Further More on Key Wrapping

2011/2/17

SKEW2011 Lyngby

Nagoya University

Yasushi Osaki, Tetsu Iwata

What is key wrapping?

- Used to encrypt specialized data, such as cryptographic keys

- A key wrapping that also ensures integrity is called an authenticated key wrapping (AKW)

- Used in key management systems
  - Used as an adapter between incompatible systems
  - e.g. between a key management system for 3DES and AES etc.

What is key wrapping?

- Key wrapping and AKW are widely used in practice
  - ANSI X9.102-2008 (2008)
  - IETF RFC 6030 (2010)
  - OASIS : Key Management Interoperability Protocol Specification Version 1.0
- NIST is in the process of specifying an AKW scheme

Two approaches in designing an AKW scheme

- Dedicated construction
  - Deterministic authenticated encryption (DAE) [RS06]
    - SIV mode [RS06]
    - HBS mode

- Generic composition
  - Hash-then-Encrypt [GH09]
    - Hash-then-ECB, Hash-then-CBC, Hash-then-CTR, etc.

[GH09]R.Gennaro,S.Halevi. More on Key Wrapping. SAC2009.
[RS06] Rogaway. P., Shrimpton. T.: A Provable-Security Treatment of the Key-Wrap Problem. EUROCRYPT 2006.

Gennaro and Halevi's results

- They examined combinations of some encryption modes and some hash functions

Encryption \ Hash	XOR	Linear	2nd-preimage resistant	universal hash
CTR	broken	broken	secure	secure
ECB	broken	somewhat	secure	broken
CBC	broken	somewhat	secure	open problem
masked ECB/CBC	somewhat	somewhat	secure	secure
XEX	secure	secure	secure	secure

Gennaro and Halevi's results

- They examined combinations of some encryption modes and some hash functions

Encryption \ Hash	XOR	Linear	2nd-preimage resistant	universal hash
CTR	broken	broken	secure	secure
ECB	broken	somewhat	secure	broken
CBC	broken	somewhat	secure	open problem
masked ECB/CBC	somewhat	somewhat	secure	secure
XEX	secure	secure	secure	secure

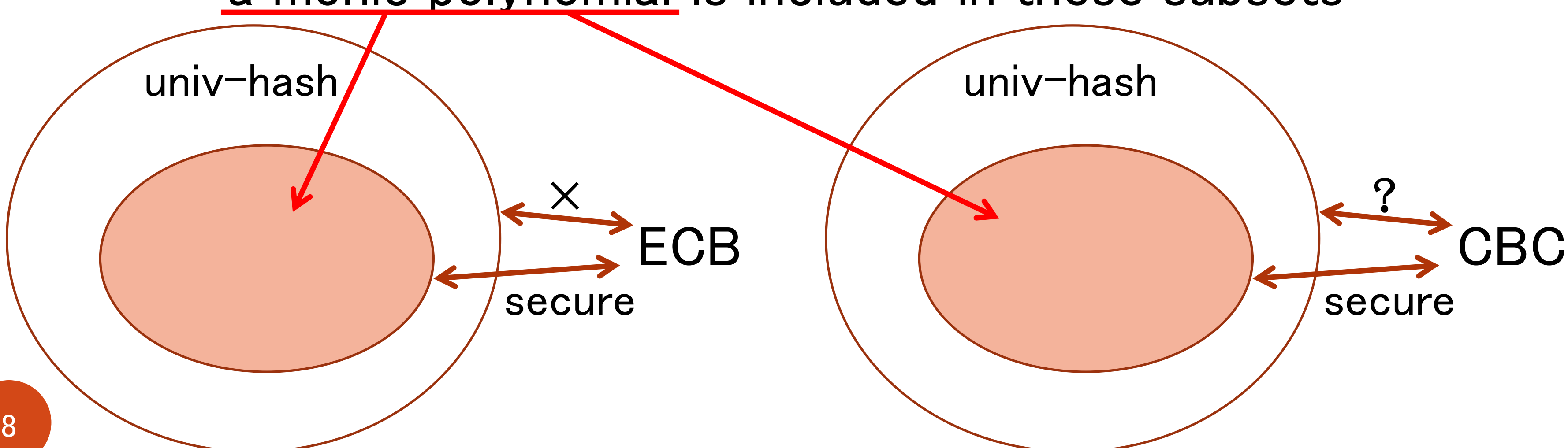
Gennaro and Halevi's results

- ECB and CBC modes are likely deployed already in existing systems
- There are a large number of efficient constructions of a univ-hash function, e.g. a polynomial hash function, MMH, etc.

Hash / Encryption	XOR	Linear	2nd-preimage resistant	universal hash
CTR	broken	broken	secure	secure
ECB	broken	somewhat	secure	broken
CBC	broken	somewhat	secure	open problem
masked ECB/CBC	somewhat	somewhat	secure	secure
XEX	secure	secure	secure	secure

Our goal

- We show
  - there exists a subset of univ-hash functions that can securely be used with ECB mode
  - there exists a subset of univ-hash functions that can securely be used with CBC mode (It is a partial answer to the open problem)
  - <u>a monic polynomial</u> is included in these subsets



AKW scheme

- Wrapping key 'W'
- Encrypt a plaintext '$D \in \{0,1\}^{nl}$' under W
  - $C \leftarrow \mathrm{AKW}_W(D)$
- Decrypt a ciphertext '$C \in \{0,1\}^{n(l+1)}$' under W
  - D or $\perp \leftarrow \mathrm{AKW}^{-1}{}_W(C)$
  - $\perp$ means reject

Security for AKW (1) [GH09]

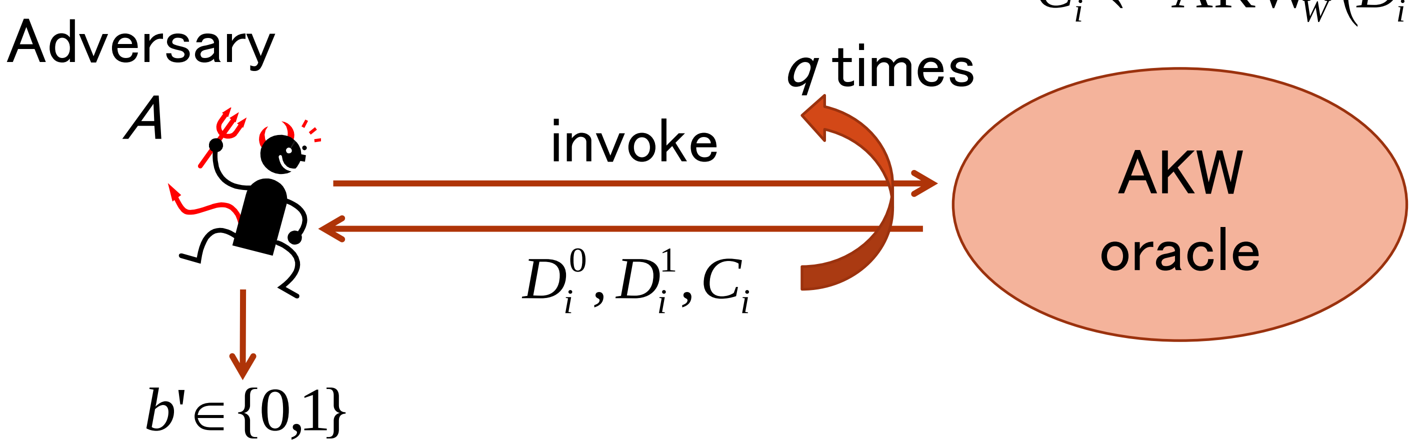
- Random-Plaintext Attack (RPA-security)

Challenge bit: $b \in \{0,1\}$

Wrapping key: W

D_i^0, D_i^1 : chosen at random

$C_i \leftarrow \mathrm{AKW}_W\left(D_i^b\right)$



$$\mathrm{Adv}_{\mathrm{AKW}}^{\mathrm{rpa}}(A) = \Pr[b' = 1 \mid b = 1] - \Pr[b' = 1 \mid b = 0]$$

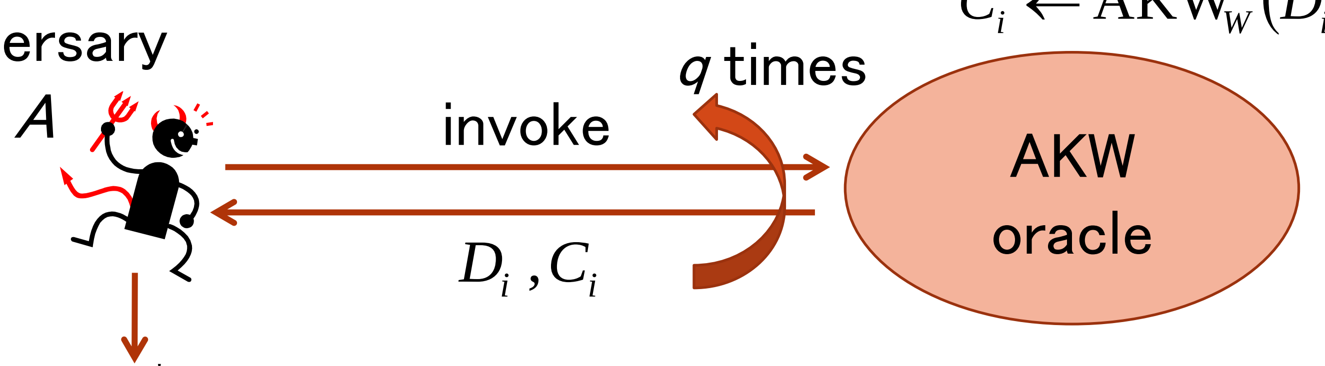
Security for AKW (2) [GH09]

- Integrity of ciphertext (INT-security)

Wrapping key : W

D_i : chosen at random

$C_i \leftarrow \mathrm{AKW}_W(D_i)$

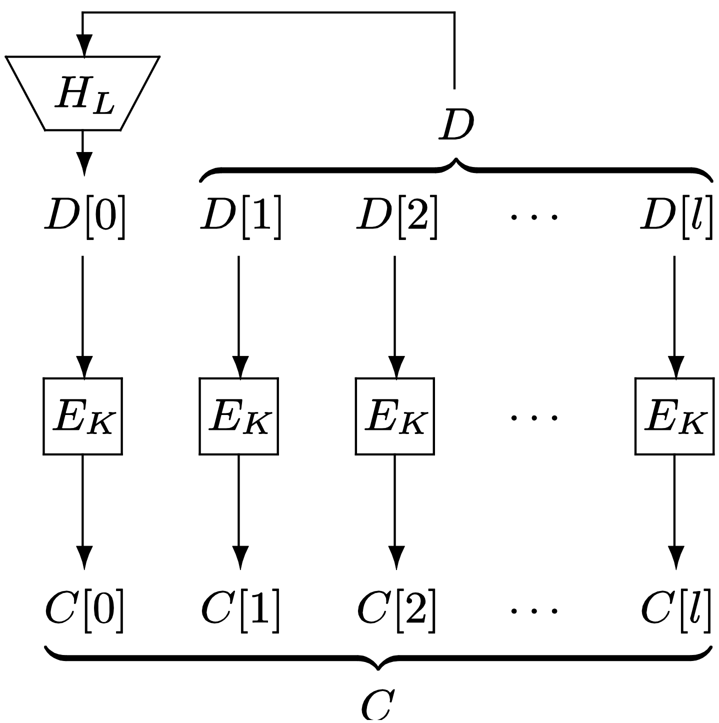


C^* : Challenge ciphertext

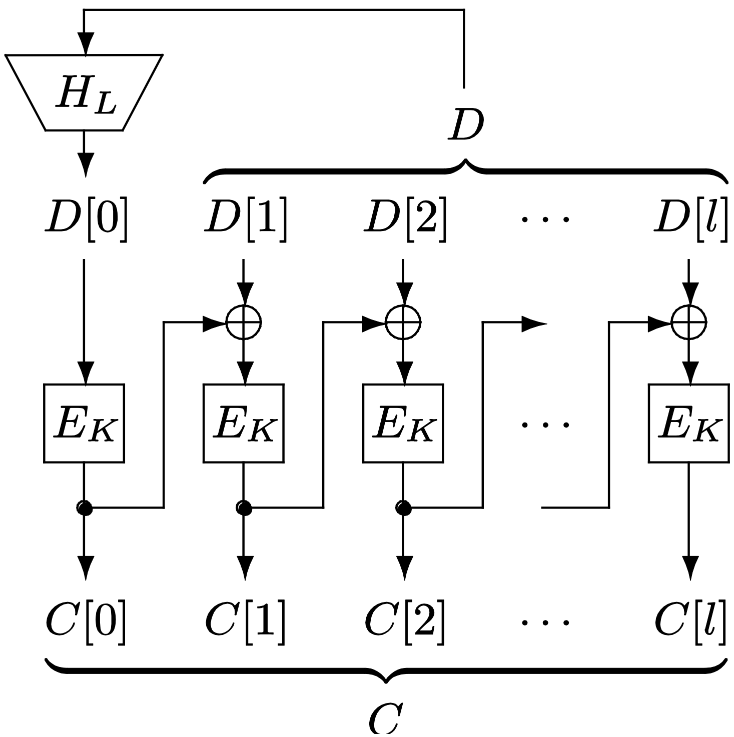
$$\mathrm{Adv}^{\mathrm{int}}_{\mathrm{AKW}}(A) = \Pr[A \text{ forges }]$$

The AKW scheme is secure, if $\mathrm{Adv}^{\mathrm{rpa}}(A)$ and $\mathrm{Adv}^{\mathrm{int}}(A)$ are sufficiently small

Hash-then-ECB [GH09] and Hash-then-CBC [GH09]



Hash-then-ECB (HtECB)

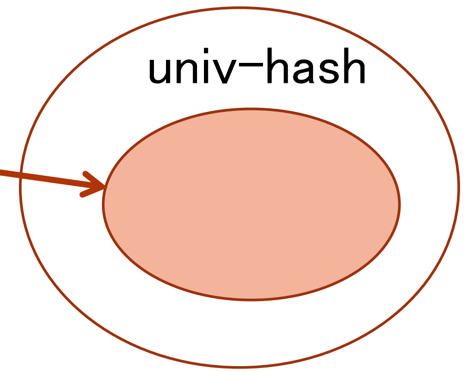


Hash-then-CBC (HtCBC)

Our results

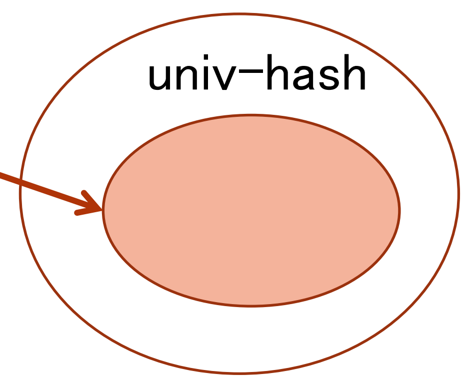
- The HtECB scheme is a secure AKW scheme if the underlying hash function is a
  - universal
  - uniform
  - universal_C
  - uniform_C

  hash function



- The HtCBC scheme is a secure AKW scheme if the underlying hash function is a
  - universal
  - uniform
  - universal_{CC}
  - uniform_{CC}

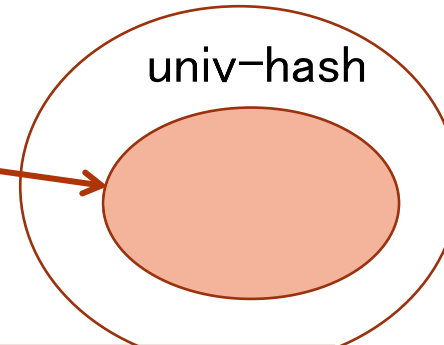
  hash function



Our results

- The HtECB scheme is a secure AKW scheme if the underlying hash function is a
  - universal
  - universal$_C$
  - uniform
  - uniform$_C$

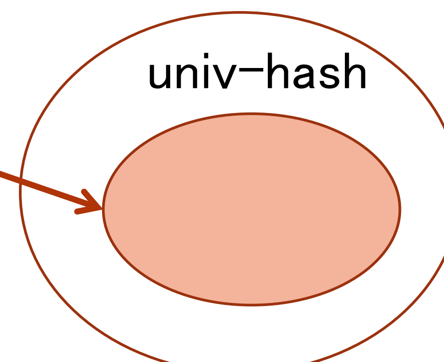
  hash function



We present these new notions

- The HtCBC scheme is a secure AKW scheme if the underlying hash function is a
  - universal
  - universal$_{CC}$
  - uniform
  - uniform$_{CC}$

  hash function



Classical notions of hash function

- universal
  - Let $X, X' \in \{0,1\}^{nl} (X \neq X')$ be arbitrary bit strings
  - A keyed hash function *H* is an ε_1−universal hash function if

$$\Pr[H_L(X) = H_L(X')] \leq \varepsilon_1$$

- uniform
  - Let $X \in \{0,1\}^{nl}, Y \in \{0,1\}^n$ be arbitrary bit strings
  - A keyed hash function *H* is an ε_2−uniform hash function if

$$\Pr[H_L(X) = Y] \leq \varepsilon_2$$

New notions of hash function

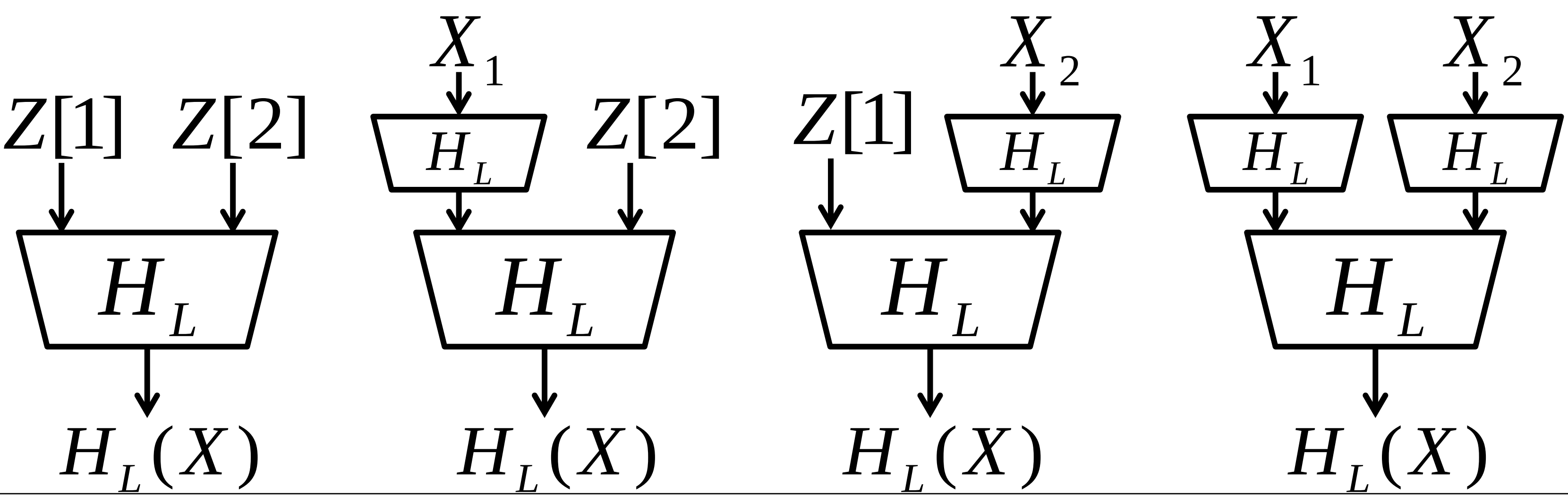
- universal$_C$ (universal with composition)
  - Let $X_1,\ldots,X_l \in \{0,1\}^{nl}, Z[1],\ldots Z[l] \in \{0,1\}^n$ and $X' \in \{0,1\}^{nl} (X' \neq (Z[1],\ldots,Z[l]))$ be arbitrary bit strings
  - A keyed hash function *H* is an ε_3–universal$_C$ hash function if, for each of the 2^l possible choices of $X \in \{Z[1], H_L(X_1)\} \times \cdots \times \{Z[l], H_L(X_l)\}$,

$$\Pr[H_L(X) = H_L(X')] \leq \varepsilon_3$$

New notions of hash function

- universal$_C$
  - For example, if l=2, we require

$$
\begin{cases}
\Pr[\; H_L(Z[1], Z[2]) = H_L(X')] \le \varepsilon_3 \\
\Pr[\; H_L(H_L(X_1), Z[2]) = H_L(X')] \le \varepsilon_3 \\
\Pr[\; H_L(Z[1], H_L(X_2)) = H_L(X')] \le \varepsilon_3 \\
\Pr[H_L(H_L(X_1), H_L(X_2)) = H_L(X')] \le \varepsilon_3
\end{cases}
$$



New notions of hash function

- uniform$_C$ (uniform with composition)
  - Let $X_1,\ldots,X_l \in \{0,1\}^{nl}, Z[1],\ldots Z[l] \in \{0,1\}^n$ and $Y \in \{0,1\}^n$ be arbitrary bit strings
  - A keyed hash function *H* is an ε_4–uniform$_C$ hash function if, for each of the 2^l possible choices of $X \in \{Z[1], H_L(X_1)\} \times \cdots \times \{Z[l], H_L(X_l)\}$,

$$\Pr[H_L(X) = Y] \le \varepsilon_4$$

New notions of hash function

- universal$_{CC}$(universal with composition and xor constant)
  - Let $X_1,\ldots,X_l \in \{0,1\}^{nl}, Z[1],\ldots Z[l] \in \{0,1\}^n, V[1],\ldots,V[l] \in \{0,1\}^n$ and $X' \in \{0,1\}^{nl} (X' \neq (Z[1],\ldots,Z[l]))$ be arbitrary bit strings
  - A keyed hash function *H* is an ε_5–universal$_{CC}$ hash function if, for each of the 2^l possible choices ,of $X \in \{Z[1], H_L(X_1) \oplus V[1]\} \times \cdots \times \{Z[l], H_L(X_l) \oplus V[l]\}$

$$\Pr[H_L(X) = H_L(X')] \leq \varepsilon_5$$

New notions of hash function

- uniform$_{CC}$ (uniform with composition and xor constant)
  - Let $X_1,\ldots,X_l \in \{0,1\}^{nl}, Z[1],\ldots Z[l] \in \{0,1\}^n, V[1],\ldots,V[l] \in \{0,1\}^n$ and $Y \in \{0,1\}^n$ be arbitrary bit strings
  - A keyed hash function H is an ε_6–uniform$_{CC}$ hash function if, for each of the 2^l possible choices ,of $X \in \{Z[1], H_L(X_1) \oplus V[1]\} \times \cdots \times \{Z[l], H_L(X_l) \oplus V[l]\}$

$$\Pr[H_L(X) = Y] \leq \varepsilon_6$$

Theorem 1 (HtECB)

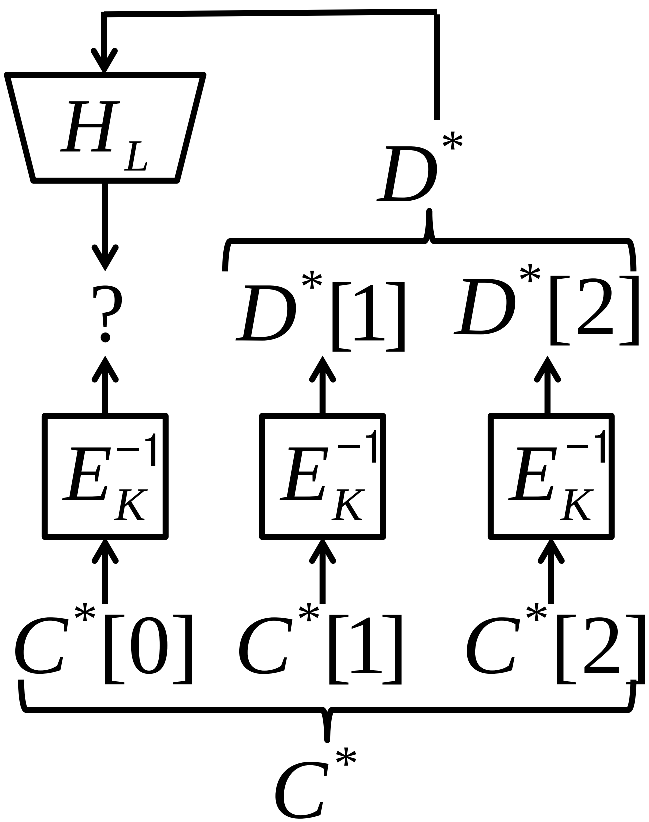
- Let H be an ε_1–universal, ε_2–uniform, ε_3–universal$_C$, ε_4–uniform$_C$ hash function
- E be a blockcipher
- Then for any A that invokes the oracle at most q times, there exist adversaries A' and A'' such that

$$\mathrm{Adv}^{\mathrm{rpa}}_{\mathrm{HtECB[H,E]}}(A) \le \mathrm{Adv}^{\mathrm{prp}}_{E}(A') + \frac{2q^2l^2}{2^n} + 2q^2\varepsilon_1 + 4q^2 l \varepsilon_2$$

$$\mathrm{Adv}^{\mathrm{int}}_{\mathrm{HtECB[H,E]}}(A) \le \mathrm{Adv}^{\mathrm{sprp}}_{E}(A'') + \frac{q^2}{2}\varepsilon_1 + q^2 l \varepsilon_2 + q(l+1)\varepsilon_2 + \max\{\varepsilon_3, \varepsilon_4\}$$

where A' makes at most $q(l+1)$ queries and A'' makes at most $(q+1)(l+1)$ queries

Proof of INT Advantage (intuition)



- l =2
- D*[j] ($0 \leqq j \leqq 2$) are a hash value or a fixed constant

- If D*[0] is a hash value, $\Pr[H_L(D^*)=D^*[0]] \leqq \varepsilon_3$ because H is ε_3-universal$_C$ hash function

- If D*[0] is a fixed constant, $\Pr[H_L(D^*)=D^*[0]] \leqq \varepsilon_4$ because H is ε_4-uniform$_C$ hash function

$$\mathrm{Adv}^{\mathrm{int}}_{\mathrm{HtECB[H,E]}}(A) \leq \mathrm{Adv}^{\mathrm{sprp}}_{E}(A'') + \frac{q^2}{2}\varepsilon_1 + q^2 l \varepsilon_2 + q(l+1)\varepsilon_2 + \max\{\varepsilon_3, \varepsilon_4\}$$

Theorem 2 (HtCBC)

- Let H be an ε_1–universal, ε_2–uniform, ε_5–universal$_{\mathrm{CC}}$, ε_6–uniform$_{\mathrm{CC}}$ hash function
- E be a blockcipher
- Then for any A that invokes the oracle at most q times, there exist adversaries A' and A'' such that

$$\mathrm{Adv}^{\mathrm{rpa}}_{\mathrm{HtCBC[H,E]}}(A) \le \mathrm{Adv}^{\mathrm{prp}}_{E}(A') + 2q^2\varepsilon_1 + \frac{14q^2(l+1)^2}{2^n}$$

$$\mathrm{Adv}^{\mathrm{int}}_{\mathrm{HtCBC[H,E]}}(A) \le \mathrm{Adv}^{\mathrm{sprp}}_{E}(A'') + \frac{q^2}{2}\varepsilon_1 + q^2 l\varepsilon_2 + q(l+1)\varepsilon_2 + \max\{\varepsilon_5, \varepsilon_6\}$$

where A' makes at most $q(l+1)$ queries and A'' makes at most $(q+1)(l+1)$ queries

Construction of a Hash Function

- A monic polynomial hash function defined in (1) suffices to obtain an

• universal	• universal_C	• universal_{CC}
• uniform	• uniform_C	• uniform_{CC}

hash function for sufficiently small $\varepsilon_1,\ldots,\varepsilon_6$

$$H_L(X) = L^{l+1} \oplus L^l \cdot X[1] \oplus \cdots \oplus L \cdot X[l] \qquad \cdots(1)$$

- Input : $X = (X[1], \ldots, X[l]) \in \{0,1\}^{nl}$
- Key : $L \in \{0,1\}^n$
- The multiplication is over $GF(2^n)$

A monic polynomial hash function

- It can be implemented easily from a polynomial hash function
- A polynomial hash function is the basic construction of a universal hash function
  - Used in [MV04][NIST800-38D][Be05]

[MV04] McGrew, D., Viega, J.: The Security and Performance of the Galois/Counter Mode (GCM) of Operation.

[NIST800-38D] NIST: Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC.

[Be05] Bernstein, D.J.: The poly1305-AES Message-Authentication Code.

Conclusions

- We proposed a total of four new notions of a keyed hash function
- Based on the new notions, we showed that HtECB and HtCBC schemes are secure AKW schemes
  - The result on the HtCBC scheme partially solves the open problem
- We showed that there exists an efficient construction of a keyed hash function that satisfies all the six notions

Thank you!

Lemma 3

- The keyed hash function defined in (1) is a
  $\frac{l}{2^n}$-universal, $\frac{l+1}{2^n}$-uniform, $\frac{2l+1}{2^n}$-universal$_{\mathrm{C}}$, $\frac{2l+1}{2^n}$-uniform$_{\mathrm{C}}$,
  $\frac{2l+1}{2^n}$-universal$_{\mathrm{CC}}$, $\frac{2l+1}{2^n}$-uniform$_{\mathrm{CC}}$ hash function

Corollary 1 (HtECB)

- Let H be the keyed hash function defined in (1)
- E be a blockcipher
- Then for any A that invokes the oracle at most q times, there exist adversaries A' and A'' such that

$$\mathrm{Adv}^{\mathrm{rpa}}_{\mathrm{HtECB[H,E]}}(A) \le \mathrm{Adv}^{\mathrm{prp}}_{E}(A') + \frac{8q^2(l+1)^2}{2^n}$$

$$\mathrm{Adv}^{\mathrm{int}}_{\mathrm{HtECB[H,E]}}(A) \le \mathrm{Adv}^{\mathrm{sprp}}_{E}(A'') + \frac{3q^2(l+1)^2}{2^n}$$

where A' makes at most $q(l+1)$ queries and A'' makes at most $(q+1)(l+1)$ queries

Corollary 2 (HtCBC)

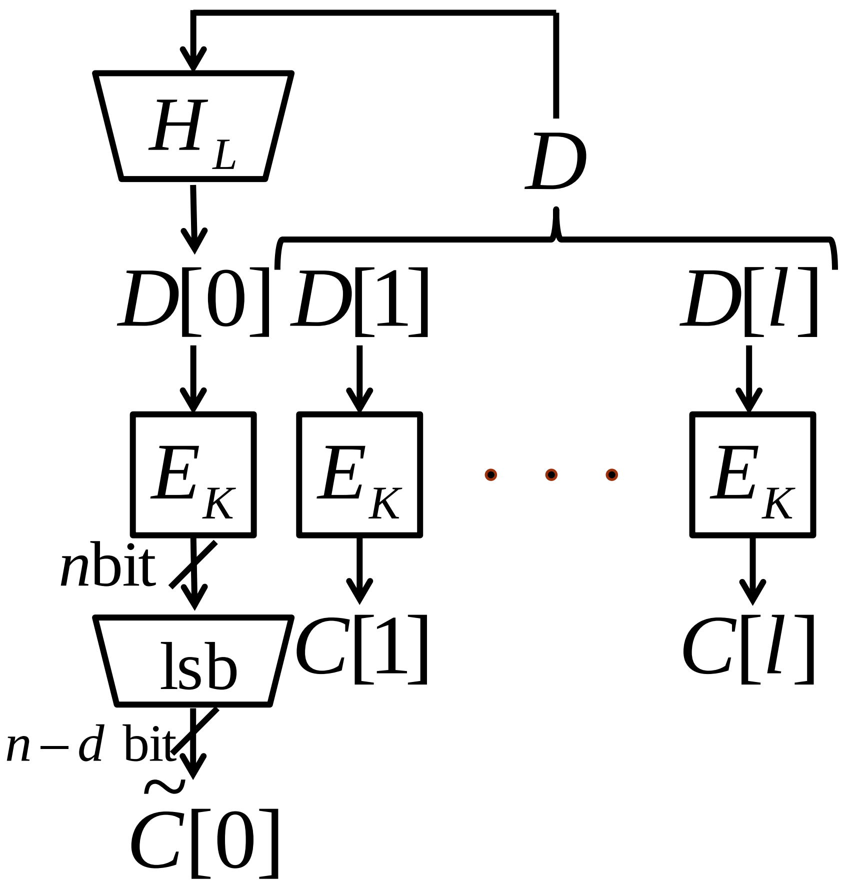
- Let H be the keyed hash function defined in (1)
- E be a blockcipher
- Then for any A that invokes the oracle at most q times, there exist adversaries A' and A'' such that

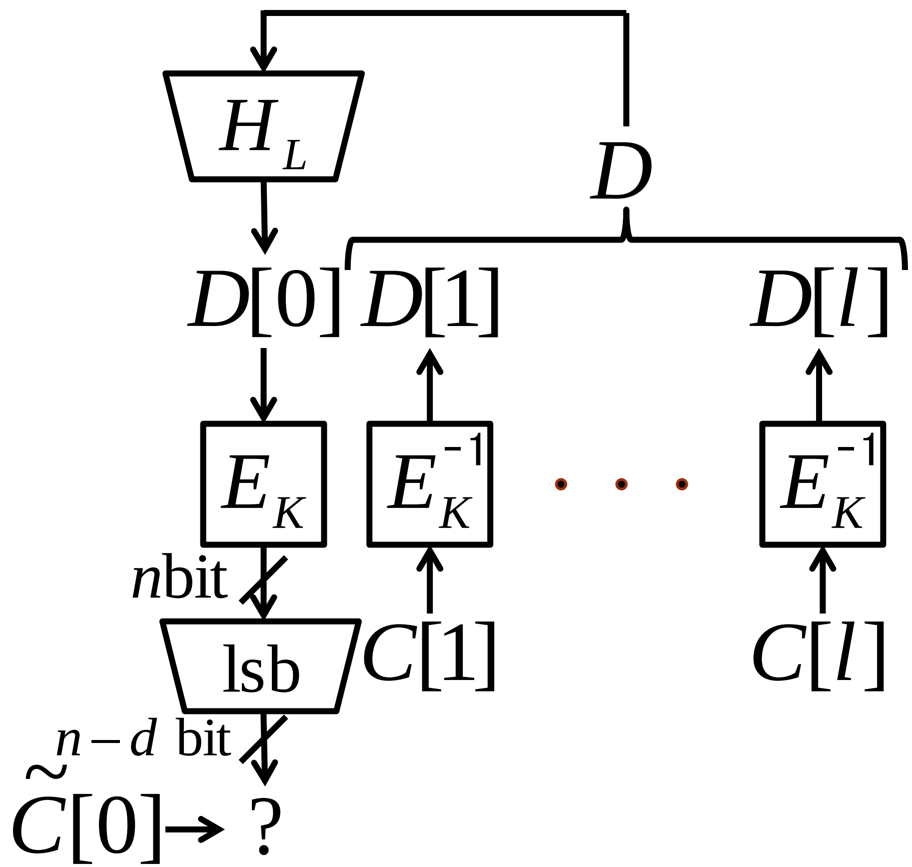
$$\mathrm{Adv}^{\mathrm{rpa}}_{\mathrm{HtCBC[H,E]}}(A) \le \mathrm{Adv}^{\mathrm{prp}}_{E}(A') + \frac{16q^2(l+1)^2}{2^n}$$

$$\mathrm{Adv}^{\mathrm{int}}_{\mathrm{HtCBC[H,E]}}(A) \le \mathrm{Adv}^{\mathrm{sprp}}_{E}(A'') + \frac{3q^2(l+1)^2}{2^n}$$

where A' makes at most $q(l+1)$ queries and A'' makes at most $(q+1)(l+1)$ queries

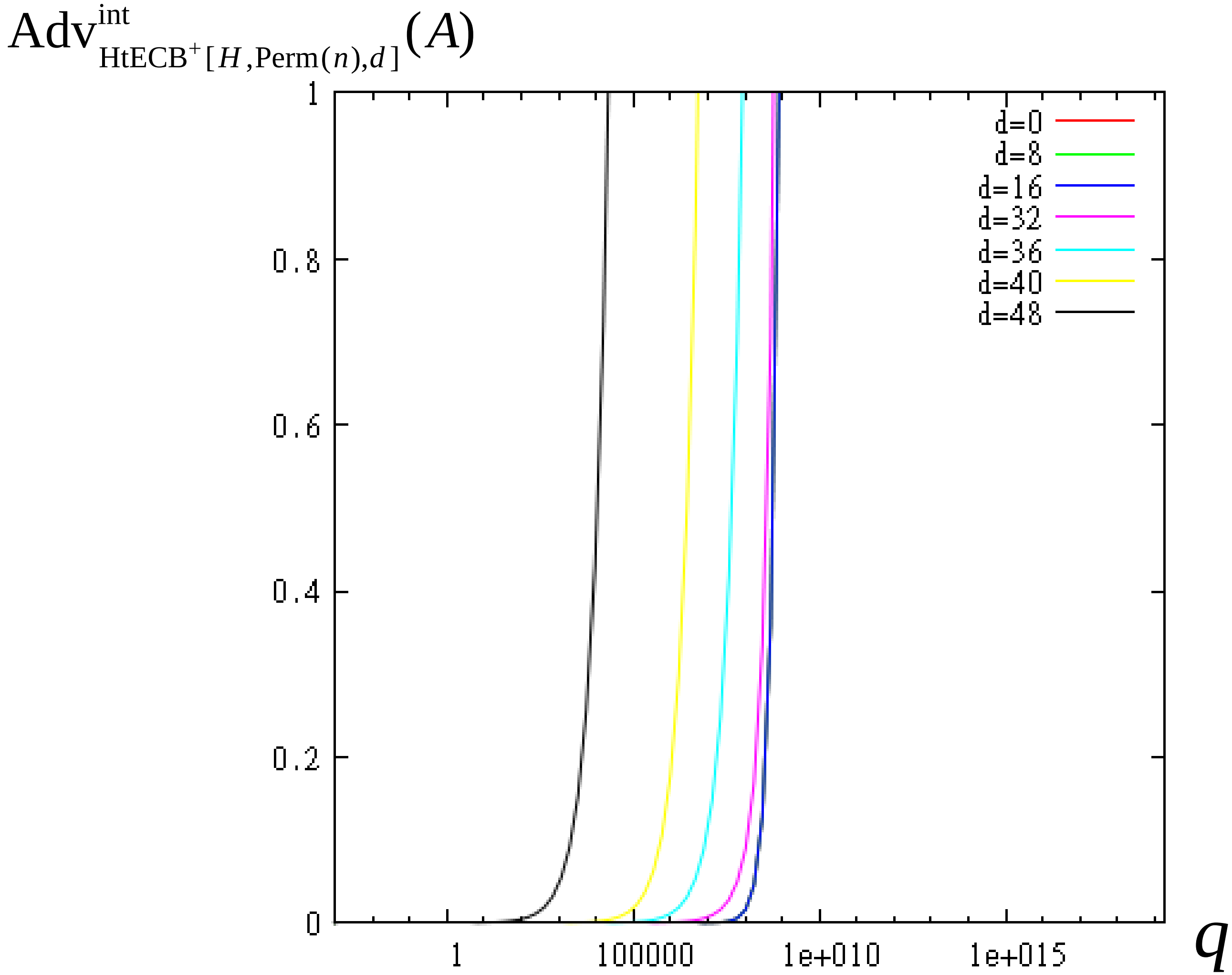
Hash-then-ECB$^+$ (HtECB$^+$)





Corollary

$$\mathrm{Adv}^{\mathrm{int}}_{\mathrm{HtECB}^{+}[H,\mathrm{Perm}(n),d]}(A) \le \frac{3q^2(l+1)^2}{2^n} + \frac{q(l+1)}{2^{n-d}} + \frac{2l+1}{2^{n-d}}$$



$n = 64$

$l = 2$