Enhanced Security Notions for Dedicated-Key Hash Functions: Definitions and Relationships

Mohammad-Reza Reyhanitabar, Willy Susilo, and Yi Mu

Centre for Computer and Information Security Research

School of Computer Science and Software Engineering

University of Wollongong

Australia

Outline:

- **Introduction**
  - **Two Settings for Hash Functions: Keyless and Dedicated-key**
  - **The Seven Security Notions** (Rogaway and Shrimpton, FSE 2004):
    Coll, Sec, aSec, eSec (TCR or UOWHF) , Pre, aPre, ePre
  - **Enhanced Target Collision Resistance** (Halevi and Krawczyk, Crypto 2006)
  - **Enhanced Collision Resistance** (Yasuda, Asiacrypt 2008)
- **Our Contributions**
  - A New Set of Enhanced Properties: Definitions
  - A Full Picture of the Relationships (Implications and Separations) among the Properties
- **Conclusion**

Two Settings for Hash Functions

1. Keyless Setting: $\mathrm{H} : \mathcal{M} \to \mathcal{C}$

   - Example: $\text{SHA-1} : \{0,1\}^{<2^{64}} \to \{0,1\}^{160}$

2. Dedicated-key Setting (Function Family): $\mathcal{H} : \mathcal{K} \times \mathcal{M} \to \mathcal{C}$

   A member of the family is chosen by a key (index or salt) $K \in \mathcal{K}$ and is a function $\mathrm{H} \triangleq \mathcal{H}_K : \mathcal{M} \to \mathcal{C}$

   - Some examples:

     ★ CRHF family (Damgård, CRYPTO 1987)
     ★ UOWHF family (Naor and Yung, STOC 1989)
     ★ VSH (Contini et al., EUROCRYPT 2006)
     ★ Some SHA-3 Proposals: e.g. Blake (Aumasson et al.), ECHO (Benadjila et al.), SHAvite-3 (Dunkelman-Biham), Skein (Ferguson et al.)

The Seven Security Notions

Rogaway and Shrimpton investigated seven variants for three basic security notions of a dedicated-key hash function at FSE 2004:

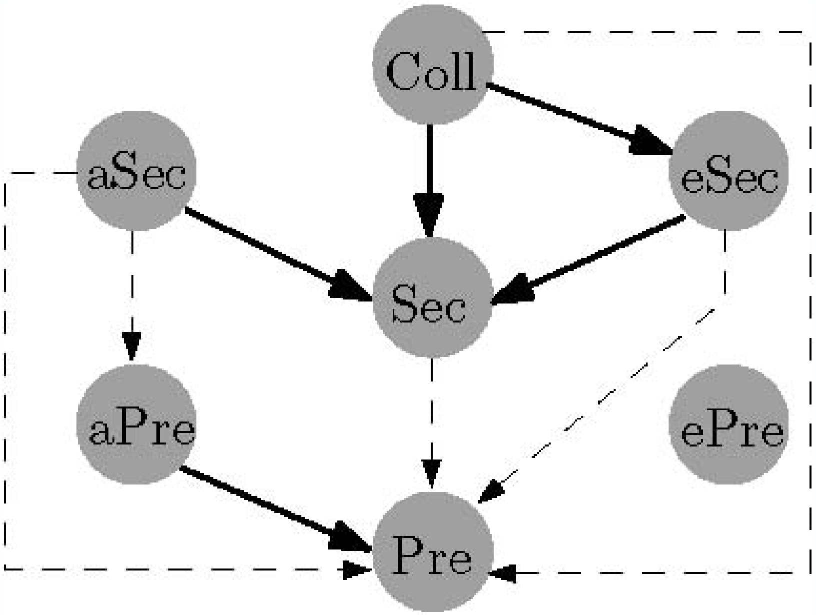
- Collision Resistance (**Coll**)
- Second-Preimage Resistance
  - **Sec**
  - **aSec**
  - **eSec**
- Preimage Resistance
  - **Pre**
  - **aPre**
  - **ePre**

The Seven Security Notions

Rogaway and Shrimpton investigated seven variants for three basic security notions of a dedicated-key hash function at FSE 2004:

- Collision Resistance (**Coll**) $\left\{\mathbf{K} \xleftarrow{\$} \mathcal{K};\ (\mathbf{M}, \mathbf{M'}) \xleftarrow{\$} \mathbf{A}(\mathbf{K}) :\ \mathbf{M} \neq \mathbf{M'}\ \wedge\ \mathcal{H}_{\mathbf{K}}(\mathbf{M}) = \mathcal{H}_{\mathbf{K}}(\mathbf{M'})\right\}$
- Second-Preimage Resistance
  - **Sec** $\left\{\mathbf{K} \xleftarrow{\$} \mathcal{K};\ \mathbf{M} \xleftarrow{\$} \{\mathbf{0},\mathbf{1}\}^{\delta};\ \mathbf{M'} \xleftarrow{\$} \mathbf{A}(\mathbf{K}, \mathbf{M}) :\ \mathbf{M} \neq \mathbf{M'}\ \wedge\ \mathcal{H}_{\mathbf{K}}(\mathbf{M}) = \mathcal{H}_{\mathbf{K}}(\mathbf{M'})\right\}$
  - **aSec** $\left\{(\mathbf{K}, \mathbf{State}) \xleftarrow{\$} \mathbf{A_1}();\ \mathbf{M} \xleftarrow{\$} \{\mathbf{0},\mathbf{1}\}^{\delta};\ \mathbf{M'} \xleftarrow{\$} \mathbf{A_2}(\mathbf{M}, \mathbf{State}) :\ \mathbf{M} \neq \mathbf{M'}\ \wedge\ \mathcal{H}_{\mathbf{K}}(\mathbf{M}) = \mathcal{H}_{\mathbf{K}}(\mathbf{M'})\right\}$
  - **eSec** $\left\{(\mathbf{M}, \mathbf{State}) \xleftarrow{\$} \mathbf{A_1}();\ \mathbf{K} \xleftarrow{\$} \mathcal{K};\ \mathbf{M'} \xleftarrow{\$} \mathbf{A_2}(\mathbf{K}, \mathbf{State}) :\ \mathbf{M} \neq \mathbf{M'}\ \wedge\ \mathcal{H}_{\mathbf{K}}(\mathbf{M}) = \mathcal{H}_{\mathbf{K}}(\mathbf{M'})\right\}$
- Preimage Resistance
  - **Pre** $\left\{\mathbf{K} \xleftarrow{\$} \mathcal{K}; \mathbf{M} \xleftarrow{\$} \{\mathbf{0},\mathbf{1}\}^{\delta}; \mathbf{Y} \leftarrow \mathcal{H}_{\mathbf{K}}(\mathbf{M});\ \mathbf{M'} \xleftarrow{\$} \mathbf{A}(\mathbf{K}, \mathbf{Y}) :\ \mathcal{H}_{\mathbf{K}}(\mathbf{M'}) = \mathbf{Y}\right\}$
  - **aPre** $\left\{(\mathbf{K}, \mathbf{State}) \xleftarrow{\$} \mathbf{A_1}();\ \mathbf{M} \xleftarrow{\$} \{\mathbf{0},\mathbf{1}\}^{\delta};\ \mathbf{Y} \leftarrow \mathcal{H}_{\mathbf{K}}(\mathbf{M});\ \mathbf{M'} \xleftarrow{\$} \mathbf{A_2}(\mathbf{Y}, \mathbf{State}) : \mathcal{H}_{\mathbf{K}}(\mathbf{M'}) = \mathbf{Y}\right\}$
  - **ePre** $\left\{(\mathbf{Y}, \mathbf{State}) \xleftarrow{\$} \mathbf{A_1}();\ \mathbf{K} \xleftarrow{\$} \mathcal{K};\ \mathbf{M'} \xleftarrow{\$} \mathbf{A_2}(\mathbf{K}, \mathbf{State}) : \mathcal{H}_{\mathbf{K}}(\mathbf{M'}) = \mathbf{Y}\right\}$

Relationships among the Seven Notions



Rogaway and Shrimpton, FSE 2004
(revised ePrint version: Report 2004/035)

Enhanced Target Collision Resistance (eTCR)

Definition (Halevi and Krawczyk, Crypto 2006)

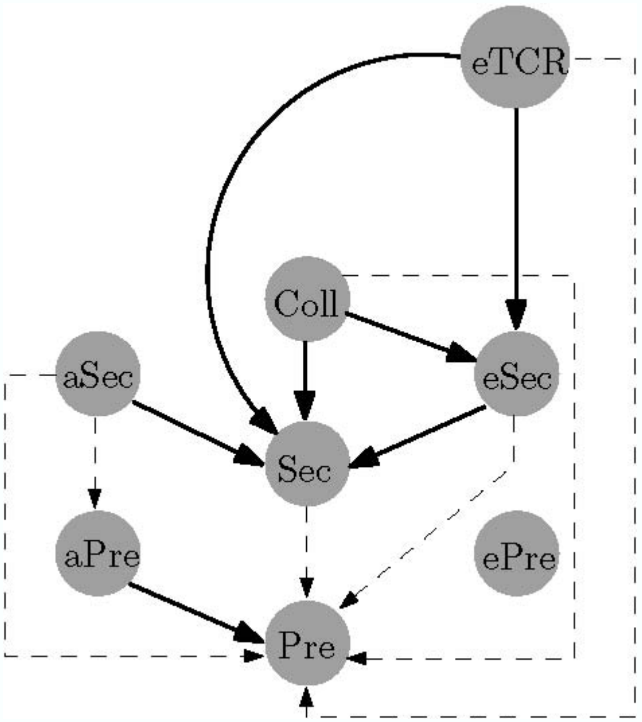
$$\mathrm{Adv}_{\mathcal{H}}^{eTCR}(A) = \Pr\left\{ \begin{array}{ll} (M, State) \stackrel{\$}{\leftarrow} A_1(); & \\ K \stackrel{\$}{\leftarrow} \mathcal{K}; & : (K, M) \neq (K', M') \ \wedge \ \mathcal{H}_K(M) = \mathcal{H}_{K'}(M') \\ (K', M') \stackrel{\$}{\leftarrow} A_2(K, State); & \end{array} \right\}$$

Enhanced Target Collision Resistance (eTCR)

Definition (Halevi and Krawczyk, Crypto 2006)

$$\mathrm{Adv}_{\mathcal{H}}^{eTCR}(A) = \Pr\left\{ \begin{array}{l} (M, State) \xleftarrow{\$} A_1(); \\ K \xleftarrow{\$} \mathcal{K}; \\ (K', M') \xleftarrow{\$} A_2(K, State); \end{array} : (K, M) \neq (K', M') \ \wedge \ \mathcal{H}_K(M) = \mathcal{H}_{K'}(M') \right\}$$

Relationships (Reyhanitabar, Susilo, and Mu, FSE 2009 and ePrint report 2009/506)



Enhanced Collision Resistance (eColl)

Definition (Yasuda, Asiacrypt 2008)

$$\mathrm{Adv}_{\mathcal{H}}^{eColl}(A) = \Pr\left\{K \xleftarrow{\$} \mathcal{K}; (K', M', M) \xleftarrow{\$} A_2(K, State) : (K, M) \neq (K', M') \ \wedge \ \mathcal{H}_K(M) = \mathcal{H}_{K'}(M')\right\}$$

Some of the relationships between eColl and other properties, especially in the complexity-theoretic sense, were considered by Yasuda at Asiacrypt 2008.

Enhanced (Strengthened) Variants of the other Properties

1. Strengthened "Coll": s-Coll (= "eColl")
2. Strengthened "Sec": s-Sec
3. Strengthened "aSec": s-aSec
4. Strengthened "eSec": s-eSec (= "eTCR")
5. Strengthened "Pre": s-Pre
6. Strengthened "aPre": s-aPre
7. Strengthened "ePre"?

Definitions

The s-XXX property, for $\mathrm{XXX} \in \{\mathbf{Coll}, \mathbf{Sec}, \mathbf{aSec}, \mathbf{eSec}, \mathbf{Pre}, \mathbf{aPre}\}$ is defined by modifying the game defining the XXX property s.t. the adversary gets to choose a second key, possibly different from the first key, and the success event is defined accordingly.

Definitions

The s-XXX property, for $\mathrm{XXX} \in \{\mathbf{Coll}, \mathbf{Sec}, \mathbf{aSec}, \mathbf{eSec}, \mathbf{Pre}, \mathbf{aPre}\}$ is defined by modifying the game defining the XXX property s.t. the adversary gets to choose a second key, possibly different from the first key, and the success event is defined accordingly.

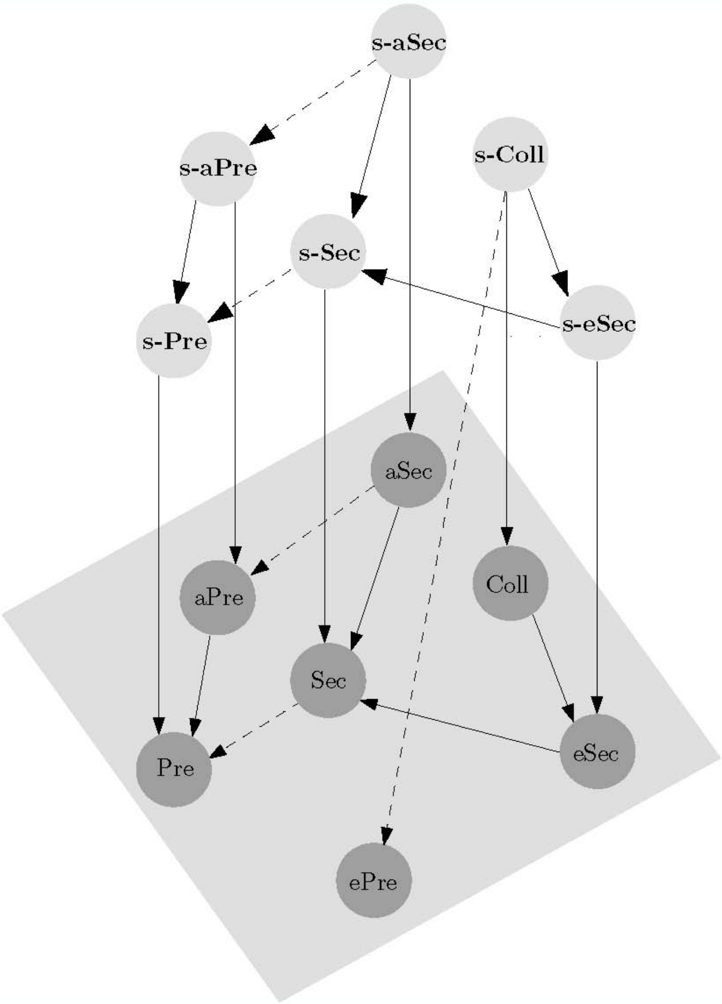
$$\mathrm{Adv}_H^{\text{s-Sec}[\delta]}(A) = \Pr\left[\begin{array}{ll} K \xleftarrow{\$} \mathcal{K}; M \xleftarrow{\$} \{0,1\}^{\delta}; & \\ K', M' \xleftarrow{\$} A(K, M) & : (K, M) \neq (K', M') \wedge H_K(M) = H_{K'}(M') \end{array}\right]$$

$$\mathrm{Adv}_H^{\text{s-aSec}[\delta]}(A) = \Pr\left[\begin{array}{ll} (K, State) \xleftarrow{\$} A_1(); & \\ M \xleftarrow{\$} \{0,1\}^{\delta}; & \\ K', M' \xleftarrow{\$} A_2(M, State) & : (K, M) \neq (K', M') \wedge H_K(M) = H_{K'}(M') \end{array}\right]$$

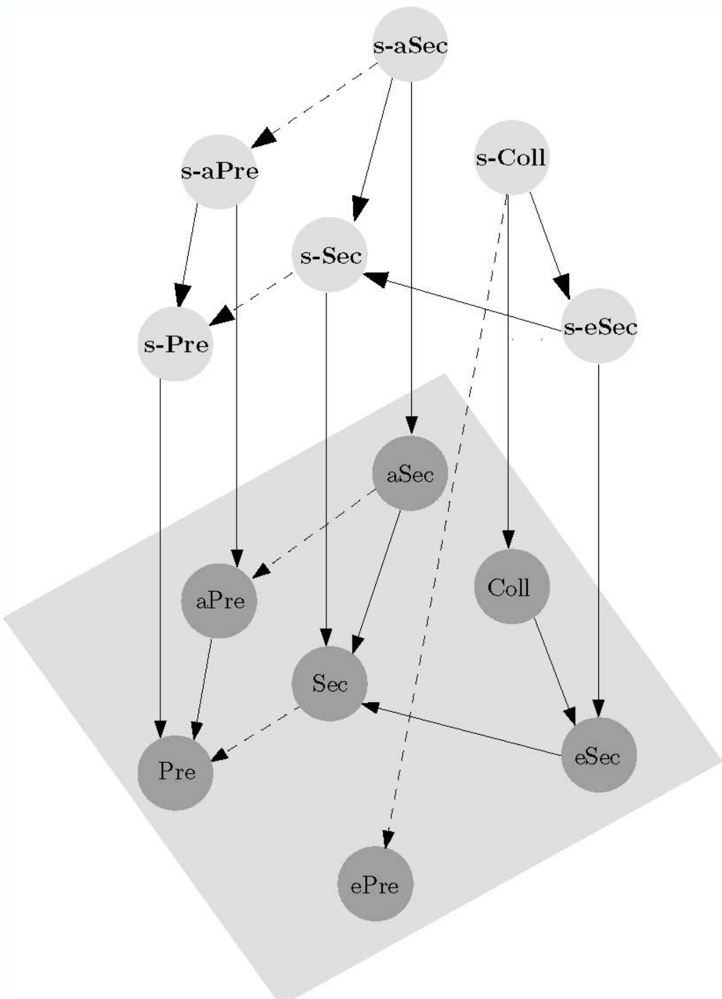
$$\mathrm{Adv}_H^{\text{s-Pre}[\delta]}(A) = \Pr\left[\begin{array}{ll} K \xleftarrow{\$} \mathcal{K}; M \xleftarrow{\$} \{0,1\}^{\delta}; Y \leftarrow H_K(M); & \\ K', M' \xleftarrow{\$} A(K, Y) & : H_{K'}(M') = Y \end{array}\right]$$

$$\mathrm{Adv}_H^{\text{s-aPre}[\delta]}(A) = \Pr\left[\begin{array}{ll} (K, State) \xleftarrow{\$} A_1(); & \\ M \xleftarrow{\$} \{0,1\}^{\delta}; Y \leftarrow H_K(M); & \\ K', M' \xleftarrow{\$} A_2(Y, State) & : H_{K'}(M') = Y \end{array}\right]$$

Relationships among the Thirteen Security Notions



Relationships among the Thirteen Security Notions



	s-Coll (eColl)	s-Sec	s-aSec	s-eSec (eTCR)	s-Pre	s-aPre
s-Coll (eColl)	=	$\rightarrow$	$\not\rightarrow$	$\rightarrow$ [27]	$\dashrightarrow$	$\not\rightarrow$
s-Sec	$\not\rightarrow$	=	$\not\rightarrow$	$\not\rightarrow$	$\dashrightarrow$	$\not\rightarrow$
s-aSec	$\not\rightarrow$	$\rightarrow$	=	$\not\rightarrow$	$\dashrightarrow$	$\dashrightarrow$
s-eSec (eTCR)	$\not\rightarrow$	$\rightarrow$	$\not\rightarrow$	=	$\dashrightarrow$	$\not\rightarrow$
s-Pre	$\not\rightarrow$	$\not\rightarrow$	$\not\rightarrow$	$\not\rightarrow$	=	$\not\rightarrow$
s-aPre	$\not\rightarrow$	$\not\rightarrow$	$\not\rightarrow$	$\not\rightarrow$	$\rightarrow$	=

	Coll	Sec	aSec	eSec (TCR)	Pre	aPre	ePre
s-Coll (eColl)	$\rightarrow$	$\rightarrow$	$\not\rightarrow$	$\rightarrow$	$\dashrightarrow$	$\not\rightarrow$	$\dashrightarrow$
s-Sec	$\not\rightarrow$	$\rightarrow$	$\not\rightarrow$	$\not\rightarrow$	$\dashrightarrow$	$\not\rightarrow$	$\not\rightarrow$
s-aSec	$\not\rightarrow$	$\rightarrow$	$\rightarrow$	$\not\rightarrow$	$\dashrightarrow$	$\dashrightarrow$	$\not\rightarrow$
s-eSec (eTCR)	$\not\rightarrow$ [20]	$\rightarrow$ [21]	$\not\rightarrow$ [21]	$\rightarrow$ [21]	$\dashrightarrow$ [21]	$\not\rightarrow$ [21]	$\not\rightarrow$ [21]
s-Pre	$\not\rightarrow$	$\not\rightarrow$	$\not\rightarrow$	$\not\rightarrow$	$\rightarrow$	$\not\rightarrow$	$\not\rightarrow$
s-aPre	$\not\rightarrow$	$\not\rightarrow$	$\not\rightarrow$	$\not\rightarrow$	$\rightarrow$	$\rightarrow$	$\not\rightarrow$

	s-Coll	s-Sec	s-aSec	s-eSec (eTCR)	s-Pre	s-aPre
Coll	$\not\rightarrow$	$\not\rightarrow$	$\not\rightarrow$	$\not\rightarrow$ [20]	$\not\rightarrow$	$\not\rightarrow$
Sec	$\not\rightarrow$	$\not\rightarrow$	$\not\rightarrow$	$\not\rightarrow$ [21]	$\not\rightarrow$	$\not\rightarrow$
aSec	$\not\rightarrow$	$\not\rightarrow$	$\not\rightarrow$	$\not\rightarrow$ [21]	$\not\rightarrow$	$\not\rightarrow$
eSec (TCR)	$\not\rightarrow$	$\not\rightarrow$	$\not\rightarrow$	$\not\rightarrow$ [21]	$\not\rightarrow$	$\not\rightarrow$
Pre	$\not\rightarrow$	$\not\rightarrow$	$\not\rightarrow$	$\not\rightarrow$ [21]	$\not\rightarrow$	$\not\rightarrow$
aPre	$\not\rightarrow$	$\not\rightarrow$	$\not\rightarrow$	$\not\rightarrow$ [21]	$\not\rightarrow$	$\not\rightarrow$
ePre	$\not\rightarrow$	$\not\rightarrow$	$\not\rightarrow$	$\not\rightarrow$ [21]	$\not\rightarrow$	$\not\rightarrow$

[20, 21] Reyhanitabar, Susilo, Mu, FSE 2009 and ePrint report 2009/506

[27] Yasuda, Asiacrypt 2008

Notions of Implications

Let xxx and yyy be two security notions defined for an *arbitrary* hash function $H : \mathcal{K} \times \mathcal{M} \to \{0,1\}^n$, and fix δ such that $\{0,1\}^\delta \subseteq \mathcal{M}$.

- ★ **Security-Preserving Implications** (xxx $\to$ yyy):
  $\mathrm{Adv}_H^{\mathsf{yyy}}(t') \leq c\mathrm{Adv}_H^{\mathsf{xxx}}(t)$, for *all* such hash functions H, where $t' = t - c'T_{H,\delta}$ and c, c' are constants.

- ★ **Provisional Implications** (xxx $\dashrightarrow$ yyy):
  We establish one of the following two concrete bounds:
  1. $\mathrm{Adv}_H^{\mathsf{yyy}}(t') \leq c\mathrm{Adv}_H^{\mathsf{xxx}}(t) + \mu(n,k,\delta)$
  2. $\mathrm{Adv}_H^{\mathsf{yyy}}(t') \leq c\mathrm{Adv}_H^{\mathsf{xxx}}(t) + c'\sqrt{\mathrm{Adv}_H^{\mathsf{xxx}}(t)} + \mu(n,k,\delta)$

, where $t' = t - c'T_{H,\delta}$; c, c' are some non-negative constants, and $\mu(n,k,\delta)$ depends on the hash function parameters n, k and δ (e.g. $\mu(n,k,\delta) = 2^{n-\delta}$).

Example: s-Coll $\dashrightarrow$ ePre

Theorem. For any $H : \mathcal{K} \times \mathcal{M} \to \{0,1\}^n$: $\mathrm{Adv}_H^{ePre}(t') \leq \sqrt{\mathrm{Adv}_H^{s-Coll}(t)} + \frac{1}{|\mathcal{K}|}$, where $t' = t - c$, for some small constant c.

Notations:

- $y \xleftarrow{\$} A(x_1, \cdots, x_n)$ means: $R \xleftarrow{\$} \{0,1\}^{r(|x|)}$ and $y = A(x_1, \cdots, x_n; R)$
- Let Verify(M, K, Y) be a deterministic predicate defined as follows:

$$\mathrm{Verify}(M, K, Y) = \begin{cases} 1 & \text{if } H_K(M) = Y \\ 0 & \text{otherwise} \end{cases}$$

Proof

ePre Experiment

$R \xleftarrow{\$} \{0,1\}^r$; $(Y, State) = A(\varnothing; R)$;

$K \xleftarrow{\$} \mathcal{K}$; $M = A(K, State; R)$; $d = \text{Verify}(M, K, Y)$;

Return d

Reset Experiment:

$R \xleftarrow{\$} \{0,1\}^r$; $(Y, State) = A(\varnothing; R)$;

$K1 \xleftarrow{\$} \mathcal{K}$; $M1 = A(K1, State; R)$; $d_1 = \text{Verify}(M1, K1, Y)$;

$K2 \xleftarrow{\$} \mathcal{K}$; $M2 = A(K2, State; R)$; $d_2 = \text{Verify}(M2, K2, Y)$;

If $(d_1 = 1 \wedge d_2 = 1 \wedge K1 \neq K2)$ then **return 1** else **return 0**

Proposition. **Let p denote the probability that the ePre Experiment returns 1 and q be the probability that the Reset Experiment returns 1; we have** $\mathbf{p} \leq \sqrt{\mathbf{q}} + \frac{1}{|\mathcal{K}|}$.

Separations

- We use xxx $\nrightarrow$ yyy to show that the notion xxx does not imply the notion yyy, in the "conventional sense".

- Assuming that there exists a function $H : \{0,1\}^k \times \{0,1\}^m \rightarrow \{0,1\}^n$ that is (t, ϵ) − xxx secure, we construct (as a counterexample) a function $G : \{0,1\}^k \times \{0,1\}^m \rightarrow \{0,1\}^n$ which is also (t', ϵ') − xxx secure, but *completely insecure* in yyy sense; *i.e.* $\mathrm{Adv}_G^{\mathsf{yyy}}(c'') \approx 1$, where c'' is a small constant.

  - In our separation results, we show counterexamples for which either $\mathrm{Adv}_G^{\mathsf{yyy}}(c'') = 1$, or $\mathrm{Adv}_G^{\mathsf{yyy}}(c'') = 1 - 2^{-m}$ which for any typical value of m becomes ≈ 1.

Counterexamples used in our Separations

$$G1_K(M) = \begin{cases} C^* & \text{if } K = K^* \\ H_K(M) & \text{otherwise} \end{cases}$$

$$G2_K(M) = \begin{cases} K_{1\ldots n} & \text{if } val(M) = val(K) \\ H_K(M) & \text{otherwise} \end{cases}$$

$$G3_K(M) = \begin{cases} H_K(0^{m-k}||K) & \text{if } M = 1^{m-k}||K \\ H_K(M) & \text{otherwise} \end{cases}$$

$$G4_K(M) = \begin{cases} C^* & \text{if } M = 0^m \vee M = 1^m \\ H_K(M) & \text{otherwise} \end{cases}$$

$$G5_K(M) = H_K(M_{1\cdots m-1}||0)$$

$$G6_K(M) = \begin{cases} C^* & \text{if } M = M^* \\ H_K(M) & \text{otherwise} \end{cases}$$

$$G7_K(M) = \begin{cases} K_{1\ldots n} & \text{if } val(M) = val(K) \\ H_K(\langle val(K)\rangle_m) & \text{if } val(M) \neq val(K) \wedge H_K(M) = K_{1\ldots n} \\ H_K(M) & \text{otherwise} \end{cases}$$

$$G8_K(M) = \begin{cases} K_{1\ldots n} & \text{if } M = M^* \\ H_K(M^*) & \text{if } M \neq M^* \wedge H_K(M) = K_{1\ldots n} \\ H_K(M) & \text{otherwise} \end{cases}$$

$$G9_K(M) = \begin{cases} K_{1\ldots n} & \text{if } M = M^* \\ H_K(M) & \text{otherwise} \end{cases}$$

Example: s-eSec (eTCR) $\not\longrightarrow$ s-Coll

Assume that we have a hash function $H : \{0,1\}^k \times \{0,1\}^m \to \{0,1\}^n$, with $m > k \geq n$, which is $(t, \epsilon) - eTCR$.

The hash function $G3 : \{0,1\}^k \times \{0,1\}^m \to \{0,1\}^n$ is $(t', \epsilon') - eTCR$, where $t' = t - c$, $\epsilon' = \epsilon + 2^{-k+1}$, but it is completely insecure in the s-Coll sense, i.e. $\mathrm{Adv}_{G3}^{s-Coll}(c') = 1$.

$$G3_K(M) = \begin{cases} H_K(0^{m-k}||K) & \text{if } M = 1^{m-k}||K \\ H_K(M) & \text{otherwise} \end{cases}$$

Conclusion

- An extended set of security notions for dedicated-key hash functions, including eTCR and eColl properties, was defined.
- A full picture of the relationships among the (thirteen) security properties, including the (six) enhanced properties and the previously considered seven properties, was provided.
- The new enhanced properties introduced in this paper may find interesting applications in practice.
- Meanwhile, these new enhanced properties can be considered by cryptanalysts as easier targets for certificational attacks against dedicated-key hash functions.

Questions?

<u>Thanks!</u>

감사합니다