One-Way Hash Function Based on Weakened Assumption

Yuliang Zheng Tsutomu Matsumoto Hideki Imai
Faculty of Engineering, Yokohama National University

1 Introduction

One-way hash function has many applications in such as authentication and digital signature. Here we consider a special kind of one-way hash function — *universal one-way hash function* (UOH). Intuitively, a length-decreasing function is a UOH if, *given an initial-string* x, it is computationally difficult to find a different string y that collides with x. It has been proved that the existence of UOH implies the existence of provably secure digital signature. A challenging subject is to construct UOH assuming the existence of *one-way function*. Previously, Naor and Yung constructed UOH assuming the existence of *one-way injection (i.e., one-way one-to-one function)*. In this abstract we report some progress in the subject. First we prove that (1) UOH with respect to initial-strings chosen *arbitrarily* exists if and only if UOH with respect to initial-strings chosen *uniformly at random* exists. Then we show that (2) UOH can be constructed under a *weaker* assumption, the existence of one-way *quasi*-injection.

2 Definitions

Denote by N the set of all positive integers, and by $\Sigma = \{0, 1\}$ the alphabet we consider. For $n \in N$, denote by Σ^n the set of all strings over Σ with length n. Denote by Σ^+ the set of all finite length strings not including the empty string. Let ℓ be a monotone increasing function from N to N, and f a function from D to R, where $D = \bigcup_n \Sigma^n$, and $R = \bigcup_n \Sigma^{\ell(n)}$. Denote by f_n the restriction of f on Σ^n. We are concerned only with the case when the range of f_n is $\Sigma^{\ell(n)}$, i.e., f_n is a function from Σ^n to $\Sigma^{\ell(n)}$. A string $x \in \Sigma^n$ is said to *have a brother* (with respect to f) if there is a different string $y \in \Sigma^n$ such that $f_n(x) = f_n(y)$. The composition of two functions f and g is defined as $f \circ g(x) = f(g(x))$.

A (probability) *ensemble* E with length $\ell(n)$ is a function $E : \Sigma^+ \to [0, 1]$ assigning to each $n \in N$ a *probability distribution* $E_n : \Sigma^{\ell(n)} \to [0, 1]$. The *uniform ensemble* U with length $\ell(n)$ assigns to each $n \in N$ the *uniform probability distribution* $U_n : \Sigma^{\ell(n)} \to [0, 1]$ that is defined as $U_n(x) = 1/2^{\ell(n)}$

for each $x \in \Sigma^{\ell(n)}$. By $x \in_E \Sigma^{\ell(n)}$ we mean that x is randomly chosen from $\Sigma^{\ell(n)}$ according to E_n, and in particular, by $x \in_R S$ we mean that x is chosen from the set S uniformly at random.

Definition 1 Let f be a polynomial time computable function from D to R. (1) f is a *one-way* function if for each probabilistic polynomial time algorithm M, for each polynomial Q and for all sufficiently large n, $\Pr\{f_n(x) = f_n(M(n, f_n(x)))\} < 1/Q(n)$, when $x \in_R D_n$. (2) f is a one-way *quasi*-injection if it is one-way and, furthermore, for each polynomial Q, for all sufficiently large $n \in N$, $\Pr\{x \text{ has a brother}\} < 1/Q(n)$ when $x \in_R \Sigma^n$.

Let ℓ be a polynomial with $\ell(n) > n$, H be a family of polynomial time computable functions defined by $H = \bigcup_n H_n$ where H_n is a (possibly multi-)set of functions from $\Sigma^{\ell(n)}$ to Σ^n. Call H a *hash function* compressing $\ell(n)$-bit input into n-bit output strings. Let E be an ensemble with length $\ell(n)$, F a probabilistic polynomial time algorithm that on input $n \in N, h \in H_n$ and $x \in_E \Sigma^{\ell(n)}$ outputs either "?" (I don't know) or a string $y \in \Sigma^{\ell(n)}$ such that $y \neq x$ and $h(x) = h(y)$. Call F a collision-string finder.

Definition 2 Let H be a hash function compressing $\ell(n)$-bit input into n-bit output strings, P a collection of ensembles with length $\ell(n)$, and F a collision-string finder. Then H is a *universal one-way hash function with respect to* P, denoted by UOH/P, if for each $E \in P$, for each F, for each polynomial Q, and for all sufficiently large n, $\Pr\{F(n, h, x) \neq ?\} < 1/Q(n)$, when $h \in_R H_n$ and $x \in_E \Sigma^{\ell(n)}$.

We are interested in UOH/$\{U\}$ and UOH/$EN[\ell(n)]$, where U is the uniform ensemble with length $\ell(n)$ and $EN[\ell(n)]$ is the collection of all ensembles with length $\ell(n)$. For notational simplicity, UOH/$\{U\}$ is abbreviated as UOH/U.

3 Main Results

This section presents our main results claimed in Introduction.

First we show that, given a one-way hash function H in the sense of UOH/U, we can construct a one-way hash function H' in the sense of UOH/$EN[\ell(n)]$. Denote by T_n the set of all permutations t over $GF(2^{\ell(n)})$ defined as $t(x) = a \cdot x + b$, where $a, b \in GF(2^{\ell(n)})$ with $a \neq 0$. Let $T = \bigcup_n T_n$. Note that there is a natural one-to-one correspondence between $\Sigma^{\ell(n)}$ and $GF(2^{\ell(n)})$.

Theorem 1 Assume that $H = \bigcup_n H_n$ is a UOH/U. Let $H'_n = \{h' \mid h' = h \circ t, h \in H_n, t \in T_n\}$, and $H' = \bigcup_n H'_n$. Then H' is a UOH/$EN[\ell(n)]$.

As a corollary of Theorem 1, we have

Corollary 1 UOH/$EN[\ell(n)]$ exists iff UOH/U exists.

Next we consider how to construct UOH/$EN[\ell(n)]$ under a *weaker* assumption — the existence of one-way *quasi*-injection. Let m be a polynomial with $m(n) \geq n$. Assume that f is a one-way quasi-injection from D to R, where $D = \bigcup_n \Sigma^n$, and $R = \bigcup_n \Sigma^{m(n)}$. Let $T = \bigcup_n T_n$ be the above defined family of permutations with ℓ being replaced by m. Finally, let $S = \bigcup_n S_n$ be a strongly universal$_2$ hash function that compresses $m(n)$-bit input into $(n-1)$-bit output strings and has the collision accessibility property [ZMI]. Note that such hash functions are available without any assumption.

Lemma 1 Let $H_n = \{h \mid h = s \circ t \circ f_{n+1}, s \in S_{n+1}, t \in T_{n+1}\}$, and $H = \bigcup_n H_n$. Then H is a UOH/U compressing $(n+1)$-bit input into n-bit output strings.

Combining Theorem 1 and Lemma 1, we get the following result: *UOH/$EN[n+1]$ can be constructed assuming the existence of one-way quasi-injection.* By a result of Naor and Yung, UOH/$EN[\ell(n)]$ can be obtained from UOH/$EN[n+1]$ for any polynomial ℓ. Thus

Theorem 2 UOH/$EN[\ell(n)]$ can be constructed assuming the existence of one-way quasi-injection.

Detailed proofs, as well as many other interesting results, can be found in [ZMI].

Reference

[ZMI] Y. Zheng, T. Matsumoto and H. Imai: "Connections between several versions of one-way hash functions", *To be presented at SCIS90*, Jan. 31–Feb. 2, 1990.