Radboud University

Security of Keyed Hashing Based on a Public Permutation

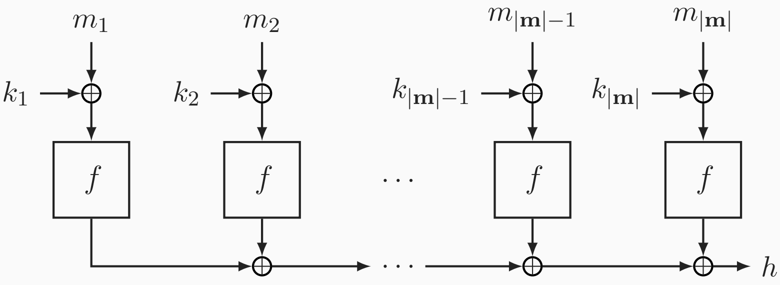
Jonathan Fuchs, Yann Rotella, Joan Daemen
Radboud University (The Netherlands)

Crypto 2023

August 24, 2023

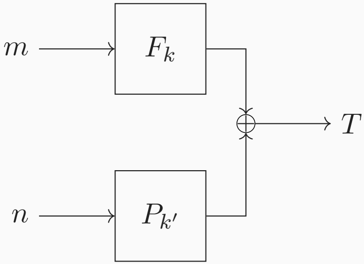
ESCADA

- Parallel keyed hashing with an underlying public permutation
- $\max_{a,\Delta \in G} \mathrm{DP}_f(a,\Delta)$-$\Delta$universal and $\max_{a \in G} \sum_{t \in G} \mathrm{DP}^2_f(a,t)$-universal

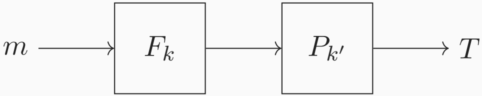


Motivation

- Keyed hash functions take arbitrary length inputs and output a fixed length digest
- We study their security when used in Wegman-Carter(-Shoup) and protected hash



Wegman-Carter(-Shoup)



Protected Hash

Security of WC(S) [WC81, Sho96]

- Security against forgery of the tuple (m, n, T)
- The attacker has to come up with a tuple (m^*, n^*, T^*):

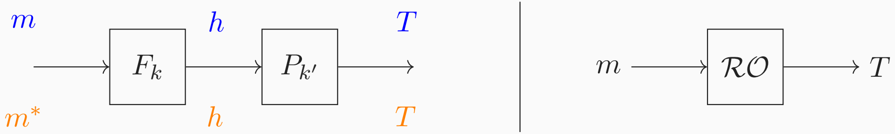
$$T = F_k(m) + P_{k'}(n)$$
$$T^* = F_k(m^*) + P_{k'}(n^*)$$
$$T - T^* = F_k(m) - F_k(m^*) + P_{k'}(n) - P_{k'}(n^*)$$
$$F_k(m) - F_k(m^*) = T - T^* - P_{k'}(n) + P_{k'}(n^*)$$

- ϵ-Δuniversality [Sti95] of F is defined over all distinct pairs of messages m, m^*:

$$Pr[F_k(m) - F_k(m^*) = \Delta] \leq \epsilon$$

Security of Protected Hash

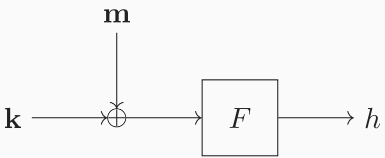
- The security is defined as a distinguishing advantage
- Assuming that $P_{k'}$ is PRP-secure and $m \neq m^*$:



- ϵ-universality [Sti95] of F is defined over all distinct pairs of messages m, m^*:

$$Pr[F_k(m) = F_k(m^*)] \leq \epsilon$$

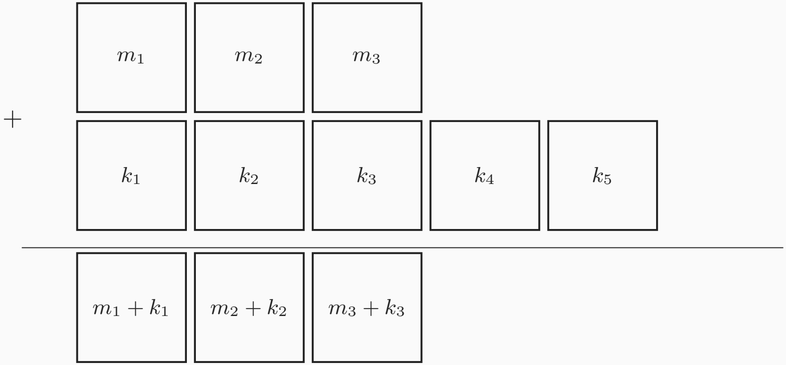
- A Key-Then-Hash function $F\colon G^{\kappa} \times BS(G,\kappa) \to G$ with:
  - Strings of length 1 to κ over the group $\langle G, + \rangle$: $BS(G,\kappa) = \bigcup_{i=1}^{\kappa} G^i$
  - Key Space: G^{κ}
  - Output Space: G
- Where $F_{\mathbf{k}}(\mathbf{m}) = F(\mathbf{k} + \mathbf{m})$:



Addition of Two Strings

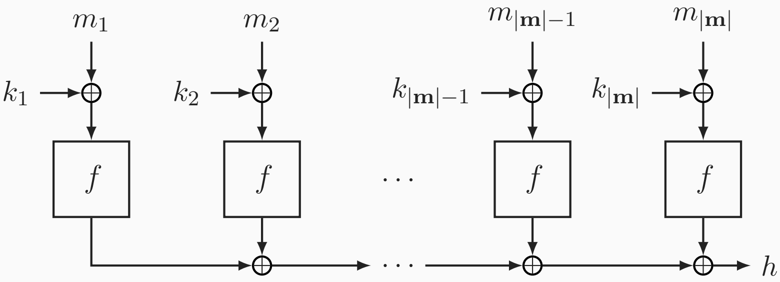
- We define the addition of any two strings $\mathbf{m}, \mathbf{m}^* \in BS(G, \kappa)$ with $|\mathbf{m}| \leq |\mathbf{m}^*|$ as:

$$\mathbf{m}' = m_1 + m_1^*, m_2 + m_2^*, m_3 + m_3^*, \ldots, m_{|\mathbf{m}|} + m_{|\mathbf{m}|}^*$$



The Parallelization of a Public Permutation

- $\mathrm{Parallel}[f]$ builds a Key-Then-Hash function using a public permutation f



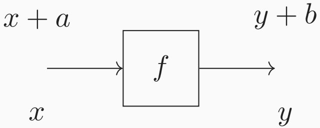
Given fixed-length permutation $f\colon G \to G$

- Input difference $a \in G$ propagates to the output difference $b \in G$ through f if

$$f(x+a) - f(x) = b$$

- The pair (a, b) is called a differential over f and happens with probability:

$$\mathsf{DP}_f(a,b) = \frac{\#\{x \in G \mid f(x+a) - f(x) = b\}}{\#G}$$



A Difference Between Two Strings

- We define the difference of any two strings $\mathbf{m}, \mathbf{m}^*$ with $|\mathbf{m}| \leq |\mathbf{m}^*|$ as:

$$\mathbf{a} = m_1 - m_1^*, m_2 - m_2^*, m_3 - m_3^*, \ldots, m_{|\mathbf{m}|} - m_{|\mathbf{m}|}^*$$
$$\lambda = |\mathbf{m}^*| - |\mathbf{m}|$$

$$\begin{array}{rccccc} & \boxed{m_1} & \boxed{m_2} & \boxed{m_3} & & \\ - & \boxed{m_1^*} & \boxed{m_2^*} & \boxed{m_3^*} & \multicolumn{2}{c}{\overbrace{\boxed{m_4^*} \; \boxed{m_5^*}}^{\lambda=2}} \\ \hline \mathbf{a} = & \boxed{m_1 - m_1^*} & \boxed{m_2 - m_2^*} & \boxed{m_3 - m_3^*} & & \end{array}$$

Universality of $\mathrm{Parallel}[f]$

- We are interested in proving bounds on the universality and Δ-universality of $\mathrm{Parallel}[f]$
  - Input difference $(\mathbf{a}, \lambda)$ leading to a Δ output difference through $\mathrm{Parallel}[f]$:

$$\sum_{i=1}^{|\mathbf{m}|} f(m_i + k_i) - \sum_{j=1}^{|\mathbf{m}^*|} f(m_j^* + k_j) = \Delta$$

  - Assuming $|\mathbf{m}| \leq |\mathbf{m}^*|$

$$\sum_{i=1}^{|\mathbf{m}|} f(m_i + k_i) - f(m_i^* + k_i) - \sum_{j=|\mathbf{m}|+1}^{|\mathbf{m}^*|} f(m_j^* + k_j) = \Delta$$

Universality of $\mathrm{Parallel}[f]$

$$\sum_{i=1}^{|\mathbf{m}|} f(m_i + k_i) - f(m_i^* + k_i) - \sum_{j=|\mathbf{m}|+1}^{|\mathbf{m}^*|} f(m_j^* + k_j) = \Delta$$

- $\Pr[f(m_i + k_i) - f(m_i^* + k_i) = b_i]$ with $a_i = m_i - m_i^*$ is given by $\mathrm{DP}_f(a_i, b_i)$
- $\Pr[f(m_j^* + k_j) = x_j]$ is uniform and is equal to $\frac{1}{\#G}$

Stochastic Variables

$$\sum_{i=1}^{|\mathbf{m}|} \underbrace{f(m_i + k_i) - f(m_i^* + k_i)}_{b_i} - \sum_{j=|\mathbf{m}|+1}^{|\mathbf{m}^*|} \underbrace{f(m_j^* + k_j)}_{x_j} = \Delta$$

Assuming $a_i = m_i - m_i^*$:

- b_i can be seen as a stochastic variable with probability mass function

$$\mathrm{DP}_{a_i}(b_i) = \mathsf{DP}_f(a_i, b_i)$$

- x_j can be seen as a stochastic variable with probability mass function

$$\mathrm{U}(x_j) = \frac{1}{\#G}$$

Addition of Two Independent Stochastic Variables

- The PMF of a stochastic variable $z = x + y$ is given by

$$g_z(v) = g_x * g_y(v) = \sum_t g_x(t) g_y(v - t)$$

- The resulting convolution is bound by the PMFs of the original two variables

$$\max_v g_z(v) \leq \min \left\{ \max_v g_x(v), \max_v g_y(v) \right\}$$

PMF of output differences of $\mathrm{Parallel}[f]$

$$\sum_{i=1}^{|\mathbf{m}|} \underbrace{f(m_i + k_i) - f(m_i^* + k_i)}_{b_i} - \sum_{j=|\mathbf{m}|+1}^{|\mathbf{m}^*|} \underbrace{f(m_j^* + k_j)}_{x_j} = \Delta$$

- The output difference of $\mathrm{Parallel}[f]$ is a stochastic variable
- It is the variable resulting from the sum of all b_i and x_j

$$\mathrm{DP}_{a_1} * \mathrm{DP}_{a_2} * \ldots * \mathrm{DP}_{a_{|m|}} * \mathrm{U}^{(|\mathbf{m}^*|-|\mathbf{m}|)}(\Delta)$$

Generalized Differentials over $\mathrm{Parallel}[f]$

- We now define a notion of differentials over $\mathrm{Parallel}[f]$ and their probability

$$\mathsf{DP}_{\mathrm{Par}}(\mathbf{a}, \lambda, \Delta) = \mathrm{DP}_{a_1} * \ldots * \mathrm{DP}_{a_{|\mathbf{a}|}} * \mathrm{U}^{(\lambda)}(\Delta)$$

- We directly get a bound on the Δuniversality

$$\max_{(\mathbf{a},\lambda,\Delta)} \mathsf{DP}_{\mathrm{Par}}(\mathbf{a}, \lambda, \Delta) \leq \max\left\{\max_{(a,\Delta)} \mathsf{DP}_f(a, \Delta), \frac{1}{\#G}\right\} = \max_{(a,\Delta)} \mathsf{DP}_f(a, \Delta)$$

- We now prove an upper bound on the universality of $\mathrm{Parallel}[f]$
  - An output difference 0 is not possible with single-block strings
  - From our definition of differentials over $\mathrm{Parallel}[f]$ we know

$$\max_{(\mathbf{a},0,\Delta)} \mathsf{DP}_{\mathrm{Par}}(\mathbf{a},0,\Delta) \geq \max_{(\mathbf{a},0,0)} \mathsf{DP}_{\mathrm{Par}}(\mathbf{a},0,0)$$

- We also know that $\max_{(\mathbf{a},0,\Delta)} \mathsf{DP}_{\mathrm{Par}}(\mathbf{a},0,\Delta)$ is maximized with $\mathbf{a} \in G^2$
  - Hence we must find

$$\max_{(\mathbf{a}\in G^2,\Delta)} \sum_t \mathsf{DP}_f(a_1,t)\mathsf{DP}_f(a_2,\Delta - t)$$

Bound on Inner Products

$$\max_{\mathbf{a}\in G^2,\Delta} \sum_t \mathsf{DP}_f(a_1, t)\mathsf{DP}_f(a_2, \Delta - t)$$

- This can be seen as the inner product of two vectors indexed by t
- The inner product of two vectors is upper bound by the product of their norm (Cauchy-Schwarz)

$$|\langle \mathbf{a}, \mathbf{b} \rangle| \leq \|\mathbf{a}\|\|\mathbf{b}\|$$

Bound on Inner Products

$$|\langle \mathbf{a}, \mathbf{b} \rangle| \le \|\mathbf{a}\| \|\mathbf{b}\| \le \max\left\{ \|\mathbf{a}\|^2, \|\mathbf{b}\|^2 \right\}$$

- Hence we get the following bound

$$\begin{aligned}
\sum_t \mathsf{DP}_f(a_1, t)\mathsf{DP}_f(a_2, \Delta - t) &\le \max\left\{ \sum_t \mathsf{DP}_f^2(a_1, t), \sum_t \mathsf{DP}_f^2(a_2, \Delta - t) \right\} \\
&= \max\left\{ \sum_t \mathsf{DP}_f^2(a_1, t), \sum_t \mathsf{DP}_f^2(a_2, t) \right\}
\end{aligned}$$

$$\sum_t \mathsf{DP}_f(a_1, t)\mathsf{DP}_f(a_2, \Delta - t) \leq \max \left\{ \sum_t \mathsf{DP}_f^2(a_1, t), \sum_t \mathsf{DP}_f^2(a_2, t) \right\}$$

- We have proven the following upper bound on the universality

$$\max_{\mathbf{a} \in G^2} \mathsf{DP}_{\mathrm{Par}}(\mathbf{a}, 0, 0) \leq \max_a \sum_t \mathsf{DP}^2(a, t)$$

- This bound is tight when we take $a_2 = -a_1$

Conclusion

Parallelization of a Public Permutation

- We have shown a parallel key-then-hash function built on a public permutation
- It is $\max_{a,\Delta} \mathsf{DP}(a,\Delta)$-$\Delta$universal and $\max_a \sum_t \mathsf{DP}_f(a,t)^2$-universal
- Its security depends solely on the differential properties of its underlying public permutation

Conclusion

Parallelization of a Public Permutation

- We have shown a parallel key-then-hash function built on a public permutation
- It is $\max_{a,\Delta} \mathsf{DP}(a,\Delta)$-$\Delta$universal and $\max_a \sum_t \mathsf{DP}_f(a,t)^2$-universal
- Its security depends solely on the differential properties of its underlying public permutation

More In The Paper

- We define the probability of differential over key-then-hash functions
- We show an analysis to a serial key-then-hash
- We apply these results $\textsc{Xoodoo}[3]$ and $\textsc{Xoodoo}[4]$

Parallelization of a Public Permutation

- We have shown a parallel key-then-hash function built on a public permutation
- It is $\max_{a,\Delta} \mathsf{DP}(a,\Delta)$-$\Delta$universal and $\max_a \sum_t \mathsf{DP}_f(a,t)^2$-universal
- Its security depends solely on the differential properties of its underlying public permutation

More In The Paper

- We define the probability of differential over key-then-hash functions
- We show an analysis to a serial key-then-hash
- We apply these results $\textsc{Xoodoo}[3]$ and $\textsc{Xoodoo}[4]$

Thank you for your attention!

Victor Shoup.
On Fast and Provably Secure Message Authentication Based on Universal Hashing.
In Neal Koblitz, editor, *Advances in Cryptology - CRYPTO '96, 16th Annual International Cryptology Conference, Santa Barbara, California, USA, August 18-22, 1996, Proceedings*, volume 1109 of *Lecture Notes in Computer Science*, pages 313–328. Springer, 1996.

Douglas R. Stinson.
On the Connections Between Universal Hashing, Combinatorial Designs and Error-Correcting Codes.
Electron. Colloquium Comput. Complex., 2(52), 1995.

Mark N. Wegman and Larry Carter.
New Hash Functions and Their Use in Authentication and Set Equality.
J. Comput. Syst. Sci., 22(3):265–279, 1981.