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

крыштаграфія การอ่านรพัส kriptografija ويسى Liliya R. Akhmetzyanova grafaiochta 密码 kriptografi cifrado קריפטוגרפיה в кірторалі сібгадо такана арантанарара на карантанара странавана справана справана справана справана справана с crittografia dulmal cripteagrafia Evgeny K. Alekseev, Grigory A. Karpunin, wolumphone product kryptografia Igor B. Oshkin, Grigory K. Sedov, สุทธมนาสาว การที่สี kriptografija حدثوبس kriptografija 암호화 criittografia dulmál cripteagrafaíochta 密码 kriptografi cifrado جرستاندس რ家外PTのPROdudyuqhunupnili kryptografia კრიპტოგრაფიის криптография крилточрафпоп cryptography 暗号化 n крыптаграфія การอ่านรพัส kriptografija حرز نوبسي kriptografija 엄호화 crittografia dulmal cripteografajechta 密

Key Lifetime

① Key Lifetime^{Ta} dudyuqhunupjnu kryptografia дбоддогдбодоов криптография криятографион стурtography 暗号化 kryptographie किप्टोगाफी salauksen крыптаграфія การอ่านรมัส kriptografija دمزنويسي kriptografiju 암호화 crittografia dulmál cripteagrafaíochta 密 หตุ 2 🖉 सह अग्रियामि मिल्लि सिल्लि सिल्ले किंद्रों वाफी salauksen крыптаграфія การอำนรพัส kriptografija (المرز نويسى kriptografiju धेडे के crittografia dulmál cripteagrafaíochta 密码 kriptografi cifrado הריפטוגרפיה mât mã hoc криптографія criptografia ծածկատիилизити krvptografia - (3) StandafdizeduInternallypuRelakeyed Modestirado جرام mât mã học κριμπογραφία criptografia อ้นเอ้นแต่hunupuntu kryptografia สูต์ออัตกอุจ์อดูดอย่ หุวนทางเวอล์หมุ หวุบสาวงุวล์ตุกอก cryptography 暗号化 kryptographie किप्टोबाफी salauksen ma 4 но Security Amalysis uchunternit kryptografia ვრიპტოგრაფიის криптография крижтоүрафпол cryptography 暗号化 KNOWTOWER Security Analysis of OMAC ACPKM Master mode with a kinoprating of SH კრიპტოვრაფიის криптография крилтографијан cryptography 暗号化 kryptographie किप्टोबाफी salauksen крыптаграфия การอ่านรหัส kriptografija 5) Practical Meaning of Pricoftsochta 密码 kriptografi cifrado קריפטוגיפיה måt må hoc криптографія criptografia kryptographie கொடுக்கு கும்பாகாறகற்க காந்து கு

rriptogrāfiju 암호화 crittografia dulmál cripteagrafaíochta 密码 kriptografi cifrado קריכשוגרפיה mật mã học หриптография criptografia huðljuuqhunnepinul kryptografia კრიპტოგრაფიის криптографяя криптоүра́фяјот cryptography 暗号化 kryptographie किप्टोबाफी 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 ≤ 160 MB) — "TEMPEST attacks against AES" paper, https://www.fox-it.com.

крыл

mật mã học криптография criptografia ծածկագիտություն клурtografia კრიპტოგრაფიის криптография кролтоүрфирал слурtography 暗号化 клурtographie किप्टोबाफी salauksen крыптаграфия การอ่านรหัส kriptografija حزنونس kriptogrāfiju 음文刻, duļmý griptografija galastija கு riptogrāfiju 암호화 crittografia dulmál cripteagrafaiochta 密码 kriptografi cifrado प्रण्यारण्य mật mã học криптографія criptografia hublµuqhunupjnu kryptografia კრიპტოგრაფიის криптография криятоурбарат cryptography 暗号化 kryptographic किप्टोबाफी 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/.

кролтоурафията стурнодгария на קון ктурнодгарие ואיילואיין אואראו אואראון אואראון אואראון אואראיין אואראיין אוא

- 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 < 160 MB) — "TEMPEST attacks against AES" paper, https://www.fox-it.com.

mật mã học криптография criptografia ðuðljuuqhunnpjntu kryptografia კრიპტოგრაფიის криптография крилтоүрафијат cryptography 暗号化 kryptographie किप्टोबाफी salauksen крыптаграфія การอ่านรหัส kriptografija جنزنویسی kriptogrāfiju_当定时tografija dujmý griptografija



(CryptoPro LLC)

Re-keying Mechanisms

kryptographie किंप्टोगाफी salauksen крыптаграфія การอ่านรมัส kriptografija دمزنويسي kriptografiju 암호화 crittografia dulmál cripteagrafaíochta 密 マククーム Re-keying Mechanisms टोवाफी salauksen สุมหาวอานุรทัส kriptografija (しんしょう) kriptogrāfiju 암호部 crittografia dulmál cripteagrafaíochta 密码 kriptografi cifrado ריביטגרפיה mát mã hoc криптографія criptografia ծածկազիտություն krvptografia - (3) StandafdizeduInternallypuRelakeyed Modestirado جرام mât mã học κριμπογραφία criptografia อ้นเอ้นแต่hunupuntu kryptografia สูต์ออัตกอุจ์อดูดอย่ หุวนทางเวอล์หมุ หวุบสาวงุวล์ตุกอก cryptography 暗号化 kryptographie किप्टोबाफी salauksen mā (4) ho Security Analysišjuuqhunnipinik kryptografia კრიპტოგრაფიის криптография криттоурафијат стурiography 暗号化 kryptographie विमरोबाफी selauksen клантаграфія การอ่านมัล briptografie (Selauksen kryptografiiu 암호화 crittografia dulmál criptografialochta 불 정 kriptografi cifrado 파고가 (Selauksen kryptografia henroradia) auditudhumnipintu kryptografia კრიპტიგრაფიის криптография KNOWTOWER Security Analysis of OMAC ACPKM Master mode with the kinoterating of SH კრიპტოვრაფიის криптография крилтографијан cryptography 暗号化 kryptographie किप्टोबाफी salauksen крыптаграфия การอ่านรหัส kriptografija 5) Practical Meaninguofi Proofsochta 密码 kriptografi cifrado קריפטערפיז måt må hoc криптографія criptografia kryptographie கொடுக்கு கும்பாகாறகற்க காந்து கு

kriptogrāfiju 암호화 crittografia dulmál cripteagrafialochta 密码 kriptografi cifrado प्राण्यात्वरण mật mã học криптография criptografia διαδίμαφηματισμαία kryptografia კრοპტოვრაფიου криптография криптография стурtography 暗号化 kryptographic किप्टोबाफी salauksen 啊 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.

អ្នកកែកក្រណ្តាញ cryptography 暗号化 kryptographie កែកចោងថា salauksen ห្ਰេសក្រាតក្នុងពុំនេ การอานรหัส kriptografija لافر نویسی kriptogrāfiju 智호章 rii Re-keying

²² An efficient way to increase the key lifetime can be the usage of re-keying mu mechanisms (using block cipher $E = (E_K \in Perm(\{0, 1\}^n) | K \in \{0, 1\}^k)$ as a pu black-box primitive):

mậ

• on the block cipher mode of operation level (internal re-keying);

• on the message processing level (external re-keying).

rrittografia dulmál cripteagrafaíochta 密码 kriptografi cifrado קריפטוגרפיה mât mã học криптографія criptografía ծածկազիտություն kryptografía

³⁶ 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

mật mã học криптография criptografia ðuðlµuqhunnupıntu kryptografia კრიპტოგრაფიის криптография крилтография стурtography 暗号化 kryptographic किप्टोबाफी salauksen крыптаграфия การอำนรหัส kriptografija حزنوسی kriptografiju 엄호討, جرزtografia kriptogrāfiju 皆호幹 crittografia dulmál cripteagrafialochta 密码 kriptografi cifrado प्राण्यात्यक māt mā hoc криптография criptografia bubljuuqhunutpinu kryptografia კრიპტოგრაფიის криптография криятоурфарац cryptography 暗号化 kryptographic किप्टोबाफी salauksen 啊 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.

ম্চাদ্বাৰ্গ্য কেন্দ্ৰ কেন্দ্ৰাৰ্গা আৰু প্ৰাৰ্গ কেন্দ্ৰ কেন্দ্ৰাৰ্গা salauksen ম্চাদ্ৰান্বক্ৰায় নাত্ৰাযাত্বৰ kriptografija হেই kriptografiju প্ৰইজ ^{crit} Re-keying

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

• on the block cipher mode of operation level (internal re-keying);

• on the message processing level (external re-keying).

rittografia dulmál cripteagrafaíochta 密码 kriptografi cifrado קריפטגרפיה mât mã học криптографія criptografia δuðljurqhunnpjníu kryptografia

⁴⁶ Concepts of internal and external re-keying approaches are described in «Increasing ⁴⁷ the Lifetime of Symmetric Keys for the GCM Mode by Internal Re-keying» provided ¹⁷ by us at https://eprint.iacr.org/2017/697.pdf

mật mã học криптография criptografia ðuðlµuqhunnıpınılı kryptografia კრიპტოგრაფიის криптография крилтография стурtography 暗号化 kryptographic किप्टोबापी salauksen крыптаграфия การอยามรหัส kriptografija جنزندیسی kriptografiju 음호朝جرrittografia kriptogrāfiju 皆호幹 crittografia dulmál cripteagrafialochta 密码 kriptografi cifrado प्राण्यात्यक māt mā hoc криптография criptografia bubljuuqhunutpinu kryptografia კრიპტოგრაფიის криптография криятоурфарац cryptography 暗号化 kryptographic किप्टोबाफी salauksen 啊 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.

স্চাল্লাক্র্যুর্বের্দ্রার برونویسی kriptographie কেন্দ্রাব্যাদ্য salauksen স্র্চানের্ব্রের্দ্রান برونویسی kriptografiju প্রতির্জ ^{crit} **Re-keying**

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

• on the block cipher mode of operation level (internal re-keying);

• on the message processing level (external re-keying).

rittografia dulmál cripteagrafaíochta 密码 kriptografi cifrado רְרִיפּטארִיפּיה mât mã học криптографія criptografia dudhuuqhunupjnú kryptografia

⁽⁶⁾ Concepts of internal and external re-keying approaches are described in «Increasing ⁽⁷⁾ the Lifetime of Symmetric Keys for the GCM Mode by Internal Re-keying» provided ⁽¹⁰⁾ by us at https://eprint.iacr.org/2017/697.pdf

mật mã học криптография criptografia ðuðlµuqhunnıpını'ı kryptografia კრიპტოგრაფიის криптография крилтография стурtography 暗号化 kryptographic किप्टोबापी salauksen крыптаграфія การอำนาหัส kriptografija جنرنویس kriptografiju 음文刻,griptografia kriptogrāfiju 皆호幹 crittografia dulmál cripteagrafialochta 密码 kriptografi cifrado प्राण्यात्यक māt mā hoc криптография criptografia bubljuuqhunutpinu kryptografia კრიპტოგრაფიის криптография криятоурфарац cryptography 暗号化 kryptographic किप्टोबाफी salauksen 啊 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.

স্চাল্লাক্র্যুর্বের্দ্রার برونویسی kriptographie কেন্দ্রাব্যাদ্য salauksen স্র্চানের্ব্রের্দ্রান برونویسی kriptografiju প্রতির্জ ^{crit} **Re-keying**

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

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

ittografia dulmál cripteagrafaíochta 密码 kriptografi cifrado בקריפטערפיה mât mã học кряптографія criptografia לא אניקען kryptografia נעסט איז איז איז איז איז געט איז איז איז איז איז איז א

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

mật mã học криптография criptografia ðuðljuuqhunnpjníu kryptografia კრიპტოგრაფიის криптография криятоүрафијат cryptography 暗号化 kryptographie किप्टोबाफी salauksen крыптаграфия การอ่านรหัส kriptografija جنزنویسی kriptogrāfiju_왕호희_erijtografia du]máj gripteggrafiaekjaae

Re-keying Mechanisms

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.



ومزنريسي kriptografiju 법호

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.

kriptoerāliju 암호화 crittoeralīa dulmál cripteaeralalochta 密码 kriptoeralī cilirado รางแรงชาว mât mã hoc коншт งน Internal Re-keying

Re-keying Mechanisms

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

رمزنويسى kriptogrāfiju 암호화 crittografia dulmal cripteagrafaíochta 密码 kriptografi cifrado קריפטוגרפה mật mã học криптографія criptografi δω **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.

ชนเงินแนตhumusimilu kryotoeratia เด็ดอัสดอสด์อององไ หอมเทางารอสมมส หองสาสงงอล์องกรก cryotoaraphy 暗号化 kryotoeraphie किप्टोबाफी salaukser ^{kpi} Parameters of obtained bounds: number of queries q, maximal message length m. ^{må} Ideally: to have more accurate bounds with parameter σ — total message length. ^{krypi}

Internal Re-keying Internal Re-keying Idea: RFC 4357 (2006), «CryptoPro Key Meshing» (CPKM). Widely spread in the Russian versions of TLS, IPsec and CMS protocols. Resident and construction of the spurrorpages employed in the Russian versions of TLS, IPsec and CMS protocols.

Re-keying Mechanisms

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

رمز لوبسر kriptogrāfiju 암호화 crittografia dulmāl cripteagrafaíochta 密码 kriptografi cifrado קריפטוגרפיה mật mã học криптографія criptografi w **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.

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

Re-keying Mechanisms

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

رمز نریسی kiptogrāfiju 암호화 crittografia dulmál cripteagrafaíochta 密码 kriptografi cifrado جریفینی mật mã học κριπτοτραφία criptografi کس 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.

ծածևասիտություն krystoarafia არօპტიფირალიის контография контоусфетен ervetoaraphy 暗号化 krystoaraphie ि 保守部分 salauksen Parameters of obtained bounds: number of queries q, maximal message length m. ^{mi} **Ideally:** to have more accurate bounds with parameter σ — total message length. Idea: RFC 4357 (2006), «CryptoPro Key Meshing» (CPKM). Widely spread in the Russian versions of TLS, IPsec and CMS protocols.

Re-keying Mechanisms

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

رمز نويسى kiptogrāfiju 암호화 erittografia dulmál eripteagrafaíochta 密码 kriptografi cifrado جرمعتند عن mật mã học κριπτοτραφία eriptografia δω <mark>Related work</mark>

- 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.

Standardized Internally Re-keyed Modes

mâ நாலக்கிலை குறைக்கு kryptographie किंप्टोगाफी salauksen крыптаграфія การอ่านรมัส kriptografija دمزنويسي kriptografiju 암호화 crittografia dulmál cripteagrafaíochta 密 crittografia dulmál cripteagrafaíochta 密码 kriptografi cifrado הריפטוגרפיה mât mã hoc криптографія criptografia ծածկատիилизити krvptografia 3 Standardized Internally Re-keyed Modes and means mit mit how representation of the representation of the second อ้นเอโนแต่หมากเจาแน่ kryptografia วอดอังคอดองคอดปี หวุ่มหากการสุดหลุ หอบสาวองอังกาก cryptography 暗号化 kryptographic किप्टोबाफी salauksen mā (4) ho Security Analysišjuuqhunnipinik kryptografia კრიპტოგრაფიის криптография криттоурафијат стурiography 暗号化 KNOWTOWER Security Analysis of OMAC ACPKM Master mode with a kinoprating of SH კრიპტოვრაფიის криптография крилтографијан cryptography 暗号化 kryptographie किप्टोबाफी salauksen крыптаграфия การอ่านรหัส kriptografija 5) Practical Meaninguofi Proofsochta 密码 kriptografi cifrado קריפטערפיז måt må hoc криптографія criptografia kryptographie கொடுக்கு கும்பாகாறகற்க காந்து கு

riptogrāfiju 암호화 crittografia dulmál cripteagrafaíochta 密码 kriptografi cifrado ராலாமரான mật mã học криптография criptografia யல்புயզիилизріли kryptografia კრიპტოგრაფიის криптография криятоγрафијат cryptography 暗号化 kryptographie किप्टोबाफी salauksen

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 m protocol.



rriptogrāfiju 암호화 crittografia dulmál cripteagrafaiochta 密码 kriptografi cifrado ராண் mā học kpuntorpaфia criptografia http://www.aluntop.nu/ kryptografia კრიპტოგრაფიის криптография криптографият cryptography 暗号化 kryptografia கெய்ன

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]
ersions: (<u>draft-cfrg-re-keying</u>) <u>00 01 02</u> 04 05 06 07 08 09 10 12	03
FRG nternet-Draft ntended status: Informational xpires: September 1, 2018	S. Smyshlyaev, Ed. CryptoPro February 28, 2018
Re-keying Mechanisms for S draft-irtf-cfrg-re-k	

mật mã học криптографія criptografia ծածկшqhunnıpınlu kryptografia კრიპტოგრაფიის криптография кролтографият сryptography 暗号化 kryptographic किप्टोबाफी salauksen крыптаграфія การอำนรหัส kriptografija кискоральных kriptografija,duļny griptografija guļny griptografija kalpu สาptogrāfiju 암호針 crittografia dulmāl cripteagrafalochta 密码 kriptografi cifrado สาของมายสาม mật mã học криштография criptografia tru CTR-ACPKM ศา



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.

(CryptoPro LLC)

riptogrāfiju 암호화 crittografia dulmál cripteagrafaíochta 密码 kriptografi cifrado ་་་་་་་་་་་་་་་་་་་་་་་་་་་་་་་ huðlµuqhunupjnu kryptografia კრიპტოგრაფიის криптография криятсурфирац cryptography 暗号化 kryptographie किप्टोबाफी salauksen фылтаграфия การอำนรหัส kriptografia (جرنريس) kriptogrāfiju 암호화 crittografia dulmál cripteagrafaíochta 密码 kriptografi cifrado प्रजाय

The ACPKM transformation

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

where $s = \lfloor k/n \rfloor$ 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, \ldots, D_s constants allows to prevent collisions of block cipher permutation inputs for key transformation and for message processing.

ծածկագիտություն kryptografia კრიპტოგრაფიის криптография криятоурфороп cryptography 暗号化 kryptographic किप्टोबाफी salauksen крыптаграфия การอำนรหัส kriptografia دورنویس kriptografiju 암호화 crittografia dulmál cripteagrafalochta 密码 kriptografi cifrado در المرابع مرابع مرابع المرابع المرابع

OMAC-ACPKM-Master OMAC-ACPKM-Master_{N T*}: ACPKM-Master_{T*} K^2 K^{l-1} M^l CBCMAC CBCMAC CBCMAC TMAC CBCMAC: TMAC:

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 r_* :

 $K^{1} ||K_{1}^{1}|| \dots ||K^{l}||K_{1}^{l} = \text{ACPKM-Master}_{T^{*}}(K, d, l) = \text{CTR-ACPKM}_{T^{*}}(K, 1^{n/2}, 0^{dln}),$ where $d = \lceil k/n \rceil + 1$. Note that the parameters d and l must satisfy the inequality $d \cdot l \leq 2^{n/2-1}$.

(CryptoPro LLC)

CTCrypt 2018 16/40

Security Analysis

kryptographie किंप्टोगाफी salauksen крыптаграфія การอ่านรมัส kriptografija دمزنويسي kriptografiju 암호화 crittografia dulmál cripteagrafaíochta 密 кр 2) के Reskeying मिलितायागेडां की दोवाणी salauksen крыштаграфія การอำนรพัส kriptografija (مرفرنيس kriptografiju 암호화 crittografia dulmál criptografíaóochta 密码 kriptografí cifrado רְרְפָטוּגָרִפּיה mât mã học криптографія criptografía budhuuqhumnipinu kryptografía - (3) StandafdizeduInternallypuRelakeyed Modestirado جرام mât mã học κριμπογραφία criptografia อ้นอยนองการแก่น kryptografia კრიპტოგრაფიის криптография кролтоүрафият cryptography 暗号化 kryptographic किप्टोबाफी salauksen mi Osecurity Analysis կագիտություն кրуродгаба კრიპტოგრაფიის криптография криятоурафијан стуродгарну 暗号化 • Security Analysis of CTR-ACPKM mode • Security Analysis of OMAC-ACPKM-Master mode კრიპტოვრაფიის криптография крилтографијан cryptography 暗号化 kryptographie किप्टोबाफी salauksen крыптаграфия การอ่านรหัส kriptografija 5) **Practical Meaning**uofi Proofisochta 密码 kriptografi cifrado קריפטערפיז måt må hoc криптографія criptografia kryptographie கொடுக்கு காழ்கள் குகமாகாறகற்க காந்து المحمد الم

criptogrāfiju 암호화 crittografia dulmál cripteagrafaíochta 密码 kriptografi cifrado দেশেওয়েখেলে ক্রেটার্বার criptografia

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.

equiprovision constant and the level of the re-keying impact on cryptographic properties of the used mode and 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.

critte

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.

mật .

kryptographie কিতৌबाफी salauksen หрыштаграфія การอ่านรทัส kriptografija درخرفیسی kriptografiju ម្នាញ kriptografija duļmaj griptegrafakeba 👸

riptogrāfiju 암호화 crittografia dulmál cripteagrafaiochta 密码 kriptografi cifrado ராசவாசன் mā học криптографія criptografia

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.

რიმატივირადიის конитография конитокойствот cryptography 暗号化 kryptographic िक्रेस्टोयाफी salauksen клуритаграфия Articlography kriptography and kriptography a

kryptographie किण्टोबाफी salauksen крыптаграфія การอ่านรหัส kriptografija رمزنوسي kriptografiju भुष्टेई جرازtografia dulmal griptegrafaachda 🕏

riptogrāfiju 암호화 crittografia dulmál cripteagrafalochta 密码 kriptografi cifrado ராசலாசன் mā học криптографія criptografia

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.

kryptographie किप्टोबाफी salauksen крыштаграфія การอำนรหัส kriptografija حذفيه kriptografija المرفوني kriptografija المرفوني المالية المالية المالية المالية المراجع

riptogrāfiju 암호화 crittografia dulmál cripteagrafaiochta 密码 kriptografi cifrado 국가영화가 mật mã học кринтографія criptografia muðljuuqhunupjnulu kryptografia კбоპტიგбაფοοს криптография криттоурафијан cryptography 暗号化 kryptographic किप्टोबाफी salauksen pp pp 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

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

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

	$\frac{\mathbf{Exp}_{SE}^{IND-CPNA-b}(A)}{Exp_{SE}^{IND-CPNA-b}(A)}$	Oracle Encrypt ^b (P, IV)	Ref.
	$K \xleftarrow{\$} SE.K()$ $b' \xleftarrow{\$} A^{Encrypt^b}$	$C \xleftarrow{\$} SE.E(K, P, IV)$ if $b = 0$ then	F
	$b' \leftarrow A^{\text{Encrypt}}$ return b'	$R \xleftarrow{\mathcal{U}} \{0,1\}^{ C }$ return R	a
διι.		return C	ň

крыптаграфія การอ่านรหัส kriptografija برفرنویسی kriptografiju 암호화 criittografia dulmál cripteagrafaíochta 密码 kriptografi cifrado एक्टायराज्य क्रि mã học крыптография крилтоурафия стурtografia לעליקטיט kryptografia ליפטוגרפיז mật mã học крыптография criptografia ბաბկազիսոււթյուն kryptografia კრიპტოგრაფიის крыптография крилтоурафия стурtography 暗号化 kryptographie किर्ण्यावाणी salauksen крыптаграфия การอ่านรหัส kriptografija دونرنوسی kriptografiju 암호하 جيه

(CryptoPro LLC)

riptogrāfiju 암호화 crittografia dulmāl cripteagrafaiochta 密码 kriptografi cifrado प्रणासिक का को boc кринтография criptografia budųuqhuntpintu kryptografia კრიპტოგრაფიის кринтография криятсурффијот cryptography 暗号化 kryptographic किण्टोबाफी salauksen pp na 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

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

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

$\frac{\mathbf{Exp}_{SE}^{IND-CPNA-b}(A)}{K \stackrel{\$}{\leftarrow} SE.K()}$ $b' \stackrel{\$}{\leftarrow} A^{Encrypt^b}$ return b'	Oracle Encrypt ^b (P, IV) $C \stackrel{\$}{\leftarrow} SE.E(K, P, IV)$ if $b = 0$ then $R \stackrel{\mathcal{U}}{\leftarrow} \{0, 1\}^{ C }$ return R return C	
	return C	J.

крыптаграфія การอำนรหัส kriptografija دونرنیسی kriptografiju 암호화 crittografia dulmál cripteagrafaíochta 密码 kriptografi cifrado प्रव्याप्यक्त mật mã học криптография criptografia ბաბկազիստություն kryptografia კრიპტოგრაფიის криптография крижтогрфиртоп cryptography 暗号化 kryptographic किप्टोबाफी salauksen крыптаграфія การอำนรหัส kriptografija درنزنیسی kriptografiju 암호카 جرازtografia niptogrāfiju 암호화 crittografia dulmāl cripteagrafaiochta 密码 kriptografi cifrado ராணமான mật mã học криптография criptografia ածկագիտություն kryptografia კრიპტოგრაფიის криптография криятоγράφηση cryptography 暗号化 kryptographie किप्टोबाफी salauksen рыптаграфія การอำนรหัส kriptografija حفز فيسى kriptografiju 암호화 crittografia dulmál cripteagrafaíochta 密码 kriptografi cifrado جردفيس

^{ma} Theorem

¹⁶ Let N be the parameter of CTR-ACPKM mode. Then for any adversary A with time ¹⁷ complexity at most t that makes queries, where the maximal message length is at ¹⁷ most m ($m \leq 2^{n/2-1}$) blocks and the total message length is at most σ blocks, there ¹⁶ exists an adversary B such that

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

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 $\sigma_j \leq 2^{n-1}$, $\sigma_1 + \ldots + \sigma_l = \sigma$. 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.

خاص المالية المراجبة معند المراجبة ال مراجبة المراجبة مراجبة المراجبة الم مراجبة مراجبة المراجبة الم مراجبة مراجبة المراجبة ال مراجبة مراجبة مراجبة المراجبة المراج مراجبة مراجبة المراجبة مراجبة المراجبة الم مريبة مراجبة مراجب ктірtogrāfiju 皆호鄄 crittografia dulmāl cripteagrafaiochta 密码 kriptografi cifrado マハロロン mật mã học криптография criptografia δυυδίμισμημητεριπί kryptografia კრοპტოგრაფიοს криптография криятоурфарот cryptography 暗号化 kryptographic किप्टोबाफी salauksen 和 **Encryption modes**

Mode	$Adv_{Mode}^{IND-CPNA}(A)$
CTR	$pprox rac{\sigma^2}{2^{n+1}}$
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 $s = \lceil k/n \rceil$, 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 $(\sigma_1 + \ldots + \sigma_l = \sigma, \text{ where } l = \lceil m/N \rceil).$

mật mã học криптография criptografia duudyuuqhunnıpıntu kryptografia კრიპტოგრაფიის криптография кролтоүрафиоп cryptography 端号化 kryptographie மெடிவாகி salauksen крыптаграфия การอำนารหัส kriptografija குட்டியாக kriptografiju පுத்துருittografi riptogrāfiju 암호화 criitografia dulmāl cripteagrafaiochta 密码 kriptografi cifrado ফাডেফেলে mật mã học криптографія criptografia uuðųuuqhunupjnulu kryptografia კრიპტოგრაფიის криптография криттогрффион cryptography 暗号化 kryptographic किप्टोबाफी salauksen рыптаграфія การก่านรมัส kriptografij (حدز نویس) kriptogrāfiju 암호화 crittografia dulmál cripteagrafaíochta 密码 kriptografi cifrado دوز نویس)

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 i 2^{30} blocks = 8 GB.

⁴ 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 ⁹ 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):

$$\frac{c_2m}{N} \cdot \frac{(qN+s)^2}{2^n} = \frac{(qm)^2}{2^n} = \delta \Longrightarrow c_2 = \left(\frac{qm}{qN+s}\right)^2 \cdot \frac{N}{m};$$

крыптаграфія การอำนรทัส kriptografija المركزيسي kriptografiju 암호화 crittografia dulmál cripteagrafialochta 密码 kriptografi cifrado технение mật mã học крыптография criptografia ბшобцицфилитериtů kryptografia კრоპტოგრაფიის крыптография крожтоурафија cryptography 暗号化 kryptographie किर्ण्यावाणी salauksen крыптаграфія การอำนรทัส kriptografija vičių citikografiju 암호화 sriptografia dulmáj gripteagrafiakada ()

(CryptoPro LLC)

CTCrypt 2018 22/40

ктірtogrāfiju 암호화 crittografia dulmál cripteagrafialochta 密码 kriptografi cifrado รางรางแรงราง mật mã học криптография criptografia διαδίμαιφhunntpinu kryptografia კრიპტოგრაფიის криптография криятоγράφηση cryptography 暗号化 kryptographic किप्टोबाफी salauksen хрыптаграфия การอ่านรหัส kriptografija رمز نویس kriptogrāfiju 암호화 crittografia dulmál cripteagrafaíochta 密码 kriptografi cifrado รางราง mā 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):

$$\frac{c_2m}{N} \cdot \frac{(qN+s)^2}{2^n} = \frac{(qm)^2}{2^n} = \delta \Longrightarrow c_2 = \left(\frac{qm}{qN+s}\right)^2 \cdot \frac{N}{m}$$

крыптаграфія การอำนรทัส kriptografija ارمزنویسی kriptografiji 암호화 orittografia dulmál cripteagrafalochta 密码 kriptografi cifrado тэтизээн mật mã học крыптография criptografia ծածկագիимпърти kryptografia კრიპტოგრაფიის крыптография крыттоүрафијан стурtography 暗号化 kryptographie किप्टोबाफी salauksen крыптаграфія การอำนรทัส kriptografija حزنویسی kriptografiju 암호희 حزنویسی kriptografija dulmál cipteagrafaladata

(CryptoPro LLC)

CTCrypt 2018 22/40

หา่ptogrāfiju 암호화 crittografia dulmál cripteagrafaiochta 密码 kriptografi cifrado จางมะอา mật mã học หุกแทรงทุลผุ่มส criptografia ծแปนแปกเกทรงกน์ kryptografia งูดจงสิงญจอง หุกแทรงทุลผุ่มส หุกมสารงทุลผุกๆ cryptography 暗号化 kryptographic किस्टोबाफी salauksen หุกมาราวลตุ่มส การอ่านรหัส kriptografija (حدر فریس) kriptogrāfiju 암호화 crittografia dulmál cripteagrafaíochta 密码 kriptografi cifrado จาราวเรื่อง กรี 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):

$$\frac{c_2m}{N} \cdot \frac{(qN+s)^2}{2^n} = \frac{(qm)^2}{2^n} = \delta \Longrightarrow c_2 = \left(\frac{qm}{qN+s}\right)^2 \cdot \frac{N}{m};$$

крыптаграфія การอำนรหัส kriptografija حفر نویسی kriptografiju 암호화 crittografia dulmál cripteagrafalochta 密码 kriptografi cifrado ருணான mật mã học криптография criptografia ծածկшզիилизриtи kryptografia კრიპტოგრაფიის криптография кроятографията cryptography 暗号化 kryptographie किप्टोबाफी salauksen крыптаграфія การอำนรหัส kriptografija حز نویسی kriptografiju 암호화 artitografia

(CryptoPro LLC)

CTCrypt 2018 22/40

Definition

^{The} 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

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

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

$K \xleftarrow{\$}$	MA.K()
$b' \xleftarrow{\$}$	A^{F^1}
retur	n <i>b</i> ′
	$F^1(M)$
retur	n MA.TAG (K, M)

$$\frac{\operatorname{Exp}_{\mathsf{MA}}^{\mathsf{PRF}-0}(A)}{\operatorname{Rnd} \leftarrow \emptyset}$$
$$b' \stackrel{\$}{\leftarrow} A^{\mathsf{F}^0}$$
$$\mathbf{return} b'$$

return T

Definition

^{The} 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

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

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

$\frac{\mathbf{Exp}_{MA}^{PRF-1}(A)}{K \stackrel{\$}{\leftarrow} MA.K()}$ $b' \stackrel{\$}{\leftarrow} A^{F^{1}}$ return b'	$\frac{\mathbf{Exp}_{MA}^{PRF-0}(A)}{Rnd \leftarrow \emptyset} \\ b' \stackrel{\$}{\leftarrow} A^{F^0} \\ \mathbf{return} \ b'$
$\frac{\text{Oracle } F^1(M)}{\text{return MA.TAG}(K, M)}$	$\begin{array}{ c c c }\hline Oracle \ F^0(M) \\ \hline \mathbf{if} \ \nexists \ T' \in \mathcal{T} : (M,T') \in \mathit{Rnd} \\ \hline \mathbf{then} \\ T \xleftarrow{\mathcal{U}} \mathcal{T} \\ \mathit{Rnd} \leftarrow \mathit{Rnd} \cup \{(M,T)\} \\ \hline \mathbf{else} \\ T \leftarrow T' \\ \mathbf{return} \ T \end{array}$
ктірtogrāfiju 皆호幹 crittografia dulmál cripteagrafalochta 密码 kriptografi cifrado प्राथयरण्डम mật mã học криптография criptografia διαδίμαφhuntpinu kryptografia კრοδტოგრაფιοού криптография криптография сгурtography 暗号化 kryptographic किप्टोबाफी salauksen 砰 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

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

 $d = \lceil k/n \rceil + 1, l = \lceil m/N \rceil, dl \leq 2^{n/2-1}, \sigma_j$ is the total block length of data processed under the section key K^j and $\sigma_j \leq 2^{n-1}, \sigma_1 + \ldots + \sigma_l = \sigma$. The adversary B makes at most max (σ_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.

mật mã học криптография criptografia duudyuuqhunnıpınlu kryptografia კრоპტოგრაფიის криптография крилтокрафијал cryptography 暗号化 kryptographic किप्टोबाफी salauksen крыптаграфія การอ่านรหัส kriptografija جنزنویسی kriptogrāfiju,음室刻,arjįttografia dulmáj griptegrafiagekja,麥 rriptogrāfiju 암호화 crittografia dulmál cripteagrafaíochta 密码 kriptografi cifrado (ריפוגרפיה) mật mã học หุมแบบบาลфия criptografi huðljuuqhunupinuli kryptografia კრიპტიგრაფიის криптография криятоγράφηση cryptography 暗号化 kryptographie किप्टोबाफी salaukse

Authentication modes

Mode	$Adv^{PRF}_{Mode}(A)$
OMAC	$pprox rac{4\sigma^2+1}{2^{n+1}}$
OMAC-ACPKM-Master _{N,∞}	$\approx \frac{4\left(\sigma_1^2 + \ldots + \sigma_l^2\right)}{2^{n+1}} + \frac{(dl)^2}{2^n}$

Table: Security bounds for the OMAC mode and the internally re-keyed OMAC-ACPKM-Master_{*N*,∞} 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 ($\sigma_1 + \ldots + \sigma_l = \sigma$, where $l = \lceil m/N \rceil$).

mật mã học криптография criptografia ðuuðluuqhunnıpınlu kryptografia კრიპტოგრაფიის криптография крилтоүрфиртоп cryptography 障号化 kryptographic किप्टोबाफी salauksen крыптаграфія การอำนรหัส kriptografija حزنونس kriptogrāfiju 암호카 جرازtografia (duļmāj griptografija 震

kryptographie किंप्टोगाफी salauksen крыптаграфія การอ่านรมัส kriptografija دمزنويسي kriptografiju 암호화 crittografia dulmál cripteagrafaíochta 密 หตุ 2 🖉 सह अग्रियामि मिल्लि सिल्लि सिल्ले किंद्रों वाफी salauksen крыптаграфія การอำนรพัส kriptografija (المرز نويسى kriptografiju धेडे के crittografia dulmál cripteagrafaíochta 密码 kriptografi cifrado הריפטוגרפיה mât mã hoc криптографія criptografia ծածկատիилизити krvptografia - (3) StandafdizeduInternallypuRelakeyed Modestirado جرام mât mã học κριμπογραφία criptografia อ้นเอ้นแต่hunupuntu kryptografia สูต์ออัตกอุจ์อดูดอย่ หุวนทางเวอล์หมุ หวุบสาวงุวล์ตุกอก cryptography 暗号化 kryptographie किप्टोबाफी salauksen ma 4 но Security Amalysis uchunternit kryptografia ვრიპტოგრაფიის криптография крижтоүрафпол cryptography 暗号化 KNOWTOWER Security Analysis of OMAC ACPKM Master mode with a kinoprating of SH კбо 🏬 უგრაფიის криптография крияточрафият стурtography 暗号化 kryptographie किप्टोबाफी salauksen крыптаграфия การอ่านรหัส kriptografija 5 Practical Meaning of Proofs chta 图码 kriptografi cifrado meruteerer måt må hoc kputtrorpadia criptografia kryptographie கொடுக்கு காழ்கள் குகமாகாறகற்க காந்து المحمد الم



riptogrāfiju 암호화 crittografia dulmāl cripteagrafaiochta 密码 kriptogrāfi cifrado சுயாசு mật mã học криптография criptografi bublµuqhunupjnu kryptografia კრიპტოგრაფიის криптография криятсурффијон cryptography 暗号化 kryptografia किप्टोबाफी salauksen фылтаграфія การอำนรหัส kriptografia კლაკა kriptogrāfiju 암호화 crittografia dulmāl cripteagrafaiochta 密码 kriptografi cifrado (خريت kriptogrāfi) 암호화 crittografia dulmāl cripteagrafia nāt mā học криптография criptografia ბლასµuqhunupjnu kryptografia კრიპტოგრაფიის криптография криятсурффијон стурtography 暗号化 клуртоgraphie किप्टोबाफी salauksen крыптаграфия การอำนรหัส kriptografia კრიპელიგერი criptography 暗号化 criptografia

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)

(CryptoPro LLC)

riptogrāfiju 암호화 crittografia dulmál cripteagrafaiochta 密码 kriptografi cifrado पर्णापारणक mật mã học криптография criptografia bubluuqhunupjnulu kryptografia კრიპტოგრაფიის криптография криятсурфирор cryptography 暗号化 kryptographic किप्टोबाफी salauksen фылтаграфія การอำนรหัส kriptografia زيرنريسي kriptogrāfiju 암호화 crittografia dulmál cripteagrafaíochta 密码 kriptografi cifrado ए пāt mã học криптография criptografia مالا يريزنوسي kriptogrāfiju 암호화 crittografia dulmál cripteagrafaíochta 密码 criptography 暗号化 ušt mā học криптография criptografia ბшბluuqhunupjnulu kryptografia კრიპტოგრაფიის криптография кроятсерфирор стурtography 暗号化 cryptographie किप्टोबाफी salauksen крыптаграфия การอ่านรหัส kriptografia kriptografia kriptografiju 암호화 crittografia dulmál cripteagrafaíochta 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)

(CryptoPro LLC)

riptogrāfiju 암호화 crittografia dulmál cripteagrafaiochta 密码 kriptografi cifrado पर्णापारणक mật mã học криптография criptografia bubluuqhunupjnulu kryptografia კრიპტოგრაფიის криптография криятсурфирор cryptography 暗号化 kryptographic किप्टोबाफी salauksen фылтаграфія การอำนรหัส kriptografia زيرنريسي kriptogrāfiju 암호화 crittografia dulmál cripteagrafaíochta 密码 kriptografi cifrado ए пāt mã học криптография criptografia مالا يريزنوسي kriptogrāfiju 암호화 crittografia dulmál cripteagrafaíochta 密码 criptography 暗号化 ušt mā học криптография criptografia ბшბluuqhunupjnulu kryptografia კრიპტოგრაფიის криптография кроятсерфирор стурtography 暗号化 cryptographie किप्टोबाफी salauksen крыптаграфия การอ่านรหัส kriptografia kriptografia kriptografiju 암호화 crittografia dulmál cripteagrafaíochta 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)

enitoğrana aumaı enpresyrana ozuna er es knpiogran eurado என்னை என்னை கை நாயானுக்குக enprograna ouoquuqpunnepinu kryptografia தல்லு குலைக்கு மல் குயானுக்கை கல்கான குலகானுக்கு வில்கு கல்கு கல்கு கல்கு கல்கள் குலக்கு கல்கள் குலகானுக்கு குல தல்லு கல்கு கல்கள் கல்கானுக்கு கல்கள் கல்க கல்கள் கல்கள்

(CryptoPro LLC)

riptogrāfiju 암호화 crittografia dulmál cripteagrafaiochta 密码 kriptografi cifrado पर्णापारणक mật mã học криптография criptografia bubluuqhunupjnulu kryptografia კრიპტოგრაფიის криптография криятсурфирор cryptography 暗号化 kryptographic किप्टोबाफी salauksen фылтаграфія การอำนรหัส kriptografia زيرنريسي kriptogrāfiju 암호화 crittografia dulmál cripteagrafaíochta 密码 kriptografi cifrado ए пāt mã học криптография criptografia مالا يريزنوسي kriptogrāfiju 암호화 crittografia dulmál cripteagrafaíochta 密码 criptography 暗号化 ušt mā học криптография criptografia ბшბluuqhunupjnulu kryptografia კრიპტოგრაფიის криптография кроятсерфирор стурtography 暗号化 cryptographie किप्टोबाफी salauksen крыптаграфия การอ่านรหัส kriptografia kriptografia kriptografiju 암호화 crittografia dulmál cripteagrafaíochta 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)

erittograma aumai enpreagramaioenia காசு காறiogran eurado எச்பலை அளை வரை கற்பாரைகளுக் enprograma ouoquiqponnipinu காறiografia புல்லுகளை குறுக்கு குறைக்கு கார்க்கு காற்மதான் குறைக்கு குறுக்கு குறுக்கு குறுக்கு குறுக்கு குறுகள் குறுக்கு குற புல்லுகள் குறுக்கு குறைக்கு குறுக்கு குறைக்கு குறுக்கு குறைக்கு குறைக்கு குறைக்கு குறுக்கு குறைக்கு குறு குறுக்கு குறு குறுக்கு கு குறுக்கு குறுக்கு குறுக்கு குறைக்கு குறைக்கு குறைக்கு குறைக்கு குறைக்கு குறு குறு குறுக்கு குறைக்கு குறைக்கு குறைக்கு குறைக்கு குறு குறுக்கு குறைக்கு கு

(CryptoPro LLC)

ктірtogrāfiju 암호화 crittografia dulmál cripteagrafialochta 密码 kriptografi cifrado प्राण्यात्यक mật mã học криптография criptografia διαδίμισμημητεριπί kryptografia კრοδეტოგრაფეიοს криптография криптография стурtography 暗号化 kryptographic किप्टोबाफी salauksen 啊 Relation with heuristic approach

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



mật mã học криптография criptografia duudµunµpınu kryptografia კრიპტოგრაფიის криптография кролтоүрбөрлөп cryptography 暗号化 kryptographie கெயியார் salauksen крыптаграфия வாப்பார்க் kriptografija பெட்டியார் குரியாருக்கு குருப்பதாவுக்கு இ riptogrāfiju 암호화 crittografia dulmāl cripteagrafaiochta 密码 kriptogrāfi cifrado ரான் mā học криптографія criptogrāfi யல்புயqhunnipjnili kryptografia კრიპტოგრაფიის криптографяя криятсоγράφηση 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, R «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.



mật mã học криптография criptografia ծածկագիտություն kryptografia კრიპტოგრაფიის криптография криятоүрифијан cryptography 暗号化 kryptographie किप्टोबाफी salauksen крыптаграфия การอ่านรหัส kriptografija جنزنویسی kriptogrāfiju 음室尊, griptografiga, duļmý griptografija cu

kriptogrāfiju 암호화 crittografia dulmál cripteagrafaiochta 密码 kriptografi cifrado ராலாமான mật mã học кринтографія criptografi ծածկագիտություն kryptografia კრօპტოგრაფითბ кринтография криятоγράφηση cryptography 暗号化 kryptographie किप्टोबाफी salauksen крынтаграфія การப்านรหัส kriptografia رمز فریس kriptogrāfiju 암호화 crittografia dulmál cripteagrafaiochta 磁码 kriptografi cifrado ராலாமாரு mật mã học кринтография criptografia ծածկագիտություն kryptografia კრიპტოგრაფითს кринтография криятоγράφηση cryptography 暗号化 kryptographie किप्टोबाफी salauksen крыятаграфия поголизหัส kriptografia კრიპტოგრაფითს криятография криятоγράφηση тато критография criptografia ბობელი cryptography 暗号化 кгуртодарны किप्टोबाफी salauksen крыятаграфия norschuruða kriptografija kriptografiju 암호화 crittografia dulmál cripteagrafaiochta ख

Thank you for your attention!

rittografia dulmál criptografia óuðluuqhunnıpınılı kryptografia א קרישטערפיד måt mä hoc криптографія criptografia óuðluuqhunnıpınılı kryptografia א סעestions?

audhuudhunnaamuli krontoorafia adalaamadaamad kenurramadaar konstrandumen erontooranho 随星化 krontooranhie किप्टोबाफी salaalase Ru Ouestions, comments:

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

(CryptoPro LLC)

CTCrypt 2018 31/40

kriptogrāfiju 암호화 crittografia dulmál cripteagrafialochta 密码 kriptografi cifrado எரலமான mật mã học кринтография criptografia ბயბկագիտություն kryptografia კრიპტოგრაფიის кринтография криятсурффијон cryptography 暗号化 kryptografia টিন্টেবীয়াজি salauksen хрынтаграфия การอ่านรทัส kriptografia კრიპტოგრაფიის кринтография криятсурффијон cryptography 暗号化 kryptografia টেন্টেবীয়াজি salauksen аркинтаграфия การอ่านรทัส kriptografia ბயბцицарилизации পিছি কो crittografia dulmál cripteagrafialochta 密码 kriptografi cifrado குரு так mã học кринтография criptografia ბuðuļuuqhunuspintu kryptografia კრიპტოგრაფითის криятсурффијон стуртоgraphy клурноварна бласдашбы salauksen криятсирафия споновала kriptografia kriptografia kriptografia dulmál cripteagrafialochta 密 ფ «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.

კრიპტოგრაფიის криптография криятоүрфироп cryptography 贈号化 kryptographie किप्टोबाफी salauksen криптаграфия การอานรหัส kriptografia روز نرویسی kriptografia dulmál cripteagrafialochta 密码 kriptografi cifrado جرسی mật mã học криптография спрtografi ბաბկագիտություն kryptografia კრიპტოგრაფიის криптография криятоүрфироп cryptography 暗号化 kryptografia icifrado اورز نرویسی криптаграфия การอำนรหัส kriptografia კრიპტოგრაფიის криптография криятоурфироп cryptography 暗号化 kryptografia icifrado اورز نرویسی קستوعنده kriptografia اورز نرویسی kriptografii የደንቋት crittografia dulmál cripteagrafialochta 密码 kriptografii cifrado اورز نرویسی شا mã học криптография criptografia ماسکان kriptografii የደንቋት crittografia dulmál cripteagrafialochta 密码 kriptografi kryptographi জ kriptografia ماسکان kryptografia ئورز ماسکان در ماسکان در ماسکان در در در سال در ماسکان در در ماسکان در نرویسی kryptografia ماسکان در ماسکان در در ماسکان در در سال در در ماسکان در ماسکان در در ماسکان در در ماسکان

ктірtogrāfiju 암호화 crittografia dulmál cripteagrafaiochta 密码 kriptografi cifrado प्राण्यात्वाभ mā boc криптография criptografia ბயბцицիилизрпи kryptografia კრიპტოგრაფიის криптография криятоγράφηση cryptography 暗号化 kryptographic किप्टोबाफी salauksen крыптаграфія การอำนรหัส kriptografia رحز نریسی kriptogrāfiju 암호화 crittografia dulmál cripteagrafaíochta 密码 kriptografi cifrado رحز نریسی māt mā hoc криптография criptografia ბшბцицфилизрпић kryptografia კრიპტოგრაფიის криптография кроятоγράφηση cryptography 暗号化 kryptographic किप्टोबाफी salauksen крыптаграфия การอำนรหัส kriptografia კრიპტოგრაფიის криптография спірtografia dulmál cripteagrafaíochta 密

Forgery threat: known relation

^{con} Let $MA = \{MA.K, MA.TAG\}$ be a message-authentication scheme. Then for any ³⁶ adversary *A* there exists an adversary *B* such that

$$\mathsf{Adv}_{\mathsf{MA}}^{\mathrm{EU-CMA}}(A) \leqslant \mathsf{Adv}_{\mathsf{MA}}^{\mathsf{PRF}}(B) + rac{1}{2^{ au}},$$

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.

erittografia dulmál criptegarafalochta 密码 kriptografi cifrado எனைனான விரை குணானைவுக்கு criptografia dulhál criptegarafalochta 密码 kriptografia cifrado குணானை விரைவில் குமையானைவுக்கு விரும் குண்ணை விருக்கு குண்ணை விருக்கு குண்ணைக்கு விருக்கு விருக்கு குண்ணைக்கு விருக்கு குண்ணைக்கு விருக்கு விருக்கு குண்ணைக்கு விருக்கு விருக்க

(CryptoPro LLC)

CTCrypt 2018 33/40

кriptogrāfiju 암호화 crittografia dulmál cripteagrafaíochta 密码 kriptografi cifrado प्रण्यास्यक mật mã bọc криптография criptografia ծшðцицիипирјпии kryptografia კრоპტთგრაფიის криптография крилтоүра́фијот cryptography 暗号化 kryptographic किप्टोबाफी salauksen

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 $Adv_E^{PRP-CPA}(B) \leq \frac{t}{2^{256}}$ 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:

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

ន្កាសព្រះជាទងទំនេ ការចារបទអធ knptogratija در دوند دوسی knptogratiju 원조와 cnitogratia dulmal cnpteagrataiochta 密码 knptograti curado লত্যাতে ব্ mật mã học криптография criptografia ծածկազիտություն kryptografia კრიპტოგრაფიის криптография кроятоγράφηση cryptography 暗号化 kryptographic কিন্দ্রীৰাজী salauksen крыптаграфия การอำนาวหัส kriptografija در دوند دو kriptografiju 음 호황 جرائروسي cupide and cupide and set an ктірtogrāfiju 암호화 crittografia dulmál cripteagrafaíochta 密码 kriptografi cifrado प्राप्ताक केद криптографія criptografia buðljuuqhunnipjnili kryptografia კრიპტოგრაფიის криптография криятоγра́фијон сryptography 暗号化 kryptographie किप्टोबाफी salauksen

Comparison

Number of sections	$CTR-ACPKM_N \succeq CTR$	$OMAC-ACPKM-Master_{N,\infty} \succeq OMAC$
<i>l</i> = 2	$s \leqslant \min(\sqrt{2N}, \sigma_2)$	$d\leqslant\min(N,2\sigma_2)$
<i>l</i> = 3	$s \leqslant \min(\sqrt{2N}, N/2)$	$d \leq \min(N, 16)$
$l \ge 4$	$s \leq \min(\sqrt{2N})$	$d\leqslant N$

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*.

mật mã học криптография criptografia ծածկագիտություն kryptografia კრоპტოგრაფიის криптография кроятоүрфирал cryptography 暗号化 kryptographie किप्टोबाफी salauksen крыптаграфия การอ่านรหัส kriptografija جنزنویسی kriptogrāfiju 음호화, arjttografia



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



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).



kriptogrāfiju 암호화 crittografia dulmál cripteagrafalochta 密码 kriptografi cifrado รารระบบราสา mật mã học หุมเทางาрафія criptografia อนปนุนฤทมานอากาน kryptografia สูต่ออัดจฎดีอสูงออบ หุมเทางาрафия หุมหารงypáตุกอา cryptography 暗号化 kryptographic किप्टोबाफी salauksen หุมเทาลายลอต์ส การย่านรมัส kriptografia (خريس) kriptografiiu 암호화 crittografia dulmál cripteagrafalochta 密码 kriptografi cifrado ราชยามายา mâ The second step



ittoerafia dulmál cripteaerafaíochta 密码 kriptoerafi cifrado דריפטוגרפה mât mã hoc криптографія criptoerafía ծածկազիտություն kryptoerafi

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

крыптаграфія การอำนรหัส kriptografija دىر ئويسى kriptografiju 암호화 crittografia dulmál cripteagrafalochta 密码 kriptografi cifrado স্তেখেতেক mật mã học крыптография criptografia ბաბկազիտություն kryptografia კრიპტოგრაფიის крыптография крыятоүрфиртоп cryptography 暗号化 kryptographic किर्ण्यावाणी salauksen крыптаграфія การอำนรหัส kriptografija در نوبسي kriptografiju 암호취 جرائروهي



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



кriptogrāfiju 암호화 crittografia dulmál cripteagrafiaíochta 密码 kriptografi cifrado קריפטוגרפיה mật mã học криптографія criptografi

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

kryptografijie ដែលចារាទៅ salauksen หрыттаграфія การอ่านรหัส kriptografija درخرفيس kriptografiju មុខខ្មែរ جرزtografiju ទៅ salauksen (ulmáj gripteggrafajeckja 🕏