SCIS 2014 The 31st Symposium on
Cryptography and Information Security
Kagoshima, Japan, Jan. 21 - 24, 2014
The Institute of Electronics,
Information and Communication Engineers

ある Diffie-Hellman 問題の変種と独立の証明法
A Variant of Diffie-Hellman Problem and How to Prove Independency

星野 文学*
Fumitaka Hoshino

あらまし 本論文では, 楕円曲線の暗号学的な模型およびある Diffie-Hellman 問題の変種を考察し, 対称ペアリング群を使用して, 非対称ペアリング群に似た暗号プリミティブの設計を行った. 対称ペアリング群上の DLIN 仮定の下で新しい暗号プリミティブは trapdoor DDH 群の性質と XDH 群のような性質を両方満たす.

キーワード DDH 問題, Trapdoor DDH 群, 双準同型

1 はじめに

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 $\mathbb{F}_q$ 上 1 次元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 $\mathbb{F}_q$ 上 2 次元ベクトル空間と見做すことができる. そして $a, b \in \mathbb{F}_q^*$ をランダムに選ぶと $g_1 := (g^a, g^b) \in \mathbb{G}'$ は高い確率で位数 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 $g_2 := (g^c, g^d) \in \mathbb{G}'$ 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 $\alpha, \beta \in \mathbb{F}_q$ を適当な定数として $e' : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ を

$$e' : (f_1, f_2), (h_1, h_2) \mapsto e(f_1, h_2)^\alpha e(h_1, f_2)^\beta$$

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 $(ad - bc \neq 0)$ 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_1, v_2) は $\mathbb{G}_1$ の元と $\mathbb{G}_2$ の元

$$\left((v_1^{\frac{d}{ad-bc}} v_2^{\frac{-c}{ad-bc}})^a, (v_1^{\frac{d}{ad-bc}} v_2^{\frac{-c}{ad-bc}})^b \right) \in \mathbb{G}_1,$$
$$\left((v_1^{\frac{-b}{ad-bc}} v_2^{\frac{a}{ad-bc}})^c, (v_1^{\frac{-b}{ad-bc}} v_2^{\frac{a}{ad-bc}})^d \right) \in \mathbb{G}_2$$

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 [40]. 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, 14, 20, 30–33, 15]. 本論文では, この方法論に習い, ある Diffie-Hellman 問題の変種を考察し, 対称ペアリング群を使用して非対称ペアリング群に似た暗号用原始関数の設計を行ない, 以下の結果を得た.

- Diffie-Hellman 問題における群模型の修正版を提案.
- 修正版の群模型の具体的な構成を与え, DLIN 仮定の下でこの構成が trapdoor DDH 群 [11, 35] の亜種となっている事を示した.
- 元々の群模型における trapdoor DDH 群の具体的構成を提案し, その安全性を上記亜種の安全性に帰着した.
- 上記 trapdoor DDH 群が XDH 群 [1] を抽象化した revocable DDH 群 [25] の性質を満たす事を示した.

2 準備

様々な暗号学的問題およびその問題が困難であるとする尤もらしい計算量的仮定が知られている [38]. そうした問題の最も有名なものの一つは離散対数問題 (discrete logarithm problem,DL 問題)[12] と呼ばれている. 離散対数問題とは群生成アルゴリズムと呼ばれる群の符号を生成する多項式時間アルゴリズム $\mathcal{G}$ に関する計算量的な問題の事である.

定義 1 (符号). 集合 S に対して $[S]$ を集合 S の記述 *(description)[11]* とする. 本論文では $[S]$ を S の符号 *(code)* と呼ぶことにする. また符号 $[S]$ によって $s \in S$

* NTT セキュアプラットフォーム研究所, 〒 180-8585 東京都武蔵野市緑町 3-9-11, NTT Secure Platform Laboratories, 3-9-11, Midori-cho Musashino-shi, Tokyo 180-8585 Japan

は $[\![s]\!]$ と記述されるとする. $[\![s]\!]$ を s の符号語 *(code word)* と呼ぶことにする.

符号を生成するアルゴリズムを議論するので, 本論文には $[S]$ や $[\![s]\!]$ と書くべき部分が大量に存在するが, 簡単のため特に必要の無い場合は省略して S や s と書く. 例えば, アルゴリズム $\mathcal{G}$ が符号 $[S]$ を出力する事を $\mathcal{G}$ は S を出力する等と表現する.

定義 2. A, B, C を準同型なアーベル群とする. A の自己準同型環を $\mathrm{End}(A)$, A から B への準同型全体を $\mathrm{Hom}(A, B)$, A および B から C への双準同型全体を $\mathrm{BiHom}(A, B, C)$ と書くとする.

2.1 DL 問題の群模型

定義 3 (群生成アルゴリズム $\mathcal{G}$). 群生成アルゴリズム

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

とは概ね次のような確率的多項式時間アルゴリズムの事である.

1. λ は安全変数. $\mathbb{G}$ は有限アーベル群. $\mathbb{L}$ は $\mathrm{End}(\mathbb{G})$ の部分環. G は $\mathbb{G}$ の部分集合. $\mathsf{aux} \in \{0,1\}^*$ は補助情報.
2. $|\mathbb{L}|, |\mathbb{G}| > 2^{\Theta(\lambda)}$.
3. $\mathbb{L}$ は和と積に関して確率的多項式時間アルゴリズムを持つ. 便宜上 $\mathbb{L}$ 上の和を加法表記し積を乗法表記する.
4. $\mathbb{G}$ は群演算に関して確率的多項式時間アルゴリズムを持つ. 便宜上 $\mathbb{G}$ 上の群演算を乗法表記する.
5. $g \in \mathbb{G}$ および $x \in \mathbb{L}$ を入力として $x(g) \in \mathbb{G}$ を出力する確率的多項式時間アルゴリズムが存在する. 便宜上 $x(g)$ を g^x と表記する.
6. $\mathsf{aux} \in \{0,1\}^*$ は便宜上追加される補助情報.

群生成アルゴリズム $\mathcal{G}$ を省略して群 $\mathcal{G}$ と呼ぶこととする. 従って群生成アルゴリズム $\mathcal{G}$ に関する DL 問題は群 $\mathcal{G}$ 上の DL 問題あるいは $\mathcal{G}$-DL 問題と呼ぶことにする. また $\mathbb{L}$ が自明なら $\mathcal{G}$ と $\mathbb{G}$ を同一視する.

$h \in \mathbb{G}$ に対して $g^x = h$ なる $x \in \mathbb{L}$ の事を g を底とする h の離散対数と呼ぶ. $\mathbb{G}$ が位数 n の巡回群なら $\mathbb{L}$ を $\mathbb{Z}/n\mathbb{Z}$ と考えて良い.

集合 G の取り方は解析すべき $\mathcal{G}$ によって異なる. G の元が 1 個しか無い事もあるし $\mathbb{G}$ の全体となる事もある.

$\mathbb{G}$ によっては $\mathbb{G}$ と準同型の標的群 $\mathbb{G}_T$ 及び非退化双線形写像 $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ の確率的多項式時間アルゴリズムが存在する事がある. 暗号プリミティブの応用がそのような情報を必要とする時は補助情報 aux にその情報が追記されるとする. そのような時, その群生成アルゴリズム $\mathcal{G}$ を対称ペアリング群 (symmetric pairing group) と呼ぶ.

簡単のため, 特に必要の無い場合は出力の $(\mathbb{G}, \mathbb{L}, G, \mathsf{aux})$ を param と省略して記す.

2.2 DL 問題の系譜

定義 4 ($\mathcal{G}$-DL 問題). 群生成アルゴリズム $\mathcal{G}$ に関する離散対数問題とは概ね次のような問題である.

sample:
$\quad \mathsf{param} \xleftarrow{\$} \mathcal{G}(1^\lambda)$,
$\quad g_0 \xleftarrow{\$} G$,
$\quad g_1 \leftarrow g_0^x \in \mathbb{G} \mid x \xleftarrow{\$} \mathbb{L}$.
given: param, g_0, g_1.
find: $y \in \mathbb{L} \mid g_0^y = g_1$.

群 $\mathcal{G}$ 上の離散対数仮定 (DL 仮定) とは群 $\mathcal{G}$ 上の離散対数問題が安全変数 λ に関して計算量的に困難であるとする仮定であり, 冪乗を $\mathbb{L}$ から $\mathbb{G}$ への準同型と見なすと, それが原像困難であるという仮定である. 離散対数仮定が尤もらしい群 $\mathcal{G}$ を DL 群と呼ぶ. 離散対数問題には膨大な量の変種が知られている [38, 7, 2]. 離散対数問題の変種で最も有名なものは Computational Diffie-Hellmann 問題 (CDH 問題) [12] と呼ばれている.

定義 5 ($\mathcal{G}$-CDH 問題). 群生成アルゴリズム $\mathcal{G}$ に関する *CDH* 問題とは概ね次のような問題である.

sample:
$\quad \mathsf{param} \xleftarrow{\$} \mathcal{G}(1^\lambda)$,
$\quad g_0 \xleftarrow{\$} G$,
$\quad g_1 \leftarrow g_0^x \in \mathbb{G} \mid x \xleftarrow{\$} \mathbb{L}$,
$\quad g_2 \leftarrow g_0^y \in \mathbb{G} \mid y \xleftarrow{\$} \mathbb{L}$.
given: $\mathsf{param}, g_0, g_1, g_2$.
find: g_0^{xy}.

群 $\mathcal{G}$ 上の CDH 仮定とは群 $\mathcal{G}$ 上の CDH 問題が安全変数 λ に関して計算量的に困難であるとする仮定であり, 概ね群 $\mathbb{G}$ を環 $\mathbb{L}$ と準同型な環と見なした時, 環 $\mathbb{G}$ 上の積が計算量的に困難であるとする仮定である. CDH 仮定が成立するなら離散対数仮定の成立も自明であるが, 逆は自明でない. CDH 仮定が尤もらしい群 $\mathcal{G}$ を CDH 群と呼ぶ. CDH 問題の最も有名な変種は decision Diffie-Hellmann 問題 (DDH 問題) [8, 3] である.

定義 6 ($\mathcal{G}$-DDH 問題). 群生成アルゴリズム $\mathcal{G}$ に関する *DDH* 問題とは概ね次のような問題である.

sample:
$\quad \mathsf{param} \xleftarrow{\$} \mathcal{G}(1^\lambda)$,
$\quad g_0 \xleftarrow{\$} G$,
$\quad g_1 \leftarrow g_0^x \in \mathbb{G} \mid x \xleftarrow{\$} \mathbb{L}$,

$g_2 \leftarrow g_0^y \in \mathbb{G} \mid y \xleftarrow{\$} \mathbb{L}$,
$g_3 \leftarrow g_0^z \in \mathbb{G} \mid z \xleftarrow{\$} \{w, xy\} | w \xleftarrow{\$} \mathbb{L}$.
given: $\mathsf{param}, g_0, g_1, g_2, g_3$.
guess: $xy \stackrel{?}{=} z$.

群 $\mathcal{G}$ 上の DDH 仮定とは群 $\mathcal{G}$ 上の DDH 問題が安全変数 λ に関して計算量的に困難であるとする仮定である. DDH 仮定は ElGamal 暗号 [21] の選択平文攻撃に対する識別不可能性と深い関係があり [37], 選択暗号文攻撃に対する安全性への改良も良く知られている [18, 10]. DDH 仮定が成立するなら CDH 仮定の成立は自明であるが, 逆は自明でない. DDH 仮定が尤もらしい群 $\mathcal{G}$ を DDH 群と呼ぶ. Decision Linear 問題 (DLIN 問題) [4] は比較的有名な DDH 問題の拡張で [38], 明確に定義されてから 10 年程の間に沢山応用された [4, 23, 31–33, 28].

定義 7 ($\mathcal{G}$-DLIN 問題). 群生成アルゴリズム $\mathcal{G}$ に関する *DLIN* 問題とは概ね次のような問題である.

sample:
$\mathsf{param} \xleftarrow{\$} \mathcal{G}(1^\lambda)$,
$(g_0, g_1, g_2) \xleftarrow{\$} G^3 | g_i \neq g_j$,
$(h_0, h_1, h_2) \leftarrow (g_0^{x_0}, g_1^{x_1}, g_2^{x_2})$
$|(x_0, x_1) \xleftarrow{\$} \mathbb{L}^2, x_2 \xleftarrow{\$} \{w, x_0 + x_1\} | w \xleftarrow{\$} \mathbb{L}$.
given: $\mathsf{param}, (g_0, h_0), (g_1, h_1), (g_2, h_2)$.
guess: $x_0 + x_1 \stackrel{?}{=} x_2$.

群 $\mathcal{G}$ 上の DLIN 仮定とは群 $\mathcal{G}$ 上の DLIN 問題が安全変数 λ に関して計算量的に困難であるとする仮定である. DLIN 仮定が成立する為には, g_0, g_1, g_2 間の関係が挑戦者にとって非自明である必要がある. DLIN 仮定が成立するなら CDH 仮定の成立は自明であるが, 逆は自明でない. また DDH 仮定が成立するなら DLIN 仮定の成立は自明であるが, 逆は自明でない. n-Decision Linear 問題 (DLIN$_n$ 問題) [24, 36] は DLIN 問題ほど有名では無いが, DLIN 問題の自然な拡張である.

定義 8 ($\mathcal{G}$-DLIN$_n$ 問題). 群生成アルゴリズム $\mathcal{G}$ に関する *DLIN$_n$* 問題とは概ね次のような問題である.

sample:
$\mathsf{param} \xleftarrow{\$} \mathcal{G}(1^\lambda)$,
$(g_0, \ldots, g_n) \xleftarrow{\$} G^{n+1} | g_i \neq g_j$,
$(h_0, \ldots, h_n) \leftarrow (g_0^{x_0}, \ldots, g_n^{x_n})$
$|(x_0, \ldots, x_{n-1}) \xleftarrow{\$} \mathbb{L}^n$,
$x_n \xleftarrow{\$} \{w, \sum_{i=0}^{n-1} x_i\} | w \xleftarrow{\$} \mathbb{F}_q$.
given: $\mathsf{param}, (g_0, h_0), \ldots, (g_n, h_n)$.
guess: $\sum_{i=0}^{n-1} x_i \stackrel{?}{=} x_n$.

群 $\mathcal{G}$ 上の DLIN$_n$ 仮定とは群 $\mathcal{G}$ 上の DLIN$_n$ 問題が安全変数 λ に関して計算量的に困難であるとする仮定である. DLIN$_n$ 仮定が成立する為には, $g_0, \cdots, g_n$ 間の関係が挑戦者にとって非自明である必要がある. DLIN$_n$ 仮定が成立するなら CDH 仮定の成立は自明であるが, 逆は自明でない. DLIN$_{n-1}$ 仮定が成立するなら DLIN$_n$ 仮定の成立は自明であるが, 逆は自明でない. DLIN$_n$ 仮定を用いると CDH 仮定と DDH 仮定の間に汎用的な帰着に基づく仮定の可算無限階層を構成出来る.

n-Decision Subspace 問題 (DSUBS$_n$ 問題) [30] はそれほど有名では無いが, 本論文においては重要な概念である. 似たような概念に Subgroup Decision 問題 [6, 17] があり, 広い意味では Subgroup Membership 問題 [39, 22] に含まれる. 本論文では線形代数の扱いを容易にする為 DSUBS$_n$ 問題を

- $\mathbb{G}$ 位数 q の素数位数巡回群
- $\mathbb{L}$ が $\mathbb{F}_q$ (体)

なる群生成アルゴリズム $\mathcal{G}$ に限り定義する. DSUBS$_n$ 問題を定義する前に幾つかの表記法を導入する.

定義 9 (離散対数行列). g を $\mathbb{G}$ の生成元とする. $n \times m$ $\mathbb{G}$ 行列の全体 $\mathbb{G}^{n \times m}$ は

$$\begin{pmatrix} g^{r_{11}} & \ldots & g^{r_{1m}} \\ \vdots & \ddots & \vdots \\ g^{r_{n1}} & \ldots & g^{r_{nm}} \end{pmatrix} \in \mathbb{G}^{n \times m} \mapsto \begin{pmatrix} r_{11} & \ldots & r_{1m} \\ \vdots & \ddots & \vdots \\ r_{n1} & \ldots & r_{nm} \end{pmatrix} \in \mathbb{F}_q^{n \times m}$$

なる写像で自明に $\mathbb{F}_q^{n \times m}$ と一対一対応する. $\mathbb{G}$ 行列 $G := (g^{r_{ij}})$ に対し $\mathbb{F}_q$ 行列 $r := (r_{ij})$ を g を底とする G の離散対数行列と呼び, G を g^r と記述する. ペアリングの標的群 $\mathbb{G}_T$ に関しても同様に $\mathbb{G}_T$ 行列 $G_T := (e(g,g)^{r_{ij}})$ に対して $\mathbb{F}_q$ 行列 $r := (r_{ij})$ を $e(g,g)$ を底とする G_T の離散対数行列と呼び, G_T を $e(g,g)^r$ と記述する.

定義 10 (正則). $n \times n$-$\mathbb{G}$ 行列のうち離散対数行列が正則なものを正則と定義し, 正則な $n \times n$-$\mathbb{G}$ 行列の集合を $GL(n, \mathbb{G})$ と記述する. $n \times n$-$\mathbb{G}$ 行列のうち離散対数行列が単位行列のものを I_n と定義し I_n を $\mathbb{G}$ 単位行列と呼ぶ.

定義 11 (左冪乗). $\mathbb{F}_q$ 行列 $x \in \mathbb{F}_q^{m \times \ell}$ および $\mathbb{G}$ 行列 $G = g^r \in \mathbb{G}^{\ell \times n}$ に対して ${}^xG \in \mathbb{G}^{m \times n}$ を

$${}^xG := g^{xr}$$

と定義する.

${}^xG$ は G の離散対数行列 $r \in \mathbb{F}_q^{\ell \times n}$ の値が分からなくても $x \in \mathbb{F}_q^{m \times \ell}$ の値 (x_{ij}) と $G \in \mathbb{G}^{\ell \times n}$ の値 (g_{jk}) だけから

$${}^xG = \left(\prod_j g_{jk}^{x_{ij}} \Big|_{\substack{i=1,\ldots,m \\ k=1,\ldots,n}} \right)$$

と多項式時間で計算することが出来る. 特に $\mathbb{F}_q$ 行列 $r = (r_{ij}) \in \mathbb{F}_q^{m\times n}$ に対して

$$g^r \equiv {}^rI_n$$

である.

定義 12 (右冪乗). $\mathbb{G}$ 行列 $G = g^r \in \mathbb{G}^{m\times\ell}$ および $\mathbb{F}_q$ 行列 $y \in \mathbb{F}_q^{\ell\times n}$ に対して $G^y \in \mathbb{G}^{m\times n}$ を

$$G^y := g^{ry}$$

と定義する.

G^y は G の離散対数行列 $r \in \mathbb{F}_q^{\ell\times n}$ の値が分からなくても $G \in \mathbb{G}^{m\times\ell}$ の値 (g_{ij}) と $y \in \mathbb{F}_q^{\ell\times n}$ の値 (y_{jk}) だけから

$$G^y = \left(\prod_j g_{ij}^{y_{jk}} \middle|_{\substack{i=1,\dots,m \\ k=1,\dots,n}} \right)$$

と多項式時間で計算することが出来る. 特に $\mathbb{F}_q$ 行列 $r = (r_{ij}) \in \mathbb{F}_q^{m\times n}$ に対して

$$g^r \equiv I_m^r$$

である.

定義 13 (ペアリング). $\mathbb{G}$ 上のペアリングを $e : \mathbb{G}\times\mathbb{G} \to \mathbb{G}_T$ とする. $\mathbb{G}$ 行列 $G = g^r \in \mathbb{G}^{m\times\ell}$ および $\mathbb{G}$ 行列 $H = g^s \in \mathbb{G}^{\ell\times n}$ に対して $e(G,H) \in \mathbb{G}_T^{m\times n}$ を

$$e(G,H) := e(g,g)^{rs}$$

と定義する.

$e(G,H)$ は G, H の離散対数行列 r, s の値が分からなくても $\mathbb{G}$ 上のペアリングの確率的多項式時間アルゴリズムが存在するなら, $G \in \mathbb{G}^{m\times\ell}$ の値 (g_{ij}) と $H \in \mathbb{G}^{\ell\times n}$ の値 (h_{jk}) だけから

$$e(G,H) = \left(\prod_j e(g_{ij}, h_{jk}) \middle|_{\substack{i=1,\dots,m \\ k=1,\dots,n}} \right)$$

と多項式時間で計算することが出来る.

定義 14 ($\mathcal{G}$-DSUBS$_n$ 問題). 幾分大雑把であるが群生成アルゴリズム $\mathcal{G}$ に関する *DSUBS$_n$* 問題とは要するに次のような問題である.

sample:
$\mathsf{param} \xleftarrow{\$} \mathcal{G}(1^\lambda)$,
$g \xleftarrow{\$} G$,
$h \leftarrow g^z \in \mathbb{G}^{n\times n} \mid z \xleftarrow{\$} \{x, y\}$
$\mid x \xleftarrow{\$} GL(n, \mathbb{F}_q)$,
$y \xleftarrow{\$} \mathbb{F}_q^{n\times n} \mid \mathrm{rank}(y) = n-1$.
given: param, h.
guess: $\det(z) \stackrel{?}{=} 0$.

群 $\mathcal{G}$ 上の DSUBS$_n$ 仮定とは群 $\mathcal{G}$ に関する DSUBS$_n$ 問題が安全変数 λ に関して計算量的に困難であるとする仮定である.

定義 15 (仮定の強弱). A, B をそれぞれ *DL* 群 $\mathcal{G}$ に関する命題 *(*仮定*)* とする. $A \Rightarrow B$ を $A \geq B$ または $B \leq A$ と書く. $A \Leftrightarrow B$ を $A = B$ と書く. $A \leq B \wedge \exists\mathcal{G}\neg B$ を $A \lneq B$ と書く.

命題 1. 汎用的な群 $\mathcal{G}$ に関する仮定の強弱について

- DSUBS$_2$ = DLIN$_1$ = DDH.
- DLIN$_2$ = DLIN.
- DLIN$_{n+1} \leq$ DLIN$_n$.
- DSUBS$_{n+1} \leq$ DSUBS$_n$.
- DSUBS$_{n+1} \leq$ DLIN$_n$*[30]*.

対称ペアリング群 $\mathcal{G}$ に関して

- CDH 仮定が成り立つなら CDH $\lneq$ DDH*[27]*.
- DLIN 仮定が成り立つなら DLIN $\lneq$ DDH*[4]*.

が知られている. まとめると図*.1* のようになる.

2.3 Trapdoor DDH 群とその系譜

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巡回群の候補は, 暗号学者の間であまり広く知られていなかった. しかし Gap 仮定や具体的な候補や応用が提案されると [26, 27, 29, 5] 研究が一気に進みより高度な機能を持つ暗号プリミティブが研究されるようになった. 指数的多数個の DDH 問題インスタンスを多項式時間で解くための落し戸を離散対数から分離できるような様々な DL 群が提案されるようになった [25, 11, 35].

定義 16 (Trapdoor DDH 群 [11, 35]). 概ね次の性質を持った群生成アルゴリズム $\mathcal{G}$ を *trapdoor DDH* 群 と呼ぶ *[11, 35]*.

(1) $\mathcal{G}$ は群生成アルゴリズムのうち補助情報に $\mathsf{aux} = (t, \mathsf{aux}')$ なる落とし戸 t を持つ.
(2) 群生成アルゴルズム $\mathcal{G}'$ を
$\mathcal{G}' : 1^\lambda \xmapsto{\$} (\mathbb{L}, \mathbb{G}, G, \mathsf{aux}')$
$\mid (\mathbb{L}, \mathbb{G}, G, (t, \mathsf{aux}')) \xleftarrow{\$} \mathcal{G}(1^\lambda)$.
と定義すると, $\mathcal{G}'$ が *DDH* 群である.
(3) $\mathcal{G}$ に関する *DDH instance* $(\mathsf{param}, g, g^x, g^y, g^z)$ を入力として $xy \stackrel{?}{=} z$ を出力する確率的多項式時間アルゴリズム $\mathsf{Solve_t}$ が存在する.
(4) $\mathcal{G}$ が *CDH* 群である.

$$
\begin{array}{ccccccccc}
\leftarrow \text{safer} & & & & & & \text{more dangerous} \rightarrow | & \quad | \leftarrow \text{ground zero} \\
& & \cdots \leq & \mathrm{DLIN}_n & \leq \cdots \leq & \mathrm{DLIN}_3 & \leq \mathrm{DLIN}_2 & \mathrm{DLIN}_1 \\
& & & & & & \| & \| \\
\mathrm{DL} \leq \mathrm{CDH} \ll \cdots & & & \vee| & \cdots & \vee| & \mathrm{DLIN} & \lneq \mathrm{DDH} \\
& & & & & & \vee| & \| \\
& & \cdots \leq \mathrm{DSUBS}_{n+1} & \leq \cdots \leq & \mathrm{DSUBS}_4 & \leq \mathrm{DSUBS}_3 & \mathrm{DSUBS}_2 &
\end{array}
$$

図 1. 仮定の強弱 (対称ペアリング群)

定義 17 (Static Trapdoor DDH 群 [35]). 概ね次の性質を持った群生成アルゴリズム $\mathcal{G}$ を *static trapdoor DDH* 群と呼ぶ *[35].*

(1) *trapdoor DDH* 群の *(1)* と同じ.
(2) *trapdoor DDH* 群の *(2)* と同じ.
(3) $\mathcal{G}$ の出力 param を入力として $x \xleftarrow{\$} \mathbb{L}$ および $g^x \in \mathbb{G}$ および静的落とし戸 *(static trapdoor)* t_x を出力する確率的多項式時間アルゴリズム Samp が存在する.
(4) $\mathcal{G}'$ の出力 param' および静的落とし戸 t_x および (g, g^x) が固定された *DDH instance* (g, g^x, g^y, g^z) を入力として $xy \stackrel{?}{=} z$ を出力する確率的多項式時間アルゴリズム $\mathsf{Solve}_{\mathsf{s}}$ が存在する.
(5) 如何なる確率的多項式時間アルゴリズムも *CDH instance* $((\mathsf{param}', t_x), g, g^x, g^y)$ を入力として g^{xy} を出力する確率は λ に関して無視可能.

定義 18 (Revocable DDH 群 [25]). 概ね次の性質を持った群生成アルゴリズム $\mathcal{G}$ を *revocable DDH* 群と呼ぶ *[25].*

(1) $\mathcal{G}$ が *DDH* 群である.
(2) *static trapdoor DDH* 群の *(3)* と同じ.
(3) *static trapdoor DDH* 群の *(4)* と同じ.
(4) *static trapdoor DDH* 群の *(5)* と同じ.

revocable DDH 群は XDH 群 [1] の抽象化である.

3 修正 Diffie-Hellman 模型

Diffie-Hellman 問題の適用領域を広げるため前の節で定義した群生成アルゴリズム $\mathcal{G}$ の仕様を少し修正する.

定義 19 (修正群生成アルゴリズム $\mathcal{E}$). 修正群生成アルゴリズム

$$\mathcal{E} : 1^\lambda \stackrel{\$}{\mapsto} (\mathbb{G}, \mathbb{L}_1, \mathbb{L}_2, \mathbb{L}_3, B, \mathsf{aux})$$

とは概ね次のような確率的多項式時間アルゴリズムの事である.

1. λ は安全変数. $\mathbb{G}, \mathbb{L}_1, \mathbb{L}_2, \mathbb{L}_3$ は *4* つの準同型な有限アーベル群. $B \subseteq \mathrm{BiHom}(\mathbb{L}_1, \mathbb{L}_2, \mathbb{G})$ は双準同型の適当な集合 . $\mathsf{aux} \in \{0,1\}^*$ は補助情報.
2. $|\mathbb{L}_i|, |\mathbb{G}| > 2^{\Theta(\lambda)}$.
3. $\mathbb{L}_i, \mathbb{G}$ は群演算に関して確率的多項式時間アルゴリズムを持つ. 便宜上 $\mathbb{L}_i$ 上の群演算を加法表記し, $\mathbb{G}$ 上の群演算を乗法表記する. また $\mathrm{BiHom}(\mathbb{L}_1, \mathbb{L}_2, \mathbb{L}_3)$, $\mathrm{BiHom}(\mathbb{L}_1, \mathbb{L}_2, \mathbb{G})$, $\mathrm{Hom}(\mathbb{L}_1, \mathbb{G})$, $\mathrm{Hom}(\mathbb{L}_2, \mathbb{G})$, が符号を持つ.
4. $r \in \mathrm{BiHom}(\mathbb{L}_1, \mathbb{L}_2, \mathbb{L}_3)$ および $x \in \mathbb{L}_1$ および $y \in \mathbb{L}_2$ に対して, $r(x, y) \in \mathbb{L}_3$ を計算する確率的多項式時間アルゴリズムが存在する. 便宜上 $x \circ y$ を $x \circ y := r(x, y)$ と定義し, 積と呼ぶ.
5. $\mathrm{BiHom}(\mathbb{L}_1, \mathbb{L}_2, \mathbb{L}_3)$ から $\mathrm{BiHom}(\mathbb{L}_1, \mathbb{L}_2, \mathbb{G})$ への非退化準同型写像 g が存在し, g は確率的多項式時間アルゴリズムを持つ. 便宜上 $r \in \mathrm{BiHom}(\mathbb{L}_1, \mathbb{L}_2, \mathbb{L}_3)$ に対して g^r を $g^r := g(r)$ と定義する.
6. $g_0 \in \mathrm{BiHom}(\mathbb{L}_1, \mathbb{L}_2, \mathbb{G})$ および $x \in \mathbb{L}_1$ および $y \in \mathbb{L}_2$ に対して, $g_0(x, \cdot) \in \mathrm{Hom}(\mathbb{L}_2, \mathbb{G})$ および $g_0(\cdot, y) \in \mathrm{Hom}(\mathbb{L}_1, \mathbb{G})$ を計算する確率的多項式時間アルゴリズムが存在する. 便宜上 ${}^x g_0$ を ${}^x g_0 := g_0(x, \cdot)$, 便宜上 g_0^y を $g_0^y := g_0(\cdot, y)$ と定義する.
7. ${}^x g_0 \in \mathrm{Hom}(\mathbb{L}_2, \mathbb{G})$ および $g_0^y \in \mathrm{Hom}(\mathbb{L}_1, \mathbb{G})$ および $x' \in \mathbb{L}_1$ および $y' \in \mathbb{L}_2$ に対して, ${}^x g_0(y') \in \mathbb{G}$ および $g_0^y(x') \in \mathbb{G}$ を計算する確率的多項式時間アルゴリズムが存在する. 便宜上 ${}^x g_0^y$ を ${}^x g_0^y := {}^x g_0(y)$ と定義する. 定義より ${}^x g_0^y = g_0^y(x) = g_0(x, y)$ である.
8. $\mathbb{L}_3$ から $\mathbb{G}$ への非退化準同型写像 h が存在し, ${}^x(g^r)^y = h(x \circ y)$ が成り立つ. さらに h は確率的多項式時間アルゴリズムを持つ. 便宜上 $z \in \mathbb{L}_3$ に対して g^z を $g^z := h(z)$ と定義する.
9. $\mathsf{aux} \in \{0,1\}^*$ は便宜上追加される補助情報.

修正群生成アルゴリズムの事を省略して修正群と呼ぶことにする. 修正群 $\mathcal{E}$ 上の修正 DDH 問題 (mDDH 問題) および修正 CDH 問題 (mCDH 問題) は概ね次のような問題となる.

定義 20 ($\mathcal{E}$-mDDH 問題).

sample:
$\mathsf{param} \xleftarrow{\$} \mathcal{E}(1^\lambda)$,
$g_0 \xleftarrow{\$} B \subseteq \mathrm{BiHom}(\mathbb{L}_1, \mathbb{L}_2, \mathbb{G})$,
$g_1 \leftarrow {}^x g_0 \in \mathrm{Hom}(\mathbb{L}_2, \mathbb{G}) | x \xleftarrow{\$} \mathbb{L}_1$,
$g_2 \leftarrow g_0^y \in \mathrm{Hom}(\mathbb{L}_1, \mathbb{G}) | y \xleftarrow{\$} \mathbb{L}_2$,

$g_3 \leftarrow h \in \mathbb{G} | h \xleftarrow{\$} \{f, {}^x g_0^y\} | f \xleftarrow{\$} \mathbb{G}$.
given: $\mathsf{param}, g_0, g_1, g_2, g_3$.
guess: $g_3 \stackrel{?}{=} {}^x g_0^y$.

定義 21 ($\mathcal{E}$-mCDH 問題).

sample: same as mDDH.
given: $\mathsf{param}, g_0, g_1, g_2$.
find: ${}^x g_0^y \in \mathbb{G}$.

4 修正群上の具体的構成

$\mathcal{G}$ を対称ペアリング群とする. 下記の修正群生成アルゴリズム $\mathcal{E}_n^{\mathcal{G}}, \mathcal{E}_n'^{\mathcal{G}}$ を考える.

$$
\begin{aligned}
\mathcal{E}_n^{\mathcal{G}} : 1^\lambda \mapsto\ & (\mathbb{G}, \mathbb{F}_q^{1\times n}, \mathbb{F}_q^{n\times 1}, \mathbb{F}_q^{1\times 1}, B, \mathsf{aux}) \\
& | (\mathbb{G}, \mathbb{F}_q, \{g\}, \mathsf{aux}') \xleftarrow{\$} \mathcal{G}(1^\lambda), \\
& B \leftarrow \{g^r\} | r \xleftarrow{\$} GL(n, \mathbb{F}_q), \\
& \mathsf{aux} \leftarrow (r, \mathsf{aux}'). \\
\mathcal{E}_n'^{\mathcal{G}} : 1^\lambda \mapsto\ & (\mathbb{G}, \mathbb{F}_q^{1\times n}, \mathbb{F}_q^{n\times 1}, \mathbb{F}_q^{1\times 1}, B, \mathsf{aux}') \\
& | \text{ same as } \mathcal{E}^{\mathcal{G}}.
\end{aligned}
$$

定義に従い上記の $\mathcal{E}_n'^{\mathcal{G}}$-mDDH 問題を書き下すと, 概ね下記のようになる.

Case 1 ($\mathcal{E}_n'^{\mathcal{G}}$-mDDH 問題).

sample:
$\mathsf{param} \xleftarrow{\$} \mathcal{E}_n'^{\mathcal{G}}(1^\lambda)$,
$g_0 \leftarrow g^r \in GL(n, \mathbb{G})$,
$g_1 \leftarrow {}^x g_0 \in \mathbb{G}^{1\times n} \ | x \xleftarrow{\$} \mathbb{F}_q^{1\times n}$,
$g_2 \leftarrow g_0^y \in \mathbb{G}^{n\times 1} \ | y \xleftarrow{\$} \mathbb{F}_q^{n\times 1}$,
$g_3 \leftarrow h \in \mathbb{G} \ | h \xleftarrow{\$} \{f, {}^x g_0^y\} | f \xleftarrow{\$} \mathbb{G}$.
given: $\mathsf{param}, g_0, g_1, g_2, g_3$.
guess: $g_3 \stackrel{?}{=} {}^x g_0^y$.

一方, 様々な文献で下記の問題と本質的に同じ概念が提案されている.[30, 15]

定義 22 ($\mathcal{G}$-gDDH$_n$ 問題).

sample:
$\mathsf{param} \xleftarrow{\$} \mathcal{G}(1^\lambda)$,
$g_0 \leftarrow g^r \in \mathbb{G}^{n\times n} \ | r \xleftarrow{\$} GL(n, \mathbb{F}_q)$
$g_1 \leftarrow {}^x g_0 \in \mathbb{G}^{1\times n} | x \xleftarrow{\$} \mathbb{F}_q^{1\times n}$,
$g_2 \leftarrow g_0^y \in \mathbb{G}^{n\times 1} \ | y \xleftarrow{\$} \mathbb{F}_q^{n\times 1}$,
$g_3 \leftarrow g^z \in \mathbb{G}^{1\times 1} \ | z \xleftarrow{\$} \{w, x \circ y\}$
$| w \xleftarrow{\$} \mathbb{F}_q^{1\times 1}, x \circ y := xry$.
given: $\mathsf{param}, g_0, g_1, g_2, g_3$.
guess: $x \circ y \stackrel{?}{=} z$.

補題 1. $\mathcal{E}_n'^{\mathcal{G}}$-mDDH $= \mathcal{G}$-gDDH$_n$.

証明概要. 定義より自明. □

補題 2. $\mathcal{G}$-gDDH$_n$ = DSUBS$_{n+1}$*[30].*

証明概要. DSUBS$_{n+1}$ のインスタンス

$$
\left(\begin{array}{ccc|c} a_{11} & \cdots & a_{1n} & c_{11} \\ \vdots & \ddots & \vdots & \vdots \\ a_{n1} & \cdots & a_{nn} & c_{n1} \\ \hline b_{11} & \cdots & b_{1n} & d_{11} \end{array}\right),
$$

と gDDH$_n$ のインスタンス

$$
g_0 = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix}, g_2 = \begin{pmatrix} c_{11} \\ \vdots \\ c_{n1} \end{pmatrix},
$$
$$
g_1 = \begin{pmatrix} b_{11} & \cdots & b_{1n} \end{pmatrix}, \quad g_3 = (d_{11}).
$$

は互いのランダム自己帰着に双方向多項式時間帰着可能. □

補題 3. $n \geq 2$ のとき gDDH$_n \leq$ DLIN.

証明概要. $n \geq 2$ のとき
gDDH$_n$ = DSUBS$_{n+1} \leq$ DLIN$_n \leq$ DLIN. □

補題 4. 群 $\mathcal{G}$ 上で *DLIN* 仮定が成立するなら $n \geq 2$ のとき修正群 $\mathcal{E}_n'^{\mathcal{G}}$ は *mDDH* 群.

証明概要. $n \geq 2$ のとき
$\mathcal{E}_n'^{\mathcal{G}}$-mDDH $= \mathcal{G}$-gDDH$_n \leq \mathcal{G}$-DLIN. □

補題 5. 修正群 $\mathcal{E}_n^{\mathcal{G}}$ 上の *mDDH* 問題は多項式時間で解ける.

証明概要. $r \in GL(n, \mathbb{F}_q)$ から r^{-1} は多項式時間で計算可能. 問題のインスタンス $(\mathsf{param}, g_0, g_1, g_2, g_3)$ に対して r^{-1} を知っているなら $e(g_1^{r^{-1}}, g_2) \stackrel{?}{=} e(g, g_3)$ を出力すれば良い. □

Case 2 ($\mathcal{E}_n^{\mathcal{G}}$-mCDH 問題).

sample: $\mathcal{E}_n'^{\mathcal{G}}$-mDDH 問題の $\mathcal{E}_n'^{\mathcal{G}}$ を $\mathcal{E}_n^{\mathcal{G}}$ に変更.
given: $\mathsf{param}, g_0, g_1, g_2$.
find: $g^{x\circ y} \in \mathbb{G}^{1\times 1} | x \circ y := xry$.

補題 6. $\mathcal{E}_n^{\mathcal{G}}$-mCDH $= \mathcal{G}$-CDH*[40].*

証明概要. $\mathcal{G}$-CDH $\leq \mathcal{E}_n^{\mathcal{G}}$-mCDH は自明. 逆は $\mathcal{G}$-CDH のインスタンス g_0, g_1, g_2 を $g = g_0$ として $\mathcal{E}_n^{\mathcal{G}}$-mCDH のインスタンス

$$
g_0' = \begin{pmatrix} g^{r_{11}} & \cdots & g^{r_{1n}} \\ \vdots & \ddots & \vdots \\ g^{r_{n1}} & \cdots & g^{r_{nn}} \end{pmatrix}, \quad g_2' = \begin{pmatrix} g_2 \\ g^{y_{21}} \\ \vdots \\ g^{y_{n1}} \end{pmatrix},
$$
$$
g_1' = \begin{pmatrix} g_1 & g^{x_{12}} & \cdots & g^{x_{1n}} \end{pmatrix}, r = (r_{ij}).
$$

のランダム自己帰着へ帰着. 出力から余分な成分を (r_{ij}), (x_{1i}), (y_{j1}), g_0, g_1, g_2 を使って取り除く. □

定理 1. $n \geq 2$ の時群 $\mathcal{G}$ 上の DLIN 仮定の下で修正群 $\mathcal{E}_n^{\mathcal{G}}$ は *trapdoor mDDH* 群.

証明概要. 補題.4,5,6, CDH≤DLIN より. □

備考 *1.* 修正群 $\mathcal{E}_n^{\mathcal{G}}$ の落し戸は群 $\mathcal{G}$ 上の DLIN 仮定を潰す訳では無いので,$\mathcal{G}$ 上の DLIN と CDH のギャップは気にする必要が無い.

5 群上の具体的構成

前の節で trapdoor DDH 群のような修正群生成アルゴリズムが構成出来た. しかし群でもなければ群生成アルゴリズムでもない修正群を堂々と trapdoor DDH 群と言うのは些か口はばかられる. この節では同じ方法論を用いて trapdoor DDH 群の群生成アルゴリズム $\mathcal{F}_n^{\mathcal{G}}$ を構成する.

$$\begin{aligned}\mathcal{F}_n^{\mathcal{G}} : 1^\lambda \mapsto\ & (GL(n,\mathbb{G}), GL(n,\mathbb{F}_q), G, \mathsf{aux}) \\ & |(\mathbb{G}, \mathbb{F}_q, \{g\}, \mathsf{aux}') \xleftarrow{\$} \mathcal{G}(1^\lambda), \\ & G \leftarrow \{g^r\} | r \xleftarrow{\$} GL(n,\mathbb{F}_q), \\ & \mathsf{aux} \leftarrow (r, \mathsf{aux}'). \\ \mathcal{F}_n'^{\mathcal{G}} : 1^\lambda \mapsto & (GL(n,\mathbb{G}), GL(n,\mathbb{F}_q), G, \mathsf{aux}') \\ & | \text{ same as } \mathcal{F}_n^{\mathcal{G}}.\end{aligned}$$

$\mathcal{F}_n^{\mathcal{G}}, \mathcal{F}_n'^{\mathcal{G}}$ は $\mathbb{L}_1 = \mathbb{L}_2 = \mathbb{L}_3 = GL(n,\mathbb{F}_q)$, $B = G$ と見なせば修正群用の mDDH 問題を適用することも出来るが, 使用する End($\mathbb{G}$) の部分環が非可換である事を認めるなら, 通常の DDH 問題を問題なく適用することが出来, 両者の外見は概ね一致する. 定義に従い $\mathcal{F}_n'^{\mathcal{G}}$-DDH 問題を書き下すと, 下記のようになる.

Case 3 ($\mathcal{F}_n'^{\mathcal{G}}$-DDH 問題).

sample:
$\mathsf{param} \xleftarrow{\$} \mathcal{F}_n'^{\mathcal{G}}(1^\lambda)$,
$g_0 \leftarrow g^r \in GL(n,\mathbb{G})$,
$g_1 \leftarrow {}^x g_0 \in \mathbb{G}^{n\times n}$ $|x \xleftarrow{\$} GL(n,\mathbb{F}_q)$,
$g_2 \leftarrow g_0^y \in \mathbb{G}^{n\times n}$ $|y \xleftarrow{\$} GL(n,\mathbb{F}_q)$,
$g_3 \leftarrow h \in \mathbb{G}^{n\times n}$ $|h \xleftarrow{\$} \{f, {}^x g_0^y\} | f \xleftarrow{\$} GL(n,\mathbb{F}_q)$.
given: $\mathsf{param}, g_0, g_1, g_2, g_3$.
guess: $g_3 \stackrel{?}{=} {}^x g_0^y$.

補題 7. $\mathcal{F}_n'^{\mathcal{G}}$-DDH = $\mathcal{E}_n'^{\mathcal{G}}$-mDDH.

証明概要. $\mathcal{E}_n'^{\mathcal{G}}$-mDDH ≤ $\mathcal{F}_n'^{\mathcal{G}}$-DDH は n^2 回 $\mathcal{E}_n'^{\mathcal{G}}$-mDDH コールを行う. 逆は $\mathcal{E}_n'^{\mathcal{G}}$-mDDH のインスタンスを水増しして $\mathcal{F}_n'^{\mathcal{G}}$-DDH インスタンスを作る. □

補題 8. 群 $\mathcal{G}$ 上で *DLIN* 仮定が成立するなら $n \geq 2$ のとき群 $\mathcal{F}_n'^{\mathcal{G}}$ は *DDH* 群.

証明概要. 補題.4,7 より. □

補題 9. 群 $\mathcal{F}_n^{\mathcal{G}}$ 上の *DDH* 問題は多項式時間で解ける.

証明概要. 補題.5 と同様に DDH 問題インスタンス (param, g_0, g_1, g_2, g_3) に対して $e(g_1^{r^{-1}}, g_2) \stackrel{?}{=} e(I_n, g_3)$ を出力すれば良い. □

補題 10. $\mathcal{F}_n^{\mathcal{G}}$-CDH = $\mathcal{G}$-CDH.

証明概要. 補題.6 と全く同様.

定理 2. 群 $\mathcal{G}$ 上で DLIN 仮定が成立するなら $n \geq 2$ のとき群 $\mathcal{F}_n^{\mathcal{G}}$ は *trapdoor DDH* 群.

証明概要. 補題.8,9,10, CDH≤DLIN より. □

補題 11. 群 $\mathcal{G}$ 上で DLIN 仮定が成立するなら $n \geq 2$ のとき群 $\mathcal{F}_n'^{\mathcal{G}}$ は *revocable DDH* 群.

証明概要. 補題.8 より群 $\mathcal{F}_n'^{\mathcal{G}}$ は DDH 群.

$$\begin{aligned}&\mathsf{Samp} : (GL(n,\mathbb{G}), GL(n,\mathbb{F}_q), \{g_0\}, \mathsf{aux}') \xmapsto{\$} (x, g_1, t_x) | \\ &\quad x \xleftarrow{\$} GL(n,\mathbb{F}_q), \\ &\quad g_1 \leftarrow {}^x g_0 \in GL(n,\mathbb{G}), \\ &\quad t_x \leftarrow g_0^x \in GL(n,\mathbb{G}). \\ &\mathsf{Solve_s} : (g_0, g_1, g_2, g_3, t_x) \xmapsto{\$} b | \\ &\quad \text{if } e(t_x, g_0) \neq e(g_0, g_1) \text{ abort}, \\ &\quad \text{if } e(t_x, g_2) \neq e(g_0, g_3)\ b \leftarrow 0, \text{ otherwize } b \leftarrow 1.\end{aligned}$$

CDH instance $((\mathsf{param}', g_0^x), g_0, {}^x g_0, g_0^y)$ から ${}^x g_0^y$ が作れるなら補題.6 等と同様に $\mathcal{G}$-CDH インスタンスを埋め込んで $\mathcal{G}$-CDH を解くことができる. □

備考 *2.* 非可換性は本質. 行列 x, r, y に何らかの制限を加えて, g^{rx} あるいは g^{yr} が推測可能になると $\mathcal{F}_n'^{\mathcal{G}}$-DDH はすぐ破れる. 例えば行列 x, r, y 等を $GL(n,\mathbb{F}_q)$ の可換な部分群に制限すると $\mathcal{F}_n'^{\mathcal{G}}$-DDH はすぐ破れる. 特に $\mathcal{F}_1'^{\mathcal{G}}$-DDH = $\mathcal{G}$-DDH は元々破れている.

6 独立の証明法

DSUBS$_n$ ≤ DLIN である事から, 与えられた $y \in \mathbb{G}^{n\times n}$ が $y \in GL(n,\mathbb{G})$ か否かを判定することは一般には難しい. $y \in GL(n,\mathbb{G})$ を標本抽出する際にこれを証明する方法が必要となる事もあろう. DL ベースの汎用証明系 [9, 23] を使えば良いが, ここでは教科書的な知識証明 [34] を紹介する.

定義 23 (Schnorr). P を証明者 V を検証者とする.

共通参照文字列 : $g \in GL(n,\mathbb{G}), y \in \mathbb{G}^{n\times n}$.
証明したいこと : $PK\{(x \in \mathbb{F}_q^{n\times n}) : g = y^x\}$.
Step.1 $(V \leftarrow P)$: $R \leftarrow y^r | r \xleftarrow{\$} \mathbb{F}_q^{n\times n}$.
Step.2 $(V \rightarrow P)$: $c \xleftarrow{\$} GL(n,\mathbb{F}_q)$.
Step.3 $(V \leftarrow P)$: $z \leftarrow r - xc$.
検証 : $R \stackrel{?}{=} y^z g^c$.

備考 *3.* 完全性, 健全性, 零知識性は [34] とほぼ同様. 離散対数が非可換環なので z を作るときの乗算の向きは重要. 最初に $g \in GL(n, \mathbb{G})$ なる g を知っている必要があるが, 初めて実行する場合は I_n を使えば良い. 非対話化も可能 [16]. $PK\{(x) : g = {}^x y\}$ の知識証明も向きに注意すれば同様に可能.

参考文献

1. L. Ballard, M. Green, B. de Medeiros, and F. Monrose. Correlation-resistant storage via keyword-searchable encryption. *IACR Cryptology ePrint Archive*, 2005:417, 2005.
2. F. Bao, R. H. Deng, and H. Zhu. Variations of diffie-hellman problem. In S. Qing, D. Gollmann, and J. Zhou, editors, *ICICS*, volume 2836 of *Lecture Notes in Computer Science*, pages 301–312. Springer, 2003.
3. D. Boneh. The decision diffie-hellman problem. In J. Buhler, editor, *ANTS*, volume 1423 of *Lecture Notes in Computer Science*, pages 48–63. Springer, 1998.
4. D. Boneh, X. Boyen, and H. Shacham. Short group signatures. In M. K. Franklin, editor, *CRYPTO*, volume 3152 of *Lecture Notes in Computer Science*, pages 41–55. Springer, 2004.
5. D. Boneh and M. K. Franklin. Identity-based encryption from the weil pairing. In J. Kilian, editor, *CRYPTO*, volume 2139 of *Lecture Notes in Computer Science*, pages 213–229. Springer, 2001.
6. D. Boneh, E.-J. Goh, and K. Nissim. Evaluating 2-dnf formulas on ciphertexts. In J. Kilian, editor, *TCC*, volume 3378 of *Lecture Notes in Computer Science*, pages 325–341. Springer, 2005.
7. X. Boyen. The uber-assumption family. In Galbraith and Paterson [19], pages 39–56.
8. S. Brands. An efficient off-line electronic cash system based on the representation problem. Technical report, CWI, Centrum Wiskunde & Informatica, Amsterdam, Netherlands, 1993.
9. J. Camenisch and M. Stadler. Proof Systems for General Statements about Discrete Logarithms. Technical Report No. 260, March 1997, Dept. of Computer Science, ETH Zurich, 1997.
10. R. Cramer and V. Shoup. A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack. In H. Krawczyk, editor, *CRYPTO*, volume 1462 of *Lecture Notes in Computer Science*, pages 13–25. Springer, 1998.
11. A. W. Dent and S. D. Galbraith. Hidden pairings and trapdoor ddh groups. In F. Hess, S. Pauli, and M. E. Pohst, editors, *ANTS*, volume 4076 of *Lecture Notes in Computer Science*, pages 436–451. Springer, 2006.
12. W. Diffie and M. E. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6):644–654, 1976.
13. I. M. Duursma and N. Kiyavash. The vector decomposition problem for elliptic and hyperelliptic curves. *IACR Cryptology ePrint Archive*, 2005:31, 2005.
14. I. M. Duursma and S. Park. Elgamal type signature schemes for n-dimensional vector spaces. *IACR Cryptology ePrint Archive*, 2006:312, 2006.
15. A. Escala, G. Herold, E. Kiltz, C. Ràfols, and J. Villar. An algebraic framework for diffie-hellman assumptions. In R. Canetti and J. A. Garay, editors, *CRYPTO (2)*, volume 8043 of *Lecture Notes in Computer Science*, pages 129–147. Springer, 2013.
16. U. Feige, A. Fiat, and A. Shamir. Zero Knowledge Proofs of Identity. In *Proc. of STOC'87*, pages 210–217, 1987.
17. D. M. Freeman. Converting pairing-based cryptosystems from composite-order groups to prime-order groups. In H. Gilbert, editor, *EUROCRYPT*, volume 6110 of *Lecture Notes in Computer Science*, pages 44–61. Springer, 2010.
18. E. Fujisaki and T. Okamoto. Secure integration of asymmetric and symmetric encryption schemes. In M. J. Wiener, editor, *CRYPTO*, volume 1666 of *Lecture Notes in Computer Science*, pages 537–554. Springer, 1999.
19. S. D. Galbraith and K. G. Paterson, editors. *Pairing-Based Cryptography - Pairing 2008, Second International Conference, Egham, UK, September 1-3, 2008. Proceedings*, volume 5209 of *Lecture Notes in Computer Science*. Springer, 2008.
20. S. D. Galbraith and E. R. Verheul. An analysis of the vector decomposition problem. In R. Cramer, editor, *Public Key Cryptography*, volume 4939 of *Lecture Notes in Computer Science*, pages 308–327. Springer, 2008.
21. T. E. Gamal. A public key cryptosystem and a signature scheme based on discrete logarithms. In G. R. Blakley and D. Chaum, editors, *CRYPTO*, volume 196 of *Lecture Notes in Computer Science*, pages 10–18. Springer, 1984.
22. K. Gjøsteen. *Subgroup Membership Problems and Public Key Cryptosystems*. PhD thesis, Norwegian University of Science and Technology, 2004.
23. J. Groth and A. Sahai. Efficient non-interactive proof systems for bilinear groups. In N. P. Smart, editor, *EUROCRYPT*, volume 4965 of *Lecture Notes in Computer Science*, pages 415–432. Springer, 2008.
24. D. Hofheinz and E. Kiltz. Secure hybrid encryption from weakened key encapsulation. In A. Menezes, editor, *CRYPTO*, volume 4622 of *Lecture Notes in Computer Science*, pages 553–571. Springer, 2007.
25. F. Hoshino, K. Suzuki, and T. Kobayashi. Revocable DDH by using Pairing and It's Application. SCIS 2005 The 2005 Symposium on Cryptography and Information Security, 3D4-3, Maiko Kobe, Japan, Jan. 25-28, 2005.
26. A. Joux. A one round protocol for tripartite diffie-hellman. In W. Bosma, editor, *ANTS*, volume 1838 of *Lecture Notes in Computer Science*, pages 385–394. Springer, 2000.
27. A. Joux and K. Nguyen. Separating decision Diffie-Hellman from Diffie-Hellman in cryptographic groups. Cryptology ePrint Archive: 2001/003, 2001.
28. K. Kurosawa and L. T. Phong. Leakage resilient ibe and ipe under the dlin assumption. In M. J. J. Jr., M. E. Locasto, P. Mohassel, and R. Safavi-Naini, editors, *ACNS*, volume 7954 of *Lecture Notes in Computer Science*, pages 487–501. Springer, 2013.
29. T. Okamoto and D. Pointcheval. The Gap Problems: A New Class of Problems for the Security of Cryptographic Primitives. In *Proc. of PKC 2001*, pages 104–118, 2001.
30. T. Okamoto and K. Takashima. Homomorphic encryption and signatures from vector decomposition. In Galbraith and Paterson [19], pages 57–74.
31. T. Okamoto and K. Takashima. Fully secure functional encryption with general relations from the decisional linear assumption. In T. Rabin, editor, *CRYPTO*, volume 6223 of *Lecture Notes in Computer Science*, pages 191–208. Springer, 2010.
32. T. Okamoto and K. Takashima. Decentralized attribute-based signatures. *IACR Cryptology ePrint Archive*, 2011:701, 2011.
33. T. Okamoto and K. Takashima. Fully secure unbounded inner-product and attribute-based encryption. *IACR Cryptology ePrint Archive*, 2012:671, 2012.
34. C.-P. Schnorr. Efficient Signature Generation by Smart Cards. *J. Cryptology*, 4(3):161–174, 1991.
35. Y. Seurin. New constructions and applications of trapdoor ddh groups. In K. Kurosawa and G. Hanaoka, editors, *Public Key Cryptography*, volume 7778 of *Lecture Notes in Computer Science*, pages 443–460. Springer, 2013.
36. H. Shacham. A cramer-shoup encryption scheme from the linear assumption and from progressively weaker linear variants. *IACR Cryptology ePrint Archive*, 2007:74, 2007.
37. Y. Tsiounis and M. Yung. On the security of elgamal based encryption. In H. Imai and Y. Zheng, editors, *Public Key Cryptography*, volume 1431 of *Lecture Notes in Computer Science*, pages 117–134. Springer, 1998.
38. 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.
39. A. Yamamura and T. Saito. Private information retrieval based on the subgroup membership problem. In V. Varadharajan and Y. Mu, editors, *ACISP*, volume 2119 of *Lecture Notes in Computer Science*, pages 206–220. Springer, 2001.
40. M. Yoshida, S. Mitsunari, and T. Fujiwara. Vector Decomposition Problem and the Trapdoor Inseparable Multiplex Transmission Scheme based the Problem. SCIS 2003 The 2003 Symposium on Cryptography and Information Security, 7B-1, Hamamatsu, Japan, Jan. 26-29, 2003.