Preimage Resistance Beyond the Birthday Barrier – The Case of Blockcipher Based Hashing

Matthias Krause[1], Frederik Armknecht[1], and Ewan Fleischmann[2]

[1] Arbeitsgruppe Theoretische Informatik und Datensicherheit, Universität Mannheim, Germany
[2] Professur für Mediensicherheit, Bauhaus-Universität Weimar, Germany

Abstract. Security proofs are an essential part of modern cryptography. Often the challenge is not to come up with appropriate schemes but rather to technically prove that these satisfy the desired security properties.
We provide for the first time techniques for proving asymptotically optimal preimage resistance bounds for block cipher based double length, double call hash functions. More precisely, we consider for some $\ell > n$ compression functions $H : \{0,1\}^{\ell+n} \to \{0,1\}^{2n}$ using two calls to an ideal block cipher with an n-bit block size. Optimally, an adversary trying to find a preimage for H should require $\Omega(2^{2n})$ queries to the underlying block cipher. As a matter of fact there have been several attempts to prove the preimage resistance of such compression functions, but no proof did go beyond the $\Omega(2^n)$ barrier, therefore leaving a huge gap when compared to the optimal bound.
In this paper, we introduce two new techniques on how to lift this bound to $\Omega(2^{2n})$. We demonstrate our new techniques for a simple and natural design of H, being the concatenation of two instances of the well-known Davies-Meyer compression function.

Keywords: Proof of Security, Hash Function, Preimage Resistance, Block Cipher, Beyond Birthday Bound, Foundations

1 Introduction

Motivation. Proofs of security are an important and technically challenging type of result in modern cryptography. The basic principle is to show that breaking the considered scheme would violate a certain underlying assumption. For example, this allows for assessing the security of more involved designs based on simpler primitives.

One prominent example is the evaluation of hash functions based on block ciphers. Generally speaking, a cryptographic hash function maps an input of arbitrary length to an output of fixed length and is one of the most important primitives in cryptography [11]. The typical way a hash function is created is by iterating a fixed-input length compression function.

Block cipher based compression functions turn a block cipher into a one-way compression function. These primitives have been designed for more than 30 years

and are still in the focus of cryptographic research (for example, see the current SHA-3 contest for a new hash function standard). The security of such compression functions is usually evaluated in the *ideal cipher model*. This means that

- the block cipher $E_K(X) := E(K, X) : \{0,1\}^\ell \times \{0,1\}^n \longrightarrow \{0,1\}^n$ included in the construction is supposed to be ideal in the sense that, from the perspective of the attacker, $\{E_K(\cdot), K \in \{0,1\}^\ell\}$ is a collection of randomly and independently chosen permutations over $\{0,1\}^n$ and
- the adversary is an oracle Turing machine which is allowed to pose oracle queries of type $E_K(X)$ (encryption query) and $E_K^{-1}(Y)$ (decryption query), $X, Y \in \{0,1\}^n$, $K \in \{0,1\}^\ell$, and
- the adversary's resources are measured by the number of oracle queries.

Regarding the security, the common notions refer to collision attacks (finding two inputs that map to the same output), preimage attacks (given an output, find a matching input), and second-preimage attack s (given an input-output pair, find another different input that maps to the same output).

Recall that for an ideal compression or hash function, *i.e.* a random function with output length v bits, the effort for finding a collision is in $\Theta(2^{v/2})$ and for finding a preimage or second-preimage is in $\Theta(2^v)$. Thus, the security of constructions should be measured in comparison to these bounds.

In a pioneering work, Preneel et al. [14] investigated single output length block cipher based compression functions of type $H(M, V) = E_K(X) \oplus U$, where E is a block cipher and $K, X, U \in \{0, M, V, M \oplus V\}$. They showed attacks on 52 out of the $4^3 = 64$ possibilities, leaving the security of the 12 remaining candidates as an open question. Almost 10 years later, Black et al. [2] introduced new techniques for a formal and quantitative treatment of those 64 constructions and proved that, in the ideal-cipher model, the 12 schemes singled out by Preneel et al. in fact are secure including the Davies-Meyer compression function $H(K, X) = E_K(X) \oplus X$ (cf. [17]), which will play a crucial role also in the context of this paper. Till today, any proof of security for block-cipher based hash functions is, in principle, built around the techniques provided by Black et al.

Summarizing, on can say that for *single length* simple compression functions designs are known that achieve optimal or near-optimal security bounds (regarding collision, preimage and 2nd-preimage resistance)

However because of the short output length of most practical block ciphers, *e.g.*, $n = 128$-bit, one is interested in sound design principles for *double length* (DL) hash functions. Such constructions usually use one block cipher with n-bit output as the building block by which messages are projected to a fixed $2n$-bit string. Here, the current state of knowledge is much less mature. Although several promising DL constructions are known where (near-)optimal preimage bounds *might* hold, no techniques are known for *assessing* these questions. Several authors, [5, 6, 10, 12, 7, 8] have tried to analyze preimage resistance, but *none* could make any statements if the number of queries exceeds the birthday bound 2^n. Due to the lack of alternatives, all known attempts were using the Black et al. techniques. Not surprisingly, several authors, *e.g.*, [5, 6, 10], called the challenge of finding more satisfying preimage bounds as one of the important open problems in the field of block cipher based hash functions.

Contribution. In this paper, we present two new techniques for deriving preimage resistance bounds for block cipher based *double length* cryptographic hash functions in the ideal cipher model. These techniques allow not only for the first time results far beyond the birthday barrier but also prove asymptotically optimal bounds. We demonstrate these by analyzing the following natural compression functions, using twice the Davies-Meyer compression function,

$$H_1(K,X) = \left(E_{K||0}(X) \oplus X, E_{\overline{K}||1}(X) \oplus X\right)$$

where $\overline{K}$ denotes the bit-by-bit complement of K and '||' the concatenation of bit strings. Note that, in the ideal cipher model, the ciphers $E_{K||0}$ and $E_{\overline{K}||1}$ are independent. Using our new techniques, we are able to prove the following:

1. No adversary can find a preimage with probability greater than $1/2$ with less than $2^{-5} \cdot 2^{2n}$ queries.
2. For greedy adversaries, *i.e.*, adversaries that make only queries for which the success probability of finding a preimage is non-zero, we prove with another technique a bound of $2^{-9} \cdot 2^{2n}$ queries.

Note that both techniques deliver an asymptotically optimal bound. The introduced techniques are based on studying the complexity of a more general algorithmic problem: the computation of a common fixed point of two independently chosen random permutations[3]. Therefore, the proof techniques developed in this paper might be also interesting for a broader community.

For similar reasons, we present the second technique here as well, although it achieves a somewhat weaker result (lower bound for a restricted class of adversaries) for H_1. It might well be that the situation is the other way around for other constructions. More precisely, there exist important constructions like Tandem-DM where the first technique is not directly applicable. Therefore, we consider it being highly important that for analyzing other constructions, several techniques are known.

Outline. In Section 2, we provide the definitions and statements used in this paper. Section 3 gives a lower bound of preimage resistance of $2^{-5} \cdot 2^{2n}$ queries for H_1. Using a completely different technique, for greedy adversaries, a bound of $2^{-9} \cdot 2^{2n}$ queries is given in Section 4. In Section 5 we discuss our results and conclude the paper.

2 Preliminaries

General Notations. An (r,n)-block cipher is a keyed family of permutations consisting of two paired algorithms $E : \{0,1\}^\ell \times \{0,1\}^n \to \{0,1\}^n$ and $E^{-1} : \{0,1\}^\ell \times \{0,1\}^n \to \{0,1\}^n$ both accepting a key of size ℓ bits and an input block

[3] For two permutations π, π' defined on the same domain D, a common fixed point is a value $x \in D$ s.t. $\pi(x) = \pi'(x) = x$.

of size n bits for some $\ell > n$. For positive n, $Block(\ell, n)$ is the set of all (ℓ, n)-block ciphers. For any $E \in Block(\ell, n)$ and any fixed key $K \in \{0,1\}^\ell$, decryption $E_K^{-1} := E^{-1}(K, \cdot)$ is the inverse function of encryption $E_K := E(K, \cdot)$, so that $E_K^{-1}(E_K(X)) = X$ holds for any input $X \in \{0,1\}^n$. In the ideal cipher model [2, 4, 9] E is modeled as a family of random permutations $\{E_K\}$ whereas the random permutations are chosen independently for each key K, *i.e.*, formally E is selected randomly from $Block(\ell, n)$. We use the convention to write oracles, that are provided to an algorithm, as superscripts. For example $\mathcal{A}^E$ is an algorithm $\mathcal{A}$ with oracle access to E to which $\mathcal{A}$ can request forward and backward queries. For ease of presentation, we identify the sets $\{0,1\}^{a+b}$ and $\{0,1\}^a \times \{0,1\}^b$. Similarly for $A \in \{0,1\}^a$ and $B \in \{0,1\}^b$, the concatenation of these bit strings is denoted by $A||B \in \{0,1\}^{a+b} = \{0,1\}^a \times \{0,1\}^b$.

Preimage Resistance. Insecurity is quantified by the success probability of an optimal resource-bounded adversary. The resource is the number of queries (forward and backward) to the block cipher E. An adversary is a computationally unbounded but always-halting algorithm $\mathcal{A}$ with access to $E \in Block(\ell, n)$. The adversary may make a *forward* query (K, X) to discover the corresponding value $Y = E_K(X)$, or a *backward* query (K, Y), so as to learn the corresponding value $X = E_K^{-1}(Y)$ such that $E_K(X) = Y$. Either way, the result of the query is stored in a triple $(K_i, X_i, Y_i) := (K, X, Y)$ and the *query history* $\mathcal{Q}$ is the tuple $(Q_1, \ldots, Q_q)$ where $Q_i = (K_i, X_i, Y_i)$ and q is the total number of queries made by the adversary. Without loss of generality, we assume that $\mathcal{A}$ asks at most once on a triplet of a key K_i, a plaintext X_i and a ciphertext Y_i obtained by a query and the corresponding reply. For a set S, let $z \xleftarrow{\$} S$ represent random sampling from S under the uniform distribution. For a probabilistic algorithm $\mathcal{M}$, let $z \xleftarrow{\$} \mathcal{M}$ mean that z is an output of $\mathcal{M}$ and its distribution is based on the random choices of $\mathcal{M}$.

A preimage finding adversary is an algorithm whose goal is to find a preimage of a specific compression function. There are several approaches known on how to define this notion [15]. We opt for the (Pre) notion of preimage resistance, which intuitively states that a function is a one-way function[4]. This notion does imply weaker notions as, *e.g.*, everywhere preimage resistance (ePre) and always preimage resistance (aPre).

Definition 1. ***(Preimage Resistance* Pre *[15])*** *Let H be a block cipher based compression function, $H : \{0,1\}^{m+l} \to \{0,1\}^l$. Fix an adversary $\mathcal{A}$ with access to oracles E, E^{-1}. The advantage of $\mathcal{A}$ to invert H is the real number*

$$\mathbf{Adv}_H^{Pre}(\mathcal{A}) = \Pr[E \xleftarrow{\$} Block(\ell, n); A \xleftarrow{\$} \{0,1\}^{m+l}; B \xleftarrow{\$} H(A); A' \xleftarrow{\$} \mathcal{A}^E(B) : H(A') = B].$$

[4] A cryptographic one-way function is a function that is easy to evaluate but practically hard to invert.

Again, for $q \geq 1$, we write

$$\mathbf{Adv}_H^{Pre}(q) = \max_{\mathcal{A}}\{\mathbf{Adv}_H^{Pre}(\mathcal{A})\}$$

where the maximum is taken over all adversaries that ask at most q oracle queries.

Online/offline model. With respect to the operation mode of the ideal cipher oracle, there exists two variants: In the offline version, the oracle in advance chooses the random (r, n)-block cipher E. In the online version, for each new query, the oracle chooses the answer at random with respect to the uniform distribution from the set of possible answers. Although both versions are *equivalent from an adversaries' perspective*, adopting one or the other model can help for more compact arguments. In that sense the bound in the following Section 3 is derived with respect to the the offline version of the E-oracle, while the bound of Section 4 is based on the online version.

3 A Technique for proving a Preimage Resistance Bound in $\Omega\left(2^{2n}\right)$ for Arbitrary Adversaries

3.1 Preliminaries

In this section we prove an $\Omega(2^{2n})$ lower bound on the number of queries necessary for finding a preimage with a chance of success of at least $1/2$. Although an adversary can pose, by definition, arbitrary queries to the E-oracle, certain pairs of queries can be naturally grouped to "meta queries". For example, asking in the H_1 case for the value $E_{K||0}(X)$ is not sufficient for deciding whether a preimage has been found without asking (or knowing) the value $E_{\overline{K}||1}(X)$. Therefore, we consider meta queries instead which are selected by the following criteria: (i) One meta query/response pair should provide all information necessary for deciding whether the asked parameters yield a preimage. (ii) The set of meta queries should not restrict the set of possible E-queries. That is, for each possible values X, Y, and K, there should exist meta queries that provide the value $E_K(X)$ resp. $E_K^{-1}(Y)$. Based on these considerations, we use the following meta queries:

Type-I: Query $Q = (I, X, K)$. Response: $Y = E_{K||0}(X)$ and $Y' = E_{\overline{K}||1}(X)$.)
Type-II: Query $Q = (II, Y, K)$. Response $X = E_{K||0}^{-1}(Y)$ and $Y' = E_{\overline{K}||1}(X)$.)
Type-III: Query $Q = (III, Y, K)$. Response $X = E_{\overline{K}||1}^{-1}(Y')$ and $Y = E_{K||0}(X)$.)

The 5-tuple (T, X, Y, Y', K), $T \in \{I, II, III\}$, is called the *query-response pair* $(Q, R(Q))$. We remark that our analysis is based on the number of meta-queries an adversary has to ask.

We continue with an important observation on H_1.

Lemma 1 (Reduction to $(0,0)$-Case). *For any $(U, V) \in \{0,1\}^{2n}$, the complexity of finding a preimage to the hash value (U, V) w.r.t. H_1 is the same as the complexity of finding a preimage to the hash value $(0, 0)$ w.r.t. H_1.*

Proof. Finding a preimage to the image $(U, V) \in \{0,1\}^{2n}$ is equivalent to finding a key-prefix $K \in \{0,1\}^{\ell-1}$ and an input $X \in \{0,1\}^n$ such that $\tilde{E}_{K||0}(X) = \tilde{E}_{K||1}(X) = X$, where the (ℓ, n)-block cipher $\tilde{E}$ is defined as follows: For any key $\kappa = (\kappa_1, \cdots, \kappa_\ell)$ and any $X \in \{0,1\}^n$ let $\tilde{E}_\kappa(X) := E_\kappa(X) \oplus U$ if $\kappa_\ell = 0$ and $\tilde{E}_\kappa(X) := E_\kappa(X) \oplus V$ if $\kappa_\ell = 1$.

Note that assigning $\tilde{E}$ to E defines a bijective mapping over $Block(\ell, n)$. The outputs of E and $\tilde{E}$ are uniformly distributed. Consequently, the effort for finding a preimage to the image (U, V) is the same as of finding a preimage to the image $(0, 0)$. □

In other words, finding a preimage is in this case equivalent to finding a common fixed point (CFP) for the two permutations $E_{K||0}$ and $E_{\overline{K}||1}$, that is a value $X \in \{0,1\}^n$ such that $E_{K||0}(X) = X$ and $E_{\overline{K}||1}(X) = X$. This lemma naturally implies the following definition:

Definition 2 (Successful Queries and Rank). *Let $\mathcal{Q} = (Q_1, \cdots, Q_q)$ be an arbitrarily fixed sequence of q queries,* i.e.*, $Q_i = (T_i, Z_i, K_i)$, where $T_i \in \{I, II, III\}$, $Z_i \in \{0,1\}^n$, $K_i \in \{0,1\}^{\ell-1}$.*

We say that the i-th query $Q_i = (T_i, Z_i, K_i)$ is successful*, if the corresponding query-response pair $(Q_i, R(Q_i)) := (T_i, X_i, Y_i, Y_i', K_i)$ satisfies $X_i = Y_i = Y_i'$. We denote this event by* $\texttt{Succ}(Q_i)$.

Analogously, we say $\mathcal{Q}$ is successful, iff at least one query in $\mathcal{Q}$ is successful*. This event will be denoted by* $\texttt{Succ}(\mathcal{Q})$.

For all i, $1 \leq i \leq q$, let $rank_{\mathcal{Q}}(i)$ denote the number of queries $Q_j = (T_j, Z_j, K_j)$ with $1 \leq j \leq i$ and key $K_j = K_i$. We say that query Q_i has rank r *if $rank_{\mathcal{Q}}(i) = r$.*

3.2 Main Result

Our aim is to derive a lower bound of the minimal number q of rounds for achieving a success probability of at least $1/2$, where the probability space is given by the uniform distribution over $Block(\ell, n)$ and the internal randomization of the adversary. In particular, we prove

Theorem 1. *For each adversary $\mathcal{A}$ the following is true: $\mathcal{A}$ has to pose at least $1/32 \cdot N^2 = 2^{2n-5}$ queries for achieving a success probability of $1/2$ in finding a preimage of $(0, 0)$.*

We will prove the theorem by considering a *friendly* (E, S)-oracle, where S is a parameter fulfilling $S < N/3$ which will be determined later. A friendly (E, S)-oracle answers queries $Q = (T, Z, K)$ in principle in the same way as the "normal" E-oracle but with the difference that in some situations, the friendly oracle provides *additional* information.

The additional information are as follows:

- If Q is a query of rank 1 and $K \in K_{\geq 2}(E)$ then the oracle outputs in addition one common fixed point.

– If Q is a query of rank S and $K \in K_0(E)$ then the oracle's response contains in addition the information that $K \in K_0(E)$, that is that no common fixed point does exist under K.
– If Q is a query of rank S and $K \in K_1(E)$ then the oracle outputs in addition the unique common fixed point.

Clearly, each adversary $\mathcal{A}'$ communicating with an E-oracle can be simulated by an adversary $\mathcal{A}$ communicating with a friendly (E, S)-oracle, and for each number of rounds, the success probability of $\mathcal{A}$ is not smaller than the success probability of $\mathcal{A}'$. Thus, it suffices to lower bound the success probabilities of an arbitrarily fixed adversary $\mathcal{A}$ communicating with a friendly (E, S)-oracles. Note that we can suppose that $\mathcal{A}$ does not pose queries of rank greater than S.

Let $Succ(q)$ denote the event that $\mathcal{A}$ is successful after q queries, and let $\mathbf{S}_i$ (resp.$\neg\mathbf{S}_i$) denote the event that the i-th query is successful (resp. unsuccessful). Note that the event $Succ(q)$ implies the existence of some round i, $1 \leq i \leq q$, such that the i-th query is successful but queries $1, \cdots, i-1$ are not, i.e.,

$$Pr[Succ(q)] \leq \sum_{i=1}^{q} Pr[\mathbf{S}_i \wedge \neg\mathbf{S}_1 \wedge \cdots \wedge \neg\mathbf{S}_{i-1}]$$

$$\leq \sum_{i=1}^{q} Pr[\mathbf{S}_i | \neg\mathbf{S}_1 \wedge \cdots \wedge \neg\mathbf{S}_{i-1}] \cdot Pr[\neg\mathbf{S}_1 \wedge \cdots \wedge \neg\mathbf{S}_{i-1}]$$

$$\leq \sum_{i=1}^{q} P_i,$$

where we denote $P_i = Pr[\mathbf{S}_i | \neg\mathbf{S}_1 \wedge \cdots \wedge \neg\mathbf{S}_{i-1}]$.

After posing $i-1$ unsuccessful queries the adversary has three possibilities:

(1) Take a *new* key prefix K and pose a query of Rank 1.
(2) Take a key prefix K for which already $r-1$, $1 \leq r \leq S-2$, unsuccessful queries have been posed and pose a query of rank r, $1 < r < S$.
(3) Take a key prefix K for which already $S-1$ unsuccessful queries have been posed and pose a query of rank S

Let P_i^1, $P_i^2(r)$ and $P_i^3(S)$ denote the probabilities P_i under the additional condition that the adversary chooses possibility (1),(2), or (3), respectively. We prove or result by deriving appropriate upper bounds $Q_1(N)$, $Q_2(N, S)$, and $Q_3(N, S)$ for the probabilities P_i^1, $P_i^2(r)$ and $P_i^3(S)$, respectively.

Let $I_j \subseteq [q]$, $1 \leq j \leq 3$, denote the indices where $\mathcal{A}$ did choose possibility j. It follows that

$$Pr[Succ(q)] \leq \sum_{i=1}^{q} P_i \leq \sum_{i \in I_1} Q_1(N) + \sum_{i \in I_2} Q_2(N, S) + \sum_{i \in I_3} Q_3(N, S)$$

$$\leq q \cdot Q_1(N) + q \cdot Q_2(N, S) + q/S \cdot Q_3(N, S)$$

Note that $\Pr[Succ(q)] \geq 1/2$ implies that at least one of the inequalities

(4) $q \cdot Q_1(N) \geq 1/6$
(5) $q \cdot Q_2(N,S) \geq 1/6$
(6) $q/S \cdot Q_3(N,S) \geq 1/6$

has to be fulfilled. Let us denote by $\Pr[K_0]$ (resp. $\Pr[K_1]$ resp. $\Pr[K_{\geq 2}]$) denote the probability that a uniformly distributed pair (π, π') of permutations over $[N]$ does not have any common fixed point (resp. has exactly one CFP, resp. has more than one CFP).

We overestimate the probabilities P_i^1, $P_i^2(r)$ and $P_i^3(S)$ by estimating the probabilities $\Pr[K_0]$, $\Pr[K_1]$, and $\Pr[K_{\geq 2}]$). In the case of P_i^1 this is quite obvious. A rank 1 query corresponding to a key prefix K is successful if $K \in K_{\geq 2}(E)$ or if $K \in K_1(E)$ and the query is successful in picking the unique CFP of $(E_{K||0}, E_{\overline{K}||1})$, i.e., for all $i \geq 1$

$$P_i^1 = Pr[K_{\geq 2}] + 1/N \cdot Pr[K_1]. \tag{1}$$

Before asking a query of rank $r > 1$ (with key prefix K) the adversary has the following information. He knows the values of $E_{K||0}$ and $E_{\overline{K}||1}$ on a set $I \subseteq [N]$ of size $r-1$. Moreover, he knows that $K \notin K_{\geq 2}(E)$ and that I does not contain a CFP of $(E_{K||0}, E_{\overline{K}||1})$. For estimating the probabilities P_i^2 and P_i^3 we have to consider the following definitions. Given a subset $I \subseteq [N]$ and injective mappings $c, c' : I \longrightarrow [N]$, let us denote by $\Pr[K_0|c,c']$ (resp. $\Pr[K_1|c,c']$ resp. $\Pr[K_{\geq 2}|c,c']$) the probability that a uniformly distributed pair (π, π') of permutations over $[N]$ does not have any common fixed point (resp. has exactly one CFP, resp. has more than one CFP) under the condition that $\pi|_I = c$ and $\pi'|_I = c'$. Finally let $\Pr[K_1|c,c',K_0 \cup K_1]$ denote the probability that a uniformly distributed pair (π, π') of permutations over $[N]$ has exactly one CFP, under the conditions that $\pi|_I = c$ and $\pi'|_I = c'$ and that $(\pi, \pi') \in K_0 \cup K_1$.

Lemma 2. *For all $i \geq 1$ and all $r, 2 \leq r \leq S-1$, there is some set $I \subseteq [N]$, $|I| = r-1$, and a CFP-free pair of injective mappings $c, c' : I \longrightarrow [N]$ such that*

$$P_i^2(r) = Pr[K_1|c,c',K_0 \cup K_1] \cdot 1/(N - |A|),$$

where $A = I \cup c(I) \cup c'(I)$.

Proof: In the situation that the adversary asks a query of rank r, $1 < r < S$, w.r.t. to a key prefix K it is clear that the pair of permutations $E_{K,0}, E_{\overline{K},1}$ has at most one CFP. The success probability is nonzero only under the condition that $E_{K,0}, E_{\overline{K},1}$ has exactly one CFP. Under the condition that there is exactly one CFP w.r.t. $E_{K||0}, E_{\overline{K}||1}$ the adversary's chance to pick the CFP is $1/(N-|A|)$, as $[N] \setminus A$ coincides with the set of all candidates for being a CFP w.r.t. $E_{K||0}, E_{\overline{K},||}$. □

By similar arguments one can show that

Lemma 3. *For all $i \geq 1$ there is some set $I \subseteq [N]$, $|I| = S-1$, and a CFP-free pair of injective mappings $c, c' : I \longrightarrow [N]$ such that*

$$P_i^3(S) = Pr[K_1|c,c',K_0 \cup K_1]. \ \square$$

We derive the upper bounds $Q_1(N)$, $Q_2(N,S)$, and $Q_3(N,S)$ by using the following technical lemma:

Lemma 4. *(i) It holds* $\Pr[K_1] < 1/N$ *and* $\Pr[K_{\geq 2}] < 1/N^2$.
(ii) For all $t, 2 \leq t \leq S-1$, *sets* $I \subseteq [N]$, $|I| = t$ *and CFP-free pairs of injective mappings* $c, c' : I \longrightarrow [N]$ *it holds that*

$$Pr[K_1|c, c', K_0 \cup K_1] < \frac{N-t}{(N-t)^2-1} \;\leq\; \frac{1}{N-S}$$

Proof. Regrading (i) observe that

$$Pr[K_1] < \sum_{x \in [N]} Pr[(\pi(x) = \pi'(x) = x)] = N \cdot \frac{1}{N^2}, = \frac{1}{N}.$$

and that

$$Pr[K_{\geq 2}] < \sum_{1 \leq x < x' \leq N} Pr[(\pi(x) = \pi'(x) = x) \wedge (\pi(x') = \pi'(x') = x')]$$

$$= \binom{N}{2} \cdot \frac{1}{(N(N-1))^2} = \frac{1}{2N(N-1)} < \frac{1}{N^2}. \; \square(i)$$

Regarding (ii) observe first that

$$Pr[K_1|c, c', K_0 \cup K_1] = \frac{Pr[K_1|c, c']}{1 - Pr[K_{\geq 2}|c, c']}. \tag{2}$$

Further observe that

$$Pr[K_1|c, c'] \leq \sum_{x \in [N] \setminus A} Pr[\pi(x) = \pi'(x) = x] \leq (N-t) \cdot \frac{1}{(N-t)^2} = \frac{1}{N-t}. \tag{3}$$

(As above let $A = I \cup c(I) \cup c'(I)$ and note that $|[N] \setminus A| \geq N - t$.) Finally observe that

$$Pr[K_{\geq 2}|c, c'] \leq \sum_{x < x' \in [N] \setminus A} Pr[(\pi(x) = \pi'(x) = x) \wedge (\pi(x') = \pi'(x') = x')] \leq$$

$$\leq \binom{N-t}{2} \frac{1}{(N-t)^2(N-t-1)^2} = \frac{1}{2(N-t)(N-t-1)} < \frac{1}{(N-t)^2} \tag{4}$$

Putting relations (2), (3), (4) together we obtain

$$Pr[K_1|c, c', K_0 \cup K_1] \leq \frac{1/(N-t)}{1 - (1/(N-t)^2)} = \frac{N-t}{(N-t)^2-1}$$

$$< \frac{N-t+1}{(N-t)^2-1} = \frac{1}{N-t-1}.$$

As $t \leq S-1$ we can write

$$Pr[K_1|c, c', K_0 \cup K_1] \leq \frac{1}{N-S}. \; \square$$

Together with equation (1) and Lemma 4, inequality (4) yields the inequality

$$q \cdot \frac{2}{N^2} \geq 1/6, \tag{5}$$

i.e. $q \geq N^2/12$.

Let us suppose that $q < N^2/12$, then $\Pr[Succ(q)] \geq 1/2$ implies that inequality (5) or inequality (6) have to be valid. Note that together with Lemma 2 and Lemma 4 inequality (5) implies that

$$q \cdot B_2(N,S) \geq 1/6,$$

where $B_2(N,S) = \frac{1}{N-S} \cdot \frac{1}{N-3S}$.

Moreover, together with lemma 4 inequality (6) implies that

$$q \cdot B_3(N,S) \geq 1/6,$$

where $B_3(N,S) = \frac{1}{N-S} \cdot \frac{1}{S}$.

Observe that these conditions must hold for any choice of S and that $B_2(N,S)$ increases with S while $B_3(N,S)$ decreases. Therefore, we are interested into the value $\max_S(\min(B_2(N,S), B_3(N,S))$ which is achieved if $B_2(N,S) = B_3(N,S)$. This is the case for $S = N/4$. Consequently, let us fix S to be $N/4$. We obtain that $\Pr[Succ(q)] \geq 1/2$ and $q < N^2/12$ implies that

$$q \cdot \frac{1}{3/4 \cdot N} \cdot \frac{4}{N} \geq 1/6,$$

which implies that

$$q \geq \frac{1}{32} \cdot N^2. \ \square$$

4 A Technique for proving a Preimage Resistance Bound in $\Omega(2^{2n})$ for Greedy Adversaries

4.1 Preliminaries

Now we present another techniques for estimating the preimage resistance of H_1. This technique if fundamentally different to the technique given in Sec.3. However, we have to restrict to the reasonable class of "greedy" adversaries. "Greedy" means that no queries are made for which it is known in advance that the success probability of finding the preimage is zero. We make this formal in the following definition:

Definition 3 (Disjoint Query). *Let $\mathcal{Q} = (Q_1, \cdots, Q_q)$ be a sequence of queries. Let $Q_i = (T_i, Z_i, K_i)$ for $i = 1, \cdots, q$ and $(Q_i, R(Q_i)) = (T_i, X_i, Y_i, Y_i', K_i)$ be the according query-response pair. For a fixed key K, we consider the set $A(\mathcal{Q}, K) \subseteq \{0,1\}^n$ of all inputs and outputs that occurred so far with respect to the same key, i.e.,*

$$A(\mathcal{Q}, K) := \bigcup_{1 \leq i \leq q : K_i = K} \{X_i, Y_i, Y_i'\}. \tag{6}$$

We call a new query $Q = (T, Z, K)$ to be disjoint *to $\mathcal{Q}$, if $Z \notin A(\mathcal{Q}, K)$.*

The reason for considering disjoint queries is that they characterize the only queries with a non-zero success probability:

Lemma 5. *Let* $\texttt{Fail}(\mathcal{Q})$ *denote the event that making queries* $\mathcal{Q} = (Q_1, \cdots, Q_q)$ *was not successful. For a single query* $Q = (T, Z, K)$*, let* $Pr[Q|\texttt{Fail}(\mathcal{Q})]$ *denote the probability that* Q *is successful under the condition that all queries in* $\mathcal{Q}$ *have not been successful before. We abbreviate* $N = 2^n$*. It holds*

$$Pr[Q|\texttt{Fail}(\mathcal{Q})] \leq \begin{cases} 1/(N-q)^2 & , Q \text{ disjoint to } \mathcal{Q} \\ 0 & , \text{else.} \end{cases} \tag{7}$$

Proof: We assume the online mode for the E-oracle. Note that the fact that $\mathcal{Q}$ is not successful implies that $X_i \neq Y_i$ or $X_i \neq Y_i'$ for all $i = 1, \cdots, q$. Furthermore, if $Z \in A(\mathcal{Q}, K)$, i.e., the query is not disjoint, then there exists an index $i \in \{1, \ldots, q\}$ such that $X_i = Z$, $Y_i = Z$, or $Y_i' = Z$. Taking both together immediately shows that Z cannot be a common fixed point.

Let us now suppose that Q is disjoint to $\mathcal{Q}$. We estimate $Pr[Q|\texttt{Fail}(\mathcal{Q})]$ under the condition that $T = I$. For the other two cases $T \in \{II, III\}$, the proof can be done in a similar way. The fact that Q is disjoint to $\mathcal{Q}$ implies that $Z \notin \{X_1, \ldots, X_q\}$ and likewise $Z \notin \{Y_1, \ldots, Y_q\}$ and $Z \notin \{Y_1', \ldots, Y_q'\}$. Consequently, the probability that $E_{K||0}(Z) = Z$ and the probability that $E_{\overline{K}||1}(Z) = Z$ are both $\leq 1/(N-q)$. As both events are independent, the success probability of Q is $\leq 1/(N-q)^2$. □

Definition 4 (Sequence of Disjoint Queries). *We call* $\mathcal{Q}$ *a* sequence of disjoint queries *if for all* i*,* $1 \leq i \leq q-1$*, query* Q_{i+1} *is disjoint to* $\mathcal{Q}_{\leq i} := \{Q_1, \ldots, Q_i\}$*.*

By Lemma 5, we know that this is the only kind of queries that have a non-zero success probability. Although it seems to be plausible that this strategy is optimal, we do not have a proof for this assumption. In other words, we cannot exclude that strategies might exist where asking some queries with zero success probability can yield globally a better success probability.

Definition 5 (Accepting Computation). *A sequence of queries* $\mathcal{Q}$ *is called an* accepting computation *(or, for short,* $\mathcal{Q}$ *is* accepting*) iff*

(1) $\mathcal{Q}$ *is a sequence of disjoint queries.*
(2) For all i*,* $1 \leq i \leq q-1$*, query* $Q_i = (T_i, Z_i, K_i)$ *is not successful, i.e.,* Z_i *is not a common fixed point, and*
(3) query $Q_q = (T_q, Z_q, K_q)$ *is successful, i.e.,* $E_{K_q||0}(Z_q) = E_{\overline{K_q}||1}(Z_q) = Z_q$*.*

4.2 Main Result

The main technical result of this section is the following estimation of the probability $Pr[\mathcal{Q}$ accepting$]$ that $\mathcal{Q}$ is an accepting computation.

Theorem 2. *Consider a sequence* $\mathcal{Q} = (Q_1, \cdots, Q_q)$ *of queries and set* $N := 2^n$*.*

(i) It holds $Pr[\mathcal{Q}\ \textit{accepting}] \leq \frac{1}{(N-q)^2}$.
(ii) If $q \geq 15/16 \cdot N$ *then* $Pr[\mathcal{Q}\ \textit{accepting}] \leq e^{-1/32 \cdot N}$.

Proof: The proof of part (i) is an straightforward consequence of Lemma 5. The proof of part (ii) is postponed to subsection 4.3. □

We show now how Theorem 2 can be used to derive a nearly maximal lower bound on the preimage resistance of H_1. Let $q \leq N^2$ and $\mathcal{Q} = (Q_1, \cdots, Q_q)$ denote an arbitrarily fixed sequence of *disjoint* queries asked by the adversary with $Q_i = (T_i, Z_i, K_i)$ for $1 \leq i \leq q$.

We call $\mathcal{Q}$ to be successful if at least one of the queries Q_i in $\mathcal{Q}$ is successful, i.e., $E_{K_i||0}(Z_i) = E^{-1}_{\overline{K_i}||1}(Z_i) = Z_i$. This implies that for at least one query $Q_i \in \mathcal{Q}$ it holds that $\mathcal{Q}_{\leq i}$ is an accepting computation. Consequently,

$$Pr\left[\mathtt{Succ}(\mathcal{Q})\right] \leq \sum_{i=1}^{q} Pr\left[\mathcal{Q}_{\leq i} \text{ accepting}\right]. \tag{8}$$

Observe that the first claim of Theorem 2 does not make any useful statements beyond the birthday bound $\geq 2^n$. Indeed, the idea is now to split the set of queries into two sets, according to the statements given in Theorem 2. Let $r_1 := \{i, rank_{\mathcal{Q}}(i) > \frac{15}{16}N\}$ and $r_2 := \{i, rank_{\mathcal{Q}}(i) \leq \frac{15}{16}N\}$. Theorem 2 and Relation (8) yield

$$Pr\left[\mathtt{Succ}(\mathcal{Q})\right] \leq \sum_{i \in r_1} Pr\left[\mathcal{Q}_{\leq i} \text{ accepting}\right] + \sum_{i \in r_2} Pr\left[\mathcal{Q}_{\leq i} \text{ accepting}\right] \tag{9}$$

$$\leq |r_1| \cdot e^{-1/32 \cdot N} + |r_2| \cdot \frac{1}{(N - 15/16 \cdot N)^2} \tag{10}$$

$$\leq q \cdot 256 \cdot N^{-2} \tag{11}$$

if $N \geq 256$. We have proved

Theorem 3. *For achieving a success probability of* $1/2$ *in finding a preimage, a greedy adversary has to ask at least* $1/512 \cdot 2^{2n} = 2^{2n-9}$ *queries.* □

4.3 The Proof of Part (ii) of Theorem 2

Let $q = 15/16 \cdot N$ and $\mathcal{Q} = (Q_1, \cdots, Q_{q+1})$ be an arbitrarily fixed sequence of $q+1$ queries w.r.t. the same key $K \in \{0,1\}^{\ell-1}$. Let $Q_i = (T_i, Z_i, K)$ for $i = 1, \cdots, q+1$. We derive an upper bound for the probability $Pr[\mathcal{Q}$ accepting$]$. For this purpose, we assume that $\mathcal{Q}$ contains only disjoint queries as this can only increase $Pr[\mathcal{Q}$ accepting$]$.

While asking $Q_1, \cdots, Q_{q+1}$, the adversary generates sets $\mathcal{X}_i = \{X_1, \cdots, X_i\}$, $\mathcal{Y}_i = \{Y_1, \cdots, Y_i\}$, and $\mathcal{Y}'_i = \{Y'_1, \cdots, Y'_i\}$ of size i. Let $\mathcal{A}_i := \mathcal{X}_i \cup Y_i \cup \mathcal{Y}'_i$. One sees easily that $|\mathcal{A}_i| + 1 \leq |\mathcal{A}_{i+1}| \leq |\mathcal{A}_i| + 3$ for $i = 0, \cdots, q$. (Let $\mathcal{A}_0 = \emptyset$). As $\mathcal{Q}$ is a sequence of disjoint queries, it must hold that the input Z_{q+1} is outside of $\mathcal{A}_q$ and in particular $|\mathcal{A}_q| < N$. This implies that

$$Pr[\mathcal{Q} \text{ accepting}] \leq Pr[|\mathcal{A}_q| < N]. \tag{12}$$

We show that the latter event is rather unlikely by taking a closer look on the size of $\mathcal{A}_\ell$ for some smaller index $\ell < q$. Fix $\ell = N/8$. Because of $|\mathcal{A}_{i+1}| \geq |\mathcal{A}_i| + 1$, one has $|\mathcal{A}_q| - |\mathcal{A}_\ell| \geq q - \ell = 15/16N - 2/16N = 13/16N$. This implies that

$$|\mathcal{A}_\ell| \leq |\mathcal{A}_q| - 13/16N < N - 13/16N = 3/16N. \tag{13}$$

It follows that

$$Pr[|\mathcal{A}_q| < N] \leq Pr[|\mathcal{A}_\ell| \leq 3/16N] =: p^*. \tag{14}$$

We show that $p^* \leq e^{-1/32 \cdot N}$ which yields the initial claim by Eqs. (12) and (14).

For this purpose, we introduce a set of independent random Bernoulli variables and make use of Chernov's Inequality [1, Appendix A, pp. 233-240]. We recall it here shortly: Let $\nu_1, \cdots, \nu_n$ be independent random Bernoulli variables. Let $\sigma = 1/n \cdot \sum_{i=1}^{n} \nu_i$ be the (normed) sum of these variables and $\mathbf{E}(\sigma) = 1/n \cdot \sum_{i=1}^{n} Pr[\nu_i = 1]$ its expectation value. Then, for all $\delta > 0$ it holds that $Pr[\mathbf{E}(\sigma) - \sigma > \delta] < e^{-2\delta^2 n}$.

For defining the Bernoulli variables, we take a closer look on what happens during asking a query Q_i. Each query Q_i is composed of two separate queries Q_i^0 and Q_i^1 to the E-oracle. In sub-query Q_i^0, the adversary asks an input Z_i^0 and gets a response $R_i^0 = E_{K_i}(Z_i)$ if a forward query has been made or $R_i^0 = E_{K_i}^{-1}(Z_i)$ in the case of a backward query. Likewise, for the other sub-query Q_i^1 she requests an input Z_i^1 and gets an answer R_i^1.

For $b \in \{0,1\}$ denote by $\mathcal{R}_i^b$ the set of possible answers for query Q_i^b. Note that $|\mathcal{R}_i^b| = N - (i-1)$ as $i-1$ responses out of N are already taken.[5] Note further that for $i \leq \ell = N/8$ it holds that

$$|\mathcal{A}_i| \leq 3i < 1/2 \cdot (N - (i-1)) = 1/2 \cdot |\mathcal{R}_i^b|. \tag{15}$$

We now introduce subsets of $\mathcal{R}_i^0$ and $\mathcal{R}_i^1$ and consider the probability that R_i^0 and R_i^1 fall into these sets, respectively. The reasons are twofold: first, it allows for deriving a lower bound on $|\mathcal{A}_\ell|$, and second do they imply Bernoulli variables ν_i^0 and ν_i^1 as explained above which allow for using Chernov's Inequality. These variables are defined as follows. Suppose that for $i = 1, \cdots, \ell$, in addition to asking Q_i^0 and Q_i^1, the adversary does the following.

- Before asking Q_i^0 she fixes a set $\tilde{\mathcal{R}}_i^0 \subseteq \mathcal{R}_i^0 \setminus (\mathcal{A}_{i-1} \cup \{Z_i\})$ of size $\lceil |\mathcal{R}_i^0|/2 \rceil$, and
- before asking Q_i^1 she fixes a set $\tilde{\mathcal{R}}_i^1 \subseteq \mathcal{R}_i^1 \setminus (\mathcal{A}_{i-1} \cup \{Z_i, Z_i'\})$ of size $\lceil |\mathcal{R}_i^1|/2 \rceil$.

Inequality (15) guarantees that this is always possible. For $i = 1, \cdots, s$ let $\nu_i^0 \in \{0,1\}$ denote the random Bernoulli variable taking 1 iff $R_i^0 \in \tilde{\mathcal{R}}_i^0$, and analogously let $\nu_i^1 \in \{0,1\}$ denote the random Bernoulli variables taking value 1 iff $R_i^1 \in \tilde{\mathcal{R}}_i^1$.

As we are considering the ideal cipher model, ν_i^0 and ν_i^1 are independent random Bernoulli variables. Let $\sigma = \frac{1}{2\ell} \cdot \sum_{i=1}^{\ell} (\nu_i^0 + \nu_i^1)$ the normed sum. We can apply Chernov's Inequality which tells that $Pr[\mathbf{E}(\sigma) - \sigma > \delta] < e^{-2\delta^2 n}$.

[5] Note that $\mathcal{R}_i^0 = \{0,1\}^n \setminus \mathcal{X}_{i-1}$ for $T_i \in \{I, II\}$ and $\mathcal{R}_i^0 = \{0,1\}^n \setminus \mathcal{Y}_{i-1}$ if $T_i = I$. Note further that $\mathcal{R}_i^1 = \{0,1\}^n \setminus \mathcal{Y}'_{i-1}$ for $T_i \in \{I, II\}$ and $\mathcal{R}_i^1 = \{0,1\}^n \setminus \mathcal{X}_{i-1}$ for $T_i = III$.

As each variable takes 1 with a probability $\geq 1/2$, one sees easily that that $\mathbf{E}(\sigma) \geq 1/2$ and in particular $1/4 \leq \mathbf{E}(\sigma) - 1/4$. Furthermore, let $\sigma^* := 2\ell \cdot \sigma = \sum_{i=1}^{\ell}(\nu_i^0 + \nu_i^1)$. Observe that $|\mathcal{A}_{i+1}| \geq |\mathcal{A}_i| + 1 + \nu_i^0 + \nu_i^1$ and hence $|\mathcal{A}_\ell| \geq \ell + \sigma^*$. Thus, $|\mathcal{A}_\ell| \leq 3/16N$ implies $\ell + \sigma^* \leq 3/16N \Leftrightarrow \sigma^* \leq 1/16N$ as $\ell = 1/8N$ by definition.

Putting everything together gives

$$p^* \leq Pr[\sigma^* < 1/16 \cdot N] = Pr[2\ell \cdot \sigma < 1/16 \cdot N] \tag{16}$$

$$= Pr[\sigma < 1/4] \leq Pr[\sigma < \mathbf{E}(\sigma) - 1/4] = Pr[\mathbf{E}(\sigma) - \sigma > 1/4] \tag{17}$$

$$< e^{-2/16 \cdot 2s} = e^{-1/32 \cdot N}. \tag{18}$$

Remark 1. Observe that one key ingredient of the proof was to show that with a high probability, the number of disjoint queries cannot grow above $15/16N$. Intuitively, one might expect that this bound is highly overrated. Indeed, computer simulations indicated that on average, only about $N/2$ disjoint queries are possible. If this bound holds in general (which is currently an open question), this would imply a lower bound of $2^{-3} \cdot 2^{2n}$ queries, being better than the bound derived with the technique discussed in Sec. 3.

5 Discussion and Conclusion

We developed and applied new techniques for determining lower bounds with respect to preimage resistance that make it possible, for the first time, to prove security bounds way beyond the birthday barrier for double length compression functions. This is a major breakthrough, especially when one considers that the first double length compression functions have been published about 20 years ago and taking into account that a lot of researchers have tried – but failed – in delivering beyond birthday bounds.

Although this result is a significant step forward, there are still a lot of challenges open in the field of block cipher based double length hashing. For example, is it possible to prove bounds with a better constant? Can the second technique be extended to any adversary and/or the conjecture stated in Remark 1 shown to be true? More general, can our techniques be adapted for assessing other known constructions like Abreast-DM or Tandem-DM or are other interesting generalizations possible? Closely related is the question of how these techniques can be applied to single call double length hash functions, *e.g.* [16].

Acknowledgement

We are very thankful to Jooyoung Lee, Martijn Stam, and John Steinberger for helpful comments. They pointed out a mistake in the first version of the first technique which eventually brought us to revise the proof.

References

1. Noga Alon and Joel Spencer. *The Probabilistic Method*. John Wiley, 1992.
2. John Black, Phillip Rogaway, and Thomas Shrimpton. Black-Box Analysis of the Block-Cipher-Based Hash-Function Constructions from PGV. In Moti Yung, editor, *CRYPTO*, volume 2442 of *Lecture Notes in Computer Science*, pages 320–335. Springer, 2002.
3. Orr Dunkelman, editor. *Fast Software Encryption, 16th International Workshop, FSE 2009, Leuven, Belgium, February 22-25, 2009, Revised Selected Papers*, volume 5665 of *Lecture Notes in Computer Science*. Springer, 2009.
4. Shimon Even and Yishay Mansour. A Construction of a Cipher From a Single Pseudorandom Permutation. In Hideki Imai, Ronald L. Rivest, and Tsutomu Matsumoto, editors, *ASIACRYPT*, volume 739 of *Lecture Notes in Computer Science*, pages 210–224. Springer, 1991.
5. Ewan Fleischmann, Michael Gorski, and Stefan Lucks. On the Security of Tandem-DM. In Dunkelman [3], pages 84–103.
6. Ewan Fleischmann, Michael Gorski, and Stefan Lucks. Security of cyclic double block length hash functions. In Parker [13], pages 153–175.
7. Shoichi Hirose. Provably Secure Double-Block-Length Hash Functions in a Black-Box Model. In Choonsik Park and Seongtaek Chee, editors, *ICISC*, volume 3506 of *Lecture Notes in Computer Science*, pages 330–342. Springer, 2004.
8. Shoichi Hirose. Some Plausible Constructions of Double-Block-Length Hash Functions. In Matthew J. B. Robshaw, editor, *FSE*, volume 4047 of *Lecture Notes in Computer Science*, pages 210–225. Springer, 2006.
9. Joe Kilian and Phillip Rogaway. How to Protect DES Against Exhaustive Key Search. In Neal Koblitz, editor, *CRYPTO*, volume 1109 of *Lecture Notes in Computer Science*, pages 252–267. Springer, 1996.
10. Jooyoung Lee, Martijn Stam, and John Steinberger. The collision security of tandem-dm in the ideal cipher model. Cryptology ePrint Archive, Report 2010/409, 2010. `http://eprint.iacr.org/`.
11. Alfred Menezes, Paul C. van Oorschot, and Scott A. Vanstone. *Handbook of Applied Cryptography*. CRC Press, 1996.
12. Onur Özen and Martijn Stam. Another glance at double-length hashing. In Parker [13], pages 176–201.
13. Matthew G. Parker, editor. *Cryptography and Coding, 12th IMA International Conference, Cryptography and Coding 2009, Cirencester, UK, December 15-17, 2009. Proceedings*, volume 5921 of *Lecture Notes in Computer Science*. Springer, 2009.
14. Bart Preneel, René Govaerts, and Joos Vandewalle. Hash Functions Based on Block Ciphers: A Synthetic Approach. In Douglas R. Stinson, editor, *CRYPTO*, volume 773 of *Lecture Notes in Computer Science*, pages 368–378. Springer, 1993.
15. Phillip Rogaway and Thomas Shrimpton. Cryptographic hash-function basics: Definitions, implications, and separations for preimage resistance, second-preimage resistance, and collision resistance. In Bimal K. Roy and Willi Meier, editors, *FSE*, volume 3017 of *Lecture Notes in Computer Science*, pages 371–388. Springer, 2004.
16. Martijn Stam. Blockcipher-based hashing revisited. In Dunkelman [3], pages 67–83.
17. Robert S. Winternitz. A secure one-way hash function built from des. In *IEEE Symposium on Security and Privacy*, pages 88–90, 1984.