Perfect structure on the edge of chaos

Nir Bitansky, Omer Paneth, Daniel Wichs

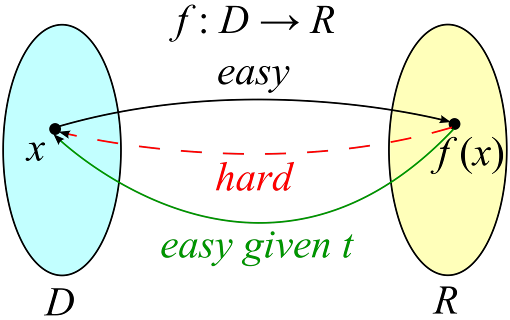
April, 2024

Results

1. OWF + iO $\implies$ iOWF
2. OWF + sub-exponential iO $\implies$ TDP

Results

1. OWF + iO $\implies$ iOWF
2. OWF + sub-exponential iO $\implies$ TDP



Why these results are interesting

OWF + iO $\implies$ iOWF
OWF + sub-exponential iO $\implies$ TDP

- **Minimizing assumptions** Ex: from BPR+GPS paper presented by Mark and Ashvin, we know that iOWF + iO $\implies$ hardeness of SVL
  Using the first result: OWF + iO $\implies$ hardness of SVL
- Technique used to prove the second result relies on techniques developed in BRP to construct hard instance of SVL
- Perfect structure on the edge of chaos?
- Previous TDP candidates would all be broken if factoring is broken/in SZK $\implies$ gives new direction to build TDP (assuming we can build iO)

First result

OWF + iO $\implies$ iOWF

Two steps:

1. OWF $\implies$ SIOWF
2. SIOWF + iO $\implies$ iOWF

SIOWF

Definition: Sometime injective OWF

$SIOWF = \{f_K : \{0,1\}^n \to \{0,1\}^*, K \in \{0,1\}^{k(n)}\}$

$\forall K, \exists I_K$ such that $\forall x \in I_K, f^{-1}(f(x)) = \{x\}$

SIOWF

Definition: Sometime injective OWF

$SIOWF = \{f_K : \{0,1\}^n \to \{0,1\}^*, K \in \{0,1\}^{k(n)}\}$

$\forall K, \exists I_K$ such that $\forall x \in I_K, f^{-1}(f(x)) = \{x\}$

1. Sometimes injectiveness:

$$\mathbb{P}_{K,x}(x \in I_K) \geq \frac{1}{p(n)}$$

SIOWF

OWF $\implies$ SIOWF

Definition: Sometime injective OWF

$SIOWF = \{f_K : \{0,1\}^n \to \{0,1\}^*, K \in \{0,1\}^{k(n)}\}$

$\forall K, \exists I_K$ such that $\forall x \in I_K, f^{-1}(f(x)) = \{x\}$

1. Sometimes injectiveness:

$$\mathbb{P}_{K,x}(x \in I_K) \geq \frac{1}{p(n)}$$

2. One-wayness over injective subdomain

Construction of *SIOWF*

OWF $\Longrightarrow$ SIOWF

Let $g : \{0,1\}^* \to \{0,1\}^*$ be a OWF

Construction of *SIOWF*

Let $g : \{0,1\}^* \to \{0,1\}^*$ be a OWF

- $K = (S, e)$ where $e \leftarrow [n]$ and S is a random seed for a hash function $h_S : \{0,1\}^n \to \{0,1\}^{e+1}$ in a n-wise independant family of hash functions.
  (can be instantiated using degree n polynomial over some large field, see appendix)

Construction of *SIOWF*

Let $g : \{0,1\}^* \to \{0,1\}^*$ be a OWF

- $K = (S, e)$ where $e \leftarrow [n]$ and S is a random seed for a hash function $h_S : \{0,1\}^n \to \{0,1\}^{e+1}$ in a n-wise independant family of hash functions.
  (can be instantiated using degree n polynomial over some large field, see appendix)
- $f_K(x) = (g(x), h_S(x))$

Construction of *IOWF*

SIOWF + iO $\implies$ iOWF

Ingredients:

- iO (for P/poly)
- *PRF* a family of puncturable PRFs *(known from OWF)*
- (COM_1, COM_2) a two message perfectly binding commitment scheme *(known from OWF)*

Puncturable PRF

SIOWF + iO $\Longrightarrow$ iOWF

$PRF = \{f_S : \{0,1\}^{p(n)} \to \{0,1\}^n, S \in \{0,1\}^{q(n)}\}$

With poly-time algo $\mathsf{Punc}(S, x)$ that outputs a punctured key S_x such that:

Puncturable PRF

SIOWF + iO $\Longrightarrow$ iOWF

$PRF = \{f_S : \{0,1\}^{p(n)} \to \{0,1\}^n, S \in \{0,1\}^{q(n)}\}$

With poly-time algo Punc(S, x) that outputs a punctured key S_x such that:

1. Functionality is preserved under puncturing: $\forall x^*$:

$$\mathbb{P}_{S \leftarrow \kappa(1^n)}(\forall x \neq x^*, f_S(x) = f_{S_{x^*}}(x)) = 1$$

Puncturable PRF

$PRF = \{f_S : \{0,1\}^{p(n)} \to \{0,1\}^n, S \in \{0,1\}^{q(n)}\}$

With poly-time algo Punc(S, x) that outputs a punctured key S_x such that:

1. Functionality is preserved under puncturing: $\forall x^*$:

$$\mathbb{P}_{S \leftarrow \kappa(1^n)}(\forall x \neq x^*, f_S(x) = f_{S_{x^*}}(x)) = 1$$

2. Indistinguishability at punctured points:

$$|\mathbb{P}(D(x^*, S_{x^*}, f_S(x^*)) = 1) - \mathbb{P}(D(x^*, S_{x^*}, u) = 1)| \leq \text{negl}$$

where $S \leftarrow \kappa(1^n)$ and $u \leftarrow \{0,1\}^n$

Commitment scheme

SIOWF + iO $\implies$ iOWF

Method that allows a user to commit to a value while keeping it hidden, and while preserving the user's ability to reveal the committed value later (takes randomness as input).

Commitment scheme

SIOWF + iO $\implies$ iOWF

Method that allows a user to commit to a value while keeping it hidden, and while preserving the user's ability to reveal the committed value later (takes randomness as input).

2 properties:

1. **Hiding**: It should be hard to distinguish between a commitment to x and to y:

$$C_r(y) \simeq C_r(x)$$

Commitment scheme

SIOWF + iO $\Longrightarrow$ iOWF

Method that allows a user to commit to a value while keeping it hidden, and while preserving the user's ability to reveal the committed value later (takes randomness as input).

2 properties:

1. **Hiding**: It should be hard to distinguish between a commitment to x and to y:

$$C_r(y) \simeq C_r(x)$$

2. **Binding**: There should be no way for a person who commits to one bit, to claim that he has committed to another value later:

$$\text{Cannot find } r_0, r_1 \text{ such that } C_{r_0}(x) = C_{r_1}(y)$$

2 message commitment scheme

SIOWF + iO $\implies$ iOWF

1. COM_1 samples message $M_1 \leftarrow \mathsf{COM}_1(1^n)$

2 message commitment scheme

SIOWF + iO $\Longrightarrow$ iOWF

1. COM_1 samples message $M_1 \leftarrow \mathrm{COM}_1(1^n)$
2. COM_2 outputs a commitment M_2 to plaintext $x \in \{0,1\}^n$ with respect to M_1 and randomness r:
   $M_2 \leftarrow \mathrm{COM}_2(x, M_1, r)$

2 message commitment scheme

SIOWF + iO $\implies$ iOWF

1. COM_1 samples message $M_1 \leftarrow \mathrm{COM}_1(1^n)$
2. COM_2 outputs a commitment M_2 to plaintext $x \in \{0,1\}^n$ with respect to M_1 and randomness r:
   $M_2 \leftarrow \mathrm{COM}_2(x, M_1, r)$

The 2 message commitment scheme that we will be using is perfectly binding (used to prove injectiveness) and computationally hiding (used to prove one-wayness)

Existence of such a scheme from PRG
We use 2 messages for the perfectly binding condition (see appendix).

Nir Bitansky, Omer Paneth, Daniel Wichs

Construction of *IOWF*

SIOWF + iO $\implies$ iOWF

The function family:

For $M_1 \leftarrow COM_1(1^n), S \leftarrow \kappa(1^n)$, let $C_{M_1,S} : \{0,1\}^n \to \{0,1\}^*$

$$C_{M_1,S}(x) = COM_2(x, M_1, f_S(x))$$

Construction of *IOWF*

SIOWF + iO $\implies$ iOWF

The function family:

For $M_1 \leftarrow COM_1(1^n), S \leftarrow \kappa(1^n)$, let $C_{M_1,S} : \{0,1\}^n \to \{0,1\}^*$

$$C_{M_1,S}(x) = COM_2(x, M_1, f_S(x))$$

- Key $K = \tilde{C} \leftarrow iO(C_{M_1,S})$
- The function is given by $OWF_K(x) = \tilde{C}(x)$

Proof intuition

SIOWF + iO $\implies$ iOWF

$$C_{M_1,S}(x) = COM_2(x, M_1, f_S(x))$$

Injectivity follows from the fact that the commitment scheme is perfectly binding.

Proof intuition

SIOWF + iO $\implies$ iOWF

$$C_{M_1,S}(x) = COM_2(x, M_1, f_S(x))$$

Injectivity follows from the fact that the commitment scheme is perfectly binding.

If we had VBB obfuscation instead of $iO \implies$ same as interacting with black-box version of C with true randomness.

Proof of (weak) one wayness

SIOWF + iO $\implies$ iOWF

First step: We define a new circuit:
Let $S_{x^*} = \mathrm{Punc}(S, x^*)$

$$C_1(x) = \begin{cases} \mathrm{COM}_2(x, M_1, f_{S_{x^*}}(x)) & \text{if } x \neq x^* \\ \mathrm{COM}_2(x^*, M_1, f_S(x^*)) & \text{if } x = x^* \end{cases}$$

By the iO guarantee:

$$p_1 = |\mathbb{P}(A(\tilde{C}, \tilde{C}(x^*)) = x^*) - \mathbb{P}(A(\tilde{C}_1, \tilde{C}_1(x^*)) = x^*)| \leq \mathrm{negl}$$

Proof of (weak) one wayness

SIOWF + iO $\Longrightarrow$ iOWF

Second step: We define a new circuit:

$$C_2(x) = \begin{cases} \mathsf{COM}_2(x, M_1, f_{S_{x^*}}(x)) & \text{if } x \neq x^* \\ \mathsf{COM}_2(x^*, M_1, r) & \text{if } x = x^* \end{cases}$$

with $r \leftarrow \{0,1\}^n$

Proof of (weak) one wayness

SIOWF + iO $\implies$ iOWF

Second step: We define a new circuit:

$$C_2(x) = \begin{cases} \mathrm{COM}_2(x, M_1, f_{S_{x^*}}(x)) & \text{if } x \neq x^* \\ \mathrm{COM}_2(x^*, M_1, r) & \text{if } x = x^* \end{cases}$$

with $r \leftarrow \{0,1\}^n$

By pseudorandomness at punctured points:

$$p_2 = |\mathbb{P}(A(\tilde{C}_1, \tilde{C}_1(x^*)) = x^*) - \mathbb{P}(A(\tilde{C}_2, \tilde{C}_2(x^*)) = x^*)| \leq \text{negl}$$

Proof of (weak) one wayness

Third step: We define a new circuit:

$$C_3(x) = \begin{cases} \mathrm{COM}_2(x, M_1, f_{S_{x^*}}(x)) & \text{if } x \neq x^* \\ \mathrm{COM}_2(0^n, M_1, r) & \text{if } x = x^* \end{cases}$$

with $r \leftarrow \{0,1\}^n$

Proof of (weak) one wayness

SIOWF + iO $\implies$ iOWF

Third step: We define a new circuit:

$$C_3(x) = \begin{cases} \mathrm{COM}_2(x, M_1, f_{S_{x^*}}(x)) & \text{if } x \neq x^* \\ \mathrm{COM}_2(0^n, M_1, r) & \text{if } x = x^* \end{cases}$$

with $r \leftarrow \{0,1\}^n$

By the computational hiding of the commitment:

$$p_3 = |\mathbb{P}(A(\tilde{C}_2, \tilde{C}_2(x^*)) = x^*) - \mathbb{P}(A(\tilde{C}_3, \tilde{C}_3(x^*)) = x^*)| \leq \mathrm{negl}$$

Proof of (weak) one wayness

SIOWF + iO $\implies$ iOWF

Fourth step: We define a new circuit:

$$C_4(x) = \begin{cases} \mathsf{COM}_2(x, M_1, f_S(x)) & \text{if } x \neq x^* \\ \mathsf{COM}_2(0^n, M_1, r) & \text{if } x = x^* \end{cases}$$

with $r \leftarrow \{0,1\}^n$

Proof of (weak) one wayness

SIOWF + iO $\implies$ iOWF

Fourth step: We define a new circuit:

$$C_4(x) = \begin{cases} \mathrm{COM}_2(x, M_1, f_S(x)) & \text{if } x \neq x^* \\ \mathrm{COM}_2(0^n, M_1, r) & \text{if } x = x^* \end{cases}$$

with $r \leftarrow \{0,1\}^n$

By the iO guarantee:

$$p_4 = |\mathbb{P}(A(\tilde{C}_3, \tilde{C}_3(x^*)) = x^*) - \mathbb{P}(A(\tilde{C}_4, \tilde{C}_4(x^*)) = x^*)| \leq \mathrm{negl}$$

Proof of (weak) one wayness

SIOWF + iO $\implies$ iOWF

Fifth step: We define a new circuit:
Let *SIOWF* be a family of sometime injective one way functions with efficient key sampler κ'.
Let $K' \leftarrow \kappa'(1^n)$ and $g_{K'}$ the associated SIOWF.

If $x^* \in I_{K'}$:

$$C_5(x) = \begin{cases} \mathrm{COM}_2(x, M_1, f_S(x)) & \text{if } g_{K'}(x) \neq g_{K'}(x^*) \\ \mathrm{COM}_2(0^n, M_1, r) & \text{if } g_{K'}(x) = g_{K'}(x^*) \end{cases}$$

with $r \leftarrow \{0,1\}^n$
Else: $C_5 = C_4$

Proof of (weak) one wayness

SIOWF + iO $\implies$ iOWF

Fifth step: We define a new circuit:
Let *SIOWF* be a family of sometime injective one way functions with efficient key sampler κ'.
Let $K' \leftarrow \kappa'(1^n)$ and $g_{K'}$ the associated SIOWF.

If $x^* \in I_{K'}$:

$$C_5(x) = \begin{cases} \mathrm{COM}_2(x, M_1, f_S(x)) & \text{if } g_{K'}(x) \neq g_{K'}(x^*) \\ \mathrm{COM}_2(0^n, M_1, r) & \text{if } g_{K'}(x) = g_{K'}(x^*) \end{cases}$$

with $r \leftarrow \{0,1\}^n$
Else: $C_5 = C_4$

By injectiveness of $g_{K'}$ over $I_{K'}$,

$$p_5 = |\mathbb{P}(A(\tilde{C}_4, \tilde{C}_4(x^*)) = x^*) - \mathbb{P}(A(\tilde{C}_5, \tilde{C}_5(x^*)) = x^*)| \leq \text{negl}$$

Proof of (weak) one wayness

SIOWF + iO $\implies$ iOWF

Finally,

$$
\begin{aligned}
p &= \mathbb{P}(A(\tilde{C}_5, \tilde{C}_5(x^*) = x^*) \\
&\leq \mathbb{P}(A(\tilde{C}_5, \tilde{C}_5(x^*)) = x^* \cap x^* \in I_{K'}) + \mathbb{P}(x^* \notin I_{K'}) \\
&\leq \mathbb{P}(A(g_{K'}(x^*)) = x^* \cap x^* \in I_{K'}) + \mathbb{P}(x^* \notin I_{K'}) \\
&\leq \mathrm{negl} + 1 - \frac{1}{p(n)}
\end{aligned}
$$

Proof of (weak) one wayness

SIOWF + iO $\implies$ iOWF

Finally,

$$
\begin{aligned}
p &= \mathbb{P}(A(\tilde{C}_5, \tilde{C}_5(x^*) = x^*) \\
&\leq \mathbb{P}(A(\tilde{C}_5, \tilde{C}_5(x^*)) = x^* \cap x^* \in I_{K'}) + \mathbb{P}(x^* \notin I_{K'}) \\
&\leq \mathbb{P}(A(g_{K'}(x^*)) = x^* \cap x^* \in I_{K'}) + \mathbb{P}(x^* \notin I_{K'}) \\
&\leq \text{negl} + 1 - \frac{1}{p(n)} \text{ So,}
\end{aligned}
$$

$$
\begin{aligned}
\mathbb{P}(A(\tilde{C}, \tilde{C}(x^*)) \neq x^*) &\geq 1 - (p_1 + p_2 + p_3 + p_4 + p_5 + p) \\
&\geq \frac{1}{p(n)} - \text{negl}
\end{aligned}
$$

So, our construction is weakly one way.

Proof of (weak) one wayness

SIOWF + iO $\implies$ iOWF

Finally,

$$p = \mathbb{P}(A(\tilde{C}_5, \tilde{C}_5(x^*) = x^*)$$
$$\leq \mathbb{P}(A(\tilde{C}_5, \tilde{C}_5(x^*)) = x^* \cap x^* \in I_{K'}) + \mathbb{P}(x^* \notin I_{K'})$$
$$\leq \mathbb{P}(A(g_{K'}(x^*)) = x^* \cap x^* \in I_{K'}) + \mathbb{P}(x^* \notin I_{K'})$$
$$\leq \text{negl} + 1 - \frac{1}{p(n)} \text{ So,}$$

$$\mathbb{P}(A(\tilde{C}, \tilde{C}(x^*)) \neq x^*) \geq 1 - (p_1 + p_2 + p_3 + p_4 + p_5 + p)$$
$$\geq \frac{1}{p(n)} - \text{negl}$$

So, our construction is weakly one way.

We can boost it to standard OWF using known techniques.

Results

1. OWF + iO $\implies$ iOWF (what we just showed)
2. OWF + sub-exponential iO $\implies$ TDP (what we will show next)

BRP paper

Constructed hard instance of SVL problem:

$$x_1 \to x_2 \to \cdots \to x_T$$

Program F mapping x_i to x_{i+1} with $x_i = (i, \mathsf{PRF}_S(i))$

BRP paper

Constructed hard instance of SVL problem:

$$x_1 \to x_2 \to \cdots \to x_T$$

Program F mapping x_i to x_{i+1} with $x_i = (i, \mathsf{PRF}_S(i))$

In class, Mark showed that:
VBB obfuscation + iOWF $\implies$ hard to find x_T given x_1 and obfuscated instance of F
(proof harder if we use iO instead, usually introduce punctured functions)

BRP paper

Constructed hard instance of SVL problem:

$$x_1 \to x_2 \to \cdots \to x_T$$

Program F mapping x_i to x_{i+1} with $x_i = (i, \mathrm{PRF}_S(i))$

In class, Mark showed that:
VBB obfuscation + iOWF $\implies$ hard to find x_T given x_1 and obfuscated instance of F
(proof harder if we use iO instead, usually introduce punctured functions)

We can similarly show:
VBB obfuscation + iOWF $\implies$ hard to find x_{i-1} given x_i and obfuscated instance of F

Candidate permutation

IOWF + iO $\implies$ TDP

Natural candidates for trapdoor permutation:

$$x_1 \to x_2 \to \cdots \to x_T \to x_1$$

PK: obfuscated instance of F
SK: seed S of pseudorandom function

Candidate permutation

IOWF + iO $\implies$ TDP

Natural candidates for trapdoor permutation:

$$x_1 \to x_2 \to \cdots \to x_T \to x_1$$

PK: obfuscated instance of F
SK: seed S of pseudorandom function

Problem: Not easy to sample random domain elements

Plan

IOWF + iO $\implies$ TDP

1. Use result 1 to get iOWF and apply BPR construction
2. Use BRP + add additional sampler to get TDP

Definition

IOWF + iO $\implies$ TDP

$TDP = \{f_{PK} : D_{PK} \to D_{PK}, PK \in \{0,1\}^{k(n)}, n \in \mathbb{N}\}$ associated with efficient (probabilistic) key and domain samplers (κ, ζ), is a (standard) TDP if it satisfies:

Definition

$TDP = \{f_{PK} : D_{PK} \to D_{PK}, PK \in \{0,1\}^{k(n)}, n \in \mathbb{N}\}$ associated with efficient (probabilistic) key and domain samplers (κ, ζ), is a (standard) TDP if it satisfies:

- **Trapdoor invertibility**: For any (PK, SK) in the support of $\kappa(1^n)$, the function f_{PK} is a permutation of a corresponding domain D_{PK}. The inverse $f_{PK}^{-1}(y)$ can be efficiently computed for any $y \in D_{PK}$, using the trapdoor SK.

Definition

$TDP = \{f_{PK} : D_{PK} \to D_{PK}, PK \in \{0,1\}^{k(n)}, n \in \mathbb{N}\}$ associated with efficient (probabilistic) key and domain samplers (κ, ζ), is a (standard) TDP if it satisfies:

- **Trapdoor invertibility**: For any (PK, SK) in the support of $\kappa(1^n)$, the function f_{PK} is a permutation of a corresponding domain D_{PK}. The inverse $f_{PK}^{-1}(y)$ can be efficiently computed for any $y \in D_{PK}$, using the trapdoor SK.
- **One wayness** over the domain D_{PK}

Definition

IOWF + iO $\implies$ TDP

- **Domain sampling**:

$$|\mathbb{P}\left(D(x,r)=1 : \begin{cases} r \leftarrow \{0,1\}^{\mathsf{poly}(n)} \\ (PK,SK) \leftarrow \kappa(1^n, r) \\ x \leftarrow \zeta(PK) \end{cases}\right) -$$

$$\mathbb{P}\left(D(x,r)=1 : \begin{cases} r \leftarrow \{0,1\}^{\mathsf{poly}(n)} \\ (PK,SK) \leftarrow \kappa(1^n, r) \\ x \leftarrow D_{PK} \end{cases}\right)| \leq \mathsf{negl}$$

Intuition for domain sampler

We would like to be able to sample $(i, PRF_S(i))$ uniformly:

- First attempt: have an additional obfuscated function that on input i outputs $PRF_S(i)$
  Problem: then it's easy to find any $x_i \implies$ easy to invert (finding x_{i-1}).

Intuition for domain sampler

We would like to be able to sample $(i, PRF_S(i))$ uniformly:

- First attempt: have an additional obfuscated function that on input i outputs $PRF_S(i)$
  Problem: then it's easy to find any $x_i \implies$ easy to invert (finding x_{i-1}).
- Second attempt: the obfuscated function on input j outputs $i = PRG(j)$ and $PRF_S(i)$ where G is a length doubling PRG *(constructible from OWF)*

Domain sampling

IOWF + iO $\Longrightarrow$ TDP

$$\mathrm{Sampler}(\gamma) \longrightarrow (\gamma, \mathrm{PRF}_s(\gamma))$$

$$\downarrow$$

$$i = \mathrm{PRG}(\gamma)$$

$$\downarrow$$

$$(i, \mathrm{PRF}_s(i))$$

$$F_s\big((i, \mathrm{PRF}_s(i))\big) = (i+1, \mathrm{PRF}_s(i+1))$$

easy

?

Given $(i+1, \mathrm{PRF}_s(i+1))$, Find $(i, \mathrm{PRF}_s(i))$

Need γ such that $\mathrm{PRG}(\gamma) = i$

$\Rightarrow$ hard to find because PRG is a OWF

Construction of TDP

IOWF + iO $\implies$ TDP

For $S \leftarrow \kappa_{PRF}(1^n)$

1. $F_S(i, \sigma)$: takes as input $i \in \mathbb{Z}_T$ and $\sigma \in \{0,1\}^n$ and checks whether $\sigma = \mathrm{PRF}_S(i)$. If so it returns $(i+1, PRFS(i+1))$ where i + 1 is computed modulo T. Otherwise it returns $\perp$
2. $X_S(j)$: takes as input a seed $j \in \{0,1\}^{log(\sqrt{T})}$ and outputs $(i, \sigma) = (\mathrm{PRG}(j), \mathrm{PRF}_S(\mathrm{PRG}(j)))$ where i is interpreted as a residue in $\mathbb{Z}_T$.

Construction of TDP

IOWF + iO $\implies$ TDP

- PK $\leftarrow \tilde{F}_S = iO(F_S)$ and $\tilde{X}_S = iO(X_S)$
  Trapdoor is S
- $D_{PK} = (i \in \mathbb{Z}_T, \mathrm{PRF}_S(i))$
- $\mathrm{TDP}_{PK}(i, \sigma) = \tilde{F}_S(i, \sigma)$
- $\mathrm{TDP}^{-1}_{PK}(i, \sigma) = (i - 1, \mathrm{PRF}_S(i - 1))$
- $\zeta(PK; j) = \tilde{X}_S(j)$ (j is randomness $\in \{0, 1\}^{log(\sqrt{T})}$)

Conclusion

2 results:

1. OWF + iO $\implies$ iOWF
2. OWF + sub-exponential iO $\implies$ TDP

Commitment scheme

http://yuyu.hk/files/commitment.pdf contain the description of the construction of (almost) perfect hiding from OWF

n-wise independant hash family

https://en.wikipedia.org/wiki/K-independent_hashingPolynomials_with_random_coefficients