Lossy Trapdoor Functions & Their Applications

Chen, Fei
2012.12.07
Reading


- CCA secure PKE
  - Naor-Young PKE cryptosystem based on NIZK
  - Dwork-Naor non-malleable PKE
Outline

- Lossy trapdoor functions
  - Backgrounds
  - Definitions
- One Construction based on DDH
- Applications
  - One-way functions
  - Hard-core bits & pseudorandom number generators
  - Collision resistant hash functions
  - CPA & CCA cryptosystem
- Future work
Definitions
Background

- One-way functions vs. one-way trapdoor functions
- One-way permutation vs. one-way trapdoor permutations

Instantiation
- RSA function (IF)
- Paillier cryptosystem (IF)
- Lattice trapdoors (LWE)

Inspiration:
- LWE based cryptosystems
- CCA security
Definition

- Syntactically, a \((n, k)\) lossy trapdoor function includes three PPT algorithms \((S_{\text{ltdf}}, F_{\text{ltdf}}, F_{\text{ltdf}}^{-1})\):
  - **Injective mode**: easy to sample and compute
    \[ S_{\text{ltdf}}(1^n, 1) \rightarrow (s, t); \quad y = F_{\text{ltdf}}(s, x); \quad x = F_{\text{ltdf}}^{-1}(t, y) \]
  - **Lossy mode**: easy to sample and compute
    \[ S_{\text{ltdf}}(1^n, 0) \rightarrow (s, \perp); \quad y = F_{\text{ltdf}}(s, x); \text{ image size } 2^r = 2^{n-k} \]
  - **In-distinguishibility**: first output \( S_{\text{ltdf}}(1^n, 1) \approx S_{\text{ltdf}}(1^n, 0) \)

Discussion

- For a definition, no single item should imply another.
- Hard to invert
All-but-one TDFs

- **Goal:** to have many branches, but not only 2
- **Syntactically:** \((S_{abo}, G_{abo}, G_{abo}^{-1})\):
  - Almost the same as \((S_{ltdf}, F_{ltdf}, F_{ltdf}^{-1})\), except the many branches
  - Let a string \(b^*\) denote the lossy branch. \(S_{abo}(b^*)\) outputs a lossy TDF; for other \(b\)'s, outputs normal TDFs.
  - In-distinguishibility: first output \(S_{abo}(1^n, b^*) \approx S_{abo}(1^n, b)\)

- **Equivalence to LTDF**
  - Reduction to each other
One Construction Based on DDH
Basic idea

- Let $xM$ be an input and $M$ be a matrix.
  - If $M = I$, $xM = x$, i.e. no information is lost.
  - If $M = 0$, $xM = 0$, i.e. substantial information is lost.
- We can also implement all the above vector-matrix operations in the ciphertext manner, i.e. homomorphically.
- Additive homomorphism.

- ElGamal PKE with a little modification: $\text{Enc}(m; r) = (g^r, g^m \cdot g^r)$
Details

- **Sampling**
  - Function index: $M$
  - Injective model: $M = I$
  - Lossy mode: $M = 0$

- **Evaluation**
  - $F_{ltdf}(M, x) = Enc(xM; r)$

- **Inversion**
  - ElGamal decryption
Construction based on LWE

- Same idea
- Simplified Regev PKE with additive homomorphism

I cannot fully understand the construction. For details, please refer to the paper.
Applications
One-way trapdoor function

- Just use the injective mode to sample a TDF

- To prove it is indeed a TDF, we need to show:
  - Easy to compute
  - Hard to convert

- Proof idea: to construct a distinguisher for the injective mode with the lossy mode.
Hard-core bits

- Definition: A hard-core bit function for $f: \{0,1\}^n \rightarrow \{0,1\}^*$ is a function $h: \{0,1\}^n \rightarrow \{0,1\}^l$ if
  \[
  \left(x \leftarrow \{0,1\}^n: f(x), h(x) \right) \approx \left(x \leftarrow \{0,1\}^n, r \leftarrow \{0,1\}^l: f(x), r \right)
  \]

- Construction based on randomness extractors
  - Let $h$ be a pair-wise independent hash function
  - Hard-core bit: $h(x)$

- Proof idea
  - Goal: $(s, h, F_{\text{ltdf}}(s, x), h(x)) \approx (s, h, F_{\text{ltdf}}(s, x), r)$
  - Tool: leftover hash lemma

- Implications: pseudorandom number generators
Collision resistant hash functions

- Let $\mathcal{H} = \{h: \{0,1\}^n \to \{0,1\}^{kn}\}$ be an universal hash function, i.e. $\forall y, y' \in \{0,1\}^n, \Pr[h(y) = h(y')] = \frac{1}{2^{kn}}$.

- Construction
  - Sample: $h \leftarrow \mathcal{H}, (s, t) \leftarrow S(1^n, \cdot)$
  - Evaluation: $h(F_{\text{ltdf}}(s, x))$, i.e. map $\{0,1\}^n$ to $\{0,1\}^{kn}$

- Proof idea
  - If $F_{\text{ltdf}}$ is in injective model, collisions happen at $h$
  - If $F_{\text{ltdf}}$ is in lossy model, collisions happen at $F_{\text{ltdf}}$ by design, i.e.
    $\Pr[\exists y \neq y' \ h(y) = h(y')] \leq 2^{2\rho n} \times 2^{-kn} = 2^{(2\rho - \kappa) n} = \text{negl}(n)$, where $\rho n = r, 2\rho < \kappa$
  - Distinguish two modes
CPA Secure PKE

- Traditional idea
  - Set up the ciphertext format such that an adversary cannot find an unknown legal ciphertext
- New idea here: modify the challenge ciphertext

- CPA secure PKE
  - Public key: \((s, h)\); secret key: \(t\)
  - Encryption: \((F_{\text{tdf}}(x), m \oplus h(x))\)
  - Decryption: first recover the randomness \(r\), then recover the message
CCA2 Secure PKE

- Public key: \((s, s', h)\); private key: \((t, t')\)
- Encryption: \((vk, F_{\text{ltdf}}(s, x), G_{\text{abo}}(s', vk, x), m \oplus h(x), \sigma)\)
- Decryption
  - Check the signature
  - Recover the randomness and check its correctness
  - If OK, then recover the message
- Proof idea
  - Modify the challenge ciphertext, such that \(G_{\text{abo}}(s', vk, x)\) is in lossy mode. In this case, the ciphertext statistically hides the message.
  - By in-distinguishability of the injective mode and the lossy mode, the PKE is CCA2 secure.
Future Work
Work that we can do

- Construct new lossy TDFs based on various assumptions
  - Efficiency
  - Other homomorphism
- CCA secure PKE based on lattices
  - From abstract constructions to instantiations. Note that we may utilize some special properties of the underlying problem to simplify the abstract construction.
- Construct other cryptographic primitives based on lossy TDFs
  - Selective opening secure encryption schemes
  - Leakage resistant schemes
  - …