An Hybrid Mode of Operation

Alexis W. Machado
email: alexis.machado@task.com.br; alexis.machado@telemigcelular.com.br
Feb/12/2004

Abstract. In this paper I propose a *tweakable* block cipher construction with a mode of operation that combines counter and chaining methods. Using a single key, the direct application of this mode produces unrepeatable message authentication tags.

Keywords: hybrid mode, tweakable cipher, message authentication, MAC.

1) Introduction

A simple tweakable cipher construction is given in [1]. In that work, the derived cipher doubles the time to encrypt a block, but promises new modes of operation easier to analyze. I present here a construction that can encrypt faster. An *hybrid mode*, combining counter and chaining modes, is defined for the new cipher and directly used for message authentication. The security of this scheme is discussed in section 5.

2) A Tweakable Block Cipher Construction

Let f' and g' be the encryption and decryption functions of an **n**-bit block cipher :

$$Y = f'(K, X)$$
$$X = g'(K, Y)$$

where K is the secret key, X the plaintext block and Y the encrypted block.

Consider a trivial *tweakable* cipher construction, based on f' and g', that reserves **t** bits of X for a tweak **T** and **b** bits for a reduced block **B**, that is, $X = T \times 2^b + B$, where $t + b = n$. The new encryption function f is

$$Y = f(K, T, B) = f'(K, T \times 2^b + B) \qquad (2a)$$

and the new decryption functions are

$$B = g(K, Y) = g'(K, Y) \bmod 2^b \qquad (2b)$$
$$T = h(K, Y) = g'(K, Y) \div 2^b \qquad (2c)$$

where "÷" is the integer division and "mod" is the remainder operator.

Function f is nothing more than a suitable way to operate isolated parts of an input block. So, any security flaw of f implies a security flaw of f'.

There will be a proportional increase t/b of ciphertext size and time to encrypt or decrypt a message when compared to the normal process. For authentication purpose, the ciphertext expansion is not a concern, because only one tag block is produced. Large blocks can reduce the overhead. For example, if (n,t,b) = (256, 64, 192) the increase ratio is t/b = 1/3 = 33%. For (n,t,b) = (512, 64, 448), t/b = 1/7 = 14%.

An obvious (and important) property is that f is injective with respect to T or B :

$$f(K, T, B) = f(K, T', B') \Leftrightarrow (T = T' \text{ and } B = B') \qquad (2d)$$

For example, the counter mode $Y_i = f(K, IV + i, B_i)$ always generate distinct outputs for distinct tweaks $IV + i$.

3) An Hybrid Mode

Given a sequence of n-bit blocks (B_1 , B_2 , B_3 , ...), the encryption of any block B_i in a counter-chaining mode is defined by the recursive formula

$$Y_i = f(K, T_i, (Y_{i-1} \bmod 2^b) \oplus B_i) \qquad (3a)$$

and the decryption defined by

$$B_i = g(K, Y_i) \oplus (Y_{i-1} \bmod 2^b) \qquad (3b)$$
$$T_i = h(K, Y_i) \qquad (3c)$$

where

a) "$\oplus$" is the bitwise exclusive-or operator.
b) $Y_0 = 0$.
c) The tweak T_i is a *global nonce*, a value that never repeats in encryptions done with K. Combined with the fact that f is injective in relation to T_i , we conclude that Y_i never repeats, even when the same block sequence is processed twice.

4) The Hybrid Mode Authentication (HMA)

Suppose we want to authenticate an L-bit message M represented by a sequence of concatenated b-bit blocks $S = B_1 \| B_2 \| ... \| B_q$. The last block B_q is right-padded with zeros if L is not a multiple of b. The number of blocks q is derived from L by

$$q = (L - 1) \div b + 1 \qquad (4a)$$

Let N be a *message nonce*, a fresh value for each authenticated message M, while a certain key is been used. The tweak T_i of equation *3a* is defined as

$$T_i = N \times 2^w + i - 1 \quad \text{if } 0 < i < q \qquad (4b)$$
$$T_i = N \times 2^w + L \quad \text{if } i = q \qquad (4c)$$

where $w < t$, $0 < L < 2^w$ and $0 \le N < 2^{t-w}$.

The **authentication tag** is the encryption of block B_q by equation *3a* :

$$Y_q = f(K, T_q, (Y_{q-1} \bmod 2^b) \oplus B_q) \qquad (4d)$$

The **sender** transmits the pair (Y_q , M). After getting (Y', M'), the **receiver** computes T_q using equation *3c*

$$T_q = h(K, Y')$$

and extracts N and L using equation *4c*

$$T_q = N \times 2^w + L \;\Rightarrow\; (N, L) = (T_q \div 2^w, T_q \bmod 2^w)$$

The number of blocks q is calculated by equation *4a*.

If necessary, the receiver right-pads M' with zeros (bits) to obtain S', the block sequence representing M'. Now he can encrypt the block B_q of S' using the formula *4d* and compare the resulting Y_q against the received Y'. If they are different, M' is rejected, otherwise is accepted as been generated by another holder of K.

Observe that we can authenticate, with each key K, a maximum of 2^{t-w} messages with at most $2^w - 1$ bits each one.

5) Observations on HMA Security

Let M' be an L'-bit message, different from M of section 4. M' is represented by the block sequence $S' = A_1 \| A_2 \| \ldots \| A_p$, where each block have b bits. Suppose that M have been authenticated by the sender (a holder of K) but M' no. An opponent want to find a valid tag Z_p for M' using a message nonce N'.

Combining equations *4c* and *4d* for M and M' results

$$Y_q = f(K, N \times 2^w + L, (Y_{q-1} \bmod 2^b) \oplus B_q) \qquad (5a)$$
$$Z_p = f(K, N' \times 2^w + L', (Z_{p-1} \bmod 2^b) \oplus A_p) \qquad (5b)$$

Since f is injective with respect to the tweak or the reduced block (equivalence *2d*), we have

$$Z_p = Y_q \Leftrightarrow N' = N \text{ and} \qquad (5c)$$
$$L' = L \text{ and} \qquad (5d)$$
$$(Z_{p-1} \bmod 2^b) \oplus A_p = (Y_{q-1} \bmod 2^b) \oplus B_q \qquad (5e)$$

So, if the attacker wants to use the tag Y_q for M' ($Z_p = Y_q$) ,

a) He must reuse the message nonce (condition *5c*). This can be done, assuming that the receiver can't verify the nonce freshness.
   Note: the **detection** of different messages with the same tag violates condition *5c*, so an attack based on tag collisions [2, 4] is not applicable.

b) He will inform the receiver that M' have the same bit-length of M (condition *5d*).
   He can't extend M to obtain M' and use the same tag. Two additional consequence are

$$L' = L \;\Rightarrow\; p = q$$
$$(L' = L \text{ and } M' \neq M) \;\Rightarrow\; S' \neq S$$

c) He must satisfy condition *5e*.

The adversary will restrict his work to the case where $A_p \neq B_q$.

Note: If $A_p = B_q$, these blocks are canceled in *5e*. The attacker may then examine the conditions for $Z_{p-1} = Y_{q-1}$, which gives an equation similar to *5e*, but involving A_{p-1} and B_{q-1}. If these blocks are the same again, he must proceed recursively until different ones are reached. At this point we have a situation equivalent to $A_p \neq B_q$, and the following arguments apply in the same way.

Combining condition *5e* with equation *4d*, making $p = q$, $N' = N$ and **omitting the key** for simplicity, we have

$$(f\,(T_{q-1}, Z) \bmod 2^b) \oplus A_q \; = \; (f\,(T_{q-1}, Y) \bmod 2^b) \oplus B_q \qquad (5f)$$

where Z and Y depends on the blocks preceding A_q and B_q respectively, and $T_i = N \times 2^w + b \times i$ (from *4b*).

Admitting that the right side of *5f* is known (see note below), the adversary must solve the equivalent equation $C = f(T_{q-1}, Z) \bmod 2^b$ for a given block C or Z. Consider the following facts about Z and $f(T_{q-1}, Z)$:

i) $Z \neq Y$, otherwise $A_q = B_q$ in equation *5f* .

ii) If the sender used the nonce T_{q-1} to encrypt Y, we can be sure he never have encrypted a different block (including Z) with this tweak (and will never do it). Therefore, the attacker can't observe $f(T_{q-1}, Z)$ computed by the sender.

iii)The attacker can't use a different tweak T, because equivalence *2d* gives
$T \neq T_{q-1} \Rightarrow f\,(T, \cdot) \neq f\,(T_{q-1}, Z)$.

We conclude that the opponent must guess the first b bits of $f(T_{q-1}, Z)$ when Z is given. When C is given, he must guess a value for Z such that the first b bits of $f(T_{q-1}, Z)$ (an unobserved encryption) is equal to C. In either case, these predictions will be right with probability $1/2^b$ for a strong cipher f .

Note: The sender doesn't need to reveal the encryption of Y, seen in equation *5f*, but we can suppose it have been leaked.

6) References

[1] M. Liskov, R. Rivest and D. Wagner, "Tweakable Block Ciphers"
http://www.cs.berkeley.edu/~daw/papers/tweak-crypto02.pdf

[2] C. Mitchell, "On the security of XCBC, TMAC and OMAC"
http://csrc.nist.gov/CryptoToolkit/modes/comments/Mitchell.pdf

[3] J. Black, "Message Authentication Codes"
http://www.cs.colorado.edu/~jrblack/papers/thesis.pdf

[4] D. Stinson, "Cryptography Theory and Pratice" Second Edition, Chapman & Hall/CRC