出部、１３４　秘密鍵通知部、２００　送信者装置、２１１　パラメータ取得部、２１２　第一要素記憶部、２１３　第二要素記憶部、２２１　自然数選択部、２２２　第四要素算出部、２２３　暗号化セッション鍵送信部、２２４　文字列選択部、２２５　自然数算出部、２２６　セッション鍵入力部、２３１　送信識別情報取得部、２３２　第五要素算出部、２３３　送信ペアリング値算出部、２３４　セッション鍵生成部、２３５　セッション鍵記憶部、２４１　平文記憶部、２４２　暗号文生成部、２４３　暗号文送信部、３００　受信者装置、３１１　受信パラメータ取得部、３２１　秘密鍵取得部、３２２　秘密鍵記憶部、３３１　暗号化セッション鍵受信部、３３３　受信ペアリング値算出部、３３４　セッション鍵復元部、３３５　受信セッション鍵記憶部、３４１　暗号文受信部、３４２　暗号文復号部、８００　ＩＤベース公開鍵暗号通信システム、９０１　表示装置、９０２　キーボード、９０３　マウス、９０４　ＦＤＤ、９０５　ＣＤＤ、９０６　プリンタ装置、９０７　スキャナ装置、９１０　システムユニット、９１１　ＣＰＵ、９１２　バス、９１３　ＲＯＭ、９１４　ＲＡＭ、９１５　通信装置、９２０　磁気ディスク装置、９２１　ＯＳ、９２２　ウィンドウシステム、９２３　プログラム群、９２４　ファイル群、９３１　電話器、９３２　ファクシミリ機、９４０　インターネット、９４１　ゲートウェイ、９４２　ＬＡＮ。

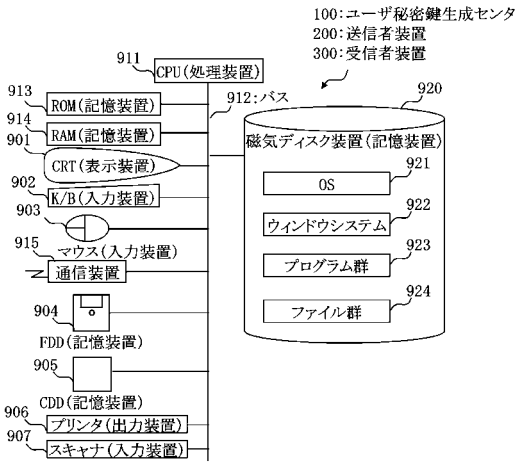
【図１】


800:IDベース公開鍵暗号通信システム(暗号通信システム)
300
受信者装置
ユーザ秘密鍵情報
100
ユーザ秘密鍵生成センタ(鍵生成装置)
ID(識別情報)
パラメータ情報
暗号化セッション鍵情報
暗号文情報
公開された情報
200
送信者装置

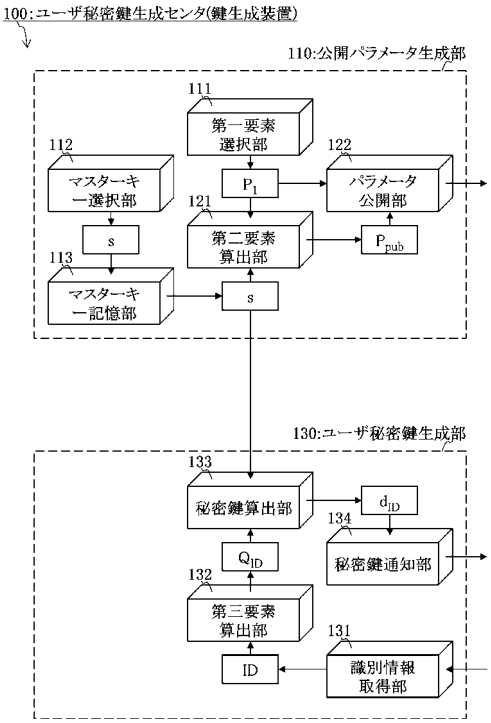
【図２】


940:インターネット
941
ゲートウェイ
932
942:LAN
931
907
906
905
904
903
910:システムユニット
901
902
100:ユーザ秘密鍵生成センタ
200:送信者装置
300:受信者装置

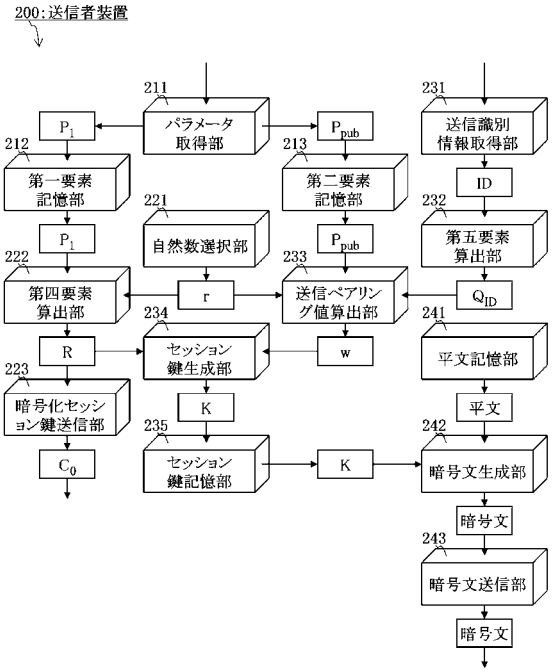
【図３】


100:ユーザ秘密鍵生成センタ
200:送信者装置
300:受信者装置
911
CPU(処理装置)
912:バス
913
ROM(記憶装置)
914
RAM(記憶装置)
901
CRT(表示装置)
902
K/B(入力装置)
903
915
マウス(入力装置)
通信装置
904
FDD(記憶装置)
905
CDD(記憶装置)
906
プリンタ(出力装置)
907
スキャナ(入力装置)
920
磁気ディスク装置(記憶装置)
921
OS
922
ウィンドウシステム
923
プログラム群
924
ファイル群

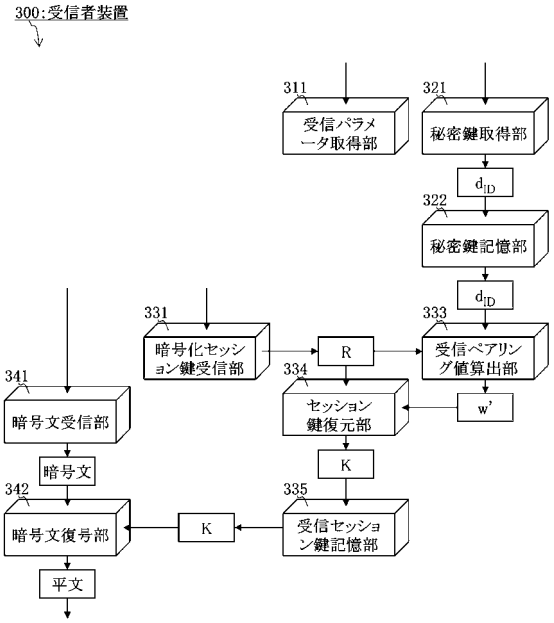
【図４】


100:ユーザ秘密鍵生成センタ(鍵生成装置)
110:公開パラメータ生成部
111
第一要素選択部
112
マスターキー選択部
122
パラメータ公開部
121
第二要素算出部
113
マスターキー記憶部
130:ユーザ秘密鍵生成部
133
秘密鍵算出部
134
秘密鍵通知部
132
第三要素算出部
131
識別情報取得部
ID

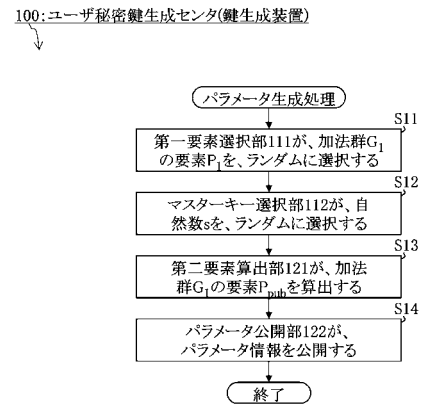
【図５】


200:送信者装置
211
パラメータ取得部
P1
Ppub
231
送信識別情報取得部
212
第一要素記憶部
213
第二要素記憶部
ID
221
自然数選択部
232
第五要素算出部
P1
Ppub
222
第四要素算出部
r
233
送信ペアリング値算出部
QID
234
セッション鍵生成部
241
平文記憶部
R
w
223
暗号化セッション鍵送信部
K
平文
235
セッション鍵記憶部
K
242
暗号文生成部
C0
暗号文
243
暗号文送信部
暗号文

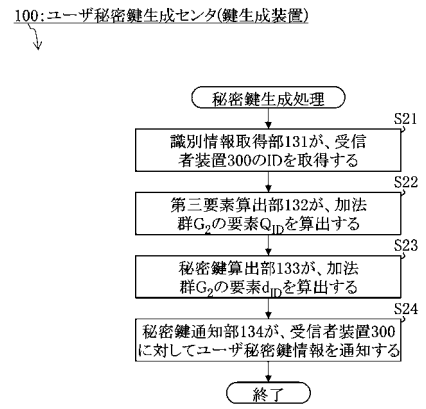
【図６】


300:受信者装置
311
受信パラメータ取得部
321
秘密鍵取得部
dID
322
秘密鍵記憶部
dID
331
暗号化セッション鍵受信部
R
333
受信ペアリング値算出部
341
334
セッション鍵復元部
w'
暗号文受信部
K
暗号文
342
335
暗号文復号部
K
受信セッション鍵記憶部
平文

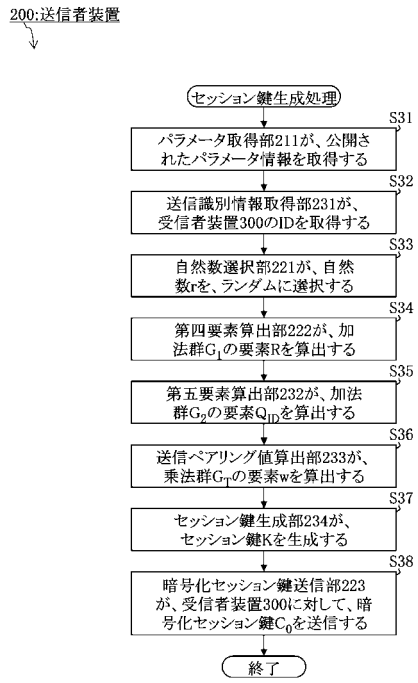
【図７】


100:ユーザ秘密鍵生成センタ(鍵生成装置)
パラメータ生成処理
S11
第一要素選択部111が、加法群G1の要素P1を、ランダムに選択する
S12
マスターキー選択部112が、自然数sを、ランダムに選択する
S13
第二要素算出部121が、加法群G1の要素Ppubを算出する
S14
パラメータ公開部122が、パラメータ情報を公開する
終了

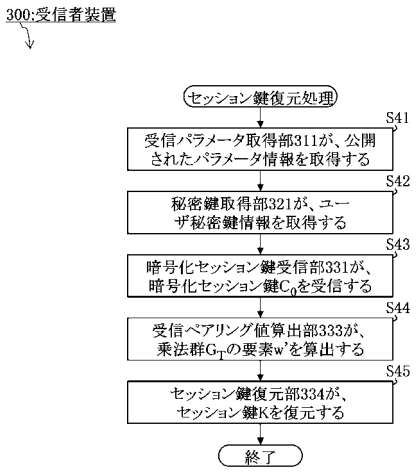
【図８】


100:ユーザ秘密鍵生成センタ(鍵生成装置)
秘密鍵生成処理
S21
識別情報取得部131が、受信者装置300のIDを取得する
S22
第三要素算出部132が、加法群G2の要素QIDを算出する
S23
秘密鍵算出部133が、加法群G2の要素dIDを算出する
S24
秘密鍵通知部134が、受信者装置300に対してユーザ秘密鍵情報を通知する
終了

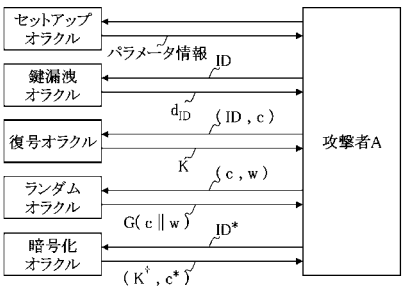
【図９】



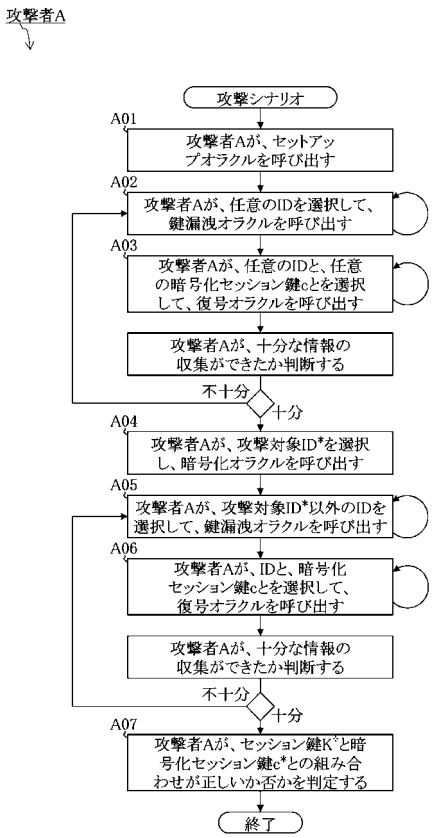
【図１０】



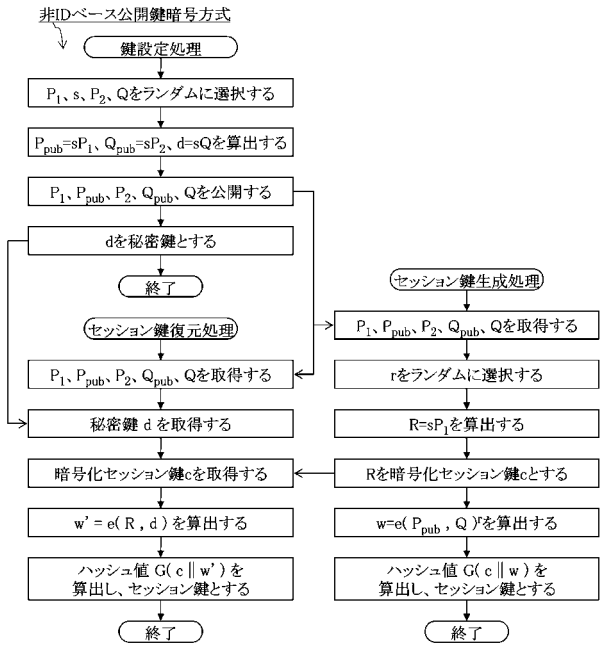
【図１１】



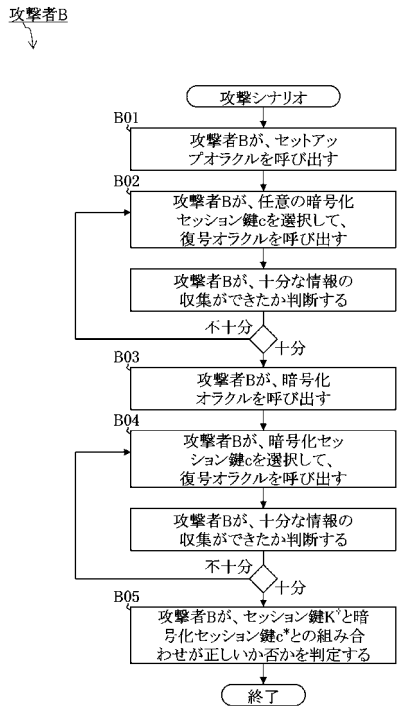
【図１２】



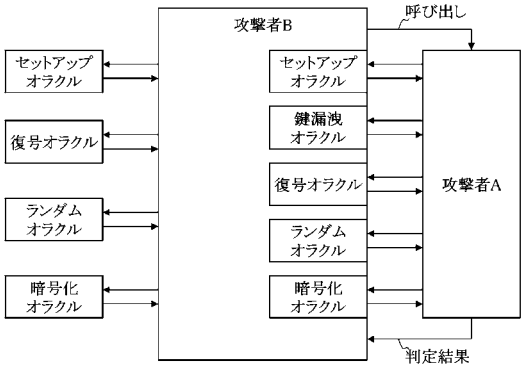
【図１３】



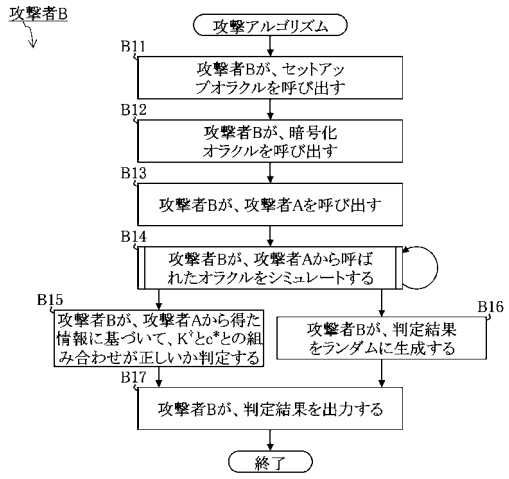
【図１４】



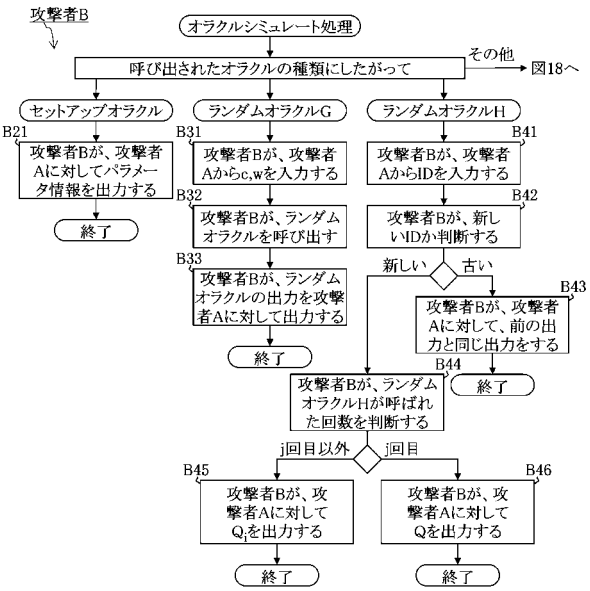
【図１５】



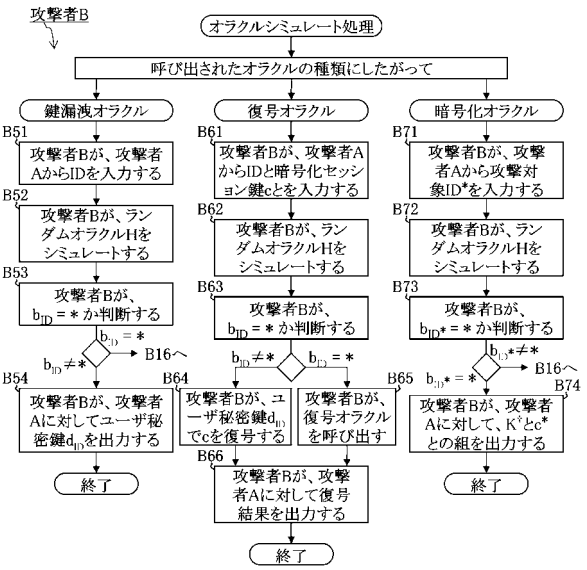
【図１６】



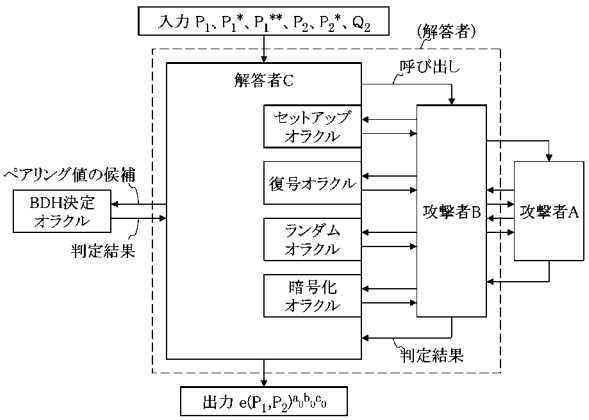
【図１７】



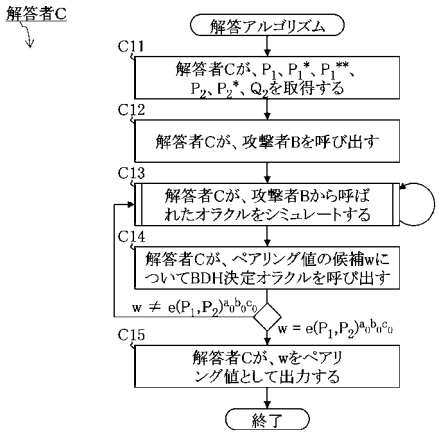
【図１８】



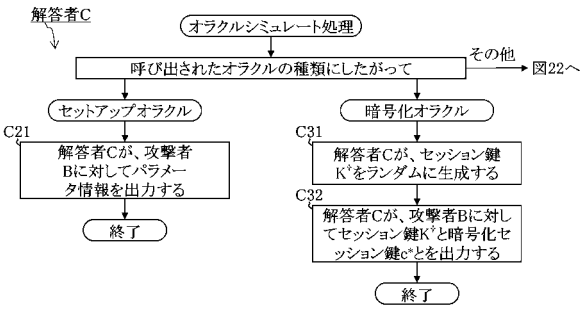
【図１９】



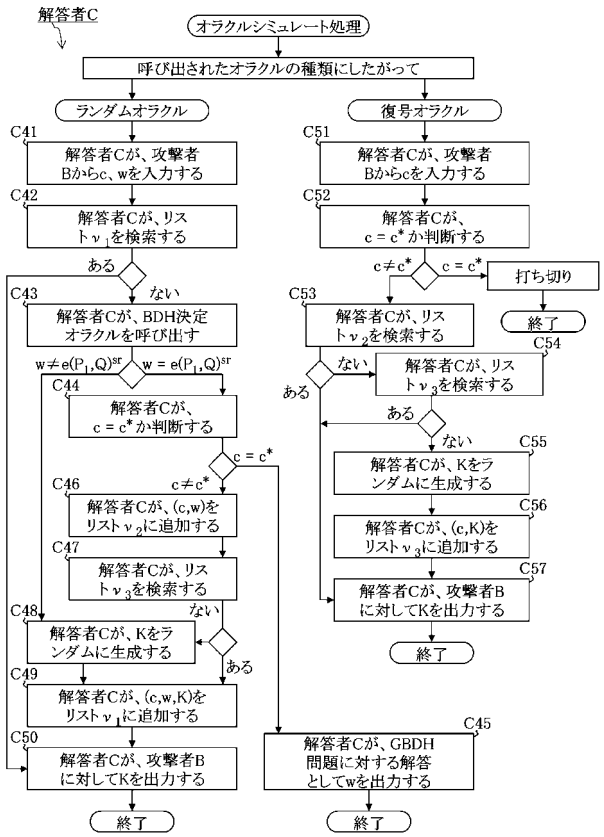
【図２０】



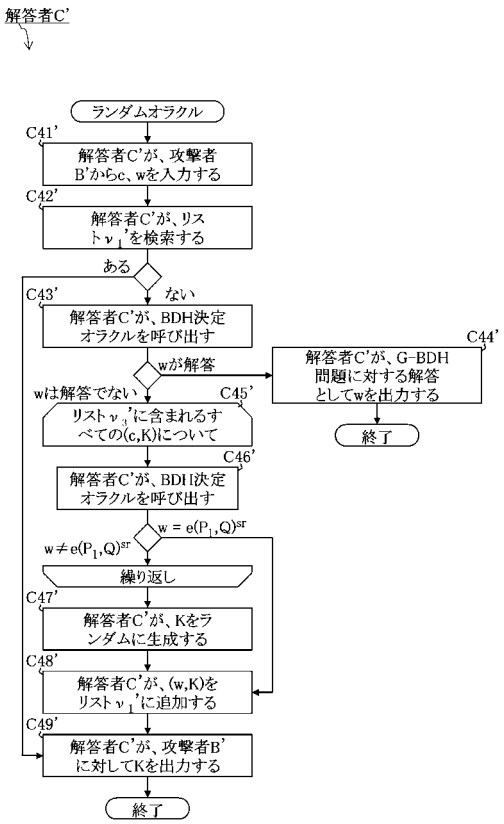
【図２１】



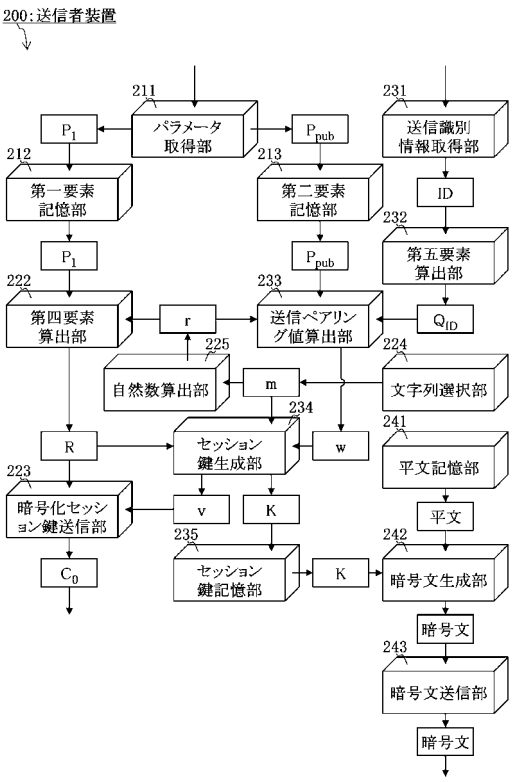
【図２２】



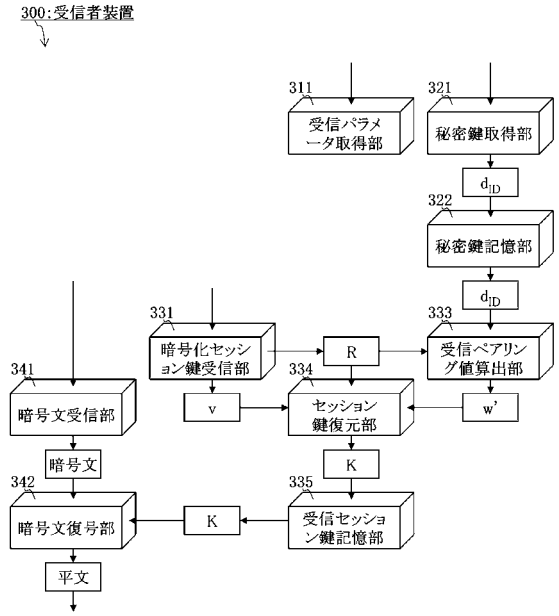
【図２３】



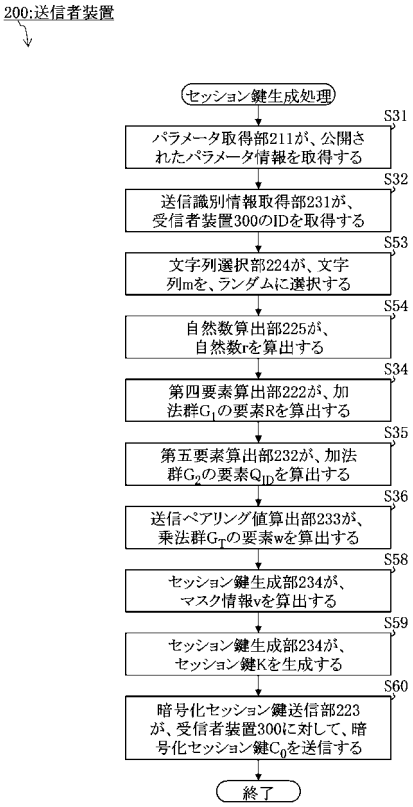
【図２４】



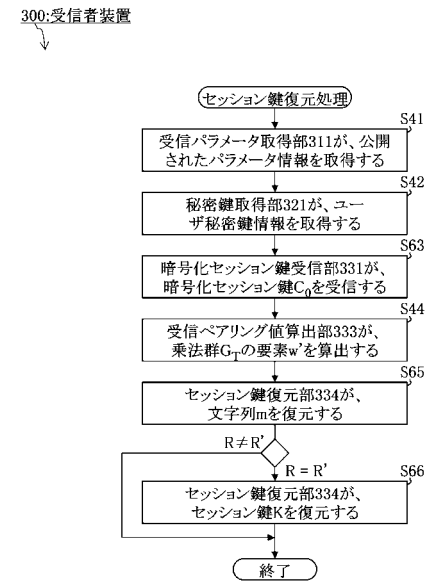
【図２５】



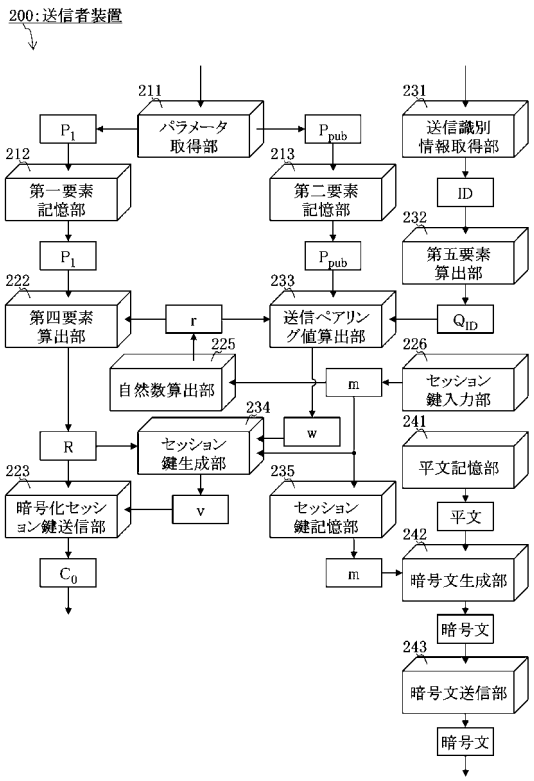
【図２６】



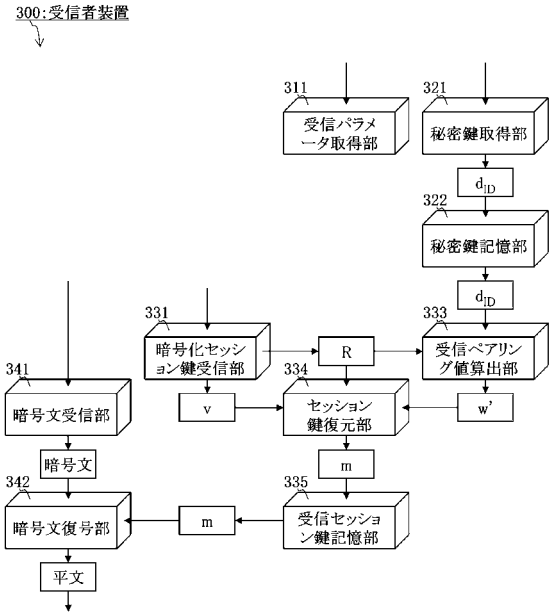
【図２７】



【図２８】



【図２９】


300:受信者装置
311
受信パラメータ取得部
321
秘密鍵取得部
d_{ID}
322
秘密鍵記憶部
d_{ID}
331
暗号化セッション鍵受信部
R
333
受信ペアリング値算出部
341
暗号文受信部
v
334
セッション鍵復元部
w'
暗号文
m
342
暗号文復号部
m
335
受信セッション鍵記憶部
平文

フロントページの続き

(56)参考文献 特表２００５－５００７４０（ＪＰ，Ａ）
国際公開第２００５／０５０９０８（WO，Ａ２）
K. Bentahar and P. Farshim and J. Malone-Lee and N.P. Smart, Generic Constructions of Identity-Based and Certificateless KEMs, [online], ２００５年 2月２５日, Cryptology ePrint Archive:Report 2005/05, [2011年11月4日検索], ＵＲＬ, http://eprint.iacr.org/2005/058

(58)調査した分野(Int.Cl., ＤＢ名)
Ｈ０４Ｌ ９／０８
ＪＳＴＰｌｕｓ／ＪＭＥＤＰｌｕｓ／ＪＳＴ７５８０（ＪＤｒｅａｍＩＩ）