The Security of “One-Block-to-Many” Modes of Operation

Henri Gilbert
France Télécom R&D
henri.gilbert@francetelecom.com

February 6, 2003

Abstract

In this paper, we investigate the security, in the Luby-Rackoff security paradigm, of blockcipher modes of operation allowing to expand a one-block input into a longer t-block output under the control of a secret key K. Such “one-block-to-many” modes of operation are of frequent use in cryptology. They can be used for stream cipher encryption purposes, and for authentication and key distribution purposes in contexts such as mobile communications. We show that although the expansion functions resulting from modes of operation of blockciphers such as the counter mode or the output feedback mode are not pseudorandom, slight modifications of these two modes provide pseudorandom expansion functions. The main result of this paper is a detailed proof, in the Luby-Rackoff security model, that the expansion function used in the construction of the third generation mobile (UMTS) example authentication and key agreement algorithm MILENAGE is pseudorandom.

1 Introduction

In this paper, we investigate the security of modes of operation of blockciphers allowing to construct a length increasing function, i.e. to expand a 1-block input value x into a longer t-block output $(z_1, z_2, \ldots, z_t)$ (where $t \geq 2$), under the control of a secret key K.

Such length increasing modes of operation of blockciphers associated with a one block to t blocks expansion function are of extremely frequent use in cryptology, mainly for pseudo-random generation purposes. They can be considered as a kind of dual of length decreasing modes of operation associated with a t blocks to one block compression function used for message authentication purpose (e.g. CBC MAC). In both cases, the essential security requirement is that the resulting one block to t blocks (respectively t blocks to one block) function be pseudorandom, i.e. (informally speaking) indistiguishable, by any reasonable adversary, from a perfect random function with the same input and output sizes. Thus the Luby and Rackoff security paradigm [LR88], which allows to relate the pseudo-randomness of a function resulting from a cryptographic construction to the pseudorandomness of the elementary function(s) encountered at the lower level of the same construction, represents a suitable tool for analysing the security of both kinds of modes of operation. However, the security and the efficiency of length increasing modes of operation have been much less investigated so far than the one of length decreasing modes of operation such as CBC MAC [BKR94, PR00], R-MAC [JJV02], etc., or than constructions of length-preserving functions or permutations such as the Feistel scheme [LR88, Pa91].

The practical significance of length increasing modes of operation of blockciphers comes from the fact that they provide the two following kinds of pseudorandom generation functions, which both represent essential ingredients for applications such as mobile communications security.

Example 1: Stream cipher modes of operation of blockciphers.

It has become usual for stream ciphers (whether they are derived or not from a mode of operation of a blockcipher) to require that the generated pseudo-random sequences used to encrypt data be not only dependent upon a secret key, but also upon an additional (non secret) input value x, sometimes referred to as an initialization vector or as an initial value (IV). This holds for most recently proposed stream ciphers, e.g. SEAL [RC98], SCREAM [HCCJ02], SNOW [EJ02], BGML [HN00], and for the stream cipher mode of operation of the KASUMI blockcipher used in the third generation mobile system UMTS [Ka00]. As a consequence, stream ciphers are more conveniently modelled as a length increasing pseudo-random function $F_K : \{0,1\}^n \rightarrow \{0,1\}^{nt}$; $x \mapsto F_K(x) = (z_1, z_2, \cdots, z_t)$ than as a mere pseudo-random numbers generator allowing to derive a pseudo-random sequence $(z_1, z_2, \cdots, z_t)$ of nt bits from a secret seed K. The advantage of modelling a stream cipher as a length increasing function generator rather than as a numbers generator is that it allows to reflect the security conditions on the dependance of the pseudo-random sequence in the input value, by requiring that F_K be a pseudo-random function, indistinguishable from a perfect random function with the same input and output sizes by any reasonable adversary.

Example 2: Combined authentication and key distribution.

In mobile communication systems (GSM, UMTS, etc.) and more generally in most secret key security architectures where authentication and encryption are provided, protected communications are initiated with a kind of "handshake" where authentication or mutual authentication between the user's device and the network and session key(s) distribution are performed. Such an initial handshake is followed by a protected communication, where the session key(s) resulting from the handshake phase are used to encrypt and/or to authenticate the data exchanges. In order for the handshake protocol not to delay the actual protected communication phase, it is essential to restrict it to two passes and to minimize the amount of data exchanged. For that purpose one of the parties (typically the network in the case of mobile communications) sends a random challenge (accompanied by additional data such as a message authenticated counter value if mutual authentication is needed), and this random challenge serves as an input to a secret key function allowing to derive an authentication response and one or several session key(s). In recent mobile communication systems such as UMTS, the length of the outputs to be produced (measured in 128-bit blocks) far exceeds the 1-block length of the random challenge. Thus, one single operation of a blockcipher does not suffice to produce the various outputs needed. In order to base the security of the cryptologic computations performed during the handshake upon the security of a trusted blockcipher, a suitable one-block-to-many mode of operation of the underlying blockcipher has to be defined. The security requirements are not only that each of the output blocks be unpredictable by an adversary. In addition, the information on one subset of the outputs (say for instance an authentication response) should not help an adversary to derive any information about the rest of the outputs (say for instance the session key used to encrypt the subsequent exchanges). These various security requirements can be again reflected, as in the example of stream cipher modes of operation, in saying that the one to t blocks function $F_K : \{0,1\}^n \rightarrow \{0,1\}^{n.t}$; $x \mapsto F_K(x) = (z_1, z_2, \cdots, z_t)$ used to derive the various output values must be indistiguishable from a perfect random function with the same input and output sizes.

In this paper, we show that although the one block to t blocks functions associated with well known modes of operation of blockciphers such as the Output Feedback mode (OFB) or the so-called Counter mode are not pseudorandom, slightly modified modes of operation in which the one-block input is first "prewhitened" before being subject to an expansion process are pseudorandom in a formally provable manner. The main result of this paper is a detailed pseudorandomness proof, in the Luby and Rackoff security model, for the one to t blocks mode of operation of a blockcipher used in the UMTS example authentication and key distribution algorithm MILENAGE [Mi00], which can be considered as a modified counter mode. We also provide pseudorandomness proofs for a modified version of the OFB mode.

Related work

The study of pseudorandomness properties of cryptographic constructions initiated Luby and Rackoff's seminal paper [LR88] has represented a very active research area for the last decade. In particular, Patarin clarified the link between the best advantage of a q-queries distinguisher and the q-ary transition probabilities associated with f and proved indistinguihability bounds for numerous r-round Feistel constructions [Pa91], Maurer showed how to generalise indistinguishability results related to perfect random functions to indistinguishability results related to nearly perfect random functions [Ma92], Bellare, Kilian, Rogaway [BKR94], and later on several other authors [PR00, JJV02, BR00] investigated the application of similar techniques to various message authentication modes of operation, Vaudenay embedded techniques for deriving indistinguishability bounds into a broader framework named the decorrelation theory [Va98, Va99]. In this paper, we apply general indistinguishability proof techniques due to Patarin [Pa91] in an essential manner.
Our approach to expansion functions constructions based on blockcipher modes of operation has some connections, but also significant differences, with the following recently proposed blockcipher based expansion function constructions:
- in [DHY02], Desai, Hevia and Yin provide security proofs, in the Luby-Rackoff paradigm, for the ANSI X9.17 pseudo random sequences generation mode of operation of a blockcipher, and for an improved version of this mode which is essentially the same as the modified OFB mode considered in this paper. However, the security model considered in [DHY02] is quite distinct (and somewhat

complementary): we consider the pseudorandomness properties of the one to t blocks expansion function resulting from the considered mode of operation, whereas [DHY02] models a PRG mode of operation as the iteration a "smaller" keyed state transition and keystream output function, and consider the pseudorandomness properties of such state transition functions.
-in [HN00], Hastad and Näslund propose a pseudorandom numbers generator named BMGL. BGML is based on a "key feedback" mode of operation of a blockcipher. The security paradigm underlying BMGL (namely the indistinguishability of pseudorandom numbers sequences from truly random sequences, based upon a combination of the Blum-Micali PRG construction [BM84] and a variant of the Goldreich Levin hard core bits construction [GL89], in which the conjectured onewayness of the key dependance of the blockcipher is used to construct PR sequences of numbers) is quite different from the one considered here (namely the indistinguishability of the constructed expansion function from a perfect random function, assuming that the underlying blockcipher is indistinguishable from a perfect random one-block permutation). The advantage of the BGML approach it that it relies upon less demanding security assumptions for the underlying blockcipher than in our approach, but the disadvantage is that it leads to less efficient constructions in terms of the number of blockcipher invocations per output block.
-in [BDJR97], Bellare, Desai, Jokipii and Rogaway provide security proofs for stream cipher modes of operation, namely the XOR scheme and a stateful variant named CTR schemes. These two modes have some connections with the insecure one block to t blocks mode of operation referred to as the counter mode in this paper. However, a major difference between these modes is that in the XOR and CTR schemes, and adversary has no control at all of the inputs to the underlying blockcipher f (she can only control the plaintext), whereas in all the one to many blocks modes we consider in this paper, an adversary can control the one-block input value. Thus, there is no contradiction between the facts that the XOR and CTR encryption schemes are shown to be secure in [BDJR97] and that the counter mode of operation can easily be shown to be totally insecure.
This paper is organized as follows: Section 2 introduces basic definitions and results on random functions and security proof techniques in the Luby-Rackoff security model. Section 3 describes various "one-block-to-many" modes of operation of blockciphers, and introduces a modified variant of the counter mode used in MILENAGE and an improved variant of the OFB mode. Sections 4 and 5 present pseudorandomness proofs for the two latter modes.

2 Security Framework

2.1 The Luby-Rackoff Security Paradigm

A key dependent cryptographic function such as a blockcipher or a mode of operation of a blockcipher can be viewed as a random function associated with a randomly selected key value. It is generally defined using a recursive construction process. Each step of the recursion consists of deriving a random function (or permutation) F from r previously defined random functions (or permutations) $f_1, \cdots, f_r$, and can be represented by a relation of the form

$F = \Phi(f_1, \cdots, f_r)$.

One of the strongest security requirement one can put on such a random function or permutation F is that F be impossible to distinguish with a non negligible success probability from a perfect random function or permutation F^* uniformly drawn from the set of all functions (or permutations) with the same input and output sizes, even if a probabilistic testing algorithm A of unlimited power is used for that purpose and if the number q of adaptively chosen queries of A to the random instance of F or F^* to be tested is large.

It is generally not possible to prove indistiguishability properties for "real life" cryptologic random functions and large numbers of queries, because this would require a far too long key length. However, it is often possible to prove or disprove that if a random function F encountered at a given level of a cryptologic function construction is related to random functions encountered at the lower recursion level by a relation of the form $f = \Phi(f_1, \cdots, f_r)$, then if we replace the actual f_1 to f_r random functions of the cipher by independent perfect random functions or permutations f_1^* to f_r^* (or, in a more sophisticated version of the same approach, by f'_1 to f'_r functions which are sufficiently indistinguishable from f_1^* to f_r^*), then the resulting modified random function F is indistinguishable from a random function (or permutation). This provides a useful method for assessing the soundness of blockcipher constructions.

For instance, in the case of a three-round Feistel construction, a well known theorem first proved by Luby and Rackoff [LR88] provides upper bounds on the $|p - p^*|$ advantage of any testing algorithm A in distinguishing the $2n$-bit random permutation $F = \Psi(f_1^*, f_2^*, f_3^*)$ deduced from three independent perfect random functions f_1^*, f_2^* and f_3^* from a perfect random $2n$-bit permutation F^* with q adaptively chosen queries to the tested instance of F or F^*. This advantage is less than $\frac{q^2}{2^n}$. Another example is for the $F = \Phi_{CBCMAC}(f)$ CBC-MAC construction allowing to derive a tn-bit to n-bit message authentication function from chained invocations of a an n-bit to n-bit function f. It was shown by Bellare, Kilian and Rogaway in [BKR94] that if $q^2t^2 \leq 2^{n+1}$, then the advantage of any testing algorithm A in distinguishing the random function $F = \Phi_{CBCMAC}(f^*)$ derived from a perfect nt -bit to n-bit random function using q adaptively chosen queries is less than $3\frac{q^2t^2}{2^{n+1}}$.

In this paper, we will consider constructions of the form $F = \Phi(f)$, allowing to derive a n-bit to nt-bit function from several invocations of the same instance of an n-bit permutation f, representing a blockcipher of blocksize n. We will show that for suitable modes of operation Φ, the random function $F = \Phi(f^*)$ derived from a perfect n-bit random permutation is indistinguishable from a perfect n-bit to nt-bit random function F^*.

2.2 Random Functions

Through the rest of this paper we are using the following notation:
- I_n denotes the set $\{0, 1\}^n$
- $F_{n,m}$ denotes the set ${I_n}^{I_m}$ of functions from I_n into I_m. Thus $|F_{n,m}| = 2^{m.2^n}$
- P_n denotes the set of permutations on I_n. Thus $|P_n| = 2^n!$.

A random function of $F_{n,m}$ is defined as a random variable F of $F_{n,m}$, and can be viewed as a probability distribution $(Pr[F = \varphi])_{\varphi \in F_{n,m}}$ over $F_{n,m}$, or

equivalently as a family $(F_\omega)_{\omega\in\Omega}$ of $F_{n,m}$ elements. In particular:
- A n-bit to m-bit key dependent cryptographic function is determined by a randomly selected key value $K \in \mathcal{K}$, and can thus be represented by the random function $F = (f_K)_{K\in\mathcal{K}}$ of $F_{n,m}$.
-A cryptographic construction of the form $F = \Phi(f_1, f_2, \cdots, f_r)$ can be viewed as a random function of $F_{n,m}$ determined by r random functions $f_i \in F_{n_i,m_i}$, $i = 1 \cdots r$.

Definition 1 *We define a perfect random function F^* of $F_{n,m}$ as a uniformly drawn element of $F_{n,m}$. In other words, F^* is associated with the uniform probability distribution over $F_{n,m}$. We define a perfect random permutation f^* on I_n as a uniformly drawn element of P_n. In other words, f^* is associated with the uniform probability distribution over P_n.*

Definition 2 *(q-ary transition probabilities associated to F). Given a random function F of $F_{n,m}$, we define the transition probability $Pr[\mathbf{x} \overset{F}{\mapsto} \mathbf{y}]$ associated with a q-tuple $\mathbf{x}$ of $I_n$inputs and a q-tuple $\mathbf{y}$ of I_m outputs as*
$Pr[\mathbf{x} \overset{F}{\mapsto} \mathbf{y}] = Pr[F(x^1) = y^1 \wedge F(x^2) = y^2 \wedge ... \wedge F(x^q) = y^q]$
$= Pr_{\omega\in\Omega}[F_\omega(x^1) = y^1 \wedge F_\omega(x^2) = y^2 \wedge ... \wedge F_\omega(x^q) = y^q]$

In the sequel we will use the following simple properties:

Property 1 *Let f^* be a perfect random permutation on I_n. If $\mathbf{x} = (x^1, ..., x^q)$ is a q-tuple of pairwise distinct I_n values and $\mathbf{y} = (y^1, ..., y^q)$ is a q-tuple of pairwise distinct $I_n$values then $Pr[\mathbf{x} \overset{f^*}{\mapsto} \mathbf{y}] = (|I_n| - q)!/|I_n|! = \frac{(2^n-q)!}{(2^n)!}$*

Property 2 *Let f^* be a perfect random permutation on I_n. If x and x' are two distinct elements of I_n and δ is any fixed value of I_n, then $Pr[f^*(x) \oplus f^*(x') = \delta] \leq \frac{2}{2^n}$.*

Proof: $\Pr[f^*(x) \oplus f^*(x') = 0] = 0$ since $x \neq x'$. If $\delta \neq 0$, $\Pr[f^*(x) \oplus f^*(x') = \delta] = \frac{2^n.2^{n-2}...1}{2^n!} = \frac{1}{2^n-1} \leq \frac{2}{2^n}$. So, $\Pr[f^*(x) \oplus f^*(x') = \delta] \leq \frac{2}{2^n}$.

2.3 Distinguishing two random functions

In proofs of security such as the one presented in this paper, we want to upper bound the probability of any algorithm to distinguish whether a given fixed φ function is an instance of a $F = \Phi(f_1^*, f_2^*, .., f_r^*)$ random function of $F_{n,m}$ or an instance of the perfect random function F^*, using less than q queries to φ.

Let A be any distinguishing algorithm of unlimited power that, when input with a φ function of $F_{n,m}$ (which can be modelled as an “oracle tape” in the probabilistic Turing Machine associated with A) selects a fixed number q of distinct chosen or adaptively chosen input values x^i (the queries), obtains the q corresponding output values $y^i = F(x^i)$, and based on these results outputs 0 or 1. Denote by p (resp by p^*) the probability for A to answer 1 when applied to a random instance of F (resp of F^*). We want to find upper bounds on the advantage $Adv_A(F, F^*) = |p - p^*|$ of A in distinguishing F from F^* with q queries.

As first noticed by Patarin [Pa91], the best advantage $Adv_A(F, F^*)$ of any distinguishing algorithm A in distinguishing F from F^* is entirely determined by the q-ary transition probabilities $Pr[\mathbf{x} \overset{F}{\mapsto} \mathbf{y}]$ associated with each $\mathbf{x} = (x^1, \cdots, x^q)$ q-tuple of pairwise distinct I_n values and each $\mathbf{y} = (y^1, \cdots, y^q)$ q-tuple of I_m values. The following Theorem, which was first proved in [Pa91] and an equivalent version of which is stated in [Va99], is a very useful tool for deriving upper bounds on $Adv_A(F, F^*)$ based on properties of the $Pr[\mathbf{x} \overset{F}{\mapsto} \mathbf{y}]$ q-ary transition probabilities.

Theorem 1 *Let F be a random function of $F_{n,m}$ and F^* be a perfect random function representing a uniformly drawn random element of $F_{n,m}$. Let q be an integer. Denote by X the subset of ${I_n}^q$ containing all the q-tuples $\mathbf{x} = (x^1, \cdots, x^q)$ of pairwise distinct elements. If there exists a subset Y of ${I_m}^q$ and two positive real numbers ϵ_1 and ϵ_2 such that*
1) $|Y| \geq (1 - \epsilon_1) \cdot |I_m|^q$ *(i)*
2) $\forall \mathbf{x} \in X \forall \mathbf{y} \in Y Pr[\mathbf{x} \overset{F}{\mapsto} \mathbf{y}] \geq (1 - \epsilon_2) \cdot \frac{1}{|I_m|^q}$ *(ii)*
then for any A distinguishing algorithm using q queries

$$Adv_A(F, F^*) \leq \epsilon_1 + \epsilon_2.$$

In order to improve the selfreadability of this paper, a short proof of Theorem 1, which structure is close to the one of the proof given in [Pa91], is provided in appendix at the end of this paper.

3 Description of length increasing modes of operation of blockciphers

We now describe a few natural length increasing modes of operation of a blockcipher. Let us denote the blocksize (in bits) by n, and let us denote by t a fixed integer such that $t \geq 2$. The purpose of one to t blocks modes of operation is to derive an n-bit to tn-bit random function F from an n-bit to tn-bit random function f (representing a blockcipher associated with a random key value K) in such a way that F be indistinguishable from a perfect n-bit to tn bit random function if f is indistinguishable from a perfect random permutation f^*. We show that the functions associated with the well known OFB mode and with the so-called counter mode of operation are not pseudorandom and introduce enhanced modes of operation, in particular the variant of the counter mode encountered in the UMTS example authentication and key distribution algorithm MILENAGE.

3.1 The expansion functions associated with the counter and OFB modes of operation are not pseudorandom

Definition 3 *Given any t fixed distinct one-block values $c_1, \cdots, c_t \in \{0,1\}^n$ and any random permutation f over $\{0,1\}^n$, the one block to t blocks function F_{CNT} associated with the Counter mode of operation of f is defined as follows:*

$$F_{CNT}(f) : \{0,1\}^n \rightarrow \{0,1\}^{nt} \qquad x \mapsto (z_1, \cdots, z_t) = (f(x \oplus c_1), \cdots, f(x \oplus c_t))$$

Given any random permutation f over $\{0,1\}^n$, the 1 block to t blocks function F_{OFB} associated with the output feedback mode of operation of f is defined as

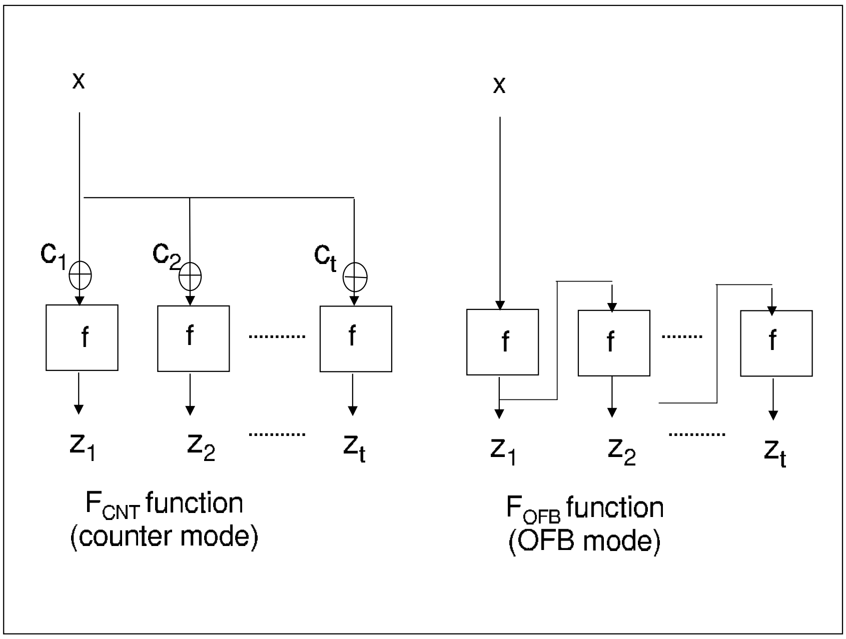

Figure 1: The counter and OFB modes of operation

follows:

$$F_{OFB}(f) : \{0,1\}^n \to \{0,1\}^{nt} \qquad x \mapsto (z_1, \cdots, z_t)$$

where the z_i are recursively given by $z_1 = f(x); z_2 = f(z_1); \cdots; z_t = f(z_{t-1})$

It is straightforward that F_{CNT} and F_{OFB} are not a pseudorandom. As a matter of fact, let us consider the case where F_{CNT} and F_{OFB} are derived from a perfect random permutation f^*. Let x denote any arbitrary value of $\{0,1\}^n$, and $(z_1, \cdots, z_t)$ denote the $F_{CNT}(x)$ value. For any fixed pair (i,j) of distinct elements of $\{1,2,..,t\}$, let us denote by $(z'_1, \cdots, z'_t)$ the F_{CNT} output value corresponding to the modified input value $x' = x \oplus c_i \oplus c_j$. The obvious property that $z'_i = z_j$ and $z'_j = z_i$ provides a distinguisher of F_{CNT} from a perfect one block to t-blocks random function F^* which requires only two oracle queries. Similarly, to proof that F_{OFB} is not pseudorandom, let us denote by x and $(z_1, \cdots, z_t)$ any arbitrary value of $\{0,1\}^n$ and the $F_{CNT}(x)$ value. With an overwhelming probability, $f^*(x) \neq x$, so that $z_1 \neq x$. Let us denote by x' the modified input value given by $x' = z_1$, and by $(z'_1, \cdots, z'_t)$ the corresponding F_{OFB} output value. It directly follows from the definition of F_{OFB} that for $i = 1, \cdots, t-1$, $z'_i = z_{i+1}$. This provides a distinguisher of F_{OFB} from a perfect one block to t-blocks random function F^* which requires only two oracle queries.

The above distinguishers indeed represent serious weaknesses in operational contexts where the input value of F_{CNT} or F_{OFB} can be controlled by an adversary. For instance if F_{CNT} or F_{OFB} is used for authentication and key distribution purposes, these distinguishers result in a lack of cryptographic separation between the output values z_i. For certain pairs (i,j) of distinct $\{1, \cdots, t\}$ values, an adversary knows how to modify the input x to the data expansion function

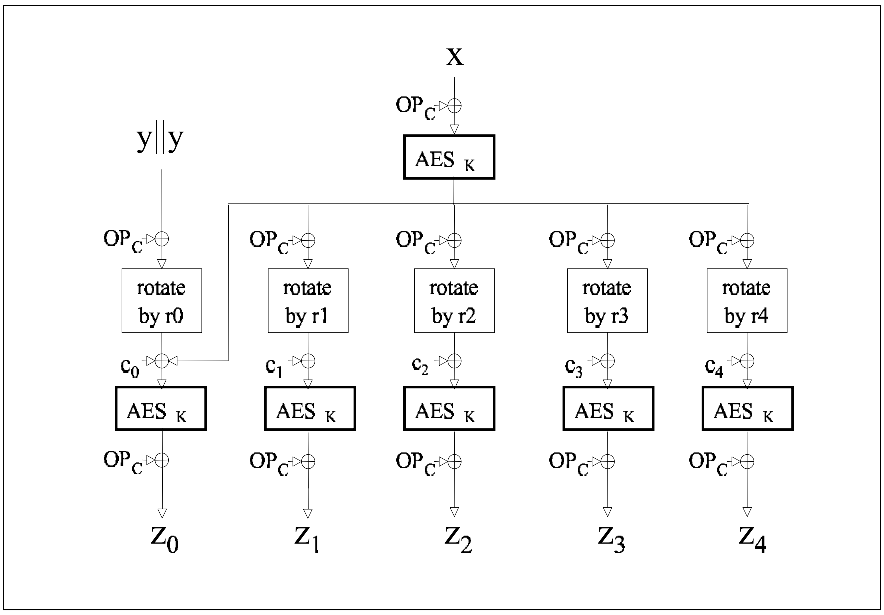

Figure 2: Milenage

in order for the i-th output corresponding to the modified input value x', which may for instance represent a publicly available authentication response), to provide her with the j-th output corresponding to the input value x, which may for instance represent an encryption key.

3.2 Modified counter mode: the MILENAGE construction

Figure 2 represents the example UMTS authentication and key distribution algorithm MILENAGE [Mi00]. Its overall structure consists of 6 invocations of a 128-bit blockcipher E_K, e.g. AES associated with a 128-bit subscriber key K. In Figure 2, c_0 to c_4 represent constant 128-bit values, and r_0 to r_5 represent rotation amounts (comprised between 0 and 127) of left circular shifts applied to intermediate 128-bit words. OP_C represents a 128-bit auxiliary (operator customisation) key.

MILENAGE allows to derive four output blocks z_1 to z_4 (which respectively provide an authentication response, an encryption key, a message authentication key, and a one-time key used for masking plaintext data contained in the authentication exchange) from an input block x representing a random authentication challenge. It also allows to derive a message authentication tag z_0 from the x challenge and a 64-bit input word y (which contains an authentication sequence number and some additional authentication management data) using a close variant of the CBC MAC mode of E_K. The security of the MAC function providing z_0, the independence between z_0 and the other output values are outside of the scope of this paper. Some analysis of these features can be found

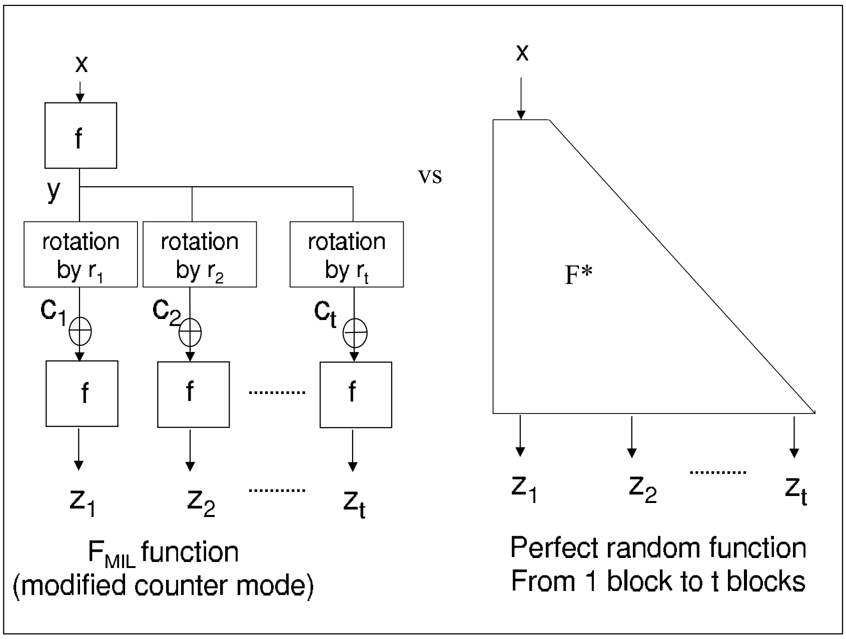

Figure 3: The MILENAGE modified counter mode construction

in the MILENAGE design and evaluation report [Mi00]. Let us also ignore the involvement of the OPc constant, and let us focus on the structure of the one block to t block construction allowing to derive the output blocks z_1 to z_4 from the input block x . This construction consists of a prewhitening computation, using E_K, of an intermediate block y, followed by applying to y a slight variant (involving some circular rotations) of the counter mode construction.

More formally, given any random permutation f over $\{0,1\}^n$, the 1 block to t blocks function $F_{MIL}(f)$ associated with the MILENAGE construction is defined as follows (cf Figure 3):

$$F_{MIL}(f) : \{0,1\}^n \rightarrow \{0,1\}^{nt} \qquad x \mapsto (z_1, \cdots, z_t)$$

$$\texttt{where } z_k = f(rot(f(x), r_k) \oplus c_k) \texttt{ for } k = 1 \texttt{ to } t$$

A detailed statement and proof of the pseudorandomness of the MILENAGE construction are given in Theorem 2 in the next Section. Theorem 2 confirms, with slightly tighter indistinguishability bounds, the claim concerning the pseudorandomness of this construction stated (without the underlying proof) in the MILENAGE design and evaluation report [Mi00].

3.3 Modified OFB construction

Figure 4 represents a one block to t blocks mode of operation of an n-bit permutation f which structure consists of a prewhitening computation of f providing an intermediate value y, followed by an OFB expansion of y.

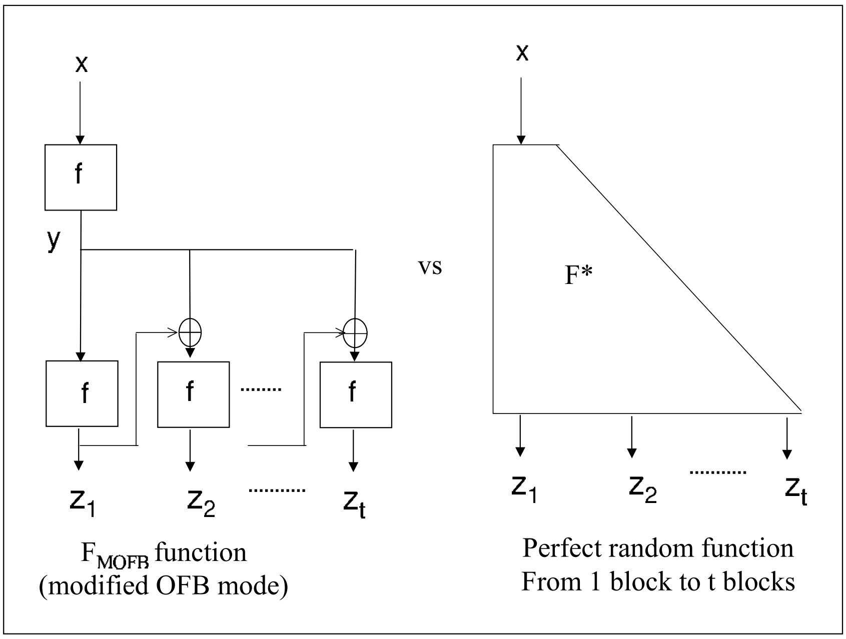

Figure 4: The modified OFB mode of operation

More formally, the $F_{MOFB}(f)$ expansion function associated with the modified OFB construction of Figure 4 is defined as follows:

$$F_{MOFB}(f) : \{0,1\}^n \rightarrow \{0,1\}^{nt} \qquad x \mapsto (z_1, \cdots, z_t)$$

$$\texttt{where } z_1 = f((f(x)) \texttt{ and } z_k = f(f(x) \oplus z_{k-1}) \texttt{ for } k = 2 \texttt{ to } t$$

A short proof of the pseudorandomness of this modified OFB construction is given in Section 5 hereafter.

It is worth noticing that the construction of the above modified OFB mode operation is identical to the one of the ANSI X9.17 PRG mode of operation introduced by Desai et al in [DHY02], so that the pseudorandomness proof (related the associated expansion function) provided in Section 5 is to some extent complementary to the pseudorandomness proof (related to the the associated state transition function) established in [DHY02]. The modified OFB mode of operation is also similar to the keystream generation mode of operation of the KASUMI blockcipher used in the UMTS encryption function f8 [Ka00], up to the fact that in the f8 mode, two additional precautions are taken: the key used in the prewhitening computation differs from the one in the rest of the computations, and in order to prevent collisions between two output blocks from resulting in short cycles in the produced keystream sequence, a mixture of the OFB and counter techniques is applied.

4 Analysis of the modified counter mode used in MILENAGE

In this Section we proof that if some conditions on the constants $c_k, k \in \{1 \cdots t\}$ and $r_k, k \in \{1 \cdots t\}$ encountered in the MILENAGE construction of Section 3 are satisfied, then the one block to t blocks expansion function $F_{MIL}(f*)$ resulting from applying this construction to the perfect random one-block permutation f^* is indistinguishable from a perfect random function of $F_{n,tn}$, even if the product of t and the number of queries q is large.

In order to formulate conditions on the constants c_k and r_k, we need to introduce some notation:

- the left circular rotations of a n-bit word w by r bits is denoted by $rot(w, r)$. Rotation amounts (parameter r) are implicitly taken modulo n.
- for any $GF(2)$-linear function $L : \{0,1\}^n \mapsto \{0,1\}^n$, $Ker(L)$ and $Im(L)$ respectively denote the kernel and image vector spaces of L.

With the above notation, these conditions can be expressed as follows:

$$\begin{array}{ll} \forall k, l \in \{1 \cdots t\} k \neq l \Rightarrow (c_k \oplus c_l) \notin Im(L) & \qquad (C) \\ \texttt{where } L = rot(., r_k) \oplus rot(., r_l) & \end{array}$$

The purpose of the above condition is to ensure that for any $y \in \{0,1\}^n$ and any two distinct integers k and $l \in \{1 \cdots t\}$, the values $rot(y, r_k) \oplus c_k$ and $rot(y, r_l) \oplus c_l$ be distinct. If t is less than 2^n, it is easy to find constants c_k and r_k satisfying condition (C) above. In particular, if one takes all r_k equal to zero, condition (C) boils down to requiring that the c_i constants be pairwise distinct.

Theorem 2 *Let n be a fixed integer. Denote by f^* a perfect random permutation of I_n. Let $F = F_{MIL}(f^*)$ denote the random function of $F_{n,tn}$ obtained by applying the MILENAGE construction of Figure 3 to f^*, and F^* denote a perfect random function of $F_{n,t \cdot n}$. If the constants c_k and r_k $(k = 1 \cdots t)$ of the construction satisfy condition (C) above, then for any distinguishing algorithm A using any fixed number q of queries such that $\frac{t^2q^2}{2^n} \leq \frac{1}{6}$ we have*

$$Adv_A(F, F^*) \leq \frac{t^2q^2}{2^{n+1}}$$

Proof Let us X denote the set of q-tuples $\mathbf{x} = (x^1, \cdots, x^q)$ of pairwise distinct I_n values and Z denote the set of q-tuples $\mathbf{z} = (z^1 = (z_1^1, \cdots, z_t^1), z^2 = (z_1^2, \cdots, z_t^2), \cdots, z^q = (z_1^q, \cdots, z_t^q))$ of pairwise distinct I_{nt} values, such that the tq values $z_1^1, \cdots, z_t^1, \cdots, z_1^q, \cdots, z_t^q$ be pairwise distinct. We want to show that there exist positive real numbers ϵ_1 and ϵ_2 such that:

$$|Z| > (1 - \epsilon_1)|I_{nt}|^q \qquad (i)$$

and

$$\forall \mathbf{x} \in X \forall \mathbf{z} \in Z Pr[x \overset{F}{\mapsto} z] \geq (1 - \epsilon_2) \cdot \frac{1}{|I_{nt}|^q} \qquad (ii)$$

so that that Theorem 1 can be applied.

We have

$$\begin{aligned}
\frac{|Z|}{|I_{nt}|^q} &= \frac{2^n \cdot (2^n-1) \cdots (2^n - tq + 1)}{2^{nqt}} \\
&= 1 \cdot (1 - \frac{1}{2^n}) \cdots (1 - \frac{qt-1}{2^n}) \\
&\geq 1 - \frac{1}{2^n} \cdot (1 + 2 + \cdots + (qt-1))
\end{aligned}$$

Since $\frac{1}{2^n} \cdot (1+2+\cdots+(qt-1)) = \frac{(qt-1)qt}{2^{n+1}} \leq \frac{q^2t^2}{2^{n+1}}$, we have $|Z| > (1-\epsilon_1)|I_{nt}|^q$, with $\epsilon_1 = \frac{q^2t^2}{2^{n+1}}$.

Let us now show that for any fixed q-tuple of I_n values $\mathbf{x} \in X$ and any q-tuple of I_{nt} values $\mathbf{z} \in Z$, we have $Pr[\mathbf{x} \overset{F}{\mapsto} \mathbf{z}] \geq \frac{1}{2^{ntq}}$.

For that purpose, let us consider from now on any two fixed q-tuples $\mathbf{x} \in X$ and $\mathbf{z} \in Z$. Let us denote by Y the set of q-tuples of pairwise distinct I_n values $\mathbf{y} = (y^1, .., y^q)$. We can partition all the possible computations $\mathbf{x} \overset{F}{\mapsto} \mathbf{z}$ according to the intermediate value $\mathbf{y} = (f^*(x^1), \cdots, f^*(x^q))$ in the F computation.

$$Pr[\mathbf{x} \overset{F}{\mapsto} \mathbf{z}] = \sum_{\mathbf{y} \in Y} Pr[\mathbf{x} \overset{f^*}{\mapsto} \mathbf{y} \wedge \forall i \in \{1..q\} \forall k \in \{1..t\} (rot(y^i, r_k) \oplus c_k) \overset{f^*}{\mapsto} z^i_k]$$

Let us denote by Y' the Y subset of those values $\mathbf{y}$ satisfying the three following additional conditions, which respectively express the requirement that all the f^* input values encountered in the q F computations be pairwise distinct (first and second condition), and that all the f^* outputs encountered in the same computations be also pairwise distinct (third condition).

(I) $\forall i \in \{1..q\} \forall j \in \{1..q\} \forall k \in \{1..t\} x^i \neq rot(y^j, r_k) \oplus c_k$

(II) $\forall i \in \{1..q\} \forall j \in \{1..q\} \forall k \in \{1..t\} \forall l \in \{1..t\}$
$(i,k) \neq (j,l) \Rightarrow rot(y^i, r_k) \oplus c_k \neq rot(y^j, r_l) \oplus c_l$

(III) $\forall i \in \{1..q\} \forall j \in \{1..q\} \forall k \in \{1..t\} y^i \neq z^j_k$

We have

$$Pr[\mathbf{x} \overset{F}{\mapsto} \mathbf{z} \geq \sum_{\mathbf{y} \in Y'} Pr[\mathbf{x} \overset{f^*}{\mapsto} \mathbf{y} \wedge \forall i \in \{1..q\} \forall k \in \{1..t\} (rot(y^i, r_k) \oplus c_k) \overset{f^*}{\mapsto} z^i_k]$$

However, if $\mathbf{y} \in Y'$, Property 1 of Section 2 can be applied to the $(t+1)q$ pairwise distinct f^* input values $x^i, i \in \{1..q\}$ and $rot(y^i, r_k) \oplus c_k, i \in \{1..q\}, k \in \{1..t\}$ and to the $(t+1)q$ distinct output values $x^i, i \in \{1..q\}$ and $z^i_k, i \in \{1..q\}, k \in \{1..t\}$, so that

$$\begin{aligned}
Pr[\mathbf{x} \overset{f^*}{\mapsto} \mathbf{y} \wedge \forall i \in \{1..q\} \forall k \in \{1..t\} (rot(y^i, r_k) \oplus c_k) \overset{f^*}{\mapsto} z^i_k] &= \tfrac{(|I_n| - (t+1)q)!}{I_n!} \\
&= \tfrac{(2^n - (t+1)q)!}{2^n!}
\end{aligned}$$

Therefore, $Pr[\mathbf{x} \overset{F}{\mapsto} \mathbf{z}] \geq |Y'| \frac{(2^n - (t+1)q)!}{2^n!}$ (1)

A lower bound on $|Y'|$ can be established, based on the fact that

$$|Y| = \frac{2^n!}{(2^n - q)!} \qquad (2)$$

and on the following properties:

- The fraction of $\mathbf{y}$ vectors of Y such that condition (I) is not satisfied is less than $\frac{q^2 t}{2^n}$ since for any fixed $i \in \{1..q\}, j \in \{1..q\}$ and $k \in \{1..t\}$ the number of $\mathbf{y} \in Y$ q-tuples such that $x^i = rot(y^j, r_k) \oplus c_k$ is $(2^n - 1) \cdots (2^n - q + 1) = \frac{|Y|}{2^n}$ and the set of the $\mathbf{y}$ vectors of Y such that condition (I) is not satisfied is the union set of these $q^2 t$ sets.

- The fraction of $\mathbf{y}$ vectors of Y such that condition (III) is not satisfied is less than $\frac{q^2 t}{2^n}$, by a similar argument.

- The fraction of $\mathbf{y}$ vectors of Y such such that condition (II) is not satisfied is upper bounded by $\frac{q(q-1)}{2} \cdot \frac{t(t-1)}{2} \cdot \frac{1}{2^n - 1}$. As a matter of fact, given any two distinct pairs $(i, k) \neq (j, l)$ of $\{1 \cdots q\} \times \{1 \cdots t\}$, we can upper bound the number of $\mathbf{y}$ vectors of Y such that $rot(y^i, r_k) \oplus c_k = rot(y^j, r_l) \oplus c_l$ by distinguishing the three following cases:

  case 1: $i = j$ and $k \neq l$. Since condition (C) on the constants involved in F is satisfied, there exists no $\mathbf{y}$ vector of Y such that $rot(y^i, r_k) \oplus c_k = rot(y^i, r_l) \oplus c_l$. So case 1 does never occur.

  case 2: $i \neq j$ and $k = l$. For any $\mathbf{y}$ vector of Y, $y^i \neq y^j$. But the $rot(\cdot, r_k) \oplus c_k$ GF(2)-affine mapping of I_n is one to one. Thus, $rot(y^i, r_k) \oplus c_k \neq rot(y^j, r_k) \oplus c_k$. In other words, case 2 does never occur.

  case 3: $i \neq j$ and $k \neq l$ The number of Y q-tuples such that $rot(y^i, r_k) \oplus c_k = rot(y^j, r_l) \oplus c_l$ is $2^n \cdot (2^n - 2) \cdot (2^n - 2) \cdot (2^n - 3) \cdots (2^n - q + 1) = \frac{|Y|}{2^n - 1}$.

  Consequently, the set of $\mathbf{y}$ vectors of Y such such that condition (II) is not satisfied is the union set of the $\frac{q(q-1)}{2} \cdot \frac{t(t-1)}{2}$ sets of cardinal $\frac{|Y|}{2^n - 1}$ considered in case 3, so that the fraction of $\mathbf{y}$ vectors of Y such such that condition (II) is not satisfied is upper bounded by $\frac{q(q-1)}{2} \cdot \frac{t(t-1)}{2} \cdot \frac{1}{2^n - 1}$, as claimed before.

As a consequence of the above properties, the overall fraction of the Y vectors which do not belong to Y' is less than $\frac{2q^2 t}{2^n} + \frac{q(q-1)}{2} \cdot \frac{t(t-1)}{2} \cdot \frac{1}{2^n - 1}$, i.e.

$$|Y'| \geq (1 - (\frac{2q^2 t}{2^n} + \frac{q(q-1)}{2} \frac{t(t-1)}{2} \frac{1}{2^n - 1}))|Y| \qquad (3)$$

Now (1) (2) and (3) result in the following inequality:

$$Pr[x \overset{F}{\mapsto} z] \geq (1 - (\frac{2q^2 t}{2^n} + \frac{q(q-1)}{2} \cdot \frac{t(t-1)}{2} \cdot \frac{1}{2^n - 1})) \cdot \frac{(2^n - (t+1)q)!}{(2^n - q)!}$$

The $\frac{(2^n - (t+1)q)!}{(2^n - q)!}$ term of the above expression can be lower bounded as follows

$$\begin{aligned} \frac{(2^n-(t+1)q)!}{(2^n-q)!} &= \frac{1}{(2^n-q)(2^n-q-1)\cdots(2^n-((t+1)q-1))} \\ &= \frac{1}{2^{ntq}}\cdot\frac{1}{(1-\frac{q}{2^n})\cdot(1-\frac{q+1}{2^n})\cdots(1-\frac{(t+1)q-1}{2^n})} \\ &\geq \frac{1}{2^{ntq}}\cdot(1+\frac{q}{2^n})\cdot(1+\frac{q+1}{2^n})\cdots(1+\frac{(t+1)q-1}{2^n}) \\ &\quad \texttt{(due to the fact that if } u<1, \frac{1}{1-u}\geq 1+u) \\ &\geq \frac{1}{2^{ntq}}\cdot(1+\frac{q}{2^n}+\frac{q+1}{2^n}+\cdots+\frac{(t+1)q-1}{2^n}) \\ &= \frac{1}{2^{ntq}}(1+tq\frac{(t+2)q-1}{2^n}) \end{aligned}$$

Thus we have

$$\begin{aligned} Pr[\mathbf{x}\overset{F}{\mapsto}\mathbf{z}] &\geq \frac{1}{2^{ntq}}(1-(\frac{2q^2t}{2^n}+\frac{q(q-1)}{2}\cdot\frac{t(t-1)}{2}\cdot\frac{1}{2^n-1}))\cdot(1+tq\frac{(t+2)q-1}{2^n}) \\ &= \frac{1}{2^{ntq}}(1+\varepsilon)(1-\varepsilon') \\ \texttt{where } \varepsilon &\triangleq tq\frac{(t+2)q-1}{2^n} \\ \texttt{and } \varepsilon' &\triangleq \frac{2q^2t}{2^n}+\frac{q(q-1)}{2}\cdot\frac{t(t-1)}{2}\cdot\frac{1}{2^n-1} \end{aligned}$$

Let us show that $\varepsilon > \frac{4}{3}\varepsilon'$. Due to the inequality $\frac{1}{2^n-1}\leq\frac{2}{2^n}$, we have

$$\varepsilon' \leq \frac{qt}{2^{n+1}}(qt+3q-t+1)$$

On the other hand, ε can be rewritten

$$\varepsilon = \frac{qt}{2^{n+1}}(2qt+4q-2)$$

Therefore

$$\begin{aligned} \varepsilon-\frac{4}{3}\varepsilon' &\geq \frac{qt}{2^{n+1}}(\frac{2}{3}qt+\frac{4}{3}t-\frac{10}{3}) \\ &\geq 0 \texttt{ since } t\geq 2 \texttt{ and } q\geq \texttt{ imply } (\frac{2}{3}qt+\frac{4}{3}t-\frac{10}{3})\geq 0 \end{aligned}$$

Moreover, it is easy to see (by going back to the definition of ε and using the fact that $t\geq 2$) that $\varepsilon\leq\frac{2t^2q^2}{2^n}$, so that the condition $\frac{t^2q^2}{2^n}\leq\frac{1}{6}$ implies $\varepsilon\leq\frac{1}{3}$.

The relations $\varepsilon\geq\frac{4}{3}\varepsilon'$ and $\varepsilon\leq\frac{1}{3}$ imply $(1+\varepsilon)(1-\varepsilon')\geq 1$ As a matter of fact

$$\begin{aligned} (1+\varepsilon)(1-\varepsilon') &= 1+\varepsilon-\varepsilon'-\varepsilon\varepsilon' \\ &\geq 1+\varepsilon-\varepsilon'-\frac{\varepsilon'}{3} \\ &= 1+\varepsilon-\frac{4}{3}\varepsilon' \\ &\geq 1 \end{aligned}$$

Thus we have shown that $Pr[\mathbf{x} \overset{F}{\mapsto} \mathbf{z}] \geq \frac{1}{2^{ntq}}$.

We can now apply Theorem 1 with $\epsilon_1 = \frac{q^2t^2}{2^{2^{n+1}}}$ and $\epsilon_2 = 0$, so that we obtain the upper bound

$$Adv_A(F, F^*) \leq \frac{q^2t^2}{2^{n+1}} \qquad \texttt{QED}$$

The unconditional security result of Theorem 2 is easy to convert (using a standard argument) to a computational security analogue.

Theorem 3 *Let f denote any random permutation of I_n. Let $F = F_{MIL}(f)$ denote the random function of $F_{n,tn}$ obtained by applying to f the MILENAGE construction of Figure 3 (where the constants c_k and r_k ($k = 1 \cdots t$) are assumed to satisfy condition (C)). Let F^* denote a perfect random function of $F_{n,t \cdot n}$. For any q number of queries such that $\frac{t^2q^2}{2^n} \leq \frac{1}{6}$, if there exists $\varepsilon > 0$ such that for any testing algorithm T with $q(t+1)$ queries and less computational resources (e.g. time, memory, etc.) than any fixed finite or infinite bound R the advantage $Adv_T(f, f^*)$ of T in distinguishing f from a perfect n-bit random permutation $f*$ be such that $Adv_T(f, f^*) < \varepsilon$, then for any distinguishing algorithm A using q queries and less computational resources than R,*

$$Adv_A(F, F^*) < \varepsilon + \frac{t^2q^2}{2^{n+1}}$$

Proof Let us show that if there existed a testing algorithm A capable to distinguish $F_{MIL}(f)$ from a perfect random function F^* of $F_{n,nt}$ with an advantage $|p - p^*|$ better than $\varepsilon + \frac{q^2t^2}{2^{n+1}}$ using less computational resources than R, then there would exist a testing algorithm T allowing to distinguish f from a perfect random permutation with $q(t+1)$ queries and less computational resources than R with a distinguishing advantage better that ϵ. The test T of a permutation φ would just consist in performing the test A on $F_{MIL}(\varphi)$. The success probability p' of the algorithm A applied to $F(f^*)$ would be such that $|p' - p^*| \leq \frac{q^2t^2}{2^{n+1}}$ (due to Theorem 2), and therefore, due to the triangular inequality $|p - p'| + |p' - p^*| \geq |p - p^*|$, one would have $|p - p'| \geq \varepsilon$, so that the advantage of T in distinguishing f from f^* would be at least ε QED.

The following heuristic estimate of the success probability of some simple distinguishing attacks against the MILENAGE mode of operation indicates that the $\frac{q^2t^2}{2^{n+1}}$ bound obtained in Theorem 2 is very tight, at least in the case where the r_i rotation amounts are equal to zero. Let us restrict ourselves to this case. Let us consider a $z = (z^1, \cdots, z^q)$ q-tuple of F_{MIL} output value, where each z^i represents a t-tuple of distinct I_n values $z^i_1, \cdots, z^i_t$ Given any two distinct indexes i and j, the occurrence probability of a collision of the form $z^i_k = z^j_l$ can be approximated (under heuristic assumptions) by $\frac{t^2}{2^n}$, so that the overall collision probability among the qt output blocks of F_{MIL} is about $\frac{q(q-1)}{2}\frac{t^2}{2^n}$. Moreover, each collision represents a distinguishing event with an overwhelming probability, due to the fact that $z^i_k = z^j_l$ implies $z^j_k = z^i_l$. Thus the distinguishing probability given by this "attack" is less than (but close to)$\frac{q^2t^2}{2^{n+1}}$. This does not hold in the particular case where $q = 1$, but in this case then another statistical bias, namely the fact that no collisions never occur among the t output blocks, provides a distinguishing property of probability about $\frac{t(t-1)}{2^{n+1}}$, which is again close to $\frac{q^2t^2}{2^{n+1}}$.

5 Analysis of the modified OFB mode of operation

The following analogue of Theorem 2 above can be established for the modified OFB mode of operation (cf Figure 4) introduced in Section 3 .

Theorem 4 *Let n be a fixed integer. Denote by f^* a perfect random permutation of I_n. Let $F = F_{MOFB}(f^*)$ denote the random function of $F_{n,tn}$ obtained by applying the modified construction of Figure 4 to f^*, and F^* denote a perfect random function of $F_{n,t \cdot n}$. For any distinguishing algorithm A using any fixed number of queries q such that $\frac{t^2q^2}{2^n} \leq 1$ we have*

$$Adv_A(F, F*) \leq \frac{7t^2q^2}{2^{n+1}}$$

Proof sketch: the structure of the proof is the same as for the MILENAGE construction. We consider the same X and Z sets of q-tuples as in Section 4. As established in Section 4, $|Z| \geq (1 - \epsilon_1)$, where $\epsilon_1 = \frac{q^2t^2}{2^{n+1}}$. For any fixed $\mathbf{x} \in X$ and $\mathbf{z} \in Z$ q-tuples of input and output values, it can be shown that $Pr[\mathbf{x} \overset{F_{MOFB}(f*)}{\mapsto} \mathbf{z}] \geq \frac{1}{2^{ntq}}(1 - \epsilon_2)$, with $\epsilon_2 = \frac{3q^2t^2}{2^n}$. We can now apply Theorem 1 with $\epsilon_1 = \frac{q^2t^2}{2^{n+1}}$ and $\epsilon_2 = \frac{3q^2t^2}{2^n}$, so that we obtain the upper bound

$$Adv_A(F, F*) \leq \frac{7q^2t^2}{2^{n+1}} \qquad \texttt{QED}$$

6 Conclusion

We have given some evidence that although “one-block-to-many” modes of operation of blockciphers are not as well known and systematically studied so far as “many-blocks-to-one” MAC modes, both kinds of modes are of equal significance for applications such as mobile communications security. We have given security proofs, in the Luby-Rackoff security paradigm, of two simple one to many blocks modes, in which all invocations of the underlying blockciphers involve the same key. We believe that the following topics would deserve some further research:

- systematic investigation of alternative one to many blocks modes, e.g. modes involving more than one key, or modes providing security “beyond the bithday paradox” ;
- formal proofs of security for hybrid modes of operation including an expansion function, for instance for the combination of the expansion function $x \mapsto (z_1, z_2, z_3, z_4)$ and the message authentication function $(x, y) \mapsto z_0$ provided by the complete MILENAGE construction.

Acknowledgements

I would like to thank Steve Babbage, Diane Godsave and Kaisa Nyberg for helpful comments on a preliminary version of the proof of Theorem 2. I would also like to thank Marine Minier for useful discussions at the beginning of this work.

References

[BDJR97] M. Bellare, A. Desai, E. Jokipii, P. Rogaway, " A Concrete Security Treatment of Symmetric Encryption: Analysis of the DES Modes of Operation", Proceedings of 38th Annual Symposium on Foundations of Computer Science, IEEE, 1997.

[BKR94] M. Bellare, J. Kilian, P. Rogaway, "The Security of Cipher Block Chaining". , Advances in Cryptology - CRYPTO'94, LNCS 839, p. 341, Springer-Verlag, Santa Barbara, U.S.A., 1994.

[BM84] M. Blum, S. Micali, "How to Generate Cryptographically Strong Sequences of Pseudo-Random Bits" SIAM J. Comput. 13(4), p. 850-864, 1984

[BR00] J. Black, P. Rogaway, "A Block-Cipher Mode of Operation for Parallelizable Message Authentication", Advances in Cryptology Eurocrypt 2002, Lecture Notes in Computer Science, Vol. 2332, Springer-Verlag, pp. 384397, 2002.

[DHY02] A. Desai, A. Hevia, Y. Yin, "A Practice-Oriented Treatment of Pseudorandom Number Generators", Eurocrypt 2002, Lecture Notes in Computer Science, Vol. 2332, Springer-Verlag, 2002.

[EJ02] P. Ekdahl, T. Johansson, "A new version of the stream cipher SNOW", proceedings of SAC'02.

[GL89] O.Goldreich, L.Levin, "A hard-core predicate for all one-way functions", Proc. ACM Symp. on Theory of Computing, pp. 25-32, 1989

[HCCJ02] S. Halevi, D. Coppersmith, C.S. Jutla,"Scream: A Software-Efficient Stream Cipher", Advances in Cryptology - FSE 2002, p. 195-209, Springer Verlag, 2002.

[HN00] J. Hastad and M. Näslund, "BMGL: Synchronous Key-stream Generator with Provable security", Revision 1, March 6, 2001) and "A Generalized Interface for the NESSIE Submission BGML", March 15, 2002, available at http://www.cosic.esat.kuleuven.ac.be/nessie/

[JJV02] E. Jaulmes, A. Joux, F. Valette, " On the Security of Randomized CBC-MAC Beyond the Birthday Paradox Limit: A New Construction.", Advances in Cryptology - FSE 2002, p. 237-251, Springer Verlag, 2002, and iacr eprint archive 2001/074

[Ka00] 3rd Generation Partnership Project - Specification of the 3GPP confidentiality and integrity algorithms ; Document 2 (TS 35.202): KASUMI algorithm specification ; Document 1:TS 35.201 f8 and f9 specifications ; Docment TR 33.904: Report on the Evaluation of 3GPP Standard Confidentiality and Integrity Algorithms, available at http://www.3gpp.org

[LR88] M. Luby, C. Rackoff, “How to Construct Pseudorandom Permutations from Pseudorandom Function”, Siam Journal on Computing , vol. 17, p. 373, 1988.

[Ma92] U. Maurer, ”A Simplified and generalised treatment of Luby-Rackoff Pseudo-random Permutation Generators”, Advances in Cryptology - Eurocrypt’92, LNCS 658 , p. 239, Springer Verlag, 1992.

[Mi00] 3rd Generation Partnership Project - Specification of the MILENAGE algorithm set: An example algorithm Set for the 3GPP Authentication and Key Generation functions f1, f1*, f2, f3, f4, f5 and f5* - Document 2 (TS 35.206): Algorithm specification ; Document 5 (TR 35.909): Summary and results of design and evaluation, available at http://www.3gpp.org

[Pa91] J. Patarin, “Etude de Générateurs de Permutation Basés sur le Schéma du D.E.S.”, Phd. Thesis, University of Paris VI, 1991.

[Pa92] J. Patarin, “How to Construct Pseudorandom and Super Pseudorandom Permutations from One Single Pseudorandom Function”, Advances in Cryptology - Eurocrypt’92, LNCS 658 , p. 256, Springer Verlag, 1992.

[PR00] E. Petrank, C. Rackoff,“CBC MAC for Real-Time Data Sources”, Journal of Cryptology 13(3), p. 315–338, 2000

[RC98] P. Rogaway, D. Coppersmith, “A Software-Optimized Encryption Algorithm”, Journal of Cryptology 11(4), p. 273-287, 1998

[Va98] S. Vaudenay, “Provable Security for Block Ciphers by Decorrelation”, STACS’98, Paris, France,Lecture Notes in Computer Science No. 1373, p. 249-275, Springer-Verlag, 1998.

[Va99] S. Vaudenay, “On Provable Security for Conventional Cryptography”, Proc. ICISC’99, invited lecture.

Appendix: A short proof of Theorem 1

Let us restrict ourselves to the case of any fixed deterministic algorithm A which uses q adaptively chosen queries (the generalization to the case of a probabilistic algorithm is easy).

A has the property that if the q-tuple of outputs encountered during an A computation is $\mathbf{y} = (y^1, \cdots, y^q)$, the value of the q-tuple $\mathbf{x} = (x^1, \cdots, x^q)$ of query inputs encountered during this computation is entirely determined. This is easy to prove by induction: the initial query input x^1 is fixed ; if for a given A computation the first query output is y^1, then x^2 is determined, etc.. We denote by $\mathbf{x}(\mathbf{y})$ the single q-tuple of query inputs corresponding to any possible $\mathbf{y}$ q-tuple of query outputs, and we denote by S_A the subset of those $\mathbf{y} \in {I_m}^q$ values such that if the q-tuples $\mathbf{x}(\mathbf{y})$ and $\mathbf{y}$ of query inputs and outputs are encountered in a A computation, then A outputs the answer 1.

The probabilities p and p^* can be expressed using S_A as

$p = \sum_{\mathbf{y} \in S_A} Pr[\mathbf{x}(\mathbf{y}) \overset{F}{\mapsto} \mathbf{y}]$ and

$p^* = \sum_{\mathbf{y} \in S_A} Pr[\mathbf{x}(\mathbf{y}) \overset{F^*}{\mapsto} \mathbf{y}]$

We can now lower bound p using the following inequalities:

$p \geq \sum_{\mathbf{y} \in S_A \cap Y} (1-\epsilon_2) \cdot Pr[\mathbf{x}(\mathbf{y}) \overset{F^*}{\mapsto} \mathbf{y}]$ due to inequality (ii)

$\geq \sum_{\mathbf{y} \in S_A} (1-\epsilon_2) \cdot Pr[\mathbf{x}(\mathbf{y}) \overset{F^*}{\mapsto} \mathbf{y}] - \sum_{\mathbf{y} \in {I_m}^q - Y} (1-\epsilon_2) \cdot Pr[\mathbf{x}(\mathbf{y}) \overset{F^*}{\mapsto} \mathbf{y}]$

But $\sum_{\mathbf{y} \in S_A} (1-\epsilon_2) \cdot Pr[\mathbf{x}(\mathbf{y}) \overset{F^*}{\mapsto} \mathbf{y}] = (1-\epsilon_2) \cdot p^*$

and

$\sum_{\mathbf{y} \in {I_m}^q - Y} (1-\epsilon_2) \cdot Pr[\mathbf{x}(\mathbf{y}) \overset{F^*}{\mapsto} \mathbf{y}] = (1-\epsilon_2) \cdot \frac{|I_m|^q - |Y|}{|I_m|^q} \leq (1-\epsilon_2) \cdot \epsilon_1$ due to inequality (i).

Therefore, $p \geq (1-\epsilon_2)(p^* - \epsilon_1) = p^* - \epsilon_1 - \epsilon_2 \cdot p^* + \epsilon_1 \cdot \epsilon_2$

thus finally (using $p^* \leq 1$ and $\epsilon_1 \cdot \epsilon_2 \geq 0$)

$p \geq p* - \epsilon_1 - \epsilon_2$ (a)

If we now consider the distinguisher A' which outputs are the inverse of those of A (i.e. A' answers 0 iff A answers 1), we obtain an inequality involving this time $1-p$ and $1-p^*$:

$(1-p) \geq (1-p^*) - \epsilon_1 - \epsilon_2$ (b)

Combining inequalities (a) and (b), we obtain $|p - p^*| \leq \epsilon_1 + \epsilon_2$ QED.