Provable Security of the Knudsen-Preneel Compression Functions

Jooyoung Lee[⋆]

Faculty of Mathematics and Statistics
Sejong University, Seoul, Korea 143-747
jlee05@sejong.ac.kr

Abstract. This paper discusses the provable security of the compression functions introduced by Knudsen and Preneel [11,12,13] that use linear error-correcting codes to build wide-pipe compression functions from underlying blockciphers operating in Davies-Meyer mode. In the information theoretic model, we prove that the Knudsen-Preneel compression function based on an $[r, k, d]_{2^e}$ code is collision resistant up to $2^{\frac{(r-d+1)n}{2r-3d+3}}$ query complexity if $2d \leq r + 1$ and collision resistant up to $2^{\frac{rn}{2r-2d+2}}$ query complexity if $2d > r + 1$. For MDS code based Knudsen-Preneel compression functions, this lower bound matches the upper bound recently given by Özen and Stam [23].

A preimage security proof of the Knudsen-Preneel compression functions has been first presented by Özen et al. (FSE '10). In this paper, we present two alternative proofs that the Knudsen-Preneel compression functions are preimage resistant up to $2^{\frac{rn}{k}}$ query complexity. While the first proof, using a wish list argument, is presented primarily to illustrate an idea behind our collision security proof, the second proof provides a tighter security bound compared to the original one.

1 Introduction

A cryptographic hash function takes a message of arbitrary length, and returns a bit string of fixed length. The most common way of hashing variable length messages is to iterate a fixed-size compression function (e.g. according to the Merkle-Damgård paradigm [7,20]). The underlying compression function can either be constructed from scratch, or be built upon off-the-shelf cryptographic primitives such as blockciphers. Recently, blockcipher-based constructions have attracted renewed interest as many dedicated hash functions, including those most common in practical applications, have started to exhibit serious security weaknesses [2,6,18,19,29,34,35,36]. By instantiating a blockcipher-based construction with an extensively studied (and fully trusted) blockcipher, one can conveniently transfer the trust in the existing blockcipher to the hash function.

[⋆] The work of J. Lee was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education, Science and Technology(2012-0003157).

X. Wang and K. Sako (Eds.): ASIACRYPT 2012, LNCS 7658, pp. 504–525, 2012.

Compression functions based on blockciphers have been widely studied [3,4,9,10,14,22,25,26,27,28,30,31,32,33]. The most common approach is to construct a $2n$-to-n bit compression function using a single call to an n-bit blockcipher. However, such a function, called a *single-block-length* (SBL) compression function, might be vulnerable to collision attacks due to its short output length. For example, one could successfully mount a birthday attack on a compression function based on AES-128 using approximately 2^{64} queries. This observation motivated substantial research on constructions whose output size is larger than the block length of the underlying blockcipher(s). A typical approach has been to construct *double-block-length* (DBL) hash functions, where the output length is twice the block length of the underlying blockcipher(s). Since the 1990s various double-block-length constructions have been proposed mostly without formal security proofs. Those constructions were mainly focused on optimizing their efficiency in terms of the rate, while only recently have a few double-block-length constructions been supported by rigorous security proofs [8,15,17,24].

The Knudsen-Preneel compression functions. On the other hand, Knudsen and Preneel [11,12,13] adopted a different approach, aiming at achieving a particular level of security using a given number of ideal compression functions as building blocks. Specifically, they used r independent cn-to-n bit random functions to build the entire compression function producing rn-bit outputs. The parameter c is typically two or three so that the inner primitives can be constructed from n-bit key or $2n$-bit key blockciphers operating in Davies-Meyer mode. The main idea of Knudsen and Preneel's approach lies in the method of deriving the inputs to the inner primitives from the input to the entire compression function. They used an $[r, k, d]$ linear error-correcting code over a finite field in a way that its generator matrix extends a kcn-bit input to the entire compression function to an rcn-bit string. This string is parsed into r blocks of the same size, and the blocks go into the inner primitives in parallel. The output of the entire compression function is the concatenation of the n-bit outputs obtained from the r inner primitives. This Knudsen-Preneel (KP) compression function is fed to the Merkle-Damgård transform, producing the final output via a random finalization function whose output size might depend on the security target.

Due to the property of linear codes of minimum distance d, two different inputs to the KP compression function determine two sets of inputs to the inner primitives that are different at least at d positions. Based on this observation, Knudsen and Preneel made a certain plausible security assumption (see [11, Section 5]) which was used for their security proof that the KP compression function is collision resistant up to $2^{\frac{(d-1)n}{2}}$ query complexity. They also expected that the KP compression function would be preimage resistant up to $2^{(d-1)n}$ query complexity. In order to maximize the query complexity, Knudsen and Preneel suggested the use of MDS codes satisfying $d = r - k + 1$.

Attack history. For KP compression functions based on an MDS code, the designers described preimage attacks matching their security conjecture, while their collision attacks were far from tight for many of the parameter sets.

Afterwards Watanabe [37] proposed a collision attack beating the original conjecture for many cases. In particular, for $2k > r$ and $d \leq k$, one could find a collision with $k2^n$ query complexity.

Özen, Shrimpton and Stam [21] presented a preimage attack of $2^{\frac{rn}{k}}$ query complexity, far less than the bound of $2^{(d-1)n}$ that was originally conjectured by the designers. By giving a preimage security proof, they proved that their attack is tight. Their result also implies that one could expect a collision with about $2^{\frac{rn}{2k}}$ queries.

Subsequently, Özen and Stam [23] presented new collision attacks using the ideas of Watanabe and the preimage attack of Özen, Shrimpton and Stam. For $2k > r$ and $d \leq k$, their attacks require $2^{\frac{kn}{3k-r}}$ query complexity. This implies that the KP compression functions do not achieve the security level they were originally designed for. On the other hand, tightness of their attack remained a open question.

1.1 Our Contribution

In this paper, we prove that the KP compression function based on an $[r, k, d]_{2^e}$ code is collision resistant up to $2^{\frac{(r-d+1)n}{2r-3d+3}}$ query complexity if $2d \leq r + 1$ and collision resistant up to $2^{\frac{rn}{2r-2d+2}}$ query complexity if $2d > r + 1$. For KP compression functions based on an MDS code, this lower bound, simplified to $2^{\frac{kn}{3k-r}}$ for $2d \leq r+1$ and $2^{\frac{rn}{2k}}$ for $2d > r+1$ respectively, matches the upper bound given by [21,23]. For two parameter sets $[4, 2, 3]_8$ and $[5, 2, 4]_8$ such that $2d > r + 1$, the collision security is proved up to the query complexity equal to or beyond the block-size of the underlying blockciphers.

Özen, Shrimpton and Stam [21] proved that the preimage finding advantage of a q-query adversary is not greater than

$$\epsilon_1(r, k) = \frac{q^{\frac{(r-k)k}{r}}}{2^{(r-k)n}} + \left(\frac{eq^{\frac{k}{r}}}{2^n}\right)^{kq^{\frac{(r-k)}{r}}},$$

where we set $\delta = \frac{r(k-1)-k^2}{r}$ in Theorem 10 of [21]. The upper bound $\epsilon_1(r, k)$ becomes negligible as q gets much smaller than $2^{\frac{rn}{k}}$. In this paper, we present two alternative preimage security proofs, where the second proof provides a tighter security bound compared to the original one. Specifically, the preimage finding advantage of a q-query adversary is upper bounded by

$$\epsilon_2(r, k) = \binom{r}{k}\frac{q^k}{2^{rn}}.$$

Our upper bound $\epsilon_2(r, k)$ is significantly smaller than $\epsilon_1(r, k)$ since $\epsilon_2(r, k) \leq \binom{r}{k}\epsilon_1(r, k)^{1+\frac{k}{r-k}}$. For example, for a $[5, 3, 3]_4$ code based KP compression function, we have $\epsilon_1(r, k) \geq \frac{q^{6/5}}{2^{2n}}$ while $\epsilon_2(r, k) = \frac{10q^3}{2^{5n}}$.

Our first preimage security proof, using a wish-list argument, is presented primarily to illustrate an idea behind our collision security proof. This proof is

Table 1. Provable security of Knudsen-Preneel constructions. Non-MDS parameters in italic. The parameter sets satisfying $r + 1 > 2k$ are $[4, 2, 3]_8$ and $[5, 2, 4]_8$.

$[\mathbf{r}, \mathbf{k}, \mathbf{d}]_{\mathbf{2^e}}$-Code	**Basing Primitive**	**Compression Function**	**Collision Resistance**			**Preimage Resistance**	
			Attack [23	**Security**	**Tightness**	**Attack** [21	**Security**
$[5, 3, 3]_4$	$2n \to n$	$(5 + 1)n \to 5n$	$2^{3n/4}$	$\boldsymbol{2^{3n/4}}$	√	$2^{5n/3}$	$\boldsymbol{2^{5n/3}}$
$[\mathit{8, 5, 3}]_{\mathit{4}}$		$(8 + 2)n \to 8n$	$2^{5n/7}$	$\boldsymbol{2^{3n/5}}$		$2^{8n/5}$	$\boldsymbol{2^{8n/5}}$
$[\mathit{12, 9, 3}]_{\mathit{4}}$		$(12 + 6)n \to 12n$	$2^{3n/5}$	$\boldsymbol{2^{5n/9}}$		$2^{4n/3}$	$\boldsymbol{2^{4n/3}}$
$[\mathit{9, 5, 4}]_{\mathit{4}}$		$(9 + 1)n \to 9n$	$2^{5n/6}$	$\boldsymbol{2^{2n/3}}$		$2^{9n/5}$	$\boldsymbol{2^{9n/5}}$
$[\mathit{16, 12, 4}]_{\mathit{4}}$		$(16 + 8)n \to 16n$	$2^{3n/5}$	$\boldsymbol{2^{13n/23}}$		$2^{4n/3}$	$\boldsymbol{2^{4n/3}}$
$[6, 4, 3]_{16}$	$2n \to n$	$(6 + 2)n \to 6n$	$2^{2n/3}$	$\boldsymbol{2^{2n/3}}$	√	$2^{3n/2}$	$\boldsymbol{2^{3n/2}}$
$[8, 6, 3]_{16}$		$(8 + 4)n \to 8n$	$2^{3n/5}$	$\boldsymbol{2^{3n/5}}$	√	$2^{4n/3}$	$\boldsymbol{2^{4n/3}}$
$[12, 10, 3]_{16}$		$(12 + 8)n \to 12n$	$2^{5n/9}$	$\boldsymbol{2^{5n/9}}$	√	$2^{6n/5}$	$\boldsymbol{2^{6n/5}}$
$[9, 6, 4]_{16}$		$(9 + 3)n \to 9n$	$2^{2n/3}$	$\boldsymbol{2^{2n/3}}$	√	$2^{3n/2}$	$\boldsymbol{2^{3n/2}}$
$[16, 13, 4]_{16}$		$(16+10)n \to 16n$	$2^{13n/23}$	$\boldsymbol{2^{13n/23}}$	√	$2^{16n/13}$	$\boldsymbol{2^{16n/13}}$
$[4, 2, 3]_8$	$3n \to n$	$(4 + 2)n \to 4n$	2^n [21]	$\boldsymbol{2^{n}}$	√	2^{2n}	$\boldsymbol{2^{2n}}$
$[6, 4, 3]_8$		$(6 + 6)n \to 6n$	$2^{2n/3}$	$\boldsymbol{2^{2n/3}}$	√	$2^{3n/2}$	$\boldsymbol{2^{3n/2}}$
$[9, 7, 3]_8$		$(9 + 12)n \to 9n$	$2^{7n/12}$	$\boldsymbol{2^{7n/12}}$	√	$2^{9n/7}$	$\boldsymbol{2^{9n/7}}$
$[5, 2, 4]_8$		$(5 + 1)n \to 5n$	$2^{5n/4}$ [21]	$\boldsymbol{2^{5n/4}}$	√	$2^{5n/2}$	$\boldsymbol{2^{5n/2}}$
$[7, 4, 4]_8$		$(7 + 5)n \to 7n$	$2^{4n/5}$	$\boldsymbol{2^{4n/5}}$	√	$2^{7n/4}$	$\boldsymbol{2^{7n/4}}$
$[10, 7, 4]_8$		$(10+11)n \to 10n$	$2^{7n/11}$	$\boldsymbol{2^{7n/11}}$	√	$2^{10n/7}$	$\boldsymbol{2^{10n/7}}$

tight only for the parameter sets of MDS codes. Table 1 summarizes these results for 16 parameter sets proposed by the original designers.

Wish list argument. In the information-theoretic model, the most typical approach for a security proof has been upper bounding the probability that a single query of an adversary achieves a certain security goal (such as finding a collision or finding a preimage of a target image). The upper bound of the total adversarial advantage is obtained by multiplying this upper bound by the number of queries allowed to the adversary. Most single-block-length constructions can be analyzed in this way [25].

However, certain constructions might not allow an upper bound small enough to uniformly apply to all the queries. One of the techniques to address this difficulty is to define a certain bad event that happens with only small probability, and prove that it is hard for a single query to achieve an adversarial goal without the occurrence of the bad event. This approach was adopted in the collision security proof of MDC-2 and MJH hash functions [16,24] as well as the preimage security proof of the KP compression functions [21].

Another technique is to cleverly modify the adversary: the modified adversary, typically using the original adversary as a subroutine, is given slightly more power than the original one. So the success probability of the modified adversary is not reduced, while it becomes much easier to upper bound. With this approach, one can prove the security of Abreast-DM and Tandem-DM hash functions [8,15,17]. Our second alternative preimage security proof of the KP compression functions also follows this approach.

As yet another technique, one might use an observation that a security goal is usually achieved by a group of queries and the last query that achieves the goal is uniquely determined by the previous queries in the group. We assume, once a new query is obtained, the adversary computes a query that might become the last winning query along with a certain group of existing queries (including the new query). If this query has not been asked, the adversary includes it in a wish list expecting this wish is accomplished sometime later. If we have upper bounds on the size of the wish list (hopefully smaller than the total number of queries) and the probability that each wish in the list is accomplished, the total adversarial advantage can be obtained by a union bound. This technique, called a *wish list argument*, was first used in the preimage security proof of certain double-length blockcipher-based compression functions [1]. This work is the first application of a wish list argument to a collision security proof (combined with a bad event argument). In our extension, each wish is typically given as a set of unasked queries, rather than a single query.

Efficiency. Unfortunately, for most of the parameter sets, the KP compression functions do not provide collision security beyond the block-size of the underlying blockcipher. However, from a practical point of view, some of the KP compression functions are still comparable to the existing blockcipher-based hash functions such as MDC-2, Abreast-DM and Tandem-DM in terms of efficiency and probable security.

In MDC-2, compression of a single n-bit message block requires two calls to the underlying n-bit key blockcipher, and it enjoys a $\frac{3n}{5}$-bit collision security proof. This construction is comparable to the KP compression functions using $[12,9,3]_4$, $[16,12,4]_4$ or $[8,6,3]_{16}$ codes: they are all of rate $\frac{1}{2}$ using $2n$-to-n bit primitives (or equivalently n-bit key blockciphers), and supported by a $\frac{3n}{5}$-bit security proof.

The compression function $H = \mathsf{KP}^1([6,4,3]_8)$ using $3n$-to-n bit primitives (or equivalently $2n$-bit key blockciphers) is supported by a $\frac{2n}{3}$-bit security proof. This construction has the same rate and the same provable security as MJH [16] using a $2n$-bit key blockcipher.

The compression function $H = \mathsf{KP}^1([4,2,3]_8)$ using $3n$-to-n bit primitives (or equivalently $2n$-bit key blockciphers) is supported by an n-bit security proof. This construction is comparable to Abreast-DM and Tandem-DM, both of which are of rate $\frac{1}{2}$ using a $2n$-bit key blockcipher. We also refer to [5] for comparison of this compression function with the other existing schemes in terms of AES driven implementations.

The compression function $H = \mathsf{KP}^1([5,2,4]_8)$ is relatively slow with rate $\frac{1}{5}$, while this is the first construction that enjoys the provable collision security beyond the block-size of the underlying blockciphers. However it remains open whether this KP compression function is still secure when the inner primitives are instantiated with $2n$-bit key n-bit blockciphers, since in general an n-bit blockcipher loses its randomness beyond 2^n queries (for a fixed key). The other open question raised here is the provable security of KP constructions where all the inner primitives are instantiated the same.

2 Preliminaries

2.1 The Knudsen-Preneel Compression Functions

An $[r, k, d]_{2^e}$ linear error-correcting code $\mathcal{C}$ is a k-dimensional subspace of $\mathbb{F}_{2^e}^r$, where $\mathbb{F}_{2^e}$ denotes a finite field of order 2^e. An $[r, k, d]_{2^e}$ code $\mathcal{C}$ can be represented by a $k \times r$ generator matrix G over $\mathbb{F}_{2^e}$ where every codeword of $\mathcal{C}$ is expressed as a linear combination of the row vectors of G, namely $w \cdot G$ for some $w \in \mathbb{F}_{2^e}^k$. Obviously, $k \le r$, and the Singleton bound states that

$$d \le r - k + 1.$$

When a code meets the equality of the Singleton bound, it is called *maximum distance separable* (MDS). As an important property of MDS codes, any k columns of a generator matrix of an MDS code are linearly independent.

Let $\mathbb{F}_{2^e} = \mathbb{F}(\omega)$ be an extension of $\mathbb{F}_2$ generated by the root ω of a primitive polynomial $p(x)$ of degree e, and let $\mathbb{F}_2^e$ be an e-dimensional vector space over $\mathbb{F}_2$. In order to clearly define the Knudsen-Preneel compression functions, we need to identify $\mathbb{F}_{2^e}$ and $\mathbb{F}_2^e$ by a group isomorphism $\psi : \mathbb{F}_{2^e} \to \mathbb{F}_2^e$ such that

$$\psi(a_{e-1}\omega^{e-1} + \cdots + a_1\omega + a_0) = (a_{e-1}, \ldots, a_1, a_0)^T.$$

For each $g \in \mathbb{F}_{2^e}$, consider a map

$$\begin{aligned} \Phi(g) : \mathbb{F}_2^e &\longrightarrow \mathbb{F}_2^e \\ u &\longmapsto \psi(g \cdot \psi^{-1}(u)), \end{aligned}$$

where "$\cdot$" denotes the field multiplication of $\mathbb{F}_{2^e}$. This is a linear map, so it is associated with an $e \times e$ matrix over $\mathbb{F}_2$ with respect to the standard basis. We will denote this matrix as $\phi(g)$. Since for every $g, h \in \mathbb{F}_{2^e}$,

1. $\Phi(g + h) = \Phi(g) + \Phi(h)$,
2. $\Phi(gh) = \Phi(g) \circ \Phi(h)$,

we also have $\phi(g + h) = \phi(g) + \phi(h)$ and $\phi(gh) = \phi(g)\phi(h)$ for all $g, h \in \mathbb{F}_{2^e}$. This implies the map $\phi : \mathbb{F}_{2^e} \to \mathbb{F}_2^{e \times e}$ is a ring homomorphism.

Suppose that $\phi(g)$ is the identity matrix, or equivalently $\Phi(g)$ is the identity map. Since this implies $g \cdot \psi^{-1}(u) = \psi^{-1}(u)$ for every $u \in \mathbb{F}_2^e$, g should be the multiplicative identity of $\mathbb{F}_{2^e}$. This implies again that ϕ is injective.

This injective ring homomorphism naturally extends to $\bar{\phi} : \mathbb{F}_{2^e}^{r \times k} \to \mathbb{F}_2^{re \times ke}$ where ϕ is applied to each component and then $(\mathbb{F}_2^{e \times e})^{r \times k}$ is identified with $\mathbb{F}_2^{re \times ke}$. Now we are ready to define the Knudsen-Preneel compression functions.

Definition 1. *Let $\mathcal{C}$ be an $[r,k,d]_{2^e}$ linear code with a generator matrix $G \in \mathbb{F}_{2^e}^{k\times r}$ and let $\phi : \mathbb{F}_{2^e} \to \mathbb{F}_2^{e\times e}$ be the injective ring homomorphism defined above. Let $e = bc$ and $n = bn'$ for some positive integers b, c, n, n', and let $ek > rb$. Then the Knudsen-Preneel compression function*

$$H = \mathsf{KP}^b([r,k,d]_{2^e}) : \{0,1\}^{kcn} \to \{0,1\}^{rn}$$

making oracle queries to public random functions $f_l : \{0,1\}^{cn} \to \{0,1\}^n$, $l = 1,\dots,r$, computes $H(W)$ for $W \in \{0,1\}^{kcn}$ as follows.

1. *Compute $X \leftarrow (\bar{\phi}(G^T) \otimes I_{n'}) \cdot W$.*
2. *Parse $X = (x_1,\dots,x_r)$, where $x_1,\dots,x_r \in \{0,1\}^{cn}$.*
3. *Make oracle queries $y_l = f_l(x_l)$ for $l = 1,\dots,r$, and output the digest $Z = y_1||\cdots||y_r$.*

Here $\otimes$ denotes the Kronecher product and $I_{n'}$ the identity matrix in $\mathbb{F}_2^{n'\times n'}$.

Example 1. The above mathematical description of Knudsen-Preneel constructions looks complicated, while the constructions themselves are very simple. For example, let $e = 2$ and let $\mathbb{F}_{2^2} = \mathbb{F}(\omega)$ for a root ω satisfying $\omega^2 + \omega + 1 = 0$. For $a_1\omega + a_0 \in \mathbb{F}_{2^2}$,

$$\omega(a_1\omega + a_0) = (a_0 + a_1)\omega + a_1.$$

This implies $\phi(\omega) = \begin{bmatrix} 1\,1 \\ 1\,0 \end{bmatrix}$. Since ϕ is an injective ring homomorphism,

$$\phi(0) = \begin{bmatrix} 0\,0 \\ 0\,0 \end{bmatrix}, \quad \phi(1) = \begin{bmatrix} 1\,0 \\ 0\,1 \end{bmatrix}, \quad \phi(\omega) = \begin{bmatrix} 1\,1 \\ 1\,0 \end{bmatrix}, \quad \phi(\omega+1) = \phi(\omega)+\phi(1) = \begin{bmatrix} 0\,1 \\ 1\,1 \end{bmatrix}.$$

Let $\mathcal{C}$ be a $[5,3,3]_4$ linear code with a generator matrix $G = \begin{bmatrix} 1\,0\,0\,1 & 1 \\ 0\,1\,0\,1 & \omega \\ 0\,0\,1\,1 & \omega+1 \end{bmatrix}$. If $c = 2$, then $b = 1$, $n = n'$ and

$$\bar{\phi}(G^T) = \left[\begin{array}{c|c|c|c|c} 1\,0 & 0\,0 & 0\,0 & 1\,0 & 1\,0 \\ 0\,1 & 0\,0 & 0\,0 & 0\,1 & 0\,1 \\ \hline 0\,0 & 1\,0 & 0\,0 & 1\,0 & 1\,1 \\ 0\,0 & 0\,1 & 0\,0 & 0\,1 & 1\,0 \\ \hline 0\,0 & 0\,0 & 1\,0 & 1\,0 & 0\,1 \\ 0\,0 & 0\,0 & 0\,1 & 0\,1 & 1\,1 \end{array}\right]^T.$$

Let $H : \{0,1\}^{6n} \to \{0,1\}^{5n}$ be the resulting KP compression function using five public random functions $f_l : \{0,1\}^{2n} \to \{0,1\}^n$, $l = 1,\dots,5$. Then for $W = \omega_1||\cdots||\omega_6$,

$$H(W) = f_1(x_1)||\cdots||f_5(x_5),$$

where $x_1 = (\omega_1||\omega_2)$, $x_2 = (\omega_3||\omega_4)$, $x_3 = (\omega_5||\omega_6)$, $x_4 = (\omega_1 \oplus \omega_3 \oplus \omega_5||\omega_2 \oplus \omega_4 \oplus \omega_6)$, $x_5 = (\omega_1 \oplus \omega_3 \oplus \omega_4 \oplus \omega_6||\omega_2 \oplus \omega_3 \oplus \omega_5 \oplus \omega_6)$.

Throughout this work, we will simply write $\mathcal{C}^{PRE}(W) = (\bar{\phi}(G^T) \otimes I_{n'}) \cdot W$. For the security analysis of H, we need to state some properties of $\mathcal{C}^{PRE}$.

Definition 2. *Let $\mathcal{I} \subset [1,r]$ and let $(x_l^*)_{l\in\mathcal{I}} \in \prod_{l\in\mathcal{I}}\{0,1\}^{cn}$. $(x_1,\ldots,x_r) \in (\{0,1\}^{cn})^r$ is called an* extension *of $(x_l^*)_{l\in\mathcal{I}}$ if there exists an input $W \in \{0,1\}^{kcn}$ such that $\mathcal{C}^{PRE}(W) = (x_1,\ldots,x_r)$ and $x_l = x_l^*$ for $l \in \mathcal{I}$. We will say $(x_l^*)_{l\in\mathcal{I}}$ is* valid *if it has an extension.*[1]

For $\mathcal{I} = [1,r]$, valid tuples are exactly the images of $\mathcal{C}^{PRE}$. Due to the linearity of $\mathcal{C}^{PRE}$ (with respect to bitwise xor "$\oplus$"), we have the following property.

Property 1. *If $(x_l)_{l\in\mathcal{I}}$ and $(x'_l)_{l\in\mathcal{I}}$ are valid, then $(x_l \oplus x'_l)_{l\in\mathcal{I}}$ is also valid.*

Property 2. *Let $\mathcal{I}$ be a subset of $[1,r]$ such that $|\mathcal{I}| = r - d + 1$. If $(x_l^*)_{l\in\mathcal{I}} \in \prod_{l\in\mathcal{I}}\{0,1\}^{cn}$ is valid, then it has a unique extension.*

Proof. Suppose that $(x_1,\ldots,x_r)$, and $(x'_1,\ldots,x'_r)$ are extensions of $(x_l^*)_{l\in\mathcal{I}}$. Then $(x_1 \oplus x'_1,\ldots,x_r \oplus x'_r)$ is also an extension of $(0)_{l\in\mathcal{I}}$. Since any nonzero codeword in $\mathcal{C}$ has at least d nonzero coordinates, we have $(x_1\oplus x'_1,\ldots,x_r\oplus x'_r) = (0,\ldots,0)$, and hence $(x_1,\ldots,x_r) = (x'_1,\ldots,x'_r)$. □

2.2 Collision Resistance and Preimage Resistance

In this section, we review security notions of collision resistance and preimage resistance in an information theoretic sense. In the collision resistance experiment, a computationally unbounded adversary $\mathcal{A}$ makes oracle queries to public random functions f_l, $l = 1,\ldots,r$, and records a *query history* $\mathcal{Q}$, which is initialized as an empty set. When $\mathcal{A}$ makes a new query $f_l(x)$, a query-response pair $(l, x, f_l(x))$ is added to $\mathcal{Q}$.[2] We will loosely write $(l,x) \in \mathcal{Q}$ indicating that the value of $f_l(x)$ has been determined by $\mathcal{A}$'s query. Furthermore, we will denote $\mathcal{A}$'s i-th query as (l^i, x^i), $i = 1,\ldots,q$, indicating the i-th query is $f_{l^i}(x^i)$.

At the end of the collision-finding attack, $\mathcal{A}$ would like to find queries

$$(1, x^{i_1}),\ldots,(r, x^{i_r}),(1, x^{j_1}),\ldots,(r, x^{j_r}) \in \mathcal{Q}$$

satisfying the following two conditions.

1. $(x^{i_1},\ldots,x^{i_r})$ and $(x^{j_1},\ldots,x^{j_r})$ are *distinct* valid tuples.
2. $f_1\left(x^{i_1}\right)||\cdots||f_r\left(x^{i_r}\right) = f_1\left(x^{j_1}\right)||\cdots||f_r\left(x^{j_r}\right)$.

[1] We regard $\prod_{l\in\mathcal{I}}\{0,1\}^{cn}$ as the set of all functions from $\mathcal{I}$ to $\{0,1\}^{cn}$. Thus, even in case $|\mathcal{I}| = |\mathcal{I}'|$, $\prod_{l\in\mathcal{I}}\{0,1\}^{cn} \neq \prod_{l\in\mathcal{I}'}\{0,1\}^{cn}$ as long as $\mathcal{I} \neq \mathcal{I}'$. We also naturally identify $(\{0,1\}^{cn})^r$ with $\{0,1\}^{crn}$.

[2] Unless stated otherwise, we will not allow any redundant query.

In this case, $(i_l, j_l)_{l\in[1,r]}$ is called an *index sequence of a collision*. The success probability of $\mathcal{A}$'s finding a collision is denoted by $\mathbf{Adv}_H^{\mathsf{col}}(\mathcal{A})$. The maximum of $\mathbf{Adv}_H^{\mathsf{col}}(\mathcal{A})$ over the adversaries making at most q queries is denoted by $\mathbf{Adv}_H^{\mathsf{col}}(q)$.

In the preimage resistance experiment, $\mathcal{A}$ chooses a target image $Z = z_1||\cdots||z_r$ at the beginning of the attack, where $z_1,\ldots,z_r \in \{0,1\}^n$. After making a certain number of oracle queries to f_l, $l = 1,\ldots,r$, $\mathcal{A}$ would like to find queries

$$(1, x^{i_1}), \ldots, (r, x^{i_r}) \in \mathcal{Q}$$

such that $f_1\left(x^{i_1}\right)||\cdots||f_r\left(x^{i_r}\right) = z_1||\cdots||z_r$. The success probability of $\mathcal{A}$'s finding a preimage is denoted by $\mathbf{Adv}_H^{\mathsf{pre}}(\mathcal{A})$, and $\mathbf{Adv}_H^{\mathsf{pre}}(q)$ is the maximum of $\mathbf{Adv}_H^{\mathsf{pre}}(\mathcal{A})$ over the adversaries making at most q queries. There might be several definitions of preimage resistance according to the distribution of a target image. The definition described here, called everywhere preimage resistance, is known as the strongest version in the sense that an adversary chooses its target image on its own.

3 Preimage Resistance Proofs

In this section, we will give two preimage resistance proofs of the KP compression functions. In both security proofs, we let $Z = z_1||\cdots||z_r$ be the range point to be inverted where $z_1,\ldots,z_r \in \{0,1\}^n$. When an adversary $\mathcal{A}$ succeeds in finding a preimage of Z, predicate Pre is set to true by definition. So we need to upper bound the probability $\mathbf{Pr}[\mathsf{Pre}]$. Throughout this work, we will write $N = 2^n$.

3.1 The First Alternative Proof

Consider a subset $\mathcal{T} \subset [1,r]$ such that $|\mathcal{T}| = r - d + 1$. With respective to this subset, we define predicate $\mathsf{Pre}_{\mathcal{T}}$, where $\mathsf{Pre}_{\mathcal{T}}$ is true if $\mathcal{A}$ obtains an index sequence of a preimage $D = (i_l)_{l\in[1,r]}$ such that

1. $(l, x^{i_l}) \in \mathcal{Q}$ and $f_l(x^{i_l}) = z_l$ for $l = 1,\ldots,r$,
2. $\max_{l\in\mathcal{T}}\{i_l\} < \min_{l\in[1,r]\setminus\mathcal{T}}\{i_l\}$.

By the second condition, $\mathcal{T}$ specifies the function indices where the first $r-d+1$ partial preimages are determined. More precisely, a partial preimage can be defined as follows.

Definition 3. *Let $\mathcal{T}$ be a subset of $[1,r]$ such that $|\mathcal{T}| = r - d + 1$. A sequence of indices*

$$P = (i_l)_{l\in\mathcal{T}}$$

is called a partial preimage at $\mathcal{T}$ *if $(l, x^{i_l}) \in \mathcal{Q}$ and $f_l(x^{i_l}) = z_l$ for $l \in \mathcal{T}$.*

We will upper bound $\mathbf{Pr}\left[\mathsf{Pre}\right]$ by using the following implication.

$$\begin{aligned}\mathsf{Pre} &\Rightarrow \bigvee_{\substack{\mathcal{T}\subset[1,r]\\|\mathcal{T}|=r-d+1}} \mathsf{Pre}_{\mathcal{T}}\\ &\Rightarrow \mathsf{Bad}(M) \vee \bigvee_{\substack{\mathcal{T}\subset[1,r]\\|\mathcal{T}|=r-d+1}} \left(\neg\mathsf{Bad}(M) \wedge \mathsf{Pre}_{\mathcal{T}}\right), \qquad (1)\end{aligned}$$

where the parameterized predicate $\mathsf{Bad}(M)$, $M > 0$, is true if there exists a subset $\mathcal{T} \subset [1,r]$ of size $r-d+1$ such that the number of partial preimages at $\mathcal{T}$ is greater than M.

In order for a preimage finding adversary $\mathcal{A}$ to set $\mathsf{Pre}_{\mathcal{T}}$ to true, $\mathcal{A}$ has to first complete a partial preimage at $\mathcal{T}$. If $(x^{i_l})_{l\in\mathcal{T}}$ is valid at the point when a partial preimage $P = (i_l)_{l\in\mathcal{T}}$ is completed, then the remaining queries $(x_l)_{l\in[1,r]\backslash\mathcal{T}}$ that might complete a preimage of Z along with $(x^{i_l})_{l\in\mathcal{T}}$ are uniquely determined by Property 2. Specifically, it is required that $f_l(x_l) = z_l$ for $l \in [1,r]\backslash\mathcal{T}$. If any of these evaluations has not been determined, we include $(x_l, z_l)_{l\in[1,r]\backslash\mathcal{T}}$ into a wish list $\mathcal{L}$, expecting all of these evaluations to happen sometime later. A single query might include a multiple number of wishes into $\mathcal{L}$ by completing a multiple number of partial preimages at $\mathcal{T}$. However a single partial preimage at $\mathcal{T}$ is associated with a unique element in $\mathcal{L}$. Therefore the size of $\mathcal{L}$ would be at most M without the occurrence of $\mathsf{Bad}(M)$. Since each wish would be accomplished with probability $1/N^{|[1,r]\backslash\mathcal{T}|} = 1/N^{d-1}$, we have the following upper bound.

$$\mathbf{Pr}\left[\neg\mathsf{Bad}(M) \wedge \mathsf{Pre}_{\mathcal{T}}\right] \le \sum_{i=1}^{M} \mathbf{Pr}\left[\text{the } i\text{-th wish is granted}\right] \le \frac{M}{N^{d-1}}. \qquad (2)$$

In order to address the remaining problem of upper bounding the probability of $\mathsf{Bad}(M)$, we will define a random variable X that counts the number of partial preimages at $\mathcal{T}$, and probabilistically upper bound the value of X using Markov's inequality.

Fix a subset $\mathcal{T} \subset [1,r]$ of size $r-d+1$, and define a random variable X_P for each sequence $P = (i_l)_{l\in\mathcal{T}} \in \prod_{l\in\mathcal{T}}[1,q]$, where $X_P = 1$ if $(l, x^{i_l}) \in \mathcal{Q}$ and $f_l(x^{i_l}) = z_l$ for every $l \in \mathcal{T}$, and $X_P = 0$ otherwise. If we define

$$X = \sum_{P\in\prod_{l\in\mathcal{T}}[1,q]} X_P,$$

then X counts the number of partial preimages at $\mathcal{T}$. Since $\left|\prod_{l\in\mathcal{T}}[1,q]\right| = q^{r-d+1}$ and

$$\mathbf{Pr}[X_P = 1] = \mathsf{Ex}(X_P) \le \frac{1}{N^{r-d+1}},$$

we have $\mathsf{Ex}(X) \le \frac{q^{r-d+1}}{N^{r-d+1}}$. Using Markov's inequality, for $M > 0$ we have

$$\mathbf{Pr}\left[X \ge M\right] \le \frac{q^{r-d+1}}{MN^{r-d+1}}.$$

Applying a union bound over subsets $\mathcal{T} \subset [1, r]$ of size $r - d + 1$, we have

$$\mathbf{Pr}[\mathsf{Bad}(M)] \leq \binom{r}{r-d+1} \frac{q^{r-d+1}}{MN^{r-d+1}} = \binom{r}{d-1} \frac{q^{r-d+1}}{MN^{r-d+1}}. \tag{3}$$

By (1), (2) and (3), we have

$$\mathbf{Pr}[\mathsf{Pre}] \leq \binom{r}{d-1} \frac{q^{r-d+1}}{MN^{r-d+1}} + \binom{r}{d-1} \frac{M}{N^{d-1}}.$$

Let

$$M = \frac{q^{\frac{r-d+1}{2}}}{N^{\frac{r-2d+2}{2}}}$$

by setting $q^{r-d+1}/(MN^{r-d+1}) = M/N^{d-1}$. Then we have

$$\mathbf{Pr}[\mathsf{Pre}] \leq 2\binom{r}{d-1} \frac{q^{\frac{r-d+1}{2}}}{N^{\frac{r}{2}}}.$$

The following theorem summarizes this result.

Theorem 1. *Let H be the Knudsen-Preneel compression function based on an $[r, k, d]_{2^e}$ code. Then we have*

$$\mathbf{Adv}_H^{\mathsf{pre}}(q) \leq 2\binom{r}{d-1} \frac{q^{\frac{r-d+1}{2}}}{N^{\frac{r}{2}}}.$$

For MDS codes, we have

$$\mathbf{Adv}_H^{\mathsf{pre}}(q) \leq 2\binom{r}{k} \frac{q^{\frac{k}{2}}}{N^{\frac{r}{2}}}.$$

Example 2. Let H be based on a $[5, 3, 3]_4$ MDS code. Then Theorem 1 implies

$$\mathbf{Adv}_H^{\mathsf{pre}}(q) \leq \frac{20q^{\frac{3}{2}}}{N^{\frac{5}{2}}}.$$

Therefore H is preimage resistant up to $N^{5/3}$ query complexity.

3.2 The Second Alternative Proof

The main idea of this proof is based on the observation that for any set of r queries to $f_1, \ldots, f_r$ that are in the range of $\mathcal{C}^{PRE}$, one can appoint k queries that expand the span. Whenever any of such queries is made by an adversary $\mathcal{A}$, we let the corresponding modified adversary $\mathcal{A}'$ immediately make any other queries that are added to the span. In this way, we can fix all the indices of queries at which $\mathcal{A}'$ obtains a full preimage of Z. This modification makes upper bounding the preimage finding advantage of $\mathcal{A}'$ much easier than $\mathcal{A}$.

To be precise, let $H = \mathsf{KP}^b([r,k,d]_{2^e})$ be given with a generator matrix

$$G = [G_1, G_2, \cdots, G_r]$$

where G_i is a $k \times 1$ column matrix for $i = 1, \ldots, r$. (G is not necessarily in standard form.) Fix a sequence

$$\mathcal{T} = (l_1, l_2, \ldots, l_k) \in [1,r]^k$$

such that column matrices $G_{l_1}, \ldots, G_{l_k}$ are linearly independent (which implies $l_1, l_2, \ldots, l_k$ are all different), and a sequence

$$P = (i_1, i_2, \ldots, i_k) \in [1,q]^k$$

such that $i_1 < i_2 < \cdots < i_k$. If partial preimages $f_{l_1}(x^{i_1}) = z_{l_1}, \cdots, f_{l_k}(x^{i_k}) = z_{l_k}$ are found,[3] then these queries uniquely determine the remaining $r-k$ queries x_l, $l \in [1,r]\backslash\mathcal{T}$, such that, setting $x_{l_j} = x^{i_j}$ for $l_j \in \mathcal{T}$, $(x_l)_{l\in[1,r]}$ is an image of $\mathcal{C}^{PRE}$. Specifically, each of the remaining queries is represented as a linear combination of $x^{i_1}, \ldots, x^{i_k}$. We define predicate $\mathsf{Pre}_{\mathcal{T},P}$ where $\mathsf{Pre}_{\mathcal{T},P}$ is true if the following two conditions are satisfied.

1. $(l_\alpha, x^{i_\alpha}) \in \mathcal{Q}$ and $f_{l_\alpha}(x^{i_\alpha}) = z_{l_\alpha}$ for $\alpha = 1, \ldots, k$.
2. For all $l \in [1,r]\backslash\mathcal{T}$, let α be the first index such that G_l is represented as a linear combination of $G_{l_1}, \ldots, G_{l_\alpha}$. $\mathcal{A}$ obtains $f_l(x_l) = z_l$ *after* $\mathcal{A}$ makes the i_α-th query. (Note that x_l is determined as a linear combination of $x^{i_1}, \ldots, x^{i_\alpha}$.)

Then we have the following implication.

$$\mathsf{Pre} \Rightarrow \bigvee_{(\mathcal{T},P)} \mathsf{Pre}_{\mathcal{T},P}. \tag{4}$$

In order to prove the above implication, suppose that $\mathcal{A}$ sets Pre to true by obtaining $f_{l_1}(x^{i_1}) = z_1, \cdots, f_{l_r}(x^{i_r}) = z_r$ in an order of $i_1 < i_2 < \ldots < i_r$. From the sequence $(l_1, \ldots, l_r) \in [1,r]^r$, we can extract a subsequence $\mathcal{T} \in [1,r]^k$ using the following algorithm.

```
$\mathcal{T} \leftarrow \emptyset$
For $\alpha = 1, \ldots, r$,
if $G_{l_\alpha}$ is not represented by a linear combination of $G_l$, $l \in \mathcal{T}$ then
    $\mathcal{T} \leftarrow l_\alpha$
```

Since G is of rank k, we have $|\mathcal{T}| = k$. We can also check that $\mathsf{Pre}_{\mathcal{T},P}$ is true with $P = (i_\alpha)$ where α satisfies $l_\alpha \in \mathcal{T}$.

Sequence P fixes the indices of queries when we need to obtain the partial preimages of z_l for $l \in \mathcal{T}$. In order to fix the indices of queries from which we obtain the remaining partial preimages, we construct a modified adversary $\mathcal{A}'$ that uses $\mathcal{A}$ as a subroutine. The behavior of $\mathcal{A}'$ can be illustrated as follows.

[3] Here we are using slightly different notations from Section 2.2 by assuming x^{i_α} is queried to f_{l_α} not f_α. This implies $l_\alpha = l^{i_\alpha}$ for $\alpha = 1, \ldots, k$.

1. Between $\mathcal{A}$ and the random function oracles, $\mathcal{A}'$ faithfully relays all the $\mathcal{A}$'s queries and the oracles' responses.
2. Once queries $f_{l_1}(x^{i_1}), \cdots, f_{l_\alpha}(x^{i_\alpha})$ are made for $\alpha = 1, \dots, r$, $\mathcal{A}'$ searches for G_l that is represented as a linear combination of $G_{l_1}, \dots, G_{l_\alpha}$ with a nonzero coefficient of G_{l_α}.
3. For such an index l, query x_l that is consistent with $x^{i_1}, \dots, x^{i_\alpha}$ is determined as a linear combination of $x^{i_1}, \dots, x^{i_\alpha}$. $\mathcal{A}'$ makes an additional query $f_l(x_l)$ without relaying the response to $\mathcal{A}$. When $\mathcal{A}$ makes a certain query, $\mathcal{A}'$ might need to make a multiple number of additional queries, while we fix an order between those queries.

In case $\mathcal{A}$ requests any of the additional queries later, $\mathcal{A}'$ would have to make a redundant query. Including the redundant queries, the number of queries made by $\mathcal{A}'$ is at most $q + r - k$. In this way, $(\mathcal{T}, P)$ induces new sequences

$$\mathcal{T}' = (l_1', l_2', \dots, l_r') \in [1, r]^r,$$

$$P' = (i_1', i_2', \dots, i_r') \in [1, q]^r$$

such that l_α' are all distinct, $i_1' < i_2' < \cdots < i_r'$, and $\mathcal{A}$ setting $\mathsf{Pre}_{\mathcal{T},P}$ to true implies that $\mathcal{A}'$ obtains $f_{l_\alpha'}(x^{i_\alpha'}) = z_{l_\alpha'}$ as fresh queries for $\alpha = 1, \dots, r$.[4]

Example 3. Let H be based on a $[5, 3, 3]_4$ MDS code with a generator matrix

$$G = [G_1, G_2, G_3, G_4, G_5].$$

Let $\mathcal{T} = (1, 5, 3)$ and $P = (i_1, i_2, i_3)$, and let $G_2 = \lambda G_1$ and $G_4 = \mu_1 G_1 + \mu_3 G_3 + \mu_5 G_5$ for some constants $\lambda, \mu_1, \mu_3, \mu_5$ where λ and μ_3 are nonzero. Then $(\mathcal{T}, P)$ induces $\mathcal{T}' = (1, \mathbf{2}, 5, 3, \mathbf{4})$ and $P' = (i_1, i_1 + 1, i_2 + 1, i_3 + 1, i_3 + 2)$. Note that i_2 and i_3 have been replaced by $i_2 + 1$ and $i_3 + 1$ respectively in P', since one additional query has been inserted right after the i_1-th query.

Since $(\mathcal{T}', P')$ fixes all query indices i_α' that determine a preimage of Z, we have

$$\mathbf{Pr}\left[\mathcal{A} \text{ sets } \mathsf{Pre}_{\mathcal{T},P} \text{ to true}\right] \le \mathbf{Pr}\left[\mathcal{A}' \text{ sets } \mathsf{Pre}_{\mathcal{T}',P'} \text{ to true}\right] \le \frac{1}{N^r}. \tag{5}$$

Since the number of possible choices for $(\mathcal{T}, P)$ is at most

$$\binom{r}{k} k! \cdot \binom{q}{k} \le \binom{r}{k} q^k,$$

and by (4), (5) we conclude

$$\mathbf{Pr}\left[\mathsf{Pre}\right] \le \binom{r}{k} \frac{q^k}{N^r}.$$

To summarize this result, we have the following theorem.

[4] Without allowing a redundant query, P' is not uniquely defined from $(\mathcal{T}, P)$. P' would be different according to the point of time when a redundant query is made.

Theorem 2. *Let H be the Knudsen-Preneel compression function based on an $[r,k,d]_{2^e}$ code. Then we have*

$$\mathbf{Adv}_H^{\mathsf{pre}}(q) \leq \binom{r}{k}\frac{q^k}{N^r}.$$

Example 4. Let H be based on a $[5,3,3]_4$ MDS code. Then Theorem 2 implies

$$\mathbf{Adv}_H^{\mathsf{pre}}(q) \leq \frac{10q^3}{N^5}.$$

4 Collision Resistance Proof

Consider two sets of evaluations $\left(f_l(x^{i_l})\right)_{l\in[1,r]}$ and $\left(f_l(x^{j_l})\right)_{l\in[1,r]}$ of the inner primitives for $H = \mathsf{KP}^b([r,k,d]_{2^e})$. Let $S \subset [1,r]$ and suppose that $i_l = j_l$ (and hence $x^{i_l} = x^{j_l}$) for $l \in S$. As long as $(x^{i_l})_{l\in[1,r]}$ and $(x^{j_l})_{l\in[1,r]}$ are valid, partial inner collisions $f_l(x^{i_l}) = f_l(x^{j_l})$ for $l \in [1,r]\backslash S$ suffice to guarantee an actual collision of H regardless of the evaluations of $f_l(x^{i_l})(= f_l(x^{j_l}))$ for $l \in S$. For this reason, we will call the indices in $\mathcal{S}$ *inactive* and the other indices *active*. The probability of finding a collision turns out to be closely related to the number of inactive indices that contribute a collision.

When a collision happens, let predicate Col be set to true by definition. Our security proof begins with decomposing this predicate into subcases according to the number of inactive indices. For $0 \leq s \leq r-d$, consider a subset $\mathcal{S} \subset [1,r]$ such that $|\mathcal{S}| = s$. With respective to this subset, we define predicate $\mathsf{Col}_{\mathcal{S}}$, where $\mathsf{Col}_{\mathcal{S}}$ is true if $\mathcal{A}$ obtains an index sequence of a collision $C = (i_l, j_l)_{l\in[1,r]}$ such that

$$i_l = j_l \text{ if and only if } l \in \mathcal{S}.$$

Note that more than $r-d$ inactive inner collisions enforce $(x^{i_1},\ldots,x^{i_r}) = (x^{j_1},\ldots,x^{j_r})$ since H is based on a code of minimum distance d. Therefore we have

$$\mathsf{Col} \Rightarrow \bigvee_{0\leq s\leq r-d}\left(\bigvee_{\substack{\mathcal{S}\subset[1,r]\\|\mathcal{S}|=s}} \mathsf{Col}_{\mathcal{S}}\right). \tag{6}$$

4.1 Inner Collisions Compatible with Inactive Indices

For $s < d-1$, we will upper bound $\mathbf{Pr}\left[\mathsf{Col}_{\mathcal{S}}\right]$ by a wish list argument. In order to upper bound the size of a certain wish list, we need a notion of partial collisions. Similar to partial preimages, each partial collision will uniquely determine a wish in the list, so the size of the wish list is upper bounded by the number of partial collisions.

Definition 4. *Let $\mathcal{S}$ and $\mathcal{T}$ be disjoint subsets of $[1, r]$. A sequence of indices*

$$P = (i_l, j_l)_{l \in \mathcal{T}}$$

is called a partial collision at $\mathcal{T}$ compatible with inactive indices $\mathcal{S}$ *if*

1. *$1 \leq i_l, j_l \leq q$ are all distinct,*
2. *(l, x^{i_l}), $(l, x^{j_l}) \in \mathcal{Q}$ and $f_l(x^{i_l}) = f_l(x^{j_l})$ for $l \in \mathcal{T}$,*
3. *$(\Delta_l)_{l \in \mathcal{S} \cup \mathcal{T}}$ is valid where $\Delta_l = 0$ for $l \in \mathcal{S}$ and $\Delta_l = x^{i_l} \oplus x^{j_l}$ for $l \in \mathcal{T}$.*

Note that even in case of $S \cup T = [1, r]$, a partial collision need not correspond to an actual collision as $(x^{i_l})_{l \in \mathcal{T}}$ and $(x^{j_l})_{l \in \mathcal{T}}$ might not be valid. A partial collision also has the following property.

Property 3. *For disjoint subsets $\mathcal{S}$ and $\mathcal{T} \subset [1, r]$, the number of partial collisions at $\mathcal{T}$ compatible with inactive indices $\mathcal{S}$ is a multiple of $2^{|\mathcal{T}|}$.*

Proof. From a single partial collision $P = (i_l, j_l)_{l \in \mathcal{T}}$, we can obtain $2^{|\mathcal{T}|}$ different partial collisions by swapping i_l and j_l for each $l \in \mathcal{T}$. Since we can define an equivalence relation between them, the total number of partial collisions is given as a multiple of $2^{|\mathcal{T}|}$. □

By the following lemma, we can upper bound the number of partial collisions at $\mathcal{T}$ compatible with inactive indices $\mathcal{S}$ for a fixed subset $\mathcal{T}$ such that $\mathcal{S} \cap \mathcal{T} = \emptyset$ and $|\mathcal{S}| + |\mathcal{T}| \geq r - d + 1$. The proof, given in Appendix A in detail, is essentially based on the application of Markov's inequality.

Lemma 1. *Let $\mathcal{S}$ and $\mathcal{T}$ be disjoint subsets of $[1, r]$ such that $|\mathcal{S}| \leq r - d$ and $|\mathcal{S}| + |\mathcal{T}| \geq r - d + 1$, and let $|\mathcal{S}| = s$ and $|\mathcal{T}| = t$. Then for $M > 0$, the number of partial collisions at $\mathcal{T}$ compatible with inactive indices $\mathcal{S}$ is smaller than $2^{t-r+d+s-1}M$ except with probability*

$$\binom{t}{r-d-s+1} \frac{q^{t+r-d-s+1}}{MN^t}.$$

4.2 Upper Bounding Pr [$\mathsf{Col}_{\mathcal{S}}$]

According to the number of inactive indices, $s = |S|$, we distinguish two cases.

Case 1. $s < d - 1$: This case is analyzed by a wish list argument.
Note that $|[1, r] \backslash \mathcal{S}| > r - d + 1$. For a subset $\mathcal{T} \subset [1, r] \backslash \mathcal{S}$ such that $|\mathcal{T}| = r - d + 1$, we define predicate $\mathsf{Col}_{\mathcal{S},\mathcal{T}}$ where $\mathsf{Col}_{\mathcal{S},\mathcal{T}}$ is true if $\mathcal{A}$ obtains an index sequence of a collision $C = (i_l, j_l)_{l \in [1,r]}$ such that

1. $i_l = j_l$ if and only if $l \in \mathcal{S}$,
2. $\max_{l \in \mathcal{T}}\{i_l, j_l\} < \min_{l \in [1,r] \backslash (\mathcal{S} \cup \mathcal{T})}\{\max\{i_l, j_l\}\}$.

Thus $\mathcal{T}$ specifies the indices where the first $r-d+1$ *active* inner collisions are completed. For $M>0$, we define predicate $\mathsf{Bad}(M)$ where $\mathsf{Bad}(M)$ is true if there exists a subset $\mathcal{T}\subset[1,r]\backslash\mathcal{S}$ of size $r-d+1$ such that the number of partial collisions at $\mathcal{T}$ compatible with inactive indices $\mathcal{S}$ is greater than

$$L=2^sM.$$

Then by Lemma 1 (with $t=r-d+1$) and a union bound, we have

$$\mathbf{Pr}[\mathsf{Bad}(M)]\le\binom{r-s}{r-d+1}\binom{r-d+1}{s}\frac{q^{2(r-d+1)-s}}{MN^{r-d+1}}. \tag{7}$$

In order to upper bound $\mathbf{Pr}\left[\mathsf{Col}_{\mathcal{S}}\right]$, we will use the following implication.

$$\mathsf{Col}_{\mathcal{S}}\Rightarrow\mathsf{Bad}(M)\vee\bigvee_{\substack{\mathcal{T}\subset[1,r]\backslash\mathcal{S}\\|\mathcal{T}|=r-d+1}}\left(\neg\mathsf{Bad}(M)\wedge\mathsf{Col}_{\mathcal{S},\mathcal{T}}\right). \tag{8}$$

Now we will focus on upper bounding $\mathbf{Pr}\left[\neg\mathsf{Bad}(M)\wedge\mathsf{Col}_{\mathcal{S},\mathcal{T}}\right]$ for fixed subsets $\mathcal{S}$ and $\mathcal{T}$. In order for $\mathcal{A}$ to set $\mathsf{Col}_{\mathcal{S},\mathcal{T}}$ to true, $\mathcal{A}$ has to first complete a partial collision at $\mathcal{T}$ compatible with inactive indices $\mathcal{S}$. At the point when a partial collision $P=(i_l,j_l)_{l\in\mathcal{T}}$ is completed, the remaining queries $(x_l,x'_l)_{l\in[1,r]\backslash(\mathcal{S}\cup\mathcal{T})}$ that could make a collision along with P are uniquely determined. (They *exist* only if $(x^{i_l})_{l\in\mathcal{T}}$ and $(x^{j_l})_{l\in\mathcal{T}}$ are valid.) If

1. $x_l\neq x'_l$ for $l\in[1,r]\backslash(\mathcal{S}\cup\mathcal{T})$,
2. any of collisions of $f_l(x_l)$ and $f_l(x'_l)$ has not been determined for $l\in[1,r]\backslash(\mathcal{S}\cup\mathcal{T})$,

then we include $(x_l,x'_l)_{l\in[1,r]\backslash(\mathcal{S}\cup\mathcal{T})}$ into a wish list $\mathcal{L}$, expecting all of the collisions to happen sometime later. A single query might include a multiple number of wishes into $\mathcal{L}$ by completing a multiple number of partial collisions. However a single partial collision is associated with a unique element in $\mathcal{L}$. Therefore without the occurrence of $\mathsf{Bad}(M)$, the size of $\mathcal{L}$ is at most L, and we have the following upper bound.

$$\mathbf{Pr}\left[\neg\mathsf{Bad}(M)\wedge\mathsf{Col}_{\mathcal{S},\mathcal{T}}\right]\le\sum_{i=1}^{L}\mathbf{Pr}\left[\text{the } i\text{-th wish is granted}\right]. \tag{9}$$

Since

$$\mathbf{Pr}\left[\text{the } i\text{-th wish is granted}\right]\le\frac{1}{N^{|[1,r]\backslash(\mathcal{S}\cup\mathcal{T})|}}=\frac{1}{N^{d-s-1}},$$

for each $i=1,\ldots,L$, and by (7), (8), (9), we have

$$\mathbf{Pr}[\mathsf{Col}_{\mathcal{S}}]\le\binom{r-s}{r-d+1}\binom{r-d+1}{s}\frac{q^{2(r-d+1)-s}}{MN^{r-d+1}}+\binom{r-s}{r-d+1}\frac{2^sM}{N^{d-s-1}}. \tag{10}$$

Case 2. $\boldsymbol{s \geq d-1}$ **:** This case might occur when $d-1 \leq r-d$. Let $\mathcal{T} = [1,r]\backslash\mathcal{S}$. In this case, $\mathsf{Col}_{\mathcal{S}}$ implies that there is a partial collision at $\mathcal{T}$ compatible with inactive indices $\mathcal{S}$. Here we can use Lemma 1 with $M = 1$ and $t = r - s$ since the number of partial collisions should be a multiple of $2^{|\mathcal{T}|} = 2^{r-s}$ but $2^{t-r+d+s-1}(= 2^{d-1})$ is smaller than 2^{r-s}. Therefore we have

$$\begin{aligned}\mathbf{Pr}[\mathsf{Col}_{\mathcal{S}}] &\leq \mathbf{Pr}[\text{there is a partial collisions at } \mathcal{T} \text{ compatible with inactive indices } \mathcal{S}] \\ &\leq \binom{r-s}{d-1}\frac{q^{2(r-s)-d+1}}{N^{r-s}}. \qquad (11)\end{aligned}$$

4.3 Putting the Pieces Together

By (6), (10) and (11), we obtain the following result.

$$\begin{aligned}\mathbf{Pr}[\mathsf{Col}] \leq &\sum_{s=0}^{d-2}\binom{r}{s}\binom{r-s}{r-d+1}\left(\binom{r-d+1}{s}\frac{q^{2(r-d+1)-s}}{M(s)N^{r-d+1}} + \frac{2^s M(s)}{N^{d-s-1}}\right) \\ &+ \sum_{s=d-1}^{r-d}\binom{r}{s}\binom{r-s}{d-1}\frac{q^{2(r-s)-d+1}}{N^{r-s}},\end{aligned}$$

where the parameter $M(s)$ might depend on the size of $\mathcal{S}$ and the second term of the right hand side appears only when $d-1 \leq r-d$. In order to optimize the right hand side of the inequality, set

$$M(s) = \binom{r-d+1}{s}^{\frac{1}{2}}\frac{q^{r-d+1-\frac{s}{2}}}{2^{\frac{s}{2}}N^{\frac{r+s}{2}-d+1}},$$

by solving

$$\binom{r-d+1}{s}\frac{q^{2(r-d+1)-s}}{M(s)N^{r-d+1}} = \frac{2^s M(s)}{N^{d-s-1}}.$$

Then we have the following theorem.

Theorem 3. *Let H be the Knudsen-Preneel compression function based on an $[r,k,d]_{2^e}$ code. Then we have*

$$\begin{aligned}\mathbf{Adv}_H^{\mathsf{col}}(q) \leq &\sum_{s=0}^{d-2}\binom{r}{s}\binom{r-s}{r-d+1}\binom{r-d+1}{s}^{\frac{1}{2}}\frac{2^{\frac{s}{2}+1}q^{r-d+1-\frac{s}{2}}}{N^{\frac{r-s}{2}}} \\ &+ \sum_{s=d-1}^{r-d}\binom{r}{s}\binom{r-s}{d-1}\frac{q^{2(r-s)-d+1}}{N^{r-s}}.\end{aligned}$$

Interpretation. Let $d-1 \leq r-d$ or equivalently $2d \leq r+1$. Assuming $N^{\frac{1}{2}} \leq q \leq N$, we have

$$\sum_{s=0}^{d-2}\binom{r}{s}\binom{r-s}{r-d+1}\binom{r-d+1}{s}^{\frac{1}{2}}\frac{2^{\frac{s}{2}+1}q^{r-d+1-\frac{s}{2}}}{N^{\frac{r-s}{2}}} = O\left(\frac{q^{r-\frac{3d}{2}+2}}{N^{\frac{r}{2}-\frac{d}{2}+1}}\right),$$

and

$$\sum_{s=d-1}^{r-d} \binom{r}{s}\binom{r-s}{d-1}\frac{q^{2(r-s)-d+1}}{N^{r-s}} = O\left(\frac{q^{2r-3d+3}}{N^{r-d+1}}\right).$$

In this case, H is collision resistant up to $N^{\frac{r-d+1}{2r-3d+3}}$ query complexity since

$$N^{\frac{1}{2}} \le N^{\frac{r-d+1}{2r-3d+3}} \le N^{\frac{r-d+2}{2r-3d+4}} \le N.$$

Let $2d > r+1$. Assuming $q \ge N$, we have

$$\sum_{s=0}^{r-d} \binom{r}{s}\binom{r-s}{r-d+1}\binom{r-d+1}{s}^{\frac{1}{2}}\frac{2^{\frac{s}{2}+1}q^{r-d+1-\frac{s}{2}}}{N^{\frac{r-s}{2}}} = O\left(\frac{q^{r-d+1}}{N^{\frac{r}{2}}}\right).$$

In this case, H is collision resistant up to $N^{\frac{r}{2r-2d+2}}$ query complexity since

$$N \le N^{\frac{r}{2r-2d+2}}.$$

We summarize this result as follows.

Corollary 1. *Let H be the Knudsen-Preneel compression function based on an $[r,k,d]_{2^e}$ code.*

(a) If $2d \le r+1$, then H is collision resistant up to $N^{\frac{r-d+1}{2r-3d+3}}$ query complexity.
(b) If $2d > r+1$, then H is collision resistant up to $N^{\frac{r}{2r-2d+2}}$ query complexity.

Corollary 2. *Let H be the Knudsen-Preneel compression function based on an $[r,k,d]_{2^e}$ MDS code.*

(a) If $r+1 \le 2k$, then H is collision resistant up to $N^{\frac{k}{3k-r}}$ query complexity.
(b) If $r+1 > 2k$, then H is collision resistant up to $N^{\frac{r}{2k}}$ query complexity.

Example 5. Let H be based on $[5,3,3]_4$ MDS code. Then

$$\begin{aligned}\mathbf{Adv}_H^{\mathsf{col}}(q) &\le \sum_{s=0}^{1}\binom{5}{s}\binom{5-s}{3}\binom{3}{s}^{\frac{1}{2}}\frac{2^{\frac{s}{2}+1}q^{3-\frac{s}{2}}}{N^{\frac{5-s}{2}}} + \binom{5}{2}\binom{3}{2}\frac{q^4}{N^3}\\ &= \frac{20q^3}{N^{\frac{5}{2}}} + \frac{40\sqrt{6}q^{\frac{5}{2}}}{N^2} + \frac{30q^4}{N^3}.\end{aligned}$$

Therefore H is collision resistant up to $N^{3/4}$ query complexity.

Acknowledgements. The author would like to thank Martijn Stam for many valuable comments.

References

1. Armknecht, F., Fleischmann, E., Krause, M., Lee, J., Stam, M., Steinberger, J.: The Preimage Security of Double-Block-Length Compression Functions. In: Lee, D.H. (ed.) ASIACRYPT 2011. LNCS, vol. 7073, pp. 233–251. Springer, Heidelberg (2011)
2. Biham, E., Chen, R., Joux, A., Carribault, P., Lemuet, C., Jalby, W.: Collisions of SHA-0 and Reduced SHA-1. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 36–57. Springer, Heidelberg (2005)
3. Black, J., Cochran, M., Shrimpton, T.: On the Impossibility of Highly-Efficient Blockcipher-Based Hash Functions. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 526–541. Springer, Heidelberg (2005)
4. Black, J., Rogaway, P., Shrimpton, T.: Black-Box Analysis of the Block-Cipher-Based Hash-Function Constructions from PGV. In: Yung, M. (ed.) CRYPTO 2002. LNCS, vol. 2442, pp. 320–325. Springer, Heidelberg (2002)
5. Bos, J.W., Özen, O., Stam, M.: Efficient Hashing Using the AES Instruction Set. In: Preneel, B., Takagi, T. (eds.) CHES 2011. LNCS, vol. 6917, pp. 507–522. Springer, Heidelberg (2011)
6. De Cannière, C., Rechberger, C.: Preimages for Reduced SHA-0 and SHA-1. In: Wagner, D. (ed.) CRYPTO 2008. LNCS, vol. 5157, pp. 179–202. Springer, Heidelberg (2008)
7. Damgård, I.B.: A Design Principle for Hash Functions. In: Brassard, G. (ed.) CRYPTO 1989. LNCS, vol. 435, pp. 416–427. Springer, Heidelberg (1990)
8. Fleischmann, E., Gorski, M., Lucks, S.: Security of Cyclic Double Block Length Hash Functions. In: Parker, M.G. (ed.) Cryptography and Coding 2009. LNCS, vol. 5921, pp. 153–175. Springer, Heidelberg (2009)
9. Hirose, S.: Provably Secure Double-Block-Length Hash Functions in a Black-Box Model. In: Park, C., Chee, S. (eds.) ICISC 2004. LNCS, vol. 3506, pp. 330–342. Springer, Heidelberg (2005)
10. Hirose, S.: Some Plausible Constructions of Double-Block-Length Hash Functions. In: Robshaw, M. (ed.) FSE 2006. LNCS, vol. 4047, pp. 210–225. Springer, Heidelberg (2006)
11. Knudsen, L.R., Preneel, B.: Construction of secure and fast hash functions using non binary error-correcting codes. IEEE Transactions on Information Theory 48(9), 2524–2539 (2002)
12. Knudsen, L.R., Preneel, B.: Fast and Secure Hashing Based on Codes. In: Kaliski Jr., B.S. (ed.) CRYPTO 1997. LNCS, vol. 1294, pp. 485–498. Springer, Heidelberg (1997)
13. Knudsen, L.R., Preneel, B.: Hash Functions Based on Block Ciphers and Quaternary Codes. In: Kim, K.-c., Matsumoto, T. (eds.) ASIACRYPT 1996. LNCS, vol. 1163, pp. 77–90. Springer, Heidelberg (1996)
14. Lai, X., Massey, J.L.: Hash Functions Based on Block Ciphers. In: Rueppel, R.A. (ed.) EUROCRYPT 1992. LNCS, vol. 658, pp. 55–70. Springer, Heidelberg (1993)
15. Lee, J., Kwon, D.: The security of Abreast-DM in the ideal cipher model. IACR ePrint Archive 2009/225 (2009)
16. Lee, J., Stam, M.: MJH: A Faster Alternative to MDC-2. In: Kiayias, A. (ed.) CT-RSA 2011. LNCS, vol. 6558, pp. 213–236. Springer, Heidelberg (2011)
17. Lee, J., Stam, M., Steinberger, J.: The Collision Security of Tandem-DM in the Ideal Cipher Model. In: Rogaway, P. (ed.) CRYPTO 2011. LNCS, vol. 6841, pp. 561–577. Springer, Heidelberg (2011)

18. Leurent, G.: MD4 is Not One-Way. In: Nyberg, K. (ed.) FSE 2008. LNCS, vol. 5086, pp. 412–428. Springer, Heidelberg (2008)
19. Mendel, F., Pramstaller, N., Rechberger, C., Rijmen, V.: Analysis of Step-Reduced SHA-256. In: Robshaw, M. (ed.) FSE 2006. LNCS, vol. 4047, pp. 126–143. Springer, Heidelberg (2006)
20. Merkle, R.C.: One Way Hash Functions and DES. In: Brassard, G. (ed.) CRYPTO 1989. LNCS, vol. 435, pp. 428–446. Springer, Heidelberg (1990)
21. Özen, O., Shrimpton, T., Stam, M.: Attacking the Knudsen-Preneel Compression Functions. In: Hong, S., Iwata, T. (eds.) FSE 2010. LNCS, vol. 6147, pp. 94–115. Springer, Heidelberg (2010)
22. Özen, O., Stam, M.: Another Glance at Double-Length Hashing. In: Parker, M.G. (ed.) Cryptography and Coding 2009. LNCS, vol. 5921, pp. 176–201. Springer, Heidelberg (2009)
23. Özen, O., Stam, M.: Collision Attacks against the Knudsen-Preneel Compression Functions. In: Abe, M. (ed.) ASIACRYPT 2010. LNCS, vol. 6477, pp. 76–93. Springer, Heidelberg (2010)
24. Steinberger, J.: The Collision Intractability of MDC-2 in the Ideal-Cipher Model. In: Naor, M. (ed.) EUROCRYPT 2007. LNCS, vol. 4515, pp. 34–51. Springer, Heidelberg (2007)
25. Preneel, B., Govaerts, R., Vandewalle, J.: Hash Functions Based on Block Ciphers: A Synthetic Approach. In: Stinson, D.R. (ed.) CRYPTO 1993. LNCS, vol. 773, pp. 368–378. Springer, Heidelberg (1994)
26. Ristenpart, T., Shrimpton, T.: How to Build a Hash Function from Any Collision-Resistant Function. In: Kurosawa, K. (ed.) ASIACRYPT 2007. LNCS, vol. 4833, pp. 147–163. Springer, Heidelberg (2007)
27. Rogaway, P., Steinberger, J.: Constructing Cryptographic Hash Functions from Fixed-Key Blockciphers. In: Wagner, D. (ed.) CRYPTO 2008. LNCS, vol. 5157, pp. 433–450. Springer, Heidelberg (2008)
28. Rogaway, P., Steinberger, J.: Security/Efficiency Tradeoffs for Permutation-Based Hashing. In: Smart, N.P. (ed.) EUROCRYPT 2008. LNCS, vol. 4965, pp. 220–236. Springer, Heidelberg (2008)
29. Sasaki, Y., Aoki, K.: Finding Preimages in Full MD5 Faster Than Exhaustive Search. In: Joux, A. (ed.) EUROCRYPT 2009. LNCS, vol. 5479, pp. 134–152. Springer, Heidelberg (2009)
30. Shrimpton, T., Stam, M.: Building a Collision-Resistant Compression Function from Non-compressing Primitives. In: Aceto, L., Damgård, I., Goldberg, L.A., Halldórsson, M.M., Ingólfsdóttir, A., Walukiewicz, I. (eds.) ICALP 2008, Part II. LNCS, vol. 5126, pp. 643–654. Springer, Heidelberg (2008)
31. Stam, M.: Beyond Uniformity: Better Security/Efficiency Tradeoffs for Compression Functions. In: Wagner, D. (ed.) CRYPTO 2008. LNCS, vol. 5157, pp. 397–412. Springer, Heidelberg (2008)
32. Stam, M.: Blockcipher-Based Hashing Revisited. In: Dunkelman, O. (ed.) FSE 2009. LNCS, vol. 5665, pp. 67–83. Springer, Heidelberg (2009)
33. Steinberger, J.: The Collision Intractability of MDC-2 in the Ideal-Cipher Model. In: Naor, M. (ed.) EUROCRYPT 2007. LNCS, vol. 4515, pp. 34–51. Springer, Heidelberg (2007)
34. Wang, X., Lai, X., Feng, D., Chen, H., Yu, X.: Cryptanalysis of the Hash Functions MD4 and RIPEMD. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 1–18. Springer, Heidelberg (2005)
35. Wang, X., Yin, Y.L., Yu, H.: Finding Collisions in the Full SHA-1. In: Shoup, V. (ed.) CRYPTO 2005. LNCS, vol. 3621, pp. 17–36. Springer, Heidelberg (2005)

36. Wang, X., Yu, H.: How to Break MD5 and Other Hash Functions. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 19–35. Springer, Heidelberg (2005)
37. Watanabe, D.: A note on the security proof of Knudsen-Preneel construction of a hash function (2006), http://csrc.nist.gov/pki/HashWorkshop/2006/UnacceptedPapers/WATANABE_kp_attack.pdf

A Proof of Lemma 1

Let $\mathcal{T} = \mathcal{U} \cup \mathcal{V}$ be a disjoint decomposition of $\mathcal{T}$ such that $|\mathcal{S}| + |\mathcal{U}| = r - d + 1$. Let $\mathbb{D}[\mathcal{U}, \mathcal{V}]$ be the set of index sequences

$$D = ((i_l, j_l)_{l\in\mathcal{U}}, (h_l)_{l\in\mathcal{V}})$$

such that

1. $1 \leq i_l, j_l, h_l \leq q$ are all distinct,
2. $\max_{l\in\mathcal{U}}\{i_l, j_l\} < \min_{l\in\mathcal{V}}\{h_l\}$.

For a sequence $D = ((i_l, j_l)_{l\in\mathcal{U}}, (h_l)_{l\in\mathcal{V}}) \in \mathbb{D}[\mathcal{U}, \mathcal{V}]$, we define a random variable X_D where $X_D = 1$ if there is a sequence $(i_l, j_l)_{l\in\mathcal{V}}$ such that

1. $\max\{i_l, j_l\} = h_l$ for $l \in \mathcal{V}$,
2. $P = (i_l, j_l)_{l\in\mathcal{U}\cup\mathcal{V}}$ is a partial collision at $\mathcal{T}$ compatible with inactive indices $\mathcal{S}$,

and $X_D = 0$ otherwise. The condition

$$\max_{l\in\mathcal{U}}\{i_l, j_l\} < \min_{l\in\mathcal{V}}\{h_l\} = \min_{l\in\mathcal{V}}\{\max\{i_l, j_l\}\}$$

implies that the inner collisions at $\mathcal{V}$ are completed after the inner collisions at $\mathcal{U}$. Therefore for $D = ((i_l, j_l)_{l\in\mathcal{U}}, (h_l)_{l\in\mathcal{V}}) \in \mathbb{D}[\mathcal{U}, \mathcal{V}]$, $\mathbf{Pr}[X_D = 1]$ is the probability that

1. For $l \in \mathcal{U}$, $f_l(x^{i_l}) = f_l(x^{j_l})$,
2. For $l \in \mathcal{V}$, $f_l(x^{h_l}) = f_l(x^{h_l} \oplus \Delta_l^*)$, where
   (a) $(\Delta_l^*)_{l\in[1,r]}$ is a unique extension of $(\Delta_l)_{l\in\mathcal{S}\cup\mathcal{U}}$, where $\Delta_l = 0$ for $l \in \mathcal{S}$ and $\Delta_l = x^{i_l} \oplus x^{j_l}$ for $l \in \mathcal{U}$ (by Property 2),
   (b) $f_l(x^{h_l} \oplus \Delta_l^*)$ has been queried before the h_l-th query.

Since t inner collisions are necessary for $X_D = 1$, we have

$$\mathbf{Pr}[X_D = 1] = \mathsf{Ex}(X_D) \leq \frac{1}{N^t}.^{5}$$

Let

$$X = \sum_{\substack{\mathcal{U}\cup\mathcal{V}=\mathcal{T} \\ \mathcal{U}\cap\mathcal{V}=\emptyset \\ |\mathcal{S}|+|\mathcal{U}|=r-d+1}} \sum_{D\in\mathbb{D}[\mathcal{U},\mathcal{V}]} X_D.$$

[5] If the extension $(\Delta_l^*)_{l\in[1,r]}$ does not exist, then $\mathbf{Pr}[X_D = 1] = 0$.

Since the number of possible decompositions of $\mathcal{T} = \mathcal{U} \cup \mathcal{V}$ such that $\mathcal{U} \cap \mathcal{V} = \emptyset$ and $|\mathcal{S}| + |\mathcal{U}| = r - d + 1$ is $\binom{t}{r-d-s+1}$ and

$$|\mathbb{D}[\mathcal{U}, \mathcal{V}]| \leq q^{2|\mathcal{U}|+|\mathcal{V}|} = q^{|\mathcal{T}|+|\mathcal{U}|} = q^{t+(r-d+1)-s}$$

for each decomposition, we have

$$\mathsf{Ex}(X) = \binom{t}{r-d-s+1} q^{t+r-d-s+1} \mathsf{Ex}(X_D) \leq \binom{t}{r-d-s+1} \frac{q^{t+r-d-s+1}}{N^t}.$$

Using Markov's inequality, for $M > 0$ we have

$$\mathbf{Pr}\left[X \geq M\right] \leq \binom{t}{r-d-s+1} \frac{q^{t+r-d-s+1}}{MN^t}. \tag{12}$$

Let $P = (i_l, j_l)_{l \in \mathcal{T}}$ be a partial collision at $\mathcal{T}$ compatible with inactive indices $\mathcal{S}$. Then we always have a unique disjoint decomposition of $\mathcal{T} = \mathcal{U} \cup \mathcal{V}$ such that $|\mathcal{U}| = r - d - s + 1$ and

$$\max_{l \in \mathcal{U}} \{i_l, j_l\} < \min_{l \in \mathcal{V}} \left\{\max\{i_l, j_l\}\right\}.$$

In this case, we have $X_D = 1$ for $D = \left((i_l, j_l)_{l \in \mathcal{U}}, (h_l)_{l \in \mathcal{V}}\right)$ where $h_l = \max\{i_l, j_l\}$. If we regard this association of P with D as a mapping, then exactly $2^{|\mathcal{V}|}(= 2^{t-(r-d-s+1)})$ different partial collisions would be mapped to the same sequence D since (i_l, j_l) can be replaced by (j_l, i_l) for each index $l \in \mathcal{V}$ without changing the image of this mapping. Therefore the inequality (12) implies that the number of partial collisions at $\mathcal{T}$ compatible with inactive indices $\mathcal{S}$ is at most $2^{t-r+d+s-1}M$ except with probability $\binom{t}{r-d-s+1} q^{t+r-d-s+1}/(MN^t)$.