On the security of the IAPM and IACBC modes

Johan Håstad*
johanh@nada.kth.se

June 27, 2006

Abstract

We give new and shorter proofs for message integrity and confidentiality of the IAPM-mode and of the IACBC-mode proposed by Jutla [6].

Keywords: Block cipher, message integrity, encryption, modes of operation, authenticated encryption.

*Royal Institute of Technology, work done while visiting IBM research and Institute for Advanced Study. The visit to IAS was supported by NSF grant CCR-9987077.

1 Introduction

A block cipher is an extremely useful primitive in cryptography. In fact one would usually tends to think of a well designed block cipher as a (family of) random permutation(s). The simplest way to use a block cipher is to treat each block separately and use what is called Electronic Code Book mode or ECB. This mode does have significant drawbacks simply because the same cleartext block gives the same ciphertext block independent of context. Traditionally a number of modes of block ciphers have been proposed and the most widely used is Cipher Block Chaining, CBC.

Jutla [6] introduced two new modes which he called IACBC (Integrity Aware CBC) and IAPM (Integrity Aware Parallelizable Mode). As the names suggest the goal is to achieve integrity in the sense that an adversary is not able to create a ciphertext that decrypts in a legal way. This broad notion was introduced with slightly different details by Bellare and Namprempre [1] and Katz and Yung [7] and has become known as authenticated encryption. There have been many proposed implementations and two constructions given shortly after the one we are currently studying were given by Gligor and Donescu [3] and by Rogaway, Bellare, Black and Krovetz [9]. We refer to the survey by Black [2] for also other proposals, their efficiency, as well as the area in general.

A potential weakness in a cryptographic construction based on a block cipher can come either from the underlying block cipher or from the construction. A standard way to analyze the construction in isolation is to assume that the block cipher is a random permutation and use this to prove that the construction does have whatever property we strive for.

Under this assumption Jutla proved that his proposed new modes give both confidentiality and integrity. His proof, as well as a later proof by Halevi [5], is rather complicated with a number of cases to consider. The goal of the current paper is to give a more direct and, in our eyes, simpler proof of the same theorem. The key to our proof is to take a line of reasoning that minimizes the amount of conditioning that needs to be addressed. Similar proof techniques have been used on many occasions as problems of conditioning are frequent. An early paper using this technique is the construction of pseudorandom permutations from pseudorandom functions by Luby and Rackoff [8].

An outline of the paper is as follows. In Section 2 we give some preliminaries. The results for IAPM are presented in Section 3 and the modifications to also handle IACBC are given in Section 4. We end with some high level comments on how certain properties of the schemes were used in the proofs in Section 5.

2 Preliminaries

We start with is a block-cipher f acting on n bits. It has a secret key K and the permutation obtained when a particular key is chosen is denoted by f_K. As stated in the introduction we analyze the constructions of Jutla by replacing f_K with a randomly chosen K by a fully random permutation. In fact, Jutla's

construction uses two different keys to the block-cipher and we model these two permutations by two random and independent permutations called F and G.

Our basic building blocks are n-bit strings and it is convenient to have arithmetical operations defined. Addition is bit-wise exclusive-or and multiplication is performed in $GF[2^n]$.

The standard requirement one wants from a cryptosystem is confidentiality, i.e., that an adversary is not able to find out any information about the cleartext from the ciphertext. A key feature of the cryptosystems we study in this paper is that we also want integrity, namely that the adversary is not able to create any ciphertext that decrypts to a correct cleartext and thus any received correct cleartext is likely to be authentic. We model this requirements using the concept "legal cleartext" which we specify later.

Integrity game: The adversary is a deterministic algorithm that is given access to an encryption oracle. He asks the oracle for the encryption of a number of messages of his choice. The adversary is successful if he manages to produce a ciphertext, not returned by the oracle, that decrypts to a legal cleartext.

It might seem more general to allow a probabilistic adversary but our results apply also to this case. Namely, for any fixed set of coin-flips of the adversary the theorem for the deterministic adversary applies and our results give the probability of success over a random choice of the functions F and G. This implies that the same bound applies when we consider the probability of success of the adversary over random choices of F, G *and* his own random coin-flips. We allow the adversary to be adaptive and may choose the next plaintext as a function of the ciphertexts seen so far.

There are several ways to formulate confidentiality of an encryption scheme [4] and the most convenient for us is indistinguishability of encryptions. Our results for this notion give results also for other notions as there are general theorems [4] relating this notion to other notions of confidentiality. It is true that a direct proof for any notion of interest would give a better bound than an application of the general results but to keep this note short we refrain from using this approach. We have the following game.

Encryption distinguishability game: The adversary is a deterministic algorithm that is given access to an encryption oracle. He asks the oracle for the encryption of a number of messages of his choice. The adversary now produces two plaintexts T^0 and T^1 of equal length. The adversary is given the encryption of T^b for a randomly chosen b. The adversary has advantage μ if he can guess the value of b and be correct with probability $(1 + \mu)/2$.

Here it might seem more general to allow the adversary to also access to a decryption oracle but as he, by the integrity property, cannot efficiently produce a ciphertext with a legal decryption it does not make much sense.

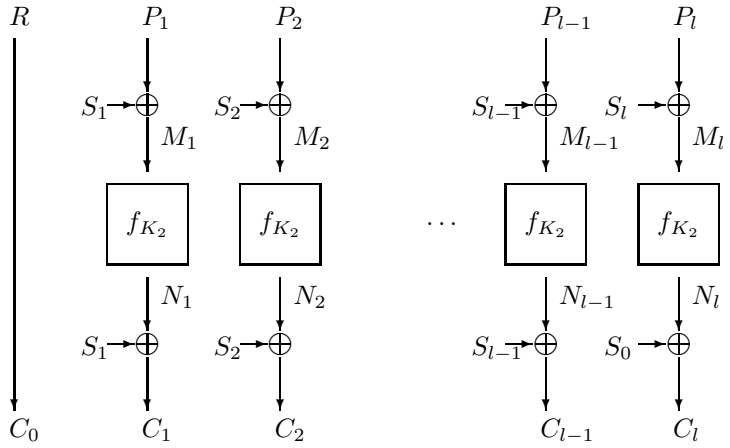

Figure 1: IAPM

3 IAPM

Given a plaintext $(P_i)_{i=1}^{l-1}$, with $l \geq 2$ we define a parity check

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

where the sum is block-wise exclusive-or and each P_i is an element of $\{0,1\}^n$.

For encryption we pick a random n-bit string R and define

$$S_i = \alpha_i f_{K_1}(R) \quad i = 0, 1 \ldots l \tag{2}$$

for a random key K_1 where α_i are distinct non-zero elements in $GF[2^n]$ and multiplication is performed in $GF[2^n]$.

We let $C_0 = R$, and for $1 \leq i \leq l-1$ we have

$$\begin{aligned} M_i &= P_i + S_i \\ N_i &= f_{K_2}(M_i) \\ C_i &= N_i + S_i, \end{aligned}$$

while for $i = l$, the two first equations are still used while the third equation is replaced by $C_l = N_l + S_0$. The resulting ciphertext that is transmitted is $(C_i)_{i=0}^{l}$. A schematic picture of the procedure is given in Figure 1.

We emphasize that for each new message the encryptor chooses a fresh random R and hence gets a fresh sequence $(S_i)_{i=0}^{l}$. We remark that Jutla suggested several ways of generating the numbers S_i stating that the key property is that the numbers are pairwise independent. In fact our proof shows that the desired properties are that each individual number, as well as the exclusive-or of any

two numbers are uniformly distributed. This is a slightly weaker condition than being pairwise independent. Our choice of constructing S_i achieves only the two needed properties and does not give pairwise independence.

Decryption is performed in the obvious way and a resulting plaintext is accepted if (1) holds. This defines the notion of a *legal* cleartext.

As discussed in the introduction we analyze the scheme by replacing f_{K_1} by a random permutation G and f_{K_2} by an independent random permutation F. As Halevi [5] points out, much less than full randomness is needed from G. In fact it is sufficient that for any two S-values (possibly from different messages) the probability that their exclusive-or takes any fixed value is small and preferably close to 2^{-n}. This would be fulfilled by taking G to be a much simpler function such as

$$G(X) = AX + B$$

where A, X and B are interpreted as elements in $GF[2^n]$ and A and B are secret and random. This construction would even be slightly preferable as in this case the probability that

$$G(X_1) + G(X_2) = Y$$

would be exactly 2^{-n} for any $X_1 \neq X_2$ and any Y. We do, however, need the full randomness of F and for symmetry reasons we assume the same property of G.

The adversary asks for encryptions of s cleartexts and we denote the j'th plaintext by P^j, its length (including the last parity check block) by l_j, and its i'th block by P_i^j. We use the equivalent notation for M, N, S, C and R-values. We assume that m total blocks of ciphertext are produced. This count includes the blocks with index 0 and hence $\sum_{j=1}^{s}(1 + l_j) = m$. The following definition is central for us.

Definition 3.1 *There is an* accident *if, for any* $(j,i) \neq (k,l)$, $1 \leq j \leq s$, $1 \leq i \leq l_j$, $1 \leq k \leq s$, $1 \leq l \leq l_k$, *we have* $M_i^j = M_l^k$ *or* $N_i^j = N_l^k$, *or* $R^j = R^k$ *for* $1 \leq j < k \leq s$.

We have the following lemma.

Lemma 3.2 *The probability of having an accident during the process of producing* m *ciphertext blocks is at most* $\binom{m}{2}2^{-n}$.

Proof: Suppose $k \leq j$, $(j,i) \neq (k,l)$ and that P^j is fixed. Then there is exactly one value of R^j such that $M_i^j = M_l^k$. Since the value of R^j is chosen after the adversary has specified P^j the probability of the equality is 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 conclude that the probability of an accident is, by the union bound, bounded by

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

■

We now state the integrity theorem.

Theorem 3.3 *Consider an attack on IAPM where the adversary receives encryptions containing a total of m blocks each of length n. Let l' be any integer such that $l' + m \leq 2^{(n-3)/2}$. The probability that the adversary produces a ciphertext C' of length l' that is accepted as legal is bounded by*

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

The probability is taken over the random choices of F and G, the two random permutations used to model f_{K_1} and f_{K_2} in the definition of IAPM.

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

$$\left(1 + l'm + \binom{l'}{2}\right) 2^{1-n}. \tag{3}$$

In view of Lemma 3.2 this is sufficient to establish the theorem as

$$\begin{aligned} \left(1 + l'm + \binom{l'}{2}\right) 2^{1-n} + \binom{m}{2} 2^{-n} &\leq \\ \left(1 + l'm + \frac{l'(l'-1)}{2} + \frac{m(m-1)}{2}\right) 2^{1-n} &= \left(1 + \binom{l'+m}{2}\right) 2^{1-n}. \end{aligned}$$

We prove the bound (3) for any fixed accident-free outcome of the encryptions asked by the adversary. Let $\vec{P} = (P^i)_{i=1}^s$ denote the set of plaintexts and $\vec{C} = (C^i)_{i=1}^s$ the ciphertexts seen. We note that the set of random seeds, $(R^i)_{i=1}^s$, used are part of the ciphertexts and hence part of $\vec{C}$.

We claim that since $\vec{P}$ and $\vec{C}$ are fixed the property of having an accident depends on G only. In particular $N_i^j = N_l^k$ is equivalent to

$$C_i^j + S_i^j = C_l^k + S_l^k$$

and a similar equality of M-values depends only on P-values and S-values. When $\vec{P}$ and $\vec{C}$ are fixed the original probability distribution induces a conditional probability distribution on F and G. This is the probability distribution we now study. We start by two simple definitions.

Definition 3.4 *A value of G is* compatible *with $\vec{C}$ and $\vec{P}$ if there is some value of F and choices of the R-values such that $\vec{C}$ gives the encryptions of the messages in $\vec{P}$.*

Definition 3.5 *A value of G is* accident-free *for $\vec{C}$ and $\vec{P}$ if there was no accident when producing the ciphertexts of $\vec{C}$ from the plaintexts $\vec{P}$.*

Note as discussed above this is a well defined notion since as discussed above the property of having an accident once $\vec{C}$ and $\vec{P}$ are fixed depends only on G.

Lemma 3.6 *Fix any values of $\vec{C}$ and $\vec{P}$ and assume that G_1 and G_2 are compatible with and accident-free for these values. Then*

$$Pr[G = G_1|\vec{C}, \vec{P}] = Pr[G = G_2|\vec{C}, \vec{P}].$$

Proof: The probability of any seeing any particular fixed value of G is proportional to the number of values of F that are compatible with the given value of G. Once G without an accident is specified together with $\vec{C}$ and $\vec{P}$, the constraint on F is exactly that it takes $m - s$ different values at $m - s$ different points. The number of of F that fulfills this constraint is independent of the choice of G. ∎

Lemma 3.7 *Fix any values of $\vec{C}$ and $\vec{P}$. The probability that a random G is compatible with and accident-free for these values is at least $1 - 2\binom{m}{2}(2^n - 1)^{-1}$.*

Please note that the probability distribution discussed here is the uniform distribution on G and not conditioned upon seeing the specific $\vec{C}$ and $\vec{P}$. By our choice of parameters the probability bound in Lemma 3.7 is at least 3/4 and this is the bound we use.

Proof: Each equality of the form $M_i^j = M_l^k$ or $N_i^j = N_l^k$, once $\vec{P}$ and $\vec{C}$ are fixed, gives an equality involving two S-values. Each such equality holds with probability at most $(2^n - 1)^{-1}$ for a random G and as we have $2\binom{m}{2}$ possible equalities, the lemma follows by 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 bound the probability that P' satisfies (1). We need the following definition.

Definition 3.8 *A block C'_i is a* forced collision *if for some j we have $C'_0 = C_0^j$ and one of the following two conditions hold*

1. *$i < \min(l', l_j)$ and $C'_i = C_i^j$*
2. *$i = l'$ and $C'_i = C_{l_j}^j$.*

We have two cases:

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

In the first case we proceed as follows. Remember that we are conditioning upon there being no accident. This implies that $R^i \neq R^j$ for $i \neq j$, and hence there is a unique j causing the forced collisions. Since C' is different from C^j and all blocks are forced collisions we must have $l_j > l'$. This gives that $P'_i = P_i^j$ for $1 \leq i \leq l' - 1$ while $P'_{l'} = P_{l_j}^j + S_{l_j}^j + S_{l'}^j$. We conclude that

$$\sum_{i=1}^{l'} P'_i = \sum_{i=1}^{l'-1} P_i^j + P_{l_j}^j + S_{l_j}^j + S_{l'}^j, \tag{4}$$

and using the definition, (2), of the S-values this equals

$$\sum_{i=1}^{l'-1} P_i^j + P_{l_j}^j + (\alpha_{l_j} + \alpha_l) G(R^j). \tag{5}$$

If we did not have any conditioning the probability of (5) being 0 would be exactly 2^{-n}. Note, however that the expression (5) only depends on G and we know by Lemma 3.6 and Lemma 3.7 that we pick G with uniform probability from a subset of density at least

$$1 - 2\binom{m}{2}(2^n - 1)^{-1} \geq \frac{3}{4}.$$

We conclude that, also taking conditioning into account, the probability of (5) and hence (4) being 0 is at most $\frac{4}{3}2^{-n} \leq 2^{1-n}$. This completes the analysis in the case when all blocks are forced collisions.

Next we turn to the second case in which at least one ciphertext block that is not a forced collision.

The final message produces a set of N-values through

$$N_i' = C_i + S_i.$$

Some of these will, through forced collisions, equal other N-values that have appeared during the encryptions. Say that we have a *spurious* collision if an N'-value which is not a forced collision equals an N-value obtained previously either during the earlier encryptions or earlier in the decryption of the adversary's message.

We have at most $l'm + \binom{l'}{2}$ pairs of ciphertext blocks that can result in a spurious collision. If we did not have any conditioning the probability of such a collision happening would be at most

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

Since the event of a spurious collision only depends on G we can reason as above and conclude that if we condition upon no accident happening this probability increases by at most a factor $(1 - 2\binom{m}{2}(2^n - 1)^{-1})^{-1} \leq \frac{4}{3}$ and we get the upper bound

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

for the probability of a spurious collision.

Now assume that we have no spurious collisions and fix the values of G at all points. Suppose N_{i_0}' does not equal any other N-value encountered in the encryption phase nor equals N_i' for $i \neq i_0$. Fix F^{-1} at all values queried during encryption and at points other than N_i' when decrypting C'. This leaves at least $2^n - m - (l' - 1)$ values that can appear as $F^{-1}(N_{i_0}')$ and only at most one of them produces a legal plaintext.

We conclude that the probability of a successful forgery conditioned upon no accident is at most

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

and the proof of the theorem is complete. ∎

We next turn to confidentiality.

Theorem 3.9 *Consider the ciphertext distinguishability game discussed in Section 2. Assume that a total of m blocks have been encrypted in IAPM-mode in the preprocessing stage and that the test messages T^0 and T^1 are of length l. Then the advantage of the adversary to win the game is at most $(2ml+l^2)2^{-n}$.*

Proof: For this theorem the question of accidents in the preprocessing stage is not important; fix any obtained vectors $\vec{C}$ and $\vec{P}$ of ciphertexts and plaintexts and the test messages T^0 and T^1 output by the adversary.

Pick a random R and mentally use it to encrypt both T^0 and T^1. Suppose that when we encrypt T^0 we do not get a value M_i that has appeared as an M-value during the preprocessing stage and that no two of the M-values obtained when encrypting T^0 are equal. Assume that the same is true when encrypting T^1 with the same R. We claim that in this case the probability distribution of the ciphertext (which is obtained by picking the needed values of F randomly) is the same when encrypting T^0 and T^1. This follows since any value of F not previously encountered has the same distribution.

It follows that the advantage of the adversary is bounded by the probability that the just stated assumption of inequality of M-values is false. It is easy to see that when choosing a random R, each equality holds with probability 2^{-n}. As we have $2ml+2\binom{l}{2}$ equalities the theorem follows. ∎

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 use a random R to generate numbers $(S_i)_{i=0}^{l}$ by the same procedure as for IAPM. We let $N_0 = C_0 = f_{K_2}(R)$, and for $1 \leq i \leq l-1$ we have

$$\begin{aligned} M_i &= P_i + N_{i-1} \\ N_i &= f_{K_2}(M_i) \\ C_i &= N_i + S_i, \end{aligned}$$

while for the last block the last equation is replaced by $C_l = N_l + S_0$. A schematic picture of IACBC is found in Figure 2.

Theorem 4.1 *Consider an attack on IACBC where the adversary receives encryptions containing a total of m blocks each of length n. Let l' be any integer*

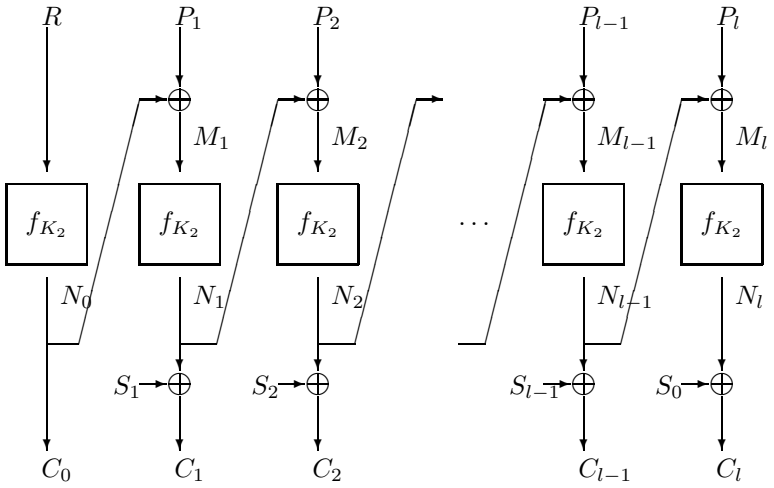

Figure 2: IACBC

such that $l' + m \leq 2^{(n-3)/2}$. *The probability that the adversary produces a ciphertext* C' *not obtained from the encryption oracle, of length* l' *that is accepted as legal is bounded by*

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

The probability is taken over the random choices of F *and* G, *the two random permutations used to model* f_{K_1} *and* f_{K_2} *in the definition of IACBC.*

Proof: The differences to the proof for IAPM mode are not substantial and hence we mainly point out the differences.

We define an accident as before and we need to establish the equivalent of Lemma 3.2. Let us analyze the probability that $M_i^j = M_l^k$. For $j > k$ this probability is exactly 2^{-n} since going over all 2^n values of R^j produces all 2^n values of each M_i^j and N_i^j, as long as the plaintext is fixed. This argument does not apply to $j = k$, $l < i$ and we have to be slightly more careful. It is enough to bound the probability that a first accident appears at M_i^j. This implies that we can assume that M_{i-1}^j is not equal to any previous M-value. Since there are at least $2^n - m$ possible values for $F(M_{i-1}^j)$ the probability that it is equal to any fixed value is at most $(2^n - m)^{-1}$ and this is at most 2^{1-n} for $m < 2^{n-1}$. This analysis implies that Lemma 3.2, except for a factor of at most two, remains true also for IACBC.

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

Lemma 3.6 remains true without any change. Note that $M_i = P_i + S_{i-1} + C_{i-1}$ for $i \geq 2$ and $M_1 = P_1 + C_0$. Thus the condition of no accident can

be phrased in terms of G only and given that we have no accident, $\vec{C}$ and $\vec{P}$ specifies the values of F at a fixed number of points.

Lemma 3.7 also remains true as both M-values and N-values can be defined in terms of $\vec{P}$, $\vec{C}$ and S-values.

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

$$P'_{l'} = P^j_{l_j} + N^j_{l_j-1} + N'_{l'-1} = P^j_{l_j} + C^j_{l_j-1} + S^j_{l_j-1} + C^j_{l'-1} + S^j_{l'-1}$$

and thus again to accept a message requires a nontrivial equality to hold which involves two S-values.

The case of not all blocks giving forced collisions is also analyzed as before. First we estimate the probability of a spurious collision and as the N-values have the same relation to the C-values as in IAPM this is exactly the same analysis as in IAPM. Finally, given that there are no spurious collision we can analyze the probability of obtaining a legal plaintext exactly as in IAPM.

We lose a factor of two in our estimate of the success probability due to the weaker bound of Lemma 4.2 compared to Lemma 3.2. ∎

We turn to confidentiality and start by stating the theorem.

Theorem 4.3 *Consider the ciphertext distinguishability game discussed in Section 2. Assume that a total of m blocks have been encrypted in IACBC-mode in the preprocessing stage and that the test messages T^0 and T^1 are of length l. Then the advantage of the adversary to win the game is at most $(2ml + l^2)(2^n - (m + l))^{-1}$.*

Proof: The proof is mostly a verbatim copy of the proof for Theorem 3.9. The only difference comes in the final estimate of the probability that all the obtained M-values during the test encryptions do not equal any previously obtained values. The probability that an M-value equals an M-value obtained during the preprocessing depends only on the randomness of R and this probability is still 2^{-n} for each possible equality.

The probability of equality of two different M-values during a test encryption has to be analyzed as in the proof of Lemma 4.2. We rely on the fact that the output of F causing the equality comes from an unused input to F and hence is uniformly random in a set of cardinality at least $2^n - (m + l)$. ∎

5 Final comments

It might be interesting to quickly comment on how some of the details of the definitions of the modes enter the analysis. The key for the proof is to make sure that there are no accidents which is more or less equivalent to the fact that the adversary cannot force identical inputs to F in two different situations. The key to this is making sure that the exclusive-or of two different S-values is unpredictable from the view of the adversary.

This latter property is ensured by having S defined through G applied to R. In the current situation we have both that R is chosen randomly and that G is modeled as a random permutation. As the proof shows this is sufficient but we could have made do with less. As long as G is a random permutation it is enough that the current value of R has not been used before and a counter would have been sufficient. This would slightly complicate the confidentiality proof which now would have to rely on the randomness of G but this could be handled using the machinery in the proof of authenticity.

If we insist on R being random, then as discussed previously simpler constructions of G such as making it a random element from a set of pairwise independent hash-functions would have been sufficient.

The key role of the randomness of the S-values also points us to the answer why we can handle adaptive adversaries without any problems. The value of R used to encrypt a message is chosen after the plaintext is presented. This ensures that the probability of an accident is small independent of the strategy for coming up with the plaintext.

Finally let us note that the last block is handled differently to avoid truncation of messages.

Acknowledgment: I am grateful to an anonymous referee for a very careful reading of the paper and helpful suggestions on how to better present the paper.

References

[1] M. Bellare and C. Nemprempre. Authenticated encryption: Relations among notions and analysis of the generic composition paradigm. In T. Okamoto, editor, *Asiacrypt 2000, LNCS Volume 1976*, pages 535–545. Springer-Verlag, 2000.

[2] J. Black. Authenticated encryption. In H. van Tilborg, editor, *Encyclopedia of Cryptography and Security*, pages 11–21. Springer-Verlag, 2005.

[3] V. Gligor and P. Donescu. Fast encryption and authentication: XCBC encryption and XECB authentication modes. In M.Matsui, editor, *FSE 2001, LNCS Volume 2355*, pages 92–108. Springer-Verlag, 2001.

[4] O. Goldreich. *Foundations of Cryptography, Volume II Basic Applications.* Cambridge University Press, Cambridge, 2004. ISBN 0-521-83084-2.

[5] S. Halevi. An observation regarding Jutla's modes of operation. Cryptology ePrint Archive: Report 2001/015, 2005.

[6] C. Jutla. Encryption modes with almost free message integrity. In Birgit Pfitzmann, editor, *Advances in Cryptology Proceedings of Eurocrypt 2001*, pages 529–544, 2003.

[7] J. Katz and M. Yung. Unforgeable encryption and chosen ciphertext secure modes of operation. In B. Schneier, editor, *FSE 2000, LNCS Volume 1978*, pages 284–299. Springer-Verlag, 2000.

[8] M.Luby and C. Rackoff. How to construct pseudorandom permutations from pseudorandom functions. *SIAM Journal on Computing*, 17:2:373–386, 1988.

[9] P. Rogaway, M. Bellare, J. Black, and T. Krovetz. OCB: A block-cipher mode of operation for efficient authenticated encryption. In *ACM Conference on Computer and Communicationss Security*, pages 195–205. ACM Press, 2001.