Efficient Lossy Trapdoor Functions based on Subgroup Membership Assumptions

Haiyang Xue, Bao Li, Xianhui Lu, Dingding Jia, Yamin Liu

Institute of Information Engineering , Chinese Academy of Sciences

2013.11.21

Outline

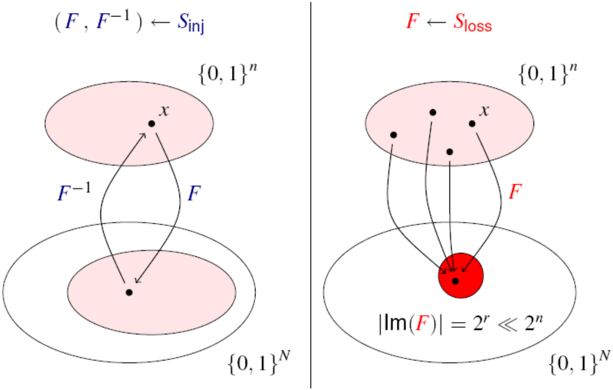
Lossy Trapdoor Function (LTDF)

Peikert and Waters proposed the LTDF in STOC 2008.

$$DDH,\ LWE \rightarrow \color{red}{LTDF} \rightarrow \begin{cases} TDF,\ Hard\ Core; \\ OT; \\ CR\ Hash; \\ CCA, \ldots \end{cases}$$

Lossy Trapdoor Function [PW'08]

From Peikert's slides



$$F \overset{c}{\approx} F$$

Definition of LTDF

Injective model

- $(s, t) \leftarrow S_{inj}(1^n)$;
- $F_{ltdf}(s, \cdot) : \{0,1\}^m \rightarrow \{0,1\}^*$
- $F_{ltdf}^{-1}(t, F_{ltdf}(s, x)) = x$.

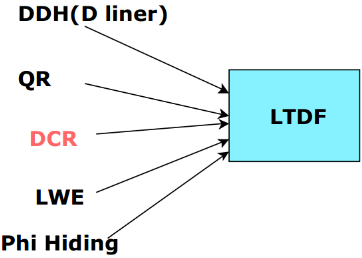
Lossy with l bits

- $s \leftarrow S_{loss}(1^n)$;
- $F_{ltdf}(s, \cdot) : \{0,1\}^m \rightarrow \{0,1\}^*$
- $F_{ltdf}(s, \cdot)$ has size at most 2^{m-l};

$$\{s : s \leftarrow S_{lossy}\} \overset{c}{\approx} \{s : (s, t) \leftarrow S_{inj}\}.$$

Constructions of LTDF

- DDH or d-liner [PW'08],[FGKRS'10], [Wee12];
- QR assumption [FGKRS'10],[JL'13], [Wee12]
- DCR assumption [BFO'08], [FGKRS'10], [Wee12]
- LWE assumption [PW'08],[Wee12]
- Φ-Hiding [KOS'10].



The DCR based construction is one of the most efficient constructions.

DCR Assumption [Pai99, Dam01]

Definition

Let $N = pq$ for $p = 2p' + 1$, $q = 2q' + 1$ and $s \geq 2$

$$P := \{a = x^{N^{s-1}} \mod N^s | x \in \mathbb{Z}_N^*\},$$

$$M := \{a = (1+N)^y x^{N^{s-1}} \mod N^s | x \in \mathbb{Z}_N^*, y \in \mathbb{Z}_{N^{s-1}}\}.$$

$$\{a \leftarrow P\} \stackrel{c}{\approx} \{a \leftarrow M\}$$

1. N^{s-1}-th residuosity is a subgroup with order $2p'q' \approx N/2$.
2. For a in M,
$$a^{2p'q'} = 1 + y2p'q'N \mod N^s.$$

DCR Based LTDF

For input $m \in [0, N^{s-1}]$, the two function models follow:

Injective model	*Lossy model*
$\{(1+N)x^{N^{s-1}}\}^m$	$\{x^{N^{s-1}}\}^m$

- $G_{N^{s-1}} = H \times K =< (1+N) > \times \{x^{N^{s-1}}\}$
- *$s \geq 3$ in order to make enough lossiness.*

Motivation

General Subgroup membership assumption $\xrightarrow{\ ?\ }$ *LTDF*

$$\bmod N^3 \xrightarrow{\ ?\ } \bmod N^2 \xrightarrow{\ ?\ } \bmod N$$

Outline

Our Contribution

Subgroup membership assumption + 2 Properties $\xrightarrow{\checkmark}$ *LTDF*

$$\bmod N^3 \xrightarrow{\checkmark} \bmod N^2 \xrightarrow{\checkmark} \bmod N$$

Shrinking the subgroup or Enlarging the quotient group.

Subgroup Membership Assumption [Gjϕsteen 05]

Definition (SMA)

Let G be a finite cyclic group.

$$G =< g >= G/K \times K = G/K\times < h >$$

The subgroup membership assumption $SM_{(G,K)}$ asserts that,

$$\{x, x \leftarrow K\} \stackrel{c}{\approx} \{x, x \leftarrow G \setminus K]\}.$$

$$\mathbb{Z}^*_{N^s} =< (1+N) \times \{x^{N^{s-1}}\} > .$$

2 Properties

1. $SDL_{(G,K,g)}$ is easy with a trapdoor t;
2. $|G/K| \gg |K|$. (Lossy property)

Definition (Subgroup Discrete Logarithm Problem [Gjϕsteen 05])

If $\varphi : G \to G/K$ is the canonical epimorphism, then $SDL_{(G,K,g)}$ is:

To compute $\log_{\varphi(g)}(\varphi(x))$ for $x \leftarrow G$.

$$(1+N)^y z^{N^{s-1}} \to y?$$

Generic construction

Let (G, K, g, h, t) be an instance of $SM_{(G,K)}$ with 2 properties. For $m \in [0, |G/K|]$, the two models follow,

Injective model

1. $a = gh^r$ *for* $r \leq |K|$ *and t=t;*
2. $F_{ltdf}(a, m) = a^m = [gh^r]^m$
3. *Recover* m *by solving* $SDL_{(G,K,g)}$ *with* t.

Lossy model

1. $a = h^r$ *for* $r \leq |K|$*;*
2. $F_{ltdf}(a, m) = a^m = [h^r]^m$
3. $|F_{ltdf}(a, \cdot)| < |K|$ *as* $F_{ltdf}(a, \cdot)$ *falls into* K *;*

SMA$\Rightarrow$ LTDF

Theorem (1 in page 240)

If the $SM_{G,K}$ with two above properties holds, This is an $(\log|G/K|, \log|G/K| - \log|K|)$ *LTDF.*

DCR& QR based LTDF

Let $N = pq$ with $p = 2^k p' + 1, q = 2^k q' + 1$.

- *For* $y \in QNR_N$*, let* $G =< (1+N)y^N >$ *with order* $N2^k p'q'$*;*
- *For* $h_1 \in \mathbb{Z}_N^*$*, let* $K =< h_1^{2^k N} >$ *with order* $p'q'$*.*

Theorem (3 in page 243)

$$DCR\&QR \Rightarrow SM_{(G,K)}.$$

Extended p-subgroup based LTDF

Let $N = p^2 q$ with $p = 2p' + 1, q = 2q' + 1$, For $y \in \mathbb{Z}_N^*$, Let $h = y^{2N^2}$

- *Let* $G =< (1 + N)h >$ *with order* $Np'q'$*;*
- *Let* $K =< h >$ *with order* $p'q'$*.*

$SM_{(G,K)}$ is a generalization of p subgroup in [OU98]

Decisional RSA [Groth 05] based LTDF

Let $N = pq$ with $p = 2p'r_p + 1, q = 2q'r_q + 1$, Let r_p, r_q be B-smooth with t distinct prime factors and $l \approx \log B$.

For $x \in \mathbb{Z}_N^*$, let $h = x^{2r_pr_q}$ and $g \leftarrow QR_N$.

- *Let $G =< g >$ with order larger than $p'q'2^{(t-d)(l-1)}$;*
- *Let $K =< h >$ with order $p'q'$.*

This $SM_{(G,K)}$ assumption is the Decisional RSA assumption in [Groth 05].

Outline

Comparison with previous constructions

Assumption	Input size	Lossiness	Index size	Efficiency
DDH	n	$n - \|\mathbb{G}\|$	$n^2\mathbb{G}$	n^2 Multi
LWE	n	cn	$n(d+w)\mathbb{Z}_q$	$n(d+w)$ Multi
d-linear	n	$n - d\|\mathbb{G}\|$	$n^2\mathbb{G}$	n^2 Multi
QR	$\log N$	1	$\mathbb{Z}_N^*$	1 Multi
DDH& QR	n	$n - \log N$	$(\frac{n}{k})^2\mathbb{Z}_N^*$	$(\frac{n}{k})^2$ Multi
Φ-hiding	$\log N$	$\log e$	$\mathbb{Z}_N^*$	$\log e \log N$
DCR	$2\log N$	$\log N$	$\mathbb{Z}_{N^3}^*$	$3\log x \log N$
QR & DCR	$\frac{9}{8}\log N$	$\frac{3}{8}\log N$	$\mathbb{Z}_{N^2}^*$	$2\log x \log N$
E p-sub	$\log N$	$\frac{1}{3}\log N$	$\mathbb{Z}_{N^2}^*$	$2\log x \log N$
D RSA	l_x	$l_x - l_{p'} - l_{q'}$	$\mathbb{Z}_N^*$	$\log x \log N$

$l_x \leq 698, l_{p'} = l_{q'} = 160$

Conclusion

We present a generic construction of LTDFs from subgroup membership assumptions.

We give three efficient constructions based on

1. DCR & QR;
2. Extended p Subgroup;
3. Decisional RSA.

Thank you