Collision Resistance of the JH Hash Function

Jooyoung Lee and Deukjo Hong

***Abstract*—In this paper, we analyze collision resistance of the JH hash function in the ideal primitive model. The JH hash function is one of the five SHA-3 candidates accepted for the final round of evaluation. The JH hash function uses a mode of operation based on a permutation, while its security has been elusive even in the random permutation model.**

One can find a collision for the JH compression function only with two backward queries to the basing primitive. However, the security is significantly enhanced in iteration. For $c \leq n/2$, we prove that the JH hash function using an ideal n-bit permutation and producing c-bit outputs by truncation is collision resistant up to $O(2^{c/2})$ queries.

***Index Terms*—hash function, collision resistance.**

I. Introduction

As many hash functions, including those most common in practical applications, have started to exhibit serious security weaknesses [2]–[9], the US National Institute for Standards and Technology (NIST) has opened a public competition to develop a new cryptographic hash function. Currently, the final candidates to replace SHA-2 has been announced, which are BLAKE, Grøstl, JH, Keccak and Skein. In this paper, we analyze collision resistance for the JH hash function in the ideal primitive model. The *JH compression function* is illustrated in Fig. 1, where π is a certain permutation. The *JH hash function* is obtained by feeding the compression function to the Merkle-Damgård transform [10]. The only known result for the security of the JH hash function is its indifferentiability from a random oracle guaranteed up to $2^{n/6}$ query complexity [1]. This translates into the collision resistance of the JH hash function up to $2^{n/6}$ query complexity, which is far from optimal.

Even if π is a truly random function, one can find a collision for the JH compression function only with two backward queries to the basing primitive. In this paper, however, we show that the security is significantly enhanced in iteration. For $c \leq n/2$, we prove that the JH hash function using an ideal n-bit permutation and producing c-bit outputs by truncation is collision resistant up to $O(2^{c/2})$ queries. This bound implies that the JH hash function provides the optimal collision resistance in the random permutation model.

II. Preliminaries

General Notation: For two bitstrings x and y, $x||y$ denotes the concatenation of x and y. Given $x \in \{0,1\}^n$ for an even integer n, x_L and x_R denote $\frac{n}{2}$-bit strings such that $x = x_L||x_R$.

J. Lee is with the Attached Institute of Electronics and Telecommunications Research Institute, Daejeon, Korea (e-mail: jlee05@ensec.re.kr).

D. Hong is with the Attached Institute of Electronics and Telecommunications Research Institute, Daejeon, Korea (e-mail: hongdj@ensec.re.kr).

Merkle-Damgård Transform: Let

$$\mathsf{pad} : \{0,1\}^* \rightarrow \bigcup_{i=1}^{\infty} \{0,1\}^{mi}$$

be an injective padding. With this padding scheme and a predetermined constant $IV \in \{0,1\}^{2n}$, the *Merkle-Damgård transform* produces a variable-input-length function $MD[F] : \{0,1\}^* \rightarrow \{0,1\}^{2n}$ from a fixed-input-length function $F : \{0,1\}^{2n} \times \{0,1\}^m \rightarrow \{0,1\}^{2n}$. For $M \in \{0,1\}^*$ such that $|\mathsf{pad}(M)| = lm$, $MD[F](M)$ is computed as follows.

Function $MD[F](M)$
 $u[0] \leftarrow IV$
 Break $\mathsf{pad}(M) = M[1]||\ldots||M[l+1]$ into m-bit blocks
 for $i \leftarrow 1$ to $l+1$ **do**
  $u[i] \leftarrow F(u[i-1], M[i])$
 return $u[l+1]$

Collision Resistance: We review the definition of collision resistance *in the information-theoretic model*. Given a function $H = H[\mathcal{P}]$ and an information-theoretic adversary $\mathcal{A}$ both with oracle access to an ideal primitive $\mathcal{P}$, the collision resistance of H against $\mathcal{A}$ is estimated by the following experiment.

Experiment $\mathbf{Exp}_{\mathcal{A}}^{\mathsf{col}}$
 $\mathcal{A}$ updates $\mathcal{Q}$ by making oracle queries to $\mathcal{P}$
 if $\exists$ $M \neq M'$ and u s.t. $u = H_{\mathcal{Q}}(M) = H_{\mathcal{Q}}(M')$ **then**
  output 1
 else
  output 0

This experiment records every query-response pair that $\mathcal{A}$ obtains by oracle queries into a *query history* $\mathcal{Q}$. We write $u = H_{\mathcal{Q}}(M)$ if $\mathcal{Q}$ contains all the query-response pairs required to compute $u = H(M)$. At the end of the experiment, $\mathcal{A}$ would like to find two distinct evaluations yielding a collision. The *collision-finding advantage* of $\mathcal{A}$ is defined to be

$$\mathbf{Adv}_H^{\mathsf{col}}(\mathcal{A}) = \mathbf{Pr}\left[\mathbf{Exp}_{\mathcal{A}}^{\mathsf{col}} = 1\right].$$

The probability is taken over the random choice of $\mathcal{P}$ and $\mathcal{A}$'s coins (if any). For $q > 0$, we define $\mathbf{Adv}_H^{\mathsf{col}}(q)$ as the maximum of $\mathbf{Adv}_H^{\mathsf{col}}(\mathcal{A})$ over all adversaries $\mathcal{A}$ making at most q queries.

III. Description of the JH Hash Function

Let π be a permutation on $\{0,1\}^n$ for an even integer n. Then the *JH compression function* $F = F[\pi]$ is defined as follows.

$$F : \{0,1\}^n \times \{0,1\}^{n/2} \longrightarrow \{0,1\}^n$$
$$(u, z) \longmapsto v,$$

where
$$v = \pi\left(u \oplus (z||0)\right) \oplus (0||z).$$

The pictorial representation is given in Fig. 1.

For $c \leq n/2$, let $\mathsf{chop}_c : \{0,1\}^n \to \{0,1\}^c$ be the function that chops off the $(n-c)$ leftmost bits of its input string, i.e., $\mathsf{chop}_c(x) = x_2$ if $x = x_1||x_2$ for some $x_1 \in \{0,1\}^{n-c}$ and $x_2 \in \{0,1\}^c$. Then the *c-bit JH hash function* is defined by $\mathsf{JH}_c = \mathsf{chop}_c \circ MD[F]$. In the original submission, $n = 1024$ and $c \in \{224, 256, 384, 512\}$.

Since the padding is injective, we can simplify our collision analysis by assuming that the domain of the JH hash function is $\bigcup_{i=1}^{\infty}\{0,1\}^{ni/2}$ (and ignore the padding scheme). In the following section, we will prove collision resistance for the JH hash function assuming π is an ideal random permutation.

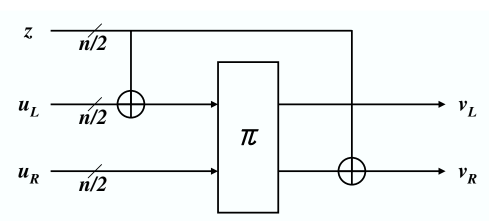

Fig. 1. JH compression function.

IV. Collision Resistance of the JH Hash Function

Suppose that an information-theoretic adversary $\mathcal{A}$ adaptively makes q forward or backward queries to an ideal random permutation π, and records a query history $\mathcal{Q} = \{(x^i, y^i) \in \{0,1\}^n : 1 \leq i \leq q\}$. Here $\pi(x^i) = y^i$ and $\mathcal{A}$'s i-th query is either $\pi(x^i)$ or $\pi^{-1}(y^i)$ for $1 \leq i \leq q$.

We define a direct graph $\mathcal{G}$ on $\{0,1\}^n$ where a direct edge from u to v labeled i is added to $\mathcal{G}$ when the i-th query-response pair (x^i, y^i) determines an evaluation $F[\pi](u,z) = v$ for some $z \in \{0,1\}^{n/2}$. We will denote such an edge by $u \xrightarrow{i} v$. We note that each query $\pi(x_L||x_R) = (y_L||y_R)$ generates $2^{n/2}$ edges from $((x_L \oplus z)||x_R)$ to $(y_L||(y_R \oplus z))$ where $z \in \{0,1\}^{n/2}$.

Definition 1: $u \in \{0,1\}^n$ is called an *orderly reachable node* if there exists a direct path
$$IV \xrightarrow{i_1} u[1] \xrightarrow{i_2} \cdots \xrightarrow{i_{t-1}} u[t-1] \xrightarrow{i_t} u,$$
such that $i_1 < i_2 < \ldots < i_{t-1} < i_t$. By convention, IV is an orderly reachable node.

For $i = 1, \ldots, q$, let U_i be the set of orderly reachable nodes determined by the first i queries, and let Rcol_i be the event that U_i contains a collision in the right-half bits. That is,
$$\mathsf{Rcol}_i : \text{there exist } u, v \in U_i \text{ such that } u \neq v \text{ and } u_R = v_R.$$

Now our security proof consists of two steps. The first step is to prove that the probability of Rcol_q is small up to the birthday bound. The next step is to show that the probability of collision is small without the occurrence of Rcol_q. We begin with the following proposition.

Proposition 1: Without the occurrence of Rcol_i, $|U_i| \leq i+1$ for $i = 0, \ldots, q$.

Proof: Note that $U_0 = \{IV\}$. If $|U_i| > i+1$ for some $i = 1, \ldots, q$, then a certain query, say the j-th query, would produce two distinct orderly reachable nodes, say w and w'. In this case, we have two paths
$$\mathsf{P}_1 : IV \xrightarrow{j_1} u[1] \xrightarrow{j_2} \cdots \xrightarrow{j_{s-1}} u[s-1] \xrightarrow{j_s} w$$
and
$$\mathsf{P}_2 : IV \xrightarrow{j'_1} v[1] \xrightarrow{j'_2} \cdots \xrightarrow{j'_{t-1}} v[t-1] \xrightarrow{j'_t} w'$$
where the labels are strictly increasing and
$$j_s = j'_t = j \leq i.$$
Since $w \neq w'$ and $j_s = j'_t = j \leq i$, $u[s-1]$ and $v[t-1]$ are distinct orderly reachable nodes in U_i such that $\mathsf{chop}_c(u[s-1]) = \mathsf{chop}_c(v[t-1])$. This contradicts the condition of $\neg\mathsf{Rcol}_i$. ■

Proposition 2: Suppose that an adversary $\mathcal{A}$ makes q queries to a random permutation π and its inverse π^{-1}. For $N = 2^{n/2}$ and $q < N$,
$$\mathbf{Pr}\left[\mathsf{Rcol}_q\right] \leq \frac{q(q+1)}{2(N-1)}.$$

Proof: Since
$$\mathbf{Pr}\left[\mathsf{Rcol}_q\right] \leq \sum_{i=1}^{q} \mathbf{Pr}\left[\mathsf{Rcol}_i \wedge \neg\mathsf{Rcol}_{i-1}\right]$$
$$\leq \sum_{i=1}^{q} \mathbf{Pr}\left[\mathsf{Rcol}_i | \neg\mathsf{Rcol}_{i-1}\right], \qquad (1)$$
(where $\mathsf{Rcol}_0 = \emptyset$), we will focus on the estimation of $\mathbf{Pr}\left[\mathsf{Rcol}_i|\neg\mathsf{Rcol}_{i-1}\right]$ for $i = 1, \ldots, q$. Note that U_{i-1} contains at most i nodes without the occurrence of event Rcol_{i-1} by Proposition 1.

Suppose that $\mathcal{A}$ makes a forward query $\pi(x^*_L||x^*_R) = (y_L||y_R)$. Since there are at most one orderly reachable node $u \in U_{i-1}$ such that $u_R = x^*_R$, the i-th query determines at most one orderly reachable node $v = (y_L||(u_L \oplus x^*_L \oplus y_R))$. The probability that $u_L \oplus x^*_L \oplus y_R = w_R$ for some $w \in U_{i-1}$ is at most $iN/(N^2-q)$. When $\mathcal{A}$ makes a backward query $\pi^{-1}(y^*_L||y^*_R) = (x_L||x_R)$, the probability that $x_R = w_R$ for some $w \in U_{i-1}$ is also at most $iN/(N^2-q)$. Therefore we conclude that
$$\mathbf{Pr}\left[\mathsf{Rcol}_i|\neg\mathsf{Rcol}_{i-1}\right] \leq \frac{iN}{N^2-q},$$
and by (1),
$$\mathbf{Pr}\left[\mathsf{Rcol}_q\right] \leq \sum_{i=1}^{q} \frac{iN}{N^2-q} \leq \frac{q(q+1)}{2(N-1)}.$$
■

Let Coll denote the event that $\mathcal{A}$ makes a collision of JH_c. This event guarantees existence of two paths
$$\mathsf{P}_1 : IV(=u[0]) \xrightarrow{i_1} u[1] \xrightarrow{i_2} \cdots \xrightarrow{i_{s-1}} u[s-1] \xrightarrow{i_s} w$$

and

$$\mathsf{P}_2 : IV(=v[0]) \xrightarrow{j_1} v[1] \xrightarrow{j_2} \cdots \xrightarrow{j_{t-1}} v[t-1] \xrightarrow{j_t} w'$$

such that $\mathsf{chop}_c(w) = \mathsf{chop}_c(w')$. We can assume that this collision is an *earliest-possible* one such that $i_s \neq j_t$.

If both w and w' are orderly reachable nodes (with the above paths) and $i^* = i_s > j_t$ (without loss of generality), then we would have the following configuration.

1) C_1: $u \xrightarrow{i^*} w$ where $u \in U_{i^*-1}$ and $\mathsf{chop}_c(w) = \mathsf{chop}_c(w')$ for some $w' \in U_{i^*-1}$.

If one of w and w' is not an orderly reachable node, assuming w is not an orderly reachable node without loss of generality, let $i^* = i_\alpha$ be the first index in path P_1 such that $i_\alpha \geq i_{\alpha+1}$. Then, $u = u[\alpha - 1]$ is an orderly reachable node in U_{i^*-1}. Starting from this node, we have one of the following two local configurations.

2) C_2: $u \xrightarrow{i^*} u' \xrightarrow{i^*} u''$, where $u \in U_{i^*-1}$.
3) C_3: $u \xrightarrow{i^*} u' \xrightarrow{j} u''$, where $u \in U_{i^*-1}$ and $j < i^*$.

To summarize, we have

$$\begin{aligned}\mathbf{Adv}^{\mathsf{col}}_{\mathsf{JH}_c}(\mathcal{A}) = \mathbf{Pr}\left[\mathsf{Coll}\right] &\leq \mathbf{Pr}\left[\bigvee_{k=1}^{3} \mathsf{C}_k\right] \\ &\leq \mathbf{Pr}\left[\mathsf{Rcol}_q\right] + \mathbf{Pr}\left[\left(\bigvee_{k=1}^{3} \mathsf{C}_k\right) \wedge \neg\mathsf{Rcol}_q\right]. \quad (2)\end{aligned}$$

Proposition 3: Suppose that an adversary $\mathcal{A}$ makes q queries to a random permutation π and its inverse π^{-1}. For $N = 2^{n/2}$ and $q < N$,

$$\mathbf{Pr}\left[\left(\bigvee_{k=1}^{3} \mathsf{C}_k\right) \wedge \neg\mathsf{Rcol}_q\right] \leq \frac{N}{N-1} \cdot \frac{q(q+1)}{2^c}.$$

Proof: Throughout the proof, we fix $1 \leq i^* \leq q$ and bound the probability that the i^*-th query completes any of the configurations C_1, C_2 and C_3 without the occurrence of event Rcol_q.

First, we suppose that the i^*-th query $\pi^{-1}(y_L^*||y_R^*) = (x_L||x_R)$ is backward. In order to make any configuration C_k, $(x'_L||x_R)$ should be contained in U_{i^*-1} for some x'_L. This event occurs with probability at most $i^*N/(N^2 - q)$ since $|U_{i^*-1}| \leq i^*$ without the occurrence of event Rcol_q.

Next, we suppose that the i^*-th query $\pi(x_L^*||x_R^*) = (y_L||y_R)$ is forward. This query determines at most one orderly reachable node $u^* \in U_{i^*-1}$ such that $u_R^* = x_R^*$, and hence a unique node $w = (y_L||(u_L^* \oplus x_L^* \oplus y_R))$ such that $u \xrightarrow{i^*} w$ for some $u \in U_{i^*-1}$.

a) Event $\mathsf{C}_1 \wedge \neg\mathsf{Rcol}_q$*:* The probability that

$$\mathsf{chop}_c(y_L||(u_L^* \oplus x_L^* \oplus y_R)) = \mathsf{chop}_c(w')$$

for a fixed $w' \in U_{i^*-1}$ is at most $2^{n-c}/(N^2 - q)$. Since $|U_{i^*-1}| \leq i^*$, the probability that the i^*-th query completes C_1 without the occurrence of event Rcol_q is at most $i^*2^{n-c}/(N^2 - q)$.

b) Event $\mathsf{C}_2 \wedge \neg\mathsf{Rcol}_q$*:* The probability that

$$u_L^* \oplus x_L^* \oplus y_R = x_R^*$$

is at most $N/(N^2 - q)$.

c) Event $\mathsf{C}_3 \wedge \neg\mathsf{Rcol}_q$*:* The probability that

$$u_L^* \oplus x_L^* \oplus y_R = x_R^j$$

for some $j < i^*$ is at most $(i^* - 1)N/(N^2 - q)$.

To summarize, we have

$$\begin{aligned}\mathbf{Pr}\left[\left(\bigvee_{k=1}^{3} \mathsf{C}_k\right) \wedge \neg\mathsf{Rcol}_q\right] &\leq \frac{N}{N^2-q}\sum_{i=1}^{q}\left(\frac{iN}{2^c} + 1 + (i-1)\right) \\ &= \left(\frac{N}{2^c} + 1\right) \cdot \frac{N}{N^2-q} \cdot \frac{q(q+1)}{2} \\ &\leq \frac{N}{N-1} \cdot \frac{q(q+1)}{2^c}.\end{aligned}$$

■

By Propositions 2 and 3, and inequality (2), we have the following theorem.

Theorem 1: For the c-bit JH hash function JH_c,

$$\mathbf{Adv}^{\mathsf{col}}_{\mathsf{JH}_c}(q) \leq \frac{q(q+1)}{2^{c-1}}.$$

Acknowledgements

The authors would like to thank John Steinberger for valuable comments.

References

[1] R. Bhattacharyya, A. Mandal and M. Nandi. Security analysis of the mode of JH hash function. FSE 2010, LNCS 6147, pp. 168–191, Springer, Heidelberg (2010).

[2] E. Biham, R. Chen, A. Joux, P. Carribault, C. Lemuet and W. Jalby. Collisions of SHA-0 and reduced SHA-1. Eurocrypt 2005, LNCS 3494, pp. 36–57, Springer-Verlag, 2005.

[3] C. De Canniere and C. Rechberger. Preimages for reduced SHA-0 and SHA-1. Crypto 2008, LNCS 5157, pp. 179–202, Springer-Verlag, 2008.

[4] G. Leurent. MD4 is not one-way. FSE 2008, LNCS 5086, pp. 412–428, Springer-Verlag, 2008.

[5] F. Mendel, N. Pramstaller, C. Rechberger and V. Rijmen. Analysis of step-reduced SHA-256. FSE 2006, LNCS 4047, pp. 126–143, Springer-Verlag, 2006.

[6] Y. Sasaki and K. Aoki. Finding preimages in full MD5 faster than exhaustive search. Eurocrypt 2009, LNCS 5479, pp. 134–152, Springer-Verlag, 2008.

[7] X. Wang, X. Lai, D. Feng, H. Chen and X. Yu. Cryptanalysis of the hash functions MD4 and RIPEMD. Eurocrypt 2005, LNCS 3494, pp. 1–18, Springer-Verlag, 2005.

[8] X. Wang, X. Lai and H. Yu. Finding collisions in the full SHA-1. Crypt0 2005, LNCS 3621, pp. 17–36, Springer-Verlag, 2005.

[9] X. Wang and H. Yu. How to break MD5 and other hash functions. Eurocrypt 2005, LNCS 3494, pp. 19–35, Springer-Verlag, 2005.

[10] H. Wu. The Hash Function JH. Submission to NIST, http://icsd.i2r.a-star.edu.sg/staff/hongjun/jh/jh.pdf, 2008.