

Security bounds for standardized internally re-keyed block cipher modes and their practical significance

Liliya R. Akhmetzyanova,
Engineer-analyst,
CryptoPro LLC

Evgeny K. Alekseev, Grigory A. Karpunin,

Igor B. Oshkin, Grigory K. Sedov,

Stanislav V. Smyshlyaev, Ekaterina S. Smyshlyaeva



kriptografija 암호화 crittografia dumlál cripteagrafaiochta 密码 kriptografi cifrado פּרעגראַפיע מאַט מאַהע криптография криптография
 δαδλϱαηηυηιυν kryptografia зродітϱвгдϱооs криптография крϱтoγράφηη cryptographϱ 暗号化 kryptographie க்ரிப்டொகாஹி salauksen
 крϱтtαγραφία காரடாநஹீச kriptografija رمز نویسی kriptografija 암호화 crittografia dumlál cripteagrafaiochta 密码 kriptografi cifrado פּרעגראַפיע

1 **Key Lifetime** maδδλϱαηηυηιυν kryptografia зродітϱвгдϱооs криптография крϱтoγράφηη cryptographϱ 暗号化 kryptographie க்ரிப்டொகாஹி salauksen
 крϱтtαγραφία காரடாநஹீச kriptografija رمز نویسی kriptografija 암호화 crittografia dumlál cripteagrafaiochta 密码 kriptografi cifrado פּרעגראַפיע

2 **Re-keying Mechanisms** kryptografia δαδλϱαηηυηιυν kryptografia зродітϱвгдϱооs криптография крϱтoγράφηη cryptographϱ 暗号化 kryptographie க்ரிப்டொகாஹி salauksen
 крϱтtαγραφία காரடாநஹீச kriptografija رمز نویسی kriptografija 암호화 crittografia dumlál cripteagrafaiochta 密码 kriptografi cifrado פּרעגראַפיע

3 **Standardized Internally Rekeyed Modes** kryptografia δαδλϱαηηυηιυν kryptografia зродітϱвгдϱооs криптография крϱтoγράφηη cryptographϱ 暗号化 kryptographie க்ரிப்டொகாஹி salauksen
 крϱтtαγραφία காரடாநஹீச kriptografija رمز نویسی kriptografija 암호화 crittografia dumlál cripteagrafaiochta 密码 kriptografi cifrado פּרעגראַפיע

4 **Security Analysis** kryptografia δαδλϱαηηυηιυν kryptografia зродітϱвгдϱооs криптография крϱтoγράφηη cryptographϱ 暗号化 kryptographie க்ரிப்டொகாஹி salauksen
 крϱтtαγραφία காரடாநஹீச kriptografija رمز نویسی kriptografija 암호화 crittografia dumlál cripteagrafaiochta 密码 kriptografi cifrado פּרעגראַפיע

• **Security Analysis of CTR-ACPKM mode**
 • **Security Analysis of OMAC-ACPKM-Master mode** kryptografia δαδλϱαηηυηιυν kryptografia зродітϱвгдϱооs криптография крϱтoγράφηη cryptographϱ 暗号化 kryptographie க்ரிப்டொகாஹி salauksen
 крϱтtαγραφία காரடாநஹீச kriptografija رمز نویسی kriptografija 암호화 crittografia dumlál cripteagrafaiochta 密码 kriptografi cifrado פּרעגראַפיע

5 **Practical Meaning of Proofs** kryptografia δαδλϱαηηυηιυν kryptografia зродітϱвгдϱооs криптография крϱтoγράφηη cryptographϱ 暗号化 kryptographie க்ரிப்டொகாஹி salauksen
 крϱтtαγραφία காரடாநஹீச kriptografija رمز نویسی kriptografija 암호화 crittografia dumlál cripteagrafaiochta 密码 kriptografi cifrado פּרעגראַפיע

maδδλϱαηηυηιυν kryptografia зродітϱвгдϱооs криптография крϱтoγράφηη cryptographϱ 暗号化 kryptographie க்ரிப்டொகாஹி salauksen
 крϱтtαγραφία காரடாநஹீச kriptografija رمز نویسی kriptografija 암호화 crittografia dumlál cripteagrafaiochta 密码 kriptografi cifrado פּרעגראַפיע

kriptografija 암호화 crittografia dumlál cripteagrafalochta 密码 kriptografi cifrado מפתח מלחמה kriptografija criptografia
 ծածկագրություն kryptografia ვრცელდება kriptografia крптография криптография cryptography 暗号化 kryptographie किप्टोग्राफी salauksen

Motivation

The effectiveness of many cryptanalytic methods depends heavily on amount of data processed under a single key, therefore this amount of data should be limited.

A certain maximal amount of data, which can be safely encrypted under a single key, is called «**key lifetime**». This amount is limited by bounds coming from

- general combinatorial properties of cipher modes of operation;
 a recent example (3DES, limit = 8 MB) — Sweet32 attack,
<https://sweet32.info/>.
- estimations of material needed for success of various cryptanalytic methods for a used cipher (linear, algebraic, differential etc.);
- side-channel cryptanalytic methods of block ciphers;
 recent example (AES, limit \lesssim 160 MB) — “TEMPEST attacks against AES”
 paper, <https://www.fox-it.com>.

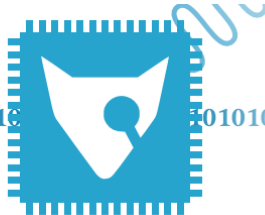
mật mã học kriptografija criptografia ծածկագրություն kryptografia ვრცელდება kriptografia крптография криптография cryptography 暗号化
 kryptographie किप्टोग्राफी salauksen крптография การเข้ารหัส kriptografija رمز نویسی kriptografija 암호화 crittografia dumlál cripteagrafalochta 密

Motivation

The effectiveness of many cryptanalytic methods depends heavily on amount of data processed under a single key, therefore this amount of data should be limited.

A certain maximal amount of data, which can be safely encrypted under a single key, is called «**key lifetime**». This amount is limited by bounds coming from

- general combinatorial properties of cipher modes of operation;
a recent example (3DES, limit = 8 MB) — Sweet32 attack,
<https://sweet32.info/>.
- estimations of material needed for success of various cryptanalytic methods for a used cipher (linear, algebraic, differential etc.);
- side-channel cryptanalytic methods of block ciphers;
recent example (AES, limit $\lesssim 160$ MB) — “TEMPEST attacks against AES”
paper, <https://www.fox-it.com>.



1010101010010101

1010101010010101

TEMPEST attacks against AES

Covertly stealing keys for €200

Overview

Side-channel attacks can recover secret keys from cryptographic algorithms (including the pervasive AES) using measurements such as power use. However, these previously-known attacks on AES tend to require unrestricted, physical access to the device. Using improved antenna and signal processing, Fox-IT and Riscure show how to covertly recover the encryption key from two realistic AES-256 implementations while:

1. Attacking at a distance of up to 1 *m* (30 *cm* in realistic conditions; "TEMPEST"),
2. Using minimal equipment (fits in a jacket pocket, costs less than €200) and
3. Needing only a few minutes (5 minutes for 1 *m* and 50 seconds for 30 *cm*).

Trivial ways to increasing the key lifetime (such as renegotiation) can reduce the total performance due to additional resource-intensive calculations.

κρυπτογράφηση cryptography 暗号化 kryptographie क्रिप्टोग्राफी salauksen kryptografia การเข้ารหัส kriptografija رمز نویسی kriptografiju 암호화

kriptografija 암호화 crittografia dumlál críteagrafaiochta 密码 kriptografi cifrado מפתח מפתח māt mā hoc криптография criptografia δαδλϑαϕηυνηυνην kryptografia ჯრბძღვღვღვღვღვ kriptografia крyптoгpафия cryptography 暗号化 kryptographie किप्टोग्राफी salauksen

Renegotiation is not a solution

Trivial ways to increasing the key lifetime (such as renegotiation) can reduce the total performance due to additional resource-intensive calculations.

кρyптoгpафия cryptography 暗号化 kryptographie किप्टोग्राफी salauksen крyптoгpафия การฉานรหัส kriptografija رمز نویسی kriptografija 암호화

Re-keying

An efficient way to increase the key lifetime can be the usage of re-keying mechanisms (using block cipher $E = (E_K \in Perm(\{0, 1\}^n) \mid K \in \{0, 1\}^k)$ as a black-box primitive):

- on the block cipher mode of operation level (**internal re-keying**);
- on the message processing level (**external re-keying**).

crittografia dumlál críteagrafaiochta 密码 kriptografi cifrado מפתח מפתח māt mā hoc криптография criptografia δαδλϑαϕηυνηυνην kryptografia

Concepts of internal and external re-keying approaches are described in «Increasing the Lifetime of Symmetric Keys for the GCM Mode by Internal Re-keying» provided by us at <https://eprint.iacr.org/2017/697.pdf>

māt mā hoc криптография criptografia δαδλϑαϕηυνηυνην kryptografia ჯრბძღვღვღვღვღვ kriptografia крyптoгpафия cryptography 暗号化 kryptographie किप्टोग्राफी salauksen крyптoгpафия การฉานรหัส kriptografija رمز نویسی kriptografija 암호화 crittografia dumlál críteagrafaiochta 密码

kriptografija 암호화 crittografia dumlál criptagrafaiochta 密码 kriptografi cifrado תּיפוסת מַתְמָטִיקַת הַמִּתְמָטִיקָה криптография криптографический cryptography 暗号化 kryptographie किप्टोग्राफी salauksen

Renegotiation is not a solution

Trivial ways to increasing the key lifetime (such as renegotiation) can reduce the total performance due to additional resource-intensive calculations.

криптография криптографический cryptography 暗号化 kryptographie किप्टोग्राफी salauksen криптография การคำนวณ kriptografija رمز نویسی kriptografija 암호화

Re-keying

An efficient way to increase the key lifetime can be the usage of re-keying mechanisms (using block cipher $E = (E_K \in Perm(\{0, 1\}^n) \mid K \in \{0, 1\}^k)$ as a black-box primitive):

- on the block cipher mode of operation level (**internal re-keying**);
- on the message processing level (**external re-keying**).

crittografia dumlál criptagrafaiochta 密码 kriptografi cifrado תּיפוסת מַתְמָטִיקַת הַמִּתְמָטִיקָה криптография криптографический cryptography 暗号化 kryptographie किप्टोग्राफी salauksen

Concepts of internal and external re-keying approaches are described in «Increasing the Lifetime of Symmetric Keys for the GCM Mode by Internal Re-keying» provided by us at <https://eprint.iacr.org/2017/697.pdf>

mat mē hoc криптография crittografia dumlál criptagrafaiochta 密码 kriptografi cifrado תּיפוסת מַתְמָטִיקַת הַמִּתְמָטִיקָה криптография криптографический cryptography 暗号化 kryptographie किप्टोग्राफी salauksen криптография การคำนวณ kriptografija رمز نویسی kriptografija 암호화 crittografia dumlál criptagrafaiochta 密码

Trivial ways to increasing the key lifetime (such as renegotiation) can reduce the total performance due to additional resource-intensive calculations.

κρυπτογράφηση cryptography 暗号化 kryptographie क्रिप्टोग्राफी salauksen kryptografia การเข้ารหัส kriptografija رمز نویسی kriptografiju 암호화

An efficient way to increase the key lifetime can be the usage of re-keying mechanisms (using block cipher $E = (E_K \in \text{Perm}(\{0, 1\}^n) \mid K \in \{0, 1\}^k)$ as a black-box primitive):

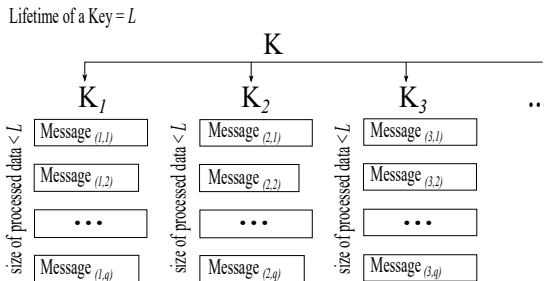
- on the block cipher mode of operation level (**internal re-keying**);
- on the message processing level (**external re-keying**) .

- criptografia dulmál cripteagrafaíochta 密码 kriptografi cifrado קריפטוגרפיה mã mã học криптография criptografia ծածկագիտություն kryptografia

mật mã học криптография cryptografia ծածկագրություն kryptografia კრიптоგრაფია криптография κρυπτογραφία cryptography 暗号化
kryptographie क्रिप्टोग्राफी salauksen kryptografia การเข้ารหัส kriptografija رمز نویسی 암호화 crittografia duma1 criptografia1chta 密碼

External re-keying

Approach to analysis: [AB2001] M. Bellare, M. Abdalla. «Increasing the Lifetime of a Key: A Comparative Analysis of the Security of Re-Keying Techniques».

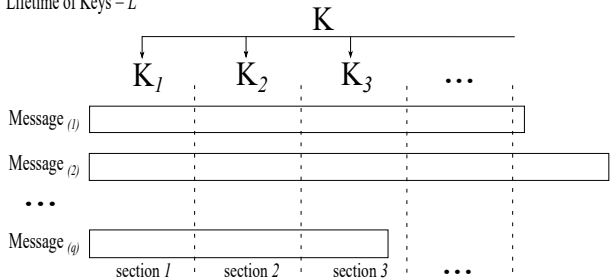


The main concept

A key, derived according to a certain key update technique, is intended to process **a fixed amount of separate messages** after which the key must be updated. Using external re-keying jointly with the block cipher mode of operation **does not change the internal structure of the mode**.

Internal re-keying

Lifetime of Keys = L



size of sections = $\text{const} = l, ql < L$

The main concept

The mechanism modifies the base mode of operation in such a way that each message is processed **starting from the same key**, which is changed using the certain key update technique during processing of the current message. It is integrated into the base mode of operation and **changes its internal structure**.

Internal Re-keying

Idea: RFC 4357 (2006), «CryptoPro Key Meshing» (CPKM). Widely spread in the Russian versions of TLS, IPsec and CMS protocols.

Unfortunately, the approach proposed in [AB2001] is not applicable to the internal re-keying mechanisms.

Related work

- Information Security Problems, analysis of probabilistic characteristics of CPKM (V. Mironkin).
- CTCrypt 2016, security analysis of CTR-CPKM; ACPKM mechanism (a slight modification of CPKM) is proposed.
- ePrint Archive 2017/697, security analysis of GCM-ACPKM.

Parameters of obtained bounds: number of queries q , maximal message length m .

Ideally: to have more accurate bounds with parameter σ — total message length.

Internal Re-keying

Idea: RFC 4357 (2006), «CryptoPro Key Meshing» (CPKM). Widely spread in the Russian versions of TLS, IPsec and CMS protocols.

Unfortunately, the approach proposed in [AB2001] is not applicable to the internal re-keying mechanisms.

Related work

- Information Security Problems, analysis of probabilistic characteristics of CPKM (V. Mironkin).
- CTCrypt 2016, security analysis of CTR-CPKM; ACPKM mechanism (a slight modification of CPKM) is proposed.
- ePrint Archive 2017/697, security analysis of GCM-ACPKM.

Parameters of obtained bounds: number of queries q , maximal message length m .

Ideally: to have more accurate bounds with parameter σ — total message length.

Internal Re-keying

Idea: RFC 4357 (2006), «CryptoPro Key Meshing» (CPKM). Widely spread in the Russian versions of TLS, IPsec and CMS protocols.

Unfortunately, the approach proposed in [AB2001] is not applicable to the internal re-keying mechanisms.

Related work

- Information Security Problems, analysis of probabilistic characteristics of CPKM (V. Mironkin).
- CTCrypt 2016, security analysis of CTR-CPKM; ACPKM mechanism (a slight modification of CPKM) is proposed.
- ePrint Archive 2017/697, security analysis of GCM-ACPKM.

Parameters of obtained bounds: number of queries q , maximal message length m .

Ideally: to have more accurate bounds with parameter σ — total message length.

Internal Re-keying

Idea: RFC 4357 (2006), «CryptoPro Key Meshing» (CPKM). Widely spread in the Russian versions of TLS, IPsec and CMS protocols.

Unfortunately, the approach proposed in [AB2001] is not applicable to the internal re-keying mechanisms.

Related work

- Information Security Problems, analysis of probabilistic characteristics of CPKM (V. Mironkin).
- CTCrypt 2016, security analysis of CTR-CPKM; ACPKM mechanism (a slight modification of CPKM) is proposed.
- ePrint Archive 2017/697, security analysis of GCM-ACPKM.

Parameters of obtained bounds: number of queries q , maximal message length m .

Ideally: to have more accurate bounds with parameter σ — total message length.

kriptografija 암호화 crittografia dumlál cripteagrafaiochta 密码 kriptografi cifrado פּרָגראַפֿיע מאַט מאַ הֶסע קריפטוגראַפֿיע criptografia
 ծածկագիտություն kryptografia շրժձժեղճընցոօս կրիպտոգրաֆիա κρυπτογράφηση cryptography 暗号化 kryptographie கிரப்டொகாஃி salauksen
 кримтаграфія การฉํานรหึส kriptografija رمز نویسی kriptografiju 암호화 crittografia dumlál cripteagrafaiochta 密码 kriptografi cifrado פּרָגראַפֿיע מאַט

Key Lifetime

ma 1 hoc kryptografija criptografia ծածկագիտություն kryptografia շրժձժեղճընցոօս կրիպտոգրաֆիա κρυπτογράφηση cryptography 暗号化 kryptographie கிரப்டொகாஃி salauksen
 кримтаграфія การฉํานรหึส kriptografija رمز نویسی kriptografiju 암호화 crittografia dumlál cripteagrafaiochta 密码 kriptografi cifrado פּרָגראַפֿיע מאַט
 kryptografia ծածկագիտություն kryptografia շրժձժեղճընցոօս կրիպտոգրաֆիա κρυπτογράφηση cryptography 暗号化 kryptographie கிரப்டொகாஃி salauksen
 кримтаграфія การฉํานรหึส kriptografija رمز نویسی kriptografiju 암호화 crittografia dumlál cripteagrafaiochta 密码 kriptografi cifrado

Re-keying Mechanisms

crittografia dumlál cripteagrafaiochta 密码 kriptografi cifrado פּרָגראַפֿיע מאַט ma hoc kryptografija criptografia ծածկագիտություն kryptografia շրժձժեղճընցոօս
 կրիպտոգրաֆիա κρυπτογράφηση cryptography 暗号化 kryptographie கிரப்டொகாஃி salauksen кримтаграфія การฉํานรหึส kriptografija
 ծածկագիտություն kryptografia շրժձժեղճընցոօս կրիպտոգրաֆիա κρυπτογράφηση cryptography 暗号化 kryptographie கிரப்டொகாஃி salauksen
 кримтаграфія การฉํานรหึส kriptografija رمز نویسی kriptografiju 암호화 crittografia dumlál cripteagrafaiochta 密码 kriptografi cifrado

Standardized Internally Re-keyed Modes

ma 4 hoc kryptografija criptografia ծածկագիտություն kryptografia շրժձժեղճընցոօս կրիպտոգրաֆիա κρυπτογράφηση cryptography 暗号化 kryptographie
 கிரப்டொகாஃி salauksen кримтаграфія การฉํานรหึส kriptografija رمز نویسی kriptografiju 암호화 crittografia dumlál cripteagrafaiochta 密码 kriptografi
 cifrado פּרָגראַפֿיע מאַט ma hoc kryptografija criptografia ծածկագիտություն kryptografia շրժձժեղճընցոօս կրիպտոգրաֆիա κρυπτογράφηση cryptography
 暗号化 kryptographie கிரப்டொகாஃி salauksen кримтаграфія การฉํานรหึส kriptografija رمز نویسی kriptografiju 암호화 crittografia dumlál cripteagrafaiochta 密码 kriptografi

Security Analysis

Security Analysis of CTR-ACPKM mode

Security Analysis of OMAC-ACPKM-Master mode

kryptografija criptografia ծածկագիտություն kryptografia շրժձժեղճընցոօս կրիպտոգրաֆիա κρυπτογράφηση cryptography 暗号化 kryptographie
 கிரப்டொகாஃி salauksen кримтаграфія การฉํานรหึส kriptografija رمز نویسی kriptografiju 암호화 crittografia dumlál cripteagrafaiochta 密码 kriptografi
 cifrado פּרָגראַפֿיע מאַט ma hoc kryptografija criptografia ծածկագիտություն kryptografia շրժձժեղճընցոօս կրիպտոգրաֆիա κρυπτογράφηση cryptography
 暗号化 kryptographie கிரப்டொகாஃி salauksen кримтаграфія การฉํานรหึส kriptografija رمز نویسی kriptografiju 암호화 crittografia dumlál cripteagrafaiochta 密码 kriptografi

Practical Meaning of Proofs

ma 5 hoc kryptografija criptografia ծածկագիտություն kryptografia շրժձժեղճընցոօս կրիպտոգրաֆիա κρυπτογράφηση cryptography 暗号化 kryptographie
 கிரப்டொகாஃி salauksen кримтаграфія การฉํานรหึส kriptografija رمز نویسی kriptografiju 암호화 crittografia dumlál cripteagrafaiochta 密码 kriptografi
 cifrado פּרָגראַפֿיע מאַט ma hoc kryptografija criptografia ծածկագիտություն kryptografia շրժձժեղճընցոօս կրիպտոգրաֆիա κρυπτογράφηση cryptography
 暗号化 kryptographie கிரப்டொகாஃி salauksen кримтаграфія การฉํานรหึส kriptografija رمز نویسی kriptografiju 암호화 crittografia dumlál cripteagrafaiochta 密码 kriptografi

Object of analysis

Internally re-keyed modes adopted in Russian Standardization System (TC 26):

- CTR-ACPKM internally re-keyed mode
- OMAC-ACPKM-Master internally re-keyed mode

The CTR-ACPKM mode is also used in the Russian ciphersuites of the TLS 1.2 protocol.



ТЕХНИЧЕСКИЙ КОМИТЕТ ПО СТАНДАРТИЗАЦИИ «КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ»

Новости Документы Проекты документов Активности О нас Форум

[Старая версия](#) [EN](#)

[Главная](#) / [Документы](#) / [Рекомендации по стандартизации](#)

Р 1323565.1.017-2018 «Информационная технология. Криптографическая защита информации. Криптографические алгоритмы, сопутствующие применению алгоритмов блочного шифрования»

Авторы: Е.К.Алексеев, Е.С.Смышляева

IETF

The proposed modes are currently being considered in IETF (passed CFRG Crypto Review and RG Last Call).

[[Docs](#)] [[txt](#)|[pdf](#)|[xml](#)|[html](#)] [[Tracker](#)] [[WG](#)] [[Email](#)] [[Diff1](#)] [[Diff2](#)] [[Nits](#)]

Versions: ([draft-cfrg-re-keying](#)) [00](#) [01](#) [02](#) [03](#)
[04](#) [05](#) [06](#) [07](#) [08](#) [09](#) [10](#) [12](#)

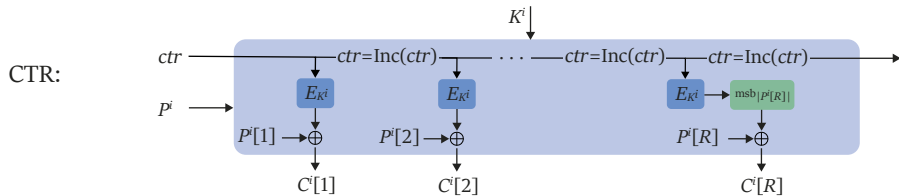
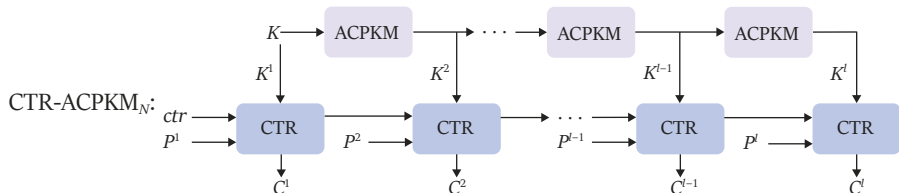
CFRG
 Internet-Draft
 Intended status: Informational
 Expires: September 1, 2018

S. Smyshlyaev, Ed.
 CryptoPro
 February 28, 2018

Re-keying Mechanisms for Symmetric Keys

draft-irtf-cfrg-re-keying-12

CTR-ACPKM



Input: a key $K \in \{0, 1\}^k$, a nonce $IV \in \{0, 1\}^{n/2}$, a plaintext $P \in \{0, 1\}^*$

Output: a ciphertext $C \in \{0, 1\}^{|P|}$

- ACPKM generates next section key using the previous section key.
- CTR processes sections of the plaintext under the corresponding section keys.

The ACPKM transformation

ACPKM:

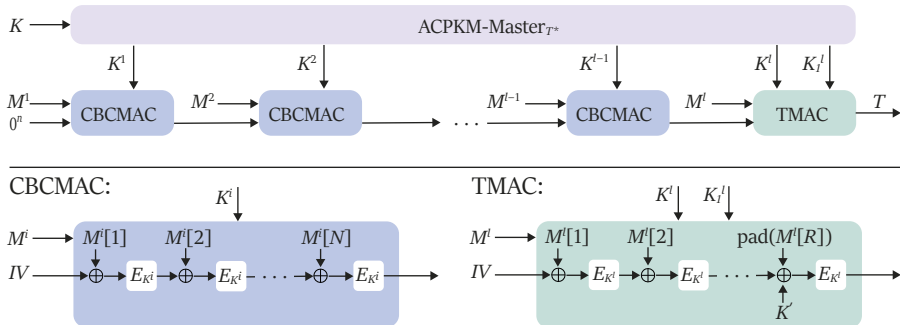
$$K^{i+1} = \text{ACPKM}(K^i) = \text{msb}_k(E_{K^i}(D_1) \parallel \dots \parallel E_{K^i}(D_s)),$$

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 for key transformation and for message processing.

OMAC-ACPKM-Master

OMAC-ACPKM-Master_{N,T*}:



Input: a key $K \in \{0, 1\}^k$, a message $M \in \{0, 1\}^*$

Output: a tag $T \in \{0, 1\}^n$

- $ACPKM-Master_{T^*}$ generates section key material using the master key K .
- $CBCMAC$ processes intermediate sections of size N blocks.
- $TMAC$ processes the final section of size of at most N blocks.

kriptografija 암호화 crittografia dumlál criptagrafaiochta 密码 kriptografi cifrado פּאַרשטײַק mât mã học крѣптoгραφiя criptografia
 ծածկագիտություն kryptografia շրժժեղացում kрѣптoгραφiя крѣптoгράφη cryptograph 暗号化 kryptographie கிப்தொகி salauksen
 крѣптaгραφiя การฉํานรหัส kriptografija رمز نویسی kriptografija 암호화 crittografia dumlál criptagrafaiochta 密码 kriptografi cifrado פּאַרשטײַק
 mât mã học крѣптoгραφiя criptografia ծածկագիտություն kryptografia շրժժեղացում kрѣптoгραφiя крѣптoгράφη cryptograph 暗号化
 kryptographie கிப்தொகி salauksen крѣптaгραφiя การฉํานรหัส kriptografija رمز نویسی kriptografija 암호화 crittografia dumlál criptagrafaiochta 密
 码 kriptografi cifrado פּאַרשטײַק mât mã học крѣптoгραφiя criptografia ծածկագիտություն kryptografia շրժժեղացում kрѣптoгραφiя

The ACPKM-Master transformation

ACPKM-Master_{T*}:

$$K^1 \| K_1^1 \| \dots \| K^l \| K_l^1 = \text{ACPKM-Master}_{T^*}(K, d, l) = \text{CTR-ACPKM}_{T^*}(K, 1^{n/2}, 0^{dln}),$$

where $d = \lceil k/n \rceil + 1$. Note that the parameters d and l must satisfy the inequality $d \cdot l \leq 2^{n/2-1}$.

kryptografija 암호화 crittografia dumlál criptagrafaiochta 密码 kriptografi cifrado פּאַרשטײַק mât mã học крѣптoгραφiя criptografia
 ծածկագիտություն kryptografia շրժժեղացում kрѣптoгραφiя крѣптoгράφη cryptograph 暗号化 kryptographie கிப்தொகி salauksen
 крѣптaгραφiя การฉํานรหัส kriptografija رمز نویسی kriptografija 암호화 crittografia dumlál criptagrafaiochta 密码 kriptografi cifrado
 פּאַרשטײַק mât mã học крѣптoгραφiя criptografia ծածկագիտություն kryptografia շրժժեղացում kрѣптoгραφiя крѣптoгράφη cryptograph 暗号化
 kryptographie கிப்தொகி salauksen крѣптaгραφiя การฉํานรหัส kriptografija رمز نویسی kriptografija 암호화 crittografia dumlál criptagrafaiochta 密
 码 kriptografi cifrado פּאַרשטײַק mât mã học крѣптoгραφiя criptografia ծածկագիտություն kryptografia շրժժեղացում kрѣптoгραφiя

Key Lifetime

Re-keying Mechanisms

Standardized Internal Re-keyed Modes

Security Analysis

- Security Analysis of CTR-ACPKM mode
- Security Analysis of OMAC-ACPKM-Master mode

Practical Meaning of Proofs

Approach to the analysis

Internal re-keying should be treated as a technique, which produces **a new set of the re-keyed modes of operation.**

Analysis of the re-keying impact on cryptographic properties of the used mode should be carried out in the **relevant security models** for encryption modes and authentication modes:

- IND-CPNA for CTR-ACPKM
- PRF for OMAC-ACPKM-Master

The analysis was carried out under PRP-CPA-security of the used block cipher assumption.

Practical significance: allows to **predict worst-case methods** and, basing on this prediction, to limit the data available to the adversary for **achieving necessary safety margin for real systems.**

Approach to the analysis

Internal re-keying should be treated as a technique, which produces **a new set of the re-keyed modes of operation.**

Analysis of the re-keying impact on cryptographic properties of the used mode should be carried out in the **relevant security models** for encryption modes and authentication modes:

- IND-CPNA for CTR-ACPKM
- PRF for OMAC-ACPKM-Master

The analysis was carried out under PRP-CPA-security of the used block cipher assumption.

Practical significance: allows to **predict worst-case methods** and, basing on this prediction, to limit the data available to the adversary for **achieving necessary safety margin for real systems.**

Approach to the analysis

Internal re-keying should be treated as a technique, which produces **a new set of the re-keyed modes of operation.**

Analysis of the re-keying impact on cryptographic properties of the used mode should be carried out in the **relevant security models** for encryption modes and authentication modes:

- IND-CPNA for CTR-ACPKM
- PRF for OMAC-ACPKM-Master

The analysis was carried out under PRP-CPA-security of the used block cipher assumption.

Practical significance: allows to **predict worst-case methods** and, basing on this prediction, to limit the data available to the adversary for **achieving necessary safety margin for real systems.**

Definition

Let $SE = \{SE.K, SE.E, SE.D\}$ 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

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

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

$\text{Exp}_{SE}^{\text{IND-CPNA}-b}(A)$

$K \xleftarrow{\$} SE.K()$

$b' \xleftarrow{\$} A^{\text{Encrypt}^b}$

return b'

Oracle $\text{Encrypt}^b(P, IV)$

$C \xleftarrow{\$} SE.E(K, P, IV)$

if $b = 0$ then

$R \xleftarrow{\mathcal{U}} \{0, 1\}^{|C|}$

return R

return C

Definition

Let $SE = \{SE.K, SE.E, SE.D\}$ 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

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

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

$\text{Exp}_{SE}^{\text{IND-CPNA}-b}(A)$

$K \xleftarrow{\$} SE.K()$

$b' \xleftarrow{\$} A^{\text{Encrypt}^b}$

return b'

Oracle $\text{Encrypt}^b(P, IV)$

$C \xleftarrow{\$} SE.E(K, P, IV)$

if $b = 0$ **then**

$R \xleftarrow{\mathcal{U}} \{0, 1\}^{|C|}$

return R

return C

Theorem

kriptogrāfija 암호화 crittografia dumlál cripteagrafalochta 密码 kriptografi cifrado תּיפוסת מֵאֵל mǎi hoc криптография criptografia
 ծածկագիտություն kryptografia ჯიბძტვჯრავთი криптография κρυπτογράφηση cryptography 暗号化 kryptographie किप्टोग्राफी salauksen

Encryption modes

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

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

mǎi mǎi hoc криптография criptografia ծածկագիտություն kryptografia ჯიბძტვჯრავთი криптография κρυπτογράφηση cryptography 暗号化 kryptographie किप्टोग्राफी salauksen криптография การเข้ารหัส kriptografija رمز نویسی kriptogrāfija 암호화 crittografia dumlál cripteagrafalochta 密码

kriptografija 암호화 crittografia dumlál criptagrafaiochta 密碼 kriptografi cifrado מְרִיטוּגְרַפְיָה mât mã học криптография criptografia
 ծածկագիտություն kryptografia շրժձժեղճաջօօժ կրիպտոգրաֆիա κρυπτογράφηση cryptography 暗号化 kryptographie किप्टोग्राफी salauksen
 крѣпѣтагрѣфія การฉำรห้ส kriptografija رمز نویسی kriptografija 암호화 crittografia dumlál criptagrafaiochta 密碼 kriptografi cifrado מְרִיטוּגְרַפְיָה

Example

Compare CTR-ACPKM and CTR.

Fix a safety margin δ of security and a key size $k = 256$ and a block size $n = 64$, which allows to process $q = 2^{10}$ messages with length $m = 2^{20}$ blocks = 8 MB in the base CTR mode. Thus, the total amount of data processed with an initial key is **2^{30} blocks = 8 GB**.

Set the optimal section size $N = 2^5$ blocks for internal re-keying. According to the security bounds presented in the Table above the message length can be securely almost quadratically increased. Thus the total amount of data processed with an initial key is **$\approx 2^{45}$ blocks = 256 TB** (due to the following relation):

$$\frac{c_2 m}{N} \cdot \frac{(qN + s)^2}{2^n} = \frac{(qm)^2}{2^n} = \delta \implies c_2 = \left(\frac{qm}{qN + s} \right)^2 \cdot \frac{N}{m};$$

кѣпѣтагрѣфія การฉำรห้ส kriptografija رمز نویسی kriptografija 암호화 crittografia dumlál criptagrafaiochta 密碼 kriptografi cifrado מְרִיטוּגְרַפְיָה
 mât mã học криптография criptografia ծածկագիտություն kryptografia շրժձժեղճաջօօժ կրիպտոգրաֆիա κρυπτογράφηση cryptography 暗号化
 kryptographie किप्टोग्राफी salauksen крѣпѣтагрѣфія การฉำรห้ส kriptografija رمز نویسی kriptografija 암호화 crittografia dumlál criptagrafaiochta 密碼

Example

Fix a safety margin δ of security and a key size $k = 256$ and a block size $n = 64$, which allows to process $q = 2^{10}$ messages with length $m = 2^{20}$ blocks = 8 MB in the base CTR mode. Thus, the total amount of data processed with an initial key is 2^{30} blocks = 8 GB.

Example

Compare CTR-ACPKM and CTR.

Fix a safety margin δ of security and a key size $k = 256$ and a block size $n = 64$, which allows to process $q = 2^{10}$ messages with length $m = 2^{20}$ blocks = 8 MB in the base CTR mode. Thus, the total amount of data processed with an initial key is **2^{30} blocks = 8 GB**.

Set the optimal section size $N = 2^5$ blocks for internal re-keying. According to the security bounds presented in the Table above the message length can be securely almost quadratically increased. Thus the total amount of data processed with an initial key is **$\approx 2^{45}$ blocks = 256 TB** (due to the following relation):

$$\frac{c_2 m}{N} \cdot \frac{(qN + s)^2}{2^n} = \frac{(qm)^2}{2^n} = \delta \implies c_2 = \left(\frac{qm}{qN + s} \right)^2 \cdot \frac{N}{m};$$

Definition

Let $MA = \{MA.K, MA.TAG\}$ be a message-authentication scheme and let A be an adversary. The advantage of A for the scheme MA in the PRF model (PRF-advantage) is defined as

$$\text{Adv}_{MA}^{\text{PRF}}(A) = \Pr \left[\text{Exp}_{MA}^{\text{PRF}-1}(A) \Rightarrow 1 \right] - \Pr \left[\text{Exp}_{MA}^{\text{PRF}-0}(A) \Rightarrow 1 \right],$$

where the experiment $\text{Exp}_{MA}^{\text{PRF}-b}(A)$, $b \in \{0, 1\}$ is defined as follows

$\text{Exp}_{MA}^{\text{PRF}-1}(A)$

$K \xleftarrow{\$} MA.K()$

$b' \xleftarrow{\$} A^{F^1}$

return b'

Oracle $F^1(M)$

return $MA.TAG(K, M)$

$\text{Exp}_{MA}^{\text{PRF}-0}(A)$

$Rnd \leftarrow \emptyset$

$b' \xleftarrow{\$} A^{F^0}$

return b'

Oracle $F^0(M)$

if $\nexists T' \in \mathcal{T} : (M, T') \in Rnd$

then

$T \xleftarrow{\mathcal{U}} \mathcal{T}$

$Rnd \leftarrow Rnd \cup \{(M, T)\}$

else

$T \leftarrow T'$

return T

Definition

Let $\text{MA} = \{\text{MA.K}, \text{MA.TAG}\}$ be a message-authentication scheme and let A be an adversary. The advantage of A for the scheme MA in the PRF model (PRF-advantage) is defined as

$$\text{Adv}_{\text{MA}}^{\text{PRF}}(A) = \Pr \left[\text{Exp}_{\text{MA}}^{\text{PRF}-1}(A) \Rightarrow 1 \right] - \Pr \left[\text{Exp}_{\text{MA}}^{\text{PRF}-0}(A) \Rightarrow 1 \right],$$

where the experiment $\text{Exp}_{\text{MA}}^{\text{PRF}-b}(A)$, $b \in \{0, 1\}$ is defined as follows

$\text{Exp}_{\text{MA}}^{\text{PRF}-1}(A)$

$K \xleftarrow{\$} \text{MA.K}()$

$b' \xleftarrow{\$} A^{F^1}$

return b'

Oracle $F^1(M)$

return $\text{MA.TAG}(K, M)$

$\text{Exp}_{\text{MA}}^{\text{PRF}-0}(A)$

$Rnd \leftarrow \emptyset$

$b' \xleftarrow{\$} A^{F^0}$

return b'

Oracle $F^0(M)$

if $\nexists T' \in \mathcal{T} : (M, T') \in Rnd$

then

$T \xleftarrow{\mathcal{U}} \mathcal{T}$

$Rnd \leftarrow Rnd \cup \{(M, T)\}$

else

$T \leftarrow T'$

return T

Theorem (special case $T^* = \infty$)

Let N be the parameter of OMAC-ACPKM-Master mode. Then for any adversary A with the time complexity of at most t that makes queries, where the maximal message length is at most m blocks and the total message length is at most σ blocks, there exists an adversary B such that

$$\text{Adv}_{\text{OMAC-ACPKM-Master}_{N,T^*}}^{\text{PRF}}(A) \leq (l+1) \cdot \text{Adv}_E^{\text{PRP-CPA}}(B) + \frac{(dl)^2}{2^n} + \frac{4(\sigma_1^2 + \dots + \sigma_l^2)}{2^n},$$

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

kriptogrāfiju 암호화 crittografia dumlál cripteagrafalochta 密碼 kriptografi cifrado תפודתהמאמץ māt mā hoc криптография criptografia
 ծածկագիտություն kryptografia շրժձժեղձձձոձոձ կրиптография крптограффет cryptograph 暗号化 kryptographie किप्टोग्राफी salauksen

kri Authentication modes

mā
 cry
 碼
 kri
 cri
 շր
 ى
 ծա
 cri
 mā
 kry
 碼
 kri
 cri
 շր
 ى
 ծա
 kri

Mode	$\text{Adv}_{\text{Mode}}^{\text{PRF}}(A)$
OMAC	$\approx \frac{4\sigma^2 + 1}{2^{n+1}}$
OMAC-ACPKM-Master $_{N,\infty}$	$\approx \frac{4(\sigma_1^2 + \dots + \sigma_l^2)}{2^{n+1}} + \frac{(dl)^2}{2^n}$

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

māt mā hoc криптография criptografia ծածկագիտություն kryptografia շրձժեղձձձոձոձ կրиптография крптограффет cryptograph 暗号化
 kryptographie किप्टोग्राफी salauksen криптография การเข้ารหัส kriptografija رمز نویسی kriptogrāfiju 암호화 crittografia dumlál cripteagrafalochta 密碼

kriptografija 암호화 crittografia dumlál cripteagrafaiochta 密码 kriptografi cifrado ԽճճԻՄԻՐՈՒՄ մât mã học крпптография criptografia
 ծածկագիտություն kryptografia շրժժժշտընցոօս կրпптография крпптографъղղ cryptographу 暗号化 kryptographie கி஑்டொகா஑ி salauksen
 крпптаграфия การฉานรหฬ kriptografija رمزنويسی kriptografija 암호화 crittografia dumlál cripteagrafaiochta 密码 kriptografi cifrado ԽճճԻՄԻՐՈՒՄ

1 Key Lifetime

mât mã học крпптография criptografia ծածկագիտություն kryptografia շրժժժշտընցոօս կրпптография крпптографъղղ cryptographу 暗号化 kryptographie கி஑்டொகா஑ி salauksen
 крпптаграфия การฉานรหฬ kriptografija رمزنويسی kriptografija 암호화 crittografia dumlál cripteagrafaiochta 密码 kriptografi cifrado ԽճճԻՄԻՐՈՒՄ

2 Re-keying Mechanisms

cryptographу 暗号化 kryptographie கி஑்டொகா஑ி salauksen крпптаграфия การฉานรหฬ kriptografija رمزنويسی kriptografija 암호화 crittografia dumlál cripteagrafaiochta 密码 kriptografi cifrado ԽճճԻՄԻՐՈՒՄ
 ծածկագիտություն kryptografia շրժժժշտընցոօս կրпптография крпптографъղղ cryptographу 暗号化 kryptographie கி஑்டொகா஑ி salauksen
 крпптаграфия การฉานรหฬ kriptografija رمزنويسی kriptografija 암호화 crittografia dumlál cripteagrafaiochta 密码 kriptografi cifrado ԽճճԻՄԻՐՈՒՄ

3 Standardized Internally Rekeyed Modes

cryptographу 暗号化 kryptographie கி஑்டொகா஑ி salauksen крпптаграфия การฉานรหฬ kriptografija رمزنويسی kriptografija 암호화 crittografia dumlál cripteagrafaiochta 密码 kriptografi cifrado ԽճճԻՄԻՐՈՒՄ
 ծածկագիտություն kryptografia շրժժժշտընցոօս կրпптография крпптографъղղ cryptographу 暗号化 kryptographie கி஑்டொகா஑ி salauksen
 крпптаграфия การฉานรหฬ kriptografija رمزنويسی kriptografija 암호화 crittografia dumlál cripteagrafaiochta 密码 kriptografi cifrado ԽճճԻՄԻՐՈՒՄ

4 Security Analysis

• Security Analysis of CTR-ACPKM mode

• Security Analysis of OMAC-ACPKM-Master mode

cryptographу 暗号化 kryptographie கி஑்டொகா஑ி salauksen крпптаграфия การฉานรหฬ kriptografija رمزنويسی kriptografija 암호화 crittografia dumlál cripteagrafaiochta 密码 kriptografi cifrado ԽճճԻՄԻՐՈՒՄ
 ծածկագիտություն kryptografia շրժժժշտընցոօս կրпптография крпптографъղղ cryptographу 暗号化 kryptographie கி஑்டொகா஑ி salauksen
 крпптаграфия การฉานรหฬ kriptografija رمزنويسی kriptografija 암호화 crittografia dumlál cripteagrafaiochta 密码 kriptografi cifrado ԽճճԻՄԻՐՈՒՄ

5 Practical Meaning of Proofs

cryptographу 暗号化 kryptographie கி஑்டொகா஑ி salauksen крпптаграфия การฉานรหฬ kriptografija رمزنويسی kriptografija 암호화 crittografia dumlál cripteagrafaiochta 密码 kriptografi cifrado ԽճճԻՄԻՐՈՒՄ
 ծածկագիտություն kryptografia շրժժժշտընցոօս կրпптография крпптографъղղ cryptographу 暗号化 kryptographie கி஑்டொகா஑ி salauksen
 крпптаграфия การฉานรหฬ kriptografija رمزنويسی kriptografija 암호화 crittografia dumlál cripteagrafaiochta 密码 kriptografi cifrado ԽճճԻՄԻՐՈՒՄ

Proof for OMAC-ACPKM-Master

The proof consists of three steps. On each step we idealize a certain component of a target mode in order to obtain a structure which is close to a truly random function at the end.

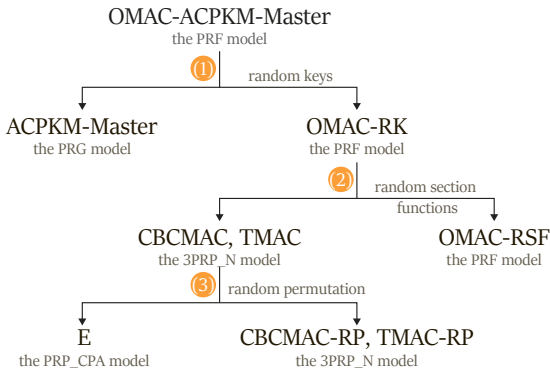


Figure: The idealization steps. The right arrows indicate the idealization results and the left arrows indicate the «costs» of the corresponding idealizations.

kriptografija 암호화 crittografia dumlál cripteagrafaiochta 密码 kriptografi cifrado תַּשְׁבָּעֵי מַתְּמָטִיקָה мәт ма һөс криптография cryptografia
 ծածկագիտություն kryptografia ვრცელვარდობის კრიპტოგრაფია κρυπτογράφηση cryptography 暗号化 kryptographie किप्टोग्राफी salauksen
 кримптография การเข้ารหัส kriptografija رمز نویسی kriptografiju 암호화 crittografia dumlál cripteagrafaiochta 密码 kriptografi cifrado תַּשְׁבָּעֵי מַתְּמָטִיקָה
 мәт ма һөс криптография cryptografia ծածկագիտություն kryptografia ვრცელვარდობის კრიპტოგრაფია κρυπτογράφηση cryptography 暗号化
 kryptographie किप्टोग्राफी salauksen кримптография การเข้ารหัส kriptografija رمز نویسی kriptografiju 암호화 crittografia dumlál cripteagrafaiochta 密

Relation with heuristic approach

The obtained reductions show that any method covered by the PRF model should be based on at least one of the following four mode properties:

- Non-Randomness of section keys (NR)
- Block Cipher design (BC)
- Mode design Combinatorics (MC)
- Correlation between Sections (CS)

crittografia dumlál cripteagrafaiochta 密码 kriptografi cifrado תַּשְׁבָּעֵי מַתְּמָטִיקָה мәт ма һөс криптография cryptografia ծածկագիտություն kryptografia
 ვრცელვარდობის კრიპტოგრაფია κρυπτογράφηση cryptography 暗号化 kryptographie किप्टोग्राफी salauksen кримптография การเข้ารหัส kriptografija
 رمز نویسی kriptografiju 암호화 crittografia dumlál cripteagrafaiochta 密码 kriptografi cifrado תַּשְׁבָּעֵי מַתְּמָטִיקָה мәт ма һөс криптография cryptografia
 ծածկագիտություն kryptografia ვრცელვარდობის კრიპტოგრაფია κρυπτογράφηση cryptography 暗号化 kryptographie किप्टोग्राफी salauksen
 кримптография การเข้ารหัส kriptografija رمز نویسی kriptografiju 암호화 crittografia dumlál cripteagrafaiochta 密码 kriptografi cifrado תַּשְׁבָּעֵי מַתְּמָטִיקָה
 мәт ма һөс криптография cryptografia ծածկագիտություն kryptografia ვრცელვარდობის კრიპტოგრაფია κρυπτογράφηση cryptography 暗号化
 kryptographie किप्टोग्राफी salauksen кримптография การเข้ารหัส kriptografija رمز نویسی kriptografiju 암호화 crittografia dumlál cripteagrafaiochta 密

kriptografija 암호화 crittografia dumlál cripteagrafaiochta 密码 kriptografi cifrado תַּשְׁבָּרְתִּי מַתְמָטִיקָה криптография criptografia
 ծածկագիտություն kryptografia շրժժեղացրացոօս криптография кρυπτογράφηση cryptography 暗号化 kryptographie किप्टोग्राफी salauksen
 крптарграфия การฉานรหึส kriptografija رمز نویسی kriptografiju 암호화 crittografia dumlál cripteagrafaiochta 密码 kriptografi cifrado תַּשְׁבָּרְתִּי מַתְמָטִיקָה
 mat mǎ hoc криптография criptografia ծածկագիտություն kryptografia շրժժեղացրացոօս криптография кρυπτογράφηση cryptography 暗号化
 kryptographie किप्टोग्राफी salauksen крптарграфия การฉานรหึส kriptografija رمز نویسی kriptografiju 암호화 crittografia dumlál cripteagrafaiochta 密

Relation with heuristic approach

The obtained reductions show that any method covered by the PRF model should be based on at least one of the following four mode properties:

- Non-Randomness of section keys (NR)
- Block Cipher design (BC)
- Mode design Combinatorics (MC)
- Correlation between Sections (CS)

crittografia dumlál cripteagrafaiochta 密码 kriptografi cifrado תַּשְׁבָּרְתִּי מַתְמָטִיקָה криптография criptografia ծածկագիտություն kryptografia
 շրժժեղացրացոօս криптография кρυπτογράφηση cryptography 暗号化 kryptographie किप्टोग्राफी salauksen крптарграфия การฉานรหึส kriptografija
 رمز نویسی kriptografiju 암호화 crittografia dumlál cripteagrafaiochta 密码 kriptografi cifrado תַּשְׁבָּרְתִּי מַתְמָטִיקָה криптография criptografia
 ծածկագիտություն kryptografia շրժժեղացրացոօս криптография кρυπτογράφηση cryptography 暗号化 kryptographie किप्टोग्राफी salauksen
 крптарграфия การฉานรหึส kriptografija رمز نویسی kriptografiju 암호화 crittografia dumlál cripteagrafaiochta 密码 kriptografi cifrado תַּשְׁבָּרְתִּי מַתְמָטִיקָה
 mat mǎ hoc криптография criptografia ծածկագիտություն kryptografia շրժժեղացրացոօս криптография кρυπτογράφηση cryptography 暗号化
 kryptographie किप्टोग्राफी salauksen крптарграфия การฉานรหึส kriptografija رمز نویسی kriptografiju 암호화 crittografia dumlál cripteagrafaiochta 密

kriptografiju 암호화 crittografia dumlál cripteagrafaiochta 密码 kriptografi cifrado תפריט מפת מאה קריפטוגרפיה criptografia
 ծածկագիտություն kryptografia շրժժեղացում kriptografia кρυπτογράφηση cryptography 暗号化 kryptographie किप्टोग्राफी salauksen
 кримптография การเข้ารหัส kriptografija رمز نویسی kriptografiju 암호화 crittografia dumlál cripteagrafaiochta 密码 kriptografi cifrado תפריט מפת מאה קריפטוגרפיה
 criptografia ծածկագիտություն kryptografia շրժժեղացում kriptografia кρυπτογράφηση cryptography 暗号化 kryptographie किप्टोग्राफी salauksen
 кримптография การเข้ารหัส kriptografija رمز نویسی kriptografiju 암호화 crittografia dumlál cripteagrafaiochta 密码

Relation with heuristic approach

The obtained reductions show that any method covered by the PRF model should be based on at least one of the following four mode properties:

- Non-Randomness of section keys (NR)
- Block Cipher design (BC)
- Mode design Combinatorics (MC)
- Correlation between Sections (CS)

crittografia dumlál cripteagrafaiochta 密码 kriptografi cifrado תפריט מפת מאה קריפטוגרפיה criptografia ծածկագիտություն kryptografia շրժժեղացում kriptografia кρυπτογράφηση cryptography 暗号化 kryptographie किप्टोग्राफी salauksen
 кримптография การเข้ารหัส kriptografija رمز نویسی kriptografiju 암호화 crittografia dumlál cripteagrafaiochta 密码 kriptografi cifrado תפריט מפת מאה קריפטוגרפיה
 criptografia ծածկագիտություն kryptografia շրժժեղացում kriptografia кρυπτογράφηση cryptography 暗号化 kryptographie किप्टोग्राफी salauksen
 кримптография การเข้ารหัส kriptografija رمز نویسی kriptografiju 암호화 crittografia dumlál cripteagrafaiochta 密码 kriptografi cifrado תפריט מפת מאה קריפטוגרפיה
 criptografia ծածկագիտություն kryptografia շրժժեղացում kriptografia кρυπτογράφηση cryptography 暗号化 kryptographie किप्टोग्राफी salauksen
 кримптография การเข้ารหัส kriptografija رمز نویسی kriptografiju 암호화 crittografia dumlál cripteagrafaiochta 密码

kriptografiju 암호화 crittografia dumlál cripteagrafaiochta 密码 kriptografi cifrado תפריט מפת מאה קריפטוגרפיה criptografia
 ծածկագիտություն kryptografia շրժժեղացրացոօս криптография кρυπτογράφηση cryptography 暗号化 kryptographie किप्टोग्राफी salauksen
 кримптография การฉานรหัส kriptografija رمز نویسی kriptografiju 암호화 crittografia dumlál cripteagrafaiochta 密码 kriptografi cifrado תפריט מפת מאה קריפטוגרפיה
 criptografia ծածկագիտություն kryptografia շրժժեղացրացոօս криптография кρυπτογράφηση cryptography 暗号化 kryptographie किप्टोग्राफी salauksen
 кримптография การฉานรหัส kriptografija رمز نویسی kriptografiju 암호화 crittografia dumlál cripteagrafaiochta 密码

Relation with heuristic approach

The obtained reductions show that any method covered by the PRF model should be based on at least one of the following four mode properties:

- Non-Randomness of section keys (NR)
- Block Cipher design (BC)
- Mode design Combinatorics (MC)
- Correlation between Sections (CS)

crittografia dumlál cripteagrafaiochta 密码 kriptografi cifrado תפריט מפת מאה קריפטוגרפיה criptografia ծածկագիտություն kryptografia շրժժեղացրացոօս
 криптография кρυπτογράφηση cryptography 暗号化 kryptographie किप्टोग्राफी salauksen кримптография การฉานรหัส kriptografija رمز نویسی
 kriptografiju 암호화 crittografia dumlál cripteagrafaiochta 密码 kriptografi cifrado תפריט מפת מאה קריפטוגרפיה criptografia ծածկագիտություն
 kryptografia շրժժեղացրացոօս криптография кρυπτογράφηση cryptography 暗号化 kryptographie किप्टोग्राफी salauksen кримптография
 การฉานรหัส kriptografija رمز نویسی kriptografiju 암호화 crittografia dumlál cripteagrafaiochta 密码 kriptografi cifrado תפריט מפת מאה קריפטוגרפיה
 criptografia ծածկագիտություն kryptografia շրժժեղացրացոօս криптография кρυπτογράφηση cryptography 暗号化 kryptographie किप्टोग्राफी salauksen
 кримптография การฉานรหัส kriptografija رمز نویسی kriptografiju 암호화 crittografia dumlál cripteagrafaiochta 密码

mật mã học криптография cryptografia daidlyuqhuunipjynin kryptografia კრიპტოგრაფიის криптография криптография cryptography 暗号化
kryptographie क्रिप्टोग्राफी salauksen kryptografia การเข้ารหัส kriptografija رمز نویسی kriptografija dulmál criptografaiochta 密



kriptografija 암호화 crittografia dumlál cripteagrafalochta 密码 kriptografi cifrado מפתח מלך māt mā hōc крпптографія criptografia
 ծածկագիտություն kryptografia շրժձՅՈՒՆՅՈՒՆ крпптография крпптографηη cryptography 暗号化 kryptographie किप्टोबाफी salauksen

Relation with heuristic approach

In order to obtain the total bound for advantage of the worst-case methods, «PRF-breaking» the target mode, we sum up (following the reduction) the success probabilities of the **worst-case methods**, which exploit only one of the properties mentioned above.

$$\begin{aligned} \text{Adv}_{\text{OMAC-ACPKM-Master}_{N,\infty}}^{\text{PRF}}(A) \leq & \underbrace{\frac{(dl)^2}{2^n} + \text{Adv}_E^{\text{PRP-CPA}}(B)}_{\text{NR property}} + \\ & \underbrace{l \cdot \text{Adv}_E^{\text{PRP-CPA}}(B)}_{\text{BC property}} + \underbrace{\frac{4(\sigma_1^2 + \dots + \sigma_l^2)}{2^n}}_{\text{MC and CS properties}}. \end{aligned}$$

māt mā hōc крпптографія criptografia ծածկագիտություն kryptografia շրժձՅՈՒՆՅՈՒՆ крпптография крпптографηη cryptography 暗号化
 kryptographie किप्टोबाफी salauksen крпптаграфия การฉานรหัส kriptografija رمز نویسی kriptografija 암호화 crittografia dumlál cripteagrafalochta 密码

kriptografiju 암호화 crittografia dumlál criptagrafaiochta 密码 kriptografi cifrado תפראגפיה מאת מא הוד криптография криптография
 ծածկագիտություն kryptografia շրժժեղանգոօս криптография кρυπτογράφηση cryptography 暗号化 kryptographie किप्टोगाफी salauksen
 крпптаграфия การฉานรหัส kriptografija رمز نویسی kriptografiju 암호화 crittografia dumlál criptagrafaiochta 密码 kriptografi cifrado תפראגפיה
 מאת מא הוד криптография криптография ծածկագիտություն kryptografia շրժժեղանգոօս криптография кρυπτογράφηση cryptography 暗号化
 kryptographie किप्टोगाफी salauksen крпптаграфия การฉานรหัส kriptografija رمز نویسی kriptografiju 암호화 crittografia dumlál criptagrafaiochta 密
 码

Thank you for your attention!

კრუ...
 crittografia dumlál criptagrafaiochta 密码 kriptografi cifrado תפראגפיה מאת מא הוד криптография криптография ծածկագիտություն kryptografia
 շր

Questions?

روئسی
 ծածկագիտություն kryptografia շրժժեղանգոօս криптография кρυπτογράφηση cryptography 暗号化 kryptographie किप्टोगाफी salauksen
 Questions, comments:

❶ alekseev@cryptopro.ru,
 ❷ lah@cryptopro.ru
 ❸ svb@cryptopro.ru

շրժժեղանգոօս криптография кρυπτογράφηση cryptography 暗号化 kryptographie किप्टोगाफी salauksen крпптаграфия การฉานรหัส kriptografija
 رمز نویسی kriptografiju 암호화 crittografia dumlál criptagrafaiochta 密码 kriptografi cifrado תפראגפיה מאת מא הוד криптография криптография
 ծածկագիտություն kryptografia շրժժեղանգոօս криптография кρυπτογράφηση cryptography 暗号化 kryptographie किप्टोगाफी salauksen
 крпптаграфия การฉานรหัส kriptografija رمز نویسی kriptografiju 암호화 crittografia dumlál criptagrafaiochta 密码 kriptografi cifrado תפראגפיה
 מאת מא הוד криптография криптография ծածկագիտություն kryptografia շրժժեղանգոօս криптография кρυπτογράφηση cryptography 暗号化
 kryptographie किप्टोगाफी salauksen крпптаграфия การฉานรหัส kriptografija رمز نویسی kriptografiju 암호화 crittografia dumlál criptagrafaiochta 密

In contrast to the heuristic approach the provable security approach considers the resistance of cryptographic scheme not to certain cryptanalytic methods, but to *all* methods covered by the used security model.

Discuss arguments about meaning of the proofs stages for OMAC-ACPKM-Master from the viewpoint of resistance to possible methods. The interpretation given below is intended to deepen understanding of the so called «provable security» concept.

Let $\text{MA} = \{\text{MA.K}, \text{MA.TAG}\}$ be a message-authentication scheme. Then for any adversary A there exists an adversary B such that

$$\text{Adv}_{\text{MA}}^{\text{EU-CMA}}(A) \leq \text{Adv}_{\text{MA}}^{\text{PRF}}(B) + \frac{1}{2^\tau},$$

where τ is a tag size. The total message length σ is the same for the adversaries A and B and the time complexity t is «almost» the same.

$$\text{Adv}_{\text{MA}}^{\text{EU-CMA}}(A) \leq \text{Adv}_{\text{MA}}^{\text{PRF}}(B) + \frac{1}{2^\tau},$$

where τ is a tag size. The total message length σ is the same for the adversaries A and B and the time complexity t is «almost» the same.

crittografia dumlál criptagrafaiochta 密码 kriptografi cifrado מאבןמאבן mat mã học криптография criptografia ծածկագիտություն kryptografia
კრიპტოგრაფია крѳтoгpaфия cryptography 暗号化 kryptographie क्रिप्टोग्राफी salauksen крѳтаграфія การเข้ารหัส kriptografija
رمز نویسی kriptogrāfiju 암호화 crittografia dumlál criptagrafaiochta 密码 kriptografi cifrado מאבןמאבן mat mã học криптография criptografia
ծածկագիտություն kryptografia კრიптоგრაფია крѳтoгpaфия cryptography 暗号化 kryptographie क्रिप्टोग्राफी salauksen
кρѳтаграфія การเข้ารหัส kriptografija رمز نویسی kriptogrāfiju 암호화 crittografia dumlál criptagrafaiochta 密码 kriptografi cifrado
מאבןמאבן mat mã học криптография criptografia ծածկագիտություն kryptografia კრიპტოგრაფია крѳтoгpaфия cryptography 暗号化
kryptographie क्रिप्टोग्राफी salauksen крѳтаграфія การเข้ารหัส kriptografija رمز نویسی kriptogrāfiju 암호화 crittografia dumlál criptagrafaiochta

Example

Suppose the block cipher with $k = 256$ and $n = 128$ be secure: for any B with time complexity at most t making at least $q = k/n$ queries (for achieving unicity distance) the inequality $\text{Adv}_E^{\text{PRP-CPA}}(B) \leq \frac{t}{2^{256}}$ holds.

Consider the OMAC-ACPKM-Master $_{N,T^*}$ mode with $N = 2^5$ and $T^* = \infty$. We process $q = 2^{20}$ messages of length $m = 2^{10}$ blocks = 16 KB (the total message length is $\sigma = m \cdot q = 2^{30}$ blocks = 16 GB).

If we consider the adversaries (in the EU-CMA model) with time complexity at most 2^{100} , then the forgery probability can be upper estimated as follows:

$$\begin{aligned} \Pr [A \text{ forges}] = \text{Adv}_{\text{OMAC-ACPKM-Master}_{N,T^*}}^{\text{EU-CMA}}(A) &\leq \frac{(2^5 + 1) \cdot 2^{130}}{2^{256}} + \frac{(3 \cdot 2^5)^2}{2^{128}} + \\ &+ \frac{4 \cdot 2^5 \cdot (2^{20} \cdot 2^5)^2}{2^{128}} + \frac{1}{2^{128}} \leq \frac{1}{2^{70}}. \end{aligned}$$

Comparison

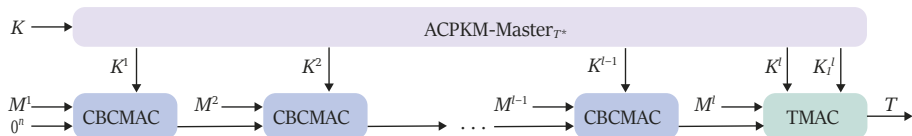
Number of sections	$\text{CTR-ACPKM}_N \succeq \text{CTR}$	$\text{OMAC-ACPKM-Master}_{N,\infty} \succeq \text{OMAC}$
$l = 2$	$s \leq \min(\sqrt{2N}, \sigma_2)$	$d \leq \min(N, 2\sigma_2)$
$l = 3$	$s \leq \min(\sqrt{2N}, N/2)$	$d \leq \min(N, 16)$
$l \geq 4$	$s \leq \min(\sqrt{2N})$	$d \leq N$

Table: Restrictions on the parameters of the internally re-keyed modes. Here N is the section size, $s = \lceil k/n \rceil$, $d = \lceil k/n \rceil + 1$. $A \succeq B$ denotes that the bound for mode A is better than the bound for mode B .

The first step

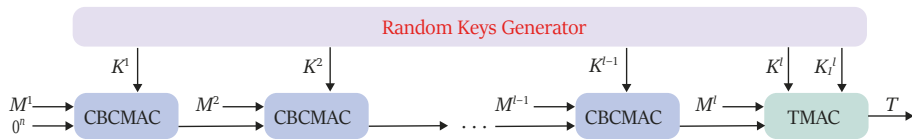
OMAC-ACPKM-Master \Rightarrow OMAC-RK (with Random Section Keys)

OMAC-ACPKM-Master $_{N,T^*}$:



Idealization

OMAC-RK $_N$:

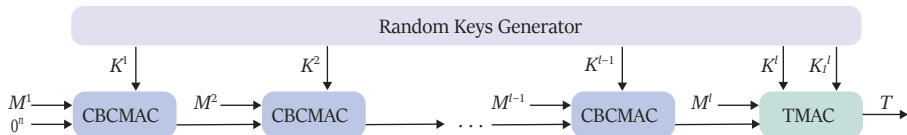


The «Cost» of the idealization depends on Non-Randomness of section keys (**NR**) which is defined by properties of ACPKM-Master (PRG model).

The second step

OMAC-RK \Rightarrow OMAC-RSF (with Random Section Functions)

OMAC-RK_N:



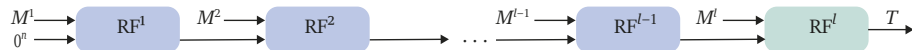
Idealization

OMAC-RSF_N:



RF = Random Function

The «Cost» of the idealization depends on Block Cipher design (**BC**) and Mode design Combinatorics (**MC**) which are defined by properties of CBCMAC and TMAC under the same key (3PRF model).

OMAC-RSF_N:

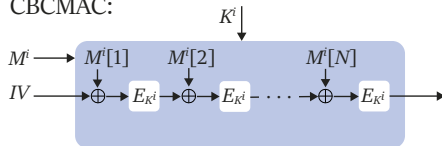
RF:



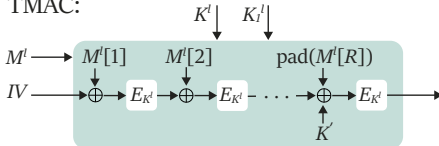
The third step

$\text{CBCMAC}_K, \text{TMAC}_K \Rightarrow \text{CBCMAC-RP}, \text{TMAC-RP}$ (with Random Permutation)

CBCMAC:

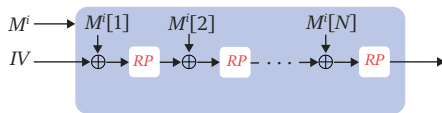


TMAC:

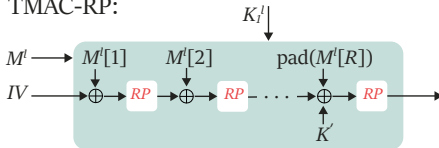


Idealization

CBCMAC-RP:



TMAC-RP:

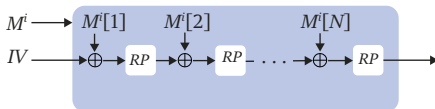


The «Cost» of the idealization depends on Block Cipher design (BC) which is defined by the used block cipher properties (PRP-CPA model);

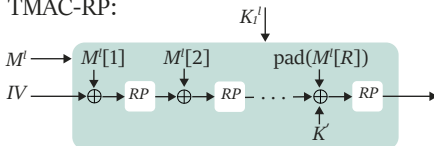
The third step

CBCMAC-RP, TMAC-RP \Rightarrow Independent Random Functions

CBCMAC-RP:



TMAC-RP:



Idealization

RF^i :



RF^l :



The «Cost» of the idealization depends on Mode design Combinatorics (MC) which is defined by the CBCMAC and TMAC structure (3PRF model);