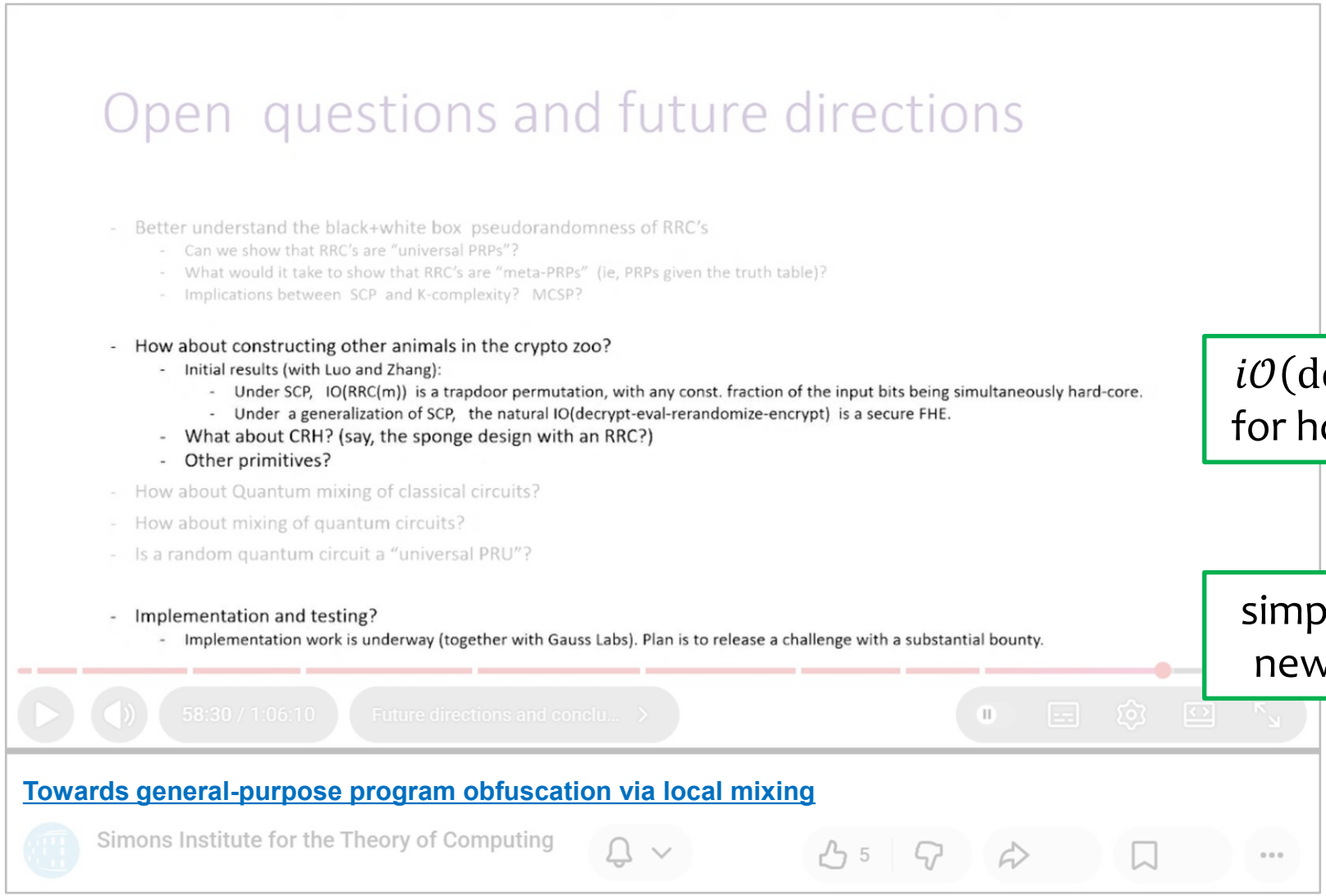
Previously on Obfuscation…



$i\mathcal{O}$(decrypt–eval–reencrypt) for homomorphic encryption

simple security challenge for new $i\mathcal{O}$ proposals (victim: PKE)

How to Encrypt with Random Reversible Circuits

Functional, Homomorphic and CCA-Secure

Ji Luo

Ran Canetti [1] ✉ 罗辑 [2] ✉ 🌐 Yiding Zhang [1] ✉

[1]BU [2]MIT → ?

Partially done when Ji Luo was at BU.

Reversible Circuits

fixed set of n **wires** (0/1-valued)
sequence of m **gates**

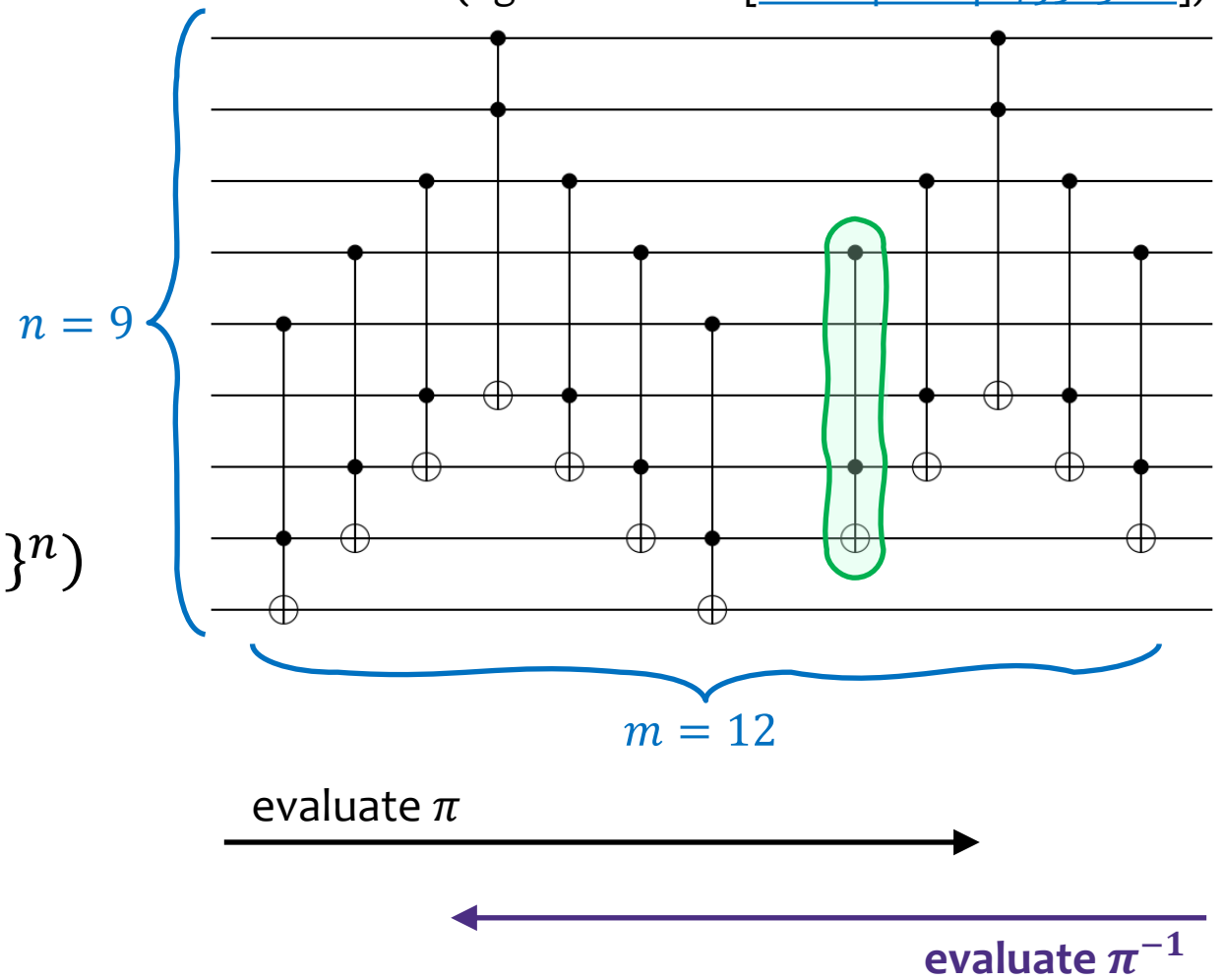
- fixed set of basis permutations
- e.g., Toffoli $w_8 \leftarrow w_8 \oplus (w_4 \wedge w_7)$
- 3-local

computes permutation $\pi \in \mathrm{Sym}(\{0,1\}^n)$

- **reversible** – easily compute π^{-1}

use reversible circuits for cryptography?

(figure credit to [arXiv:quant-ph/9503016])



Reversible Circuits and Cryptography

random reversible circuits $\mathrm{RRC}_{n,m}$

ε-close to k-**wise independence**

- $m = \mathrm{poly}(n, k, \log(1/\varepsilon))$ suffices [Gowers96, HooryMagenMyersRackoff05, HooryBrodsky05, GrettaHePelecanos25, GayHeKocurekO'Donnell25]

pseudorandom permutations (PRP) ✓ secret-key encryption

- conjectured for some $m = \mathrm{poly}(\lambda, n)$ [Gowers96]

program obfuscation based on RRC ? public-key encryption

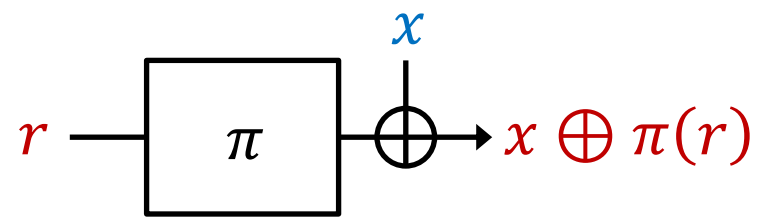
[CanettiChamonMuccioloRuckenstein24]

PRP and Secret-Key Encryption

PRP (a.k.a. **block ciphers**)

- efficient distribution $\mathcal{D}$ over $\mathrm{Sym}(\{0,1\}^n)$
- efficient evaluation in both directions
- $(\pi, \pi^{-1}) \approx (\pi', (\pi')^{-1})$ as **oracles**

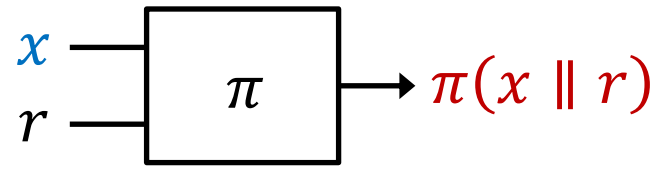
$$\pi \xleftarrow{\$} \mathcal{D}, \quad \pi' \xleftarrow{\$} \mathrm{Sym}(\{0,1\}^n).$$



$$\mathrm{ct} = \left(r,\ x \oplus \pi(r)\right)$$

candidates.

- Feistel using any PRF [LubyRackoff88]
- AES, $\mathrm{RRC}_{n,\mathrm{poly}(\lambda,n)}$



$$\mathrm{ct} = \pi(x \parallel r)$$

numerous ways to construct SKE

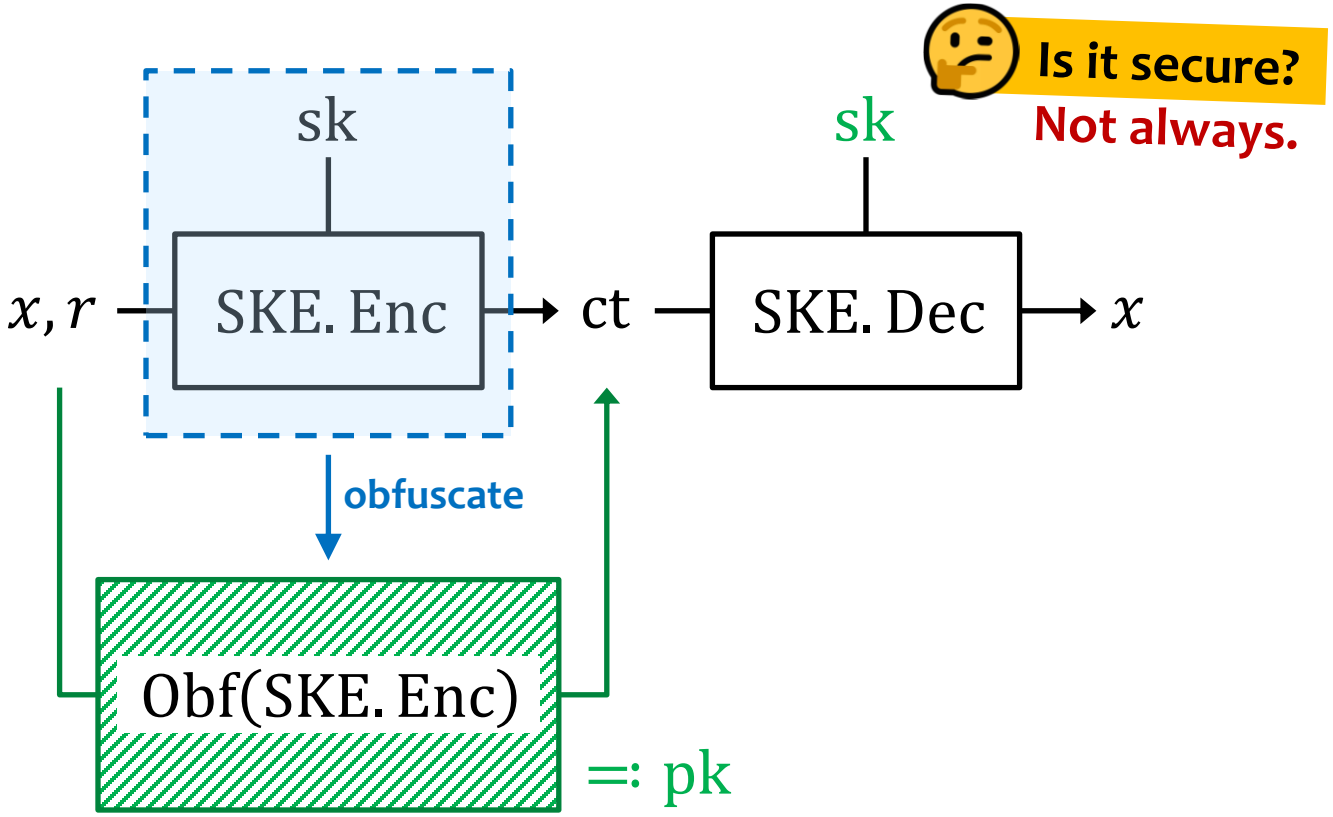
- (1-block) CTR
- 1-block ECB with random nonce

CCA-secure!

PKE from Obfuscated SKE

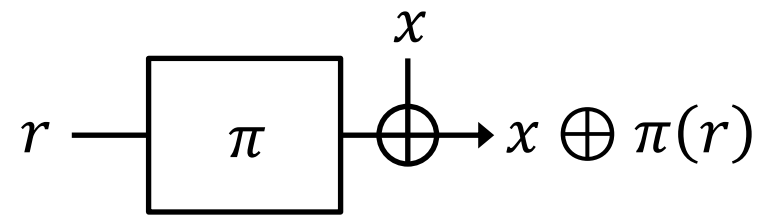
reversible circuits $\longrightarrow$ PRP + obfuscation
$\longrightarrow$ SKE

[DiffieHellman76] **PKE by obfuscating SKE**



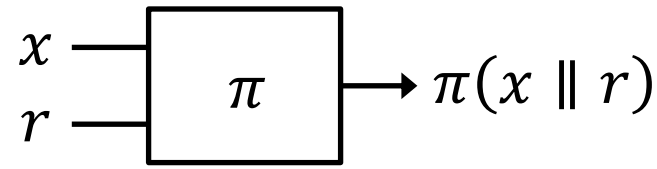
Is it secure?
Not always.

PKE can't be public-coin



$$\mathrm{ct} = \left(r,\ x \oplus \pi(r)\right)$$

When π is RRC?



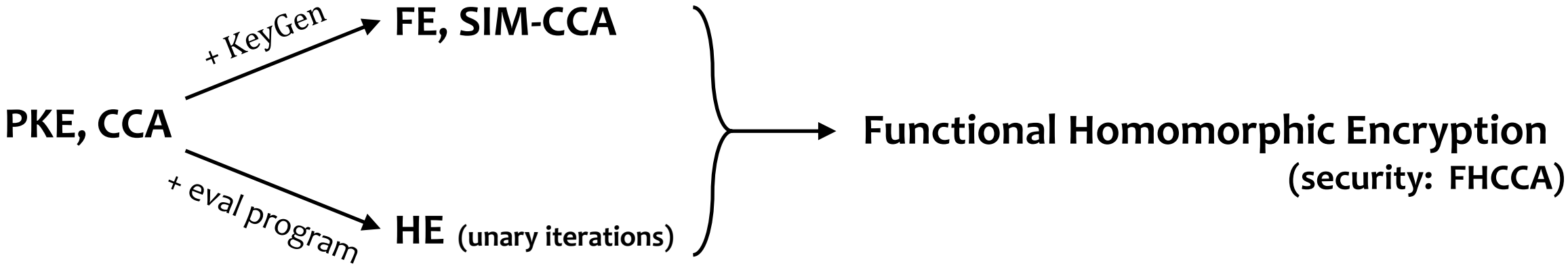
$$\mathrm{ct} = \pi(x \parallel r)$$

Yes!
- ✓ **CCA**
- ✓ **FE/HE**

Our Results

- RRC is permutable PRP [ShmueliZhandry25]
  (under SCP assumption [CanettiChamonMuccioloRuckenstein24])

- $\mathrm{Enc}(\overbrace{i\mathcal{O}(\pi)}^{\mathrm{pk}}, x; r) = \mathrm{pk}(x \parallel r)$ with PPRP π



- additional results

Talk Roadmap

- permutable PRP [ShmueliZhandry25]
- CCA security of simple PKE + upgrades
  - FE with SIM-CCA
  - HE for unary iterations
- functional homomorphic encryption
  - IND-FHCCA
- concluding remarks

Permutable PRP [ShmueliZhandry25]

efficient distribution $\pi \in \mathrm{Sym}(\{0,1\}^n)$
efficient evaluation both ways

e.g., $G = \{\text{transpositions}\}$

$\Gamma \in G \subseteq \mathrm{Sym}(\{0,1\}^n)$

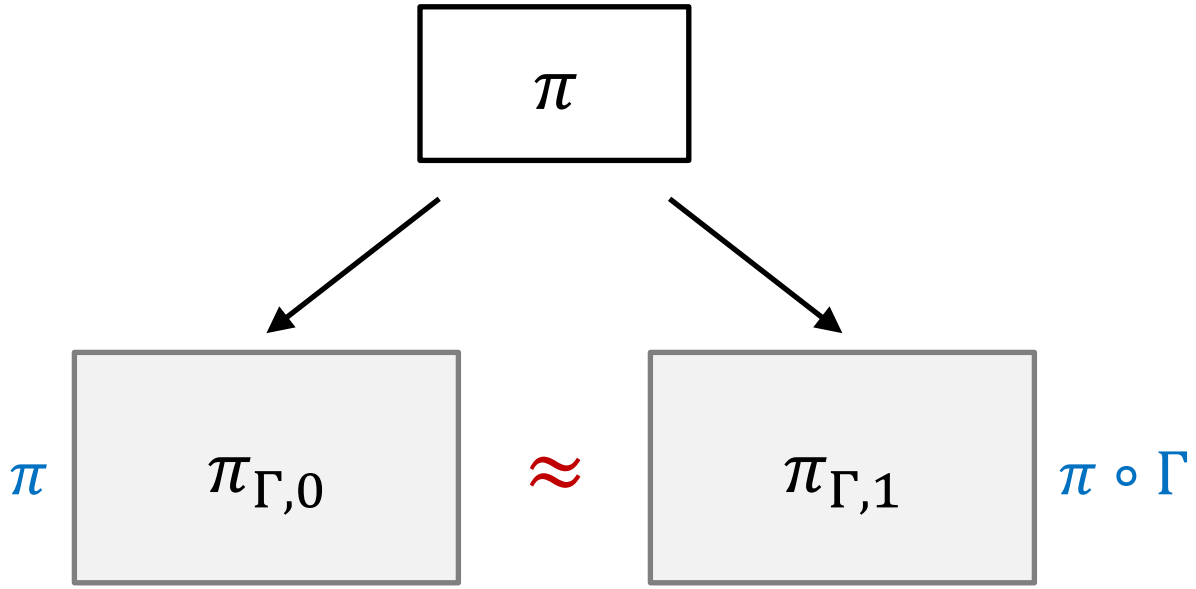
$\mathrm{Permute}(\pi, \Gamma, b) \to \pi_{\Gamma,b}$

- ***potentially*** permuted
- $\pi_{\Gamma,b}$ implements $\pi \circ \Gamma^{(b)}$
- two-way evaluation

in [ShmueliZhandry25]

- $i\mathcal{O}$ + OWF $\Longrightarrow$ PPRP
- $i\mathcal{O}$ + PPRP $\Longrightarrow$ **full-domain** TDP

Yes, TDP $\Longrightarrow$ PKE, but…



PPRF analogy.

$\pi_{\Gamma,0} \sim (k^\circ, f(k, x^*))$

$\pi_{\Gamma,1} \sim (k^\circ, \text{random})$

Simple PKE is CCA-Secure

$\mathrm{sk} = \pi^{-1}, \quad \mathrm{pk} \xleftarrow{\$} i\mathcal{O}(\pi)$.

encrypt. $x \parallel r \xrightarrow{\mathrm{pk}} \mathrm{ct}$

decrypt. $\mathrm{ct} \xrightarrow{\pi^{-1}} x \parallel$ ~~r~~

crux of CCA.

- provide pk
- change challenge ct
- provide decryption ~~oracle~~ **program**

implies *quantum* CCA

proof core

Permute π by $(x^* \parallel r^* \quad u^*)$.

simple + good.

- ✓ just [DiffieHellman76]
- ✓ no "checks" (NIZK, signature, etc.)
- ✓ no invalid ct / "wastage"
- ✓ already rate-1

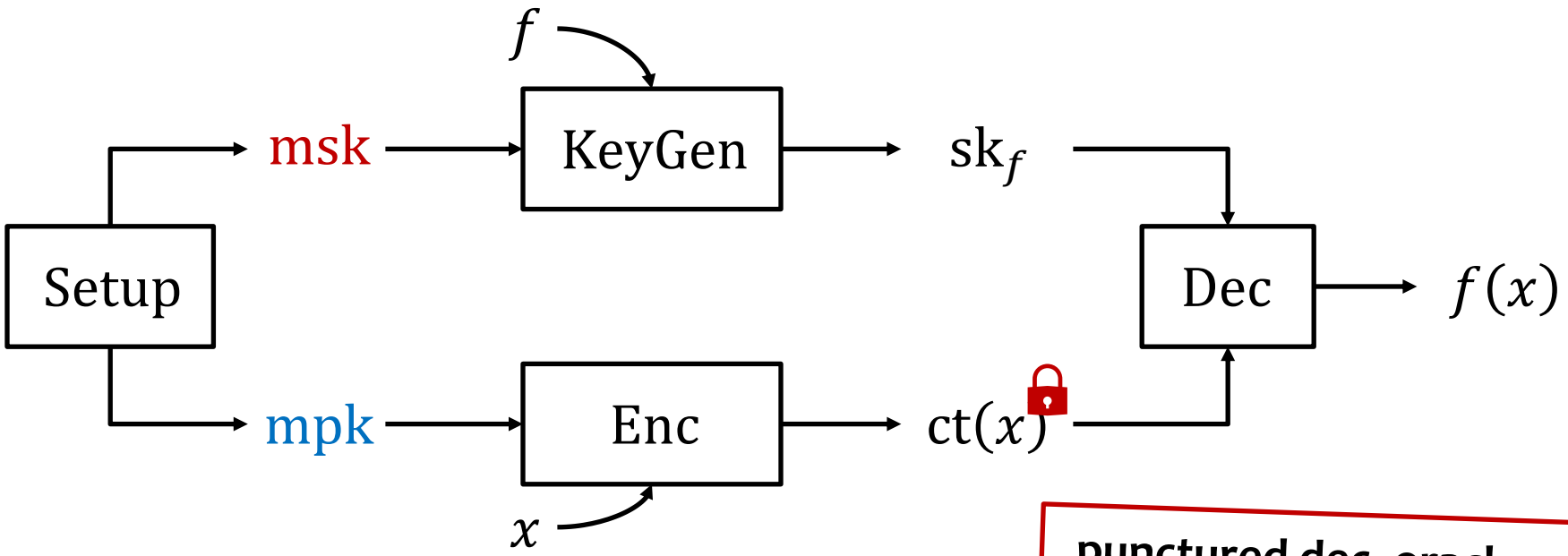
security core lemma. For any x^*,

$$\left(i\mathcal{O}(\pi),\ i\mathcal{O}(\pi^{-1} \setminus \{y^*\}),\ y^* \leftarrow \pi(x^* \parallel r^*)\right)$$

$$\approx \left(i\mathcal{O}(\pi),\ i\mathcal{O}(\pi^{-1} \setminus \{y^*\}),\ y^* \xleftarrow{\$} \{0,1\}^{\cdots}\right).$$

pk **punctured dec. prog.** **challenge ct**

Functional Encryption



punctured dec. oracle

- can use key ***without*** retrieving it
- ***no*** $f(x^*)$ for sim. to answer dec.
- (IND.) can use ***distinguishing*** keys

simulation security against chosen-ciphertext attacks.

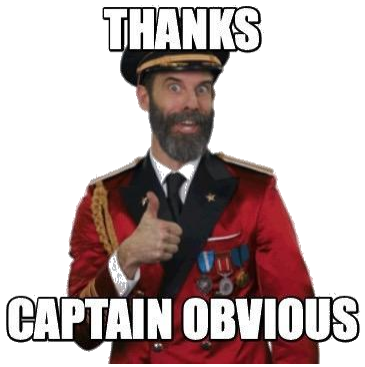
$$\left(\mathrm{mpk}, \mathrm{ct}(x^*), \{\mathrm{sk}_{f_j}\}_j\right) \approx \left(\widehat{\mathrm{mpk}}, \widehat{\mathrm{ct}}(\not{x}^*), \{\widehat{\mathrm{sk}}_{f_j}(f_j(x^*))\}_j\right)$$

Free Upgrade to FE with SIM-CCA

$\mathrm{msk} = \pi^{-1}, \quad \mathrm{mpk} \xleftarrow{\$} i\mathcal{O}(\pi)$.

encrypt. $x \parallel r \xrightarrow{\mathrm{mpk}} \mathrm{ct}$

key. $i\mathcal{O}(\mathrm{ct} \xmapsto{\pi^{-1}} x \parallel r \xmapsto{f} f(x))$



simulator.
- use R for dec.
- use y^* for $\widehat{\mathrm{ct}}$
- use R for $\widehat{\mathrm{sk}}_f \xleftarrow{\$} i\mathcal{O}(F)$

✓ **first*** CCA-secure general FE (+ SIM-CCA)
✓ **no** NIZK/signature/etc. **inside** $i\mathcal{O}$

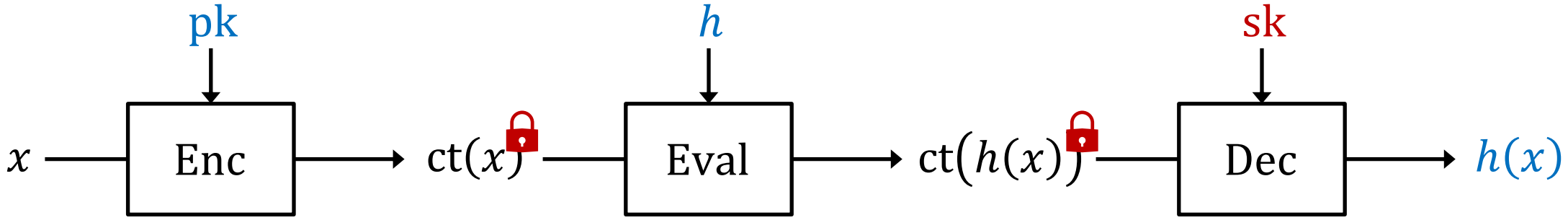
$$F(\mathrm{ct}) = \begin{cases} f(x^*), & \text{if } \mathrm{ct} = y^*; \\ f(x), & \text{else } R(\mathrm{ct}) = x \parallel r. \end{cases}$$

same lemma.

$$\left(i\mathcal{O}(\pi), R \xleftarrow{\$} i\mathcal{O}(\pi^{-1} \setminus \{y^*\}), y^* \leftarrow \pi(x^* \parallel r^*)\right) \approx \left(i\mathcal{O}(\pi), R \xleftarrow{\$} i\mathcal{O}(\pi^{-1} \setminus \{y^*\}), y^* \xleftarrow{\$} \{0,1\}^{\cdots}\right).$$

* The only previous work has a bug in proof.

Homomorphic Encryption



our scheme. $h(x) = g^{(t)}(x)$ (one g + any $t \in \mathbb{N}$).

- e.g., g = one step of TM

$$\mathrm{sk} = \pi^{-1}, \quad \mathrm{pk} \xleftarrow{\$} i\mathcal{O}(\pi).$$

$$\mathrm{ct} = \pi(x \parallel \ell \parallel r) \xrightarrow{\pi^{-1}} x \parallel \ell \parallel r \xrightarrow{g,+1,\sigma} g(x) \parallel (\ell+1) \parallel \sigma(r) \xrightarrow{\pi} \mathrm{ct}\big(g(x)\big)$$

for proof

random in fresh ct

another PPRP

✓ **same encryption as PKE**

Unary HE (continued)

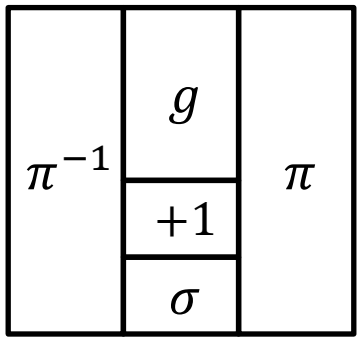
- ✓ unleveled
- ✓ no errors to handle
- ✓ full-domain homomorphism (not just 1-bit)
- ✓ already rate-1
- ✗ unary — **less functionality, but controlled homomorphism**

our scheme. $h(x) = g^{(t)}(x)$ (one g + any $t \in \mathbb{N}$).

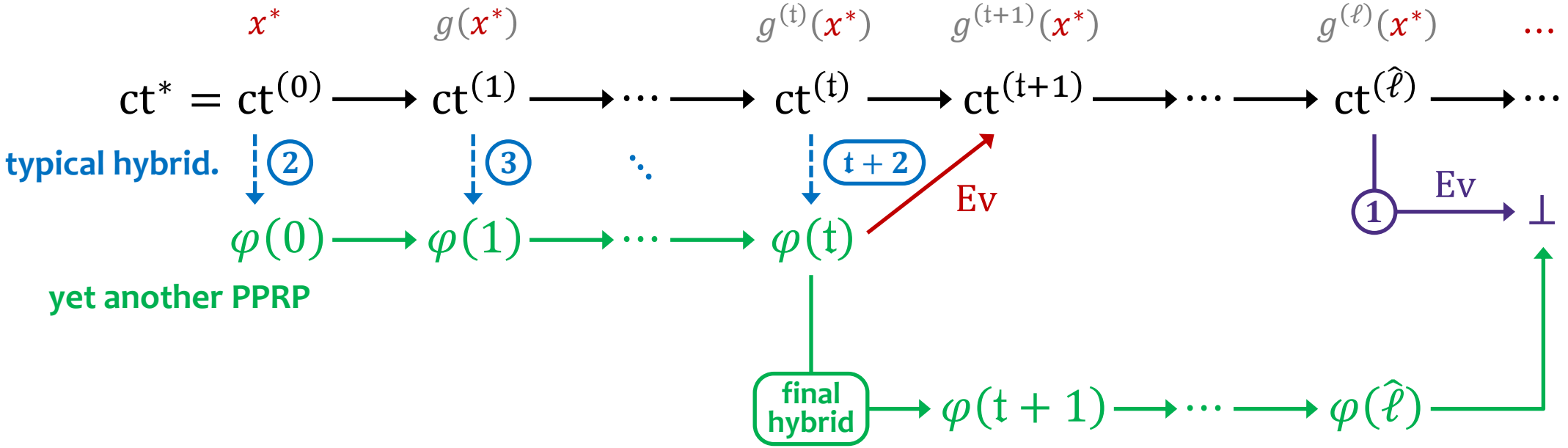
- e.g., g = one step of TM

$\mathrm{sk} = \pi^{-1}, \quad \mathrm{pk} \xleftarrow{\$} (i\mathcal{O}(\pi), i\mathcal{O}(\mathrm{Ev})), \quad \mathrm{Ev}:$

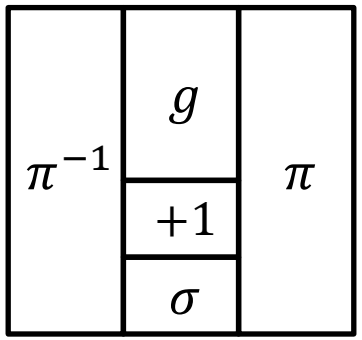
$\mathrm{ct} = \pi(x \parallel \ell \parallel r)$



Unary HE: Glimpse of Security Proof



$\mathrm{sk} = \pi^{-1}, \quad \mathrm{pk} \xleftarrow{\$} (i\mathcal{O}(\pi), i\mathcal{O}(\mathrm{Ev})), \quad$ Ev:



$\mathrm{ct} = \pi(x \parallel \ell \parallel r)$

Ideas for Combining FE and HE

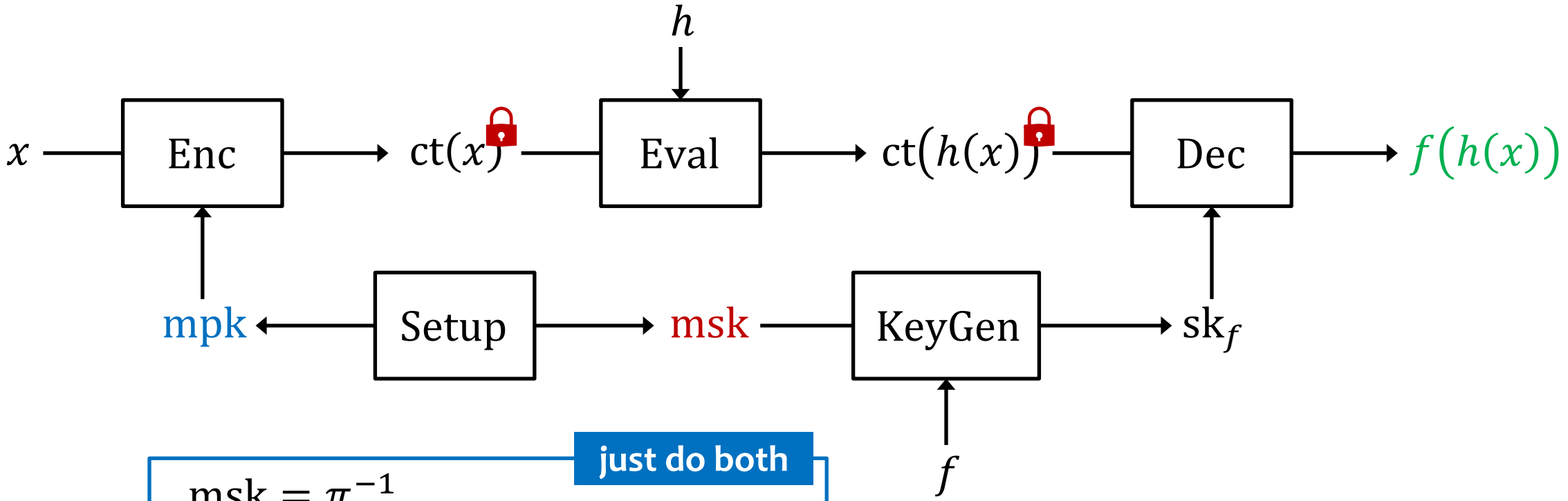
FE+FE. already collusion-resistant

HE+HE. (standard) ***multi-ary***? unary iterations for ***two*** functions?

- black-box **barrier** (collision resistance [AsharovSegev15])
- proof "**explodes**" (too many hybrids)
- ☯ *known.* lossiness + change pk at each Eval [CanettiLinTessaroVaikuntanathan14]

FE+HE. **Yes, new + interesting + achievable!**

Functional Homomorphic Encryption



just do both

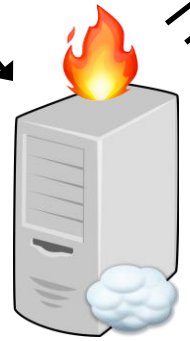
$$\mathrm{msk} = \pi^{-1},$$
$$\mathrm{mpk} \xleftarrow{\$} (i\mathcal{O}(\pi), i\mathcal{O}(\mathrm{Ev})),$$
$$\mathrm{ct}(x) = \pi(x \parallel \cdots),$$
$$\mathrm{Ev}: \quad \pi(x \parallel \cdots) \mapsto \pi(g(x) \parallel \widetilde{\cdots}),$$
$$\mathrm{sk}_f = i\mathcal{O}\big(\pi(x \parallel \cdots) \mapsto f(x)\big).$$

Applications

ψ = initial state of the world
g = unit-time evolution operator

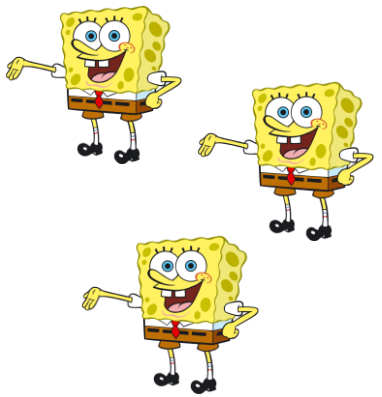
$\mathrm{sk}_{f_1}, \mathrm{sk}_{f_2}, \ldots$

$\mathrm{ct}(\psi)$



$\mathrm{ct}(g^{(t)}(\psi))$ for $t = 1,2, \ldots$

f_i = Bob$_i$'s observation



$f_2(g^{(t)}(\psi))$ for $t \in T_2$ of interest to Bob$_2$

- ✓ Alice's work minimal, non-interactive
- ✓ Bob$_i$'s work $\propto |T_i| \cdot |f_i|$, not $|g|$ or $\max t$
- ✓ Server can be untrusted

when not on steroids…

- instance-specific HE for TM [GoldwasserKalaiPopaVaikuntanathanZeldovich13]
  x = init. config., g = step, f = "halted?"
- randomized encoding for long output
  x = init. config., g = step,
  f = current-step output + "halted?"

Security: Intuitions and Observations

Intuition. Only $\{f_j(h(x^*))\}$ is revealed, for h by design + f_j queried for key.

- E.g., $\{f_j(g^{(t)}(x^*))\}$ for f_j queried for key + all t.

Observation 1. Simulation in general is impossible.

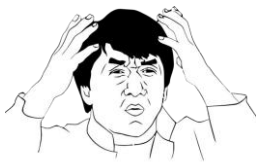
- $\{f(g^{(t)}(x^*))\}$ could be ***pseudorandom + longer*** than $M = |\mathrm{mpk}| + |\mathrm{sk}_f| + |\mathrm{ct}|$.

$$x = (k, t), \quad f(x) = \mathrm{PRF}(k, t), \quad g(k, t) = (k, (t+1) \bmod (M+1))$$

requires compressing PRF truth table

Observation 2. Security inherently has non-malleability.

- but **NM + HE** $\not\rightarrow$
- inspiration from (SIM-)HCCA [PrabhakaranRosuleko8]
  controlled homomorphism



$$x_0^* = 0, \quad x_1^* = 2, \qquad f(x) = \begin{cases} x, & \text{if } x \text{ is odd;} \\ 0, & \text{if } x \text{ is even;} \end{cases} \qquad g(x) = x + 2$$

must forbid changing $\mathrm{ct}(x)$ to $\mathrm{ct}(x+1)$

Security: IND-FHCCA

$\mathrm{Link}(\mathrm{mpk}, \mathrm{ct}^*, \mathrm{ct}') \to h/\perp$

"ct′ has $h(x^*)$ for x^* under ct^*"
or "they're unrelated"

ours. $(\ell' - \ell^*)$ if they are close enough

Decryption Consistency.
Adversary cannot cause Link to find ***incorrect*** relation against ***honest*** ct^*.

Ciphertext Indistinguishability. With dec. oracle,

$$\left(\mathrm{mpk}, \mathrm{ct}(x_0^*), \{\mathrm{sk}_{f_j}\}_j\right) \approx \left(\mathrm{mpk}, \mathrm{ct}(x_1^*), \{\mathrm{sk}_{f_j}\}_j\right)$$

if $f_j(h(x_0^*)) = f_j(h(x_1^*))$ for all h ***allowed by design***.

The dec. oracle decrypts ct′ ***if and only if*** (unrelated to ct^*)

$$\mathrm{Link}(\mathrm{mpk}, \mathrm{ct}^*, \mathrm{ct}') = \perp$$

or pre-challenge. It can use ***distinguishing*** keys.

- Random reversible circuits are PPRP.
- Powers of $i\mathcal{O}(\pi)$: CCA PKE, SIM-CCA FE, CPA HE.
- New primitive: functional homomorphic encryption (FHCCA).

clopen.

- requires breaking barrier of [AsharovSegev15]
  - more homomorphisms
  - CRHF from ($i\mathcal{O}$ +) OWF (candidate: RRC sponge construction)
- adaptive security of simple HE (we do this for PKE; cheating kills rate)
- FE with CCA security (upcoming: for RAM, no subexp. assumptions)

Thanks!

ePrints: 2026/1398 + to appear soon