Security bound for CTR-ACPKM internally re-keyed encryption mode

Liliya R. Akhmetzyanova, Evgeny K. Alekseev, and Stanislav V. Smyshlyaev
Crypto-Pro LLC, Moscow, Russia
{lah,alekseev,svs}@cryptopro.ru

Abstract

In 2018 the CTR-ACPKM internally re-keyed block cipher mode was adopted in Russian Standardization System and must pass through the last formal standardization stages in IETF. The main distinctive feature of this mode is that during each message processing, the key, used for data blocks transformation, is periodically changed. In the current paper we obtained the security bound for this mode in the standard IND-CPNA security model.

Keywords: block cipher mode of operation, CTR, re-keying, provable security

1 Introduction

The effectiveness of many cryptanalytic methods (see, e.g. [14, 11, 15]) depends heavily on amount of data processed under a single key, therefore this amount of data should be limited. A certain maximum amount of data, which can be safely encrypted under a single key, is called «key lifetime». The trivial way to increasing the key lifetime (such as renegotiation) can reduce the total performance due to termination of application data transmission, the use of random number generators and many other resource-intensive additional calculations.

For the protocols based on block ciphers an efficient way to increasing the key lifetime is to use various re-keying mechanisms. Re-keying mechanisms can be applied on the different protocol levels: on the block cipher level (*fresh re-keying* [13]), on the block cipher mode of operation level (*internal re-keying* [7]), and on the message processing level (*external re-keying* [7]). From the viewpoint of cryptographic and operational properties each of these approaches has its own advantages and disadvantages (see [17] for details). For instance, the external re-keying approach doesn't require the development of new block ciphers or modes of operation and allows to apply a quite simple modular security analysis for resulting protocol [5], while the fresh re-keying approach often changes the internal structure of the used block cipher, that requires a nontrivial security analysis [13]. In the Russian protocols, the internal re-keying approach is widely spread. For example, it is used in the protocols TLS [3], IPsec [1], CMS [2]. This approach is associated with the development of a special class of *internally re-keyed block cipher modes of operation*. Their main feature is that during each message processing, the key, used for data blocks transformation, is periodically changed.

The current paper contains the security analysis of the CTR-ACPKM internally re-keyed mode, which was adopted in Russian Standardization System and is currently being considered in IETF. In addition, the CTR-ACPKM mode is also supposed to be used in the Russian ciphersuites of the TLS 1.2 protocol [4]. The analysis of the CTR-ACPKM mode was carried out in the paradigm of provable security, in other words, lower security bound was obtained in security model relevant for encryption modes (the IND-CPNA model [9, 16]).

The proof for the CTR-ACPKM mode is similar to the proof for the GCM-ACPKM mode presented in [7], since the GCM-ACPKM encryption part is based on the CTR-ACPKM mode. However, the bounds for the GCM-ACPKM mode [7] are expressed in the term of the maximum plaintext length, while the current paper contains tighter bound for CTR-ACPKM in the term of the total plaintext length. This bound was obtained using the new more clear proof that simplifies verification and comparison.

2 Preliminaries and Basic Security Notions

By $\{0,1\}^u$ we denote the set of u-component bit strings and by $\{0,1\}^*$ we denote the set of all bit strings of finite length. Let 0^u be the string, consisting of u zeros. For bit strings U and V we denote by $U\|V$ their concatenation. Let $|U|$ be the bit length of the string U. We denote by $|U|_u = \lceil |U|/u \rceil$ the length of the string U in u-bit blocks.

For a bit string U and a positive integer $l \leqslant |U|$ let $\mathrm{msb}_l(U)$ ($\mathrm{lsb}_l(U)$) be the string, consisting of the leftmost (rightmost) l bits of U. For nonnegative integers l and i let $\mathrm{str}_l(i)$ be l-bit representation of i with the least significant bit on the right. For a nonnegative integer l and a bit string $U \in \{0,1\}^l$ let $\mathrm{int}(U)$ be an integer i such that $\mathrm{str}_l(i) = U$. Let $\mathrm{Inc}(U)$ be the function, which takes the input $U \in \{0,1\}^u$ and outputs the string $\mathrm{msb}_{u/2}(U)\|\mathrm{str}_{u/2}(\mathrm{int}(\mathrm{lsb}_{u/2}(U)) + 1 \bmod 2^{u/2})$.

For any set S, define $Perm(S)$ as the set of all bijective mappings on S (permutations on S), and $Func(S)$ as the set of all mappings from S to S. A block cipher E (or just a cipher) with block size n and key size k is the permutation family $\big(E_K \in Perm(\{0,1\}^n) \mid K \in \{0,1\}^k\big)$, where K is a key. If the value s is chosen from a set S uniformly at random, then we denote $s \xleftarrow{\mathcal{U}} S$.

For a bit string U we denote by $U[i] \in \{0,1\}^n$, $1 \leqslant i \leqslant |U|_n - 1$, and $U[|U|_n] \in \{0,1\}^h$, $h \leqslant n$, such strings that $U = U[1]\|U[2]\|\ldots\|U[|U|_n]$ and call them «blocks» of the string U.

We model an adversary using an interactive probabilistic algorithm that has access to one or more oracles. The resources of A are measured in terms of time and query complexities. For a fixed model of computation and a method of encoding the time complexity includes the description size of A. The query complexity usually includes the number of queries and the maximum length of queries or the total length of queries. Denote by $\mathsf{Adv}^{\mathrm{M}}_{\mathrm{S}}(A)$ the measure of the success of the adversary A in realizing a certain threat, defined by the model M, for the cryptographic scheme S. The formal definition of this measure will be given in each specific case.

A block cipher is usually regarded as a family of permutations, which on its own does not provide such application-level security properties as integrity, confidentiality or authenticity (see, e.g. [8]). The cipher is usually used as a base function for constructing other schemes

or protocols that solve the above-mentioned cryptographic challenges. The security of such constructions is proven under assumption that the block cipher is secure. In a paradigm of the practice-oriented provable security (see [10]) we should quantify the security as a function of the used cipher security for appropriate models. Standard security model for block ciphers is PRP-CPA («Pseudo Random Permutation under Chosen Plaintext Attack») (see, e.g. [8]). The formal definition can be found in Appendix B.

3 Internally Re-keyed CTR-ACPKM mode

Internal re-keying is an approach to increasing the key lifetime by using a transformation of a data processing key (a section key) during each separate message processing. Such key transformation mechanisms are built into the particular base mode of operation and depend heavily on the internal features of its structure, therefore they are called «internal» re-keying mechanisms.

Each message is processed starting with the same key (the first section key) and each section key is updated using the certain key update technique after processing certain amount of message blocks (a section). The mode parameter, hereinafter called section size and denoted as N, is measured in blocks and is fixed within a specific protocol depending on the requirements of the system capacity and the key lifetime.

In this section we define the CTR-ACPKM internally re-keyed mode with section size N (CTR-ACPKM$_N$). The mode structure is shown in Figure 1. During the processing of the input plaintext P of the block length $m = |P|_n$ under the initial key K the message is divided into $l = \lceil m/N \rceil$ sections (denoted as $P = P^1\|P^2\|...\|P^l$, where $P^i \in \{0,1\}^{nN}$ for $i \in \{1,2,...,l-1\}$, $P^l \in \{0,1\}^r$, $r \leqslant nN$). The first section of each message is processed under the section key $K^1 = K$ using the CTR subroutine. The $(i+1)$-th section of message is continued to be processed using the CTR subroutine under the K^{i+1} section key, which is calculated using ACPKM transformation as follows:

$$K^{i+1} = \text{ACPKM}(K^i) = \text{msb}_k(E_{K^i}(D_1)\| \dots \|E_{K^i}(D_s)),$$

where $s = \lceil k/n \rceil$ and $D_1, D_2, \dots, D_s \in \{0,1\}^n$ are arbitrary pairwise different constants such that the $(n/2)$-th bit (counting from the right) side of each D_i is equal to 1. The plaintext length must be at most $2^{n/2-1}$ blocks. Note that the internal state (counter) of the CTR-ACPKM$_N$ mode is not reset for each new section and the condition on the $D_1, D_2, \dots, D_s$ constants allows to prevent collisions of block cipher permutation inputs in cases of key transformation and message processing (see [17, 6] for details).

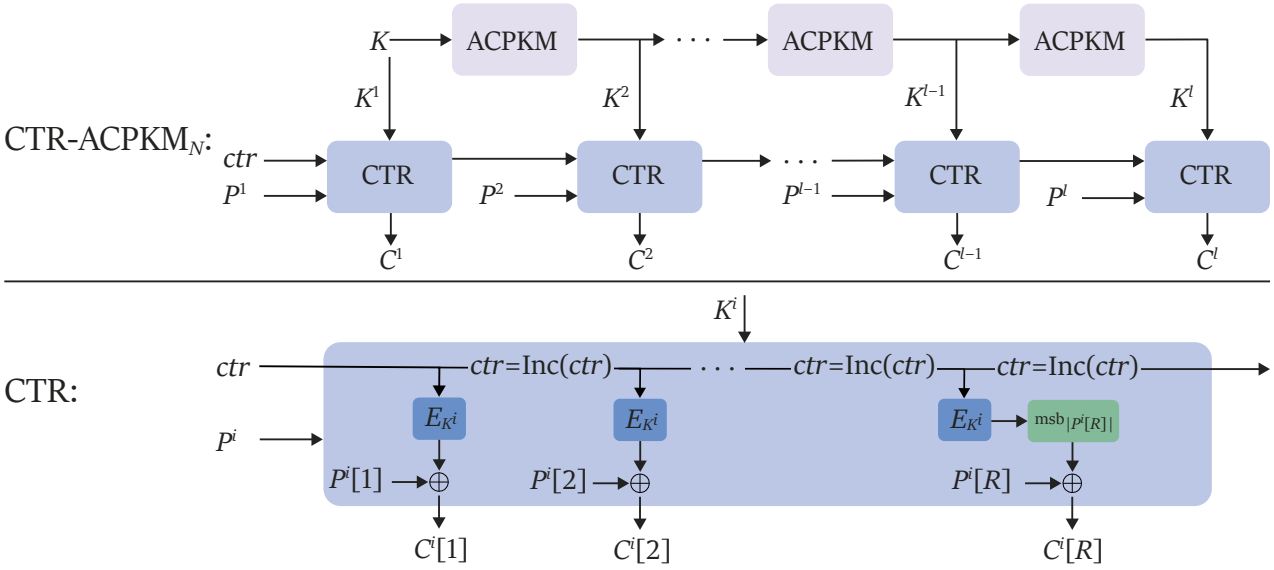

Figure 1: The CTR-ACPKM$_N$ encryption mode takes a key $K \in \{0,1\}^k$, a nonce $IV \in \{0,1\}^{n/2}$ (here $ctr = IV\|0^{n/2}$) and a plaintext $P \in \{0,1\}^*$ as inputs and returns a ciphertext $C \in \{0,1\}^{|P|}$ as an output. The ACPKM subroutine generates next section key K^{i+1} using the previous section key K^i. The CTR subroutine processes sections $P^1, \ldots, P^l$ of the plaintext P under the corresponding section keys. Each section consists of R blocks, where $R = N$ for intermediate sections and $R \leqslant N$ for a final section.

3.1 Security Analysis of the CTR-ACPKM mode

The security analysis of the CTR-ACPKM mode has been carried out in the IND-CPNA («Indistinguishability under Chosen Plaintext and Nonce Attack») model, which is strictly formalized in Appendix B. This model is similar to the standard IND-CPA security model [9] but considers nonce-respecting adversaries [16]. Informally, in this model the adversary has to distinguish the obtained ciphertexts from the «garbage», having the capability to adaptively choose plaintexts and nonces (in a unique manner). The IND-CPNA is the strongest standard security model (known at the time) which allows to analyze the cryptographic properties of the mode from the viewpoint of computational «closeness» to the ideal one-time pad encryption [16].

Theorem 3.1. *Let N be the parameter of CTR-ACPKM mode. Then for any adversary A with time complexity at most t that makes queries, where the maximum message length is at most m ($m \leqslant 2^{n/2-1}$) blocks and the total message length is at most σ blocks, there exists an adversary B such that*

$$\mathsf{Adv}^{IND\text{-}CPNA}_{CTR\text{-}ACPKM_N}(A) \leqslant l \cdot \mathsf{Adv}^{PRP\text{-}CPA}_{E}(B) + \frac{(\sigma_1 + s)^2 + \ldots + (\sigma_{l-1} + s)^2 + (\sigma_l)^2}{2^{n+1}}$$

where $s = \lceil k/n \rceil$, $l = \lceil m/N \rceil$, σ_j is the total data block length processed under the section key K^j and $\sigma_j \leqslant 2^{n-1}$, $\sigma_1 + \ldots + \sigma_l = \sigma$. The adversary B makes at most $\sigma_1 + s$ queries. Furthermore, the time complexity of B is at most $t + cn(\sigma + ls)$, where c is a constant that depends only on the model of computation and the method of encoding.

The proof can be found in Appendix D.

3.2 Comparative bounds analysis

In the current section we consider the obtained bound for the internally re-keyed CTR-ACPKM mode in more detail and compare it with the security bound for the CTR (see [9]) mode without re-keying. The bounds are presented in Table 1. The bound for the internally re-keyed mode shows that the insecurity of the mode reaches minimum if $\sigma_1 = \ldots = \sigma_l$, i.e. if all messages are of the same length.

Mode	$\mathsf{Adv}^{\text{IND-CPNA}}_{\text{Mode}}(A)$
CTR	$\approx \frac{\sigma^2}{2^{n+1}}$
CTR-ACPKM$_N$	$\approx \frac{(\sigma_1 + s)^2 + \ldots + \sigma_l^2}{2^{n+1}}$

Table 1: Security bounds for the CTR mode and the internally re-keyed CTR-ACPKM$_N$ mode with the section size N (under secure block cipher). Here $s = \lceil k/n \rceil$, σ is the total plaintexts block length, m is the maximum plaintext block length and σ_j is the total block length of data, processed under the section key K^j ($\sigma_1 + \ldots + \sigma_l = \sigma$, where $l = \lceil m/N \rceil$).

Consider the case $l = 1$ (no re-keying during message processing). Note, that for the CTR and CTR-ACPKM$_N$ modes the bounds are equal that is explained by total equivalence of the considered modes.

4 Conclusion

Results obtained in this paper show that, under security of the used block cipher, the cryptographic properties of the CTR-ACPKM mode are improved compared to the properties of the associated CTR mode without internal re-keying for all practical cases.

References

[1] "Information processing systems. Cryptographic protection. Technical specification for the use of GOST 28147-89 for attachments encryptions in the IPSEC ESP protocol.", Technical specification, Federal Agency for Technical Regulation and Metrology (ROSSTANDART), 2013 (Russian).

[2] "Information technology. Cryptographic protection of information. Using algorithms GOST 28147-89, GOST R 34.11 and GOST R 34.10 in cryptographic messages of the CMS format.", Recommendations for standardization, Federal Agency for Technical Regulation and Metrology (ROSSTANDART), 2014 (Russian).

[3] "Information technology. Cryptographic protection of information. Using ciphersuites based on GOST 28147-89 for Transport Layer Security (TLS).", Recommendations for standardization, Federal Agency for Technical Regulation and Metrology (ROSSTANDART), 2014 (Russian).

[4] "Information technology. Cryptographic protection of information. The use of Russian cryptographic algorithms in the Transport Lyer Security protocol (TLS 1.2).", Recommendations for

standardization, Technical Committee For Standardization «Cryptography and Security Mechanisms», 2017 (The project of recommendations on standardization).

[5] M. Bellare, M. Abdalla, "Increasing the Lifetime of a Key: A Comparative Analysis of the Security of Re-keying Techniques", Advances in Cryptology — ASIACRYPT 2000, Lecture Notes in Computer Science, **1976**, eds. Okamoto, Tatsuaki, Springer, Berlin, Heidelberg, 2000, 546–559.

[6] L. Ahmetzyanova, E. Alekseev, I. Oshkin, S. Smyshlyaev, L. Sonina, "On the properties of the CTR encryption mode of the Magma and Kuznyechik block ciphers with re-keying method based on CryptoPro Key Meshing", CTCrypt 2016, Mat. Vopr. Kriptogr., **8**, 2017, 39–50.

[7] L. Ahmetzyanova, E. Alekseev, I. Oshkin, S. Smyshlyaev, "Increasing the Lifetime of Symmetric Keys for the GCM Mode by Internal Re-keying", *IACR ePrint Archive*, 2017, Report 2017/697, https://eprint.iacr.org/2017/697.

[8] M. Bellare and P. Rogaway, "Introduction to modern cryptography, chapter 2: Block Ciphers", 2004, http://www-cse.ucsd.edu/users/mihir/cse207.

[9] M. Bellare and P. Rogaway, "Introduction to modern cryptography, chapter 4: Symmetric Encryption", 2004, http://www-cse.ucsd.edu/users/mihir/cse207.

[10] M. Bellare, "Practice-Oriented Provable-Security", Lectures on Data Security, EEF School 1998, Lecture Notes in Computer Science, **1561**, eds. I. Damgård, Springer, Berlin, Heidelberg, 1999, 1–15.

[11] E. Biham and A. Shamir, "Differential Cryptanalysis of DES-like Cryptosystems", Advances in Cryptology — CRYPTO 1990, Lecture Notes in Computer Science, **537**, eds. A. Menezes, S. Vanstone, Springer, Berlin, Heidelberg, 1991, 2–21.

[12] D. Chang and M. Nandi, "A Short Proof of the PRP/PRF Switching Lemma", *IACR ePrint Archive*, 2008, Report 2008/078, https://eprint.iacr.org/2008/078.

[13] S. Dziembowski, S. Faust, G. Herold, A. Journault, D. Masny, and F.-X. Standaert., "Towards Sound Fresh Re-Keying with Hard (Physical) Learning Problems", *IACR ePrint Archive*, 2016, Report 2016/573, https://eprint.iacr.org/2016/573.

[14] M. Matsui, "Linear Cryptanalysis Method for DES Cipher", Advances in Cryptology — EUROCRYPT 1993, Lecture Notes in Computer Science, **765**, eds. T. Helleseth, Springer, Berlin, Heidelberg, 1994, 402–415.

[15] C. Ramsay and J. Lohuis., "TEMPEST attacks against AES. Covertly stealing keys for 200 euro", 2017.

[16] P. Rogaway, "Nonce-Based Symmetric Encryption", Fast Software Encryption (FSE 2004), Lecture Notes in Computer Science, **3017**, eds. B Roy, and W Meier, Springer, Berlin, Heidelberg, 2004, 348–358.

[17] S. Smyshlyaev, "Re-keying Mechanisms for Symmetric Keys draft-irtf-cfrg-re-keying-13", Internet-Draft (Work in Progress), Internet Engineering Task Force (IETF), January 2018, https://tools.ietf.org/html/draft-irtf-cfrg-re-keying-13.

A Additional notations

Introduce additional notions which are used in further proofs. For an algorithm A by $A \Rightarrow s$ we denote an event, that occurs if the algorithm A returns value s as its execution result. Denote by $A^{\mathcal{O}_1,\mathcal{O}_2,\cdots}$ an adversary A that interacts with oracles $\mathcal{O}_1, \mathcal{O}_2, \ldots$ by making queries. Notation $b \xleftarrow{\$} A^{\mathcal{O}_1,\mathcal{O}_2,\cdots}$ means that the algorithm A, after interacting with oracles $\mathcal{O}_1, \mathcal{O}_2, \ldots$, outputs bit $b \in \{0,1\}$. For the deterministic algorithm A by $A \to x$ or by $x \leftarrow A$ is denoted that A returns the value x.

For any set S and distribution $\mathcal{D}$ on S by $s \xleftarrow{\mathcal{D}} S$ we denote that value s is chosen in set S by random according to the distribution $\mathcal{D}$.

B Security Models

For a cipher E with parameters n and k define

$$\mathsf{Adv}_E^{\text{PRP-CPA}}(A) = \Pr\left[\mathbf{Exp}_E^{\text{PRP-CPA}-1}(A) = 1\right] - \Pr\left[\mathbf{Exp}_E^{\text{PRP-CPA}-0}(A) = 1\right],$$

where the experiments $\mathbf{Exp}_E^{\text{PRP-CPA}-1}(A)$ and $\mathbf{Exp}_E^{\text{PRP-CPA}-0}(A)$ are defined in the following way:

$\underline{\mathbf{Exp}_E^{\text{PRP-CPA}-b}(A)}$
if $b = 0$ **then**
  $P \xleftarrow{\mathcal{U}} Perm(\{0,1\}^n)$
else
  $K \xleftarrow{\mathcal{U}} \{0,1\}^k$
$b' \xleftarrow{\$} A^{\mathsf{P}^b}$
return b'

$\underline{\text{Oracle } \mathsf{P}^b(M),\ M \in \{0,1\}^n}$
if $b = 0$ **then**
  return $P(M)$
else
  return $E_K(M)$

The PRF notion is defined in the same way as PRP-CPA except for the random permutation $P \xleftarrow{\mathcal{U}} Perm(\{0,1\}^n)$, which is replaced by the random function $F \xleftarrow{\mathcal{U}} Func(\{0,1\}^n)$:

$$\mathsf{Adv}_E^{\text{PRF}}(A) = \Pr\left[\mathbf{Exp}_E^{\text{PRF}-1}(A) = 1\right] - \Pr\left[\mathbf{Exp}_E^{\text{PRF}-0}(A) = 1\right].$$

Definition B.1. A symmetric encryption scheme SE *for a set of keys* $\mathcal{K}$*, a set of plaintexts* $\mathcal{P}$*, a set of ciphertexts* $\mathcal{C}$*, and a set of nonces* $\mathcal{N}$ *consists of three algorithms* $\{\mathsf{SE.K}, \mathsf{SE.E}, \mathsf{SE.D}\}$*, as follows:*

- $\mathsf{SE.K}() \xrightarrow{\$} K$*: The randomized key generation algorithm that returns a key* $K \in \mathcal{K}$*. This algorithm is often defined by taking security parameter as input. But in this work it will be omitted.*
- $\mathsf{SE.E}(K, P, IV) \to C$*: The deterministic encryption algorithm, takes a key* $K \in \mathcal{K}$*, a plaintext* $P \in \mathcal{P}$*, and a nonce* $IV \in \mathcal{N}$ *to return a ciphertext* $C \in \mathcal{C}$*.*
- $\mathsf{SE.D}(K, C, IV) \to P$*: The deterministic decryption algorithm, takes a key* $K \in \mathcal{K}$*, a ciphertext* $C \in \mathcal{C}$*, and a nonce* $IV \in \mathcal{N}$ *to return a plaintext* $P \in \mathcal{P}$*.*

Definition B.2. *Let* $\mathsf{SE} = \{\mathsf{SE.K},\ \mathsf{SE.E},\ \mathsf{SE.D}\}$ *be a symmetric encryption scheme and let* A *be an adversary. The advantage of* A *for the scheme* SE *in the IND-CPNA model (IND-CPNA-*advantage*) is defined as*

$$\mathsf{Adv}^{\mathit{IND\text{-}CPNA}}_{\mathsf{SE}}(A) = \Pr\left[\mathbf{Exp}^{\mathit{IND\text{-}CPNA-1}}_{\mathsf{SE}}(A) \Rightarrow 1\right] - \Pr\left[\mathbf{Exp}^{\mathit{IND\text{-}CPNA-0}}_{\mathsf{SE}}(A) \Rightarrow 1\right],$$

where the experiment $\mathbf{Exp}^{\mathit{IND\text{-}CPNA-b}}_{\mathsf{SE}}(A),\ b \in \{0,1\}$ *is defined as follows*

$\underline{\mathbf{Exp}^{\mathit{IND\text{-}CPNA-b}}_{\mathsf{SE}}(A)}$
$K \xleftarrow{\$} \mathsf{SE.K}()$
$b' \xleftarrow{\$} A^{\mathsf{Encrypt}^b}$
return b'

$\underline{\mathsf{Oracle}\ \ \mathsf{Encrypt}^b(P, IV)}$
$C \xleftarrow{\$} \mathsf{SE.E}(K, P, IV)$
if $b = 0$ ***then***
  $R \xleftarrow{\mathcal{U}} \{0,1\}^{|C|}$
  return R
return C

C Internally Re-keyed Mode

$\underline{\text{CTR-ACPKM}_N(K, IV, X)}$
$CTR \leftarrow IV \| \text{str}_{n/2}(0)$
$b \leftarrow |X|_n$
$K^1 \leftarrow K$
for $j \leftarrow 2$ to $\lceil b/N \rceil$ do
  $K^j \leftarrow \text{ACPKM}(K^{j-1})$
for $i \leftarrow 1$ to b do
  $j \leftarrow \lceil i/N \rceil$
  $CTR_i \leftarrow \pi(CTR, i-1)$
  $G_i \leftarrow E_{K^j}(CTR_i)$
$Y \leftarrow X \oplus \text{msb}_{|X|}(G_1 \| \ldots \| G_b)$
return Y

$\underline{\text{CTR-ACPKM}_N.\mathsf{K}()}$
Key generation:
  $K \xleftarrow{\mathcal{U}} \{0,1\}^k$
return K

$\underline{\text{CTR-ACPKM}_N.\mathsf{E}(K, IV, M)}$
Ciphertext computation:
  $C \leftarrow \text{CTR-ACPKM}_N(K, IV, M)$
return C

$\underline{\text{CTR-ACPKM}_N.\mathsf{D}(K, IV, C)}$
Plaintext computation:
  $M \leftarrow \text{CTR-ACPKM}_N(K, IV, C)$
return M

Pseudocode 2: The CTR-ACPKM Mode.

D Security Analysis of the CTR-ACPKM mode

Proof. Define hybrid experiments $Hybrid_j(A),\ j = 0, 1, \ldots, \lceil m/N \rceil$. In the experiment $Hybrid_j(A)$ the oracle in the IND-CPNA notion is replaced by the oracle, which operates in the following way:

- The oracle chooses key $K^{j+1} \xleftarrow{\mathcal{U}} \{0,1\}^k$;
- In response to a query (P, IV) the oracle returns C, where

$$C = M \oplus \mathrm{msb}_{|P|}(C' \| C^{j+1} \| \ldots \| C^{\lceil m/N \rceil}),$$

  here $C' \xleftarrow{\mathcal{U}} \{0,1\}^{nNj}$ and $C^i,\ i = (j+1), \ldots, \lceil m/N \rceil$, is the result of the i-th section processing under the K^i section key. Note that the $(j+1)$-th section is processed under the «truly» random K^{j+1} key and each next key is produced according to ACPKM.

The result of any experiment described above is what the adversary A returns as a result.

Note that the $Hybrid_0(A)$ experiment totally coincides with the $\mathbf{Exp}^{\text{IND-CPNA}-1}_{\text{CTR-ACPKM}_N}(A)$ experiment, and the experiment $Hybrid_{\lceil m/N \rceil}(A)$ coincides with $\mathbf{Exp}^{\text{IND-CPNA}-0}_{\text{CTR-ACPKM}_N}(A)$ experiment, i.e. the following inequalities hold:

$$\Pr\left[Hybrid_0(A) \Rightarrow 1\right] = \Pr\left[\mathbf{Exp}^{\text{IND-CPNA}-1}_{\text{CTR-ACPKM}_N}(A) \Rightarrow 1\right],$$

$$\Pr\left[Hybrid_{\lceil m/N \rceil}(A) \Rightarrow 1\right] = \Pr\left[\mathbf{Exp}^{\text{IND-CPNA}-0}_{\text{CTR-ACPKM}_N}(A) \Rightarrow 1\right].$$

Construct a set of adversaries B_j, $j = 1, \ldots, \lceil m/N \rceil$, for the block cipher in the PRF model, which uses A as a black box.

After receiving a query (P, IV) from A the adversary B_j processes this query as in the $Hybrid_j(A)$ experiment but the encrypted blocks for masking the j-th section and blocks of the $(j+1)$-th section key are obtained by making queries to the oracle provided by the PRF experiment. Note that B_j, $j = 1, \ldots, \lceil m/N \rceil - 1$, makes at most $\sigma_j + s$ queries and $B_{\lceil m/N \rceil}$ makes at most $\sigma_{\lceil m/N \rceil}$ queries. The adversary B_j returns 1, if the adversary A returns 1, and returns 0, otherwise.

Note that

$$\Pr\left[\mathbf{Exp}^{\text{PRF}-1}_E(B_j) \Rightarrow 1\right] = \Pr\left[Hybrid_{j-1}(A) \Rightarrow 1\right],$$
$$\Pr\left[\mathbf{Exp}^{\text{PRF}-0}_E(B_j) \Rightarrow 1\right] = \Pr\left[Hybrid_j(A) \Rightarrow 1\right].$$

The last equality is proceeded from that the input blocks for producing the K^{j+1} section key and the input blocks for masking the j-th section are different for the random function. Therefore, the K^{j+1} variable distribution is statistically indistinguishable from the «truly» random one.

Then for the advantages of the adversaries B_j

$$\sum_{j=1}^{\lceil m/N \rceil} \mathsf{Adv}^{\text{PRF}}_E(B_j) = \sum_{j=1}^{\lceil m/N \rceil} \Pr\left[Hybrid_{j-1}(A) \Rightarrow 1\right] - \sum_{j=1}^{\lceil m/N \rceil} \Pr\left[Hybrid_j(A) \Rightarrow 1\right] =$$
$$= \Pr\left[Hybrid_0(A) \Rightarrow 1\right] - \Pr\left[Hybrid_{\lceil m/N \rceil}(A) \Rightarrow 1\right] = \mathsf{Adv}^{\text{IND-CPNA}}_{\text{CTR-ACPKM}_N}(A).$$

From the PRP/PRF switching lemma [12] for any block cipher E and any adversary B' making at most q queries we have

$$\mathsf{Adv}_E^{\text{PRF}}(B') \leqslant \mathsf{Adv}_E^{\text{PRP-CPA}}(B') + \frac{q(q-1)}{2^{n+1}} \leqslant \mathsf{Adv}_E^{\text{PRP-CPA}}(B') + \frac{q^2}{2^{n+1}}.$$

Thus,

$$\begin{aligned}\mathsf{Adv}^{\text{IND-CPNA}}_{\text{CTR-ACPKM}_N}(A) = \sum_{j=1}^{\lceil m/N \rceil} \mathsf{Adv}_E^{\text{PRF}}(B_j) \leqslant \sum_{j=1}^{\lceil m/N \rceil - 1} \left(\mathsf{Adv}_E^{\text{PRP-CPA}}(B_j) + \frac{(\sigma_i + s)^2}{2^{n+1}} \right) + \\ + \mathsf{Adv}_E^{\text{PRP-CPA}}(B_{\lceil m/N \rceil}) + \frac{(\sigma_{\lceil m/N \rceil})^2}{2^{n+1}} \leqslant \\ \leqslant \left\lceil \frac{m}{N} \right\rceil \mathsf{Adv}_E^{\text{PRP-CPA}}(B) + \frac{(\sigma_1 + s)^2 + \ldots + (\sigma_{\lceil m/N \rceil - 1} + s)^2 + (\sigma_{\lceil m/N \rceil})^2}{2^{n+1}},\end{aligned}$$

where B is an adversary which makes at most $\sigma_1 + s$ queries. The last relation is due to $\sigma_1 \geqslant \ldots \geqslant \sigma_{\lceil m/N \rceil}$ and $\mathsf{Adv}_E^{\text{PRP-CPA}}(B') \leqslant \mathsf{Adv}_E^{\text{PRP-CPA}}(B'')$ for such adversaries B' and B'' with the same computational resources that the queries number made by B' is less than the queries number made by B''. □