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

Stanislav V. Smyshlyaev,
Head of information security department,
Crypto-Pro LLC

Liliya R. Ahmetzyanova,
Evgeny K. Alekseev,
Grigory A. Karpunin

CTCrypt 2017

- 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.

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.

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

- «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»

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

- «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»

- «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»

- «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»

To obtain a set of protocols using Russian algorithms, sufficient to provide complete data protection in the payment system.

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.

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).

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

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.

CVV

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.

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.

Decimalization procedure

- $\mathbb{H} = \{0, 1, \ldots, 9, A, B, \ldots, F\}$ — hex-symbols
- $\mathbb{D} = \{0, 1, \ldots, 9\}$ — decimal symbols

The function of two-pass decimalization is the mapping of $DEC^2_{m,r} : \mathbb{H}^m \to \mathbb{D}^r$, $m \geqslant r$, 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 $DEC^2_{m,r}(X)$ 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 $DEC^2_{m,r}(X)$ is the concatenation of these s symbols and $r - s$ residues of dividing first hex-symbols of X by 10.

Example

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

Decimalization procedure: alternative

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

Example

$$\mathrm{DEC}^{\mathrm{M}}_{5,3}(0\|1\|\mathrm{C}\|\mathrm{D}\|\mathrm{E}) = \mathrm{0x1CDE} \mod 10^3 =$$
$$= 7390 \mod 10^3 = 3\|9\|0$$

CVV

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).

Procedure of generating Card Verification Value

1. $B_1 = (\mathrm{PAN}||0\ldots0)$ — 64 bits;
2. $B_2 = (\mathrm{ExpDate}||\mathrm{SVC}||0\ldots0)$ — 64 bits;
3. $C = E_{CVK}(E_{CVK}(B_1) \oplus B_2)$, where $E_{CVK}(\cdot)$ — «Magma» cipher;
4. $$\mathrm{CVV} = \begin{cases} \mathrm{DEC}^2_{16,3}(C) & \text{— as in VISA payment system;} \\ \mathrm{DEC}^M_{16,3}(C) & \text{— only for MIR payment system.} \end{cases}$$

PVV

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.

Output

PVV — PIN Verification Value (4 decimal digits).

Procedure of generating PIN Verification Value

1. $TSP = (PAN|_{11}||PVKI||PIN)$, where $PAN|_{11}$ — first 11 decimal digits of PAN.
2. $C = E_{PVK}(TSP)$, where $E_{PVK}(\cdot)$ — «Magma» cipher.
3. $$PVV = \begin{cases} DEC^{2}_{16,4}(C) & \text{— as in VISA payment system;} \\ DEC^{M}_{16,4}(C) & \text{— only for MIR payment system.} \end{cases}$$

Distributions of decimalization functions

Distributions of $\mathrm{DEC}^2_{m,r}$ for CVV and PVV cases

CVV case (m = 16, r = 3)		PVV case (m = 16, r = 4)	
# values $V \in \mathbb{D}^3$	$\Pr\left[\mathrm{DEC}^2_{16,3}(H) = V\right]$	# values $V \in \mathbb{D}^4$	$\Pr\left[\mathrm{DEC}^2_{16,4}(H) = V\right]$
240	$\approx 10^{-3} + 2.975 \cdot 10^{-8}$	864	$\approx 10^{-4} + 3.696 \cdot 10^{-8}$
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	$\approx 10^{-4} - 4.517 \cdot 10^{-8}$

Distributions of $\mathrm{DEC}^M_{m,r}$ for CVV and PVV cases

CVV case (m = 16, r = 3)		PVV case (m = 16, r = 4)	
# values $V \in \mathbb{D}^3$	$\Pr\left[\mathrm{DEC}^M_{16,3}(H) = V\right]$	# values $V \in \mathbb{D}^4$	$\Pr\left[\mathrm{DEC}^M_{16,4}(H) = V\right]$
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

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

CVV case (m = 16, r = 3)		PVV case (m = 16, r = 4)	
# values $V \in \mathbb{D}^3$	$\Pr\left[DEC^2_{16,3}(H) = V\right]$	# values $V \in \mathbb{D}^4$	$\Pr\left[DEC^2_{16,4}(H) = V\right]$
240	$\approx 10^{-3} + 2.975 \cdot 10^{-8}$	864	$\approx 10^{-4} + 3.696 \cdot 10^{-8}$
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	$\approx 10^{-4} - 4.517 \cdot 10^{-8}$

Distributions of $DEC^M_{m,r}$ for CVV and PVV cases

CVV case (m = 16, r = 3)		PVV case (m = 16, r = 4)	
# values $V \in \mathbb{D}^3$	$\Pr\left[DEC^M_{16,3}(H) = V\right]$	# values $V \in \mathbb{D}^4$	$\Pr\left[DEC^M_{16,4}(H) = V\right]$
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	$\approx 10^{-4} - 8.760 \cdot 10^{-21}$

Krzysztof Pietrzak

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

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)

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: adversary model

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 $(\mathrm{PAN}_1, \mathrm{ExpDate}_1, \mathrm{SVC}_1), \ldots, (\mathrm{PAN}_q, \mathrm{ExpDate}_q, \mathrm{SVC}_q)$ and corresponding correct values $\mathrm{CVV}_1, \ldots, \mathrm{CVV}_q$ are known; the key CVK is unknown.

Threat

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

The security proof for the CVV case

Theorem

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

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

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.

Theorem

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

$$\mathrm{Adv}^{\mathrm{MAC-CPA}}_{\mathrm{FC}} \leqslant 10^{-3} + 10^{-4.36} + 10^{-9.69}.$$

PVV: adversary models

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 $(\mathrm{PAN}_1, \mathrm{PVKI}_1), \ldots, (\mathrm{PAN}_q, \mathrm{PVKI}_q)$ and corresponding correct pairs $(\mathrm{PIN}_1, \mathrm{PVV}_1), \ldots, (\mathrm{PIN}_q, \mathrm{PVV}_q)$ are known; the key PVK is unknown.

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.

Adversary model II: searching 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 $(\mathrm{PAN}_1, \mathrm{PVKI}_1), \ldots, (\mathrm{PAN}_q, \mathrm{PVKI}_q)$ and corresponding correct pairs $(\mathrm{PIN}_1, \mathrm{PVV}_1), \ldots, (\mathrm{PIN}_q, \mathrm{PVV}_q)$ 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.

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 $(\mathrm{PAN}_1, \mathrm{PVKI}_1), \ldots, (\mathrm{PAN}_q, \mathrm{PVKI}_q)$ and corresponding correct pairs $(\mathrm{PIN}_1, \mathrm{PVV}_1), \ldots, (\mathrm{PIN}_q, \mathrm{PVV}_q)$ are known; for a certain attacked card with known parameters $(\mathrm{PAN}, \mathrm{PVKI})$ the correct value PVV is also known; the key PVK is unknown.

Threat

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

The security proof for the PVV case 1

Theorem

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

$$\mathrm{Adv}^{\mathrm{MAC-CPA}}_{\mathrm{FP}}(t, q) \leqslant 10^{-4} + \frac{t + 2q + qn}{2^k} + \frac{q^2}{2^{n-1}} + \frac{2.3q}{10^{16}}$$

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.

Theorem

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

$$\mathrm{Adv}^{\mathrm{MAC-CPA}}_{\mathrm{FP}} \leqslant 10^{-4} + 10^{-4.96} + 10^{-8.63}.$$

The security proof for the PVV case 2

Theorem

For the payment system with $\mathrm{DEC}^{\mathrm{M}}_{16,3}$ 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

$$\mathrm{Adv}^{\mathrm{PR}}_{\mathrm{FP}}(t, q) \leqslant \frac{t + q + 2 + qn}{2^k} + \frac{(q+2)^2}{2^{n-1}} + \frac{2.3(q+2)}{10^{16}} + \frac{2}{10^4} - \frac{1}{10^8}$$

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.

Theorem

For the MIR payment system with $\mathrm{DEC}^{M}_{16,3}$ 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

$$\mathrm{Adv}^{\mathrm{PR}}_{\mathrm{FP}} \leqslant 2 \cdot 10^{-4} + 10^{-4.96} + 10^{-8.63}.$$

Remark

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

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

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

Remark

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

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

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

1 Procedures of generating CVV and PVV

2 Approach, models, security proofs
- CVV
- PVV

3 Conclusion

Main results for CVV/PVV

- It is shown that for the usage of existing $\mathrm{DEC}^2_{16,3}$ Visa procedure provable security methods yield degenerated estimations of the adversary success probability.
- The new decimalization procedure $\mathrm{DEC}^{\mathrm{M}}_{16,3}$ 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.

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.

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.

Thank you for your attention!

Questions?

Questions, comments:

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