(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6006809号
(P6006809)
(45)発行日　平成28年10月12日(2016.10.12)　(24)登録日　平成28年9月16日(2016.9.16)

(51)Int.Cl.　　F I
H04L 9/30 (2006.01)　H04L 9/00 663A
G09C 1/00 (2006.01)　G09C 1/00 620A

請求項の数 14　(全 17 頁)

(21)出願番号　特願2014-557480 (P2014-557480)
(86)(22)出願日　平成26年1月15日 (2014.1.15)
(86)国際出願番号　PCT/JP2014/050574
(87)国際公開番号　WO2014/112523
(87)国際公開日　平成26年7月24日 (2014.7.24)
審査請求日　平成27年7月8日 (2015.7.8)
(31)優先権主張番号　特願2013-5282 (P2013-5282)
(32)優先日　平成25年1月16日 (2013.1.16)
(33)優先権主張国　日本国 (JP)

(73)特許権者　000004226
日本電信電話株式会社
東京都千代田区大手町一丁目５番１号
(74)代理人　100121706
弁理士　中尾　直樹
(74)代理人　100128705
弁理士　中村　幸雄
(74)代理人　100147773
弁理士　義村　宗洋
(72)発明者　小林　鉄太郎
東京都千代田区大手町一丁目５番１号　日本電信電話株式会社内
(72)発明者　山本　剛
東京都千代田区大手町一丁目５番１号　日本電信電話株式会社内

最終頁に続く

(54)【発明の名称】復号サービス提供装置、処理装置、安全性評価装置、プログラム、および記録媒体

(57)【特許請求の範囲】
【請求項１】
元の位数の算出が計算量的に困難な半群上のElGamal暗号方式に則った秘密鍵を保持する記憶部と、
前記ElGamal暗号方式に則った暗号文に対応する情報が入力される入力部と、
前記秘密鍵を用い、前記ElGamal暗号方式に則って前記暗号文に対応する情報を復号して、前記暗号文の復号結果に対応する情報を得る復号部と、
前記復号結果に対応する情報を出力する出力部と、
を有する復号サービス提供装置。
【請求項２】
請求項１の復号サービス提供装置であって、
前記秘密鍵がｓであり、前記半群がＨであり、前記暗号文が前記半群Ｈの元c_1，c_2∈Ｈを含み、前記復号結果が$c_1 \cdot c_2^{s}$∈Ｈである、復号サービス提供装置。
【請求項３】
請求項１または２の復号サービス提供装置であって、
Ｇ，Ｈが前記半群、ｆ（ｘ）が前記ElGamal暗号方式に則って前記半群Ｈの元である前記暗号文ｘを特定の秘密鍵で復号して前記半群Ｇの元を得るための復号関数、X_1，X_2が前記半群Ｇに値を持つ確率変数、x_1が確率変数X_1の実現値、x_2が確率変数X_2の実現値、前記暗号文に対応する情報が、前記半群Ｈの元である、第一入力情報τ_1および第二入力情報τ_2であり、

前記復号部は、
前記第一入力情報τ_1を用いてｆ（τ_1）を正しく計算可能であり、得られた計算結果を第一出力情報z_1とし、
前記第二入力情報τ_2を用いてｆ（τ_2）を正しく計算可能であり、得られた計算結果を第二出力情報z_2とし、
前記復号結果に対応する情報は、前記第一出力情報z_1および前記第二出力情報z_2を含む、復号サービス提供装置。
【請求項４】
Ｇ，Ｈが元の位数の算出が計算量的に困難な半群、ｆ（ｘ）がElGamal暗号方式に則って前記半群Ｈの元である暗号文ｘを特定の秘密鍵で復号して前記半群Ｇの元を得るための復号関数、X_1，X_2が前記半群Ｇに値を持つ確率変数、x_1が確率変数X_1の実現値、x_2が確率変数X_2の実現値、ａ，ｂ，ａ’，ｂ’が整数であり、ｄ≠０であり、ｄ＝ａ’ａ＋ｂ’ｂであり、
計算結果$u=f(x)^b x_1$を生成する第一計算部と、
計算結果$v=f(x)^a x_2$を生成する第二計算部と、
前記計算結果ｕ及びｖが$u^a=v^b$を満たす場合に、$(u^{b'}v^{a'})^{1/d}$を出力する最終出力部と、
を有する処理装置。
【請求項５】
半群上のElGamal暗号方式に則った秘密鍵を保持し、前記ElGamal暗号方式に則った暗号文に対応する情報が入力され、前記秘密鍵を用いて前記ElGamal暗号方式に則って前記暗号文に対応する情報を復号して得られる、前記暗号文の復号結果に対応する情報を出力する復号サービス提供装置、で使用される前記半群の元の位数を算出することの計算量的な困難性または容易性を判定する判定部と、
前記判定部での判定結果に基づいて前記復号サービス提供装置の安全性を評価する評価部と、
を有する安全性評価装置。
【請求項６】
請求項５の安全性評価装置であって、
前記秘密鍵がｓであり、前記半群がＨであり、前記暗号文が前記半群Ｈの元c_1，c_2∈Ｈを含み、前記復号結果が$c_1 \cdot c_2^{\,s}$∈Ｈである、
ことを特徴とする安全性評価装置。
【請求項７】
記憶部と入力部と復号部と出力部とを有する復号サービス提供装置の復号サービス提供方法であって、
元の位数の算出が計算量的に困難な半群上のElGamal暗号方式に則った暗号文に対応する情報が前記入力部に入力される入力ステップと、
前記復号部が、前記記憶部に保持された前記ElGamal暗号方式に則った秘密鍵を用い、前記ElGamal暗号方式に則って前記暗号文に対応する情報を復号して、前記暗号文の復号結果に対応する情報を得る復号ステップと、
前記出力部が、前記復号結果に対応する情報を出力する出力ステップと、
を有する復号サービス提供方法。
【請求項８】
請求項７の復号サービス提供方法であって、
前記秘密鍵がｓであり、前記半群がＨであり、前記暗号文が前記半群Ｈの元c_1，c_2∈Ｈを含み、前記復号結果が$c_1 \cdot c_2^{\,s}$∈Ｈである、復号サービス提供方法。
【請求項９】
請求項７または８の復号サービス提供方法であって、
Ｇ，Ｈが前記半群、ｆ（ｘ）が前記ElGamal暗号方式に則って前記半群Ｈの元である前記暗号文ｘを特定の秘密鍵で復号して前記半群Ｇの元を得るための復号関数、X_1，X_2が

前記半群Ｇに値を持つ確率変数、x_1が確率変数X_1の実現値、x_2が確率変数X_2の実現値、前記暗号文に対応する情報が、前記半群Ｈの元である、第一入力情報τ_1および第二入力情報τ_2であり、

前記復号ステップは、

前記第一入力情報τ_1を用いてｆ（τ_1）を正しく計算可能であり、得られた計算結果を第一出力情報z_1とし、

前記第二入力情報τ_2を用いてｆ（τ_2）を正しく計算可能であり、得られた計算結果を第二出力情報z_2とし、

前記復号結果に対応する情報は、前記第一出力情報z_1および前記第二出力情報z_2を含む、復号サービス提供方法。

【請求項１０】

第一計算部と第二計算部と最終出力部とを有する処理装置の処理方法であって、

Ｇ，Ｈが元の位数の算出が計算量的に困難な半群、ｆ（ｘ）がElGamal暗号方式に則って前記半群Ｈの元である暗号文ｘを特定の秘密鍵で復号して前記半群Ｇの元を得るための復号関数、X_1，X_2が前記半群Ｇに値を持つ確率変数、x_1が確率変数X_1の実現値、x_2が確率変数X_2の実現値、ａ，ｂ，ａ’，ｂ’が整数であり、ｄ≠０であり、ｄ＝ａ’ａ＋ｂ’ｂであり、

前記第一計算部が、計算結果$u=f(x)^b x_1$を生成する第一計算ステップと、

前記第二計算部が、計算結果$v=f(x)^a x_2$を生成する第二計算ステップと、

前記最終出力部が、前記計算結果ｕ及びｖが$u^a=v^b$を満たす場合に、$(u^{b'}v^{a'})^{1/d}$を出力する最終出力ステップと、

を有する処理方法。

【請求項１１】

判定部と評価部とを有する安全性評価装置の安全性評価方法であって、

半群上のElGamal暗号方式に則った秘密鍵を保持し、前記ElGamal暗号方式に則った暗号文が入力され、前記秘密鍵を用いて前記ElGamal暗号方式に則って前記暗号文を復号して得られる復号結果を出力する復号サービス提供方法、で使用される前記半群の元の位数を算出することの計算量的な困難性または容易性を前記判定部が判定する判定ステップと、

前記評価部が前記判定ステップでの判定結果に基づいて前記復号サービス提供方法の安全性を評価する評価ステップと、

を有する安全性評価方法。

【請求項１２】

請求項１１の安全性評価方法であって、

前記秘密鍵がｓであり、前記半群がＨであり、前記暗号文が前記半群Ｈの元c_1，$c_2 \in H$を含み、前記復号結果が$c_1 \cdot c_2^{\,s} \in H$である、

ことを特徴とする安全性評価方法。

【請求項１３】

請求項１から３の何れかの復号サービス提供装置、請求項４の処理装置、または、請求項５もしくは６の安全性評価装置としてコンピュータを機能させるためのプログラム。

【請求項１４】

請求項１から３の何れかの復号サービス提供装置、請求項４の処理装置、または、請求項５もしくは６の安全性評価装置としてコンピュータを機能させるためのプログラムを格納したコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、情報セキュリティ技術に関し、特に、暗号化された情報を復号して利用できる関係者を制限するための、鍵管理技術に関する。

【背景技術】

【０００２】

現在一般的な技術で暗号化された情報を復号するためには、暗号を復号するための鍵を用いて、暗号文から平文を直接計算する方法を採る（例えば、非特許文献１参照）。

【０００３】

しかしながら、この方法では一度関係者に鍵を渡したあとで事情が変わり、その関係者についてその鍵による復号を禁止したいときに、暗号の復号禁止を強制することができない。

【０００４】

そこで、鍵を関係者に配る代わりに、信頼できるサーバ装置の内部に保持して、サーバ装置は関係者の要求に対して復号サービスを提供する方法が考えられている。そのような方法をクラウド鍵管理型暗号と呼ぶ。この方法では暗号を復号するための鍵を利用者に直接渡すことがないので、復号サービスを停止することで、利用者が暗号化されたデータを使用することを停止できるのではないかと期待されている。

【先行技術文献】

【非特許文献】

【０００５】

【非特許文献１】Taher Elgamal, A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms, IEEE Transactions on Information Theory, v. IT-31, n. 4, 1985, pp. 469-472 or CRYPTO 84, pp. 10-18, Springer-Verlag.

【発明の概要】

【発明が解決しようとする課題】

【０００６】

鍵を内部に保持して復号サービスを提供する場合、暗号方式によっては利用者が復号サービスを繰り返し利用することで、暗号を復号する能力を獲得し、復号サービスを停止しても利用者が暗号化されたデータを利用することを止められない可能性がある。そのようなクラウド鍵管理型暗号は安全性に問題がある。

【０００７】

本発明はこのような点に鑑みてなされたものであり、クラウド鍵管理型暗号の安全性を向上させる技術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】

【０００８】

元の位数の算出が計算量的に困難な半群上のElGamal暗号方式に則った秘密鍵を保持し、当該ElGamal暗号方式に則った暗号文に対応する情報が入力され、秘密鍵ｓを用い、ElGamal暗号方式に則って暗号文に対応する情報を復号して、暗号文の復号結果に対応する情報を得て出力する。

【発明の効果】

【０００９】

本発明を用いることで、利用者が復号サービスを繰り返し利用することで暗号を復号する能力を獲得することを抑制することができ、クラウド鍵管理型暗号の安全性を向上させることができる。

【図面の簡単な説明】

【００１０】

【図１】図１は、第１実施形態のセキュリティシステムの構成を説明するためのブロック図である。

【図２】図２は、第１実施形態の復号サービス提供処理を説明するためのフロー図である。

【図３】図３は、第２実施形態のセキュリティシステムの構成を説明するためのブロック図である。

【図４】図４は、第２実施形態の安全性評価処理を説明するためのフロー図である。

【図５】図５は、第３実施形態のセキュリティシステムの構成を説明するためのブロック図である。

【図６】図６は、第３実施形態の処理装置の構成を説明するためのブロック図である。
【図７】図７は、第３実施形態の復号サービス提供装置の構成を説明するためのブロック図である。
【図８】図８は、第３実施形態の処理装置の処理を説明するためのフロー図である。
【図９】図９は、第３実施形態の復号サービス提供装置の処理を説明するためのフロー図である。
【発明を実施するための形態】
【００１１】
本発明の実施形態を説明する。
＜原理＞
各実施形態に共通する原理を説明する。各実施形態では、信頼できる復号サービス提供装置の内部に鍵を保持し、復号サービス提供装置は関係者の要求に対して復号サービスを提供する（クラウド鍵管理型暗号）。ただし、元の位数の算出が計算量的に困難な半群（例えば、可換半群や有限可換半群）Ｈを用い、暗号方式として当該半群Ｈ上のElGamal暗号を採用した復号サービスを用いる。以下に当該復号サービスが安全である理由を述べる。
【００１２】
[ElGamal暗号方式]
次に半群Ｈ上のElGamal暗号について説明する。ElGamal暗号は、半群Ｈのある可逆元を$g \in H$とし、ランダムに選ばれた秘密鍵$s \in Z_q$について、公開鍵を$y = g^{-s} \in H$とする暗号方式であり、平文$m \in g$の暗号文は$(c_1, c_2) = (m \cdot y^r, g^r) \in H^2$で与えられる。$r \in Z_q$は暗号化の過程で決められる乱数であり、$Z_q$はｑによる剰余群であり、ｑは半群Ｈの位数（正整数、例えば素数）であり、$\beta \in H$はβが半群Ｈの元であることを表し、「・」は半群Ｈで定義された演算を表す。暗号文(c_1, c_2)を復号するためには、秘密鍵ｓを用いて$m' = c_1 \cdot c_2^{\,s} \in H$を計算すればよい。
【００１３】
ElGamal暗号を用いた復号サービス提供装置は、秘密鍵ｓを安全に保持し、利用者が暗号文(c_1, c_2)を入力するたびに、その暗号文(c_1, c_2)を復号して復号結果ｍ’を出力する。このとき、復号サービス提供装置は、認証手段で利用者を特定し、復号サービスを正当に受けることができる利用者を記憶した認証データベースを用いて、利用者に復号サービスを行うかどうかを判定してから復号結果を出力しても良い。
【００１４】
[ElGamal暗号を用いた復号サービス提供装置に対する攻撃]
ElGamal暗号を用いた復号サービス提供装置を利用して秘密鍵ｓを抽出しようとする攻撃者である多項式時間確率的アルゴリズムＢを定式化する。与えられた公開鍵$y = g^{-s}$について、Ｂは次の通り攻撃を行う。
１．Ｂはｉ＝１，２，３，...，ｕ（ただしｕは正整数）について暗号文ｃ（ｉ）＝（c_1（ｉ），c_2（ｉ））を生成し、それぞれを復号サービス提供装置に入力し、復号結果$w(i) = c_1(i) \cdot c_2(i)^{s}$を得る。
２．Ｂはｃ（ｉ）およびｗ（ｉ）の情報を用いながら計算し、$y = g^{-\alpha}$となる$\alpha \in Z_q$を出力する。
【００１５】
仮に上記攻撃に成功するＢが存在するとする。攻撃者である任意の多項式時間確率的アルゴリズムＡは、次の方法によってＢを用いて半群Ｈの元ｇの位数を計算できる。ただし、ｋは正整数のセキュリティパラメータである。
１．Ａはｉ＝１，２，３，...，３ｋについて次を実行してβ_iを得る。
（ａ）半群Ｈの元がたかだかＬビットで表現されているとして、ＡはＬよりも十分長いビット列λをランダムに選び、λを２進数として解釈した値を秘密鍵ｓとする。
（ｂ）Ａは$y = g^{-s}$を計算し、それを公開鍵とする。
（ｃ）ＡはＢを用いて$y = g^{-\alpha}$となるαを得る。途中でＢから復号要求があれば、Ａは

ｓを用いて復号してＢに与える。
（ｄ）Ａは$\beta_i = s - \alpha$とする。
２．Ａは、β_1，β_2，...，β_{3k}の最大公約数を計算する。
【００１６】
Ａは、たかだかＯ（2^{-k}）程度（Ｏ-記法）の無視できる確率を除いて、元ｇの位数ｎを出力する。以下にその理由を説明する。$y = g^{-s} = g^{-\alpha}$なので、各ｉについて$g^{\beta_i} = 1$である（上付き添え字のβｉはβ_iを表す）。よってβ_iは半群Ｈの元ｇの位数ｎの整数倍である。ｓはランダムに選ばれているので、$\beta_i = n r_i$となる整数r_iはランダムである。r_1，r_2，...，r_{3k}の最大公約数が１にならない確率は、リーマンのゼータ関数を用いて評価することができて、たかだかＯ（2^{-k}）以下であることを証明できる（この証明はたとえば次の文献に書かれている：山本剛，小林鉄太郎，「準同型写像に対する自己訂正について」，数論応用，ＳＣＩＳ２０１０）。よって、β_1，β_2，...，β_{3k}の最大公約数は元ｇの位数ｎとなる。このように、ElGamal暗号を用いた復号サービス提供装置に対する上述の攻撃が成功するのであれば、半群Ｈの元ｇの位数を計算できる。この対偶も真であり、半群Ｈの元ｇの位数を算出することが困難なのであれば、ElGamal暗号を用いた復号サービス提供装置に対する上述の攻撃を行うことも困難である。
【００１７】
元の位数の計算が困難な半群には、例えば次の例がある。Ｎを素因数分解が困難な数として、剰余環Ｒ＝Ｚ／ＮＺを考える。Ｒの乗法群の元の位数を計算することは、Ｎを素因数分解することと同等に困難であることが知られている（この証明はたとえば次の文献に書かれている：G. Miller, “Riemann’s hypothesis and tests for primality,” Journal of Computer Systems Science, vol.13, pp.300-317, 1976.）。すなわち、元の位数の計算が困難な半群として、例えば、Ｎを法とした剰余環Ｒ＝Ｚ／ＮＺの乗法群を用いることができる。また別の例としては、上記の環Ｒ上の楕円曲線がある。通常の楕円曲線は体の上で構成されるが、その演算規則を形式的に環Ｒ上に適用すると、楕円曲線と同様に結合法則が成り立ち、半群が構成される。これをＨとして用いると、Ｈから抽出したランダムな元は非常に高い確率で可逆元となる。これを元ｇとして用いるとき、元ｇの位数を計算することはＮの素因数分解を計算することと同等に困難であることが分かっている（この詳細はたとえば次の文献に書かれている：Lenstra Jr., H. W., “Factoring integers with elliptic curves,” Annals of Mathematics 126 (3): 649-673, 1987.）。すなわち、元の位数の計算が困難な半群として、例えば、上記の環Ｒ上の楕円曲線上の点（有理点）からなる半群を用いることができる。元の位数の計算が困難な半群は、例えば、因数分解問題を解くために元の位数の計算を行うことが困難な半群である。ある計算や問題が「困難」であるとは、多項式時間内にその計算結果や解を得ることができないことを意味する。すなわち、「元の位数の算出が計算量的に困難な半群」とは、例えば、多項式時間内に元の位数の算出を行うことができない半群を意味する。「元の位数の算出が計算量的に困難な半群」は、逆元が存在するものであってもよいし、逆元が存在しないものであってもよい。また、「元の位数の算出が計算量的に困難な半群」は、例えば、モノイド（単位元を持つ半群）であってもよい。「多項式時間」とは、例えば、秘密鍵ｓのサイズ（長さ）の多項式で表現可能な時間（計算時間）を意味する。言い換えると、「多項式時間」とは、例えば、秘密鍵ｓの長さ（例えばビット長）をχとした場合のχについての任意の多項式で表現可能な時間（計算時間）を意味する。「容易」とは困難でないことを意味する。
【００１８】
＜第１実施形態＞
次に第１実施形態を説明する。本形態では、元ｇの位数の算出が計算量的に困難な半群（可換半群）Ｈを用い、暗号方式として半群Ｈ上のElGamal暗号を採用した復号サービスを提供する。本形態では、「ElGamal暗号方式に則った暗号文に対応する情報」がElGamal暗号方式に則った暗号文であり、「暗号文の復号結果に対応する情報」が暗号文の復号結

果である。

【００１９】

[構成]

図１に例示するように、本形態のセキュリティシステム１は、暗号化装置１１と処理装置１２と復号サービス提供装置１３とを有する。暗号化装置１１は処理装置１２に対し、ネットワークや可搬型記録媒体等を介した情報の提供が可能なように構成されている。また処理装置１２と復号サービス提供装置１３とは、ネットワークや可搬型記録媒体等を介して互いに情報のやり取りが可能なように構成されている。

【００２０】

暗号化装置１１は、記憶部１１１と入力部１１２と暗号化部１１３と出力部１１４とを有する。処理装置１２は、入力部１２１と処理部１２２と出力部１２３と入力部１２４とを有する。復号サービス提供装置１３は、記憶部１３１と入力部１３２と復号部１３３と出力部１３４とを有する。暗号化装置１１と処理装置１２と復号サービス提供装置１３とは、それぞれ、ＣＰＵ（central processing unit）、ＲＡＭ（random-access memory）等を含む汎用または専用のコンピュータに所定のプログラムが読み込まれて構成された特別な装置である。暗号化装置１１と処理装置１２と復号サービス提供装置１３とは、それぞれの制御部（図示せず）の制御のもとで各処理を実行する。各部で得られたデータはそれぞれの一時メモリ（図示せず）に格納され、必要に応じて各部に読み込まれる。

【００２１】

[パラメータ設定処理]

本形態のパラメータ設定処理では、元ｇの位数の算出が計算量的に困難な半群Ｈおよびその元ｇを含むシステムパラメータが暗号化装置１１および復号サービス提供装置１３に設定される。半群Ｈ上のElGamal暗号方式に則った秘密鍵$s \in Z_q$がランダムに選択され、復号サービス提供装置１３の記憶部１３１に安全に格納される。また当該半群Ｈ上のElGamal暗号方式に則った公開鍵$y = g^s \in H$が生成され、暗号化装置１１の記憶部１１１に格納される。

【００２２】

[暗号化・復号サービス提供処理]

図２に例示するように、まず、暗号化装置１１の入力部１１２に平文$m \in H$が入力され、暗号化部１１３に送られる（ステップＳ１０１）。暗号化部１１３は、記憶部１１１に格納されている公開鍵ｙを用い、平文ｍを半群Ｈ上のElGamal暗号方式に則って暗号化し、暗号文$(c_1, c_2) = (m \cdot y^r, g^r) \in H^2$を得て出力する（ステップＳ１０２）。出力部１１４は暗号文(c_1, c_2)を出力する（ステップＳ１０３）。

【００２３】

暗号文(c_1, c_2)は処理装置１２の入力部１２１に入力され、処理部１２２に送られる。（ステップＳ１０４）。処理部１２２は、暗号文(c_1, c_2)を含む復号依頼情報を生成して出力部１２３から出力する（ステップＳ１０５）。

【００２４】

暗号文(c_1, c_2)を含む復号依頼情報は、復号サービス提供装置１３の入力部１３２に入力され、暗号文(c_1, c_2)が復号部１３３に送られる（ステップＳ１０６）。復号部１３３は記憶部１３１に格納されている秘密鍵ｓを用い、半群Ｈ上のElGamal暗号方式に則って暗号文(c_1, c_2)を復号して復号結果$m' = c_1 \cdot c_2^{\,s} \in H$を得て出力する（ステップＳ１０７）。出力部１３４は、復号結果ｍ’を含む応答情報を出力する（ステップＳ１０８）。応答情報は処理装置１２に入力され、処理部１２２に送られる（ステップＳ１０９）。

【００２５】

[本形態の特徴]

本形態では、元ｇの位数の算出が計算量的に困難と考えられる半群Ｈ上のElGamal暗号を採用した復号サービス提供装置１３を用い、復号サービスを提供する。この構成では、利用者がたとえ復号演算サービスを繰り返し用いたとしても秘密鍵を得ることが困難であ

ることを証明でき、原理的に秘密鍵が漏洩しないことが保証される。一般に安全とされる暗号方式では、秘密鍵を得ることなく復号能力を獲得することはできないと考えられている。したがって、復号演算サービスを利用者に許可した後で許可を取り消す制御を行うとき、どのような挙動を取る利用者を想定したとしても、サービスの利用を取り消された以降は利用者が暗号化された文書を復号することができないといえる。

【００２６】

＜第２実施形態＞

次に第２実施形態を説明する。本形態では、復号サービスに用いられる半群Ｈの元ｇの位数を算出することの計算量的な困難性または容易性を判定することで、復号サービスの安全性を評価する。これにより、復号サービスの安全性を評価することができる。このような復号サービスの安全性の評価は、システムパラメータの設定時に行われてもよいし、既に提供されている復号サービスに対して行われてもよい。以下では、一例としてシステムパラメータの設定時に復号サービスの安全性の評価を行い、安全性が低いと判断された場合にシステムパラメータを再設定する形態を説明する。本形態では、「ElGamal暗号方式に則った暗号文に対応する情報」がElGamal暗号方式に則った暗号文であり、「暗号文の復号結果に対応する情報」が暗号文の復号結果である。また、第１実施形態と共通する事項については、第１実施形態と同じ参照番号を用いて説明を省略する。

【００２７】

[構成]

図３に例示するように、本形態のセキュリティシステム２は、暗号化装置１１と処理装置１２と復号サービス提供装置１３と設定装置２４と安全性評価装置２５とを有する。設定装置２４は暗号化装置１１および復号サービス提供装置１３に対し、ネットワークや可搬型記録媒体等を介した情報の提供が可能なように構成されている。設定装置２４と安全性評価装置２５とは、ネットワークや可搬型記録媒体等を介して互いに情報のやり取りが可能なように構成されている。設定装置２４および安全性評価装置２５は、汎用または専用のコンピュータに所定のプログラムが読み込まれて構成された特別な装置である。

【００２８】

安全性評価装置２５は、記憶部２５１と入力部２５２と判定部２５３と評価部２５４と出力部２５５とを有する。安全性評価装置２５は、制御部（図示せず）の制御のもとで各処理を実行する。各部で得られたデータはそれぞれの一時メモリ（図示せず）に格納され、必要に応じて各部に読み込まれる。

【００２９】

[パラメータ設定処理]

本形態のパラメータ設定処理の前処理として、安全性評価装置２５の記憶部２５１に、半群Ｈの元ｇの位数を算出することの計算量的な困難性または容易性を判定するために必要な情報を格納する。このような情報の例は、元の位数を算出することが困難と考えられている半群およびその元のリスト、元の位数を算出することが容易と考えられている半群およびその元のリスト、またはこの困難性もしくは容易性を判定するアルゴリズムなどである。

【００３０】

図４に例示するように、パラメータ設定処理では、設定装置２４が半群（例えば、可換半群や有限可換半群）Ｈおよびその元ｇを含むシステムパラメータを生成し（ステップＳ２０１）、生成した半群Ｈおよび元ｇを特定する情報を出力する（ステップＳ２０２）。

【００３１】

半群Ｈおよび元ｇを特定する情報は安全性評価装置２５の入力部２５２に入力され、判定部２５３に送られる（ステップＳ２０３）。判定部２５３は、記憶部２５１に格納された情報を用い、当該半群Ｈの元ｇの位数を算出することの困難性または容易性を判定する。例えば、半群の元の位数を算出することが困難と考えられている半群およびその元のリストが記憶部２５１に格納されている場合、判定部２５３は、判定対象の半群Ｈの元ｇが当該リストに含まれるかを判定し、含まれれば当該半群Ｈの元ｇの位数を算出することが

困難であると判定する。或いは、半群の元の位数を算出することが容易と考えられている半群およびその元のリストが記憶部２５１に格納されている場合、判定部２５３は、判定対象の半群Ｈの元ｇが当該リストに含まれるかを判定し、含まれれば当該半群Ｈの元ｇの位数を算出することが容易であると判定する。半群の元の位数を算出することの困難性または容易性を判定するアルゴリズムが記憶部２５１に格納されている場合、判定部２５３は、このアルゴリズムを用い、判定対象の半群Ｈの元ｇの位数を算出することが困難であるかを判定するか、または判定対象の半群Ｈの元ｇの位数を算出することが容易であるかを判定する。例えば、数体ふるい法や関数体ふるい法などを用いて所定処理時間内に当該半群Ｈでの離散対数問題が解ければ、その半群Ｈの元ｇの位数を算出することも容易であると判定する（ステップＳ２０４）。

【００３２】

判定部２５３から出力された判定結果は評価部２５４に入力され、評価部２５４はこの判定結果に基づいて復号サービス提供装置１３の安全性を評価する。すなわち、判定部２５３で元の位数を算出することが困難であると判定されるか、元の位数を算出することが容易であると判定されなかった場合、評価部２５４は復号サービス提供装置１３の安全性が高い旨の評価結果（ａｃｃ）を出力する（ステップＳ２０５）。一方、判定部２５３で元の位数を算出することが困難であると判定されなかったか、元の位数を算出することが容易であると判定された場合、評価部２５４は復号サービス提供装置１３の安全性が低い旨の評価結果（ｒｅｊ）を出力する（ステップＳ２０６）。

【００３３】

評価部２５４から出力された評価結果は、設定装置２４に入力される（ステップＳ２０７）。設定装置２４はこの評価結果が安全性が高い旨を示すかを判定する（ステップＳ２０８）。当該評価結果が安全性が低い（ｒｅｊ）ことを示す場合、ステップＳ２０１に戻る。当該評価結果が安全性が高い（ａｃｃ）ことを示す場合、設定装置２４は半群Ｈおよびその元ｇを含むシステムパラメータを出力し、暗号化装置１１および復号サービス提供装置１３に設定する（ステップＳ２０９）。

【００３４】

＜第３実施形態＞

次に第３実施形態を説明する。本形態では、元の位数の算出が計算量的に困難な半群を用い、自己訂正技術を用いて復号サービスを行う。自己訂正技術の詳細は、例えば、参考文献１（国際公開ＷＯ／２０１１／０８６９９２号公報）や参考文献２（国際公開ＷＯ／２０１２／０５７１３４号公報）等に開示されている。以下では、第１実施形態との相違点を中心に説明する。

【００３５】

＜構成＞

図５に例示するように、第三実施形態のセキュリティシステム３は、例えば、前述の暗号化装置１１と、秘密鍵を保持していない処理装置３２１と、前述のElGamal暗号方式に則った秘密鍵を保持する復号サービス提供装置３３２とを有し、処理装置３２１が復号サービス提供装置３３２に暗号文の復号能力の提供を依頼し、復号サービス提供装置３３２から提供された復号能力を用いて暗号文を復号する。処理装置３２１と復号サービス提供装置３３２とは情報のやり取りが可能なように構成される。例えば、処理装置３２１と復号サービス提供装置３３２とは、伝送線やネットワークや可搬型記録媒体などを経由した情報のやり取りが可能とされている。

【００３６】

図６に例示するように、第三実施形態の処理装置３２１は、例えば、整数選択部２１０２と入力情報提供部２１０４と第一計算部２１０５と第一べき乗計算部２１０６と第一リスト記憶部２１０７と第二計算部２１０８と第二べき乗計算部２１０９と第二リスト記憶部２１１０と判定部２１１１と最終出力部２１１２と制御部２１１３とを有する。処理装置３２１の例は、カードリーダライタ装置や携帯電話などの計算機能と記憶機能とを備えた機器や、特別なプログラムが読み込まれたＣＰＵ（central processing unit）やＲＡ

M（random-access memory）を備えた公知又は専用のコンピュータなどである。

【００３７】

図７に例示するように、第三実施形態の復号サービス提供装置３３２は、例えば、第一出力情報計算部２２０１（復号部）と第二出力情報計算部２２０２（復号部）と鍵記憶部２２０４（記憶部）と制御部２２０５と入力部３１３２と出力部３１３４を有する。復号サービス提供装置３３２の例は、ＩＣカードやＩＣチップなどの耐タンパ性モジュールや、携帯電話などの計算機能と記憶機能とを備えた機器や、特別なプログラムが読み込まれたＣＰＵやＲＡＭを備えた公知又は専用のコンピュータなどである。

【００３８】

＜処理＞

次に本形態の処理を説明する。処理の前提として、Ｇ，Ｈを、前述した元の位数の算出が計算量的に困難な半群（例えば、可換半群や有限可換半群）（例えば、Ｈ＝Ｇ×Ｇ、Ｈ＝Ｇ）とし、ｆ（ｘ）を、前述のElGamal暗号方式に則って、半群Ｈの元である暗号文ｘを特定の秘密鍵ｓで復号して半群Ｇの元を得るための復号関数とし、半群Ｇ，Ｈの生成元をそれぞれμ_g，μ_hとし、X_1，X_2を半群Ｇに値を持つ確率変数とし、確率変数X_1の実現値をx_1、確率変数X_2の実現値をx_2とする。処理装置３２１の各処理は制御部２１１３の制御のもとで実行され、復号サービス提供装置３３２の各処理は制御部２２０５の制御のもとで実行される。

【００３９】

図８に例示するように、まず、処理装置３２１（図６）の整数選択部２１０２が、整数ａ，ｂ，ａ’，ｂ’を選択する（ステップＳ２１０１）。ａ，ｂは、例えば、互いに素な自然数である。ａ，ｂは例えばランダムに選択される。ａ’，ｂ’は、ランダムに選択されてもよいし、ｄ＝ａ’ａ＋ｂ’ｂを満たすように選択されてもよい。整数ａ，ｂの少なくとも一部の情報は、入力情報提供部２１０４、第一べき乗計算部２１０６、および第二べき乗計算部２１０９に送られる。整数ａ，ｂ，ａ’，ｂ’の情報は最終出力部２１１２に送られる。

【００４０】

制御部１１１３は、ｔ＝１とする（ステップＳ２１０２）。

【００４１】

入力情報提供部２１０４は、入力された前述のElGamal暗号方式に則った暗号文ｘにそれぞれ対応する半群Ｈの元である第一入力情報τ_1及び第二入力情報τ_2（暗号文ｘに対応する情報）を生成して出力する（ステップＳ２１０３）。好ましくは、第一入力情報τ_1及び第二入力情報τ_2はそれぞれ暗号文ｘとの関係をかく乱させた情報である。これにより、処理装置３２１は、暗号文ｘを復号サービス提供装置３３２に対して隠蔽できる。好ましくは、本形態の第一入力情報τ_1は整数選択部２１０２で選択された整数ｂにさらに対応し、第二入力情報τ_2は整数選択部２１０２で選択された整数ａにさらに対応する。これにより、復号サービス提供装置３３２から提供された復号能力を処理装置３２１が高い精度で評価することが可能となる。τ_1，τ_2の具体例は、例えば、参考文献１，２等に例示されている。例えば、ｘ＝（c_1，c_2）であり、（Ｖ，Ｗ）が群Ｈの元であり、ｆ（Ｖ，Ｗ）＝Ｙであり、r_4～r_7が０以上の自然数の乱数であり、τ_1＝（$c_2{}^{b}W^{r_4}$，$c_1{}^{b}V^{r_4}\mu_g{}^{r_5}$）であり、$\tau_2$＝（$c_2{}^{a}W^{r_6}$，$c_1{}^{a}V^{r_6}\mu_g{}^{r_7}$）である。

【００４２】

図９に例示するように、第一入力情報τ_1は、復号サービス提供装置３３２（図７）の入力部３１３２に入力され、そこから第一出力情報計算部２２０１に入力される。第二入力情報τ_2は、入力部３１３２に入力され、そこから第二出力情報計算部２２０２に入力される（ステップＳ２２００）。

【００４３】

第一出力情報計算部２２０１は、第一入力情報τ_1と鍵記憶部２２０４に格納された秘密鍵ｓとを用い、或る確率より大きな確率でｆ（τ_1）を正しく計算し、得られた計算結

果を第一出力情報z_1とする。すなわち、第一出力情報計算部２２０１は、第一入力情報τ_1と鍵記憶部２２０４に格納された秘密鍵ｓとを用いてｆ（τ_1）を正しく計算可能であり、得られた計算結果を第一出力情報z_1とする（ステップＳ２２０１）。第二出力情報計算部２２０２は、第二入力情報τ_2と鍵記憶部１２０４に格納された秘密鍵ｓとを用い、或る確率より大きな確率でｆ（τ_2）を正しく計算し、得られた計算結果を第二出力情報z_2とする。すなわち、第二出力情報計算部２２０２は、第二入力情報τ_2と鍵記憶部１２０４に格納された秘密鍵ｓとを用いてｆ（τ_2）を正しく計算可能であり、得られた計算結果を第二出力情報z_2とする（ステップＳ２２０２）。すなわち、第一出力情報計算部２２０１や第二出力情報計算部２２０２は、意図的又は意図的ではない誤差を含んだ計算結果を出力する。言い換えると、第一出力情報計算部２２０１での計算結果がｆ（τ_1）の場合もあればｆ（τ_1）でない場合もあり、第二出力情報計算部２２０２での計算結果がｆ（τ_2）の場合もあればｆ（τ_2）でない場合もある。「計算可能」とは、無視することができない確率以上の確率で計算することができることを意味する。無視することができない確率とは、セキュリティパラメータｋについての広義単調関数である多項式を多項式Ｆ（ｋ）として、１／Ｆ（ｋ）以上の確率である。

【００４４】

第一出力情報計算部２２０１は第一出力情報z_1を出力し、第二出力情報計算部２２０２は第二出力情報z_2を出力し、出力部３１３４は、第一出力情報z_1および第二出力情報z_2（暗号文ｘの復号結果に対応する情報）を出力する（ステップＳ２２０３）。

【００４５】

図８に戻り、第一出力情報z_1は処理装置３２１（図６）の第一計算部２１０５に入力され、第二出力情報z_2は第二計算部２１０８に入力される。これらの第一出力情報z_1及び第二出力情報z_2が、復号サービス提供装置３３２から処理装置３２１に与えられた復号能力に相当する（ステップＳ２１０４）。

【００４６】

第一計算部２１０５は、第一出力情報z_1から計算結果$u=f(x)^b x_1$を生成する（例えば、$u=z_1 Y^{-r_4} \mu_g^{-r_5}$を満たす）。計算結果ｕは第一べき乗計算部２１０６に送られる（ステップＳ２１０５）。

【００４７】

第一べき乗計算部２１０６は$u'=u^a$を計算する。計算結果ｕとその計算結果に基づいて計算されたｕ’との組（ｕ，ｕ’）は、第一リスト記憶部２１０７に記憶される（ステップＳ２１０６）。

【００４８】

判定部２１１１は、第一リスト記憶部２１０７に記憶された組（ｕ，ｕ’）及び第二リスト記憶部２１１０に記憶された組（ｖ，ｖ’）の中で、ｕ’＝ｖ’となるものがあるか判定する（ステップＳ２１０７）。もし、第二リスト記憶部２１１０に組（ｖ，ｖ’）が記憶されていない場合には、このステップＳ２１０７の処理を行わずに、次のステップＳ２１０８の処理を行う。ｕ’＝ｖ’となるものがあった場合には、ステップＳ２１１５に進む。ｕ’＝ｖ’となるものがなかった場合には、ステップＳ２１０８に進む。

【００４９】

ステップＳ２１０８では、第二計算部２１０８が、第二出力情報z_2から計算結果$v=f(x)^a x_2$を生成する（例えば、$v=z_2 Y^{-r_6} \mu_g^{-r_7}$を満たす）。計算結果ｖは第二べき乗計算部２１０９に送られる（ステップＳ２１０８）。

【００５０】

第二べき乗計算部２１０９は$v'=v^b$を計算する。計算結果ｖとその計算結果に基づいて計算されたｖ’との組（ｖ，ｖ’）は、第二リスト記憶部２１１０に記憶される（ステップＳ２１０９）。

【００５１】

判定部２１１１は、第一リスト記憶部２１０７に記憶された組（ｕ，ｕ’）及び第二リスト記憶部２１１０に記憶された組（ｖ，ｖ’）の中で、ｕ’＝ｖ’となるものがあるか

判定する（ステップＳ２１１０）。ｕ’＝ｖ’となるものがあった場合には、ステップＳ２１１５に進む。ｕ’＝ｖ’となるものがなかった場合には、ステップＳ２１１１に進む。

【００５２】

ステップＳ２１１１では、制御部２１１３がｔ＝T_{max}であるか判定する（ステップＳ２１１１）。T_{max}は予め定められた自然数である。ｔ＝T_{max}であれば、制御部２１１３は、計算をすることができなかった旨の情報、例えば記号「⊥」を出力して（ステップＳ２１１３）、処理を終える。ｔ＝T_{max}でない場合には、制御部２１１３は、ｔを１だけインクリメント、すなわちｔ＝ｔ＋１として（ステップＳ２１１２）、ステップＳ２１０３に戻る。

【００５３】

ステップＳ２１１５では、最終出力部２１１２が、ｕ’＝ｖ’となるｕ’及びｖ’に対応するｕ及びｖ、並びにｄ＝ａ’ａ＋ｂ’ｂ（例えば、ｄ＝１）を満たすａ’，ｂ’及びｄを用い、$(u^{b'}v^{a'})^{1/d}$を計算して出力する（ステップＳ２１１５）。すなわち、最終出力部２１１２は、ｄ＝ａ’ａ＋ｂ’ｂについての$(u^{b'}v^{a'})^{1/d}$を出力する。例えば、ｄ＝１の場合、最終出力部２１１２は、１＝ａ’ａ＋ｂ’ｂについての$u^{b'}v^{a'}$を出力する。出力された$(u^{b'}v^{a'})^{1/d}$は高い確率で暗号文ｘの復号結果ｆ（ｘ）となる（この理由は、例えば、参考文献１，２参照）。また、上述した処理を複数回繰り返し、ステップＳ２１１５で得られた値のうち最も頻度の高い値を復号結果としてもよい。

【００５４】

＜第三実施形態の変形例＞

整数ａ，ｂの一方が１などの定数であってもよく、整数ａ’，ｂ’の少なくとも一方が定数であってもよい。整数ａ，ｂ，ａ’，ｂ’の一部を定数とし、一部の処理部やステップが省略されてもよい。例えば、ｂが定数１である場合には、ステップＳ２１０１での整数ｂの選択が不要となり、ｖ’＝ｖとなり、第二べき乗計算部２１０９およびステップＳ２１０９が不要となる。或いは、ｄを定数または乱数とし、ステップＳ２１０１でｄ＝ａ’ａ＋ｂ’ｂを満たす整数ａ，ｂ，ａ’，ｂ’が選択されてもよい。或いは、ステップＳ２１１５でｄ＝ａ’ａ＋ｂ’ｂが計算されてもよい。或いは、ステップＳ２１０１で、整数選択部２１０２が整数ａ，ｂ，ａ’，ｂ’の選択とｄ＝ａ’ａ＋ｂ’ｂの計算とを行ってもよい。或いは、ステップＳ２１０２よりも後、ステップＳ２１１５よりも前の何れかの時点で、整数選択部２１０２がｄ＝ａ’ａ＋ｂ’ｂを計算してもよい。また、最終出力部２１１２が、ｄ≠０のときに$(u^{b'}v^{a'})^{1/d}$を出力することとしてもよい。ｄ＝０の場合にエラー終了することにしてもよいし、ｄ＝０の場合にステップＳ２１０１で整数ａ，ｂ，ａ’，ｂ’の少なくとも一部が再選択され、処理がやり直されてもよい。また、演算にａ’，ｂ’が必要となる前であれば、どの時点でａ’，ｂ’が選択されてもよい。

【００５５】

＜その他の変形例等＞

なお、本発明は上述の実施の形態に限定されるものではない。例えば、特開２０１２－２３７８８１、特開２０１２－２２０８３４、特開２０１２－２２０８１４、および特開２０１２－１５１７５６等の各実施形態の自己訂正技術の群を上述の半群に置換した形態であってもよい。例えば、セキュリティシステムが、さらに、復号サービス提供装置１３で復号サービスの提供を受けた利用者のリストおよび復号結果を含むログを保存する履歴保存装置を有してもよい。各実施形態の構成では、利用者がたとえ復号演算サービスを繰り返し用いたとしても秘密鍵を得ることは困難である。そのため、当該秘密鍵を用いて得られる復号結果はすべて復号サービス提供装置１３から出力されたものである。よって、例えば復号結果が漏洩した場合に、当該履歴保存装置に保存された利用者のリストやログを検証することで、その漏洩経路を追跡するための情報を得ることができる。また、上記の各実施形態では半群Ｈの位数がZ_qの位数と同じｑであった。しかしながら、半群Ｈの

位数がｑよりも大きくてもよいし、小さくてもよい。また暗号方式によっては半群Ｈが可換でなくてもよい。

【００５６】

上述の各種の処理は、記載に従って時系列に実行されるのみならず、処理を実行する装置の処理能力あるいは必要に応じて並列的にあるいは個別に実行されてもよい。その他、本発明の趣旨を逸脱しない範囲で適宜変更が可能であることはいうまでもない。

【００５７】

上述の構成をＣＰＵ等のハードウェアプロセッサやＲＡＭ等のメモリ等を備えたコンピュータによって実現する場合、各装置が有すべき機能の処理内容はプログラムによって記述される。このプログラムをコンピュータで実行することにより、上記処理機能がコンピュータ上で実現される。この処理内容を記述したプログラムは、コンピュータで読み取り可能な記録媒体に記録しておくことができる。コンピュータで読み取り可能な記録媒体の例は、非一時的な（non-transitory）記録媒体である。このような記録媒体の例は、磁気記録装置、光ディスク、光磁気記録媒体、半導体メモリ等である。

【００５８】

このプログラムの流通は、例えば、そのプログラムを記録したＤＶＤ、ＣＤ－ＲＯＭ等の可搬型記録媒体を販売、譲渡、貸与等することによって行う。さらに、このプログラムをサーバコンピュータの記憶装置に格納しておき、ネットワークを介して、サーバコンピュータから他のコンピュータにそのプログラムを転送することにより、このプログラムを流通させる構成としてもよい。

【００５９】

このようなプログラムを実行するコンピュータは、例えば、まず、可搬型記録媒体に記録されたプログラムもしくはサーバコンピュータから転送されたプログラムを、一旦、自己の記憶装置に格納する。処理の実行時、このコンピュータは、自己の記録装置に格納されたプログラムを読み取り、読み取ったプログラムに従った処理を実行する。このプログラムの別の実行形態として、コンピュータが可搬型記録媒体から直接プログラムを読み取り、そのプログラムに従った処理を実行することとしてもよく、さらに、このコンピュータにサーバコンピュータからプログラムが転送されるたびに、逐次、受け取ったプログラムに従った処理を実行することとしてもよい。サーバコンピュータから、このコンピュータへのプログラムの転送は行わず、その実行指示と結果取得のみによって処理機能を実現する、いわゆるＡＳＰ（Application Service Provider）型のサービスによって、上述の処理を実行する構成としてもよい。

【００６０】

上記実施形態では、コンピュータ上で所定のプログラムを実行させて本装置の処理機能が実現されたが、これらの処理機能の少なくとも一部が専用または汎用のハードウェアで実現されてもよい。

【符号の説明】

【００６１】

１，２，３　セキュリティシステム
１１　暗号化装置
１２，３２１　処理装置
１３，３３２　復号サービス提供装置
２４　設定装置
２５　安全性評価装置

【図１】

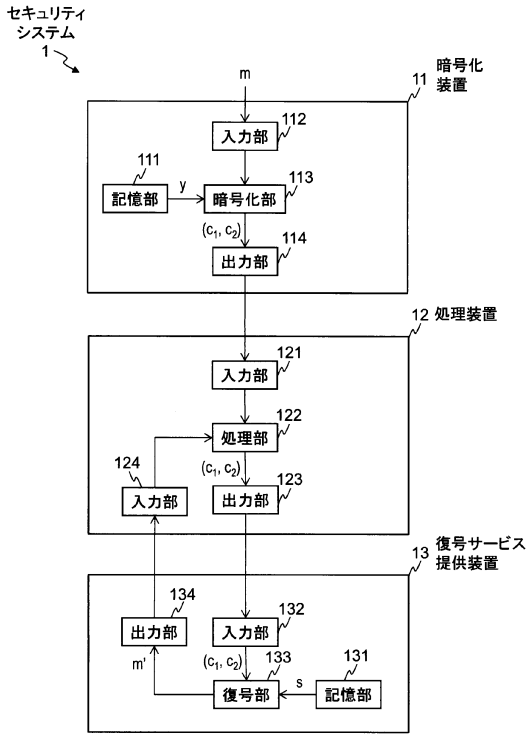

図1

【図２】

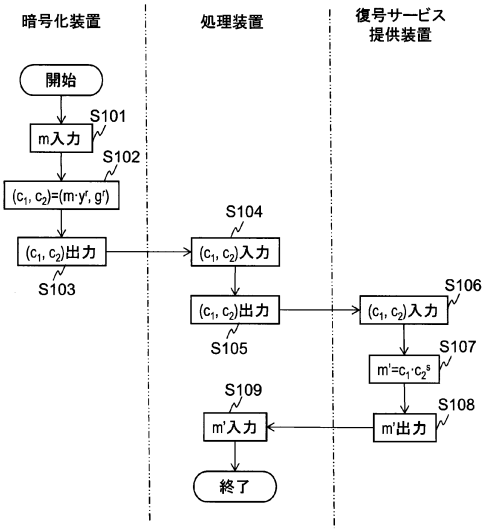

図2

【図３】

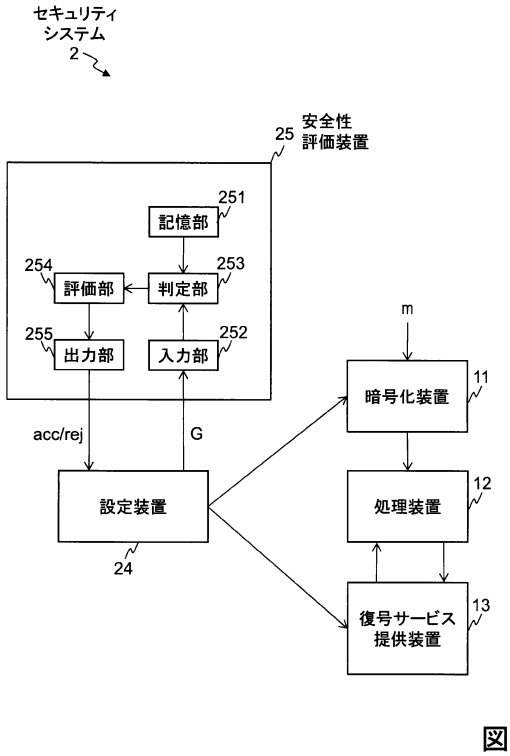

図3

【図４】

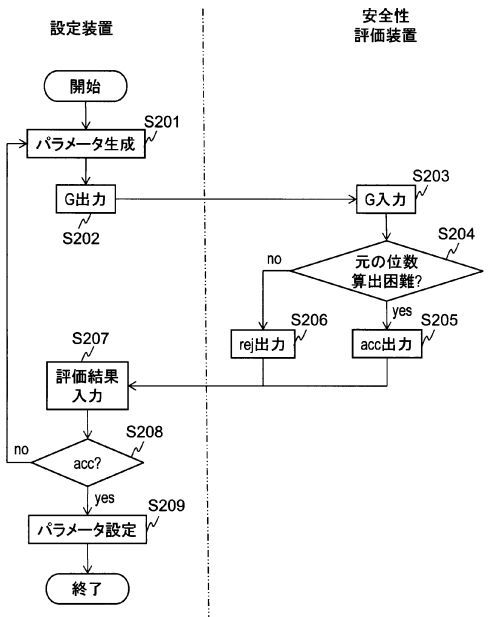

図4

【図５】

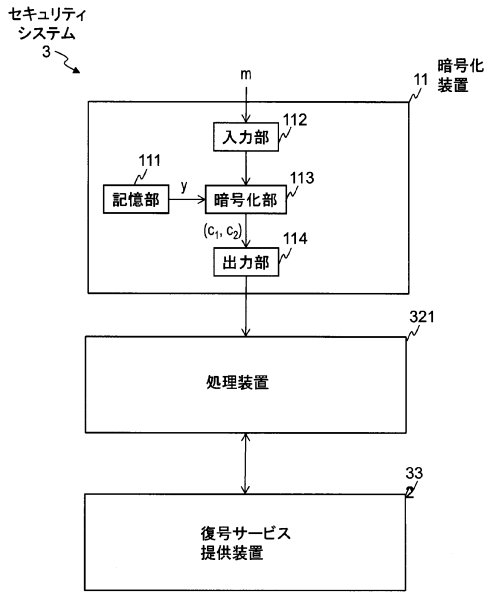

図5

【図６】

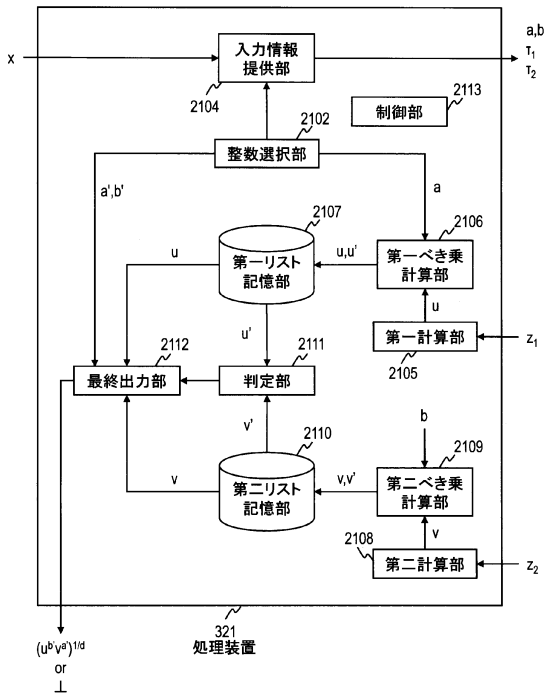

図6

【図７】

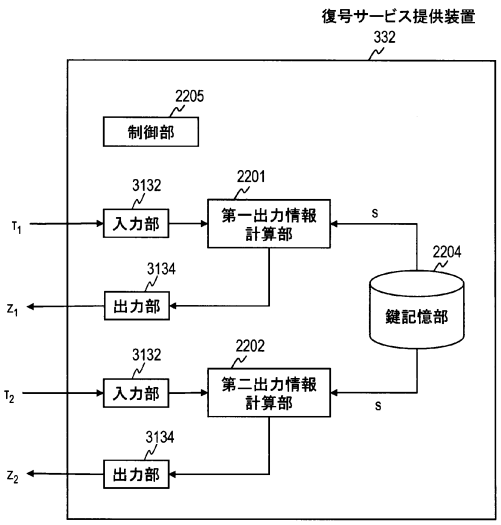

図7

【図８】

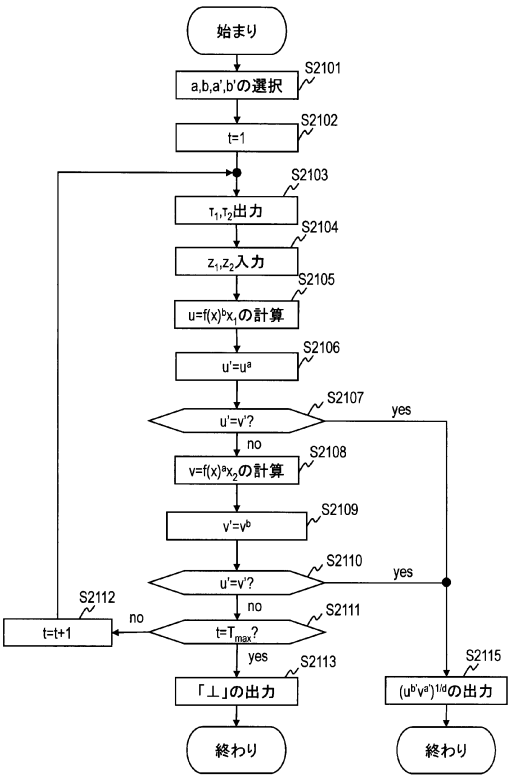

図8

【図９】

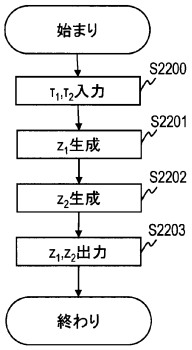
始まり
S2200
τ_1,τ_2入力
S2201
z_1生成
S2202
z_2生成
S2203
z_1,z_2出力
終わり

図9

フロントページの続き

(72)発明者　冨士　仁
東京都千代田区大手町一丁目５番１号　日本電信電話株式会社内
(72)発明者　山本　具英
東京都千代田区大手町一丁目５番１号　日本電信電話株式会社内
(72)発明者　吉田　麗生
東京都千代田区大手町一丁目５番１号　日本電信電話株式会社内

審査官　中里　裕正

(56)参考文献　特開平１０－３０１４９１（ＪＰ，Ａ）
特開２０１２－１５１７５６（ＪＰ，Ａ）
特表２００７－５０７１７５（ＪＰ，Ａ）
Boneh, D. et al., A Method for Fast Revocation of Public Key Certificates and Security Capabilities, Proceedings of the 10th USENIX Security Symposium, The Internet, ２００１年, [2013年12月13日 検索], ＵＲＬ, https://www.usenix.org/legacy/publications/library/proceedings/sec01/technical.html

(58)調査した分野(Int.Cl., ＤＢ名)
Ｈ０４Ｌ　　９／３０
Ｇ０９Ｃ　　１／００
ＪＳＴＰｌｕｓ／ＪＭＥＤＰｌｕｓ／ＪＳＴ７５８０（ＪＤｒｅａｍＩＩＩ）
ＩＥＥＥ　Ｘｐｌｏｒｅ