

(19) 日本国特許庁 (JP)

(12) 特 許 公 報 (B2)

(11) 特許番号

特許第5501482号

(P5501482)

(45) 発行日 平成26年5月21日 (2014. 5. 21)

(24) 登録日 平成26年3月20日 (2014. 3. 20)

(51) Int. Cl.

F I

G09C 1/00 (2006.01)

G09C 1/00 620A

H04L 9/08 (2006.01)

H04L 9/00 601D

請求項の数 14 (全 57 頁)

(21) 出願番号 特願2012-553498 (P2012-553498)
 (86) (22) 出願日 平成23年1月18日 (2011. 1. 18)
 (86) 国際出願番号 PCT/JP2011/050778
 (87) 国際公開番号 W02012/098649
 (87) 国際公開日 平成24年7月26日 (2012. 7. 26)
 審査請求日 平成25年3月13日 (2013. 3. 13)

(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
 (74) 代理人 100122035
 弁理士 渡辺 敏雄
 (72) 発明者 服部 充洋
 日本国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
 (72) 発明者 平野 貴人
 日本国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

最終頁に続く

(54) 【発明の名称】 暗号システム、暗号システムの暗号処理方法、暗号化装置、暗号化プログラム、復号装置および復号プログラム

(57) 【特許請求の範囲】

【請求項1】

階層構造を有する組織内で第k階層（kは2以上の特定の整数）に属する特定ユーザのユーザ識別子を第k階層を識別する階層識別子として含むと共に第1階層から第k-1階層までの階層を識別するk-1個の階層識別子を含むユーザ識別子IDを用いる暗号システムにおいて、

暗号化する平文データMを入力し、入力した平文データMを暗号化して平文暗号値C₀を算出し、階層識別子と任意のユーザを意味するワイルドカード値と不要な階層を意味する空欄値とのいずれかを階層毎にパターン値として含んだパターンPを入力し、入力したパターンPに基づいて前記パターン値がワイルドカード値である階層をワイルドカード階層として判定し、k個の階層に対応付けられたk個の鍵値Hを含むH鍵値群を含んだ公開鍵PKを入力し、入力した公開鍵PKに含まれるH鍵値群から前記ワイルドカード階層に対応付けられた鍵値Hをワイルドカード鍵値として抽出し、抽出したワイルドカード鍵値を用いて前記平文暗号値C₀の復号に用いるワイルドカード暗号値C₁を算出し、入力したパターンPに基づいて前記パターン値が階層識別子である階層を識別階層として判定し、入力した公開鍵PKに含まれるH鍵値群から前記識別階層に対応付けられた鍵値Hを識別鍵値として抽出し、抽出した識別鍵値を用いて前記平文暗号値C₀の復号に用いる識別暗号値C₃を算出し、算出した平文暗号値C₀とワイルドカード暗号値C₁と識別暗号値C₃とを含むと共に前記ワイルドカード階層を示すワイルドカード階層値Wを含む暗号文データCTを生成し、生成した暗号文データCTを出力する暗号化装置と、

10

20

前記暗号文データCTと前記ユーザ識別子IDとを入力し、入力した暗号文データCTに含まれるワイルドカード階層値Wに基づいて入力したユーザ識別子IDから前記ワイルドカード階層の階層識別子をワイルドカード識別子として抽出し、抽出したワイルドカード識別子と入力した暗号文データCTに含まれるワイルドカード暗号値 C_1 と識別暗号値 C_3 とを用いて入力した暗号文データCTに含まれる平文暗号値 C_0 を復号し、前記平文暗号値 C_0 を復号して得られる前記平文データMを出力する復号装置とを備えたことを特徴とする暗号システム。

【請求項2】

前記公開鍵PKは、k個の階層に対応付けられたk個の鍵値 H' を含む H' 鍵値群を含み、

10

前記暗号化装置は、入力した公開鍵PKに含まれる H' 鍵値群から前記ワイルドカード階層に対応付けられた鍵値 H' を第2のワイルドカード鍵値として抽出し、抽出した第2のワイルドカード鍵値を用いて前記平文暗号値 C_0 の復号に用いるワイルドカード暗号値 C_1' を算出し、入力した公開鍵PKに含まれる H' 鍵値群から前記識別階層に対応付けられた鍵値 H' を第2の識別鍵値として抽出し、抽出した第2の識別鍵値を用いて前記平文暗号値 C_0 の復号に用いる識別暗号値 C_3' を算出し、算出したワイルドカード暗号値 C_1' と識別暗号値 C_3' とを含めて前記暗号文データCTを出力し、

前記復号装置は、抽出したワイルドカード識別子と入力した暗号文データCTに含まれるワイルドカード暗号値 C_1 と識別暗号値 C_3 とワイルドカード暗号値 C_1' と識別暗号値 C_3' とを用いて入力した暗号文データCTに含まれる平文暗号値 C_0 を復号することを特徴とする請求項1記載の暗号システム。

20

【請求項3】

前記暗号化装置は、さらに、特定の平文データMWを暗号化して平文暗号値 CW_0 を算出し、前記暗号文データCTの検索に用いるキーワードKWを入力し、前記パターンPを含むと共に前記キーワードKWを第 $K+1$ 階層を識別する階層識別子として含むパターンPWを用いてワイルドカード暗号値 CW_1 と識別暗号値 CW_3 とを算出し、算出した平文暗号値 CW_0 とワイルドカード暗号値 CW_1 と識別暗号値 CW_3 とを含んだ暗号文データCTWを前記暗号文データCTに対応付けて出力し、

前記暗号システムは、さらに、

前記ユーザ識別子IDと前記キーワードKWとを入力し、入力したユーザ識別子IDとキーワードKWとを用いて前記平文暗号値 CW_0 の復号に用いる鍵値 y_0 を算出し、算出した鍵値 y_0 と前記ユーザ識別子IDとを含んだ検索クエリQKを生成し、生成した検索クエリQKを出力する検索クエリ生成装置と、

30

複数の暗号文データCTと複数の暗号文データCTWとを対応付けて記憶する暗号文記憶部を有する検索装置とを備え、

前記検索装置は、前記検索クエリQKと前記ワイルドカード階層値Wとを入力し、前記暗号文記憶部から暗号文データCTWを選択し、入力したワイルドカード階層値Wに基づいて入力した検索クエリQKに含まれるユーザ識別子IDから前記ワイルドカード階層の階層識別子をワイルドカード識別子として抽出し、抽出したワイルドカード識別子と選択した暗号文データCTWに含まれるワイルドカード暗号値 CW_1 と識別暗号値 CW_3 と入力した検索クエリQKに含まれる鍵値 y_0 とを用いて選択した暗号文データCTWに含まれる平文暗号値 CW_0 を復号し、前記平文暗号値 CW_0 を復号して得られた復号データが前記平文データMWと一致するか否かを判定し、前記復号データが前記平文データMWと一致した場合、選択した暗号文データCTWに対応する暗号文データCTを前記暗号文記憶部から取得し、取得した暗号文データCTを入力した検索クエリQKに対する検索結果として出力する

40

ことを特徴とする請求項1記載の暗号システム。

【請求項4】

前記暗号化装置は、前記暗号文データCTのハッシュ値を前記平文データMWとして算出し、算出した平文データMWを暗号化して前記平文暗号値 CW_0 を算出し、

50

前記検索装置は、選択した暗号文データCTWに対応する暗号文データCTのハッシュ値を前記平文データMWとして算出し、前記復号データが算出した平文データMWと一致するか否かを判定する

ことを特徴とする請求項3記載の暗号システム。

【請求項5】

前記暗号化装置は、前記平文データMWとして所定の検索定数を予め記憶し、予め記憶した検索定数を暗号化して前記平文暗号値CW₀を算出し、

前記検索装置は、前記平文データMWとして前記検索定数を予め記憶し、前記復号データが前記検索定数と一致するか否かを判定する

ことを特徴とする請求項3記載の暗号システム。

10

【請求項6】

前記検索装置は、検索する権限が無いユーザのユーザ識別子IDを非検索識別子として記憶する非検索識別子記憶部を備え、

前記検索装置は、入力した検索クエリQKに含まれるユーザ識別子IDと前記非検索識別子記憶部に記憶された非検索識別子とが一致するか否かを判定し、前記ユーザ識別子IDと前記非検索識別子とが一致する場合に前記検索結果を出力しない

ことを特徴とする請求項3記載の暗号システム。

【請求項7】

前記検索装置は、検索する権限が無いユーザが属する階層より上位の階層の階層識別子を非検索識別子として記憶する非検索識別子記憶部を備え、

20

前記検索装置は、入力した検索クエリQKに含まれるユーザ識別子IDに前記非検索識別子記憶部に記憶された非検索識別子が含まれるか否かを判定し、前記ユーザ識別子IDに前記非検索識別子が含まれる場合に前記検索結果を出力しない

ことを特徴とする請求項3記載の暗号システム。

【請求項8】

前記ユーザ識別子IDは、前記特定のユーザの第1のユーザ識別子を第k階層を識別する階層識別子として含むと共に前記特定のユーザの第2のユーザ識別子を第k+1階層を識別する階層識別子として含み、

前記公開鍵PKに含まれるH鍵値群は、k+1個の階層に対応付けられたk+1個の鍵値Hを含み、

30

前記パターンPは、第k階層と第k+1階層との少なくともいずれかの階層のパターン値としてワイルドカード値を含む

ことを特徴とする請求項3記載の暗号システム。

【請求項9】

階層構造を有する組織内で第k階層（kは2以上の特定の整数）に属する特定ユーザのユーザ識別子を第k階層を識別する階層識別子として含むと共に第1階層から第k-1階層までの階層を識別するk-1個の階層識別子を含むユーザ識別子IDを用いる暗号システムの暗号処理方法において、

暗号化装置が、暗号化する平文データMを入力し、入力した平文データMを暗号化して平文暗号値C₀を算出し、階層識別子と任意のユーザを意味するワイルドカード値と不要な階層を意味する空欄値とのいずれかを階層毎にパターン値として含んだパターンPを入力し、入力したパターンPに基づいて前記パターン値がワイルドカード値である階層をワイルドカード階層として判定し、k個の階層に対応付けられたk個の鍵値Hを含むH鍵値群を含んだ公開鍵PKを入力し、入力した公開鍵PKに含まれるH鍵値群から前記ワイルドカード階層に対応付けられた鍵値Hをワイルドカード鍵値として抽出し、抽出したワイルドカード鍵値を用いて前記平文暗号値C₀の復号に用いるワイルドカード暗号値C₁を算出し、入力したパターンPに基づいて前記パターン値が階層識別子である階層を識別階層として判定し、入力した公開鍵PKに含まれるH鍵値群から前記識別階層に対応付けられた鍵値Hを識別鍵値として抽出し、抽出した識別鍵値を用いて前記平文暗号値C₀の復号に用いる識別暗号値C₃を算出し、算出した平文暗号値C₀とワイルドカード暗号値C

40

50

C_1 と識別暗号値 C_3 とを含むと共に前記ワイルドカード階層を示すワイルドカード階層値 W を含む暗号文データ CT を出力し、

復号化装置が、前記暗号文データ CT と前記ユーザ識別子 ID とを入力し、入力した暗号文データ CT に含まれるワイルドカード階層値 W に基づいて入力したユーザ識別子 ID から前記ワイルドカード階層の階層識別子をワイルドカード識別子として抽出し、抽出したワイルドカード識別子と入力した暗号文データ CT に含まれるワイルドカード暗号値 C_1 と識別暗号値 C_3 とを用いて入力した暗号文データ CT に含まれる平文暗号値 C_0 を復号し、前記平文暗号値 C_0 を復号して得られる前記平文データ M を出力することを特徴とする暗号システムの暗号処理方法。

【請求項10】

前記暗号化装置は、さらに、特定の平文データ MW を暗号化して平文暗号値 CW_0 を算出し、前記暗号文データ CT の検索に用いるキーワード KW を入力し、前記パターン P を含むと共に前記キーワード KW を第 $K+1$ 階層を識別する階層識別子として含むパターン PW を用いてワイルドカード暗号値 CW_1 と識別暗号値 CW_3 とを算出し、算出した平文暗号値 CW_0 とワイルドカード暗号値 CW_1 と識別暗号値 CW_3 とを含んだ暗号文データ CTW を前記暗号文データ CT に対応付けて出力し、

検索クエリ生成装置が、前記ユーザ識別子 ID と前記キーワード KW とを入力し、入力したユーザ識別子 ID とキーワード KW とを用いて前記平文暗号値 CW_0 の復号に用いる鍵値 y_0 を算出し、算出した鍵値 y_0 と前記ユーザ識別子 ID とを含んだ検索クエリ QK を出力し、

検索装置が、複数の暗号文データ CT と複数の暗号文データ CTW とを対応付けて記憶する暗号文記憶部を有し、

前記検索装置は、前記検索クエリ QK と前記ワイルドカード階層値 W とを入力し、前記暗号文記憶部から暗号文データ CTW を選択し、入力したワイルドカード階層値 W に基づいて入力した検索クエリ QK に含まれるユーザ識別子 ID から前記ワイルドカード階層の階層識別子をワイルドカード識別子として抽出し、抽出したワイルドカード識別子と選択した暗号文データ CTW に含まれるワイルドカード暗号値 CW_1 と識別暗号値 CW_3 と入力した検索クエリ QK に含まれる鍵値 y_0 とを用いて選択した暗号文データ CTW に含まれる平文暗号値 CW_0 を復号し、前記平文暗号値 CW_0 を復号して得られた復号データが前記平文データ MW と一致するか否かを判定し、前記復号データが前記平文データ MW と一致した場合、選択した暗号文データ CTW に対応する暗号文データ CT を前記暗号文記憶部から取得し、取得した暗号文データ CT を入力した検索クエリ QK に対する検索結果として出力する

ことを特徴とする請求項9記載の暗号システムの暗号処理方法。

【請求項11】

暗号化する平文データ M を入力し、 k 個（ k は2以上の特定の整数）の階層に対応付けられた k 個の鍵値 H を含む H 鍵値群を含んだ公開鍵 PK を入力し、階層を識別する階層識別子と任意のユーザを意味するワイルドカード値と不要な階層を意味する空欄値とのいずれかを階層毎にパターン値として含んだパターン P を入力する暗号化入力部と、

前記暗号化入力部が入力した平文データ M を暗号化して平文暗号値 C_0 を算出し、前記暗号化入力部が入力したパターン P に基づいて前記パターン値がワイルドカード値である階層をワイルドカード階層として判定し、前記暗号化入力部が入力した公開鍵 PK に含まれる H 鍵値群から前記ワイルドカード階層に対応付けられた鍵値 H をワイルドカード鍵値として抽出し、抽出したワイルドカード鍵値を用いて前記平文暗号値 C_0 の復号に用いるワイルドカード暗号値 C_1 を算出し、前記パターン P に基づいて前記パターン値が階層識別子である階層を識別階層として判定し、前記公開鍵 PK に含まれる H 鍵値群から前記識別階層に対応付けられた鍵値 H を識別鍵値として抽出し、抽出した識別鍵値を用いて前記平文暗号値 C_0 の復号に用いる識別暗号値 C_3 を算出する暗号値算出部と、

前記暗号値算出部により算出された平文暗号値 C_0 とワイルドカード暗号値 C_1 と識別暗号値 C_3 とを含むと共に前記ワイルドカード階層を示すワイルドカード階層値 W を含む

暗号文データC Tを生成し、生成した暗号文データC Tを出力する暗号文出力部とを備えたことを特徴とする暗号化装置。

【請求項12】

暗号化する平文データMを入力し、 k 個（ k は2以上の特定の整数）の階層に対応付けられた k 個の鍵値Hを含むH鍵値群を含んだ公開鍵PKを入力し、階層を識別する階層識別子と任意のユーザを意味するワイルドカード値と不要な階層を意味する空欄値とのいずれかを階層毎にパターン値として含んだパターンPを入力する暗号化入力処理と、

前記暗号化入力処理により入力された平文データMを暗号化して平文暗号値 C_0 を算出し、前記暗号化入力処理により入力されたパターンPに基づいて前記パターン値がワイルドカード値である階層をワイルドカード階層として判定し、前記暗号化入力処理により入力された公開鍵PKに含まれるH鍵値群から前記ワイルドカード階層に対応付けられた鍵値Hをワイルドカード鍵値として抽出し、抽出したワイルドカード鍵値を用いて前記平文暗号値 C_0 の復号に用いるワイルドカード暗号値 C_1 を算出し、前記パターンPに基づいて前記パターン値が階層識別子である階層を識別階層として判定し、前記公開鍵PKに含まれるH鍵値群から前記識別階層に対応付けられた鍵値Hを識別鍵値として抽出し、抽出した識別鍵値を用いて前記平文暗号値 C_0 の復号に用いる識別暗号値 C_3 を算出する暗号値算出処理と、

前記暗号値算出処理により算出された平文暗号値 C_0 とワイルドカード暗号値 C_1 と識別暗号値 C_3 とを含むと共に前記ワイルドカード階層を示すワイルドカード階層値Wを含む暗号文データC Tを生成し、生成した暗号文データC Tを出力する暗号文出力処理とをコンピュータに実行させることを特徴とする暗号化プログラム。

【請求項13】

階層構造を有する組織内で第 k 階層（ k は2以上の特定の整数）に属する特定ユーザのユーザ識別子を第 k 階層を識別する階層識別子として含むと共に第1階層から第 $k-1$ 階層までの階層を識別する $k-1$ 個の階層識別子を含むユーザ識別子IDを用いる復号装置において、

階層識別子と任意のユーザを意味するワイルドカード値と不要な階層を意味する空欄値とのいずれかを階層毎にパターン値として含んだパターンPを用いて生成された暗号文データC Tであって平文データMを暗号化した平文暗号値 C_0 と特定のワイルドカード暗号値 C_1 と特定の識別暗号値 C_3 とを含むと共に前記パターンPに含まれるパターン値がワイルドカード値である階層を示すワイルドカード階層値Wを含む暗号文データC Tを入力し、前記ユーザ識別子IDを入力する復号入力部と、

前記復号入力部が入力した暗号文データC Tに基づいて、前記復号入力部が入力したユーザ識別子IDから前記ワイルドカード階層値Wによって示される階層の階層識別子をワイルドカード識別子として抽出し、抽出したワイルドカード識別子と前記暗号文データC Tに含まれるワイルドカード暗号値 C_1 と識別暗号値 C_3 とを用いて前記暗号文データC Tに含まれる平文暗号値 C_0 を復号し、前記平文暗号値 C_0 を復号して得られる前記平文データMを出力する復号部と

を備えたことを特徴とする復号装置。

【請求項14】

階層構造を有する組織内で第 k 階層（ k は2以上の特定の整数）に属する特定ユーザのユーザ識別子を第 k 階層を識別する階層識別子として含むと共に第1階層から第 $k-1$ 階層までの階層を識別する $k-1$ 個の階層識別子を含むユーザ識別子IDを用いる復号プログラムにおいて、

階層識別子と任意のユーザを意味するワイルドカード値と不要な階層を意味する空欄値とのいずれかを階層毎にパターン値として含んだパターンPを用いて生成された暗号文データC Tであって平文データMを暗号化した平文暗号値 C_0 と特定のワイルドカード暗号値 C_1 と特定の識別暗号値 C_3 とを含むと共に前記パターンPに含まれるパターン値がワイルドカード値である階層を示すワイルドカード階層値Wを含む暗号文データC Tを入力し、前記ユーザ識別子IDを入力する復号入力処理と、

前記復号入力処理により入力された暗号文データC Tに基づいて、前記復号入力処理により入力されたユーザ識別子I Dから前記ワイルドカード階層値Wによって示される階層の階層識別子をワイルドカード識別子として抽出し、抽出したワイルドカード識別子と前記暗号文データC Tに含まれるワイルドカード暗号値C₁と識別暗号値C₃とを用いて前記暗号文データC Tに含まれる平文暗号値C₀を復号し、前記平文暗号値C₀を復号して得られる前記平文データMを出力する復号処理と
をコンピュータに実行させることを特徴とする復号プログラム。

【発明の詳細な説明】

【技術分野】

【0001】

10

本発明は、例えば、暗号システム、暗号システムの暗号処理方法、暗号化装置、暗号化プログラム、復号装置、復号プログラム、セットアップ装置、セットアッププログラム、鍵生成装置、鍵生成プログラム、鍵委譲装置および鍵委譲プログラムに関するものである。

【背景技術】

【0002】

公開鍵暗号の技術分野の一つとして階層型I Dベース暗号について多く実現方式が知られており、それぞれ実現方式は様々な特徴を有している。

その中で、暗号文に匿名性を持たせることのできる匿名性階層型I Dベース暗号方式がいくつか知られている（例えば特許文献1、非特許文献1）。

20

匿名性とは、暗号文を見ても、どのI D宛ての暗号文であるかがわからないという性質である。

【0003】

階層型I Dベース暗号の使われ方によっては、匿名性が必要不可欠な性質となる場合がある。

例えば、インターネットの掲示板やファイルサーバを利用して、階層型I Dベース暗号の暗号文をある特定のユーザに送る場合を考える。

ここで、宛先を知られることがまずい場合（例えば合併前の会社同士のやりとりであって、やりとりをしていること自体を知られることがまずい場合）には、匿名性のない方式を使用することはできない。

30

なぜならば、暗号文が解析されることで宛先が漏洩してしまうからである。

したがって、このような場合には匿名性が必要不可欠となる。

【0004】

また、階層型I Dベース暗号は秘匿検索へも応用できることが知られている。秘匿検索とは、暗号化したままキーワード検索する技術であり、検索可能暗号とも言う。

この場合にも匿名性が必要不可欠である。なぜならば、I Dベース暗号におけるI Dが秘匿検索におけるキーワードに対応しており、匿名性がない（すなわちI Dが漏洩することとキーワードが漏洩することとが対応するからである）。

【0005】

上述のとおり、暗号文に匿名性を持たせることのできる匿名性階層型I Dベース暗号方式がいくつか知られている（例えば特許文献1、非特許文献1）。

40

しかし、これらの方式では、同一内容の暗号文を複数の宛先I Dに対して作成する場合、I D数分の暗号文を作成しなければならず、暗号文の個数が増大してしまう。

そこで、発展方式として、1個の暗号文で同一階層に属するユーザ全員宛てに送ることのできる「ワイルドカード対応の匿名性階層型I Dベース暗号方式」が知られている（非特許文献2）。

【0006】

また、「ワイルドカード対応の階層型I Dベース暗号方式」を公開鍵型の秘匿検索の分野に応用することで、「グループ共有型公開鍵秘匿検索方式」を実現できることが知られている（非特許文献2）。

50

「グループ共有型公開鍵秘匿検索方式」では、1個の暗号文をグループ内で共有することができ、グループ内の各ユーザが自分の秘密鍵を使って暗号文に対する検索用クエリを作成することができる。

【先行技術文献】

【特許文献】

【0007】

【特許文献1】特開2010-161523号公報

【非特許文献】

【0008】

【非特許文献1】Xavier Boyen and Brent Waters, “Anonymous hierarchical identity-based encryption (without random oracles),” *Crypto 2006, Lecture Notes in Computer Science*, vol. 4117, pp. 290–307, 2006. 10

【非特許文献2】Mitsuhiro Hattori, Takumi Mori, Takashi Ito, Nori Matsuda, Takeshi Yoneda, and Kazuo Ohta, “Anonymous HIBE with wildcards and its application to secure keyword search for group-oriented multi-user system,” *SCIS 2010*, 2010. 20

【非特許文献3】Dan Boneh, Eu-Jin Goh, and Kobbi Nissim, “Evaluating 2-DNF formulas on ciphertexts,” *Theory of Cryptography Conference, Lecture Notes in Computer Science*, vol. 3378, pp. 325–341, 2005.

【非特許文献4】Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone, “Handbook of applied cryptography,” 4.4 Prime number generation, *CRC Press*, pp. 145–154, 1996. 30

【非特許文献5】Jae Hong Seo, Tetsutaro Kobayashi, Miyako Ohkubo, and Koutarou Suzuki, “Anonymous hierarchical identity-based encryption with constant size ciphertexts,” *Public Key Cryptography, Lecture Notes in Computer Science*, vol. 5443, pp. 215–234, 2009.

【非特許文献6】David Mandell Freeman, “Converting pairing-based cryptosystems from composite-order groups to prime-order groups,” *Eurocrypt 2010, Lecture Notes in Computer Science*, vol. 6110, pp. 44–61, 2010. 40

【非特許文献7】Elaine Shi and Brent Waters, “Delegating capabilities in predicate encryption systems,” *ICALP 2008, Lecture Notes in Computer Science*, vol. 5126, pp. 560–578, 2008.

【非特許文献8】Tatsuaki Okamoto and Katsuyuki Takashima, “Hierarchical predicate Encryp 50

tion for inner-products, " Asiacypt 2009, Lecture Notes in Computer Science, vol. 5912, pp. 214-231, 2009.

【発明の概要】

【発明が解決しようとする課題】

【0009】

非特許文献2に記載の「ワイルドカード対応の匿名性階層型IDベース暗号方式」は、復号演算で最も時間がかかるペアリング演算の回数が階層の高さに比例してしまうため、大企業や官公庁のように大きな階層を持つ組織では利用しづらい。

ペアリング演算の回数が階層の高さに比例してしまうのは、階層の高さに比例した個数の要素が暗号文の構成要素として含まれており、復号時にその各々をペアリング演算しなければならないためである。

10

【0010】

また、非特許文献2に記載の「ワイルドカード対応の匿名性階層型IDベース暗号方式」では、暗号化やユーザ秘密鍵の作成において対象となるユーザのユーザID（ユーザ識別子）を指定する際に、上位階層から順に漏れ無く要素を指定する必要がある。

そのため、部・課・係などの階層を備える大規模な組織において、部直属のユーザのように、通常の階層構造から外れるユーザに対応することが出来なかった。

つまり、対応可能な階層構造に制約があり、柔軟性が低いという課題があった。

【0011】

20

また、非特許文献2に記載の「グループ共有型公開鍵秘匿検索方式」は、「ワイルドカード対応の匿名性階層型IDベース暗号方式」と同様に、検索演算におけるペアリング演算の回数が階層数の高さに比例してしまうため、大企業や官公庁のように大きな階層を持つ組織では利用しづらい。

【0012】

また、非特許文献2には「ワイルドカード対応の匿名性階層型IDベース暗号方式」を用いて「グループ共有型公開鍵秘匿検索方式」を実現する方法は開示されていたが、「グループ共有型公開鍵秘匿検索方式」を実現するためのより一般的な方法は開示されていない。

そのため、「グループ共有型公開鍵秘匿検索方式」を構成する際の選択肢が少ないという課題があった。

30

【0013】

また、非特許文献2には「グループ共有型公開鍵秘匿検索方式」においてグループ内で暗号文を共有し、グループにメンバを加入させる方法が開示されているが、グループからメンバを脱退させる方法は開示されていない。また、加入・脱退にかかわらずメンバ自体を失効させるための方法も開示されていない。

そのため、異動や出向、あるいは退職があるような組織では利用しづらいという課題があった。

【0014】

本発明は、例えば、以下のようなことを目的とする。

40

【0015】

ワイルドカード対応の匿名性階層型IDベース暗号方式において、復号演算中のペアリング演算の回数が階層数に比例せず一定回数となるような方式を提供することを目的とする。

【0016】

また、グループ共有型公開鍵秘匿検索方式において、検索演算中のペアリング演算の回数が階層数に比例せず一定回数となるような方式を提供することを目的とする。

【0017】

また、グループ共有型公開鍵秘匿検索方式を実現するためのより一般的な方法を提供することを目的とする。

50

【0018】

また、グループ共有型公開鍵秘匿検索方式において、グループからメンバを脱退する方法を提供することを目的とする。

【0019】

また、グループ共有型公開鍵秘匿検索方式においてメンバを失効させる方法を提供することを目的とする。

【課題を解決するための手段】

【0020】

本発明の暗号システムは、階層構造を有する組織内で第 k 階層（ k は2以上の特定の整数）に属する特定ユーザのユーザ識別子を第 k 階層を識別する階層識別子として含むと共に第1階層から第 $k-1$ 階層までの階層を識別する $k-1$ 個の階層識別子を含むユーザ識別子IDを用いる暗号システムである。

10

前記暗号システムは、暗号化装置と復号装置とを備える。

前記暗号化装置は、暗号化する平文データ M を入力し、 k 個の階層に対応付けられた k 個の鍵値 H を含む H 鍵値群を含んだ公開鍵 PK を入力し、入力した平文データ M を暗号化して平文暗号値 C_0 を算出し、階層識別子と任意のユーザを意味するワイルドカード値と不要な階層を意味する空欄値とのいずれかを階層毎にパターン値として含んだパターン P を入力し、入力したパターン P に基づいて前記パターン値がワイルドカード値である階層をワイルドカード階層として判定し、入力した公開鍵 PK に含まれる H 鍵値群から前記ワイルドカード階層に対応付けられた鍵値 H をワイルドカード鍵値として抽出し、抽出したワイルドカード鍵値を用いて前記平文暗号値 C_0 の復号に用いるワイルドカード暗号値 C_1 を算出し、入力したパターン P に基づいて前記パターン値が階層識別子である階層を識別階層として判定し、入力した公開鍵 PK に含まれる H 鍵値群から前記識別階層に対応付けられた鍵値 H を識別鍵値として抽出し、抽出した識別鍵値を用いて前記平文暗号値 C_0 の復号に用いる識別暗号値 C_3 を算出し、算出した平文暗号値 C_0 とワイルドカード暗号値 C_1 と識別暗号値 C_3 とを含むと共に前記ワイルドカード階層を示すワイルドカード階層値 W を含む暗号文データ CT を生成し、生成した暗号文データ CT を出力する。

20

前記復号装置は、前記暗号文データ CT と前記ユーザ識別子IDとを入力し、入力した暗号文データ CT に含まれるワイルドカード階層値 W に基づいて入力したユーザ識別子IDから前記ワイルドカード階層の階層識別子をワイルドカード識別子として抽出し、抽出したワイルドカード識別子と入力した暗号文データ CT に含まれるワイルドカード暗号値 C_1 と識別暗号値 C_3 とを用いて入力した暗号文データ CT に含まれる平文暗号値 C_0 を復号し、前記平文暗号値 C_0 を復号して得られる前記平文データ M を出力する。

30

【発明の効果】

【0021】

本発明によれば、例えば、ワイルドカード対応の匿名性階層型IDベース暗号方式において、復号演算中のペアリング演算の回数が階層数に比例せず一定回数になる。

【図面の簡単な説明】

【0022】

【図1】実施の形態1における階層型IDベース暗号システム100の構成図。

40

【図2】実施の形態1における階層型IDベース暗号システム100の階層構造の一例を示す図。

【図3】実施の形態1における階層型IDベース暗号システム100のユーザ識別子IDの一例を示す図。

【図4】実施の形態1における階層型IDベース暗号システム100のパターン P の一例を示す図。

【図5】実施の形態1におけるセットアップ装置200の概要図。

【図6】実施の形態1におけるセットアップ装置200の機能構成図。

【図7】実施の形態1における復号装置300の概要図。

【図8】実施の形態1における復号装置300の機能構成図。

50

【図 9】実施の形態 1 における暗号化装置 400 の概要図。

【図 10】実施の形態 1 における暗号化装置 400 の機能構成図。

【図 11】実施の形態 1 におけるセットアップ装置 200 によるセットアップ方法を示すフローチャート。

【図 12】実施の形態 1 におけるセットアップ装置 200 による鍵生成方法を示すフローチャート。

【図 13】実施の形態 1 における復号装置 300 による鍵委譲方法を示すフローチャート。

【図 14】実施の形態 1 における暗号化装置 400 による暗号化方法を示すフローチャート。

10

【図 15】実施の形態 1 における復号装置 300 による復号方法を示すフローチャート。

【図 16】実施の形態における階層型 ID ベース暗号システム 100 のハードウェア資源の一例を示す図。

【図 17】実施の形態 3 における公開鍵秘匿検索システム 110 の構成図。

【図 18】実施の形態 3 における復号装置 300 の概要図。

【図 19】実施の形態 3 における検索装置 500 の概要図。

【図 20】実施の形態 3 における検索装置 500 の機能構成図。

【図 21】実施の形態 3 における階層型 ID ベース暗号システム 100 の階層構造の一例を示す図。

【図 22】実施の形態 3 における階層型 ID ベース暗号システム 100 のパターン PW の一例を示す図。

20

【図 23】実施の形態 3 における暗号化装置 400 による暗号化方法を示すフローチャート。

【図 24】実施の形態 3 における復号装置 300 によるクエリ生成方法を示すフローチャート。

【図 25】実施の形態 3 における検索装置 500 による検索方法を示すフローチャート。

【図 26】実施の形態 4 におけるユーザ識別子 ID の一例を示す図。

【図 27】実施の形態 4 における削除者リストの一例を示す図。

【図 28】実施の形態 4 における検索装置 500 の検索方法を示すフローチャート。

【図 29】実施の形態 5 におけるユーザ識別子 ID の一例を示す図。

30

【図 30】実施の形態 5 におけるパターン P の一例を示す図。

【発明を実施するための形態】

【0023】

実施の形態 1.

「ワイルドカード対応の匿名性階層型 ID ベース暗号方式」の実現方法について説明する。

【0024】

図 1 は、実施の形態 1 における階層型 ID ベース暗号システム 100 の構成図である。

実施の形態 1 における階層型 ID ベース暗号システム 100 の構成について、図 1 に基づいて説明する。

40

【0025】

階層型 ID ベース暗号システム 100（暗号システムの一部）は、セットアップ装置 200（鍵生成装置の一部）と復号装置 300（鍵委譲装置の一部）と暗号化装置 400 とを備える。

セットアップ装置 200 と復号装置 300 と暗号化装置 400 とは、それぞれにネットワークに接続し、互いに通信を行う。

【0026】

階層型 ID ベース暗号システム 100 には複数の復号装置 300 が存在し、セットアップ装置 200 と複数の復号装置 300 とはツリー状の階層構造を構成している。

図 1 では、セットアップ装置 200 が階層構造の根（第 0 階層）を構成し、4 台の復号

50

装置 300A-D が 2 つの階層（第 1、2 階層）を構成している。

復号装置 300A・B は第 1 階層を構成し、復号装置 300C・D は復号装置 300A を上位の復号装置 300（親装置）として第 2 階層を構成している。

但し、復号装置 300 の台数は 2 または 3 台であっても構わないし、5 台以上であっても構わない。

また、複数の復号装置 300 は 3 階層以上の階層を構成しても構わない。

【0027】

セットアップ装置 200 は、各復号装置 300 によって共通に使用される公開鍵 PK（公開鍵データ）を生成すると共に、第 1 階層の復号装置 300 毎にユーザ秘密鍵 SK を生成する。

10

セットアップ装置 200 は、第 1 階層に限らず第 2 階層以下の階層の復号装置 300 を対象にしてユーザ秘密鍵 SK を生成しても構わない。

【0028】

暗号化装置 400 は、暗号化されていないデータ（以下、「平文データ M」という）を暗号化し、暗号文データ CT を生成する。

【0029】

復号装置 300 は、暗号化装置 400 によって生成された暗号文データ CT を公開鍵 PK と自己のユーザ秘密鍵 SK とを用いて復号し、平文データ M を生成する。

【0030】

また、復号装置 300 は、自己のユーザ秘密鍵 SK を用いて下位の復号装置 300（子装置）毎にユーザ秘密鍵 SK を生成する。

20

例えば、復号装置 300A は、自己のユーザ秘密鍵 SK（ID_A）を用いて、復号装置 300C 用のユーザ秘密鍵 SK（ID_C）と復号装置 300D 用のユーザ秘密鍵 SK（ID_D）とを生成する。

【0031】

図 2 は、実施の形態 1 における階層型 ID ベース暗号システム 100 の階層構造の一例を示す図である。

階層型 ID ベース暗号システム 100 を適用する A 社の階層構造について、図 2 に基づいて説明する。

【0032】

30

例えば、階層型 ID ベース暗号システム 100 は会社組織に適用することができる。

ここで、A 社には総務部、開発部、広報部などの「部」が存在し、「部」には人事課、経理課などの「課」が存在し、「課」には採用係、研修係などの「係」が存在しているものとする。

この場合、「部」を第 1 階層、「課」を第 2 階層、「係」を第 3 階層として扱い、社員を第 4 階層として扱う。但し、社員はいずれかの「係」に配属されるものとは限らず、「部」または「課」に直属で配属されても構わない。図 2 では、田中さんが総務部の直属の社員である。

【0033】

そして、A 社はセットアップ装置 200 と暗号化装置 400 とを所有する。

40

また、各「部」は部長が使用する復号装置 300 を所有し、各「課」は課長が使用する復号装置 300 を所有し、各「係」は係長が使用する復号装置 300 を所有する。

さらに、各社員は復号装置 300 を所有する。

【0034】

また、部長、課長、係長および社員（それぞれユーザの一例）には各自を識別する「ユーザ識別子 ID」を割り当てる。

さらに、個人（ユーザ）または部署（階層）毎に暗号処理用のデータ「パターン P」を予め定義しておく。

【0035】

図 3 は、実施の形態 1 における階層型 ID ベース暗号システム 100 のユーザ識別子 I

50

Dの一例を示す図である。

階層型IDベース暗号システム100を適用するA社内のユーザ識別子IDについて、図3に基づいて説明する。

【0036】

ユーザ識別子IDは、階層数と同じ個数の要素（識別子）を含んだデータである。

つまり、A社の階層数は「4」（図2参照）であるため、A社で使用するユーザ識別子IDには4つの要素が含まれる。

【0037】

図中において、「φ」は不要な階層（対応する情報が無い階層）を意味する要素（空欄値）である。

10

【0038】

例えば、総務部長のユーザ識別子ID₁は（総務部、φ、φ、φ）であり、人事課長のユーザ識別子ID₂は（総務部、人事課、φ、φ）である。

同様に、採用係長のユーザ識別子ID₅は（総務部、人事課、採用係、φ）であり、山田さんのユーザ識別子ID₆は（総務部、人事課、採用係、山田）である。

また、総務部直属の社員である田中さんのユーザ識別子ID₈は（総務部、φ、φ、田中）となる。

【0039】

ユーザ識別子IDに含まれる要素は、数字、文字、記号またはそれらの組み合わせたものなど、自由に定めることができる。

20

例えば、識別子“総務部”は文字列であっても構わないし、総務部に対応付けられた番号（整数値）であっても構わない。

【0040】

以下、ユーザ識別子IDに含まれる要素を「階層識別子」という。

【0041】

図4は、実施の形態1における階層型IDベース暗号システム100のパターンPの一例を示す図である。

階層型IDベース暗号システム100を適用するA社内のパターンPについて、図4に基づいて説明する。

【0042】

30

パターンPは、階層数と同じ個数の要素（識別子）を含んだデータである。

つまり、A社の階層数は「4」（図2参照）であるため、A社で使用するパターンPには4つの要素が含まれる。

【0043】

図中において、「＊」は当該部署または階層に属する任意の個人（全てのユーザ）を意味する要素（ワイルドカード値）である。

【0044】

例えば、山田さん用のパターンP₁は（総務部、人事課、採用係、山田）であり、人事課長用のパターンP₄は（総務部、人事課、φ、φ）であり、総務部直属の田中さん用のパターンP₈は（総務部、φ、φ、田中）である。

40

このように、個人用のパターンPはユーザ識別子IDと同一である（図3参照）。

【0045】

また、採用係に属する社員用のパターンP₂は（総務部、人事課、採用係、＊）であり、総務部に属する課長用のパターンP₅は（総務部、＊、φ、φ）である。

さらに、部長または課長用のパターンP₆は（＊、＊、φ、φ）であり、部長、課長、係長または社員用のパターンP₇は（＊、＊、＊、＊）である。

このように、個人用ではなく部署または階層用のパターンPには「＊」が含まれる。

【0046】

以下、パターンPに含まれる要素を「パターン値」という。

【0047】

50

次に、階層型IDベース暗号システム100を構成する各装置（図1参照）について説明する。

【0048】

図5は、実施の形態1におけるセットアップ装置200の概要図である。

実施の形態1におけるセットアップ装置200の概要について、図5に基づいて説明する。

【0049】

セットアップ装置200は、セットアップ処理部210と鍵生成処理部220とセットアップ記憶部290（鍵生成記憶部の一例）とを備える。

【0050】

セットアップ処理部210は、セキュリティパラメータ λ と階層数 L とを入力し、公開鍵 PK とマスタ秘密鍵 MSK とを生成し、生成した公開鍵 PK とマスタ秘密鍵 MSK とを出力する。

【0051】

鍵生成処理部220は、公開鍵 PK とマスタ秘密鍵 MSK とユーザ i のユーザ識別子 ID_i とを入力し、ユーザ i のユーザ秘密鍵 $SK(ID_i)$ を生成し、生成したユーザ i のユーザ秘密鍵 $SK(ID_i)$ を出力する。

【0052】

セットアップ記憶部290は、セットアップ装置200で使用するデータを記憶する記憶部である。

例えば、セキュリティパラメータ λ 、階層数 L 、公開鍵 PK 、マスタ秘密鍵 MSK 、ユーザ識別子 ID_i 、ユーザ秘密鍵 $SK(ID_i)$ は、セットアップ記憶部290に記憶されるデータの一例である。

【0053】

図6は、実施の形態1におけるセットアップ装置200の機能構成図である。

実施の形態1におけるセットアップ装置200の機能構成について、図6に基づいて説明する。

【0054】

セットアップ装置200（鍵生成装置の一例）は、前述の通り、セットアップ処理部210と鍵生成処理部220とセットアップ記憶部290（鍵生成記憶部の一例）とを備える。

【0055】

セットアップ処理部210は、例えば、 L 個（ L は2以上の特定の整数）の階層を有する組織に属するユーザの公開鍵 PK を生成する。

【0056】

セットアップ処理部210は、セットアップ入力部211、セットアップ前処理部212、公開鍵値算出部213、公開鍵生成部214、マスタ秘密鍵生成部215およびセットアップ出力部216を備える。

【0057】

セットアップ入力部211は、セットアップ入力処理を行う。

例えば、セットアップ入力部211は、セキュリティパラメータ λ と階層数 L とを入力する。

【0058】

セットアップ前処理部212（要素値選択部の一例）は、セットアップ前処理（要素値選択処理を含む）を行う。

例えば、セットアップ前処理部212は、セットアップ前処理において以下の処理を行う。

【0059】

セットアップ前処理部212は、セキュリティパラメータ λ に基づいて素数 p と素数 q との積 n を位数とする巡回群 G であって n 個の要素値を含む巡回群 G を算出する。

10

20

30

40

50

セットアップ前処理部 2 1 2 は、算出した巡回群 G の一部を構成する部分群 G_p であって素数 p を位数とする部分群 G_p から L 個の要素値を L 個の階層に対応付けて L 個の鍵値 h として選択する。

セットアップ前処理部 2 1 2 は、前記部分群 G_p から L 個の要素値を L 個の階層に対応付けて L 個の鍵値 h' として選択する。

セットアップ前処理部 2 1 2 は、算出した巡回群 G の一部を構成する部分群 G_q であって素数 q を位数とする部分群 G_q から L 個の要素値を L 個の階層に対応付けて L 個の鍵値 R として選択する。

セットアップ前処理部 2 1 2 は、前記部分群 G_q から L 個の要素値を L 個の階層に対応付けて L 個の鍵値 R' として選択する。

10

【0060】

公開鍵値算出部 2 1 3 は、公開鍵値算出処理を行う。

例えば、公開鍵値算出部 2 1 3 は、公開鍵値算出処理において以下の処理を行う。

【0061】

公開鍵値算出部 2 1 3 は、セットアップ前処理部 2 1 2 により選択された L 個の鍵値 h と L 個の鍵値 R とを階層毎に乗算して L 個の階層に対応付けられた L 個の鍵値 H を H 鍵値群として算出する。

公開鍵値算出部 2 1 3 は、セットアップ前処理部 2 1 2 により選択された L 個の鍵値 h' と L 個の鍵値 R' とを階層毎に乗算して L 個の階層に対応付けられた L 個の鍵値 H' を H' 鍵値群として算出する。

20

【0062】

公開鍵生成部 2 1 4 は、公開鍵生成処理を行う。

例えば、公開鍵生成部 2 1 4 は、公開鍵生成処理において以下の処理を行う。

【0063】

公開鍵生成部 2 1 4 は、公開鍵値算出部 2 1 3 により算出された H 鍵値群と H' 鍵値群とを含んだ公開鍵 PK を生成する。

【0064】

マスタ秘密鍵生成部 2 1 5 は、マスタ秘密鍵生成処理を行う。

例えば、マスタ秘密鍵生成部 2 1 5 は、マスタ秘密鍵生成処理において以下の処理を行う。

30

【0065】

マスタ秘密鍵生成部 2 1 5 は、セットアップ前処理部 2 1 2 により選択された L 個の鍵値 h を h 鍵値群として含んだマスタ秘密鍵 MSK を生成する。

【0066】

セットアップ出力部 2 1 6 は、セットアップ出力処理を行う。

例えば、セットアップ出力部 2 1 6 は、公開鍵生成部 2 1 4 により生成された公開鍵 PK とマスタ秘密鍵生成部 2 1 5 により生成されたマスタ秘密鍵 MSK とを出力する。

【0067】

鍵生成処理部 2 2 0 は、例えば、階層構造を有する組織内で第 k 階層 (k は 2 以上の特定の整数) に属する特定ユーザのユーザ秘密鍵 SK を生成する。

40

【0068】

鍵生成処理部 2 2 0 は、鍵生成入力部 2 2 1、鍵生成前処理部 2 2 2、ユーザ秘密鍵値算出部 2 2 3 およびユーザ秘密鍵生成部 2 2 4 を備える。

【0069】

鍵生成入力部 2 2 1 は、鍵生成入力処理を行う。

例えば、鍵生成入力部 2 2 1 は、鍵生成入力処理において以下の処理を行う。

【0070】

鍵生成入力部 2 2 1 は、特定ユーザのユーザ識別子を第 k 階層を識別する階層識別子として含むと共に第 1 階層から第 $k-1$ 階層までの階層を識別する $k-1$ 個の階層識別子を含むユーザ識別子 ID を入力する。

50

鍵生成入力部 2 2 1 は、 k 個の階層に対応付けられた k 個の鍵値 h を含む h 鍵値群と k 個の階層に対応付けられた k 個の鍵値 h' を含む h' 鍵値群とを含むマスタ秘密鍵 MSK を入力する。

【0071】

鍵生成前処理部 2 2 2 は、鍵生成前処理を行う。

例えば、鍵生成前処理部 2 2 2 は、ユーザ識別子 ID に含まれる階層識別子が文字列である場合、階層識別子を文字列から整数値に変換する。

【0072】

ユーザ秘密鍵値算出部 2 2 3 は、ユーザ秘密鍵値算出処理を行う。

例えば、ユーザ秘密鍵値算出部 2 2 3 は、ユーザ秘密鍵値算出処理において以下の処理を行う。 10

【0073】

ユーザ秘密鍵値算出部 2 2 3 は、鍵生成入力部 2 2 1 が入力したユーザ識別子 ID とマスタ秘密鍵 MSK とを用いて、暗号文データ CT の復号に用いる鍵値 a_0 を算出する。

【0074】

ユーザ秘密鍵生成部 2 2 4 は、ユーザ秘密鍵生成処理を行う。

例えば、ユーザ秘密鍵生成部 2 2 4 は、ユーザ秘密鍵生成処理において以下の処理を行う。

【0075】

ユーザ秘密鍵生成部 2 2 4 は、ユーザ秘密鍵値算出部 2 2 3 により算出された鍵値 a_0 を含んだユーザ秘密鍵 SK を生成し、生成したユーザ秘密鍵 SK を出力する。 20

【0076】

図 7 は、実施の形態 1 における復号装置 3 0 0 の概要図である。

実施の形態 1 における復号装置 3 0 0 の概要について、図 7 に基づいて説明する。

【0077】

復号装置 3 0 0 は、復号処理部 3 1 0 と鍵委譲処理部 3 2 0 と復号記憶部 3 9 0（鍵委譲記憶部の一例）とを備える。

但し、最下層の復号装置 3 0 0（例えば、社員用の復号装置 3 0 0）には鍵委譲処理部 3 2 0 を備えなくても構わない。

【0078】

復号処理部 3 1 0 は、公開鍵 PK とユーザ i のユーザ秘密鍵 $SK(ID_i)$ とユーザ i 用に生成された暗号文データ CT とユーザ i のユーザ識別子 ID_i とを入力し、暗号文データ CT を復号して平文データ M を生成し、生成した平文データ M を出力する。 30

【0079】

鍵委譲処理部 3 2 0 は、公開鍵 PK とユーザ i のユーザ秘密鍵 $SK(ID_i)$ とユーザ i の一つ下の階層に属するユーザ j のユーザ識別子 ID_j とを入力し、ユーザ j の秘密鍵 $SK(ID_j)$ を生成し、生成したユーザ j の秘密鍵 $SK(ID_j)$ を出力する。

【0080】

復号記憶部 3 9 0 は、復号装置 3 0 0 で使用するデータを記憶する記憶部である。

例えば、公開鍵 PK 、ユーザ秘密鍵 $SK(ID_x)$ 、暗号文データ CT 、ユーザ識別子 ID_x 、平文データ M は、復号記憶部 3 9 0 に記憶されるデータの一つである。 40

【0081】

図 8 は、実施の形態 1 における復号装置 3 0 0 の機能構成図である。

実施の形態 1 における復号装置 3 0 0 の機能構成について、図 8 に基づいて説明する。

【0082】

復号装置 3 0 0（鍵委譲装置の一例）は、前述の通り、復号処理部 3 1 0 と鍵委譲処理部 3 2 0 と復号記憶部 3 9 0（鍵委譲記憶部の一例）とを備える。

【0083】

復号処理部 3 1 0 は、復号入力部 3 1 1、復号前処理部 3 1 2 および復号部 3 1 3 を備える。 50

【0084】

復号入力部311は、復号入力処理を行う。

例えば、復号入力部311は、復号入力処理において以下の処理を行う。

【0085】

復号入力部311は、暗号文データCTとユーザ識別子IDとを入力する。

暗号文CTは、平文データMを暗号化した平文暗号値 C_0 と特定のワイルドカード暗号値 C_1 と特定の識別暗号値 C_3 とワイルドカード階層値Wとを含む。ワイルドカード階層値Wは、パターンPに含まれるパターン値がワイルドカード値である階層を示す。

【0086】

復号前処理部312は、復号前処理を行う。

例えば、復号前処理部312は、ユーザ識別子IDに含まれる階層識別子が文字列である場合、階層識別子を文字列から整数値に変換する。

【0087】

復号部313は、復号処理を行う。

例えば、復号部313は、復号処理において以下の処理を行う。

【0088】

復号部313は、復号入力部311が入力した暗号文データCTに基づいて、復号部313が入力したユーザ識別子IDから前記ワイルドカード階層値Wによって示される階層の階層識別子をワイルドカード識別子として抽出する。

復号部313は、抽出したワイルドカード識別子と前記暗号文データCTに含まれるワイルドカード暗号値 C_1 と識別暗号値 C_3 とを用いて、前記暗号文データCTに含まれる平文暗号値 C_0 を復号する。

復号部313は、前記平文暗号値 C_0 を復号して得られる前記平文データMを出力する。

【0089】

鍵委譲処理部320は、階層構造を有する組織内で第k階層（kは2以上の特定の整数）に属するユーザjのユーザ秘密鍵 SK_j を生成する。

【0090】

鍵委譲処理部320は、鍵委譲入力部321、鍵委譲前処理部322、委譲鍵値算出部323および委譲鍵生成部324を備える。

【0091】

鍵委譲入力部321は、鍵委譲入力処理を行う。

例えば、鍵委譲入力部321は、鍵委譲入力処理において以下の処理を行う。

【0092】

鍵委譲入力部321は、ユーザjのユーザ識別子を第k階層を識別する階層識別子として含むと共に第1階層から第k-1階層までの階層を識別するk-1個の階層識別子を含むユーザ識別子ID_jを入力する。

鍵委譲入力部321は、第k-1階層に属するユーザiのユーザ秘密鍵 SK_i であって暗号文データCTの復号に用いる鍵値 a_0 を含んだユーザ秘密鍵 SK_i を入力する。

【0093】

鍵委譲前処理部322は、鍵委譲前処理を行う。

例えば、鍵委譲前処理部322は、ユーザ識別子IDに含まれる階層識別子が文字列である場合、階層識別子を文字列から整数値に変換する。

【0094】

委譲鍵値算出部323は、委譲鍵値算出処理を行う。

例えば、委譲鍵値算出部323は、委譲鍵値算出処理において以下の処理を行う。

【0095】

委譲鍵値算出部323は、鍵委譲入力部321が入力したユーザ識別子ID_jとユーザ秘密鍵 SK_i とを用いて、前記暗号文データCTの復号に用いる鍵値 x_0 を算出する。

【0096】

10

20

30

40

50

委譲鍵生成部 324 は、委譲鍵生成処理を行う。

例えば、委譲鍵生成部 324 は、委譲鍵生成処理において以下の処理を行う。

【0097】

委譲鍵生成部 324 は、委譲鍵値算出部 323 により算出された鍵値 x_0 を含んだユーザ秘密鍵 SK_j を生成し、生成したユーザ秘密鍵 SK_j を出力する。

【0098】

図 9 は、実施の形態 1 における暗号化装置 400 の概要図である。

実施の形態 1 における暗号化装置 400 の概要について、図 9 に基づいて説明する。

【0099】

暗号化装置 400 は、暗号処理部 410 と暗号化記憶部 490 とを備える。

10

【0100】

暗号処理部 410 は、公開鍵 PK と（個人または）階層 i 用のパターン P_i と平文データ M とを入力し、平文データ M を暗号化して（個人または）階層 i 用の暗号文データ CT を生成し、生成した暗号文データ CT を出力する。

【0101】

暗号化記憶部 490 は、暗号化装置 400 で使用するデータを記憶する記憶部である。

例えば、公開鍵 PK 、パターン P_i 、平文データ M 、暗号文データ CT は、暗号化記憶部 490 に記憶されるデータの一例である。

【0102】

図 10 は、実施の形態 1 における暗号化装置 400 の機能構成図である。

20

実施の形態 1 における暗号化装置 400 の機能構成について、図 10 に基づいて説明する。

【0103】

暗号化装置 400 は、前述の通り、暗号処理部 410 と暗号化記憶部 490 とを備える。

【0104】

暗号処理部 410 は、暗号化入力部 411、暗号化前処理部 412、暗号値算出部 413 および暗号文生成部 414 を備える。

【0105】

暗号化入力部 411 は、暗号化入力処理を行う。

30

例えば、暗号化入力部 411 は、暗号化入力処理において以下の処理を行う。

【0106】

暗号化入力部 411 は、暗号化する平文データ M を入力する。

暗号化入力部 411 は、 k 個（ k は 2 以上の特定の整数）の階層に対応付けられた k 個の鍵値 H を含む H 鍵値群を含んだ公開鍵 PK を入力する。

暗号化入力部 411 は、階層を識別する階層識別子と任意のユーザを意味するワイルドカード値と不要な階層を意味する空欄値とのいずれかを階層毎にパターン値として含んだパターン P を入力する。

【0107】

暗号化前処理部 412 は、暗号化前処理を行う。

40

例えば、暗号化前処理部 412 は、パターン P に含まれるパターン値（例えば、階層識別子）が文字列である場合、パターン値を文字列から整数値に変換する。

【0108】

暗号値算出部 413 は、暗号値算出処理を行う。

例えば、暗号値算出部 413 は、暗号値算出処理において以下の処理を行う。

【0109】

暗号値算出部 413 は、暗号化入力部 411 が入力した平文データ M を暗号化して平文暗号値 C_0 を算出する。

暗号値算出部 413 は、暗号化入力部 411 が入力したパターン P に基づいて前記パターン値がワイルドカード値である階層をワイルドカード階層として判定する。

50

暗号値算出部 4 1 3 は、暗号化入力部 4 1 1 が入力した公開鍵 PK に含まれる H 鍵値群から前記ワイルドカード階層に対応付けられた鍵値 H をワイルドカード鍵値として抽出する。

暗号値算出部 4 1 3 は、抽出したワイルドカード鍵値を用いて前記平文暗号値 C_0 の復号に用いるワイルドカード暗号値 C_1 を算出する。

暗号値算出部 4 1 3 は、前記パターン P に基づいて前記パターン値が階層識別子である階層を識別階層として判定する。

暗号値算出部 4 1 3 は、前記公開鍵 PK に含まれる H 鍵値群から前記識別階層に対応付けられた鍵値 H を識別鍵値として抽出する。

暗号値算出部 4 1 3 は、抽出した識別鍵値を用いて前記平文暗号値 C_0 の復号に用いる識別暗号値 C_3 を算出する。

10

【0 1 1 0】

暗号文生成部 4 1 4 は、暗号文生成処理を行う。

例えば、暗号文生成部 4 1 4 は、暗号文生成処理において以下の処理を行う。

【0 1 1 1】

暗号文生成部 4 1 4 は、暗号値算出部 4 1 3 により算出された平文暗号値 C_0 とワイルドカード暗号値 C_1 と識別暗号値 C_3 とを含むと共に前記ワイルドカード階層を示すワイルドカード階層値 W を含む暗号文データ CT を生成する。

暗号文生成部 4 1 4 は、生成した暗号文データ CT を出力する。

【0 1 1 2】

20

次に、階層型 ID ベース暗号システム 1 0 0 を構成する各装置（図 1 参照）の処理方法について説明する。

【0 1 1 3】

図 1 1 は、実施の形態 1 におけるセットアップ装置 2 0 0 によるセットアップ方法を示すフローチャートである。

セットアップ装置 2 0 0 のセットアップ処理部 2 1 0 が実行するセットアップ方法の処理の流れについて、図 1 1 に基づいて説明する。

【0 1 1 4】

$S 1 1 0$ において、セットアップ入力部 2 1 1 は、セキュリティパラメータ λ と階層数 L と入力装置またはセットアップ記憶部 2 9 0 から入力する。

30

$S 1 1 0$ の後、 $S 1 2 0$ に進む。

【0 1 1 5】

$S 1 2 0$ において、セットアップ前処理部 2 1 2 は、セキュリティパラメータ λ に基づいて素数 p 、 q を生成（算出）し、生成した素数 p 、 q を乗算して合成数 $n (= p q)$ を算出する。

セットアップ前処理部 2 1 2 は、算出した合成数 n と所定の写像 e と、 $S 1 1 0$ で入力されたセキュリティパラメータ λ と階層数 L とに基づいて群 G 、 G_T を生成する。

【0 1 1 6】

群 G 、 G_T は合成数 n を位数とする巡回群であり、 n 個の要素値を含む。巡回群 G 、 G_T は加法群と乗法群とのどちらであっても構わない。以下、巡回群 G 、 G_T が乗法群であるものとして説明を続ける。

40

【0 1 1 7】

写像 e は 2 つの入力値から 1 つの出力値を得る関数であり、次の性質 (a) (b) を満たす。

【0 1 1 8】

【数 1】

性質 (a) : $e(g, g)$ が G_T の生成元となる g が存在する。但し、 g は G の生成元である。

性質 (b) : $u, v \in G, a, b \in \mathbb{Z}$ に対し、 $e(u^a, v^b) = e(u, v)^{ab}$ が成立する。但し、 $\mathbb{Z}$ は整数の集合である。

【0 1 1 9】

性質 (a) (b) を満たす写像 e をペアリングという。ペアリング e は以下のように表すことができる。

10

【0 1 2 0】

【数 2】

$$e : G \times G \rightarrow G_T$$

【0 1 2 1】

ペアリング e の演算を「ペアリング演算」という。

ペアリング e によって定義される群 G, G_T を「ペアリング群」という。

例えば、ペアリング群 G, G_T として、楕円曲線上の有理点から成る群 G と有限体上の群 G_T とが挙げられる。

20

群 G と群 G_T とのペアリングは対称ペアリングと非対称ペアリングとのどちらであっても構わない。以下、対称ペアリングを対象にして説明を続ける。非対称ペアリングを対象にする場合については、当業者であれば以下の説明から容易に理解し得ることである。

【0 1 2 2】

素数 p, q の生成方法は、例えば、非特許文献 4 に開示されている。

ペアリング群 G, G_T の生成方法は、例えば、非特許文献 3 に開示されている。

【0 1 2 3】

S 1 2 0 の後、S 1 3 0 に進む。

【0 1 2 4】

S 1 3 0 において、セットアップ前処理部 2 1 2 は、群 G を用いて群 G の一部を構成する部分群 G_p を生成する。部分群 G_p は素数 p を位数として p 個の要素値を含む要素値群である。

30

セットアップ前処理部 2 1 2 は、式 [S U 1] に示すように、生成した部分群 G_p から複数の要素値をランダムに選択する。

【0 1 2 5】

【数 3】

$$g_p, f, v, v', w, h_1, h'_1, \dots, h_L, h'_L \xleftarrow{U} G_p \quad \text{式 [S U 1]}$$

40

ここで、

$a_1, a_2, \dots, a_m \xleftarrow{U} A$ は、 A から m 個の要素のランダムな選択を意味する。

【0 1 2 6】

S 1 3 0 の後、S 1 3 1 に進む。

【0 1 2 7】

S 1 3 1 において、セットアップ前処理部 2 1 2 は、群 G を用いて群 G の一部を構成する部分群 G_q を生成する。部分群 G_q は素数 q を位数として q 個の要素値を含む要素値群である。

50

セットアップ前処理部 2 1 2 は、式 [S U 2] に示すように、生成した部分群 G_q から複数の要素値をランダムに選択する。

【0 1 2 8】

【数 4】

$$g_q, R_f, R_v, R'_v, R_{h,1}, R'_{h,1}, \dots, R_{h,L}, R'_{h,L} \xleftarrow{U} G_q \quad \text{式 [S U 2]}$$

【0 1 2 9】

S 1 3 1 の後、S 1 4 0 に進む。

10

【0 1 3 0】

S 1 4 0 において、公開鍵値算出部 2 1 3 は、S 1 3 0 で選択された複数の要素値と S 1 3 1 で選択された複数の要素値とを用いて複数の公開鍵値を算出する。

以下に、複数の公開鍵値を算出する複数の算出式 [S U 3] を示す。

【0 1 3 1】

【数 5】

$$\begin{aligned} F &:= fR_f, V := vR_v, V' := v'R'_v, E := e(g, w), \\ H_1 &:= h_1R_{h,1}, H'_1 := h'_1R'_{h,1}, \dots, H_L := h_LR_{h,L}, H'_L := h'_LR'_{h,L} \end{aligned} \quad \text{式 [S U 3]}$$

20

ここで、

$a := b$ は、変数 a に値 b を代入することを意味する。

【0 1 3 2】

S 1 4 0 の後、S 1 5 0 に進む。

【0 1 3 3】

S 1 5 0 において、公開鍵生成部 2 1 4 は、S 1 4 0 で算出された複数の公開鍵値を含んだ公開鍵 PK を生成する。

以下に、公開鍵 PK を表す式 [S U 4] を示す。

30

【0 1 3 4】

【数 6】

$$PK = [G, G_T, n, e, g_p, g_q, F, V, V', H_1, H'_1, \dots, H_L, H'_L, E] \quad \text{式 [S U 4]}$$

【0 1 3 5】

S 1 5 0 の後、S 1 6 0 に進む。

【0 1 3 6】

S 1 6 0 において、マスタ秘密鍵生成部 2 1 5 は、S 1 3 0 で選択された複数の要素値をマスタ秘密鍵値として含んだマスタ秘密鍵 MSK を生成する。

40

以下に、マスタ秘密鍵 MSK を表す式 [S U 5] を示す。

【0 1 3 7】

【数 7】

$$MSK = [p, q, f, v, v', h_1, h'_1, \dots, h_L, h'_L, w] \quad \text{式 [S U 5]}$$

【0 1 3 8】

S 1 6 0 の後、S 1 7 0 に進む。

50

【0139】

S170において、セットアップ出力部216は、S150で生成された公開鍵PKとS160で生成されたマスタ秘密鍵MSKとをセットアップ記憶部290に記憶する。

また、セットアップ出力部216は、システム全体でできるように公開鍵PKをシステムの共有サーバ（図示省略）に記憶する。但し、セットアップ出力部216は、公開鍵PKを各復号装置300および暗号化装置400に送信しても構わない。

S170により、セットアップ方法の処理は終了する。

【0140】

図12は、実施の形態1におけるセットアップ装置200による鍵生成方法を示すフローチャートである。

10

セットアップ装置200の鍵生成処理部220が実行する鍵生成方法の処理の流れについて、図12に基づいて説明する。

【0141】

S210において、鍵生成入力部221は、セットアップ処理部210により生成された公開鍵PKとマスタ秘密鍵MSKとをセットアップ記憶部290から入力する。

鍵生成入力部221は、特定のユーザ i に割り当てられたユーザ識別子 ID_i を入力装置またはセットアップ記憶部290から入力する。

S210の後、S220に進む。

【0142】

S220において、鍵生成前処理部222は、ユーザ識別子 ID_i を構成する要素を整数値群 Z_n に含まれるいずれかの整数値に変換する。整数値群 Z_n は、0から $n-1$ までの整数値で構成される群である。図11のS120で説明したように、 n は素数 p と素数 q との積であり、群 G の位数である。

20

【0143】

例えば、鍵生成前処理部222は、要素を表す2進数を10進数の整数値に変換する。鍵生成前処理部222は、得られた10進数の整数値を法 n で剰余演算し、剰余値を整数値として求めてもよい。

また、鍵生成前処理部222は、ハッシュ関数に要素を代入して整数値を得てもよい。

また、要素と整数値とを対応付けた変換テーブルをセットアップ記憶部290に予め記憶しておき、鍵生成前処理部222が要素に対応する整数値をセットアップ記憶部290から取得しても構わない。

30

【0144】

但し、ユーザ識別子 ID_i を構成する全ての要素が整数値である場合、S220を実行する必要はない。また、ユーザ識別子 ID_i を構成する複数の要素のうち整数値で表す要素については、S220を実行しなくても構わない。

【0145】

S220の後、S230に進む。

【0146】

S230において、鍵生成前処理部222は、式[KG1]に示すように、整数値群 Z_n （0から $n-1$ の整数値）から複数の整数値をランダムに選択する。

40

但し、条件式[KG1-1]を満たさない場合、鍵生成前処理部222は複数の整数値を選択し直す。

【0147】

【数 8】

$$r, r', s, s', t, t' \xleftarrow{U} Z_n \quad \text{式 [KG 1]}$$

$$\det A \neq 0 \bmod p \wedge \det A \neq 0 \bmod q \quad \text{式 [KG 1-1]}$$

ここで、

$$A = \begin{pmatrix} s & t \\ s' & t' \end{pmatrix} \text{である。}$$

10

【0 1 4 8】

S 2 3 0 の後、S 2 4 0 に進む。

【0 1 4 9】

S 2 4 0 において、鍵生成前処理部 2 2 2 は、ユーザ識別子 ID_i に含まれる複数の要素のうち空欄値「 ϕ 」以外の要素を判定する。

さらに、鍵生成前処理部 2 2 2 は、空欄値「 ϕ 」以外の要素に対応する階層の番号を「非空欄階層値 D」として判定する。以下、空欄値「 ϕ 」以外の要素に対応する階層を「非空欄階層」という。

20

また、鍵生成前処理部 2 2 2 は、ユーザ識別子 ID_i に含まれる複数の要素のうち空欄値「 ϕ 」を示す要素を判定し、空欄値「 ϕ 」を示す要素に対応する階層の番号を「空欄階層値 N」として判定する。以下、空欄値「 ϕ 」を示す要素に対応する階層を「空欄階層」という。

以下に、非空欄階層値 D を表す式 [KG 2] と空欄階層値 N を表す式 [KG 3] とを示す。

【0 1 5 0】

【数 9】

$$D(ID_i) = \{1 \leq j \leq L \mid p_j \neq \phi\} \quad \text{式 [KG 2]}$$

30

$$N(ID_i) = \{1 \leq j \leq L \mid p_j = \phi\} \quad \text{式 [KG 3]}$$

ここで、

$D(ID_i)$: ユーザ識別子 ID_i の非空欄階層値 D

$N(ID_i)$: ユーザ識別子 ID_i の空欄階層値 N

である。

40

【0 1 5 1】

例えば、図 3 に示した経理課長のユーザ識別子 ID_3 (総務部、経理課、 ϕ 、 ϕ) の場合、非空欄階層値 D は「1」と「2」であり、空欄階層値 N は「3」と「4」である。

また、田中さんのユーザ識別子 ID_8 (総務部、 ϕ 、 ϕ 、田中) の場合、非空欄階層値 D は「1」と「4」であり、空欄階層値 N は「2」と「3」である。

【0 1 5 2】

S 2 4 0 の後、S 2 5 0 に進む。

【0 1 5 3】

50

S 2 5 0において、ユーザ秘密鍵値算出部 2 2 3 は、マスタ秘密鍵 M S K とユーザ識別子 I D_i とユーザ識別子 I D_i の非空欄階層値 D と S 2 3 0 で選択された整数値とを用いて、複数の復号鍵値を算出する。

ここで、ユーザ i の属する階層の番号を「K」とする。

以下に、複数の復号鍵値を算出する複数の算出式 [K G 4] を示す。

【 0 1 5 4 】

【数 1 0】

$$a_0 := w \left(v \prod_{\substack{j \in \bar{D}(ID_i) \\ 1 \leq j \leq k}} h_j^{I_j} \right)^r \left(v' \prod_{\substack{j \in \bar{D}(ID_i) \\ 1 \leq j \leq k}} h'_j^{I_j} \right)^{r'}, \quad 10$$

$$a_1 := f^r,$$

$$a'_1 := f^{r'}, \left\{ b_j := h_j^r h'_j{}^{r'} \right\}_{j=k+1, \dots, L} \quad 20$$

式 [K G 4]

ここで、

$$a_0, a_1, a'_1, \{b_j\} : \text{復号鍵値}$$

である。

【 0 1 5 5 】

S 2 5 0 の後、S 2 5 1 に進む。

【 0 1 5 6 】

S 2 5 1において、ユーザ秘密鍵値算出部 2 2 3 は、S 2 5 0 と同様に複数の攪乱鍵値 (A) を算出する。

以下に、複数の攪乱鍵値 (A) を算出する複数の算出式 [K G 5] を示す。

【 0 1 5 7 】

30

【数 1 1】

$$\alpha_0 := \left(v \prod_{\substack{j \in D(ID_i) \\ 1 \leq j \leq k}} h_j^{I_j} \right)^s \left(v' \prod_{\substack{j \in D(ID_i) \\ 1 \leq j \leq k}} h'_j{}^{I_j} \right)^{s'},$$

$$\alpha_1 := f^s,$$

$$\alpha'_1 := f^{s'}, \left\{ \beta_j := h_j^s h'_j{}^{s'} \right\}_{j=k+1, \dots, L}$$

10

式 [K G 5]

ここで、

$$\alpha_0, \alpha_1, \alpha'_1, \left\{ \beta_j \right\} : \text{攪乱鍵値 (A)}$$

である。

20

【0 1 5 8】

S 2 5 1 の後、S 2 5 2 に進む。

【0 1 5 9】

S 2 5 2 において、ユーザ秘密鍵値算出部 2 2 3 は、S 2 5 1 と同様に複数の攪乱鍵値 (B) を算出する。

以下に、複数の攪乱鍵値 (B) を算出する複数の算出式 [K G 6] を示す。

【0 1 6 0】

【数 1 2】

30

$$\tilde{\alpha}_0 := \left(v \prod_{\substack{j \in D(ID_i) \\ 1 \leq j \leq k}} h_j^{I_j} \right)^t \left(v' \prod_{\substack{j \in D(ID_i) \\ 1 \leq j \leq k}} h'_j{}^{I_j} \right)^{t'},$$

$$\tilde{\alpha}_1 := f^t,$$

$$\tilde{\alpha}'_1 := f^{t'}, \left\{ \tilde{\beta}_j := h_j^t h'_j{}^{t'} \right\}_{j=k+1, \dots, L}$$

40

式 [K G 6]

ここで、

$$\tilde{\alpha}_0, \tilde{\alpha}_1, \tilde{\alpha}'_1, \left\{ \tilde{\beta}_j \right\} : \text{攪乱鍵値 (B)}$$

である。

50

【0161】

S 2 5 2 の後、S 2 6 0 に進む。

【0162】

S 2 6 0 において、ユーザ秘密鍵生成部 2 2 4 は、S 2 5 0 で算出された複数の復号鍵値を含んだ復号鍵 dk を生成する。

さらに、ユーザ秘密鍵生成部 2 2 4 は、S 2 5 1 で算出された複数の攪乱鍵値 (A) と S 2 5 2 で算出された複数の攪乱鍵値 (B) とを含んだ攪乱鍵 rk を生成する。

以下に、復号鍵 dk を表す式 [KG 7] と攪乱鍵 rk を表す式 [KG 8] とを示す。

【0163】

【数 1 3】

10

$$dk(ID_i) := \left[a_0, a_1, a'_1, \{b_j\}_{j=k+1, \dots, L} \right], \quad \text{式 [KG 7]}$$

$$rk(ID_i) := \left[\left[\alpha_0, \alpha_1, \alpha'_1, \{\beta_j\}_{j=k+1, \dots, L} \right], \left[\tilde{\alpha}_0, \tilde{\alpha}_1, \tilde{\alpha}'_1, \{\tilde{\beta}_j\}_{j=k+1, \dots, L} \right] \right] \quad \text{式 [KG 8]}$$

ここで、

$dk(ID_i)$: ユーザ i の復号鍵 dk

20

$rk(ID_i)$: ユーザ i の攪乱鍵 rk

である。

【0164】

S 2 6 0 の後、S 2 7 0 に進む。

【0165】

S 2 7 0 において、ユーザ秘密鍵生成部 2 2 4 は、S 2 6 0 で生成した復号鍵 dk と攪乱鍵 rk とを用いてユーザ i のユーザ秘密鍵 SK を生成する。

30

そして、ユーザ秘密鍵生成部 2 2 4 は、生成したユーザ秘密鍵 SK を出力する。例えば、ユーザ秘密鍵生成部 2 2 4 は、生成したユーザ秘密鍵 SK をユーザ i の復号装置 3 0 0 へ送信する。

以下に、ユーザ i のユーザ秘密鍵 SK を表す式 [KG 9] を示す。

【0166】

【数 1 4】

$$SK(ID_i) := [dk(ID_i), rk(ID_i)] \quad \text{式 [KG 9]}$$

40

ここで、

$SK(ID_i)$: ユーザ i のユーザ秘密鍵 SK

である。

【0167】

S 2 7 0 により、鍵生成方法の処理は終了する。

【0168】

ユーザ秘密鍵 SK に含まれる復号鍵 dk は、復号装置 3 0 0 が暗号文データ CT の復号に用いるデータであり、ユーザ秘密鍵 SK に含まれる攪乱鍵 rk は、復号装置 3 0 0 が鍵

50

委譲に用いるデータである。

鍵委譲とは、復号装置 300 が自己のユーザ秘密鍵 SK を用いて下位層に属するユーザのユーザ秘密鍵を生成する処理である。

【0169】

図 13 は、実施の形態 1 における復号装置 300 による鍵委譲方法を示すフローチャートである。

復号装置 300 の鍵委譲処理部 320 が実行する鍵委譲方法の処理の流れについて、図 13 に基づいて説明する。

【0170】

S310 において、鍵委譲入力部 321 は、公開鍵 PK を入力装置、共有サーバ（図示省略）または復号記憶部 390 から入力する。

鍵委譲入力部 321 は、ユーザ i のユーザ秘密鍵 SK (ID_i) を入力装置または復号記憶部 390 から入力する。ユーザ i は、例えば、この復号装置を使用するユーザである。

鍵委譲入力部 321 は、ユーザ j のユーザ識別子 ID_j を入力装置または復号記憶部 390 から入力する。ユーザ j は、ユーザ i の一つ下の階層に属するユーザあってユーザ秘密鍵の委譲先のユーザである。

以下、ユーザ j（委譲先）の属する階層の番号を「k」とし、ユーザ i の属する階層の番号を「k-1」とする。

S310 の後、S320 に進む。

【0171】

S320 において、鍵委譲前処理部 322 は、ユーザ識別子 ID_j に含まれる要素 I_k を整数値群 Z_n（0 から n-1 の整数値）に含まれるいずれかの整数値に変換する。

要素 I_k は、ユーザ識別子 ID_j に含まれる複数の要素のうち k 番目の要素、つまり、ユーザ j（委譲先）が属する第 k 階層に対応する要素である。

変換方法は、S220（図 12 参照）と同様である。

S320 の後、S330 に進む。

【0172】

S330 において、鍵委譲前処理部 322 は、式 [KT1] に示すように、整数値群 Z_n から複数の整数値をランダムに選択する。

但し、条件式 [KT1-1] を満たさない場合、鍵委譲前処理部 322 は複数の整数値を選択し直す。

【0173】

【数 15】

$$\gamma_1, \gamma_2, \gamma_3, \delta_1, \delta_2, \delta_3 \xleftarrow{U} Z_n \quad \text{式 [KT1]}$$

$$g_p^{\det B} \neq 1 \wedge g_q^{\det B} \neq 1 \quad \text{式 [KT1-1]}$$

ここで、

$$B = \begin{pmatrix} \gamma_2 & \gamma_3 \\ \delta_2 & \delta_3 \end{pmatrix} \text{である。}$$

【0174】

S330 の後、S340 に進む。

【0175】

S340 において、委譲鍵値算出部 323 は、ユーザ秘密鍵 SK (ID_i) に含まれるユーザ i の復号鍵 dk (ID_i) とユーザ j のユーザ識別子 ID_j に含まれる要素 I_k と

10

20

30

40

50

を用いて、複数の作業値（a）を算出する。

以下に、複数の作業値（a）を算出する算出式〔K T 2〕を示す。

【0 1 7 6】

【数 1 6】

$$\left(\zeta_0, \zeta_1, \zeta'_1, \{\eta_l\}_{l=k+1, \dots, L} \right) := \left(a_0 \cdot b_k^{I_k}, a_1, a'_1, \{b_l\}_{l=k+1, \dots, L} \right) \quad \text{式 [K T 2]}$$

ここで、

10

$\zeta_0, \zeta_1, \zeta'_1, \{\eta_l\}$: 作業値（a）

である。

【0 1 7 7】

S 3 4 0 の後、S 3 4 1 に進む。

【0 1 7 8】

S 3 4 1 において、委譲鍵値算出部 3 2 3 は、ユーザ秘密鍵 SK（ID_i）に含まれるユーザ i の攪乱鍵 rk（ID_i）とユーザ j のユーザ識別子 ID_j に含まれる要素 I_k と

20

を用いて、複数の作業値（b）を算出する。

以下に、複数の作業値（b）を算出する算出式〔K T 3〕を示す。

【0 1 7 9】

【数 1 7】

$$\left(\theta_0, \theta_1, \theta'_1, \{\phi_l\}_{l=k+1, \dots, L} \right) := \left(\alpha_0 \cdot \beta_k^{I_k}, \alpha_1, \alpha'_1, \{\beta_l\}_{l=k+1, \dots, L} \right) \quad \text{式 [K T 3]}$$

ここで、

30

$\theta_0, \theta_1, \theta'_1, \{\phi_l\}$: 作業値（b）

である。

【0 1 8 0】

S 3 4 1 の後、S 3 4 2 に進む。

【0 1 8 1】

S 3 4 2 において、委譲鍵値算出部 3 2 3 は、S 3 4 1 と同様に複数の作業値（c）を算出する。

以下に、複数の作業値（c）を算出する算出式〔K T 4〕を示す。

40

【0 1 8 2】

【数 1 8】

$$\left(\tilde{\theta}_0, \tilde{\theta}_1, \tilde{\theta}'_1, \{\tilde{\phi}_l\}_{l=k+1, \dots, L}\right) := \left(\tilde{\alpha}_0 \cdot \tilde{\beta}_k^{I_k}, \tilde{\alpha}_1, \tilde{\alpha}'_1, \{\tilde{\beta}_l\}_{l=k+1, \dots, L}\right) \quad \text{式 [K T 4]}$$

ここで、

$$\tilde{\theta}_0, \tilde{\theta}_1, \tilde{\theta}'_1, \{\tilde{\phi}_l\} : \text{作業値 (c)}$$

10

である。

【0 1 8 3】

S 3 4 2 の後、S 3 5 0 に進む。

【0 1 8 4】

S 3 5 0 において、委譲鍵値算出部 3 2 3 は、S 3 4 0 から S 3 4 2 で算出した作業値 (a) - (c) と S 3 3 0 で選択された整数値とを用いて、複数の復号鍵値を算出する。

以下に、複数の復号鍵値を算出する算出式 [K T 5] を示す。

【0 1 8 5】

【数 1 9】

$$\left(x_0, x_1, x'_1, \{w_l\}_{l=k+1, \dots, L}\right) := \left(\zeta_0 \theta_0^{\gamma_1} \tilde{\theta}_0^{\delta_1}, \zeta_1 \theta_1^{\gamma_1} \tilde{\theta}_1^{\delta_1}, \zeta'_1 \theta'_1{}^{\gamma_1} \tilde{\theta}'_1{}^{\delta_1}, \{\eta_l \phi_l^{\gamma_1} \tilde{\phi}_l^{\delta_1}\}_{l=k+1, \dots, L}\right)$$

20

式 [K T 5]

ここで、

$$x_0, x_1, x'_1, \{w_l\} : \text{復号鍵値}$$

である。

【0 1 8 6】

S 3 5 0 の後、S 3 5 1 に進む。

【0 1 8 7】

S 3 5 1 において、委譲鍵値算出部 3 2 3 は、S 3 4 1 で算出した作業値 (b) と S 3 4 2 で算出した作業値 (c) と S 3 3 0 で選択された整数値とを用いて、複数の攪乱鍵値 (A) を算出する。

以下に、複数の攪乱鍵値 (A) を算出する算出式 [K T 6] を示す。

【0 1 8 8】

【数 2 0】

$$\left(\chi_0, \chi_1, \chi'_1, \{\omega_l\}_{l=k+1, \dots, L}\right) := \left(\theta_0^{\gamma_2} \tilde{\theta}_0^{\delta_2}, \theta_1^{\gamma_2} \tilde{\theta}_1^{\delta_2}, \theta'_1{}^{\gamma_2} \tilde{\theta}'_1{}^{\delta_2}, \{\phi_l^{\gamma_2} \tilde{\phi}_l^{\delta_2}\}_{l=k+1, \dots, L}\right)$$

40

式 [K T 6]

ここで、

$$\chi_0, \chi_1, \chi'_1, \{\omega_l\} : \text{攪乱鍵値 (A)}$$

である。

【0 1 8 9】

S 3 5 1 の後、S 3 5 2 に進む。

50

【0190】

S352において、委譲鍵値算出部323は、S351と同様に複数の攪乱鍵値（B）を算出する。

以下に、複数の攪乱鍵値（B）を算出する算出式〔KT7〕を示す。

【0191】

【数21】

$$\left(\tilde{\chi}_0, \tilde{\chi}_1, \tilde{\chi}'_1, \{\tilde{\omega}_l\}_{l=k+1, \dots, L} \right) := \left(\theta_0^{\gamma_3} \tilde{\theta}_0^{\delta_3}, \theta_1^{\gamma_3} \tilde{\theta}_1^{\delta_3}, \theta'_1{}^{\gamma_3} \tilde{\theta}'_1{}^{\delta_3}, \{\phi_l^{\gamma_3} \tilde{\phi}_l^{\delta_3}\}_{l=k+1, \dots, L} \right) \quad \text{式〔KT7〕}$$

ここで、

$\tilde{\chi}_0, \tilde{\chi}_1, \tilde{\chi}'_1, \{\tilde{\omega}_l\}$ ：攪乱鍵値（B）

である。

【0192】

S352の後、S360に進む。

【0193】

S360において、委譲鍵生成部324は、S350で算出された複数の復号鍵値を用いて、ユーザjの復号鍵dk（ID_j）を生成する。 20

さらに、委譲鍵生成部324は、S351で算出された複数の攪乱鍵値（A）とS352で算出された複数の攪乱鍵値（B）とを用いて、攪乱鍵rk（ID_j）を生成する。

以下に、ユーザjの復号鍵dk（ID_j）を表す式〔KT8〕とユーザjの攪乱鍵rk（ID_j）を表す式〔KT9〕とを示す。

【0194】

【数22】

$$dk(ID_j) := \left[x_0, x_1, x'_1, \{w_l\}_{l=k+1, \dots, L} \right], \quad \text{式〔KT8〕}$$

$$rk(ID_j) := \left[\left[\chi_0, \chi_1, \chi'_1, \{\omega_l\}_{l=k+1, \dots, L} \right], \left[\tilde{\chi}_0, \tilde{\chi}_1, \tilde{\chi}'_1, \{\tilde{\omega}_l\}_{l=k+1, \dots, L} \right] \right] \quad \text{式〔KT9〕}$$

ここで、

$dk(ID_j)$ ：ユーザjの復号鍵dk

$rk(ID_j)$ ：ユーザjの攪乱鍵rk

である。

【0195】

S360の後、S370に進む。

【0196】

S370において、委譲鍵生成部324は、S360で生成した復号鍵dk（ID_j）と攪乱鍵rk（ID_j）とを用いてユーザjのユーザ秘密鍵SK（ID_j）を生成し、生成したユーザ秘密鍵SK（ID_j）を復号記憶部390に記憶する。

また、委譲鍵生成部324は、生成したユーザ秘密鍵SK（ID_j）を出力する。例えば、委譲鍵生成部324は、生成したユーザ秘密鍵SK（ID_j）をユーザjの復号装置 50

300へ送信する。

以下に、ユーザ j のユーザ秘密鍵 $SK(ID_j)$ を表す式 [KT10] を示す。

【0197】

【数23】

$$SK(ID_j) := [dk(ID_j), rk(ID_j)] \quad \text{式 [KT10]}$$

ここで、

$SK(ID_j)$: ユーザ j のユーザ秘密鍵 SK

10

である。

【0198】

S370により、鍵委譲方法の処理は終了する。

但し、ユーザ j の一つ下の階層に属するユーザ j_2 のユーザ秘密鍵 $SK(ID_{j_2})$ を生成する場合には、ユーザ i をユーザ j に置き換えると共にユーザ j をユーザ j_2 に置き換えて鍵委譲方法の処理 (S310-S370) を繰り返す。

【0199】

図12で説明した鍵生成方法と図13で説明した鍵委譲方法とで見掛け上の処理は異なるが、鍵生成方法と鍵委譲方法とは同一ユーザについて同一のユーザ秘密鍵 SK を生成することができる。

20

そのため、鍵生成方法と鍵委譲方法とのいずれかを用いて、特定のユーザのユーザ秘密鍵 SK を生成すればよい。

【0200】

図14は、実施の形態1における暗号化装置400による暗号化方法を示すフローチャートである。

暗号化装置400の暗号処理部410が実行する暗号化方法の処理の流れについて、図14に基づいて説明する。

【0201】

S410において、暗号化入力部411は、公開鍵 PK を入力装置、共有サーバ (図示省略) または復号記憶部390から入力する。

30

暗号化入力部411は、ユーザ i 用のパターン P_i を入力装置、共有サーバまたは復号記憶部390から入力する。ユーザ i は、暗号文データ CT を復号できる一人のユーザまたは複数のユーザを意味する。

暗号化入力部411は、平文データ M を入力装置または復号記憶部390から入力する。

S410の後、S420に進む。

【0202】

S420において、暗号化前処理部412は、パターン P_i に含まれる要素を整数値群 Z_n (0から $n-1$ の整数値) に含まれるいずれかの整数値に変換する。

40

変換方法は、S220 (図12参照) と同様である。

S420の後、S421に進む。

【0203】

S421において、暗号化前処理部412は、式 [EN1] に示すように、整数値群 Z_n から整数値 ρ をランダムに選択する。

【0204】

【数 2 4】

$$\rho \leftarrow \frac{U}{Z_n} \quad \text{式 [EN 1]}$$

【0 2 0 5】

S 4 2 1 の後、S 4 2 2 に進む。

【0 2 0 6】

S 4 2 2 において、暗号化前処理部 4 1 2 は、パターン P_i に含まれる複数の要素のうちワイルドカード値「*」を示す要素を判定する。

さらに、暗号化前処理部 4 1 2 は、ワイルドカード値「*」を示す要素に対応する階層の番号を「ワイルドカード階層値W」として判定する。以下、ワイルドカード値「*」を示す要素に対応する階層を「ワイルドカード階層」という。

また、暗号化前処理部 4 1 2 は、パターン P_i に含まれる複数の要素のうち空欄値「φ」を示す要素を判定し、空欄値「φ」を示す要素に対応する階層の番号を「空欄階層値N」として判定する。以下、空欄値「φ」を示す要素に対応する階層を「空欄階層」という。

また、暗号化前処理部 4 1 2 は、パターン P_i に含まれる複数の要素のうちワイルドカード値「*」および空欄値「φ」以外の要素を判定し、ワイルドカード値「*」および空欄値「φ」以外の要素に対応する階層の番号を「識別階層値D」として判定する。以下、ワイルドカード値「*」および空欄値「φ」以外の要素に対応する階層を「識別階層」という。

以下に、ワイルドカード階層値Wを表す式 [EN 2] と空欄階層値Nを表す式 [EN 3] と識別階層値Dを表す式 [EN 4] とを示す。

【0 2 0 7】

【数 2 5】

$$W(P_i) = \{1 \leq j \leq L \mid p_j = *\} \quad \text{式 [EN 2]}$$

$$N(P_i) = \{1 \leq j \leq L \mid p_j = \phi\} \quad \text{式 [EN 3]}$$

$$D(P_i) = \{1 \leq j \leq L \mid p_j \neq * \wedge p_j \neq \phi\} \quad \text{式 [EN 4]}$$

ここで、

$W(P_i)$: パターン P_i のワイルドカード階層値W

$N(P_i)$: パターン P_i の空欄階層値N

$D(P_i)$: パターンの識別階層値D

p_j : パターン P_i の j 番目の要素

である。

【0 2 0 8】

例えば、図 4 に示したパターン P_5 (総務部、*、φ、φ) の場合、ワイルドカード階層値Wは「2」であり、空欄階層値Nは「3」と「4」であり、識別階層値Dは「1」である。

また、パターン P_8 (総務部、φ、φ、田中) の場合、ワイルドカード階層値Wは無く

、空欄階層値Nは「2」と「3」であり、識別階層値Dは「1」と「4」である。

【0209】

S422の後、S423に進む。

【0210】

S423において、暗号化前処理部412は、ワイルドカード階層値Wに基づいて整数値群 Z_n から複数の整数値をランダムに選択し、選択した整数値毎に整数値を公開鍵PKに含まれる公開鍵値 g_q にべき乗する。

この処理は、式[EN5]に示すように、素数 q を位数とする群 G_q から複数の要素値をランダムに選択することと等しい。

【0211】

【数26】

$$\{Z_{1,j}, Z'_{1,j}\}_{j \in W(P_i)}, Z_2, Z_3, Z'_3 \xleftarrow{U} G_q \quad \text{式 [EN5]}$$

【0212】

S423の後、S430に進む。

【0213】

S430において、暗号値算出部413は、公開鍵PKとパターン P_i と平文データMとS421で選択された整数値 ρ とS423で算出された複数の整数値とを用いて、複数の暗号値を算出する。

以下に、複数の暗号値を算出する複数の算出式[EN6]を示す。

【0214】

【数27】

$$C_0 := ME^\rho, \{C_{1,j} := H_i^\rho Z_{1,j}, C'_{1,j} := H'_i{}^\rho Z'_{1,j}\}_{j \in W(P_i)}, C_2 := F^\rho Z_2, \\ C_3 := \left(V \prod_{j \in D(P_i)} H_j^{p_j} \right)^\rho Z_3, C'_3 := \left(V' \prod_{j \in D(P_i)} H'_j{}^{p_j} \right)^\rho Z'_3 \quad \text{式 [EN6]}$$

ここで、

$$C_0, \{C_{1,j}, C'_{1,j}\}, C_2, C_3, C'_3 : \text{暗号値}$$

である。

【0215】

S430の後、S440に進む。

【0216】

S440において、暗号文生成部414は、S422で判定されたワイルドカード階層値WとS430で算出された複数の暗号値とを用いてユーザi用の暗号文データCTを生成し、生成した暗号文データCTを暗号化記憶部490に記憶する。

以下に、暗号文CTを表す式[EN7]を示す。

【0217】

10

20

30

40

【数 2 8】

$$CT = \left[W(P_i), C_0, \left\{ C_{1,j}, C'_{1,j} \right\}_{j \in W(P_i)}, C_2, C_3, C'_3 \right] \quad \text{式 [EN 7]}$$

ここで、

CT : ユーザ i 用の暗号文データ

である。

10

【0 2 1 8】

また、暗号文生成部 4 1 4 は、生成した暗号文データ CT を出力する。例えば、暗号文生成部 4 1 4 は、暗号文データ CT を共有サーバ（図示省略）に記憶する。

S 4 4 0 により、暗号化方法の処理は終了する。

【0 2 1 9】

上記の暗号化方法において、平文データ M はペアリング群 G_T （図 1 1 の S 1 2 0 参照）の要素であるものとする。

但し、平文データ M がペアリング群 G_T の要素でない場合、ハイブリッド暗号方式を用いればよい。ハイブリッド暗号方式において、平文データ M はセッション鍵を用いて共通鍵暗号方式で暗号化する。そして、平文データ M をセッション鍵に置き換えて上記暗号化方法の処理を実行する。

20

【0 2 2 0】

図 1 5 は、実施の形態 1 における復号装置 3 0 0 による復号方法を示すフローチャートである。

復号装置 3 0 0 の復号処理部 3 1 0 が実行する復号方法の処理の流れについて、図 1 5 に基づいて説明する。

【0 2 2 1】

S 5 1 0 において、復号入力部 3 1 1 は、公開鍵 PK と暗号文データ CT とを入力装置、共有サーバ（図示省略）または復号記憶部 3 9 0 から入力する。

30

復号入力部 3 1 1 は、ユーザ i のユーザ秘密鍵 $SK(I D_i)$ とユーザ識別子 $I D_i$ とを入力装置または復号記憶部 3 9 0 から入力する。ユーザ i は、暗号文データ CT を復号するユーザであって、この復号装置 3 0 0 を使用するユーザである。

S 5 1 0 の後、S 5 2 0 に進む。

【0 2 2 2】

S 5 2 0 において、復号前処理部 3 1 2 は、ユーザ識別子 $I D_i$ に含まれる要素を整数値群 Z_n （0 から $n - 1$ の整数値）に含まれるいずれかの整数値に変換する。

変換方法は、S 2 2 0（図 1 2 参照）と同様である。

S 5 2 0 の後、S 5 2 1 に進む。

【0 2 2 3】

S 5 2 1 において、復号前処理部 3 1 2 は、ユーザ識別子 $I D_i$ に基づいて非空欄階層値 D を判定する。

40

判定方法は、S 2 4 0（図 1 2 参照）と同様である。

S 5 2 1 の後、S 5 3 0 に進む。

【0 2 2 4】

S 5 3 0 において、復号部 3 1 3 は、暗号文データ CT とユーザ識別子 $I D_i$ と S 5 2 1 で判定した非空欄階層値 D とを用いて、複数の作業値を算出する。

以下に、複数の作業値を算出する複数の算出式 [D E 1] を示す。

【0 2 2 5】

【数 2 9】

$$\tilde{C}_3 := C_3 \prod_{j \in W(P_i) \cap D(ID_i)} C_{1,j}^{I_j}, \quad \tilde{C}'_3 := C'_3 \prod_{j \in W(P_i) \cap D(ID_i)} C'_{1,j}^{I_j} \quad \text{式 [DE 1]}$$

ここで、

$\tilde{C}_3, \tilde{C}'_3$: 作業値

である。

10

【0 2 2 6】

S 5 3 0 の後、S 5 4 0 に進む。

【0 2 2 7】

S 5 4 0 において、復号部 3 1 3 は、暗号文データ C T とユーザ秘密鍵 S K (I D_i) と公開鍵 P K に含まれる写像の関数 e と S 5 3 0 で算出した複数の作業値とを用いて平文データ M を算出する。

以下に、平文データ M を算出する算出式 [DE 2] を示す。

【0 2 2 8】

【数 3 0】

20

$$\tilde{M} := C_0 \frac{e(a_1, \tilde{C}_3) e(a'_1, \tilde{C}'_3)}{e(a_0, C_2)} \quad \text{式 [DE 2]}$$

ここで、

$\tilde{M}$: 復号した平文データ M

である。

30

【0 2 2 9】

復号部 3 1 3 は、算出した平文データ M を出力する。例えば、復号部 3 1 3 は、平文データ M を表示装置に表示する。

S 5 4 0 により、復号方法は終了する。

【0 2 3 0】

階層型 I D ベース暗号システム 1 0 0 において、平文データ M の暗号化に使用されたパターン P に該当する正当なユーザであれば、自分のユーザ秘密鍵 S K とユーザ識別子 I D とを用いて暗号化データ C T を復号することができる。

パターン P に含まれる複数の要素 p のうちユーザ識別子 I D の非空欄階層 (≠ φ) に対応する要素 p_j がユーザ識別子 I D の要素 I_j またはワイルドカード値「*」であり、復号処理 (図 1 5 の S 5 3 0) でワイルドカード値「*」がユーザ識別子 I D の要素 I_j で「焼き直し」されるからである。

40

【0 2 3 1】

一方、パターン P に該当するユーザ以外の不正なユーザは、自分のユーザ秘密鍵 S K とユーザ識別子 I D とを用いて暗号化データ C T を復号することができない。

復号処理でワイルドカード値「*」が不正なユーザ識別子 I D の要素 I_j で「焼き直し」されるからである。

【0 2 3 2】

以下に、暗号文データ C T を復号して得られる平文データ M と暗号化する前の平文データ M との関係式を示す。

50

【0233】

【数31】

$$\begin{aligned}
\tilde{M} &:= C_0 \frac{e(a_1, \tilde{C}_3) e(a'_1, \tilde{C}'_3)}{e(a_0, C_2)} \\
&= ME^\rho \frac{e(g^r, \left(V \prod_{j \in D(ID)} H_j^{I_j} \right)^\rho Z_3) \cdot e(g^{r'}, \left(V' \prod_{j \in D(ID)} H'_j{}^{I_j} \right)^\rho Z'_3)}{e(w \left(v \prod_{j \in D(ID)} h_j^{I_j} \right)^r \left(v' \prod_{j \in D(ID)} h'_j{}^{I_j} \right)^{r'}, G^\rho Z_2)} \\
&= Me(g, w)^\rho \frac{e(g^r, \left(v \prod_{j \in D(ID)} h_j^{I_j} \right)^\rho) \cdot e(g^{r'}, \left(v' \prod_{j \in D(ID)} h'_j{}^{I_j} \right)^\rho)}{e(w \left(v \prod_{j \in D(ID)} h_j^{I_j} \right)^r \left(v' \prod_{j \in D(ID)} h'_j{}^{I_j} \right)^{r'}, g^\rho)} \\
&= Me(g, w)^\rho \frac{e(g^r, \left(v \prod_{j \in D(ID)} h_j^{I_j} \right)^\rho) \cdot e(g^{r'}, \left(v' \prod_{j \in D(ID)} h'_j{}^{I_j} \right)^\rho)}{e(w, g^\rho) \cdot e\left(v \prod_{j \in D(ID)} h_j^{I_j} \right)^r, g^\rho \cdot e\left(v' \prod_{j \in D(ID)} h'_j{}^{I_j} \right)^{r'}, g^\rho)} \\
&= M
\end{aligned}$$

【0234】

一行目の式は、上記式「DE2」（図15のS540参照）である。

二行目の式は、一行目の右辺を上記式「DE1」（図15のS530参照）に基づいて展開した式である。

三行目の式は、二行目の式を以下に示すペアリング群の（性質1）に基づいて展開した式である。

四行目の式は、三行目の式の分母を分解した式である。

そして、四行目の式の分母と分子とで共通項を消去することにより平文データMが得られる。

【0235】

以下に、ペアリング群の性質（1）を示す。

【0236】

【数32】

性質（1）：任意の $x_p \in G_p$, $y_q \in G_q$ に対し、 $e(x_p, y_q) = 1$

【0237】

階層型IDベース暗号システム100は、暗号文の匿名性を確保することができる。なお、ここでいう匿名性とは、非特許文献5のANON-SIDで定義されるような安全性

10

20

30

40

50

のことをいう。言い換えれば、暗号文からワイルドカード箇所を除く要素 p_j すなわちユーザ識別子に関する情報が漏洩しないという性質である。

【0238】

また、暗号文の秘匿性を確保することができる。なお、ここでいう秘匿性とは、非特許文献5のIND-sIDで定義されるような安全性のことをいう。言い換えれば、暗号文から平文に関する情報が漏洩しないという性質である。

【0239】

上記の匿名性および秘匿性については、暗号分野で一般的なシミュレーションベースの安全性証明によって示される。その際の数論仮定は、非特許文献5に記載の仮定と同じである。当業者であればその安全性について理解でき、必要であれば安全性証明を再現できるものとする。

10

【0240】

本実施の形態では対称ペアリングを用いて構成する方法を説明したが、これを非対称ペアリングを用いる構成に拡張することは、当業者であれば容易に理解し得ることである。

【0241】

本実施の形態によれば、ワイルドカード対応の匿名性階層型IDベース暗号方式を実現することができる。すなわち、階層内のある層に属する全てのユーザに対してユーザ毎に暗号文を生成する必要がなく、1つの暗号文を生成すればよい。

これにより、暗号文のサイズ（数）を低減することができる。

【0242】

20

さらに、復号演算（図15のS540参照）において、ペアリング e の演算回数を階層数に比例した回数ではなく、一定回数（具体的には3回）にすることができる。

これは、暗号文の構成要素の中で階層数に比例する要素を除去したためである。

これにより、大企業や官公庁のように大きな階層を持つ組織においても高速な復号演算を実現することができる。

【0243】

さらに、中間の階層に対応付けてユーザ識別子に空欄「 ϕ 」をおくことができる。

これにより、図2に示した田中さんのように通常の階層構造から外れるようなユーザにも柔軟に対応することができる。

つまり、特異な階層構造にも柔軟に対応できるという効果がある。

30

【0244】

実施の形態において、セットアップ装置200は、セットアップ装置（セットアップ処理部210）と鍵生成装置（鍵生成処理部220）とに分割しても構わない。

また、復号装置300は、復号装置（復号処理部310）と鍵委譲装置（鍵委譲処理部320）とに分割しても構わない。

【0245】

図16は、実施の形態における階層型IDベース暗号システム100のハードウェア資源の一例を示す図である。

図16において、セットアップ装置200、復号装置300、暗号化装置400および検索装置500（実施の形態3参照）は、CPU901（Central Processing Unit）を備えている。CPU901は、バス902を介してROM903、RAM904、通信ボード905、ディスプレイ装置911、キーボード912、マウス913、ドライブ装置914、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。ドライブ装置914は、FD（Flexible Disk Drive）、CD（Compact Disc）、DVD（Digital Versatile Disc）などの記憶媒体を読み書きする装置である。

40

【0246】

通信ボード905は、有線または無線で、LAN（Local Area Network）、インターネット、電話回線などの通信網に接続している。

【0247】

50

磁気ディスク装置 920 には、OS 921（オペレーティングシステム）、プログラム群 922、ファイル群 923 が記憶されている。

【0248】

プログラム群 922 には、実施の形態において「～部」として説明する機能を実行するプログラムが含まれる。プログラムは、CPU 901 により読み出され実行される。すなわち、プログラムは、「～部」としてコンピュータを機能させるものであり、また「～部」の手順や方法をコンピュータに実行させるものである。

【0249】

ファイル群 923 には、実施の形態において説明する「～部」で使用される各種データ（入力、出力、判定結果、計算結果、処理結果など）が含まれる。

10

【0250】

実施の形態において構成図およびフローチャートに含まれている矢印は主としてデータや信号の入出力を示す。

【0251】

実施の形態において「～部」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」として説明するものは、ファームウェア、ソフトウェア、ハードウェアまたはこれらの組み合わせのいずれで実装されても構わない。

【0252】

実施の形態 2.

20

合成数 $n (=pq)$ を位数とするペアリング群を用いる代わりに、素数 p を位数とするペアリング群の直積を用いる形態について説明する。

以下、実施の形態 1 と異なる事項について主に説明する。説明を省略する事項については実施の形態 1 と同様である。

【0253】

以下、合成数を位数とするペアリング群のことを「合成数位数のペアリング群」といい、素数を位数とするペアリング群のことを「素数位数のペアリング群」という。

【0254】

素数位数 p のペアリング群（非対称ペアリング群）の直積から成る直積群は、式（2-1）で定義される。

30

【0255】

【数 3 3】

$$G^{\wedge} = G_{-1} \times G_{-1}, H^{\wedge} = G_{-2} \times G_{-2}, G_T^{\wedge} = G_{-t} \quad \text{式 (2-1)}$$

ここで、

G_{-1}, G_{-2}, G_{-t} は、素数位数 p の非対称ペアリング群であり、

$e : G_{-1} \times G_{-2} \rightarrow G_{-t}$ は、 G_{-1}, G_{-2}, G_{-t} 上で定義される

非対称ペアリング

である。

40

また、

$G^{\wedge}, H^{\wedge}, G_T^{\wedge}$ は直積群

である。

【0256】

直積群の一部を構成する部分群は式（2-2）で定義される。

【0257】

【数 3 4】

$$G_1^\wedge = \langle (g_1, g_1^x) \rangle, \quad G_2^\wedge = \langle (g_2, g_2^y) \rangle, \quad H_1^\wedge = \langle (h_1^{-y}, h_1) \rangle, \quad H_2^\wedge = \langle (h_2^{-x}, h_2) \rangle$$

式 (2-2)

ここで、

 $G_1^\wedge, G_2^\wedge, H_1^\wedge, H_2^\wedge$: 部分群、

$$g_1, g_2 \xleftarrow{U} G_1, \quad h_1, h_2 \xleftarrow{U} G_2,$$

$$x, y \xleftarrow{U} Z_p,$$

$$x - y \neq 0,$$

 $\langle g \rangle$: g で生成される群

である。

【0 2 5 8】

ペアリング e は式 (2-3) で定義される。

【0 2 5 9】

【数 3 5】

$$e^\wedge((g, g'), (h, h')) = e(g, h) e(g', h') \quad \text{式 (2-3)}$$

ここで、

 g, g' は群 G_1 の任意の要素であり、 h, h' は群 G_2 の任意の要素である。

【0 2 6 0】

上記の定義において性質 (2) が成り立つ。

【0 2 6 1】

【数 3 6】

性質 (2) : 任意の $x_1 \in G_1^\wedge$, $y_2 \in H_2^\wedge$ に対し、 $e^\wedge(x_1, y_2) = 1$ であり、
 任意の $x_2 \in G_2^\wedge$, $y_1 \in H_1^\wedge$ に対し、 $e^\wedge(x_2, y_1) = 1$ である。

【0 2 6 2】

この性質 (2) は次のように確かめることができる。

【0 2 6 3】

【数 3 7】

a, b をある整数として、 $x_1 = (g_1^a, g_1^{ax})$, $y_2 = (h_2^{-xb}, h_2^b)$ と表すことができるから、以下の通りである。

$$\begin{aligned} e^\wedge(x_1, y_2) &= e^\wedge((g_1^a, g_1^{ax}), (h_2^{-xb}, h_2^b)) \\ &= e(g_1^a, h_2^{-xb}) e(g_1^{ax}, h_2^b) \\ &= 1 \end{aligned}$$

【0 2 6 4】

この性質 (2) は、実施の形態 1 で説明した性質 (1) と同等の性質である。

したがって、素数位数 p のペアリング群の直積を用いて、階層型 ID ベース暗号システム 100 を構成することができる。

つまり、実施の形態 1 で説明した各群を以下のように上記の各群に置き換えることにより、階層型 ID ベース暗号システム 100 を構成することができる。

【0265】

【数 38】

群 $G \rightarrow$ 群 $\hat{G}$, $\hat{H}$ 、
 群 $G_p \rightarrow$ 群 $\hat{G}_1$, $\hat{H}_1$ 、
 群 $G_q \rightarrow$ 群 $\hat{G}_2$, $\hat{H}_2$ 、
 群 $G_T \rightarrow$ 群 $\hat{G}_T$ 、
 ペアリング $e \rightarrow$ ペアリング $\hat{e}$

10

【0266】

ここでは、素数位数のペアリング群の直積を用いる場合の一例を示した。

但し、合成数位数のペアリング群を素数位数のペアリング群に変換する変換方法を用いても構わない。このような変換方法は、例えば、非特許文献 6 に開示されている。

【0267】

本実施の形態によれば、合成数位数のペアリング群ではなく、素数位数のペアリング群を用いてワイルドカード対応の匿名性階層型 ID ベース暗号方式を実現することができる。

20

通常、素数位数のペアリング群は合成数位数のペアリング群よりも小さいビットサイズで同等の安全性を実現できる。

したがって、暗号文や秘密鍵のサイズを実施の形態 1 よりも小さくすることができる。

【0268】

また、ビットサイズが小さいほど群演算の時間は短縮される。つまり、演算速度を実施の形態 1 よりも向上させることができる。

【0269】

また、実施の形態 1 と同様に、復号演算で行うペアリング演算の回数を階層数に比例した回数ではなく、一定の回数にすることができる。

30

【0270】

実施の形態 3.

実施の形態 1、2 で説明した「ワイルドカード対応の匿名性階層型 ID ベース暗号方式」を応用して「グループ共有型公開鍵秘匿検索方式」について説明する。

以下、実施の形態 1、2 と異なる事項について主に説明する。説明を省略する事項については実施の形態 1、2 と同様である。

【0271】

図 17 は、実施の形態 3 における公開鍵秘匿検索システム 110 の構成図である。

実施の形態 3 における公開鍵秘匿検索システム 110 の構成について、図 17 に基づいて説明する。

40

【0272】

公開鍵秘匿検索システム 110 は、実施の形態 1 で説明した階層型 ID ベース暗号システム 100 の構成（図 1 参照）に加えて、検索装置 500 を備える。

【0273】

検索装置 500 は、暗号化装置 400 により生成された複数の暗号文データ CT を記憶した検索記憶部 590（暗号文記憶部の一例）を備える。

【0274】

検索装置 500 は、検索クエリ QK を入力し、入力した検索クエリ QK を用いて検索記憶部 590 を検索し、検索クエリ QK に該当する暗号文データ CT を出力する。

50

【0275】

復号装置300は、検索装置500によって検索された暗号文データCTを復号し、平文データMを出力する。

【0276】

図18は、実施の形態3における復号装置300の概要図である。

実施の形態3における復号装置300の概要について、図18に基づいて説明する。

【0277】

復号装置300は、実施の形態1で説明した構成（図7参照）に加えて、クエリ生成処理部330を備える。

【0278】

クエリ生成処理部330は、クエリ生成入力部、クエリ生成前処理部、クエリ鍵値算出部およびクエリ生成部（図示省略）を備える。

【0279】

クエリ生成処理部330は、公開鍵PKとユーザiのユーザ秘密鍵SK(ID_i)とユーザiのユーザ識別子ID_iとキーワードKWとを入力し、検索クエリQK(ID_i, KW)を出力する。

【0280】

図19は、実施の形態3における検索装置500の概要図である。

実施の形態3における検索装置500の概要について、図19に基づいて説明する。

【0281】

検索装置500は、検索処理部510と検索記憶部590とを備える。

【0282】

検索処理部510は、公開鍵PKと検索クエリQK(ID_i, KW)とを入力し、検索記憶部590に記憶された暗号文データCTを検索し、検索クエリQK(ID_i, KW)に該当する暗号文データCTを出力する。

【0283】

検索記憶部590は、検索装置500で使用するデータを記憶する記憶部である。

公開鍵PK、検索クエリQK(ID_i, KW)、暗号文データCTは検索記憶部590に記憶されるデータの一例である。

【0284】

図20は、実施の形態3における検索装置500の機能構成図である。

実施の形態3における検索装置500の機能構成について、図20に基づいて説明する。

【0285】

検索装置500は、前述の通り、検索処理部510と検索記憶部590とを備える。

【0286】

検索記憶部590は、複数の暗号文データCTと複数の暗号文データCTWとを予め記憶する。

【0287】

暗号文データCTWは、暗号化装置400（図10参照）によって以下のように生成される。

暗号値算出部413は、特定の平文データMWを暗号化して平文暗号値CW₀を算出する。

暗号化入力部411は、前記暗号文データCTの検索に用いるキーワードKWを入力する。

暗号値算出部413は、前記パターンPを含むと共に前記キーワードKWを第K+1階層を識別する階層識別子として含むパターンPWを用いてワイルドカード暗号値CW₁と識別暗号値CW₃とを算出する。

暗号文生成部414は、算出された平文暗号値CW₀とワイルドカード暗号値CW₁と識別暗号値CW₃とを含んだ暗号文データCTWを生成し、生成した暗号文データCTW

10

20

30

40

50

を前記暗号文データCTに対応付けて出力する。

【0288】

図20に戻り、検索装置500の説明を続ける。

【0289】

検索処理部510は、検索クエリ入力部511と検索部512と検索結果出力部513とを備える。

【0290】

検索クエリ入力部511は、検索クエリ入力処理を行う。

例えば、検索クエリ入力部511は、検索クエリQKとワイルドカード階層値Wとを入力する。

10

【0291】

検索クエリQKは、復号装置300（図18参照）によって以下のように生成される。

クエリ生成処理部330のクエリ生成入力部（図示省略）は、前記ユーザ識別子IDと前記キーワードKWとを入力する（クエリ生成入力）。

クエリ生成処理部330のクエリ鍵値算出部（図示省略）は、入力されたユーザ識別子IDとキーワードKWとを用いて前記平文暗号値CW₀の復号に用いる鍵値aW₀を算出する（クエリ鍵値算出処理）。

クエリ生成処理部330のクエリ生成部（図示省略）は、算出された鍵値aW₀と前記ユーザ識別子IDとを含んだ検索クエリQKを生成し、生成した検索クエリQKを出力する（検索クエリ生成処理）。

20

【0292】

図20に戻り、検索装置500の説明を続ける。

【0293】

検索部512は、検索記憶部590から暗号文データCTWを選択する。

検索部512は、入力されたワイルドカード階層値Wに基づいて入力された検索クエリQKに含まれるユーザ識別子IDから前記ワイルドカード階層の階層識別子をワイルドカード識別子として抽出する。

検索部512は、抽出したワイルドカード識別子と選択した暗号文データCTWに含まれるワイルドカード暗号値CW₁と識別暗号値CW₃と入力された検索クエリQKに含まれる鍵値aW₀とを用いて、選択した暗号文データCTWに含まれる平文暗号値CW₀を復号する。

30

検索部512は、前記平文暗号値CW₀を復号して得られた復号データが前記平文データMWと一致するか否かを判定する。

検索部512は、前記復号データが前記平文データMWと一致した場合、選択した暗号文データCTWに対応する暗号文データCTを検索記憶部590から取得する。

【0294】

検索結果出力部513は、取得された暗号文データCTを入力された検索クエリQKに対する検索結果として出力する。

【0295】

図21は、実施の形態3における階層型IDベース暗号システム100の階層構造の一例を示す図である。

40

図22は、実施の形態3における階層型IDベース暗号システム100のパターンPWの一例を示す図である。

【0296】

図21に示すように階層構造にはキーワード用の階層（第5階層）が含まれ、図22に示すようにパターンPWにはパターンPと暗号文データCTの検索用のキーワードKWとが含まれる。

【0297】

図23は、実施の形態3における暗号化装置400による暗号化方法を示すフローチャートである。

50

実施の形態 3 における暗号化方法の処理の流れについて、図 2 3 に基づいて説明する。

【0298】

S 4 1 1 において、暗号化入力部 4 1 1 は、S 4 1 0（図 1 4 参照）と同様に、公開鍵 PK とユーザ i 用のパターン PW_i と平文データ M とを入力する。

S 4 1 1 の後、S 4 2 0 に進む。

【0299】

S 4 2 0 – S 4 4 0 において、暗号処理部 4 1 0 は、パターン PW_i に含まれるパターン P_i を用いてユーザ i 用の暗号文データ CT を生成する（図 1 4 参照）。

S 4 4 0 の後、S 4 5 0 に進む。

【0300】

S 4 5 0 において、暗号化前処理部 4 1 2 は、暗号文データ CT を入力として所定のハッシュ関数 h を計算し、暗号文データ CT のハッシュ値 $h(CT)$ を算出する。

ハッシュ値 $h(CT)$ は暗号文データ CT を群 G_T の要素に写した値である。例えば、ハッシュ値 $h(CT)$ は、暗号文データ CT をビット列として入力した場合のハッシュ関数 SHA-1 の出力値である。

S 4 5 0 の後、S 4 6 0 に進む。

【0301】

S 4 6 0 – S 4 8 0 において、暗号処理部 4 1 0 は、S 4 5 0 で算出されたハッシュ値 $h(CT)$ を平文データ MW として S 4 2 0 – S 4 4 0 と同様に、パターン PW_i を用いてユーザ i 用の暗号文データ CTW を生成する。このとき、キーワード KW に対応する階層は「識別階層」として扱う。

S 4 8 0 の後、S 4 9 0 に進む。

【0302】

S 4 9 0 において、暗号文生成部 4 1 4 は、S 4 4 0 で生成した暗号文データ CT と S 4 8 0 で生成した暗号文 CTW とを含んだ暗号文データ CT_w を生成し、生成した暗号文データ CT_w を出力する。

S 4 9 0 により、暗号化方法の処理は終了する。

【0303】

図 2 4 は、実施の形態 3 における復号装置 3 0 0 によるクエリ生成方法を示すフローチャートである。

復号装置 3 0 0 のクエリ生成処理部 3 3 0 が実行するクエリ生成方法の処理の流れについて、図 2 4 に基づいて説明する。

【0304】

S 6 1 0 において、クエリ生成処理部 3 3 0 は、公開鍵 PK とユーザ i のユーザ秘密鍵 SK (ID_i) とユーザ i のユーザ識別子 ID_i とキーワード KW とを入力する。

S 6 1 0 の後、S 6 2 0 に進む。

【0305】

S 6 2 0 – S 6 5 0 において、クエリ生成処理部 3 3 0 は、ユーザ識別子 ID_i にキーワード KW を加えたデータをユーザ j のユーザ識別子 ID_j として扱い、鍵委譲処理部 3 2 0 と同様に（図 1 3 の S 3 2 0 – S 3 5 0 参照）、複数の復号鍵値を算出する。

S 6 5 0 の後、S 6 6 0 に進む。

【0306】

S 6 6 0 において、クエリ生成処理部 3 3 0 は、ユーザ i のユーザ識別子 ID_i と S 6 5 0 で算出した複数の復号鍵値とを含んだ検索クエリ QK を生成し、生成した検索クエリ QK を出力する。

S 6 6 0 により、クエリ生成方法の処理は終了する。

【0307】

図 2 5 は、実施の形態 3 における検索装置 5 0 0 による検索方法を示すフローチャートである。

検索装置 5 0 0 の検索処理部 5 1 0 が実行する検索方法の処理の流れについて、図 2 5

10

20

30

40

50

に基づいて説明する。

【0308】

S710において、検索クエリ入力部511は、検索クエリQKと公開鍵PKとを入力する。

S710の後、S711に進む。

【0309】

S711において、検索クエリ入力部511は、検索記憶部590から未処理の暗号文データCT_wを順番にまたはランダムに一つ選択する。

S712の後、S720に進む。

【0310】

S720～S740において、検索部512は、公開鍵PKと検索クエリQKに含まれる復号鍵値と検索クエリQKに含まれるユーザ識別子ID_iと暗号文データCT_wに含まれる暗号文データCT_wとを用いて、平文データMWを算出する。

平文データMWの算出方法は、復号方法（図15のS520～S540参照）と同様である。

S740の後、S750に進む。

【0311】

S750において、検索部512は、暗号文データCT_wに含まれる暗号文データCTのハッシュ値h(CT)を算出する。

ハッシュ値h(CT)の算出方法は、S450（図23参照）と同様である。

S750の後、S760に進む。

【0312】

S760において、検索部512は、S740で算出した平文データMWとS750で算出したハッシュ値h(CT)とを比較する。

平文データMWとハッシュ値h(CT)とが一致する場合（YES）、S770に進む。

平文データMWとハッシュ値h(CT)とが一致しない場合（NO）、S711に戻る。

【0313】

S770において、検索部512は、暗号文データCT_wに含まれる暗号文データCTを出力する。

S770により、検索方法の処理は終了する。

【0314】

S770で出力された暗号文データCTは、実施の形態1で説明した復号方法（図15参照）により復号される。

【0315】

公開鍵秘匿検索システム110は、キーワードを秘匿したままキーワード検索を行うことができる。なぜならば、検索される暗号文が秘匿性に加えて匿名性を有しており、暗号文を見てもキーワードについて何ら情報を得ることが出来ないからである。

【0316】

また、ワイルドカードの使用に対応しているため、実施の形態1と同様にグループ内で暗号文を共有することができる。

【0317】

検索キーワードは複数設けても構わない。つまり、キーワードに対応する階層を複数設けても構わない。

この場合、暗号文データCT_wは検索キーワードと同じ数の暗号文データCT_wを含み、少なくともいずれかの暗号文データCT_wについてハッシュ値h(CT)が一致した場合に検索にヒットしたと判定し、暗号文データCTを出力する。但し、全ての暗号文データCT_wについてハッシュ値h(CT)が一致した場合に検索にヒットしたと判定しても構わない。さらに、暗号文データCT_wの順番、つまり、検索キーワードの階層順序が一

10

20

30

40

50

致した場合に検索にヒットしたと判定しても構わない。

【0318】

暗号化処理（図23参照）および検索方法（図25参照）において、ハッシュ値 h （CT）の代わりに検索定数（例えば、定数0）を平文データMWとして扱ってもよい。つまり、検索時に復号された値が検索定数と一致した場合に検索にヒットしたと判定する。

これにより、暗号文データCTと暗号文データCTW（暗号化キーワード）とを一緒に保持しておく必要はなくなり、別々に管理しておくことができる。したがって、データ管理の柔軟性を向上させることができる。

【0319】

本実施の形態では、検索クエリに検索ユーザのユーザ識別子を含ませる構成とした。これは、検索時に暗号文の中のワイルドカードに対応する要素を検索ユーザのユーザ識別子で「焼き直す」ためである。

しかし、「焼き直し」を必要としない場合（すなわち自分宛の暗号文のみを検索する場合）には、検索クエリにユーザ識別子を含まない構成にしてもよい。

このようにすれば、検索ユーザは検索装置に対して自らのユーザ識別子を隠したまま検索を依頼することができる。

【0320】

本実施の形態では、実施の形態1と同様に合成数位数のペアリング群を用いることもできるし、実施の形態2と同様に素数位数のペアリング群の直積を用いることもできる。

【0321】

また、より一般に、「委譲可能な秘匿ベクトル暗号」（Delegatable hidden vector encryption）を用いて「グループ共有型公開鍵秘匿検索」を実現することもできる。

ここで言う「委譲可能な秘匿ベクトル暗号」とは、IDベース暗号または属性ベース暗号などのいわゆる述語暗号（Predicate encryption）または関数型暗号（Functional encryption）である。

但し、「委譲可能な秘匿ベクトル暗号」は、鍵委譲の機能を備え、かつ暗号化のIDまたは属性としてワイルドカード相当の機能を備えているものとする。さらに、「委譲可能な秘匿ベクトル暗号」は、IDまたは属性の情報が暗号文から漏洩しない匿名性を備えているものとする。

この具体的な実現方式には、例えば非特許文献7に記載のDelegatable HVEや、非特許文献8に記載のHierarchical predicate encryptionなどがある。

それぞれの暗号方式によって具体的なアルゴリズムやパラメータ、あるいは根拠とする数論仮定は異なる。しかし、いずれの暗号方式も基本的には実施の形態1と同様にセットアップ手段、鍵生成手段、鍵委譲手段、暗号化手段および復号手段、またはそれらに類するものを含む構成となっている。このため、本実施の形態に開示した構成に準じた構成をとることにより、本実施の形態と同様に「グループ共有型公開鍵秘匿検索」を実現することができる。これは、当業者であれば容易に理解し得ることである。

【0322】

本実施の形態によれば、グループ共有型公開鍵秘匿検索を実現することができる。

【0323】

さらに、検索演算および復号演算（検索にヒットした暗号文を復号する演算）の中のペアリング演算の回数を階層数に比例せず一定回数（具体的には3回）にすることができる。

これにより、大企業や官公庁のように大きな階層を持つ組織においても高速な検索および復号を実現することができる。

【0324】

さらに、実施の形態1と同様に、ユーザ秘密鍵の生成・委譲においても、また暗号化においても、ユーザ識別子を指定する際に中間の階層部分に空欄をおくことができる。

これによって、図 2 1 に示した田中さんのように通常の階層構造から外れるようなユーザにも柔軟に対応することができる。つまり、特異な階層構造にも柔軟に対応することができる。

【0 3 2 5】

さらに、より一般に、「委譲可能な秘匿ベクトル暗号」を用いて「グループ共有型公開鍵秘匿検索」を実現することができる。これによって、グループ共有型公開鍵秘匿検索方式を実現するためのより一般的な方法を提供することができる。

【0 3 2 6】

実施の形態 4.

検索可能なユーザを追加または削除する形態について説明する。

10

以下、実施の形態 3 と異なる事項について主に説明する。説明を省略する事項については実施の形態 3 と同様である。

【0 3 2 7】

まず、検索可能なユーザを追加する形態について説明する。

【0 3 2 8】

検索可能なユーザを追加するには、追加するユーザにユーザ識別子 I D を割り当てればよい。

【0 3 2 9】

図 2 6 は、実施の形態 4 におけるユーザ識別子 I D の一例を示す図である。

例えば、採用係に高橋さんが新たに配属された場合、図 2 6 に示すように高橋さんのユーザ識別子 I D₉ を生成する。

20

採用係長は実施の形態 1 で説明した鍵委譲方法により高橋さんにユーザ秘密鍵 S K を委譲し、高橋さんは委譲されたユーザ秘密鍵 S K を用いて実施の形態 3 で説明したクエリ生成方法により検索クエリ Q K を生成する。

【0 3 3 0】

また、人事課に査定係が新たに設けられた場合、図 2 6 に示すように査定係（査定係長）のユーザ識別子 I D₁₀ を生成する。

人事課長は査定係長にユーザ秘密鍵 S K を委譲し、査定係長は委譲されたユーザ秘密鍵 S K を用いて検索クエリを生成する。また、査定係長は委譲されたユーザ秘密鍵 S K を用いて査定係の各社員にユーザ秘密鍵 S K を委譲する。

30

【0 3 3 1】

次に、検索可能なユーザを削除する形態について説明する。

【0 3 3 2】

検索可能なユーザを削除するには、検索できないユーザのリスト（削除者リスト）を作成すればよい。

【0 3 3 3】

図 2 7 は、実施の形態 4 における削除者リストの一例を示す図である。

例えば、図 2 7 に示すような削除者リストを検索装置 5 0 0 の検索記憶部 5 9 0（検索識別子記憶部の一例）に記憶しておく。

削除者リストは、検索できないユーザ（検索権限が無いユーザ）のユーザ識別子 I D（非検索識別子）の一覧を示す。

40

【0 3 3 4】

例えば、採用係の山田さんが別の部署に異動になった場合、採用係長は山田さんのユーザ識別子 I D₁₃ を検索装置 5 0 0 に入力し、削除者リストへの山田さんの登録を依頼する。検索装置 5 0 0 のユーザ管理部（図示省略）は、入力されたユーザ識別子 I D₁₃ を図 2 7 に示すように削除者リストに追加することにより、削除者リストに山田さんを登録する。

人事課の研修係が廃止になった場合、同様に、人事課長が削除者リストへの研修係の登録を依頼し、検索装置 5 0 0 のユーザ管理部が研修係のユーザ識別子 I D₃₇ を図 2 7 に示すように削除者リストに追加する。

50

【0335】

また、山田さんが採用係に再び配属になった場合、採用係長は山田さんのユーザ識別子ID₁₃を検索装置500に入力し、削除者リストからの消去を依頼する。検索装置500のユーザ管理部は、入力されたユーザ識別子ID₁₃を削除者リストから消去する。

人事課の研修係が復活した場合、同様に、人事課長が削除者リストからの消去を依頼し、検索装置500のユーザ管理部が研修係のユーザ識別子ID₃₇を削除者リストから消去する。

【0336】

このとき、他人からの虚偽の依頼を防ぐため、依頼者の電子署名の入力を要求してもよい。検索装置500のユーザ管理部は入力された電子署名を従来の署名検証方法により検証し、電子署名が正しい場合に依頼を受け付ける。

10

【0337】

図28は、実施の形態4における検索装置500の検索方法を示すフローチャートである。

実施の形態4における検索装置500の検索方法について、図28に基づいて説明する。

【0338】

実施の形態4では、実施の形態3で説明した処理（図25参照）に加えて、S712とS713とを実行する。

【0339】

20

S712において、検索クエリ入力部511は、検索クエリQKに含まれるユーザ識別子IDが削除者リストに含まれているか否かを判定する。つまり、検索クエリQKに含まれるユーザ識別子IDが削除者リストに含まれるユーザ識別子IDと一致するか否かを判定する。

ユーザ識別子IDが削除者リストに含まれている場合（YES）、検索方法の処理を終了する。

ユーザ識別子IDが削除者リストに含まれていない場合（NO）、S713に進む。

【0340】

例えば、検索クエリQKに山田さんのユーザ識別子ID₁₃が含まれている場合、図23の削除者リストには山田さんのユーザ識別子ID₁₃が含まれているため、検索方法の処理を終了する。

30

この場合、山田さんは検索装置500を用いて検索を行うことができない。

【0341】

S713において、検索クエリ入力部511は、検索クエリQKに含まれるユーザ識別子IDより上位の階層のユーザ識別子IDが削除者リストに含まれているか否かを判定する。つまり、検索クエリQKに含まれるユーザ識別子IDが削除者リスト内のユーザ識別子IDを含んでいるか否かを判定する。

ユーザ識別子IDより上位の階層のユーザ識別子が削除者リストに含まれている場合（YES）、検索方法の処理を終了する。

ユーザ識別子IDより上位の階層のユーザ識別子が削除者リストに含まれていない場合（NO）、S711に進む。

40

【0342】

例えば、検索クエリQKに研修係の社員のユーザ識別子IDが含まれている場合、図23の削除者リストには研修係のユーザ識別子ID₃₇が含まれているため、検索方法の処理を終了する。

この場合、研修係の社員は検索装置500を用いて検索を行うことができない。

【0343】

ところで、削除者リストに含まれている山田さんが検索装置500に対して検索クエリを送る際、削除されていない別のユーザの名前を騙って検索依頼をする可能性もある。

しかしその場合でも、山田さんは、採用係宛て（あるいはそれより広範囲の人事課宛て

50

や総務部宛て、全社員宛ても含む)の暗号文を検索することができない。

【0344】

例えば、山田さんが佐藤さんの名前(ユーザ識別子)を使って検索依頼した場合、山田さんが属する採用係用のパターンP₂は図22に示したように社員名の欄(第4階層)がワイルドカードになっているはずである。

したがって、検索手順の中で、暗号文の各要素のうちワイルドカードに対応する要素の「焼き直し」が行われる。山田さんは佐藤氏の名前を使っているので、暗号文のワイルドカードは佐藤さんの名前で焼き直される。

一方、山田さんが送った検索クエリの中に含まれている復号鍵dkは、山田さんの名前を使って委譲された鍵であり、名前に対応する箇所には山田さんの名前が含まれている。

このように、焼き直しに使われる名前(佐藤)と復号鍵に含まれる名前(山田)とが異なるので、仮にキーワードが一致していても、検索にヒットすることはない。

【0345】

ここでは、社員名の欄がワイルドカードになっている場合で説明したが、それ以外の欄がワイルドカードになっている場合でも同様である。

【0346】

したがって、削除されていない別のユーザの名前を使って検索依頼をしても、暗号文を検索することができない。

【0347】

なお、これを逆手にとれば、削除者リストに山田さんが含まれていても、山田さん宛ての暗号文を検索することができる。

なぜならば、山田さん用のパターン(図22のパターンP₁)にはワイルドカードが含まれていないからである。このため、暗号文の「焼き直し」が発生せず、山田さんの復号鍵dkが有効に機能する。

このようにするには、実施の形態3にも記載のように、山田さんの検索クエリの中にユーザ識別子IDを含まない構成にすればよい。

【0348】

本実施の形態は、実施の形態3と同様に、「委譲可能な秘匿ベクトル暗号」であればどの方式でも実現可能である。

【0349】

本実施の形態によれば、グループ(階層)に新たにユーザまたは下位グループを追加し、新たに追加したユーザまたは下位グループにキーワード検索を実行させることができる。

また、グループからユーザまたは下位グループを削除して、そのグループに関連するキーワード検索をできないようにすることができる。

したがって、ユーザやグループの追加および脱退に柔軟に対応することができる。

【0350】

実施の形態5.

削除者リストに含まれるユーザが個人宛ての暗号文も検索できない形態について説明する。

以下、実施の形態4と異なる事項について主に説明する。説明を省略する事項については実施の形態4と同様である。

【0351】

図29は、実施の形態5におけるユーザ識別子IDの一例を示す図である。

図29に示すように、実施の形態5では社員(ユーザの一例)を対応付ける階層を複数設ける。

例えば、山田さんのユーザ識別子ID₆には第4階層と第5階層との2つの階層に“山田”が含まれている。つまり、社員層が二重化されている。

【0352】

図30は、実施の形態5におけるパターンPの一例を示す図である。

図30に示すように、実施の形態5では社員を対応付けた複数の階層のうち少なくとも1つの階層にワイルドカード値「*」を設定する。

例えば、山田さん用のパターンP₁には、第4階層の要素としてワイルドカード値「*」が含まれている。

【0353】

これにより、ユーザの失効を実現することができる。なぜならば、そのユーザが検索できる暗号文には必ずワイルドカードが含まれ、検索クエリの中にユーザ識別子が必ず含まれるからである。また、実施の形態4で述べたように、他人の名前を使って検索クエリを出すことができないためである。

したがって、削除者リストに名前が載れば、そのユーザは検索を行うことができなくなる。つまり、そのユーザの検索権限は失効する。

10

【0354】

本実施の形態において、社員層より上位の階層を失効させる場合には、その階層を多重化すればよい。また、予め、全ての階層を多重化してもおいてもよい。

【0355】

本実施の形態によれば、ユーザまたはグループを失効させ、キーワード検索をできないようにすることができる。

したがって、ユーザやグループの失効に柔軟に対応することができる。

【符号の説明】

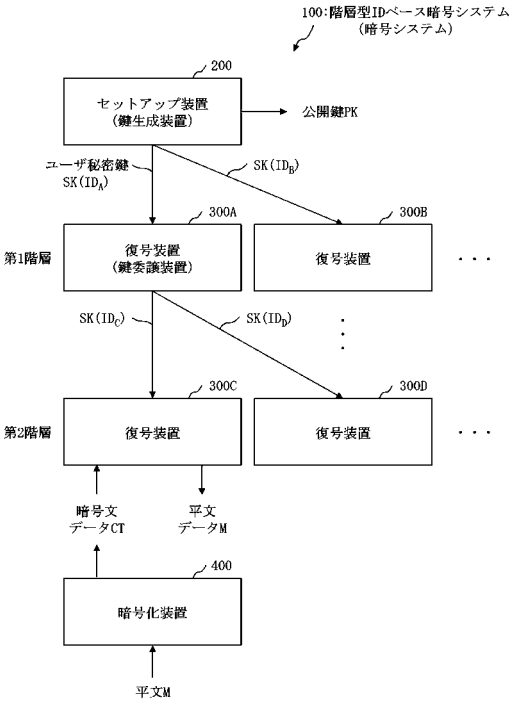
【0356】

20

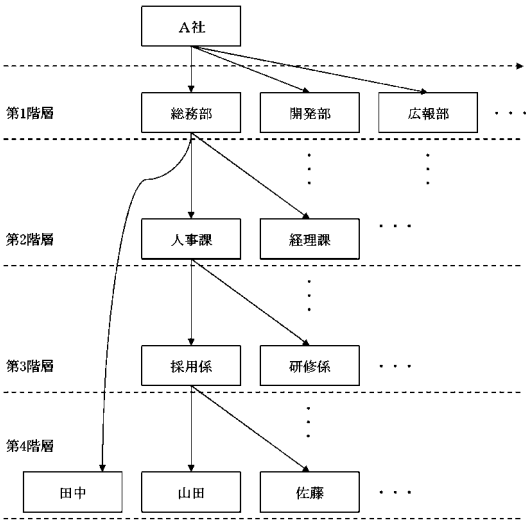
100 階層型IDベース暗号システム、110 公開鍵秘匿検索システム、200 セットアップ装置、210 セットアップ処理部、211 セットアップ入力部、212 セットアップ前処理部、213 公開鍵値算出部、214 公開鍵生成部、215 マスタ秘密鍵生成部、216 セットアップ出力部、220 鍵生成処理部、221 鍵生成入力部、222 鍵生成前処理部、223 ユーザ秘密鍵値算出部、224 ユーザ秘密鍵生成部、290 セットアップ記憶部、300 復号装置、310 復号処理部、311 復号入力部、312 復号前処理部、313 復号部、320 鍵委譲処理部、321 鍵委譲入力部、322 鍵委譲前処理部、323 委譲鍵値算出部、324 委譲鍵生成部、330 クエリ生成処理部、390 復号記憶部、400 暗号化装置、410 暗号処理部、411 暗号化入力部、412 暗号化前処理部、413 暗号値算出部、414 暗号文生成部、490 暗号化記憶部、500 検索装置、510 検索処理部、511 検索クエリ入力部、512 検索部、513 検索結果出力部、590 検索記憶部、901 CPU、902 バス、903 ROM、904 RAM、905 通信ボード、911 ディスプレイ装置、912 キーボード、913 マウス、914 ドライブ装置、920 磁気ディスク装置、921 OS、922 プログラム群、923 ファイル群。

30

【図 1】



【図 2】



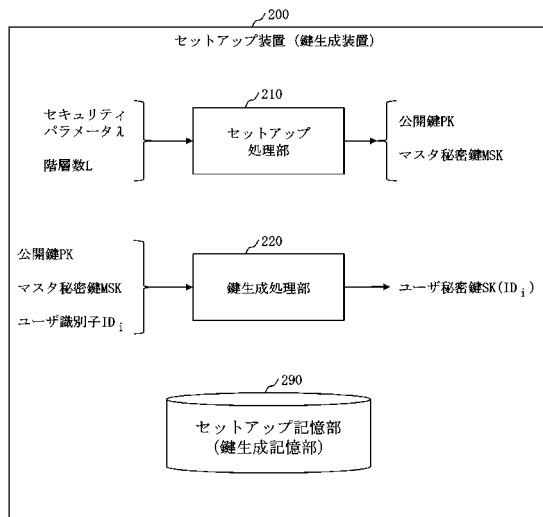
【図 3】

No.	第1階層	第2階層	第3階層	第4階層
	部 (部長)	課 (課長)	係 (係長)	社員
ID ₁	総務部	φ	φ	φ
ID ₂	総務部	人事課	φ	φ
ID ₃	総務部	経理課	φ	φ
ID ₄	総務部	人事課	研修係	φ
ID ₅	総務部	人事課	採用係	φ
ID ₆	総務部	人事課	採用係	山田
ID ₇	総務部	人事課	採用係	佐藤
ID ₈	総務部	φ	φ	田中

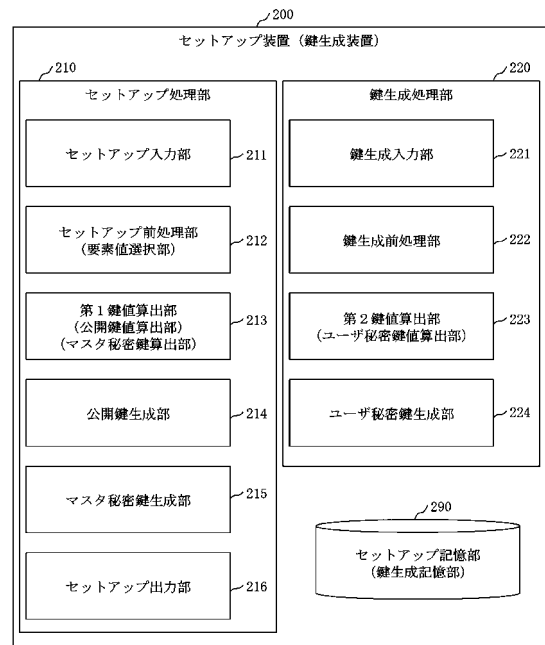
【図 4】

No.	第1階層	第2階層	第3階層	第4階層
	部 (部長)	課 (課長)	係 (係長)	社員
P ₁	総務部	人事課	採用係	山田
P ₂	総務部	人事課	採用係	*
P ₃	総務部	経理課	*	*
P ₄	総務部	人事課	φ	φ
P ₅	総務部	*	φ	φ
P ₆	*	*	φ	φ
P ₇	*	*	*	*
P ₈	総務部	φ	φ	田中

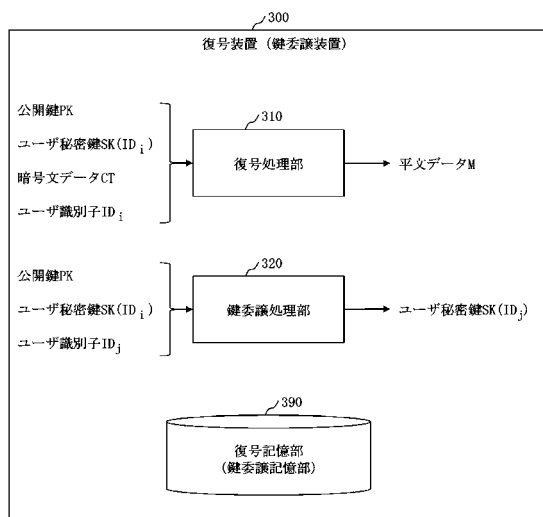
【図 5】



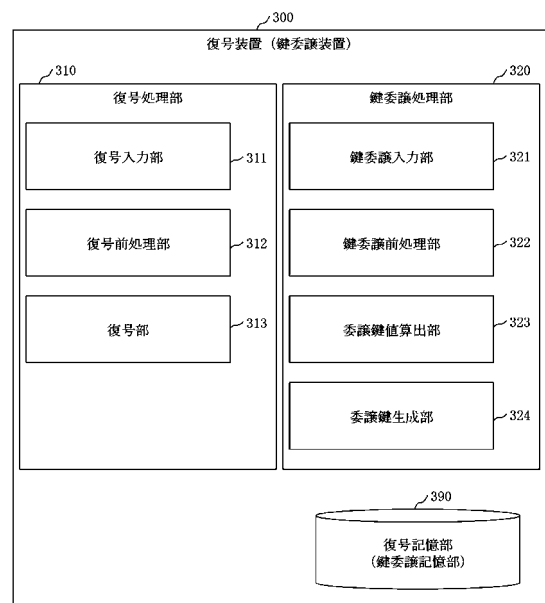
【図 6】



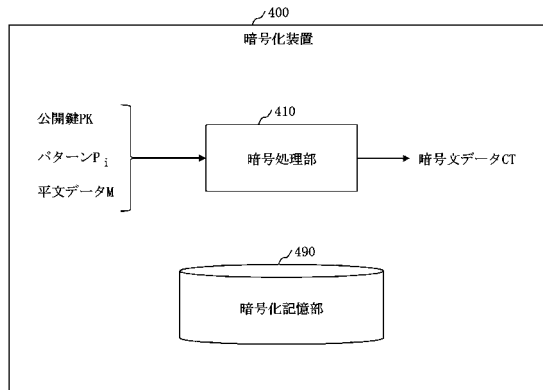
【図 7】



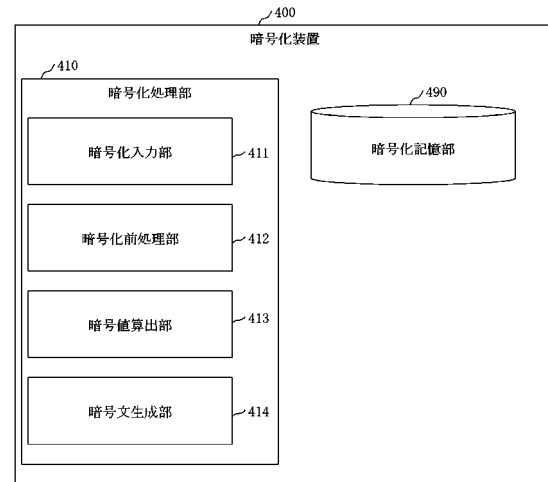
【図 8】



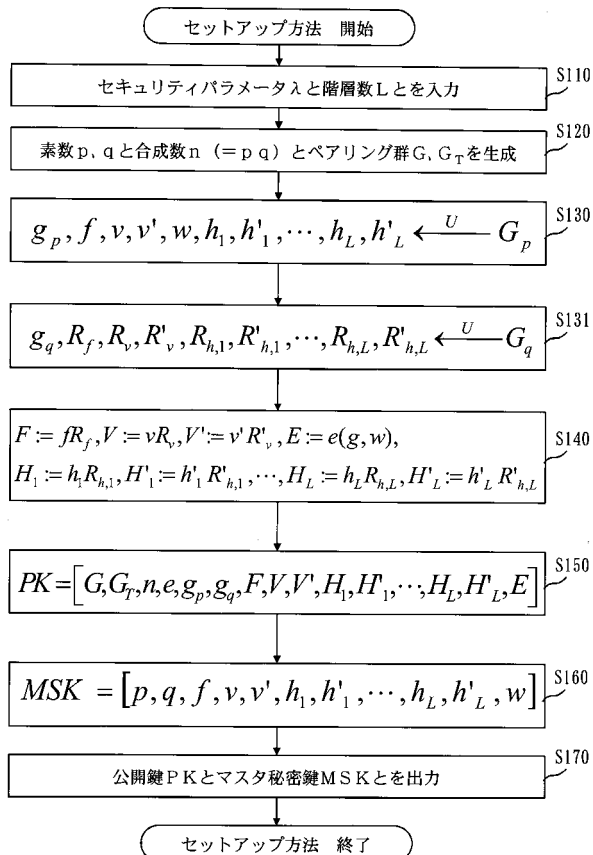
【図 9】



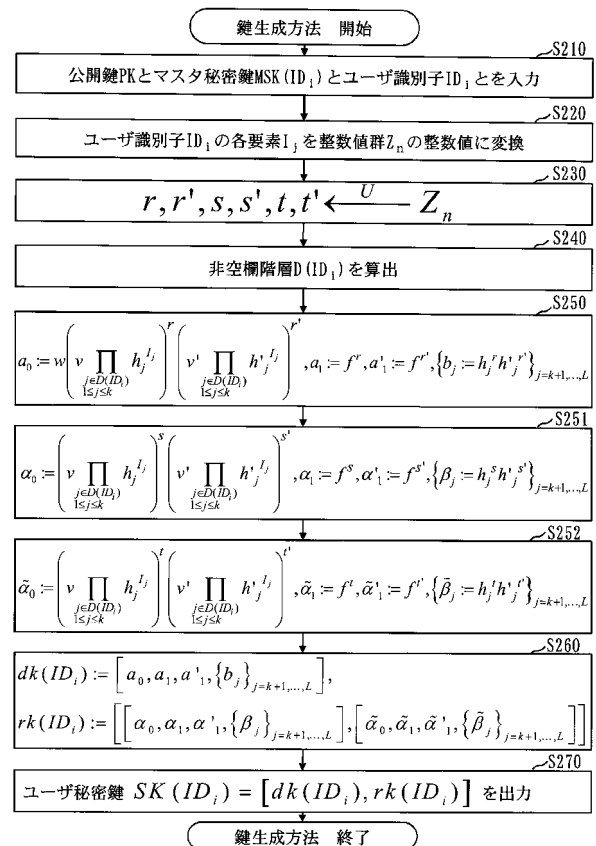
【図 10】



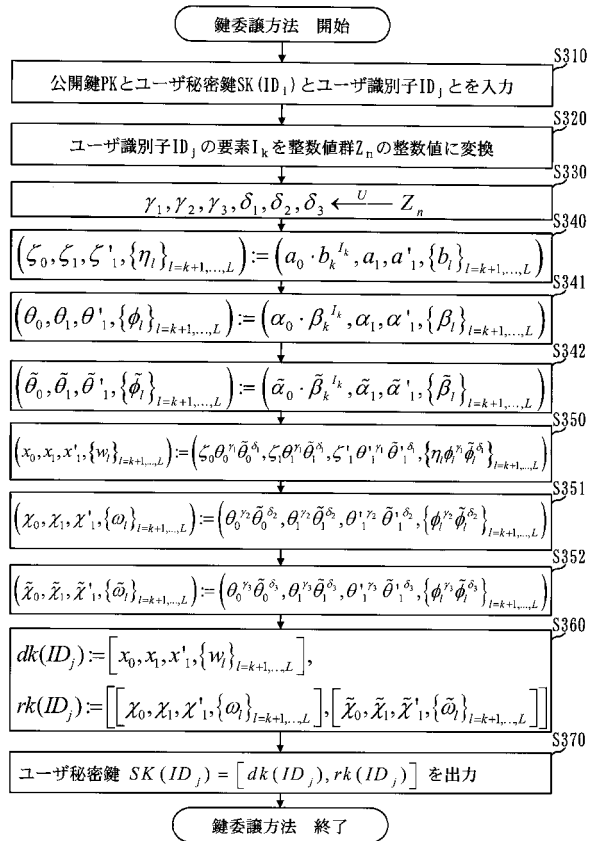
【図 11】



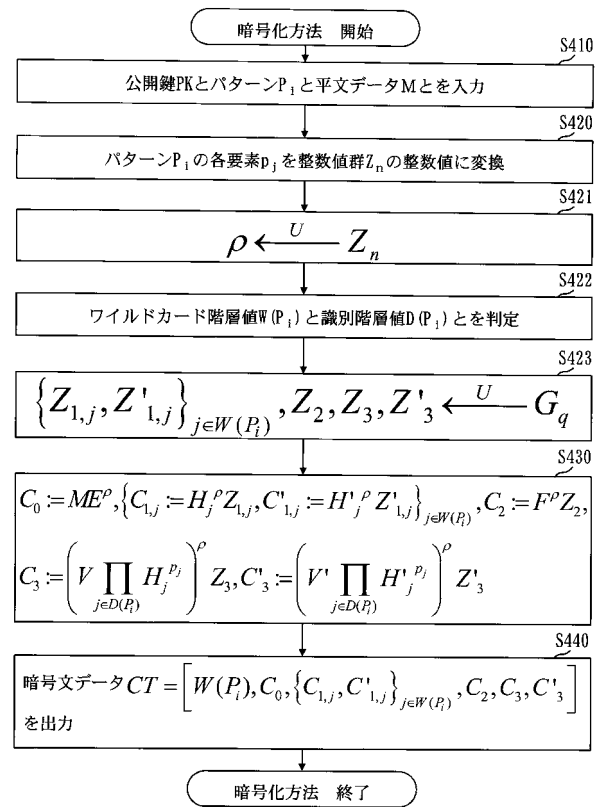
【図 12】



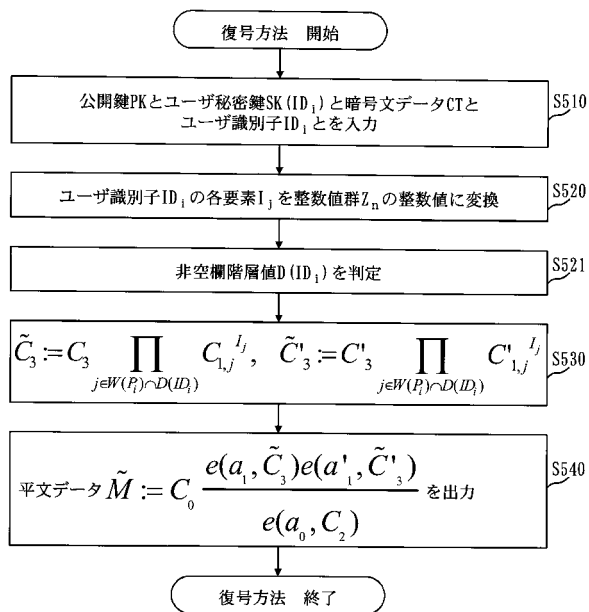
【図 1 3】



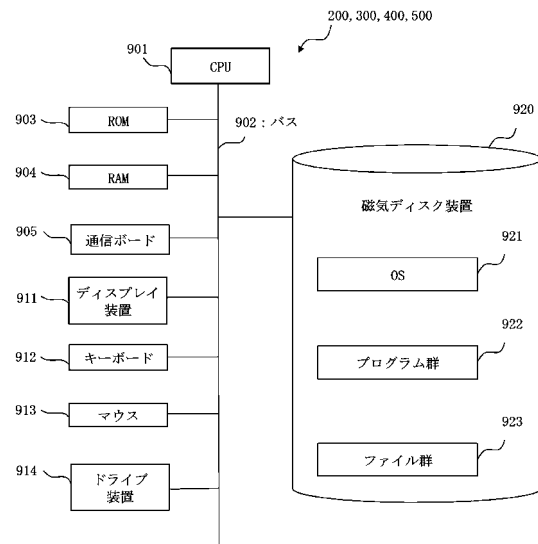
【図 1 4】



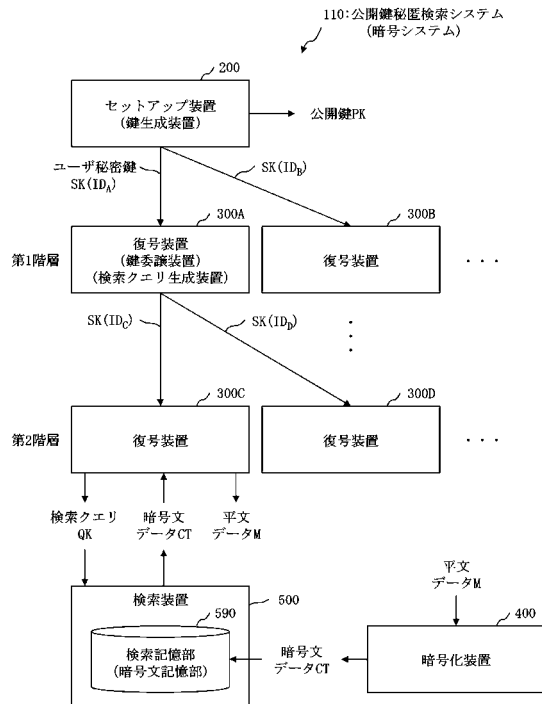
【図 1 5】



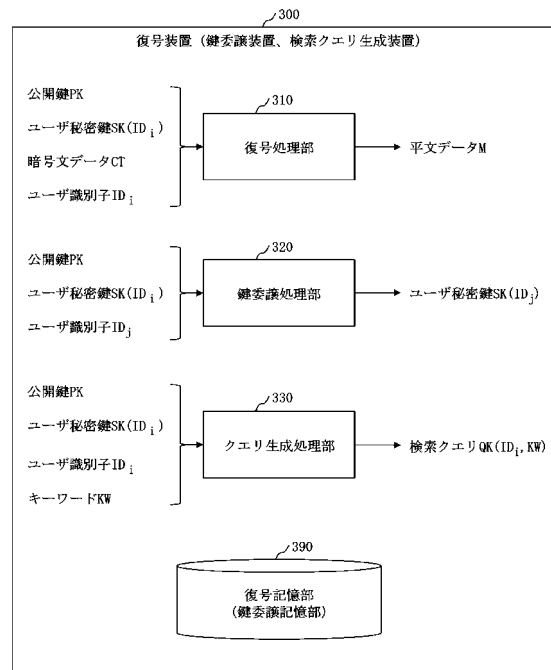
【図 1 6】



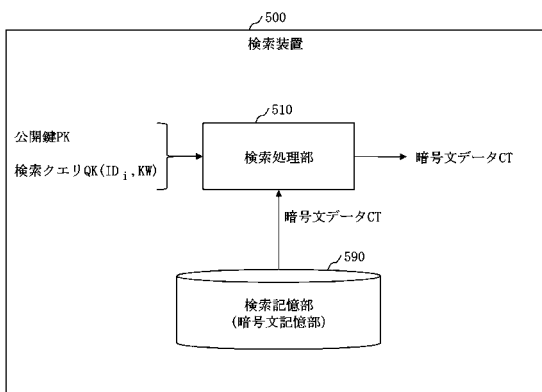
【図 17】



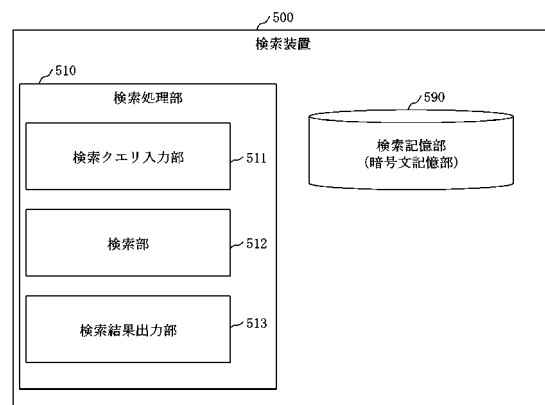
【図 18】



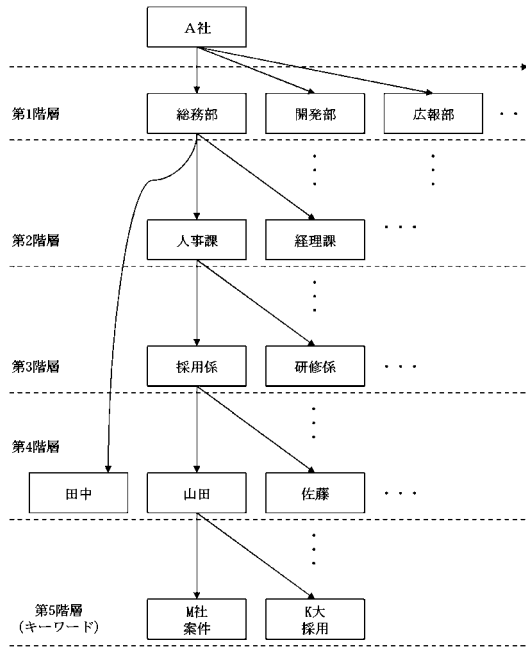
【図 19】



【図 20】



【図 2 1】



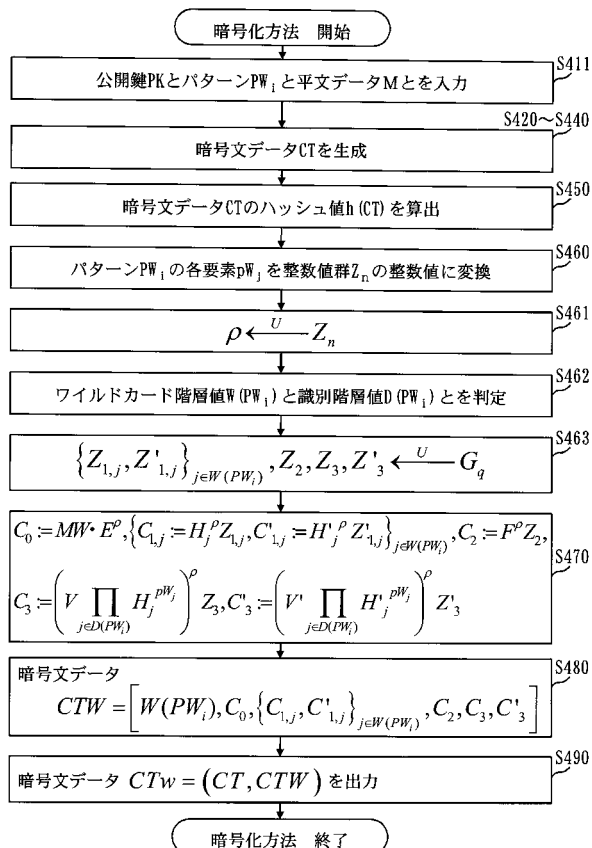
【図 2 2】

No.	パターンPW				
	第1階層 (部長)	第2階層 (課長)	第3階層 (係長)	第4階層 社員	第5階層 キーワード
PW ₁	総務部	人事課	採用係	山田	M社案件
PW ₂	総務部	人事課	採用係	*	K大採用
PW ₃	総務部	経理課	*	*	H氏異動
PW ₄	総務部	人事課	φ	φ	S課解体
PW ₅	総務部	*	φ	φ	総務X案
PW ₆	*	*	φ	φ	部課長秘
PW ₇	*	*	*	*	E製品案
PW ₈	総務部	φ	φ	田中	始末書案

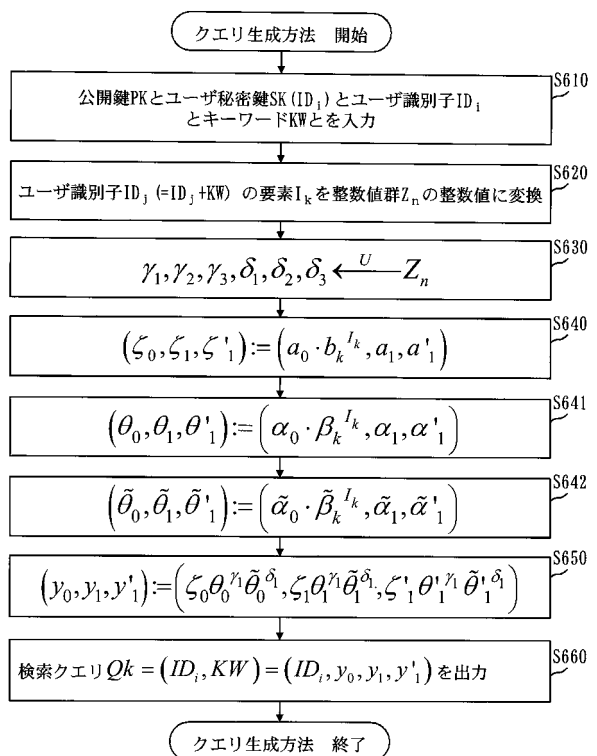
パターンP

キーワードKW

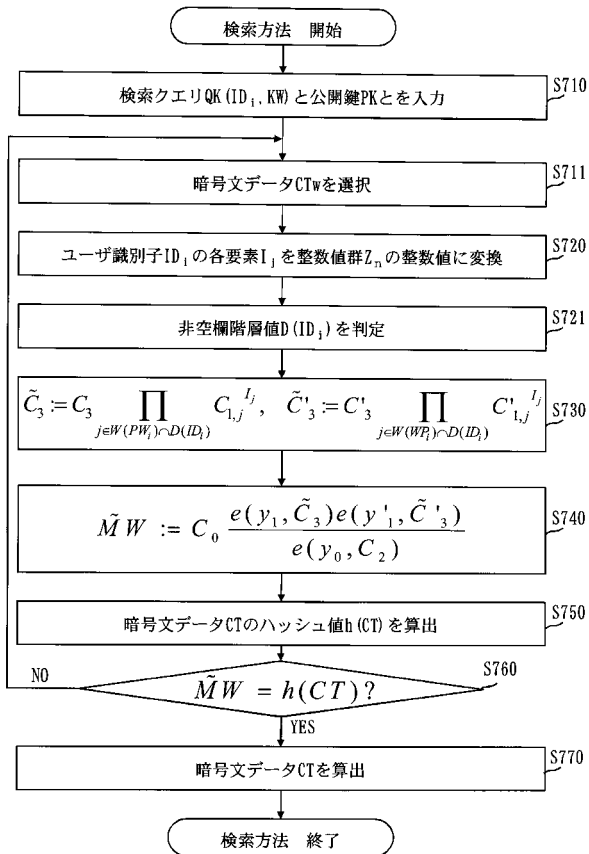
【図 2 3】



【図 2 4】



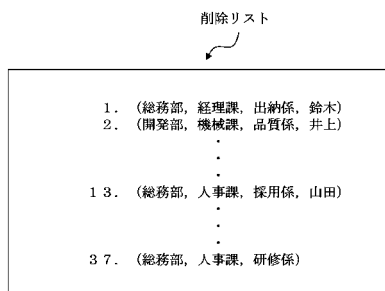
【図 25】



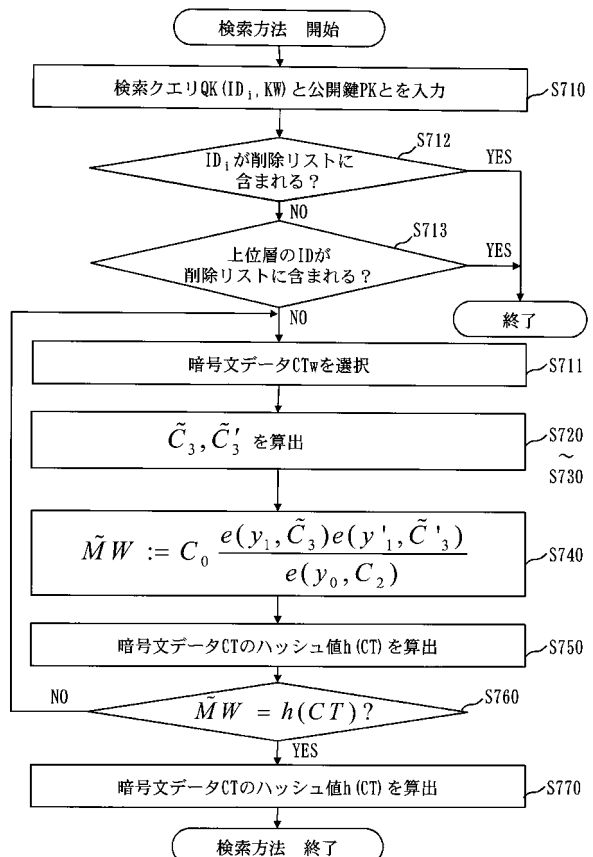
【図 26】

No.	第1階層 部 (部長)	第2階層 課 (課長)	第3階層 係 (係長)	第4階層 社員[1]
...	...	...	...	...
ID_5	総務部	人事課	ϕ	ϕ
...	...	...	...	...
ID_5	総務部	人事課	採用係	Φ
ID_9	総務部	人事課	採用係	高橋
...	...	...	...	...
ID_{10}	総務部	人事課	査定係	ϕ
...	...	...	...	...

【図 27】



【図 28】



【図 29】

No.	第1階層	第2階層	第3階層	第4階層	第5階層
	部 (部長)	課 (課長)	係 (係長)	社員[1]	社員[2]
ID ₁	総務部	φ	φ	φ	φ
ID ₂	総務部	人事課	φ	φ	φ
ID ₃	総務部	経理課	φ	φ	φ
ID ₄	総務部	人事課	研修係	φ	φ
ID ₅	総務部	人事課	採用係	φ	φ
ID ₆	総務部	人事課	採用係	山田	山田
ID ₇	総務部	人事課	採用係	佐藤	佐藤
ID ₈	総務部	φ	φ	田中	田中

【図 30】

No.	第1階層	第2階層	第3階層	第4階層	第5階層	第6階層
	部 (部長)	課 (課長)	係 (係長)	社員[1]	社員[2]	キーワード
P ₁	総務部	人事課	採用係	*	山田	M社案件
P ₂	総務部	人事課	採用係	*	*	K大採用
P ₃	総務部	人事課	*	*	*	H氏異動
P ₄	総務部	人事課	φ	φ	φ	S課解体
P ₅	総務部	*	φ	φ	φ	総務X案
P ₆	*	*	φ	φ	φ	部課長秘
P ₇	*	*	*	*	*	E製品案
P ₈	総務部	φ	φ	*	田中	始末書案

フロントページの続き

- (72)発明者 森 拓海
日本国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
- (72)発明者 伊藤 隆
日本国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
- (72)発明者 松田 規
日本国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
- (72)発明者 坂上 勉
日本国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 石田 信行

- (56)参考文献 特開2010-161523 (JP, A)
特開2010-165275 (JP, A)
特開2010-273317 (JP, A)
小林鉄太郎, Anonymous HIBE とその応用, 2009年 暗号と情報セキュリティ
シンポジウム (SCIS2009) [CD-ROM], 2009年 1月20日, 第1~6頁

- (58)調査した分野(Int.Cl., DB名)
- | | |
|------|------|
| G09C | 1/00 |
| H04L | 9/08 |