On cryptographic properties of the CVV and PVV parameters generation procedures in payment systems

iptogrāfiju 암호화 crittografia dulmāl cripteagrafalochta 密码 kriptografi cifrado 까ㅋㅋㅋㅋㅋ mật mã học 护で文字中TOPRC

kriptogrāfiju 암호화 crittografia dulmál cripteagrafaíochta 密码 kriptografi cifrado אריפטוגרפיה mát mã hoc криптографія criptografia uðljughunnipindi kryptografia კრიპტოგრა Stanislav V. Smyshlyaev, ^{暗号化} kryptographie किप्टोगफी salauksen รมกาลกอลфiя การอ่านรหัส kriptografi Head of information security department, pptographie क्रिप्टोबाफी salauksen крыптаграфія การอ่ $\mathrm{Grypto-Pro}_{\mathrm{LLG}}$ togrāfiju धेर्डके crittografia dulmál cripteagrafalochta 🕸 ணாலழக்குறி cryptography 暗号化 kryptographi (பிச்சியாக) allahan spannerpadia ராகப்பான் kriptografija பெல் kriptografija utografia dulmál cripteagrafaíochta 密码 kriptografia na spanner zv spinner zv ыздердбадово криптография крыттоурбарот с ${
m Evgeny}$ ${
m K}_{
m ev}$ ${
m Alekseev}$ сы salauksen крыптография криттоурбарот с ${
m Evgeny}$ رمز فره kriptogrāfiju 암호화 crittografia dulmā $\operatorname{Grigory}$ taĀāā Karpunin جريوني شائل mā hoc xpurrorpaķis criptografia սծկագիտություն kryptografia კრიპტოგრაფიის πογράφηση cryptography 暗号化 kryptographie किप्टोगाफी salauksen স্বান্যর্গন মার্চাব্যর্কার কিল্পের্বার্টা কেন্দ্রির مرفريسي kiptografiju প্রিইক crittografia dulmál cripteagrafaíochta 密码 kriptografi cifrado ব্রেজিয়ে ব্যেত্যারেশ ät mä học криптографія criptografia διυδίμαqhunnıəjnili kryptografia კრοპტოგრაფიის криптография криятоура́артор cryptography 暗号化 CTCrvpt 201

S. V. Smyshlyaev (Crypto-Pro LLC)

CTCrypt 2017 1 / 36

hptogrāfiju 암호화 crittografia dulmál cripteagrafalochta 密码 kriptografi cifrado ரையாரை mật mã hoc பாருமுற்றாகிia huðljuuqhunnpjnul kryptografia კრიპტოგრაფიის криптография криятоурфирор cryptography 暗号化 kryptografia குலப்பியனி sumrarpadvis การอ่านรหัส kriptografia جرينيي kriptogrāfiju 암호화 crittografia dulmál cripteagrafalochta 密码 kriptografi cifrado

- Technical Committee for Standardization TC 26 «Cryptography and security mechanisms».
- Subcommittee 3 (SC 3 TC 26) «Cryptographic algorithms and mechanisms for the national payment system of Russian Federation».
- Work in progress from 2016.

и ma noc крыптография сприодгана ошоциционироны клурюдгана зосо-доозоодоод крыптография крижкоурафион слурюдгарну на т У Main objective

To define how to apply Russian cryptographic algorithms in all segments of the payment system in conformance with the Russian requirements for cryptographic data protection.

CTCrvpt 2017

2/36

iptogrāfiju 암호화 crittografia dulmāl cripteagrafalochta 密码 kriptografi cifrado ราชระมะชาวร māt mā hoc CRYPTOPRO แอ้ปุณฤโมภาเราเกเป kryptografia კრიპტოგრაფიის криптографии криптографион cryptography 暗号化 kryptografi

- Preparing the specs: «SPB».
- Cryptographic analysis (7 of 8 documents): «CryptoPro».
- Finalizing the document projects to pass them to expertise: «Infotecs».
- Ker trinfooraffin 2000 rrittoorafi dulmail crinteeoraficochte 2000 trinfoorafi ciffado 2000 mait ma has rourmoroadic crinteer
 ≪The Usage of the KDF to Produce Derived Keys Of
 Payment Applications»
 - «The Usage of Key Agreement Mechanisms and Block Ciphers for Offline PIN Verification»
 - «The Usage of Message Authentication Codes Built from Block Ciphers for Applied Cryptograms Processing in the Payment Systems»

אריקטארפיה אוויספוגען אוויערפיה אוויערפיה אוויערפיה אוויערפיה אוויערפיה אוויערפיה אוויערפיה אוויערפיזיא אוויערפיז אוויערפיה אוויערפיה אוויערפיה אוויערפיה אוויערפיה אוויערפיה אוויערפיה אוויערפיה אוויערפיה אוויערפיינגערפיינגערפי אוויערפיה אוויערפיה אוויערפיה אוויערפיינגערפיה אוויערפיינגערפיה אוויערפיינגערפיה אוויערפיינגערפיינגערפיינגערפיי iptogrāfiju 암호화 crittografia dulmāl cripteagrafalochta 密码 kriptografi cifrado ராஜாலான māt mā hoc CRYPTOPRO ubluuchunupuntu kryptografia კრიპტოგრაფეიის криптография криттография cryptography 暗号化 kryptograp கொடனின் sala

- Preparing the specs: «SPB».
- Cryptographic analysis (7 of 8 documents): «CryptoPro».
- Finalizing the document projects to pass them to expertise: «Infotecs».

) a chintoorātim 史を夢 mitnoratis dulmāl mintesoratsiochts 鄭恩 krintoorati nifrado かいいかい māt mā hon kourmonnaduls mintoorg

- «The Usage of the KDF to Produce Derived Keys Of Payment Applications»
- «The Usage of Key Agreement Mechanisms and Block Ciphers for Offline PIN Verification»
- «The Usage of Message Authentication Codes Built from Block Ciphers for Applied Cryptograms Processing in the Payment Systems»

акылгаграфия Лтэанияма knptogratija שרע אוואס nät mä hoe криптография enptogratia buolyuqhunnipintu kryptografia კრიპტოგრაფიის криптография кроктографият eryptography 暗号化 אוואס אוואס

CTCrvpt 2017

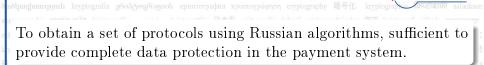
3 / 36

iptogrāfiju 암호화 crittografis dulmāl cripteagrafaiochta 密码 kriptografi cifrado קריפטוגרפיה mật mā hoe אייעראסער rafit ubljuuqhunupjnulu kryptografis კრიპტოგრაფიის криптография криптография слурtography 暗号化 kryptografi cifrado איי אריפטוגרפיה אודר אודי געינעה געינעה געינעה געינעה געינעה געינעה געינעה געינעריט געינערפיר אודר געינער געינערפיר אריפטוגרפיה אודער געינעה געינער געינעה געינערפיר געינעה געינערפיר געינער געינערפיר געינערערפיר געינערערער געינערערפיר געינערפיר געינערפיר געינערפיר געינערפיר געינערער

- «The Usage of Block Ciphers for Producing Card Verification and PIN Verification Values»
- «The Usage of Block Cipher Modes of Operation for Secure Messaging (SM) between an Issuing Bank and a Payment Application»
- «The Choice of Digital Signature and Hash Algorithms for Profiles of Public Key Certificates of Payment Systems»
- «The Usage of Block Ciphers Modes of Operation, Digital Signature and Hash Algorithms for Offline Authentication Procedures of Payment Applications»

hiptogrāfiju 암호화 crittografia dulmāl cripteagrafalochta 密码 kriptografi cifrado קריפטוגרפיה māt mā hoc ערפיערפית rafit uduluiqhunipiniti kryptografia კრიპტოგრაფიის криптография криятоурафијот cryptography 暗号化 kryptografi კრიპტოგრაფიის криптография слитоурафијот cryptography 暗号化 kryptografi კრიპტოგრაფიის криптография слитоурафијот cryptography 暗号化 kryptografi კრიპტოგრაფიის криптография слитоурафијот cryptography 暗号化 kryptografi kryptografi salaukser თაштаграфия การอำนรหัส kriptografija در نریس kriptogrāfiju 암호화 crittografia dulmál cripteagrafalochta 密码 kriptografi cifrado слите сливи слитери криторафия криторафия

- «The Usage of Block Ciphers for Producing Card Verification and PIN Verification Values»
- «The Usage of Block Cipher Modes of Operation for Secure Messaging (SM) between an Issuing Bank and a Payment Application»
- «The Choice of Digital Signature and Hash Algorithms for Profiles of Public Key Certificates of Payment Systems»
- «The Usage of Block Ciphers Modes of Operation, Digital Signature and Hash Algorithms for Offline Authentication Procedures of Payment Applications»



notogrāfiju 암호화 crittografia dulmāl cripteagrafalochta 密码 kriptografi cifrado קריפטוגרפיה mật mã học propropro

- Sufficiency of the set of TC 26 documents
 - The payment systems use a wide range of basic and additional cryptographic algorithms.
 - Before 2016 payment systems were completely out of scope of TC 26, all document development plans were prepared without taking them into account.
 - The existing (in 2016) set of algorithms and protocols in TC 26 had been created without specific thoughts about the payment systems.

sumarpadia אוווס kriptografia איל איין kriptografia איל איין kriptografia dulmál cripteagrafalochta 密码 kriptografi cifrado אינע איין איי V. Smyshlyaev (Crypto-Pro LLC)

CTCrvpt 2017

6 / 36

To make changes in reasonable period with sufficient reliability

- Impossibility of making such changes in protocols that lead to external changes in protocol structures.
- Necessity to use existing primitives to have existing hardware solutions (e.g. GOST 28147-89 implementations in chips).

The need to provide high security level

- The existing EMV protocol set is more than 20 years old.
- Necessity to take specific properties of Russian cryptographic standards into account.
- Necessity to meet the existing set of the requirements.
- Theoretical vulnerabilities lead to practical ones sooner or later (e.g., POODLE, BEAST, Lucky13).
- It wasn't possible to organize a competition for finding vulnerabilities (e.g., the Streebog contest).

To make changes in reasonable period with sufficient reliability

- Impossibility of making such changes in protocols that lead to external changes in protocol structures.
- Necessity to use existing primitives to have existing hardware solutions (e.g. GOST 28147-89 implementations in chips).

The need to provide high security level

- The existing EMV protocol set is more than 20 years old.
- Necessity to take specific properties of Russian cryptographic standards into account.
- Necessity to meet the existing set of the requirements.
- Theoretical vulnerabilities lead to practical ones sooner or later (e.g., POODLE, BEAST, Lucky13).
- It wasn't possible to organize a competition for finding vulnerabilities (e.g., the Streebog contest).

iptogrāfiju 암호화 crittografia dulmál cripteagrafaíochta 密码 kriptografi cifrado எல்லான் இருந்து இருந்து குடிப்புக விபுயழியமாறும் kryptografia தல்தல்குலை குறுக்குக்கு குறைக்குகள் குறுக்குற்று குறுக்குகள் 暗号化 kryptogra

The objective: to obtain a set of security proofs in a provable security paradigm.

тая так пос криптография спроедкана ошочиндилицалии ктургодтана дооодожузовооо المرابعة ا

Requirements for the security analysis process

- The security analysis must have been conducted in adversary models relevant to the current practice of the usage of developed protocols there were a lot of consultations with NSPK (I.M. Goldovsky).
- Modifications of the constructions to obtain end mechanisms with complete security proofs.
- The choice of all parameters in a way that the end security bounds would not contradict existing requirements for cryptographic protection.

CTCrvpt 2017

8 / 36

Procedures of generating CVV and PVV

nptogrāfiju 암호화 crittografia dulmāl cripteagrafalochta 密码 kriptografi cifrado न्द्राधारण्य mật mã học proproprafia uðljuughunnupinuh kryptografia კრიპტოგრაფიის криптография крияточрафион eryptography 暗号化 kryptograft किटोबाफी salauksen সোদাৰাস্বক্ষি মান্চtografija درفرنوسی kriptografiju 암호화 crittografia dulmál cripteagrafaíochta 密码 kriptografi cifrado رمزنوسی ät mä hoc криптографія criptografia ծածկագիտություն kryptografia კრоპტოგრაფიის криптография крултоурафпол cryptography 暗号化 yptographie किप्टोगाफी salauksen крыптаграфія การอ่านรหัส kriptografija رمزنویسی kriptografiju 암호화 crittografia dulmál cripteagrafaíochta 密 Procedures of generating CVV/1 and PV/Vn/1 kryptografia 3603(203659900) криптография மனாலும்டிறை cryptography 暗号化 kryptographie किप्टोगाफी salauksen крыттаграфія การอ่านรหัส kriptografija பி முக்கி ntografia dulmál cripteagrafaíochta 密码 kriptografi cifrado ריפטוגרפה mât mã hoc криптографія criptografia ծածկազիտություն kryptografia лоддоодбодоов криптография крилтоура́флоп cryptography 暗号化 kryptographie किप्टोबाफी salauksen крыптаграфія การอ่านรหัส kriptografija uðljughugnugnafnin 大大yptografia კრიპტოგრაფიის криптография криятографияоп cryptography 暗号化 kryptographie किप्टोगाफी salauksen مستعام مريد من المان المريد kriptografija در نويسي kriptografija المرزيوسي kriptografija المرزيوس kriptografija at mā hoē крыптографія criptografia δшоцицфилицерици kryptografia კრоპტოგრაფიის кринтография крилтография стурtografia у vptoeraphie क्रिप्टोगाफी salauksen หวมกาลrpaфia או איז אווילא kriptografija (يمز نويسي kriptogrāfiju 암호화 crittografia dulmál cripteagrafaíochta 密 боддолдбадоов криптография коилтоурафилоп cryptography 暗号化 kryptographie किप्टोबाफी salauksen крыптаграфія การอ่านรหัส kriptografija אוווססביד crittografi dulmál cripteagrafaíochta 密码 kriptografi cifrado ריפטערפה mât mã hoc ארטוויסרים criptografi ciptografía uðljuughinniðinni kryptografia კრоðტოგრაფიის криптография крилтоурафион cryptography 暗号化 kryptographie किप्टोगाफी salauksen הריפטערפה kriptografija אל אייד kriptografija אל אייד kriptografija או אייד kriptografija אין אייד אייד אייד איי āt mā hoc криптографія criptografia διωδίμισμιπιτριπίι kryptografia კრоპტოგრაფიის криптография крилтоγράφηση cryptography 暗号化

이 이 이 가지지 않는 것 같아. 이 것 같아. 이 것 같아.

Procedures of generating CVV and PVV

The CVV (Card Verification Value) value is used for the control of card attributes (card number, expiration date, service code). CVV is stored at a card and is sent to an issuing bank during a transaction.

อัปแนนูเนนนายุแนน หมายเอนูเลม สูงของกางสูงสุของ มุมแบบเหลยุมม มุยองการกิจสุขายๆ เรายุเอนูเลยมร คม มายอามารถไม่ การสาขายนั้น brintoarafiia من المعالية brintoarafiin முத்தி crittoarafis dulmál crinteaorafaíoduta இது brintoarafi PVV

The PVV (PIN Verification Value) value is used for the control of a card number and a PIN-code. PVV is either stored on a card or at issuing bank storage. If a PVV is stored at a card, it is sent to an issuing bank during a transaction.

auðlµuqhunnpjníu kryptografia კრიპტოგრაფიის криптография криятоγрафијој cryptography 暗号化 kryptographie (シーマ) allauksen mannarpaфia การอำนริทัส kriptografia ريز كريسي kriptografiju 암호화 crittografia dulmál cripteagrafalochta 密码 kriptografi cifrado בريز كريسي alt mā học криптография criptografia ծածկшqhunnpjníu kryptografia კრიპტოგრაფიის криптография криятоурафијој стуртоgraphy 暗号化

Decimalization procedure

•
$$\mathbb{H} = \{0, 1, \dots, 9, A, B, \dots, F\} - hex-symbols$$

•
$$\mathbb{D} = \{0, 1, \dots, 9\}$$
 – decimal symbols

The function of two-pass decimalization is the mapping of $DEC_{m,r}^2: \mathbb{H}^m \to \mathbb{D}^r, m \ge r$, which gives the output on an input $X \in \mathbb{H}^m$ by the following algorithm. If in X there are r decimal symbols, then the string $DEC_{m,r}^2(X)$ is the concatenation of the first r of them (from left to right). If the total number s of decimal symbols is less than r, then the string of $DEC_{m,r}^2(X)$ is the concatenation of these s symbols and r - s residues of dividing first hex-symbols of X by 10.

Example

 $\text{DEC}_{5,3}^2(0||1||C||D||E) = 0||1||(12 \mod 10) = 0||1||2$

11 / 36

Decimalization procedure: alternative

ät mä hoc криптография criptografia ბաბկազիտություն kryptografia კრიპტოგრაფიის криптография криятоүрафиоп cryptography 暗号化 yptographie किप्टोबाफी salauksen крыптаграфия การอ่านรหัส kriptografija kriptografiju 암호화 crittografia dulmál cripteagrafalochta 密 kriptografi cifrado אני מולה מולה מווירים מולה kriptografia לשליק אין אוויס מוויס מוויס מוויס מוויס אוויס אוויס

The function of modular decimalization is the mapping of $DEC_{m,r}^{M} : \mathbb{H}^{m} \to \mathbb{D}^{r}, m \ge r$, the output of which on the input of $X \in \mathbb{H}^{m}$ is equal to $DEC_{m,r}^{M}(X) = INT(X) \mod 10^{r}$.

mrarpaфia א אואטרבארא knptografija (حفر لويسى knptogrāfiju 出京野 cnitografia dulmāl cripteagrafaiochta 被码 knptografi cifrado المتعنين Example

$$\begin{split} DEC_{5,3}^{M}(0\|1\|C\|D\|E) &= 0x1CDE \mod 10^{3} = \\ &= 7390 \mod 10^{3} = 3\|9\|0 \end{split}$$

לאליקעות אואסטער אואסטע אריפטעריד אראסטער אוין געריקער אוין געריקער גען גען געריקעער אואסטער אוין געריקער געריקער געריקער געריקער אויער און אראסער געריקער גערי געריקער געריקער

CVV

ät mä hoo κριμποιραφία criptografia διαδίμαιφμοπιεριτώ kryptografia კრοპტოგრაფიοს κριμποιραφία κρυπτογράφηση cryptography 暗号化 ynterenetis Carabanti aslasian merenenaskis operaturite bistometic and tee bistometiciis () 考虑 minerastic bistof allerenasticiates 磨 Input parameters

- PAN Personal Account Number (usually, 12-16 decimal digits).
- ExpDate Expiration Date (4 decimal digits in the form YYMM).
- SVC Service Code (3 decimal digits, can take the only 6 values: 000, 999, 200, 201, 220, 221).
- CVK key value for generating CVV (256 bits). CVK is stored and managed by an issuing bank.

Output

CVV - Card Verification Value (3 decimal digits).

Procedures of generating CVV and PVV

 Integrafiju 営主部 crittografia dulmál criptegrafialochia 密码 kriptografi cifrado エアコルビアマ mět mě hoc CRYPTOPRO affa habituchumupinu kryptografia globějováčegobě spurnorpadnu sportovpádnom cryptography 暗号化 kryptografia dulmál criptegrafia dulmál dulmál criptegrafia dulmál dul

• $\text{CVV} = \begin{cases} \text{DEC}_{16,3}^2(\text{C}) & -\text{ as in VISA payment system;} \\ \text{DEC}_{16,3}^M(\text{C}) & -\text{ only for MIR payment system.} \end{cases}$

PVV

ät mä hoe криптографія criptografia dudljuuqhunnıpınılı kryptografia კбозტюдбъздоов криптография криятоүрафороп cryptography 暗号化

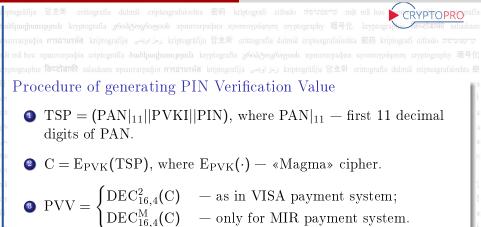
Input parameters

- PAN Personal Account Number (usually, 12-16 decimal digits);
- PIN Personal Identification Number (4 decimal digits, if PIN length greater than 4, then 4 left digits are used);
- PVKI PIN Verification Key Indicator (decimal digit from 0 to 6);
- PVK key value for generating PVV (256 bits). PVK is stored and managed by an issuing bank.

ريوز فريس kriptogrāfiju 암호좌 crittografia dulmál cripteagrafaíochta 密码 kriptografi cifrado جرستان المراجع mật mã học kpunrorpaφia criptografia • Output

 $\mathrm{PVV}-\mathrm{PIN}$ Verification Value (4 decimal digits).

Procedures of generating CVV and PVV



مائل المرابعة على المائلة المرابعة المائلة المرابعة الم المرابعة الم المرابعة الم المرابعة الم المرابعة الم المرابعة الم المرابعة ال المرابعة الم المرابعة الم المرابعة الم المرابعة الم المرابعة الم

Distributions of decimalization functions

at mã học криптографія criptografía ðuðljuuqþunnupjníu kryptografia კრიპტოგრაფიის криптография крилтографият стурtography 暗号化

Distributions of $DEC_{m,r}^2$ for CVV and PVV cases

ſ	CVV case	(m = 16, r = 3)	PVV case $(m = 16, r = 4)$	
	$\#$ values $\mathbf{V}\in\mathbb{D}^3$	$\Pr\left[\mathrm{DEC}_{16,3}^{2}(\mathrm{H})=\mathrm{V}\right]$	$\#$ values $\mathbf{V}\in\mathbb{D}^4$	$\Pr\left[\mathrm{DEC}_{16,4}^2(\mathrm{H}) = \mathrm{V}\right]$
ſ	240	$\approx 10^{-3} + 2.975 \cdot 10^{-8}$	864	$\approx 10^{-4} + 3.696 \cdot 10^{-8}$
ſ	144	$\approx 10^{-3} + 4.108 \cdot 10^{-8}$	2400	$\approx 10^{-4} + 2.091 \cdot 10^{-8}$
	216	$\approx 10^{-3} + 4.179 \cdot 10^{-8}$	1440	$\approx 10^{-4} + 3.507 \cdot 10^{-8}$
	400	$\approx 10^{-3} - 5.520 \cdot 10^{-8}$	1296	$\approx 10^{-4} + 3.707 \cdot 10^{-8}$
			4000	$\approx 10^{-4} - 4.517 \cdot 10^{-8}$

kriptografi cifrado קריפטוגרפיה mật mã học криптографія criptografia ծածկագիտություն kryptografia კრоპტოგრაფიоს криптогр

Distributions of $DEC_{m,r}^{M}$ for CVV and PVV cases

6	CVV case $(m = 16, r = 3)$		PVV case $(m = 16, r = 4)$	
44	$\#$ values $\mathbf{V}\in\mathbb{D}^3$	$\Pr\left[\mathrm{DEC}_{16,3}^{\mathrm{M}}(\mathrm{H})=\mathrm{V} ight]$	$\#$ values $V \in \mathbb{D}^4$	$\Pr\left[\mathrm{DEC}_{16,4}^{\mathrm{M}}(\mathrm{H})=\mathrm{V} ight]$
	616	$\approx 10^{-3} + 2.082 \cdot 10^{-20}$	1616	$\approx 10^{-4} + 4.545 \cdot 10^{-20}$
	384	$\approx 10^{-3} - 3.339 \cdot 10^{-20}$	8384	$\approx 10^{-4} - 8.760 \cdot 10^{-21}$

Distributions of decimalization functions

at mã học криптографія criptografía ðuðljuuqþunnupjníu kryptografia კრიპტოგრაფიის криптография крилтографият стурtography 暗号化

Distributions of $DEC_{m,r}^2$ for CVV and PVV cases

ſ	CVV case	(m = 16, r = 3)	PVV case $(m = 16, r = 4)$	
	$\#$ values $\mathbf{V}\in\mathbb{D}^3$	$\Pr\left[\mathrm{DEC}_{16,3}^{2}(\mathrm{H})=\mathrm{V}\right]$	$\#$ values $\mathbf{V}\in\mathbb{D}^4$	$\Pr\left[\mathrm{DEC}_{16,4}^2(\mathrm{H}) = \mathrm{V}\right]$
ľ	240	$\approx 10^{-3} + 2.975 \cdot 10^{-8}$	864	$\approx 10^{-4} + 3.696 \cdot 10^{-8}$
ſ	144	$\approx 10^{-3} + 4.108 \cdot 10^{-8}$	2400	$\approx 10^{-4} + 2.091 \cdot 10^{-8}$
	216	$\approx 10^{-3} + 4.179 \cdot 10^{-8}$	1440	$\approx 10^{-4} + 3.507 \cdot 10^{-8}$
	400	$\approx 10^{-3} - 5.520 \cdot 10^{-8}$	1296	$\approx 10^{-4} + 3.707 \cdot 10^{-8}$
			4000	$\approx 10^{-4} - 4.517 \cdot 10^{-8}$

kriptografi cifrado קריפטוגרפיה mật mã học криптографія criptografia ծածկազիտություն kryptografia კრоგტაფარაფითს криптогр

Distributions of $DEC_{m,r}^{M}$ for CVV and PVV cases

6	CVV case $(m = 16, r = 3)$		PVV case $(m = 16, r = 4)$		
44	$\#$ values $\mathbf{V}\in\mathbb{D}^3$	Pr	$\left[\mathrm{DEC}_{16,3}^{\mathrm{M}}(\mathrm{H})=\mathrm{V} ight]$	# values $V \in \mathbb{D}^4$	$\Pr\left[\mathrm{DEC}_{16,4}^{\mathrm{M}}(\mathrm{H})=\mathrm{V} ight]$
ų.	616	≈ 10	$0^{-3} + 2.082 \cdot 10^{-20}$	1616	$\approx 10^{-4} + 4.545 \cdot 10^{-20}$
DE	384	≈ 10	$0^{-3} - 3.339 \cdot 10^{-20}$	8384	$\approx 10^{-4} - 8.760 \cdot 10^{-21}$

Approach, models, security proofs

nptogrāfiju 암호화 crittografia dulmāl cripteagrafalochta 密码 kriptografi cifrado न्द्राधारण्य mật mã học proproprafia uðluughunnipinu kryptografia კრоპტოგრაფიის криптография крилтоүра́фηση cryptography 暗号化 kryptografia კრიპტოგრაფიის криптография крилтография с সোদাৰাস্বকান নাম্বন্য মার্ক kriptografija حرفريسي kriptografiju 암호화 crittografia dulmál cripteagrafaíochta 密码 kriptografi cifrado جرموسي ät mä hoc криптографія criptografia ծածկազիտություն kryptografia კრоპტოგრაფიის криптография крултоурафпол cryptography 暗号化 yptographie किप्टोगाफी salauksen крыптаграфія การอ่านรหัส kriptografija رمزنویسی kriptografiju 암호화 crittografia dulmál cripteagrafaíochta 密 سر فریسی kriptografija در فریسی kriptografija کر فریسی kriptografija کر فریسی kriptografija کر فریسی kriptografija کر فریسی ttografia dulmál cripteagrafaíochta 密码 kriptografi cifrado ריפטגרפה mât mã hoc криптографія criptografía budhunntænnú kryptografía лоддоодбодоов криптография крилтоурафилоп cryptography 暗号化 kryptographie किप्टोबाफी salauksen крыптаграфія การอ่านรหัส kriptografija 2) Approach, models security proofs lografi cifudo memory mit mit hoc epumorpadia ciptografia uòlµuqhuənən məy və alauksen ماريك المعارية الم مرتونيد وهم kriptogrāfiju 암호화 crittografia dulmál cripteagrafaíochta 密码 kriptografi cifrado رمز نويسي āt mā ho。крЕптураУая criptografia dudljuqhunupjnu kryptografia კრიპტთკრაფიის криптография криятоγрафијач cryptography 晴号化 vptographie किप्टोगाफी salauksen xpsurrarpaфia مترافعته kriptografija مرفريسي kriptografiju 암호화 crittografia dulmál cripteagrafaíochta 密 лоддоядоводов криптография крилтографият cryptography 暗号化 kryptographie किप्टोबाफी salauksen крыптаграфія การอ่านรหัส kriptografija kriptogrāfiju 암호화 crittografia dulmál cripteagrafaíochta 密码 kriptografi cifrado קריפטוגרפיה mật mã học криптографія criptografia uðljuughinniðinni kryptografia კრоðტოგრაფიის криптография крилтоурафион cryptography 暗号化 kryptographie किप्टोगाफी salauksen রেন্দ্রের্টার মোর্চাব্রের্বার مِنْ فَرَسِتْ (kiptografija دَمِنْ فَرَسِتْ) kiptografija دَمَنْ فَرَسْ at mā hoe криптографія criptografia δшобµшqhunnpintu kryptografia კრоპტოგრაფიის криптография крилтоγра́фηση cryptography 暗号化

iptogrāfiju 암호화 crittografia dulmāl cripteagrafalochta 密码 kriptografi cifrado קרישטוגרפיה māt mā hoc רקיעסוגרפיה uðljuuqhunnıpjnılı kryptografia კრიპტოგრაფიის криптография криптографият cryptography 暗号化 kryptografia cifrado nurrarpaфiя การอำนรหัส kriptografija حرنريس kriptogrāfiju 암호화 crittografia dulmál cripteagrafalochta 密码 kriptografi cifrado resussory

Krzysztof Pietrzak

«The modern approach to cryptography is provable security, ...» (Provable Security for Physical Cryptography, 2009)

боддодбъёдоов криптография кроятографорт cryptography 暗号化 kryptographie किण्टोबाफी salauksen крыптаграфія การอำบรหัส kriptografiji - Ivan Damgard

«We believe that the only reasonable approach is to construct cryptographic systems with the objective of being able to give security reductions for them.» (A "proof-reading" of some issues in cryptography, 2007)

«We should not settle for protocols just because we think they "look natural" and "seem to be secure".» (the same one article)

анафинфиппърний kryptografia კრიპტოგრაფიის криптография криятоγрафијоп cryptography 暗号化 kryptographic किण्टोबाफी salauksen стыптаграфія การอำบรหัส kriptografija جریویی kriptografiju 암호화 crititografia dulmál cripteagrafaiochta 密码 kriptografi cifrado суртостичен аф mã học криптография criptografia ბшафинфиппърний kryptografia კრიპტოგრაფიის криптография криятоγрафијоп cryptography 暗号化

In the real world

We need to determine specific system parameters values which guarantee system to be secure in the adversary model.

TLS 1.3 draft-ietf-tls-tls13-20 (5.5. Limits on Key Usage)

«For AES-GCM, up to $2^{24.5}$ full-size records (about 24 million) may be encrypted on a given connection while keeping a safety margin of approximately 2^{-57} for Authenticated Encryption (AE) security.»

So what do we need?

We need to provide an analysis of system parameters limits under the assumption that the underlying primitives (Magma cipher in PRP-CPA) has no weaknesses.

CVV

CVV: adversary model

at mā học криптографія criptografia ბლბկшզիտություն kryptografia კრоპტოგრაფიის криптография крилтография cryptography 暗号化 yptographie किप्टोबाफी salauksen xpsmrarpaфia אוֹק אריבויסא kriptografiju 암호화 crittografia dulmál cripteagrafaíochta 密 Adversary model: searching for the CVV value for a certain attacked card

The adversary knows the parameters of $q \leq 10^7$ cards that have been issued by the issuer using the same key CVK, i.e., q tuples $(PAN_1, ExpDate_1, SVC_1), \ldots, (PAN_q, ExpDate_q, SVC_q)$ and corresponding correct values CVV_1, \ldots, CVV_q are known; the key CVK is unknown.

Threat

The adversary finds the correct value CVV for a certain (attacked) card with known parameters (PAN, ExpDate, SVC), for which the corresponding value CVV remained unknown.

CVV

The security proof for the CVV case

at mā học криптографія criptografia ბლბկшզիտություն kryptografia კრоპტოგრაფიის криптография крилтография cryptography 暗号化 yptographie किप्टोगाफी salauksen xpsurrarpaфia กาอ่านรมัส kriptografija مرفريسي kriptografiju 암호화 crittografia dulmál cripteagrafalochta 密 Theorem

For the payment system with $DEC_{16,3}^{M}$ the adversary success probability of finding a correct value CVV for a certain attacked card does not exceed:

$$Adv_{FC}^{MAC-CPA}(t,q) \leq 10^{-3} + \frac{t+2q+2qn}{2^k} + \frac{4q^2}{2^{n-1}} + \frac{2q}{10^{17}}$$

боддодободов криптография крилтоурфолоп cryptography 暗号化 kryptographie किप्टोबाफी salauksen крыптаграфія лтатизйа kriptografija kriptogrāfiju 암호화 crittografia dulmál cripteagrafaíochta 密码 kriptografi cifrado קריפטוגרפיה mật mã học криптографія criptografia uðljuughunnipjiníu kryptografia კრიპტოგრაფიის криптография криятоγрафизи cryptography 暗号化 kryptographie किप्टोगाफी salauksen ระการอานรหัส kriptografija (جرنوسي) kriptografiju 암호화 crittografija dulmál cripteagrafalochta 密码 kriptografi cifrado (جنوبي) ật mã học криптография criptografia διυδίμυσμυπιτιρηπίι kryptografia კრοპტოგრაფიοს криптография криятоγράφηση cryptography 暗号化

Approach, models, security proofs CVV

hptogrāfiju 암호화 crittografia dulmál cripteagrafalochta 密码 kriptografi cifrado ராசுயனான mát mã hoc பாருமுற்றைகளின யலியுயுரியமாதறப்பி kryptografia து603.60%க்குமைல் முயாராதைக்காக முலார்க்றும்றைக்கு cryptography 暗号化 kryptografi கயாசுநகற்க மாகப்பதிக் kriptografija குக்கும் kriptografiju 암호화 crittografia dulmál cripteagrafalochta 密码 kriptografi cifrado ராசுயனான லி NSPK/MIR case

- E_k is «Magma» cipher, n = 256, k = 64;
- secure in the standard PRP-CPA model;
- adversary's resources correspond to the NSPK/MIR model.

For the MIR payment system with $DEC_{16,3}^{M}$ the adversary success probability of finding a correct value CVV for a certain attacked card does not exceed

$$Adv_{FC}^{MAC-CPA} \leq 10^{-3} + 10^{-4.36} + 10^{-9.69}.$$

PVV: adversary models

ât mã học криптография criptografia ბաბկազիտություն kryptografia კრიპტოგრაფიის криптография кролтоүрафијат cryptography 暗号化 yptographie किप्टोगाफी salauksen крыптаграфия การอำนรหัส kriptografija குல்லுகளிய குற்று kriptografiju 암호화 crittografia dulmál cripteagrafalochta 密

Adversary model I: searching of the correct (PIN, PVV) pair for a certain attacked card

The adversary knows the parameters of $q \leq 10^7$ cards that have been issued by the issuer using the same key PVK, i.e., q tuples (PAN₁, PVKI₁), ..., (PAN_q, PVKI_q) and corresponding correct pairs (PIN₁, PVV₁), ..., (PIN_q, PVV_q) are known; the key PVK is unknown.

kriptografi cifrado דריפצוגרפת mät mä hoc криптографія criptografia dudhuuqhunupuuli kryptografia дбоддюдб59006 криптограф Threat

The adversary finds the correct pair (PIN, PVV) for the certain (attacked) card with known parameters (PAN, PVKI), for which such a pair remained unknown.

მi mã học криптография criptografía ბლბկազիտություն kryptografia კრიპტოგრაფიის криптография крижкоγράφηση cryptography 暗号化 კოლიცსა მოპორმ ასასალი ფილიცისსა იაივითარი სიცილინეა ასასა სიცილინების კოლიცისა მიკისალის ასახალიცის კოლიცის ფი კოლიცისა მოპორმ ასასალიციალი სიცილიციალის სიცილინების კასასა სიცილიციალის გამაკარი და ასახალიციალი კასასა და მა

CTCrypt 2017

25 / 36

ptografiju 암호針 crittografia dulmál criptegrafalochta 密码 kriptografi cifrado アマロロンア mát má hoc CRYPTOPRO nátuuqhunnipinuk kryptografia 36036008509000 криптографии криптографии стурtography 暗号化 kryptografia 36036008509000 криптографии сриттографии distribution and a solution of the correct PIN value for a certain attacked card with fixed unknown PVV

The adversary knows the parameters of $q \leq 10^7$ cards that have been issued by the issuer using the same key PVK, i.e., q tuples (PAN₁, PVKI₁), ..., (PAN_q, PVKI_q) and corresponding correct pairs (PIN₁, PVV₁), ..., (PIN_q, PVV_q) are known; for a certain attacked card with known parameters (PAN, PVKI) the correct value PVV is fixed but unknown; the key PVK is also unknown.

Threat

The adversary finds the correct PIN value for the certain (attacked) card with known parameters (PAN, PVKI) and fixed unknown value PVV.



iptografiju 암호화 crittografia dulmál cripteografiaiochta 密码 kriptografi cilindo ரசாயமான mát mã hoc CRYPTOPROrafi மல்புயழியமாழாயம் kryptografia தல்தைன்னுமை நயராசாறுஷ்ஷ முராசலும்றானு cryptography 暗号化 kryptografi வாளாசாறுஷ்க ராசப்பரலிக் kriptografija பெயன் குர்ப்புகளில் கான்பில் கான்பில் Adversary model III: searching of the correct PIN value for a certain attacked card with known PVV value

The adversary knows the parameters of $q \leq 10^7$ cards that have been issued by the issuer using the same key PVK, i.e., q tuples (PAN₁, PVKI₁), ..., (PAN_q, PVKI_q) and corresponding correct pairs (PIN₁, PVV₁), ..., (PIN_q, PVV_q) are known; for a certain attacked card with known parameters (PAN, PVKI) the correct value PVV is also known; the key PVK is unknown.

kriptografi cifrado רישטערפא mật mã học криптографія criptografia duudhunuphulu kryptografia אראשטערפא spиnrorpa Threat

The adversary finds the correct PIN value for the certain (attacked) card with known parameters (PAN, PVKI) and known value PVV.

The security proof for the PVV case 1

ât mã học криптография criptografia ბաბկազիտություն kryptografia კრიპტოგრაფიის криптография крожтоүрафијат cryptografiy 暗号化 yptographie किप्टोबाफी salauksen крыптаграфия การอำบรหัส kriptografija درخر نجب kriptografija 암호화 crittografia dulmál criptegrafiachta হ kriptografi cifrado குழுமாரு மரி கில்கு முறைக்கு மர்ந்துகள் குழுமாருக்கு மர்ந்து குழுக்கு மர்கள் குறுக்குற்று www.orgpaфијал cryptography 暗号化 kryptografije किप्टोबाफी salauksen крыптаграфия การอำบรหัส kriptografia தில் kriptografiju 암호화 மருதுகள் குறுகள் குறு மர்கள் கில்கு மர்ந்துகள் குறுகள்கு வில்கு மர்து கில்கு குறுகள் குறுகள்கள் மருதுகள் குறுகள் குறுகள் கில்கு குறுகள் கில்கு கில்கு குறுகள் குறுகள் குறுகள் குறுகள் மருதுகள் கில்கள் கில்கள் கில்கள் கில்கள் கில்கள் குறுகள் குறுகள் குறுகள் குறுகள் மர்கள் கில்கள் கில்கள் கில்கள் கில்கள் கில்கள் கில்கள் கில்கள் குறுகள் குறுகள் கில்கள் கில்கள் மருதுகள் கில்கள் மருதுகள் கில்கள் க

Theorem

For a payment system with $DEC_{16,3}^{M}$ the adversary success probability of finding a correct pair (PIN, PVV) for a certain attacked card does not exceed

$$Adv_{F^{P}}^{MAC-CPA}(t,q) \leqslant 10^{-4} + \frac{t+2q+qn}{2^{k}} + \frac{q^{2}}{2^{n-1}} + \frac{2.3q}{10^{16}}$$

องอัดกลุดงฐองบ кринтография криятоүрафион cryptograpny 朝今16 клурtograpnie เคาะстилия satauksen крынтаграфия การอานรหส رمز نزید uoluuqhunnipintu kryptografia dolmál cripteagrafálóchta 密码 kriptografi cifrado पारण्डाण्यात्व केर криптография строgrafía uoluuqhunnipintu kryptografía კრоპტოგრაფοου криптография кроятоγράφηση cryptography 暗号化 kryptografia (arvet) satauksen имптаграфія การอานรหัส kriptografía კრоპტოგრაფοου криптография кроятоурафиран cryptography 暗号化 kryptografia cifrado сутежитет hintografía (cifrado حرار kriptografía) (cifrado repeter a cifrado cipte agrafalochta 密码 kriptografí infraore a citrado ciptografía (cifrado حرار در زید) it mã hoc криптография criptografía buoluuqhunnipintu kryptografía კრοპტოგრაფοου криптография кроятоурафира cryptography 暗号化

Approach, models, security proofs PVV

- E_k is «Magma» cipher, n = 256, k = 64;
- secure in the standard PRP-CPA model;
- adversary's resources correspond to the NSPK/MIR model.

Mundummandu brostonestis should markamada enumeranadase concensionen erostonendu EEU brostonendus fatelatuk edeukse Theorem

For the MIR payment system with $DEC_{16,3}^{M}$ the adversary success probability of finding a correct pair (PIN, PVV) for a certain attacked card does not exceed

$$Adv_{FP}^{MAC-CPA} \leq 10^{-4} + 10^{-4.96} + 10^{-8.63}.$$

The security proof for the PVV case 2

For the payment system with $DEC_{16,3}^{M}$ the adversary success probability of finding a correct PIN value for a certain attacked card both with known or unknown PVV value does not exceed

$$Adv_{F^{P}}^{PR}(t,q) \leqslant \frac{t+q+2+qn}{2^{k}} + \frac{(q+2)^{2}}{2^{n-1}} + \frac{2.3(q+2)}{10^{16}} + \frac{2}{10^{4}} - \frac{1}{10^{8}}$$

Approach, models, security proofs PVV

iptogrāfiju 암호화 crittografia dulmāl cripteagrafalochta 密码 kriptogrāfi cifrado ராணமான māt mā hoc பாலார்ப்புக்கு மலியுவும்மாநாய் kryptografia தல்லத்துல்ல முயாராதைக்கும் குமராரைம்குற்ற cryptography 暗号化 kryptografia வாராதுதைக்கு வாத்பாக்க் kriptogrāfiju 암호화 crittografia dulmāl cripteagrafalochta 密码 kriptografi cifrado ராணான லாராதுதைக்கு Angelandi பிக்கு kriptografi cifrado குறையில் குறையில் குறையில் குறையில் குறையில் குறையில் குறையில லாதுதுக்கு குறுக்கு குறையில் குறைய கிறைக்கு குறையில் குற கிறுக்கு குறையில் குறை

- E_k is «Magma» cipher, n = 256, k = 64;
- secure in the standard PRP-CPA model;
- adversary's resources correspond to the NSPK/MIR model.

plmohunnamili brontoaralis shoùðonahannoli enumrarnadus causravakanan erentaaradus 信号化 brentaaradus fateðstöði eslaulgg Theorem

For the MIR payment system with $DEC_{16,3}^{M}$ the adversary success probability of finding a correct PIN value for a certain attacked card both with known and unknown PVV value does not exceed

$$\operatorname{Adv}_{\mathrm{F}^{\mathrm{PR}}}^{\mathrm{PR}} \leq 2 \cdot 10^{-4} + 10^{-4.96} + 10^{-8.63}.$$

ងปลัปนณุกายแกาสามารถาวันสังหม่องอยู่เลกส สงจอยู่เหลงจะอยู่เงอง ออกแก่งกรองแลง สงอนอยู่เจอา เรารายอยู่เลกสาม รลเลยสรัตก สายแกลรายอยู่เล การอำปรหัส kriptografi (المَوْ نَوَيَعَانَ kriptografii) 암호화 crittografia dulmál cripteagrafalochta 密码 kriptografi cifrado (المَوْ نَوَيَعَانَ المَعَانَ) หารกระจาก รลเลยสรัตก กล่า mã học криптография criptografia อันอัปแนตู่แบกบรุกามใน kryptografia 3603ტოგრაფοοს криптография кролторифио กล่า mã học криптография criptografia อันอัปแนตู่แบกบรุกามใน kryptografia 3603ტოგრაფοοს криптография кролториф เป็น อาสลามร์สา แต่คนอยู่เลา เป็นอาสลามร์สา แต่คนอยู่เลา เป็นอยู่เลา เป็นอยู่เลา เป็นอยู่เลา เป็นอาสลามร์สา เลา เป็นอยู่เล่าเป็น อาสลามร์สา แต่คนอยู่เลา เป็นอยู่เลา เป็นอยู่เลา เป็นอยู่เลา เป็นอยู่เลา เป็นอยู่เลา เป็นอาสลาม

CTCrypt 2017

31 / 36

stoeräfilin 兒友學 erittoerafia dulmål erinteaerafalochta 原母 krintoerafi eifrado 元句2027, måt må hoe Kalkobyentro pokyra Remark

For the MIR payment system with $DEC_{16,3}^2$ for CVV the provable security methods yield degenerated estimations of the adversary success probability.

Reason:

$$d_{\text{stat}}(\text{DEC}_{16,3}^2,\mathcal{U}) \gg d_{\text{stat}}(\text{DEC}_{16,3}^{\text{M}},\mathcal{U}),$$

where \mathcal{U} is the uniform distribution on \mathbb{D}^3 .

иптаграфия по مرجوعي кпрюдтаціц א جين ومربوعي кпрюдтаціц א איז спиодтаці duimai cripteagrataioema Remark

For the MIR payment system with $DEC_{16,4}^2$ for PVV the provable security methods yield degenerated estimations of the adversary success probability.

Reason:

$$d_{\text{stat}}(\text{DEC}_{16,4}^2, \mathcal{U}) \gg d_{\text{stat}}(\text{DEC}_{16,4}^M, \mathcal{U}),$$

where \mathcal{U} is the uniform distribution on \mathbb{D}^4 .

Conclusion

nptogrāfiju 암호화 crittografia dulmāl cripteagrafalochta 密码 kriptografi cifrado न्द्राधारण्य mật mã học proproprafia uðluughunnipinu kryptografia კრоპტოგრაფიის криптография крилтоүра́фηση cryptography 暗号化 kryptografia კრიპტოგრაფიის криптография крилторафия с সোদাৰাস্বকান নাম্বন্য মার্ক kriptografija حرفريسي kriptografiju 암호화 crittografia dulmál cripteagrafaíochta 密码 kriptografi cifrado جرموسي at mã học криптографія criptografia ծածկազիտություն kryptografia კრоპტოგრაფიის криптография криятоγράφηση cryptography 暗号化 yptographie किप्टोगाफी salauksen крыптаграфія การอ่านรหัส kriptografija رمزنویسی kriptografiju 암호화 crittografia dulmál cripteagrafaíochta 密 1 oPirocedures vofatgeneratingis Chronatianchu Puruntu kryptografia 2603203659900 криптография سر فریسی kriptografija در فریسی kriptografija در فریسی kriptografija در فریسی kriptografija کر فریسی ttografia dulmál cripteagrafaíochta 密码 kriptografi cifrado ריפטגרפה mât mã hoc криптографія criptografía budhuuqhunntænnú kryptografía лоддоодбодоов криптография крилтоура́флоп cryptography 暗号化 kryptographie किप्टोबाफी salauksen крыптаграфія การอ่านรหัส kriptografija uðljughugnugnafnin 大大yptografia კრიპტოგრაფიის криптография криятографияоп cryptography 暗号化 kryptographie किप्टोगाफी salauksen مستعام مريد من المان المريد kriptografija در نويسي kriptografija المرزيوسي kriptografija المرزيوس kriptografija at mã hoc pphiny padia criptografia dudhunghungannu kryptografia კრიპტოგრაფიის кринтография крилточофился cryptography 暗号化 vptographie क्रिप्टोगाफी salauksen крыптаграфія तार्डावीय क्रिप्टोगाफी (يمزنويسي kriptogrāfiju 암호화 crittografia dulmál cripteagrafaíochta 密 3), Conclusion_{chta} 密码 kriptografi cifrado ரானமான கிறக் குமாராருக்கு criptografia ծածկագիտություն kryptografia бобдолдболоов криптография крилтографотоп cryptography 暗号化 kryptographie किप्टोबाफी salauksen крыптаграфія การอ่านรหัส kriptografija kriptogrāfiju 암호화 crittografia dulmál cripteagrafaíochta 密码 kriptografi cifrado קריפטוגרפיה mật mã học криптографія criptografia uðljuughinniðinni kryptografia კრоðტოგრაფიის криптография крилтоурафион cryptography 暗号化 kryptographie किप्टोगाफी salauksen রেন্দ্রের্টার মোর্চাব্রের্বার مِنْ فَرَسِتْ (kiptografija دَمِنْ فَرَسِتْ) kiptografija دَمَنْ فَرَسْ āt mā hoc криптографія criptografia διωδίμισμιπιτριπίι kryptografia კრоპტოგრაფიის криптография крилтоγράφηση cryptography 暗号化

nptogrāfiju 암호화 crittografia dulmāl cripteagrafalochta 密码 kriptografi cifrado קריפשוגרפיה māt mā hoc אריפשוגרפיה udluuqhunnıpınılı kryptografia კრიპტოგრაფიის криптография қриятоүра́фиุกๆ cryptography 暗号化 kryptografi cifrado גע עניים גע געוויסיה אווויזרידשיאל kriptografia גע עניים kriptografiju 암호화 crittografia dulmāl cripteagrafalochta 密码 kriptografi cifrado גע עניים זו mā hoc криптография criptografia dulbuudhunumınılı kryptografia კრიპტოგრაფიის криптография коиятоуса́алог сиртодарон Main results for CVV/PVV

- It is shown that for the usage of existing $DEC_{16,3}^2$ Visa procedure provable security methods yield degenerated estimations of the adversary success probability.
- The new decimalization procedure DEC^M_{16,3} was proposed, the complete security analysis was conducted.
- The security bounds regarding the forgery threat were obtained it is shown that an adversary's advantage is not more that negligible.

องออ้ดงสูงพูดออบ หุมมมาอาจุลมุต หุมหรางๆคนดุกจก cryptography 暗号化 kryptographic เดิษยาสมาตร salauksen หุมมมาลาจลมุต การมานรหส kriptografija วงป้องสูงการของการของการของการของการของการของการของการของการของการของการของการของการของการของการของการของการของ แล้ว แล้วของการของการของการของการของการของการของการของการของการของการของการของการของการของการของการของการของการ การของการของการของการของการของการของการของการของการของการของการของการของการของการของการของการของการของการของการ การของการของการของการของการของการของการของการของการของการของการของการของการของการของการของการของการของการของการ การของการของการของการของการของการของการของการของการของการของการของการของการของการของการของการของการของการของการข

Conclusion

Overall results of the WG

- The modifications and complete security analysis were conducted for 7 groups of mechanisms of the payment system.
- For the final solutions complete results in the provable security paradigm were obtained.
- The obtained results mean that the obtained mechanisms conform to the existing set of requirements.

indings

- The set of standards and recommendations, obtained during 10 years of TC 26 was enough to build a secure set of mechanisms for a payment system.
- Strict requirements for the level of cryptanalysis and security estimations for the TC 26 document projects allowed to obtain a set of security bounds, which is sufficient to obtain end security estimations of higher-level mechanisms in an extremely short time period.

Conclusior

Overall results of the WG

- The modifications and complete security analysis were conducted for 7 groups of mechanisms of the payment system.
- For the final solutions complete results in the provable security paradigm were obtained.
- The obtained results mean that the obtained mechanisms conform to the existing set of requirements.

Findings

- The set of standards and recommendations, obtained during 10 years of TC 26 was enough to build a secure set of mechanisms for a payment system.
- Strict requirements for the level of cryptanalysis and security estimations for the TC 26 document projects allowed to obtain a set of security bounds, which is sufficient to obtain end security estimations of higher-level mechanisms in an extremely short time period.

S. V. Smyshlyaev (Crypto-Pro LLC

u 암호화 crittografia dulmál cripteagrafaíochta 密码 kriptografi cifrado קריפטוגרפיה mật mã học

Thank you for your attention!

at ma noc криптография criptografia owołjwejnim kryptografia 30000080000 криптография криятографијет сгурtograpny 🖷 t

Questions?

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

CRYPTOPRO