SCIS 2022 2022 Symposium on
Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics,
Information and Communication Engineers

Lossy Trapdoor function の幾つかの亜種について
On some variants of lossy trapdoor function

星野 文学 *
Fumitaka Hoshino

あらまし Peikert と Waters は STOC 2008 において lossy trapdoor function (LTDF) の概念を提唱し, その具体的構成と応用を提案した [1–3]. その後 LTDF の構成法や拡張および応用などに関して様々な研究が行われている [4–15]. ところで LTDF の拡張は方式を構成する多項式時間アルゴリズムの数が比較的多く, 複雑すぎて様々なプロトコルへの流用が難しいという問題があり, オーダーメイド的に LTDF の亜種が構成される傾向がある. ところが, 実際にはそうした拡張を具体的に構成する際は Peikert-Waters の DDH による構成をベースに機能を追加していくことが多い. そうした状況を鑑み, 本稿では様々な応用が出来そうな LTDF の比較的シンプルな亜種について考察を行いたい.

Keywords: Lossy Trapdoor Function, Lossy Trapdoor Homomorphism, Lossy Trapdoor Algebra

1 はじめに

Peikert と Waters は STOC 2008 において lossy trapdoor function (LTDF) の概念を提唱し, その具体的構成と応用を提案した [1–3]. LTDF とは trapdoor function (TDF) の拡張であり, LTDF の関数のインスタンスを生成する時は単射関数とするか不可逆関数とするかを選択できる. 単射関数を生成した場合にはインスタンス生成時に同時に生成されるトラップドアにより逆関数を効率的に計算可能である. そして安全な LTDF においては関数のインスタンスが単射であるか不可逆であるかは識別できないとされる. LTDF には様々な構成法, 応用, 拡張が存在し, 様々な研究が行われている [4–15]. ところで LTDF の拡張は方式を構成する多項式時間アルゴリズムの数が比較的多く, 複雑すぎて様々なプロトコルへの流用が難しいという問題があり, オーダーメイド的に LTDF の亜種が構成される傾向がある. ところが, 実際にはそうした拡張を具体的に構成する際は Peikert-Waters の DDH による構成をベースに機能を追加していくことが多い. そうした状況を鑑み, 本稿では様々な応用が出来そうな LTDF の比較的シンプルな亜種について考察を行いたい.

* 長崎県立大学, 〒851-2195 長崎県西彼杵郡長与町まなび野 1-1-1,University of Nagasaki, 1-1-1 Manabino, Nagayo-cho, Nishi-Sonogi-gun, Nagasaki 851-2195, JAPAN,hoshino@sun.ac.jp

2 準備

2.1 One-way Function

$\lambda \in \mathbb{N}$ をセキュリティパラメタとして, 確率的多項式時間アルゴリズムの組 $\Pi := (\mathtt{Gen}, \mathtt{Eval})$

$$\mathtt{Gen} : 1^\lambda \xmapsto{\$} s.$$
$$\mathtt{Eval} : x, s \xmapsto{\$} f_s(x) \text{ s.t. } f_s : \mathcal{X}_s \to \mathcal{Y}_s.$$

が one-way であるとは λ に関する如何なる確率的多項式時間アルゴリズム $\mathcal{A}$ に対しても

$$\mathsf{Adv}^{\mathcal{A}}(\lambda) := \Pr\left[y = f_s(x^*) \middle| \begin{array}{l} s \xleftarrow{\$} \mathtt{Gen}(\lambda); \\ x \xleftarrow{\$} \mathcal{X}_s; \\ y \xleftarrow{\$} \mathtt{Eval}(s, x); \\ x^* \xleftarrow{\$} \mathcal{A}(y, \lambda, s, \Pi); \end{array} \right]$$

が λ に関して無視可能なことである.

2.2 Trapdoor Function

trapdoor function (TDF) とは one-way function の拡張であり, 次の確率的多項式時間アルゴリズムの組 $\Pi := (\mathtt{Gen}, \mathtt{Eval}, \mathtt{Invert})$ のことである.

$$\mathtt{Gen} : 1^\lambda \xmapsto{\$} (s, t).$$
$$\mathtt{Eval} : x, s \xmapsto{\$} f_s(x) \text{ s.t. } f_s : \mathcal{X}_s \hookrightarrow \mathcal{Y}_s$$

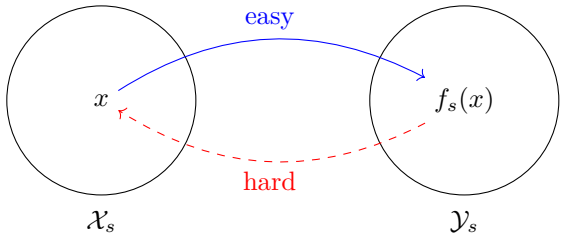

図 1　One-way

$$\texttt{Invert} : t, f_s(x) \mapsto x.$$

Gen の出力の一部 t を trapdoor と呼ぶ。$\mathcal{A}$ に t を渡さないと約束しておけば, trapdoor function にも自然に one-way が定義出来る.

2.3　Lossy Trapdoor Function (LTDF)

Peikert と Waters は STOC 2008 において LTDF の概念を提唱し, その具体的構成と応用を提案した [1–3]. その後 LTDF に関して様々な研究が行われている [6–15]. $\lambda \in \mathbb{N}$ をセキュリティパラメタとすると lossy trapdoor function (LTDF) とは次の確率的多項式時間アルゴリズムの組 $\Pi := (\texttt{Gen}, \texttt{Eval}, \texttt{Invert})$ のことである.

$$\texttt{Gen} : 1^\lambda, b \overset{\$}{\mapsto} (s, t).$$
$$\texttt{Eval} : x, s \overset{\$}{\mapsto} f_s(x).$$
$$\texttt{Invert} : t, f_s(x) \mapsto x \text{ if } b = 1.$$

ここで

- s は関数 $f_s : \mathcal{X}_s \to \mathcal{Y}_s$ を指定する関数 index.
- t は trapdoor.
- $b = 1$ のとき関数 f_s は単射写像であり, そのような Gen の出力を injective instance と呼ぶ. このとき $|\mathcal{X}_s|/|f_s(\mathcal{X}_s)| = 1$.
- $b = 0$ のとき関数 f_s は不可逆写像であり, そのような Gen の出力を lossy instance と呼ぶ. このとき $|\mathcal{X}_s|/|f_s(\mathcal{X}_s)| \geq \texttt{poly}(\lambda)$.

LTDF の injective instance と lossy instance が識別不能であるとは λ に関する如何なる確率的多項式時間アルゴリズム $\mathcal{A}$ に対しても

$$\mathsf{Adv}^{\mathcal{A}}(\lambda) := \left| \Pr\left[b = b^* \middle| \begin{array}{l} b \overset{\$}{\leftarrow} \{0,1\}; \\ (s,t) \overset{\$}{\leftarrow} \texttt{Gen}(\lambda, b); \\ b^* \overset{\$}{\leftarrow} \mathcal{A}(s, \lambda, \Pi); \end{array} \right] - \frac{1}{2} \right|$$

が λ に関して無視可能なことである. 概ね次のような簡単な議論によって, LTDF の injective instance の one-way は injective instance と lossy instance の識別不能性から直ちに導かれる [1–3].

補題 1 (Peikert-Waters [1])**.** *ある LTDF の injective instance と lossy instance が識別不能であるとき, その LTDF の injective instance は one-way TDF である.*

証明のスケッチ. 安全性を無視すれば, 形式的な LTDF の injective instance が形式的な TDF である事は定義により明らか. もし LTDF の injective instance の one-way を $1/\texttt{poly}(\lambda)$ の確率で破る確率的多項式時間チューリング機械 $\mathcal{I} : s, f_s(x) \overset{\$}{\mapsto} x'$ があるなら

$$\begin{array}{l} \mathcal{A}^{\mathcal{I}} : s, \lambda, (\texttt{Gen}, \texttt{Eval}, \texttt{Invert}) \overset{\$}{\mapsto} b^* : \\ \quad x \overset{\$}{\leftarrow} \mathcal{X}_s; \\ \quad y \overset{\$}{\leftarrow} \texttt{Eval}(x, s); \\ \quad b^* \overset{\$}{\leftarrow} (\mathcal{I}(s, y) \overset{?}{=} x); \end{array}$$

なるオラクルチューリング機械により LTDF (Gen, Eval, Invert) の injective instance と lossy instance を $1/\texttt{poly}(\lambda)$ の確率で識別可能である. 従って LTDF の injective instance と lossy instance が識別不能であるとき, その LTDF の injective instance は one-way である. □

2.4　離散対数仮定

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で, 形式的には安全変数 1^λ を入力とし, λ でパラメタライズされる記述 $(\mathbb{L}, \mathbb{G})$ を出力する確率的多項式時間アルゴリズム

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

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式を記述する文字列 (パラメータ) であるが, 回りくどいので以降は $\mathbb{L}, \mathbb{G}$ と代数的構造を同一視する. $\mathbb{L}$ は離散対数と呼ばれる単位的可換環で $\mathbb{G}$ は $\mathbb{L}$ 上の加群であるが, 歴史的経緯により, 典型的には $\mathbb{G}$ を素数位数 q をもつ巡回群とし $\mathbb{L} := \mathbb{F}_q$ などとし, $\mathbb{G}$ 上の群演算は積で記述されることが多い. 本稿でもこれを踏襲し, $\mathbb{G}$ 上の加群としての和を積で, 加群としてのスカラー倍を冪乗で記述する. $s = (\mathbb{G}, q, g)$ をサンプリングするアルゴリズム $\texttt{Gen} \simeq \mathcal{G}$ および冪乗を計算するアルゴリズム $\texttt{Eval} : s, x \mapsto g^x$ がどちらも効率的であるなら, $\Pi := (\texttt{Gen}, \texttt{Eval})$ が one-way であるか否かを議論する事が出来る. 上記の構成で $\mathbb{G}$ に有限体の加法群を用いると, (Gen, Eval) は明らかに one-way ではない. 一方 $\mathbb{G}$ に有限体の乗法群や楕円曲線を用いると one-way となる (Gen, Eval) を構成で

きると広く信じられており, そのような仮説を離散対数仮定と呼ぶ. 離散対数仮定が成立しそうな $\mathcal{G}$ を離散対数群と呼ぶ.

2.5 Decisional Diffie-Hellman 仮定

暗号方式の設計者は方式を構成する為に仮定しなくてはならない事をなるべく減らしたいと考える. 従って one-way function のような抽象化された暗号プリミティブは非常にシンプルな構造を持ち, 余計な構造は仮定しない. しかし, そのような暗号設計のミニマリズムとは裏腹に離散対数群のような良く知られた具体的プリミティブは意外に複雑な構造を備えている. 離散対数群において冪乗は単なる one-way function ではなく, 実際には $\mathbb{G}$, $\mathbb{L} \to \mathbb{G}, g, x \mapsto g^x$ なる双準同型の構造を持つ. Diffie-Hellman 鍵交換 [16] のように, 大抵の実用的な暗号方式や暗号プロトコルはそのような構造を利用する. λ に関す

Alice	$(\mathbb{L}, \mathbb{G}) \xleftarrow{\$} \mathcal{G}(\lambda),\ g \xleftarrow{\$} \mathbb{G}$	**Bob**
$a \xleftarrow{\$} \mathbb{L}$		$b \xleftarrow{\$} \mathbb{L}$
$A \leftarrow g^a$	$\xrightarrow{A}$	$B \leftarrow g^b$
	$\xleftarrow{B}$	
$K_a \leftarrow B^a$	$= (g^b)^a = g^{ab} = (g^a)^b =$	$K_b \leftarrow A^b$

図 2 Diffie-Hellman 鍵交換

る如何なる確率的多項式時間アルゴリズム $\mathcal{A}$ に対しても

$$\mathsf{Adv}^{\mathcal{A}}(\lambda) := \Pr\left[C = g^{ab} \middle| \begin{array}{l} (\mathbb{L}, \mathbb{G}) \xleftarrow{\$} \mathcal{G}(1^\lambda); \\ (g, a, b) \xleftarrow{\$} (\mathbb{G} \setminus \{1\}) \times \mathbb{L}^2; \\ (A, B) \leftarrow (g^a, g^b); \\ C \xleftarrow{\$} \mathcal{A}(g, A, B, \lambda, \mathbb{L}, \mathbb{G}); \end{array}\right]$$

が λ に関して無視可能なことを Computational Diffie-Hellman (CDH) 仮定と呼ぶ. CDH 仮定が成立しそうな $\mathcal{G}$ を CDH 群と呼ぶ.

また, λ に関する如何なる確率的多項式時間アルゴリズム $\mathcal{A}$ に対しても

$$\mathsf{Adv}^{\mathcal{A}}(\lambda) := \left|\Pr\left[d = d^* \middle| \begin{array}{l} d \xleftarrow{\$} \{0,1\}; \\ (\mathbb{L}, \mathbb{G}) \xleftarrow{\$} \mathcal{G}(1^\lambda); \\ (g, a, b, c) \xleftarrow{\$} (\mathbb{G} \setminus \{1\}) \times \mathbb{L}^3; \\ (A, B, C) \leftarrow (g^a, g^b, g^{ab+cd}); \\ d^* \xleftarrow{\$} \mathcal{A}(g, A, B, C, \lambda, \mathbb{L}, \mathbb{G}); \end{array}\right] - \frac{1}{2}\right|$$

が λ に関して無視可能なことを Decisional Diffie-Hellman (DDH) 仮定と呼ぶ. DDH 仮定が成立しそうな $\mathcal{G}$ を DDH 群と呼ぶ.

2.6 ElGamal 暗号

(教科書) ElGamal 暗号は Diffie-Hellman 鍵交換と Vernam 暗号を組み合わせた構造を持つ良く知られた公開鍵暗号で, その IND-CPA が DDH 仮定に直接帰着できることに加えて, 主要なアルゴリズムを群演算で構成できるため群構造を使用する様々なアプリケーションに用いられる.

$$\begin{aligned} \mathtt{KeyGen}: 1^\lambda &\xmapsto{\$} (sk, pk) \\ &(\mathbb{L}, \mathbb{G}) \xleftarrow{\$} \mathcal{G}(1^\lambda); \\ &(g, sk) \xleftarrow{\$} (\mathbb{G} \setminus \{1\}) \times \mathbb{L}; \\ &h \leftarrow g^{sk}; \\ &pk \leftarrow (g, h); \\ \mathtt{Enc}: pk, m &\xmapsto{\$} (c_1, c_2) \\ &(g, h) \leftarrow pk; \\ &r \xleftarrow{\$} \mathbb{L}; \\ &(c_1, c_2) \leftarrow (g^r, m \cdot y^r); \\ \mathtt{Dec}: sk, (c_1, c_2) &\mapsto m \\ &m \leftarrow c_2 / c_1^{sk}; \end{aligned}$$

3 Peikert-Waters の構成

3.1 記法

離散対数のある自然な拡張に関して次のような記法 [17] を用いる.

- $\mathbb{G}$ を素数位数 q をもつ巡回群とし g をその生成元とする. 写像 : $\mathbb{G}^{n\times m} \to \mathbb{F}_q^{n\times m}$,

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

を考える. $\mathbb{F}_q$ 行列 $x := (x_{ij}) \in \mathbb{F}_q^{n\times m}$ を g を底とする $X := (g^{x_{ij}}) \in \mathbb{G}^{n\times m}$ の離散対数と呼び x を $\log_g X$ と書く. また, X を g の x による冪乗, あるいは g の x 乗と呼び X を g^x と書く.

- $x, y \in \mathbb{F}_q^{n\times m}$, $X := g^x$, $Y := g^y$ とする. 積 $X \cdot Y$ を

$$\begin{aligned} X \cdot Y : \mathbb{G}^{n\times m} \times \mathbb{G}^{n\times m} &\to \mathbb{G}^{n\times m}, \\ g^x \quad , \quad g^y \quad &\mapsto g^{x+y}, \end{aligned}$$

と定義する. 積 $X \cdot Y$ は可換である. 慣例に従い積 $X \cdot Y$ を XY と略記する.

- $x \in \mathbb{F}_q^{n\times\ell}$, $y \in \mathbb{F}_q^{\ell\times m}$ とし, $X := g^x$, $Y := g^y$ とする. 非退化双準同型 X^y を

$$\begin{aligned} X^y : \mathbb{G}^{n\times\ell} \times \mathbb{F}_q^{\ell\times m} &\to \mathbb{G}^{n\times m}, \\ g^x \quad , \quad y \quad &\mapsto \quad g^{xy}, \end{aligned}$$

非退化双準同型 ${}^xY$ を

$$\begin{aligned} {}^xY : \mathbb{F}_q^{n\times\ell} \times \mathbb{G}^{\ell\times m} &\to \mathbb{G}^{n\times m}, \\ x \quad , \quad g^y \quad &\mapsto \quad g^{xy}, \end{aligned}$$

と定義する. X^y を右冪乗 ${}^xY$ を左冪乗と呼ぶ. また $Z = X^y$ なるとき y を X を底とする Z の右離散対数と呼び y を $\mathrm{rlog}_X Z$ と書く. 同様に $Z = {}^xY$ なるとき x を Y を底とする Z の左離散対数と呼び x を $\mathrm{llog}_Y Z$ と書く.
- $x, y \in \mathbb{F}_q^{n\times m}$, $a \in \mathbb{F}_q$, $X := g^x$, $Y := g^y$ とする. 写像 $X^a (= {}^aX)$ を

$$\begin{aligned} X^a : \mathbb{G}^{n\times m} \times \mathbb{F}_q &\to \mathbb{G}^{n\times m}, \\ g^x \quad , \quad a \quad &\mapsto \quad g^{ax}, \end{aligned}$$

と定義する. また商 Y/X を

$$Y/X := Y \cdot X^{-1} = g^{y-x}$$

と定義する.
- X や Y の離散対数を知らなくとも $\mathbb{G}$ 上の群演算を用いて 右冪乗, 左冪乗, 積および商は効率的に計算可能である.
- $\mathbb{G}$ が離散対数群であれば, 離散対数 $\log_g X$, 右離散対数 $\mathrm{rlog}_X Z$ および左離散対数 $\mathrm{llog}_Y Z$ は 一般には効率的な計算方法は知られていないとして良い.
- 通常の離散対数と同様に, 解となる離散対数候補の分布が極端に偏っている場合は効率的に解くことが可能な事がある. 通常の離散対数と異なる点は成分ごとにそれが可能となる事である. つまり離散対数が部分的に解けるという事が起こり得る.

3.2 DDH 群による構成

Peikert と Waters は ElGamal 暗号の拡張を用いて LTDF の具体的構成を与えている [1–3].

$$\begin{aligned} &\texttt{Gen} : 1^* \times \{0,1\} \xrightarrow{\$} (\mathbb{G}^{n\times 1} \times \mathbb{G}^{n\times n}) \times \mathbb{F}_q^{1\times n}, \\ &\quad 1^\lambda, b \xmapsto{\$} (s,t) : \\ &\qquad (\mathbb{F}_q, \mathbb{G}) \xleftarrow{\$} \mathcal{G}(1^\lambda); \\ &\qquad (g,t) \xleftarrow{\$} (\mathbb{G} \setminus \{1\}) \times \mathbb{F}_q^{1\times n}; \\ &\qquad h \leftarrow g^t; \\ &\qquad r \xleftarrow{\$} \mathbb{F}_q^{n\times 1}; \\ &\qquad m \leftarrow g^{b\cdot I_n}; \\ &\qquad (c_1, c_2) \leftarrow ({}^rg, m \cdot {}^rh); \\ &\qquad s \leftarrow (c_1, c_2); \end{aligned}$$

$$\begin{aligned} &\texttt{Eval} : \{0,1\}^{1\times n} \times (\mathbb{G}^{n\times 1} \times \mathbb{G}^{n\times n}) \xrightarrow{\$} (\mathbb{G}^{1\times 1} \times \mathbb{G}^{1\times n}), \\ &\quad x, s \xmapsto{\$} y : \\ &\qquad (c_1, c_2) \leftarrow s; \\ &\qquad (c_1', c_2') \leftarrow ({}^xc_1, {}^xc_2); \\ &\qquad y \leftarrow (c_1', c_2'); \end{aligned}$$

$$\begin{aligned} &\texttt{Invert} : \mathbb{F}_q^{1\times n} \times (\mathbb{G}^{1\times 1} \times \mathbb{G}^{1\times n}) \xrightarrow{\$} \{0,1\}^{1\times n}, \\ &\quad t, y \xmapsto{\$} x : \\ &\qquad (c_1', c_2') \leftarrow y; \\ &\qquad m \leftarrow c_2'/(c_1')^t \in \mathbb{G}^{1\times n}; \\ &\qquad x \leftarrow \log_g m \in \mathbb{F}_q^{1\times n}; \end{aligned}$$

ここで,

- $I_n \in \mathbb{F}_q^{n\times n}$ は $n \times n$ 単位行列である.
- `Invert` において, 離散対数を解く必要があるが, これは成分ごとに離散対数候補の分布が極端に偏っている ($\{0,1\}$) 事を想定している.
- 幾分煩雑になるが, ElGamal 暗号の代わりに Paillier 暗号 [18] を用いることによってそのような制限を外す事ができる [7].

4 LTDF の変種

4.1 Lossy Trapdoor Homomorphism

LTDF は one-way function (trapdoor function) の拡張であり, 非常にシンプルな構造を持ち余計な構造は仮定していない. 一方, 上記の DDH による具体的構成は実際には単なる LTDF よりも相当に複雑な構造を備えている. LTDF と具体的構成の間に one-way function と離散対数群の違いのような明確な機能の差が存在している. そのことを明確化する為に `Eval` の出力結果が, 関数 index としてもう一度 `Eval` に入力できるような LTDF を考えてみる. ここではそのような LTDF を lossy trapdoor homomorphism と呼ぶことにする. $\lambda \in \mathbb{N}$ をセキュリ

ティパラメタとすると lossy trapdoor homomorphism とは次の確率的多項式時間アルゴリズムの組 $\Pi := (\mathtt{Gen}, \mathtt{Eval}, \mathtt{Invert})$ のことである.

$$\mathtt{Gen} : 1^\lambda, b \overset{\$}{\mapsto} (f(1), t).$$
$$\mathtt{Eval} : x, f(y) \overset{\$}{\mapsto} f(x \cdot y).$$
$$\mathtt{Invert} : t, f(z) \mapsto z.$$

ここで

- x, y, z は何らかの群 $\mathbb{L}$ 上の元とし, $\mathbb{L}$ は必ずしも可換とは限らないとする.
- $f(x)$ は正確には x の関数 $f(x)$ の値の符号語という事になるが, LTDF の DDH による具体的構成と同様に $f(x)$ の値から符号語への対応は必ずしも 1 対 1 とは限らず 1 対多でも良いとする.

lossy trapdoor homomorphism の injective instance と lossy instance が識別不能であるとは λ に関する如何なる確率的多項式時間アルゴリズム $\mathcal{A}$ に対しても

$$\mathsf{Adv}^{\mathcal{A}}(\lambda) := \left| \Pr\left[b = b^* \middle| \begin{array}{l} b \overset{\$}{\leftarrow} \{0,1\}; \\ (f(1), t) \overset{\$}{\leftarrow} \mathtt{Gen}(\lambda, b); \\ b^* \overset{\$}{\leftarrow} \mathcal{A}(\lambda, f(1)); \end{array} \right] - \frac{1}{2} \right|$$

が λ に関して無視可能なことである.

4.2 Peikert-Waters の構成の単純な拡張

上記の Peikert-Waters の DDH による具体的構成の $\mathtt{Eval}$ アルゴリズムにおいて

$$\mathtt{Eval} : (\mathbb{G}^{n\times 1} \times \mathbb{G}^{n\times n}) \times \mathbb{L}^{1\times n} \overset{\$}{\to} (\mathbb{G}^{1\times 1} \times \mathbb{G}^{1\times n}),$$

の部分を

$$\mathtt{Eval} : (\mathbb{G}^{n\times 1} \times \mathbb{G}^{n\times n}) \times \mathbb{L}^{n\times n} \overset{\$}{\to} (\mathbb{G}^{n\times 1} \times \mathbb{G}^{n\times n}),$$

のように変更すれば, $\mathtt{Eval}$ の出力結果をもう一度 $\mathtt{Eval}$ に入力できそうである. 以下に Peikert-Waters の具体的構成をこの方針で単純に拡張した lossy trapdoor homomorphism の具体的方式を示し, その問題点を述べる.

$\mathtt{Gen} : 1^* \times \{0,1\} \overset{\$}{\to} (\mathbb{G}^{n\times 1} \times \mathbb{G}^{n\times n}) \times \mathbb{F}_q^{1\times n}$,
$1^\lambda, b \overset{\$}{\mapsto} (s, t)$:
$(\mathbb{F}_q, \mathbb{G}) \overset{\$}{\leftarrow} \mathcal{G}(1^\lambda)$;
$(g, t) \overset{\$}{\leftarrow} (\mathbb{G} \setminus \{1\}) \times \mathbb{F}_q^{1\times n}$;
$h \leftarrow g^t$;
$r \overset{\$}{\leftarrow} \mathbb{F}_q^{n\times 1}$;
$m \leftarrow g^{b \cdot I_n}$;
$(c_1, c_2) \leftarrow ({}^r g, m \cdot {}^r h)$;
$s \leftarrow (c_1, c_2)$;

$\mathtt{Eval} : \mathbb{L} \times (\mathbb{G}^{n\times 1} \times \mathbb{G}^{n\times n}) \overset{\$}{\to} (\mathbb{G}^{n\times 1} \times \mathbb{G}^{n\times n})$,
$x, s \overset{\$}{\mapsto} s'$:
$(c_1, c_2) \leftarrow s$;
$(c_1', c_2') \leftarrow ({}^x c_1, {}^x c_2)$;
$s' \leftarrow (c_1', c_2')$;

$\mathtt{Invert} : \mathbb{F}_q^{1\times n} \times (\mathbb{G}^{n\times 1} \times \mathbb{G}^{n\times n}) \overset{\$}{\to} \mathbb{L}$,
$t, s' \overset{\$}{\mapsto} x$:
$(c_1', c_2') \leftarrow s'$;
$m \leftarrow c_2' / (c_1')^t \in \mathbb{G}^{n\times n}$;
$x \leftarrow \log_g m \in \mathbb{F}_q^{n\times n}$;

ここで

- $n \sim \mathtt{poly}(\lambda)$ とする.
- $\mathbb{L}$ を $n \times n$ の置換行列全体とする.

上記の構成はおよそ次のような特徴を持つ.

- $\mathtt{Gen}$ は Peikert-Waters の $\mathtt{Gen}$ と全く同じ.
- $\mathtt{Eval}$ は Peikert-Waters の $\mathtt{Eval}$ を n 回呼び出すのと全く同じ.
- $\mathtt{Invert}$ は Peikert-Waters の $\mathtt{Invert}$ を n 回呼び出すのと全く同じ.
- この LTDF の injective instance と lossy instance の識別不能が破れるならどう見ても Peikert-Waters の LTDF も破れる.
- 関数の定義域の $\mathbb{L}$ は $|\mathbb{L}| = n! \sim O(2^\lambda)$ で十分大きい.

ところで補題 1 により, LTDF の injective instance と lossy instance の識別不能が破れるなら, injective instance は one-way となるはずである. 従って, この LTDF の injective instance も one-way が成立しそうな錯覚に陥るが, 実際には (c_1', c_2') は単に (c_1, c_2) の各成分を入れ替えただけに過ぎず, 実は以下のアルゴリズムによって lossy instance においてさえ $f(x)$ から x を多項

式時間で導出可能である.

$$
\begin{aligned}
&\mathcal{A} : (\mathbb{G}^{n\times 1} \times \mathbb{G}^{n\times n}) \times (\mathbb{G}^{n\times 1} \times \mathbb{G}^{n\times n}) \xrightarrow{\$} \mathbb{F}_q^{n\times n},\\
&\quad f(1) = (c_1, c_2), f(x) = (c_1', c_2') \xmapsto{\$} x :\\
&\qquad S \leftarrow c_1;\\
&\qquad D \leftarrow c_1';\\
&\qquad \forall (i,j) \in \{1,\dots,n\}^2,\ x_{ij} \leftarrow 0;\\
&\qquad \forall j \in \{1,\dots,n\},\\
&\qquad\quad \text{find } i \text{ s.t. } D_i = S_j;\\
&\qquad\quad x_{ij} \leftarrow 1;
\end{aligned}
$$

このような一見パラドックスに見える問題は, 加法的準同型確率暗号で行列を作って LTDF を構成する方法 [1–3] で, 確率暗号の乱数部分に関数の原像の情報が残る可能性があるために起こっている. Peikert-Waters の元の方式でも離散対数とナップザック問題が解けるなら同じような問題が起こるので, 補題 1 は慎重に取り扱う必要があるかもしれない.

$$
\begin{aligned}
&\mathcal{A} : (\mathbb{G}^{n\times 1} \times \mathbb{G}^{n\times n}) \times (\mathbb{G}^{1\times 1} \times \mathbb{G}^{1\times n}) \xrightarrow{\$} \mathbb{F}_q^{1\times n},\\
&\quad (c_1, c_2), (c_1', c_2') \xmapsto{\$} x :\\
&\qquad S \leftarrow c_1;\\
&\qquad D \leftarrow c_1';\\
&\qquad \forall i \in \{1,\dots,n\},\ a_i \leftarrow \log_g S_i;\\
&\qquad b \leftarrow \log_g D\\
&\qquad \text{find } \{x_i\} \text{ s.t. } b = \textstyle\sum_i x_i \cdot a_i;
\end{aligned}
$$

4.3 西巻らの構成 [4, 5]

ElGamal 暗号の Re-encryption を用いれば確率暗号の乱数部分に含まれる関数の原像の情報を情報理論的に取り除く事が可能である. このような概念は LTDF が発表された後, すぐに西巻らにより考案され, Non-Interactive Universally Composable Commitment Scheme に応用された [4, 5]. 但し, この場合 lossy trapdoor homomorphism は確定的関数ではなく確率的関数となる.

$$
\begin{aligned}
&\mathtt{Gen} : 1^* \times \{0,1\} \xrightarrow{\$} (\mathbb{G} \times \mathbb{G}^{1\times n} \times \mathbb{G}^{n\times 1} \times \mathbb{G}^{n\times n}) \times \mathbb{F}_q^{1\times n},\\
&\quad 1^\lambda, b \xmapsto{\$} (s,t) :\\
&\qquad (\mathbb{F}_q, \mathbb{G}) \xleftarrow{\$} \mathcal{G}(1^\lambda);\\
&\qquad (g,t) \xleftarrow{\$} (\mathbb{G} \setminus \{1\}) \times \mathbb{F}_q^{1\times n};\\
&\qquad h \leftarrow g^t;\\
&\qquad r \xleftarrow{\$} \mathbb{F}_q^{n\times 1};\\
&\qquad m \leftarrow g^{b\cdot I_n};\\
&\qquad (c_1, c_2) \leftarrow ({}^r g, m \cdot {}^r h);\\
&\qquad s \leftarrow (g, h, c_1, c_2);
\end{aligned}
$$

$$
\begin{aligned}
&\mathtt{Eval} : \mathbb{F}_q^{n\times n} \times (\mathbb{G} \times \mathbb{G}^{1\times n} \times \mathbb{G}^{n\times 1} \times \mathbb{G}^{n\times n})\\
&\qquad \xrightarrow{\$} (\mathbb{G} \times \mathbb{G}^{1\times n} \times \mathbb{G}^{1\times n} \times \mathbb{G}^{n\times n}),\\
&\quad x, s \xmapsto{\$} s' :\\
&\qquad (g, h, c_1, c_2) \leftarrow s;\\
&\qquad r \xleftarrow{\$} \mathbb{F}_q^{n\times 1};\\
&\qquad s' \leftarrow (g, h, {}^r g \cdot {}^x c_1, {}^r h \cdot {}^x c_2);
\end{aligned}
$$

$$
\begin{aligned}
&\mathtt{Invert} : \mathbb{F}_q^{1\times n} \times (\mathbb{G} \times \mathbb{G}^{1\times n} \times \mathbb{G}^{n\times 1} \times \mathbb{G}^{n\times n}) \xrightarrow{\$} \mathbb{F}_q^{n\times n},\\
&\quad t, y \xmapsto{\$} x :\\
&\qquad (g, h, c_1', c_2') \leftarrow y;\\
&\qquad m \leftarrow c_2'/(c_1')^t \in \mathbb{G}^{1\times n};\\
&\qquad x \leftarrow \log_g m \in \mathbb{F}_q^{1\times n};
\end{aligned}
$$

4.4 Lossy Trapdoor Algebra

Peikert-Waters の 具体的構成に近い lossy trapdoor homomorphism という LTDF の拡張を考えたが, 上記の具体的構成がもつ数学的構造はそれより遥かに複雑である. 上記の具体的構成により近い形の LTDF の拡張を考えたい. そのような暗号プリミティブを lossy trapdoor algebra と呼ぶことにする. $\lambda \in \mathbb{N}$ をセキュリティパラメタとすると lossy trapdoor algebra とは次の確率的多項式時間アルゴリズムの組 $\Pi := (\mathtt{Gen}, \mathtt{Eval}_{\mathtt{Rexp}}, \mathtt{Eval}_{\mathtt{Lexp}}, \mathtt{Eval}_{\mathtt{Mul}}, \mathtt{Invert}_{\mathtt{Rexp}}, \mathtt{Invert}_{\mathtt{Lexp}})$ のことである.

$$
\begin{aligned}
\mathtt{Gen} &: 1^\lambda, b \xmapsto{\$} (\mathbb{L}, \mathbb{G}_b, g, t).\\
\mathtt{Eval}_{\mathtt{Rexp}} &: \mathbb{G} \times \mathbb{L} \xrightarrow{\$} \mathbb{G},\ h, x \xmapsto{\$} h^x.\\
\mathtt{Eval}_{\mathtt{Lexp}} &: \mathbb{L} \times \mathbb{G} \xrightarrow{\$} \mathbb{G},\ x, h \xmapsto{\$} {}^x h.\\
\mathtt{Eval}_{\mathtt{Mul}} &: \mathbb{G} \times \mathbb{G} \xrightarrow{\$} \mathbb{G},\ h_1, h_2 \xmapsto{\$} h_1 \cdot h_2.\\
\mathtt{Invert}_{\mathtt{Rexp}} &: \{0,1\}^*, \tilde{\mathbb{G}} \xrightarrow{\$} \mathbb{L},\ t, h \mapsto \mathrm{rlog}_g h.\\
\mathtt{Invert}_{\mathtt{Lexp}} &: \{0,1\}^*, \tilde{\mathbb{G}} \xrightarrow{\$} \mathbb{L},\ t, h \mapsto \mathrm{llog}_g h.
\end{aligned}
$$

ここで

- $\mathbb{L}$ は単位的環
- $\mathbb{L}_0$ は $\mathbb{L}$ の真の両側イデアル
- $\mathbb{G}_1$ は $\mathbb{L}$-両側加群

- $\mathbb{G}_0 = {}^{\mathbb{L}_0}\mathbb{G}_1^{\mathbb{L}_0}$ とし，

$$|\mathbb{G}_1|/|\mathbb{G}_0| \geq \mathtt{poly}(\lambda)$$

とする．

- $\mathtt{Eval}_{\mathtt{Rexp}}, \mathtt{Eval}_{\mathtt{Lexp}}$ は加群としてのスカラー倍 $\mathtt{Eval}_{\mathtt{Mul}}$ は加群としての和

lossy trapdoor algebra の injective instance と lossy instance が識別不能であるとは λ に関する如何なる確率的多項式時間アルゴリズム $\mathcal{A}$ に対しても

$$\mathsf{Adv}^{\mathcal{A}}(\lambda) := \left| \Pr\left[b = b^* \middle| \begin{array}{l} b \xleftarrow{\$} \{0,1\}; \\ (\mathbb{L}, \mathbb{G}_b, t) \xleftarrow{\$} \mathtt{Gen}(\lambda, b); \\ b^* \xleftarrow{\$} \mathcal{A}(\mathbb{L}, \mathbb{G}_b); \end{array} \right] - \frac{1}{2} \right|$$

が λ に関して無視可能なことである．上記の lossy trapdoor homomorphism の具体的構成は実際には lossy trapdoor algebra の構造を備えている．lossy trapdoor algebra の概念は subgroup membership problem [19] や subset membership problem の概念にかなり近い．

参考文献

[1] C. Peikert and B. Waters, “Lossy trapdoor functions and their applications,” IACR Cryptol. ePrint Arch., p.279, 2007. URL: http://eprint.iacr.org/2007/279.

[2] C. Peikert and B. Waters, “Lossy trapdoor functions and their applications,” Proceedings of the 40th Annual ACM Symposium on Theory of Computing, Victoria, British Columbia, Canada, May 17-20, 2008, ed. C. Dwork, pp.187–196, ACM, 2008. doi:10.1145/1374376.1374406.

[3] C. Peikert and B. Waters, “Lossy trapdoor functions and their applications,” SIAM J. Comput., vol.40, no.6, pp.1803–1844, 2011. doi:10.1137/080733954.

[4] R. Nishimaki, E. Fujisaki, and K. Tanaka, “Efficient Non-Interactive Universally Composable Commitment Schemes.” In *Proc. of SCIS 2009 2009 Symposium on Cryptography and Information Security 2009*. IEICE, 2009.

[5] R. Nishimaki, E. Fujisaki, and K. Tanaka, “An efficient non-interactive universally composable string-commitment scheme,” IEICE Trans. Fundam. Electron. Commun. Comput. Sci., vol.95-A, no.1, pp.167–175, 2012. doi:10.1587/transfun.E95.A.167.

[6] T. Matsuda, R. Nishimaki, and K. Tanaka, “CCA proxy re-encryption without bilinear maps in the standard model,” Public Key Cryptography - PKC 2010, 13th International Conference on Practice and Theory in Public Key Cryptography, Paris, France, May 26-28, 2010. Proceedings, ed. P.Q. Nguyen and D. Pointcheval, Lecture Notes in Computer Science, vol.6056, pp.261–278, Springer, 2010. doi:10.1007/978-3-642-13013-7_16.

[7] B. Hemenway and R. Ostrovsky, “Extended-ddh and lossy trapdoor functions,” Public Key Cryptography - PKC 2012 - 15th International Conference on Practice and Theory in Public Key Cryptography, Darmstadt, Germany, May 21-23, 2012. Proceedings, ed. M. Fischlin, J. Buchmann, and M. Manulis, Lecture Notes in Computer Science, vol.7293, pp.627–643, Springer, 2012. doi:10.1007/978-3-642-30057-8_37.

[8] B. Hemenway and R. Ostrovsky, “Building lossy trapdoor functions from lossy encryption,” Advances in Cryptology - ASIACRYPT 2013 - 19th International Conference on the Theory and Application of Cryptology and Information Security, Bengaluru, India, December 1-5, 2013, Proceedings, Part II, ed. K. Sako and P. Sarkar, Lecture Notes in Computer Science, vol.8270, pp.241–260, Springer, 2013. doi:10.1007/978-3-642-42045-0_13.

[9] B. Hemenway and R. Ostrovsky, “Building lossy trapdoor functions from lossy encryption,” IACR Cryptol. ePrint Arch., p.156, 2015. URL: http://eprint.iacr.org/2015/156.

[10] H. Xue, X. Lu, B. Li, and Y. Liu, “Lossy trapdoor relation and its applications to lossy encryption and adaptive trapdoor relation,” Provable Security - 8th International Conference, ProvSec 2014, Hong Kong, China, October 9-10, 2014. Proceedings, ed. S.S.M. Chow, J.K. Liu, L.C.K. Hui, and S. Yiu, Lecture Notes in Computer Science, vol.8782, pp.162–177, Springer, 2014. doi:10.1007/978-3-319-12475-9_12.

[11] H. Xue, Y. Liu, X. Lu, and B. Li, “Lossy pro-

jective hashing and its applications," Progress in Cryptology - INDOCRYPT 2015 - 16th International Conference on Cryptology in India, Bangalore, India, December 6-9, 2015, Proceedings, ed. A. Biryukov and V. Goyal, Lecture Notes in Computer Science, vol.9462, pp.64–84, Springer, 2015. doi:10.1007/978-3-319-26617-6_4.

[12] Z. Zhang, Y. Chen, S.S.M. Chow, G. Hanaoka, Z. Cao, and Y. Zhao, "All-but-one dual projective hashing and its applications," Applied Cryptography and Network Security - 12th International Conference, ACNS 2014, Lausanne, Switzerland, June 10-13, 2014. Proceedings, ed. I. Boureanu, P. Owesarski, and S. Vaudenay, Lecture Notes in Computer Science, vol.8479, pp.181–198, Springer, 2014. doi:10.1007/978-3-319-07536-5_12.

[13] T. Yamakawa, S. Yamada, G. Hanaoka, and N. Kunihiro, "Adversary-dependent lossy trapdoor function from hardness of factoring semi-smooth RSA subgroup moduli," Advances in Cryptology - CRYPTO 2016 - 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part II, ed. M. Robshaw and J. Katz, Lecture Notes in Computer Science, vol.9815, pp.3–32, Springer, 2016. doi:10.1007/978-3-662-53008-5_1.

[14] D. Hofheinz, "Circular chosen-ciphertext security with compact ciphertexts," Advances in Cryptology - EUROCRYPT 2013, 32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Athens, Greece, May 26-30, 2013. Proceedings, ed. T. Johansson and P.Q. Nguyen, Lecture Notes in Computer Science, vol.7881, pp.520–536, Springer, 2013. doi:10.1007/978-3-642-38348-9_31.

[15] B. Libert and C. Qian, "Lossy algebraic filters with short tags," Public-Key Cryptography - PKC 2019 - 22nd IACR International Conference on Practice and Theory of Public-Key Cryptography, Beijing, China, April 14-17, 2019, Proceedings, Part I, ed. D. Lin and K. Sako, Lecture Notes in Computer Science, vol.11442, pp.34–65, Springer, 2019. doi:10.1007/978-3-030-17253-4_2.

[16] 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.

[17] 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=.

[18] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," Advances in Cryptology — EUROCRYPT '99, ed. J. Stern, LNCS, vol.1592, pp.223–238, Springer-Verlag, 1999.

[19] A. Yamamura and T. Saito, "Private information retrieval based on the subgroup membership problem," ACISP, ed. V. Varadharajan and Y. Mu, Lecture Notes in Computer Science, vol.2119, pp.206–220, Springer, 2001.

[20] R. Cramer and V. Shoup, "Universal hash proofs and a paradigm for adaptive chosen ciphertext secure public-key encryption," Advances in Cryptology—EUROCRYPTO 2002, ed. L. Knudsen, LNCS, vol.2332, pp.45–64, Springer-Verlag, 2002.