Candidate Trapdoor Claw-Free Functions from Group Actions with Applications to Quantum Protocols

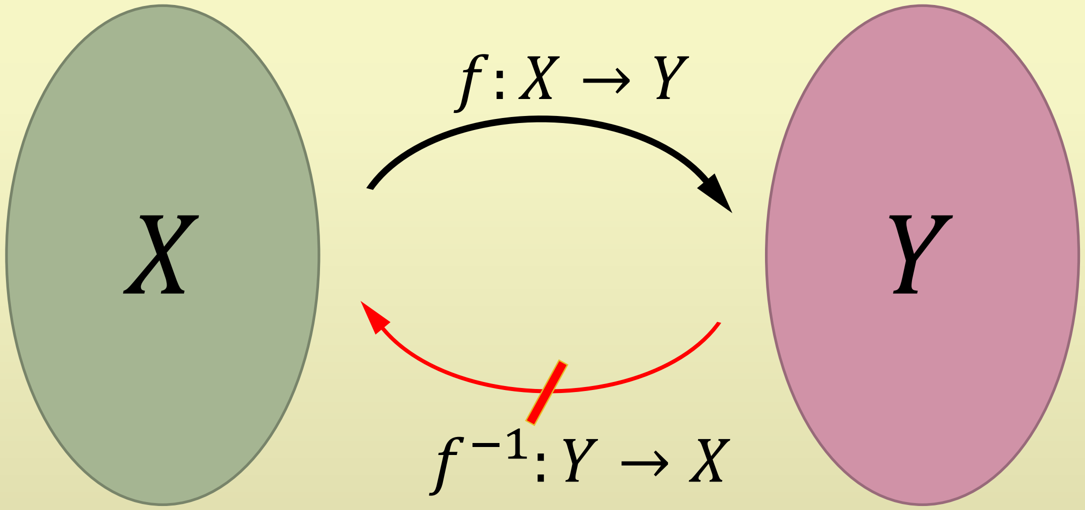
Navid Alamati[1], Giulio Malavolta[2] and Ahmadreza Rahimi[2]

1: Visa Research, USA

2: Max Planck Institute for Security and Privacy, Germany

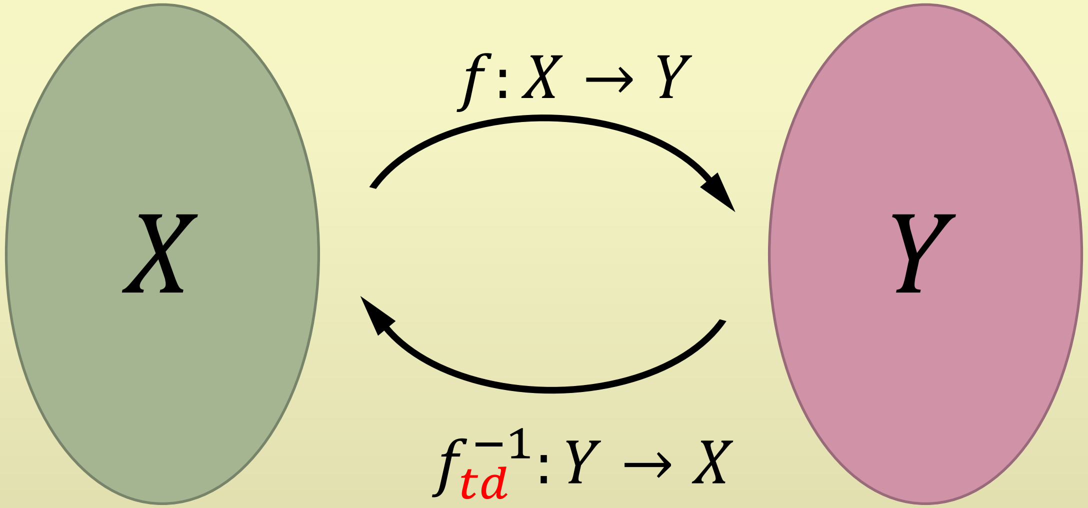
What is a TCF?

Trapdoor Function:



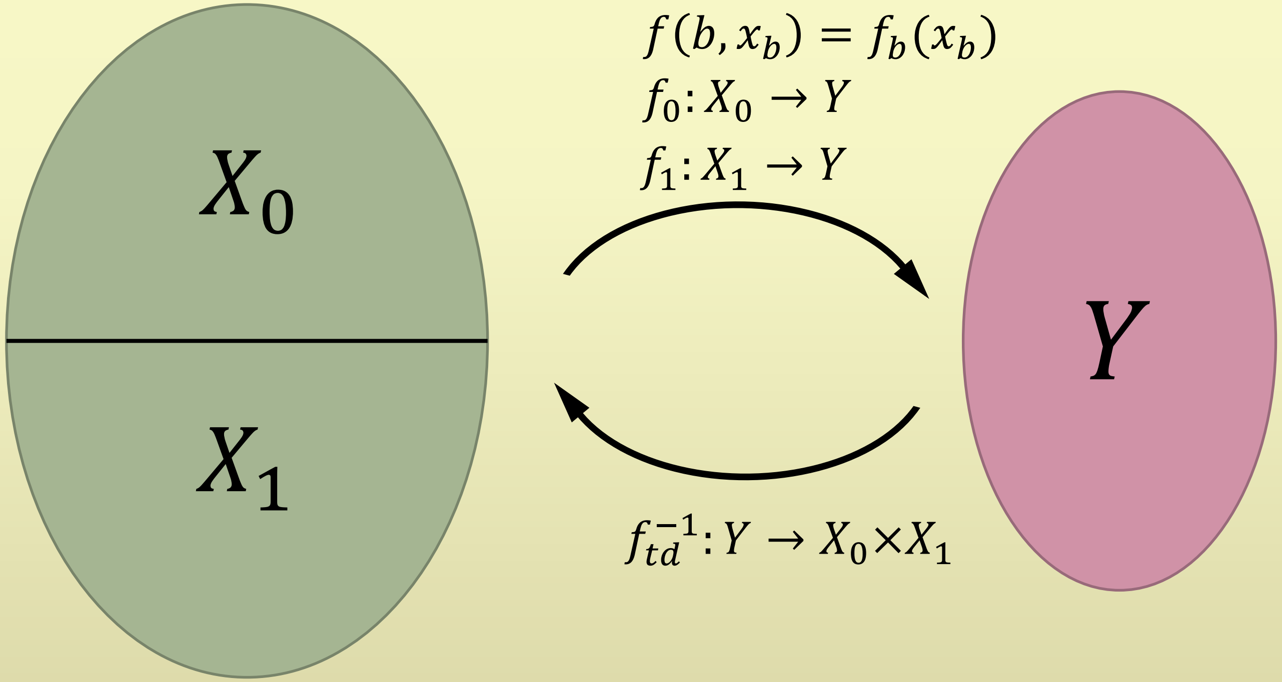
What is a TCF?

Trapdoor Function:



What is a TCF?

Trapdoor Claw Free Function:



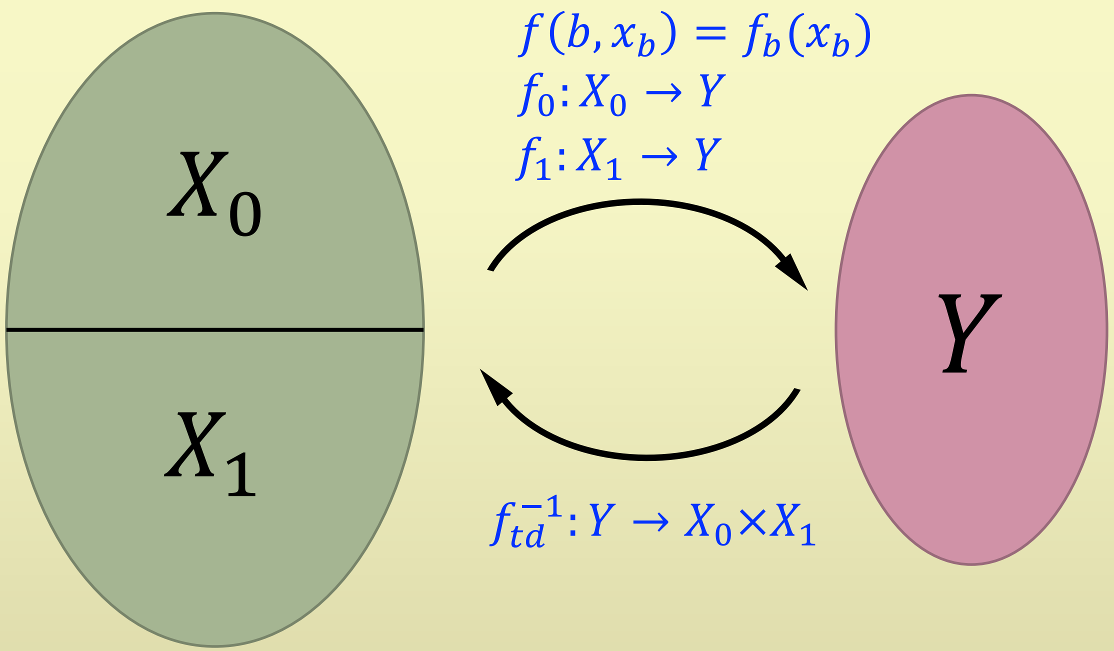
$f_0(x_0) = f_1(x_1) = y$

(x_0, x_1, y) is a **claw**

Finding a claw is hard!

What is a TCF?

Trapdoor Claw Free Function with Adaptive Hardcore Bit:



(x_0, x_1, y) is a **claw** if $f_0(x_0) = f_1(x_1) = y$

Adaptive hardcore bit:

For any $x_0, f_0\ (x_0)$, we know that:
$\exists x_1$ s.t. $f_1(x_1) = f_0(x_0)$ **but:**

Getting any infromation on x_1 must be hard

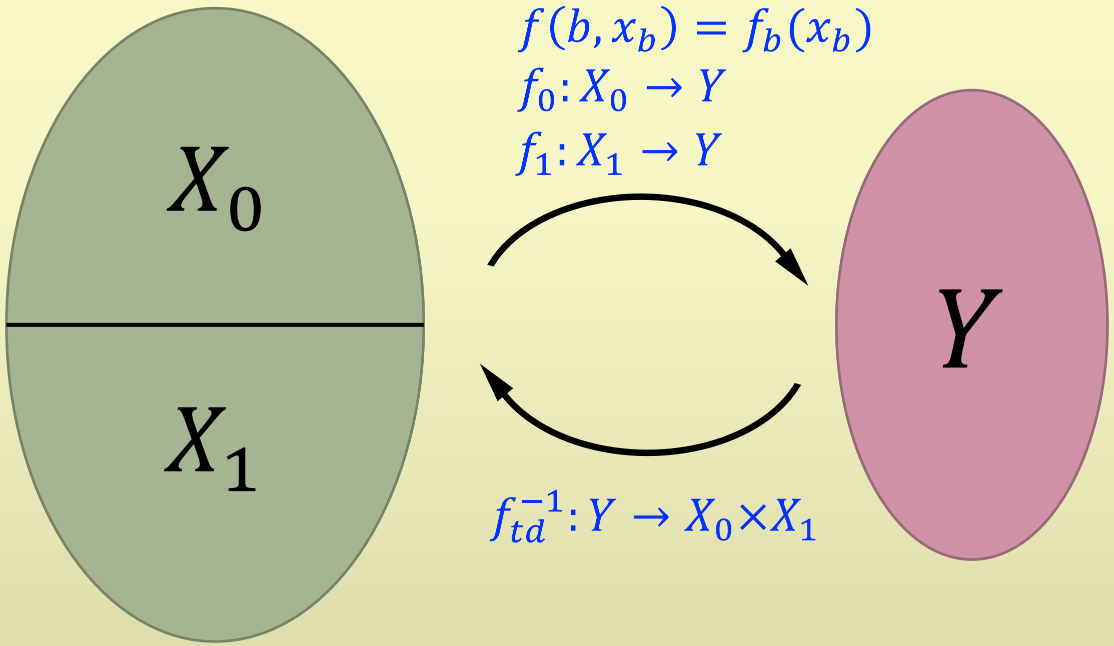
More formally:

Hard to find x_0 and binary vector $\mathbf{d} \neq \mathbf{0}$ and bit c s.t.

$$\mathbf{d} \cdot (x_0 \oplus x_1) = c \text{ and } f_0(x_0) = f_1(x_1)$$

What is a TCF?

Trapdoor Claw Free Function with Adaptive Hardcore Bit:



(x_0, x_1, y) is a **claw** if $f_0(x_0) = f_1(x_1) = y$

Adaptive hardcore bit:

Hard to find x_0 <u>and</u> binary vector $\mathbf{d} \neq \mathbf{0}$ and bit c s.t.

$$\langle \mathbf{d}, (x_0 \oplus x_1) \rangle = c \text{ and } f_0(x_0) = f_1(x_1)$$

Why do we care about this?

Finding both pre-image x_b and pair $(\mathbf{d}, \langle \mathbf{d}, (x_0 \oplus x_1) \rangle)$,

is **hard** for any **QPT** adversary.

Applications of TCFs

TCFs have been around for a while.

Some Recent Quantum Applications of TCFs:

- Test of Quantumness/Randomness [BCMVV'18]
- Classical Verification of Quantum Computation [Mah18b]
- Qunamtum Fully Homomorphic Encryption [Mah18a]
- Remote State Preparation [GV19]
- Verifiable Test of Quantumness [BKVV20]
- Proof of Quantumness [KCVY'21]
- Deniable Encryption [CGV22]
- …

Current Post-Quantum TCFs

All based on **quantum hardness** of **LWE** 😑

What about other **quantum hard** assumptions?

***TCFs** from isogeny-based **group actions**! ☺*

Group Actions: Effective Group Actions

Group

$\star: \mathbb{G} \times \mathbb{X} \to \mathbb{X}$

Set

For all $g \in \mathbb{G}, x \in \mathbb{X}$, $g \star x$ can be **efficiently** computed.

$g, h \in \mathbb{G}, x \in \mathbb{X}$: $(g + h) \star x = g \star (h \star x)$

For all $x \in \mathbb{X}$, $e \star x = x$ where e is identity element of $\mathbb{G}$.

One-Way EGA

Given $(x, g \star x)$ | $g \leftarrow_{\$} \mathbb{G}$

No attacker can find g

Example: Given $x, g \star x \; := x^g$

Think of DLOG

Linear Hidden Shift (LHS) [ADMP'20]

$n > \log|\mathbb{G}|, \; \ell = poly(\lambda)$

$(\mathbf{M}, \mathbf{x}, \mathbf{M}\mathbf{v} \star \mathbf{x}) \approx_c (\mathbf{x}, \mathbf{M}, \mathbf{u})$

$\mathbf{M} \leftarrow_{\$} \mathbb{G}^{\ell \times n}$ $\quad \mathbf{x} \leftarrow_{\$} \mathbb{X}^{\ell}$

$\mathbf{v} \leftarrow_{\$} \{0,1\}^n$ $\quad \mathbf{u} \leftarrow_{\$} \mathbb{X}^{\ell}$

Think of LWE, No **noise** but **action**

Components of $\mathbf{M}\mathbf{v} \star \mathbf{x}$ cannot be combined.

Simple Claw Free Function

$\star: \mathbb{G}\times\mathbb{X} \to \mathbb{X}$, $n > \log|\mathbb{G}|$, Large integer B

Goal: two-to-one CF $f: \{0,1\}\times[B]^n \to \mathbb{X}^n$

Parameter Generation
$\mathbf{v} \leftarrow \{0,1\}^n$
$pp \coloneqq (\mathbf{x} \leftarrow \mathbb{X}^n, \mathbf{M} \leftarrow \mathbb{G}^{n\times n}, \mathbf{Mv} \star \mathbf{x})$ *LHS Challenge!*
Evaluation
For $b \in \{0,1\}$ and $\mathbf{s} \in [B]^n$
$f_{pp}(b, \mathbf{s}) = \mathbf{M}(\mathbf{s} + b \cdot \mathbf{v}) \star \mathbf{x}$
Claw Free: $f_{pp}(0, \mathbf{s}_0) = f_{pp}(1, \mathbf{s}_1)$
Finding a claw $((0, \mathbf{s}_0), (1, \mathbf{s}_1))$ **Breaks LHS!**
$\mathbf{v} = \mathbf{s}_0 - \mathbf{s}_1$
No **Trapdoor** and hard to argue **adaptive HC bit**

Adaptive Hardcore Bit

For any ***QPT*** adversary $\mathcal{A}$:

Finding $(b, \mathbf{s}_b)$ $\mathbf{d}$ $\langle \mathbf{s}_{1-b}, \mathbf{d} \rangle$ Is **hard**!

$(b, \mathbf{s}_b)$: pre-image; $\mathbf{d}$: arbitrary non zero binary vector; $\langle \mathbf{s}_{1-b}, \mathbf{d} \rangle$: any information

where $f_{pp}(b, \mathbf{s}_b) = f_{pp}(1 - b, \mathbf{s}_{1-b})$

[BCM+'18]:*There exists efficient transformation* $\mathcal{T}$*:*

$$((b, \mathbf{s}_b), \mathbf{d}, \langle \mathbf{s}_{1-b}, \mathbf{d} \rangle) \to \boxed{\mathcal{T}} \to (\mathbf{d}', \langle \mathbf{d}', \mathbf{v} \rangle)$$

adaptive hardcore bit → any <u>non-trivial</u> parity of **shift vector**

Direct Prodcut Adaptive HC Bit

$\mathbf{v} \leftarrow \{0,1\}^n$

$pp \coloneqq (\mathbf{x} \leftarrow_\$ \mathbb{X}^n, \mathbf{M} \leftarrow_\$ \mathbb{G}^{n\times n}, \mathbf{Mv} \star \mathbf{x})$

For $b \in \{0,1\}$ and $\mathbf{s} \in [B]^n$

$f_{pp}(b, \mathbf{s}) = \mathbf{M}(\mathbf{s} + b \cdot \mathbf{v}) \star \mathbf{x}$

$((b, \mathbf{s}_b), \mathbf{d}, \langle \mathbf{s}_{1-b}, \mathbf{d} \rangle) \to \boxed{\mathcal{T}} \to (\mathbf{d}', \langle \mathbf{d}', \mathbf{v} \rangle)$

$f_{pp}(b, \mathbf{s})$ $\qquad$ $f_{pp'}(\mathbf{v})$

$pp' \coloneqq (\mathbf{x} \leftarrow_\$ \mathbb{X}^n, \mathbf{M} \leftarrow_\$ \mathbb{G}^{n\times n})$

Direct Product Adaptive HC bit

For <u>any</u> **QPT** adversary $\mathcal{A}$

Given:

$(pp_1, \cdots, pp_n, f_{pp_1}(\mathbf{v}_1), \cdots, f_{pp_n}(\mathbf{v}_n))$

Hard to **simultaniously** find:

$(\mathbf{d}_1', \langle \mathbf{d}_1', \mathbf{v}_1 \rangle), \cdots, (\mathbf{d}_n', \langle \mathbf{d}_n', \mathbf{v}_n \rangle)$

Open problem ☺

Conjecture ⇒

Adaptive HC bit

For <u>any</u> **QPT** adversary $\mathcal{A}$

Given:

$(pp_1, \cdots, pp_n, f_{pp_1}(\mathbf{v}_1), \cdots, f_{pp_n}(\mathbf{v}_n))$

Hard to find:

$(\mathbf{d}_1', \cdots, \mathbf{d}_n', \langle \mathbf{d}_1', \mathbf{v}_1 \rangle \oplus \cdots \oplus \langle \mathbf{d}_n', \mathbf{v}_n \rangle)$

Function with Direct Prodcut Adaptive HC Bit

Goal: A function family $f_{pp}: \{0,1\}^n \rightarrow Y$ that satisfies **direct product adaptive hardcore bit**.

Correlated Pseudorandomness: $\mathbf{w} \leftarrow_\$ \{0,1\}^n$ $pp_1, \cdots, pp_n$ are ***independently*** sampled

uniform

$$\left(pp_1, \cdots, pp_n, f_{pp_1}(\mathbf{w}), \cdots, f_{pp_n}(\mathbf{w})\right) \approx_c (pp_1, \cdots, pp_n, u_1, \cdots, u_n)$$

Efficient Procedure $\mathcal{P}$

$\left(pp_1, \cdots, pp_n, f_{pp_1}(\mathbf{w}), \cdots, f_{pp_n}(\mathbf{w})\right) \rightarrow$

Uniform binary vectors $\mathbf{r}_1, \cdots, \mathbf{r}_n \rightarrow$

$\mathcal{P}$

$$\rightarrow \left(pp'_1, \cdots, pp'_n, f_{pp'_1}(\mathbf{w} \oplus \mathbf{r}_1), \cdots, f_{pp'_n}(\mathbf{w} \oplus \mathbf{r}_n)\right)$$

$$\approx_s$$

$$\left(\overline{pp}_1, \cdots, \overline{pp}_n, f_{\overline{pp}_1}(\mathbf{v}_1), \cdots, f_{\overline{pp}_n}(\mathbf{v}_n)\right)$$

Theorem: If f is a function family with *correlated pseudorandomness* and there is a corresponding procedure $\mathcal{P}$ for f, then, it satisfies **direct product adaptive hardcore bit** property.

Our Results

This Work: A Trapdoor Claw Free function family F with procedure $\mathcal{P}$, from ***extended-LHS*** assumption.

This Work: A quantum protocol for *qubit test* from our TCF function.

Thank you ☺