Comments to NIST concerning AES Modes of Operations:

A Suggestion for Handling Arbitrary-Length Messages with the CBC MAC

John Black
University of Nevada, Reno (USA)
jrb@cs.unr.edu
www.cs.unr.edu/~jrb

Phillip Rogaway
University of California at Davis (USA) and
Chiang Mai University (Thailand)
rogaway@cs.ucdavis.edu
www.cs.ucdavis.edu/~rogaway

1 Introduction

The CBC MAC is the customary way to make a message authentication code (MAC) from a block cipher. It is the subject of several standards, including [1, 5, 6]. It is well-known and well-understood. Given all this, it seems likely that the CBC MAC will be standardized as an AES mode of operation. In this note we suggest a nice version of the CBC MAC that one might select for this purpose.

We recall that the CBC MAC actually comes in a number of different versions. These versions differ in details involving *padding* (what to do when a message is *not* a non-zero multiple of the block length), *length-variability* (how to properly authenticate messages that come in a variety of lengths), and *key-search strengthening* (making the mode more secure against key-search attacks).

Our CBC MAC variant is described in [4], where it is called XCBC. Let us now review this MAC's definition, as well as the definition for the basic CBC MAC.

2 CBC MAC

Let $E_K(X)$ denote the encipherment of an n-bit block X using key K and a block cipher E. For concreteness we assume that $E = \text{AES}$, so $n = 128$. Let $a \oplus b$ denote the bitwise exclusive-or of a and b. Let $a \parallel b$ denote the concatenation of strings a and b and let $|a|$ denote the length, in bits, of a. Let 0^i denote i zero-bits.

Basic CBC MAC. To authenticate with the basic CBC MAC, one starts with a message M whose length is a positive multiple of n, and a key K for E. Let $M_1 \parallel M_2 \parallel \cdots \parallel M_m = M$ with $|M_i| = n$ for $1 \le i \le m$. Then the CBC MAC of M is defined as C_m, where $C_i = E_K(M_i \oplus C_{i-1})$ for $1 \le i \le m$ and $C_0 = 0^n$.

We remind the reader of the well-known fact that the CBC MAC (as just defined) is *insecure* across messages of varying lengths—in fact, it is trivial to produce forgeries for some second message given the MAC of some first message. (On the other hand, the basic CBC MAC is demonstrably secure across messages of some one fixed length [2], while minor variants of the CBC MAC are provably secure across messages of varying lengths [8, 4].)

Extending the Domain. To extend the domain of the CBC MAC to include messages of arbitrary bit length, and to obtain security across varying bit lengths, we start with a message $M \in \{0,1\}^*$ and three keys, $K1$, $K2$, and $K3$. The key $K1$ is of the desired length for E, while $K2$ and $K3$ are n-bit strings. Let $m = \max\{1, \lceil |M|/n \rceil\}$ and write M as $M = M_1 \parallel M_2 \parallel \cdots \parallel M_m$, where $|M_i| = n$ for $1 \le i < m$. We then compute the MAC as follows. When $|M|$ is a positive multiple of n, modify the last block of M by XORing in the key $K2$, and then compute the basic CBC MAC under key $K1$, When $|M| = 0$ or $|M|$ is not divisible by n, pad M by appending a single 1 bit followed by the minimum number of 0 bits needed to bring $|M|$ up to the next multiple of n, then modify the last block by XORing in the key $K3$, and then compute the basic CBC MAC under key $K1$. See Figure 1 and the following description.

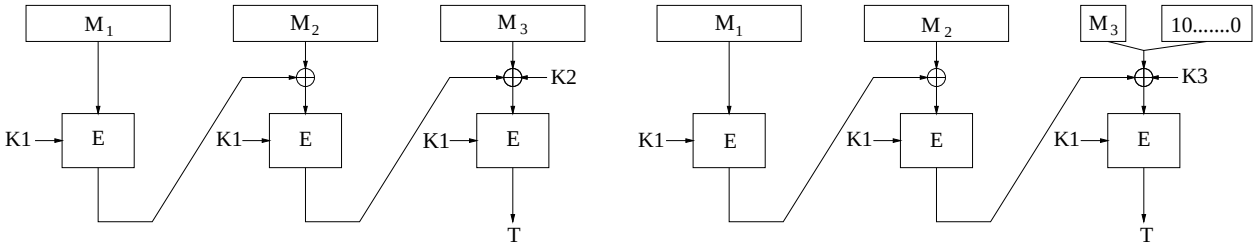

Figure 1: *The suggested CBC MAC using E and keys $K1$, $K2$, $K3$. On the left is the case where $|M|$ is a positive multiple of n; on the right is the case where $|M|$ is not a positive multiple of n.*

Algorithm $\mathrm{MAC}_{K1,K2,K3}(M)$
if $|M_m| = n$
  then $K \leftarrow K2$, and $P \leftarrow M$
  else $K \leftarrow K3$, and $P \leftarrow M \,\|\, 10^i$, where $i \leftarrow n - 1 - |M| \bmod n$
Let $P = P_1 \cdots P_m$, where $|P_1| = \cdots = |P_m| = n$
$C_0 \leftarrow 0^n$
for $i \leftarrow 1$ **to** $m - 1$ **do**
  $C_i \leftarrow E_{K1}(P_i \oplus C_{i-1})$
return $E_{K1}(P_m \oplus C_{m-1} \oplus K)$

Key Derivation. One may prefer to regard the MAC key as some k-bit string K, where k is the length of the AES key, and explicitly derive $(K1, K2, K3)$ from K. The customary approach for doing this is to apply a pseudorandom function (say AES itself) keyed by K, to distinct points; set $K1$ to be the first k bits of $E_K(\mathrm{Const1A}) \,\|\, E_K(\mathrm{Const1B})$, set $K2 = E_K(\mathrm{Const2})$, and set $K3 = E_K(\mathrm{Const3})$.

3 Advantages

The scheme just described has several advantages over comparable modes. We list the principal ones.

Arbitrary Message Lengths. Whereas correct operation of the basic CBC MAC requires messages to be of one fixed length, the specified MAC works correctly on messages of varying lengths. Furthermore, these lengths need not be a multiple of the block length—any bit string will do. While there are other approaches that support one or both of these properties, the story on this has never been simple or clear. Since in practice variable-length messages are the norm, as are messages whose length is not a multiple of 128 bits, we believe that any MAC defined as a NIST standard should correctly deal with messages of any length.

Efficiency. For any CBC MAC variant, the major computational effort is expended in computing the underlying block cipher. Our scheme uses a minimum number of AES invocations: one for each block of message, or fraction thereof: $\max\{1, \lceil |M|/128 \rceil\}$ block-cipher calls in all.

Simplicity and Familiarity. Because the algorithm is simple and familiar, implementations will be easily done. Since the CBC MAC has long-been accepted and trusted, we expect that this variant will be as well.

No Re-Keying. Whereas some competing schemes (e.g., in [1, 3]) would require invoking E with two or three different keys, the method here requires only one key. Therefore any key-setup costs are minimized. This enhances efficiency in both software and hardware.

Proven Security. The above efficiency characteristics are not obtained at the expense of security. In fact, what has become the "standard" cryptographic assumption about a block cipher's security—that it is a "pseudorandom permutation" [7, 2]—is enough to prove the security of the CBC MAC variant presented here. See [4], which proves, roughly said, that an attacker's probability of forgery after seeing q messages with lengths at most m blocks is no more than $5m^2q^2/2^{128}$. Concretely, if an attacker saw 1000 messages per second for a month, and none of these messages was longer than 10,000 bytes, his chances of forging a new message would be less than 1 in 10 trillion.

4 Disadvantages (Actual and Perceived)

Mandatory Serial Evaluation. It is not possible to extract much parallelism when computing the CBC MAC, in any of its variants. This has not been too serious a drawback in the past (authentication for Gbit networks being a notable exception), but it could become a more significant drawback in the future.

No Added Resistance to Key-Search Attacks. While other CBC MAC variants use additional keys to improve resistance to key-search attacks, what is presented here does not. One can perform an exhaustive key-search on the MAC presented just as efficiently as on the underlying AES primitive. But this concern, quite appropriate for DES, would seem to be moot for AES.

Acknowledgments

Thanks to **David Wagner** for debunking a silly optimization we had considered.

References

[1] ANSI X9.19. American national standard — Financial institution retail message authentication. ASC X9 Secretariat – American Bankers Association, 1986.

[2] M. BELLARE, J. KILIAN, and P. ROGAWAY. The security of the cipher block chaining message authentication code. To appear in *J. of Computer and System Science.* Earlier version in *Advances in Cryptology—Crypto '94*, Lecture Notes in Computer Science, Vol. 839. Y. Desmedt, ed., Springer-Verlag, 1994.

[3] A. BERENDSCHOT, B. DEN BOER, J.P. BOLY, A. BOSSELAERS, J. BRANDT, D. CHAUM, I. DAMGÅRD, M. DICHTL, W. FUMY, M. VAN DER HAM, C.J.A. JANSEN, P. LANDROCK, B. PRENEEL, G. ROELOFSEN, P. DE ROOIJ, J. VANDEWALLE. Final Report of Race Integrity Primitives. Lecture Notes in Computer Science, vol. 1007, Springer-Verlag, 1995.

[4] J. BLACK, P. ROGAWAY. CBC MACs for arbitrary-length messages: The three-key constructions. *Advances in Cryptology—Crypto 2000*, Lecture Notes in Computer Science, vol. 1880, Springer-Verlag, Mihir Bellare, editor, pp. 197–215, 2000.

[5] FIPS 113. Computer data authentication. Federal Information Processing Standards Publication 113, U.S. Department of Commerce/National Bureau of Standards, National Technical Information Service, Springfield, Virginia, 1994.

[6] ISO/IEC 9797-1. Information technology – Security techniques – Data integrity mechanism using a cryptographic check function employing a block cipher algorithm. International Organization for Standards, Geneva, Switzerland, 1999. Second Edition.

[7] M. LUBY and C. RACKOFF. How to construct pseudorandom permutations from pseudorandom functions. *SIAM J. Comput.*, vol. 17, No. 2, April 1988.

[8] E. PETRANK and C. RACKOFF. CBC MAC for real-time data sources. Journal of Cryptology, Vol. 13, No. 3 (2000), pp. 315–338.