S e M c u i o r o d i n t

Rishiraj Bhattacharyya[1], Avradip Mandal[2], and Mridul Nandi[3⋆]

[1] Indian Statistical Institute, Kolkata, India
rishi_r@isical.ac.in
[2] Université du Luxembourg, Luxembourg
avradip.mandal@uni.lu
[3] NIST, USA and Computer Science Department, The George Washington University
mridul.nandi@gmail.com

A Recently, NIST has selected 14 second round candidates of SHA3 competition. One of these candidates will win the competition and eventually become the new hash function standard. Hence it is essential for these candidates to meet the state of the art security notions. In TCC'04, Maurer *et al* introduced indifferentiability as a generalization of the concept of the indistinguishability of two systems. Indifferentiability is the appropriate notion of modeling a random oracle as well as a strong security criteria for a hash-design. In this paper we analyze the indifferentiability and preimage resistance of JH hash function which is one of the SHA3 second round candidates. JH uses a $2n$ bit fixed permutation based compression function and applies chopMD domain extension with specific padding.

- We show under the assumption that the underlying permutations is a $2n$-bit random permutation, JH mode of operation with output length $2n - s$ bits, is indifferentiable from a random oracle with distinguisher's advantage bounded by $O(\frac{q^2\sigma}{2^s} + \frac{q^3}{2^n})$ where σ is the total number of blocks queried by distinguisher.
- We show that the padding in JH is essential as there is a simple indifferentiablity distinguisher (with constant query complexity) against JH mode of operation without length padding outputting n bit digest.
- We prove that a little modification (namely chopping different bits) of JH mode of operation enables us to construct a hash function based on random permutation (without any length padding) with similar bound of sponge constructions (with fixed output size) and with same efficiency.
- On the other hand, we improve the preimage attack of query complexity $2^{510.3}$ due to Mendel and Thompson. Using multicollisions in both forward and reverse direction, we show a preimage attack on JH with $n = 512, s = 512$ in 2^{507} queries to the permutation.

K e y differentiability, chop-MD, random permutation**r d s :**

1 I n t r o d u c

Designing secure hash function is a primary objective of symmetric key cryptography. Popular methods to build a hash function involve two steps. First, one designs a compression function $f : \{0,1\}^m \to \{0,1\}^n$ where $m > n$. Then a domain extension algorithm that utilizes f as a black box[4] is applied to implement the hash function $H^f : \{0,1\}^* \to \{0,1\}^n$. This is also known as design or mode of the hash function. The well known Merkle-Damgård domain extension technique is used often as it preserves the collision resistance property of the compression function: If f is collision resistant then so is H^f. This enables the designers to focus on designing collision resistant compression functions.

INDIFFERENTIABILITY. While collision resistance remains an essential property of a cryptographic hash function, current usage indicates that it no more suffices the modern security goals. Today hash functions are used as PRFs, MACs, (2nd) preimage-secure or even as to replace Random Oracles in different Cryptographic Protocols. In [6], Coron et al considered the problem of designing secure cryptographic hash function based on the *indifferentiability* framework [15]. Informally speaking, to prove indifferentiablity of an iterated hash function H (based on some ideal primitive f), one has to design a simulator S. The job of S is to simulate the behavior of f while maintaining consistency with the random oracle R. If no distinguisher D can distinguish the output distribution of the pair (H^f, f) from that of (R, S^R), the construction H is said to be indifferentiable from a Random Oracle (RO). By proving indifferentiability, we are guaranteed that there is no trivial flaw in the design of the hash function. Today, indifferentiability is considered to be a desirable property of any secure hash function design. Coron et al showed in [6], the design principle (Strengthened Merkle-Damgård) behind the current standard hash functions like MD5 or SHA-1 does not satisfy indifferentiability from RO property. They also proved that different variant of MD constructions, including chopped MD constructions can be

⋆ Supported in part by the National Science Foundation, Grant CNS-0937267

[4] The domain extension can be applied independent of compression functions except that it depends on the parameters m and n.

proven indifferentiable from a Variable Input Length Random Oracle if the compression function is constructed as an ideal component like Fixed Input Length Random Oracle or from Ideal Cipher with Davis Meyer technique. Subsequently, authors of [2,4,9,12] proved indifferentiability of different constructions of iterated hash functions. In [5], Chang and Nandi proved an indifferentiability bound beyond birthday bound for chopped MD constructions under the assumption that the compression function is a fixed input length random oracle.

In 2007, NIST announced a competition for a new hash function standard, to be called SHA-3. 64 designs were submitted and after an internal review of the submissions, 51 were selected for meeting the minimum submission requirements and accepted as the First Round Candidates. Recently, NIST declared the names of 14 candidates for the second round of the competition. One of these candidates will win the competition and eventually become the next standard cryptographic hash function. Hence, it is essential for these candidate designs to meet the state of the art security notions.

In this paper, we consider the mode of operation of the JH hash function, one of the second round candidates of SHA3 competition. It uses a novel construction, somewhat reminiscent of a sponge construction [4], to build a hash algorithm out of a single, large, fixed permutation using chopped-MD domain extension [21]. We also consider a little modified mode of operation of JH where the chopping is done on the other bits. For a formal and detailed description of mode of operation of JH and the modified mode of operation, we refer the reader to Section 2. Although the mode of JH is novel, it has withstand many cryptanalysis attempts so far. The only noticeable attack is due to Mendel and Thompson who has recently shown a preimage attack on JH mode of operation through finding r- multicollisions in the forward direction of JH mode [16]. The query complexity of their attack is $2^{510.3}$ to get a preimage of JH outputting 512-bits.

Our Result

In this paper we examine the indifferentiability and preimage resistance of JH mode of operation in $2n$ bit random permutation model. Let s denote the number of chopped bits. We extend the technique of Chang and Nandi [5] to random permutation model. We prove that under the assumption that the fixed permutation of JH is a random permutation, JH mode of operation with specific length padding is indifferentiable from random oracle with distinguisher's advantage bounded by $O(\frac{q^2\sigma}{2^s} + \frac{q^3}{2^n})$. When $s = 3n/2$ (as in case of JH hash function with 256 bit output), our result gives beyond the birthday bound security guarantee for JH. To the best of our knowledge this is the first indifferentiability bound under fixed random permutation model beyond the birthday bound. Although chopMD constructions do not need the length padding in general, we show the padding is *essential* to protect one indifferentiability attacker, working in *constant* JH mode of operation without padding with n-bit output number of queries. This result also shows that the method used in [4] to prove indifferentiability of sponge constructions (where length padding in last block is not required) cannot be readily extended to prove indifferentiability of JH.

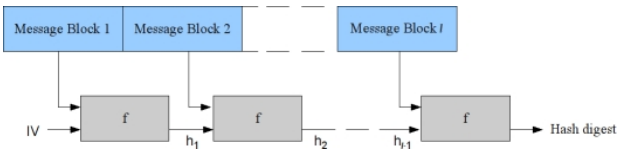
Next we consider the preimage resistance of JH mode of operation and improve the preimage attack of Mendel and Thompson [16]. Our preimage attack works with query complexity 2^{507} for finding a preimage of 512-bit JH hash function. Even though it marginally reduces the complexity of the previous known attack (with $2^{510.3}$ queries), theoretically the new attack requires asymptotically less complexity. Looking ahead, we exploit the multicollision in both forward and backward direction unlike in only forward direction used in [16].

Simultaneously, we look at other constructions, modifying JH mode of operation, where the chopping is done on the first instead of last s bits.

- We show that when the length of longest query is less than $2^{n/2}$, then the modified JH mode of operation without the length padding is indifferentiable from an RO with distinguisher's advantage bounded by $\mathcal{O}(\frac{q^2}{2^{\min(s,n)}})$ where q is the maximum number of queries made by the distinguisher.
- We show one indifferentiability attacker against modified JH mode of operation with $\Omega(2^{n/2})$ query complexity. This shows for $s \geq n$ the previous security bound is actually optimal.
- If we set $s = n$, we get a random permutation based secure mode of operation with n-bit digest using $2n$ bit permutation. We note that this construction is *more efficient* than based on $2n$ bit random permutation. where the indifferentiability bound is $\mathcal{O}(\frac{\sigma^2}{2^n})$ [4][5]. Here σ is the number blocks that the adversary queries.

On a secondary note, even though our proof techniques for indifferentiable security bounds are closely related to the techniques used in [5,12], we give a more formal argument behind some implicit assumptions made over there.

[5] We note that, however JH needs to store the message block for one more iteration unlike Sponge.



F **i** ård m**g**ode of operation base**l** on compression fun**c**tion Merkle-Damg

O r e g r a n i z a t i

The rest of the paper is organized as follows. In next section, we mention the notations, formal description of JH mode of operation and modified mode of operation, a short introduction to Indifferentiability of hash functions and some useful definitions and facts. In Section 3, we build our tools for extending Chang and Nandi's proof to random permutation model. For simplicity of of explanation, first we describe the indifferentiability of modified JH mode without padding in Section 4 followed by indifferentiability of original JH mode with padding in Section 5. In Section 6 and Section 7, we describe our indifferentiability distinguisher against JH mode of operation and modified mode of operation without the padding. Finally in Section 8, we present our improved preimage attack on JH mode of operation with padding.

2 P r e l i m i n

In this section we describe the notations and definitions used throughout the paper. Let us begin with a formal definition of mode of operation.

2 . 1 M o d e o f

Informally speaking, a mode of operation is an algorithm to construct a hash function from a compression function.

D *A* **e** *m* **fi***C* *w* **o**n *i* *t*p **i** *h* *t*r $f\{0,1\}^m \to$ **o**$\{0,1\}^n$ *a* *a*n **n** *n* *i* *c* *p* **l** *al* *d* *e* $f : \{0,1\}^* \to \{0,1\}^n$. *e* *s* *a* *f* *u* *n* *c*

Below we describe the well known Merkle-Damgård or MD mode of operation.

D *L* $IV \in \{0,1\}^n$ **b**fi *t* *e* **n** *i* **i** *fi* **t** *e* **i**ox f **n** $\{0,1\}^m \to \{0,1\}^n$, *ct* **2** *h* *o* *k* *n* *å* *o* *r* *w* *d* *i* *gn* *m* . *M* *l* *o*) *de* *i* *res* *k* *do* *l* *ef*

$$MD^f(m_1\|m_2\|\ldots\|m_l) = f(f(\ldots f(f(IV\|m_1)\|m_2)\ldots)\|m_l)$$

w $_1, m_2, \ldots$ *h* $m_l \in \{0,1\}^{m-n}$. *r* *e* *m*

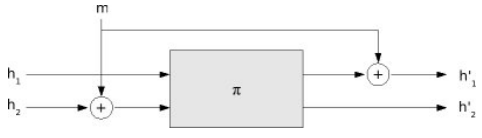
There is a subtle difference between a hash function and a mode of operation. The mode of operation is actually a domain extension algorithm. If we supply a particular compression function f to the mode of operation algorithm we get a particular hash function. So when we think about a hash function, the compression function is fixed.

2 . 2 t i J o H n M o d

The compression function of JH, $f^\pi : \{0,1\}^{3n} \to \{0,1\}^{2n}$ is defined as follows:

$$f^\pi(h_1\|h_2\|m) = \pi(h_1\|(h_2 \oplus m)) \oplus (m\|0^n)$$

where $h_1, h_2, m \in \{0,1\}^n$ and $\pi : \{0,1\}^{2n} \to \{0,1\}^{2n}$ is a fixed permutation.



F **i** **g** ction **.** **2** **.** The JH compression fun

The JH mode of operation based on a permutation π is the chopMD mode of operation based on the above compression function f^π. The usual Merkle-Damgård technique is applied on f^π and the output of the hash function is the first $2n-s$ bits of the final f^π query output. For any, $0 \leq s \leq |m|$, $\text{CHOPR}_s(m)$ is defined as m_L where $m = m_L \| m_R$ and $|m_R| = s$. Formally the JH mode of operation based on a permutation π with initial value $IV_1 \| IV_2$ is defined as

$$JH^\pi(\cdot) : (\{0,1\}^n)^+ \rightarrow \{0,1\}^{2n-s} \equiv \text{CHOPR}_s(MD^{f^\pi}(\cdot)).$$

Where, MD^{f^π} is the Merkle-Damgård mode of operation with initial value as $IV_1 \| IV_2$ and compression function as f^π. According to [21], typically $s = n$. Also it is suggested to have $s \geq n$.

We also define a modified version of JH mode of operation (referred as JH$'$ throughout the paper) where instead of chopping right most s bits we chop left most s bits. Let for $0 \leq s \leq |m|$, $\text{CHOPL}_s(m)$ is defined as m_R where $m = m_L \| m_R$ and $|m_L| = s$.

$$JH'^\pi(\cdot) : (\{0,1\}^n)^+ \rightarrow \{0,1\}^{2n-s} \equiv \text{CHOPL}_s(MD^{f^\pi}(\cdot)).$$

Throughout the paper JH-t denotes the JH mode of operation with t bit output. Similarly JH$'$-t denotes JH' mode of operation with t bit output.

2.3 Padding

To encode messages whose lengths are not multiple of block size (n bit) we need some padding rule, so that padded message becomes a multiple of block size. A simple padding rule can be zero padding, that is adding sufficient number of zero bits so that the padded message becomes a multiple of block size, even though this is not secure. We will see as in the case of JH a well designed padding rule leads to additional security guarantee.

Definition 3 *A padding rule is a pair of functions*

$$P \equiv (\text{PAD} : \{0,1\}^* \rightarrow (\{0,1\}^n)^+, \text{DEPAD} : (\{0,1\}^n)^+ \rightarrow \{0,1\}^* \cup \{\perp\})$$

such that for all $M \in \{0,1\}^*$ we have

$$\text{DEPAD}(\text{PAD}(M)) = M.$$

For $y \in (\{0,1\}^n)^+$, $\text{DEPAD}(y)$ outputs $x \in \{0,1\}^*$ such that $\text{PAD}(M) = y$. If no such x exists then it outputs $\perp$.

The function PAD takes a message of arbitrary length and outputs the padded message which is multiple of block length. Where as, the function DEPAD takes the padded message which is multiple of block length and outputs the original message. Normally, when we specify a padding rule we only specify the function PAD, but usually definition of DEPAD can be trivially derived from the description of PAD. In our context, we are interested in a specialized class of padding rules, namely with the following additional properties.

1. $\frac{|\text{PAD}(M)|}{n} = \lceil \frac{|M|}{n} \rceil + 1$.
2. For any $M \in (\{0,1\}^n)^+$, $LB(M) \subseteq \{0,1\}^n$ be the set of n-bit elements (possible last blocks) such that, $\text{DEPAD}(M \| m) \neq \perp$ for any $m \in LB(M)$. We want, $|LB(M)|$ to be small for all $M \in \{0,1\}^*$(smaller than some constant).

Here, if $x \in \{0,1\}^*$, $|x|$ denotes the length of x in bits. Also, if A is a set, $|A|$ denotes the number of elements in A. Any padding which satisfies the above two properties is called *good*. Now we are ready to define the JH padding rule. Now we define JH mode of operation with padding.

Definition 4 *We first fix a padding rule $P = (\text{PAD}, \text{DEPAD})$. Then we define the JH hash function with padding rule P as follows*

$$JH_P^\pi(\cdot) : \{0,1\}^* \rightarrow \{0,1\}^{2n-s} \equiv JH^\pi(\text{PAD}(\cdot)) \equiv \text{CHOPL}_s(MD^{f^\pi}(\text{PAD}(\cdot))).$$

The padding rule. In [21], the following padding rule is mentioned for JH hash function with block length $n = 512$. *Suppose M is a message of length $\ell(M)$ bits. Append a single 1 bit to M, then append $(-\ell(M) - 1 + (-\ell(M) \bmod 512)) \bmod 512$ zero bits, then append a 128-bit block containing $\ell(M)$ in its least significant bits.* It is easy to check that the padding rule is actually a good padding rule.

2.4 Indifferentiability

The notion of indifferentiability, introduced by Maurer et. al. in [15], is a generalization of classical notion of indistinguishability. Loosely speaking, if an ideal primitive $\mathcal{G}$ is indifferentiable with a construction C based on another ideal primitive $\mathcal{F}$, then $\mathcal{G}$ can be safely replaced by $C^{\mathcal{F}}$ in any cryptographic construction. In other terms if a cryptographic construction is secure in $\mathcal{G}$ model then it is secure in $\mathcal{F}$ model.

Definition 5 *Let F_i, G_i be ... or ... bit ... $\mathcal{A}$ a ... (F_1, F_2) ... (G_1, G_2) as*

$$\mathsf{Adv}_{\mathcal{A}}((F_1, F_2), (G_1, G_2)) = |\Pr[\mathcal{A}^{F_1, F_2} = 1] - \Pr[\mathcal{A}^{G_1, G_2} = 1]|.$$

Definition [6] *A ... C ... $\mathcal{F}$ ... $(q_C, q_S, \ldots, \varepsilon)$ ... $\mathcal{G}$ ... S ... $\mathcal{G}$ ... D ... ε.*

$$\mathsf{Adv}_D((C^{\mathcal{F}}, \mathcal{F}), (\mathcal{G}, S^{\mathcal{G}})) < \varepsilon.$$

... q_C ... C ... $\mathcal{G}$ ... $\mathcal{F}$ ... S. ... $C^{\mathcal{F}}$ ... (... $\mathcal{G}$ ...) ... p ... k. ...

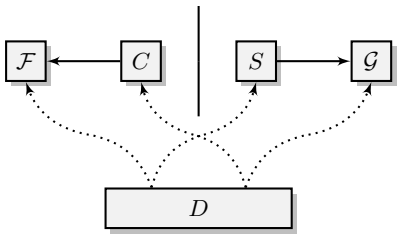


Figure 3. The indifferentiability no...

We stress that in the above definition $\mathcal{G}$ and $\mathcal{F}$ can be two completely different primitives. As shown in Fig 3 the role of the simulator is to not only simulate the behavior of $\mathcal{F}$ but also remain consistent with the behavior of $\mathcal{G}$. Note that, the simulator does not know the queries made directly to $\mathcal{G}$, although it can query $\mathcal{G}$ whenever it needs.

In this paper $\mathcal{G}$ is a variable input length Random oracle and $\mathcal{F}$ is a random permutation. Intuitively a random function (oracle) is a function $f : X \to Y$ chosen uniformly at random from the set of all functions from X to Y.

Definition 7 *... $x \in X$ ... $f(x)$ ... Y. ...*

$$\Pr[f(x) = y \mid f(x_1) = y_1, f(x_2) = y_2, \ldots, f(x_q) = y_q] = \frac{1}{|Y|}$$

... $x, x_1, \ldots, x_q$ ... $y, y_1, \ldots, y_q \in Y$. ...

A random permutation is similar to random oracle except that it is a permutation. So similarly one can view a random permutation $\pi : X \to X$ as a permutation chosen uniformly at random from the set of all permutation from X to X.

Definition 8

$$\Pr[\pi(x) = y \mid \pi(x_1) = y_1, \pi(x_2) = y_2, \ldots, \pi(x_q) = y_q] = \frac{1}{|X| - q}$$

... $x, x_1, \ldots, x_q$ ... $y_1, \ldots, y_q \in X$ ... $|X|$ ... $y \in X \setminus \{y_1, \ldots, y_q\}$ ...

Definition 9 *... $\{0,1\}^{2n} \to \{0,1\}^n$ ... $\{0,1\}^{2n} \to \{0,1\}^n$ ...*

Often we refer FH as left half and LH as right half. Below we state a few basic inequalities as a lemma which will be useful later.

Lemma 1. *Let $m, s, n \in \mathbb{N}$, $c \in \{0,1\}^n$, $\mathcal{S} \subseteq \{0,1\}^n$ and $\mathcal{T} \subseteq \{0,1\}^{2n}$. Then*

1. $|\{z \in \{0,1\}^n : z \oplus y \in \mathcal{S}\}| \leq |\mathcal{S}|$ *and* $|\{z \in \{0,1\}^n : z \oplus y \in \mathcal{S}\}| \leq |\mathcal{S}|$
2. $|\{(y,z) \in \{0,1\}^{2n} : FH(z \| y) \oplus c \in \mathcal{T}\}| \leq 2^n |\mathcal{T}|$ *and* $|\{(y,z) \in \{0,1\}^{2n} : FH(z \| y) \oplus c \in \mathcal{T}\}| \leq \frac{2^s}{2^{\min(s,n)}} |\mathcal{T}|$

3 Modeling the Attacker and Main Theorem Statement

We follow a similar approach to [5,12] for proving indifferentiability security over here. We start with modeling the attacker. Then we construct a simulator, for which the information the attacker sees remain statistically close whether the attacker is interacting with JH Hash function and the random permutation it is based on, or it is interacting with a random function and the simulator. Compared to [5] we do not restrict ourselves to some particular type of *iterated* underlying small domain oracle being a random permutation we also need to answer inverse queries.

Consistent

Intuitively, a small domain oracle is said to be consistent to a big domain oracle with respect to some mode of operation if querying the mode of operation based on the small domain oracle is equivalent to querying the big domain oracle.

Definition 1. *A small domain oracle G_1 is said to be consistent to a big domain oracle G_2 with respect to a mode of operation MO if there exists a polynomial time algorithm $\mathcal{B}$ (called the consistency algorithm) such that*

$$\Pr[G_1(x) = MO^{G_2}(x)] = 1.$$

The notion of consistent oracles is nothing new. In fact, in all the previous works e.g. [4,5,6,7,9,10,12] and many others, the simulators mentioned over there are always consistent to the big domain oracle (or they abort, when they fail to be consistent). Also note, π is always consistent to JH^π with respect to JH-mode of operation.

Evaluatable

There might be some point x for which the value of $MO^{G_2}(x)$ gets fixed by the relations $G_2(x_1) = y_1, \cdots, G_2(x_q) = y_q$. Such x's are called evaluatable by the relations $G_2(x_1) = y_1, \cdots, G_2(x_q) = y_q$. Formally,

Definition 2. *A point $x \in Domain(MO^{G_2})$ is said to be evaluatable by $G_2(x_1) = y_1, \cdots, G_2(x_q) = y_q$, if there exists a polynomial time algorithm $\mathcal{B}$ (called the evaluation algorithm) such that*

$$\Pr[MO^{G_2}(x) = \mathcal{B}(x, (x_1, y_1), \cdots, (x_q, y_q)) | G_2(x_1) = y_1, \cdots, G_2(x_q) = y_q] = 1.$$

Modeling the Attacker

In this paper the adversary is modeled as a deterministic, computationally unbounded[6] distinguisher $\mathcal{A}$ which has access to two oracles $\mathcal{O}_1$ and $\mathcal{O}_2$. Recall that $\mathcal{A}$ tries to distinguish the output distribution of (JH^π, π) from that of (R, S^R). We say $\mathcal{A}$ queries $\mathcal{O}_1$ when it queries the oracle JH^π or R and queries $\mathcal{O}_2$ when it queries the oracle π or S^R. As we model π as a random permutation, the distinguisher is allowed to make inverse queries to oracle $\mathcal{O}_2$. We denote the forward query as $(\mathcal{O}_2(+,\cdot,\cdot))$ and inverse query as $(\mathcal{O}_2(-,\cdot,\cdot))$. The view $\mathcal{V}$ of the distinguisher is the list query-response tuple

$$((M_1, h_1), \ldots, (M_{q_1}, h_{q_1}), (x_1^1, x_1^2, y_1^1, y_1^2), \ldots, (x_{q_2+q_3}^1, x_{q_2+q_3}^2, y_{q_2+q_3}^1, y_{q_2+q_3}^2)) \tag{1}$$

Where,

$$\mathcal{O}_1(M_1) = h_1, \ldots, \mathcal{O}_1(M_{q_1}) = h_{q_1}$$
$$\mathcal{O}_2(+, x_1^1, x_1^2) = (y_1^1, y_1^2), \ldots, \mathcal{O}_2(+, x_{q_2}^1, x_{q_2}^2) = (y_{q_2}^1, y_{q_2}^2)$$
$$\mathcal{O}_2(-, y_{q_2+1}^1, y_{q_2+1}^2) = (x_{q_2+1}^1, x_{q_2+1}^2), \ldots, \mathcal{O}_2(-, y_{q_2+q_3}^1, y_{q_2+q_3}^2) = (x_{q_2+q_3}^1, x_{q_2+q_3}^2)$$

[6] Any deterministic adversary with unlimited resource is as powerful as a randomized adversary [18].

Definition 1

$$\mathcal{I}(\mathcal{V}) = (M_1, \ldots, M_q, (x_1^1, x_1^2), \ldots, (x_{q_2}^1, x_{q_2}^2), (y_{q_2+1}^1, y_{q_2+1}^2), \ldots, (y_{q_2+q_3}^1, y_{q_2+q_3}^2))$$
$$\mathcal{O}(\mathcal{V}) = (h_1, \ldots, h_q, (y_1^1, y_1^2), \ldots, (y_{q_2}^1, y_{q_2}^2), (x_{q_2+1}^1, x_{q_2+1}^2), \ldots, (x_{q_2+q_3}^1, x_{q_2+q_3}^2))$$

Below we point out some important observations,

1. $\mathcal{V}$, $\mathcal{I}(\mathcal{V})$ and $\mathcal{O}(\mathcal{V})$ are actually ordered tuples. That means, the position of any element inside the tuple actually denotes the corresponding query number. So, in general $\mathcal{O}_1(.)$, $\mathcal{O}_2(+,(.,.))$ and $\mathcal{O}_2(-,(.,.))$ queries should not be grouped together. But we write it like this to avoid further notational complexity.
2. For any deterministic *n o n - a d a p t*
3. For any deterministic *a d a p t i v e* attacker $\mathcal{I}(\mathcal{V})$
4. For any deterministic attacker (adaptive or non-adaptive) $\mathcal{V}$ is actually determined by $\mathcal{O}(\mathcal{V})$.

I r r e d u c i b

Loosely speaking an irreducible view does not contain any duplicate query, and none of the $\mathcal{O}_1$ queries are evaluatable from the $\mathcal{O}_2$ queries present in the view.

Definition 1

$$\mathcal{V} = ((M_1, h_1), \ldots, (M_{q_1}, h_{q_1}), (x_1^1, x_1^2, y_1^1, y_1^2), \ldots, (x_{q_2+q_3}^1, x_{q_2+q_3}^2, y_{q_2+q_3}^1, y_{q_2+q_3}^2))$$

i s c a l l e d irreducible *i f*

- $_1, \ldots, M_{q_1}$ *M r e d i s t i n c t*
- $_1^1, x_1^2), \ldots, (x_{q_2+q_3}^1, x_{q_2+q_3}^2)$ *a r e d i s t i n c*
- $_1^1, y_1^2), \ldots, (y_{q_2+q_3}^1, y_{q_2+q_3}^2)$ *a r e d i s t i n c*
- $_1, \cdots, M_{q_1}$ *M r e r n e b a t t e i v o a n l s*

$$\pi(x_1^1, x_1^2) = (y_1^1, y_1^2), \ldots, \pi(x_{q_2+q_3}^1, x_{q_2+q_3}^2) = (y_{q_2+q_3}^1, y_{q_2+q_3}^2)$$

w i t h r o π*. e n s f p e c t t*

A l s o o t i d n n e c y d i v b u i l c e w v l

D F e o fi a r V i s i n c t u a i t l p V i l m s e u i d 1 t r o u t p r a u d t v u i c e i w b l w e

Let $\mathcal{OV}^{\mathcal{A}}_{\mathcal{O}_1,\mathcal{O}_2}$ be the random variable corresponding to the output view of attacker $\mathcal{A}$, obtained after interacting with $\mathcal{O}_1, \mathcal{O}_2$. Also, $\mathcal{V}^{\mathcal{A}}_{\mathcal{O}_1,\mathcal{O}_2}$ be the random variable corresponding to the view of attacker $\mathcal{A}$, obtained after interacting with $\mathcal{O}_1, \mathcal{O}_2$.

The theorem below shows, if the probability distributions for all possible output views in two scenarios are close, then the attacker advantage is small. Theorems similar to this were mentioned in literatures before [5,12,18]. The only difference is, here we concentrate on *o u t p u* er $\mathcal{A}$*,* there is always an *i* one to *e* one mapping between any view and output view.

T $_i, G_i$**h b e e e o h a r e h e g c m o k o r e b r t a h**

$$\Pr[\mathcal{OV}^{\mathcal{A}}_{F_1,F_2} = \mathcal{OV}] \geq (1-\varepsilon)\Pr[\mathcal{OV}^{\mathcal{A}}_{G_1,G_2} = \mathcal{OV}],$$

h o l d t s v $f_{\mathcal{A}}((F_1, F_2), (G_1, G_2)) \leq \varepsilon$ *a s l* $\mathcal{OV}$*, p h o*

P r o rem we refer the reader to Appendix A for a proof of this Theo □

Even though we have Theorem 1, in general it is hard to show the necessary condition of Theorem 1 for all possible output views. Theorem 2 actually proves that it is sufficient to work with irreducible output views instead of all possible output views. In fact, one can reduce any output view to an irreducible output view and then can apply Theorem 1.

T *I* **h** *f t* **e** *h* S^R *c* **o** *e o r* **r** *na e R* **e** *v sc e* **m** *i JHx s t m i h* **2** *e rot n.*
t h a t f o r a n y a t

$$\Pr[\mathcal{OV}^{\mathcal{A}}_{JH^\pi,\pi} = \mathcal{OV}] \geq (1-\varepsilon)\Pr[\mathcal{OV}^{\mathcal{A}}_{R,S^R} = \mathcal{OV}],$$

h o l d $\mathcal{OV}$ *(f w o* $\mathcal{A}$*) ir, t t a h* $\mathcal{A}$ *m l r el q qaep n uk o*
w e h a v e

$$\mathsf{Adv}_{\mathcal{A}}((JH^\pi,\pi),(R,S^R)) \leq \varepsilon.$$

P This theorem differs from Theorem 1, only in the aspect that here probability distributions are close only for the irreducible output views. For any reducible output view $\mathcal{OV}$ and the corresponding attacker $\mathcal{A}$, let $\mathcal{V}$ be the view fixed by $\mathcal{OV}$ and $\mathcal{A}$. Let, $\mathcal{V}'$ be the view obtained by deleting the computable $\mathcal{O}_1$ queries and repeated $\mathcal{O}_2$ queries of $\mathcal{V}$. The input view $\mathcal{I}(\mathcal{V}')$ actually specifies a non-adaptive attacker $\mathcal{A}'$. The output view $\mathcal{OV}' = \mathcal{O}(\mathcal{V}')$ is actually an irreducible output view with respect to $\mathcal{A}'$. As, π is consistent to JH^π and S^R is consistent to R with respect to JH-mode of operation we have,

$$\Pr[\mathcal{OV}^{\mathcal{A}}_{JH^\pi,\pi} = \mathcal{OV}] = \Pr[\mathcal{OV}^{\mathcal{A}'}_{JH^\pi,\pi} = \mathcal{OV}']$$
$$\Pr[\mathcal{OV}^{\mathcal{A}}_{R,S^R} = \mathcal{OV}] = \Pr[\mathcal{OV}^{\mathcal{A}'}_{R,S^R} = \mathcal{OV}'].$$

Note, $\mathcal{A}'$ actually makes less number of queries compared to $\mathcal{A}$. Hence, even for reducible views, we have

$$\begin{aligned}\Pr[\mathcal{OV}^{\mathcal{A}}_{JH^\pi,\pi} = \mathcal{OV}] &= \Pr[\mathcal{OV}^{\mathcal{A}'}_{JH^\pi,\pi} = \mathcal{OV}'] \\ &\geq (1-\varepsilon)\Pr[\mathcal{OV}^{\mathcal{A}'}_{R,S^R} = \mathcal{OV}'] \\ &= (1-\varepsilon)\Pr[\mathcal{OV}^{\mathcal{A}}_{R,S^R} = \mathcal{OV}].\end{aligned}$$

So the required condition of Theorem 1 remains true. Now, by applying Theorem 1 we get the result. □

In many previous works e.g. [4,5,12] ideas similar to Theorem 2 have been used implicitly. But to our knowledge, we are the first to formalize it.

4 I c n u d ′ r i if t f y e A e

4 . 1 n S t e i mr p u o l l a a t

The simulator maintains one partial permutation $e_1 : \{0,1\}^{2n} \to \{0,1\}^{2n}$ initially empty, one partial function $e_1^* : (\{0,1\}^n)^* \to \{0,1\}^{2n}$ initialized with $e_1^*(\phi) = IV_1 \| IV_2$. It also maintains two sets C_1, C_2 initialized as $C_1 = \{IV_1\}$ and C_2 as empty. Let I_1 denotes the set of points on which e_1 is defined, O_1 denotes the output points of e_1. $FH, LH : \{0,1\}^{2n} \to \{0,1\}^n$ be the two functions outputting first n-bits and last n-bits of any $2n$-bit number respectively.

The goal of the simulator is to remain consistent to R with respect to JH-mode of operation while behaving like a random permutation. Before describing the simulator, we give some insight informally on how the simulator works.

1. In the partial permutation e_1, the simulator maintains its history.
2. In the partial function e_1^*, the simulator maintains the list of queries evaluatable by e_1 with respect to JH-mode of operation.
3. C_1 is the set of fi *r s* $_1^*$ outputs. *h a l f* (first n-bits) of e
4. Even though e_1^* is evaluatable by the partial permutation e_1, it might happen that e_1 is also defined at some points which do not help in evaluating e_1^*. C_2 is the set of first half of such points.
5. The simulator makes sure, C_1 and C_2 always remain mutually exclusive.
6. Because of 5, there are no so called *a c c* tacker is interacting with (R, S^R) and it wants *t s* to evaluate $\mathcal{O}_1(m_1 \| \cdots \| m_\ell)$ through a series of $\mathcal{O}_2$ queries, she will always have to make a series of ℓ queries starting with $\mathcal{O}_2(IV_1, IV_2 \oplus m_1)$. The attacker can not hope to skip a query in the middle.

$S'^R(+, x_1, x_2)$

- F $e_1(x_1\|x_2)$ I = z RETURN z
- F t h I $e_1^*(M) = x_1\|x'$ e e x
  1. $m = x' \oplus x_2$
  2. $y = R(M\|m) \oplus \text{CHOPL}(m\|0^n)$
  3. $w \in_R \{0,1\}^s$
  4. $z = w\|y$
  5. IF ($z \in O_1$ OR $FH(z) \oplus m \in C_1 \cup C_2$)
     - GOTO 3
  6. $C_1 = C_1 \cup \{FH(z) \oplus m\}$
  7. $e_1^*(M\|m) = z \oplus (m\|0^n)$
  8. $e_1(x_1\|x_2) = z$
  9. RETURN z
- LSE E
  10. $z \in_R \{0,1\}^{2n}$
  11. IF $z \in O_1$
      - GOTO 10
  12. $e_1(x_1\|x_2) = z$
  13. $C_2 = C_2 \cup \{x_1\}$
  14. RETURN z

$S'^R(-, y_1, y_2)$

- F t h I $_1\|z_2$ s e $u_1(x_1\|z_2) = y_1\|y_2$ h e xt h
  - RETURN $z_1\|z_2$ t s M, s . t e
- LSE E
  1. $z_1 \in_R \{0,1\}^n$
  2. IF $z_1 \in C_1$
     - GOTO 1
  3. $z_2 \in_R \{0,1\}^n$
  4. IF $z_1\|z_2 \in I_1$
     - GOTO 3
  5. $C_2 = C_2 \cup \{z_1\}$
  6. RETURN $z_1\|z_2$

F i ′ g . 4 . Simulator for JH

S i ′π ≡mCH L$_s(MD^{f^\pi})$O u l a t o r f

We note at any point of time, the following conditions hold.

$$|O_1| \le q_2 + q_3 \text{ and } |I_1| \le q_2 + q_3 \text{ and } |C_1 \cup C_2| \le q_2 + q_3 \text{ and } |C_1| \le q_2 + 1$$

T h e ′ a o n r tl e v a mi a e wy 3 i $\mathcal{OV}$

$$\Pr[\mathcal{OV}^{\mathcal{A}}_{R,S'^R} = \mathcal{OV}] \le \frac{1}{2^{(2n-s)q_1 + 2n(q_2+q_3)}} \times \frac{1}{(1 - \frac{2(q_2+q_3)}{2^{\min(s,n)}})^{q_2}} \times \frac{1}{(1 - \frac{2(q_2+q_3)}{2^n})^{q_3}}$$

w $^s > 2(q_2$ *h* $+ q_3)2^{min(s,n)}$*e*. *r e* 2

P As $\mathcal{OV}$ i*s* irreducib*x*le, R query o*u*tputs are ind*e*pendent of the other queries, hence R being a Random Function for q_1 many R queries we get the term $\frac{1}{2^{(2n-s)q_1}}$. For an $S'^R(+,\cdot,\cdot)$ queries, simulator is giving output as $w\|y$, there are two scenarios.

1. y is distributed uniformly over $\{0,1\}^{2n-s}$ and w is distributed uniformly over $\{0,1\}^s \setminus \{z \in \{0,1\}^s : z\|y \in O_1$ *or* $FH(z\|y) \oplus (x' \oplus x_2) \in C_1 \cup C_2\}$.
2. $w\|y$ is distributed uniformly over $\{0,1\}^{2n} \setminus O_1$.

By Lemma 1 we know,

$$|\{z \in \{0,1\}^s : y\|z \in O_1\}| \le |O_1| \le (q_2 + q_3).$$

On the other hand, using Lemma 1 here we have,

$$|\{z \in \{0,1\}^s : FH(z\|y) \oplus (x' \oplus x_2) \in C_1 \cup C_2\}| \le \frac{2^s}{2^{\min(s,n)}}|C_1 \cup C_2| \le \frac{2^s}{2^{\min(s,n)}}(q_2 + q_3).$$

Hence, for $2^s > 2(q_2 + q_3)2^{min(s,n)}$ and any $(w\|y) \in \{0,1\}^{2n}$ we have,

$$\Pr[S'^R(+,\cdot,\cdot) \textit{ query outputs } (w\|y)] \le \max\left(\frac{1}{2^{2n-s}} \frac{1}{2^s - \frac{2^s}{2^{\min(s,n)}}(q_2+q_3) - (q_2+q_3)}, \frac{1}{2^{2n} - (q_2+q_3)}\right)$$
$$\le \frac{1}{2^{2n}} \frac{1}{(1 - \frac{2(q_2+q_3)}{2^{\min(s,n)}})}$$

For $S^R(-,\cdot,\cdot)$ query giving output as $z_1\|z_2$ we know,

1. z_1 is uniformly distributed over $\{0,1\}^n \setminus C_1$
2. z_2 is uniformly distributed over $\{0,1\}^n \setminus \{w \in \{0,1\}^n : z_1 \| w \in I_1\}$

We know, $|C_1| \leq (q_2+1)$ and $|I_1| \leq (q_2+q_3)$. Hence, for any $(z_1\|z_2) \in \{0,1\}^{2n}$ we have

$$\begin{aligned}\Pr[S^R(-,\cdot,\cdot) \text{ query outputs } (z_1\|z_2)] &\leq \frac{1}{2^n-(q_2+1)}\frac{1}{2^n-(q_2+q_3)} \\ &\leq \frac{1}{2^{2n}}\frac{1}{1-\frac{2(q_2+q_3)}{2^n}}\end{aligned}$$

Hence, all together we get

$$\Pr[\mathcal{OV}^{\mathcal{A}}_{R,S^R} = \mathcal{OV}] \leq \frac{1}{2^{(2n-s)q_1+2n(q_2+q_3)}} \times \frac{1}{(1-\frac{2(q_2+q_3)}{2^{\min(s,n)}})^{q_2}} \times \frac{1}{(1-\frac{2(q_2+q_3)}{2^n})^{q_3}}$$

□

Next we wish to show that our simulator is efficient. The condition $2^{\min(s,n)} > 4(q_2+q_3)2^n$ ensures the GOTO statement at Step 5 in forward query in Figure 4.1 gets executed with probability less than $\frac{1}{2}$ at each iteration. We also know $|O_1| \leq (q_2+q_3)$ and $|C_1 \cup C_2| \leq (q_2+q_3)$. Hence expect with negligible probability, Step 5 takes at most $\mathcal{O}(q_2+q_3)$ time to satisfy the condition. The same argument holds for other GOTO statements as well. Hence we get the following result.

T *I* $2^{\min(s,n)} > 4(q_2+q_3)$, *t* **o** *h* S'^R *t* **r** $\mathcal{O}(q_2+q_3)$ *t i* **m** *m m s* (*a u* **4** *e e t l t x*
e x p r ***o*** ***h*** ***e*** *nb t i i l ai t l y l y*

4 . 2 a I $\mathcal{A}_{JH'^\pi,\pi}$ n i l t i e t ry p o of

In Theorem 3 we have shown upper bound for $\Pr[\mathcal{OV}^{\mathcal{A}}_{R,S'^R} = \mathcal{OV}]$ for any irreducible output views $\mathcal{OV}$. The Theorem below gives a lower bound for $\Pr[\mathcal{OV}^{\mathcal{A}}_{JH'^\pi,\pi} = \mathcal{OV}]$ for any irreducible output view $\mathcal{OV}$. Later we will apply Theorem 2 to prove the indifferentiability bound using these upper and lower bounds.

T h e o *u* **r** *t* **e** *v* **m** *e e w* **5** $\mathcal{OV}$

$$\Pr[\mathcal{OV}^{\mathcal{A}}_{JH'^\pi,\pi} = \mathcal{OV}] \geq \frac{1}{2^{(2n-s)q_1+2n(q_2+q_3)}} \times (1-\frac{2\sigma^2}{2^{2n}}) \times (1-\frac{2q_1(q_1+q_2+q_3)}{2^{\min(s,n)}}).$$

The proof of the above theorem involves two steps. Starting with an attacker $\mathcal{A}$ against $JH'^\pi \equiv$ CHOPL(MD^{f^π}) we construct another attacker $\mathcal{A}'$ against MD^{f^π} which essentially makes same queries as $\mathcal{A}$ but has access to unchopped output view.

- In Definition 15 we define the notion of *M* *D* -we actually show for the output *e* view $\mathcal{OV}_{MD}$ corresponding to any *M* *D* - *i r r e d*

$$\Pr[\mathcal{OV}^{\mathcal{A}'}_{MD^{f^\pi},\pi} = \mathcal{OV}_{MD}] \geq \frac{1}{2^{2nq_1+2n(q_2+q_3)}} \times (1-\frac{2\sigma^2}{2^{2n}})$$

- In Theorem 15 we actually show, given an irreducible output view $\mathcal{OV}$ and an attacker $\mathcal{A}$, if $\mathbf{OV}_{MD}$ is the set of all *M* *D* - ker $\mathcal{A}'$ such that, *r e d u c*

$$\Pr[\mathcal{OV}^{\mathcal{A}}_{JH'^\pi,\pi} = \mathcal{OV} | \mathcal{OV}^{\mathcal{A}'}_{MD^{f^\pi},\pi} = \mathcal{OV}_{MD}] = 1$$

  for all $\mathcal{OV}_{MD} \in \mathbf{OV}_{MD}$; then

$$|\mathbf{OV}_{MD}| \geq 2^{sq_1} \times (1-\frac{2q_1(q_1+q_2+q_3)}{2^{\min(s,n)}})$$

The above two results readily imply Theorem 5. For details the reader can refer to Appendix B.

4.3 S I e n c du ir f i f t e y r

We are now ready to prove the main result of this section. For any attacker $\mathcal{A}$, making at most q_1, q_2, q_3 queries to the oracles $\mathcal{O}_1, \mathcal{O}_2(+,\cdot,\cdot), \mathcal{O}_2(-,\cdot,\cdot)$ respectively we show an upper bound for $\mathsf{Adv}_{\mathcal{A}}$.

T *T* JH'^{π}- *h c* **e** *e* $(2n-s)$- *n b* **r** *s i* **e** *tt r o* **h** *ui* $(\mathcal{O}(q_2+q_3)), (q_1, q_2+$ *i.* $q_3, \epsilon)$ *i n d n i d f f o e m r e o n r t ai a c*

$$\epsilon \leq \frac{2\sigma^2}{2^{2n}} + \frac{2q_3(q_2+q_3)}{2^n} + \frac{2q_2(q_2+q_3)+2q_1(q_1+q_2+q_3)}{2^{\min(s,n)}},$$

w σ *i sh t e lf m e e m* q_1 *i s s a t s hux a* JH'^{π} *g R* $q_2 + q_3$ *i s u t h e u m e* $^{-1}$ *o* $'^R(+,\cdot,\cdot), S'^R(-,\cdot,\cdot)$. *H s m t* $2 + q_3 < 2^{\min(s,n)}/4$ *me w*

P r o o f view $\mathcal{OV}$ from Theorem 3 and Theorem 5 we have, output

$$\Pr[\mathcal{OV}^{\mathcal{A}}_{JH^{\pi},\pi} = \mathcal{OV}] \geq \left(1 - \left(\frac{2\sigma^2}{2^{2n}} + \frac{2q_3(q_2+q_3)}{2^n} + \frac{2q_2(q_2+q_3)+2q_1(q_1+q_2+q_3)}{2^{\min(s,n)}}\right)\right)$$
$$\times \Pr[\mathcal{OV}^{\mathcal{A}}_{R,S'^R} = \mathcal{OV}]$$

Now, applying Theorem 2 we get the required result. □

When maximum query length ℓ is smaller than $2^{n/2}$, for any attacker $\mathcal{A}$ (making at most q many queries) against the JH$'$ construction we have

$$\mathsf{Adv}_{\mathcal{A}} = \mathcal{O}(\frac{q^2}{2^{\min(s,n)}})$$

5 I c n u d P r i if t f y e A e

In this section we prove the indifferentiability of JH mode of operation with padding.

5.1 n S t e i m p u o l l a a t

We describe our simulator in Fig 5. Similar to previous section, the following notation we used in describing the simulator.

- Partial permutation $e : \{0,1\}^{2n} \to \{0,1\}^{2n}$, initially empty. I denotes set of points where e is defined and O denotes the output points of e.
- Partial function $e^* : (\{0,1\}^n)^* \to \{0,1\}^{2n}$ initialized to $e^*(\phi) = IV_1 \| IV_2$.
- Set $C \subseteq \{0,1\}^n$ initialized to $C = \{IV_1\}$ is the FH (first half) of e^* outputs.

For a padding rule $P = (\textsc{Pad}, \textsc{Depad})$ and $M \in (\{0,1\}^n)^+$, we recall $LB(M) \subseteq \{0,1\}^n$ is defined as $\{m \in \{0,1\}^n : \textsc{Depad}(M\|m) \neq \perp\}$. As in case of the actual JH padding rule we assume, $|LB(M)| \leq 2$.

We recall the design philosophy behind the JH' simulator from Section 4.1. Over there the simulator was maintaining a list of *e v a l* pped outputs in the partial permutation e_1^*. When the simulator receives some que query the goal of the simulators goals are three fold.

1. Give a random output keeping in mind the permutation property.
2. Do not create some new evaluatable query unless forced to. That means output of the simulator will never create a new evaluatable query.
3. But it might happen, only the input of the simulator forces another new evaluatable query. (This happens if attacker is trying to find some $\mathcal{O}_1$ query output through $\mathcal{O}_2$ query.) If this happens, then adjust the output of the simulator so that it remains *c o n s* e query *i s t e n t* to R, w.r.t.

One crucial point is at during one simulator query the simulator must prevent creation of more than one evaluatable query. Because then the simulator can not remain consistent to both of them. In forward queries to JH' simulator with $s = n$, when the attacker has forced creation of one new evaluatable query the LH (last half) of the possible output gets fixed by R response of that evaluatable query, but the simulator has control over FH output with which it makes sure, another evaluatable query is not created.

Here the situation is reversed. FH gets fixed by R, the simulator has control only over LH. This is problematic, because only FH can lead to creation of more evaluatable queries (with one more message block after the current evaluatable query). In fact, in Section 6 the attacker against JH mode operation without padding exploits this fact. But the simulator can play with LH to change the actual evaluatable query (even though it can not prevent the creation.) By doing so, the simulator ensures the new evaluatable query is not a valid padded message, hence for that query the simulator need not be consistent with R. The simulator also need to be careful such that no new evaluatable queries of length (current evaluatable query length + 2) or more are created. But that can be easily handled. Formally we have the following Theorem.

$S^R(+, x_1, x_2)$

1. IF $e(x_1\|x_2) = z$ RETURN z
2. IF t h $\check{e}(M) = x_r\|x'$ e e
   (a) $m = x' \oplus x_2$
   (b) IF $M \neq \phi$ AND $m \in LB(M)$
      i. $y = R(\text{DEPAD}(M\|m)) \oplus \text{CHOPR}(m\|0^n)$
      ii. $w \in_R \{0,1\}^s$
      iii. $z = y\|w$
   (c) ELSE
      i. $z \in_R \{0,1\}^{2n}$
   (d) IF $z \in O$ GOTO 2b
   (e) $e^{*\prime} = e^*$
   (f) $C' = C$
   (g) FOR EACH $i_1\|i_2 \in I \cup \{x_1\|x_2\}$
      i. IF $FH(z) \oplus m \neq i_1$ CONTINUE
      ii. IF $LH(z) \oplus i_2 \in LB(M\|m)$
         – OTO 2b G
      iii. IF $i_1\|i_2 = x_1\|x_2$
         – $_1\|o_2 = z$ o
      iv. ELSE
         – $_1\|o_2 = e(i_1\|i_2)$
      v. $e^{*\prime}(M\|m\|LH(z) \oplus i_2) = (o_1 \oplus LH(z) \oplus i_2)\|o_2$
      vi. $C' = C' \cup \{o_1 \oplus LH(z) \oplus i_2\}$
      vii. FOR EACH $i_1'\|i_2' \in I \cup \{x_1\|x_2\}$
         – F $LH(z) \oplus i_2 = o_1 \oplus i_1'$
            • GOTO 2b
   (h) $e^* = e^{*\prime}$
   (i) $C = C'$
   (j) $e^*(M\|m) = z \oplus (m\|0^n)$
   (k) $C = C \cup \{FH(z) \oplus m\}$
3. ELSE
   (a) $z \in_R \{0,1\}^{2n}$
   (b) IF $z \in O$ GOTO 3a
4. $e(x_1\|x_2) = z$
5. RETURN z

$S^R(-, y_1, y_2)$

1. IF t h $_1\|z_2$ s e u $r\|z_2) = y_1\|y_2$ he xt h
   x – i ETURN $z_1\|z_2$ t s M, s.t. e
2. ELSE
   (a) $z_1 \in_R \{0,1\}^n$
   (b) IF $z_1 \in C$
      – OTO 2a G
   (c) $z_2 \in_R \{0,1\}^n$
   (d) IF $z_1\|z_2 \in I$
      – OTO 2c G
   (e) $e(z_1\|z_2) = y_1\|y_2$
   (f) RETURN $z_1\|z_2$

F i g dding **. 5 .** Simulator for JH with pa

T h $^R i$ **e** n **o** F e **r** iR **g** a **m** $\pi_P m$ i sd **7** o c o **.**

The next two theorems describe the running time and interpolation probability upper bound corresponding to the simulator.

T *F* **h** *o* $\mathcal{A}$ *a* **e** $JH^{\pi}_{P,\pi}$ **o** *a* *a* **r** *n* *iy* **e** *y* *h* *i* **m** *as* $\mathcal{OV}$ *w* *o* *t* **8** *f a i* *d o t*
w *e* *h* *a* *v* *e*

$$\Pr[\mathcal{OV}^{\mathcal{A}}_{R,S^R} = \mathcal{OV}] \leq \frac{1}{2^{(2n-s)q_1+2n(q_2+q_3)}} \times \frac{1}{(1-\frac{(q_2+q_3+3)^2}{2^s})^{q_2}} \times \frac{1}{(1-\frac{(q_2+q_3+1)^2}{2^n})^{q_3}}$$

w $_2 + q_3 + 3)^2 < 2^{\min(s,n)}$. *n* $(q$

P *r* *o* ppendix C. *f* . We refer the reader to A □

T *I* $2(q_2 + q_3 + 3)^2 < 2^{\min(s,n)}$, **o** *t* hS^R **r** *t* *ae* **e** $\mathcal{O}((q_2 + q_3)^2)$ *t i e* *i m* *s m* **9** *a u* *e*
(*e* *x* *y* *c* *n* *e* *e* *p* *g* *t* *l w* *i* *g* *i* *t i* *h b* *el* *e*

5 . 2 a $\mathbf{H}^{\mathcal{A}}_{JH^{\pi}_{P},\pi}$ **n i l t i e t r y p o o f**

The following theorem is analogous to Theorem 5, used in Section 4.

T **h** **e** **o** *u* **r** *t* **e** *v* **m** *i* *e* *e* *w* **1** **0**

$$\Pr[\mathcal{OV}^{\mathcal{A}}_{JH^{\pi}_{P},\pi} = \mathcal{OV}] \geq \frac{1}{2^{(2n-s)q_1+2n(q_2+q_3)}} \times (1 - \frac{2\sigma^2}{2^{2n}}) \times (1 - \frac{2\sigma q_1(q_1+q_2+q_3)}{2^s}).$$

For the proof of above theorem we refer the reader to Appendix D

5 . 3 S I e n c du i r f i f t e y r H

T *T* **h** JH^{π}_{P} *m* *h* **e** *e o* **o** $(2n-s)$- **r** *b e* **e** *i o n* **m** *fo d* *o* π *i* $(\mathcal{O}(1((q_2 +$ *t* *m* **1**
$q_3)^2), q_1, q_2+q_3, \epsilon)$ *i* *n* *d* *n* *i* *d f* *f* *o* *e* *m r* *e* *o* *n* *r* *t* *a i*

$$\epsilon \leq \frac{2\sigma^2}{2^{2n}} + \frac{q_2(q_2+q_3+3)^2}{2^s} + \frac{q_3(q_2+q_3+1)^2}{2^n} + \frac{2\sigma q_1(q_1+q_2+q_3)}{2^s},$$

w σ *i* *s h* *t* *e* *lf* *m* *e* *e* *m* q_1 *i* *s s* *a* *t s* *h u x a* JH^{π}_{P} *o g R m* $q_2 + q_3$ *r i* *e* *i s u*
t *h* *e* *u* *m* π, π^{-1} *o* $S'^R(\cdot,\cdot,\cdot), S^R(\cdot,\cdot,\cdot)$. *i H s m* *t* $2(q_2 + q_3 + 3)^2 < 2^{\min(s,n)}$. *w*

Under reasonable assumptions, for an attacker making at most q queries with total σ many compression function invocations we have

$$\mathsf{Adv}_{\mathcal{A}} = \mathcal{O}(\frac{\sigma^2}{2^{2n}} + \frac{q^3}{2^n} + \frac{q^2\sigma}{2^s}).$$

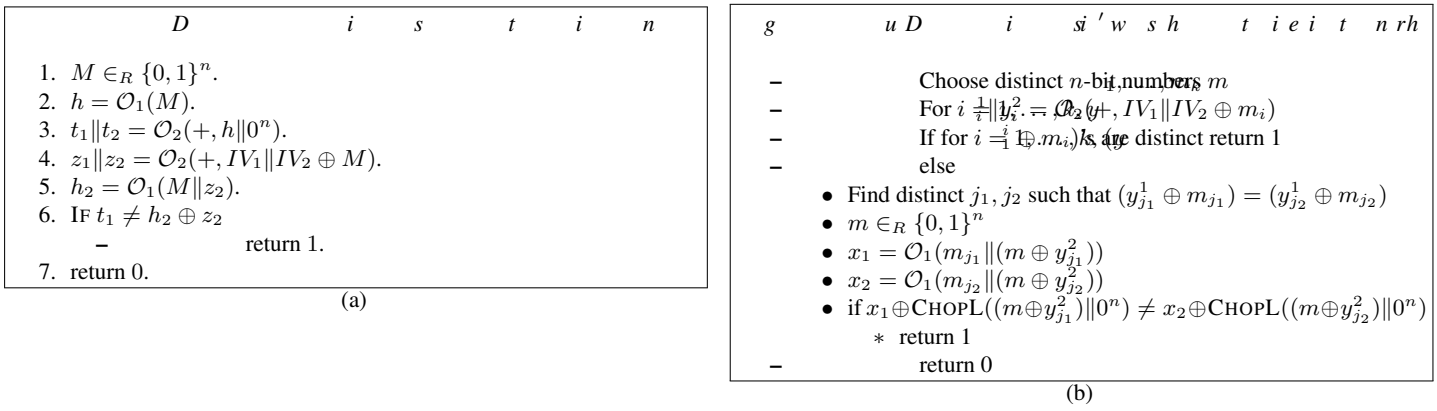
6 D i s t i n g u

Recall that the compression function of JH is based on a fixed permutation π. On input of the n-bit message block m and $2n$-bit chaining value $h_1||h_2$ the compression function outputs $f(m, h_1, h_2) = \pi(h_1, h_2 + m) + m||0^n$. JH applies chopped Merkle-Damgård transformation and outputs first t ($t = 2n - s$) bits of the output of final compression function. Here s denotes the number of chopped bits.

In case of JH-n, we have $s = n$. Our distinguisher first queries $h = C^{\pi}(M)$ with a random n-bit message M_1. The distinguisher appends 0^n with h and queries $t_1\|t_2 = \pi(+, h\|0^n)$. Note that when the distinguisher is interacting with (π, C^{π}), the second π query made by $C^{\pi}(M_1||M_2)$ will be on the input $(h||z)$ where z is the last n bit output of $\pi(+, IV_1, IV_2 \oplus M_1)$ xor-ed with M_2. So if we set M_2 to be the last n bit output of $\pi(+, IV_1, IV_2 \oplus M_1)$ then $z = 0^n$. Note that in case of JH with padding, we couldnot choose M_2 this way. To get M_2, the distinguisher queries $z_1\|z_2 = \mathcal{O}_2(+, IV_1\|IV_2 \oplus M)$. Now $\mathcal{D}$ sets $M_2 = z_2$ and queries $h_2 = C^{\pi}(M\|z_2)$. Finally the distinguisher checks whether $h_2 = t_1 \oplus z_2$. Formal algorithm of the distinguisher is described in Figure 6(a).

T **h** **e** **o** **r** **e** *s* **m** *i* *n* $_{\mathcal{A}} \geq 1 - 3\frac{2k+1}{2^n}$ *l* **2**

P *r* *o* ppendix E. *f* . We refer the reader to A □



F i g -n without padding, 6(b): Distinguisher for DH using the padding

7 D ′ i s t i n g u

In this section, we show one distinguisher with $\Omega(2^{n/2})$ many queries, which is successful against any simulator with non-negligible probability. Hence, when maximum query length ℓ is bounded by $2^{n/2}$, we get tight security bound.

The distinguisher has access to two oracles $\mathcal{O}_1, \mathcal{O}_2$ and is trying to differentiate between the two scenarios whether $(\mathcal{O}_1, \mathcal{O}_2)$ is (JH^π, π) or (R, S^R). Formal description of our distinguisher is given in Fig 6(b). The success probability of the distinguisher is established by following theorem. For a proof we refer the reader to Appendix F.

T h $^{n/2})$, e $\mathcal{A}$Adv so n r s o e m m - u n 1 l e a 3

Note, if we use CHOPR instead of CHOPL then the same attack actually applies for the original JH mode of construction without padding as well.

8 P J r H e i m a g

In this section we demonstrate a preimage attack on Merkle-Damgård based the JH compression function. As the JH hash output is a part of MD^{f^π}, having preimage attack on MD^{f^π} immediately translate a preimage attack on JH hash function. We use multicollision as it has been used in [16]. Let $Q(r)$ denote expected number of queries to get r-collision of a n-bit random oracle. In [20], it was shown that $Q(r) \sim 2^{n(r-1)/r}(r!)^{1/r}$. In [16], a preimage attack on JH has been shown based on multicollision of the forward direction of the JH mode. The query-complexity of the attack is $\mathcal{O}(Q(r))$ where r is a solution of the equation $r^{1/2}Q(r) = 2^n$. We use two sided multicollision (both from forward and backward direction) to improve the attack complexity little bit. The new query-complexity is $\mathcal{O}(Q(r))$ where $Q(r)r = 2^n$. Now we describe our preimage attack for MD^{f^π} where f^π is the compression function defined in JH based on a permutation π (see Fig 2). Let $h\|h' \in \{0,1\}^{2n}$ be a randomly chosen target. Note that given any m, h, h', $f^{-1}(h, h', m)$ is easily computable by making only one π^{-1} query.

1. Choose an arbitrary message block M_5 with correct padding, and compute $H_4 := h_4\|h'_4 = f^{-1}(h\|h', M_5)$.
2. Compute $Q(r)$ candidates for $H_3 = f^{-1}(H_4, M_4)$ to obtain r-collision on the last half of H_3. This is possible since we assume that π is a random permutation. Let L be the list of r many H_3's such that $LH(H_3)$'s are identical to say h'_3.
3. Similarly we do it for forward computation of f for the first message block M_1. We have a list L' of r values of H_1 such that $FH(H_1) = h_1$ for all $H_1 \in L'$.
4. Now we run a kind of meet-in-the-middle attack for the chaining value H_2. We compute $Q(r)$ values of $\pi(h_1, h'_1)$ and $\pi^{-1}(h_3, h'_3)$ for $Q(r)$ choices of h'_1 and h_3. Note that h_1 and h'_3 are fixed from the previous two steps. Find h'_1 and h_3 such that

$$FH(\pi(h_1, h'_1) \oplus \pi^{-1}(h_3, h'_3)) \oplus h'_1 \in L',\ LH(\pi(h_1, h'_1) \oplus \pi^{-1}(h_3, h'_3)) \oplus h_3 \in L.$$

For any pair (h'_1, h_3) the probability of the above event is $\frac{r^2}{2^{2n}}$. Since we have $Q^2(r)$ such pairs we can expect one such pair (h'_1, h_3) satisfying the above condition provided r is the at least the solution of the equation $rQ(r) = 2^n$.

Let $M_2 = FH(\pi(h_1, h_1') \oplus \pi^{-1}(h_3, h_3'))$, $M_3 = LH(\pi(h_1, h_1') \oplus \pi^{-1}(h_3, h_3'))$. Moreover we choose M_1 and M_4 from the list L' and L respectively such that $H_1 := h_1 \| h_1'$ and $H_3 := h_3 \| h_3'$ are the corresponding chaining value.

It is easy to verify that $MD^{f^\pi}(M_1 \| M_2 \| M_3 \| M_4 \| M_5) = h \| h'$. In [16], $r = 51$ to satisfy the equation $r^{1/2}Q(r) = 2^{512}$ where $n = 512$. The query complexity of their attack is roughly 2^{510}. We can choose $r = 46$ a solution of $rQ(r) \sim 2^{512}$. In this case the query complexity of π and π^{-1} is roughly 2^{507}. Compared with the previous preimage attack, it does not have significant reduction in complexity. However, asymptotically it has non-trivial reduction finding preimage of JH. The solution of r in $r^{1/2}Q(r) = 2^n$ is larger than that of $rQ(r) = 2^n$. Since $Q(r)$ is strictly increasing function in r our attack complexity is asymptotically less than that of [16]. However, we do not know any concrete forms of the query complexities for these two attacks.

References

1. M. Bellare and P. Rogaway. Random Oracles Are Practical : A Paradigm for Designing Efficient Protocols. In *1 s t u C t i C o m m 3. u n i c a t i o n*
2. M. Bellare and T. Ristenpart. Multi-Property-Preserving Hash Domain Extension and the EMD Transform. In *A d - v A a 2 0 0 6* , volume 4284 of *L N C S* , pages 299-314, Springer-Verlag, 2006.
3. R. Barke On the Security of Iterated MACs. Diploma Thesis '03. ETH Zurich
4. G. Bertoni, J. Daemen, M. Peeters, and G. Van Assche. On the indifferentiability of the sponge construction. In *A d - v E u r o* pages 181-197. Springer-Verlag, 2008. *p t 2 0 0 8*
5. D. Chang and M. Nandi. Improved Indifferentiability Security Analysis of chopMD Hash Function. In *F a 2 s t 0 S* 5086/2008, pages 429–443.
6. J. S. Coron, Y. Dodis, C. Malinaud and P. Puniya. Merkle-Damgard Revisited: How to Construct a Hash Function. In *A d v C r y p t o* r-Verlag, 2005. *0 0 5* , volume 3621 of *L*
7. J. S. Coron, J. Patarin and Y Seurin. The Random Oracle Model and the Ideal Cipher Model Are Equivalent. In *A d C v a r 2 0 0 8* volume 5157 of *L N C S* , Springer- Verlag, pages
8. I. Damgård A Design Principles for hash functions. In *A d - v C a R n Y e P s* Springer-Verlag, 1989.
9. Y. Dodis, K. Pietrzak, and P. Puniya. A new mode of operation for block ciphers and length-preserving MACs. In *A d v E U R O* -Verlag, 2008. *R Y P T 2*
10. Y. Dodis, L. Reyzin, R. Rivest and E. Shen. Indifferentiability of Permutation-Based Compression Functions and Tree-Based Modes of Operation, with Applications to MD6. In FSE 2009.
11. Y. Dodis, T. Ristenpart and T. Shrimpton. Salvaging Merkle-Damgård for Practical Applications. In Advances in Cryptology, Eurocrypt 2009, volume 5479 of *L N* -Verlag, 2009. *S* , pages 371-388,Springer
12. D. Chang, S. Lee, M. Nandi, and M. Yung. Indifferentiable security analysis of popular hash functions with prefix-free padding. In *A d C r 0y p t* volume 4284 of *L l* -Verlag, 2006 *g C y - S A* , pages 283-298, Springer
13. R. Canetti, O. Goldreich and S. Halevi. The random oracle methodology, revisited. In *S T O C '*
14. U. Maurer. Indistinguishability of Random Systems. In Advances in Cryptology- EUROCRYPT 2002,volume 2332 of *L N C* Springer-Verlag, 2002.
15. U. Maurer, R. Renner and C. Holenstein. Indifferentiability, Impossibility Results on Reductions, and Applications to the Random Oracle Methodology. In *T C C ' 2* erlag, 2004 *0 0 4* , volume 2951 of *L*
16. F. Mendel, S. Thomsen. An Observation on JH-512. Available at http://ehash.iaik.tugraz.at/uploads/d/da/Jh_preimage.pdf
17. J. Nielsen. Separating Random Oracle Proofs from Complexity Theoretic Proofs: The Non-committing Encryption Case. In *A d C r y p t o l o g y - C r y*
18. M. Nandi A Simple and Unified Method of Proving Indistinguishability In *P r l o n g d r o e s* pages 317-334, Springer-Verlag, 2002.
19. SHA 3 official website *h t t s p / : S / s T u x c / h s h r h a c 1 s i . s h h s i*
20. K., D. Tonien, K. Kurosawa, and K. Toyota. Birthday Paradox for Multi-collisions. In Min Surp Rhee and Byoungcheon Lee, editors, ICISC, volume 4296 of LNCS, pages 2940. Springer, 2006.
21. H. Wu. The Hash Function JH. Submission to NIST, 2008. Available online: http://icsd.i2r.a-star.edu.sg/staff/hongjun/jh/jh.pdf.
22. S. Vaudenay, Decorrelation: A Theory for Block Cipher Security, J. Cryptology, Volume **1 6** , no 4, 2003, pp 249-286.

A Proof of

Let for any $\mathcal{OV} \in \mathbf{OV}_1$, $\mathcal{A}$ outputs 1 and for any $\mathcal{OV} \in \mathbf{OV}_0$, $\mathcal{A}$ outputs 0. Clearly, $\mathbf{OV}_0$ and $\mathbf{OV}_1$ are mutually exclusive and $\mathbf{OV} = \mathbf{OV}_0 \cup \mathbf{OV}_1$ be the set of all possible output views. Note,

$$|\Pr[\mathcal{OV}^{\mathcal{A}}_{F_1,F_2} \in \mathbf{OV}_1] - \Pr[\mathcal{OV}^{\mathcal{A}}_{G_1,G_2} \in \mathbf{OV}_1]| = |\Pr[\mathcal{OV}^{\mathcal{A}}_{F_1,F_2} \in \mathbf{OV}_0] - \Pr[\mathcal{OV}^{\mathcal{A}}_{G_1,G_2} \in \mathbf{OV}_0]|$$

Also, $\mathbf{OV}' \subseteq \mathbf{OV}$ be the set of output views such that, $\mathcal{OV} \in \mathbf{OV}'$ iff

$$\Pr[\mathcal{OV}^{\mathcal{A}}_{G_1,G_2} = \mathcal{OV}] \geq \Pr[\mathcal{OV}^{\mathcal{A}}_{F_1,F_2} = \mathcal{OV}]$$

$$\begin{aligned}
\mathsf{Adv}_{\mathcal{A}}((F_1,F_2),(G_1,G_2)) &= |\Pr[\mathcal{A}^{F_1,F_2} = 1] - \Pr[\mathcal{A}^{G_1,G_2} = 1]| \\
&= |\Pr[\mathcal{OV}^{\mathcal{A}}_{F_1,F_2} \in \overline{\mathcal{OV}}_1] - \Pr[\mathcal{OV}^{\mathcal{A}}_{G_1,G_2} \in \overline{\mathcal{OV}}_1]| \\
&= \frac{1}{2} \times \Big(\big|\Pr[\mathcal{OV}^{\mathcal{A}}_{F_1,F_2} \in \mathbf{OV}_1] - \Pr[\mathcal{OV}^{\mathcal{A}}_{G_1,G_2} \in \mathbf{OV}_1]\big| \\
&\qquad + \big|\Pr[\mathcal{OV}^{\mathcal{A}}_{F_1,F_2} \in \mathbf{OV}_0] - \Pr[\mathcal{OV}^{\mathcal{A}}_{G_1,G_2} \in \mathbf{OV}_0]\big| \Big) \\
&\leq \frac{1}{2} \sum_{\mathcal{OV} \in \mathbf{OV}} \big|\Pr[\mathcal{OV}^{\mathcal{A}}_{F_1,F_2} = \mathcal{OV}] - \Pr[\mathcal{OV}^{\mathcal{A}}_{G_1,G_2} = \mathcal{OV}]\big| \\
&= \sum_{\mathcal{OV} \in \mathbf{OV}'} \big(\Pr[\mathcal{OV}^{\mathcal{A}}_{G_1,G_2} = \mathcal{OV}] - \Pr[\mathcal{OV}^{\mathcal{A}}_{F_1,F_2} = \mathcal{OV}]\big) \\
&\leq \sum_{\mathcal{OV} \in \mathbf{OV}'} \varepsilon \times \Pr[\mathcal{OV}^{\mathcal{A}}_{G_1,G_2} = \mathcal{OV}] \leq \varepsilon
\end{aligned}$$

□

B Proof of T

D e fi n i t i o n 1

$$MD^{f^{\mathcal{O}_2}}(M_1\|m_1) = g_1, \ldots, MD^{f^{\mathcal{O}_2}}(M_{q_1}\|m_{q_1}) = g_{q_1}$$
$$\mathcal{O}_2(x^1_1, x^2_1) = (y^1_1, y^2_1), \ldots, \mathcal{O}_2(x^1_{q_2+q_3}, x^2_{q_2+q_3}) = (y^1_{q_2+q_3}, y^2_{q_2+q_3}) \ldots \textit{Rel A}$$

i s MD-irreducible *i f* ,

1 $_1 \oplus (m_1\|0^n), .. g, g_{q_1} \oplus (m_{q_1}\|0^n), y^1_1\|y^2_1, \ldots, y^1_{q_2+q_3}\|y^2_{q_2+q_3}$ *a r e a l l*

2 . $_1$,*F o o n c r e o i* $= 1 \rho \ldots q$ *f d t h i t e i ϕ o*
(a i) i s) $_1$*d F.H.(g* $x^1_{q_2+q_3}$ *i a f* $_1$*. n f e d r IVe n t f*
(b b e) *Z h l MD* $^{f^{\mathcal{O}_2}}$ *q s c FH(g* $_i$*) k = IV* $_1$*e t s LH(g* $_i$*) b IV* $_2$ *f Σ. c e a I e*
$FH(g_i) = x^1_j$ *f o* $_2$*r + q*$_3$*, s t* $_i$*) h x*$^2_j \notin \Sigma$*. e m n e* $LH(g$ $1 \leq j \leq q$
3 $_1\|m_1, \ldots, M_{q_1}\|m_{q_1}$ *a r e r ne b a t te i v o a n*

$$\mathcal{O}_2(x^1_1, x^2_1) = (y^1_1, y^2_1), \ldots, \mathcal{O}_2(x^1_{q_2+q_3}, x^2_{q_2+q_3}) = (y^1_{q_2+q_3}, y^2_{q_2+q_3})$$

w i t h d $^{\mathcal{O}_2}$ *e o s n p f e c t t*

W e a l s o s a y t h

$$v = ((M_1\|m_1, g_1), \ldots, (M_{q_1}\|m_{q_1}, g_{q_1}), (x^1_1, x^2_1, y^1_1, y^2_1), \ldots, (x^1_{q_2+q_3}, x^2_{q_2+q_3}, y^1_{q_2+q_3}, y^2_{q_2+q_3}))$$

i s MD-irreducible *i f o a n n d d i o i bng l l R ey*

The definition above is similar to the definition of irreducible view (Definition 13). But here we are interested in the view without any chopping. Note, condition 2 ensures $M_i\|m_i$ is not evaluatable even with the help of the relations $MD^{f^{\mathcal{O}_2}}(M_j\|m_j) = h_j$ for $j \neq i$. Loosely speaking, the Theorem below gives a lower bound of the probability of getting a particular MD-irreducible tuple v, when a attacker interacts with $(MD^{f^{\pi}}, \pi)$.

T h e o r e m 1 4 $v = ((M_1\|m_1, g_1), \ldots, (M_{q_1}\|m_{q_1}, g_{q_1}), (x_1^1, x_1^2, y_1^1, y_1^2), \ldots, (x_{q_2+q_3}^1, x_{q_2+q_3}^2, y_{q_2+q_3}^1, y_{q_2+q_3}^2))$ *i s* MD-irreducible, *t u h t e a n t i t o h n e sn* π

$$MD^{f^\pi}_{IV_1\|IV_2}(M_1\|m_1) = g_1, \ldots, MD^{f^\pi}_{IV_1\|IV_2}(M_{q_1}\|m_{q_1}) = g_{q_1}$$
$$\pi(x_1^1, x_1^2) = (y_1^1, y_1^2), \ldots, \pi(x_{q_2+q_3}^1, x_{q_2+q_3}^2) = (y_{q_2+q_3}^1, y_{q_2+q_3}^2) \ldots \textit{Rel B}$$

i s a t l e a s t

$$\frac{|\Pi|}{2^{2nq_1+2n(q_2+q_3)}} \times (1 - \frac{2\sigma^2}{2^{2n}}),$$

w $|\Pi| = (2^{2n})!$ *i s e t r h m e e* $\{0,1\}^{2n}$ *t* $\{0,1\}^{2n}$ *a a σ i t n s t a i t d l o h s n a n e b l o M c k D s q B u r h e e o d l l e d u*

$$\frac{1}{2^{2nq_1+2n(q_2+q_3)}} \times (1 - \frac{2\sigma^2}{2^{2n}}),$$

w h e . n π i s a r a n d

P r o d from $(\{0,1\}^n)^+$ whose $MD^{f^\pi}_{IV_1\|IV_2}$ values are determined from the relations

$$\pi(x_1^1, x_1^2) = (y_1^1, y_1^2), \ldots, \pi(x_{q_2+q_3}^1, x_{q_2+q_3}^2) = (y_{q_2+q_3}^1, y_{q_2+q_3}^2).$$

Since v is MD-irreducible, $M_i\|m_i \notin D$ for all $1 \le i \le q_1$. let P denote the set of all nonempty prefixes of M_i's. More precisely,

$$P = \{M \in (\{0,1\}^n)^+ : M \textit{ is prefix of } M_i \textit{ for some } 1 \le i \le q_1\}.$$

We enumerate the set $P \setminus D \equiv \{N_1, \ldots, N_{\sigma'}\}$. Note that, $|P| + q_1 \le \sum_i \|M_i\|$. Now, we have

$$\sigma = q_2 + q_3 + \sum_i \|M_i\| \ge q_2 + q_3 + |P| + q_1 \ge q_1 + q_2 + q_3 + \sigma' \equiv \sigma''$$

Similar to the proof of Lemma 1 in [5], we can choose outputs of $MD^{f^{\mathcal{O}_2}}_{IV_1\|IV_2}(N_1), \ldots, MD^{f^{\mathcal{O}_2}}_{IV_1\|IV_2}(N_{\sigma'})$ in at least

$$(2^{2n} - 2(q_1 + q_2 + q_3))(2^{2n} - 2(q_1 + q_2 + q_3 + 1)) \ldots (2^{2n} - 2(q_1 + q_2 + q_3 + \sigma' - 1))$$

ways. (In the negative term, the factor 2 comes because, any output value should not be same as other output values and the next input value induced by the output value should not be same as other input values.) Hence,

$$\begin{aligned}
&|\{\pi : \{0,1\}^{2n} \to \{0,1\}^{2n} \textit{ such that } \pi \textit{ is a permutation and satisfies Rel B}\}| \\
&\ge (2^{2n} - \sigma'')! \times (2^{2n} - 2(q_1 + q_2 + q_3))(2^{2n} - 2(q_1 + q_2 + q_3 + 1)) \ldots (2^{2n} - 2(q_1 + q_2 + q_3 + \sigma' - 1)) \\
&\ge \frac{(2^{2n})!}{2^{2n\sigma''}} \times 2^{2n\sigma'} \times (1 - \frac{2\sigma'^2}{2^{2n}}) \ge \frac{|\pi|}{2^{2nq_1+2n(q_2+q_3)}} \times (1 - \frac{2\sigma^2}{2^{2n}})
\end{aligned}$$

□

D e fi c n i b i l t e i o i n e w 1 $\mathcal{V} = ((M_1\|m_1, h_1), \ldots, (M_{q_1}\|m_{q_1}, h_{q_1}), (x_1^1, x_1^2, y_1^1, y_1^2), \ldots, (x_{q_2+q_3}^1, x_{q_2+q_3}^2, y_{q_2+q_3}^1, y_{q_2+q_3}^2))$, *a M D* HOPL-matching *i i f r r e d u c*

$$v = ((M_1\|m_1, w_1\|h_1), \ldots, (M_{q_1}\|m_{q_1}, w_{q_1}\|h_{q_1}), (x_1^1, x_1^2, y_1^1, y_1^2), \ldots, (x_{q_2+q_3}^1, x_{q_2+q_3}^2, y_{q_2+q_3}^1, y_{q_2+q_3}^2)),$$

f o $_1$- *r* $_1, \ldots, w_{q_1})$. *p o l m e* $v = (w$ *q*

Let $M'_{\mathcal{V}}$ be the set of all such CHOPL- *m a t c h i n*

T h e o r e m 1 5

$$\mathcal{V} = ((M_1\|m_1, h_1), \ldots, (M_{q_1}\|m_{q_1}, h_{q_1}), (x_1^1, x_1^2, y_1^1, y_1^2), \ldots, (x_{q_2+q_3}^1, x_{q_2+q_3}^2, y_{q_2+q_3}^1, y_{q_2+q_3}^2))$$

w e h a v e ,

$$|M'_{\mathcal{V}}| \geq 2^{sq_1} \times (1 - \frac{q_1(q_1+q_2+q_3)}{2^{\min(s,n)}}).$$

P r o o f . By Lemma 1, we know

$$\begin{aligned}&|\{z \in \{0,1\}^s : z\|h_1 \oplus (m_1\|0^n) \in \{y_1^1\|y_1^2, \ldots, y_{q_2+q_3}^1\|y_{q_2+q_3}^2\}\}| \\ &= |\{z \in \{0,1\}^s : z\|h_1 \in \{y_1^1\|y_1^2 \oplus (m_1\|0^n), \ldots, y_{q_2+q_3}^1\|y_{q_2+q_3}^2 \oplus (m_1\|0^n)\}\}| \leq q_2+q_3\end{aligned}$$

and

$$|\{z \in \{0,1\}^s : FH(z\|h_1) \in \{x_1^1, \ldots, x_{q_2+q_3}^1, IV_1\}\}| \leq \frac{2^s}{2^{\min(s,n)}}(q_2+q_3+1).$$

Hence there are at least $(2^s - (q_2+q_3+\frac{2^s}{2^{\min(s,n)}}(q_2+q_3+1)))$ many possible values for w_1. Similarly once w_1 is selected there are at least $(2^s - (q_2+q_3+\frac{2^s}{2^{\min(s,n)}}(q_2+q_3+1)+1))$ many possible values for w_2 and so on. Hence,

$$\begin{aligned}|M'_{\mathcal{V}}| &= \textit{Number of valid } w \textit{ tuples} \\ &\geq (2^s - (q_2+q_3+\frac{2^s}{2^{\min(s,n)}}(q_2+q_3+1))) \ldots (2^s - (q_2+q_3+\frac{2^s}{2^{\min(s,n)}}(q_2+q_3+1)+q_1-1)) \\ &\geq 2^{sq_1} \times (1 - \frac{2q_1(q_1+q_2+q_3)}{2^{\min(s,n)}})\end{aligned}$$

□

Now we are ready to prove Theorem 5, with help of Theorem 14 and Theorem 15.Let $\mathcal{V}$ be the irreducible view determined by $\mathcal{A}$ and irreducible output view $\mathcal{OV}$. Consider an Attacker $\mathcal{A}'$, which makes queries at the same input points as of $\mathcal{A}$, but has access to $MD^{f^{\mathcal{O}_2}}$ instead of $JH'^{\mathcal{O}_2}$. Hence,

$$\begin{aligned}\Pr[\mathcal{OV}^{\mathcal{A}}_{JH'^{\pi},\pi} = \mathcal{OV}] = \Pr[\mathcal{V}^{\mathcal{A}}_{JH'^{\pi},\pi} = \mathcal{V}] &= \sum_{v \in M_{\mathcal{V}}} \Pr[\mathcal{V}^{\mathcal{A}'}_{MD^{f^{\pi}},\pi} = v] \geq \sum_{v \in M_{\mathcal{V}}} \frac{1}{2^{2nq_1+2n(q_2+q_3)}} \times (1 - \frac{2\sigma^2}{2^{2n}}) \\ &\geq \frac{1}{2^{2nq_1+2n(q_2+q_3)}} \times (1 - \frac{2\sigma^2}{2^{2n}}) \times 2^{sq_1} \times (1 - \frac{2q_1(q_1+q_2+q_3)}{2^{\min(s,n)}}) \\ &= \frac{1}{2^{(2n-s)q_1+2n(q_2+q_3)}} \times (1 - \frac{2\sigma^2}{2^{2n}}) \times (1 - \frac{2q_1(q_1+q_2+q_3)}{2^{\min(s,n)}})\end{aligned}$$

□

C P r o o f o f

As $\mathcal{OV}$ is irreducible R query outputs are independent of the other queries, hence R being a Random Function for q_1 many R queries we get the term $\frac{1}{2^{(2n-s)q_1}}$. For $S^R(+,\cdot,\cdot)$ query giving output as $y\|w$ we actually have two scenarios:

1. y is distributed uniformly over $\{0,1\}^{2n-s}$ and w is distributed uniformly over $\{0,1\}^s \setminus (B_1 \cup B_2 \cup \cdots \cup B_7)$, where
   (a) $B_1 = \{z \in \{0,1\}^s : y\|z \in O\}$
   (b) $B_2 = \{z \in \{0,1\}^s : FH(y\|z) \oplus x_1 = m, LH(y\|z) \oplus x_2 \in LB(M\|m)\}$
   (c) $B_3 = \{z \in \{0,1\}^s : FH(y\|z) \oplus i_1 = m, LH(y\|z) \oplus i_2 \in LB(M\|m)$ for some $i_1\|i_2 \in I\}$
   (d) $B_4 = \{z \in \{0,1\}^s : FH(y\|z) \oplus x_1 = m, LH(y\|z) \oplus x_2 = FH(y\|z) \oplus x_1\}$
   (e) $B_5 = \{z \in \{0,1\}^s : FH(y\|z) \oplus x_1 = m, LH(y\|z) \oplus x_2 = FH(y\|z) \oplus i'_1$ for some $i'_1\|i'_2 \in I\}$
   (f) $B_6 = \{z \in \{0,1\}^s : FH(y\|z) \oplus i_1 = m, LH(y\|z) \oplus i_2 = FH(e(i_1\|i_2)) \oplus x_1$ for some $i_1\|i_2 \in I\}$
   (g) $B_7 = \{z \in \{0,1\}^s : FH(y\|z) \oplus i_1 = m, LH(y\|z) \oplus i_2 = FH(e(i_1\|i_2)) \oplus i'_1$for some$i_1\|i_2, i'_1\|i'_2 \in I\}$
2. $y\|w$ is uniformly distributed over $\{0,1\}^{2n} \setminus O$

We know $|O| = |I| \leq q_2 + q_3$, we would also like to have upper bounds for $|B_1|, |B_2|, \cdots, |B_7|$.

1. By Lemma 1, $|B_1| \leq |O| \leq q_2 + q_3$. Also, $|B_2| \leq |LB(M\|m)| \leq 2$
2. We partition I as $I_1 \cup I_2 \cup \cdots$ depending on the first r bits. Now, $a, b \in I_j$ implies $FH(a) = FH(b)$.
   Now,
$$\begin{aligned}|B_3| &= |\{z \in \{0,1\}^s : FH(y\|z) \oplus i_1 = m, LH(y\|z) \oplus i_2 \in LB(M\|m) \text{ for some } i_1\|i_2 \in I\}| \\ &= \sum_j |\{z \in \{0,1\}^s : FH(y\|z) \oplus i_1 = m, LH(y\|z) \oplus i_2 \in LB(M\|m) \text{ for some } i_1\|i_2 \in I_j\}| \\ &\leq \sum_j |I_j| \times |LB(M\|m)| \leq 2|I| \leq 2(q_2 + q_3)\end{aligned}$$
3. $|B_4| \leq 1$ and $|B_5| \leq |I| \leq (q_2 + q_3)$
4. We partition I as before. Now,
$$\begin{aligned}|B_6| &= |\{z \in \{0,1\}^s : FH(y\|z) \oplus i_1 = m, LH(y\|z) \oplus i_2 = FH(e(i_1\|i_2)) \oplus x_1 \text{ for some } i_1\|i_2 \in I\}| \\ &= \sum_j |\{z \in \{0,1\}^s : FH(y\|z) \oplus i_1 = m, LH(y\|z) \oplus i_2 = FH(e(i_1\|i_2)) \oplus x_1 \text{ for some } i_1\|i_2 \in I_j\}| \\ &\leq \sum |I_j| = |I| \leq (q_2 + q_3)\end{aligned}$$
5. We partition I as before. Now,
$$\begin{aligned}|B_7| &= |\{z \in \{0,1\}^s : FH(y\|z) \oplus i_1 = m, LH(y\|z) \oplus i_2 = FH(e(i_1\|i_2) \oplus i_1' \text{ for some} \\ &\qquad i_1\|i_2, i_1'\|i_2' \in I\}| \\ &= \sum_j |\{z \in \{0,1\}^s : FH(y\|z) \oplus i_1 = m, LH(y\|z) \oplus i_2 = FH(e(i_1\|i_2) \oplus i_1' \text{ for some} \\ &\qquad i_1\|i_2 \in I_j, i_1'\|i_2' \in I\}| \leq \sum_j |I_j| \times |I| = |I|^2 \leq (q_2 + q_3)^2\end{aligned}$$

Hence all together we have

$$|B_1 \cup B_2 \cup \cdots \cup B_3| \leq (q_2 + q_3)^2 + 5(q_2 + q_3) + 3 \leq (q_2 + q_3 + 3)^2.$$

So, when $(q_2 + q_3 + 3)^2 < 2^s$ for any $y\|w \in \{0,1\}^{2n}$ we have,

$$\Pr[S^R(+,\cdot,\cdot) \text{ query outputs } y\|w] \leq \max\left(\frac{1}{2^{2n-s}} \frac{1}{2^s - (q_2 + q_3 + 3)^2}, \frac{1}{2^{2n} - (q_2 + q_3)}\right) \leq \frac{1}{2^{2n}} \frac{1}{1 - \frac{(q_2+q_3+3)^2}{2^s}}$$

For $S^R(-,\cdot,\cdot)$ query giving output as $z_1\|z_2$, we know

- $_1$ is uniformly distributed over $\{0,1\}^n \setminus C$
- $_2$ is uniformly distributed over $\{0,1\}^n \setminus \{w \in \{0,1\}^n : z_1\|w \in I\}$

Initially size of C is 1 and during each query, by size of C can grow by atmost $|I| + 1$ amount. Hence we have,

$$|C| \leq (q_2 + q_3)^2.$$

Also, by Lemma 1 we know,

$$|\{w \in \{0,1\}^n : z_1\|w \in I\}| \leq |I| \leq q_2 + q_3.$$

So, when $(q_2 + q_3)^2 \leq 2^n$ for any $z_1\|z_2 \in \{0,1\}^{2n}$ we have,

$$\Pr[S^R(-,\cdot,\cdot) \text{ query outputs } z_1\|z_2] \leq \frac{1}{2^n - (q_2 + q_3)^2} \frac{1}{2^n - (q_2 + q_3)} \leq \frac{1}{2^{2n}} \frac{1}{1 - \frac{(q_2+q_3+1)^2}{2^n}}$$

Hence, all together we have

$$\Pr[\mathcal{OV}^{\mathcal{A}}_{R,S^R} = \mathcal{OV}] \leq \frac{1}{2^{(2n-s)q_1 + 2n(q_2+q_3)}} \times \frac{1}{(1 - \frac{(q_2+q_3+3)^2}{2^s})^{q_2}} \times \frac{1}{(1 - \frac{(q_2+q_3+1)^2}{2^n})^{q_3}}.$$

□

D P0 r o o f o f T

To prove the theorem we need an analog of Theorem 15 when chopping is done on the rightmost (most significant) bits. We define the notion of CHOPR-matching in exact same way as of CHOPL-matching defined in Definition 16. Let $M_{\mathcal{V}}$ be the set of all such CHOPR-matching MD-irreducible tuples. Now we have the following theorem

T h e o r e m 1 6

$$\mathcal{V} = ((M_1\|m_1, h_1), \ldots, (M_{q_1}\|m_{q_1}, h_{q_1}), (x_1^1, x_1^2, y_1^1, y_1^2), \ldots, (x_{q_2+q_3}^1, x_{q_2+q_3}^2, y_{q_2+q_3}^1, y_{q_2+q_3}^2))$$

w e h a v e ,

$$|M_{\mathcal{V}}| \geq 2^{sq_1} \times (1 - \frac{2\sigma q_1(q_1+q_2+q_3)}{2^s}).$$

P r o o f . By Lemma 1, we know

$$\begin{aligned}&|\{z \in \{0,1\}^s : h_1\|z \oplus (m_1\|0^n) \in \{y_1^1\|y_1^2, \ldots, y_{q_2+q_3}^1\|y_{q_2+q_3}^2\}\}| \\ &= |\{z \in \{0,1\}^s : h_1\|z \in \{y_1^1\|y_1^2 \oplus (m_1\|0^n), \ldots, y_{q_2+q_3}^1\|y_{q_2+q_3}^2 \oplus (m_1\|0^n)\}\}| \leq q_2+q_3\end{aligned}$$

Also, we would like to have an upper bound for

$$|\{z \in \{0,1\}^s : h_1\|z \oplus 0^n\|m \in \{x_1^1\|x_1^2, \ldots, x_{q_2+q_3}^1\|x_{q_2+q_3}^2, IV_1\|IV_2\} \textit{ for some } m \in \Sigma\}|$$

Consider the case when $s \geq n$. We partition $\{x_1^1\|x_1^2, \ldots, x_{q_2+q_3}^1\|x_{q_2+q_3}^2, IV_1\|IV_2\}$ as $S_1 \cup S_2 \cup \cdots$ such that for any $a, b \in \{x_1^1\|x_1^2, \ldots, x_{q_2+q_3}^1\|x_{q_2+q_3}^2, IV_1\|IV_2\}$, a and b goes to the same partition (i.e. $a, b \in S_i$) iff $FH(a) = FH(b)$. Clearly,

$$\sum |S_i| = (q_2+q_3+1).$$

Hence,

$$\begin{aligned}&|\{z \in \{0,1\}^s : h_1\|z \oplus 0^n\|m \in \{x_1^1\|x_1^2, \ldots, x_{q_2+q_3}^1\|x_{q_2+q_3}^2, IV_1\|IV_2\} \textit{ for some } m \in \Sigma\}| \\ &= \sum_i |\{z \in \{0,1\}^s : h_1\|z \oplus 0^n\|m \in S_i \textit{ for some } m \in \Sigma\}| \leq \sum_i |S_i||\Sigma| \leq (q_2+q_3+1)\sigma\end{aligned}$$

In a similar way, we can also show

$$|\{z \in \{0,1\}^s : h_1\|z \oplus 0^n\|m \in \{x_1^1\|x_1^2, \ldots, x_{q_2+q_3}^1\|x_{q_2+q_3}^2, IV_1\|IV_2\} \textit{ for some } m \in \Sigma\}| \leq (q_2+q_3+1)\sigma$$

when $s < n$. Hence, there are at least $(2^s - (q_2+q_3+(q_2+q_3+1)\sigma))$ many possible values for w_1. Once w_1 is selected there are at least $(2^s - (q_2+q_3+(q_2+q_3+1)\sigma+1))$ choices for w_2 and so on.Hence,

$$\begin{aligned}|M_{\mathcal{V}}| = &\ \textit{Number of valid } w \textit{ tuples} \\ &\geq (2^s - (q_2+q_3+(q_2+q_3+1)\sigma)) \ldots (2^s - (q_2+q_3+(q_2+q_3+1)\sigma+q_1-1)) \\ &\geq 2^{sq_1} \times (1 - \frac{2\sigma q_1(q_1+q_2+q_3)}{2^s})\end{aligned}$$

□

The rest follows similar to proof of Theorem 5.

E P r o o f o f T

When $\mathcal{A}$ interacts with (JH^π, π) it always returns 0. Now, we will see when $\mathcal{A}$ interacts with $(\mathcal{R}, \mathcal{S}^{\mathcal{R}})$ it returns 1 with probability at least $1 - \frac{2k+1}{2^n}$. As simulators running time is bounded by some polynomial in n, the distinguisher succeeds with overwhelming probability.

Clearly, to work against the above distinguisher, the simulator has to output $\mathcal{R}(M\|z_2) \oplus z_2$ for the first query. In order to do so the simulator either has to find M from h or "guess" the value of $\mathcal{R}(M\|z_2)$. $\mathcal{R}$, being a Random Function, is preimage resistant and collision resistant. So given the information $R(M) = h$, the probability that the simulator finds M is $O(\frac{k}{2^n})$. Hence, if $\mathcal{B}$ is the event, that the simulator does not make the query $\mathcal{R}(M\|*)$ before answering the first query then we have

$$\Pr[\mathcal{B}] \geq 1 - \frac{k}{2^n}.$$

Now, let $\mathcal{C}$ be the event that the simulator made some $R(M\|z)$ query and received $t_1 + z$ as output, before answering second $\mathcal{O}_2$ query. $\mathcal{R}$ being a Random Function again we have,

$$\Pr[C|B] \leq \frac{k}{2^n}$$

If the simulator have not made $\mathcal{R}(M\|z_2)$ query while answering first or second $\mathcal{O}_2$ query then

$$\Pr[\mathcal{R}(M\|z_2) = t_1 \oplus z_2] = \frac{1}{2^n}.$$

So, we have

$$\mathsf{Adv}_{\mathcal{A}} \geq 1 - \frac{k}{2^n} - \frac{k}{2^n} - \frac{1}{2^n} = 1 - \frac{2k+1}{2^n}.$$

□

F Proof of Theorem 2

If there exists a simulator S against which $\mathcal{A}(k)$ has negligible advantage with $k = \Omega(2^{n/2})$, then the simulator must output a collision among $(y_1^1 \oplus m_1), \ldots, (y_k^1 \oplus m_k)$ with non-negligible probability. But the simulator also should find $y_{j_1}^2$ and $y_{j_2}^2$ such that the relation

$$R(m_{j_1}\|(m \oplus y_{j_1}^2)) \oplus \textsc{Chop}((m \oplus y_{j_1}^2)\|0^n) = R(m_{j_2}\|(m \oplus y_{j_2}^2)) \oplus \textsc{Chop}((m \oplus y_{j_2}^2)\|0^n)$$

holds with non negligible probability for $m \in_R \{0,1\}^n$. But R being a Random Oracle clearly that is not possible. □