On the Complexity of the Herding Attack and Some Related Attacks on Hash Functions

Simon R. Blackburn
Department of Mathematics, Royal Holloway, University of London
Egham, Surrey TW20 0EX, United Kingdom
s.blackburn@rhul.ac.uk

Douglas R. Stinson[*] and Jalaj Upadhyay
David R. Cheriton School of Computer Science
University of Waterloo
Waterloo Ontario N2L 3G1, Canada
{dstinson,jkupadhy}@cs.uwaterloo.ca

August 30, 2010

Abstract

In this paper, we analyze the complexity of the construction of the 2^k-diamond structure proposed by Kelsey and Kohno [15]. We point out a flaw in their analysis and show that their construction may not produce the desired diamond structure. We then give a more rigorous and detailed complexity analysis of the construction of a diamond structure. For this, we appeal to random graph theory (in particular, to the theory of random intersection graphs), which allows us to determine sharp necessary and sufficient conditions for the *message complexity* (i.e., the number of hash computations required to build the required structure). We also analyze the *computational complexity* for constructing a diamond structure, which has not been previously studied in the literature. Finally, we study the impact of our analysis on herding and other attacks that use the diamond structure as a subroutine. Precisely, our results shows the following:

1. The message complexity for the construction of a diamond structure is $\sqrt{k}$ times more than the amount previously stated in literature.
2. The time complexity is n times the message complexity, where n is the size of hash value.

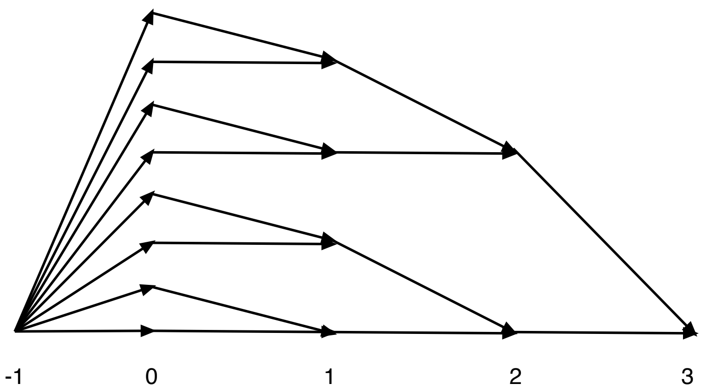
Due to the above two results, the herding attack [15] and the second preimage attack [3] on iterated hash functions have increased complexity. We also show that the message complexity of herding and second preimage attacks on "hash twice" is n times the complexity claimed by [2], by giving a more detailed analysis of the attack.

1 Introduction

In a recent paper, Kelsey and Kohno [15] proposed a new attack on Damgård-Merkle hash functions, called the *herding attack*. In such an attack, the adversary first commits to a hash value and is then provided with a prefix. The attacker is required to find a suitable suffix that "herds" to the previously committed hash value. That is, given x, h, and a hash function H, the adversary must find y such that $H(x \parallel y) = h$.

[*] Research supported by NSERC grant 203114-06

Figure 1: A 2^3 diamond structure



To launch the attack, [15] proposed a 2^k-*diamond structure*, which permits the construction of certain multi-collisions, but which is structurally different from Joux's multicollision attack [13].

A 2^k-diamond structure contains a complete binary tree of depth k. There are $2^{k-\ell}$ nodes at level ℓ, for $k \geq \ell \geq 0$. There is also a single node at level -1, which we will call the *source node*. The source node is joined to every node at level 0. The nodes at level 0 are called the *leaves* of the diamond structure and the node at level k is called the *root* of the diamond structure.

Every edge e in the diamond structure is labeled by a string $\sigma(e)$. Typically, a string $\sigma(e)$ consists of one or more message blocks. We also assign a label $h(N)$ to every node N in the structure at level at least 0, as follows. Consider a directed path P from the source node to the node N in the diamond structure. P will consist of some edges $e_0 e_1 \cdots e_\ell$, where N is at level ℓ in the tree. Then we define

$$h(N) = H(\sigma(e_0) \parallel \sigma(e_1) \parallel \cdots \parallel \sigma(e_\ell)).$$

The diamond structure will be constructed in such a way that all paths leading to a given node N yield the same value $h(N)$, so $h(N)$ will be well-defined.

At any level ℓ of the structure there are $2^{k-\ell}$ hash values. These must be paired up in such a way that, when the next message blocks are appended, $2^{k-\ell-1}$ collisions occur. Thus there are $2^{k-\ell-1}$ hash values at the next level, which is level $\ell+1$. The entire structure yields a 2^k-multicollision, but it has other uses, as well.

A diagram of a 2^3 diamond structure is given in Figure 1.

The diamond structure has found applications in attacks on hash functions that resisted other techniques such as Joux's multicollision [13] and Kelsey-Schneier's expandable message attack [16]. Andreeva *et al* [3] used the diamond structure to launch a second-preimage attack on Rivest's dithered hash construction [23], which resisted the attack by Kelsey and Schneier [16]. They used the same dithering symbol for all the edges at the same level of the diamond structure. Using a similar technique, they also launched an attack on Shoup's domain extension algorithm for universal one-way hash functions [25]. In a recent paper, Andreeva *et al* [2] extended the application of diamond structures to launch herding attacks on four variants of hash functions, namely, hash twice, concatenated hash, zipper hash, and tree based hash, as well as a second preimage attack on hash twice construction.

All these attacks are based on the analysis of Kelsey and Kohno [15], which claims that construction of a diamond structure is not as expensive as a naive approach would suggest. They stated that for herding an n-bit hash function, one requires $2^{(n+k+4)/2}$ messages to construct a 2^k-diamond structure. In this paper, we show a problem with their analysis and present a corrected and more detailed analysis of the herding attack. We also perform the first analysis of the computational complexity for constructing a diamond structure. The main results are as follows:

1. The message complexity of constructing a 2^k-diamond structure using the Kelsey-Kohno algorithm is $\Theta(\sqrt{k} \times 2^{(n+k)/2})$ (Theorem 1).

2. If each hash computation takes unit time, the computational complexity of constructing a 2^k-diamond structure is $O(n \times \sqrt{k} \times 2^{(n+k)/2})$ (Theorem 2).

Using these results, we revisit the analysis of various attacks, such as [2, 3, 15], that are based on diamond structure.

The paper is organized as follows. In Section 2, we outline the definitions and notations that are used in the paper. In Section 3, we formally present the diamond construction and give an overview of the analysis of Kelsey and Kohno [15], pointing out the problem with their analysis. Also, in Section 3, we analyse the construction of a diamond structure using the Erdös-Rényi random graph model. In Section 4, we perform a more rigorous analysis in the setting of random intersection graphs. In Section 5, we revisit the complexity of the attacks that are based on diamond structure in the light of our analysis.

2 Preliminaries

In this section, we discuss some preliminaries that are required to understand this paper. We define the notation that we use in the paper, basics of hash functions, and variants of hash functions which are attacked using the diamond structure, as well as some concepts from the graph theory that we require in our analysis.

2.1 Notation

We let $\mathbb{N}$ denote the set of all natural numbers. For any integer $k \in \mathbb{N}$, denote by $[k]$ the set $\{1, 2, \ldots, k\}$. Let $n \in \mathbb{N}$, then $\{0,1\}^n$ denotes all the n-bit strings. For any $x \in \{0,1\}^*$, we denote the bit-length of x by $|x|$. We denote the concatenation of two strings x and y by $x\|y$. We denote the message blocks of any message M by $M_1\|M_2\|\cdots\|M_l$, where l denotes the number of message blocks. We write $\log n$ for the logarithm of n to the base 2 and $\ln n$ for natural logarithm of n. We use the following asymptotic notation [7, p. 336]. If $f : \mathbb{N} \to \mathbb{R}$ and $g : \mathbb{N} \to \mathbb{R}$ are two functions such that $g(n) > 0$ for n sufficiently large, then we write:

$$\begin{aligned} f \ll g \quad &\text{if} \quad f(n)/g(n) \to 0 \text{ as } n \to \infty \\ f \gg g \quad &\text{if} \quad f(n)/g(n) \to \infty \text{ as } n \to \infty. \end{aligned}$$

2.2 Basic hash function constructions

Hash functions have been defined in two settings: traditional keyless hash function and as a family of hash functions. In a traditional keyless hash function, we have a single hash function H that maps an arbitrary length input to a fixed length output. We now give a formal definition of the keyed hash functions.

Definition 2.1. *For a finite* key space $\mathcal{K}$*, a space of* messages $\mathcal{M}$*, and a finite space of possible outputs called* message digests*,* $\mathcal{Y}$*, we define a* hash function family *as*

$$\mathcal{H} : \mathcal{K} \times \mathcal{M} \to \mathcal{Y}.$$

We denote the family of hash functions by $\mathcal{H} := \{H_k\}_{k \in \mathcal{K}}$.

A key $k \in \mathcal{K}$ acts as an index which defines which hash function is chosen from the family. We usually denote the hash function $H(k, M)$ by $H_k(M)$ for $k \in \mathcal{K}$ and $M \in \mathcal{M}$. We even drop the subscript when the function is clear from the context. Note that a traditional keyless hash function is a hash family with $|\mathcal{K}| = 1$.

A hash function, h, with $\mathcal{Y} \in \{0,1\}^n$ is required to have three basic security properties [14, 27, 28]: collision resistance, preimage resistance, and second preimage resistance. Kelsey and Kohno [15] defined a new security property: the chosen-target-forced-prefix resistance. This property is also studied in [21] in connection with the Schnorr signature scheme, under the name *random-prefix preimage problem*. In this paper, we deal with second preimage resistance and chosen-target-forced-prefix resistance. These are defined informally as follows.

1. *Second preimage-resistance*: An attacker, when given one message M, should not be able to find another message M' such that $h(M) = h(M')$ with less than 2^n hash computations.

2. *Chosen-target-forced-prefix resistance*: An attacker commits to a hash value, h_c, and is then challenged with a *prefix* P. The attacker should not be able to find a *suffix* S such that $h(P \| S) = h_c$ with less than 2^n hash computations. The attack is also called the *herding attack*.

A second preimage attack or herding attack with less than 2^n work is considered to be a *break* of the hash function.

In this paper, we deal with a standard form of hash function, the *iterated hash function*. In an iterated hash function, we first define a function over a small domain, called the *compression function*, and then we extend the domain by using the compression function in an iterative manner.

Let $f : \{0,1\}^n \times \{0,1\}^b \to \{0,1\}^n$ be a compression function. We denote the n-bit output of every iteration by h and call them *chaining values*; they are the input to the next iteration. The hash function based on a compression function f is denoted by H^f. With a little abuse of notation, we drop the super-script if the compression function is clear from the context. For the rest of the paper, we assume that the message M is padded such that the padded message is a multiple of b. For this section, we assume that the padded message has a bit length bl and for simplicity, we denote the padded message by M. We represent the message in block form as $M = M_1 \| M_2 \| \cdots \| M_l$, where $|M_i| = b$ for all $i \in [l]$.

We next define some iterative hash functions that are susceptible to the herding attack and second preimage attack using the diamond structure.

MERKLE-DAMGARD.

The *Merkle-Damgård construction* is simple iteration, where

$$h_i = f(h_{i-1}, M_i) \ \forall i \in [l]$$

and h_0 is a publicly known initial hash value. The output of the computation is $\mathcal{MD}^f := h_l$.

HASH TWICE.

In *hash twice*, one hashes two consecutive copies of the message M. Formally, for a hash function H, it is defined as

$$\mathcal{HT} := H(H(IV, M), M)$$

where IV is the publicly known initial hash value.

DITHERED HASH FUNCTIONS.

In the *dithered hash function*, every call to the compression function has three inputs: the *dithering sequence* which depends on the iteration, the chaining hash value, and the next message block. In the construction of Rivest [23], the author uses a dithering sequence that is abelian square free. We give a brief overview of such sequence to the generality required to understand the construction of dithered hash functions. For details, we refer the reader to reference [1].

Definition 2.2. *A* word *w is a sequence of letters over some finite alphabet. If a word w can be written as xyz (where y is non-empty and x and/or z can be empty), then y is called a* factor *of w. A word w is called* square free *if no factor of w can be represented in the form yy for any non-empty word y.*

Thus, square free words are strongly non-periodic and non-repeating. A much stronger notion of non-repeating word is *abelian square free word* which Rivest used in his construction.

Definition 2.3. *A word w is said to be* abelian square free *if it cannot be written in the form $w = xyy'z$, where y is a non-empty word and y' is a permutation of y.*

To capture the idea correctly, abcbca is square free, but not abelian square free as abc is followed by bca which is a permutation of abc.

Rivest construction. Let $\mathbf{z} = \{z_i\}_{i=0}^{\infty}$ be any abelian square free dithering sequence, then the construction of Rivest is

$$h_i = f(h_{i-1}, M_i, z_i) \quad \text{for all } i \in [l],$$

where $|M_i| + |z_i| = b$ and $\mathcal{DH}^f := h_l$.

2.3 Random graph theory

Our analysis uses some basic notions from graph theory (for more information, see a standard textbook such as Bondy and Murty [7]). An *undirected graph* $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ consists of a finite set of *vertices* (or *nodes*), $\mathcal{V}$, and a finite set of *edges*, $\mathcal{E}$, where an edge joins two distinct vertices. The edge joining two vertices u and v is denoted by the pair (u, v) or (v, u), or more briefly by uv or vu, and the vertices u and v are called *adjacent* vertices. A *path* is a finite set of vertices $(v_1, \ldots, v_k)$, such that v_i and v_{i+1} are adjacent for $1 \leq i \leq k-1$. If it is possible to reach any vertex from any other vertex in the graph via some finite path, then the graph is *connected.* If there exists a set of edges, no two of which share a vertex, then the set of edges is called a *matching.* M is a *maximum matching* in $\mathcal{G}$ if no matching in $\mathcal{G}$ contains more edges than M does. If a matching M contains every vertex of $\mathcal{G}$, then M is called a *perfect matching* or a *one-factor.*

All the above-defined characteristics of graph are preserved under any relabelling of the vertices. We term such a characteristics of a graph as a *property.* More formally, we have the following definition.

Definition 2.4. *A* graph property *is defined to be a predicate that is preserved under all possible isomorphisms of a graph. A property of a graph is* monotone *if the property is preserved by addition of arbitrary new edges to the graph.*

Many natural properties of graphs are monotone properties, e.g., being connected, being two-connected, containing a Hamiltonian cycle, containing a perfect matching, containing a triangle, etc.

In this paper, we deal with random graphs. An *Erdős-Rényi random graph*, $\mathcal{G}(\nu, p)$, is a graph on ν labelled vertices, obtained by selecting each pair of vertices to be an edge randomly and independently with a fixed probability p. When we use this graph, we say we are *working in the Erdős-Rényi model.*

The probability p has a very important role, as it can be seen as a parameter which determines the sparsity or density of the graph. As p ranges from 0 to 1, the graph becomes more and more dense on average. Moreover, many natural monotone graph-theoretic properties become true within a very small range of values of p. More precisely, given a monotone graph-theoretic property, there is typically a value of p (which will be a function of ν, the number of vertices) called the called *threshold function*. The given property holds in the model $\mathcal{G}(\nu, p)$ with probability close to 0 for p significantly less than the threshold, and the property holds with probability close to 1 for p significantly greater than the threshold. Formally, the notion of a threshold function is defined as follows:

Definition 2.5. *[7, p. 347] A function $t(\nu)$ is a* threshold function *for a monotone property P if, whenever $p \ll t(\nu)$, then $\mathcal{G}(\nu, p)$ does not satisfy P asymptotically almost surely, and whenever $p \gg t(\nu)$, then $\mathcal{G}(\nu, p)$ satisfies P asymptotically almost surely.*

Here the phrase *asymptotically almost surely* means with probability tending to 1 as $\nu \to \infty$. We sometimes abbreviate this phrase to *a.a.s.*

2.4 Random intersection graphs

Let $\mathcal{V}$ be a set (of vertices) with $|\mathcal{V}| = \nu$, and let F be a set (of colours) with $|F| = m$. For each $v \in \mathcal{V}$, let F_v be a subset of the set F of colours. The *intersection graph* $\mathcal{G}(\{F_v\})$ has vertex set $\mathcal{V}$, and has an edge uv if and only if $F_u \cap F_v \neq \emptyset$.

There are various models for *random* intersection graphs, where the sets F_v in an intersection graph are chosen independently using some probability distribution on the subsets of F that does not depend on v. The most widely studied model is the *binomial random intersection graph* $\mathcal{G}_{\text{bin}}(n, m, p)$ introduced by Singer-Cohen [26], where p is a real number such that $0 \leq p \leq 1$. In this model, we choose F_v by selecting each colour $f \in F$ to lie in F_v independently with probability p. The term 'binomial' comes from an alternative way of generating $\mathcal{G}_{\text{bin}}(n, m, p)$, which can be described as follows. To choose the set F_v, first choose $k_v \in \{0, 1, 2, \dots, m\}$ according to the binomial distribution $\mathsf{Bin}(m, p)$ (so the probability that $k_v = i$ is $\binom{m}{i} p^i (1-p)^{m-i}$). Then choose F_v uniformly from the set of all k_v-subsets of F.

We will also consider the *uniform random intersection graph* $\mathcal{G}_{\text{u}}(\nu, m, L)$, where L is an integer. Here we choose each subset F_v uniformly (and independently) from the L-subsets of F. Here the term 'uniform' comes from the fact that all subsets F_v have the same size, rather than anything to do with the uniform distribution.

Our main object of study is the *Sampling With Replacement random intersection graph* (or *SWR random intersection graph*) $\mathcal{G}_{\text{swr}}(\nu, m, L)$, where L is an integer. In this model, F_v is the result of sampling L times from F, with replacement.

We should note that random intersection graphs have been already been applied to cryptography: these graphs have been used [4, 22] to model the effectiveness of the Eschenauer-Gligor key predistribution scheme for wireless sensor networks [10].

3 Analysis of the complexity of constructing a diamond structure

We begin by recalling the analysis provided by Kelsey and Kohno [15]. Before we begin, we note that this analysis implies that $n > k$. Kelsey and Kohno [15] argued as follows:

> *The work done to build the diamond structure is based on how many messages must be tried from each of 2^k starting values, before each has collided with at least one other value. Intuitively, we can make the following argument, which matches experimental data for small parameters: When we try $2^{n/2+k/2+1/2}$ messages spread out from*

> *2^k starting hash values (lines), we get $2^{n/2+k/2+1/2-k}$ messages per line, and thus between any pair of these starting hash values, we expect about $(2^{n/2+k/2+1/2-k})^2 \times 2^{-n} = 2^{n+k+1-2k-n} = 2^{-k+1}$ collisions. We thus expect about $2^{-k+k+1} = 2$ other hash values to collide with any given starting hash value.*

We agree with this conclusion. Unfortunately, we will prove that this line of reasoning does not imply that the 2^k nodes can be paired up in such a way that we get 2^{k-1} collisions. It is useful to think of this problem in a graph-theoretic setting. Suppose we label the nodes as $1, 2, \dots, 2^k$. Then we construct a graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ in the following manner. The vertex set is $\mathcal{V} = \{v_1, \dots, v_{2^k}\}$ and $(v_i, v_j) \in \mathcal{E}$ if the nodes i and j collide at the next level of the diamond structure. $\mathcal{G}$ is an SWR random intersection graph (and we will treat it as such later), but based on the analysis above it seems reasonable to model $\mathcal{G}$ by a random graph in $\mathcal{G}(2^k, 2^{-k+1})$. Now, the question is if this random graph contains a perfect matching, as this is precisely what is required in order to be able to find the desired 2^{k-1} pairs of collisions.

Unfortunately, random graph theory tells us that it is very unlikely that there is a perfect matching in a random graph in $\mathcal{G}(2^k, 2^{-k+1})$. This is because Erdös and Rényi [9] proved that the threshold function for having a perfect matching in $\mathcal{G}(\nu, p)$ (for ν even) is $\ln \nu/\nu$. The class of random graphs $\mathcal{G}(2^k, 2^{-k+1})$ has $p = 2/\nu$, which is well below the required threshold. Note also that the threshold function for not having an isolated vertex is $\ln \nu/\nu$ [8], and a graph that contains an isolated vertex obviously cannot contain a perfect matching.

3.1 Fixing the problem

In view of the above discussion concerning the threshold function for having a perfect matching, we assume that a random graph in $\mathcal{G}(\nu, \ln \nu/\nu)$ will have a perfect matching. We proceed in a similar manner to [15]. Suppose we construct $\nu = 2^k$ lists, each containing L messages. The probability that any two given messages collide under H is 2^{-n}. The probability that no message in one list collides with a message in another list can be estimated to be

$$\left(1 - \frac{1}{2^n}\right)^{L^2} \approx 1 - \frac{L^2}{2^n}.$$

The probability (which we denote by p) that there is at least one collision between two given lists is

$$p \approx \frac{L^2}{2^n}. \tag{1}$$

In view of our analysis above, we want

$$p \approx \frac{\ln \nu}{\nu}.$$

Recalling that $\nu = 2^k$, it is clear that we need to take

$$L \approx \sqrt{k \ln 2} \times 2^{(n-k)/2} \approx 0.83 \times \sqrt{k} \times 2^{(n-k)/2}. \tag{2}$$

The *message complexity* (i.e., the number of hash computations) at level 0 is therefore

$$2^k L \approx 0.83 \times \sqrt{k} \times 2^{(n+k)/2}. \tag{3}$$

Ignoring constant factors, this is a factor of about $\sqrt{k}$ bigger than the estimate in [15].

Remark. If we take $L = 2^{(n-k+1)/2}$ in (1), then we obtain $p \approx 2^{-k+1}$, in agreement with [15].

Theorem 1. *The total message complexity required to construct a 2^k-diamond structure using the Kelsey–Kohno algorithm is $\Theta(\sqrt{k} \times 2^{(n+k)/2})$.*

Proof. The entire diamond structure requires finding collisions at levels $0, 1, \ldots, k-1$. The above analysis shows that, at level ℓ, the message complexity is about $0.83 \times \sqrt{k-\ell} \times 2^{(n+k-\ell)/2}$. Therefore the total message complexity is

$$\begin{aligned}
\sum_{\ell=0}^{k-1} 0.83 \times \sqrt{k-\ell} \times 2^{(n+k-\ell)/2} &= \sum_{i=1}^{k} 0.83 \times \sqrt{i} \times 2^{(n+i)/2} \\
&= 0.83 \times 2^{n/2} \sum_{i=1}^{k} \sqrt{i} \times 2^{i/2} \\
&< 0.83 \times \sqrt{k} \times 2^{n/2} \sum_{i=1}^{k} 2^{i/2} \\
&= 0.83 \times \sqrt{k} \times 2^{n/2} \times \frac{2^{1/2}(2^{(k+1)/2} - 1)}{2^{1/2} - 1} \\
&= O(\sqrt{k} \times 2^{(n+k)/2}). \qquad (4)
\end{aligned}$$

For the lower bound, we have

$$\begin{aligned}
\sum_{\ell=0}^{k-1} 0.83 \times \sqrt{k-\ell} \times 2^{(n+k-\ell)/2} &= \sum_{i=1}^{k} 0.83 \times \sqrt{i} \times 2^{(n+i)/2} \\
&= 0.83 \times 2^{n/2} \sum_{i=1}^{k} \sqrt{i} \times 2^{i/2} \\
&> 0.83 \times \sqrt{\frac{k}{2}} \times 2^{n/2} \times \sum_{i=k/2}^{k} 2^{i/2} \\
&= 0.83 \times \sqrt{\frac{k}{2}} \times 2^{n/2} \times \frac{2^{k/4}(2^{(k/2+1)/2} - 1)}{\sqrt{2} - 1} \\
&= \Omega(\sqrt{k} \times 2^{(n+k)/2}).
\end{aligned}$$

The result follows. □

3.2 Computational complexity

So far, we have only considered the message complexity of constructing the diamond structure. In this section, we look at the computational complexity. The computational complexity of constructing a diamond structure has not previously been considered in the literature. However, this clearly is an important and relevant issue if these structures are ever going to be implemented in a real attack.

There are three main steps required to proceed from one level of the diamond structure to the next. As before, we start by analyzing the work done to go from level 0 to level 1 (the work done at other levels can be analyzed in the same way).

1. Compute $L = 0.83 \times \sqrt{k} \times 2^{(n-k)/2}$ hash values for each of the 2^k lists.
2. Construct the associated graph, i.e., for each pair of lists, determine if there is a common hash value.
3. Determine if the associated graph contains a perfect matching.

Under the assumption that each hash computation takes unit time, the complexity of step 1 is just the message complexity, which we have already computed to be $\Theta(2^k L)$ in (3).

In step 2, we have to search every pair of lists for a repeated value. Various solutions are possible. Asymptotically, we cannot do better than concatenating all the lists, sorting them, and then performing a single pass through the sorted list to detect duplicates. The total time is therefore

$$O(2^k L \log(2^k L)).$$

In step 3, we need to find a perfect matching in a graph on 2^k vertices. Motwani [20] gives a randomised algorithm that finds a maximal matching (with high probability) in a graph with ϵ edges and with average degree at least $\ln \nu$ in time $O\left((\epsilon \log \nu)/(\log\log \nu)\right)$. (The best known algorithm under worst case analysis is due to Micali and Vazirani [19]; the running time is $O(\epsilon\sqrt{\nu})$. However, for our purposes, the randomized algorithm of Motwani suffices.) In our case, we have a graph that almost surely contains a perfect matching and the expected number of edges is $k \times 2^k$, so an algorithm that finds a maximum matching will in fact find a perfect matching. This will take time

$$O\left(\frac{k^2 2^k}{\log k}\right).$$

Combining the three steps, we see that the total time required at level 0 is

$$O\left(2^k L + 2^k L \log(2^k L) + \frac{k^2 2^k}{\log k}\right) = O\left(2^k L \log(2^k L) + \frac{k^2 2^k}{\log k}\right).$$

Recall from (2) that $L = \Theta(\sqrt{k} \times 2^{(n-k)/2})$. Then we have

$$\begin{aligned} 2^k L \log(2^k L) &= \Theta(\sqrt{k} \times 2^{(n+k)/2} \times \log(\sqrt{k} \times 2^{(n+k)/2})) \\ &= \Theta\left(\sqrt{k} \times 2^{(n+k)/2} \times \left(\frac{n+k}{2} + \frac{1}{2}\log k\right)\right) \\ &= \Theta(\sqrt{k} \times 2^{(n+k)/2} \times n), \end{aligned} \tag{5}$$

since $k < n$.

The total computation time at level 0 is thus

$$O\left(\sqrt{k} \times 2^{(n+k)/2} \times n + \frac{k^2 2^k}{\log k}\right). \tag{6}$$

Finally, we determine the total computation time over all k levels. From (6), this total is seen to be

$$O\left(\sum_{\ell=0}^{k-1} n \times \sqrt{k-\ell} \times 2^{(n+k-\ell)/2} + \frac{(k-\ell)^2 2^{k-\ell}}{\log(k-\ell)}\right). \tag{7}$$

The first part of the sum is just the message complexity multiplied by n. For the second part, note that

$$\begin{aligned} \sum_{\ell=0}^{k-2} \frac{(k-\ell)^2 \times 2^{k-\ell}}{\log(k-\ell)} &< \sum_{\ell=0}^{k-2} \left((k-\ell)^2 \times 2^{k-\ell}\right) \\ &= \underbrace{\sum_{i=1}^{k} \left(i^2 \times 2^i\right)}_{S} - 2. \end{aligned} \tag{8}$$

We now evaluate the sum S

$$\begin{aligned} S &= 1^2 \times 2 + 2^2 \times 2^2 + 3^2 \times 2^3 + \cdots k^2 \times 2^k \qquad (9) \\ 2S &= 1^2 \times 2^2 + 2^2 \times 2^3 + 3^2 \times 2^4 \cdots (k-1)^2 \times 2^k + k^2 \times 2^{k+1} \qquad (10) \end{aligned}$$

(10)−(9) yields

$$S = k^2 \times 2^{k+1} - \sum_{i=1}^{k} (i^2 - (i-1)^2) \times 2^i = O(k^2 \times 2^k) \tag{11}$$

Combining equations (7) and (11), we have the total computation time as,

$$O(n \times \sqrt{k} \times 2^{(n+k)/2} + k^2 \times 2^k) = O(n \times \sqrt{k} \times 2^{(n+k)/2}),$$

since $n > k$. We can summarize it as the following theorem.

Theorem 2. *If each hash computation takes unit time, the computational complexity of constructing a 2^k-diamond structure using the Kelsey–Kohno algorithm is*

$$O(n \times \sqrt{k} \times 2^{(n+k)/2}). \tag{12}$$

Therefore, the computational complexity is n times the message complexity.

4 Analysis of diamond structures using random intersection graphs

The analysis carried out in the previous section used the Erdös-Rényi model for random graphs. It was straightforward but a slight simplification of the real picture. To be specific, the Erdös-Rényi model does not exactly capture the way in which the diamond structure is constructed. In this section, we perform a more rigorous analysis using the setting of random intersection graphs. However, we will see that this does not change any of the conclusions reached in the previous section.

We are interested in analysing the SWR random intersection graph $\mathcal{G}$ from the previous section directly, rather than modelling it as an Erdős-Rényi random graph. So we want to find a threshold function for the existence of a perfect matching in an SWR random intersection graph. We only consider the case when $m > \nu$, as this is the case of interest for our application. Roughly speaking, we prove that $L^2\nu/(m \ln \nu)$ is a threshold for a perfect matching. More precisely, we prove the following theorem.

Theorem 3. *Let $\alpha > 1$ be a fixed real number. Let m and L be functions of an integer ν, and suppose that $L \le m = \lfloor \nu^\alpha \rfloor$.*

(i) *Whenever*

$$\liminf_{\nu \to \infty} \frac{L^2 \nu}{m \ln \nu} < 1, \tag{13}$$

then asymptotically almost surely $\mathcal{G}_{\mathrm{swr}}(\nu, m, L)$ does not contain a perfect matching.

(ii) *Whenever*

$$\liminf_{\nu \to \infty} \frac{L^2 \nu}{m \ln \nu} > 1, \tag{14}$$

then asymptotically almost surely $\mathcal{G}_{\mathrm{swr}}(\nu, m, L)$ contains a perfect matching when ν is even.

Our proof of Theorem 3 uses a combination of known techniques from the theory of random intersection graphs, in particular from [4, 5, 11, 12, 24, 26]. We believe that the condition that

$m = \lfloor \nu^\alpha \rfloor$ can be replaced by the weaker condition that $\nu \log \nu = o(m)$, without changing the proof of the theorem significantly. We also believe that the perfect matching threshold will have a different form when $\alpha \leq 1$.

Proof. We begin by proving Part (i) of the theorem. Assume that the condition (13) holds. The proof works by observing that the SWR graph $\mathcal{G}_{\mathrm{swr}}(\nu, m, L)$ is closely related to the uniform random intersection graph $\mathcal{G}_{\mathrm{u}}(\nu, m, L)$ (indeed, there is a simple coupling between these two graphs). For we may generate an instance of the uniform random intersection graph by a two stage process, as follows. We first generate an instance G of an SWR-graph, where $G = \mathcal{G}(\{F_v\})$. For each vertex $v \in \mathcal{V}$, we then construct a subset F'_v of size L by adding $L - |F_v|$ distinct colours from $F \setminus F_v$ uniformly and independently at random to F_v. We may do this, since $|F_v| \leq L$. It is now easy to check that the graph $G' = \mathcal{G}(\{F'_v\})$ is an instance of a uniform random intersection graph. Since $F_v \subseteq F'_v$ for all $v \in V$, we see that G is a subgraph of G' and so G' has a perfect matching whenever G has a perfect matching. So the probability that $\mathcal{G}_{\mathrm{swr}}(\nu, m, L)$ has no perfect matching is bounded below by the probability that $\mathcal{G}_{\mathrm{u}}(\nu, m, L)$ has no perfect matching. But Blackburn and Gerke [4, Theorem 2] show that a.a.s. $\mathcal{G}_{\mathrm{u}}(\nu, m, L)$ has an isolated vertex when $\liminf_{\nu\to\infty}(L^2\nu/(m \ln \nu) < 1$, and so in particular a.a.s. $\mathcal{G}_{\mathrm{u}}(\nu, m, L)$ does not have a perfect matching. This establishes Part (i) of the theorem.

We now prove Part (ii) of the theorem. Suppose that (14) holds, so there exists a positive real number ϵ so that $L^2\nu/(m \ln \nu) \geq 1 + \epsilon$ for all sufficiently large integers ν. The probability of $\mathcal{G}_{\mathrm{swr}}(\nu, m, L)$ possessing a perfect matching increases as L increases so, by replacing L by a smaller function of ν if necessary, it suffices to prove the theorem in the case when

$$\frac{L^2\nu}{m \ln \nu} \to 1 + \epsilon \text{ as } \nu \to \infty.$$

Define

$$\tilde{p} = (1 + \epsilon')\sqrt{\frac{\ln \nu}{m\nu}},$$

where ϵ' is a positive real number so that $1 + \epsilon' < \sqrt{1+\epsilon}$. Since

$$L \to \sqrt{1+\epsilon}\sqrt{\frac{m \ln \nu}{\nu}}$$

there exist constants c and c' with $1 < c$ and $c' < 1$ and such that

$$\tilde{p}m < c\tilde{p}m < c'L < L \tag{15}$$

for all sufficiently large ν.

We define the following process, which produces a pair (G, G') of graphs. For each vertex v, choose (uniformly and independently) a random bijection $f_v : \{1, 2, \ldots, m\} \to F$. Choose (independently) an integer $k_v \in \{0, 1, \ldots, m\}$ according to the distribution $\mathsf{Bin}(m, \tilde{p})$. Choose (independently) an integer $k'_v \in \{1, 2, \ldots, L\}$, with respect to the distribution of the number of distinct elements sampled after L samples with replacement from an m-set. Define $F_v = \{f_v(1), f_v(2), \ldots, f_v(k_v)\}$ and $F'_v = \{f_v(1), f_v(2), \ldots, f_v(k'_v)\}$. Then set $G = \mathcal{G}(\{F_v\})$ and $G' = \mathcal{G}(\{F'_v\})$.

Note that $G = \mathcal{G}_{\mathrm{bin}}(\nu, m, \tilde{p})$ and $G' = \mathcal{G}_{\mathrm{swr}}(\nu, m, L)$. The event that G contains a perfect matching occurs asymptotically almost surely when ν is even, by Rybarczyk [24, Theorem 6]. We aim to prove that the event that G is a subgraph of G' also occurs asymptotically almost surely. This is sufficient to prove the theorem, since the intersection of these two events is a subset of the event that G' contains a perfect matching, and the intersection of two a.a.s. events occurs asymptotically almost surely.

For $v \in V$, let π be the probability that $k_v > k'_v$. (Clearly π does not depend on v.) We have that G is a subgraph of G' whenever $k_v \leq k'_v$ for all $v \in V$, so the event that G is a subgraph of G' occurs with probability at least $1 - \nu\pi$. It remains to show that $\nu\pi \to 0$ as $\nu \to \infty$.

Since $c\tilde{p}m < c'L$ by (15),

$$\pi \leq \Pr(k_v \geq c\tilde{p}m) + \Pr(k'_v \leq c'L).$$

Since k_v is chosen according to the distribution $\mathsf{Bin}(m, \tilde{p})$, the Chernoff bound (see Bollobas [6, Corollary 1.4], for example) implies that

$$\Pr(k_v \geq c\tilde{p}m) \leq \exp\left(\frac{-(c-1)^2\tilde{p}m}{3(1-\tilde{p})} + \frac{c-1}{1-\tilde{p}}\right) = o(1/\nu), \tag{16}$$

the final bound following since the leading term of

$$\frac{-(c-1)^2\tilde{p}m}{3(1-\tilde{p})} + \frac{c-1}{1-\tilde{p}} \tag{17}$$

is negative and has order of magnitude $\sqrt{\nu^{\alpha-1}\ln\nu}$. In more detail, we have the following: we see that $\tilde{p} \to 0$, and so $(c-1)(1-\tilde{p}) \to c-1 = O(1)$. We have that $-(c-1)^2 < 0$. Moreover, $\tilde{p}$, m and $1-\tilde{p}$ are all positive. So the first term of (17) is negative. We have that $1/(3(1-\tilde{p})) \to 1/3$ and

$$\tilde{p}m \to (1+\epsilon')\sqrt{(m\ln\nu)/\nu} = (1+\epsilon')\sqrt{\nu^{\alpha-1}\ln\nu},$$

and this clearly tends to infinity faster than $\ln\nu$, since $\alpha > 1$. So (16) holds. Now, we have that

$$\begin{aligned}
\Pr(k'_v \leq c'L) &\leq \binom{m}{\lfloor c'L \rfloor}\left(\frac{c'L}{m}\right)^L \\
&\leq \left(\frac{me}{\lfloor c'L \rfloor}\right)^{c'L}\left(\frac{c'L}{m}\right)^L, \qquad \text{since } \binom{n}{k} \leq \left(\frac{ne}{k}\right)^k \\
&= O\left(e^{c'L}\left(\frac{c'L}{m}\right)^{(1-c')L}\right) \\
&= \exp\big(c'L - (1-c')L\ln(m/(c'L)) + O(1)\big).
\end{aligned}$$

Since $m/(c'L) \to \infty$, we see that the exponent in this expression is negative for sufficiently large ν, and has order of magnitude greater than L. Since $\ln\nu \leq \nu^{\frac{1}{2}(\alpha-1)} = o(L)$, we see that $\Pr(k'_v \leq c'L) = o(1/\nu)$. So

$$\nu\pi \leq \nu\big(\Pr(k_v \geq c\tilde{p}m) + \Pr(k'_v \leq c'L)\big) = o(1),$$

as required. □

To close this section, we show that the estimate obtained in the SWR random intersection graph model agrees with the estimate obtained in the Erdös-Rényi graph model. Recall from Section 3.1 that we determined L by solving the equation $L^2/2^n = \ln\nu/\nu$. In the SWR random intersection graph, we have $m = 2^n$. Theorem 3 says that we should (roughly) take $L^2\nu = m\ln\nu$, which becomes $L^2/2^n = \ln\nu/\nu$, as before. So none of the results change when we carry out the analysis in the SWR random intersection graph model.

5 Revised analysis of the other attacks

The diamond structure has been used in second preimage attacks [3, 2] and in herding attacks [15, 2]. The steps followed in both attacks are the same except that they occur in a different order. In case of a herding attack, the attacker first computes the hash of the prefix, then finds a linking message that links the hash of prefix to one of the intermediate hash values of the diamond structure. Finally, she appends the messages on the path inside the diamond structure from the intermediate node to the root in front of the prefix and the linking message. The suffix is the message formed by appending the linking message with the message on the path.

In the case of finding a second preimage, the attacker first finds a linking message that links the root of the diamond structure to one of the intermediate hash value of the original message. Then she finds a prefix that hashes to one of the nodes at level 0 of the diamond structure. She then appends the messages associated with the edges on the path inside the diamond structure that leads to the root of the diamond structure. The output is the message in the proper order.

We analyze the complexity of some known attacks in light of our revised analysis of the diamond structure. We use the term *offline phase* for the steps carried out by adversary before she is given the challenge and the term *online phase* for the steps followed by adversary after she is provided with the challenge.

5.1 Herding attack on Merkle-Damgård construction

Kelsey and Kohno [15] proposed the construction of diamond structure and the herding attack on Mekle-Damgård construction using the diamond structure. According to their analysis, the message complexity of the attack is $O(2^{(n+k)/2} + 2^{n-k})$. We revisit the attack in the light of our correction of their analysis.

Message complexity

We proceed step by step. We already analyzed the complexity of the construction of the diamond structure. In the online phase, the attacker has to find a linking message that links the hash of the prefix to one of the leaves of the diamond structure. The complexity of finding the linking message is $O(2^{n-k})$. Therefore, from Theorem 1, we can calculate the message complexity of the attack as

$$O(\sqrt{k} \times 2^{(n+k)/2} + 2^{n-k}).$$

From the arithmetic-geometric mean inequality, we can find the minimum of the message complexity by finding the value of k satisfying the following equation

$$n - 3k - \log k = 0$$

The solution to this equation has the form $k = n/3 - \frac{1}{3}\log(n/3) + O(\log n/n) \approx n/3$. For lower values of k, the message complexity is dominated by $O(2^{n-k})$. Therefore, we see the same trend as in [15]. However, for larger values of k, the message complexity is dominated by the construction of diamond structure. In this case, the major contribution is from the term $O(\sqrt{k} \times 2^{(n+k)/2})$ and we see the factor of $\sqrt{k}$ coming in to the picture.

Time complexity

The time complexity of the offline phase is the same as given by Theorem 2. However, in the online phase, we need to find the linking message and then actually find the hash value at the leaves to which it maps. We can safely assume that the nodes at level 0 are sorted by their hash values. This is because, if the nodes are not sorted by their hash values, we can perform the sorting in the offline phase, which takes $O(k \times 2^k)$ time. However, this has no impact in asymptotic analysis as it get subsumed by the complexity of construction of diamond structure (we will use this fact in the sequel and never explicitly mention it). Hence, the time complexity to hash the required number of messages and then to find if it links to any of the leaves is $O(k \times 2^{n-k})$. Therefore, the time complexity comes out to be

$$O(n \times \sqrt{k} \times 2^{(n+k)/2} + k \times 2^{n-k}).$$

The minimum occurs at the solution of the equation

$$n - 3k - 2\log n + \log k = 0.$$

We can proceed as before, to calculate $k = n/3 - \frac{2}{3}\log n + \frac{1}{3}\log(n/3) + O(\log n/n) \approx n/3$. When k is larger than $n/3$, then the time complexity is n times the message complexity and it is k times the message complexity for smaller values of k.

We tabulate the complexity for some fixed values of n and compare our result with the analysis of [15] for certain values of k in Table 1.

5.2 Second preimage attack on dithered hash

The dithered hash construction was proposed by Rivest [23] to counter the second preimage attack of Kelsey and Schenier [16]. However, recently, Andreeva *et al.* [3] proposed an attack based on the diamond construction. For a challenge message M of block length 2^l, the adversary first finds a linking message that links the root of the diamond structure to one of intermediate hash values in the hash computation of M. She then finds a linking message that hashes to one of the intermediate hash values (say N_0) in the diamond structure. The adversary then finds the path inside the diamond structure that leads from N_0 to the root.

The success of the attack depends on the fact that although dithering sequences are non-periodic and non-repeating, they have large size factors. The attack uses such a factor with the messages that are used in the construction of diamond structure. If $Fact_{\mathbf{z}}(\ell)$ denote the number of factors of size ℓ in the sequence $\mathbf{z}$, then Andreeva *et al.* evaluated the message complexity of their attack as

$$O(Fact_{\mathbf{z}}(\ell) \times 2^{n-l} + 2^{n-k} + 2^{(n+k)/2})$$

They also stated following lemmas about two dithering sequences that were advocated by Rivest.

Lemma 4. *For $\ell \leq 85$, for the Keränen sequence [17, 18] $\boldsymbol{z}$, we have*

$$Fact_{\boldsymbol{z}}(\ell) \leq 8l + 332.$$

Lemma 5. *Let $\boldsymbol{c}$ denote the sequence obtained by diluting the Keränen sequence $\boldsymbol{z}$ with a 13-bit*

n	Example	$k = \lfloor n/3 \rfloor$			$k = \lfloor 2n/5 \rfloor$		
		Message Complexity		Time	Message Complexity		Time
		[15]	Actual	Complexity	[15]	Actual	Complexity
128	MD5	2^{85}	2^{88}	2^{96}	2^{89}	2^{93}	2^{100}
160	SHA-1	2^{106}	2^{110}	2^{117}	2^{112}	2^{117}	2^{123}
192	Tiger	2^{128}	2^{131}	2^{139}	2^{134}	2^{138}	2^{145}
256	SHA-256	2^{170}	2^{174}	2^{182}	2^{179}	2^{183}	2^{191}
512	Whirlpool	2^{341}	2^{345}	2^{354}	2^{358}	2^{362}	2^{371}

Table 1: Comparison of complexity of herding attack (all calculations are done without considering the constants.)

counter [23]*. Then for every* $\ell \in [0, 2^{13}]$*, we have*

$$Fact_{\mathbf{c}}(\ell) = 8l + 32760.$$

In other words, if we represent the above dithering sequence by $\mathbf{z}$, the number of factors of size ℓ is bounded by

$$Fact_{\mathbf{z}}(\ell) = O(\ell)$$

Using the Lemma 4 and Lemma 5, the message complexity evaluated by [3] for the second preimage of a 2^l-block message, using a 2^k-diamond structure is

$$O(k \times 2^{n-l} + 2^{n-k} + 2^{(n+k)/2}).$$

We reconsider this analysis in the light of our analysis of diamond structure.

5.2.1 Message complexity

In the attack on the dithered hash, Andreeva *et al* used the same dithering sequence for all edges at the same depth of the diamond structure, and one dithered sequence to connect the root of diamond structure to M. Thus, for a 2^k-diamond structure, the size of dithering sequence they need on the diamond structure is exactly $k+1$. In the worst case, when all the factors have same size in the dithering sequence, the probability that a randomly chosen factor of size k in the sequence $\mathbf{z}$ is the one used in the construction of diamond structure is $(Fact_{\mathbf{z}}(k))^{-1}$. Therefore, the message complexity to connect the root of the diamond structure to M is

$$O(Fact_{\mathbf{z}}(k+1) \times 2^{n-l}) = O(k \times 2^{n-l}). \tag{18}$$

Suppose the root gets linked to the i^{th} iteration of the hashing of M.

We have already calculated the message complexity of the construction of diamond structure in Theorem 1. To find the complexity of the attack, note that the attacker needs to hash a message (let us say M') of block length $i-2-k$, where k is the depth of diamond structure, in order to defy the Merkle-Damgård strengthening. This is upper bounded by 2^k hash computations. Since $k < n$, we see that this has no impact on the asymptotic calculation as it is subsumed by the construction of the diamond structure (we use this fact again in sequel and never explicitly mention it). The message complexity to find a linking message that links $H(M')$ to one of the leaves of the diamond structure is $O(2^{n-k})$. We calculate the message complexity of the second preimage attack on dithered hash function as

$$O\left(2^k + \sqrt{k} \times 2^{(n+k)/2} + 2^{n-k} + k \times 2^{n-l}\right) = O\left(\sqrt{k} \times 2^{(n+k)/2} + 2^{n-k} + k \times 2^{n-l}\right),$$

Under the assumption that $l \approx k$, it can be further simplified to

$$O\left(\sqrt{k} \times 2^{(n+k)/2} + k \times 2^{n-k}\right).$$

5.2.2 Computational complexity

We note that the attack uses the simple diamond structure as constructed in Section 3. Hence, the total time required to construct the diamond structure is as stated in Theorem 2. For the time required in the online phase, note that we need to find the intermediate hash value to which we link the root of the diamond structure. Moreover, we can safely assume that the intermediate hash values in the hash computation of M are sorted. If not, then we first sort them in the online phase, which takes $O(l \times 2^l)$ time. Note that it does not effect the computational complexity, because it is subsumed by the construction of the diamond structure (we implicitly use this fact again in the analysis of second preimage attack on hash twice construction). Hence, it takes a factor of l time more than what is required in message complexity (equation (18)) resulting in total time $O(l \times k \times 2^{n-l})$. Also, as in the herding attack, we need to find the leaf to which the linking message maps. Thus, the time complexity to find that leaf is $O(k \times 2^{n-k})$. Therefore, the total time required for the attack is given by

$$T(k,l) = O\left(k \times 2^{n-k} + k \times l \times 2^{n-l} + n \times \sqrt{k} \times 2^{(n+k)/2}\right).$$

Under the assumption that $k \approx l$, we have

$$\begin{aligned} M(k,l) &= O\left(\sqrt{k} \times 2^{(n+k)/2} + k \times 2^{n-k}\right). \\ T(k,l) &= O\left(k^2 \times 2^{n-k} + n \times \sqrt{k} \times 2^{(n+k)/2}\right). \end{aligned}$$

It is easy to check that the message complexity is minimized when k is the solution of following equation,

$$n - 3k + \log k = 0,$$

which is roughly $n/3$. Following the argument in Section 5.1, we can say that the message complexity of the attack is dominated by $O(k \times 2^{n-k})$ for $k < n/3$ and therefore it is the same as in [3]. However, for large values of k, a factor of $\sqrt{k}$ comes into the picture.

Also, the time complexity is minimized when k satisfies the following equation:

$$n - 3k + 3\log k - \log n = 0$$

We present a comparison of the computational complexity of the attack with the message complexity and compare it with the analysis of [3] in Table 2.

5.3 Herding attack and second preimage attack on hash twice function

Andreeva *et al* [2] proposed a herding attack and a second preimage attack on the hash twice function by building a diamond structure on multicollisions. For a hash twice function of the form defined in Section 2.2, both the attacks constructed Joux's multicollisions on first pass of hash function, and then used the messages that caused the multicollisions to build a diamond structure for the second pass. In total, the attack requires the construction of two diamond structures, one on each of the two passes. In fact, the adversary performs the following steps during the offline phase:

1. Construct a 2^k-diamond structure (let us say $\mathcal{D}_1$) for the first pass.

n	Example	$k = \lfloor n/3 \rfloor$			$k = \lfloor 2n/5 \rfloor$		
		Message Complexity		Time	Message Complexity		Time
		[3]	Actual	Complexity	[3]	Actual	Complexity
128	MD5	2^{89}	2^{91}	2^{95}	2^{90}	2^{93}	2^{100}
160	SHA-1	2^{111}	2^{113}	2^{117}	2^{112}	2^{115}	2^{122}
192	Tiger	2^{132}	2^{134}	2^{139}	2^{134}	2^{138}	2^{145}
256	SHA-256	2^{175}	2^{177}	2^{182}	2^{179}	2^{183}	2^{191}
512	Whirlpool	2^{347}	2^{349}	2^{354}	2^{358}	2^{362}	2^{371}

Table 2: Comparison of message and computational complexity of second preimage attack on dithered hash (all calculations are done without considering the constants).

2. Construct 2^{n-k+r}-multicollisions (let us say $\mathcal{M}$) in front of $\mathcal{D}_1$, where the value of r is to be calculated later. Let the hash value at the end of multi-collision be h_1.

3. Construct a diamond structure (let us say $\mathcal{D}_2$) on the second pass using the messages from the last r blocks of messages in $\mathcal{M}$.

5.3.1 Herding attack on hash twice

After the offline phase, the adversary commits to the hash value at the root of $\mathcal{D}_2$. In the online phase, the adversary is given a prefix P. She calculates $H(P)$ and then finds a linking message, m that links $H(P)$ to one of the leaves of $\mathcal{D}_1$. Using h_1 as inital value, the adversary hashes $P\|m$. She uses the first 2^{n-k}-multicollisions of $\mathcal{M}$ to find the linking message to $\mathcal{D}_2$. Finally, she finds a path inside $\mathcal{D}_2$ that leads to the root. Andreeva *et al* [2] calculated the total message complexity of the attack to be $O(2^{n-k} + 2^{(n+k)/2})$. We next perform a more detailed analysis of the attack and compute the message complexity and the computational complexity of the attack.

Message complexity

Step 1 is the simple diamond construction for which we gave a detailed analysis in Section 3. To find the complexity of Step 2, we need to calculate the value of r, the number of blocks of messages required to construct the second diamond structure. Since, we need $0.83 \times \sqrt{k-\ell} \times 2^{(n+k-\ell)/2}$ messages to herd from level ℓ to level $(\ell + 1)$, the total number of multicollisions required to construct the diamond structure is

$$C = \sum_{\ell=0}^{k-1} 0.83 \times \sqrt{k-\ell} \times 2^{(n+k-\ell)/2} = \Theta(\sqrt{k} \times 2^{(n+k)/2}).$$

The last equality is due to equation (4). Hence, the message complexity to find a 2^{n-k+r}-multicollision is

$$\Theta\left(((n-k) + \log C)\, 2^{n/2}\right) = \Theta(n \times 2^{n/2}) \tag{19}$$

For Step 3, we find the message complexity to go from level 0 to level 1 (the rest of them can be done analogously). Note that every message that needs to be hashed is in fact of block length $\log 2^k L$ and there are $2^k L$ such messages. From equation (5), the total hash computation is,

$$2^k L \log 2^k L = \Theta(n \times \sqrt{k} \times 2^{(n+k)/2}).$$

Therefore, the message complexity to construct $\mathcal{D}_2$ is

$$\Theta\left(\sum_{\ell=0}^{k-1} \sqrt{k-\ell} \times 2^{(n+k-\ell)/2} \times n\right) = \Theta(n \times \sqrt{k} \times 2^{(n+k)/2}). \tag{20}$$

For the online phase, we comment that the total time is the time required to find the two linking messages (one to $\mathcal{D}_1$ and another one to $\mathcal{D}_2$). The work done to find the linking message to $\mathcal{D}_1$ is simply 2^{n-k}. However, the message complexity to find the linking message to $\mathcal{D}_2$ is $O((n-k)\times 2^{n-k})$, because each message is $n-k$ blocks long. Therefore, the total message complexity in the online phase is

$$O((n-k) \times 2^{n-k}) = O(n \times 2^{n-k}) \tag{21}$$

Using equation (4) and (19)$-$(21), the message complexity for the attack is

$$O\left(\sqrt{k} \times 2^{(n+k)/2} + n \times \left(2^{n/2} + \sqrt{k} \times 2^{(n+k)/2} + 2^{n-k}\right)\right) = O\left(n \times \left(\sqrt{k} \times 2^{(n+k)/2} + 2^{n-k}\right)\right).$$

Computational complexity

Since $\mathcal{D}_1$ is a simple diamond structure, we note that the time required to construct $\mathcal{D}_1$ is the same as equation (12). Also, Step 2 is just finding the required number of multicollisions. Therefore, its time complexity equals the message complexity of finding the required number of multicollisions, which is precisely equal to equation (19). For the final part of the attack, we analyze each step of Section 3.2 for the construction of $\mathcal{D}_2$ for level 0 (the other levels are analyzed analogously). Recall that to proceed from one level to the next in a diamond structure, we first hash certain lists of messages, construct an associated graph by creating an edge when a pair of lists has a common hash value, and then find a perfect matching on that graph.

For the construction of $\mathcal{D}_2$, we have L lists of messages for each of 2^k hash values, but now all the messages are $\log(2^k L)$ blocks long. Using equation (5), we calculate the total time required to hash the $2^k L$ lists as

$$2^k L \log(2^k L) = \Theta(\sqrt{k} \times 2^{(n+k)/2} \times n).$$

Now, we comment that the time complexity to construct the associated graph and then to find a perfect matching in that graph for $\mathcal{D}_2$ is same as in the construction of a simple diamond structure. This is because we need to sort the same number of hash values (which defines the complexity of the construction of the graph) and we have the same number of vertices, the same expected number of edges, and the same average degree (which determines the complexity of finding a perfect matching). Therefore, the total time required at level 0 is,

$$O\left(2^k L \log(2^k L) + 2^k L \log(2^k L) + \frac{k^2 2^k}{\log k}\right) = O\left(2^k L \log(2^k L) + \frac{k^2 2^k}{\log k}\right).$$

Note that this is same as in the construction of simple diamond structure. Hence, the time complexity of the construction of $\mathcal{D}_2$ is the same as equation (12).

Arguing in a similar fashion as in the previous cases for the online phase, we comment that the total time is k times the message complexity to link the message. Therefore, the total time complexity of the attack (pre-computation and online phase) is

$$O\left(n \times \left(2^{n/2} + \sqrt{k} \times 2^{(n+k)/2} + k \times 2^{n-k}\right)\right) = O\left(n \times \left(\sqrt{k} \times 2^{(n+k)/2} + k \times 2^{n-k}\right)\right).$$

Therefore, the message complexity of the attack on hash twice is just n times the message complexity of the herding attack of Kelsey and Kohno (see Section 5.1 and compare Table 1 and Table 3).

5.3.2 Second preimage attack on hash twice

Let M be a 2^l blocks long challenge message for the adversary. The steps followed by the adversary are similar to the herding attack. The only additional step for the adversary is in the online phase when she creates the prefix of the required block length that links to one of the leaves of $\mathcal{D}_1$ and has to find a linking message that links the root of $\mathcal{D}_2$ to one of the intermediate hash values in the second pass of M. The analysis of [2] showed the message complexity of the attack is $O(2^{n-k} + 2^{(n+k)/2} + 2^{n-l})$. We perform a more detailed analysis and tabulate the effect of the difference in the Table 3.

Let M be a 2^l block challenge message for the adversary. The steps followed by the adversary are similar to the herding attack. She creates two diamond structures $\mathcal{D}_1$ and $\mathcal{D}_2$ in a similar manner as in the herding attack. The only additional step for the adversary is in the online phase when she creates the prefix of the required block length that links to one of the leaves of $\mathcal{D}_1$ and has to find a linking message that links the root of $\mathcal{D}_2$ to one of the intermediate hash values in the second pass of M. Hence, the total hash computation is $O(2^{n-k})$ for finding the linking message to $\mathcal{D}_1$ and $O(2^{n-l})$ to find the linking message from the root of $\mathcal{D}_2$ to one of the intermediate hash values in the second pass of M. However, every message that the adversary uses to link to $\mathcal{D}_2$ is $n-k$ blocks long. Therefore, the number of hash computations the adversary has to perform is $O((n-k) \times 2^{n-k})$. Thus the total message complexity of the online phase is

$$O(2^{n-l} + (n-k) \times 2^{n-k} + 2^{n-k}) = O(2^{n-l} + n \times 2^{n-k}).$$

We can now estimate the message complexity as

$$O\left(n \times (2^{n-k} + \sqrt{k} \times 2^{(n+k)/2}) + 2^{n-l}\right).$$

Arguing in a similar fashion for the online phase as in Section 5.2.2, we can say that the time complexity for linking the message to the diamond structure is k times the message complexity, and the time complexity for linking the root of $\mathcal{D}_2$ to one of the intermediate hash value in the hash computation of M is l times its message complexity. Therefore, the time complexity comes out to be

$$O\left(n \times (\sqrt{k} \times 2^{(n+k)/2} + k \times 2^{n-k}) + l \times 2^{n-l}\right)$$

n	Example	$k = \lfloor n/3 \rfloor$			$k = \lfloor 2n/5 \rfloor$		
		Message Complexity		Time	Message Complexity		Time
		[2]	Actual	Complexity	[2]	Actual	Complexity
128	MD5	2^{85}	2^{95}	2^{98}	2^{90}	2^{100}	2^{102}
160	SHA-1	2^{107}	2^{117}	2^{120}	2^{112}	2^{122}	2^{125}
192	Tiger	2^{128}	2^{139}	2^{142}	2^{134}	2^{145}	2^{148}
256	SHA-256	2^{171}	2^{182}	2^{185}	2^{179}	2^{191}	2^{194}
512	Whirlpool	2^{341}	2^{354}	2^{358}	2^{358}	2^{371}	2^{375}

Table 3: Comparison of message complexity of second preimage attack (assuming $l \approx k$) on hash twice construction (all calculations are done without considering the constants).

Remark. We can analyze the time and the message complexity of the herding attack on concatenated hash functions of the form

$$H^{f_1}(M) \| H^{f_2}(M),$$

where f_1 and f_2 can be the same or different compression functions, in a similar fashion as in Section 5.3. This is because the basic construction is the same as for the hash twice function. The only difference lies in the commitment stage, where the adversary commits to the $h_1 \| h_2$, where h_1 is the hash value as in Step 2 of the herding attack on hash twice, and h_2 is the hash value of the root of $\mathcal{D}_2$ constructed in the attack.

6 Conclusion

In this paper, we pointed out that the analysis of diamond structure proposed by Kelsey-Kohno is not complete and may not yield the desired structure. We also gave a rigorous analysis of the construction of the diamond structure using concepts from random graph theory. There are some consequences of this, as enumerated below:

1. Our analysis showed that the message complexity of the construction of a 2^k-diamond structure is about $\sqrt{k}$ times more than [15] claimed (Theorem 1).

2. We also showed that the computational complexity of the construction of a diamond structure is n times the message complexity (Theorem 2).

3. For the Merkle-Damgård construction, the ratio of time complexity and the message complexity of the attacks is k if we choose the value of k to be strictly less than $n/3$ and it is n if we choose k to be larger than $n/3$.

4. For the hash twice construction and concatenated hash functions, the ratio of computational and message complexity is linear in k when k is strictly less than $n/3$, and it is constant for larger values of k.

We summarize the values of k to minimize message complexity in Table 4 and to minimize computational complexity in Table 5 for different attacks. We summarize our results on the message complexity in Table 6 and time complexity in Table 7.

References

[1] J. P. Allouche and J. Shallit. *Automatic Sequences: Theory, Applications, Generalizations.* Cambridge University Press, Cambridge, UK, 2003.

[2] E. Andreeva, C. Bouillaguet, O. Dunkelman, and J. Kelsey. Herding, second preimage and Trojan message attacks beyond Merkle-Damgård. In *Selected Areas in Cryptography*, volume 5867 of *Lecture Notes in Computer Science*, pages 393–414, 2009.

[3] E. Andreeva, C. Bouillaguet, P. A. Fouque, J. J. Hoch, J. Kelsey, A. Shamir, and S. Zimmer. Second preimage attacks on dithered hash functions. In *EUROCRYPT*, volume 4965 of *Lecture Notes in Computer Science*, pages 270–288, 2008.

[4] S. R. Blackburn and S. Gerke. Connectivity of the uniform random intersection graph. *Discrete Mathematics*, 309(16):5130–5140, 2009.

[5] M. Bloznelis, J. Jaworski, and K. Rybarczyk. Component evolution in a secure wireless sensor network. *Networks*, 53(1):19–26, 2009.

[6] B. Bollobás. *Random Graphs (2nd Edition).* Cambridge University Press, Cambridge, UK, 2001.

[7] J. A. Bondy and U. S. R. Murty. *Graph Theory.* Springer, 2008.

[8] P. Erdös and A. Renyi. On the evolution of random graphs. In *Proceedings of the Hungarian Academy of Sciences*, volume 5, pages 17–61, 1960.

[9] P. Erdös and A. Rényi. On the existence of a factor of degree one of a connected random graph. *Acta Mathematica Academiae Scientiarum Hungaricae Tomus*, 17(3–4):359–368, 1966.

[10] L. Eschenauer and V. Gligor. A key-management scheme for distributed sensor networks. In *Proc. 9th ACM conference on Computer and Communications Security*, pages 41–47, 2002.

[11] J. A. Fill, E. R. Scheinerman, and K. B. Singer-Cohen. Random intersection graphs when $m = \Omega(n)$: An equivalence theorem relating the evolution of the $g(n, m, p)$ and $g(n, p)$ models. *Random Struct. Algorithms*, 16(2):156–176, 2000.

[12] E. Godehardt and J. Jaworski. Two models of random intersection graphs for classification. In O. Optiz and M. Schwaiger, editors, *Studies in Classification, Data Analysis and Knowledge Organization*, volume 22, pages 67–82. Springer, Berlin, 2003.

n	Example	Herding Attack	Second Preimage on Dithered Hash	Herding and Second Preimage on Hash Twice
128	MD5	41	45	41
160	SHA-1	52	55	52
192	Tiger	62	66	62
256	SHA-256	83	88	83
512	Whirlphool	168	173	168

Table 4: Values of k to get minimum message complexity (assuming $l \approx k$)

n	Example	Herding Attack	Second Preimage on Dithered Hash	Herding and Second Preimage on Hash Twice
128	MD5	40	43	45
160	SHA-1	48	54	55
192	Tiger	61	65	66
256	SHA-256	82	87	87
512	Whirlphool	166	172	173

Table 5: Values of k to get minimum time complexity (assuming $l \approx k$)

	Message Complexity
Herding attack on Merkle-Damgård	$O(\sqrt{k} \times 2^{(n+k)/2} + 2^{n-k})$
Second Preimage on Dithered Hash	$O(\sqrt{k} \times 2^{(n+k)/2} + 2^{n-k} + k \times 2^{n-l})$
Herding attack on Hash Twice	$O(n \times (\sqrt{k} \times 2^{(n+k)/2} + 2^{n-k}))$
Second Preimage on Hash Twice	$O(n \times (\sqrt{k} \times 2^{(n+k)/2} + 2^{n-k}) + 2^{n-l})$

Table 6: Message complexity for various attacks

	Time Complexity
Herding attack on Merkle-Damgård	$O(n \times \sqrt{k} \times 2^{(n+k)/2} + k \times 2^{n-k})$
Second Preimage on Dithered Hash	$O(n \times \sqrt{k} \times 2^{(n+k)/2} + k \times 2^{n-k} + l \times k \times 2^{n-l})$
Herding attack on Hash Twice	$O(n \times (k \times 2^{n-k} + \sqrt{k} \times 2^{(n+k)/2}))$
Second Preimage on Hash Twice	$O(n \times (k \times 2^{n-k} + \sqrt{k} \times 2^{(n+k)/2}) + l \times 2^{n-l})$

Table 7: Time complexity for various attacks

[13] A. Joux. Multicollisions in iterated hash functions. Application to cascaded constructions. In *CRYPTO*, volume 3152 of *Lecture Notes in Computer Science*, pages 306–316, 2004.

[14] J. Katz and Y. Lindell. *Introduction to Modern Cryptography.* Chapman and Hall, CRC Press, 2007.

[15] J. Kelsey and T. Kohno. Herding hash functions and the Nostradamus attack. In *EUROCRYPT*, volume 4004 of *Lecture Notes in Computer Science*, pages 183–200, 2006.

[16] J. Kelsey and B. Schneier. Second preimages on n-bit hash functions for much less than 2^n work. In *EUROCRYPT*, volume 3494 of *Lecture Notes in Computer Science*, pages 474–490, 2005.

[17] V. Keränen. Abelian squares are avoidable on 4 letters. In *ICALP*, pages 41–52, 1992.

[18] V. Keränen. On abeliean square-free DT0L-languages over 4 letters. In *Proceedings of Conference on Combinatorics on Words*, pages 41–52, 2003.

[19] S. Micali and V. V. Vazirani. An $\mathrm{O}(m\sqrt{n})$ algorithm for finding maximum matching in general graphs. In *FOCS*, pages 17–27, 1980.

[20] R. Motwani. Average-case analysis of algorithms for matchings and related problems. *J. ACM*, 41(6):1329–1356, 1994.

[21] G. Neven, N. Smart, and B. Warinschi. Hash function requirements for schnorr signatures. *Journal of Mathematical Cryptology*, 3:69–87, 2009.

[22] R. D. Pietro, L. Mancini, A. Mei, A. Panconesi, and J. Radhakrishnan. Redoubtable sensor networks. *ACM Trans. Inform. Systems Security*, 11:1–22, 2008.

[23] R. Rivest. Abelian square-free dithering for iterated hash functions. 2005.

[24] K. Rybarczyk. Sharp threshold functions for the random intersection graph via coupling method. http://arxiv.org/abs/0910.0749, November 2009.

[25] V. Shoup. A composition theorem for universal one-way hash functions. In *EUROCRYPT*, volume 1807 of *Lecture Notes in Computer Science*, pages 445–452, 2000.

[26] K. B. Singer-Cohen. *Random intersection graphs.* PhD thesis, Johns Hopkins University, Baltimore, Maryland, 1995.

[27] W. Stallings. *Cryptography and Network Security.* Prentice Hall, 2006.

[28] D. Stinson. *Cryptography: Theory and Practice.* Chapman & Hall/CRC Press Inc., 2006.