Blockwise Adversarial Model for On-line Ciphers and Symmetric Encryption Schemes

Pierre-Alain Fouque[1], Antoine Joux[2], and Guillaume Poupard[2]

[1] École normale supérieure, Département d'Informatique, 45 rue d'Ulm, 75230 Paris 5, France, Pierre-Alain.Fouque@ens.fr

[2] DCSSI CryptoLab, 51, rue de Latour-Maubourg, 75007 Paris SP, France, Antoine.Joux@m4x.org, Guillaume.Poupard@m4x.org

Abstract. This paper formalizes the security adversarial games for *on-line* symmetric cryptosystems in a unified framework for deterministic and probabilistic encryption schemes. On-line encryption schemes allow to encrypt messages even if the whole message is not known at the beginning of the encryption. The new introduced adversaries better capture the on-line properties than *classical* ones. Indeed, in the new model, the adversaries are allowed to send messages block-by-block to the encryption machine and receive the corresponding ciphertext blocks on-the-fly. This kind of attacker is called *blockwise* adversary and is stronger than standard one which treats messages as atomic objects.

In this paper, we compare the two adversarial models for on-line encryption schemes. For probabilistic encryption schemes, we show that security is not preserved contrary to for deterministic schemes. We prove in appendix of the full version that in this last case, the two models are polynomially equivalent in the number of encrypted blocks. Moreover in the blockwise model, a polynomial number of *concurrent accesses* to encryption oracles have to be taken into account. This leads to the strongest security notion in this setting. Furthermore, we show that this notion is valid by exhibiting a scheme secure under this security notion.

1 Introduction

In 2002, Joux, Martinet and Valette introduce the *blockwise adaptive attacks* (BA) in [17], in order to better model attackers in the real world. This adversarial model is particularly relevant to study the security of *on-line* schemes where output blocks are viewed gradually by the adversary since for example the whole encrypted message cannot be stored by the encryption machine. Indeed, usually in order to encrypt a message M with a symmetric scheme, M is first split into blocks of the length of the block cipher: $M = M[1]M[2]\dots M[l]$. An encryption scheme is said to be *on-line* if the encryption of the block $M[i]$ only depends on the previous blocks $M[1], M[2], \dots, M[i]$ and not on the next ones $M[i+1]\dots M[l]$. Consequently, the encryption function can compute and return $C[i]$ before the introduction of $M[i+1]\dots M[l]$. There exist a lot of *on-line* encryption schemes such as ECB, CBC, OFB, CFB [19] or OCB [1]. However, some schemes

require a pre-treatment on the whole plaintext before the encryption process [20] or require two encryption passes in two directions [16], and thus are not *on-line*.

In this paper, we propose to study the relations between the security notions in the standard and blockwise models for probabilistic and deterministic on-line encryption schemes.

1.1 Standard vs. Blockwise Adversarial Model

The standard attack model for the CPA security is *message oriented*: *i.e.* the messages are viewed as atomic object which cannot be split into blocks. Thus, adversaries can only be adaptive between the messages. This model correctly captures the interactions of an adversary with an encryption machine for schemes which require the whole plaintext before to start the encryption process or implementations that can record the entire plaintext before the beginning of the encryption.

However, sometimes the encryption process has to be started even if the entire plaintext is not known. For example, in real-time applications, the cryptographic device cannot store the whole plaintext before the starting of the encryption. Consequently, on-line encryption schemes are useful in such scenario. Moreover, in many practical applications, cryptographic devices (smart cards) are memory restricted. Then, if messages are too large, they cannot be stored in the cryptographic module before the beginning of the encryption process. Therefore, the message must be sent block by block to the cryptographic module which returns on-the-fly the output block $C[i]$, say just after the query of the input block $M[i]$ in some implementations. As a consequence, the adversary model needs to be changed to take into account attackers querying messages block by block. In the BA model, attackers are more adaptive than standard adversaries: they are *adaptive during the encryption query*, *i.e.* between each block of messages, and not only *between the encryption queries*, *i.e.* between the messages. Hence the name of "blockwise" adversaries. Obviously the BA model is stronger than the standard one. In the sequel, we respectively denote BCPA and CPA adversaries in the BA and standard models.

It is important to thwart such adversaries since they can lead to theoretical attacks on traditional cryptosystems, such as on the CBC encryption mode or on the authenticated encryption mode presented by Jutla [17]. In [3], Bellare *et al.* have proved that the CBC encryption scheme is secure in the standard model up to the encryption of $2^{n/2}$ blocks, where n denotes the block length of a block cipher. However, in [17], Joux, Martinet and Valette have presented a new simple attack showing that the CBC encryption scheme is not secure in the BA model after only two encrypted blocks. This kind of adversary is mainly meaningful in the private-key setting when long messages are encrypted. It is worth noticing that blockwise adversaries are not only of theoretical interest as the attacks in [17] seem to show. In [17], the attacks invalidate the security proof by building distinguisher but do not allow to recover the secret key or to totally break the scheme. However, it is easy to show that for example the CBC encryption scheme in the BA model is as sensible as the ECB mode in the

standard model against a key recovery attack since the adversary can adapt his queries to the block cipher by xoring its queries to the previous output blocks.

1.2 Backgrounds and Previous Results

Usually, in cryptography, *security notions* are defined by combining a *security goal* and an *attack model* [4]. Different security goals have been proposed so far, such as *indistinguishability of ciphertexts* (IND), *one-wayness*, *non-malleability*,... For example, semantic security [14] formalizes the adversary's inability to learn any information about a plaintext M underlying a challenge ciphertext C. This captures a strong notion of privacy and is also defined as indistinguishability of ciphertexts. In the symmetric setting of interest to us, IND has been redefined as left-or-right (LOR), real-or-random (ROR), and find-then-guess (FTG) indistinguishability. All these latter notions, described in [3], encompass the same security definition. Bellare *et al.* in [3] have defined several security goals, while Katz and Yung, in [18], present a complete characterization of the security notions for encryption scheme in the standard model. Based on these two works, we examine the relations between the standard and the blockwise models.

The blockwise model has been introduced at Crypto 2002 by Joux, Martinet and Valette in [17]. They show that several encryption schemes such as the CBC and IACBC are not secure in the BA model. At FSE 2003, Fouque, Martinet and Poupard in [10] show that a slight variant of the on-line CBC encryption scheme, and the CFB mode of operation can be proved secure against blockwise chosen plaintext attack. For this, they introduce a strong security model. We show here that this model is the strongest one. At SAC 2003, Fouque *et al.* in [9] study the security of authenticated on-line encryption mode against blockwise chosen ciphertext attacks. Finally, at RSA Conf 2004, Boldyreva and Taesombut introduced new security notions for chosen-ciphertext attacks in [6]. We will not here take into account such adversaries due to lack of places.

1.3 Our Results

Several papers have considered blockwise adversaries either in order to attack some schemes such as in [17] or in order to prove security against such adversaries as in [10, 9, 7]. Our aim is to study the relations between the security notions in the standard model and in the blockwise model. Therefore, in section 2 we define more formally several security notions in order to study the relationship between these notions and the related notions in the standard attacker model. Then, in section 3, we study relations between the FTG and LOR security goals for blockwise adaptive chosen plaintext attacks (BCPA) and standard chosen plaintext attacks (CPA). First of all, in theorem 1, we generalize the result stating that security in the standard model does not imply security in the blockwise model. We also show that an equivalence for probabilistic schemes does not hold for on-line encryption schemes against the new adversarial model. In [18], Katz and Yung have mainly analyzed the relations between the non-malleability and the FTG notions for different adversaries having access or not to encryption or

decryption oracles. For the FTG security game, they have proved that oracle accesses only before the challenge phase is equivalent to oracle accesses before and after this phase. We show in theorems 2 and 3 that this equivalence no longer holds in the BA model.

Furthermore, the equivalence of the LOR and FTG security goal is not security preserving. In fact, the main results of Bellare *et al.* in [3] of interest for us about probabilistic schemes are that LOR is the strongest security notion and that LOR and FTG are not security preserving but are polynomially-equivalent in the number of messages. We show in theorem 5 (section 3) that LOR and FTG are *not* security preserving in the BA model. We show that in the BA model two definitions of LOR exist. The stronger one corresponds to adversaries which can *concurrently* access the oracles. This is the strongest security notion we define. Moreover, we also exhibit in section 4 a special class of encryption schemes for which the weakest LOR definition and FTG are exactly equivalent in both models and not only polynomially related (theorems 4 and 6). This allows better reductions for these schemes since security is preserved once we have a security proof under the FTG security notion. Finally, in section 5, we show that the security under concurrent blockwise adversarial can be achieved with the counter mode for example.

In appendix A, we fully characterize the relations between the security of ciphers in the BA model and in the standard one and prove that for on-line ciphers, also known as deterministic schemes, the two models are polynomially-equivalent in the number of encrypted blocks. However, this reduction does not preserve the security since it is quadratic in the number of encrypted blocks. Furthermore, we show that the bound is tight by exhibiting an on-line cipher for which the security in the BA adversary model is not guaranteed if the cipher encrypts more than N blocks although the security in the standard model is preserved up to the encryption of $(N-1)(N-2)/2$ blocks.

1.4 Notations

In the rest of this paper, we use standard notations and conventions for writing probabilistic algorithms and experiments. If A is a probabilistic algorithm, then $A(x_1, x_2, \ldots; r)$ is the result of running A on inputs $x_1, x_2, \ldots$ and coins r. We let $y \leftarrow A(x_1, x_2, \ldots; r)$ denote the experiment of picking r at random and letting y be $A(x_1, x_2, \ldots; r)$. If S is a finite set then $x \leftarrow S$ is the operation of picking an element uniformly from S. We say that y *can be output by* $A(x_1, x_2, \ldots)$ if there is some r such that $A(x_1, x_2, \ldots; r) = y$. If $p(x_1, x_2, \ldots)$ is a predicate, the notation $\Pr[x_1 \leftarrow S; x_2 \leftarrow A(x_1, y_2, \ldots); \ldots : p(x_1, x_2, \ldots)]$ denotes the probability that $p(x_1, x_2, \ldots)$ is true after ordered execution of the listed experiments. In the sequel, q denotes the number of message queries and μ denotes the total number of blocks queried. We note by $D_{d,n}$ the set of d-bit strings, where d is a multiple of n, and by Perm_n, the set of permutations on n-bit blocks.

2 Security notions for on-line encryption schemes

2.1 Description of on-line encryption schemes

We assume that if $C = C[0] \dots C[l]$ is the encryption of $M = M[1]M[2] \dots$, then $C[0]$ represents some information used to randomize the encryption process such as the initialization vector in the CBC encryption mode. Encryption of $M[i]$ is denoted by $C[i]$. This formalism is not restrictive and most of the encryption schemes satisfy it. Moreover, it can be adapted to more exotic schemes.

A *(symmetric) on-line encryption scheme* $\mathcal{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ consists in three algorithms.

- The randomized *key generation* algorithm $\mathcal{K}$ takes as input a security parameter $k \in \mathsf{N}$ and returns a key k; we write $\mathsf{k} \xleftarrow{R} \mathcal{K}(k)$.
- The *encryption* algorithm $\mathcal{E}$ can be randomized or stateful. It takes the key k and a *plaintext* M and returns a *ciphertext* C; we write $C \xleftarrow{R} \mathcal{E}_{\mathsf{k}}(M)$. (If randomized it flips new coins on each invocations. If stateful, it uses and then updates a state that is maintained across invocations such as a counter.) Moreover, *on-line* encryption schemes can encrypt block $M[i]$ using only $M[1], M[2], \dots, M[i]$.
- The *decryption* algorithm $\mathcal{D}$ is deterministic and stateless. It takes the key k and a string C and returns either the corresponding plaintext M or the symbol $\perp$; we write $x \leftarrow \mathcal{D}_{\mathsf{k}}(C)$ where $x \in \{0,1\}^* \cup \{\perp\}$. We require that $\mathcal{D}_{\mathsf{k}}(\mathcal{E}_{\mathsf{k}}(M)) = M$ for all $M \in \{0,1\}^*$. Moreover, on-line decryption can decrypt $C[i]$ only using $C[0], \dots, C[i]$.

2.2 Security notions for on-line encryption schemes

In this section, we adapt the standard security notions for symmetric encryption schemes to the BA model. Find-Then-Guess. Semantic security captures the intuitive notion of privacy for an encrypted text. The formulation of semantic security stipulates that given a ciphertext, a polynomially-bounded adversary cannot gain any information about the corresponding plaintext (except maybe its length). The Find-Then-Guess (FTG) goal is an equivalent security notion, as shown in [3]. The adversary A, viewed as three sub-adversaries $A = (A_1, A_c, A_2)$, tries to win the following game: in the find phase, A_1 tries to get some information and returns some state information in s_0. Then in the challenge phase, A_c gradually submits two messages M_0 and M_1 to the encryption oracle which chooses a random bit b at the beginning of the encryption process, encrypts the blocks of M_b and returns the corresponding blocks C_b to A_c in an interactive manner. Finally in the guess phase, A_2 tries to distinguish whether C_b is the encryption of M_0 or M_1. In the standard model, the adversary A_1 chooses the messages M_0 and M_1. In the BA model, we need to assume that in some cases, the two messages are chosen by the adversary A_c since this new attacker is more

adaptive and can choose the two messages either at the beginning of the challenge phase or during it. We add the adversary A_c in order to take into account the two adversarial models in a single definition.

In the FTG game, A may have access to different oracles during each phase. To avoid obfuscating security notions, we only define the three most representative notions: if A is blockwise adaptive in the find phase, then we write BCPA-P1, or in the find and guess phases, then we write BCPA-P2, or during the challenge phase and in the find and guess phases, and then we write BCPA-D. The adversary advantage in winning the FTG game in these different settings for a symmetric scheme Π is given by:

$$\mathsf{Adv}^{\mathrm{ftg-atk}}_{\Pi,A}(k) \stackrel{\mathrm{def}}{=} \left| 2 \cdot \Pr \left[\begin{array}{c} \mathsf{k} \leftarrow \mathcal{K}(1^k); b \leftarrow \{0,1\}; s_0 \leftarrow A_1^{\mathcal{O}_1}(1^k); \\ (M_0, M_1, s_1, C) \leftarrow A_c^{\mathcal{O}_c}(s_0) : \\ A_2^{\mathcal{O}_2}(s_1, M_0, M_1, C) = b \end{array} \right] - 1 \right|$$

where

if atk=BCPA-P1,	then $\mathcal{O}_1 = \mathcal{E}^{\mathrm{bl}}_{\mathsf{k}}(.)$	and $\mathcal{O}_c = \mathcal{E}_{\mathsf{k}}(.,.,b)$	and $\mathcal{O}_2 = \varepsilon$
if atk=BCPA-P2,	then $\mathcal{O}_1 = \mathcal{E}^{\mathrm{bl}}_{\mathsf{k}}(.)$	and $\mathcal{O}_c = \mathcal{E}_{\mathsf{k}}(.,.,b)$	and $\mathcal{O}_2 = \mathcal{E}^{\mathrm{bl}}_{\mathsf{k}}(.)$
if atk=BCPA-D,	then $\mathcal{O}_1 = \mathcal{E}^{\mathrm{bl}}_{\mathsf{k}}(.)$	and $\mathcal{O}_c = \mathcal{E}^{\mathrm{bl}}_{\mathsf{k}}(.,.,b)$	and $\mathcal{O}_2 = \mathcal{E}^{\mathrm{bl}}_{\mathsf{k}}(.)$

We measure as $\mathsf{Adv}^{\mathrm{ftg-atk}}_{\Pi}(k,t,q,\mu) = \max_A\{\mathsf{Adv}^{\mathrm{ftg-atk}}_{\Pi,A}(k)\}$ the security of the scheme Π, where the maximum is over all legitimate A having time-complexity t, making to the oracle at most q encryption queries totaling μ blocks. A secret-key encryption scheme is said to be FTG *-secure against blockwise adaptive chosen plaintext attack* in the FTG sense if for all polynomial-time probabilistic adversaries, the advantage in this guessing game is negligible as a function of the security parameter k.

Left-Or-Right Indistinguishability. In the LOR security goal, the adversary is allowed to make queries of the form (M_0, M_1) where M_0 and M_1 are equal-length messages. Two experiments are considered. In the first one, each query is answered with the encryption of the left message; in the second, the right message is encrypted. Formally, the adversary has access to the *left-or-right* oracle $\mathcal{E}_K(\mathcal{LR}(.,.,b))$, where $b \in \{0,1\}$: it takes as input pairs of messages (M_0, M_1) and, if $b = 0$, it computes $C \leftarrow \mathcal{E}_K(M_0)$ and returns C; else it computes $C \leftarrow \mathcal{E}_K(M_1)$ and returns C. We consider an encryption scheme to be "good" if a "reasonable" adversary cannot obtain "significant" advantage in distinguishing the cases $b = 0$ and $b = 1$ given access to the left-or-right oracle.

In the BA model, adversaries are allowed to feed the oracle block by block. This introduces new interactions since the adversary can interleave encryption blocks for different messages. Consequently, we present two LOR games. In the first game, called LORS, for LOR with sequential message queries, the adversary has to finish an encryption query before requesting the next message. In the second game, called LORC, for LOR with concurrent accesses, the adversary can interleaved the block queries of different messages.

The $\mathcal{E}_{\mathsf{k}}^{\mathrm{bl},s}(M_0[i], M_1[i], b)$ oracle is a LOR-block encryption oracle: the adversary is allowed to query multiple pairs of messages (M_0^j, M_1^j) with the restriction that it begins the encryption of a new pair of messages only if it has finished the encryption of the previous pair. In the $\mathcal{E}_{\mathsf{k}}^{\mathrm{bl},c}(M_0^j[i], M_1^j[i], b)$ oracle, we add a session identifier sid since the adversary is not limited to sequence its pairs of messages but can interleaved the session queries. The session identifier will be the first element in the query. Equivalently, we can say that the adversary can run multiple $\mathcal{E}_{\mathsf{k}}^{\mathrm{bl},c}(\mathsf{sid}, M_0^j[i], M_1^j[i], b)$ oracles concurrently.

$$\mathsf{Adv}_{\Pi,A}^{\mathrm{lors-bcpa}}(k) = \left|2 \cdot \Pr\left[\mathsf{k} \leftarrow \mathcal{K}(1^k); b \leftarrow \{0,1\} : A^{\mathcal{E}_{\mathsf{k}}^{\mathrm{bl},s}(\mathcal{LR}(.,.,b))}(k) = b\right] - 1\right|$$
$$\mathsf{Adv}_{\Pi,A}^{\mathrm{lorc-bcpa}}(k) = \left|2 \cdot \Pr\left[\mathsf{k} \leftarrow \mathcal{K}(1^k); b \leftarrow \{0,1\} : A^{\mathcal{E}_{\mathsf{k}}^{\mathrm{bl},c}(\mathcal{LR}(.,.,.,b))}(k) = b\right] - 1\right|$$

Therefore, we define the $\mathsf{Adv}_{\Pi}^{\mathrm{lors-bcpa}}(k,t,q,\mu) = \max_A\{\mathsf{Adv}_{\Pi,A}^{\mathrm{lors-bcpa}}(k)\}$, where the maximum is over all legitimate A having time-complexity t, making to the concurrent oracles at most q encryption queries totaling μ blocks (resp. $\mathsf{Adv}_{\Pi}^{\mathrm{lorc-bcpa}}(k,t,q,\mu) = \max_A\{\mathsf{Adv}_{\Pi,A}^{\mathrm{lorc-bcpa}}(k)\}$). A secret-key encryption scheme is said to be *LOR-secure against blockwise adaptive chosen plaintext attack* in the LORS sense (resp. LORC) if, for all polynomial-time probabilistic adversaries, the advantage in this guessing game is negligible as a function of the security parameter k.

3 Relations between the standard and blockwise models

In this section, we study relations between the BA and standard models for probabilistic schemes. Figure 1 presents the main relations we prove in the sequel. First, it is easy to see that FTG-BCPA-P1 implies FTG-CPA-P1, FTG-BCPA-P2 implies FTG-CPA-P2, and LORS-BCPA implies LOR-CPA since the standard model can be easily simulated in the BA model. Secondly, it is also clear from the definitions of FTG-BCPA-P1, FTG-BCPA-P2, FTG-BCPA-D, LORC and LORS, that FTG-BCPA-P2 implies FTG-BCPA-P1, FTG-BCPA-D implies FTG-BCPA-P2, and LORC-BCPA implies LORS-BCPA. Thirdly, using hybrid arguments, it is easy to prove the implication between LORS-BCPA and FTG-BCPA-D (see in appendix of the full version).

In a lot of counterexamples, we use encryption schemes Π that treat the blocks such that there is no way to distinguish an input block from an output (in particular no redundancy is added on the input blocks): $\forall i \geq 1$, $n = |C[0]| = |M[i]| = |C[i]|$.

We use the notation $A \Rightarrow B$ to indicate a security-preserving reduction from notion A to notion B. $A \stackrel{q}{\rightarrow} B$ indicates a reduction (not necessarily security-preserving) from A to B. We also assume that $\mathcal{E}$ is a symmetric encryption scheme operating on n-bit blocks with a k-bit secret key k.

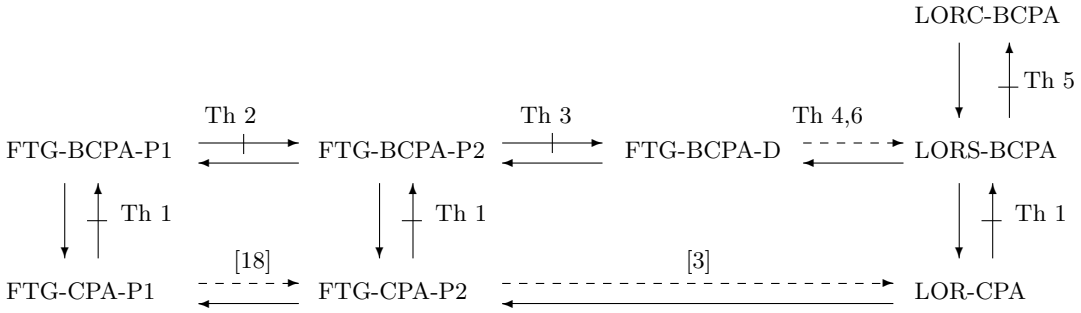

Fig. 1. Relations between the FTG and LOR security goals in the standard and BA models. In the figure, a plain arrow means that security in the first notion implies security in the second, a hatched arrow means that the first notion does not imply the second, and a dashed arrow indicates that the security between the two notions is not preserved.

3.1 Blockwise adversaries are stronger than standard ones

The following theorem shows the separation between BCPA and CPA adversaries for the goals FTG-P1, FTG-P2 and LORS. It is a generalization of a result of paper [17] which only state that FTG-CPA-P2 $\not\Rightarrow$ FTG-BCPA-P2.

Theorem 1. *[FTG-CPA-P1 $\not\Rightarrow$ FTG-BCPA-P1 and FTG-CPA-P2 $\not\Rightarrow$ FTG-BCPA-P2 and LOR-CPA$\not\Rightarrow$ LORS-BCPA] If there exists an on-line encryption scheme Π which is secure in the sense of FTG-CPA-P1 (resp. FTG-CPA-P2 or LOR-CPA), then there exists an on-line encryption scheme Π' which is also secure in the sense of FTG-CPA-P1 (resp. FTG-CPA-P2 or LOR-CPA) but which is not FTG-BCPA-P1 secure (resp. FTG-BCPA-P2 or BCPA-LORS) assuming the existence of pseudo-random permutations.*

Proof. Assume that there exists some FTG-CPA-P1 secure on-line encryption scheme $\Pi = (\mathcal{K}, \mathcal{E}, \mathcal{D})$, since otherwise the theorem is vacuously true. We now modify Π to a new on-line encryption scheme $\Pi' = (\mathcal{K}, \mathcal{E}', \mathcal{D}')$ which is also FTG-CPA-P1 secure but not secure in the FTG-BCPA-P1 sense:

$\mathtt{Algorithm}\ \mathcal{E}'_{\mathsf{k}}(M[i])$	$\mathtt{Algorithm}\ \mathcal{D}'_{\mathsf{k}}(C[i]\|v)$
$\quad\mathtt{If}\ i = 2$ and $M[2] = C[1]$	$\quad\mathtt{return}\ \mathcal{D}_{\mathsf{k}}(C[i])$
$\quad\quad\mathtt{then\ return}\ \mathcal{E}_{\mathsf{k}}(M[2])\|\mathsf{k}$	
$\quad\mathtt{else\ return}\ \mathcal{E}_{\mathsf{k}}(M[i])\|0^k$	

In the description of Π', 0^k denotes the concatenation of k zeros, and v denotes a k-bit value.

A BCPA adversary can choose the message blocks so that the relation $M[2] = C[1]$ holds with probability 1. Hence a BCPA adversary obtains the secret key and easily wins the FTG game. Thus Π' is not FTG-BCPA-P1 secure.

However a CPA adversary cannot choose the blocks. Then the relation holds with probability $1/2^n$ for each message queried if $\mathcal{E}_k$ is a pseudo-random permutation. Indeed, except if the relation $M[2] = C[1]$ holds, the CPA adversary gains no additional advantage in winning the FTG game against Π' than against Π. Therefore, it is easy to show that if Π is secure, then so is Π': $\mathsf{Adv}^{\mathrm{ftg-cpa-p1}}_{\Pi'}(k,t,q,\mu) \leq \mathsf{Adv}^{\mathrm{ftg-cpa-p1}}_{\Pi}(k,t,q,\mu) + 2q/2^n$. We can prove this result using different games as in [21]. The first game G_0 is the real security game and in the next game G_1, the simulation is stopped as soon as the relation $M[2] = C[1]$ holds. The difference between the two games can be analyzed using the probability of collision. Let F be the event $M[2] = C[1]$, S be the event of the adversary wins the FTG security game against Π and S' be the event the adversary wins the FTG security game against Π'. As long as F does not occur, $\Pr[S] = \Pr[S']$ so $\Pr[S \wedge \neg F] = \Pr[S' \wedge \neg F]$. Therefore, $|\Pr[S] - \Pr[S']| \leq \Pr[F]$ as a lemma in [21] shows. Then, it is easy to upper bound $\Pr[F]$ by $q/2^n$ since each call will be independent (a new random value is used for each message query) and $\mathsf{Adv}^{\mathrm{ftg-cpa-p1}}_{\Pi'}(k,t,q,\mu) \leq \mathsf{Adv}^{\mathrm{ftg-cpa-p1}}_{\Pi}(k,t,q,\mu) + 2q/2^n$. The factor of 2 comes from the fact that the advantage is twice the probability of success minus 1. Consequently, Π' is FTG-CPA-P1 secure but is not FTG-BCPA-P1 secure. This conversion can be adapted to prove the separation between FTG-BCPA-P2 and FTG-CPA-P2, and between LORS-BCPA and LOR-CPA.

3.2 Adaptive adversaries can be more powerful in the blockwise model

Adaptive adversaries. Katz and Yung show in [18] that accesses to an adaptive encryption oracle after the challenge phase do not help an CPA adversary. Formally, they show that FTG-CPA-P1 is polynomially-equivalent in the number of message queries to FTG-CPA-P2. In the BA model, this equivalence is no longer valid and we prove that BCPA-P2 adversaries are strictly stronger than BCPA-P1 ones since the CBC encryption mode is FTG-BCPA-P1 but not FTG-BCPA-P2 according to [17]. Finally, it is worth noticing in the following proof that if the condition $M[4] = C[3]$ is not present, the scheme Π' is not FTG-CPA-P1. Thus, as one could believe at first glance, the counterexample we use in the proof cannot be applied in the standard model.

Theorem 2. *[FTG-BCPA-P1 $\not\Rightarrow$ FTG-BCPA-P2] If there exists an on-line encryption scheme Π which is FTG-BCPA-P1 secure, then there exists an on-line encryption scheme Π' which is also secure FTG-BCPA-P1 secure but not FTG-BCPA-P2 secure assuming the existence of pseudo-random permutations.*

Proof. Assume that there exists some FTG-BCPA-P1 secure on-line encryption scheme $\Pi = (\mathcal{K}, \mathcal{E}, \mathcal{D})$, since otherwise the theorem is vacuously true. We now modify Π to a new on-line encryption scheme $\Pi' = (\mathcal{K}, \mathcal{E}', \mathcal{D}')$ which is also FTG-BCPA-P1 secure but not secure in the FTG-BCPA-P2 sense. The new on-line encryption scheme $\Pi' = (\mathcal{K}, \mathcal{E}', \mathcal{D}')$ is defined as follows:

Algorithm $\mathcal{E}'_{\mathsf{k}}(M[i])$	Algorithm $\mathcal{D}'_{\mathsf{k}}(C[i]\|b')$
If $(i=4) \wedge (M[4]=C[3]) \wedge (\mathcal{D}^{\mathrm{m}}_{\mathsf{k}}(M[2]\|M[3])=M[1])$ then return $\mathcal{E}_{\mathsf{k}}(M[4])\|1$	return $\mathcal{D}_{\mathsf{k}}(C[i])$
else return $\mathcal{E}_{\mathsf{k}}(M[i])\|0$	

where $\mathcal{D}^{\mathrm{m}}_{\mathsf{k}}(C)$ denotes the decryption of the whole ciphertext C using the secret key k and not only as the decryption of one block of the ciphertext. More precisely, in the above description, the block $M[2]$ is treated for example as the initialization vector $C[0]$ and $M[3]$ is the encryption of the first block.

Every BCPA adversary can choose the blocks of messages such that the relation $M[4] = C[3]$ holds with probability 1. We show that a FTG-BCPA-P2 adversary A, can win its FTG game, *i.e.* distinguish between the encryption of M_0 and M_1. Now A tries to correctly guess the bit b. In the challenge phase, A chooses two different random blocks $\{0,1\}^n$, $M_0[1]$ and $M_1[1]$ and sends them to the encryption oracle which returns $C_b[0]\|C_b[1]$. In the guess phase, A sends $M[1] = M_0[1]$ and receives $C[0]\|C[1]$. Then, A sends $M[2] = C_b[0]$, receives $C[2]$, and sends $M[3] = C_b[1]$ except the last bit and receives $C[3]$. Finally, A sends $M[4] = C[3]$ and the encryption oracle returns $\mathcal{E}_{\mathsf{k}}(M[4])\|d$. If $d = 1$, then A has correctly guessed the bit $b = 0$, since $\mathcal{D}^{\mathrm{m}}_{\mathsf{k}}(M[2]\|M[3]) = M[1]$ (because if $b = 0$, then $\mathcal{D}^{\mathrm{m}}_{\mathsf{k}}(C_b[0]\|C_b[1]) = M_0[1]$). Therefore A wins the FTG game with probability 1. Hence a FTG-BCPA-P1 adversary B, which has not access to a blockwise encryption oracle after the challenge phase cannot win the game with significant advantage. Indeed, assume that there exists a FTG-BCPA-P1 adversary A against scheme Π', then we will construct a FTG-BCPA-P1 attacker B against scheme Π. The attacker B will simulate the challenger to the adversary A. The event $\mathcal{D}^{\mathrm{m}}_{\mathsf{k}}(M[2]\|M[3]) = M[1]$ can appear in two situations: either at random with probability $1/2^n$ for each message, if $\mathcal{E}_{\mathsf{k}}$ is a pseudo-random permutation, or since the attacker B knows all encryption queries of A, he can decide when this event occurs in the second case. Consequently, B is able to simulate the encryption process to A except in the first case which appears with small probability. Consequently, Π' is FTG-BCPA-P1 secure but is not FTG-BCPA-P2 secure.

Adaptive adversaries during the challenge phase. We also prove that adversaries adaptive before, during and after the challenge phase, BCPA-D, are stronger than adversary, BCPA-P2 adaptive before and after. The notion of BCPA-D adversaries is equivalent to BCPA-P2 in the standard adversarial model since messages are treated as atomic objects.

Theorem 3. *[FTG-BCPA-P2 $\not\Rightarrow$ FTG-BCPA-D] If there exists an on-line encryption scheme Π which is FTG-BCPA-P2 secure, then there exists an on-line encryption scheme Π' which is also FTG-BCPA-P2 secure but not FTG-BCPA-D secure assuming the existence of pseudo-random permutations.*

Proof. Assume that there exists some FTG-BCPA-P2 secure on-line encryption scheme $\Pi = (\mathcal{K}, \mathcal{E}, \mathcal{D})$, since otherwise the theorem is vacuously true. We now modify Π to a new on-line encryption scheme $\Pi' = (\mathcal{K}, \mathcal{E}', \mathcal{D}')$ which is also

FTG-BCPA-P2 secure but not FTG-BCPA-D secure. The new on-line encryption scheme $\Pi' = (\mathcal{K}, \mathcal{E}', \mathcal{D}')$ is a slight modification of the encryption function $\mathcal{E}$ defined as follows:

$\texttt{Algorithm } \mathcal{E}'_{\mathsf{k}}(M[i])$	$\texttt{Algorithm } \mathcal{D}'_{\mathsf{k}}(C[i])$
$\quad\texttt{If } i = 3 \text{ and } M[2] = C[1]$	$\quad\texttt{If } i = 3 \text{ and } M[2] = C[1]$
$\quad\quad\texttt{then return } M[3]$	$\quad\quad\texttt{then return } C[3]$
$\quad\texttt{else return } \mathcal{E}_{\mathsf{k}}(M[i])$	$\quad\texttt{else return } \mathcal{D}_{\mathsf{k}}(C[i])$

Clearly Π' is FTG-BCPA-P2 secure as Π as shown in the previous proofs. A BCPA adversary can choose the blocks of messages such that the relation $M[2] = C[1]$ holds with probability 1 during the challenge phase. Therefore a FTG-BCPA-D adversary A can distinguish between the encryption of M_0 and M_1: A first sends $(M_0[1], M_1[1])$, gets $C[0]\|C[1]$, and then queries $(M_0[2], M_1[2])$ where $M_0[2] = C[1]$ and $M_0[2] \neq C[1]$. Finally, he queries $(M_0[3], M_1[3])$ such that $M_0[3] \neq M_1[3]$. Consequently, if he receives $C[3] = M_0[3]$, then $b = 0$, otherwise $b = 1$. Hence Π' is FTG-BCPA-P2 secure but is not FTG-BCPA-D secure.

Relation between FTG and LOR in the BA model. In [3] Bellare *et al.* prove that in the standard model FTG and LOR are polynomially-equivalent in the number of encrypted queries. We prove here in the BA model that this relation holds between FTG-BCPA-D and LORS-BCPA. The proof is an adaptation of [3] and uses the same hybrid argument (introduced in [12]) in the blockwise setting. It is given in appendix of the full version.

Theorem 4. *[LORS-BCPA $\Rightarrow$ FTG-BCPA-D $\xrightarrow{q}$ LORS-BCPA] For any scheme $\mathcal{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$,*

$$\mathsf{Adv}^{\mathrm{ftg-bcpa-d}}_{\mathcal{SE}}(k, t, q, \mu) \leq \mathsf{Adv}^{\mathrm{lors-bcpa}}_{\mathcal{SE}}(k, t, q, \mu) \leq q \times \mathsf{Adv}^{\mathrm{ftg-bcpa-d}}_{\mathcal{SE}}(k, t, q, \mu)$$

3.3 Concurrent adversaries

Finally, we show that LORC-BCPA is the strongest security notion in the blockwise model. Concurrent adversaries have already been considered in other contexts such as zero-knowledge proofs in [8]. According to our knowledge, it is the first time that concurrent adversaries appear in encryption schemes. In the BA model and for the LOR game, this notion is natural.

Theorem 5. *[LORS-BCPA$\not\Rightarrow$ LORC-BCPA] If there exists an on-line encryption scheme Π which is LORS-BCPA secure, then there exists an on-line encryption scheme Π' which is also LORS-BCPA secure but not LORC-BCPA secure assuming the existence of pseudo-random permutations.*

Proof. Assume that there exists some LORS-BCPA secure on-line encryption scheme $\Pi = (\mathcal{K}, \mathcal{E}, \mathcal{D})$, since otherwise the theorem is vacuously true. We now modify Π to a new on-line encryption scheme $\Pi' = (\mathcal{K}', \mathcal{E}', \mathcal{D}')$ which is also LORS-BCPA secure but not secure in the LORC-BCPA sense. The new on-line

encryption scheme $\Pi' = (\mathcal{K}, \mathcal{E}', \mathcal{D}')$ is a slight modification of the functions $\mathcal{E}$ and $\mathcal{D}$:

```
Algorithm E'_k(M[i])
    If i = 3 and C[1] = D^m_k(M[2]||M[3])
       then return M[3]
    else return E_k(M[i])
```

where $\mathcal{D}^{\mathrm{m}}_{\mathsf{k}}(M)$ denotes the decryption of the whole message M using the key k and the decryption can be easily adapted.

Clearly Π' is LORS-BCPA secure as the initial scheme Π. Indeed, assume for the sake of contradiction that there exists a LORS-BCPA adversary A' against Π'. We must show that there also exists a LORS-BCPA adversary A against Π. We have to simulate the challenger against A'. The only difference between the two schemes is in the encryption of the third block if some relation occurs. The relation can hold either by a correct guess of the adversary which is negligible if $\mathcal{E}_{\mathsf{k}}$ behaves as a pseudo-random permutation or if a collision occurs with previous encryption queries. The last event is easily detectable by adversary A since all encryption queries goes through A which forwards them to its challenger. Hence, it is easy for A to not encrypt the third block if the relation occurs. In this case, the simulation is quite perfect.

Any LORC-BCPA adversary can choose the message blocks such that the relation $C[1] = \mathcal{D}^{\mathrm{m}}_{\mathsf{k}}(M[2]\|M[3])$ holds with probability 1. Indeed, a LORC-BCPA adversary A begins the encryption of a pair of messages (M_0, M_1) by sending $(M_0[1], M_1[1])$ to a first instance of the LOR-block encryption oracle which returns $C_b[0]\|C_b[1]$. Then, he sends $(M'_0[1], M'_1[1])$ where $M'_0[1] = C_b[1]$ to a second instance running concurrently and gets $C'_b[0]\|C'_b[1]$. He continues the encryption of (M_0, M_1) by sending $(M_0[2], M_1[2])$ such that $M_0[2] = C'_b[0]$ and $M_1[2]$ is a random block. Finally, he queries $(M_0[3], M_1[3])$ with $M_0[3] = C'_b[1]$. A simple manipulation shows that if $b = 0$, then $C_0[1] = \mathcal{D}^{\mathrm{m}}_{\mathsf{k}}(C'_0[0]\|C'_0[1])$ and consequently $\mathcal{E}_{\mathsf{k}}(M_0[3]) = M_0[3]$. Therefore Π' is LORS-BCPA secure but is not LORC-BCPA secure.

4 On-line Encryption Schemes with a special property

In this section we define a new property for on-line encryption schemes, called *Resettable-Or-Continuous* (ROC). For these schemes, the two security notions LORS-BCPA and FTG-BCPA-D are exactly equivalent.

The Resettable-Or-Continuous property can be defined informally as follows: it is computationally hard for a polynomial-time adversary to distinguish with non-negligible advantage between the encryption of the concatenation of a polynomial number of messages, $\mathcal{E}(M_1\|M_2\|\ldots\|M_{\ell(k)})$, and the concatenation of the encryptions of the same messages $\mathcal{E}(M_1)\|\mathcal{E}(M_2)\|\ldots\|\mathcal{E}(M_{\ell(k)})$ for stateful encryption schemes such as the counter mode or for a stateless encryption scheme between $\mathcal{E}(M_1\|r_1\|M_2\|r_2\ldots\|r_{\ell(k)-1}\|M_{\ell(k)})$, where the r_i's denote random blocks such that the length of the two bitstring be the same. This special

class captures many important on-line encryption schemes such as the CBC and CTR mode [3].

Formally, we define the *resettable-or-continuous* oracle $ROC(\mathcal{E}_{\mathsf{k}}^{\mathrm{bl}}(.), b)$, taking as input a message M and working as follows for a stateless encryption scheme such as the CBC. At the beginning of the game, the ROC oracle chooses a random bit b. The first message $M = M[1]M[2]\dots M[l]$ is encrypted by the ROC oracle which returns $C[0]C[1]\dots C[l]$. The adversary is free to stop this encryption by using the `stop` command or to submit a new message block by block. When the adversary submits the `stop` command and if $b = 0$, the ROC encryption oracle stops the encryption of M and starts the encryption of the new message $M'[1], \dots M[l']$ under the key k and a new random value $C'[0]$ and returns $C' = C'[0]C'[1]\dots C'[l']$. However if $b = 1$, the ROC oracle does not stop the encryption of the first message. He takes a random block $r_1 \in \{0,1\}^n$, encrypts it into $C'[0]$ as if r_1 was the next block in M. Then, he encrypts the message $M'[1]M'[2]\dots M'[l']$ block by block and returns gradually $C'[0]C'[1]C'[2]\dots C'[l']$. In the case $b = 1$, the ROC encryption oracle has encrypted the concatened message $M[1]\dots M[l]\|r_1\|M'[1]\dots M'[l']$. This game continues for the other queries. This simulation can be made for any stateless encryption scheme such as the CBC mode. For a stateful encryption scheme such as the CTR mode, the random block is not present when $b = 1$. This property can also be defined in the standard model.

$$\mathsf{Adv}_{\Pi,A}^{\mathrm{ind-roc}}(k,t,q,\mu) \stackrel{\mathrm{def}}{=} \left|2 \cdot \Pr\left[\mathsf{k} \leftarrow \mathcal{K}(1^k); b \leftarrow \{0,1\} : A^{ROC(\mathcal{E}_{\mathsf{k}}^{\mathrm{bl}}(.),b)}(k) = b\right] - 1\right|$$

Therefore, the security bound for the scheme Π is given by $\mathsf{Adv}_{\Pi}^{\mathrm{ind-roc}}(k,t,q,\mu) = \max_A\{\mathsf{Adv}_{\Pi,A}^{\mathrm{ind-roc}}(k)\}$, where the maximum is over all legitimate A having time-complexity t, making to the oracle at most q encryption queries totaling μ blocks. A secret-key encryption scheme is said to be *IND-secure against blockwise adaptive chosen plaintext attack* in the ROC sense if for all polynomial-time probabilistic adversaries, the advantage in this game is negligible as a function of the security parameter. The ROC class is the set of encryption schemes satisfying the ROC property.

Theorem 6. *[FTG-BCPA-D $\stackrel{ROC}{\Rightarrow}$ LORS-BCPA] For any ROC scheme $\mathcal{SE}$,*

$$\mathsf{Adv}_{\mathcal{SE}}^{\mathrm{lors-bcpa}}(k,t,q,\mu) \leq \mathsf{Adv}_{\mathcal{SE}}^{\mathrm{ftg-bcpa-d}}(k,t,q,\mu) + \mathsf{Adv}_{\mathcal{SE}}^{\mathrm{ind-roc}}(k,t,q,\mu)$$

Proof. The proof goes by contradiction. Let $\mathcal{SE}$ be a ROC encryption scheme. Assume for the sake of contradiction that a LORS-BCPA adversary A wins the LORS game against $\mathcal{SE}$ with non-negligible advantage. Then it can be used to build a BCPA-D attacker B winning a FTG game against $\mathcal{SE}$ with non-negligible advantage. The FTG adversary B does not use his find phase and begins the challenge phase by running A. To simulate the LORS encryption queries of A, B forwards the pairs of messages block by block and does not send the `stop` command at the end of a message query. All messages are chained. The messages

are separated with a random block chosen by B in the case of stateless schemes and are not separated for stateful schemes. This simulation is perfect for schemes having the ROC property. Therefore, A wins the LORS game with non-negligible advantage and B forwards the bit guessed by A and also wins the FTG game with non-negligible advantage.

5 Security under concurrent adversary

In this section, we prove that security against concurrent adversaries can be achieved. We prove that the randomized counter mode, called XOR in [3] is secure. We note that encryption with XOR or CTR mode of operation does not require permutations. Therefore we use only functions. We prove such scheme and not the standard counter mode where the counter is incremented between each message since in the concurrent scenario, the adversary can begin the encryption of several messages in parallel.

We consider several attacker games such that the distance between each game can be easily shown. In the last game, it will be clear that the adversary has no way to get some information about the random bit b in the LORC security game.

Theorem 7. *For any adversary $\mathcal{A}$ running within time bound t, with less than $q < 2^{n/2}$ calls to the function F, totalling at most μ blocks,*

$$\mathsf{Adv}^{\mathsf{lorc-bcpa}}_{\mathsf{XOR},A}(k,t,q,\mu) \leq \mathsf{Adv}^{\mathsf{prf}}_{F,A}(k,t,q) + \frac{q(q-1)}{2^n}$$

where n denotes the block length, $\mathsf{Adv}^{\mathsf{prf}}_{F,A}(k,t,q)$, the advantage of the adversary A in distinguishing a function taken from F to a random function with at most q black-box queries within time bounded by t. The same kind of definition can be given for $\mathsf{Adv}^{\mathsf{lorc-bcpa}}_{\mathsf{XOR},A}(k,t,q,\mu)$.

Proof. Let $\mathcal{A}$ be an adversary, and let $\mathbf{G}_0$ be the attack game. Let b the value chosen by the challenger in the LORC security game and b' the bit returned by $\mathcal{A}$, and let S_0 be the event that $b = b'$.

Game $\mathbf{G}_0$: This is the real protocol. In this game, we are interested in the event S_0, which occurs if $b = b'$, where b is the bit chosen by the encryption oracle and b' is the output of the LORC-adversary $\mathcal{A}$.

Game $\mathbf{G}_1$: We modify the encryption oracle as follows. If a collision happens between two inputs of the block cipher, we stop the encryption where the collision is going to happen.

Let F_1 be the event that in game $\mathbf{G}_1$ a collision happens that would not have been stopped under the rules of game $\mathbf{G}_0$. Since these two games proceed identically until F_1 occurs, we have $\Pr[S_0 \wedge \neg F_1] = \Pr[S_1 \wedge \neg F_1]$, and applying Lemma 1 of [21] with (S_0, S_1, F_1), we have $|\Pr[S_1] - \Pr[S_0]| \leq \Pr[F_1]$.

So it suffices to bound $\Pr[F_1]$. This probability is bounded by $\frac{q(q-1)}{2^n}$ as shown in [3] we have the following result :

$$|\Pr[S_1] - \Pr[S_0]| \leq \frac{q(q-1)}{2^n} \tag{1}$$

Game $\mathbf{G}_2$: In this game, we try to avoid the use of the secrete key in the scheme. Instead of using a block cipher, we use a truly random function that we construct when we need to define it at some point.

Indeed, assume that $\mathcal{A}$ is an attacker that breaks the LORC security game with advantage ε running in time t, then we construct a $\mathcal{A}'$ adversary which is able to distinguish the output of a random function taken in the family F of the output of a truly random function with advantage ε' in time t'. At the beginning of this game, $\mathcal{A}'$ has access to a function f, for which its task is to tell whether it is a random function ($b = 0$)or a member of F ($b = 1$). Also $\mathcal{A}'$ chooses at random a bit b' and according to this bit, $\mathcal{A}'$ will encrypt either the left or the right message in the LORC security game. Then $\mathcal{A}'$ runs the attacker $\mathcal{A}$ using f to simulate all the queries as in the previous game. Eventually, $\mathcal{A}$ will reply with a bit b''. Then, if $b' = b''$, then $\mathcal{A}$ correctly guesses the bit b' and wins the LORC game. $\mathcal{A}'$ returns a bit $b^\star$ which is equal to 0 if $b' = b''$.

$$\begin{aligned}
\frac{\varepsilon' + 1}{2} &= \Pr[b^\star = b] = \frac{1}{2} \cdot [\Pr[b^\star = 0 | b = 0] + \Pr[b^\star = 1 | b = 1]] \\
&= \frac{1}{2} \cdot [\Pr[b' = b'' | f \leftarrow F] + \Pr[b' \neq b'' | f \ random \ function]] \\
&= \frac{1}{2} \cdot [\Pr[S_2] + (1 - \Pr[b' = b'' | f \ random \ function])] \\
&= \frac{1}{2} \cdot [\Pr[S_2] + (1 - \Pr[S_3])]
\end{aligned}$$

Consequently, $|\Pr[S_2] - \Pr[S_1]| = |\varepsilon'|$ and

$$|\Pr[S_2] - \Pr[S_1]| \leq \mathsf{Adv}^{\mathsf{prf}}_{F,A}(k, t, q) \tag{2}$$

Finally,

$$\Pr[S_2] = 1/2 \tag{3}$$

since we can replace the random output by the function F xored the message block by a random block. According to the properties of the xor, this is equivalent and therefore, as the message is no longer used, in this last game, the advantage of the adversary is clearly 0.

Putting together (1), (2), (3) we obtain

$$\mathsf{Adv}^{\mathsf{lorc}}_{\mathsf{XOR},A}(k, t, q, \mu) \leq \mathsf{Adv}^{\mathsf{prf}}_{F,A}(k, t, q) + \frac{q(q-1)}{2} \tag{4}$$

6 Conclusion

In this paper we have analyzed the relations between the block adversary and the standard models for probabilistic and deterministic schemes. For probabilistic schemes, the relations are modified and we introduce new security notions. The resettable-or-continuous property extends the result of Bellare *et al.*. Moreover, we also prove that concurrent accesses lead to the strongest security notion and we show that some schemes can be secure in this setting. Finally, we show that the models are equivalent for deterministic schemes in appendix of the full version.

References

1. M. Bellare, J. Black, T. Krovetz, and P. Rogaway. OCB : A Block-Cipher Mode of Operation for Efficient Authenticated Encryption. Available at `http://www.cs.ucdavis.edu/users/~rogaway`, 2001.
2. M. Bellare, A. Boldyreva, L. Knudsen, and C. Namprempre. On-Line Ciphers and the Hash-CBC Constructions. In *Crypto '01*, LNCS 2139, pages 292–309. Springer-Verlag, 2001.
3. M. Bellare, A. Desai, E. Jokipii, and P. Rogaway. A Concrete Security Treatment for Symmetric Encryption. In *Proc. 38th of FOCS*, pages 394–403. IEEE, 1997.
4. M. Bellare, A. Desai, D. Pointcheval, and P. Rogaway. Relations Among Notions of Security for Public-Key Encryption Schemes. In *Crypto '98*, LNCS 1462, pages 26–45. Springer-Verlag, 1998.
5. M. Bellare and P. Rogaway. On the Construction of Variable-Input-Length Ciphers. In *FSE '99*, LNCS 1636. Springer-Verlag, 1999.
6. A. Boldyreva and N. Taesombut. On-line Encryption Schemes: New Security Notions and Constructions. In *RSA Conf 2004*, LNCS, pages –. Springer-Verlag, Berlin, 2003.
7. Y. Dodis and J. H. An. Concealment and Its Applications to Authenticated Encryption. In *Eurocrypt '03*, LNCS 2656, pages 312–329. Springer-Verlag, 2003.
8. C. Dwork, M. Naor, and A. Sahai. Concurrent Zero-Knowledge. In *Proc. of the 30th STOC*, pages 409–418. ACM Press, New York, 1998.
9. P. A. Fouque, A. Joux, G. Martinet, and F. Valette. Authenticated On-line Encryption. In *Selected Areas in Cryptography '03*, LNCS. Springer-Verlag, 2003. *To appear.*
10. P. A. Fouque, G. Martinet, and G. Poupard. Practical Symmetric On-line Encryption. In *Fast Software Encryption '03*, LNCS. Springer-Verlag, 2003. *To appear.*
11. P. A. Fouque, A. Joux, and G. Poupard. Blockwise Adversarial Model for On-line Ciphers and Symmetric Encryption Schemes. In *Selected Areas in Cryptography '04*, LNCS. Springer-Verlag, 2004. `http://www.di.ens.fr/~fouque/pubs/`.
12. O. Goldreich. *Foundations of Cryptography.* Cambridge University Press, Weizmann Institute of Science, 2001. Basic Tools.
13. O. Goldreich, S. Goldwasser, and S. Micali. How to Construct Random Functions. *Journal of the ACM*, 33(4):210–217, 1986.
14. S. Goldwasser and S. Micali. Probabilistic encryption. *Journal of Computer and System Sciences*, 28:270–299, 1984.
15. A. Herzberg, S. Jarecki, H. Krawczyk, and M. Yung. A Tweakable Enciphering Mode. In *Crypto '03*, LNCS. Springer-Verlag, 2003.

16. R. Housley. Cryptographic message syntax. S/MIME Working Group of the IETF, Internet-draft `draft-ietf-smime-cms-12.txt`, March 1999.
17. A. Joux, G. Martinet, and F. Valette. Blockwise-Adaptive Attackers: Revisiting the (in)security of some provably secure Encryptions Modes: CBC, GEM, IACBC. In *Crypto '02*, LNCS 2442, pages 17–31. Springer-Verlag, 2002.
18. J. Katz and M. Yung. Complete characterization of security notions for probabilistic private-key encryption. In *STOC '00*. ACM Press, 2000.
19. NBS. FIPS PUB 81 - DES Modes of Operation, December 1980.
20. R. Rivest. All-or-nothing encryption and the package transform. In *FSE '97*, LNCS 1267. Springer-Verlag, 1997.
21. V. Shoup. OAEP Reconsidered. In *Crypto '2001*, LNCS 2139, pages 239–259. Springer-Verlag, Berlin, 2001.

7 Appendix A : On-line Ciphers

7.1 Description of on-line ciphers

A *cipher* over a domain D is a function $F : \{0,1\}^k \times D \to D$ such that, for each key k, the map $F(\mathsf{k}, .)$ is a length-preserving permutation on D. The knowledge of k enables to both compute and invert $F(\mathsf{k}, .)$. The most popular examples are block ciphers, where $D = \{0,1\}^n$ for some n, called the block length. However, one might want to encipher large data. In this case one needs a cipher with domain D appropriately large. Consequently, ciphers with variable input length have been built from ciphers with fixed input length such as block ciphers [5]. Ciphers are interesting since they can be used in order to construct disk sector encryption (cf. [15]). On-line ciphers are ciphers that the enciphering of the block $M[i]$ only depends on the block $M[1]...M[i]$.

7.2 Security notions for ciphers

To analyze the security of a block cipher E, it is usual to view it as a family of permutations indexed by a key K and to use the notion of a pseudorandom permutation (PRP) as defined in [13]. A family of permutations is pseudorandom if no probabilistic algorithm A running in polynomial time in the security parameter k can distinguish the permutations in E from Perm_n, the set of all permutations on $\{0,1\}^n$. In [2], this security goal has been adapted for on-line ciphers with arbitrarily large domain. Indeed, since an on-line cipher is a deterministic scheme enciphering gradually the plaintext blocks, if two messages have the same first blocks, then their encryptions collide on these first blocks. Therefore, such ciphers are no longer indistinguishable from permutations on the whole domain D. The relevant security goal is called indistinguishability from on-line pseudorandom permutation (OPRP).

On-line Pseudorandom Permutations. In [2], Bellare *et al.* have defined the OPRP security notion. Let $\mathsf{OPerm}_{d,n}$ be the set of all on-line permutations π on domain $D_{d,n}$. A cipher is secure in the sense of on-line PRP if it is computationally infeasible, given an oracle $\mathcal{O}_b$, to have non-negligible advantage in

distinguishing between the case where $\mathcal{O}_b$ is a random instance of E and the case where $\mathcal{O}_b$ is a random element of $\mathsf{OPerm}_{d,n}$. On-line PRP is a weaker security notion than PRP. However, this notion is meaningful to capture practical security of schemes. We denote by $\mathcal{O}^{\mathrm{bl}}(.)$ (respectively by $\mathcal{O}(.)$), a ciphering oracle block oriented (respectively message oriented). The difference between the two models is that in the BA model, messages can be queried block by block. We say that an on-line cipher is OPRP-BCPA secure (resp. OPRP-CPA secure), if it is indistinguishable from an OPRP against a BCPA (resp. CPA) adversary:

$$\mathsf{Adv}_{E,A}^{\mathrm{oprp-bcpa}}(k) \stackrel{\mathrm{def}}{=} \left| 2 \cdot \Pr \left[\begin{array}{c} \mathsf{k} \leftarrow \mathcal{K}(1^k); \mathcal{O}_0^{\mathrm{bl}}(.) \leftarrow \mathsf{OPerm}_{d,n}; \\ \mathcal{O}_1^{\mathrm{bl}}(.) \leftarrow E_{\mathsf{k}}(.); b \leftarrow \{0,1\} : A^{\mathcal{O}_b^{\mathrm{bl}}(.)}(1^k) = b \end{array} \right] - 1 \right|$$

$$\mathsf{Adv}_{E,A}^{\mathrm{oprp-cpa}}(k) \stackrel{\mathrm{def}}{=} \left| 2 \cdot \Pr \left[\begin{array}{c} \mathsf{k} \leftarrow \mathcal{K}(1^k); \mathcal{O}_0(.) \leftarrow \mathsf{OPerm}_{d,n}; \\ \mathcal{O}_1(.) \leftarrow E_{\mathsf{k}}(.); b \leftarrow \{0,1\} : A^{\mathcal{O}_b(.)}(1^k) = b \end{array} \right] - 1 \right|$$

We define $\mathsf{Adv}_{E}^{\mathrm{oprp-atk}}(k,t,q,\mu) = \max_{A}\{\mathsf{Adv}_{E,A}^{\mathrm{oprp-atk}}(k)\}$, where the maximum is over all legitimate A having at most time-complexity t, making to the oracle at most q encryption queries totaling μ blocks. As stated in [3], we define the time complexity as the worst case total execution time of the experiment, plus the size of the code of the adversary in some fixed RAM model of computation.

7.3 On-line ciphers: Equivalence of the models

In this section we prove that security of on-line ciphers in both adversarial models are polynomially-equivalent. Furthermore we present an on-line cipher achieving the bounds, proving that our reduction is tight.

An on-line cipher $\mathcal{OLC}$ is secure in the OPRP sense if it is difficult for a polynomial-time adversary to distinguish with non-negligible advantage $\mathcal{OLC}$ from a random on-line permutation operating on $\{0,1\}^{nl}$, where n is the block length of the underlying PRP and l is the number of blocks.

Clearly OPRP-BCPA secure ciphers are also OPRP-CPA secure. The opposite is also true and the proof goes by contradiction. Assume, for the sake of contradiction, that there exists an OPRP-BCPA adversary A against some cipher $\mathcal{OLC}$. Then, we construct an OPRP-CPA attacker B against $\mathcal{OLC}$ which uses A. The attacker B simulates the blockwise encryption oracle of A by using its own message encryption queries: if A queries the message $M = M[1]M[2]\dots M[l]$, B queries l successive messages $M[1]$, then $M[1]M[2]$, ..., and finally $M[1]M[2]\dots M[l]$. The total number of encrypted blocks asked by adversary B is $(\mu-1)(\mu-2)/2$. This simulation is perfect and polynomial in the total number of blocks. At the end of the game, B forwards the bit guessed by A. Finally, we obtain the following theorem:

Theorem 8. *Let $\mathcal{OLC} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ be an on-line cipher. If $\mathcal{OLC}$ is secure in the BA model, then $\mathcal{OLC}$ is secure in the standard model. Moreover, if $\mathcal{OLC}$ is*

secure in the standard model, then $\mathcal{OLC}$ is secure in the BA model. Furthermore, we have:

$$\mathsf{Adv}^{\mathrm{oprp-cpa}}_{\mathcal{OLC}}(k,t,q,\mu) \leq \mathsf{Adv}^{\mathrm{oprp-bcpa}}_{\mathcal{OLC}}(k,t,q,\mu) \leq \mathsf{Adv}^{\mathrm{oprp-cpa}}_{\mathcal{OLC}}(k,t',\mu')$$

where $t' = t + (\mu-1)(\mu-2)/2 \times T_E$, $\mu' = (\mu-1)(\mu-2)/2$, and T_E represents the time to encrypt one block with the block cipher E.

Proof. Moreover, we show that the second bound is tight by constructing an on-line cipher for which a BCPA adversary can win the OPRP security goal with $\bar{\mu}$ blocks but a CPA adversary cannot gain significant advantage if strictly less than $(\bar{\mu}-1)(\bar{\mu}-2)/2$ blocks are queried. Assume that there exists some OPRP-CPA secure on-line cipher $\mathcal{OLC} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$, since otherwise the theorem is vacuously true. We now modify $\mathcal{OLC}$ to a new on-line cipher $\mathcal{OLC}' = (\mathcal{K}, \mathcal{E}', \mathcal{D})$ which is also OPRP-CPA secure if strictly less than $(\bar{\mu}-1)(\bar{\mu}-2)/2$ blocks are queried but not secure against an OPRP-BCPA adversary querying $\bar{\mu}$ blocks. The new on-line cipher $\mathcal{OLC}' = (\mathcal{K}, \mathcal{E}', \mathcal{D})$ is obtained by slightly modifying $\mathcal{E}$ in the following way:

```
Algorithm E'_k(M[i])
    If i = μ̄ and M[2] = C[1] and M[3] = C[2] and ... and M[μ̄ − 1] = C[μ̄ − 2]
       then return M[μ̄]
    else return E_k(M[i])
```

By using a single message of $\bar{\mu}$ blocks, a BCPA adversary can gradually choose all the blocks such that all the relations $M[2] = C[1]$, $M[3] = C[2]$, ..., $M[\bar{\mu}-1] = C[\bar{\mu}-2]$ hold. A CPA adversary A can correctly choose the first i blocks with the following strategy. He first queries $M[1]$ and receives $C[1]$. Then, A can query the message $M[1]C[1]$ and receives $C[1]C[2]$, and so on... This technique can be used recursively to find a $\bar{\mu}$ blocks message for which all the relations hold. Furthermore, one can show that either this method requires at least $(\bar{\mu}-1)(\bar{\mu}-2)/2$ blocks or A correctly guesses the answer of some blocks. This last event can be upper bounded by $1/2^n$ which is negligible.

8 Appendix B : Proof of theorem 4

[LORS-BCPA $\Rightarrow$ FTG-BCPA-D $\xrightarrow{q}$ LORS-BCPA] *For any scheme $\mathcal{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$,*

$$\mathsf{Adv}^{\mathrm{ftg-bcpa-d}}_{\mathcal{SE}}(k,t,q,\mu) \leq \mathsf{Adv}^{\mathrm{lors-bcpa}}_{\mathcal{SE}}(k,t,q,2\mu) \leq q \cdot \mathsf{Adv}^{\mathrm{ftg-bcpa-d}}_{\mathcal{SE}}(k,t,q,\mu)$$

Proof: Theorem 4.3 states that FTG-BCPA-D and LORS-BCPA are polynomially-equivalent in the number of message queries. It is easy to prove that LORS-BCPA implies FTG-BCPA-D. The proof goes by contradiction. Assume for the sake of contradiction that a BCPA-D adversary A wins the FTG game with non-negligible advantage. We turn it into a BCPA attacker B which wins the LORS game with non-negligible advantage. Adversary B simulates the encryption queries of A as follows. When A submit a message M, B forwards the

pair of message ($M_0 = M, M_1 = M$) block by block. This gives access to an encryption oracle. The oracle queries of A are transmitted to the challenge oracle without modification by B. This simulation of the block encryption oracle of A is perfect. Finally, B transmits the bit guessed by A. Since A wins the LORS game with non-negligible advantage, consequently B wins the FTG game with non-negligible advantage.

Now, we prove that FTG-BCPA-D implies LORC-BCPA. The proof goes by contradiction. Assume for the sake of contradiction that a BCPA adversary A wins the LORS game with non-negligible advantage. We turn it into a BCPA attacker B, winning the FTG game also with non-negligible advantage. The FTG attacker picks at random i in $\{1, \ldots, q\}$. He runs the LORS-BCPA adversary and answers its encryption oracle queries by encrypting the first message thanks to its encryption oracle in the find phase, until the point at which it makes the ith encryption oracle query which we denote (M_0^i, M_1^i). To encrypt the pair of messages (M_0^i, M_1^i), the FTG-BCPA-D adversary queries its FTG block encryption oracle in the challenge phase and receives block by block the ciphertext C. Then, he answers block by block the encryption of the LORS adversary to the ith pair by forwarding C. Then, the same simulation as in the find phase is performed answering pair of messages by encrypting the right message. Clearly, $t' = t$, $q' = q$ and $\mu' = \mu$.

We can compute the advantage of the FTG attacker using a hybrid argument. We define a sequence of $q+1$ experiments: for $j = 0, \ldots, q$ define $\mathsf{Exp}^{\mathrm{hyb-atk-j}}_{\mathcal{SE},A}(k)$ to be an experiment in which one chooses $K \leftarrow \mathcal{K}(1^k)$ and runs A, answering the first j encryption oracle queries of A via $\mathcal{E}_K(\mathcal{LR}(.,.,0))$ and the rest via $\mathcal{E}_K(\mathcal{LR}(.,.,1))$. The output of the experiment is defined to be the output of A.

Now consider the experiment $\mathsf{Exp}^{\mathrm{ftg-bcpa-b}}_{\mathcal{SE},B}(k)$ where B is the algorithm. In this experiment, if $b = 0$, then $C = \mathcal{E}_K(M_0^i)$ and, in the simulation, A's output would be that of $\mathsf{Exp}^{\mathrm{hyb-atk-(i+1)}}_{\mathcal{SE},A}(k)$. On the other hand, if $b = 1$ then $C = \mathcal{E}_K(M_1^i)$ and, in the simulation, A's output would be the same as $\mathsf{Exp}^{\mathrm{hyb-atk-i}}_{\mathcal{SE},A}(k)$. Since i is chosen randomly from $\{1, \ldots, q\}$ by B, we have:

$$\begin{aligned}
\mathsf{Adv}^{\mathrm{ftg-bcpa}}_{\mathcal{SE},B}(k) &= (1/q) \cdot \sum_{i=0}^{q-1} (\Pr[\mathsf{Exp}^{\mathrm{hyb-atk-i}}_{\mathcal{SE},A}(k)] - \Pr[\mathsf{Exp}^{\mathrm{hyb-atk-(i+1)}}_{\mathcal{SE},A}(k)]) \\
&= (1/q) \cdot (\Pr[\mathsf{Exp}^{\mathrm{hyb-atk-0}}_{\mathcal{SE},A}(k)] - \Pr[\mathsf{Exp}^{\mathrm{hyb-atk-q}}_{\mathcal{SE},A}(k)]) \\
&= (1/q) \cdot (\mathsf{Adv}^{\mathrm{lors-bcpa}}_{\mathcal{SE},A}(k))
\end{aligned}$$

Since A is an arbitrary adversary, the claimed relation in the advantage functions follows. □