Improved Security Analyses for CBC MACs

Mihir Bellare[1], Krzysztof Pietrzak[2], and Phillip Rogaway[3]

[1] Dept. of Computer Science & Engineering, University of California San Diego, 9500 Gilman Drive, La Jolla, CA 92093, USA. Email: `mihir@cs.ucsd.edu` URL: `www-cse.ucsd.edu/users/mihir`

[2] Dept. of Computer Science, ETH Zürich, CH-8092 Zürich Switzerland, E-mail: `pietrzak@inf.ethz.ch`

[3] Dept. of Computer Science, University of California, Davis, California, 95616, USA; and Dept. of Computer Science, Faculty of Science, Chiang Mai University, Chiang Mai 50200, Thailand. E-mail: `rogaway@cs.ucdavis.edu` URL: `www.cs.ucdavis.edu/~rogaway/`

Abstract. We present an improved bound on the advantage of any q-query adversary at distinguishing between the CBC MAC over a random n-bit permutation and a random function outputting n bits. The result assumes that no message queried is a prefix of any other, as is the case when all messages to be MACed have the same length. We go on to give an improved analysis of the encrypted CBC MAC, where there is no restriction on queried messages. Letting m be the block length of the longest query, our bounds are about $mq^2/2^n$ for the basic CBC MAC and $m^{o(1)}q^2/2^n$ for the encrypted CBC MAC, improving prior bounds of $m^2q^2/2^n$. The new bounds translate into improved guarantees on the probability of forging these MACs.

1 Introduction

Some definitions. The CBC function CBC_π associated to a key $\pi\colon \{0,1\}^n \to \{0,1\}^n$ takes as input a message $M = M^1 \cdots M^m$ that is a sequence of n-bit blocks and returns the n-bit string C^m computed by setting $C^i = \pi(C^{i-1} \oplus M^i)$ for each $i \in [1..m]$, where $C^0 = 0^n$. Consider three types of attacks for an adversary given an oracle: $\mathsf{atk} = \mathsf{eq}$ means all queries are exactly m blocks long; $\mathsf{atk} = \mathsf{pf}$ means they have at most m blocks and no query is a prefix of any another; $\mathsf{atk} = \mathsf{any}$ means the queries are arbitrary distinct strings of at most m blocks. Let $\mathbf{Adv}^{\mathsf{atk}}_{\mathrm{CBC}}(q,n,m)$ denote the maximum advantage attainable by any q-query adversary, mounting an atk attack, in distinguishing whether its oracle is CBC^π_n for a random permutation π on n bits, or a random function that outputs n bits. We aim to upper bound this quantity as a function of n, m, q.

Past work and our results on CBC. Bellare, Kilian and Rogaway [2] showed that $\mathbf{Adv}^{\mathsf{eq}}_{\mathrm{CBC}}(q,n,m) \le 2m^2q^2/2^n$. Maurer reduced the constant 2 to 1 and provided a substantially different proof [13]. Petrank and Rackoff [15] showed that the same bounds hold (up to a constant) for $\mathbf{Adv}^{\mathsf{pf}}_{\mathrm{CBC}}(q,n,m)$. In this paper we show that $\mathbf{Adv}^{\mathsf{pf}}_{\mathrm{CBC}}(q,n,m) \le 20mq^2/2^n$ for $m \le 2^{n/3}$. (The result

Construct	atk	Previous bound	Our bound
CBC	pf	$m^2q^2/2^n$ [2, 13, 15]	$mq^2/2^n \cdot (12 + 8m^3/2^n)$
ECBC	any	$2.5\, m^2q^2/2^n$ [7]	$q^2/2^n \cdot (d'(m) + 4m^4/2^n)$

Fig. 1. Bounds on $\mathbf{Adv}^{\mathsf{pf}}_{\mathrm{CBC}}(q, n, m)$ and $\mathbf{Adv}^{\mathsf{any}}_{\mathrm{ECBC}}(q, n, m)$, assuming $m \le 2^{n/2-1}$.

is actually a little stronger. See Fig. 1.) This implies the same bound holds for $\mathbf{Adv}^{\mathsf{eq}}_{\mathrm{CBC}}(q, n, m)$.

Context and discussion. When $\pi = E(K, \cdot)$, where $K \in \mathcal{K}$ is a random key for blockcipher E: $\mathcal{K} \times \{0,1\}^n \to \{0,1\}^n$, the function CBC_π is a popular message authentication code (MAC). Assuming E is a good pseudorandom permutation (PRP), the dominant term in a bound on the probability of forgery in an atk-type chosen-message attack is $\mathbf{Adv}^{\mathsf{atk}}_{\mathrm{CBC}}(q, n, m)$, where q is the sum of the number of MAC-generation and MAC-verification queries made by the adversary (cf. [1]). Thus the quality of guarantee we get on the security of the MAC is a function of how good an upper bound we can prove on $\mathbf{Adv}^{\mathsf{atk}}_{\mathrm{CBC}}(q, n, m)$.

It is well known that the CBC MAC is insecure when the messages MACed have varying lengths (specifically, it is forgeable under an any-attack that uses just one MAC-generation and one MAC-verification query, each of at most two blocks) so the case $\mathsf{atk} = \mathsf{any}$ is not of interest for CBC. The case where all messages MACed have the same length ($\mathsf{atk} = \mathsf{eq}$) is the most basic one, and where positive results were first obtained [2]. The case $\mathsf{atk} = \mathsf{pf}$ is interesting because one way to get a secure MAC for varying-length inputs is to apply a prefix-free encoding to the data before MACing it. The most common such encoding is to include in the first block of each message an encoding of its length.

We emphasize that our results are about CBC_π for a random permutation π: $\{0,1\}^n \to \{0,1\}^n$, and not about CBC_ρ for a random function ρ: $\{0,1\}^n \to \{0,1\}^n$. Since our bounds are better than the cost to convert between a random n-bit function and a random n-bit permutation using the switching lemma [2], the distinction is significant. Indeed for the prefix-free case, applying CBC over a random function on n bits is known to admit an attack more effective than that which is ruled out by our bound [6].

Encrypted CBC. The ECBC function $\mathrm{ECBC}_{\pi_1,\pi_2}$ associated to permutations π_1, π_2 on n bits takes a message M that is a multiple of n bits and returns $\pi_2(\mathrm{CBC}_{\pi_1}(M))$. Define $\mathbf{Adv}^{\mathsf{atk}}_{\mathrm{ECBC}}(q, n, m)$ analogously to the CBC case above ($\mathsf{atk} \in \{\mathsf{any}, \mathsf{eq}, \mathsf{pf}\}$). Petrank and Rackoff [15] showed that $\mathbf{Adv}^{\mathsf{any}}_{\mathrm{ECBC}}(q, n, m) \le 2.5\, m^2q^2/2^n$. A better bound, $\mathbf{Adv}^{\mathsf{eq}}_{\mathrm{ECBC}}(q, n, m) \le q^2/2^n \cdot (1 + cm^2/2^n + cm^6/2^{2n})$ for some constant c, is possible for the $\mathsf{atk} = \mathsf{eq}$ case based on a lemma of Dodis *et al.* [9], but the point of the ECBC construction is to achieve any-security. We improve on the result of Petrank and Rackoff to show that $\mathbf{Adv}^{\mathsf{any}}_{\mathrm{ECBC}}(q, n, m) \le q^2/2^n \cdot (d'(m) + 4m^4/2^n)$ where $d'(m)$ is the maximum, over all $m' \le m$, of the number of divisors of m'. (Once again see Fig. 1.) Note that the function $d'(m) \approx m^{1/\ln\ln(m)}$ grows slowly.

The MAC corresponding to ECBC (namely $\mathrm{ECBC}_{\pi_1,\pi_2}$ when $\pi_1 = E(K_1,\cdot)$ and $\pi_2 = E(K_2,\cdot)$ for random keys $K_1, K_2 \in \mathcal{K}$ of a blockcipher $E\colon \mathcal{K}\times\{0,1\}^n \to \{0,1\}^n$) was developed by the RACE project [5]. This MAC is interesting as a natural and practical variant of the CBC MAC that correctly handles messages of varying lengths. A variant of ECBC called CMAC was recently adopted as a NIST-recommended mode of operation [14]. As with the CBC MAC, our results imply improved guarantees on the forgery probability of the ECBC MAC under a chosen-message attack, but this time of type any rather than merely pf, and with the improvement being numerically more substantial.

More definitions. The collision-probability $\mathbf{CP}^{\mathsf{atk}}_{n,m}$ of the CBC MAC is the maximum, over all pairs of messages (M_1, M_2) in an appropriate atk-dependent range, of the probability, over random π, that $\mathrm{CBC}_\pi(M_1) = \mathrm{CBC}_\pi(M_2)$. For $\mathsf{atk} = \mathsf{any}$ the range is any pair of distinct strings of length a positive multiple of n but at most mn; for $\mathsf{atk} = \mathsf{pf}$ it is any such pair where neither string is a prefix of the other; and for $\mathsf{atk} = \mathsf{eq}$ it is any pair of distinct strings of exactly mn bits. The *full collision probability* $\mathbf{FCP}^{\mathsf{atk}}_{n,m}$ is similar except that the probability is of the event $C_2^{m_2} \in \{C_1^1, \ldots, C_1^{m_1}, C_2^1, \ldots, C_2^{m_2-1}\}$ where, for each $b \in \{1,2\}$, we have $C_b^i = \pi(C_b^{i-1} \oplus M_b^i)$ for $m_b = |M_b|/n$ and $i \in [1..m_b]$ and $C_b^0 = 0^n$. Note that these definitions do not involve an adversary and in this sense are simpler than the advantage functions considered above.

Reductions to FCP and CP. By viewing ECBC as an instance of the Carter-Wegman paradigm [18], one can reduce bounding $\mathbf{Adv}^{\mathsf{atk}}_{\mathrm{ECBC}}(q,n,m)$ (for $\mathsf{atk} \in \{\mathsf{any}, \mathsf{eq}, \mathsf{pf}\}$) to bounding $\mathbf{CP}^{\mathsf{atk}}_{n,m}$ (see [7], stated here as Lemma 3). This simplifies the analysis because one is now faced with a combinatorial problem rather than consideration of a dynamic, adaptive adversary.

The first step in our analysis of the CBC MAC is to provide an analogous reduction (Lemma 1) that reduces bounding $\mathbf{Adv}^{\mathsf{pf}}_{\mathrm{CBC}}(q,n,m)$ to bounding $\mathbf{FCP}^{\mathsf{pf}}_{n,m}$. Unlike the case of ECBC, the reduction is not immediate and does not rely on the Carter-Wegman paradigm. Rather it is proved directly using the game-playing approach [4, 16].

Bounds on FCP and CP. Black and Rogaway [7] show that $\mathbf{CP}^{\mathsf{any}}_{n,m} \le 2(m^2 + m)/2^n$. Dodis, Gennaro, Håstad, Krawczyk, and Rabin [9] show that $\mathbf{CP}^{\mathsf{eq}}_{n,m} \le 2^{-n} + cm^2/2^{2n} + cm^3/2^{3n}$ for some absolute constant c. (The above-mentioned bound on $\mathbf{Adv}^{\mathsf{eq}}_{\mathrm{ECBC}}(q,n,m)$ is obtained via this.) We build on their techniques to show (cf. Lemma 4) that $\mathbf{CP}^{\mathsf{any}}_{n,m} \le 2d'(m)/2^n + 8m^4/2^{2n}$. Our bound on $\mathbf{Adv}^{\mathsf{any}}_{\mathrm{ECBC}}(q,n,m)$ then follows. We also show that $\mathbf{FCP}^{\mathsf{pf}}_{n,m} \le 8m/2^n + 8m^4/2^{2n}$. Our bound on $\mathbf{Adv}^{\mathsf{pf}}_{\mathrm{CBC}}(q,n,m)$ then follows.

We remark that the security proof of RMAC [11] had stated and used a claim that implies $\mathbf{CP}^{\mathsf{any}}_{n,m} \le 12m/2^n$, but the published proof was wrong. Our Lemma 4 both fixes and improves that result.

Further related work. Other approaches to the analysis of the CBC MAC and the encrypted CBC MAC include those of Maurer [13] and Vaudenay [17], but they only obtain bounds of $m^2q^2/2^n$.

2 Definitions

Notation. The empty string is denoted ε. If x is a string then $|x|$ denotes its length. We let $B_n = \{0,1\}^n$. If $x \in B_n^*$ then $|x|_n = |x|/n$ denotes the number of n-bit blocks in it. If $X \subseteq \{0,1\}^*$ then $X^{\leq m}$ denotes the set of all non-empty strings formed by concatenating m or fewer strings from X and X^+ denotes the set of all strings formed by concatenating one or more strings from X. If $M \in B_n^*$ then M^i denotes its i-th n-bit block and $M^{i \to j}$ denotes the string $M^i \| \cdots \| M^j$, for $1 \leq i \leq j \leq |M|_n$. If S is a set equipped with some probability distribution then $s \xleftarrow{\$} S$ denotes the operation of picking s from S according to this distribution. If no distribution is explicitly specified, it is understood to be uniform.

We denote by $\mathrm{Perm}(n)$ the set of all permutations over $\{0,1\}^n$, and by $\mathrm{Func}(n)$ the set of all functions mapping $\{0,1\}^*$ to $\{0,1\}^n$. (Both these sets are viewed as equipped with the uniform distribution.) A blockcipher E (with block-length n and key-space $\mathcal{K}$) is identified with the set of permutations $\{E_K\colon K \in \mathcal{K}\}$ where $E_K\colon \{0,1\}^n \to \{0,1\}^n$ denotes the map specified by key $K \in \mathcal{K}$. The distribution is that induced by a random choice of K from $\mathcal{K}$, so $f \xleftarrow{\$} E$ is the same as $K \xleftarrow{\$} \mathcal{K},\ f \leftarrow E_K$.

Security. An adversary is a randomized algorithm that always halts. Let $\mathcal{A}^{\mathsf{atk}}_{q,n,m}$ denote the class of adversaries that make at most q oracle queries, where if $\mathsf{atk} = \mathsf{eq}$, then each query is in B_n^m; if $\mathsf{atk} = \mathsf{pf}$, then each query is in $B_n^{\leq m}$ and no query is a prefix of another; and if $\mathsf{atk} = \mathsf{any}$ then each query is in $B_n^{\leq m}$. We remark that the adversaries considered here are computationally unbounded. In this paper we always consider deterministic, stateless oracles and thus we will assume that an adversary never repeats an oracle query. We also assume that an adversary never asks a query outside of the implicitly understood domain of interest.

Let $F\colon D \to \{0,1\}^n$ be a set of functions and let $A \in \mathcal{A}^{\mathsf{atk}}_{q,n,m}$ be an adversary, where $\mathsf{atk} \in \{\mathsf{eq}, \mathsf{pf}, \mathsf{any}\}$. By "$A^f \Rightarrow 1$" we denote the event that A outputs 1 with oracle f. The advantage of A (in distinguishing an instance of F from a random function outputting n bits) and the advantage of F are defined, respectively, as

$$\mathbf{Adv}_F(A) = \Pr[f \xleftarrow{\$} F:\ A^f \Rightarrow 1] - \Pr[f \xleftarrow{\$} \mathrm{Func}(n):\ A^f \Rightarrow 1] \quad \text{and}$$
$$\mathbf{Adv}_F^{\mathsf{atk}}(q,n,m) = \max_{A \in \mathcal{A}^{\mathsf{atk}}_{q,n,m}} \{\ \mathbf{Adv}_F(A)\ \}\ .$$

Note that since $\mathcal{A}^{\mathsf{eq}}_{q,n,m} \subseteq \mathcal{A}^{\mathsf{pf}}_{q,n,m} \subseteq \mathcal{A}^{\mathsf{any}}_{q,n,m}$, we have

$$\mathbf{Adv}_F^{\mathsf{eq}}(q,n,m)\ \leq\ \mathbf{Adv}_F^{\mathsf{pf}}(q,n,m)\ \leq\ \mathbf{Adv}_F^{\mathsf{any}}(q,n,m)\ . \tag{1}$$

Cbc and Ecbc. Fix $n \geq 1$. For $M \in B_n^m$ and $\pi\colon B_n \to B_n$ then define $\mathrm{CBC}_\pi^M[i]$ inductively for $i \in [0..m]$ via $\mathrm{CBC}_\pi^M[0] = 0^n$ and $\mathrm{CBC}_\pi^M[i] = \pi(\mathrm{CBC}_\pi^M \oplus M^i)$ for $i \in [1..m]$. We associate to π the CBC MAC function $\mathrm{CBC}_\pi\colon B_n^+ \to B_n$ defined by $\mathrm{CBC}_\pi(M) = \mathrm{CBC}_\pi^M[m]$ where $m = |M|_n$. We let $\mathrm{CBC} = \{\mathrm{CBC}_\pi\colon \pi \in \mathrm{Perm}(n)\}$. This set of functions has the distribution induced by picking π uniformly from $\mathrm{Perm}(n)$.

To functions $\pi_1, \pi_2\colon B_n \to B_n$ we associate the encrypted CBC MAC function $\mathrm{ECBC}_{\pi_1,\pi_2}\colon B_n^+ \to B_n$ defined by $\mathrm{ECBC}_{\pi_1,\pi_2}(M) = \pi_2(\mathrm{CBC}_{\pi_1}(M))$ for all $M \in B_n^+$. We let $\mathrm{ECBC} = \{\mathrm{ECBC}_{\pi_1,\pi_2}\colon \pi_1, \pi_2 \in \mathrm{Perm}(n)\}$. This set of functions has the distribution induced by picking π_1, π_2 independently and uniformly at random from $\mathrm{Perm}(n)$.

Collisions. For $M_1, M_2 \in B_n^*$ we define the *prefix predicate* $\mathsf{pf}(M_1, M_2)$ to be true if either M_1 is a prefix of M_2 or M_2 is a prefix of M_1, and false otherwise. Note that $\mathsf{pf}(M, M) = \mathsf{true}$ for any $M \in B_n^*$. Let

$$\begin{aligned}
\mathcal{M}_{n,m}^{\mathsf{eq}} &= \{(M_1, M_2) \in B_n^m \times B_n^m : M_1 \neq M_2\}, \\
\mathcal{M}_{n,m}^{\mathsf{pf}} &= \{(M_1, M_2) \in B_n^{\leq m} \times B_n^{\leq m} : \mathsf{pf}(M_1, M_2) = \mathsf{false}\}, \quad \text{and} \\
\mathcal{M}_{n,m}^{\mathsf{any}} &= \{(M_1, M_2) \in B_n^{\leq m} \times B_n^{\leq m} : M_1 \neq M_2\}\ .
\end{aligned}$$

For $M_1, M_2 \in B_n^+$ and $\mathsf{atk} \in \{\mathsf{eq}, \mathsf{pf}, \mathsf{any}\}$ we then let

$$\begin{aligned}
\mathbf{CP}_n(M_1, M_2) &= \Pr[\pi \stackrel{\$}{\leftarrow} \mathrm{Perm}(n) : \mathrm{CBC}_\pi(M_1) = \mathrm{CBC}_\pi(M_2)] \\
\mathbf{CP}_{n,m}^{\mathsf{atk}} &= \max_{(M_1,M_2) \in \mathcal{M}_{n,m}^{\mathsf{atk}}} \{\, \mathbf{CP}_n(M_1, M_2) \,\}\ .
\end{aligned}$$

For $M_1, M_2 \in B_n^+$ we let $\mathbf{FCP}_n(M_1, M_2)$ (the full collision probability) be the probability, over $\pi \stackrel{\$}{\leftarrow} \mathrm{Perm}(n)$, that $\mathrm{CBC}_\pi(M_2)$ is in the set

$$\{\mathrm{CBC}_\pi^{M_1}[1], \ldots, \mathrm{CBC}_\pi^{M_1}[m_1], \mathrm{CBC}_\pi^{M_2}[1], \ldots, \mathrm{CBC}_\pi^{M_2}[m_2 - 1]\}$$

where $m_b = |M_b|_n$ for $b = 1, 2$. For $\mathsf{atk} \in \{\mathsf{eq}, \mathsf{pf}, \mathsf{any}\}$ we then let

$$\mathbf{FCP}_{n,m}^{\mathsf{atk}} = \max_{(M_1,M_2) \in \mathcal{M}_{n,m}^{\mathsf{atk}}} \{\, \mathbf{FCP}_n(M_1, M_2) \,\}\ .$$

3 Results on the CBC MAC

We state results only for the $\mathsf{atk} = \mathsf{pf}$ case; results for $\mathsf{atk} = \mathsf{eq}$ follow due to (1). To bound $\mathbf{Adv}_{\mathrm{CBC}}^{\mathsf{pf}}(q, n, m)$ we must consider a dynamic adversary that adaptively queries its oracle. Our first lemma reduces this problem to that of bounding a more "static" quantity whose definition does not involve an adversary, namely the full collision probability of the CBC MAC. The proof is in Section 5.

Lemma 1. *For any n, m, q,*

$$\mathbf{Adv}_{\mathrm{CBC}}^{\mathsf{pf}}(q, n, m) \leq q^2 \cdot \mathbf{FCP}_{n,m}^{\mathsf{pf}} + \frac{4mq^2}{2^n}\ . \quad \blacksquare$$

The next lemma bounds the full collision probability of the CBC MAC. The proof is given in Section 8.

Lemma 2. *For any n, m with $m^2 \leq 2^{n-2}$,*

$$\mathbf{FCP}^{\mathsf{pf}}_{n,m} \leq \frac{8m}{2^n} + \frac{8m^4}{2^{2n}} \ . \quad \blacksquare$$

Combining the above two lemmas we bound $\mathbf{Adv}^{\mathsf{pf}}_{\mathrm{CBC}}(q, n, m)$:

Theorem 1. *For any n, m, q with $m^2 \leq 2^{n-2}$,*

$$\mathbf{Adv}^{\mathsf{pf}}_{\mathrm{CBC}}(q, n, m) \leq \frac{mq^2}{2^n} \cdot \left(12 + \frac{8m^3}{2^n}\right) \ . \quad \blacksquare$$

4 Results on the Encrypted CBC MAC

Following [7], we view ECBC as an instance of the Carter-Wegman paradigm [18]. This enables us to reduce the problem of bounding $\mathbf{Adv}^{\mathsf{atk}}_{\mathrm{ECBC}}(q, n, m)$ to bounding the collision probability of the CBC MAC, as stated in the next lemma. A proof of the following is provided in [3].

Lemma 3. *For any $n, m, q \geq 1$ and any $\mathsf{atk} \in \{\mathsf{eq}, \mathsf{pf}, \mathsf{any}\}$,*

$$\mathbf{Adv}^{\mathsf{atk}}_{\mathrm{ECBC}}(q, n, m) \leq \frac{q(q-1)}{2} \cdot \left(\mathbf{CP}^{\mathsf{atk}}_{n,m} + \frac{1}{2^n}\right) \ . \quad \blacksquare$$

Petrank and Rackoff [15] show that

$$\mathbf{Adv}^{\mathsf{any}}_{\mathrm{ECBC}}(q, n, m) \leq 2.5\, m^2 q^2 / 2^n \ . \tag{2}$$

Dodis *et al.* [9] show that $\mathbf{CP}^{\mathsf{eq}}_{n,m} \leq 2^{-n} + cm^2 \cdot 2^{-2n} + cm^6 \cdot 2^{-3n}$ for some absolute constant c. Combining this with Lemma 3 leads to

$$\mathbf{Adv}^{\mathsf{eq}}_{\mathrm{ECBC}}(q, n, m) \leq \frac{q^2}{2^n} \cdot \left(1 + \frac{cm^2}{2^n} + \frac{cm^6}{2^{2n}}\right) \ .$$

However, the case of $\mathsf{atk} = \mathsf{eq}$ is not interesting here, since the point of ECBC is to gain security even for $\mathsf{atk} = \mathsf{any}$. To obtain an improvement for this, we show the following, whose proof is in Section 7:

Lemma 4. *For any n, m with $m^2 \leq 2^{n-2}$,*

$$\mathbf{CP}^{\mathsf{any}}_{n,m} \leq \frac{2d'(m)}{2^n} + \frac{8m^4}{2^{2n}}$$

where $d'(m)$ is the maximum, over all $m' \leq m$, of the number of positive numbers that divide m'. $\blacksquare$

The function $d'(m)$ grows slowly; in particular, $d'(m) < m^{0.7/\ln\ln(m)}$ for all sufficiently large m [10, Theorem 317]. We have verified that $d'(m) \le m^{1.07/\ln\ln m}$ for all $m \le 2^{64}$ (and we assume for all m), and also that $d'(m) \le \lg^2 m$ for all $m \le 2^{25}$.

Combining the above with Lemma 3 leads to the following:

Theorem 2. *For any n, m, q with $m^2 \le 2^{n-2}$,*

$$\mathbf{Adv}^{\mathsf{any}}_{\mathrm{ECBC}}(q,n,m) \le \frac{q^2}{2^n} \cdot \left(d'(m) + \frac{4m^4}{2^n} \right) . \quad \blacksquare$$

5 Bounding FCP Bounds CBC (Proof of Lemma 1)

The proof is by the game-playing technique [2, 4]. Let A be an adversary that asks exactly q queries, $M_1, \ldots, M_q \in B_n^{\le m}$, where no queries M_r and M_s, for $r \ne s$, share a prefix in B_n^+. We must show that $\mathbf{Adv}_{\mathrm{CBC}}(A) \le q^2 \cdot \mathbf{FCP}^{\mathsf{pf}}_{n,m} + 4mq^2/2^n$.

Refer to games D0–D7 as defined in Fig. 2. Sets $\mathrm{Dom}(\pi)$ and $\mathrm{Ran}(\pi)$ start off as empty and automatically grow as points are added to the domain and range of the partial function π. Sets $\overline{\mathrm{Dom}}(\pi)$ and $\overline{\mathrm{Ran}}(\pi)$ are the complements of these sets relative to $\{0,1\}^n$. They automatically shrink as points join the domain and range of π. We write boolean values as 0 (false) and 1 (true), and we sometimes write **then** as a colon. The flag *bad* is initialized to $\mathsf{0}$ and the map π is initialized as everywhere undefined. We now briefly explain the sequence.

D1: Game D1 faithfully simulates the CBC MAC construction. Instead of choosing a random permutation π up front, we fill in its values as-needed, so as to not to create a conflict. Observe that if $bad = \mathsf{0}$ following lines 107–108 then $\widehat{C}_s^{m_s} = C_s^{m_s}$ and so game D1 always returns $C_s^{m_s}$, regardless of *bad*. This makes clear that $\Pr[A^{\mathrm{D1}} \Rightarrow 1] = \Pr[\pi \stackrel{\$}{\leftarrow} \mathrm{Perm}(n) :\ A^{\mathrm{CBC}_\pi} \Rightarrow 1]$. **D0:** Game D0 is obtained from game D1 by omitting line 110 and the statements that immediately follow the setting of *bad* at lines 107 and 108. Thus this game returns the random n-bit string $C_s^{m_s} = \widehat{C}_s^{m_s}$ in response to each query M_s, so $\Pr[A^{\mathrm{D0}} \Rightarrow 1] = \Pr[\rho \stackrel{\$}{\leftarrow} \mathrm{Func}(n) :\ A^{\rho} \Rightarrow 1]$. Now games D1 and D0 have been defined so as to be syntactically identical except on statements that immediately follow the setting of *bad* to true or the checking if *bad* is true, so the fundamental lemma of game-playing [4] says us that $\Pr[A^{\mathrm{D1}} \Rightarrow 1] - \Pr[A^{\mathrm{D0}} \Rightarrow 1] \le \Pr[A^{\mathrm{D0}}$ sets *bad* $]$. As $\mathbf{Adv}_{\mathrm{CBC}}(A) = \Pr[A^{\mathrm{CBC}_\pi} \Rightarrow 1] - \Pr[A^{\rho} \Rightarrow 1] = \Pr[A^{\mathrm{D1}} \Rightarrow 1] - \Pr[A^{\mathrm{D0}} \Rightarrow 1]$, the rest of the proof bounds $\mathbf{Adv}_{\mathrm{CBC}}(A)$ by bounding $\Pr[A^{\mathrm{D0}}$ sets *bad* $]$.

D0→D2: We rewrite game D0 as game D2 by dropping the variable $\widehat{C}_s^{m_s}$ and using variable $C_s^{m_s}$ in its place, as these are always equal. We have that $\Pr[A^{\mathrm{D0}}$ sets *bad* $] = \Pr[A^{\mathrm{D2}}$ sets *bad* $]$. **D2→D3**: Next we eliminate line 209 and then, to compensate, we set *bad* any time the value $X_s^{m_s}$ or $C_s^{m_s}$ would have been accessed. This accounts for the new line 303 and the new disjunct on lines 310. To compensate for the removal of line 209 we must also set *bad* whenever C_s^i, chosen at line 204, happens to be a prior value $C_r^{m_r}$. This is done at line 306. We have that $\Pr[A^{\mathrm{D2}}$ sets *bad* $] \le \Pr[A^{\mathrm{D3}}$ sets *bad* $]$. **D3→D4**: Next we remove the

On the s^{th} query $F(M_s)$ — Game D1

$m_s \leftarrow |M_s|_n, \quad C_s^0 \leftarrow 0^n$
for $i \leftarrow 1$ **to** $m_s - 1$ **do**
$\quad X_s^i \leftarrow C_s^{i-1} \oplus M_s^i$
$\quad$ **if** $X_s^i \in \mathrm{Dom}(\pi)$ **then** $C_s^i \leftarrow \pi(X_s^i)$
$\qquad$ **else** $\pi(X_s^i) \leftarrow C_s^i \xleftarrow{\$} \overline{\mathrm{Ran}}(\pi)$
$X_s^{m_s} \leftarrow C_s^{m_s-1} \oplus M_s^{m_s}$
$\widehat{C}_s^{m_s} \leftarrow C_s^{m_s} \xleftarrow{\$} \{0,1\}^n$
if $C_s^{m_s} \in \mathrm{Ran}(\pi)$: $bad \leftarrow 1$, $C_s^{m_s} \xleftarrow{\$} \overline{\mathrm{Ran}}(\pi)$
if $X_s^{m_s} \in \mathrm{Dom}(\pi)$: $bad \leftarrow 1$, $C_s^{m_s} \leftarrow \pi(X_s^{m_s})$
$\pi(X_s^{m_s}) \leftarrow C_s^{m_s}$
if bad **then return** $C_s^{m_s}$
return $\widehat{C}_s^{m_s}$

On the s^{th} query $F(M_s)$ — Game D2

$m_s \leftarrow |M_s|_n, \quad C_s^0 \leftarrow 0^n$
for $i \leftarrow 1$ **to** $m_s - 1$ **do**
$\quad X_s^i \leftarrow C_s^{i-1} \oplus M_s^i$
$\quad$ **if** $X_s^i \in \mathrm{Dom}(\pi)$ **then** $C_s^i \leftarrow \pi(X_s^i)$
$\qquad$ **else** $\pi(X_s^i) \leftarrow C_s^i \xleftarrow{\$} \overline{\mathrm{Ran}}(\pi)$
$X_s^{m_s} \leftarrow C_s^{m_s-1} \oplus M_s^{m_s}$
$C_s^{m_s} \xleftarrow{\$} \{0,1\}^n$
if $X_s^{m_s} \in \mathrm{Dom}(\pi) \vee C_s^{m_s} \in \mathrm{Ran}(\pi)$
$\quad$ **then** $bad \leftarrow 1$
$\pi(X_s^{m_s}) \leftarrow C_s^{m_s}$
return $C_s^{m_s}$

On the s^{th} query $F(M_s)$ — Game D3

$m_s \leftarrow |M_s|_n, \quad C_s^0 \leftarrow 0^n$
for $i \leftarrow 1$ **to** $m_s - 1$ **do**
$\quad X_s^i \leftarrow C_s^{i-1} \oplus M_s^i$
$\quad$ **if** $(\exists r < s)(X_s^i = X_r^{m_r})$: $bad \leftarrow 1$
$\quad$ **if** $X_s^i \in \mathrm{Dom}(\pi)$ **then** $C_s^i \leftarrow \pi(X_s^i)$
$\qquad$ **else** $\pi(X_s^i) \leftarrow C_s^i \xleftarrow{\$} \overline{\mathrm{Ran}}(\pi)$,
$\qquad\quad$ **if** $(\exists r < s)(C_s^i = C_r^{m_r})$: $bad \leftarrow 1$
$X_s^{m_s} \leftarrow C_s^{m_s-1} \oplus M_s^{m_s}$
$C_s^{m_s} \xleftarrow{\$} \{0,1\}^n$
if $X_s^{m_s} \in \mathrm{Dom}(\pi) \vee C_s^{m_s} \in \mathrm{Ran}(\pi) \vee$
$\quad (\exists r < s)(X_s^{m_s} = X_r^{m_r} \vee C_s^{m_s} = C_r^{m_r})$
$\quad$ **then** $bad \leftarrow 1$
return $C_s^{m_s}$

On the s^{th} query $F(M_s)$ — Game D4

$m_s \leftarrow |M_s|_n, \quad C_s^0 \leftarrow 0^n$
for $i \leftarrow 1$ **to** $m_s - 1$ **do**
$\quad X_s^i \leftarrow C_s^{i-1} \oplus M_s^i$
$\quad$ **if** $(\exists r < s)(X_s^i = X_r^{m_r})$: $bad \leftarrow 1$
$\quad$ **if** $X_s^i \in \mathrm{Dom}(\pi)$ **then** $C_s^i \leftarrow \pi(X_s^i)$
$\qquad$ **else** $\pi(X_s^i) \leftarrow C_s^i \xleftarrow{\$} \overline{\mathrm{Ran}}(\pi)$
$X_s^{m_s} \leftarrow C_s^{m_s-1} \oplus M_s^{m_s}$
if $X_s^{m_s} \in \mathrm{Dom}(\pi) \vee$
$\quad (\exists r < s)(X_s^{m_s} = X_r^{m_r})$ **then** $bad \leftarrow 1$
$C_s^{m_s} \xleftarrow{\$} \{0,1\}^n$
return $C_s^{m_s}$

Game D5

for $s \leftarrow 1$ **to** q **do**
$\quad C_s^0 \leftarrow 0^n$
$\quad$ **for** $i \leftarrow 1$ **to** $\mathtt{m}_s - 1$ **do**
$\qquad X_s^i \leftarrow C_s^{i-1} \oplus \mathtt{M}_s^i$
$\qquad$ **if** $(\exists r < s)(X_s^i = X_r^{\mathtt{m}_r})$: $bad \leftarrow 1$
$\qquad$ **if** $X_s^i \in \mathrm{Dom}(\pi)$ **then** $C_s^i \leftarrow \pi(X_s^i)$
$\qquad\quad$ **else** $\pi(X_s^i) \leftarrow C_s^i \xleftarrow{\$} \overline{\mathrm{Ran}}(\pi)$
$\quad X_s^{\mathtt{m}_s} \leftarrow C_s^{\mathtt{m}_s-1} \oplus \mathtt{M}_s^{\mathtt{m}_s}$
$\quad$ **if** $(\exists r < s)$ $(X_s^{\mathtt{m}_s} \in \mathrm{Dom}(\pi) \vee$
$\qquad X_s^{\mathtt{m}_s} = X_r^{\mathtt{m}_r})$ **then** $bad \leftarrow 1$

Game D6

$\pi \xleftarrow{\$} \mathrm{Perm}(n)$
for $s \in [1\,..\,q]$ **do**
$\quad C_s^0 \leftarrow 0^n$
$\quad$ **for** $i \leftarrow 1$ **to** $\mathtt{m}_s - 1$ **do**
$\qquad X_s^i \leftarrow C_s^{i-1} \oplus \mathtt{M}_s^i$
$\qquad C_s^i \leftarrow \pi(X_s^i)$
$\quad X_s^{\mathtt{m}_s} \leftarrow C_s^{\mathtt{m}_s-1} \oplus \mathtt{M}_s^{\mathtt{m}_s}$
$bad \leftarrow (\exists (r,i) \neq (s,\mathtt{m}_s))\ [X_r^i = X_s^{\mathtt{m}_s}]$

Game D7

$\pi \xleftarrow{\$} \mathrm{Perm}(n)$
$C_1^0 \leftarrow C_2^0 \leftarrow 0^n$
for $i \leftarrow 1$ **to** $\mathtt{m}_1$ **do**
$\quad X_1^i \leftarrow C_1^{i-1} \oplus \mathtt{M}_1^i,\ C_1^i \leftarrow \pi(X_1^i)$
for $i \leftarrow 1$ **to** $\mathtt{m}_2$ **do**
$\quad X_2^i \leftarrow C_2^{i-1} \oplus \mathtt{M}_2^i,\ C_2^i \leftarrow \pi(X_2^i)$
$bad \leftarrow X_2^{\mathtt{m}_2} \in \{X_1^1, \ldots, X_1^{\mathtt{m}_1},$
$\qquad\qquad X_2^1, \ldots, X_2^{\mathtt{m}_2-1}\}$

Fig. 2. Games D0–D7 used in the proof of Lemma 1.

test $(\exists r < s)(C_s^i = C_r^{m_r})$ at line 306, the test if $C_s^{m_s} \in \mathrm{Ran}(\pi)$ at line 309, and the test for $C_s^{m_s} = C_r^{m_r}$ at line 310, bounding the probability that *bad* gets set due to any of these three tests. To bound the probability of *bad* getting set at line 306: A total of at most mq times we select at line 305 a random sample C_s^i from a set of size at least $2^n - mq \geq 2^{n-1}$. (We may assume that $mq \leq 2^{n-1}$ since the probability bound given by our lemma exceeds 1 if $mq > 2^{n-1}$.) The chance that one of these points is equal to any of the at most q points $C_r^{m_r}$ is thus at most $2mq^2/2^n$. To bound the probability of *bad* getting set by the $C_s^{m_s} \in \mathrm{Ran}(\pi)$ test at line 309: easily seen to be at most $mq^2/2^n$. To bound the probability of *bad* getting set by the $C_s^{m_s} = C_r^{m_r}$ test at line 310: easily seen to be at most $q^2/2^n$. Overall then, $\Pr[A^{\mathrm{D3}} \text{ sets } \mathit{bad}\,] \leq \Pr[A^{\mathrm{D4}} \text{ sets } \mathit{bad}\,] + 4mq^2/2^n$.

D4→D5: The value $C_s^{m_s}$ returned to the adversary in response to a query in game D4 is never referred to again in the code and has no influence on the game and the setting of *bad*. Accordingly, we may think of these values as being chosen up-front by the adversary who, correspondingly, makes an optimal choice of message queries $\mathtt{M}_1, \ldots, \mathtt{M}_q$ so as to maximize the probability that *bad* gets set in game D4. Queries $\mathtt{M}_1, \ldots, \mathtt{M}_q \in B_n^{\leq m}$ are prefix-free (meaning that no two strings from this list share a prefix $P \in B_n^+$) and the strings have block lengths of $\mathtt{m}_1, \ldots, \mathtt{m}_q$, respectively, where each $\mathtt{m}_i \leq m$. We fix such an optimal vector of messages and message lengths in passing to game D5, so that $\Pr[A^{\mathrm{D4}} \text{ sets } \mathit{bad}\,] \leq \Pr[\mathrm{D5} \text{ sets } \mathit{bad}\,]$. The adversary has effectively been eliminated at this point.

D5→D6: Next we postpone the evaluation of *bad* and undo the "lazy defining" of π to arrive at game D6. We have $\Pr[\mathrm{D5} \text{ sets } \mathit{bad}\,] \leq \Pr[\mathrm{D6} \text{ sets } \mathit{bad}\,]$. **D6→D7**: Next we observe that in game D6, some pair r, s must contribute at least an average amount to the probability that *bad* gets set. Namely, for any $r, s \in [1 \,..\, q]$ where $r \neq s$ define $\mathit{bad}_{r,s}$ as

$$(X_s^{\mathtt{m}_s} = X_r^i \text{ for some } i \in [1 \,..\, \mathtt{m}_r]) \vee (X_s^{\mathtt{m}_s} = X_s^i \text{ for some } i \in [1 \,..\, \mathtt{m}_s - 1])$$

and note that *bad* is set at line 607 iff $\mathit{bad}_{r,s} = 1$ for some $r \neq s$, and so there must be an $r \neq s$ such that $\Pr[\mathrm{D6} \text{ sets } \mathit{bad}_{r,s}] \geq (1/q(q-1)) \Pr[\mathrm{D6} \text{ sets } \mathit{bad}\,]$. Fixing such an r, s and renaming $\mathtt{M}_1 = \mathtt{M}_r$, $\mathtt{M}_2 = \mathtt{M}_s$, $\mathtt{m}_1 = \mathtt{m}_r$, and $\mathtt{m}_2 = \mathtt{m}_s$, we arrive at game D7 knowing that

$$\Pr[\mathrm{D6} \text{ sets } \mathit{bad}\,] \;\leq\; q^2 \cdot \Pr[\mathrm{D7} \text{ sets } \mathit{bad}\,]\,. \tag{3}$$

Now $\Pr[\mathrm{D7} \text{ sets } \mathit{bad}\,] = \mathbf{FCP}_n(\mathtt{M}_1, \mathtt{M}_2) \leq \mathbf{FCP}^{\mathsf{pf}}_{n,m}$ by the definition of FCP and the fact that π is a permutation. Putting all the above together we are done.

6 A Graph-Based Representation of CBC

In this section we describe a graph-based view of CBC computations and provide some lemmas that will then allow us to reduce the problem of upper bounding the collision probabilities $\mathbf{CP}^{\mathsf{any}}_{n,m}$ and $\mathbf{FCP}^{\mathsf{pf}}_{n,m}$ to combinatorial counting problems.

We fix for the rest of this section a blocklength $n \geq 1$ and a pair of distinct messages $M_1 = M_1^1 \cdots M_1^{m_1} \in B_n^{m_1}$ and $M_2 = M_2^1 \cdots M_2^{m_2} \in B_n^{m_2}$ where $m_1, m_2 \geq 1$. We let $\ell = \max(m_1, m_2)$.

```
algorithm Perm2Graph(M_1, M_2, π)            //M_1 ∈ B_n^{m_1}, M_2 ∈ B_n^{m_2}, π ∈ Perm(n)
   σ(0) ← 0^n,   ν ← 0,   E ← ∅
   for b ← 1 to 2 do
      v ← 0
      for i ← 1 to m_b do
         if ∃w s.t. (v, w) ∈ E and L((v, w)) = M_b^i then v ← w
         else if ∃w s.t. π(σ(v) ⊕ M_b^i) = σ(w) then
                  E ← E ∪ {(v, w)}, L((v, w)) ← M_b^i, v ← w
              else ν ← ν + 1, σ(ν) ← π(σ(v) ⊕ M_b^i),
                  E ← E ∪ {(v, ν)}, L((v, ν)) ← M_b^i, v ← ν
   return G ← ([0..ν], E, L)
```

```
algorithm Graph2Profs(G)            //G ∈ 𝒢(M_1, M_2), M_1 ∈ B_n^{m_1}, M_2 ∈ B_n^{m_2}
   Prof_1 ← Prof_2 ← Prof_3 ← ( ), V' ← {0}, E' ← ∅
   for b ← 1 to 2 do
      for i ← 1 to m_b do
         if ∃w ∈ V' s.t. V_b^i(G) = w then
            if b = 1 then p ← (w, i) else p ← (w, m_1 + i)
            Prof_1 ← Prof_1 || p
            if (V_b^{i-1}(G), w) ∉ E' then Prof_2 ← Prof_2 || p
            if Cycle_G(V', E', V_b^{i-1}(G), w) = 0 then Prof_3 ← Prof_3 || p
         V' ← V' ∪ {V_b^i(G)}, E' ← E' ∪ {(V_b^{i-1}(G), V_b^i(G))}
   return (Prof_1, Prof_2, Prof_3)
```

```
algorithm Prof2Graph(A)            //A = ((i_1, t_1), ..., (i_a, t_a)) ∈ Prof_2(M_1, M_2)
   V ← {0}, E ← ∅, c ← 1, v_0^1 ← v_0^2 ← ν ← 0
   for b ← 1 to 2 do
      for i ← 1 to m_b do
         if i = t_c then v_i^b ← i_c, c ← c + 1 else ν ← ν + 1, v_i^b ← ν
         E ← E ∪ {(v_{i-1}^b, v_i^b)}, L((v_{i-1}^b, v_i^b)) ← M_b^i
   return G ← ([0..ν], E, L)
```

Fig. 3. The first algorithm above builds the structure graph $G_\pi^{M_1,M_2}$ associated to M_1, M_2 and a permutation $\pi \in \mathrm{Perm}(n)$. The next associates to $G \in \mathcal{G}(M_1, M_2)$ its type-1, type-2 and type-3 collision profiles. The last algorithm constructs a graph from its type-2 collision profile $A \in \mathsf{Prof}_2(M_1, M_2)$.

Structure graphs. To M_1, M_2 and any $\pi \in \mathrm{Perm}(n)$ we associate the *structure graph* $G_\pi^{M_1,M_2}$ output by the procedure Perm2Graph (permutation to graph) of Fig. 3. The structure graph is a directed graph (V, E) together with an edge-labeling function L: $E \to \{M_1^1, \ldots, M_1^{m_1}, M_2^1, \ldots, M_2^{m_2}\}$, where $V = [0..\nu]$ for some $\nu \le m_1 + m_2 + 1$. To get some sense of what is going on here, let

$$C_\pi^{M_1,M_2} = \{\mathrm{CBC}_\pi^{M_1}[i] :\ 0 \le i \le m_1\} \cup \{\mathrm{CBC}_\pi^{M_2}[i] :\ 0 \le i \le m_2\}\ .$$

Note that due to collisions the size of the set $C_\pi^{M_1,M_2}$ could be strictly less than the maximum possible size of $m_1 + m_2 + 1$. The structure graph $G_\pi^{M_1,M_2}$ has vertex set $V = [0..\eta]$ where $\eta = |C_\pi^{M_1,M_2}|$. Associated to a vertex $v \in V$ is a label $\sigma(v) \in C_\pi^{M_1,M_2}$, with $\sigma(0) = 0^n$. (This label is constructed by the code but not part of the final graph.) An edge from a to b with label x exists in the structure graph iff $\pi(\sigma(a) \oplus x) = \sigma(b)$.

Let $\mathcal{G}(M_1, M_2) = \{G_\pi^{M_1,M_2} : \pi \in \mathrm{Perm}(n)\}$ denote the set of all structure graphs associated to messages M_1, M_2. This set has the probability distribution induced by picking π at random from $\mathrm{Perm}(n)$.

We associate to $G = (V, E, L) \in \mathcal{G}(M_1, M_2)$ sequences $V_b^0, \ldots, V_b^{m_b} \in V$ that for $b = 1, 2$ are defined inductively as follows: set $V_b^0 = 0$ and for $i \in [1..m_b]$ let V_b^i be the unique vertex $w \in V$ such that there is an edge $(V_b^{i-1}, w) \in E$ with $L(e) = M_b^i$. Note that this defines the following walks in G:

$$\begin{array}{l} 0 = V_1^0 \xrightarrow{\ M_1^1\ } V_1^1 \xrightarrow{\ M_1^2\ } V_1^2 \xrightarrow{\qquad} \cdots \xrightarrow{\qquad} V_1^{m_1} \xrightarrow{\ M_1^{m_1}\ } V_1^{m_1} \quad \text{and} \\ 0 = V_2^0 \xrightarrow{\ M_2^1\ } V_2^1 \xrightarrow{\ M_2^2\ } V_2^2 \xrightarrow{\qquad} \cdots \xrightarrow{\qquad} V_2^{m_2-1} \xrightarrow{\ M_2^{m_2}\ } V_2^{m_2} \,. \end{array}$$

If $G = G_\pi^{M_1,M_2}$ then observe that $\sigma(V_b^i) = \mathrm{CBC}_\pi^{M_1,M_2}[i]$ for $i \in [0..m_b]$ and $b = 1, 2$, where $\sigma(\cdot)$ is the vertex-labeling function defined by $\mathsf{Perm2Graph}(\pi)$. We emphasize that V_b^i depends on G (and thus implicitly on M_1 and M_2), and if we want to make the dependence explicit we will write $V_b^i(G)$.

Collisions. We use the following notation for sequences. If $s = (s_1, \ldots, s_k)$ is a sequence then $|s| = k$; $y \in s$ iff $y = s_i$ for some $i \in [1..k]$; $s \,\|\, x = (s_1, \ldots, s_k, x)$; and $(\,)$ denotes the empty sequence. For $G = (V, E) \in \mathcal{G}$, $E' \subseteq E$, $V' \subseteq V$ and $a, b \in V$ we define $\mathrm{Cycle}_G(V', E', a, b) = 1$ if adding edge (a, b) to graph $G' = (V', E')$ closes a cycle of length at least four with directions of edges on the cycle alternating. Formally, $\mathrm{Cycle}_G(V', E', a, b) = 1$ iff there exists $k \geq 2$ and vertices $a = v_1, v_2, \ldots, v_{2k-1}, v_{2k} = b \in V'$ such that $(v_{2i-1}, v_{2i}) \in E'$ for all $i \in [1..k]$, $(v_{2i+1}, v_{2i}) \in E'$ for all $i \in [1..k-1]$, and $(b, a) \in E$. To a graph $G \in \mathcal{G}$ we associate sequences $\mathsf{Prof}_1(G), \mathsf{Prof}_2(G), \mathsf{Prof}_3(G)$ called, respectively, the type-1, type-2 and type-3 collision profiles of G. They are returned by the algorithm $\mathsf{Graph2Profs}$ (graph to collision profiles) of Fig. 3 that refers to the predicate Cycle_G we have just defined. We say that G has a type-a (i, t)-collision ($a \in \{1, 2, 3\}$) if $(i, t) \in \mathsf{Prof}_a(G)$. Type-3 collisions are also called *accidents*, and type-1 collisions that are not accidents are called *induced collisions*. We let $\mathsf{col}_i(G) = |\mathsf{Prof}_i(G)|$ for $i = 1, 2, 3$.

Lemma 5. *Let $n \geq 1$, $M_1 \in B_n^{m_1}, M_2 \in B_n^{m_2}$, $\ell = \max(m_1, m_2)$. Let $H \in \mathcal{G}(M_1, M_2)$ be a structure graph. Then*

$$\Pr[G \stackrel{\$}{\leftarrow} \mathcal{G}(M_1, M_2) : \; G = H] \;\leq\; \frac{1}{(2^n - m - m')^{\mathsf{col}_3(H)}} \;\leq\; \frac{1}{(2^n - 2\ell)^{\mathsf{col}_3(H)}} \,. \;\blacksquare$$

The lemma builds on an unpublished technique from [8, 9]. A proof is given in [3]. For $i = 1, 2, 3$ let $\mathsf{Prof}_i(M_1, M_2) = \{\mathsf{Prof}_i(G) : G \in \mathcal{G}(M_1, M_2)\}$. Note that if $A = ((w_1, t_1), \ldots, (w_a, t_a)) \in \mathsf{Prof}_2(M_1, M_2)$ then $1 \leq t_1 < \cdots < t_a \leq m_1 + m_2$ and $w_i < t_i$ for all $i \in [1..a]$. Algorithm $\mathsf{Prof2Graph}$ (collision profile to graph) of Fig. 3 associates to $A \in \mathsf{Prof}_2(M_1, M_2)$ a graph in a natural way. We leave the reader to verify the following:

Lemma 6. $\mathsf{Prof2Graph}(\mathsf{Prof}_2(G)) = G$ *for any $G \in \mathcal{G}(M_1, M_2)$.* $\blacksquare$

This means that the type-2 collision profile of a graph determines it uniquely. Now for $i = 1, 2, 3$ and an integer $a \geq 0$ we let $\mathcal{G}_i^a(M_1, M_2) = \{G \in \mathcal{G}(M_1, M_2) : \mathsf{col}_i(G) = a\}$ and $\mathsf{Prof}_i^a(M_1, M_2) = \{A \in \mathsf{Prof}_i(M_1, M_2) : |A| = a\}$

Lemma 7. *Let $n \geq 1$, $M_1 \in B_n^{m_1}, M_2 \in B_n^{m_2}$, $\ell = \max(m_1, m_2)$, and assume $\ell^2 \leq 2^{n-2}$. Then*

$$\Pr[G \stackrel{\$}{\leftarrow} \mathcal{G}(M_1, M_2) : \mathsf{col}_3(G) \geq 2] \leq \frac{8\ell^4}{2^{2n}} . \quad \blacksquare$$

Proof. By Lemma 5

$$\begin{aligned}
&\Pr[G \stackrel{\$}{\leftarrow} \mathcal{G}(M_1, M_2) : \mathsf{col}_3(G) \geq 2] \\
&= \sum_{a=2}^{\ell} \sum_{H \in \mathcal{G}_3^a(M_1, M_2)} \Pr[G \stackrel{\$}{\leftarrow} \mathcal{G}(M_1, M_2) : G = H] \\
&\leq \sum_{a=2}^{\ell} \frac{|\mathcal{G}_3^a(M_1, M_2)|}{(2^n - 2\ell)^a} .
\end{aligned}$$

Since every type-3 collision is a type-2 collision, $|\mathcal{G}_3^a(M_1, M_2)| \leq |\mathcal{G}_2^a(M_1, M_2)|$. By Proposition 6, $|\mathcal{G}_2^a(M_1, M_2)| = |\mathsf{Prof}_2^a(M_1, M_2)|$. Now $|\mathsf{Prof}_2^a(M_1, M_2)| \leq (\ell(\ell+1)/2)^a \leq \ell^{2a}$, so we have

$$\sum_{a=2}^{\ell} \frac{|\mathcal{G}_3^a(M_1, M_2)|}{(2^n - 2\ell)^a} \leq \sum_{a=2}^{\ell} \frac{\ell^{2a}}{(2^n - 2\ell)^a} .$$

Let $x = \ell^2/(2^n - 2\ell)$, and observe that the assumption $\ell^2 \leq 2^{n-2}$ made in the lemma statement implies that $x \leq 1/2$. Thus the above is

$$\sum_{a=2}^{\ell} x^a = x^2 \cdot \sum_{a=0}^{\ell-2} x^a \leq x^2 \cdot \sum_{a=0}^{\infty} x^a \leq 2x^2 = \frac{2\ell^4}{(2^n - 2\ell)^2} \leq \frac{8\ell^4}{2^{2n}} ,$$

where the last inequality used the fact that $\ell \leq 2^{n-2}$. $\blacksquare$

Let P denote a predicate on graphs. Then $\phi_{M_1,M_2}[P]$ will denote the set of all $G \in \mathcal{G}_3^1(M_1, M_2)$ such that G satisfies P. (That is, it is the set of structure graphs G having exactly one type-3 collision and satisfying the predicate.) For example, predicate P might be $V_1^{m_1}(\cdot) = V_2^{m_2}(\cdot)$ and in that case $\phi_{M_1,M_2}[V_1^{m_1} = V_2^{m_2}]$ is $\{G \in \mathcal{G}_3^1(M_1, M_2) : V_1^{m_1}(G) = V_2^{m_2}(G)\}$.

Note that if G has exactly one accident then $\mathsf{Prof}_2(G) = \mathsf{Prof}_3(G)$, meaning the accident was both a type-2 and a type-3 collision. We will use this below. In this case when we talk of an (i, t)-accident, we mean a type-2 (i, t)-collision.

Finally, let $\mathsf{in}_G(v)$ denote the in-degree of a vertex v in a structure graph G.

7 Bounding $\mathbf{CP}^{\mathsf{any}}_{n,m}$ (Proof of Lemma 4)

In this section we prove Lemma 4, showing that $\mathbf{CP}^{\mathsf{any}}_{n,\ell} \le 2d'(\ell)/2^n + 8\ell^4/2^{2n}$ for any n, ℓ with $\ell^2 \le 2^{n-2}$, thereby proving Lemma 4.

Lemma 8. *Let $n \ge 1$ and $1 \le m_1, m_2 \le \ell$. Let $M_1 \in B_n^{m_1}$ and $M_2 \in B_n^{m_2}$ be distinct messages and assume $\ell^2 \le 2^{n-2}$. Then*

$$\mathbf{CP}^{\mathsf{any}}_{n,\ell}(M_1, M_2) \le \frac{2 \cdot |\phi_{M_1,M_2}[V_1^{m_1} = V_2^{m_2}]|}{2^n} + \frac{8\ell^4}{2^{2n}} \ . \ \blacksquare$$

Proof. With the probability over $G \xleftarrow{\$} \mathcal{G}(M_1, M_2)$, we have:

$$\begin{aligned}
&\mathbf{CP}_n(M_1, M_2) \\
&\quad = \Pr[\, V_1^{m_1} = V_2^{m_2} \,] \\
&\quad = \Pr[\, V_1^{m_1} = V_2^{m_2} \wedge \mathsf{col}_3(G) = 1 \,] + \Pr[\, V_1^{m_1} = V_2^{m_2} \wedge \mathsf{col}_3(G) \ge 2 \,] && (4) \\
&\quad \le \frac{|\phi_{M_1,M_2}[V_1^{m_1} = V_2^{m_2}]|}{2^n - 2\ell} + \frac{8\ell^4}{2^{2n}} && (5) \\
&\quad \le \frac{2 \cdot |\phi_{M_1,M_2}[V_1^{m_1} = V_2^{m_2}]|}{2^n} + \frac{8\ell^4}{2^{2n}} \ . && (6)
\end{aligned}$$

In (4) above we used that $\Pr[\, V_1^{m_1} = V_2^{m_2} \wedge \mathsf{col}_3(G) = 0 \,] = 0$ as $V_1^{m_1} = V_2^{m_2}$ with $M_1 \ne M_2$ implies that there is at least one accident. In (5) we first used Lemma 5, and then used Lemma 7. In (6) we used the fact that $\ell \le 2^{n-2}$, which follows from the assumption $\ell^2 \le 2^{n-2}$. $\blacksquare$

Next we bound the size of the set that arises above:

Lemma 9. *Let $n, \ell \ge 1$ and $1 \le m_2 \le m_1 \le \ell$. Let $M_1 \in B_n^{m_1}$ and $M_2 \in B_n^{m_2}$ be distinct messages. Then*

$$|\phi_{M_1,M_2}[V_1^{m_1} = V_2^{m_2}]| \le d'(\ell) \ . \quad \blacksquare$$

Putting together Lemmas 8 and 9 completes the proof of Lemma 4.

Proof (Lemma 9). Let $k \ge 0$ be the largest integer such that M_1, M_2 have a common suffix of k blocks. Note that $V_1^{m_1} = V_2^{m_2}$ iff $V_1^{m_1-k} = V_2^{m_2-k}$. Thus, we may consider M_1 to be replaced by $M_1^{1\to m_1-k}$ and M_2 to be replaced by $M_2^{1\to m_2-k}$, with m_1, m_2 correspondingly replaced by $m_1 - k, m_2 - k$ respectively. We now have distinct messages M_1, M_2 of at most ℓ blocks each such that either $m_2 = 0$ or $M_1^{m_1} \ne M_2^{m_2}$. (Note that now m_2 could be 0, which was not true before our transformation.) Now consider three cases. The first is that $m_2 \ge 1$ and M_2 is a prefix of M_1. This case is covered by Lemma 10. (Note in this case it must be that $m_1 > m_2$ since M_1, M_2 are distinct and their last blocks are different.) The second case is that $m_2 = 0$ and is covered by Lemma 11. (In this case, $m_1 \ge 1$ since M_1, M_2 are distinct.) The third case is that $m_2 \ge 1$ and M_2 is not a prefix of M_1. This case is covered by Lemma 12. $\blacksquare$

Lemma 10. *Let $n \geq 1$ and $1 \leq m_2 < m_1 \leq \ell$. Let $M_1 \in B_n^{m_1}, M_2 \in B_n^{m_2}$. Assume M_2 is a prefix of M_1 and $M_1^{m_1} \neq M_2^{m_2}$. Then $|\phi_{M_1,M_2}[V_1^{m_1} = V_2^{m_2}]| \leq d'(\ell)$.* ▮

Proof. Because M_2 is a prefix of M_1 we have that $V_2^{m_2} = V_1^{m_2}$, and thus $|\phi_{M_1,M_2}[V_1^{m_1} = V_2^{m_2}]| = |\phi_{M_1,M_2}[V_1^{m_2} = V_1^{m_1}]|$. We now bound the latter.

Let $G \in \mathcal{G}_3^1(M_1, M_2)$. Then $V_1^{m_1}(G) = V_1^{m_2}(G)$ iff $\exists t \geq m_2$ such that G has a type-2 $(t, V_1^{m_2}(G))$-collision. (This is also a type-3 $(V_1^{m_2}(G), t)$-collision since G has exactly one accident.) To see this note that since there was at most one accident, we have $\mathsf{in}_G(V_1^i(G)) \leq 1$ for all $i \in [1..m_1]$ except one, namely the i such that $V_1^i(G)$ was hit by the accident. And it must be that $i = m_2$ since $V_1^{m_2}(G)$ has in-going edges labeled $M_1^{m_2}$ and $M_1^{m_1}$, and these edges cannot be the same as $M_1^{m_1} \neq M_1^{m_2}$.

Let $c \geq 1$ be the smallest integer such that $V_1^{m_2+c}(G) = V_1^{m_2}(G)$. That is, we have a cycle $V_1^{m_2}(G), V_1^{m_2+1}(G), \ldots, V_1^{m_2+c}(G) = V_1^{m_2}(G)$. Now, given that there is only one accident and $V_1^{m_2}(G) = V_1^{m_1}(G)$, it must be that $m_1 = m_2 + kc$ for some integer $k \geq 1$. (That is, starting from $V_1^{m_2}(G)$, one traverses the cycle k times before reaching $V_1^{m_1}(G) = V_1^{m_2}(G)$.) This means that c must divide $m_1 - m_2$. But $|\phi_{M_1,M_2}[V_1^{m_2} = V_1^{m_1}]|$ is at most the number of possible values of c, since this value uniquely determines the graph. So $|\phi_{M_1,M_2}[V_1^{m_2} = V_1^{m_1}]| \leq d(m_1 - m_2)$, where $d(s)$ is the number of positive integers $i \leq s$ such that i divides s. But $d(m_1 - m_2) \leq d'(\ell)$ by definition of the latter. ▮

Lemma 11. *Let $n \geq 1$ and $1 \leq m_1 \leq \ell$. Let $M_1 \in B_n^{m_1}$, let $M_2 = \varepsilon$ and let $m_2 = 0$. Then $|\phi_{M_1,M_2}[V_1^{m_1} = V_2^{m_2}]| \leq d'(\ell)$.* ▮

Proof. Use an argument similar to that of Lemma 10, noting that $V_{m_1}^0(G) = V_1^0(G)$ implies that $\mathsf{in}_G(V_1^0(G)) \geq 1$. ▮

Lemma 12. *Let $n \geq 1$ and $1 \leq m_2 \leq m_1 \leq \ell$. Let $M_1 \in B_n^{m_1}, M_2 \in B_n^{m_2}$. Assume M_2 is not a prefix of M_1 and $M_1^{m_1} \neq M_2^{m_2}$. Then $|\phi_{M_1,M_2}[V_1^{m_1} = V_2^{m_2}]| \leq 1$.* ▮

Proof. Let $p \in [0..m_2 - 1]$ be the largest integer such that $M_1^{1\to i} = M_2^{1\to i}$ for all $i \in [1..p]$. Then $V_1^i = V_2^i$ for $i \in [1..p]$ and $V_1^{p+1} \neq V_2^{p+1}$. Now to have $V_1^{m_1} = V_2^{m_2}$ we need an accident. Since $M_1^{m_1} \neq M_2^{m_2}$ and there is only one accident, the only possibility is that this is a $(V_1^{m_1}, m_1 + m_2)$-collision. Thus, there is only one way to draw the graph. ▮

8 Bounding $\mathbf{FCP}_{n,\ell}^{\mathsf{pf}}$ (Proof of Lemma 2)

In this section we show that $\mathbf{FCP}_{n,\ell}^{\mathsf{pf}} \leq 8\ell/2^n + 8\ell^4/2^{2n}$ for any n, ℓ with $\ell^2 \leq 2^{n-2}$, thereby proving Lemma 2. Recall that $\mathsf{pf}(M_1, M_2) = \mathsf{false}$ iff M_1 is not a prefix of M_2 and M_2 is not a prefix of M_1. The proof of the following is similar to the proof of Lemma 8 and is omitted.

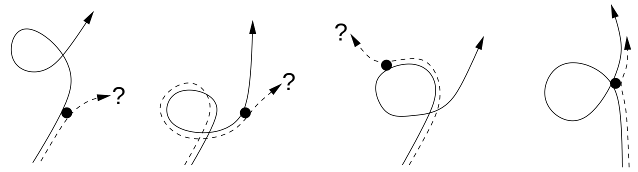

Fig. 4. Some shapes where the M_1-path (solid line) makes a loop. In the first three cases the M_1-path passes only once through V_1^p (the dot), and we see that we cannot draw the M_2-path such that $V_2^{m_2} \in \{V_1^{p+1}, \ldots, V_1^{m_1}\}$ without a second accident in any of those cases. In the last graph $V_2^{m_2} \in \{V_1^{p+1}, \ldots, V_1^{m_1}\}$, but there also $V_1^p \in \{V_1^0, \ldots, V_1^{p-1}, V_1^{p+1}, \ldots, V_1^{m_1}\}$.

Lemma 13. *Let $n \geq 1$ and $1 \leq m_1, m_2 \leq \ell$. Let $M_1 \in B_n^{m_1}, M_2 \in B_n^{m_2}$ with $\mathsf{pf}(M_1, M_2) = \mathsf{false}$. Assume $\ell^2 \leq 2^{n-2}$. Then*

$$\mathbf{FCP}^{\mathsf{pf}}_{n,\ell}(M_1, M_2) \leq \frac{2 \cdot \left|\phi_{M_1,M_2}[V_2^{m_2} \in \{V_1^1, \ldots, V_1^{m_1}, V_2^1, \ldots, V_2^{m_2-1}\}]\right|}{2^n} + \frac{8\ell^4}{2^{2n}} . \blacksquare$$

Next we bound the size of the set that arises above:

Lemma 14. *Let $n, \ell \geq 1$ and $1 \leq m_1, m_2 \leq \ell$. Let $M_1 \in B_n^{m_1}, M_2 \in B_n^{m_2}$ with $\mathsf{pf}(M_1, M_2) = \mathsf{false}$. Then*

$$\left|\phi_{M_1,M_2}[V_2^{m_2} \in \{V_1^1, \ldots, V_1^{m_1}, V_2^1, \ldots, V_2^{m_2-1}\}]\right| \leq 4\ell . \quad \blacksquare$$

Putting together Lemmas 13 and 14 completes the proof of Lemma 2.

We denote by $\mathsf{cpl}(M_1, M_2)$ the number of blocks in the longest common block-prefix of M_1, M_2. That is, $\mathsf{cpl}(M_1, M_2)$ is the largest integer p such that $M_1^i = M_2^i$ for all $i \in [1..p]$. Define the predicate $\mathsf{NoLoop}(G)$ to be true for structure graph $G \in \mathcal{G}_2^1(M_1, M_2)$ iff $V_1^0(G), \ldots, V_1^{m_1}(G)$ are all distinct and also $V_2^0(G), \ldots, V_2^{m_2}(G)$ are all distinct. Let Loop be the negation of NoLoop.

Proof (Lemma 14). Let $p = \mathsf{cpl}(M_1, M_2)$. Since $\mathsf{pf}(M_1, M_2) = \mathsf{false}$, it must be that $p < m_1, m_2$ and $M_1^{p+1} \neq M_2^{p+1}$. Note then that $V_1^i = V_2^i$ for all $i \in [0..p]$ but $V_1^{p+1} \neq V_2^{p+1}$. Now we break up the set in which we are interested as

$$\begin{aligned} &\phi_{M_1,M_2}[V_2^{m_2} \in \{V_1^1, \ldots, V_1^{m_1}, V_2^1, \ldots, V_2^{m_2-1}\}] \\ &\quad = \phi_{M_1,M_2}[V_2^{m_2} \in \{V_2^1, \ldots, V_2^{m_2-1}\}] \cup \phi_{M_1,M_2}[V_2^{m_2} \in \{V_1^{p+1}, \ldots, V_1^{m_1}\}] . \end{aligned}$$

Lemma 15 implies that $|\phi_{M_1,M_2}[V_2^{m_2} \in \{V_2^1, \ldots, V_2^{m_2-1}\}]| \leq m_2$ and Lemma 17 says that $|\phi_{M_1,M_2}[V_2^{m_2} \in \{V_1^{p+1}, \ldots, V_1^{m_1}\} \wedge \mathsf{NoLoop}]| \leq m_1$. It remains to bound $|\phi_{M_1,M_2}[V_2^{m_2} \in \{V_1^{p+1}, \ldots, V_1^{m_1}\} \wedge \mathsf{Loop}]|$. We use a case analysis, which is illustrated in Fig. 4. The condition Loop means that either the M_1- or the M_2-path (or both) must make a loop. If the M_1-path makes a loop then we can only draw the M_2-path such that $V_2^{m_2} \in \{V_1^{p+1}, \ldots, V_1^{m_1}\}$ if the loop goes twice through V_1^p. The same argument works if only the M_2-path makes a loop. Thus

$$\phi_{M_1,M_2}[V_2^{m_2} \in \{V_1^{p+1}, \ldots, V_1^{m_1}\} \wedge \mathsf{Loop}] \subseteq \mathcal{S}_1 \cup \mathcal{S}_2$$

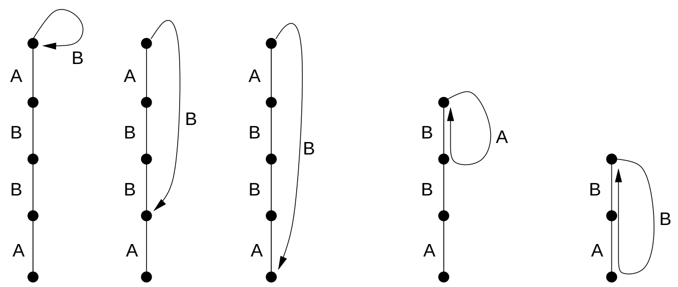

Fig. 5. An example for the proof of Lemma 15 with $m_1 = 5$ and $M_1 = A\|B\|B\|A\|B$ for distinct $A, B \in \{0,1\}^n$. Here we have $N_5 = 5 - \mu_1(M_1^5) + 1 = 5 - \mu_1(B) + 1 = 5 - 3 + 1 = 3$ and $N_4 = \mu_1(M_1^5) - \mu_1(M_1^{4\to 5}) = \mu_1(B) - \mu_1(A\|B) = 3 - 2 = 1$ and $N_3 = \mu_1(M_1^{4\to 5}) - \mu_1(M_1^{3\to 5}) = \mu_1(A\|B) - \mu_1(B\|A\|B) = 2 - 1 = 1$ and $N_2 = N_1 = 0$. The first three graphs show the N_5 cases, the fourth and the fifth graph show the single cases for N_4 and N_3.

where

$$\mathcal{S}_1 = \phi_{M_1,M_2}[V_1^p \in \{V_1^0, \ldots, V_1^{p-1}, V_1^{p+1}, \ldots, V_1^{m_1}\}]$$
$$\mathcal{S}_2 = \phi_{M_1,M_2}[V_2^p \in \{V_2^0, \ldots, V_2^{p-1}, V_2^{p+1}, \ldots, V_2^{m_2}\}] \,.$$

Lemma 16 says that $|\mathcal{S}_1| \le m_1$ and $|\mathcal{S}_2| \le m_2$. Putting everything together, the lemma follows as $2(m_1 + m_2) \le 4\ell$. ▮

Lemma 15. *Let $n, m_1, m_2 \ge 1$. Let $M_1 \in B_n^{m_1}, M_2 \in B_n^{m_2}$ with* $\mathsf{pf}(M_1, M_2) =$ false*. Then for $b \in \{1, 2\}$,*

$$\left|\phi_{M_1,M_2}[V_b^{m_b} \in V_b^0, V_b^1, \ldots, V_b^{m_b-1}\}]\right| = m_b \qquad ▮$$

Proof. We prove the claim for $b = 1$ and then briefly discuss how to extend the proof to $b = 2$. If $V_1^{m_1} \in \{V_1^0, \ldots, V_1^{m_1-1}\}$ then there must be a (V_1^i, j)-accident for some $i \in [0..m_1 - 1]$ and $j \in [i + 1..m_1]$ and then induced collisions in steps $j + 1$ to m_1. Thus $V_1^{j+k} = V_1^{i+k}$ for all $k \in [0..m_1 - j]$. For $j \in [1..m_1]$ let N_j be the number of structure graphs $G \in \mathcal{G}_2^1(M_1, M_2)$ such that $V_1^{m_1}(G) \in \{V_1^0(G), \ldots, V_1^{m_1-1}(G)\}$ and there is a $(V_1^i(G), j)$-accident for some $i \in [0..j-1]$. Then

$$\left|\phi_{M_1,M_2}[V_1^{m_1} \in \{V_1^0, \ldots, V_1^{m_1-1}\}]\right| = \sum_{j=1}^{m_1} N_j \,.$$

Let $\mu_1(S)$ denote the number of block-aligned occurrences of the substring S in M_1. (For example, $\mu_1(A \,\|\, B) = 2$ if $M_1 = A \,\|\, B \,\|\, B \,\|\, \| \, A \,\|\, B$ for some distinct $A, B \in \{0,1\}^n$.) It is possible to have a (V_1^i, m_1)-accident for any $i \in [0..m_1 - 1]$ for which $M_1^i \ne M_1^{m_1}$ (cf. Fig. 5) and thus $N_{m_1} = m_1 - \mu_1(M_1^{m_1}) + 1$. It is possible to have a $(V_1^i, m_1 - 1)$-accident and also have $V_1^{m_1} \in \{V_1^0, \ldots, V_1^{m_1-1}\}$ for any $i \in [0..m_1 - 2]$ for which $M_1^i \ne M_1^{m_1-1}$ and $M_1^{i+1} = M_1^{m_1}$ and thus

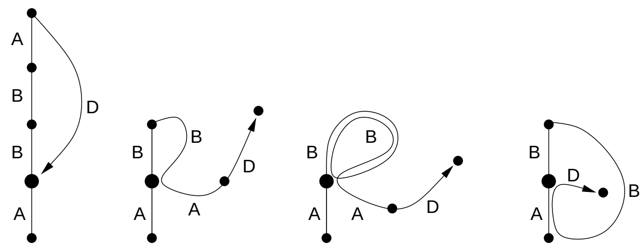

Fig. 6. An example for the proof of Lemma 16 with $m_1 = 5, M_1 = A\|B\|B\|A\|D$ and $r = 1$, where $A, B, D \in \{0,1\}^n$ are distinct. (The large dot is $V_1^r = V_1^1$.) Here we have $N_r = m - r = \mu_2(M_1^1) = N_1 = m_1 - 1 - \mu_2(M_1^1) = 5 - 1 - \mu_2(A) = 5 - 1 - 1 = 3$. Those cases correspond to the first three graphs in the figure. The fourth graph corresponds to $N_{r-1} = N_0 = \mu_2(\star \,\|\, M_1^{1\to r}) = \mu_2(\star \,\|\, A) = 1$.

$N_{m_1-1} = \mu_1(M_1^{m_1}) - \mu_1(M_1^{m_1-1\to m_1})$. In general for $j \in [1..m_1 - 1]$ we have $N_j = \mu_1(M_1^{j+1\to m_1}) - \mu_1(M_1^{j\to m_1})$. Using cancellation of terms in the sum we have

$$\sum_{j=1}^{m_1} N_j = m_1 + 1 - \mu_1(M_1^{1\to m_1}) = m_1$$

which proves the lemma for the case $b = 1$. For $b = 2$ we note that we can effectively ignore the part of the graph related to M since it must be a straight line, and thus the above counting applies again with the (V_1^i, j)-accident now being a $(V_2^i, m_1 + j)$-accident and M_1, m_1 replaced by M_2, m_2 respectively. ∎

Next we have a generalization of Lemma 15.

Lemma 16. *Let $n, m_1, m_2 \geq 1$. Let $M_1 \in B_n^{m_1}, M_2 \in B_n^{m_2}$ with $\mathsf{pf}(M_1, M_2) =$ false. Then for $b \in \{1,2\}$ and any $r \in [0..m_b]$,*

$$\left|\phi_{M_1,M_2}[V_b^r \in \{V_b^0, \ldots, V_b^{r-1}, V_b^{r+1}, \ldots, V_b^{m_b}\}]\right| \leq m_b \,. \quad ∎$$

Proof. We prove it for the case $b = 1$. (The case $b = 2$ is analogous.) By Lemma 15 we have $|\phi_{M_1,M_2}[V_1^r \in \{V_1^0, \ldots, V_1^{r-1}\})| = r$. It remains to show that

$$\left|\phi_{M_1,M_2}[V_1^r \in \{V_1^{r+1}, \ldots, V_1^{m_1}\} \wedge V_1^r \notin \{V_1^0, \ldots, V_1^r\}]\right| \leq m_1 - r \,.$$

We may assume that $V_1^i \neq V_1^j$ for all $0 \leq i < j \leq r - 1$, as otherwise we have already used up our accident and there's no way to get $V_1^r \in \{V_1^{r+1}, \ldots, V_1^{m_1}\}$ any more. If $V_r^{\in}\{V_1^{r+1}, \ldots, V_1^{m_1}\}$ then there is a (V_1^j, i)-accident for some $0 \leq j \leq r < i$. For $j \in [0..r]$ let N_j be the number of structure graphs $G \in \mathcal{G}_2^1(M_1, M_2)$ such that $V_1^r(G) \in \{V_1^{r+1}(G), \ldots, V_1^{m_1}(G)\}$, $V_1^r(G) \notin \{V_1^0(G), \ldots, V_1^r(G)\}$ and there is a (V_1^j, i)-accident for some $i \in [r + 1..m_1]$. Then

$$\left|\phi_{M_1,M_2}[V_1^r \in \{V_1^{r+1}, \ldots, V_1^{m_1}\} \wedge V_1^r \notin \{V_1^0, \ldots, V_1^r\}]\right| = \sum_{j=0}^{r} N_j \,.$$

Let $\mu_2(S)$ be the number of block-aligned occurrences of the substring S in $M_1^{r+1\to m_1}$, and adopt the convention that $\mu_2(M_1^0)=0$. Since we can only have an (V_1^r,j)-accident when $M_1^j \neq M_1^r$ we have $N_r = m-r-\mu_2(M_1^r)$. For $i>r$, a (V_1^r,i)-accident is possible and will result in $V_1^r \in \{V_1^{r+1},\ldots,V_1^{m_1}\}$ only if $M_1^{i\to i+1} = X\|M_r$ for some $X \neq M_1^{r-1}$. Now with $\star$ being a wildcard standing for an arbitrary block we have $N_{r-1} = \mu_2(\star \parallel M_1^r) - \mu_2(M_1^{r-1\to r})$. In general, for $j\in[1..r-1]$ we have $N_j = \mu_2(\star \parallel M_1^{j+1\to r}) - \mu_2(M_1^{j\to r})$ and $N_0 = \mu_2(\star \parallel M_1^{1\to r})$. Now, as $\mu_2(\star \parallel S) \le \mu_2(S)$ for any S, we get

$$\sum_{j=0}^{r} N_j \le m_1 - r \ . \qquad \blacksquare$$

The proof of the following is in [3].

Lemma 17. *Let $n,m_1,m_2 \geq 1$. Let $M_1 \in B_n^{m_1}$, $M_2 \in B_n^{m_2}$ with* $\mathsf{pf}(M_1,M_2) = \mathsf{false}$. *Let $p=\mathsf{cpl}(M_1,M_2)$. Then*

$$\left|\phi_{M_1,M_2}[V_2^{m_2} \in \{V_1^{p+1},\ldots,V_1^{m_1}\} \wedge \mathsf{NoLoop}]\right| \le m_1 \ . \qquad \blacksquare$$

Acknowledgments

Bart Preneel was the first we heard to ask, back in 1994, if the m^2 term can be improved in the CBC MAC bound of $m^2q^2/2^n$.

Bellare was supported by NSF grants ANR-0129617 and CCR-0208842, and by an IBM Faculty Partnership Development Award. Pietrzak was supported by the Swiss National Science Foundation, project No. 200020-103847/1. Rogaway carried out most of this work while hosted by the Department of Computer Science, Faculty of Science, Chiang Mai University, Thailand. He is currently hosted by the School of Information Technology, Mae Fah Luang University, Thailand. He is supported by NSF grant CCR-0208842 and a gift from Intel Corp.

References

1. M. Bellare, O. Goldreich, and A. Mityagin. The power of verification queries in message authentication and authenticated encryption. Cryptology ePrint Archive: Report 2004/309.
2. M. Bellare, J. Kilian, and P. Rogaway. The security of the cipher block chaining message authentication code. *Journal of Computer and System Sciences* (JCSS), vol. 61, no. 3, pp. 362–399, 2000. Earlier version in *Crypto '94*.
3. M. Bellare, K. Pietrzak, and P. Rogaway. Improved security analyses for CBC MACs. Full version of this paper. Available via authors' web pages.
4. M. Bellare and P. Rogaway. The game-playing technique. Cryptology ePrint Archive: Report 2004/331.
5. A. Berendschot, B. den Boer, J. Boly, A. Bosselaers, J. Brandt, D. Chaum, I. Damgård, M. Dichtl, W. Fumy, M. van der Ham, C. Jansen, P. Landrock, B. Preneel, G. Roelofsen, P. de Rooij, and J. Vandewalle. *Final Report of Race Integrity Primitives*. Lecture Notes in Computer Science, vol. 1007, Springer-Verlag, 1995

6. R. Berke. On the security of iterated MACs. Diploma Thesis, ETH Zürich, August 2003.
7. J. Black and P. Rogaway. CBC MACs for arbitrary-length messages: the three-key constructions. *Advances in Cryptology – CRYPTO '00*, Lecture Notes in Computer Science Vol. 1880, M. Bellare ed., Springer-Verlag, 2000.
8. Y. Dodis. Personal communication to K. Pietrzak. 2004.
9. Y. Dodis, R. Gennaro, J. Håstad, H. Krawczyk, and T. Rabin. Randomness extraction and key derivation using the CBC, Cascade, and HMAC modes. *Advances in Cryptology – CRYPTO '04*, Lecture Notes in Computer Science Vol. 3152 , M. Franklin ed., Springer-Verlag, 2004.
10. G. Hardy and E. Wright. *An Introduction to the Theory of Numbers*. Oxford University Press, 1980.
11. E. Jaulmes, A. Joux, and F. Valette. On the security of randomized CBC-MAC beyond the birthday paradox limit: a new construction. *Fast Software Encryption '02*, Lecture Notes in Computer Science Vol. 2365 , J. Daemen, V. Rijmen ed., Springer-Verlag, 2002.
12. J. Kilian and P. Rogaway. How to protect DES against exhaustive key search (an analysis of DESX). *Journal of Cryptology*, vol. 14, no. 1, pp. 17–35, 2001. Earlier version in *Crypto '96*.
13. U. Maurer. Indistinguishability of random systems. *Advances in Cryptology – EUROCRYPT '02*, Lecture Notes in Computer Science Vol. 2332, L. Knudsen ed., Springer-Verlag, 2002.
14. National Institute of Standards and Technology, U.S. Department of Commerce, M Dworkin, author. Recommendation for block cipher modes of operation: the CMAC mode for authentication. NIST Special Publication 800-38B, May 2005.
15. E. Petrank and C. Rackoff. CBC MAC for real-time data sources. *Journal of Cryptology*, vol. 13, no. 3, pp. 315–338, 2000.
16. V. Shoup. Sequences of games: a tool for taming complexity in security proofs. Cryptology ePrint report 2004/332, 2004.
17. S. Vaudenay. Decorrelation over infinite domains: the encrypted CBC-MAC case. *Communications in Information and Systems* (CIS), vol. 1, pp. 75–85, 2001.
18. M. Wegman and L. Carter. New classes and applications of hash functions. *Symposium on Foundations of Computer Science* (FOCS), pp. 175–182, 1979.