**SCIS 2021** 2021 Symposium on
Cryptography and Information Security
On-line, Jan. 19 – 22, 2021
The Institute of Electronics,
Information and Communication Engineers

# 対称ペアリングに基づく非対称ペアリングの限界について
# On the Restriction of Asymmetric Pairing based on Symmetric Pairing

星野 文学 *
Fumitaka Hoshino

**あらまし** 対称ペアリングを用いて非対称ペアリングに似た性質を持つ暗号プリミティブを構成できる事が知られている．そのように構成した暗号プリミティブは対称ペアリングと非対称ペアリングを折衷したような性質を持ち, 高機能な暗号方式への適用が期待できる．しかし, そのようなプリミティブが, どのような制約を持つかは, それほど明確になっていない．本稿ではそのような暗号プリミティブの適用限界について論じる．

**Keywords:** ペアリング, 非可換環, 行列多項式方程式

## 1 はじめに

対称ペアリングを用いて非対称ペアリングに似た性質を持つ暗号プリミティブを構成できる事が知られており, そのような暗号プリミティブ上では, ある種の DDH 問題の trapdoor が CDH 問題の trapdoor から分離出来る事が知られている [1–3]．このプリミティブと通常のペアリングとの間には離散対数の可換性に関する代数的構造に大きな違いが存在する．にもかかわらず, かなり多数の暗号の方式構成に, このプリミティブが適用可能である．さらに trapdoor を持たない時の, このプリミティブの DDH 安全性は (語義に反し) 通常の対称ペアリングの DLIN 仮定に帰着を持つ．一般に, DDH ベースの暗号方式を DLIN ベースに設計し直すのは煩雑な手続きであるが, 離散対数の可換性を見直すだけなら, かなりの手間が省略できる．つまり, 従来の暗号方式を新しいプリミティブを使ってインプリメントするという方法論によって, 新たな機能を持つ暗号が容易に得られる事が期待できる．しかし, 新しいプリミティブと通常のペアリングの代数的構造の違いが, 方式の安全性証明にどれだけの影響を与えるかについては, 別途検討する必要があるであろう．そこで, 本稿では, ほとんど同じような安全性証明を持つ Schnorr 認証の special soundness, Pedersen commitment の binding property, 情報理論的な hash function family の universal property について, プリミティブの置き換えによる影響を調査し, その違いを明確にした．

* Secure Platform Laboratories, NTT Corporation, Japan

## 2 準備

### 2.1 離散対数

計算量的暗号方式の設計においては, 離散対数とは様々な暗号学的応用が可能な暗号プリミティブ (原始方式) の事であり, 形式的には安全変数 $\lambda \in \mathbb{N}$ を入力とし, $\lambda$ でパラメタライズされる安全性を満たす (と思しき), ある代数的構造の効率的な符号に関する記述 $(\mathbb{L}, \mathbb{G}, \mathsf{aux})$ を出力する確率的多項式時間アルゴリズム

$$\mathcal{G} : 1^\lambda \xmapsto{\$} (\mathbb{L}, \mathbb{G}, \mathsf{aux})$$

であると定義される．$\mathbb{L}, \mathbb{G}$ は代数的構造の効率的な符号化方法を記述する文字列であるが, 回りくどいので以降は $\mathbb{L}, \mathbb{G}$ と代数的構造とを同一視する．従って $|\mathbb{L}|$ や $|\mathbb{G}|$ 等と記述した時, それは記述の長さや符号語の数等ではなくて, 記述された代数的構造の位数を意味するとする．典型的には $\mathbb{G}$ を素数位数巡回群 $\langle g \rangle$ (位数 $q$) とし $\mathbb{L} := \mathbb{F}_q$ とされるが, ここではその拡張を扱うので,

1. $\mathbb{L}$ を単位的環, $\mathbb{G}$ をその環上の加群とする．また $\mathsf{aux} \in \{0,1\}^*$ は補助情報とする．

情報理論的な安全性に関する要請により少なくとも

2. $|\mathbb{L}|, |\mathbb{G}| \geq 2^{\Theta(\lambda)}$

が必要である．典型的な離散対数とのアナロジーにより加群としての和とスカラー倍を $\mathbb{G}$ 上の積および冪乗と呼び, 記法も巡回群の積および冪乗に準じる．一般の $\mathbb{L}$ について左右 2 種類の冪乗が存在するが, $\mathbb{L}$ が可換の場合には両者は一致する．これから, この拡張に合わせて離散対数の概念を幾分精密に定義していくが, この定義は $\mathbb{G} := \langle g \rangle$, $\mathbb{L} := \mathbb{F}_q$ とすれば典型的な離散対数の定義と一致する．

3. 次の $\lambda$ に関する確率的多項式時間アルゴリズムが自明であるか, あるいは $(\mathbb{L}, \mathbb{G}, \mathsf{aux})$ の何れかに含まれる．
   - $\mathbb{L}, \mathbb{G}$ 上の標本．
   - $\mathbb{L}, \mathbb{G}$ の元の識別 $(=, \neq)$．
   - $\mathbb{L}$ 上の環演算．
   - $\mathbb{G}$ 上の積 : $\mathbb{G} \times \mathbb{G} \to \mathbb{G}$．
   - $\mathbb{G}$ 上の右冪乗 (非退化双準同型) : $\mathbb{G} \times \mathbb{L} \to \mathbb{G}$．
   - $\mathbb{G}$ 上の左冪乗 (非退化双準同型) : $\mathbb{L} \times \mathbb{G} \to \mathbb{G}$．

一般に暗号認証技術の設計において安全性の証明を行う際には, 暗号プリミティブに対して定義される何らかの暗号学的問題を考察する．$\lambda$ は安全変数と呼ばれ, 暗号学的問題を解こうと試みる確率的多項式時間攻撃者 $\mathcal{A}$ に対して定義される利得が, 如何なる $\mathcal{A}$ に対しても $\lambda$ に関して無視可能となる事が暗号プリミティブが安全である事の差し当たっての定義である．暗号プリミティブの安全性を数学的に証明する事は多くの場合は困難であり, 通常は経験的に成立すると予想される仮説が用いられる．そのような仮説を暗号学的仮定と呼ぶ．通常, 離散対数プリミティブにおいては暗号学的仮定は少なくとも次の仮定を含意する．

4. $\mathcal{G}$-離散対数仮定: オラクルチューリングマシン
   $\mathrm{Exp}^{\mathcal{G},\mathcal{A}}(1^\lambda) :=$
   $(\mathbb{L}, \mathbb{G}, \mathsf{aux}) \xleftarrow{\$} \mathcal{G}(1^\lambda)$,
   $x \xleftarrow{\$} \mathbb{L},\ g \xleftarrow{\$} \mathbb{G},\ y \leftarrow g^x$,
   $x^* \xleftarrow{\$} \mathcal{A}(\mathbb{L}, \mathbb{G}, \mathsf{aux}, g, y)$,
   $\mathtt{Output}\ (y \stackrel{?}{=} g^{x^*})$.
   に対し定義される利得 $\mathsf{Adv}^{\mathcal{G},\mathcal{A}}(\lambda) := \Pr[\mathrm{Exp}^{\mathcal{G},\mathcal{A}}(1^\lambda) = 1]$ が如何なる確率的多項式時間チューリングマシン $\mathcal{A}$ に対しても無視可能である．

概ね底をランダムに一つ選んだ時に冪を変数とした冪乗関数の原像困難性を言っている．(厳密には左右の冪乗の両方に対して離散対数問題を考える事が出来るが, 本稿で扱う具体例については双方向に帰着がある.) 離散対数仮定が尤もらしい $\mathcal{G}$ を離散対数群と呼ぶ．回りくどいので $\mathcal{G}$ が離散対数群である事を $\mathbb{G}$ が離散対数群であるとも言う．膨大な量の離散対数仮定を含意する仮定 (眷属) が提案されており [4], その中でも次の computational Diffie-Hellman (CDH) 仮定が特に有名である．

> $\mathcal{G}$-CDH 仮定: オラクルチューリングマシン
> $\mathrm{Exp}^{\mathcal{G},\mathcal{A}}(1^\lambda) :=$
> $(\mathbb{L}, \mathbb{G}, \mathsf{aux}) \xleftarrow{\$} \mathcal{G}(1^\lambda)$,
> $g_0 \xleftarrow{\$} \mathbb{G}$,
> $g_1 \leftarrow {}^a g_0 \mid a \xleftarrow{\$} \mathbb{L}$,
> $g_2 \leftarrow g_0^b \mid b \xleftarrow{\$} \mathbb{L}$,
> $g_3 \xleftarrow{\$} \mathcal{A}(\mathbb{L}, \mathbb{G}, \mathsf{aux}, g_0, g_1, g_2)$,
> $\mathtt{Output}\ (g_3 \stackrel{?}{=} {}^a g_0^b)$.
> に対し定義される利得 $\mathsf{Adv}^{\mathcal{G},\mathcal{A}}(\lambda) := \Pr[\mathrm{Exp}^{\mathcal{G},\mathcal{A}}(1^\lambda) = 1]$ が如何なる確率的多項式時間チューリングマシン $\mathcal{A}$ に対しても無視可能である．

CDH 仮定が尤もらしい $\mathcal{G}$ あるいは $\mathbb{G}$ を CDH 群と呼ぶ．$\mathbb{G}$ に有限体の乗法群を用いたものや有限体上定義された楕円曲線を用いたものが CDH 群の有名な例である．一方, 同じ代数的構造 (巡回群) でも $\mathbb{L} = \mathbb{F}_q$, $\mathbb{G} = (\mathbb{Z}/q\mathbb{Z})^+$ とすれば, その CDH 問題 (および離散対数問題) は自明に解くことが出来る．こうした仮定が困難そうであるか, あるいは明らかに簡単であるかは $\mathbb{L}$ や $\mathbb{G}$ をどのように符号化するかに依存する．

### 2.2 ペアリング

ペアリングとは概ね次のような離散対数の拡張 (確率的多項式時間アルゴリズム) である．

$$\mathcal{G}' : 1^\lambda \xmapsto{\$} (\mathbb{L}, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, \mathsf{aux}')$$

1. $\forall x \in \{1, 2, T\}$ に関してオラクルチューリングマシン $\mathcal{G}_x^{\mathcal{G}'}(1^\lambda) :=$
   $(\mathbb{L}, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, \mathsf{aux}') \xleftarrow{\$} \mathcal{G}'(1^\lambda)$,
   $\mathsf{aux} \leftarrow (\mathbb{L}, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, \mathsf{aux}')$,
   $\mathtt{Output}(\mathbb{L}, \mathbb{G}_x, \mathsf{aux})$.
   が全て CDH 群である．即ち $\mathbb{G}_x$ が全て CDH 群である．
2. 次の $\lambda$ に関する確率的多項式時間アルゴリズムが自明であるか, あるいは $(\mathbb{L}, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, \mathsf{aux}')$ の何れかに含まれる．
   - ペアリング (非退化双準同型) $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$．

$\mathbb{G}_1, \mathbb{G}_2$ をソース群 (source group), $\mathbb{G}_T$ を標的群 (target group) と呼ぶ．Galbraith らは, 暗号方式に用いられるペアリングを大雑把に以下の 3 つの型に分類した [5].

Type 1: $\psi : \mathbb{G}_2 \to \mathbb{G}_1$, $\psi^{-1} : \mathbb{G}_1 \to \mathbb{G}_2$ なる多項式時間非退化準同型写像が存在する. (即ち $\mathbb{G}_1 = \mathbb{G}_2$ として良い.)
Type 2: $\psi : \mathbb{G}_2 \to \mathbb{G}_1$ なる一方向非退化準同型写像が存在する.
Type 3: $\mathbb{G}_1, \mathbb{G}_2$ の間に多項式時間非退化準同型写像が存在しない.

一般に Type 1 を対称ペアリングと呼び, Type 2, Type 3 を非対称ペアリングと呼ぶ. CDH 群 $\mathcal{G}$ に対して次の仮定は decisional Diffie-Hellman (DDH) 仮定と呼ばれる.

$\mathcal{G}$-DDH 仮定: オラクルチューリングマシン
$\mathrm{Exp}^{\mathcal{G},\mathcal{A}}(1^\lambda) :=$
$(\mathbb{L}, \mathbb{G}, \mathsf{aux}) \xleftarrow{\$} \mathcal{G}(1^\lambda)$,
$g_0 \xleftarrow{\$} \mathbb{G}$,
$g_1 \leftarrow {}^a g_0 \mid a \xleftarrow{\$} \mathbb{L}$,
$g_2 \leftarrow g_0^b \mid b \xleftarrow{\$} \mathbb{L}$,
$h_0 \leftarrow g_0^c \mid c \xleftarrow{\$} \mathbb{L}$,
$h_1 \leftarrow {}^a g_0^b$,
$g_3 \leftarrow h_d \mid d \xleftarrow{\$} \{0,1\}$,
$d^* \xleftarrow{\$} \mathcal{A}(\mathbb{L}, \mathbb{G}, \mathsf{aux}, g_0, g_1, g_2, g_3)$,
$\mathtt{Output}\ (d \stackrel{?}{=} d^*)$.
に対し定義される利得 $\mathsf{Adv}^{\mathcal{G},\mathcal{A}}(\lambda) := |\Pr[\mathrm{Exp}^{\mathcal{G},\mathcal{A}}(1^\lambda) = 1] - 1/2|$ が如何なる確率的多項式時間チューリングマシン $\mathcal{A}$ に対しても無視可能である.

DDH 仮定が尤もらしい $\mathcal{G}$ あるいは $\mathbb{G}$ を DDH 群と呼ぶ. 多項式時間非退化双準同型 $e$ の存在により, $\mathbb{L}$ が可換の時はペアリングのソース群に関して次の事が自明に分かる.

Type 1 では $\mathbb{G}_1 = \mathbb{G}_2$ 上で DDH 仮定は成立しない.
Type 2 では $\mathbb{G}_2$ 上で DDH 仮定は成立しない.

それ以外の $\mathbb{G}_x$ では DDH 仮定が成立していてもペアリングの形式的な定義とは矛盾しないので, そのような仮定, 例えば SXDH 仮定などはプロトコルの設計にしばしば用いられる. また $\mathbb{L}$ が非可換であるときは DDH 仮定とペアリングの形式的な定義とは矛盾しない.

### 2.3 trapdoor DDH

trapdoor DDH 群とは落とし戸があれば DDH 仮定を破ることができる DDH 群の拡張で, 本稿で扱うのは, 次の 2 つの確率的多項式時間アルゴリズムが存在するものである.

- $\mathbb{G}$ の元および対応する落とし戸の組をランダムに出力する確率的多項式時間アルゴリズム

$$\begin{array}{rccccc} \mathtt{tsamp}: & 1^* & \xrightarrow{\$} & \mathbb{G} & \times & \{0,1\}^* \\ & 1^\lambda & \mapsto & g_0 & , & t \end{array}$$

- 上記 tsamp によって生成された $g_0$ を用いて生成された DDH インスタンス $(\mathbb{L}, \mathbb{G}, \mathsf{aux}, g_0, {}^a g_0, g_0^b, g_3)$ と対応する落とし戸 $t$ を入力として, $(g_3 \stackrel{?}{=} {}^a g_0^b)$ であるか否かを出力する確率的多項式時間アルゴリズム

$$\mathtt{solve} : (\mathbb{L}, \mathbb{G}, \mathsf{aux}, g_0, {}^a g_0, g_0^b, g_3), t \xrightarrow{\$} (g_3 \stackrel{?}{=} {}^a g_0^b)$$

### 2.4 trapdoor DDH 構成の素朴なアイディア

素数位数巡回群 $\mathbb{G}$ を対称ペアリング群とし, $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ をペアリングとする. $\mathbb{G}$ は $(\mathbb{Z}/q\mathbb{Z})^+$ と同型であるから, これを $\mathbb{F}_q$ だと思えば, 群演算を和, 冪をスカラー倍として, $\mathbb{G}$, は階数 1 の $\mathbb{F}_q$ ベクトル空間と見做すことができる. 従って $\mathbb{G}' := \mathbb{G} \oplus \mathbb{G}$ は成分毎の群演算を和, 成分毎の冪をスカラー倍とした階数 2 の $\mathbb{F}_q$ ベクトル空間と見做すことができる. $\alpha$ を $\mathbb{G}$ の生成元として $a, b \in \mathbb{F}_q^*$ をランダムに選ぶと $g_1 := (\alpha^a, \alpha^b) \in \mathbb{G}'$ は位数 $q$ の巡回群 $\mathbb{G}_1 = \langle g_1 \rangle$ を生成する. 同様に $c, d \in \mathbb{F}_q^*$ をランダムに選ぶと $g_2 := (\alpha^c, \alpha^d) \in \mathbb{G}'$ は高い確率で位数 $q$ の巡回群 $\mathbb{G}_2 = \langle g_2 \rangle \neq \mathbb{G}_1$ を生成する. さらに $\gamma, \gamma' \in \mathbb{F}_q$ を適当な定数として $e' : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ を

$$e' : (f_1, f_2), (h_1, h_2) \mapsto e(f_1, h_2)^\gamma e(h_1, f_2)^{\gamma'}$$

と定義すれば, $e'$ は非退化双線形写像の確率的多項式時間アルゴリズムとなる. 従って $(\mathbb{G}_1, \mathbb{G}_2)$ は安全かどうかは別として, 非対称ペアリング群と見なすことが出来る.

今, 上記の $a, b, c, d$ ($\Delta := ad - bc \neq 0$) が予め分かっている場合, ベクトル空間 $\mathbb{G}' := \mathbb{G} \oplus \mathbb{G}$ の任意の元 $v := (v_1, v_2)$ は $\mathbb{G}_1$ の元と $\mathbb{G}_2$ の元

$$\begin{pmatrix} ({v_1}^d \cdot {v_2}^{-c})^{\Delta^{-1} \cdot a}, ({v_1}^d \cdot {v_2}^{-c})^{\Delta^{-1} \cdot b} \end{pmatrix} \in \mathbb{G}_1, \\ \begin{pmatrix} ({v_1}^{-b} \cdot {v_2}^a)^{\Delta^{-1} \cdot c}, ({v_1}^{-b} \cdot {v_2}^a)^{\Delta^{-1} \cdot d} \end{pmatrix} \in \mathbb{G}_2 \qquad (1)$$

の和 (成分毎の群演算) に多項式時間で分解できる. では $a, b, c, d$ が明かされない場合, このような分解は簡単であろうか? 吉田らは上記のベクトル分解問題を $\mathbb{G}$ 上の CDH 問題へ帰着し, $a, b, c, d$ を落し戸として使用する暗号プロトコルへの応用を示した [6]. この方法論はその後発展し, 様々な解析や応用が検討されている [7–14].

ところで, 80 年代に静谷らは, 概ね次のような離散対数の自然な拡張を考案した [15].

- $\langle\alpha\rangle$ を素数位数巡回群とし $\alpha$ をその生成元とし, その位数 (素数) を $q$ とする. 写像 : $\langle\alpha\rangle^{n\times m} \to \mathbb{F}_q^{n\times m}$,

$$\begin{pmatrix} \alpha^{x_{11}} & \dots & \alpha^{x_{1m}} \\ \vdots & \ddots & \vdots \\ \alpha^{x_{n1}} & \dots & \alpha^{x_{nm}} \end{pmatrix} \mapsto \begin{pmatrix} x_{11} & \dots & x_{1m} \\ \vdots & \ddots & \vdots \\ x_{n1} & \dots & x_{nm} \end{pmatrix}$$

を考える. $\mathbb{F}_q$ 行列 $x := (x_{ij}) \in \mathbb{F}_q^{n\times m}$ を $\alpha$ を底とする $X := (\alpha^{x_{ij}}) \in \langle\alpha\rangle^{n\times m}$ の離散対数と呼び, $X$ を $\alpha^x$ と書く.
- $x, y \in \mathbb{F}_q^{n\times m}$, $X := \alpha^x$, $Y := \alpha^y$ とする. 積 $XY$ を

$$\begin{array}{rccccc} XY: & \langle\alpha\rangle^{n\times m} & \times & \langle\alpha\rangle^{n\times m} & \to & \langle\alpha\rangle^{n\times m}, \\ & \alpha^x & , & \alpha^y & \mapsto & \alpha^{x+y}, \end{array}$$

と定義する. 積 $XY$ は可換.
- $x \in \mathbb{F}_q^{n\times\ell}$, $y \in \mathbb{F}_q^{\ell\times m}$ とし, $X := \alpha^x$, $Y := \alpha^y$ とする. 非退化双準同型 $X^y$ を

$$\begin{array}{rccccc} X^y: & \langle\alpha\rangle^{n\times\ell} & \times & \mathbb{F}_q^{\ell\times m} & \to & \langle\alpha\rangle^{n\times m}, \\ & \alpha^x & , & y & \mapsto & \alpha^{xy}, \end{array}$$

非退化双準同型 ${}^xY$ を

$$\begin{array}{rccccc} {}^xY: & \mathbb{F}_q^{n\times\ell} & \times & \langle\alpha\rangle^{\ell\times m} & \to & \langle\alpha\rangle^{n\times m}, \\ & x & , & \alpha^y & \mapsto & \alpha^{xy}, \end{array}$$

と定義する. $X^y$ を右冪乗 ${}^xY$ を左冪乗と呼ぶ.
- $X$ や $Y$ の離散対数を知らなくとも $\langle\alpha\rangle$ 上の群演算を用いて右冪乗, 左冪乗および積は効率的に計算可能.

このような概念を用いると, 例えば式 (1) のベクトル分解は

$$(\phi_1(v^{t^{-1}}))^t \in \mathbb{G}_1,\ (\phi_2(v^{t^{-1}}))^t \in \mathbb{G}_2$$

のように見通し良く記述できる. ここで $\phi_1 : (v_1, v_2) \mapsto (v_1, 1)$, $\phi_2 : (v_1, v_2) \mapsto (1, v_2)$ は射影演算で $t := \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ とする. $\alpha^t$ が公開されている状況で, 離散対数 $t$ を知っていればこの分解は簡単だが, 知らないものがこの分解を行う事は容易ではなさそうなので, $t$ を trapdoor とすることが可能である. この "非対称ペアリング" $(\mathbb{G}_1, \mathbb{G}_2)$ をそのまま trapdoor DDH とする事は出来ないが, $t$ は $\psi : \mathbb{G}_2 \to \mathbb{G}_1$ および $\psi^{-1} : \mathbb{G}_1 \to \mathbb{G}_2$ の trapdoor と見なすことが出来る.

### 2.5 trapdoor DDH の具体的な構成

[1] の trapdoor DDH 群の具体的構成を要約すると, およそ次のようになる.

- $\langle\alpha\rangle$ を (通常の) 対称ペアリングのソース群とし, $\alpha$ をその生成元とする. 同様に $\langle\alpha_T\rangle$ を対応する標的群とし, $\alpha_T$ をその生成元とする.

$$\mathbb{G} := \langle\alpha\rangle^{n\times n},\ \mathbb{L} := \mathbb{F}_q^{n\times n},\ \mathbb{G}_T := \langle\alpha_T\rangle^{n\times n}.$$

$\mathbb{G}$ は成分毎の群演算を群演算とするアーベル群で, これを trapdoor DDH 群と見なす. 静谷らの定義と同様に非可換環 $\mathbb{L}$ を $\mathbb{G}$ に対する離散対数と見なし, 積や冪乗も同様に定義する. また, 非退化双準同型 $e$ を

$$\begin{array}{rccccc} e: & \mathbb{G} & \times & \mathbb{G} & \to & \mathbb{G}_T, \\ & \alpha^x & , & \alpha^y & \mapsto & \alpha_T^{xy}, \end{array}$$

と定義する. 離散対数 $x$ や $y$ を知らなくとも $\langle\alpha\rangle$ 上のペアリングを用いて $e$ は効率的に計算可能である. $e$ を改めてペアリングと呼ぶ. このようなペアリング関数 $e$ の拡張は暗号プロトコルの設計の分野で良く知られており, 既に多用されている [16]. $\mathbb{G}$ 上の冪乗やペアリングを使って, `tsamp` および `solve` を次のように構成する.

$\texttt{tsamp}(1^\lambda) :=$
  $t \xleftarrow{\$} \mathbb{L}^*$,
  $g_0 \leftarrow \alpha^t$,
  $\texttt{Output}\ (g_0, t)$.
$\texttt{solve}((g_0, g_1, g_2, g_3), t) :=$
  $\texttt{Output}\ (e(g_1^{t^{-1}}, g_2) \stackrel{?}{=} e(I, g_3))$.

但し $\mathbb{L}^*$ は $\mathbb{L}$ の正則元 (非零因子) の集合とし $i$ を $\mathbb{L}$ 上の単位行列として $I = \alpha^i$ とする. また $\mathbb{L}^*$ 上の乗法逆元を計算する確率的多項式時間アルゴリズムが必要であるが, $\mathbb{L}^* = \mathrm{GL}(n, \mathbb{F}_q)$ 上の乗法逆元は効率的に計算可能なので問題ない. 厳密には $\mathbb{G}$ の分布と $\mathbb{G}^* = \mathrm{GL}(n, \langle\alpha\rangle) := \alpha^{\mathbb{L}^*}$ の分布は異なるが, $g_0 \in \langle\alpha\rangle^{n\times n}$ が正則であるか否か判定する問題を考えれば, $n \geq 3$ の場合, それが $\langle\alpha\rangle$ 上の DLIN 仮定の亜種であるという事が直ちに分かる. $n = 2$ の場合はこの判定は効率的に可能なので, $g_0$ のランダム標本が正則とならない確率を評価する必要があるが, それは

$$1 - \frac{q^{n(n-1)/2} \prod_{m=1}^{n} (q^m - 1)}{q^{n^2}} \tag{2}$$

であり, およそ $1/q$ と見積もればよい. また $t$ を知らない攻撃者に対する, このプリミティブの DDH 安全性は行列 $\left(\begin{smallmatrix} g_0 & g_1 \\ g_2 & g_3 \end{smallmatrix}\right) \in \langle g\rangle^{2n\times 2n}$ (の離散対数) が正則であるか否かという問題を考えれば, やはり $\langle\alpha\rangle$ 上の DLIN 仮定の亜種であるという事が直ちに分かる. もちろん $n = 1$ の場合はこの安全性は壊れている (通常の対称ペアリング群).

## 3　暗号プロトコルへの応用

前述の定義によれば $\mathbb{L}$ が非可換でも, $\mathbb{L}$ の非可換性や冪乗に左右がある事に目を瞑れば, 離散対数やペアリングの定義はそれほど大きな変更を迫られない上に, $\mathbb{G}$ 上の DDH 仮定に対して落とし戸を構成できるという新しい機能を追加できることが分かった. 従って, 既存の暗号プロトコルで使用されてきた典型的な離散対数群やペアリング群を前述の構成で置き換える事が出来れば, プロトコルにに新たな機能を付加できるかもしれない.

### 3.1　Schnorr 認証 [17]

Schnorr 認証は, 公開鍵に紐づく離散対数を知ってることの honest な検証者に対する知識のゼロ知識証明である. Schnorr 認証は, 下記のように $\mathbb{L} = \mathbb{F}_q^{n\times n}$ でもほとんど問題なく実行できる.

- Prover は秘密鍵 $x \in \mathbb{L}$ を生成し, 公開鍵 $y = g^x$ を公開する.
- Prover は $t \in \mathbb{L}$ を生成し, コミット $T = g^t$ を Verifier に送信.
- Verifier はチャレンジ $c \in \mathbb{L}$ を生成し Prover に送信.
- Prover はレスポンス $s = t - xc$ を Verifier に送信.
- Verifier は $T \stackrel{?}{=} g^s y^c$ を調べる.

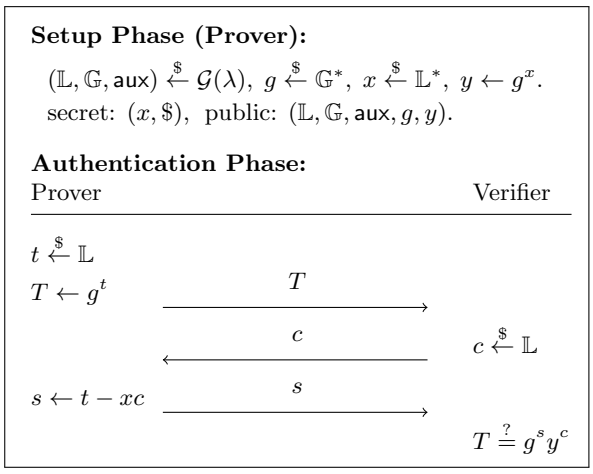


図 1　Schnorr 認証 ($PK\{(x) : y = g^x\}$)

Schnorr 認証は暗号アプリケーションのビルディングブロックとして多用されるプロトコルで, Chaum-Pedersen のプロトコル [18], Cramer-Damgård-Schoenmakers のプロトコル [19], Fiat-Shamir heuristic [20] といった常套手段を介して様々な暗号プロトコルの構成に利用される. Schnorr 認証の honest verifier zero-knowledgeness は,

- $(c', s') \xleftarrow{\$} \mathbb{L}^2$
- $T' \leftarrow g^{s'} y^{c'}$
- `Output` $(T', c', s')$.

なるシミュレーションが生成するトランスクリプト $(T', c', s')$ の分布と実際のプロトコルのトランスクリプト $(T, c, s)$ の分布を比較する事によって示される. $\mathbb{L} = \mathbb{F}_q^{n\times n}$ でも $\mathbb{L} = \mathbb{F}_q$ の場合と同様に $(T', c', s')$ の分布は $(T, c, s)$ の分布と完全に一致する. 即ち Schnorr 認証の honest verifier zero-knowledgeness は, $\mathbb{L} = \mathbb{F}_q^{n\times n}$ でも perfect である. Schnorr 認証の special soundness は, 単一の $T$ をコミットした攻撃者が二つのランダムなチャレンジ $c_1, c_2 \in \mathbb{L}$ に対して, それぞれ正しいレスポンス $s_1, s_2 \in \mathbb{L}$ を返す事が出来るなら, secret key $x$ を

$$x = (s_2 - s1)/(c_1 - c_2)$$

によって extract 出来る事によって示される. $\mathbb{L} = \mathbb{F}_q$ の場合, この extract に失敗するのは $c_1 - c_2 = 0$ となる場合のみであり, その確率は $1/q$ である. 同様に $\mathbb{L} = \mathbb{F}_q^{n\times n}$ の場合, この extract に失敗するのは $c_1 - c_2 \notin \mathbb{L}^*$ となる場合のみである. そのような確率は式 (2) であり, およそ $1/q$ と見積もればよい.

### 3.2　Pedersen commitment [21]

Pedersen commitment は $g, h \in \mathbb{G}$ が受信者と送信者に公開されているとき, 送信者がメッセージ $m \in \mathbb{L}$ をコミットする commitment 方式である.

Setup Phase

- Dealer は $(\mathbb{L}, \mathbb{G}, \mathsf{aux}) \xleftarrow{\$} \mathcal{G}(\lambda)$ を生成する.
- Dealer は $(g, h) \xleftarrow{\$} (\mathbb{G}^*)^2$ を生成する.
- Dealer は $(\mathbb{L}, \mathbb{G}, \mathsf{aux}, g, h)$ を公開する.

Commitment Phase

- Sender はデコミットメント $d \xleftarrow{\$} \mathbb{L}$ を生成する.
- Sender はメッセージ $m \in \mathbb{L}$ に対してコミットメント $c = g^m h^d$ を計算する.
- Sender はコミットメント $c$ を Reciever に送る.

Decommitment Phase

- Sender は $(m, d)$ を Reciever に送る.
- Reciever は $c \stackrel{?}{=} g^m h^d$ を検証する.

Pedersen commitment は 準同型性を持つので, 電子投票方式のような様々な暗号プロトコルの構成に有用であ

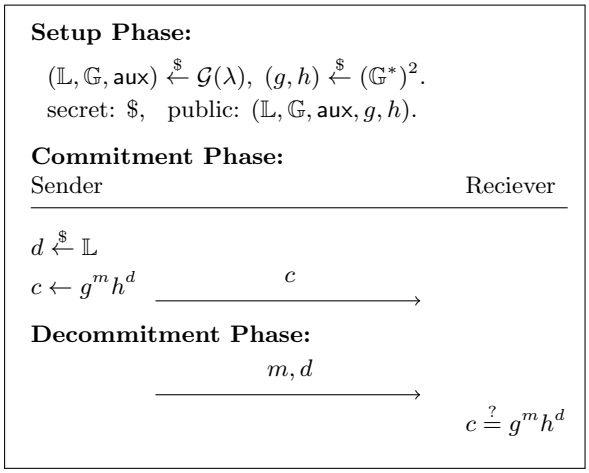


図 2　Pedersen Commitment

る．binding property については sender が $g, h$ 間の離散対数の知識を計算量的に持たない事を前提とする為, 離散対数を経由しないサンプリングアルゴリズムか, 信頼できる dealer を用意する必要がある．逆に $g, h$ 間の離散対数が binding property の trapdoor となり, 暗号プロトコルの部品として利用する際, 使い勝手が良いので多用される．そのような commitment は trapdoor commitment あるいは chameleon commitment などと呼ばれる．$g$ や $h$ が $\mathbb{G}^*$ からサンプルされているなら, 与えられた $c \in \mathbb{G}$ および $m \in \mathbb{L}$ より

$$h^d = c \cdot g^{-m}$$

なる $d$ が一意に定まるので, Pedersen commitment は perfect hiding となる．$g$ や $h$ が $\mathbb{G}^*$ からではなく $\mathbb{G}$ からランダムにサンプルされるなら, (2) により大抵の場合は $\mathbb{G}^*$ からサンプルされる事になるので, Pedersen commitment は statistical hiding となる．従って Pedersen commitment の hiding property は $\mathbb{L} = \mathbb{F}_q^{n \times n}$ でもほとんど問題ない．binding property については, 同じコミットメント $c$ に対して攻撃者が $c = g^m h^d = g^{m'} h^{d'}$ なる $(m, d)$ および $(m', d')$ が計算出来たとすると,

$$h^{d''} = g^{m''}$$

なる $(m'', d'') := (m - m', d' - d)$ が計算可能という事となる．$\mathbb{L} = \mathbb{F}_q^{n \times n}$ のとき $d''$ が正則であるなら $\mathbb{L} = \mathbb{F}_q$ と同様

$$\log_g h = m''/d'' \tag{3}$$

にて直ちに computational bind が言える．従って $d''$ が圧倒的確率で正則とならないような攻撃者から離散対数を extract 出来るか？ という事が問題となる．しかし, $g$ や $h$ が $\mathbb{G}^*$ からサンプルされているなら, $(m'', d'')$ には離散対数の部分情報 (離散対数の部分空間に関する情報) が含まれる事となる．さらに, このコミットメントは問題インスタンスをランダム自己帰着により容易に他の問題インスタンスに帰着できるので, 攻撃者を何度か呼び出す事によって, 高い確率で $h^{d''} = g^{m''}$ なる $(m'', d'')$ のうち $d''$ が正則なものが計算可能となる．従って (3) により computational bind が言える．

## 4　情報理論的なプロトコルに関して

上記のように, 計算量的なプロトコルでは非正則性によって起こる問題を, ランダム自己帰着によって無理やり解決するというような事ができた．このような無理やりな解決法は, 情報理論的なプロトコルでは通用しないと思われる．本節では Schnorr 認証の special soundness や Pedersen commitment の binding property と同じような安全性証明の構造を持つ情報理論的なプロトコルについて考察する．

### 4.1　$\mathbb{L}$ 上のある hash function family [22]

$\mathcal{M}$ をメッセージ空間, $\mathcal{K}$ を鍵空間, $\mathcal{R}$ をハッシュ値の値域とする．hash function family (keyed hash)

$$\mathcal{H} := \{(h_k : \mathcal{M} \to \mathcal{R}) \mid k \in \mathcal{K}\}$$

が $\forall m, m' \in \mathcal{M},\ m \neq m'$,

$$\Pr_{k \in \mathcal{K}}[h_k(m) = h_k(m')] \leq 1/|\mathcal{R}|$$

なるとき, $\mathcal{H}$ は universal であると呼ばれる [22]．一般に上記不等式を定数倍や漸近的表現によって緩和する事で, universal の概念は拡張される．$\mathcal{M} = \mathcal{R} = \mathbb{L}$, $\mathcal{K} := \mathbb{L}^2$ とし, $m \in \mathcal{M}$, $k := (k_0, k_1) \in \mathcal{K}$ とする．$\mathbb{L}$ 上の hash function family

$$h_k : m \mapsto k_0 + m \cdot k_1 \tag{4}$$

は $\mathbb{L} = \mathbb{F}_q$ の場合に, $\forall m, m' \in \mathbb{L},\ m \neq m'$,

$$\begin{aligned}
&\Pr_{k \in \mathcal{K}}[h_k(m) = h_k(m')] \\
&\quad = \Pr_{k \in \mathcal{K}}[(m - m') \cdot k_1 = 0] \\
&\quad = \Pr_{k \in \mathcal{K}}[k_1 = 0] \\
&= 1/|\mathbb{L}|
\end{aligned}$$

であるから universal である．このような $h_k$ は非常に効率の良いワンタイム安全なメッセージ認証符号 (MAC) を得るために良く利用される．ワンタイム安全な MAC は, 例えば CPA 安全な ID ベース暗号などから CCA 安全な方式を得る Boneh-Katz 変換 [23] などで利用される．

ところで $\mathbb{L} = \mathbb{F}_q^{n\times n}$, $n \geq 2$ の場合は零因子の存在により $\exists m, m' \in \mathbb{L}$, $m \neq m'$,

$$\Pr_{k\in\mathcal{K}}[(m-m')\cdot k_1 = 0] \gg \Pr_{k\in\mathcal{K}}[k_1 = 0]$$

であるから, universal の定義を定数倍程度緩和したとしても $h_k$ は universal とは言い難い. つまり $h_k$ の性質は零因子の存在により大幅に劣化する.

### 4.2 $h_k$ を用いた MAC

$h_k$ を用いた MAC がワンタイム安全とは, どのような確率的機械の組, 即ち攻撃者 $\mathcal{A} := (\mathcal{A}_1, \mathcal{A}_2)$ に対しても, 存在的攻撃が成功する確率

$$P_{\mathcal{A}} := \Pr_{\$}\left[\begin{array}{l|l} & k \xleftarrow{\$} \mathcal{K}, \\ h_k(m') = t' & (m,s) \xleftarrow{\$} \mathcal{A}_1(h), \\ \wedge\, m \neq m' & t \leftarrow h_k(m), \\ & (m',t') \xleftarrow{\$} \mathcal{A}_2(h,m,s,t) \end{array}\right]$$

が無視可能であると定義される. 無視可能の定義によりワンタイム安全のレベルが変化する. 上記の universal の定義に習うなら $P_{\mathcal{A}} \leq 1/|\mathcal{R}|$ である. $\mathbb{L} = \mathbb{F}_q$ の場合の上記 $h_k$ のワンタイム安全は次のような議論により示される.

- 攻撃者に与えられたヒント $(m,t)$ により, 取り得る秘密鍵 $(k_0, k_1)$ は

$$t = k_0 + m\cdot k_1 \tag{5}$$

  なる制約を受ける. このとき可能な $(k_0,k_1)$ は $|\mathbb{L}|$ 通りあり, その分布は一様である.
- 最終的に攻撃者が $x \neq y$ なる $(m',t')$ を出力し, それが正解だったとすると

$$t' = k_0 + m'\cdot k_1. \tag{6}$$

- (5), (6) の線形連立方程式により

$$k_1 = (t-t')/(m-m'),$$
$$k_0 = t - m\cdot k_1,$$

  と $(k_0,k_1)$ は一意に定まり, それ以外の鍵で等式 (5), (6) が同時に満たされる事は無い.
- 従って攻撃が成功する確率は, 等式 (5) を満たす $|\mathbb{L}|$ 通りの鍵の中から, たまたま正しい唯一の鍵を選ぶ確率 $1/|\mathbb{L}|$ に他ならない.

$\mathbb{L} = \mathbb{F}_q^{n\times n}$, $n \geq 2$ の場合は $(x-y)$ が正則とならないような攻撃を考える必要がある. $(x-y)$ のランクが 1 であるならそのような攻撃が成功する確率は期待される $1/|\mathbb{L}|$ よりかなり大きい ($\sim 1/q^n$).

### 4.3 より効率的な MAC

前節の MAC はメッセージ空間 $\mathcal{M} = \mathbb{L}$ が小さいという欠点を持つ. 実用的には $\ell$ を適当な定数, $\mathcal{M} = \mathbb{L}^\ell$ として, 次のような $h_k$ が良く知られている.

$$h_k : (m_1, \ldots, m_\ell) \mapsto k_0 + \sum_{i=1}^{\ell} m_i \cdot k_1^i \tag{7}$$

$\mathbb{L} = \mathbb{F}_q$ の場合に, 前節と同様の議論により, 定数倍程度緩和されたワンタイム安全が示される. つまり

$$t = k_0 + \sum_{i=1}^{\ell} m_i \cdot k_1^i,$$
$$t' = k_0 + \sum_{i=1}^{\ell} m'_i \cdot k_1^i$$

の連立方程式により

$$(t'-t) + \sum_{i=1}^{\ell} (m_i - m'_i)\cdot k_1^i = 0. \tag{8}$$

$\mathbb{L}$ が体 (整域) であるなら, 代数学の基本定理のアナロジーにより (8) を満たす $k_1 \in \mathbb{L}$ は高々 $\ell$ 個しか存在しない. 従って攻撃が成功する確率は高々 $\ell/|\mathbb{L}|$ である. ところで $\mathbb{L} = \mathbb{F}_q^{n\times n}$, $n \geq 2$ の場合は零因子の存在により

$$f(X)\cdot g(X) = 0 \;\Rightarrow\; f(X) = 0 \vee g(X) = 0$$

が必ずしも成り立たず, このような議論は破綻する. $\mathbb{L}$ 上の代数方程式 (8) の解の個数を評価する煩わしい議論が必要となるし, 前節同様安全性はかなり劣化する.

### 4.4 対策

使用する MAC に特に拘りがないなら, 大きい攻撃成功確率や, 煩わしい解の個数の議論を避ける為, $\mathbb{L} = \mathbb{F}_q^{n\times n}$ 上の元を $\mathbb{F}_{q^{n\times n}}$ 上の元に写像してから $\mathbb{F}_{q^{n\times n}}$ 上で (7) を構成する方が賢明である. 例えば $f(X)$ を $\mathbb{F}_q$ 上 $n\times n$ 次の既約多項式とすると

$$\mathbb{F}_q^{n\times n} \to \mathbb{F}_q[X]/(f(X)),\;\; (a_{ij}) \mapsto \sum_{i,j} a_{ij} X^{i\cdot n+j},$$

を使って, $\mathbb{F}_q^{n\times n}$ と $\mathbb{F}_{q^{n\times n}} \simeq \mathbb{F}_q[X]/(f(X))$ の間は効率的に行き来できる[*1]. $\mathbb{F}_{q^{n\times n}}$ 上で (7) を構成すれば, 零因子に煩わされる事は無くなる.

[*1] 全単射だが, 体ではない環と有限体との間の写像なので, 環同型ではない. 勿論, 和に関しては群同型である.

## 参考文献


[1] F. Hoshino, "A Variant of Diffie-Hellman Problem and How to Prove Independency." In *Proc. of SCIS 2014 2014 Symposium on Cryptography and Information Security 2014*. IEICE, 2014.

[2] F. Hoshino and T. Kobayashi, "On an Application of a Variant of Trapdoor DDH Group." In *Proc. of CSS 2019 Computer Security Symposium 2019 in Nagasaki, Japan, Oct. 21-24, 2019*. IPSJ, SIG CSEC, 2019.

[3] F. Hoshino and T. Kobayashi, "Asymmetric Pairing based on Symmetric Pairing." In *Proc. of SCIS 2020 2020 Symposium on Cryptography and Information Security 2019*. IEICE, 2020.

[4] F. Vercauteren, editor, "Final Report on Main Computational Assumptions in Cryptography." ECRYPT II European Network of Excellence in Cryptology II, Deliverables of Multi-party and Asymmetric Algorithms Virtual Lab. (MAYA), D.MAYA.6, 2013. URL: https://www.ecrypt.eu.org/ecrypt2/documents/D.MAYA.6.pdf.

[5] S.D. Galbraith, K.G. Paterson, and N.P. Smart, "Pairings for cryptographers," Discrete Applied Mathematics, vol.156, no.16, pp.3113–3121, 2008. doi:10.1016/j.dam.2007.12.010.

[6] M. Yoshida, S. Mitsunari, and T. Fujiwara, "Vector Decomposition Problem and the Trapdoor Inseparable Multiplex Transmission Scheme based the Problem." In *Proc. of SCIS 2003 The 2003 Symposium on Cryptography and Information Security Hamamatsu, Japan, Jan. 26-29, 2003*. IEICE, 2003.

[7] I.M. Duursma and N. Kiyavash, "The vector decomposition problem for elliptic and hyperelliptic curves," IACR Cryptology ePrint Archive, vol.2005, p.31, 2005. URL: http://eprint.iacr.org/2005/031.

[8] I.M. Duursma and S. Park, "Elgamal type signature schemes for n-dimensional vector spaces," IACR Cryptology ePrint Archive, vol.2006, p.312, 2006. URL: http://eprint.iacr.org/2006/312.

[9] S.D. Galbraith and E.R. Verheul, "An analysis of the vector decomposition problem," Public Key Cryptography - PKC 2008, 11th International Workshop on Practice and Theory in Public-Key Cryptography, Barcelona, Spain, March 9-12, 2008. Proceedings, ed. R. Cramer, Lecture Notes in Computer Science, vol.4939, pp.308–327, Springer, 2008. doi:10.1007/978-3-540-78440-1_18.

[10] T. Okamoto and K. Takashima, "Homomorphic encryption and signatures from vector decomposition," Pairing-Based Cryptography - Pairing 2008, Second International Conference, Egham, UK, September 1-3, 2008. Proceedings, ed. S.D. Galbraith and K.G. Paterson, Lecture Notes in Computer Science, vol.5209, pp.57–74, Springer, 2008. doi:10.1007/978-3-540-85538-5_4.

[11] T. Okamoto and K. Takashima, "Fully secure functional encryption with general relations from the decisional linear assumption," Advances in Cryptology - CRYPTO 2010, 30th Annual Cryptology Conference, Santa Barbara, CA, USA, August 15-19, 2010. Proceedings, ed. T. Rabin, Lecture Notes in Computer Science, vol.6223, pp.191–208, Springer, 2010. doi:10.1007/978-3-642-14623-7_11.

[12] T. Okamoto and K. Takashima, "Decentralized attribute-based signatures," IACR Cryptology ePrint Archive, vol.2011, p.701, 2011. URL: http://eprint.iacr.org/2011/701.

[13] T. Okamoto and K. Takashima, "Fully secure unbounded inner-product and attribute-based encryption," IACR Cryptology ePrint Archive, vol.2012, p.671, 2012. URL: http://eprint.iacr.org/2012/671.

[14] A. Escala, G. Herold, E. Kiltz, C. Ràfols, and J.L. Villar, "An algebraic framework for diffie-hellman assumptions," Advances in Cryptology - CRYPTO 2013 - 33rd Annual Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2013. Proceedings, Part II, ed. R. Canetti and J.A. Garay, Lecture Notes in Computer Science, vol.8043, pp.129–147, Springer, 2013. doi:10.1007/978-3-642-40084-1_8.

[15] H. SHIZUYA and T. TAKAGI, "A Public-Key Cryptosystem Based upon Generalized Inverse Matrix over Discrete Logarithmic Domain of Finite Field," 電子情報通信学会論文誌 A, vol.J71-A, no.3, pp.825–832, 1988. URL: https://search.ieice.org/bin/summary.php?id=j71-a_3_825&category=A&year=1988&lang=J&abst=.

[16] J. Groth and A. Sahai, "Efficient noninteractive proof systems for bilinear groups," SIAM J. Comput., vol.41, no.5, pp.1193–1232, 2012. doi:10.1137/080725386.

[17] C. Schnorr, "Efficient signature generation by smart cards," J. Cryptology, vol.4, no.3, pp.161–174, 1991. doi:10.1007/BF00196725.

[18] D. Chaum and T.P. Pedersen, "Wallet databases with observers," Advances in Cryptology - CRYPTO '92, 12th Annual International Cryptology Conference, Santa Barbara, California, USA, August 16-20, 1992, Proceedings, ed. E.F. Brickell, Lecture Notes in Computer Science, vol.740, pp.89–105, Springer, 1992. doi:10.1007/3-540-48071-4_7.

[19] R. Cramer, I. Damgård, and B. Schoenmakers, "Proofs of partial knowledge and simplified design of witness hiding protocols," Advances in Cryptology - CRYPTO '94, 14th Annual International Cryptology Conference, Santa Barbara, California, USA, August 21-25, 1994, Proceedings, ed. Y. Desmedt, Lecture Notes in Computer Science, vol.839, pp.174–187, Springer, 1994. doi:10.1007/3-540-48658-5_19.

[20] A. Fiat and A. Shamir, "How to prove yourself: Practical solutions to identification and signature problems," Advances in Cryptology — CRYPTO '86, ed. A.M. Odlyzko, LNCS, vol.263, pp.186–199, Springer-Verlag, 1987.

[21] T.P. Pedersen, "A threshold cryptosystem without a trusted party (extended abstract)," Advances in Cryptology - EUROCRYPT '91, Workshop on the Theory and Application of of Cryptographic Techniques, Brighton, UK, April 8-11, 1991, Proceedings, ed. D.W. Davies, Lecture Notes in Computer Science, vol.547, pp.522–526, Springer, 1991. doi:10.1007/3-540-46416-6_47.

[22] J. Carter and M.N. Wegman, "Universal Classes of Hash Functions," Journal of Computer and System Sciences, vol.18, no.2, pp.143 – 154, 1979. doi:https://doi.org/10.1016/0022-0000(79)90044-8.

[23] D. Boneh and J. Katz, "Improved efficiency for cca-secure cryptosystems built using identity-based encryption," CT-RSA, ed. A. Menezes, Lecture Notes in Computer Science, vol.3376, pp.87–103, Springer, 2005.