Message integrity of IAPM and IACBC

Johan Håstad*
johanh@nada.kth.se

June 26, 2001

Abstract

We give a short proof for message integrity of the IAPM modes and IACBC modes proposed by Jutla [1].

1 Introduction

Jutla [1] gave two schemes to combine message integrity with encryption. The methods use a block-cipher as the main ingredient. To analyze these schemes we replace the block encryption by a random permutation and analyze the construction in an information theoretic way. The rationale behind this is that a good block cipher should be a pseudorandom permutation and thus for an attacker that does not know the key the real situation is computationally indistinguishable from the situation described above.

Note that this is a preliminary paper and in the full paper we will have a more complete introduction which also compares to related work.

2 Preliminaries

The primitive we start with is a block-cipher f acting on n bits. Jutla describes two different modes, a CBC inspired mode called IACBC and a parallel mode call IAPM. In both modes a block cipher with one random key is used together with a random number r to generate a sequence of values S_i which have the property that each of them is uniformly picked and the difference of of S_i and S_j is also uniformly distributed for $i \neq j$.

One efficient implementation of this setup is to have

$$W = f_{K_1}(r)$$

*Royal Institute of Technology, work done while visiting IBM research and Institute for Advanced Study. For the latter visit supported by NSF grant CCR-9987077.

and

$$S_i \quad \alpha_i \quad ,$$

where α_i are distinct non-zero elements in $GF[2^n]$ and is interpreted as an element in $GF[2^n]$.

The main use of encryption is through applying f with an independent key K_2. We model f_1 as a random permutation G and f_2 as an independent random permutation F. If the underlying block cipher gives a family of pseudorandom permutations under the choice of random key this only introduces negligible error when dealing with a computationally bounded adversary.

We study two attacks of the adversary. In both cases the adversary asks for the encryption of a number of messages at his choice. The adversary is allowed to be adaptive and hence each plaintext can depend on all the encryptions seen so far.

To violate message integrity the adversary should produce a cipher text C' which is accepted as a valid encryption.

He violates security of encryption with advantage μ if he can produce two plaintexts P^0 and P^1 of equal length and then given the encryption of one of them guess the correct plaintext with probability$(1+\mu)/2$.

3 IAPM

The mode is defined as follows. Given a plaintext $P_i\ _{i=1}^{l-1}$, we define a parity check

$$P_l \quad \sum_{i=1}^{l-1} P_i \tag{1}$$

where the sum is block-wise exclusive-or. Numbers $S_i\ _{i=0}^{l}$ are generated as described in Section 2 and we let $C_0 \quad r$, the random seed used to generate the S_i and for other i we have

$$\begin{aligned} M_i &\quad P_i + S_i \\ N_i &\quad F\ M_i \\ C_i &\quad N_i + S_i, \end{aligned}$$

except for the last block where $C_l \quad N_l + S_0$.

Decryption is performed in the obvious way and a resulting plaintext is accepted if (1) holds.

Now we let the adversary ask for encryptions of plaintexts. We denote the j'th plaintext by P^j and its i'th block by P_i^j. Similar notation applies to M, N, S and r-values. We start by a definition.

Definition 3.1 *There is an* accident *in the preprocessing stage if for any* j, i k, l *we have* $M_i^j \quad M_l^k$ *or* $N_i^j \quad N_l^k$, *or* $r^j \quad r^k$ *for* $j \quad k$.

We have the following lemma.

Lemma 3.2 *If a total of m blocks are encrypted in the preprocessing stage the probability of having an accident is at most $\binom{m}{2}2^{-n}$.*

Proof: Since the the value of r^j is chosen after the adversary has specified P^j the probability that $M_i^j = M_l^k$ for any pair $j,i \neq k,$ is exactly 2^{-n}. If $M_i^j \neq M_l^k$ then $N_i^j \neq N_l^k$ since F is a permutation. The probability of two different r's being equal is also 2^n. We have $\binom{m}{2}$ different pairs of cryptoblocks and the lemma follows by the union bound. ∎

We now have the integrity theorem.

Theorem 3.3 *Consider IAPM. Suppose $\tau' + m \leq 2^{(n-1)/2}$. The probability that the adversary produces a ciphertext C' of length τ' that is accepted as legitimate after having had m blocks encrypted in the preprocessing phase is at most*

$$\left(1 + \binom{\tau' + m}{2}\right) 2^{1-n}.$$

Proof: We prove that the probability of a successful forgery conditioned upon no accident in the preprocessing stage is at most

$$\left(1 + \tau' m + \binom{\tau'}{2}\right) 2^{1-n}.$$

In view of Lemma 3.2 this is sufficient to establish the theorem. We prove this bound for any fixed outcome of the preprocessing stage. We concentrate of triples F, G, r that lead to one specific node where the adversary has seen m encryptions. Note that once both all plaintexts and ciphertexts are fixed the property of having an accident depends on G, r only. This follows since it can be written as equalities involving only P, C and S-values. We have the following lemma.

Lemma 3.4 *After any preprocessing all G, r with no accident are equally likely.*

Proof: Once G, r without an accident is specified the condition on F is that it takes m different values at m different points and thus the probability that F fulfills this is always the same. ∎

Lemma 3.5 *The fraction of G, r without any accident after m block encryptions is at least $1 - \binom{m}{2}2^{1-n}$.*

Proof: This follows since the probability that $M_i^j = M_l^k$ or $N_i^j = N_l^k$ for $j,i \neq k,$ or $r^j = r^k$ for $j \neq k$ is each 2^{-n} and we apply the union bound. ∎

Let us return to the proof of Theorem 3.3. The adversary has produced a ciphertext $C'_i{}_{i=0}^{l'}$ which at decryption produces $P'_i{}_{i=1}^{l'}$. We need to estimate the probability that P' satisfies (1). We need the following definition.

Definition 3.6 *A block C'_i is a* forced collision *if for some j in the preprocessing stage C_0^j C'_0 and if $i <$ ' C'_i C_i^j or i ' and C'_i C_l^j where is the length of message j.*

We have two cases:

1. All blocks of C' are forced collision.
2. Some block of C' is not a forced collision.

In the first case we reason as follows. Since the r's are all different there is a unique j causing the forced collisions and let be the length of this message. Since C' is different from C^j and all blocks are forced collisions we must have '. This gives that P'_i P_i^j for $1 \leq i \leq$ ' -1 while $P'_{l'}$ $>P_l^j + S_l + S_{l'}$. We conclude that

$$\sum_{i=1}^{l'} P'_i \qquad \sum_{i=1}^{l'-1} P_i^j + P_l^j + S_l + S_{l'} \tag{2}$$

If we did not have any conditioning the probability of this being 0 would be exactly 2^{-n}. Note that this is only a probability over G, r and thus conditioning is in fact easy to deal with. We know by Lemma 3.4 and Lemma 3.5 that we pick(G, r with uniform probability from a subset of density at least $1 - \binom{m}{2}2^{1-n}$ e conclude that also in the conditioned case the probability ofw (2) being 0 is at most

$$2^{-n}\, 1 - \binom{m}{2}2^{-n\ -1} \leq 2^{1-n}$$

and this completes the analysis in the case of all blocks being forced collisions.

In the case where at least one block is not a forced collision we argue as follows. Say that we have a spurious collision if two N-values that are not equal with probability 1 are equal. By the property of no accident in the preprocessing stage we have no spurious collision in the preprocessing steps. We have at most $'m + \binom{l'}{2}$ pairs that can result in an spurious collision. If we did not have any conditioning the probability of such a collision happening would be at most

$$2^{-n}\ \ 'm + \binom{'}{2}\ .$$

Since the event of a spurious collision only depends on G, r we can reason as above and conclude that if we condition upon no accident happening in the preprocessing this probability increases by at most a factor $(1-\binom{m}{2}2^{1-n\ -1} \leq 2$.

Now assume that we have no spurious collisions and take one N'_i which does not appear in preprocessing or as $N'_{i'}$ for $i' \quad i$. Fix F^{-1} at all values queried in preprocessing and at points other than N'_i when decrypting C'. This leaves $2^n - m - \quad ' - 1)$ values that can appear as $F^{-1}\ N'_i$ and only one of them produces a valid plaintext. We conclude that the probability of a successful forgery conditioned upon no accident in the preprocessing stage is at most

$$2^{1-n} \quad 'm + \binom{'}{2} \qquad 2^n - \quad m + \quad ' \quad ^{-1} \leq 2^{1-n}(1 + \quad 'm + \binom{'}{2} \ ,$$

and the proof of the theorem is complete. ∎

We next turn to security.

Theorem 3.7 *If a total of m blocks have been encrypted in IAPM-mode then assuming $m \leq 2^{(n-1)/2}$ the advantage of the adversary in the encrypt and compare game is at most $3\binom{m}{2}2^{-n}$.*

Proof: Since all r's are picked randomly the probability of an accident during the encryptions, including the two test encryptions is at most $\binom{m}{2}2^{-n}$. We assume that there is no such accident and fix one transcript.

Now consider the changed transcript where the two test ciphertext are interchanged. Keeping the same S-values we can calculate the N-values used in decryptions of these messages. Say that we have a post-accident if two N-values produced this way are equal or one of these N-values have been seen elsewhere. If we did not have any conditioning the probability of a post accident would be at most $\binom{m}{2}2^{-n}$. The conditioning can only increase by a factor $1 - \binom{m}{2}2^{1-n\ -1} \leq 2$. If there is no accident or a post-accident the changed transcript happens with exactly the same probability as the original transcript and in this case the adversary has no advantage in guessing which is the correct encryption. This proves the theorem. ∎

4 IACBC

The mode is similar to IAPM but it chains the blocks. We first expand the plaintext using the same parity-check (1) and generate numbers $S_i\ _{i=0}^{l}$. We let $N_0 \quad C_0 \quad G\ r)$, where r is the random seed used to generate the S_i and for other i we have

$$\begin{aligned} M_i \qquad & P_i + N_{i-1} \\ N_i \qquad & F\ M_i \\ C_i \qquad & N_i + S_i, \end{aligned}$$

except for the last block where $C_{l+1} \quad N_{l+1} + S_0$.

Theorem 4.1 *Consider IACBC. Suppose* $' + m \leq 2^{(n-1)/2}$. *The probability that the adversary produces a ciphertext* C' *of length* $'$ *after having had* m *blocks encrypted in the preprocessing phase is at most*

$$\left(1 + \binom{' + m}{2}\right) 2^{1-n}.$$

Proof: The differences to the proof in IAPM mode not substantial and let us mainly point out the differences.

We define an accident as before. The probability of $M_i^j \quad M_l^k$ is still about 2^{-n}. For $j \quad k$ this is exactly true since going over all 2^n values of r produces all 2^n values of each M_i and N_i (as long as the plaintext is fixed). This argument does not apply to $j \quad k, \quad i$ but, and we have to be slightly more careful. We can estimate the probability of a first accident at some point and conditioning upon M_{i-1}^j not being equal to any previous M-value we see that the probability of an accident involving M_i^j given that it is the m'th encrypted block is at most $2^{\,n} - m^{\,-1}$ and thus at most 2^{1-n} for $m < 2^{n-1}$.

In particular assuming that $m < 2^{n-1}$ Lemma 3.2 remains true upto a factor of 2.

Lemma 4.2 *If a total of* m *blocks are encrypted in the preprocessing stage of IACBC, the probability of having an accident is at most* $\binom{m}{2}2^{1-n}$.

Lemma 3.4 remains true without any change. Note that $M_i \quad P_i + S_{i-1} + C_{i-1}$ for $i \geq 2$ and $M_1 \quad P_1 + C_0$. Thus the condition of no accident can be phrased in terms of G, r only and once it is fulfilled we only specify F at a fixed number of points.

Lemma 3.5 also remains true. The equalities we check are either independent of G, r (i.e. involving only M_1^j for different j's) or hold with probability 2^{-n}. The number of equalities is the same.

In the proof of the theorem itself we have the same two cases. When we only have forced collisions then

$$P'_{l'} \quad P_l^j + N_{l-1}^j + N'_{l'-1} \quad P_l^j + C_{l-1}^j + S_{l-1}^j + C_{l'-1}^j + S_{l'-1}^j$$

and thus again to accept a message requires a nontrivial equality involving of S-values.

The case when we have some spurious collisions is analyzed as before. We first analyze the probability that all values are different and then fixing everything except this last value of F^{-1}, the argument is as before. ∎

The case of encryption is equally similar and we omit the details.

Theorem 4.3 *If a total of* m *blocks have been encrypted in IACBC-mode then the advantage of the adversary in the encrypt and compare game is at most* $3\binom{m}{2}2^{1-n}$.

The change of the bound comes from the loss of a factor of two in Lemma 4.2 compared to Lemma 3.2.

References

[1] C. Jutla, Encryption Modes with Almost Free Message Integrity, to appear at Eurocrypt 2001.