On the Security of Cipher Block Chaining Message Authentication Code[⋆]

Charles Rackoff and Serge Gorbunov

Dept. of Computer Science
University of Toronto,
Toronto, Ontario, Canada M5S 3G4
rackoff@cs.toronto.edu, serge.gorbunov@utoronto.ca

Abstract. In [4], Bernstein presented a simple proof of security of Cipher Block Chaining (CBC) Message Authentication Code (MAC) against adversaries querying messages all of which are of the same length. In this paper we show that Bernstein's proof can be used to prove security of CBC MAC against adversaries querying non-empty messages that are not prefixes of each other. This implies that "length-prepend CBC MAC" presented by Bellare, Kilian, and Rogaway in [1] is a secure authentication method, handling variable message lengths.

1 Introduction

CBC MAC is an authentication standard widely used in practice. Two parties, sharing a secret key α, can authenticate a message $x = (x_1, x_2, ..., x_m)$ by adding the following tag to the message:

$$f'_\alpha(x) = f_\alpha(f_\alpha(\ldots f_\alpha(f_\alpha(x_1) \oplus x_2) \oplus \ldots \oplus x_{m-1}) \oplus x_m) \tag{1}$$

The underlying function $f_\alpha : \{0,1\}^n \rightarrow \{0,1\}^n$ can be based on any preudo-random function generator for a fixed length. Bellare, Kilian, and Rogaway were first to prove the security of the standard CBC MAC applied on messages of fixed length [1]. In particular, they showed that the advantage of any k-query adversary at distinguishing between CBC MAC, that uses a randomly chosen underlying function $f : \{0,1\}^n \rightarrow \{0,1\}^n$, and a randomly chosen function outputting n bits is $m^2k^2/2^n$, where m is the number of blocks in each query. In [4], Bernstein achieved the same results, providing a simpler proof.

It is well known that the standard CBC MAC is only secure against adversaries querying messages all of which are of the same length and it is not secure against adversaries querying messages of different lengths. Bellare, Kilian and Rogaway proposed in [1] to encode each message by appending to it its length encoding as the first block and then apply the standard CBC MAC [1]. They called this version of CBC MAC as "length-prepend CBC MAC". It is easy to see that, given a list of distinct messages possibly of different lengths, once this encoding it applied, no message can be a prefix of any other message. In [11], Petrank and Rackoff showed that the standard CBC MAC is secure when applied on non-empty messages that are not prefixes of each other by extending the proof provided in [1]. Bellare, Pietrzak and Rogaway improved this results providing stronger bounds [2]. In particular, they showed that the advantage of any k-query adversary, querying non-empty messages that are not prefixes of each other, at distinguishing between CBC MAC, that uses a randomly chosen underlying function $f : \{0,1\}^n \rightarrow \{0,1\}^n$, and a randomly chosen function outputting n bits is $\leq 20mk^2/2^n$ for $m \leq 2^{n/3}$, where m is the number of blocks in the longest query.

In this paper we modify Bernstein's proof [4] to show that the standard CBC MAC is secure against adversaries querying non-empty messages that are not prefixes of each other. As a conclusion of our theorem, any k-query adversary querying non-empty messages that are not prefixes of each other has an advantage of $m^2k^2/2^n$ at distinguishing between CBC MAC, that uses a randomly

[⋆] This work was funded by Natural Sciences and Engineering Research Council of Canada (NSERC).

[1] Some other constructions handling variable message lengths are EMAC [11], XMAC [3], TMAC [6] and OMAC [7].

chosen underlying function $f : \{0,1\}^n \rightarrow \{0,1\}^n$, and a randomly chosen function outputting n bits. This also implies the security of "length-prepend CBC MAC" presented in [1]. Although we prove that CBC is a secure MAC, it is also a preudo-random generator. Bernstein's proof has also been applied by Nandi in [8] to show security of other constructions handling variable inputs such as XMAC [3], TMAC [6], OMAC [7] and PMAC [5]. In [9], he generalized the proof to show the security of a class of CBC MAC algorithms (*gcbc*), which includes "length-prepend CBC MAC". In [10], he achieved better quantitative results ($11tk/2^n$, where t is the total number of blockcipher computations needed for all k queries) on CBC MAC applied on non-empty messages that are not prefixes of each other. However, understanding the security of "length-prepend CBC MAC" based on [9] or [10] requires first understanding of Nandi's general classes of CBC MAC constructions and associated proofs.

2 CBC MAC is secure applied on non-empty messages that are not prefixes of each other

Lemma 1: *Let $G = \{0,1\}^n$. Let F be a family of functions from G to G. Let f be a function chosen randomly from F. Define f' recursively as follows: $f'(\lambda) = 0^n$, where λ is the empty string and $f'(\bar{x}y) = f(f'(\bar{x}) \oplus y)$, where $\bar{x}$ is a string of length divisible by n and y is an n-bit string. Let $k \geq 0$ and $m \geq 1$. Let G' denote the set of all non-empty strings formed by concatenating m or fewer strings from G. Let $y_1, y_2, \ldots, y_k$ be distinct elements of G' such that no y_i is a prefix of y_j for all i, j and $i \neq j$. Let $z_1, z_2, \ldots, z_k$ be elements of G. Then the probability that $(f'(y_1) = z_1, f'(y_2) = z_2, \ldots, f'(y_k) = z_k)$ is at least $\frac{(1-\epsilon)}{|G|^k}$ where $\epsilon = \frac{mk(mk-1)}{2|G|}$.*

Proof of Lemma 1: Define P as the set of non-empty prefixes of $y_1, y_2, \ldots, y_k$ whose length is divisible by n. For all $p \in P$, define $chop(p)$ = everything but the last n-bit block of p, and $last(p)$ = the last n-bit block of p. Define $\varphi : \{\lambda\} \cup P \rightarrow G$ as admissible if:

$C1$. $\varphi(\lambda) = 0^n$.

$C2$. $\varphi(y_i) = z_i$ for all $1 \leq i \leq k$.

$C3$. For all $p, p' \in P$ such that $p \neq p'$, $\varphi(chop(p)) \oplus last(p) \neq \varphi(chop(p')) \oplus last(p')$.

Define an admissible $\varphi : \{\lambda\} \cup P \rightarrow G$ as compatible with $f : G \rightarrow G$ if for all $p \in P$, $f(\varphi(chop(p)) \oplus last(p)) = \varphi(p)$.

The proofs of the next two claims are identical to the proofs presented in Theorem 2.1 of [4] and we leave them to the reader.

Claim 1: For all admissible functions φ, the probability that φ is compatible with a randomly chosen f from F is $\frac{1}{|G|^{|P|}}$.

Claim 2: Let φ be an admissible and a compatible function with $f : G \rightarrow G$, then for all $p \in \{\lambda\} \cup P$, $f'(p) = \varphi(p)$.

Claim 3: There are at least $\frac{(1-\epsilon)|G|^{|P|}}{|G|^k}$ admissible functions where $\epsilon = \frac{mk(mk-1)}{2|G|}$.

Proof of Claim 3: To count the number of admissible functions we look at $\varphi : \{\lambda\} \cup P \rightarrow G$ chosen randomly. $C1$ is satisfied with probability $\frac{1}{|G|}$. $C2$ is satisfied with probability $\frac{1}{|G|^k}$, since all y_i's are distinct. Also, since y_i's are not empty, $C1$ is independent of $C2$ and so the probability that both are satisfied is $\frac{1}{|G|^{k+1}}$.

From now on, assume that $C1$ and $C2$ hold. We now calculate the probability that $C3$ fails. Now, consider $p, p' \in P$ such that $p \neq p'$. We cannot have that $chop(p) = chop(p')$ and $last(p) = last(p')$ since $p \neq p'$. If $chop(p) = chop(p')$ and $last(p) \neq last(p')$, then $\varphi(chop(p)) \oplus last(p) \neq \varphi(chop(p')) \oplus last(p')$. Assume $chop(p) \neq chop(p')$ **(1)**. Then, either $chop(p)$ or $chop(p')$ is not equal to λ. Assume $chop(p) \neq \lambda$ **(2)**. Then, $\varphi(chop(p)) \oplus last(p) = \varphi(chop(p')) \oplus last(p')$ can be rewritten as $\varphi(chop(p)) = \varphi(chop(p')) \oplus last(p') \oplus last(p)$. Now, $chop(p)$ is a proper prefix of one of the messages and no message is a proper prefix of any other. Therefore, $chop(p) \neq y_i$ for all $1 \leq i \leq k$ **(3)**. Therefore, by **(1)**, **(2)** and **(3)** $\varphi(chop(p))$ is chosen randomly and independently. Hence, the probability that $\varphi(chop(p)) = \varphi(chop(p')) \oplus last(p') \oplus last(p)$ is $\frac{1}{|G|}$. Now, since there are at most $\binom{mk}{2}$ such cases in P over all distinct p, p', the probability that $C3$ fails is $\leq \frac{mk(mk-1)}{2|G|} = \epsilon$.

So, the probability that $\varphi : \{\lambda\} \cup P \to G$ is admissible $\geq \frac{(1-\epsilon)}{|G|^{k+1}}$. And since there is a total of $|G|^{|P|+1}$ functions from $\{\lambda\} \cup P$ to G, there are at least $\frac{(1-\epsilon)|G|^{|P|}}{|G|^k}$ admissible functions. This completes the proof of Claim 3.

Since there are at least $\frac{(1-\epsilon)|G|^{|P|}}{|G|^k}$ admissible functions, the probability that one of them is compatible with a randomly chosen f from F is at least $\frac{(1-\epsilon)}{|G|^k}$ where $\epsilon = \frac{mk(mk-1)}{2|G|}$. This completes the proof of Lemma 1.

Finally, we can apply Theorem 3.1 from [4], thus proving that CBC MAC is secure applied on non-empty messages that are not prefixes of each other.

References

1. 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.
2. M. Bellare, K. Pietrzak and P. Rogaway. Improved Security Analysis for CBC MACs. Advances in Cryptology - CRYPTO 2005. Lecture Notes in Computer Science, Volume 3621, pp 527-545.
3. M. Bellare and P. Rogaway. Code-based game-playing proofs and the security of triple encryption. In S. Vaudenay, editor, Advances in Cryptology EUROCRYPT 2006, volume 4004 of Lecture Notes in Computer Science, St.-Petersburg, Russia, May 29 June 1, 2006. Springer-Verlag, Berlin, Germany. Available as Cryptology ePrint Report 2005/334.
4. D. J. Bernstein. A short proof of the unpredictability of cipher block chaining. http://cr.yp.to/antiforgery/easycbc-20050109.pdf, 2005.
5. J. Black and P. Rogaway. A Block-Cipher Mode of Operations for Parallelizable Message Authentication. Advances in Cryptology - Eurocrypt 2002. Lecture Notes in Computer Science, Volume 2332, pp 384-397.
6. K. Kurosawa and T. Iwata. TMAC : Two-Key CBC MAC. Topics in Cryptology - CT-RSA. 2003: The Cryptographers' Track at the RSA Conference 2003. Lecture Notes in Computer Science, Volume 2612, pp 33-49.
7. K. Kurosawa and T. Iwata. OMAC : One-Key CBC MAC. Fast Software Encryption. 10th International Workshop, FSE 2003. Lecture Notes in Computer Science, Volume 2887, pp 129- 153.
8. M. Nandi. A simple and unified method of proving indistinguishability. In Rana Barua and Tanja Lange, editors, Progress in Cryptology INDOCRYPT 2006, volume 4329 of Lecture Notes in Computer Science, pages 317334, Kolkata, India, December 1113, 2006. Springer- Verlag, Berlin, Germany.
9. M. Nandi. Fast and secure CBC-type MAC algorithms. In Orr Dunkelman, editor, FSE, volume 5665 of Lecture Notes in Computer Science, pages 375-393. Springer, 2009.
10. M. Nandi. A Unified Method for Improving PRF Bounds for a Class of Blockcipher based MACs. FSE, volume 6147 of Lecture Notes in Computer Science, pages 212-229. Springer, 2010.
11. E. Petrank and C. Rackoff. CBC MAC for real-time data sources. Journal of Cryptology, vol. 13, no. 3, pp 315-338, 2000.