**SCIS 2020** 2020 Symposium on
Cryptography and Information Security
Kochi, Japan, Jan. 28 – 31, 2020
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
# Asymmetric Pairing based on Symmetric Pairing

星野 文学 * 小林 鉄太郎 *
Fumitaka Hoshino Tetsutaro Kobayashi

**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. 本発表ではそのような暗号プリミティブの構成について解説し, 教科書的な各種の離散対数ベースの応用プロトコルに対して、本プリミティブの適用性を評価し, 様々な問題点を議論する.

**Keywords:** Diffie-Hellman 判定問題, trapdoor DDH 群, 双準同型, 非可換環

## 1 はじめに

2000 年頃までは DDH 仮定は成立しないが CDH 仮定を満足しそうな具体的な暗号プリミティブの候補は, あまり広く知られていなかった. しかし pairing の構成的応用が提案されると研究が一気に進み [1–4], より高度な機能を持つ暗号プリミティブである trapdoor DDH 群が研究されるようになった [5–8].

一般に trapdoor DDH 群とは, DDH 群 $\mathbb{G}$ であって, 指数的多数個の正当な DH タプル $(g, g^a, g^b, g^{ab}) \in \mathbb{G}^4$ についてランダムな DH タプル $(g, g^a, g^b, g^c) \in \mathbb{G}^4$ からの効率的識別が可能となる多項式長の trapdoor が離散対数 $a$ や $b$ 等から分離可能 (trapdoor を知っても CDH 問題は依然として困難) なもののことである.

trapdoor DDH 群の構成には, 一般の CDH 群に, かなり特殊な構造を入れる必要がある. 例えば CDH 群 $\mathbb{G}$ 上の元 $g$ に対して, $g, g^a, g^b$ を固定して DH タプルを効率的に識別するためには, $g^{ab}$ なる情報を知っていれば十分であるが, これは単一の正当な DH タプルについての trapdoor であるから, これを trapdoor DDH 群と呼ぶわけにはいかない. あるいは $g, g^a$ を固定して, 指数的多数個の $(g^b, g^{ab})$ を並べたテーブルは指数的多数個の正当な DH タプルについての trapdoor であるが, 多項式長の trapdoor ではないので, これを trapdoor DDH 群とする事は出来ない. また $g, g^a$ を固定すると $a$ は指数的多数個の正当な DH タプルについての trapdoor であるが, 離散対数 $a$ から分離できてない ($a$ を秘匿したまま trapdoor を与えることが出来ない) ので, やはり trapdoor DDH 群ではない.

2005 年に Hoshino-Suzuki-Kobayashi [5] は非対称ペアリングを用いて $g, g^a$ を固定して, DH タプルを効率的に識別できる trapdoor を離散対数から分離した. この $g, g^a$ を固定したタイプの trapdoor DDH 群は, 現在では Static trapdoor DDH 群と呼ばれる [7].

2006 年 Dent-Galbraith [6] は RSA modulus 上定義された超特異楕円曲線を用いて hidden pairing なる概念を導入し, これを用いて $g$ を固定して, DH タプルを効率的に識別できる trapdoor DDH 群を構成した. この $g$ を固定したタイプのものを (狭義の) trapdoor DDH 群と呼ぶ [7]. 本稿でも以降 trapdoor DDH 群と言ったら, この狭義のものを指すとする.

2013 年 Seurin は合成数剰余に基づく trapdoor DDH 群および, それぞれ RSA 問題および素因数分解問題に基づく 2 つの Static trapdoor DDH 群を構成し, trapdoor DDH 群の望ましい性質に関するいくつかの未解決問題を提案した [7].

2019 年 Kutas-Petit-Silva [8] は超特異楕円曲線のペアリングと同種写像を用いて Seurin の未解決問題を解決する trapdoor DDH 群の構成を示した.

2014 年 Hoshino は超特異楕円曲線のペアリングを用いて離散対数が非可換環となる trapdoor DDH 群の亜種を提案した [9]. この構成では, 離散対数が非可換環とな

* Secure Platform Laboratories, NTT Corporation, Japan

る不利益はあるものの, Seurin の未解決問題は解決される上に, pairing を open に使用できるという大きな利点があり, 高機能な暗号プロトコルへの応用が期待できる.

## 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

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

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
   $\mathrm{Exp}^{\mathcal{G},\mathcal{A}}(1^\lambda) :=$
   $(\mathbb{L}, \mathbb{G}, \mathsf{aux}) \overset{\$}{\leftarrow} \mathcal{G}(1^\lambda)$,
   $x \overset{\$}{\leftarrow} \mathbb{L}$, $g \overset{\$}{\leftarrow} \mathbb{G}$, $y \leftarrow g^x$,
   $x^* \overset{\$}{\leftarrow} \mathcal{A}(\mathbb{L}, \mathbb{G}, \mathsf{aux}, g, y)$,
   $\mathtt{Output}\ (y \overset{?}{=} g^{x^*})$.
   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 [10], 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
$\mathrm{Exp}^{\mathcal{G},\mathcal{A}}(1^\lambda) :=$
$(\mathbb{L}, \mathbb{G}, \mathsf{aux}) \overset{\$}{\leftarrow} \mathcal{G}(1^\lambda)$,
$g_0 \overset{\$}{\leftarrow} \mathbb{G}$,
$g_1 \leftarrow {}^a g_0 \mid a \overset{\$}{\leftarrow} \mathbb{L}$,
$g_2 \leftarrow g_0^b \mid b \overset{\$}{\leftarrow} \mathbb{L}$,
$g_3 \overset{\$}{\leftarrow} \mathcal{A}(\mathbb{L}, \mathbb{G}, \mathsf{aux}, g_0, g_1, g_2)$,
$\mathtt{Output}\ (g_3 \overset{?}{=} {}^a g_0^b)$.
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 $\mathcal{G}'^{\prime}_x(1^\lambda) :=$
   $(\mathbb{L}, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, \mathsf{aux}') \xleftarrow{\$} \mathcal{G}'(1^\lambda)$,
   $\mathsf{aux} \leftarrow (\mathbb{L}, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, \mathsf{aux}')$,
   $\mathtt{Output}(\mathbb{L}, \mathbb{G}_x, \mathsf{aux})$.
   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 [11].

> 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. $\mathbb{L}$ が非可換であるときの $\mathbb{G}_x$ の DDH 仮定の応用が本稿のテーマである.

### 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

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

- 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

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

### 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 [12]. 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 [13–20].

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 [21].

- $\langle \alpha \rangle$ 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

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

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

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

非退化双準同型 ${}^xY$ を

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

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 $t := \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ 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

[9] 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

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

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 [22]. $\mathbb{G}$ 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.

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

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 $\begin{pmatrix} g_0 & g_1 \\ g_2 & g_3 \end{pmatrix} \in \langle g\rangle^{2n\times 2n}$ (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 Diffie-Hellman 鍵交換 [23]

Diffie-Hellman 鍵交換は幾分対称性が失われるが, $\mathbb{L}$ が非可換でも問題なく実行できる.

- Alice が $a \in \mathbb{L}$ を生成し, ${}^a g$ を Bob に送信.
- Bob が $b \in \mathbb{L}$ を生成し, $g^b$ を Alice に送信.
- Alice は $K_a = {}^a(g^b)$ を計算.
- Bob は $K_b = ({}^a g)^b$ を計算.
- $K_a$ と $K_b$ は同じ値となる.

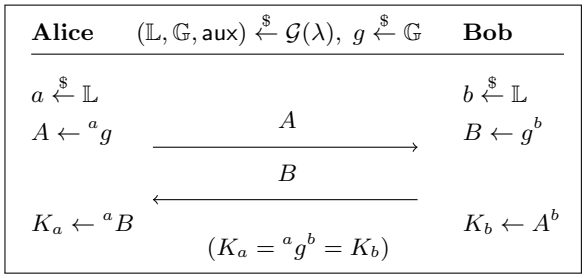


図 1 DH 鍵交換

ElGamal 暗号 [24], Cramer-Shoup 暗号 [25], Boneh-Franklin IBE [4] なども左右の冪乗を正しく配置する事により $\mathbb{L}$ が非可換でも問題なく実行できる. Joux の Tripartite Diffie-Hellman [1] の一般の元 $g \in \mathbb{G}$ に関する DBDH 仮定については, 対称ペアリングの時とは異なる型の仮定が必要となる. これは非対称ペアリングにおいて一般的に起こる.

### 3.2 Schnorr 認証 [?]

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 $\mathbb{L}$ が非可換でもほとんど問題なく実行できる. ゼロ知識性に関しては何の問題も無い. special soundness を証明する為には, ふたつのチャレンジ $c_1, c_2 \in \mathbb{L}$ が $c_1 - c_2 \in \mathbb{L}^*$ となる確率, 即ち式 (2) を評価する必要があるが, これも普通の素数位数巡回群の Schnorr 認証で $c_1$ と $c_2$ が一致してしまう確率とそう大差ない.

- 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.

### 3.3 Chaum-Pedersen [26]

Chaum-Pedersen のプロトコルは $A = g^x$ かつ $B = h^x$ なる $(g, h, A, B) \in \mathbb{G}^4$ が検証者に公開されているとき, $x$ を知る証明者が $x$ を教えることなく, それが正当な DH タプルである事を証明するプロトコルである. ベースとなる Schnorr 認証と同様に $\mathbb{L}$ が非可換でもこのプロトコルはほとんど問題なく実行できる. $\mathbb{G}$ が trapdoor DDH 群の時は, trapdoor を持つ者は, この証明を見なく

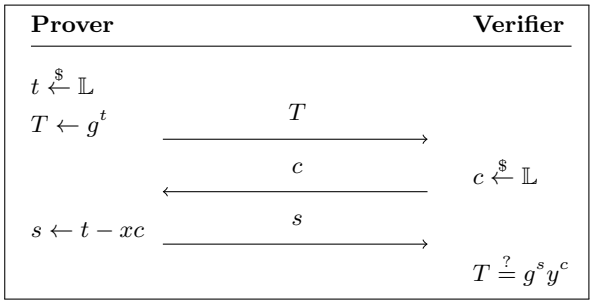


図 2　Schnorr 認証 ($PK\{(x) : y = g^x\}$)

とも $(g, h, A, B)$ が正当な DH タプルであるか否かを判定できる能力を持つ. trapdoor を持つ者は DH タプルを生成する事は出来ないが, 上記ような性質を用いて代理で DH タプルの正当性を証明できる.

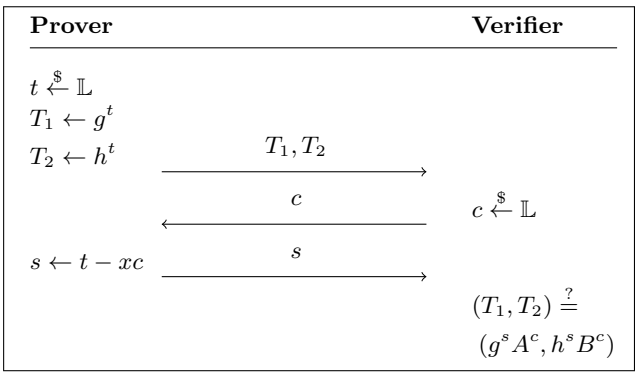


図 3　CP92 ($PK\{(x) : A = g^x \text{ and } B = h^x\}$)

### 3.4　Cramer-Damgård-Schoenmakers [27]

Cramer-Damgård-Schoenmakers のプロトコルは $A = g^x$ かつ $B = h^y$ なる $(g, h, A, B) \in \mathbb{G}^4$ が検証者に公開されているとき, $x$ または $y$ を知る証明者が $x$ あるいは $y$ を教えることなく, 少なくともどちらか一方を知っている事を証明する, honest な検証者に対する知識のゼロ知識証明で, リング署名などを構成するのに頻繁に利用される. やはりベースとなる Schnorr 認証と同様に $\mathbb{L}$ が非可換でもこのプロトコルもほとんど問題なく実行できる.

### 3.5　Pedersen commitment [28]

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. 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る.

- メッセージ $m$ をコミットする.

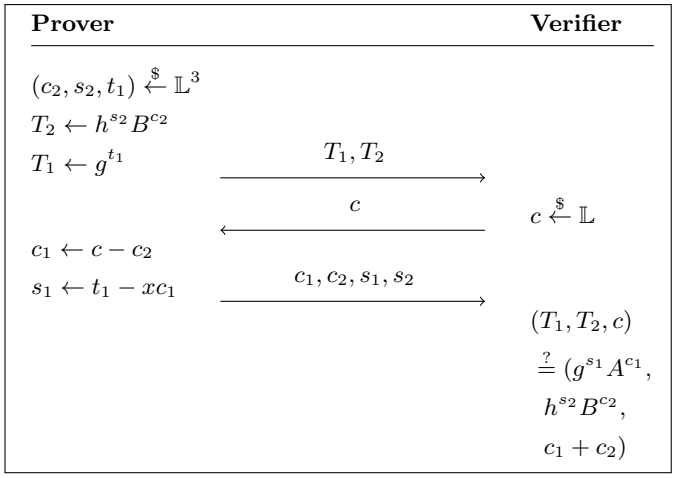


図 4　CDS94 ($PK\{(x, y) : A = g^x \text{ or } B = h^y\}$)

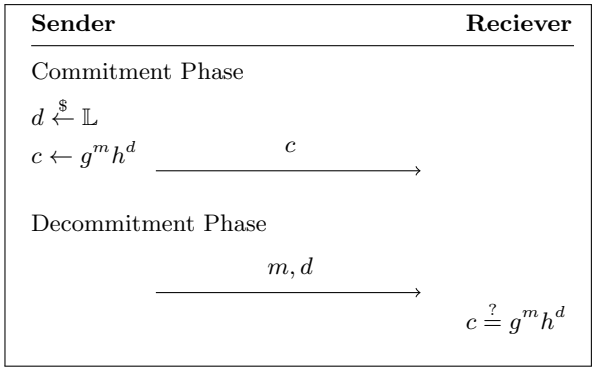


図 5　Pedersen Commitment

Pedersen commitment の hiding および binding property はそれぞれ Schnorr 認証のゼロ知識性および special soundness とほとんど一緒なので, $\mathbb{L}$ が非可換でも問題ない.

### 3.6　Boneh-Lynn-Shacham (BLS) 署名 [4]

2001 年 Boneh-Lynn-Shacham はペアリングのソース群における CDH 問題と DDH 問題とのギャップを上手く利用した署名方式を提案した [4]. 簡単のため以下では, まず対称ペアリング版の BLS 署名を説明する. 以下 $\lambda \in \mathbb{N}$ を安全パラメタとし $\mathcal{G}$ をペアリング (の生成アルゴリズム) とする. BLS 署名 $\Sigma$ は次の 3 つの確率的多項式時間アルゴリズム ($\mathtt{KeyGen}, \mathtt{Sign}, \mathtt{Verify}$) により構成される.

**鍵生成アルゴリズム** $\mathtt{KeyGen}(1^\lambda) \xrightarrow{\$} (\mathtt{sk}, \mathtt{pk})$ : は安全パラメタ $1^k$ を入力とし秘密鍵 $\mathtt{sk}$ および公開鍵 $\mathtt{pk}$ を出力とする, 次のアルゴリズムである.

$(\mathbb{L}, \mathbb{G}, \mathbb{G}_T, \mathsf{aux}) \xleftarrow{\$} \mathcal{G}(1^\lambda)$,
$g \xleftarrow{\$} \mathbb{G}$, $x \xleftarrow{\$} \mathbb{L}$, $y \leftarrow g^x$,

$\mathtt{sk} \leftarrow (\mathbb{L}, \mathbb{G}, \mathbb{G}_T, \mathsf{aux}, g, y, x)$,

$\mathtt{pk} \leftarrow (\mathbb{L}, \mathbb{G}, \mathbb{G}_T, \mathsf{aux}, g, y)$.

**署名アルゴリズム** $\mathtt{Sign}(\mathtt{sk}, m) \xrightarrow{\$} \sigma$ : は秘密鍵 sk およびメッセージ $m \in \mathbb{G}$ を入力とし署名 $\sigma \in \mathbb{G}$ を出力とする, 次のアルゴリズムである.

$(\mathbb{L}, \mathbb{G}, \mathbb{G}_T, \mathsf{aux}, g, y, x) \leftarrow \mathtt{sk}$,

$\sigma \leftarrow m^x$.

**検証アルゴリズム** $\mathtt{Verify}(\mathtt{pk}, m, \sigma) \xrightarrow{\$} 0/1$ : は公開鍵 pk, メッセージ $m \in \mathbb{G}$, および署名 $\sigma \in \mathbb{G}$, を入力とし, 単一ビット $b \in \{0,1\}$ を出力とする, 次のアルゴリズムである.

$(\mathbb{L}, \mathbb{G}, \mathbb{G}_T, \mathsf{aux}, g, y) \leftarrow \mathtt{pk}$,

$b \leftarrow (e(m, y) \stackrel{?}{=} e(g, \sigma))$.

上記の対称ペアリング版の BLS 署名においては正しく作られた署名 $(g, y, m, \sigma)$ は $(g, g^x, m, m^x)$ なる 正当な DH タプルとなっている.

[4] では署名長をコンパクトに保つため, (通常の) 非対称ペアリングを使用する事が推奨されている. この時, 署名方式が correctness を満たすには少なくとも以下の条件を満足しなくてはならない.

- KeyGen において $y$ は $g$ に群演算を施して導出されるので $g$ と $y$ は同じ ソース群に属する必要がある.
- Sign において $\sigma$ は $m$ に群演算を施して導出されるので $m$ と $\sigma$ は同じ ソース群に属する必要がある.
- Verify において $m$ と $y$ はペアリングの入力対となるため, 異なる ソース群に属する必要がある. 同様に $g$ と $\sigma$ も異なる ソース群に属する必要がある.

では, もし $g, y, m, \sigma$ が単一のソース群に属した場合には何が起こるだろうか ? この時正しく作られた署名は $(g, g^x, m, m^x)$ なる 正当な DH タプルとなっているので, 署名の正しさを検証する為には正当な DH タプルをランダムな DH タプルから識別できる必要がある. もしこのソース群が trapdoor DDH group なら $g$ に対応する trapdoor を持つ者だけがこの署名を検証できる事になる.

### 3.7 その他

Oblivious Transfer [29] は非可換の $\mathbb{L}$ で実行可能である. 通常の素数位数巡回群を用いた Feldman's VSS [30] では reconstruction phase において Lagrange 多項式を用いた復元アルゴリズムが用いられることが多いが, これは明らかに $\mathbb{L}$ の可換性に基づくので, $\mathbb{L}$ が非可換性の場合には別の方法を考える必要があり, 一般の非可換な $\mathbb{L}$ では Vandermonde 行列に関する非可換線形代数が必要になる. [9] の trapdoor DDH 群の場合は, この Vandermonde 行列を大きい $\mathbb{F}_q$ 行列と見なせば容易に解くことができる. また, share を指定するラベルを全て対角行列から選んで良いなら Lagrange 多項式を用いた方法がそのまま使用できる.

## 参考文献


[1] A. Joux, "A one round protocol for tripartite diffie-hellman," Algorithmic Number Theory, 4th International Symposium, ANTS-IV, Leiden, The Netherlands, July 2-7, 2000, Proceedings, ed. W. Bosma, Lecture Notes in Computer Science, vol.1838, pp.385–394, Springer, 2000. doi:10.1007/10722028_23.

[2] A. Joux and K. Nguyen, "Separating decision Diffie-Hellman from Diffie-Hellman in cryptographic groups." Cryptology ePrint Archive: 2001/003, 2001. URL: http://eprint.iacr.org/2001/003.

[3] T. Okamoto and D. Pointcheval, "The gap-problems: A new class of problems for the security of cryptographic schemes," Public Key Cryptography, 4th International Workshop on Practice and Theory in Public Key Cryptography, PKC 2001, Cheju Island, Korea, February 13-15, 2001, Proceedings, ed. K. Kim, Lecture Notes in Computer Science, vol.1992, pp.104–118, Springer, 2001. doi:10.1007/3-540-44586-2_8.

[4] D. Boneh and M.K. Franklin, "Identity-based encryption from the weil pairing," Advances in Cryptology - CRYPTO 2001, 21st Annual International Cryptology Conference, Santa Barbara, California, USA, August 19-23, 2001, Proceedings, ed. J. Kilian, Lecture Notes in Computer Science, vol.2139, pp.213–229, Springer, 2001. doi:10.1007/3-540-44647-8_13.

[5] F. Hoshino, K. Suzuki, and T. Kobayashi, "Revocable DDH by using Pairing and It's Application." In *Proc. of SCIS 2005 The 2005 Symposium on Cryptography and Information Security Maiko Kobe, Japan, Jan. 25-28, 2005, 3D4-3.* IEICE, 2005.

[6] A.W. Dent and S.D. Galbraith, "Hidden pairings and trapdoor DDH groups," Algorithmic Number Theory, 7th International Symposium, ANTS-VII, Berlin, Germany, July 23-28, 2006, Proceedings, ed. F. Hess, S. Pauli, and M.E. Pohst, Lecture Notes in Computer Science, vol.4076, pp.436–451, Springer, 2006. doi:10.1007/11792086_31.

[7] Y. Seurin, "New constructions and applications of trapdoor DDH groups," Public-Key Cryptography - PKC 2013 - 16th International Conference on Practice and Theory in Public-Key Cryptography, Nara, Japan, February 26 - March 1, 2013. Proceedings, ed. K. Kurosawa and G. Hanaoka, Lecture Notes in Computer Science, vol.7778, pp.443–460, Springer, 2013. doi:10.1007/978-3-642-36362-7_27.

[8] P. Kutas, C. Petit, and J. Silva, "Trapdoor DDH groups from pairings and isogenies," IACR Cryptology ePrint Archive, vol.2019, p.1290, 2019. URL: https://eprint.iacr.org/2019/1290.

[9] F. Hoshino, "A Variant of Diffie-Hellman Problem and How to Prove Independency." In *Proc. of SCIS 2014 2014 Sym-*

*posium on Cryptography and Information Security 2014*. IEICE, 2014.

[10] 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.

[11] 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.

[12] 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.

[13] 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.

[14] 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.

[15] 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.

[16] 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.

[17] 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.

[18] 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.

[19] 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.

[20] 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.

[21] 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=.

[22] 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.

[23] W. Diffie and M.E. Hellman, "New directions in cryptography," IEEE Transactions on Information Theory, vol.22, no.6, pp.644–654, 1976. URL: http://doi.ieeecomputersociety.org/10.1109/TIT.1976.1055638.

[24] T.E. Gamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," Advances in Cryptology, Proceedings of CRYPTO '84, Santa Barbara, California, USA, August 19-22, 1984, Proceedings, ed. G.R. Blakley and D. Chaum, Lecture Notes in Computer Science, vol.196, pp.10–18, Springer, 1984. doi:10.1007/3-540-39568-7_2.

[25] R. Cramer and V. Shoup, "A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack," Advances in Cryptology - CRYPTO '98, 18th Annual International Cryptology Conference, Santa Barbara, California, USA, August 23-27, 1998, Proceedings, ed. H. Krawczyk, Lecture Notes in Computer Science, vol.1462, pp.13–25, Springer, 1998. doi:10.1007/BFb0055717.

[26] 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.

[27] 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.

[28] 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.

[29] M. Bellare and S. Micali, "Non-interactive oblivious transfer and spplications," Advances in Cryptology - CRYPTO '89, 9th Annual International Cryptology Conference, Santa Barbara, California, USA, August 20-24, 1989, Proceedings, ed. G. Brassard, Lecture Notes in Computer Science, vol.435, pp.547–557, Springer, 1989. doi:10.1007/0-387-34805-0_48.

[30] P. Feldman, "A practical scheme for non-interactive verifiable secret sharing," 28th Annual Symposium on Foundations of Computer Science, Los Angeles, California, USA, 27-29 October 1987, pp.427–437, IEEE Computer Society, 1987. doi:10.1109/SFCS.1987.4.