(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第3562262号
(P3562262)
(45)発行日　平成16年9月8日(2004.9.8)　(24)登録日　平成16年6月11日(2004.6.11)

(51)Int.Cl.[7]　F I
G09C 1/00　G09C 1/00 640C
H04L 9/32　G09C 1/00 640B
H04L 9/00 675C

請求項の数 32　(全 26 頁)

(21)出願番号　特願平9-285007
(22)出願日　平成9年10月17日(1997.10.17)
(65)公開番号　特開平11-119649
(43)公開日　平成11年4月30日(1999.4.30)
審査請求日　平成11年6月10日(1999.6.10)

前置審査

(73)特許権者　000005496
富士ゼロックス株式会社
東京都港区赤坂二丁目１７番２２号
(74)代理人　100086531
弁理士　澤田　俊夫
(74)代理人　100093241
弁理士　宮田　正昭
(74)代理人　100101801
弁理士　山田　英治
(72)発明者　寺尾　太郎
神奈川県足柄上郡中井町境４３０　グリーンテクなかい　富士ゼロックス株式会社内
(72)発明者　申　吉浩
神奈川県足柄上郡中井町境４３０　グリーンテクなかい　富士ゼロックス株式会社内
最終頁に続く

(54)【発明の名称】認証方法および装置

(57)【特許請求の範囲】
【請求項１】
ｐを素数、F_pをｐ元体、Ｇを零化域を求めることが計算量的に困難な有限アーベル群、Ｄをコミットメントの空間、πをＧからＤへの写像として、コミットメントｒ∈Ｄを生成し、ドキュメントｍとチャレンジｃ∈F_pに対してレスポンスｓ∈Ｇを生成し、検証情報Ｉ∈Ｇ、コミットメントｒおよびレスポンスｓに基づいて検証側装置および証明側装置の間で認証を行う認証方法であって、
（ａ）上記証明側装置の非再現性秘密情報生成部（図３の３０４）により非再現性秘密情報ｋ∈Ｇをランダムに生成するステップと、
（ｂ）上記（ａ）のステップで生成した非再現性秘密情報ｋを用いて上記証明装置のコミットメント計算部（図３の３０５、３０６）によりコミットメントｒ＝π（k^p）を計算するステップと、
（ｃ）上記証明側装置のドキュメント秘密情報計算部（図３の３０７）により、ｆをＧへの秘密関数として、ドキュメント秘密情報μ＝ｆ（ｍ）を計算するステップと、
（ｄ）上記（ａ）のステップで生成した非再現性秘密情報ｋおよび上記（ｃ）のステップで生成したドキュメント秘密情報μを用いて上記証明側装置の補助レスポンス計算部（図３の３０５）により補助レスポンスσ＝ｋμ^cを計算するステップと、
（ｅ）検証情報Ｉに対して$I x^p = 1$を満たす認証の特徴情報ｘ∈Ｇと、ドキュメント秘密情報μとに基づいて生成された認証補助情報ｔ＝$x\mu^{-1}$を上記証明側装置において入力して上記証明側装置の記憶部（図２のｔのブロック）に記憶するステップと、

（ｆ）上記検証側装置（図２の１００）により生成されて送られてきたチャレンジｃ∈F_pを上記証明側装置において入力するステップと、
（ｇ）上記証明側装置のレスポンス計算部（図２のｓ＝σｆのブロック）においてレスポンスｓ＝σt^cを上記（ｆ）のステップにおいて入力されたチャレンジｃ、上記（ｅ）のステップにおいて入力された認証補助情報ｔ、および上記（ｄ）のステップにおいて生成された補助レスポンスσから生成するステップと、
（ｈ）生成されて上記検証側装置に送られてきた上記レスポンスｓがｒ＝π（$s^p I^c$）であることを上記検証側装置により検証するステップとを有することを特徴とする認証方法。

【請求項２】
ｐを素数、F_pをｐ元体、Ｇを零化域を求めることが計算量的に困難な有限アーベル群、Ｄをコミットメントの空間、πをＧからＤへの写像として、コミットメントｒ∈Ｄを生成し、ドキュメントｍとチャレンジｃ∈F_pに対してレスポンスｓ∈Ｇを生成し、検証情報Ｉ∈Ｇ、コミットメントｒおよびレスポンスｓに基づいて検証側装置および証明側装置の間で認証を行う、上記検証側装置および上記証明側装置からなる認証システムであって、
上記証明側装置は、
（ａ）非再現性秘密情報ｋ∈Ｇをランダムに生成する手段と、
（ｂ）上記（ａ）の手段で生成した非再現性秘密情報ｋを用いてコミットメントｒ＝π（k^p）を計算する手段と、
（ｃ）ｆをＧへの秘密関数として、ドキュメント秘密情報μ＝ｆ（ｍ）を計算する手段と、
（ｄ）上記（ａ）の手段で生成した非再現性秘密情報ｋおよび上記（ｃ）の手段で生成したドキュメント秘密情報μを用いて補助レスポンスσ＝ｋμ^cを計算する手段と、
（ｅ）検証情報Ｉに対してIx^pを満たす認証の特徴情報ｘ∈Ｇと、ドキュメント秘密情報μとに基づいて生成された認証補助情報ｔ＝ｘμ^{-1}を入力する手段と、
（ｆ）上記検証側装置からチャレンジｃ∈F_pを入力する手段と、
（ｇ）レスポンスｓ＝σt^cを上記（ｆ）の手段により入力されたチャレンジｃ、上記（ｅ）の手段により入力された認証補助情報ｔ、および上記（ｄ）の手段により生成された補助レスポンスσから生成する手段とを有し、
上記検証側装置は、
（ｈ）生成された上記レスポンスｓを上記証明側装置から受取り、上記レスポンスｓがｒ＝π（$s^p I^c$）であることを検証する手段を有することを特徴とする認証システム。

【請求項３】
請求項１記載の認証方法に用いられ、上記証明側装置の一部を構成する耐タンパー性の対話装置において実行される対話方法であって、
上記対話方法は、ｐを素数、F_pをｐ元体、Ｇを零化域を求めることが計算量的に困難な有限アーベル群、Ｄをコミットメントの空間、πをＧからＤへの写像として、コミットメントｒ∈Ｄを生成し、ドキュメントｍとチャレンジｃ∈F_pに対して補助レスポンスσ∈Ｇを生成するものであり、
上記耐タンパー性の対話装置は、情報の入出力手段と、情報の記憶手段と、乱数を生成する手段と、Ｇにおける算法を実行する手段と、πを計算する手段と、固有の秘密関数ｆを計算する手段とを備え、これら各手段を用いて、
（ａ）非再現性秘密情報ｋ∈Ｇをランダムに生成するステップと、
（ｂ）上記（ａ）のステップにより生成された上記非再現性秘密情報ｋを用いてコミットメントｒ＝π（k^p）を計算するステップと、
（ｃ）ｆをＧへの秘密関数として、ドキュメント秘密情報μ＝ｆ（ｍ）を計算するステップと、
（ｄ）上記（ａ）のステップにより生成された上記非再現性秘密情報ｋおよび上記（ｃ）のステップにより生成された上記ドキュメント秘密情報μを用いて補助レスポンスσ＝ｋμ^cを計算するステップとを実行することを特徴とする対話方法。

【請求項４】
ｐ＝２であることを特徴とする請求項３に記載の対話方法。
【請求項５】
ｐがＧの零化域の生成元λと互いに素であることを特徴とする請求項３に記載の対話方法。
【請求項６】
Ｇが合成数ｎを法とする有理整数環の剰余類環の乗法群（Ｚ／ｎＺ）＊であることを特徴とする請求項３に記載の対話方法。
【請求項７】
Ｇが合成数ｎを法とする有理整数環の剰余類環Ｚ／ｎＺ上の群概型ＥのＺ／ｎＺに値を持つ点のなす群Ｅ（Ｚ／ｎＺ）であることを特徴とする請求項３に記載の対話方法。
【請求項８】
πが恒等写像であり、ることを特徴とする請求項３に記載の対話方法。
【請求項９】
特に、πがハッシュ関数を用いて計算されることを特徴とする請求項３に記載の対話方法。
【請求項１０】
請求項３記載の対話方法を実行するために上記証明側装置の一部として用いられ、コミットメントｒを出力し、ドキュメントｍとチャレンジｃとを入力し、補助レスポンスσを出力する対話装置であって、
（ａ）情報の入出力手段と、
（ｂ）情報の記憶手段と、
（ｃ）乱数を生成する手段と、
（ｄ）Ｇにおける算法を実行する手段と、
（ｅ）πを計算する手段と、
（ｆ）固有の秘密関数ｆを計算する手段とを備え、
これら（ａ）～（ｆ）の各手段を用いて、
非再現性秘密情報ｋ∈Ｇをランダムに生成し、
生成した非再現性秘密情報ｋを用いてコミットメントｒ＝π（ｋ^{p}）を計算し、
ｆをＧへの秘密関数として、ドキュメント秘密情報μ＝ｆ（ｍ）を計算し、
生成した非再現性秘密情報ｋおよび生成したドキュメント秘密情報μを用いて補助レスポンスσ＝ｋμ^{c}を計算することを特徴とする対話装置。
【請求項１１】
内部の実行処理過程が外部から観測することが困難であることを特徴とする請求項１０に記載の対話装置。
【請求項１２】
携帯可能な小型演算装置として構成されていることを特徴とする請求項１０に記載の対話装置。
【請求項１３】
固有の秘密関数ｆを計算する手段は、
（ａ）固有の秘密情報ｄを保持する手段と、
（ｂ）ハッシュ関数ｈを計算する手段と、
からなり、ドキュメント秘密情報μが、固有の秘密情報ｄとドキュメントｍよりハッシュ関数ｈを用いて計算されることを特徴とする請求項１０に記載の対話装置。
【請求項１４】
請求項１０に記載の対話装置に、さらに、ドキュメントｍに応じた処理を行なう手段を備えたことを特徴とする対話装置。
【請求項１５】
ドキュメントｍがＧ、ｐ、πの少なくとも一部を規定することを特徴とする請求項１４に記載の対話装置。

【請求項１６】
ドキュメントｍがレスポンス生成の条件を規定することを特徴とする請求項１４に記載の対話装置。
【請求項１７】
請求項１０記載の対話装置に認証用補助情報ｔ（ただしｔ∈Ｇ）を発行する認証用補助情報発行方法において、
情報の入出力手段と、情報の記憶手段と、固有の秘密関数ｆを計算する手段と、Ｇにおける算法を実行する手段とを用い、
（ａ）ドキュメント秘密情報μ＝ｆ（ｍ）を計算するステップと、
（ｂ）上記（ａ）のステップｐで生成された上記ドキュメント秘密情報μを用いて認証用補助情報$t = x\mu^{-1}$（ただし検証情報Ｉ∈Ｇに対応する認証の特徴情報ｘ∈Ｇは$Ix^{p}=1$を満たす）を計算するステップと、
からなることを特徴とする認証用補助情報発行方法。
【請求項１８】
ドキュメントｍが認証の特徴情報ｘに依存することを特徴とする請求項１７に記載の認証用補助情報発行方法。
【請求項１９】
ドキュメントｍが認証の特徴情報ｘを識別する情報を含むことを特徴とする請求項１７に記載の認証用補助情報発行方法。
【請求項２０】
請求項１０記載の対話装置に対して認証用補助情報ｔ（ただしｔ∈Ｇ）を発行する認証用補助情報発行装置において、
（ａ）情報の入出力手段と、
（ｂ）情報の記憶手段と、
（ｃ）固有の秘密関数ｆを計算する手段と、
（ｄ）Ｇにおける算法を実行する手段と、
を備え、
認証の特徴情報ｘとドキュメントｍと対話装置を識別する情報とを受取り、
受け取った上記ドキュメントｍを用いてドキュメント秘密情報μ＝ｆ（ｍ）を計算し、
受け取った上記特徴情報ｘおよび計算した上記ドキュメント秘密情報μを用いて認証用補助情報$t = x\mu^{-1}$（ただし検証情報Ｉ∈Ｇに対応する認証の特徴情報ｘ∈Ｇは$Ix^{p}=1$を満たす）を計算し、
計算した上記認証用補助情報ｔを出力することを特徴とする認証用補助情報発行装置。
【請求項２１】
請求項１７の認証用補助情報発行方法により、検証情報$I_1 \ldots I_N$（ただし$I_i \in G$）に対応して請求項１０の対話装置に対応して生成された認証用補助情報$I_1, t_1, \ldots, I_N, t_N$（ただし$t_i \in G$）を、Ｇおける算法を実行する手段を用いて、合成された検証情報$I = I_1 \cdots I_N$に対応する合成された認証用補助情報ｔを$t = t_1 \cdots t_N$として生成することを特徴とする認証用補助情報合成方法。
【請求項２２】
複数のドキュメント$m_1, \ldots, m_N$に対して、ドキュメント秘密情報$\mu = f(m_1) \cdots f(m_N)$を計算することを特徴とする請求項１０に記載の対話装置。
【請求項２３】
請求項１記載の認証方法を実行する為に実行される証明方法であって、請求項１０に記載の対話装置と請求項１７あるいは請求項２１に記載の検証情報Ｉに対する認証用補助情報ｔとドキュメントｍとを用いて、コミットメントｒを生成し、チャレンジｃに対して、レスポンスｓを$r = \pi(s^{p} I^{c})$を満たすように生成する証明方法であって、
（ａ）請求項１０記載の対話装置を用いて、コミットメントｒを取得するステップと、
（ｂ）請求項１０記載の対話装置を用いて、ドキュメントｍとチャレンジｃに対応する補助レスポンスσを取得するステップと、

（ｃ）レスポンスｓ＝ｔ^{c} σを計算するステップと、
からなることを特徴とする証明方法。
【請求項２４】
請求項１記載の認証方法を実行する為に用いられる証明装置であって、
（ａ）情報の入出力手段と、
（ｂ）情報の記憶手段と、
（ｃ）Ｇにおける算法を実行する手段と、
を備え、
認証用補助情報ｔとドキュメントｍを保持し、
請求項１０記載の対話装置を用いて、コミットメントｒを取得し、
取得した上記コミットメントｒを出力し、
チャレンジｃを入力し、
請求項１０記載の対話装置を用いて、上記ドキュメントｍと上記チャレンジｃに対応する補助レスポンスσを取得し、
取得した上記補助レスポンスσからレスポンスｓ＝ｔ^{c} σを計算し、
計算した上記レスポンスｓを出力することを特徴とする証明装置。
【請求項２５】
Ｍをメッセージの空間、φをＧとＭとの積からＦ$_{p}$ への写像として、請求項１０に記載の対話装置と請求項１７あるいは請求項２１に記載の検証情報Ｉに対する認証用補助情報ｔとドキュメントｍとを用いて、メッセージＭに対する署名（ｒ，ｓ）を
【数１】

$$r = \pi(s^{p} I \phi(r, M))$$

を満たすように生成する署名生成方法であって、
情報の入出力手段と、情報の記憶手段と、Ｇにおける算法を実行する手段と、πを計算する手段とを用いて、
（ａ）請求項１０記載の対話装置から送出されるコミットメントｒを取得するステップと、
（ｂ）上記コミットメントｒおよびメッセージＭとからチャレンジｃ＝φ（ｒ、Ｍ）を計算するステップと、
（ｃ）請求項１０記載の対話装置から送出される、ドキュメントｍとチャレンジｃに対応する補助レスポンスσを、取得するステップと、
（ｄ）上記チャレンジｃおよび上記補助レスポンスσからレスポンスｓ＝ｔ^{c} σを計算するステップと、
からなりレスポンスｓを署名として出力することを特徴とする署名生成方法。
【請求項２６】
φがハッシュ関数を用いて計算されることを特徴とする請求項２５に記載の署名生成方法。
【請求項２７】
請求項２５記載の署名生成方法を実行する装置であって、
（ａ）情報の入出力手段と、
（ｂ）情報の記憶手段と、
（ｃ）Ｇにおける算法を実行する手段と、
（ｄ）πを計算する手段と
を備え、
認証用補助情報ｔとドキュメントｍを保持し、
請求項１０記載の対話装置を用いて、コミットメントｒを取得し、
チャレンジｃ＝φ（ｒ、Ｍ）を計算し、
請求項１０記載の対話装置を用いて、ドキュメントｍとチャレンジｃに対応する補助レスポンスσを取得し、

上記チャレンジｃと上記補助レスポンスσとからレスポンスｓ＝ｔ^{c} σを計算して署名生成を実行することを特徴とする署名生成装置。
【請求項２８】
請求項１７あるいは請求項２１に記載の検証情報Ｉに対する認証用補助情報ｔの検証方法であって、
情報の入出力手段と、情報の記憶手段と、乱数を生成する手段と、Ｇにおける算法を実行する手段とを用い、
（ａ）コミットメントｒを取得するステップと、
（ｂ）チャレンジｃをランダムに生成するステップと、
（ｃ）補助レスポンスσを取得するステップと、
（ｄ）上記（ａ）のステップにより取得したコミットメントｒと、上記（ｂ）のステップにより生成したチャレンジｃと上記（ｃ）のステップにより取得した補助レスポンスσとを用いてｒ＝π（（σｔ^{c}）^{p}Ｉ^{c}）を確認するステップと、
を実行することを特徴とする認証用補助情報検証方法。
【請求項２９】
請求項１７あるいは請求項２１に記載の検証情報Ｉに対する認証用補助情報ｔを検証する検証装置であって、
（ａ）情報の入出力手段と、
（ｂ）情報の記憶手段と、
（ｃ）乱数を生成する手段と、
（ｄ）Ｇにおける算法を実行する手段と、
（ｅ）πを計算する手段と、
を備え、
検証情報Ｉと認証用補助情報ｔを保持し、
コミットメントｒを取得し、
チャレンジｃをランダムに生成して出力し、
補助レスポンスσを取得し、
上記検証情報Ｉ、上記認証用補助情報ｔ、上記コミットメントｒおよび上記チャレンジｃを用いて補助レスポンスσｒ＝π（（σｔ^{c}）^{p}Ｉ^{c}）を確認して認証用補助情報ｔの検証を実行することを特徴とする認証用補助情報検証装置。
【請求項３０】
πが恒等写像である場合には、πを計算する手段を省略した請求項１０記載の対話装置。
【請求項３１】
πが恒等写像である場合には、πを計算する手段を省略した請求項２７記載の署名生成装置。
【請求項３２】
πが恒等写像である場合には、πを計算する手段を省略した請求項２９記載の認証用補助情報検証装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は、情報セキュリティ技術に関するものであり、特に、零化域決定問題の困難性に安全性の根拠を置く認証方式において、システムの利用者に秘密情報に基づいた証明者の機能を付与しながら秘密情報自体を隠蔽することを可能にする方法および装置に関するものである。
【０００２】
【従来の技術】
［従来技術の概要］
従来の公開鍵暗号における復号鍵、署名における署名鍵、認証における認証鍵は、これらの秘密情報を所持するものであることを認証するための特徴情報である。

【０００３】
例えば、ＧｕｉｌｌｏｕとＱｕｉｓｑｕａｔｅｒによって「伝送量および記憶量を最小化する機密化マイクロプロセッサに適合した実用的な零知識プロトコル」（”Ａ ｐｒａｃｔｉｃａｌ ｚｅｒｏ－ｋｎｏｗｌｅｄｇｅ ｐｒｏｔｏｃｏｌ ｆｉｔｔｅｄ ｔｏ ｓｅｃｕｒｉｔｙ ｍｉｃｒｏｐｒｏｃｅｓｓｏｒ ｍｉｎｉｍｉｚｉｎｇｂｏｔｈ ｔｒａｎｓｍｉｓｓｉｏｎ ａｎｄ ｍｅｍｏｒｙ”）、Ａｄｖａｎｃｅｓ ｉｎ Ｃｒｙｐｔｏｌｏｇｙ ＥＵＲＯＣＲＹＰＴ’８７、Ｃ．Ｇ．Ｇｕｅｎｔｈｅｒ（ｅｄ．）、Ｓｐｒｉｎｇｅｒ－Ｖｅｒｌａｇ、ｐｐ．１２３－１２８で提案された認証方式を例にとって説明する。この文献でも、暗号分野に慣用されているように、検証者（ベリファイヤ）や証明者（プルーバ）の用語を用いるが、これらは、その計算の質、量から、また上記文献のタイトルからも明らかなように、計算機装置である。以下の説明においても、検証者、証明者の用語を用いるが、これは検証を行なう装置（検証側装置）および証明を行なう装置（証明側装置）と等価である。

【０００４】
図１は、この認証方式の流れを説明する図である。

【０００５】
ｎを素因数分解の困難な合成数、Ｇを有理整数環のｎを法とする剰余類環の乗法群（Ｚ／ｎＺ）*、ｐをｎのＣａｒｍｉｃｈａｅｌ関数λ（ｎ）を割らない素数、Ｄをコミットメントの空間、πをＧからＤへの関数、Ｉ∈Ｇを公開の検証情報として、$Ｉｘ^{ｐ}＝１$を満たすｘ∈Ｇを認証の特徴情報とする。

【０００６】
認証の特徴情報ｘの保持者は、以下の証明者２００の動作を行なうことができる：
１．乱数ｋ∈Ｇを生成し、コミットメントｒ＝π（ｋp）を送る。

【０００７】
２．与えられたチャレンジ$ｃ∈Ｆ_{ｐ}$に対して、レスポンス$ｓ＝ｋｘ^{ｃ}$を送る。

【０００８】
検証情報Ｉを知り得るものは誰でも、以下の検証者１００の動作を行なうことによって、証明者の動作を検証することが可能であり、証明者が確かに認証の特徴情報を保持することを確かめることができる。

【０００９】
１．コミットメントｒを与えられた後に、ランダムに生成したチャレンジ$ｃ∈Ｆ_{ｐ}$を証明者に送る。

【００１０】
２．与えられたレスポンスｓが$ｒ＝π（ｓ^{ｐ}Ｉ^{ｃ}）$を満たすことを確かめる。

【００１１】
これらの技術は、上記の秘密情報を所持するものが、これを公開しないことを前提に作られている。それゆえに、これらの秘密情報を所持するもののみが復号できる暗号文、これらの秘密情報を所持するもののみが生成できる署名や、これらの秘密情報を所持するもの以外の誰にもなりすませない認証が可能となる。

【００１２】
したがって、上記技術は、これらの秘密情報の所持者にとって、これを暴露することが不利益な状況である場合にのみ利用できる。このような状況の典型的な例は、上記秘密情報が、特定の個人のみが所持するものであり、その個人を認証する特徴情報である場合である。

【００１３】
この場合、上記特徴情報はちょうど自宅の鍵や個人の印鑑のような役割を担っている。実際、実世界における鍵や印鑑をディジタル情報として構成することは、これらの暗号学的手法の直接的な応用として実現できることは易しい。たとえば、自宅の錠を上記Ｇｕｉｌｌｏｕ－Ｑｕｉｓｑｕａｔｅｒの方式における検証者として構成し、検証に成功した場合のみ開錠するように構成すれば、認証の特徴情報ｘの所持は、ちょうど自宅の鍵の所持に

対応することになる。
【００１４】
［従来技術の問題点］
上記の、個人の自宅の鍵のように、認証の特徴情報の暴露が個人の不利益になる場合とは逆に、その暴露が暴露したものの利益につながる場合が存在する。それは、認証するものが、特定のサービスを受ける権利や資格である場合である。
【００１５】
この場合、上記の個人を認証する例と同様に、権利や資格を持つものに、権利や資格を表す特徴情報を配布し、その特徴情報を所持していることを検証するというやりかたはとれない。なぜなら、特徴情報の暴露が、特徴情報の所持者には不利益にならないため、特徴情報を権利や資格を持たない第三者に教え、その第三者から利益を得るといった不正行為が可能であるからである。
【００１６】
したがって、従来は、上記の公開鍵暗号技術をそのまま使った認証方式を取らず、以下の３種の方式をとっていた。
【００１７】
▲１▼第１の方法は、個人が個人に帰属する秘密の特徴情報を保持し、権利や資格の保持を検証する側が、権利や資格を保持している個人とその個人が持つ秘密の特徴情報を保持する方法である。この方法によれば、特徴情報を漏洩させることは個人にとって不利益になるので、権利や資格の認証に利用可能である。
【００１８】
▲２▼第２の方法は、個人が個人に帰属する秘密の特徴情報を保持し、権利や資格の保持を検証する側が、権利や資格を保持している個人とその個人が持つ秘密の特徴情報に対応する公開情報を保持する方法である。この方法によれば、特徴情報を漏洩させることは個人にとって不利益になるので、権利や資格の認証に利用可能である。
【００１９】
▲３▼第３の方法は、権利や資格を付与するものが、自身が持つ特徴情報で作成した署名を権利や資格を付与されるものに渡し、検証側が、その署名を検証することで、権利や資格を持つことを認証するものである。この方式の例としては、Ｄ．Ｃｈａｕｍによる”Ｏｎｌｉｎｅ Ｃａｓｈ Ｃｈｅｃｋｓ”、Ａｄｖａｎｃｅｓ ｉｎ Ｃｒｙｐｔｏｌｏｇｙ ＥＵＲＯＣＲＹＰＴ’８９、Ｊ．Ｊ．Ｑｕｉｓｑｕａｔｅｒ、Ｊ．Ｖａｎｄｅｗａｌｌｅ（ｅｄ．）、Ｓｐｒｉｎｇｅｒ－Ｖｅｒｌａｇ、ｐｐ．２８８－２９３がある。
【００２０】
この方法によれば、権利や資格の所持を証明する側が、特徴情報を持たないので、特徴情報の漏洩の問題は起こらない。
【００２１】
しかし、第１の方法では、検証側が権利や資格を保持しているもののリストを保持しなければならない。これは、リストの記憶と管理の負荷を検証側に課すことになり、必然的に高性能な検証装置を必要とすることになる。また、権利や資格を付与するものと独立に検証装置を作ることができないので、検証装置と、権利や資格を付与するものとの間の情報の交換が、常に必要になる。
【００２２】
また、検証側が個人の特徴情報を持つことになるので、この方法によって認証される個人は、検証側による不正な特徴情報の漏洩のリスクを負うことになる。
【００２３】
第２の方法では、検証側が権利や資格を保持しているもののリストを保持しなければならない。これは、リストの記憶と管理の負荷を検証側に課すことになり、必然的に高性能な検証装置を必要とすることになる。また、権利や資格を付与するものと独立に検証装置を作ることができないので、検証装置と、権利や資格を付与するものとの間の情報の交換が、常に必要になる。

【００２４】
第３の方法では、配布した署名情報は誰によっても使用可能なので、その複製を防がなければならない。これは、署名値の二重使用を防ぐという方法で行われる。具体的には、一度認証に使用された署名値をすべて検証側で記憶し、検証側が二重使用でないことをチェックできるようにする。しかし、この機能を検証側に設けるためには、必然的に高性能な検証装置を必要とすることになる。また、同じ権利や資格を認証する全ての検証装置で、一度認証に使用された署名値のリストを共有しなければならず、検証装置同士の情報の交換が、常に必要となる。
【００２５】
このように、従来の３つの方式には、どれも重大な問題があり、とくに検証側を小規模な装置やソフトウエアで構成することを困難にしている。
【００２６】
これに対し、前述の権利や資格を示す特徴情報を使った認証の方式は、検証側で行うことが権利や資格を示す特徴情報を保持していることの認証だけで済むので、有利である。
【００２７】
以上述べたとおり、従来の技術では、権利や資格を認証する場合に、小規模の検証装置で構成すると認証の特徴情報が第三者に洩れる危険があり、その危険をなくそうとすれば、検証装置が大規模なものになるという問題点があった。
【００２８】
【発明が解決しようとする課題】
以上に説明してきたように、本発明は、小規模な検証装置で、権利や資格を認証する場合にも、認証の特徴情報が第三者に洩れることのない認証方法および装置を提供することを目的としている。
【００２９】
【課題を解決するための手段】
本発明の認証方法および装置は、
１．チケットの発行時に定められ、公開可能な情報であるドキュメントよりドキュメント秘密情報を生成し、ドキュメント秘密情報に基づいて対話を行なう対話装置と、
２．ドキュメント秘密情報と認証の特徴情報より生成され、公開可能な情報であるチケットとを利用するものである。
【００３０】
【発明の実施の形態】
実施例の詳細な説明に入る前に、本発明の利用形態について簡略に説明する。
【００３１】
図２は、本発明の全体の構成を表している。ここでも、検証者および証明者の用語を用いるが、検証者１００は検証側の装置を構成する計算機資源であり、証明者２００は対話装置３００とともに証明側の装置を構成する計算機資源であることは明らかである。
【００３２】
チケット発行者は、固有の秘密関数で特徴付けられる対話装置３００を発行し、利用者に配布する。対話装置３００を特徴付ける秘密関数が利用者に知られると、対話装置３００の複製が自由に行なえて、チケット発行者の制御不能なチケットの濫用が可能となる。そこで、対話装置３００の秘密関数は、対話装置３００の正当な保持者であっても、これを窃取することができないように保護されるようにできる。対話装置３００は、例えば、スマートカード（ＩＣカード）として構成しても良い。
【００３３】
対話装置３００は、ドキュメントと呼ばれるデータｍを入力されると、その対話装置３００に固有の秘密関数ｆを用いてドキュメント秘密情報を生成し、ドキュメント秘密情報に基づいた対話を行なう。
【００３４】
対話は具体的には、

１．　コミットメントｒの出力
２．　チャレンジｃの入力
３．　レスポンスσの出力
という形になっている。
【００３５】
Ｇｕｉｌｌｏｕ－Ｑｕｉｓｑｕａｔｅｒ認証における証明者の行なう対話と形の上では同一である。Ｇｕｉｌｌｏｕ－Ｑｕｉｓｑｕａｔｅｒ認証については図１に示した。
【００３６】
Ｇｕｉｌｌｏｕ－Ｑｕｉｓｑｕａｔｅｒ認証における証明者２００の行なう対話においても、対話の基となる認証の特徴情報ｘは第三者には公開されないが、対応する検証情報Ｉは公開され、その検証情報に基づいて対話の真正性、つまり、対話が検証情報に対応する認証の特徴情報を用いて生成されたことを確認できるのに対し、本発明では、対話装置３００の対話の基となるドキュメント秘密情報に対応する検証情報はあらかじめ与えられているわけではないことに注意されたい。
【００３７】
ドキュメントは、必ずしも、ドキュメント秘密情報を生成するために利用されるだけとは限らない。例えば、ドキュメントは対話装置３００が実行可能なプログラムやコマンド、あるいは、対話装置３００の行なう処理のパラメータなどでありえる。
【００３８】
チケット発行者が、認証の特徴情報ｘに対応付けてチケットｔを発行するときは、認証の特徴情報に基づく対話（ｒ，ｃ，ｓ）を生成する機能を、以下に述べる方法で利用者に頒布することによって実現する。
【００３９】
チケット発行者は、チケット発行装置４００を用いて、利用者の所持する対話装置３００の秘密関数ｆと対話を生成する際に対話装置３００に伝達すべきドキュメントｍよりドキュメント秘密情報μを算出し、認証の特徴情報ｘとドキュメント秘密情報μより生成したチケットｔを利用者に発行する。
【００４０】
認証の特徴情報ｘとドキュメント秘密情報とは、利用者に対して秘匿される。
【００４１】
利用者は、指定されたドキュメントｍを対話装置３００に入力することによって、対話（ｒ，ｃ，σ）を生成し、発行されたチケットｔを用いて、その対話（ｒ，ｃ，σ）をチケットの対応する認証の特徴情報に基づいた対話（ｒ，ｃ，ｓ）へ変換する。
【００４２】
ドキュメントに対話装置３００への処理の指示が記述される場合、チケットを用いた対話生成はドキュメントに記述された指示に関係付けられ、これによってチケットの有効性に条件を付けることが可能となる。
【００４３】
対話の変換は、具体的には、チャレンジｃと対話装置３００のレスポンスσとチケットｔとより、レスポンスｓを計算することにより可能となる。
【００４４】
変換された対話（ｒ，ｃ，ｓ）が、図１におけるＧｕｉｌｌｏｕ－Ｑｕｉｓｑｕａｔｅｒ認証の証明者が生成する対話に他ならないことを実施例において説明する。
【００４５】
チケットの対応する認証の特徴情報ｘは、各々の対話装置３００の様々なドキュメント毎にことなるドキュメント秘密情報とは独立に生成される。
【００４６】
チケット発行者は、任意の認証の特徴情報ｘに基づく対話の機能を、認証の特徴情報自体を開示することなく任意のドキュメントと対応付けてチケットの形で利用者に頒布することができる。

【００４７】
［実施例］
［基本構成要素］
本発明においては、
ｐ：　素数
F_p：　ｐ元体
Ｇ：　零化域の決定が計算量的に困難なアーベル群
Ｄ：　コミットメントの空間
π：　ＧからＤへの写像
が暗号学的な基本構成要素である。
【００４８】
以後、特に説明せずに使用される数学的な概念はいずれも基本的なものであるのでとくに説明しない。例えば、岩波数学辞典第３版、日本数学会編集、岩波書店を参照されたい。
【００４９】
一般に、アーベル群Ｇの零化域Ａｎｎ（Ｇ）とは、群の算法を乗法的に記すとして、
【００５０】
【数２】
$Ann(G) = \{l \in Z ; (\forall g \in G)\ g^l = 1\}$
（ここで「ｌ」はアルファベットＬの小文字である）
で定義される有理整数環Ｚのイデアルであり、有理整数環は単項イデアル整域であるので、Ａｎｎ（Ｇ）の生成元λ∈ＺによってＡｎｎ（Ｇ）＝λＺと書ける（ここにλＺはλの倍元の全体）。零化域を決定することは、Ａｎｎ（Ｇ）の生成元λ∈Ｚを求めることに他ならない。
【００５１】
ｎ∈Ｚを合成数とし、Ｇを、ｎを法とする有理整数環の剰余類環の乗法群$(Z/nZ)^*$としたとき、λ＝λ（ｎ）となる。ここにλ（ｎ）はｎのＣａｒｍｉｃｈａｅｌ関数であり、ｎが２の冪の場合は
【００５２】
【数３】

$$\lambda(n) = \begin{cases} 1 & n = 2 \\ 2 & n = 4 \\ n/4 & n \notin \{2,4\} \end{cases}$$

であり、ｎが奇素数ｐの冪の場合はλ（ｎ）＝ｎ（１－p^{-1}）であり、一般のｎに対しては、$n = \Pi p^{e_p}$をｎの素因数分解とすると、λ（ｎ）はλ（p^{e_p}）の最小公倍数である。
【００５３】
したがって、ｎの素因数分解を既知とすれば、Ｇの零化域をｌｏｇ（ｎ）の多項式時間で求めることができ、また、逆に、零化域の生成元λを既知とすると、非自明な１の平方根、つまり、
【００５４】
【数４】

$$g \in G;\ g \notin \{1,-1\};\ g^2 = 1$$

:
を満たすｇを生成することによって、ｌｏｇ（ｎ）の確率的多項式時間でｎの素因数分解を求めることができることから、この場合の零化域決定問題は計算量的に困難であると期待できる。

【００５５】
また、p_1，p_2を$p_1 \equiv p_2 \equiv 2 \mod 3$となる相異なる奇素数、$n = p_1 p_2$、ｂをｎと互いに素な整数、Ｅを同次式
【００５６】
【数５】
$$Y^2 Z = X^3 + bZ^3$$
でＺ＝ｎＺ上に定義されるアーベル概型，つまり、
【００５７】
【数６】
$$E = Proj(Z/nZ[X, Y, Z] / (Y^2 Z - X^3 - bZ^3))$$
とし、ＧをＥのＺ／ｎＺ値点のなす有限群Ｅ（Ｚ／ｎＺ）としたとき、λは$p_1 + 1$と$p_2 + 1$の最小公倍数であり、この場合も零化域決定問題は計算量的に困難であることが期待できる。
【００５８】
πは、例えば、恒等写像ｉｄ：Ｇ→Ｇとしても良いし、あるいは、ハッシュ関数ｈを用いてｈ：Ｇ→Ｄとしても良い。ハッシュ関数とは、ｈ（ｍ）＝ｈ（ｍ’）を満たす相異なるｍ，ｍ’を見い出すことが計算量的に困難であることが期待されている関数であり、例えば、ＲＳＡ Ｄａｔａ Ｓｅｃｕｒｉｔｙ Ｉｎｃ．によるＭＤ５や米国連邦政府による規格ＳＨＳ（Ｓｅｃｕｒｅ Ｈａｓｈ Ｓｔａｎｄａｒｄ）が良く知られている。
【００５９】
πが恒等写像である場合は、もちろん、πを計算するコストは不要である。また、πがハッシュ関数であり、Ｄの元を表現するのに必要なビット長がＧの元を表現するのに必要なビット長より小さい場合には通信量を削減する効果がある。例えば、素因数分解の困難な１０２４ビット程度の合成数ｎに対して、$G = (Z/nZ)^*$とし、πとしてＳＨＳを用いれば、コミットメントｒのサイズを１６０ビットまで圧縮できる。
【００６０】
ちなみに、ｐのビット長は、質疑応答型の認証の場合は４０ビット程度、署名の場合でも１６０ビット程度で良く、これがＧｕｉｌｌｏｕ－Ｑｕｉｓｑｕａｔｅｒ認証が高速に行なえることの根拠となっている。
【００６１】
［対話装置］
図３は対話装置３００の構成を示している。対話装置３００は耐タンパー性を有する容器として実装され、固有の秘密関数によって特徴付けられて、利用者に配布される。対話装置３００をスマートカード（ＩＣカード）などの携帯可能な小型演算装置として構成しても良い。対話装置３００は、入出力部３０１、記憶部３０２、ドキュメント処理部３０３、乱数生成部３０４、Ｇの算法実行部３０５、π計算部３０６、ｆ計算部３０７を含んで構成されている。
【００６２】
図４は対話装置３００の動作を示している。以下、対話装置３００の動作を説明する。
１．　乱数生成部３０４を用いて、非再現性秘密情報$k \in G$を生成し、記憶部３０２に保持する。
２．　Ｇにおける算法実行部３０５とπの計算部３０６を用いて、記憶部３０２に保持された非再現性秘密情報ｋからコミットメントｒを
【００６３】
【数７】
$$r = \pi(k^p)$$
として計算し、記憶部３０２に保持する。もちろん、πが恒等写像である場合は、πの計算部３０６は不要である。
３．　入出力部３０１を用いて、記憶部３０２に保持されたコミットメントｒを出力する。

４．　入出力部３０１を用いて、チャレンジｃ∈Ｆ$_{p}$を入力し、記憶部３０２に保持する。
５．　入出力部３０１を用いて、ドキュメントｍを入力し、記憶部３０２に保持する。
６．　ドキュメント処理部３０３を用いて、記憶部に保持されたドキュメントｍに応じた処理を行なう。
７．　対話装置３００固有の秘密関数ｆの計算部３０７を用いて、記憶部３０２に保持されたドキュメントｍからドキュメント秘密情報μ∈Ｇを
【００６４】
【数８】
μ＝ｆ（ｍ）
として計算し、記憶部３０２に保持する。
【００６５】
関数ｆの計算部３０７は、例えば、対話装置３００固有の秘密情報ｄの記憶部とハッシュ関数ｈの計算部とで構成し、
【００６６】
【数９】
ｆ（ｍ）＝ｈ（ｄ｜ｍ）
を計算するようにしても良い。ここで、「｜」はビットの連結を表す。
８．　Ｇにおける算法実行部３０５を用いて、記憶部３０２に保持された非再現性秘密情報ｋとドキュメント秘密情報μとチャレンジｃからレスポンスσを
【００６７】
【数１０】
$\sigma = k\mu^{c}$
として計算し、記憶部３０２に保持する。
９．　入出力部３０１を用いて、記憶部３０２に保持されたレスポンスσを出力する。
【００６８】
動作６は、応用によっては、必ずしも必須ではない。したがって、ドキュメント処理部３０３を持たない対話装置３００の構成も可能である。
【００６９】
ドキュメント処理部３０３を設けることによって、対話毎に対話装置３０３の実行する処理を可変にでき、後述するチケットに多様な機能性を付与することができるようになる。
【００７０】
▲１▼動作の実行順序についての制約
動作１ないし動作９は、必ずしもこの順序で逐次的になされる必要はない。動作「い」が動作「こ」に先だって実行されなければならないという順序関係を
【００７１】
【数１１】
い→こ
で表すものとして、諸動作の実行順序についての制約を説明する。
【００７２】
【数１２】
１→２→３→４
５→６，７
４，７→８→９
は常に満たされなければならない実行順序についての制約となっている。
【００７３】
ドキュメント処理部３０３の動作が他の動作に影響を与える場合は、さらに、以下に説明するような実行順序の制約が生じる。
【００７４】
▲２▼Ｇ，ｐ，πが可変な場合

ドキュメントｍが、Ｇを規定する場合、６→２が要請される。これは、ドキュメントｍにＧを規定するパラメターが記述されており、動作６において、これらのパラメターが設定され、Ｇにおける算法実行部３０５は設定されたパラメターにしたがって計算を行なえるように構成した場合である。

【００７５】

ドキュメントｍが、ｐを規定する場合、６→２が要請される。これは、ドキュメントｍにｐを規定するパラメターが記述されており、動作６において、これらのパラメターが設定され、Ｇにおける算法実行部３０５は設定されたパラメターにしたがって計算を行なえるように構成した場合である。

【００７６】

ドキュメントｍが、πを規定する場合、６→２が要請される。これは、ドキュメントｍにπを規定するパラメターが記述されており、動作６において、このパラメターが設定され、πの計算部は設定されたパラメターにしたがって計算を行なえるように構成した場合である。

【００７７】

これらの例では、Ｇ，ｐ，πは対話の都度に可変だが、これらを固定する構成も、もちろん可能である。

【００７８】

▲３▼冪計算の事前実行

ここでは、Ｇ，ｐ，πは固定されたものとする。

【００７９】

記憶部３０２に非再現性秘密情報とコミットメントの組（ｋ，ｒ）を複数保持することができるならば、動作１および動作２をこの順序で予め繰り返し実行しておくことによって、チャレンジｃが入力される直前にコミットメントｒを生成しなくて良いので、対話装置３００の対話に要する時間を短縮することができる。

【００８０】

また、対話装置３００の装置毎に固有な部分は秘密関数ｆのみであり、コミットメントｒの生成部分を分離して共有化することができる。

【００８１】

図８は冪計算部を分離した構成を示している。この構成例では、対話装置３００は、レスポンス生成部３０８およびコミットメント生成部３０９に分かれ、動作１および動作２はコミットメント生成部３０９において行なわれる。なお、図８において図３に対応する箇所には対応する符号を付した。

【００８２】

コミットメント生成部３０９からレスポンス生成部３０８に、非再現性秘密情報ｋが秘密通信によって伝達される。レスポンス生成部３０８をスマートカードとして構成しても良い。

【００８３】

▲４▼レスポンス生成の条件が可変な場合

ドキュメントｍが、レスポンス生成の条件を規定する場合、これは、ドキュメントｍにレスポンス生成の条件が記述されており、動作６において、条件が満たされなければ、処理を中断するように構成すれば良い。

【００８４】

ドキュメントｍに応じた処理の具体例を述べる。

【００８５】

例えば、ドキュメントｍにレスポンスの生成を許すチャレンジｃの条件が記述されており、動作６において、情報記憶部３０２に保持されたチャレンジｃが条件を満たされなければ対話装置３００の処理を中断するように構成する。

【００８６】

レスポンスの生成を許すチャレンジの条件の例を挙げる。ドキュメントｍにレスポンス生

成の有効期限を規定するパラメターが記述されており、また、チャレンジｃをビット列として表現した場合の特定のビットフィールドを現在時刻の表現と見なし、有効期限と現在時刻を比較し、有効期限を過ぎていた場合は対話装置の処理を中断するように構成する。

【００８７】

また、例えば、ドキュメント処理部が現在時刻を保持する計時部を持ち、ドキュメントｍにレスポンス生成の有効期限を規定するパラメターが記述されており、動作６において、有効期限と現在時刻を比較し、有効期限を過ぎていた場合は対話装置の処理を中断するように構成する。

【００８８】

また、例えば、ドキュメント処理部がカウンターを持ち、ドキュメントｍにカウンターの値をディクリメントするかしないかを規定するフラグが記述されており、動作６において、フラグがディクリメントを指示した場合、カウンターの値が０でなければ、カウンターの値を１だけディクリメントし、０であれば対話装置３００の処理を中断するように構成する。

【００８９】

また、例えば、ドキュメント処理部３０３がカウンターを持ち、ドキュメントｍにカウンターをディクリメントする値が記述されており、動作６において、カウンターの値がディクリメントする値より小さくなければカウンターの値を指示された値だけディクリメントし、そうでなければ対話装置３００の処理を中断するように構成する。

【００９０】

また、例えば、ドキュメント処理部３０３が複数のカウンターを持ち、ドキュメントｍに対応するカウンターを規定するポインターが記述されており、動作６において、規定されたカウンターの値が０でなければ、カウンターの値を１だけディクリメントし、０であれば対話装置３００の処理を中断するように構成する。

【００９１】

また、例えば、ドキュメント処理部が複数のカウンターを持ち、ドキュメントｍに対応するカウンターを規定するポインターとディクリメントする値が記述されており、動作６において、規定されたカウンターの値がディクリメントする値より小さくなければカウンターの値を指示された値だけディクリメントし、そうでなければ対話装置３００の処理を中断するように構成する。

【００９２】

▲５▼ドキュメント処理のその他の例

例えば、ドキュメント処理部３０３がカウンターを持ち、ドキュメントｍにインクリメントする値が記述されており、動作６において、カウンターの値を指示された値だけインクリメントするように構成する。

【００９３】

また、例えば、ドキュメント処理部３０３が複数のカウンターを持ち、ドキュメントｍに対応するカウンターを規定するポインターとインクリメントする値が記述されており、動作６において、規定されたカウンターの値を指示された値だけインクリメントするように構成する。

【００９４】

また、例えば、ドキュメント処理部３０３が現在時刻を保持する計時部と履歴の保持部を持ち、ドキュメントｍに履歴を記録するか記録しないかを規定するフラグが記述されており、動作６において、フラグが履歴の記録を指示した場合、履歴の保持部に、計時部に保持された現在時刻とドキュメントｍのタプルを保持するように構成する。

【００９５】

▲６▼複数ドキュメントの一括処理

以上に述べた諸例では、一回の対話において一つのドキュメントｍしか関与しないが、複数のドキュメントm_1，．．．，m_Nが関与するように構成することも可能である。

【００９６】

図１０は、複数ドキュメントの一括処理を行なう対話装置の動作を示している。複数のドキュメントを一回の対話において扱う場合、動作５ないし動作７を以下の動作１０ないし動作１２に置き換えれば良い。

１０．　入出力部３０１を用いて、ドキュメント$m_1, \ldots, m_N$を入力し、記憶部３０２に保持する。

１１．　ドキュメント処理部３０３を用いて、記憶部３０２に保持されたドキュメント$m_1, \ldots, m_N$に応じた処理を順次行なう。

１２．　対話装置固有の秘密関数ｆの計算部３０７を用いて、記憶部３０２に保持されたドキュメント$m_1, \ldots, m_N$からドキュメント秘密情報$\mu \in G$を

【００９７】

【数１３】

$$\mu = f(m_1) \cdots f(m_N)$$

として計算し、記憶部３０２に保持する。

【００９８】

もちろん、複数のドキュメントを一回の対話において扱う場合には、各ドキュメントm_iに応じた処理の実行結果が競合しないようにしなければならない。

［チケット発行装置］

$I \in G$：　検証情報

$x \in G$：　認証の特徴情報

とする。ここで、認証の特徴情報ｘと検証情報Ｉとは、$Ix^p = 1$という関係を満たす。

【００９９】

Ｇの零化域Ａｎｎ（Ｇ）の生成元λを既知とする。ｐがλと互いに素ならば、

【０１００】

【数１４】

$$pd \equiv 1 \mod \lambda$$

を満たすｄが計算できるので任意の検証情報Ｉに対して、対応する認証の特徴情報ｘを

【０１０１】

【数１５】

$$x = I^{-d}$$

として求めることができる。

【０１０２】

ｐ＝２の場合も、$G = (Z/nZ)^*$でｎがＢｌｕｍ数ならば、Ｉをほとんど任意に定めることができる。詳しくは、Ｆｉａｔ　とＳｈａｍｉｒ　による”Ｈｏｗ　ｔｏ　ｐｒｏｖｅ　ｙｏｕｒｓｅｌｆ：ｐｒａｃｔｉｃａｌ　ｓｏｌｕｔｉｏｎｓ　ｔｏ　ｉｄｅｎｔｉｆｉｃａｔｉｏｎ　ａｎｄ　ｓｉｇｎａｔｕｒｅｐｒｏｂｌｅｍｓ”、Ａｄｖａｎｃｅｓ　ｉｎＣｒｙｐｔｏｌｏｇｙ　ＣＲＹＰＴＯ’８６、Ａ．Ｍ．Ｏｄｌｙｚｋｏ　（ｅｄ．）、Ｓｐｒｉｎｇｅｒ－Ｖｅｒｌａｇ、ｐｐ．１８６－１９４を参照されたい。

【０１０３】

図５はチケット発行装置４００の構成を示し、図６はチケット発行装置４００の動作を示している。チケット発行装置４００は入出力部４０１、記憶部４０２、Ｇの算法実行部４０３、ｆ計算部４０４を含んで構成されている。以下、チケット発行装置４００の動作を説明する。

１．　入出力部４０１を用いて、認証の特徴情報ｘを入力し、記憶部４０２に保持する。

２．　入出力部４０１を用いて、ドキュメントｍを入力し、記憶部４０２に保持する。

３．　入出力部４０１を用いて、対話装置３００の識別子Ｕを入力し、記憶部４０２に保持する。

４．　記憶部４０２に保持された識別子Ｕに対応する対話装置３００固有の秘密関数ｆの計算部４０４を用いて、記憶部４０２に保持されたドキュメントｍからドキュメント秘密情報μを

【０１０４】

【数１６】
μ＝ｆ（ｍ）
として計算し、記憶部４０２に保持する。
５．　Ｇにおける算法実行部４０３を用いて、記憶部４０２に保持された認証の特徴情報ｘとドキュメント秘密情報μからチケットｔを
【０１０５】
【数１７】
$t = x\mu^{-1}$
として計算し、記憶部４０２に保持する。
６．　入出力部４０１を用いて、記憶部４０２に保持されたチケットｔを出力する。
【０１０６】
対話装置３００固有の秘密関数ｆは、例えば、対話装置３００の項で述べたように対話装置３００固有の秘密情報ｄとハッシュ関数ｈを用いて、ｆ（ｍ）＝ｈ（ｄ｜ｍ）として計算するようにしても良い。
【０１０７】
対話装置３００固有の秘密情報ｄは、例えば、チケット発行者がランダムに生成し、対話装置の識別子Ｕとのタプル（Ｕ，ｄ）を保持するようにしても良い。
【０１０８】
また、チケット発行者の秘密情報Ｄを用いて、対話装置３００の識別子Ｕに対して、対話装置３００固有の秘密情報ｄを
【０１０９】
【数１８】
ｄ＝Ｕ｜Ｄ
としても良い。ただし、このようにｄを生成すると、対話装置３００の耐タンパー性が崩れた場合チケット発行者の秘密情報Ｄが漏洩するという問題をはらんでいる。
【０１１０】
ハッシュ関数ｈを用いて、
【０１１１】
【数１９】
ｄ＝ｈ（Ｕ｜Ｄ）
としてｄを生成すれば、対話装置３００にはＤを保持する必要がなく、ハッシュ関数の一方向性よりｄからＤを求めることは困難であるのでより望ましい。
【０１１２】
ドキュメントｍは、秘密関数ｆの入力値となりえる任意の値を与えることができる。
【０１１３】
さらに、ドキュメントｍは、対話装置３００の項で述べたように対話装置３００のドキュメント処理部３０３に与える処理を記述するようにしても良い。
【０１１４】
さらに、ドキュメントｍには、チケットを識別する情報を記述するようにしても良い。例えば、プロバイダーの識別子やチケットが対応するサービスの識別子、チケット発行順に振られるシーケンシャルＩＤが含まれても良い。また、例えば、チケットの発行者が認証の特徴情報ｘとその識別子を管理し、その識別子を含ませるようにしても良い。また、例えば、認証の特徴情報ｘに対応する公開情報Ｉから定まる値を含ませるようにしても良い。
【０１１５】
［チケット合成方法］
ここでは、Ｇ，ｐ，πはシステムに共通であり、対話装置３００は複数ドキュメントに対応するものとする。
【０１１６】
$t_1, \ldots, t_N \in G$を、固有の秘密関数ｆを持つ対話装置３００に対して生成された

チケットとし、１≦ｉ≦Ｎに対して、$I_i \in G$を各チケットt_iに対応する検証情報とする。

【０１１７】

合成された検証情報$I = I_1 \cdots I_N$に対応する合成されたチケットｔを

【０１１８】

【数２０】

$$t = t_1 \cdots t_N$$

として生成することができる。

【０１１９】

チケットt_iにドキュメントm_iが対応し、検証情報I_iに認証の特徴情報x_iが対応している、つまり、$I_i x_i{}^p = 1$とすると、ドキュメントm_iに対応するドキュメント秘密情報$\mu_i = f(m_i)$は

【０１２０】

【数２１】

$$\mu_i = t_i{}^{-1} x_i$$

なので、$x = x_1 \cdots x_N$とすると、ｘは合成された検証情報Ｉに対応する認証の特徴情報、つまり、$I x^p = 1$であり、複数ドキュメント$m_1, \ldots, m_N$に対応するドキュメント秘密情報$\mu = f(m_1) \cdots f(m_N)$は

【０１２１】

【数２２】

$$\mu = t^{-1} x$$

を満たしている。

【０１２２】

［チケットを用いた証明方法］

図１１はチケットを用いた証明方法の流れを示している。以下、チケットと対話装置を用いた証明方法を説明する。この証明方法では、認証補助情報としてチケットと呼ぶ形態を用いている。

【０１２３】

利用者は、秘密関数ｆで特徴付けられる対話装置と$t = x f(m)^{-1}$を満たすドキュメントｍとチケットｔを保持するものとする。コミットメントｒと、チャレンジｃに対するレスポンスｓを生成する方法は以下のとおりである。

１．　対話装置３００を用いて、コミットメントｒを取得する。

２．　対話装置３００を用いて、ドキュメントｍとチャレンジｃに対応するレスポンスσを取得する。

３．　チケットｔとチャレンジｃと取得したレスポンスσよりレスポンスｓを

【０１２４】

【数２３】

$$s = t^c \sigma$$

として計算する。このとき、（ｒ，ｃ，ｓ）は

【０１２５】

【数２４】

$$r = \pi(s^p I^c)$$

を満たしている。

【０１２６】

このようにして、利用者に認証の特徴情報ｘを知らすことなく、対話装置３００とチケットｔを用いることによって、検証情報Ｉに対応する図１に記載の証明者２００の機能を頒布することができる。

【０１２７】

この証明者２００に対応する検証者１００は、図１に記載された従来例と全く同一なので、検証装置３００は唯一の検証情報Ｉ　を保持する必要があるだけで、極めて小規模な装

置で多数の利用者の認証を、完結して行なうことができる。
【０１２８】
▲１▼Ｆｉａｔ－Ｓｈａｍｉｒ認証
特に、ｐ＝２の場合、
【０１２９】
【数２５】
$r=\pi(s^2 I^c)$
を満たしており、いわゆるＦｉａｔ－Ｓｈａｍｉｒ認証の関係を満たしている。
【０１３０】
このようにして、利用者に秘密情報ｘを知らすことなく、対話装置３００とチケットｔを用いることによって、検証情報Ｉに対応するＦｉａｔ－Ｓｈａｍｉｒ認証の証明者の機能を頒布することができる。
【０１３１】
なお、Ｆｉａｔ－Ｓｈａｍｉｒ認証の詳細については、前述の”Ｈｏｗ ｔｏｐｒｏｖｅ ｙｏｕｒｓｅｌｆ： ｐｒａｃｔｉｃａｌ ｓｏｌｕｔｉｏｎｓｔｏ ｉｄｅｎｔｉｆｉｃａｔｉｏｎ ａｎｄ ｓｉｇｎａｔｕｒｅ ｐｒｏｂｌｅｍｓ”を参照されたい。
【０１３２】
▲２▼Ｇｕｉｌｌｏｕ－Ｑｕｉｓｑｕａｔｅｒ認証
特に、ｐがＧの零化域の生成元λと互いに素な場合、利用者はＧｕｉｌｌｏｕ－Ｑｕｉｓｑｕａｔｅｒ認証の証明者としてふるまったことになる。
【０１３３】
このようにして、利用者に秘密情報ｘを知らすことなく、対話装置とチケットｔを用いることによって、検証情報Ｉに対応するＧｕｉｌｌｏｕ－Ｑｕｉｓｑｕａｔｅｒ認証の証明者の機能を頒布することができる。
【０１３４】
［チケットを用いた署名生成方法］
図１３はチケットを用いた署名生成方法の流れを示している。以下、チケットと対話装置を用いた署名生成方法を説明する。なお、ここでも慣用的に署名者の用語を用いたが、電子署名の性質上、署名者が、計算機資源を有する署名装置と等価であることは明らかである。
【０１３５】
利用者は、秘密関数ｆで特徴付けられる対話装置３００と$t=xf(m)^{-1}$を満たすドキュメントｍとチケットｔを保持するものとする。また、Ｇとメッセージの空間Ｍとの積Ｇ×ＭからＦ$_p$への写像φが公開されているものとする。
【０１３６】
例えば、φを、ハッシュ関数ｈを用いて、φ（ｒ，Ｍ）＝ｈ（ｒ｜Ｍ）としても良い。
【０１３７】
メッセージＭに対して署名（ｒ，ｓ）を生成する方法は以下のとおり。
１．　対話装置３００を用いて、コミットメントｒを取得する。
２．　コミットメントｒとメッセージＭよりチャレンジｃをｃ＝φ（ｒ，Ｍ）として計算する。
３．　対話装置を用いて、ドキュメントｍとチャレンジｃに対応するレスポンスσを取得する。
４．　チケットｔとチャレンジｃと取得したレスポンスσよりレスポンスｓを
【０１３８】
【数２６】
$s=t^c\sigma$
として計算する。
【０１３９】
このとき、署名（ｒ，ｓ）は

【０１４０】
【数２７】

$$r=\pi\left(s^{p}I^{\phi(r,M)}\right)$$

を満たしている。
【０１４１】
このようにして、利用者に認証の特徴情報ｘを知らすことなく、対話装置３００とチケットｔを用いることによって、検証情報Ｉに対応する署名の機能を頒布することができる。つまり、署名鍵を開示せずに署名の機能を頒布することができる。さらに、ドキュメントｍに、鍵の有効期限情報や鍵の利用可能回数情報を付与することによって、有効期限付きの署名鍵や利用回数制限付きの署名鍵を実現することもできる。
【０１４２】
［チケット検証装置］
図９はチケット検証装置の構成を示し、図７はチケット検証装置の動作を示している。
【０１４３】
チケット検証装置５００は、対話装置３００と対話を行なうことによってチケットの検証を行なう。チケット検証装置５００は入出力部５０１、記憶部５０２、ドキュメント処理部５０３、乱数生成部５０４、Ｇの算法実行部５０５、π計算部５０６を含んで構成されている。以下、チケット検証装置５００の動作を説明する。
【０１４４】
チケット検証装置５００は、検証情報Ｉとチケットｔを記憶部５０２に保持している。
１．　入出力部５０１を用いて、コミットメントｒを入力し、記憶部５０２に保持する。
２．　乱数生成部５０４を用いて、チャレンジｃを生成し、記憶部５０２に保持する。
３．　入出力部５０１を用いて、記憶部５０２に保持されたチャレンジｃを出力する。
４．　入出力部５０１を用いて、レスポンスσを入力し、記憶部５０２に保持する。
５．　Ｇにおける算法実行部５０５と、必要ならば、πの計算部５０６を用いて、記憶部５０２に保持されたｃ，σ，Ｉとチケットｔから
【０１４５】
【数２８】

$$r'=\pi\left(\left(t^{c}\sigma\right)^{p}I^{c}\right)$$

を計算し、記憶部５０２に保持する。
【０１４６】
もちろん、πが恒等写像である場合は、πの計算部５０６は不要である。
【０１４７】
また、ｒ’は、例えば、
【０１４８】
【数２９】

$$r'=\pi\left(\left(t^{p}I\right)^{c}\sigma^{p}\right)$$

として計算しても構わない。
６．　記憶部５０２に保持されたｒ，ｒ’を比較する。チケットｔがドキュメント秘密情報と認証の特徴情報ｘ　に対応したものであるならば
【０１４９】
【数３０】

$$\mu=t^{-1}x$$

を満たしており、ドキュメント秘密情報μに基づいた対話では、（ｒ，ｃ，σ）は
【０１５０】
【数３１】

$$r=k^{p}$$

$$\sigma=k\mu^{c}$$

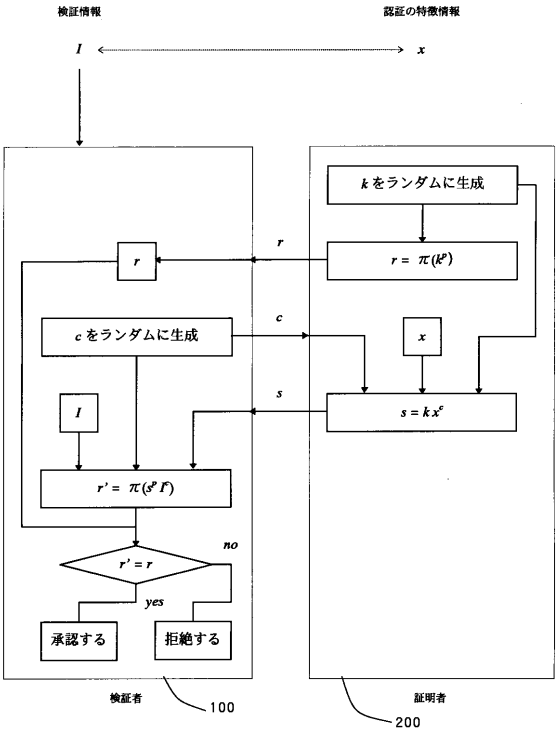
を満たしている。したがって、秘密関数ｆがμ＝ｆ（ｍ）を満たす対話装置と検証装置と

の対話のときにはｒ＝ｒ’が満たされる。
【０１５１】
（チケットが可変な構成）
ここでは、入出力部５０１にチケットｔを入力し、入力されたチケットｔを記憶部５０２に保持する構成を述べる。
【０１５２】
動作１ないし動作６に先だって、チケット検証装置５００は、以下の動作を実行する。
７．　入出力部５０１を用いて、チケットｔを入力し、記憶部５０２に保持する。このように構成することによって複数のチケットの検証を行なうことができる。
【０１５３】
また、チャレンジｃを、ランダムに生成したチャレンジχとコミットメントｒからハッシュ関数ｈを用いて
【０１５４】
【数３２】
$$c = h(\chi \mid r)$$
として生成することにして、検証に成功した対話に対して、署名（χ，ｒ，ｓ）を検証の履歴として記憶部に保持するように構成しても良い。このように構成することによってチケットの検証を確かに行なったことを第三者に証明することができる。もちろん、第三者が署名（χ，ｒ，ｓ）を検証する際の検証式は、
【０１５５】
【数３３】
$$r = s^{p} I^{h(\chi \mid r)}$$
である。
【０１５６】
［応用例：鍵］
以上に述べてきた対話装置とチケットを用いた証明者の機能を、実際の応用上の局面に適用した例について述べる。この応用例では、認証の特徴情報x_Aをある施設の会議室Ａの鍵に対応させるものとする。
【０１５７】
チケット発行者は施設の管理者であり、会議室Ａの錠を
１．　スマートカードリーダー
２．　施錠・開錠部
３．　計時部
４．　スマートカードリーダー内のＲＯＭに焼き付けられたプログラムとして実現されたチケット検証器
によって構成する。
【０１５８】
施錠・開錠部は、通常はロックされており、チケット検証に成功した場合、６０秒開錠した後に再びロックを行なう。スマートカードリーダーは、スマートカードを挿入するスロットを持ち、スマートカードとの通信を行なう。計時部は現在時間を保持する。
【０１５９】
ドキュメントは、９月１６日を表すような日付けのフィールドと１４時００分を表すような利用開始時間のフィールドと１６時００分を表すような利用終了時間のフィールドとからなる。施設の利用者には、チケットおよびドキュメント保持部と対話装置からなるスマートカードが貸与されるものとする。
【０１６０】
会議室の利用の予定がある場合、予約代表者が会議室予約システム（チケット発行装置）にアクセスして、利用時間と会議出席者の保持する対話装置のＩＤを指定すると、会議室予約システムは電子メールで、会議出席者それぞれにあててチケットを配る。会議出席者

はチケットを入手し、利用時間であるドキュメントと併せてスマートカードに記録する。
【０１６１】
会議室を利用する場合は、会議室のドアに取り付けられたスロットにスマートカードを挿入し、チケット認証を行なう。この際、会議室の錠はチャレンジの特定のビットフィールドに計時部に保持された現在時間を埋め込み、対話装置のドキュメント処理部が、チャレンジに埋め込まれた現在時間がドキュメントに記述された利用時間の範囲外の場合は処理を中断する。
【０１６２】
この例では、チケットは有効期限付きの共用の鍵として利用されている。
【０１６３】
【発明の効果】
以上、説明してきたように、本発明は、公開鍵暗号における認証の特徴情報を開示することなく、認証の特徴情報に基づいた証明の機能を配布することができる。したがって、従来不可能であった、利害関係を持たない複数の個人が同一の認証の特徴情報に基づいた証明を安全に行なえるようになった。
【０１６４】
このことは、必ずしも個人に帰属しない性格を有するチケットを、そのまま、公開鍵暗号の認証の特徴情報に対応付けることを可能にし、チケットの検証側は、公開された唯一の検証情報に基づき公開された手順で、チケットの真贋を判定するのみで検証を行なえるので検証側の負担を大幅に軽減できる。また、チケットの所持を証明する利用者側から見ても、検証側の有する先に述べた特質は、検証側の公正が確認でき、チケットの検証に伴って個人の特定がなされない（なぜならば個人に帰属しない認証の特徴情報のみが検証に関わるので）ことなどの効用がある。
【０１６５】
さらに、利用者にとっては、チケットおよび対話装置はチケット発行者のみに理解し得るブラックボックスであり、チケットを対話装置に入力するならば、認証方式を実現するのには関与していないコバートチャネルが存在しないことを確信できないが、本発明においては、対話装置への情報伝達は、利用者にも完全な解釈を許してもプロテクト側の安全性を損ねないドキュメントとして実現し、ブラックボックスであるチケットをブラックボックスである対話装置に入力することもない。
【０１６６】
また、本発明においては、Ｇｕｉｌｌｏｕ－Ｑｕｉｓｑｕａｔｅｒ認証をベースの公開鍵暗号として採用しているが、Ｇｕｉｌｌｏｕ－Ｑｕｉｓｑｕａｔｅｒ認証はＧｕｉｌｌｏｕ　Ｑｕｉｓｑｕａｔｅｒにより”Ａ　’ｐａｒａｄｏｘｉｃａｌ’　ｉｄｅｎｔｉｔｙ－ｂａｓｅｄ　ｓｉｇｎａｔｕｒｅ　ｓｃｈｅｍｅｒｅｓｕｌｔｉｎｇ　ｆｒｏｍ　ｚｅｒｏ－ｋｎｏｗｌｅｄｇｅ”、Ａｄｖａｎｃｅｓ　ｉｎ　Ｃｒｙｐｔｏｌｏｇｙ　ＣＲＹＰＴＯ’８８、Ｓ．Ｇｏｌｄｗａｓｓｅｒ（ｅｄ．）、Ｓｐｒｉｎｇｅｒ－Ｖｅｒｌａｇ、ｐｐ．２１６－２３１において零知識性が証明されている。
【図面の簡単な説明】
【図１】従来技術に係わる認証方法の原理を示す図である。
【図２】全体の構成を示す図である。
【図３】対話装置の構成を示す図である。
【図４】対話装置の動作を示す図である。
【図５】チケット発行装置の構成を示す図である。
【図６】チケット発行装置の動作を示す図である。
【図７】チケット検証装置の動作を示す図である。
【図８】対話装置の構成を示す図である。
【図９】チケット検証装置の構成ををを示す図である。
【図１０】対話装置の動作を示す図である。
【図１１】チケットを用いた証明方法の原理を示す図である。

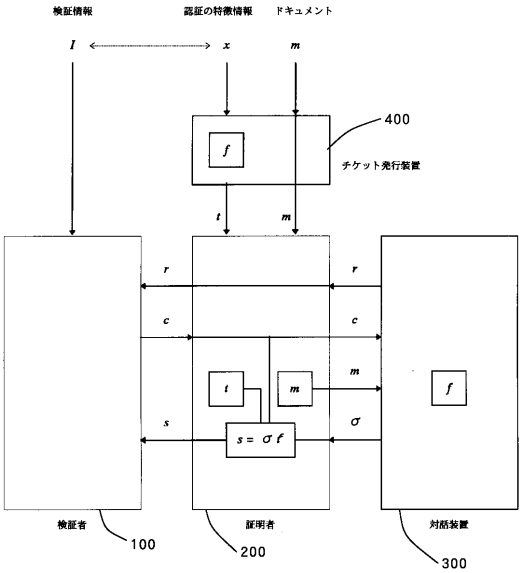
【図１２】応用例の構成を示す図である。
【図１３】チケットを用いた署名生成方法の原理を示す図である。
【符号の説明】
１００　検証者
２００　証明者
３００　対話装置
３０１　対話装置３００の入出力部
３０２　対話装置３００の記憶部
３０３　対話装置３００のドキュメント処理部
３０４　対話装置３００の乱数生成部
３０５　対話装置３００のＧにおける算法実行部
３０６　対話装置３００のπ計算部
３０７　対話装置３００のｆ計算部
４００　チケット発行装置
４０１　チケット発行装置４００の入出力部
４０２　チケット発行装置４００の記憶部
４０３　チケット発行装置４００のＧにおける算法実行部
４０４　チケット発行装置４００のｆ計算部
５００　チケット検証装置
５０１　チケット検証装置５００の入出力部
５０２　チケット検証装置５００の記憶部
５０３　チケット検証装置５００のドキュメント処理部
５０４　チケット検証装置５００の乱数生成部
５０５　チケット検証装置５００のＧにおける算法実行部
５０６　チケット検証装置５００のπ計算部

【図１】



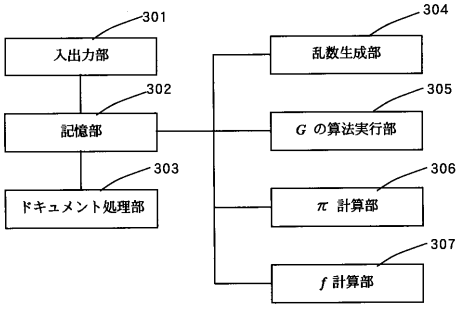
従来技術の動作

【図２】



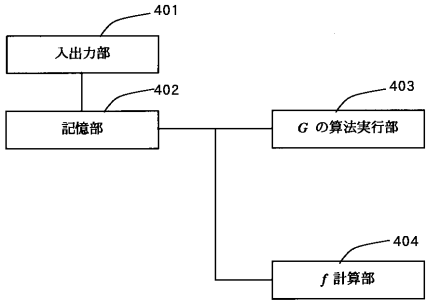
全体の構成図

【図３】



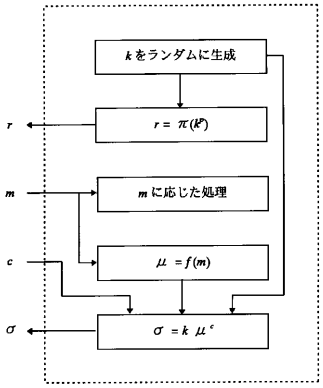
対話装置の構成

【図５】



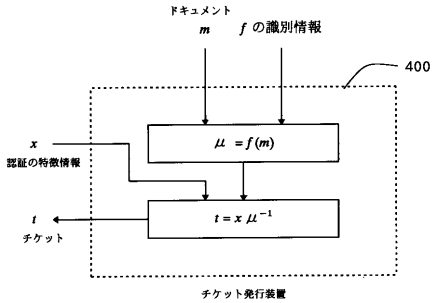
チケット発行装置の構成

【図４】



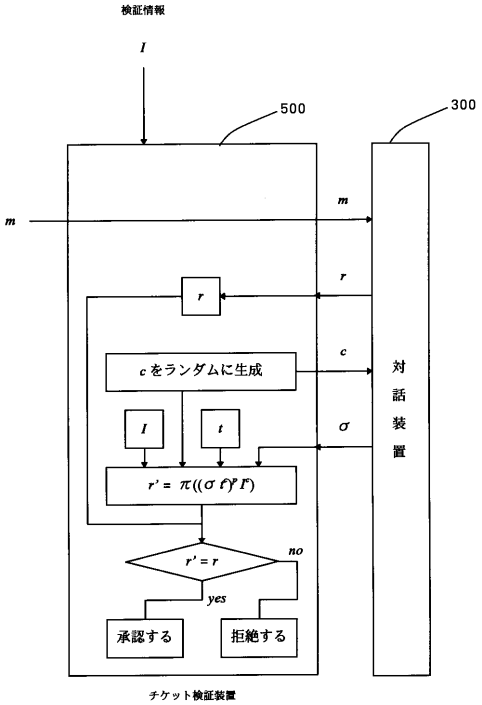
対話装置の動作

【図６】



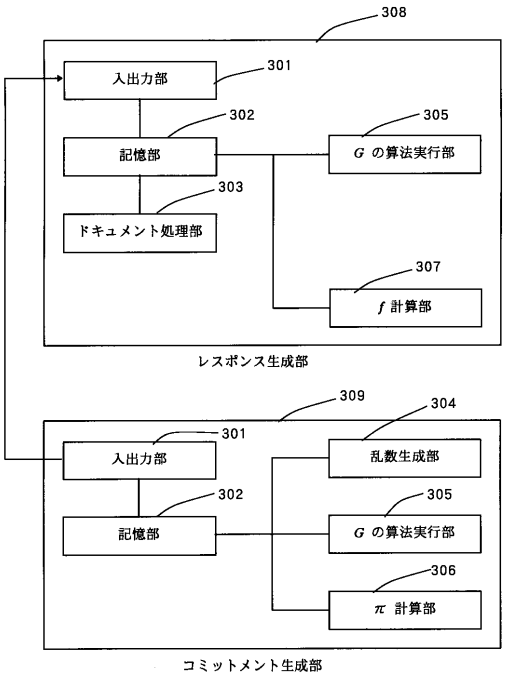
チケット発行装置の動作

【図７】



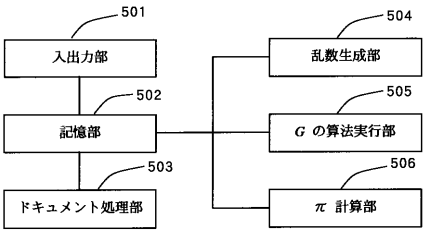
チケット検証装置の動作

【図８】



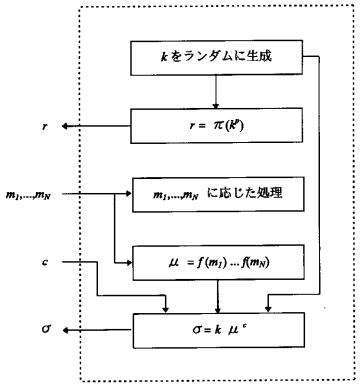
対話装置の構成

【図９】



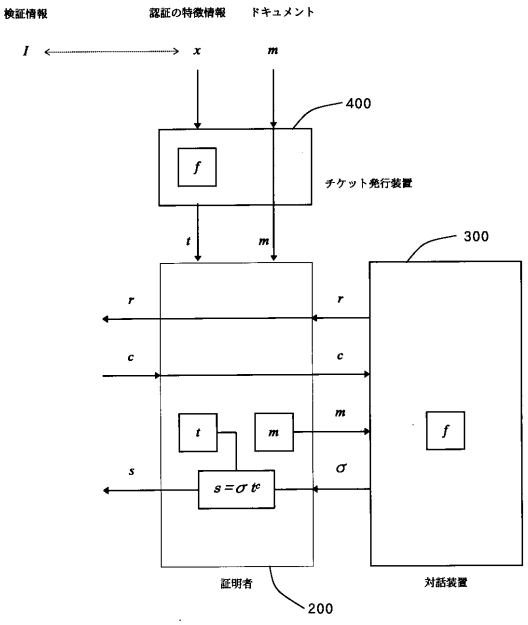
チケット検証装置

【図１０】



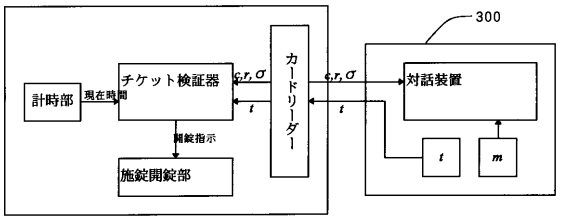
対話装置の動作

【図１１】



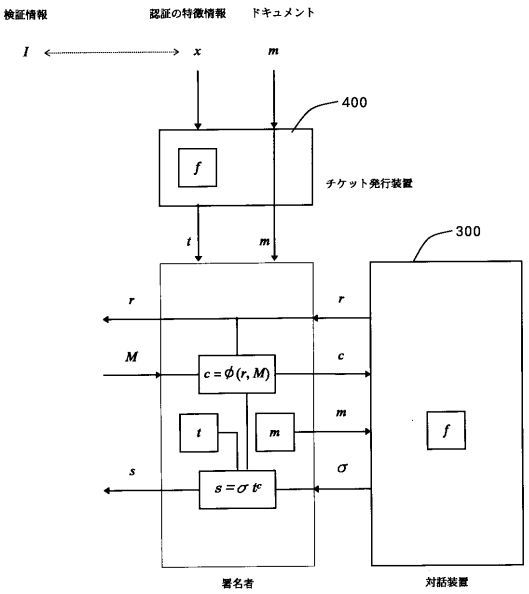
チケットを用いた証明方法

【図１２】



応用例（鍵）構成図

【図１３】



チケットを用いた署名生成方法

フロントページの続き

審査官　青木　重徳

(56)参考文献　Louis C. Guillou and Jean-Jacques Quisquater, “A PRACTICAL ZERO-KNOWLEDGE PROTOCOL FITTED TO SECURITY MICROPROCESSOR MINIMIZING BOTH TRANSMISSI”, Lecture Notes in Computer Science(EUROCRYPT'88), １９８８年１０月１４日, Vol.330, p.123-128

(58)調査した分野(Int.Cl.[7], ＤＢ名)
G09C 1/00 640
H04L 9/32