Non-Malleable Functions and Their Applications

Yu Chen[1,2] Baodong Qin[3] Jiang Zhang[4]
Yi Deng[1,4] Sherman S.M. Chow[2]

[1]SKLOIS, IIE, Chinese Academy of Sciences
[2]IE Dept., The Chinese University of Hong Kong
[3]CS Dept., Southwest University of Science and Technology
[4]State Key Laboratory of Cryptology, Beijing, China

PKC 2016

March 6, 2016

Outline

1. Backgrounds
2. NMFs: Syntax and Definition
3. Relations among OW and NM
4. Constructions of NMFs
5. Applications of NMFs

Outline

Non-Malleable Cryptography

OWF

Codes

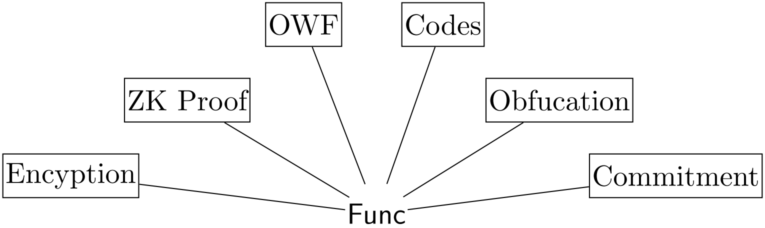
ZK Proof

Obfucation

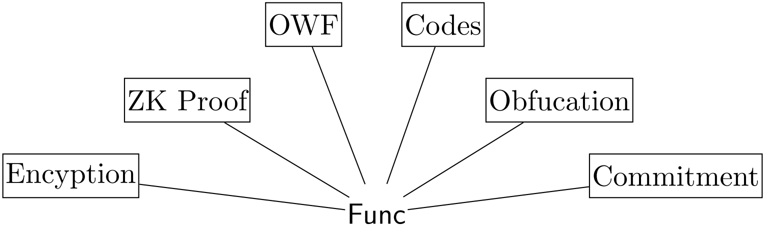
Encyption

Commitment

Non-Malleable Cryptography



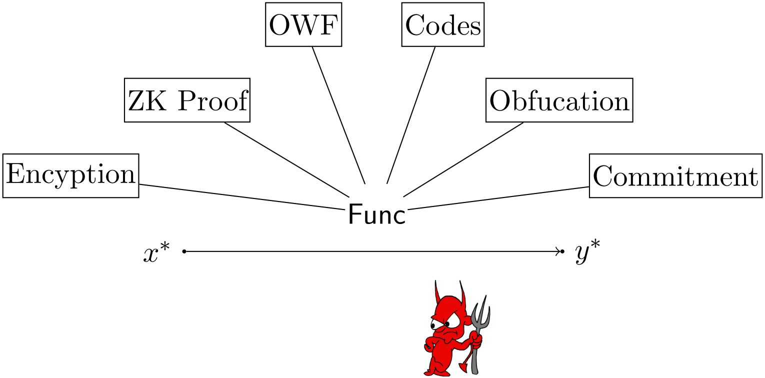
Non-Malleable Cryptography



Non-Malleability

ensure some level of independence between inputs and outputs

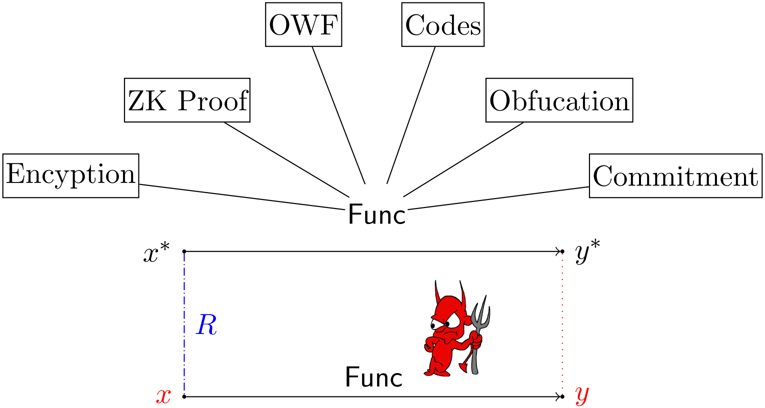
Non-Malleable Cryptography



Non-Malleability

ensure some level of independence between inputs and outputs

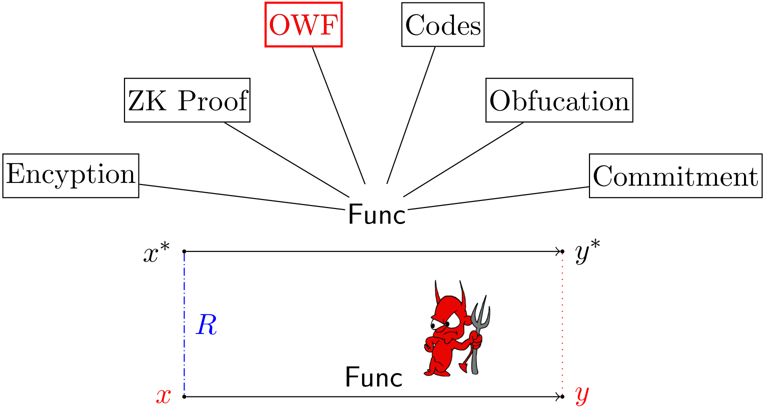
Non-Malleable Cryptography



Non-Malleability

ensure some level of independence between inputs and outputs

Non-Malleable Cryptography



Non-Malleability

ensure some level of independence between inputs and outputs

Non-Malleable One-Way/Hash Functions (NMOWHF)

[Boldyreva, Cash, Fischlin, and Warinschi, Asiacrypt 2009]

- simulation-based non-malleability
- standard model: POWHF+NIZKPoK
- applications:
  - partially instantiate RO in the Bellare-Rogaway PKE
  - enhance security of client-sever cryptographic puzzle

Non-Malleable One-Way/Hash Functions (NMOWHF)

[Boldyreva, Cash, Fischlin, and Warinschi, Asiacrypt 2009]

- simulation-based non-malleability
- standard model: POWHF+NIZKPoK
- applications:
  - partially instantiate RO in the Bellare-Rogaway PKE
  - enhance security of client-sever cryptographic puzzle

☹ simulation-based NM: too strong + hard to work with

Non-Malleable One-Way/Hash Functions (NMOWHF)

[Boldyreva, Cash, Fischlin, and Warinschi, Asiacrypt 2009]

- simulation-based non-malleability
- standard model: POWHF+NIZKPoK
- applications:
  - partially instantiate RO in the Bellare-Rogaway PKE
  - enhance security of client-sever cryptographic puzzle

☹ simulation-based NM: too strong + hard to work with

[Baecher, Fischlin, and Schröder, CT-RSA 2011]

- game-based NM w.r.t. admissible transformation class Φ
- RO model: Merkle-Damgård transformation is Φ^{xor}-NM
- suffice for the RO-replacement of the Bellare-Rogaway PKE

Motivations

The state-of-art about NMFs

- the function is already OW and (possibly) probabilistic
  - blur the relation between OW and NM
  - same input will not lead to the same output
- current game-based notion is not strong enough
- no efficient construction in the standard model
- few applications

Motivations

The state-of-art about NMFs

- the function is already OW and (possibly) probabilistic
  - blur the relation between OW and NM
  - same input will not lead to the same output
- current game-based notion is not strong enough
- no efficient construction in the standard model
- few applications

This work: OW & probabilistic F $\rightarrow$ deterministic F

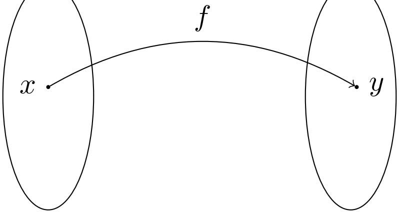
Goals

- seek a strong yet handy non-malleability notion
- figure out relations between NM and OW
- provide efficient construction without RO
- find new interesting applications

Outline

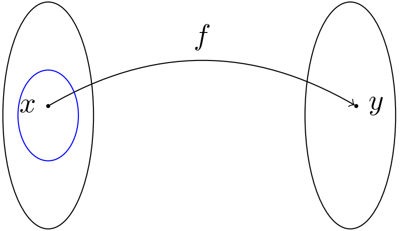
Efficient Computable Deterministic Functions

$$X \xrightarrow{f} Y$$



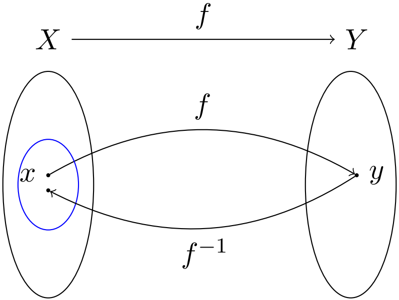
Efficient Computable Deterministic Functions

$$X \xrightarrow{f} Y$$



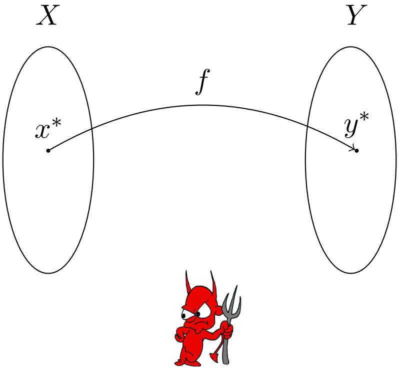
- poly-to-1: $\forall y \in Y$, $|f^{-1}(y)| \leq \mathsf{poly}(\lambda)$.

Efficient Computable Deterministic Functions

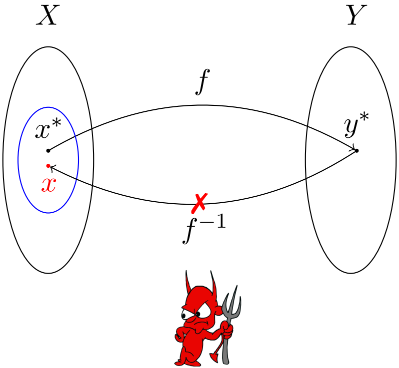


- poly-to-1: $\forall y \in Y$, $|f^{-1}(y)| \leq \mathsf{poly}(\lambda)$.
- trapdoor: f^{-1} is efficiently computable with a *td*.

(Adaptive) One-Wayness

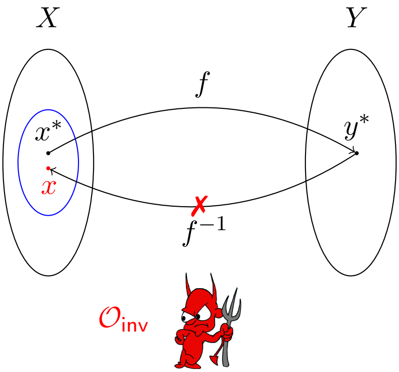


(Adaptive) One-Wayness



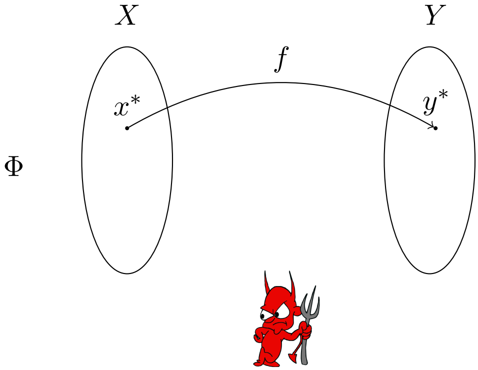
- OW: $\Pr[\mathcal{A}(f, y^* \leftarrow f(x^*)) \in f^{-1}(y^*)] = \mathsf{negl}(\lambda)$.

(Adaptive) One-Wayness

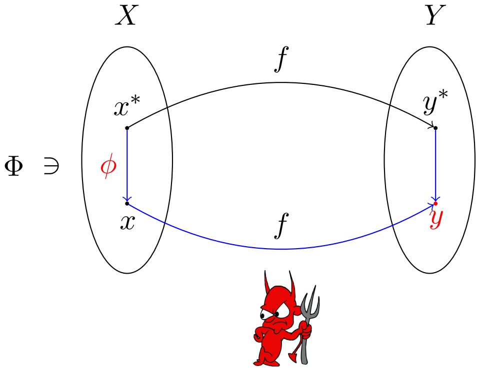


- OW: $\Pr[\mathcal{A}(f, y^* \leftarrow f(x^*)) \in f^{-1}(y^*)] = \mathsf{negl}(\lambda)$.
- AOW: $\Pr[\mathcal{A}^{\mathcal{O}_{\mathsf{inv}}}(f, y^* \leftarrow f(x^*)) \in f^{-1}(y^*)] = \mathsf{negl}(\lambda)$.

(Adaptive) Φ-Non-Malleability

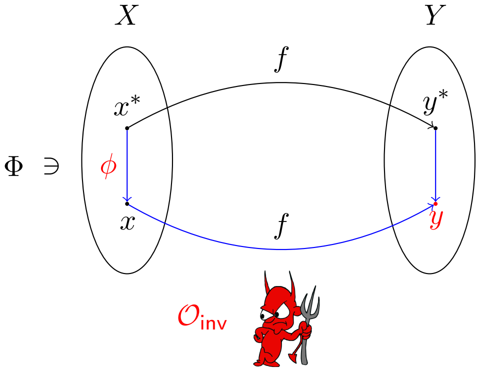


(Adaptive) Φ-Non-Malleability



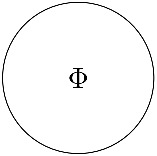
- NM: $\Pr[\mathcal{A}(f, y^*) = (\phi, y) \text{ s.t. } y = f(\phi(x^*))] = \mathsf{negl}(\lambda)$.

(Adaptive) Φ-Non-Malleability



- NM: $\Pr[\mathcal{A}(f, y^*) = (\phi, y) \text{ s.t. } y = f(\phi(x^*))] = \mathsf{negl}(\lambda)$.
- ANM: $\Pr[\mathcal{A}^{\mathcal{O}_{\mathsf{inv}}}(f, y^*) = (\phi, y) \text{ s.t. } y = f(\phi(x^*))] = \mathsf{negl}(\lambda)$.

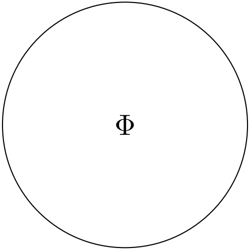
Our NM Notion v.s. Baecher et al.'s NM Notion



Common

- both of the NM notions are defined w.r.t. Φ.

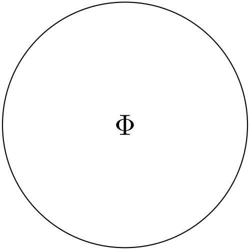
Our NM Notion v.s. Baecher et al.'s NM Notion



Common

- both of the NM notions are defined w.r.t. Φ.
- NM notions become stronger when Φ is larger

Our NM Notion v.s. Baecher et al.'s NM Notion



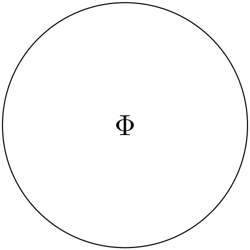
Common

- both of the NM notions are defined w.r.t. Φ.
- NM notions become stronger when Φ is larger

Difference

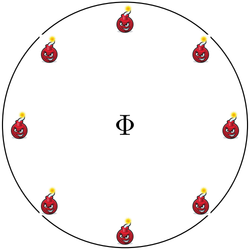
- $\underline{\phi \in \Phi}$ v.s. $\underline{\phi \in \Phi \wedge \phi(x^*) \neq x^*}$
- Φ cannot contain ϕ having fixed points — exclude many natural transformations — weaken the notion

Our NM Notion v.s. Baecher et al.'s NM Notion



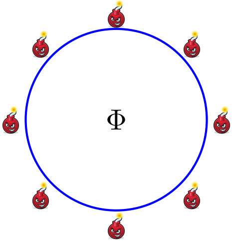
- $\mathcal{A}$'s power is completely expressed through Φ — make Φ as large as possible to yield a strong notion

Our NM Notion v.s. Baecher et al.'s NM Notion



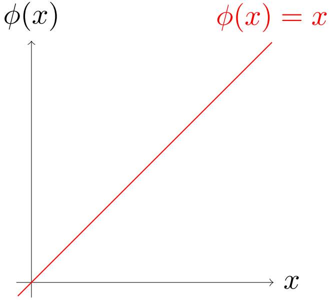
- $\mathcal{A}$'s power is completely expressed through Φ — make Φ as large as possible to yield a strong notion
- Φ may contain some dangerous $T \Rightarrow \Phi$-NM is impossible

Our NM Notion v.s. Baecher et al.'s NM Notion



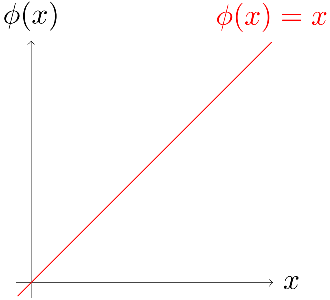
- $\mathcal{A}$'s power is completely expressed through Φ — make Φ as large as possible to yield a strong notion
- Φ may contain some dangerous $T \Rightarrow \Phi$-NM is impossible
- find a safe broader of admissible Φ to exclude dangerous T

Dangerous Transformations



identity transformation: id

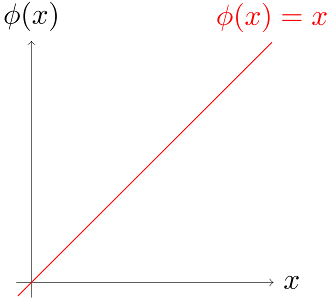
Dangerous Transformations



identity transformation: id

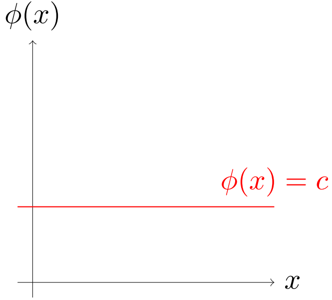
$$\mathcal{A} : f(\mathsf{id}(x^*)) = y^*$$

Dangerous Transformations



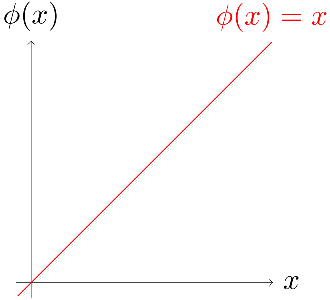
identity transformation: id

$\mathcal{A} : f(\mathsf{id}(x^*)) = y^*$



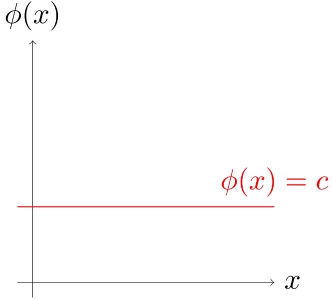
constant transformations: ϕ_c

Dangerous Transformations



identity transformation: id

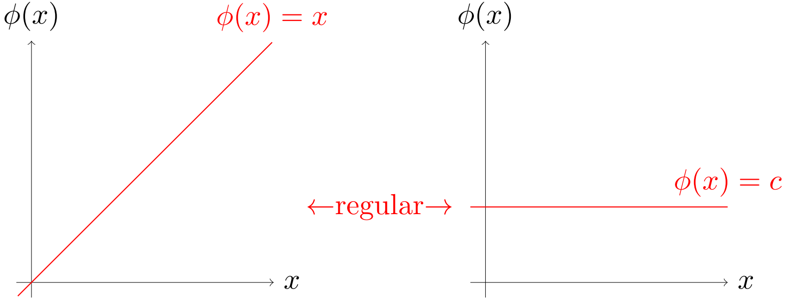
$\mathcal{A} : f(\mathsf{id}(x^*)) = y^*$



constant transformations: ϕ_c

$\mathcal{A} : f(\phi_c(x^*)) = f(c)$

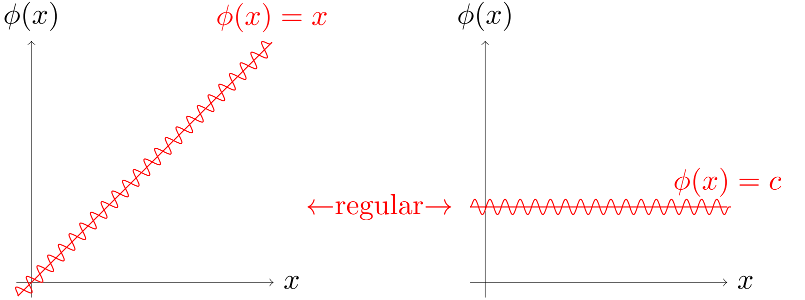
Dangerous Transformations



identity transformation: id
$\mathcal{A} : f(\mathsf{id}(x^*)) = y^*$
record all information

constant transformations: ϕ_c
$\mathcal{A} : f(\phi_c(x^*)) = f(c)$
lose all information

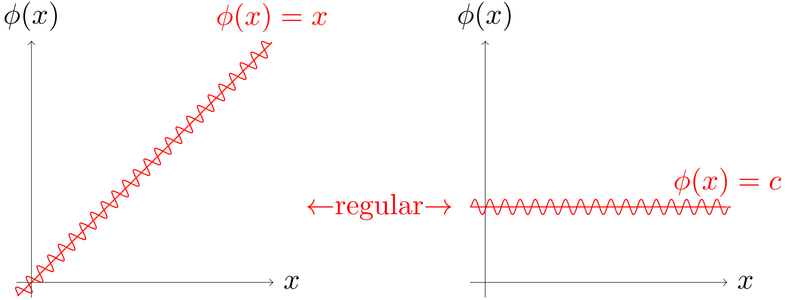
Dangerous Transformations



identity transformation: id constant transformations: ϕ_c

$$\boxed{\text{dangerous: regular transformations + “near” ones}}$$

Dangerous Transformations

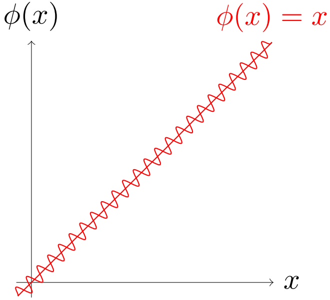


identity transformation: id constant transformations: ϕ_c

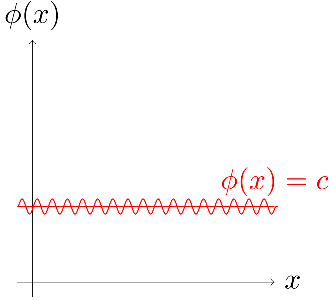
$\boxed{\text{dangerous: regular transformations + "near" ones}}$

intersection of transformations $X_{\phi,\phi'} = \{x : \phi(x) = \phi'(x)\}$
distance between transformations: $\|\phi, \phi'\| = (|X| - |X_{\phi,\phi'}|)/|X|$

Dangerous Transformations



identity transformation: id



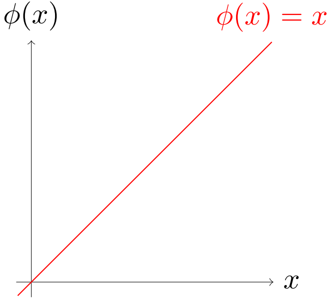
constant transformations: ϕ_c

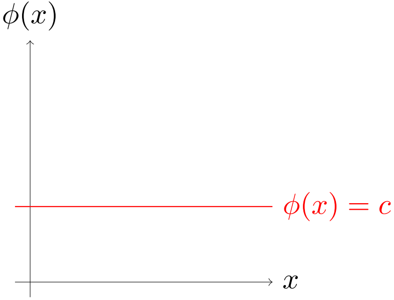
$\boxed{\text{dangerous: regular transformations + “near” ones}}$

intersection of transformations $X_{\phi,\phi'} = \{x : \phi(x) = \phi'(x)\}$
distance between transformations: $\|\phi, \phi'\| = (|X| - |X_{\phi,\phi'}|)/|X|$

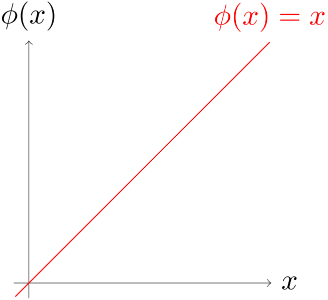
example of near: $|X_{\phi,\phi'}|/|X|$ is non-negligible in λ

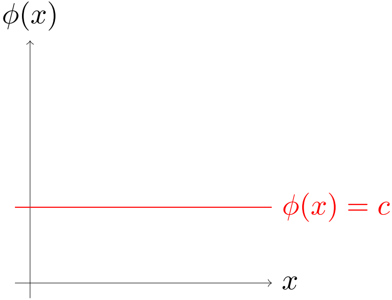
Admissible Transformation Class





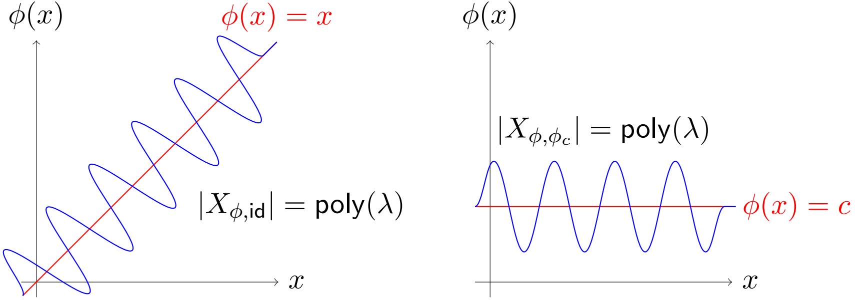
Admissible Transformation Class





Intuition: Φ contains ϕ that is far away from regular ones

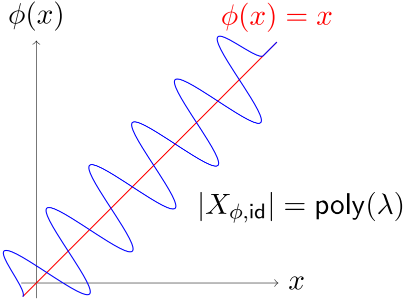
Admissible Transformation Class

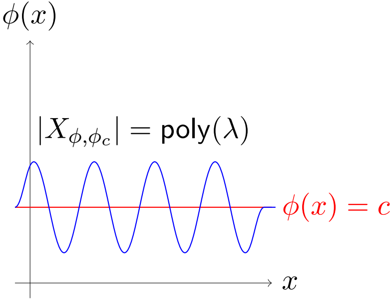


Intuition: Φ contains ϕ that is far away from regular ones

- Bounded Root Space (BRS)
  $\forall \phi \in \Phi$, RS of $\phi - \mathsf{id}$ and $\phi - \phi_c$ are poly bounded.

Admissible Transformation Class



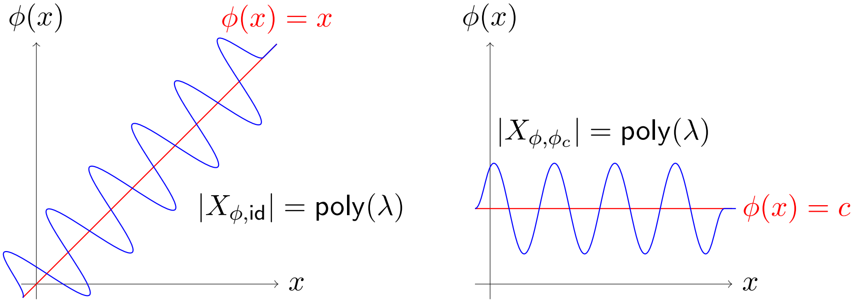


Intuition: Φ contains ϕ that is far away from regular ones

- Bounded Root Space (BRS)
  $\forall \phi \in \Phi$, RS of $\phi - \mathsf{id}$ and $\phi - \phi_c$ are poly bounded.
- Sampleable Root Space (SRS)
  $\forall \phi \in \Phi$, RS of $\phi - \mathsf{id}$ and $\phi - \phi_c$ are sampleable.

$$\mathsf{SampRS}(\phi') \xleftarrow{\mathrm{R}} \mathrm{RS}_{\phi'}$$

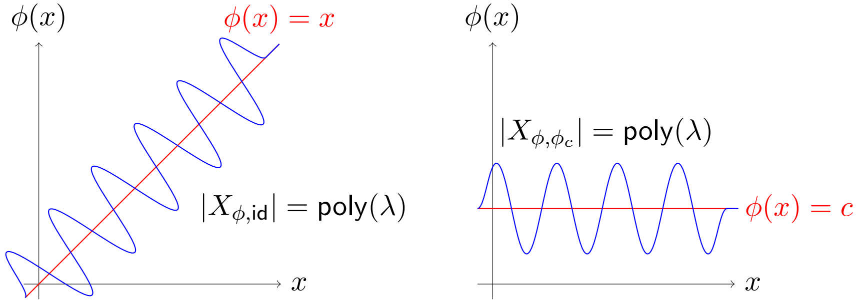
Admissible Transformation Class



Intuition: Φ contains ϕ that is far away from regular ones

$\Phi^{\text{srs}}_{\text{brs}}$

Admissible Transformation Class

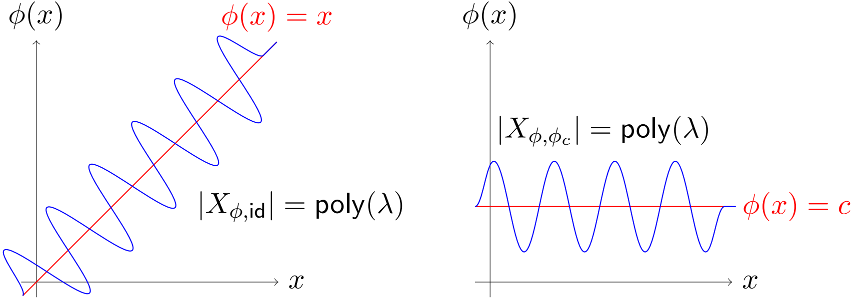


Intuition: Φ contains ϕ that is far away from regular ones

$\Phi^{\text{srs}}_{\text{brs}}$ covers most algebra-induced classes:

$\Phi^{\text{lin}} \backslash \mathsf{id}$

Admissible Transformation Class

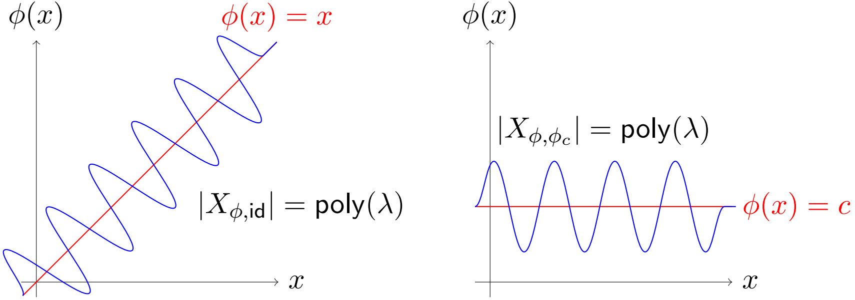


Intuition: Φ contains ϕ that is far away from regular ones

$\Phi^{\text{srs}}_{\text{brs}}$ covers most algebra-induced classes:

$\Phi^{\text{lin}} \backslash \mathsf{id}$ $\Phi^{\text{aff}} \backslash (\mathsf{id} \cup \mathsf{cf})$

Admissible Transformation Class



Intuition: Φ contains ϕ that is far away from regular ones

$\Phi^{\mathrm{srs}}_{\mathrm{brs}}$ covers most algebra-induced classes:

$\Phi^{\mathrm{lin}} \backslash \mathsf{id}$ $\quad$ $\Phi^{\mathrm{aff}} \backslash (\mathsf{id} \cup \mathsf{cf})$ $\quad$ $\Phi^{\mathrm{poly}_d} \backslash (\mathsf{id} \cup \mathsf{cf})$, $d = \mathsf{poly}(\lambda)$

Outline

Relations among One-Wayness and Non-Malleability

$$\begin{tikzcd}
\mathrm{NM} & ? & \mathrm{ANM} \\
? & & ? \\
\mathrm{OW} \arrow[rr, shift left, "/" marking] & & \mathrm{AOW} \arrow[ll, shift left]
\end{tikzcd}$$

Non-Malleability $\Rightarrow$ One-Wayness

Lemma: $\forall$ achievable Φ, Φ-NM $\Rightarrow$ OW when f is poly-to-1.

Non-Malleability $\Rightarrow$ One-Wayness

Lemma: $\forall$ achievable Φ, Φ-NM $\Rightarrow$ OW when f is poly-to-1.

Proof sketch: $\mathcal{A}$ breaks OW $\Rightarrow$ $\mathcal{B}$ breaks Φ-NM.

Non-Malleability $\Rightarrow$ One-Wayness

Lemma: $\forall$ achievable Φ, Φ-NM $\Rightarrow$ OW when f is poly-to-1.

Proof sketch: $\mathcal{A}$ breaks OW $\Rightarrow$ $\mathcal{B}$ breaks Φ-NM.

Setup: Given f and $y^* \leftarrow f(x^*)$ for $x^* \stackrel{\mathrm{R}}{\leftarrow} X$, $\mathcal{B} \looparrowright (f, y^*) \hookrightarrow \mathcal{A}$.

Lemma: $\forall$ achievable Φ, Φ-NM $\Rightarrow$ OW when f is poly-to-1.

Proof sketch: $\mathcal{A}$ breaks OW $\Rightarrow$ $\mathcal{B}$ breaks Φ-NM.

Setup: Given f and $y^* \leftarrow f(x^*)$ for $x^* \xleftarrow{R} X$, $\mathcal{B} \looparrowright (f, y^*) \hookrightarrow \mathcal{A}$.

Attack: When $\mathcal{A}$ outputs x against OW, $\mathcal{B}$ picks $\phi \xleftarrow{R} \Phi$, outputs $(\phi, f(\phi(x)))$ against NM.

Non-Malleability $\Rightarrow$ One-Wayness

Lemma: $\forall$ achievable Φ, Φ-NM $\Rightarrow$ OW when f is poly-to-1.

Proof sketch: $\mathcal{A}$ breaks OW $\Rightarrow$ $\mathcal{B}$ breaks Φ-NM.

Setup: Given f and $y^* \leftarrow f(x^*)$ for $x^* \xleftarrow{\text{R}} X$, $\mathcal{B} \hookleftarrow (f, y^*) \hookrightarrow \mathcal{A}$.

Attack: When $\mathcal{A}$ outputs x against OW, $\mathcal{B}$ picks $\phi \xleftarrow{\text{R}} \Phi$, outputs $(\phi, f(\phi(x))$ against NM.

If $\mathcal{A}$ succeeds $(x \in f^{-1}(y^*)) \Rightarrow \Pr[x = x^*] \geq 1/\mathsf{poly}(\lambda)$

Non-Malleability $\Rightarrow$ One-Wayness

Lemma: $\forall$ achievable Φ, Φ-NM $\Rightarrow$ OW when f is poly-to-1.

Proof sketch: $\mathcal{A}$ breaks OW $\Rightarrow$ $\mathcal{B}$ breaks Φ-NM.

Setup: Given f and $y^* \leftarrow f(x^*)$ for $x^* \xleftarrow{\text{R}} X$, $\mathcal{B} \looparrowright (f, y^*) \hookrightarrow \mathcal{A}$.

Attack: When $\mathcal{A}$ outputs x against OW, $\mathcal{B}$ picks $\phi \xleftarrow{\text{R}} \Phi$, outputs $(\phi, f(\phi(x))$ against NM.

If $\mathcal{A}$ succeeds $(x \in f^{-1}(y^*)) \Rightarrow \Pr[x = x^*] \geq 1/\mathsf{poly}(\lambda)$

- f is poly-to-1: at most $\mathsf{poly}(\lambda)$ preimages x s.t. $f(x) = y^*$ and they are all equally likely in $\mathcal{A}$'s view.
- The probability is taken over the choice of $x^* \xleftarrow{\text{R}} X$.

Non-Malleability $\Rightarrow$ One-Wayness

Lemma: $\forall$ achievable Φ, Φ-NM $\Rightarrow$ OW when f is poly-to-1.

Proof sketch: $\mathcal{A}$ breaks OW $\Rightarrow$ $\mathcal{B}$ breaks Φ-NM.

Setup: Given f and $y^* \leftarrow f(x^*)$ for $x^* \xleftarrow{\text{R}} X$, $\mathcal{B} \looparrowleft (f, y^*) \hookrightarrow \mathcal{A}$.

Attack: When $\mathcal{A}$ outputs x against OW, $\mathcal{B}$ picks $\phi \xleftarrow{\text{R}} \Phi$, outputs $(\phi, f(\phi(x)))$ against NM.

$$\mathsf{Adv}_{\mathcal{B}}^{\text{NM}} \geq \mathsf{Adv}_{\mathcal{A}}^{\text{OW}} / \mathsf{poly}(\lambda)$$

Non-Malleability $\Rightarrow$ One-Wayness

Lemma: $\forall$ achievable Φ, Φ-NM $\Rightarrow$ OW when f is poly-to-1.

Proof sketch: $\mathcal{A}$ breaks OW $\Rightarrow$ $\mathcal{B}$ breaks Φ-NM.

Setup: Given f and $y^* \leftarrow f(x^*)$ for $x^* \xleftarrow{\mathrm{R}} X$, $\mathcal{B} \looparrowleft (f, y^*) \hookrightarrow \mathcal{A}$.

Attack: When $\mathcal{A}$ outputs x against OW, $\mathcal{B}$ picks $\phi \xleftarrow{\mathrm{R}} \Phi$, outputs $(\phi, f(\phi(x)))$ against NM.

$$\mathsf{Adv}_{\mathcal{B}}^{\mathrm{NM}} \geq \mathsf{Adv}_{\mathcal{A}}^{\mathrm{OW}} / \mathsf{poly}(\lambda)$$

The above reduction loses a factor of $1/\mathsf{poly}(\lambda)$. When f is injective, the reduction becomes tight.

Non-Malleability $\Rightarrow$ One-Wayness

Lemma: $\forall$ achievable Φ, Φ-NM $\Rightarrow$ OW when f is poly-to-1.

Proof sketch: $\mathcal{A}$ breaks OW $\Rightarrow$ $\mathcal{B}$ breaks Φ-NM.

Setup: Given f and $y^* \leftarrow f(x^*)$ for $x^* \xleftarrow{\text{R}} X$, $\mathcal{B} \looparrowleft (f, y^*) \hookrightarrow \mathcal{A}$.

Attack: When $\mathcal{A}$ outputs x against OW, $\mathcal{B}$ picks $\phi \xleftarrow{\text{R}} \Phi$, outputs $(\phi, f(\phi(x)))$ against NM.

This lemma rigorously confirms the intuition that in common cases NM implies OW.

Lemma: OW $\not\Rightarrow$ $\Phi^{\text{srs}}_{\text{brs}}$-NM

One-Wayness $\not\Rightarrow$ Non-Malleability

Lemma: OW $\not\Rightarrow$ $\Phi^{\text{srs}}_{\text{brs}}$-NM

Proof: start point — a one-way function $f : \{0,1\}^n \to \{0,1\}^m$

One-Wayness $\not\Rightarrow$ Non-Malleability

Lemma: OW $\not\Rightarrow$ $\Phi^{\text{srs}}_{\text{brs}}$-NM

Proof: start point — a one-way function $f : \{0,1\}^n \to \{0,1\}^m$

$f \to f'$: still OW but malleable w.r.t. $\Phi^{\text{srs}}_{\text{brs}}$

One-Wayness $\not\Rightarrow$ Non-Malleability

Lemma: OW $\not\Rightarrow$ $\Phi_{\text{brs}}^{\text{srs}}$-NM

Proof: start point — a one-way function $f : \{0,1\}^n \to \{0,1\}^m$

$f \to f'$: still OW but malleable w.r.t. $\Phi_{\text{brs}}^{\text{srs}}$

$$\{0,1\}^{n+1} \to \{0,1\}^{m+1} \sim f'(x||\beta) := f(x)||\beta$$

One-Wayness $\not\Rightarrow$ Non-Malleability

Lemma: OW $\not\Rightarrow$ $\Phi^{\text{srs}}_{\text{brs}}$-NM

Proof: start point — a one-way function $f : \{0,1\}^n \to \{0,1\}^m$

$f \to f'$: still OW but malleable w.r.t. $\Phi^{\text{srs}}_{\text{brs}}$

$$\{0,1\}^{n+1} \to \{0,1\}^{m+1} \sim f'(x||\beta) := f(x)||\beta$$

Claim 1: f' is OW (inherits OW from that of f)

Lemma: OW $\not\Rightarrow$ $\Phi^{\text{srs}}_{\text{brs}}$-NM

Proof: start point — a one-way function $f : \{0,1\}^n \to \{0,1\}^m$

$f \to f'$: still OW but malleable w.r.t. $\Phi^{\text{srs}}_{\text{brs}}$

$$\{0,1\}^{n+1} \to \{0,1\}^{m+1} \sim f'(x||\beta) := f(x)||\beta$$

Claim 1: f' is OW (inherits OW from that of f)

Claim 2: f' is $(\Phi^{\text{xor}} \setminus \mathsf{id})$-malleable

Lemma: OW $\not\Rightarrow$ $\Phi^{\mathrm{srs}}_{\mathrm{brs}}$-NM

Proof: start point — a one-way function $f : \{0,1\}^n \to \{0,1\}^m$

$f \to f'$: still OW but malleable w.r.t. $\Phi^{\mathrm{srs}}_{\mathrm{brs}}$

$$\{0,1\}^{n+1} \to \{0,1\}^{m+1} \sim f'(x||\beta) := f(x)||\beta$$

Claim 1: f' is OW (inherits OW from that of f)

Claim 2: f' is $(\Phi^{\mathrm{xor}} \backslash \mathsf{id})$-malleable

Given f' and $y'^* \leftarrow f'(x'^*)$, $\mathcal{A}'$ parses $y'^* = y^*||\beta^*$, sets $a = 0^n||1$, outputs ϕ_a and $y' = y^*||(\beta^* \oplus 1)$.

One-Wayness $\not\Rightarrow$ Non-Malleability

Lemma: OW $\not\Rightarrow$ $\Phi_{\mathrm{brs}}^{\mathrm{srs}}$-NM

Proof: start point — a one-way function $f : \{0,1\}^n \to \{0,1\}^m$

$f \to f'$: still OW but malleable w.r.t. $\Phi_{\mathrm{brs}}^{\mathrm{srs}}$

$$\{0,1\}^{n+1} \to \{0,1\}^{m+1} \sim f'(x||\beta) := f(x)||\beta$$

Claim 1: f' is OW (inherits OW from that of f)

Claim 2: f' is $(\Phi^{\mathrm{xor}} \backslash \mathsf{id})$-malleable

Given f' and $y'^* \leftarrow f'(x'^*)$, $\mathcal{A}'$ parses $y'^* = y^*||\beta^*$, sets $a = 0^n||1$, outputs ϕ_a and $y' = y^*||(\beta^* \oplus 1)$.

- $\phi_a \in \Phi^{\mathrm{xor}} \backslash \mathsf{id} \subset \Phi_{\mathrm{brs}}^{\mathrm{srs}}$;
- $y' = f'(x^*||(\beta^* \oplus 1)) = f'(x^*||\beta^* \oplus 0^n||1) = f'(\phi_a(x'^*))$

One-Wayness $\not\Rightarrow$ Non-Malleability

Lemma: OW $\not\Rightarrow$ $\Phi^{\mathrm{srs}}_{\mathrm{brs}}$-NM

more simple and intuitive counterexample: homomorphic OWF

$$\forall x \in D : f(\phi(x)) = \phi(f(x)) \text{ e.g. } f(x) = g^x$$

Lemma: OW $\not\Rightarrow$ $\Phi^{\mathrm{srs}}_{\mathrm{brs}}$-NM

more simple and intuitive counterexample: homomorphic OWF

$$\forall x \in D : f(\phi(x)) = \phi(f(x)) \text{ e.g. } f(x) = g^x$$

- easily malleable since $f(x^*) = y^*$ implies $f(\phi(x^*)) = \phi(y^*)$

One-Wayness $\not\Rightarrow$ Non-Malleability

Lemma: OW $\not\Rightarrow$ $\Phi^{\mathrm{srs}}_{\mathrm{brs}}$-NM

more simple and intuitive counterexample: homomorphic OWF

$$\forall x \in D : f(\phi(x)) = \phi(f(x)) \text{ e.g. } f(x) = g^x$$

- easily malleable since $f(x^*) = y^*$ implies $f(\phi(x^*)) = \phi(y^*)$
- such counterexample usually requires number-theoretic assumptions

One-Wayness $\not\Rightarrow$ Non-Malleability

Lemma: OW $\not\Rightarrow$ $\Phi^{\text{srs}}_{\text{brs}}$-NM

more simple and intuitive counterexample: homomorphic OWF

$$\forall x \in D : f(\phi(x)) = \phi(f(x)) \text{ e.g. } f(x) = g^x$$

- easily malleable since $f(x^*) = y^*$ implies $f(\phi(x^*)) = \phi(y^*)$
- such counterexample usually requires number-theoretic assumptions

functions with nice algebraic structure are unlikely to be non-malleable

Adaptive Non-Malleability $\Rightarrow$ Adaptive One-Wayness

Lemma: $\forall$ achievable Φ, Φ-ANM $\Rightarrow$ AOW when f is poly-to-1.

Adaptive Non-Malleability $\Rightarrow$ Adaptive One-Wayness

Lemma: $\forall$ achievable Φ, Φ-ANM $\Rightarrow$ AOW when f is poly-to-1.

The proof is similar to the non-adaptive setting.

Adaptive One-Wayness $\Rightarrow$ Adaptive Non-Malleability

Lemma: AOW $\Rightarrow \Phi^{\mathrm{srs}}_{\mathrm{brs}}$-ANM when f is injective.

Adaptive One-Wayness $\Rightarrow$ Adaptive Non-Malleability

Lemma: AOW $\Rightarrow$ $\Phi^{\mathrm{srs}}_{\mathrm{brs}}$-ANM when f is injective.

High level idea: $\mathcal{A}$ against ANM $\Rightarrow$ $\mathcal{B}$ against AOW

Adaptive One-Wayness $\Rightarrow$ Adaptive Non-Malleability

Lemma: AOW $\Rightarrow \Phi^{\mathrm{srs}}_{\mathrm{brs}}$-ANM when f is injective.

High level idea: $\mathcal{A}$ against ANM $\Rightarrow \mathcal{B}$ against AOW

finding x^* appears harder than mauling its image

Adaptive One-Wayness $\Rightarrow$ Adaptive Non-Malleability

Lemma: AOW $\Rightarrow \Phi^{\mathrm{srs}}_{\mathrm{brs}}$-ANM when f is injective.

High level idea: $\mathcal{A}$ against ANM $\Rightarrow \mathcal{B}$ against AOW

finding x^* appears harder than mauling its image

Technical hurdle: how to utilize $\mathcal{A}$'s power to break AOW

Adaptive One-Wayness ⇒ Adaptive Non-Malleability

Lemma: AOW ⇒ $\Phi_{\text{brs}}^{\text{srs}}$-ANM when f is injective.

- the challenge instance of OW already provides $\mathcal{B}$ an equation about x^*, $\underline{f(x^*) = y^*}$

Adaptive One-Wayness $\Rightarrow$ Adaptive Non-Malleability

Lemma: AOW $\Rightarrow \Phi_{\text{brs}}^{\text{srs}}$-ANM when f is injective.

- the challenge instance of OW already provides $\mathcal{B}$ an equation about x^*, $\underline{f(x^*) = y^*}$
- $\mathcal{A}$'s solution (ϕ, y) against NM provides $\mathcal{B}$ another equation about x^*, $\underline{f(\phi(x^*)) = y}$

Adaptive One-Wayness $\Rightarrow$ Adaptive Non-Malleability

Lemma: AOW $\Rightarrow \Phi_{\text{brs}}^{\text{srs}}$-ANM when f is injective.

- the challenge instance of OW already provides $\mathcal{B}$ an equation about x^*, $\underline{f(x^*) = y^*}$
- $\mathcal{A}$'s solution (ϕ, y) against NM provides $\mathcal{B}$ another equation about x^*, $\underline{f(\phi(x^*)) = y}$

☹ these two equations are hard to solve due to the involvement of f, which unlikely has nice algebraic structure.

Adaptive One-Wayness $\Rightarrow$ Adaptive Non-Malleability

Lemma: AOW $\Rightarrow$ $\Phi_{\mathrm{brs}}^{\mathrm{srs}}$-ANM when f is injective.

$$\begin{tikzcd} x^* \arrow[r, "f"] \arrow[d, "\phi"'] & y^* \arrow[d] \\ x \arrow[r, "f"] & y \end{tikzcd}$$

☺ by utilizing the injectivity of f and $\mathcal{O}_{\mathsf{inv}}$, $\mathcal{B}$ can obtain a new solvable equation about x^*. (break $\mathcal{A}$'s solution into two cases)

Adaptive One-Wayness ⇒ Adaptive Non-Malleability

Lemma: AOW ⇒ $\Phi^{\text{srs}}_{\text{brs}}$-ANM when f is injective.

$$
\begin{tikzcd}
x^* \arrow[r, "f"] \arrow[d, "\phi"'] & y^* \arrow[d] \\
x \arrow[r, "f"] & y
\end{tikzcd}
$$

☺ by utilizing the injectivity of f and $\mathcal{O}_{\mathsf{inv}}$, $\mathcal{B}$ can obtain a new solvable equation about x^*. (break $\mathcal{A}$'s solution into two cases)

- $y = y^*$: injectivity of $f \Rightarrow \phi(x^*) = x^*$

Adaptive One-Wayness $\Rightarrow$ Adaptive Non-Malleability

Lemma: AOW $\Rightarrow$ $\Phi_{\text{brs}}^{\text{srs}}$-ANM when f is injective.

$$\begin{tikzcd}
x^* \arrow[r, "f"] \arrow[d, "\phi"'] & y^* \arrow[d] \\
x \arrow[r, "f"] & y
\end{tikzcd}$$

☺ by utilizing the injectivity of f and $\mathcal{O}_{\mathsf{inv}}$, $\mathcal{B}$ can obtain a new solvable equation about x^*. (break $\mathcal{A}$'s solution into two cases)

- $y = y^*$: injectivity of $f \Rightarrow \phi(x^*) = x^*$
- $y \neq y^*$: injectivity of f + $\boxed{x \leftarrow \mathcal{O}_{\mathsf{inv}}(y)}$ $\Rightarrow \phi(x^*) = x$

Adaptive One-Wayness ⇒ Adaptive Non-Malleability

Lemma: AOW ⇒ $\Phi_{\text{brs}}^{\text{srs}}$-ANM when f is injective.

$$\begin{tikzcd}
x^* \arrow[r, "f"] \arrow[d, "\phi"'] & y^* \arrow[d] \\
x \arrow[r, "f"] & y
\end{tikzcd}$$

☺ by utilizing the injectivity of f and $\mathcal{O}_{\mathsf{inv}}$, $\mathcal{B}$ can obtain a new solvable equation about x^*. (break $\mathcal{A}$'s solution into two cases)

- $y = y^*$: injectivity of $f \Rightarrow \phi(x^*) = x^*$
- $y \neq y^*$: injectivity of f + $\boxed{x \leftarrow \mathcal{O}_{\mathsf{inv}}(y)} \Rightarrow \phi(x^*) = x$

In either case, $\mathcal{B}$ can successfully

1. confine x^* in a poly-bounded space (BRS property),
2. extract it with noticeable probability (SRS property).

Adaptive One-Wayness ⇒ Adaptive Non-Malleability

Lemma: AOW ⇒ $\Phi_{\text{brs}}^{\text{srs}}$-ANM when f is injective.

$$\begin{tikzcd}
x^* \arrow[r, "f"] \arrow[d, "\phi"'] & y^* \arrow[d] \\
x \arrow[r, "f"] & y
\end{tikzcd}$$

☺ by utilizing the injectivity of f and $\mathcal{O}_{\mathsf{inv}}$, $\mathcal{B}$ can obtain a new solvable equation about x^*. (break $\mathcal{A}$'s solution into two cases)

- $y = y^*$: injectivity of $f \Rightarrow \phi(x^*) = x^*$
- $y \neq y^*$: injectivity of f + $\boxed{x \leftarrow \mathcal{O}_{\mathsf{inv}}(y)} \Rightarrow \phi(x^*) = x$

In either case, $\mathcal{B}$ can successfully

1. confine x^* in a poly-bounded space (BRS property),
2. extract it with noticeable probability (SRS property).

Injectivity is necessary to guarantee $\mathcal{B}$ obtains a correct equation.

Adaptive One-Wayness $\Rightarrow$ Adaptive Non-Malleability

Lemma: AOW $\Rightarrow \Phi^{\mathrm{srs}}_{\mathrm{brs}}$-ANM when f is injective.

Proof sketch: $\mathcal{A}$ against ANM $\Rightarrow \mathcal{B}$ against AOW

Adaptive One-Wayness $\Rightarrow$ Adaptive Non-Malleability

Lemma: AOW $\Rightarrow$ $\Phi^{\mathrm{srs}}_{\mathrm{brs}}$-ANM when f is injective.

Proof sketch: $\mathcal{A}$ against ANM $\Rightarrow$ $\mathcal{B}$ against AOW

Setup: Given f and $y^* \leftarrow f(x^*)$ for $x^* \xleftarrow{\mathrm{R}} X$, $\mathcal{B} \looparrowright (f, y^*) \hookrightarrow \mathcal{A}$.

Adaptive One-Wayness $\Rightarrow$ Adaptive Non-Malleability

Lemma: AOW $\Rightarrow \Phi^{\mathrm{srs}}_{\mathrm{brs}}$-ANM when f is injective.

Proof sketch: $\mathcal{A}$ against ANM $\Rightarrow \mathcal{B}$ against AOW

Setup: Given f and $y^* \leftarrow f(x^*)$ for $x^* \xleftarrow{\mathrm{R}} X$, $\mathcal{B} \looparrowleft (f, y^*) \hookrightarrow \mathcal{A}$.

Attack: $\mathcal{A} \rightleftarrows \mathcal{O}_{\mathsf{inv}} \leftrightsquigarrow \mathcal{B} \rightleftarrows \mathcal{CH}$. When $\mathcal{A}$ outputs its solution (ϕ, y) against ANM, $\mathcal{B}$ proceeds as follows:

Adaptive One-Wayness $\Rightarrow$ Adaptive Non-Malleability

Lemma: AOW $\Rightarrow \Phi_{\mathrm{brs}}^{\mathrm{srs}}$-ANM when f is injective.

Proof sketch: $\mathcal{A}$ against ANM $\Rightarrow \mathcal{B}$ against AOW

Setup: Given f and $y^* \leftarrow f(x^*)$ for $x^* \xleftarrow{\mathrm{R}} X$, $\mathcal{B} \looparrowleft (f, y^*) \hookrightarrow \mathcal{A}$.

Attack: $\mathcal{A} \rightleftarrows \mathcal{O}_{\mathsf{inv}} \leftrightsquigarrow \mathcal{B} \rightleftarrows \mathcal{CH}$. When $\mathcal{A}$ outputs its solution (ϕ, y) against ANM, $\mathcal{B}$ proceeds as follows:

- $y = y^*$: $\mathcal{B}$ runs $\mathsf{SampRS}(\phi')$ to output a random solution of $\phi'(\alpha) = 0$ where $\phi'(\alpha) = \phi(\alpha) - \alpha$.

Adaptive One-Wayness $\Rightarrow$ Adaptive Non-Malleability

Lemma: AOW $\Rightarrow$ $\Phi^{\text{srs}}_{\text{brs}}$-ANM when f is injective.

Proof sketch: $\mathcal{A}$ against ANM $\Rightarrow$ $\mathcal{B}$ against AOW

Setup: Given f and $y^* \leftarrow f(x^*)$ for $x^* \xleftarrow{\text{R}} X$, $\mathcal{B} \nleftrightarrow (f, y^*) \hookrightarrow \mathcal{A}$.

Attack: $\mathcal{A} \rightleftarrows \mathcal{O}_{\mathsf{inv}} \leftrightsquigarrow \mathcal{B} \rightleftarrows \mathcal{CH}$. When $\mathcal{A}$ outputs its solution (ϕ, y) against ANM, $\mathcal{B}$ proceeds as follows:

- $y = y^*$: $\mathcal{B}$ runs $\mathsf{SampRS}(\phi')$ to output a random solution of $\phi'(\alpha) = 0$ where $\phi'(\alpha) = \phi(\alpha) - \alpha$.
- $y \neq y^*$: $\mathcal{B} \rightleftarrows x \leftarrow \mathcal{O}_{\mathsf{inv}}(y)$, runs $\mathsf{SampRS}(\phi'')$ to output a random solution of $\phi''(\alpha) = 0$ where $\phi''(\alpha) = \phi(\alpha) - x$.

Adaptive One-Wayness $\Rightarrow$ Adaptive Non-Malleability

Lemma: AOW $\Rightarrow$ $\Phi^{\text{srs}}_{\text{brs}}$-ANM when f is injective.

Proof sketch: $\mathcal{A}$ against ANM $\Rightarrow$ $\mathcal{B}$ against AOW

Setup: Given f and $y^* \leftarrow f(x^*)$ for $x^* \xleftarrow{\text{R}} X$, $\mathcal{B} \looparrowleft (f, y^*) \hookrightarrow \mathcal{A}$.

Attack: $\mathcal{A} \rightleftarrows \mathcal{O}_{\mathsf{inv}} \leftrightsquigarrow \mathcal{B} \rightleftarrows \mathcal{CH}$. When $\mathcal{A}$ outputs its solution (ϕ, y) against ANM, $\mathcal{B}$ proceeds as follows:

- $y = y^*$: $\mathcal{B}$ runs $\mathsf{SampRS}(\phi')$ to output a random solution of $\phi'(\alpha) = 0$ where $\phi'(\alpha) = \phi(\alpha) - \alpha$.
- $y \neq y^*$: $\mathcal{B} \rightleftarrows x \leftarrow \mathcal{O}_{\mathsf{inv}}(y)$, runs $\mathsf{SampRS}(\phi'')$ to output a random solution of $\phi''(\alpha) = 0$ where $\phi''(\alpha) = \phi(\alpha) - x$.

If $\mathcal{A}$ succeeds ($f(\phi(x^*)) = y$), injectivity of f $\Rightarrow$ x^* is a root of ϕ' or ϕ''. BRS & SRS $\Rightarrow$ $\Pr[\mathsf{SampRS}(\phi', \phi'') = x^*] = 1/\mathsf{poly}(\lambda)$.

Adaptive One-Wayness $\Rightarrow$ Adaptive Non-Malleability

Lemma: AOW $\Rightarrow \Phi_{\text{brs}}^{\text{srs}}$-ANM when f is injective.

Proof sketch: $\mathcal{A}$ against ANM $\Rightarrow \mathcal{B}$ against AOW

Setup: Given f and $y^* \leftarrow f(x^*)$ for $x^* \xleftarrow{\text{R}} X$, $\mathcal{B} \looparrowleft (f, y^*) \hookrightarrow \mathcal{A}$.

Attack: $\mathcal{A} \rightleftarrows \mathcal{O}_{\mathsf{inv}} \leftrightsquigarrow \mathcal{B} \rightleftarrows \mathcal{CH}$. When $\mathcal{A}$ outputs its solution (ϕ, y) against ANM, $\mathcal{B}$ proceeds as follows:

- $y = y^*$: $\mathcal{B}$ runs $\mathsf{SampRS}(\phi')$ to output a random solution of $\phi'(\alpha) = 0$ where $\phi'(\alpha) = \phi(\alpha) - \alpha$.
- $y \neq y^*$: $\mathcal{B} \rightleftarrows x \leftarrow \mathcal{O}_{\mathsf{inv}}(y)$, runs $\mathsf{SampRS}(\phi'')$ to output a random solution of $\phi''(\alpha) = 0$ where $\phi''(\alpha) = \phi(\alpha) - x$.

If $\mathcal{A}$ succeeds ($f(\phi(x^*)) = y$), injectivity of $f \Rightarrow x^*$ is a root of ϕ' or ϕ''. BRS & SRS $\Rightarrow \Pr[\mathsf{SampRS}(\phi', \phi'') = x^*] = 1/\mathsf{poly}(\lambda)$.

Note: Here Pr is taken over SampRS but not $x^* \xleftarrow{\text{R}} X$.

Adaptive One-Wayness $\Rightarrow$ Adaptive Non-Malleability

Lemma: AOW $\Rightarrow \Phi^{\mathrm{srs}}_{\mathrm{brs}}$-ANM when f is injective.

Proof sketch: $\mathcal{A}$ against ANM $\Rightarrow \mathcal{B}$ against AOW

Setup: Given f and $y^* \leftarrow f(x^*)$ for $x^* \xleftarrow{\mathrm{R}} X$, $\mathcal{B} \nleftrightarrow (f, y^*) \hookrightarrow \mathcal{A}$.

Attack: $\mathcal{A} \rightleftarrows \mathcal{O}_{\mathsf{inv}} \leftrightsquigarrow \mathcal{B} \rightleftarrows \mathcal{CH}$. When $\mathcal{A}$ outputs its solution (ϕ, y) against ANM, $\mathcal{B}$ proceeds as follows:

- $y = y^*$: $\mathcal{B}$ runs $\mathsf{SampRS}(\phi')$ to output a random solution of $\phi'(\alpha) = 0$ where $\phi'(\alpha) = \phi(\alpha) - \alpha$.
- $y \neq y^*$: $\mathcal{B} \rightleftarrows x \leftarrow \mathcal{O}_{\mathsf{inv}}(y)$, runs $\mathsf{SampRS}(\phi'')$ to output a random solution of $\phi''(\alpha) = 0$ where $\phi''(\alpha) = \phi(\alpha) - x$.

$$\mathsf{Adv}^{\mathrm{anm}}_{\mathcal{B}} \geq \mathsf{Adv}^{\mathrm{aow}}_{\mathcal{A}} / \mathsf{poly}(\lambda)$$

Adaptive One-Wayness $\Rightarrow$ Adaptive Non-Malleability

Lemma: AOW $\Rightarrow \Phi_{\text{brs}}^{\text{srs}}$-ANM when f is injective.

Proof sketch: $\mathcal{A}$ against ANM $\Rightarrow \mathcal{B}$ against AOW

Setup: Given f and $y^* \leftarrow f(x^*)$ for $x^* \xleftarrow{\text{R}} X$, $\mathcal{B} \looparrowleft (f, y^*) \hookrightarrow \mathcal{A}$.

Attack: $\mathcal{A} \rightleftarrows \mathcal{O}_{\mathsf{inv}} \leftrightsquigarrow \mathcal{B} \rightleftarrows \mathcal{CH}$. When $\mathcal{A}$ outputs its solution (ϕ, y) against ANM, $\mathcal{B}$ proceeds as follows:

- $y = y^*$: $\mathcal{B}$ runs $\mathsf{SampRS}(\phi')$ to output a random solution of $\phi'(\alpha) = 0$ where $\phi'(\alpha) = \phi(\alpha) - \alpha$.
- $y \neq y^*$: $\mathcal{B} \rightleftarrows x \leftarrow \mathcal{O}_{\mathsf{inv}}(y)$, runs $\mathsf{SampRS}(\phi'')$ to output a random solution of $\phi''(\alpha) = 0$ where $\phi''(\alpha) = \phi(\alpha) - x$.

core technique of reduction — equation solving

1. use $\mathcal{A}$'s NM solution to establish equation
2. exploit BRS and SRS to extract x^*

Non-Malleability $\not\Rightarrow$ Adaptive Non-Malleability

Lemma: NM $\not\Rightarrow$ ANM for any Φ when f is poly-to-1.

Non-Malleability $\not\Rightarrow$ Adaptive Non-Malleability

Lemma: NM $\not\Rightarrow$ ANM for any Φ when f is poly-to-1.

Anti-Intuition: $\mathcal{O}_{\mathsf{inv}}$ seems useless against NM

Lemma: NM $\nRightarrow$ ANM for any Φ when f is poly-to-1.

Anti-Intuition: $\mathcal{O}_{\mathsf{inv}}$ seems useless against NM

$\mathcal{A}$ against ANM: given f and $y^* \leftarrow f(x^*)$, aims to output (ϕ, y) s.t. $f(\phi(x^*)) = y$ with the help of $\mathcal{O}_{\mathsf{inv}}$. Since querying $\mathcal{O}_{\mathsf{inv}}$ at y^* is not allowed, the only strategy is:

Non-Malleability $\not\Rightarrow$ Adaptive Non-Malleability

Lemma: NM $\not\Rightarrow$ ANM for any Φ when f is poly-to-1.

Anti-Intuition: $\mathcal{O}_{\mathsf{inv}}$ seems useless against NM

$\mathcal{A}$ against ANM: given f and $y^* \leftarrow f(x^*)$, aims to output (ϕ, y) s.t. $f(\phi(x^*)) = y$ with the help of $\mathcal{O}_{\mathsf{inv}}$. Since querying $\mathcal{O}_{\mathsf{inv}}$ at y^* is not allowed, the only strategy is:

<u>pick $y \xleftarrow{\mathrm{R}} Y$; obtain $x \leftarrow \mathcal{O}_{\mathsf{inv}}(y)$; compute ϕ s.t. $\phi(x^*) = x$.</u>

Non-Malleability $\not\Rightarrow$ Adaptive Non-Malleability

Lemma: NM $\not\Rightarrow$ ANM for any Φ when f is poly-to-1.

Anti-Intuition: $\mathcal{O}_{\mathsf{inv}}$ seems useless against NM

$\mathcal{A}$ against ANM: given f and $y^* \leftarrow f(x^*)$, aims to output (ϕ, y) s.t. $f(\phi(x^*)) = y$ with the help of $\mathcal{O}_{\mathsf{inv}}$. Since querying $\mathcal{O}_{\mathsf{inv}}$ at y^* is not allowed, the only strategy is:

pick $y \xleftarrow{\text{R}} Y$; obtain $x \leftarrow \mathcal{O}_{\mathsf{inv}}(y)$; compute ϕ s.t. $\phi(x^*) = x$.

NM $\Rightarrow$ OW when f is poly-to-1 $\Rightarrow$ x^* is computationally hidden $\Rightarrow$ $\mathcal{A}$ fails!

Lemma: NM $\not\Rightarrow$ ANM for any Φ when f is poly-to-1.

Anti-Intuition: $\mathcal{O}_{\mathsf{inv}}$ seems useless against NM

$\mathcal{A}$ against ANM: given f and $y^* \leftarrow f(x^*)$, aims to output (ϕ, y) s.t. $f(\phi(x^*)) = y$ with the help of $\mathcal{O}_{\mathsf{inv}}$. Since querying $\mathcal{O}_{\mathsf{inv}}$ at y^* is not allowed, the only strategy is:

<u>pick $y \xleftarrow{\mathrm{R}} Y$; obtain $x \leftarrow \mathcal{O}_{\mathsf{inv}}(y)$; compute ϕ s.t. $\phi(x^*) = x$.</u>

NM $\Rightarrow$ OW when f is poly-to-1 $\Rightarrow$ x^* is computationally hidden $\Rightarrow$ $\mathcal{A}$ fails!

The intuition is deceptive: $\mathcal{O}_{\mathsf{inv}}$ always behaves benignly

$$\mathcal{O}_{\mathsf{inv}}(y) = \begin{cases} x & \text{if } y \in \mathrm{Img}(f) \\ \perp & \text{if } y \notin \mathrm{Img}(f) \end{cases}$$

Lemma: NM $\not\Rightarrow$ ANM for any Φ when f is poly-to-1.

Anti-Intuition: $\mathcal{O}_{\mathsf{inv}}$ seems useless against NM

$\mathcal{A}$ against ANM: given f and $y^* \leftarrow f(x^*)$, aims to output (ϕ, y) s.t. $f(\phi(x^*)) = y$ with the help of $\mathcal{O}_{\mathsf{inv}}$. Since querying $\mathcal{O}_{\mathsf{inv}}$ at y^* is not allowed, the only strategy is:

<u>pick $y \xleftarrow{\text{R}} Y$; obtain $x \leftarrow \mathcal{O}_{\mathsf{inv}}(y)$; compute ϕ s.t. $\phi(x^*) = x$.</u>

NM $\Rightarrow$ OW when f is poly-to-1 $\Rightarrow$ x^* is computationally hidden $\Rightarrow$ $\mathcal{A}$ fails!

$\mathcal{O}_{\mathsf{inv}}$ could behave wildly (align with the real TdInv).

$$\mathcal{O}_{\mathsf{inv}}(y) = \begin{cases} x & \text{if } y \in \mathrm{Img}(f) \\ td & \text{if } y \notin \mathrm{Img}(f) \end{cases}$$

and this will lead to a separation!

Lemma: NM $\not\Rightarrow$ ANM for any Φ when f is poly-to-1.

Separation: f is NM $\rightarrow$ f' is still NM but not ANM.

Lemma: NM $\not\Rightarrow$ ANM for any Φ when f is poly-to-1.

Separation: f is NM $\rightarrow f'$ is still NM but not ANM.

Idea: make $\mathcal{O}_{\mathsf{inv}}^{f'}$ dangerous. Let $f : \{0,1\}^n \rightarrow \{0,1\}^m$ be a trapdoor NMF, we build f' as below:

$$\begin{aligned} f'(x) :&\ = 0||f(x) \text{ strings with prefix '1' must be invalid} \\ f'.td :&\ = f.td \\ f'.\mathsf{TdInv}(y') :&\ = \begin{cases} f.\mathsf{TdInv}(y) & \text{if } y' = 0||y \\ td & \text{if } y' = 1||y \end{cases} \end{aligned}$$

Non-Malleability $\not\Rightarrow$ Adaptive Non-Malleability

Lemma: NM $\not\Rightarrow$ ANM for any Φ when f is poly-to-1.

Separation: f is NM $\to$ f' is still NM but not ANM.

Idea: make $\mathcal{O}_{\mathsf{inv}}^{f'}$ dangerous. Let $f : \{0,1\}^n \to \{0,1\}^m$ be a trapdoor NMF, we build f' as below:

$$\begin{aligned} f'(x) : &\quad = 0||f(x) \text{ strings with prefix `1' must be invalid} \\ f'.td : &\quad = f.td \\ f'.\mathsf{TdInv}(y') : &\quad = \begin{cases} f.\mathsf{TdInv}(y) & \text{if } y' = 0||y \\ td & \text{if } y' = 1||y \end{cases} \end{aligned}$$

Claim 1: f' inherits correctness and NM from that of f.

Non-Malleability $\not\Rightarrow$ Adaptive Non-Malleability

Lemma: NM $\not\Rightarrow$ ANM for any Φ when f is poly-to-1.

Separation: f is NM $\rightarrow$ f' is still NM but not ANM.

Idea: make $\mathcal{O}_{\mathsf{inv}}^{f'}$ dangerous. Let $f : \{0,1\}^n \rightarrow \{0,1\}^m$ be a trapdoor NMF, we build f' as below:

$$\begin{aligned} f'(x): &= 0||f(x) \text{ strings with prefix '1' must be invalid} \\ f'.td: &= f.td \\ f'.\mathsf{TdInv}(y'): &= \begin{cases} f.\mathsf{TdInv}(y) & \text{if } y' = 0||y \\ td & \text{if } y' = 1||y \end{cases} \end{aligned}$$

Claim 1: f' inherits correctness and NM from that of f.

Claim 2: f' is not ANM w.r.t. any Φ.
$\mathcal{A}$ can obtain td by querying $\mathcal{O}_{\mathsf{inv}}^{f'}$ at $1||0^m$, then computes the right x^* with probability $1/\mathsf{poly}(\lambda)$ and breaks NM.

Lemma: NM $\not\Rightarrow$ ANM for any Φ when f is poly-to-1.

Separation: f is NM $\to$ f' is still NM but not ANM.

Idea: make $\mathcal{O}_{\mathsf{inv}}^{f'}$ dangerous. Let $f : \{0,1\}^n \to \{0,1\}^m$ be a trapdoor NMF, we build f' as below:

$$\begin{aligned} f'(x): &= 0||f(x) \text{ strings with prefix `1' must be invalid} \\ f'.td: &= f.td \\ f'.\mathsf{TdInv}(y'): &= \begin{cases} f.\mathsf{TdInv}(y) & \text{if } y' = 0||y \\ td & \text{if } y' = 1||y \end{cases} \end{aligned}$$

This separation is similar in spirit to IND-CPA $\not\Rightarrow$ IND-CCA1 in PKE setting.

A Short Summary

$$\begin{tikzcd}[column sep=huge, row sep=huge]
\mathrm{NM} & \mathrm{ANM} \\
\mathrm{OW} \arrow[r, shift left, "/" marking] & \mathrm{AOW} \arrow[l, shift left]
\end{tikzcd}$$

A Short Summary

$$
\begin{tikzcd}
\mathrm{NM} \arrow[d, bend right, "\substack{\text{poly-to-1}\\ \forall\Phi}"'] & & \mathrm{ANM} \arrow[d, bend right, "\substack{\text{poly-to-1}\\ \forall\Phi}"'] \\
\mathrm{OW} \arrow[rr, shift left, "/" marking] & & \mathrm{AOW} \arrow[ll, shift left]
\end{tikzcd}
$$

A Short Summary

$$
\begin{tikzcd}[row sep=huge, column sep=huge]
\text{NM} \arrow[d, bend right, swap, "\substack{\text{poly-to-1}\\ \forall\Phi}"] & & \text{ANM} \arrow[d, bend right, swap, "\substack{\text{poly-to-1}\\ \forall\Phi}"] \\
\text{OW} \arrow[u, bend right, swap, "\Phi^{\text{srs}}_{\text{brs}}", "/" marking] \arrow[rr, shift left, "/" marking] & & \text{AOW} \arrow[ll, shift left]
\end{tikzcd}
$$

A Short Summary

$$
\begin{tikzcd}[column sep=huge, row sep=huge]
\mathrm{NM} \arrow[d, bend right, "\text{poly-to-1}\ \forall\Phi"'] & \mathrm{ANM} \arrow[d, bend right, "\text{poly-to-1}\ \forall\Phi"'] \\
\mathrm{OW} \arrow[u, bend right, "/" marking, "\Phi^{\mathrm{srs}}_{\mathrm{brs}}"'] \arrow[r, shift left, "/" marking] & \mathrm{AOW} \arrow[l, shift left] \arrow[u, bend right, "\text{injective}\ \Phi^{\mathrm{srs}}_{\mathrm{brs}}"']
\end{tikzcd}
$$

A Short Summary

$$
\begin{tikzcd}[row sep=huge, column sep=huge]
\mathrm{NM} \arrow[d, bend right, "\begin{array}{c}\text{poly-to-1}\\ \forall\Phi\end{array}"'] & \mathrm{ANM} \arrow[d, bend right, "\begin{array}{c}\text{poly-to-1}\\ \forall\Phi\end{array}"'] \\
\mathrm{OW} \arrow[u, bend right, "/" marking, "\Phi^{\mathrm{srs}}_{\mathrm{brs}}"'] \arrow[r, shift left, "/" marking] & \mathrm{AOW} \arrow[u, bend right, "\begin{array}{c}\text{injective}\\ \Phi^{\mathrm{srs}}_{\mathrm{brs}}\end{array}"'] \arrow[l, shift left]
\end{tikzcd}
$$

extend to the trapdoor functions $\Rightarrow$ solve the open problem posed in [Kiltz, Mohassel, O'Neill, Eurocrypt 2010].

A Short Summary

$$
\begin{tikzcd}[row sep=huge, column sep=huge]
\mathrm{NM} \arrow[d, bend right, "\substack{\text{poly-to-1}\\ \forall\Phi}"'] & \mathrm{ANM} \arrow[l] \arrow[d, bend right, "\substack{\text{poly-to-1}\\ \forall\Phi}"'] \\
\mathrm{OW} \arrow[u, bend right, "/" marking, "\Phi^{\mathrm{srs}}_{\mathrm{brs}}"'] \arrow[r, shift left, "/" marking] & \mathrm{AOW} \arrow[l, shift left] \arrow[u, bend right, "\substack{\text{injective}\\ \Phi^{\mathrm{srs}}_{\mathrm{brs}}}"']
\end{tikzcd}
$$

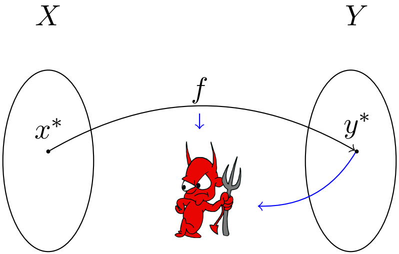
extend to the trapdoor functions $\Rightarrow$ solve the open problem posed in [Kiltz, Mohassel, O'Neill, Eurocrypt 2010].

A Short Summary

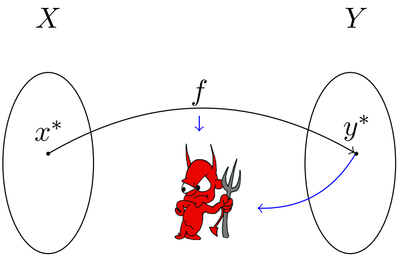
$$
\begin{tikzcd}[row sep=huge, column sep=huge]
\mathrm{NM} \arrow[rr, bend left, "\text{poly-to-1 } \forall\Phi", "/" marking] \arrow[dd, bend right, "\substack{\text{poly-to-1}\\ \forall\Phi}"'] & & \mathrm{ANM} \arrow[ll] \arrow[dd, bend right, "\substack{\text{poly-to-1}\\ \forall\Phi}"'] \\
& & \\
\mathrm{OW} \arrow[uu, bend right, "\Phi^{\mathrm{srs}}_{\mathrm{brs}}"', "/" marking] \arrow[rr, shift left, "/" marking] & & \mathrm{AOW} \arrow[ll, shift left] \arrow[uu, bend right, "\substack{\text{injective}\\ \Phi^{\mathrm{srs}}_{\mathrm{brs}}}"']
\end{tikzcd}
$$

extend to the trapdoor functions $\Rightarrow$ solve the open problem posed in [Kiltz, Mohassel, O'Neill, Eurocrypt 2010].

Hinted Notions

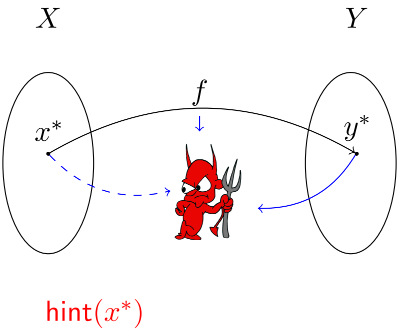


Hinted Notions



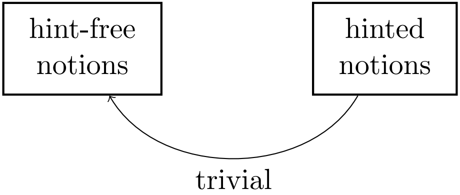
- OWF or NMF might be used in various different high-level protocols simultaneously.

Hinted Notions

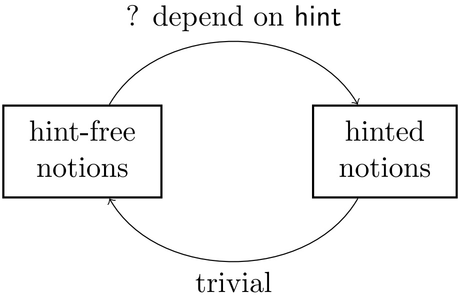


- OWF or NMF might be used in various different high-level protocols simultaneously.
- $\mathcal{A}$ may collect some auxiliary info about x^* — hint of x^* — probabilistic $\mathsf{hint} : X \to \{0,1\}^{m(\lambda)}$ — hinted notions
- hinted notion is generally more strong and useful.

Relations between hinted notions and hint-free notions



Relations between hinted notions and hint-free notions



When hint-free notions imply hinted notions?

hinted
notions

hint-free
notions

When hint-free notions imply hinted notions?

$\mathcal{R}$

hinted notions

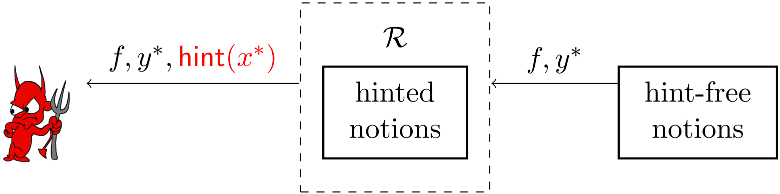
hint-free notions

When hint-free notions imply hinted notions?

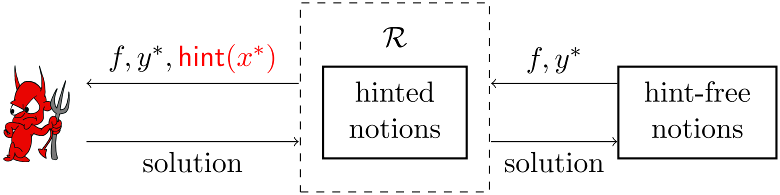
$\mathcal{R}$

$$\boxed{\text{hinted notions}} \xleftarrow{\;f,\,y^*\;} \boxed{\text{hint-free notions}}$$

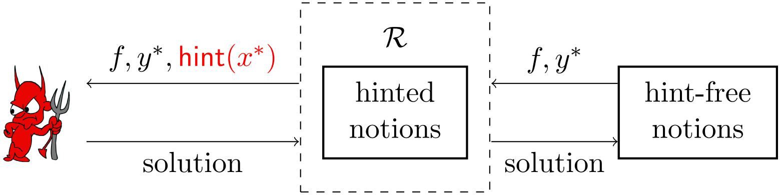
When hint-free notions imply hinted notions?



When hint-free notions imply hinted notions?



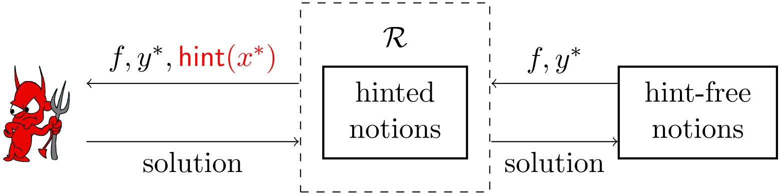
When hint-free notions imply hinted notions?



- statistically simulatable: with some noticeable $p(\lambda)$

$$(f, y^*, \mathcal{R}(f, y^*)) \approx_s (f, y^*, \mathsf{hint}(x^*))$$

When hint-free notions imply hinted notions?



- statistically simulatable: with some noticeable $p(\lambda)$

$$(f, y^*, \mathcal{R}(f, y^*)) \approx_s (f, y^*, \mathsf{hint}(x^*))$$

- computationally simulatable: with some noticeable $p(\lambda)$

$$(f, y^*, \mathcal{R}(f, y^*)) \approx_c (f, y^*, \mathsf{hint}(x^*))$$

based on the hint-free notions.

Examples of Simulatable Hint Functions

$$\mathsf{hint} : X \to \{0,1\}^{m(\lambda)}$$

Examples of Simulatable Hint Functions

$$\mathsf{hint} : X \to \{0,1\}^{m(\lambda)}$$

- bounded output length, i.e., $m(\lambda) \le O(\log(\lambda))$
  $\mathcal{R}$ can always output a right $\mathsf{hint}(x^*)$ by making a random guess $\Rightarrow$ $1/\mathsf{poly}(\lambda)$-perfectly simulatable.

Examples of Simulatable Hint Functions

$$\mathsf{hint} : X \to \{0,1\}^{m(\lambda)}$$

- bounded output length, i.e., $m(\lambda) \leq O(\log(\lambda))$
  $\mathcal{R}$ can always output a right $\mathsf{hint}(x^*)$ by making a random guess $\Rightarrow$ $1/\mathsf{poly}(\lambda)$-perfectly simulatable.

- beyond the bound $O(\log(\lambda))$
  Let f be a OWF $X \to Y$, h be its hardcore function from $X \to \{0,1\}^{m(\lambda)}$.

$$\mathsf{hint}(x;b) = \begin{cases} h(x) & \text{if } b = 0 \\ r \xleftarrow{\mathrm{R}} \{0,1\}^{m(\lambda)} & \text{if } b = 1 \end{cases}$$

now $m(\lambda)$ is possibly beyond $O(\log(\lambda))$.
OW $\Rightarrow h(x^*) \approx_c U_{m(\lambda)} \Rightarrow \mathsf{hint}(x^*;b) \approx_c U_{m(\lambda)} \Rightarrow$
1-computationally simulatable ☺ application

Outline

1. Backgrounds
2. NMFs: Syntax and Definition
3. Relations among OW and NM
4. Constructions of NMFs
5. Applications of NMFs

Constructions of NMFs

Random oracle model

Constructions of NMFs

Random oracle model

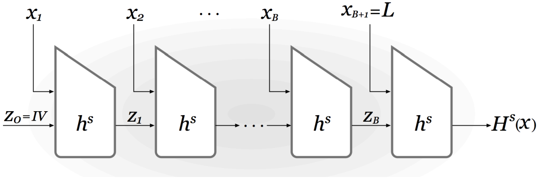


Figure: The Merkle-Damgåd Transformation

By modeling the compression function h as a random oracle, we show that the MD is $\Phi^{\mathrm{srs}}_{\mathrm{brs}}$-NM.

Constructions of NMFs

Random oracle model

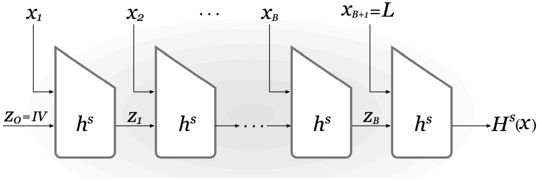


Figure: The Merkle-Damgåd Transformation

By modeling the compression function h as a random oracle, we show that the MD is $\Phi^{\mathrm{srs}}_{\mathrm{brs}}$-NM.

- improve previous result [BFS, CT-RSA 2011]: $\underline{\Phi^{\mathrm{xor}}\text{-NM}}$.
- provide us a practical candidate of NMFs.

Constructions of NMFs

Standard model

Constructions of NMFs

Standard model

$$\begin{array}{c}\text{ATDF}\\ \big\downarrow\\ \Phi^{\text{srs}}_{\text{brs}}\text{-NMFs}\end{array} \qquad \text{AOW} \Rightarrow \Phi^{\text{srs}}_{\text{brs}}\text{-ANM}$$

Constructions of NMFs

Standard model

$$\begin{array}{ccc} \text{II-RSA} & & \\ & \searrow & \\ & \text{ATDF} & \\ & \downarrow & \quad \text{AOW} \Rightarrow \Phi_{\text{brs}}^{\text{srs}}\text{-ANM} \\ & \Phi_{\text{brs}}^{\text{srs}}\text{-NMFs} & \end{array}$$

Constructions of NMFs

Standard model

$$
\begin{tikzcd}
 & & & \mathrm{LTDF} \arrow[dl] \\
 \text{II-RSA} \arrow[dr] & & \text{CP-TDF} \arrow[dl] & \\
 & \mathrm{ATDF} \arrow[d] & & \\
 & \Phi_{\mathrm{brs}}^{\mathrm{srs}}\text{-NMFs} & &
\end{tikzcd}
$$

$\mathrm{AOW} \Rightarrow \Phi_{\mathrm{brs}}^{\mathrm{srs}}\text{-ANM}$

Constructions of NMFs

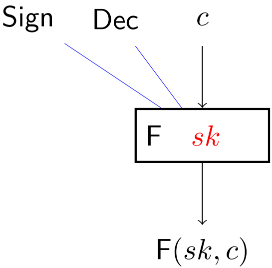
Standard model

$$\begin{tikzcd}
 & & \mathrm{LWE} \arrow[drr] & \mathrm{DDH} \arrow[dr] & & \mathrm{QR} \arrow[dl] & \mathrm{DCR} \arrow[dll] \\
 & & & & \mathrm{LTDF} \arrow[dll] & & \\
\mathrm{II\text{-}RSA} \arrow[dr] & & \mathrm{CP\text{-}TDF} \arrow[dl] & & & & \\
 & \mathrm{ATDF} \arrow[d] & & & & & \\
 & \Phi_{\mathrm{brs}}^{\mathrm{srs}}\text{-}\mathrm{NMFs} & & & & &
\end{tikzcd}$$

$\mathrm{AOW} \Rightarrow \Phi_{\mathrm{brs}}^{\mathrm{srs}}\text{-}\mathrm{ANM}$

Outline

Related-key Attacks



Related-key Attacks

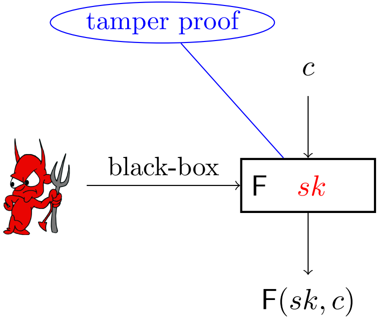
tamper proof

c

F sk

$\mathsf{F}(sk, c)$

Related-key Attacks



Related-key Attacks

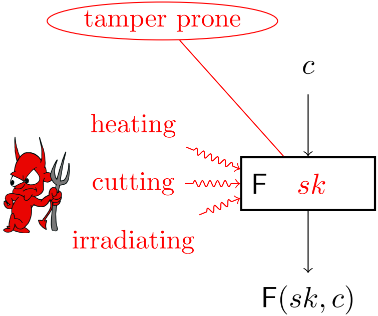
tamper prone

c

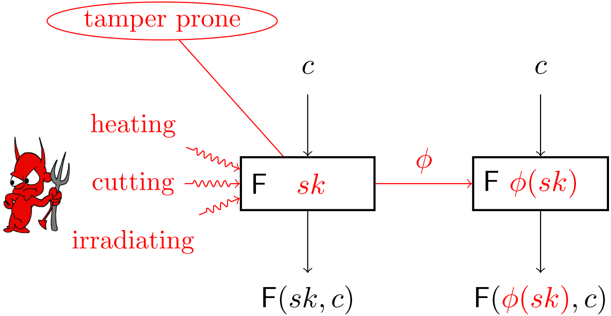
F sk

F(sk, c)

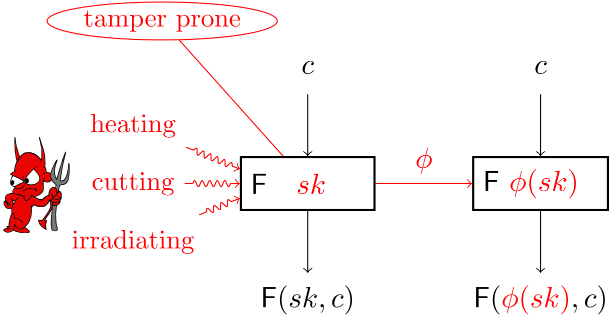
Related-key Attacks



Related-key Attacks



Related-key Attacks



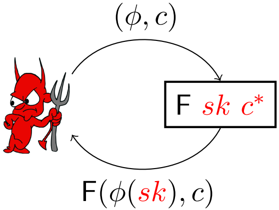
Security against related-key attacks is called RKA-security.

RKA-security model for PKE and Copy-attacks

RKA-security w.r.t. RKD class $\Phi = \{\phi : SK \to SK\}$

RKA-security model for PKE and Copy-attacks

RKA-security w.r.t. RKD class $\Phi = \{\phi : SK \to SK\}$



RKA-security model for PKE and Copy-attacks

RKA-security w.r.t. RKD class $\Phi = \{\phi : SK \to SK\}$

(ϕ, c)

$\phi(sk) \neq sk \vee c \neq c^*$

$\underline{\phi(sk) = sk \wedge c = c^*}$

$\boxed{\mathsf{F}\ sk\ c^*}$

$\mathsf{F}(\phi(sk), c)$

RKA-security model for PKE and Copy-attacks

RKA-security w.r.t. RKD class $\Phi = \{\phi : SK \to SK\}$

(ϕ, c)

$\phi(sk) \neq sk \vee c \neq c^*$

$\underline{\phi(sk) = sk \wedge c = c^*}$

copy attacks

$\boxed{\mathsf{F}\ sk\ c^*}$

$\mathsf{F}(\phi(sk), c)$

RKA-security model for PKE and Copy-attacks

RKA-security w.r.t. RKD class $\Phi = \{\phi : SK \to SK\}$

(ϕ, c)

$\phi(sk) \neq sk \lor c \neq c^*$

$\underline{\phi(sk) = sk \land c = c^*}$

copy attacks

$\phi = \mathsf{id}$ (trivial)

$\phi \neq \mathsf{id}$ (non-trivial)

$\boxed{\mathsf{F}\ sk\ c^*}$

$\mathsf{F}(\phi(sk), c)$

RKA-security model for PKE and Copy-attacks

RKA-security w.r.t. RKD class $\Phi = \{\phi : SK \to SK\}$

(ϕ, c)

$\phi(sk) \neq sk \vee c \neq c^*$

$\underline{\phi(sk) = sk \wedge c = c^*}$

copy attacks

$\phi = \mathsf{id}$ (trivial)

$\phi \neq \mathsf{id}$ (non-trivial)

$\boxed{\mathsf{F}\ sk\ c^*}$

$\mathsf{F}(\phi(sk), c)$

- trivial: must be forbidden to avoid trivial definition

RKA-security model for PKE and Copy-attacks

RKA-security w.r.t. RKD class $\Phi = \{\phi : SK \to SK\}$

(ϕ, c)

$\phi(sk) \neq sk \vee c \neq c^*$

$\phi(sk) = sk \wedge c = c^*$

copy attacks

$\phi = \mathsf{id}$ (trivial)

$\phi \neq \mathsf{id}$ (non-trivial)

$\boxed{\mathsf{F}\ sk\ c^*}$

$\mathsf{F}(\phi(sk), c)$

- trivial: must be forbidden to avoid trivial definition
- non-trivial: practical $\Rightarrow$ strong definition

RKA-security model for PKE and Copy-attacks

RKA-security w.r.t. RKD class $\Phi = \{\phi : SK \to SK\}$

(ϕ, c)

$\mathsf{F}\ sk\ c^*$

$\mathsf{F}(\phi(sk), c)$

$\phi(sk) \neq sk \vee c \neq c^*$

$\underline{\phi(sk) = sk \wedge c = c^*}$

copy attacks

$\phi = \mathsf{id}$ (trivial)

$\phi \neq \mathsf{id}$ (non-trivial)

- trivial: must be forbidden to avoid trivial definition
- non-trivial: practical $\Rightarrow$ strong definition
    - directly reject ([Wee, PKC 2012]) $\Rightarrow$ weak RKA-security

RKA-security model for PKE and Copy-attacks

RKA-security w.r.t. RKD class $\Phi = \{\phi : SK \to SK\}$

(ϕ, c)

$\phi(sk) \neq sk \vee c \neq c^*$

$\phi(sk) = sk \wedge c = c^*$

copy attacks

$\phi = \mathsf{id}$ (trivial)

$\phi \neq \mathsf{id}$ (non-trivial)

$\boxed{\mathsf{F}\ sk\ c^*}$

$\mathsf{F}(\phi(sk), c)$

- trivial: must be forbidden to avoid trivial definition
- non-trivial: practical $\Rightarrow$ strong definition
  - directly reject ([Wee, PKC 2012]) $\Rightarrow$ weak RKA-security
  - rule out ([Bellare and Cash, Crypto 2010]) $\Rightarrow$ Φ is claw-free

RKA-security model for PKE and Copy-attacks

RKA-security w.r.t. RKD class $\Phi = \{\phi : SK \to SK\}$

(ϕ, c)

$\phi(sk) \neq sk \vee c \neq c^*$

$\phi(sk) = sk \wedge c = c^*$

copy attacks

$\phi = \mathsf{id}$ (trivial)

$\phi \neq \mathsf{id}$ (non-trivial)

$\boxed{\mathsf{F}\ sk\ c^*}$

$\mathsf{F}(\phi(sk), c)$

- trivial: must be forbidden to avoid trivial definition
- non-trivial: practical $\Rightarrow$ strong definition
  - directly reject ([Wee, PKC 2012]) $\Rightarrow$ weak RKA-security
  - rule out ([Bellare and Cash, Crypto 2010]) $\Rightarrow$ Φ is claw-free
  - specific property ([Abdalla et al., Crypto 2014]) $\Rightarrow$ tie to scheme algebra $\Rightarrow$ Φ unlike to be general

Insight in Addressing Non-trivial Copy-attacks

- Our NM notion is defined via RKA-like framework

Insight in Addressing Non-trivial Copy-attacks

- Our NM notion is defined via RKA-like framework
- strengthening — allowing $\phi(x^*) = x^*$ somehow resembles non-trivial copy attacks

Insight in Addressing Non-trivial Copy-attacks

- Our NM notion is defined via RKA-like framework
- strengthening — allowing $\phi(x^*) = x^*$ somehow resembles non-trivial copy attacks

  Q: Does previous result shed light?

Insight in Addressing Non-trivial Copy-attacks

- Our NM notion is defined via RKA-like framework
- strengthening — allowing $\phi(x^*) = x^*$ somehow resembles non-trivial copy attacks

  Q: Does previous result shed light?

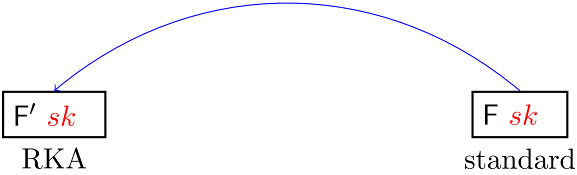
  A: Yes! $\underline{\text{AOW} \Rightarrow \Phi_{\text{brs}}^{\text{srs}}\text{-ANM}}$ indicates that $\phi \in \Phi_{\text{brs}}^{\text{srs}}$ s.t. $\phi(x^*) = x^*$ possibly exists but hard to find assuming AOW.

Insight in Addressing Non-trivial Copy-attacks

- Our NM notion is defined via RKA-like framework
- strengthening — allowing $\phi(x^*) = x^*$ somehow resembles non-trivial copy attacks

  Q: Does previous result shed light?

  A: Yes! $\underline{\mathrm{AOW} \Rightarrow \Phi^{\mathrm{srs}}_{\mathrm{brs}}\text{-ANM}}$ indicates that $\phi \in \Phi^{\mathrm{srs}}_{\mathrm{brs}}$ s.t. $\phi(x^*) = x^*$ possibly exists but hard to find assuming AOW.



Insight in Addressing Non-trivial Copy-attacks

- Our NM notion is defined via RKA-like framework
- strengthening — allowing $\phi(x^*) = x^*$ somehow resembles non-trivial copy attacks

  Q: Does previous result shed light?

  A: Yes! $\underline{\text{AOW} \Rightarrow \Phi_{\text{brs}}^{\text{srs}}\text{-ANM}}$ indicates that $\phi \in \Phi_{\text{brs}}^{\text{srs}}$ s.t. $\phi(x^*) = x^*$ possibly exists but hard to find assuming AOW.

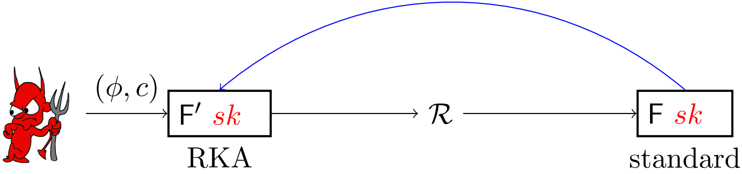
$$
\begin{tikzcd}
\boxed{\mathsf{F}'\ sk} \arrow[r] & \mathcal{R} \arrow[r] & \boxed{\mathsf{F}\ sk} \arrow[ll, bend right] \\
\text{RKA} & & \text{standard}
\end{tikzcd}
$$

Insight in Addressing Non-trivial Copy-attacks

- Our NM notion is defined via RKA-like framework
- strengthening — allowing $\phi(x^*) = x^*$ somehow resembles non-trivial copy attacks

  Q: Does previous result shed light?

  A: Yes! $\underline{\text{AOW} \Rightarrow \Phi_{\text{brs}}^{\text{srs}}\text{-ANM}}$ indicates that $\phi \in \Phi_{\text{brs}}^{\text{srs}}$ s.t. $\phi(x^*) = x^*$ possibly exists but hard to find assuming AOW.

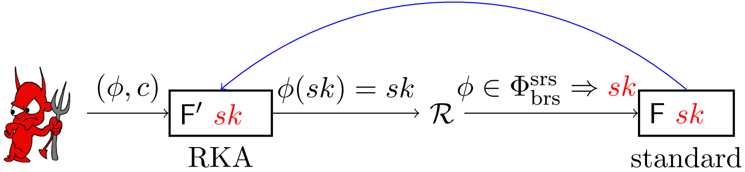


Insight in Addressing Non-trivial Copy-attacks

- Our NM notion is defined via RKA-like framework
- strengthening — allowing $\phi(x^*) = x^*$ somehow resembles non-trivial copy attacks

  Q: Does previous result shed light?

  A: Yes! $\underline{\text{AOW} \Rightarrow \Phi^{\text{srs}}_{\text{brs}}\text{-ANM}}$ indicates that $\phi \in \Phi^{\text{srs}}_{\text{brs}}$ s.t. $\phi(x^*) = x^*$ possibly exists but hard to find assuming AOW.



Insight in Addressing Non-trivial Copy-attacks

- Our NM notion is defined via RKA-like framework
- strengthening — allowing $\phi(x^*) = x^*$ somehow resembles non-trivial copy attacks

  Q: Does previous result shed light?

  A: Yes! $\underline{\text{AOW} \Rightarrow \Phi_{\text{brs}}^{\text{srs}}\text{-ANM}}$ indicates that $\phi \in \Phi_{\text{brs}}^{\text{srs}}$ s.t. $\phi(x^*) = x^*$ possibly exists but hard to find assuming AOW.

$$\begin{tikzcd} \ \arrow[r, "{(\phi, c)}"] & \boxed{\mathsf{F}'\ sk} \arrow[r, "\phi(sk) = sk"] & \mathcal{R} \arrow[r, "\phi \in \Phi_{\text{brs}}^{\text{srs}} \Rightarrow sk"] & \boxed{\mathsf{F}\ sk} \arrow[ll, bend right] \\ & \text{RKA} & & \text{standard} \end{tikzcd}$$

- w.r.t. $\Phi_{\text{brs}}^{\text{srs}}$ resilience against non-trivial copy-attacks is a built-in property guaranteed by standard security.

Authenticated Key Derivation Functions

[Qin et al. PKC 2015] extended NM KDFs [Faust et al. Eurocrypt 2014] to continuously NM KDFs, which we call RKA-secure Authenticated KDFs.

Authenticated Key Derivation Functions

[Qin et al. PKC 2015] extended NM KDFs [Faust et al. Eurocrypt 2014] to continuously NM KDFs, which we call RKA-secure Authenticated KDFs.

$$\mathsf{Setup}(\lambda) \to pp$$

Authenticated Key Derivation Functions

[Qin et al. PKC 2015] extended NM KDFs [Faust et al. Eurocrypt 2014] to continuously NM KDFs, which we call RKA-secure Authenticated KDFs.

$$\begin{array}{c} \mathsf{Setup}(\lambda) \rightarrow pp \\ \downarrow \\ \mathsf{Sample}(pp) \rightarrow (s, t) \end{array}$$

Authenticated Key Derivation Functions

[Qin et al. PKC 2015] extended NM KDFs [Faust et al. Eurocrypt 2014] to continuously NM KDFs, which we call RKA-secure Authenticated KDFs.

$$\begin{array}{l}\mathsf{Setup}(\lambda) \to pp \\ \qquad\qquad\downarrow \\ \qquad\mathsf{Sample}(pp) \to (s, t) \\ \qquad\qquad\qquad\qquad\downarrow \\ \qquad\qquad\mathsf{Derive}(s, t) \to k \text{ or } \perp\end{array}$$

Authenticated Key Derivation Functions

[Qin et al. PKC 2015] extended NM KDFs [Faust et al. Eurocrypt 2014] to continuously NM KDFs, which we call RKA-secure Authenticated KDFs.

$$\begin{array}{l}\mathsf{Setup}(\lambda) \to pp \\ \qquad\qquad\quad \downarrow \\ \qquad \mathsf{Sample}(pp) \to (s, t) \\ \qquad\qquad\qquad\qquad\qquad \downarrow \\ \qquad\qquad \mathsf{Derive}(s, t) \to k \text{ or } \perp\end{array}$$

RKA-security: For all PPT $\mathcal{A}$, we have:

$$\Pr\left[b' = b : \begin{array}{l} pp \leftarrow \mathsf{Setup}(\lambda), (s^*, t^*) \leftarrow \mathsf{Sample}(pp); \\ k_0^* \leftarrow \mathsf{Derive}(s^*, t^*), k_1^* \xleftarrow{\mathrm{R}} \{0,1\}^m; \\ b \xleftarrow{\mathrm{R}} \{0,1\}, b' \leftarrow \mathcal{A}^{\mathcal{O}_{\mathsf{dev}}^{\Phi}(\cdot,\cdot)}(pp, t^*, k_b^*); \end{array}\right] - \frac{1}{2} = \mathsf{negl}(\lambda).$$

$\mathcal{O}_{\mathsf{dev}}^{\Phi}(\phi, t)$ returns same^* if $\underline{\phi(s^*) = s^* \text{ and } t = t^*}$, and returns $\mathsf{Derive}(\phi(s^*), t)$ otherwise.

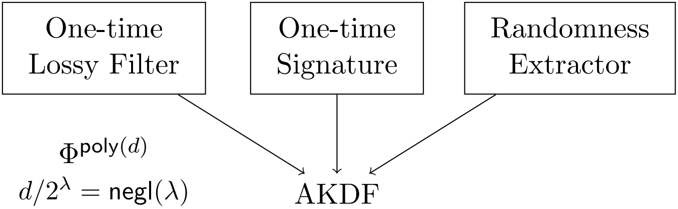
[Qin et al. PKC 2015], Revisited

$$
\begin{tikzcd}
\boxed{\text{One-time Lossy Filter}} \arrow[dr] & \boxed{\text{One-time Signature}} \arrow[d] & \boxed{\text{Randomness Extractor}} \arrow[dl] \\
 & \text{AKDF} &
\end{tikzcd}
$$

$\Phi^{\mathsf{poly}(d)}$

$d/2^\lambda = \mathsf{negl}(\lambda)$

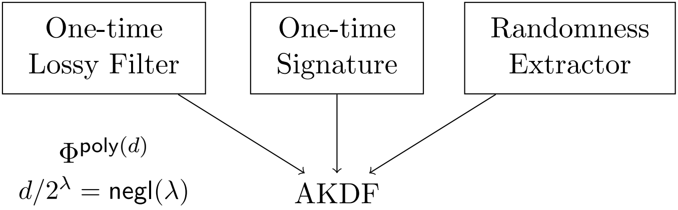
[Qin et al. PKC 2015], Revisited



Efficiency

- large public parameters size: $pp = pp_1 + pp_2 + pp_3$
- slow tagging & large tag size: randomized tag generation

[Qin et al. PKC 2015], Revisited



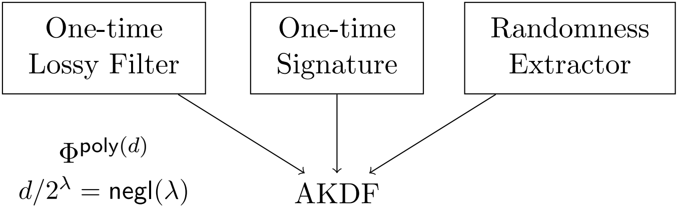
Efficiency

- large public parameters size: $pp = pp_1 + pp_2 + pp_3$
- slow tagging & large tag size: randomized tag generation

Security

- non-trivial copy attack is not allowed.
- $\Phi^{\mathsf{poly}(d)}$ is large but still specific.

[Qin et al. PKC 2015], Revisited



Efficiency

- large public parameters size: $pp = pp_1 + pp_2 + pp_3$
- slow tagging & large tag size: randomized tag generation

Security

- non-trivial copy attack is not allowed.
- $\Phi^{\mathsf{poly}(d)}$ is large but still specific.

We expect...

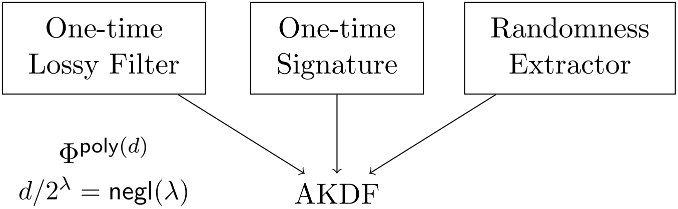
[Qin et al. PKC 2015], Revisited

$$\begin{tikzcd}
\boxed{\text{One-time Lossy Filter}} \arrow[dr] & \boxed{\text{One-time Signature}} \arrow[d] & \boxed{\text{Randomness Extractor}} \arrow[dl] \\
\begin{array}{c} \Phi^{\mathsf{poly}(d)} \\ d/2^{\lambda} = \mathsf{negl}(\lambda) \end{array} & \text{AKDF} &
\end{tikzcd}$$

High Efficiency

- compact public parameters
- quick tag generation & short tag size

[Qin et al. PKC 2015], Revisited



High Efficiency

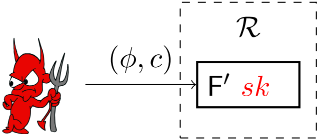
- compact public parameters
- quick tag generation & short tag size

Strong RKA-security

- capture non-trivial copy attacks
- Φ is large and general

Attempt

Technical hurdle: simulate RKA oracle

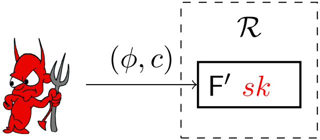


Attempt

Technical hurdle: simulate RKA oracle

Typical approach: exploit so called Φ-key-malleability

$$\underline{\mathsf{F}'(\phi(sk), c) = \mathsf{F}(sk, \mathsf{T}(\phi, c))}$$

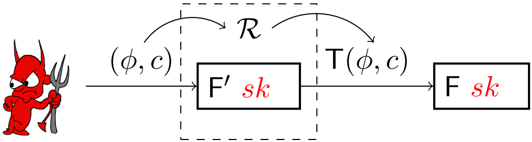


Attempt

Technical hurdle: simulate RKA oracle

Typical approach: exploit so called Φ-key-malleability

$$\underline{\mathsf{F}'(\phi(sk), c) = \mathsf{F}(sk, \mathsf{T}(\phi, c))}$$

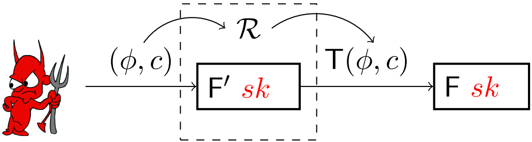


Attempt

Technical hurdle: simulate RKA oracle

Typical approach: exploit so called Φ-key-malleability

$$\underline{\mathsf{F}'(\phi(sk), c) = \mathsf{F}(sk, \mathsf{T}(\phi, c))}$$



- We do not have the underlying primitive.
- Φ-key-malleability requires nice algebra property, e.g. homomorphism $\Rightarrow$ Φ cannot be general

Our Construction

Core idea: acquire RKA-security from Non-Malleability

$t^* \sim s^*$

$\mathcal{R}$

$\boxed{\textsf{AKDF}\ s^*}$

Our Construction

Core idea: acquire RKA-security from Non-Malleability

hard to find

$t^* \sim s^*$

(ϕ, t)

$t \sim \phi(s^*)$

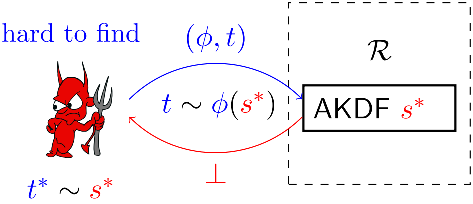
$\mathcal{R}$

AKDF s^*

t is a non-malleable tag of s

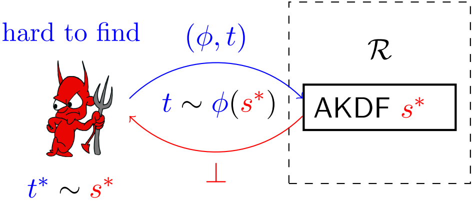
Our Construction

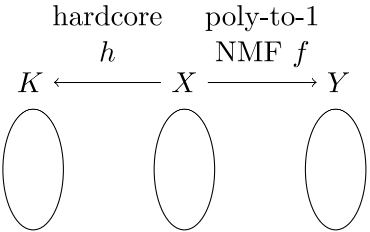
Core idea: acquire RKA-security from Non-Malleability



Our Construction

Core idea: acquire RKA-security from Non-Malleability

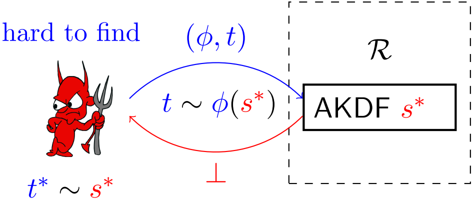


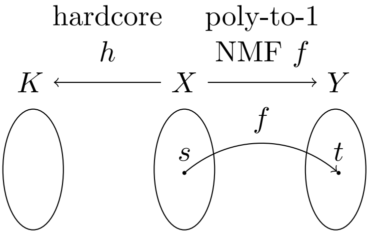


- Setup(λ): $pp = (f, h)$.

Our Construction

Core idea: acquire RKA-security from Non-Malleability

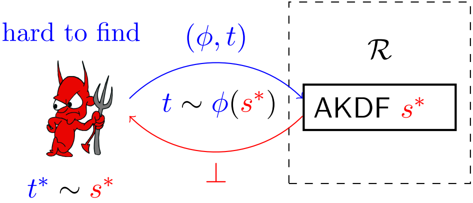


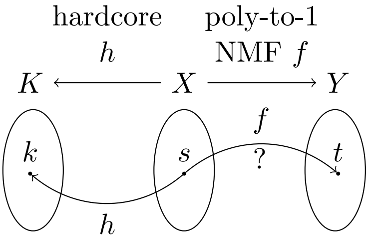


- Setup(λ): $pp = (f, h)$.
- Sample(pp): $s \xleftarrow{\text{R}} X$, $t \leftarrow f(s)$.

Our Construction

Core idea: acquire RKA-security from Non-Malleability





- Setup(λ): $pp = (f, h)$.
- Sample(pp): $s \xleftarrow{R} X$, $t \leftarrow f(s)$.
- Derive(s, t): $h(s)$ if $t = f(s)$ or $\perp$ otherwise.

Security Proof

If f is Φ-non-malleable, AKDF is $\Phi \cup \mathsf{id} \cup \mathsf{cf}$-RKA-secure.

Security Proof

If f is Φ-non-malleable, AKDF is $\Phi \cup \mathsf{id} \cup \mathsf{cf}$-RKA-secure.

Proof (high level idea): (1) NM $\Rightarrow$ rejecting all RKA queries; (2) OW $\Rightarrow$ derived key is pseudorandom

Security Proof

If f is Φ-non-malleable, AKDF is $\Phi \cup \mathsf{id} \cup \mathsf{cf}$-RKA-secure.

Proof (high level idea): (1) NM $\Rightarrow$ rejecting all RKA queries; (2) OW $\Rightarrow$ derived key is pseudorandom

Game 0 (the real experiment) $\mathcal{CH}$ runs $\mathsf{Setup}(\lambda) \rightarrow (f, h)$, $\mathsf{Sample}(f, h) \rightarrow (s^*, t^*)$, computes $k_0^* \leftarrow h(s^*)$, $k_1^* \xleftarrow{R} K$, picks $b \xleftarrow{R} \{0, 1\}$, sends (f, h, t^*, k_b^*).

1. $\phi = \mathsf{id} \wedge t = t^*$: return same^* indicating illegal.
2. $\phi = \mathsf{id} \wedge t \neq t^*$: return $\perp$ indicating invalid. (f is deterministic thus tag is unique).
3. $\phi = \mathsf{cf}$ and t: return $h(c)$ if $f(c) = t$ and $\perp$ else.
4. $\phi \notin \mathsf{id} \cup \mathsf{cf}$ and t: return $h(\phi(s^*))$ if $t = f(\phi(s^*))$ and $\perp$ else.

Security Proof

If f is Φ-non-malleable, AKDF is $\Phi \cup \mathsf{id} \cup \mathsf{cf}$-RKA-secure.

Proof (high level idea): (1) NM $\Rightarrow$ rejecting all RKA queries; (2) OW $\Rightarrow$ derived key is pseudorandom

Game 0 (the real experiment) $\mathcal{CH}$ runs $\mathsf{Setup}(\lambda) \to (f, h)$, $\mathsf{Sample}(f, h) \to (s^*, t^*)$, computes $k_0^* \leftarrow h(s^*)$, $k_1^* \xleftarrow{\text{R}} K$, picks $b \xleftarrow{\text{R}} \{0, 1\}$, sends (f, h, t^*, k_b^*).

1. $\phi = \mathsf{id} \wedge t = t^*$: return same^* indicating illegal.
2. $\phi = \mathsf{id} \wedge t \neq t^*$: return $\perp$ indicating invalid. (f is deterministic thus tag is unique).
3. $\phi = \mathsf{cf}$ and t: return $h(c)$ if $f(c) = t$ and $\perp$ else.
4. $\phi \notin \mathsf{id} \cup \mathsf{cf}$ and t: return $h(\phi(s^*))$ if $t = f(\phi(s^*))$ and $\perp$ else.

Game 1 (handle type-4 queries without s^*) directly return $\perp$.

Security Proof

If f is Φ-non-malleable, AKDF is $\Phi \cup \mathsf{id} \cup \mathsf{cf}$-RKA-secure.

Claim 1: NM of $f \Rightarrow |\mathsf{Adv}_{\mathcal{A}}^{\text{Game 1}}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{\text{Game 0}}(\lambda)| = \mathsf{negl}(\lambda)$

Security Proof

If f is Φ-non-malleable, AKDF is $\Phi \cup \mathsf{id} \cup \mathsf{cf}$-RKA-secure.

Claim 1: NM of $f \Rightarrow |\mathsf{Adv}_{\mathcal{A}}^{\text{Game }1}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{\text{Game }0}(\lambda)| = \mathsf{negl}(\lambda)$

Define E — $\mathcal{A}$ issues $\langle \phi, t \rangle$ such that $f(\phi(s^*)) = t$ in Game 1.
Game 0 and Game 1 are identical if E never happens.

Security Proof

If f is Φ-non-malleable, AKDF is $\Phi \cup \mathsf{id} \cup \mathsf{cf}$-RKA-secure.

Claim 1: NM of $f \Rightarrow |\mathsf{Adv}_{\mathcal{A}}^{\text{Game 1}}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{\text{Game 0}}(\lambda)| = \mathsf{negl}(\lambda)$

Define E — $\mathcal{A}$ issues $\langle \phi, t \rangle$ such that $f(\phi(s^*)) = t$ in Game 1.
Game 0 and Game 1 are identical if E never happens.

f is NM $\Rightarrow \Pr[E] = \mathsf{negl}(\lambda) \Rightarrow$ Game 0 $\approx_c$ Game 1

Security Proof

If f is Φ-non-malleable, AKDF is $\Phi \cup \mathsf{id} \cup \mathsf{cf}$-RKA-secure.

Claim 1: NM of $f \Rightarrow |\mathsf{Adv}_{\mathcal{A}}^{\text{Game 1}}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{\text{Game 0}}(\lambda)| = \mathsf{negl}(\lambda)$

Define E — $\mathcal{A}$ issues $\langle \phi, t \rangle$ such that $f(\phi(s^*)) = t$ in Game 1.
Game 0 and Game 1 are identical if E never happens.

f is NM $\Rightarrow \Pr[E] = \mathsf{negl}(\lambda) \Rightarrow$ Game 0 $\approx_c$ Game 1

Note: NM is insufficient — except (pp, t^*), $\mathcal{A}$ gets to see

$$k_b^* = \mathsf{hint}(s^*; b) = \begin{cases} k^* = h(s^*) & \text{if } b = 0 \\ k^* \xleftarrow{\text{R}} K & \text{if } b = 1 \end{cases}$$

Security Proof

If f is Φ-non-malleable, AKDF is $\Phi \cup \mathsf{id} \cup \mathsf{cf}$-RKA-secure.

Claim 1: NM of $f \Rightarrow |\mathsf{Adv}_{\mathcal{A}}^{\text{Game 1}}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{\text{Game 0}}(\lambda)| = \mathsf{negl}(\lambda)$

Define E — $\mathcal{A}$ issues $\langle \phi, t \rangle$ such that $f(\phi(s^*)) = t$ in Game 1.
Game 0 and Game 1 are identical if E never happens.

f is NM $\Rightarrow \Pr[E] = \mathsf{negl}(\lambda) \Rightarrow$ Game 0 $\approx_c$ Game 1

Note: NM is insufficient — except (pp, t^*), $\mathcal{A}$ gets to see

$$k_b^* = \mathsf{hint}(s^*; b) = \begin{cases} k^* = h(s^*) & \text{if } b = 0 \\ k^* \xleftarrow{\text{R}} K & \text{if } b = 1 \end{cases}$$

hinted NM is required! ▸ luckily hint-free NM $\Rightarrow$ hinted NM ☺

Security Proof

If f is Φ-non-malleable, AKDF is $\Phi \cup \mathsf{id} \cup \mathsf{cf}$-RKA-secure.

Claim 1: NM of $f \Rightarrow |\mathsf{Adv}_{\mathcal{A}}^{\text{Game 1}}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{\text{Game 0}}(\lambda)| = \mathsf{negl}(\lambda)$

Define E — $\mathcal{A}$ issues $\langle \phi, t \rangle$ such that $f(\phi(s^*)) = t$ in Game 1.
Game 0 and Game 1 are identical if E never happens.

f is NM $\Rightarrow \Pr[E] = \mathsf{negl}(\lambda) \Rightarrow$ Game 0 $\approx_c$ Game 1

Note: NM is insufficient — except (pp, t^*), $\mathcal{A}$ gets to see

$$k_b^* = \mathsf{hint}(s^*; b) = \begin{cases} k^* = h(s^*) & \text{if } b = 0 \\ k^* \xleftarrow{\text{R}} K & \text{if } b = 1 \end{cases}$$

hinted NM is required! ▸ luckily hint-free NM $\Rightarrow$ hinted NM

Claim 2: f is NM and poly-to-1 $\Rightarrow \mathsf{Adv}_{\mathcal{A}}^{\text{Game 1}}(\lambda) = \mathsf{negl}(\lambda)$.

Security Proof

If f is Φ-non-malleable, AKDF is $\Phi \cup \mathsf{id} \cup \mathsf{cf}$-RKA-secure.

Claim 1: NM of $f \Rightarrow |\mathsf{Adv}_{\mathcal{A}}^{\text{Game 1}}(\lambda) - \mathsf{Adv}_{\mathcal{A}}^{\text{Game 0}}(\lambda)| = \mathsf{negl}(\lambda)$

Define E — $\mathcal{A}$ issues $\langle \phi, t \rangle$ such that $f(\phi(s^*)) = t$ in Game 1.
Game 0 and Game 1 are identical if E never happens.

f is NM $\Rightarrow \Pr[E] = \mathsf{negl}(\lambda) \Rightarrow$ Game 0 $\approx_c$ Game 1

Note: NM is insufficient — except (pp, t^*), $\mathcal{A}$ gets to see

$$k_b^* = \mathsf{hint}(s^*; b) = \begin{cases} k^* = h(s^*) & \text{if } b = 0 \\ k^* \xleftarrow{\text{R}} K & \text{if } b = 1 \end{cases}$$

hinted NM is required! ▸ luckily hint-free NM $\Rightarrow$ hinted NM

Claim 2: f is NM and poly-to-1 $\Rightarrow \mathsf{Adv}_{\mathcal{A}}^{\text{Game 1}}(\lambda) = \mathsf{negl}(\lambda)$.

f is NM and poly-to-1 $\Rightarrow f$ is OW $\Rightarrow k_0^* \approx_c k_1^*$

Summary

Summary

Better efficiency

- compact public parameters
- short tag size and quick tag generation and verification

Summary

Better efficiency

- compact public parameters
- short tag size and quick tag generation and verification

Strong RKA-Security

- strong NM $\Rightarrow$ secure against non-trivial copy attacks
- $\Phi_{\text{brs}}^{\text{srs}}$-NM f $\Rightarrow$ $\Phi_{\text{brs}}^{\text{srs}} \cup \mathsf{id} \cup \mathsf{cf}$ is large yet general

Summary

Better efficiency

- compact public parameters
- short tag size and quick tag generation and verification

Strong RKA-Security

- strong NM $\Rightarrow$ secure against non-trivial copy attacks
- $\Phi_{\text{brs}}^{\text{srs}}$-NM f $\Rightarrow$ $\Phi_{\text{brs}}^{\text{srs}} \cup \mathsf{id} \cup \mathsf{cf}$ is large yet general

Optimizations

- NM functions $\Rightarrow$ NM relations — typically more efficient
- $h = \mathsf{GL} \Rightarrow |k| = 1$, obtain multiple hardcore bits by:
  1. f is OWP — iteration
  2. rely on decisional assumptions
  3. poly-many hardcore bits from differing-input obfuscation
  4. apply PRG at the end

Conclusion

- a formal study of NMFs
  - with simplified syntax
  - a strong game-based security definition
- connections between (A)NM and (A)OW
  - w.r.t. our algebraic abstraction of Φ
- relations between hint-free v.s. hinted notions
- efficient constructions of NMFs
  - (in)directly via the implication AOW $\Rightarrow$ ANM
- address non-trivial copy attacks in RKA area
  - leverage the algebraic technique used in AOW $\Rightarrow$ ANM
- elegant construction of RKA-secure authenticated KDFs
  - via a simple twist of NMFs

Future Works

- direct construction of NMFs
- new construction of NMFs w.r.t. $\Phi \supset \Phi_{\mathrm{brs}}^{\mathrm{srs}}$
- new interesting applications
- connections to other primitives, e.g., non-malleable codes, non-malleable extractors

Any Questions?

Thanks for listening!