# 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

## 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`.

## 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`.

# 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*).

1. Key Lifetime
2. **Re-keying Mechanisms**
3. Standardized Internally Re-keyed Modes
4. Security Analysis
   - Security Analysis of CTR-ACPKM mode
   - Security Analysis of OMAC-ACPKM-Master mode
5. Practical Meaning of Proofs

## 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.

## Re-keying

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

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

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`

## 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.

## Re-keying

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

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

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`

## 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.



## Re-keying

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

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



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`

## 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.

## Re-keying

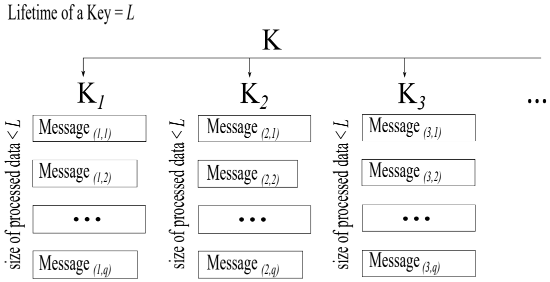
An efficient way to increase the key lifetime can be the usage of re-keying mechanisms (using block cipher $E = \left(E_K \in Perm(\{0,1\}^n) \mid K \in \{0,1\}^k\right)$ as a black-box primitive):

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

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`

## External re-keying

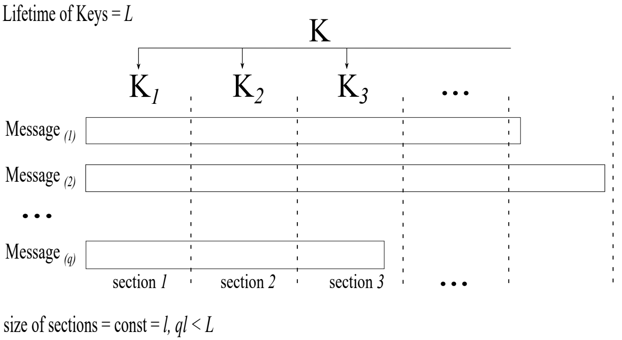
Approach to analysis: [AB2001] M. Bellare, M. Abdalla. «Increasing the Lifetime of a Key: A Comparative Analysis of the Security of Re-Keying Techniques».




## 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




## 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 $\sigma$ — 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 $\sigma$ — 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 $\sigma$ — 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.

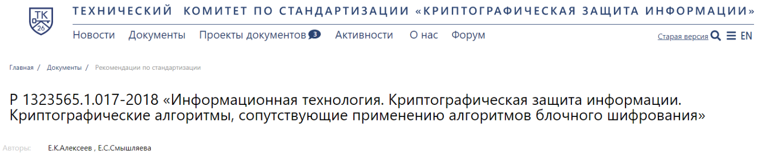
Parameters of obtained bounds: number of queries $q$, maximal message length $m$.
**Ideally:** to have more accurate bounds with parameter $\sigma$ — total message length.

# 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.



# IETF

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

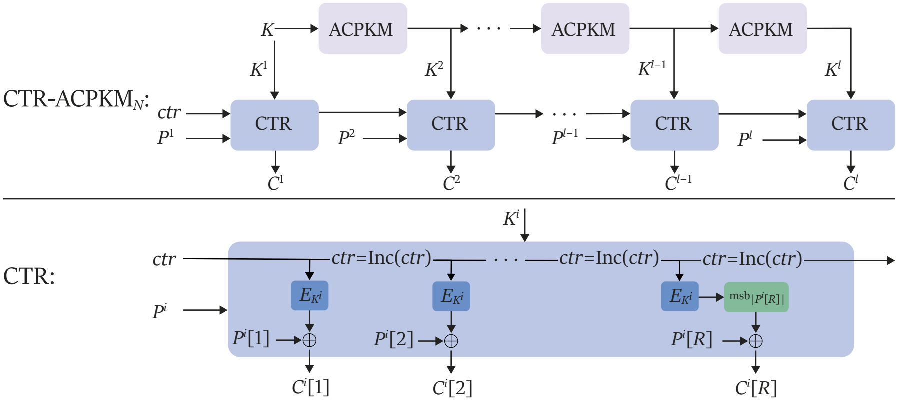
[Docs] [txt|pdf|xml|html] [Tracker] [WG] [Email] [Diff1] [Diff2] [Nits]

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

| | |
|---|---|
| CFRG | S. Smyshlyaev, Ed. |
| Internet-Draft | CryptoPro |
| Intended status: Informational | February 28, 2018 |
| Expires: September 1, 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:

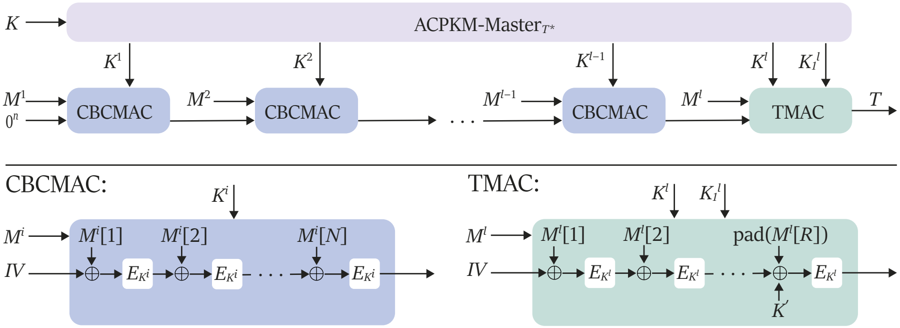
$$K^{i+1} = \mathrm{ACPKM}(K^i) = \mathrm{msb}_k(E_{K^i}(D_1)\| \ldots \|E_{K^i}(D_s)),$$

where $s = \lceil k/n \rceil$ and $D_1, D_2, \ldots, D_s \in \{0,1\}^n$ 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 $D_1, D_2, \ldots, D_s$ 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.

## The ACPKM-Master transformation

ACPKM-Master$_{T^*}$:

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

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

1 Key Lifetime

2 Re-keying Mechanisms

3 Standardized Internally Re-keyed Modes

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

5 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 $= \{\mathsf{SE.K},\ \mathsf{SE.E},\ \mathsf{SE.D}\}$ 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

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

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

| $\mathbf{Exp}_{\mathsf{SE}}^{\text{IND-CPNA}-b}(A)$ | Oracle $\mathsf{Encrypt}^b(P, IV)$ |
|---|---|
| $K \xleftarrow{\$} \mathsf{SE.K}()$ | $C \xleftarrow{\$} \mathsf{SE.E}(K, P, IV)$ |
| $b' \xleftarrow{\$} A^{\mathsf{Encrypt}^b}$ | **if** $b = 0$ **then** |
| **return** $b'$ | $\quad R \xleftarrow{\mathcal{U}} \{0,1\}^{\lvert C\rvert}$ |
| | $\quad$ **return** $R$ |
| | **return** $C$ |

## Definition

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 $\mathsf{SE}$ in the IND-CPNA model (IND-CPNA-*advantage*) is defined as

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

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

| $\mathbf{Exp}^{\text{IND-CPNA}-b}_{\mathsf{SE}}(A)$ | $\mathsf{Oracle\ \ Encrypt}^{b}(P, IV)$ |
|---|---|
| $K \xleftarrow{\$} \mathsf{SE.K}()$<br>$b' \xleftarrow{\$} A^{\mathsf{Encrypt}^b}$<br>**return** $b'$ | $C \xleftarrow{\$} \mathsf{SE.E}(K, P, IV)$<br>**if** $b = 0$ **then**<br>    $R \xleftarrow{\mathcal{U}} \{0,1\}^{\lvert C\rvert}$<br>    **return** $R$<br>**return** $C$ |

## Theorem

*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 maximal message length is at most m ($m \leqslant 2^{n/2-1}$) blocks and the total message length is at most $\sigma$ blocks, there exists an adversary B such that*

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

*where $s = \lceil k/n \rceil$, $l = \lceil m/N \rceil$, $\sigma_j$ 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.*

# Encryption modes

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

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 $s = \lceil k/n \rceil$, $\sigma$ is the total plaintexts block length, $m$ is the maximal plaintext block length and $\sigma_j$ is the total block length of data, processed under the section key $K^j$ $(\sigma_1 + \ldots + \sigma_l = \sigma$, where $l = \lceil m/N \rceil)$.

# Example

Compare CTR-ACPKM and CTR.

Fix a safety margin $\delta$ 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):

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

# Example

Compare CTR-ACPKM and CTR.

Fix a safety margin $\delta$ 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):

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

# Example

Compare CTR-ACPKM and CTR.

Fix a safety margin $\delta$ 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):

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

## Definition

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

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

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

$\mathbf{Exp}^{\mathrm{PRF}-1}_{\mathsf{MA}}(A)$

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

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

**return** $b'$

Oracle $\mathsf{F}^1(M)$

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

$\mathbf{Exp}^{\mathrm{PRF}-0}_{\mathsf{MA}}(A)$

$Rnd \leftarrow \emptyset$

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

**return** $b'$

Oracle $\mathsf{F}^0(M)$

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

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

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

$\mathbf{Exp}^{\mathrm{PRF}-1}_{\mathsf{MA}}(A)$

- $K \xleftarrow{\$} \mathsf{MA.K}()$
- $b' \xleftarrow{\$} A^{\mathsf{F}^1}$
- **return** $b'$

Oracle $\mathsf{F}^1(M)$

- **return** $\mathsf{MA.TAG}(K, M)$

$\mathbf{Exp}^{\mathrm{PRF}-0}_{\mathsf{MA}}(A)$

- $Rnd \leftarrow \emptyset$
- $b' \xleftarrow{\$} A^{\mathsf{F}^0}$
- **return** $b'$

Oracle $\mathsf{F}^0(M)$

- **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 $\sigma$ blocks, there exists an adversary $B$ such that*

$$\mathsf{Adv}^{PRF}_{OMAC\text{-}ACPKM\text{-}Master_{N,T^*}}(A) \leqslant (l+1)\cdot \mathsf{Adv}^{PRP\text{-}CPA}_{E}(B) + \frac{(dl)^2}{2^n} + \\ + \frac{4\left(\sigma_1^2 + \ldots + \sigma_l^2\right)}{2^n},$$

*$d = \lceil k/n \rceil + 1$, $l = \lceil m/N \rceil$, $dl \leqslant 2^{n/2-1}$, $\sigma_j$ is the total block length of data 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 $\max(\sigma_1, dl)$ 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.*

# Authentication modes

| Mode | $\mathsf{Adv}^{\mathrm{PRF}}_{\mathrm{Mode}}(A)$ |
|---|---|
| OMAC | $\approx \dfrac{4\sigma^2+1}{2^{n+1}}$ |
| OMAC-ACPKM-Master$_{N,\infty}$ | $\approx \dfrac{4\left(\sigma_1^2+\ldots+\sigma_l^2\right)}{2^{n+1}} + \dfrac{(dl)^2}{2^n}$ |

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 $d = \lceil k/n \rceil + 1$, $\sigma$ is the total plaintexts block length, $m$ is the maximal plaintext block length and $\sigma_j$ is the total block length of data, processed under the section key $K^j$ ($\sigma_1 + \ldots + \sigma_l = \sigma$, where $l = \lceil m/N \rceil$).

# 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.

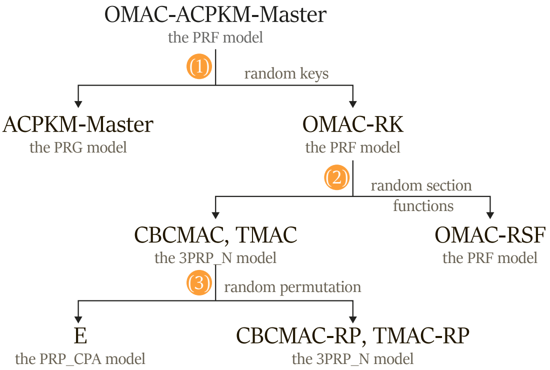



Figure: The idealization steps. The right arrows indicate the idealization results and the left arrows indicate the «costs» of the corresponding idealizations.

## 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**)

## 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**)

## 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**)

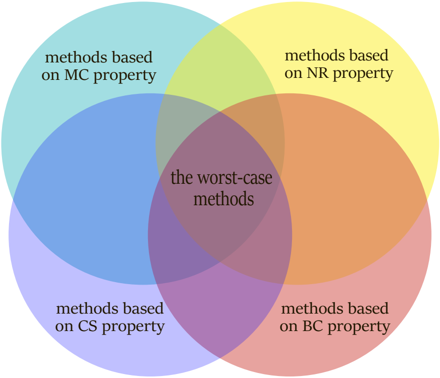
## Relation with heuristic approach

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**)

# Relation with heuristic approach

Any method covered by the PRF model should be based on at least one of the following four mode properties:



## 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.

$$\mathsf{Adv}^{\text{PRF}}_{\text{OMAC-ACPKM-Master}_{N,\infty}}(A) \leqslant \underbrace{\frac{(dl)^2}{2^n} + \mathsf{Adv}^{\text{PRP-CPA}}_{E}(B)}_{\textbf{NR}\text{ property}} + {} + \underbrace{l \cdot \mathsf{Adv}^{\text{PRP-CPA}}_{E}(B)}_{\textbf{BC}\text{ property}} + \underbrace{\frac{4\left(\sigma_1^2 + \ldots + \sigma_l^2\right)}{2^n}}_{\textbf{MC}\text{ and }\textbf{CS}\text{ properties}}.$$

## Thank you for your attention!

## Questions?

## Questions, comments:

- alekseev@cryptopro.ru,
- lah@cryptopro.ru
- svs@cryptopro.ru

## «Provable security»

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.

## Meaning of the proofs

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.

## Forgery threat: known relation

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

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

where $\tau$ is a tag size. The total message length $\sigma$ is the same for the adversaries $A$ and $B$ and the time complexity $t$ is «almost» the same.

## 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 $\mathsf{Adv}_E^{\text{PRP-CPA}}(B) \leqslant \frac{t}{2^{256}}$ 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:

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

# Comparison

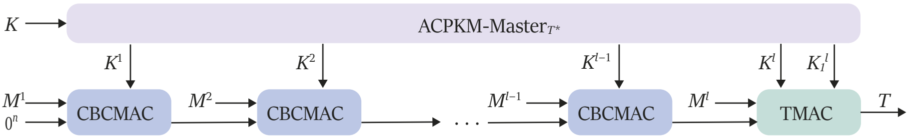
| Number of sections | CTR-ACPKM$_N \succeq$ CTR | OMAC-ACPKM-Master$_{N,\infty} \succeq$ OMAC |
|---|---|---|
| $l = 2$ | $s \leqslant \min(\sqrt{2N}, \sigma_2)$ | $d \leqslant \min(N, 2\sigma_2)$ |
| $l = 3$ | $s \leqslant \min(\sqrt{2N}, N/2)$ | $d \leqslant \min(N, 16)$ |
| $l \geqslant 4$ | $s \leqslant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

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

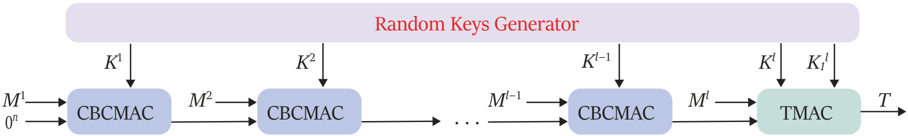
OMAC-ACPKM-Master ⇒ OMAC-RK (with Random Section Keys)

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




## Idealization

OMAC-RK$_N$:

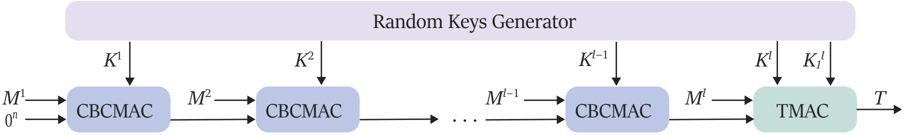



The «Cost» of the idealization depends on Non-Randomness of section keys (**NR**) which is defined by properties of ACPKM-Master (PRG model).

## The second step

OMAC-RK ⇒ 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).

## The second step

OMAC-RSF $\Rightarrow$ Random Function

OMAC-RSF$_N$:


Idealization

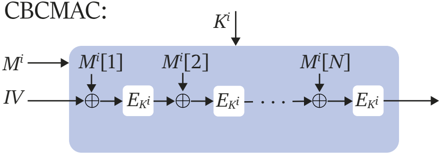
RF:


The «Cost» of the idealization depends on Correlation between Sections (**CS**) which is defined by properties of the proposed re-keying construction (PRF model);

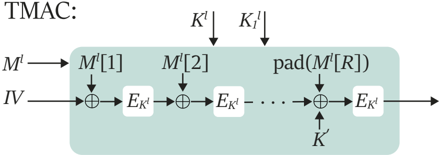
## The third step

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

CBCMAC:

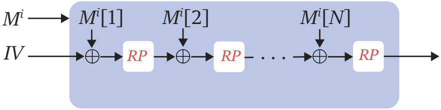



TMAC:

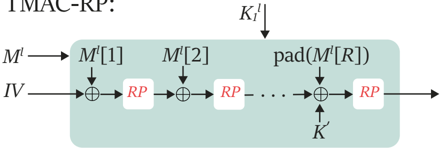



## Idealization

CBCMAC-RP:



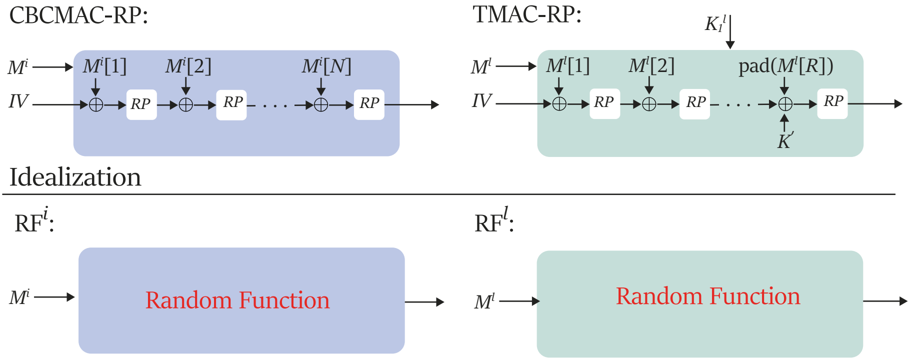

TMAC-RP:




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




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