Related-Key Almost Universal Hash Functions: Definitions, Constructions and Applications

Peng Wang, Yuling Li, Liting Zhang and Kaiyan Zheng

State Key Laboratory of Information Security,
Institute of Information Engineering, Chinese Academy of Sciences
Data Assurance and Communication Security Research Center,
Chinese Academy of Sciences
University of Chinese Academy of Sciences
Institution of Software, Chinese Academy of Sciences

FSE 2016
March 23, 2016

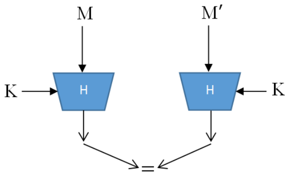
Outline

Outline

Universal hash functions

Almost Universal (AU)

$H : \mathcal{K} \times \mathcal{D} \rightarrow \mathcal{R}$



Definition (AU)

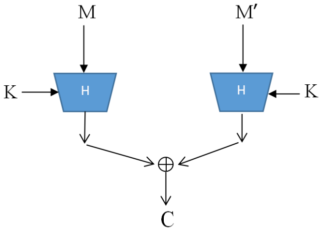
H is an ϵ-almost-universal (ϵ-AU) hash function, if for any $M, M' \in \mathcal{D}$, $M \neq M'$,

$$Pr[K \xleftarrow{\$} \mathcal{K} : H_K(M) = H_K(M')] \leq \epsilon$$

When ϵ is negligible, we say that H is AU.

Universal hash functions

Almost XOR Universal (AXU)



Definition (AXU)

Let $(\mathcal{R}, \oplus)$ *be an abelian group.* H *is an* ϵ*-almost-XOR- universal (*ϵ*-AXU), if for any* $M, M' \in \mathcal{D}$, $M \neq M'$ *and* $C \in \mathcal{R}$,

$$Pr[K \xleftarrow{\$} \mathcal{K} : H_K(M) \oplus H_K(M') = C] \leq \epsilon$$

When ϵ *is negligible, we say that* H *is AXU.*

Example

- $H_K(M) = MK$ $\quad$ $1/2^n$-AXU

$$H_K(M) \oplus H_K(M') = C$$

$$MK \oplus M'K = C$$

$$(M \oplus M')K = C$$

$$K = C(M \oplus M')^{-1}$$

$$\Pr[K \xleftarrow{\$} \mathcal{K} : H_K(M) \oplus H_K(M') = C] = 1/2^n$$

Example

- $H_K(M) = MK$
- $Poly : \{0,1\}^n \times \{0,1\}^{nm} \to \{0,1\}^n$,

$$Poly_K(M) = M_1K^m \oplus M_2K^{m-1} \oplus \cdots \oplus M_mK$$

$$M = M_1 \| M_2 \| \cdots \| M_m \in \{0,1\}^{nm}, M_i \in \{0,1\}^n, i = 1, \cdots, m.$$

$Poly$ is $m/2^n$-AXU.

Universal hash functions

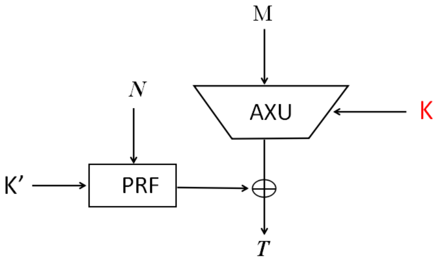
UHF-based schemes

- Message authentication code (MAC)
- Tweakable block cipher (TBC)
- Authenticated encryption (AE) scheme

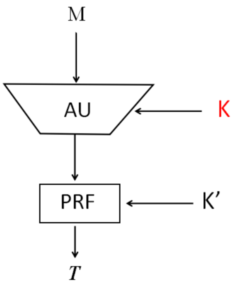
Universal hash functions

UHF-based schemes

- MAC



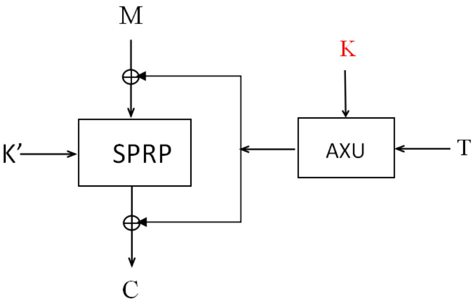
[Wegman and Carter, 1981]



[Brassard, 1982]

UHF-based schemes

- TBC



[Liskov et al., 2002]

Outline

Related-key attacks

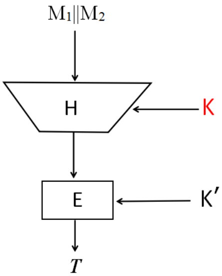
- firstly applied to block ciphers [Biham, 1993]
- Bellare and Kohno gave a formal definition of RKA-PRP and RKA-PRF [Bellare and Kohno, 2003]
- widely applied to MACs, TESes and AE schemes
  - Peyrin, et al: *Generic related-key attacks for HMAC*. ASIACRYPT 2012.
  - Dobraunig, et al: *Related-key forgeries for Prøst-OTR*. FSE 2015.
  - Sun, et al: *Weak-key and related-key analysis of hash-counter- hash tweakable enciphering schemes*. ACISP 2015.

Outline

RKA against UHF-based schemes

MAC

$Eg\ 1.\ H_K(M_1\|M_2) = M_1K^2 \oplus M_2K$ $\quad$ $2/2^n$-AXU



Query:

$$M\|M \xrightarrow{(K',\ K\oplus 1)} T$$

$$\begin{aligned} T &= E_{K'}(H_{K\oplus 1}(M\|M)) \\ &= E_{K'}(M(K\oplus 1)^2 \oplus M(K\oplus 1)) \\ &= E_{K'}(MK^2 \oplus MK) \end{aligned}$$

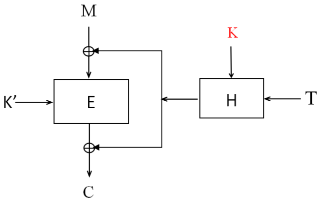
Forge:

$$M\|M \xrightarrow{(K',\ K)} T$$

RKA against UHF-based schemes

TBC

$Eg\ 2.\ \ H_K(T) = TK$ $\qquad$ $1/2^n$-AXU



Query:

$$(T, M) \xrightarrow{(K',\ K \oplus 1)} C$$

$$C = E_{K'}(M \oplus T(K \oplus 1)) \oplus T(K \oplus 1)$$

$$C \oplus T = E_{K'}((M \oplus T) \oplus TK) \oplus TK$$

Predict:

$$(T, M \oplus T) \xrightarrow{(K',\ K)} C \oplus T$$

Problems in the two-key schemes

$Eg\ 1.\quad H_{K\oplus 1}(M\|M) = H_K(M\|M)$

$Eg\ 2.\quad H_{K\oplus 1}(T) \oplus H_K(T) = T$

Collisions

The attacks have nothing to do with the block cipher.

RKA against UHF-based schemes

Almost all the existing two-key schemes which

based on universal hash function are

not related-key secure.

Outline

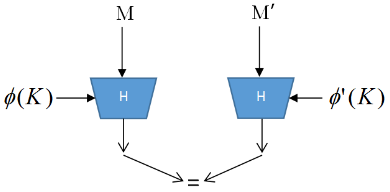
RKA-AU

Definition (RKA-AU)

H is an ϵ-related-key-almost-universal (ϵ-RKA-AU) hash function for the RKD set Φ, if $\forall \phi, \phi' \in \Phi$, $M, M' \in \mathcal{D}$, $(\phi, M) \neq (\phi', M')$,

$$Pr[K \xleftarrow{\$} \mathcal{K} : H_{\phi(K)}(M) = H_{\phi'(K)}(M')] \leq \epsilon.$$

When ϵ is negligible we say that H is RKA-AU.



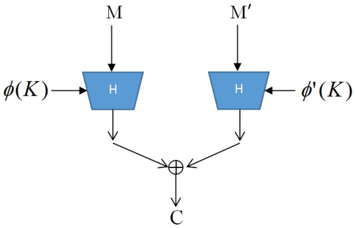
RKA-AXU

Definition (RKA-AXU)

Let $(\mathcal{R}, \oplus)$ be an abelian group. H is an ϵ-related-key-almost-XOR-universal (ϵ-RKA-AXU) hash function for the RKD set Φ, if $\forall \phi, \phi' \in \Phi$, $M, M' \in \mathcal{D}$, $(\phi, M) \neq (\phi', M')$ and $C \in \mathcal{R}$,

$$Pr[K \stackrel{\$}{\leftarrow} \mathcal{K} : H_{\phi(K)}(M) \oplus H_{\phi'(K)}(M') = C] \leq \epsilon.$$

When ϵ is negligible we say that H is RKA-AXU.



Restrictions on the RKD sets

Default RKD set

$$\Phi^{\oplus} = \{XOR_{\Delta} : K \mapsto K \oplus \Delta, \Delta \in \mathcal{K}\}$$

Not ideal functions

$Poly : \{0,1\}^n \times \{0,1\}^{nm} \to \{0,1\}^n,$

$$Poly_K(M) = M_1K^m \oplus M_2K^{m-1} \oplus \cdots M_mK$$

$M = M_1 \| M_2 \| \cdots \| M_m \in \{0,1\}^{nm}, M_i \in \{0,1\}^n, i = 1, 2, \cdots, m$

Let $M = M' = 0^{mn}$, $\phi \neq \phi'$.

$$Poly_{\phi(K)}(0^{mn}) = Poly_{\phi'(K)}(0^{mn}) = 0$$

$Poly$ is not RKA-AU.

Not ideal functions

Almost all the existing UHFs are not RKA-AU.

- MMH : $H_K(M) = (((\sum_{i=1}^{t} M_i K_i) \bmod 2^{64}) \bmod p) \bmod 2^{32}$, $M_i, K_i \in \mathbf{Z}_{2^{32}}$ and $p = 2^{32} + 15$;
- Square Hash : $H_K(M) = \sum_{i=1}^{t} (M_i + K_i)^2 \bmod p$, $M_i, K_i \in \mathbf{Z}_p$;
- NMH : $H_K(M) = (\sum_{i=1}^{t/2} (M_{2i-1} + K_{2i-1})(M_{2i} + K_{2i})) \bmod p$, $M_i, K_i \in \mathbf{Z}_{2^{32}}$, $p = 2^{32} + 15$;
- NH , WH ...

Outline

Constructions

- FIL-RKA-AXU: RH1
- VIL-RKA-AXU: RH2

FIL-RKA-AXU

$\mathrm{RH1} : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n,$

$$\mathrm{RH1}_K(M) = MK + K^3.$$

Proof. Let $F(K) = \mathrm{RH1}_{K\oplus\Delta_1}(M) \oplus \mathsf{RH1}_{K\oplus\Delta_2}(M')$.

$F(K) = (\Delta_1 \oplus \Delta_2)K^2 \oplus (\Delta_1^2\Delta_2^2 \oplus M \oplus M')K \oplus (\Delta_1^3 \oplus \Delta_2^3 \oplus M\Delta_1 \oplus M'\Delta_2).$

CASE 1. $\Delta_1 \neq \Delta_2$. $F(K) = C$ has 2 roots at most.
CASE 2. $\Delta_1 = \Delta_2$. Then $M \neq M'$. $F(K) = C$ has 1 root.

$$\Pr[K \xleftarrow{\$} \{0,1\}^n : F(K) = C] \leq 2/2^n.$$

RH1 is $2/2^n$-RKA-AXU over the RKD set $\Phi^{\oplus}$.

FIL-RKA-AXU

Remark from one of reviewers

$$\mathrm{RH1}_K(M) = MK + K^3.$$

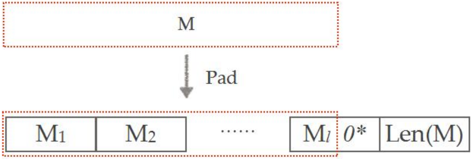
$\Phi_0 = \{id, f_\alpha\}$. $f_\alpha(K) = \alpha K,\ \alpha \in GF(2^n),\ \alpha^3 = 1.$

$$RH1_{f_\alpha(K)}(\alpha^{-1}M) = RH1_K(M)$$

RH1 is not RKA-AU over the RKD set Φ_0 .

VIL-RKA-AXU

$$Poly_K(M) = M_1K^m \oplus M_2K^{m-1} \oplus \cdots M_mK$$



$$pad(M) = M\|0^i\||M|$$

$Poly_K(pad(M))$ is VIL-AXU but not RKA-AXU.

VIL-RKA-AXU

$$Poly_K(M) = M_1K^m \oplus M_2K^{m-1} \oplus \cdots M_mK$$

$$\mathrm{RH2} : \{0,1\}^n \times \{0,1\}^* \to \{0,1\}^n,$$

$$\mathrm{RH2}_K(M) = \begin{cases} K^{l+2} \oplus Poly_K(pad(M)), & l\ is\ \ odd \\ K^{l+3} \oplus Poly_K(pad(M))K, & l\ is\ \ even \end{cases}$$

$$l = \lceil |M|/n \rceil + 1.$$

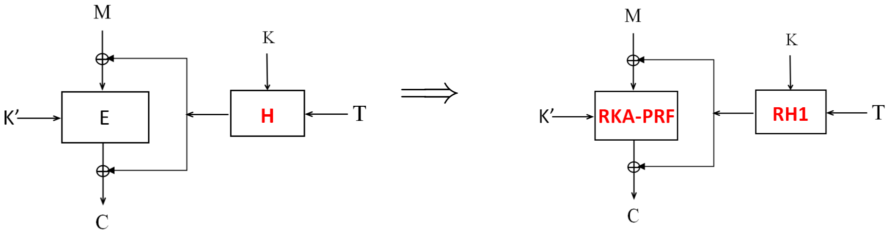
RH2 is $\mathrm{RKA\text{-}AXU}$ over the RKD set $\Phi^{\oplus}$.

RH2 VS Poly

$\mathrm{RH2}_K(M)$:	$Poly_K(pad(M))$
$T \leftarrow K^2$	$T \leftarrow 0$
for $i = 1$ **to** l	**for** $i = 1$ **to** l
$T \leftarrow (T \oplus M_i)K$	$T \leftarrow (T \oplus M_i)K$
if l is even	
$T \leftarrow TK$	
return T	**return** T

Solution

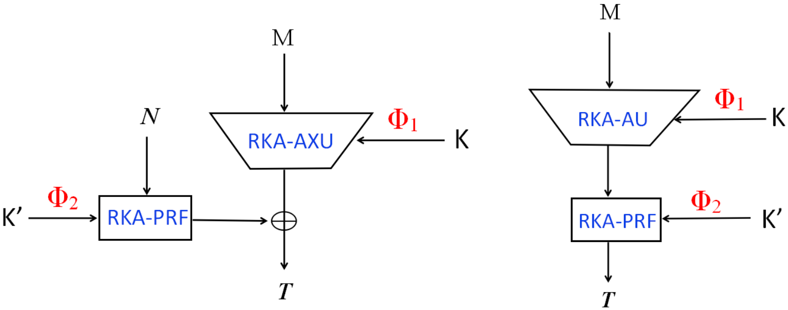
Whether it is secure ?



Outline

Applications

- related-key secure MACs



$\mathsf{MAC1}_{K,K'}(N, M) = H_K(M) \oplus F_{K'}(N)$

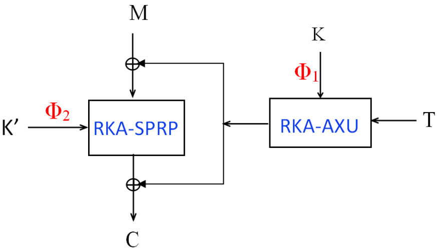
over $\Phi_1 \times \Phi_2$

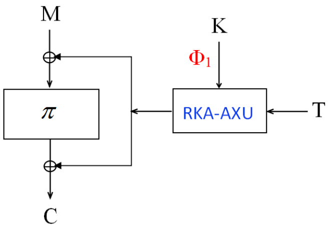
$\mathsf{MAC2}_{K,K'}(M) = F_{K'}(H_K(M))$

over $\Phi_1 \times \Phi_2$

Applications

- related-key secure MACs
- related-key secure TBCs





$\mathsf{TBC1}_{K,K'}(T,M) = E_{K'}(M \oplus H_K(T)) \oplus H_K(T)$

over $\Phi_1 \times \Phi_2$

$\mathsf{TBC2}_{K}(T,M) = \pi(M \oplus H_K(T)) \oplus H_K(T)$

over Φ_1

Conclusion

1. Propose a new concept of related-key almost universal hash function: RKA-AXU and RKA-AU.
2. Provide several efficient constructions named RH1, RH2 and RH3.
3. Show related-key secure MACs and TBCs, composed of RKA-AXU (RKA-AU) hash functions and other primitives such as RKA-PRPs and RKA-PRFs.

Thanks!

Bellare, M. and Kohno, T. (2003).
A theoretical treatment of related-key attacks: RKA-PRPs, RKA-PRFs, and applications.
In Biham, E., editor, *EUROCRYPT*, volume 2656 of *Lecture Notes in Computer Science*, pages 491–506. Springer.

Biham, E. (1993).
New types of cryptoanalytic attacks using related keys (extended abstract).
In Helleseth, T., editor, *EUROCRYPT*, volume 765 of *Lecture Notes in Computer Science*, pages 398–409. Springer.

Brassard, G. (1982).
On Computationally Secure Authentication Tags Requiring Short Secret Shared Keys.
In *International Crytology Conference*, pages 79–86.

Liskov, M., Rivest, R. L., and Wagner, D. (2002).
Tweakable block ciphers.
In Yung, M., editor, *CRYPTO 2012*, volume 2442 of *Lecture Notes in Computer Science*, pages 31–46. Springer.

Wegman, M. N. and Carter, L. (1981).
New hash functions and their use in authentication and set equality.

J. Comput. Syst. Sci., 22(3):265–279.