【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第７部門第３区分
【発行日】平成23年1月20日(2011.1.20)

【公開番号】特開2008-136193(P2008-136193A)
【公開日】平成20年6月12日(2008.6.12)
【年通号数】公開・登録公報2008-023
【出願番号】特願2007-280287(P2007-280287)
【国際特許分類】
Ｈ０４Ｌ　9/32　(2006.01)
【ＦＩ】
Ｈ０４Ｌ　9/00　６７５Ｂ

【手続補正書】
【提出日】平成22年11月30日(2010.11.30)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
署名生成を行う署名生成装置であって、
整数の秘密鍵をｘとし、Ｍビットのリカバリメッセージを$m_{rec} \in \{0, 1\}^M$とした場合における、
整数の任意値ｋを選択する任意値生成部と、
位数ｑの巡回群をＧとし、当該巡回群Ｇの生成元をｇとした場合における$R = g^k \in G$を算出し、当該演算結果Ｒを得る群演算部と、
入力値に対してＬビット（Ｌは署名検証装置と共有される正の整数）のハッシュ値を出力するハッシュ関数$H_1 : \{0, 1\}^* \rightarrow \{0, 1\}^L$を、上記演算結果Ｒとリカバリメッセージ$m_{rec}$とに対応する値αに作用させ、その演算結果であるＬビットのハッシュ値$h = H_1(\alpha) \in \{0, 1\}^L$を得る第２ハッシュ演算部と、
上記リカバリメッセージm_{rec}のビット長Ｍに応じて出力ビット長がＭビットに定まるハッシュ関数$H_2 : \{0, 1\}^* \rightarrow \{0, 1\}^M$を、上記演算結果Ｒと上記ハッシュ値ｈとに対応する値βに作用させ、その演算結果であるＭビットのハッシュ値$u = H_2(\beta) \in \{0, 1\}^M$を得る第３ハッシュ演算部と、
上記リカバリメッセージm_{rec}と上記ハッシュ値ｕとの排他的論理和を$w = m_{rec} (+) u \in \{0, 1\}^M$（（＋）は排他的論理和演算子）とし、上記ハッシュ値$h \in \{0, 1\}^L$を第１ビット位置に配置し、上記排他的論理和値$w \in \{0, 1\}^M$を第２ビット位置に配置したＬ＋Ｍビットのビット結合値$r = h \mid w \in \{0, 1\}^{L+M}$を算出し、当該ビット結合値ｒを得るビット結合部と、
入力値に対して整数を出力するハッシュ関数$H_3 : \{0, 1\}^* \rightarrow Z$（整数）を、上記ビット結合値ｒに対応する値γに作用させ、その演算結果であるハッシュ値$t = H_3(\gamma) \in Z$を得る第４ハッシュ演算部と、
$s = k - t \cdot x \in Z$を算出し、当該演算結果ｓを得る整数演算部と、
署名$\sigma = (r, s)$を出力する署名出力部と、
を有することを特徴とする署名生成装置。
【請求項２】
署名生成を行う署名生成装置であって、
整数の秘密鍵をｘとし、Ｍビットのリカバリメッセージを$m_{rec} \in \{0, 1\}^M$とし

た場合における、
整数の任意値ｋを生成する任意値生成部と、
位数ｑの巡回群をＧとし、当該巡回群Ｇの生成元をｇとした場合における$R = g^k \in G$を算出し、当該演算結果Ｒを得る群演算部と、
上記リカバリメッセージm_{rec}のビット長Ｍに応じて出力ビット長がＬ＋Ｍビット（Ｌは署名検証装置と共有される正の整数）に定まるハッシュ関数$H_0 : \{0, 1\}^* \rightarrow \{0, 1\}^{L+M}$を上記演算結果Ｒに作用させ、その演算結果であるＬ＋Ｍビットのハッシュ値$\Pi = H_0(R) \in \{0, 1\}^{L+M}$を得る第１ハッシュ演算部と、
入力値に対してＬビットのハッシュ値を出力するハッシュ関数$H_1 : \{0, 1\}^* \rightarrow \{0, 1\}^L$を、上記ハッシュ値Πとリカバリメッセージ$m_{rec}$とに対応する値αに作用させ、その演算結果であるＬビットのハッシュ値$h = H_1(\alpha) \in \{0, 1\}^L$を得る第２ハッシュ演算部と、
上記リカバリメッセージm_{rec}のビット長Ｍに応じて出力ビット長がＭビットに定まるハッシュ関数$H_2 : \{0, 1\}^* \rightarrow \{0, 1\}^M$を、上記ハッシュ値Πと上記ハッシュ値ｈとに対応する値βに作用させ、その演算結果であるＭビットのハッシュ値$u = H_2(\beta) \in \{0, 1\}^M$を得る第３ハッシュ演算部と、
上記リカバリメッセージm_{rec}と上記ハッシュ値ｕとの排他的論理和$w = m_{rec}(+)u \in \{0, 1\}^M$（（＋）は排他的論理和演算子）を算出し、当該排他的論理和値ｗを得る第１排他的論理和演算部と、
上記ハッシュ値$h \in \{0, 1\}^L$を第１ビット位置に配置し、上記排他的論理和値$w \in \{0, 1\}^M$を第２ビット位置に配置したＬ＋Ｍビットのビット結合値$d = h \mid w \in \{0, 1\}^{L+M}$を算出し、当該ビット結合値ｄを得るビット結合部と、
上記ハッシュ値Πと上記ビット結合値ｄとの排他的論理和$r = \Pi(+)d \in \{0, 1\}^{L+M}$を算出し、当該排他的論理和値ｒを得る第２排他的論理和演算部と、
入力値に対して整数を出力するハッシュ関数$H_3 : \{0, 1\}^* \rightarrow Z$（整数）を、上記排他的論理和値ｒに対応する値γに作用させ、その演算結果であるハッシュ値$t = H_3(\gamma) \in Z$を得る第４ハッシュ演算部と、
$s = k - t \cdot x \in Z$を算出し、当該演算結果ｓを得る整数演算部と、
署名$\sigma = (r, s)$を出力する署名出力部と、
を有することを特徴とする署名生成装置。
【請求項３】
請求項１又は２に記載の署名生成装置であって、
Ｎビットのクリアメッセージを$m_{clr} \in \{0, 1\}^N$とし、
上記第４ハッシュ演算部は、
上記ハッシュ関数$H_3 : \{0, 1\}^* \rightarrow Z$を、上記ｒと上記クリアメッセージ$m_{clr}$とに対応する値γに作用させ、その演算結果であるハッシュ値$t = H_3(\gamma) \in Z$を得、
上記署名出力部は、
上記署名$\sigma = (r, s)$と上記クリアメッセージm_{clr}とを出力する、
ことを特徴とする署名生成装置。
【請求項４】
請求項２に記載の署名生成装置であって、
上記巡回群Ｇの生成元は、楕円曲線Ｅ上の点であり、
上記$R = g^k \in G$は、上記楕円曲線Ｅ上の点$k \cdot g \in E$であり、
上記ハッシュ関数$H_0 : \{0, 1\}^* \rightarrow \{0, 1\}^{L+M}$を上記演算結果Ｒに作用させる演算は、楕円曲線上の点である上記演算結果Ｒを一義的又は限定的に特定する値に、上記ハッシュ関数H_0を作用させる演算である、
ことを特徴とする署名生成装置。
【請求項５】
請求項１に記載の署名生成装置であって、
上記巡回群Ｇの生成元は、楕円曲線Ｅ上の点であり、

上記Ｒ＝ｇ^{k}∈Ｇは、上記楕円曲線Ｅ上の点ｋ・ｇ∈Ｅである、
ことを特徴とする署名生成装置。
【請求項６】
請求項１又は２に記載の署名生成装置であって、
上記Ｒ＝ｇ^{k}∈Ｇは、ｇ^{x}ｍｏｄ　ｐ（ただし、ｇは２以上の整数，ｐ＝２ｑ＋１）である、
ことを特徴とする署名生成装置。
【請求項７】
署名検証を行う署名検証装置であって、
位数ｑの巡回群をＧとし、当該巡回群Ｇの生成元をｇとし、署名生成装置の秘密鍵ｘ∈Ｚに対応する公開鍵をｙ＝ｇ^{x}∈Ｇとした場合における、
署名σ’＝（ｒ’，ｓ’）の入力を受け付ける署名入力部と、
入力値に対して整数を出力するハッシュ関数Ｈ$_{3}$：｛０，１｝*→Ｚ（整数）を、上記署名σ’が有するｒ’に対応する値γ’に作用させ、その演算結果であるハッシュ値ｔ’＝Ｈ$_{3}$（γ’）∈Ｚを得る第１ハッシュ演算部と、
Ｒ’＝ｇ$^{s'}$・ｙ$^{t'}$∈Ｇの演算を行い、その演算結果Ｒ’を得る群演算部と、
上記署名σ’に対応するリカバリメッセージｍ$_{rec}$’のビット長Ｍ’に応じて出力ビット長がＭ’ビットに定まるハッシュ関数Ｈ$_{2}$：｛０，１｝*→｛０，１｝$^{M'}$を、上記演算結果Ｒ’とｒ’の第１ビット位置のＬビット（Ｌは署名生成装置と共有される正の整数）の値ｈ’∈｛０，１｝^{L}とに対応する値β’に作用させ、その演算結果であるＭ’ビットのハッシュ値ｕ’＝Ｈ$_{2}$（β’）∈｛０，１｝$^{M'}$を得る第３ハッシュ演算部と、
上記ｒ’の第２ビット位置のＭ’ビットの値ｗ’∈｛０，１｝$^{M'}$と上記ハッシュ値ｕ’との排他的論理和ｗ’（＋）ｕ’を算出し、その演算結果をリカバリメッセージｍ$_{rec}$’∈｛０，１｝$^{M'}$として得る第２排他的論理和演算部と、
入力値に対してＬビットのハッシュ値を出力するハッシュ関数Ｈ$_{1}$：｛０，１｝*→｛０，１｝^{L}を、上記演算結果Ｒ’と上記リカバリメッセージｍ$_{rec}$’とに対応する値α’に作用させ、その演算結果であるＬビットのハッシュ値Ｈ$_{1}$（α’）∈｛０，１｝^{L}を得る第４ハッシュ演算部と、
上記Ｌビットの値ｈ’と上記ハッシュ値Ｈ$_{1}$（α’）とを比較する比較部と、
を有することを特徴とする署名検証装置。
【請求項８】
署名検証を行う署名検証装置であって、
位数ｑの巡回群をＧとし、当該巡回群Ｇの生成元をｇとし、署名生成装置の秘密鍵ｘ∈Ｚに対応する公開鍵をｙ＝ｇ^{x}∈Ｇとし、
署名σ’＝（ｒ’，ｓ’）の入力を受け付ける署名入力部と、
入力値に対して整数を出力するハッシュ関数Ｈ$_{3}$：｛０，１｝*→Ｚ（整数）を、上記署名σ’が有するｒ’に対応する値γ’に作用させ、その演算結果であるハッシュ値ｔ’＝Ｈ$_{3}$（γ’）∈Ｚを得る第１ハッシュ演算部と、
Ｒ’＝ｇ$^{s'}$・ｙ$^{t'}$∈Ｇの演算を行い、その演算結果Ｒ’を得る群演算部と、
上記署名σ’に対応するリカバリメッセージｍ$_{rec}$’のビット長Ｍ’に応じて出力ビット長がＬ＋Ｍ’ビット（Ｌは署名生成装置と共有される正の整数）に定まるハッシュ関数Ｈ$_{0}$：｛０，１｝*→｛０，１｝$^{L+M'}$を上記演算結果Ｒ’に作用させ、その演算結果であるＬ＋Ｍ’ビットのハッシュ値Π’＝Ｈ$_{0}$（Ｒ’）∈｛０，１｝$^{L+M'}$を得る第２ハッシュ演算部と、
上記ハッシュ値Π’と上記署名σ’が有するｒ’との排他的論理和ｄ’＝Π’（＋）ｒ’∈｛０，１｝$^{L+M'}$を算出し、当該排他的論理和値ｄ’を得る第１排他的論理和演算部と、
上記リカバリメッセージｍ$_{rec}$’のビット長Ｍ’に応じて出力ビット長がＭ’ビットに定まるハッシュ関数Ｈ$_{2}$：｛０，１｝*→｛０，１｝$^{M'}$を、上記ハッシュ値Π’と上記排他的論理和値ｄ’の第１ビット位置のＬビットの値ｈ’∈｛０，１｝^{L}とに対応する

値β’に作用させ、その演算結果であるM’ビットのハッシュ値u’＝H_2（β’）∈{0，1}$^{M'}$を得る第３ハッシュ演算部と、
上記排他的論理和値d’の第２ビット位置のM’ビットの値w’∈{0，1}$^{M'}$と上記ハッシュ値u’との排他的論理和w’（＋）u’を算出し、その演算結果をリカバリメッセージm_{rec}’∈{0，1}$^{M'}$とする第２排他的論理和演算部と、
入力値に対してLビットのハッシュ値を出力するハッシュ関数H_1：{0，1}*→{0，1}^{L}を、上記ハッシュ値Π’と上記第２排他的論理和演算部で算出された上記リカバリメッセージm_{rec}’とに対応する値α’に作用させ、その演算結果であるLビットのハッシュ値H_1（α’）∈{0，1}^{L}を得る第４ハッシュ演算部と、
上記Lビットの値h’と上記ハッシュ値H_1（α’）とを比較する比較部と、
を有することを特徴とする署名検証装置。
【請求項９】
請求項７又は８に記載の署名検証装置であって、
上記署名入力部は、
上記署名σ’と上記署名σ’に対応するクリアメッセージm_{clr}’との入力を受け付け、
上記第１ハッシュ演算部は、
上記ハッシュ関数H_3：{0，1}*→Zを、上記署名σ’が有するr’と上記クリアメッセージm_{clr}’とに対応する値γ’に作用させ、その演算結果であるハッシュ値t’＝H_3（γ’）∈Zを得る、
ことを特徴とする署名検証装置。
【請求項１０】
請求項８に記載の署名検証装置であって、
上記巡回群Gの生成元は、楕円曲線E上の点であり、
上記公開鍵y＝g^x∈Gは、上記楕円曲線E上の点k・g∈Eであり、
上記R’＝$g^{s'}\cdot y^{t'}$∈Gは、上記楕円曲線E上の点s’・g＋t’・y∈Eであり、
上記ハッシュ関数H_0：{0，1}*→{0，1}$^{L+M'}$を上記演算結果R’に作用させる演算は、楕円曲線E上の点である上記演算結果R’を一義的又は限定的に特定する値に、上記ハッシュ関数H_0を作用させる演算である、
ことを特徴とする署名検証装置。
【請求項１１】
請求項７に記載の署名検証装置であって、
上記巡回群Gの生成元は、楕円曲線E上の点であり、
上記公開鍵y＝g^x∈Gは、上記楕円曲線E上の点k・g∈Eであり、
上記R’＝$g^{s'}\cdot y^{t'}$∈Gは、上記楕円曲線E上の点s’・g＋t’・y∈Eである、
ことを特徴とする署名検証装置。
【請求項１２】
請求項７又は８に記載の署名検証装置であって、
上記公開鍵y＝g^x∈Gは、g^xｍｏｄ ｐ（ただし、gは２以上の整数，p＝２q＋１）であり、
上記R’＝$g^{s'}\cdot y^{t'}$∈Gは、$g^{s'}\cdot y^{t'}$ｍｏｄ ｐである、
ことを特徴とする署名検証装置。
【請求項１３】
署名生成装置の署名生成方法であって、
整数の秘密鍵をxとし、Mビットのリカバリメッセージをm_{rec}∈{0，1}^{M}とした場合における、
整数の任意値kを選択するステップと、
位数qの巡回群をGとし、当該巡回群Gの生成元をgとした場合におけるR＝g^k∈G

を算出し、当該演算結果Ｒを得るステップと、
入力値に対してＬビット（Ｌは署名検証装置と共有される正の整数）のハッシュ値を出力するハッシュ関数H_1：｛０，１｝＊→｛０，１｝^{L}を、上記演算結果Ｒとリカバリメッセージm_{rec}とに対応する値αに作用させ、その演算結果であるＬビットのハッシュ値$h=H_1(\alpha)\in\{0,1\}^L$を得るステップと、
上記リカバリメッセージm_{rec}のビット長Ｍに応じて出力ビット長がＭビットに定まるハッシュ関数H_2：｛０，１｝＊→｛０，１｝^{M}を、上記演算結果Ｒと上記ハッシュ値ｈとに対応する値βに作用させ、その演算結果であるＭビットのハッシュ値$u=H_2(\beta)\in\{0,1\}^M$を得るステップと、
上記リカバリメッセージm_{rec}と上記ハッシュ値ｕとの排他的論理和を$w=m_{rec}(+)u\in\{0,1\}^M$（（＋）は排他的論理和演算子）とし、上記ハッシュ値$h\in\{0,1\}^L$を第１ビット位置に配置し、上記排他的論理和値$w\in\{0,1\}^M$を第２ビット位置に配置したＬ＋Ｍビットのビット結合値$r=h\mid w\in\{0,1\}^{L+M}$を算出し、当該ビット結合値ｒを得るステップと、
入力値に対して整数を出力するハッシュ関数H_3：｛０，１｝＊→Ｚ（整数）を、上記ビット結合値ｒに対応する値γに作用させ、その演算結果であるハッシュ値$t=H_3(\gamma)\in Z$を得るステップと、
$s=k-t\cdot x\in Z$を算出し、当該演算結果ｓを得るステップと、
署名$\sigma=(r,s)$を出力するステップと、
を有することを特徴とする署名生成方法。
【請求項１４】
署名生成装置の署名生成方法であって、
整数の秘密鍵をｘとし、Ｍビットのリカバリメッセージを$m_{rec}\in\{0,1\}^M$とした場合における、
任意値生成部が、整数の任意値ｋを生成するステップと、
群演算部が、位数ｑの巡回群をＧとし、当該巡回群Ｇの生成元をｇとした場合における$R=g^k\in G$を算出し、当該演算結果Ｒを得るステップと、
第１ハッシュ演算部が、上記リカバリメッセージm_{rec}のビット長Ｍに応じて出力ビット長がＬ＋Ｍビット（Ｌは署名検証装置と共有される正の整数）に定まるハッシュ関数H_0：｛０，１｝＊→｛０，１｝$^{L+M}$を、上記演算結果Ｒに作用させ、その演算結果であるＬ＋Ｍビットのハッシュ値$\Pi=H_0(R)\in\{0,1\}^{L+M}$を得るステップと、
第２ハッシュ演算部が、入力値に対してＬビットのハッシュ値を出力するハッシュ関数H_1：｛０，１｝＊→｛０，１｝^{L}を、上記ハッシュ値Πとリカバリメッセージm_{rec}とに対応する値αに作用させ、その演算結果であるＬビットのハッシュ値$h=H_1(\alpha)\in\{0,1\}^L$を得るステップと、
第３ハッシュ演算部が、上記リカバリメッセージm_{rec}のビット長Ｍに応じて出力ビット長がＭビットに定まるハッシュ関数H_2：｛０，１｝＊→｛０，１｝^{M}を、上記ハッシュ値Πと上記ハッシュ値ｈとに対応する値βに作用させ、その演算結果であるＭビットのハッシュ値$u=H_2(\beta)\in\{0,1\}^M$を得るステップと、
第１排他的論理和演算部が、上記リカバリメッセージm_{rec}と上記ハッシュ値ｕとの排他的論理和$w=m_{rec}(+)u\in\{0,1\}^M$（（＋）は排他的論理和演算子）を算出し、当該排他的論理和値ｗを得るステップと、
ビット結合部が、上記ハッシュ値$h\in\{0,1\}^L$を第１ビット位置に配置し、上記排他的論理和値$w\in\{0,1\}^M$を第２ビット位置に配置したＬ＋Ｍビットのビット結合値$d=h\mid w\in\{0,1\}^{L+M}$を算出し、当該ビット結合値ｄを得るステップと、
第２排他的論理和演算部が、上記ハッシュ値Πと上記ビット結合値ｄとの排他的論理和$r=\Pi(+)d\in\{0,1\}^{L+M}$を算出し、当該排他的論理和値ｒを得るステップと、
第４ハッシュ演算部が、入力値に対して整数を出力するハッシュ関数H_3：｛０，１｝＊→Ｚ（整数）を、上記排他的論理和値ｒに対応する値γに作用させ、その演算結果であるハッシュ値$t=H_3(\gamma)\in Z$を得るステップと、

整数演算部が、ｓ＝ｋ－ｔ・ｘ∈Ｚを算出し、当該演算結果ｓを得るステップと、
署名出力部が署名σ＝（ｒ，ｓ）を出力するステップと、
を有することを特徴とする署名生成方法。
【請求項１５】
署名検証装置の署名検証方法であって、
位数ｑの巡回群をＧとし、当該巡回群Ｇの生成元をｇとし、署名生成装置の秘密鍵ｘ∈Ｚ（整数）に対応する公開鍵をｙ＝g^{x}∈Ｇをとした場合における、
署名σ’＝（ｒ’，ｓ’）の入力を受け付けるステップと、
入力値に対して整数を出力するハッシュ関数H_3：｛０，１｝＊→Ｚを、上記署名σ’が有するｒ’に対応する値γ’に作用させ、その演算結果であるハッシュ値ｔ’＝H_3（γ’）∈Ｚ（整数）を得るステップと、
Ｒ’＝$g^{s'}\cdot y^{t'}$∈Ｇの演算を行い、その演算結果Ｒ’を得るステップと、
上記署名σ’に対応するリカバリメッセージm_{rec}’のビット長Ｍ’に応じて出力ビット長がＭ’ビットに定まるハッシュ関数H_2：｛０，１｝＊→｛０，１｝$^{M'}$を、上記演算結果Ｒ’と上記ｒ’の第１ビット位置のＬビット（Ｌは署名生成装置と共有される正の整数）の値ｈ’∈｛０，１｝^{L}とに対応する値β’に作用させ、その演算結果であるＭ’ビットのハッシュ値ｕ’＝H_2（β’）∈｛０，１｝$^{M'}$を得るステップと、
上記ｒ’の第２ビット位置のＭ’ビットの値ｗ’∈｛０，１｝$^{M'}$と上記ハッシュ値ｕ’との排他的論理和ｗ’（＋）ｕ’を算出し、その演算結果をリカバリメッセージm_{rec}’∈｛０，１｝$^{M'}$として得るステップと、
入力値に対してＬビットのハッシュ値を出力するハッシュ関数H_1：｛０，１｝＊→｛０，１｝^{L}を、上記演算結果Ｒ’と上記リカバリメッセージm_{rec}’とに対応する値α’に作用させ、その演算結果であるＬビットのハッシュ値H_1（α’）∈｛０，１｝^{L}を得るステップと、
上記Ｌビットの値ｈ’と上記ハッシュ値H_1（α’）とを比較するステップと、
を有することを特徴とする署名検証方法。
【請求項１６】
署名検証装置の署名検証方法であって、
位数ｑの巡回群をＧとし、当該巡回群Ｇの生成元をｇとし、署名生成装置の秘密鍵ｘ∈Ｚ（整数）に対応する公開鍵をｙ＝g^{x}∈Ｇとした場合における、
署名入力部が、署名σ’＝（ｒ’，ｓ’）の入力を受け付けるステップと、
第１ハッシュ演算部が、入力値に対して整数を出力するハッシュ関数H_3：｛０，１｝＊→Ｚを、上記署名σ’が有するｒ’に対応する値γ’に作用させ、その演算結果であるハッシュ値ｔ’＝H_3（γ’）∈Ｚを出力するステップと、
群演算部が、Ｒ’＝$g^{s'}\cdot y^{t'}$∈Ｇの演算を行い、その演算結果Ｒ’を得るステップと、
第２ハッシュ演算部が、上記署名σ’に対応するリカバリメッセージm_{rec}’のビット長Ｍ’に応じて出力ビット長がＬ＋Ｍ’ビット（Ｌは署名生成装置と共有される正の整数）に定まるハッシュ関数H_0：｛０，１｝＊→｛０，１｝$^{L+M'}$を、上記演算結果Ｒ’に作用させ、その演算結果であるＬ＋Ｍ’ビットのハッシュ値Π’＝H_0（Ｒ’）∈｛０，１｝$^{L+M'}$を得るステップと、
第１排他的論理和演算部が、上記ハッシュ値Π’と上記署名σ’が有するｒ’との排他的論理和ｄ’＝Π’（＋）ｒ’∈｛０，１｝$^{L+M'}$を算出し、当該排他的論理和値ｄ’を得るステップと、
第３ハッシュ演算部が、上記リカバリメッセージm_{rec}’のビット長Ｍ’に応じて出力ビット長がＭ’ビットに定まるハッシュ関数H_2：｛０，１｝＊→｛０，１｝$^{M'}$を、上記ハッシュ値Π’と上記排他的論理和値ｄ’の第１ビット位置のＬビットの値ｈ’∈｛０，１｝^{L}とに対応する値β’に作用させ、その演算結果であるＭ’ビットのハッシュ値ｕ’＝H_2（β’）∈｛０，１｝$^{M'}$を得るステップと、
第２排他的論理和演算部が、上記排他的論理和値ｄ’の第２ビット位置のＭ’ビットの

値ｗ’∈｛０，１｝$^{M'}$と上記ハッシュ値ｕ’との排他的論理和ｗ’（＋）ｕ’を算出し、その演算結果をリカバリメッセージm_{rec}’∈｛０，１｝$^{M'}$とするステップと、

第４ハッシュ演算部が、入力値に対してＬビットのハッシュ値を出力するハッシュ関数H_1：｛０，１｝*→｛０，１｝^{L}を、上記ハッシュ値Π’と上記第２排他的論理和演算部で算出された上記リカバリメッセージm_{rec}’とに対応する値α’に作用させ、その演算結果であるＬビットのハッシュ値H_1（α’）∈｛０，１｝^{L}を得るステップと、

比較部が、上記Ｌビットの値ｈ’と上記ハッシュ値H_1（α’）とを比較するステップと、

を有することを特徴とする署名検証方法。

【請求項１７】

請求項１又は２に記載の署名生成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１８】

請求項７又は８に記載の署名検証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。

【手続補正２】

【補正対象書類名】明細書

【補正対象項目名】０００９

【補正方法】変更

【補正の内容】

【０００９】

請求項２及び１４の発明では上記課題を解決するために、以下のように署名生成を行う。

まず、整数の秘密鍵をｘとし、Ｍビットのリカバリメッセージをm_{rec}∈｛０，１｝^{M}とする。ここで、リカバリメッセージm_{rec}が、署名対象の少なくとも一部となる。そして、署名生成装置の任意値生成部が、整数の任意値ｋを生成し、群演算部が、位数ｑの巡回群をＧとし、当該巡回群Ｇの生成元をｇとした場合における$R=g^{k}\in G$を算出し、当該演算結果Ｒを得る。なお、「$g^{k}\in G$」とは、巡回群Ｇをなす演算をｇについてｋ回実行することを意味する（詳細は後述）。次に、署名生成装置の第１ハッシュ演算部が、リカバリメッセージm_{rec}のビット長Ｍに応じて出力ビット長がＬ＋Ｍビット（Ｌは署名検証装置と共有される正の整数）に定まるハッシュ関数H_0：｛０，１｝*→｛０，１｝$^{L+M}$を、演算結果Ｒに作用させ、その演算結果であるＬ＋Ｍビットのハッシュ値$\Pi=H_0(R)\in\{0,1\}^{L+M}$を得る。なお、「関数εをδに作用させる」とは、「δ又はδを特定するための値を関数εに代入する」ことを意味する。次に、署名生成装置の第２ハッシュ演算部が、入力値に対してＬビットのハッシュ値を出力するハッシュ関数H_1：｛０，１｝*→｛０，１｝^{L}を、ハッシュ値Πとリカバリメッセージm_{rec}とに対応する値αに作用させ、その演算結果であるＬビットのハッシュ値$h=H_1(\alpha)\in\{0,1\}^{L}$を得る。また、署名生成装置の第３ハッシュ演算部が、リカバリメッセージm_{rec}のビット長Ｍに応じて出力ビット長がＭビットに定まるハッシュ関数H_2：｛０，１｝*→｛０，１｝^{M}を、ハッシュ値Πとハッシュ値ｈとに対応する値βに作用させ、その演算結果であるＭビットのハッシュ値$u=H_2(\beta)\in\{0,1\}^{M}$を得る。さらに、署名生成装置の第１排他的論理和演算部が、リカバリメッセージm_{rec}とハッシュ値ｕとの排他的論理和$w=m_{rec}(+)u\in\{0,1\}^{M}$（（＋）は排他的論理和演算子）を算出し、当該排他的論理和値ｗを得る。またビット結合部が、ハッシュ値$h\in\{0,1\}^{L}$を第１ビット位置に配置し、排他的論理和値$w\in\{0,1\}^{M}$を第２ビット位置に配置したＬ＋Ｍビットのビット結合値$d=h\mid w\in\{0,1\}^{L+M}$を算出し、当該ビット結合値ｄを得る。なお、第１ビット位置は必ずしも連続したＬビットの位置である必要はなく、離散的に配置された合計Ｌビットの位置でもよい。同様に、第２ビット位置も必ずしも連続したＭビットの位置である必要はなく、離散的に配置された合計Ｍビットの位置でもよい。ただし、「第１ビット位置」及び「第２ビット位置」がどのビット位置であるか

については、署名生成装置と署名検証装置とで統一しておく。次に、署名生成装置の第２排他的論理和演算部が、ハッシュ値Πとビット結合値ｄとの排他的論理和ｒ＝Π（＋）ｄ∈｛０，１｝$^{L+M}$を算出し、当該排他的論理和値ｒを得る。また署名生成装置の第４ハッシュ演算部が、入力値に対して整数を出力するハッシュ関数H_3：｛０，１｝*→Ｚを、排他的論理和値ｒに対応する値γに作用させ、その演算結果であるハッシュ値ｔ＝H_3（γ）∈Ｚを得る。そして、整数演算部が、ｓ＝ｋ－ｔ・ｘ∈Ｚを算出し、当該演算結果ｓを得、署名出力部が署名σ＝（ｒ，ｓ）を出力する。

【手続補正３】
【補正対象書類名】明細書
【補正対象項目名】００１１
【補正方法】変更
【補正の内容】
【００１１】

署名生成装置の公開鍵をｙ＝g^x∈Ｇとする。そして、署名検証装置の署名入力部に署名σ’＝（ｒ’，ｓ’）が入力される。また、署名σ’に対応するリカバリメッセージm_{rec}’のビット長Ｍ’とする。なお、署名検証装置がビット長Ｍ’の値を取得する方法については後述する。そして、署名検証装置の第１ハッシュ演算部が、入力値に対して整数を出力するハッシュ関数H_3：｛０，１｝*→Ｚを、署名σ’が有するｒ’に対応する値γ’に作用させ、その演算結果であるハッシュ値ｔ’＝H_3（γ’）∈Ｚを得る。さらに、署名検証装置の群演算部が、Ｒ’＝$g^{s'}\cdot y^{t'}$∈Ｇの演算を行い、その演算結果Ｒ’を得る。なお、「$g^{s'}\cdot y^{t'}$∈Ｇ」とは、巡回群Ｇをなす演算をｇについてｓ’回施し、当該演算をｙについてｔ’回施し、それらの各演算結果に対して当該演算を施す演算を意味する（詳細は後述）。次に、署名検証装置の第２ハッシュ演算部が、リカバリメッセージm_{rec}’のビット長Ｍ’に応じて出力ビット長がＬ＋Ｍ’ビット（Ｌは正の整数）に定まるハッシュ関数H_0：｛０，１｝*→｛０，１｝$^{L+M'}$を、演算結果Ｒ’に作用させ、その演算結果であるＬ＋Ｍ’ビットのハッシュ値Π’＝H_0（Ｒ’）∈｛０，１｝$^{L+M'}$を得る。さらに、署名検証装置の第１排他的論理和演算部が、ハッシュ値Πと署名σ’が有するｒ’との排他的論理和ｄ’＝Π’（＋）ｒ’∈｛０，１｝$^{L+M'}$を算出し、当該排他的論理和値ｄ’を得る。また、署名検証装置の第３ハッシュ演算部が、リカバリメッセージm_{rec}’のビット長Ｍ’に応じて出力ビット長がＭ’ビットに定まるハッシュ関数H_2：｛０，１｝*→｛０，１｝$^{M'}$を、ハッシュ値Π’と排他的論理和値ｄ’の第１ビット位置のＬビットの値ｈ’∈｛０，１｝^{L}とに対応する値β’に作用させ、その演算結果であるＭ’ビットのハッシュ値ｕ’＝H_2（β’）∈｛０，１｝$^{M'}$を得る。また、第２排他的論理和演算部が、排他的論理和値ｄ’の第２ビット位置のＭ’ビットの値ｗ’∈｛０，１｝$^{M'}$とハッシュ値ｕ’との排他的論理和ｗ’（＋）ｕ’を算出し、その演算結果をリカバリメッセージm_{rec}’∈｛０，１｝$^{M'}$として得る。さらに、第４ハッシュ演算部が、入力値に対してＬビットのハッシュ値を出力するハッシュ関数H_1：｛０，１｝*→｛０，１｝^{L}を、ハッシュ値Π’と第２排他的論理和演算部で算出されたリカバリメッセージm_{rec}’とに対応する値α’に作用させ、その演算結果であるＬビットのハッシュ値H_1（α’）∈｛０，１｝^{L}を得る。そして、比較部が、Ｌビットの値ｈ’とH_1（α’）とを比較する。