Стандартизированные решения по использованию российских криптоалгоритмов в платежных системах: вопросы безопасности

Алексеев Е.К., к.ф.-м.н., эксперт ТК26
Елистратов А.А., эксперт ТК26

РусКрипто'2018

- Технический комитет по стандартизации «Криптографическая защита информации» (ТК 26).
- Подкомитет 3 (ПК 3 ТК 26) «Криптографические алгоритмы и механизмы в национальной платежной системе Российской Федерации».
- Работы проводятся с 2016 года.

Основная цель

Определить порядок использования российских криптографических алгоритмов во всех сегментах платежной системы с учетом действующих требований ФСБ России по криптографической защите.

Сформировать набор протокольных решений на российских криптоалгоритмах, в полной мере обеспечивающий защиту информации в платежной системе.

Требование наличия в системе стандартизации всех конструктивных блоков

- Использует широкий спектр базовых и сопутствующих криптографических алгоритмов.
- До 2016 года при определении планов разработки документов в ТК 26 платежные системы не рассматривались как одна из областей применения.
- Перечень действующих алгоритмов и протоколов создавался без прицела на платежные системы.

Переход в разумные сроки с допустимой надежностью

- Невозможность вносить радикальные изменения в протоколы, приводящие ко внешним изменениям в структуре протокола.
- Необходимость в отношении аппаратных компонент использовать уже существующие разработки (пример: реализации ГОСТ 28147-89 в чипах).

Необходимость обеспечить высокий уровень безопасности

- Существующей системе протоколов EMV более 20 лет.
- Необходимо учитывать отличия российских стандартов.
- Необходимо соответствовать действующей системе требований ФСБ России.
- Теоретические уязвимости рано или поздно приводят к практическим (пример: POODLE, BEAST, Lucky13).
- Возможности организовывать многолетний поиск уязвимостей (пример: Стрибог) нет.

Переход в разумные сроки с допустимой надежностью

- Невозможность вносить радикальные изменения в протоколы, приводящие ко внешним изменениям в структуре протокола.
- Необходимость в отношении аппаратных компонент использовать уже существующие разработки (пример: реализации ГОСТ 28147-89 в чипах).

Необходимость обеспечить высокий уровень безопасности

- Существующей системе протоколов EMV более 20 лет.
- Необходимо учитывать отличия российских стандартов.
- Необходимо соответствовать действующей системе требований ФСБ России.
- Теоретические уязвимости рано или поздно приводят к практическим (пример: POODLE, BEAST, Lucky13).
- Возможности организовывать многолетний поиск уязвимостей (пример: Стрибог) нет.

Цель: получить набор обоснований в парадигме доказуемой стойкости.

Требования к проведению обоснований

- Анализ стойкости в моделях нарушителя, релевантных для практики использования разрабатываемых протоколов — консультации с НСПК (И.М. Голдовский).
- Модификация порядка использования криптоалгоритмов в механизмах платежных систем в целях получения набора механизмов, для которых получены обоснования в терминах доказуемой стойкости.
- Выбор параметров механизмов для соответствия итоговых нижних оценок стойкости действующим требованиям к СКЗИ.

- Создание спецификаций: «СПБ».
- Криптографический анализ (7 из 8 документов): «КриптоПро».
- Формирование проектов документов для передачи на экспертизу: «ИнфоТеКС».

- «Использование функции диверсификации для формирования производных ключей платежного приложения»
- «Использование алгоритмов согласования ключа и блочного шифрования при офлайновой проверке PIN»
- «Использование режима имитозащиты алгоритма блочного шифрования при формировании прикладных криптограмм в платежных системах»

- Создание спецификаций: «СПБ».
- Криптографический анализ (7 из 8 документов): «КриптоПро».
- Формирование проектов документов для передачи на экспертизу: «ИнфоТеКС».

- «Использование функции диверсификации для формирования производных ключей платежного приложения»
- «Использование алгоритмов согласования ключа и блочного шифрования при офлайновой проверке PIN»
- «Использование режима имитозащиты алгоритма блочного шифрования при формировании прикладных криптограмм в платежных системах»

- «Использование алгоритмов блочного шифрования при формировании проверочного параметра платежной карты и проверочного значения PIN»
- «Использование режимов алгоритма блочного шифрования и имитозащиты в защищенном обмене сообщениями (ЗОС) между эмитентом и платежным приложением»
- «Задание параметров алгоритмов электронной подписи и функции хэширования в профиле сертификатов открытых ключей платежных систем»
- «Использование режимов алгоритма блочного шифрования, алгоритмов электронной подписи и функции хэширования в процедуре офлайновой аутентификации платежного приложения»

Традиционный подход

Описание криптосистемы → криптоанализ → уязвимость → модификация → описание новой версии криптосистемы → криптоанализ → уязвимость → модификация → ...

Недостатки

- В итоге имеем: на момент проведения анализа криптосистему не смогли взломать те, кто проводил анализ.
- Методов криптоанализа очень много: статистический, теоретико-кодовый, алгебраический и т.д. и т.п. ⇒ нужно очень много разноплановых специалистов.
- В больших системах возможные незамеченные уязвимости накапливаются.

Современный подход

Основан на доказуемой стойкости (правильнее — «доказуемой при условии стойкости примитива»).

- Krzysztof Pietrzak: «The modern approach to cryptography is provable security, ...» (Provable Security for Physical Cryptography, 2009)
- Ivan Damgard: «We should not settle for protocols just because we think they ”look natural” and ”seem to be secure”.» (A ”proof-reading” of some issues in cryptography, 2007)
- Matthew Green: «... it’s why we should be using security proofs. Not to mislead people, but to help us better allocate our very scarce resources — of smart people who can do this work...» (In defense of Provable Security, 2013)

Современный подход

Определение релевантной модели противника → описание криптосистемы → построение сведения (= получение оценки стойкости) → эксплуатация.

И что, следанные таким образом криптосистемы не могут быть взломаны?!

Могут! Из-за того, что условия эксплуатации ставят криптосистему в условия, в которых противник имеет более широкие возможности, чем заявленные в теореме о стойкости данной криптосистемы. Другая причина: обнаружена уязвимость примитива.

Современный подход

Определение релевантной модели противника → описание криптосистемы → построение сведения (= получение оценки стойкости) → эксплуатация.

И что, следанные таким образом криптосистемы не могут быть взломаны?!

Могут! Из-за того, что условия эксплуатации ставят криптосистему в условия, в которых противник имеет более широкие возможности, чем заявленные в теореме о стойкости данной криптосистемы. Другая причина: обнаружена уязвимость примитива.

Современный подход

Определение релевантной модели противника → описание криптосистемы → построение сведения (= получение оценки стойкости) → эксплуатация.

И что, следанные таким образом криптосистемы не могут быть взломаны?!

Могут! Из-за того, что условия эксплуатации ставят криптосистему в условия, в которых противник имеет более широкие возможности, чем заявленные в теореме о стойкости данной криптосистемы. Другая причина: обнаружена уязвимость примитива.

Доказуемая стойкость

Определение релевантной модели противника → описание криптосистемы → построение сведения (= получение оценки стойкости) → уязвимость в расширенной модели → расширение модели → модификация системы → оценка стойкости → ...

Преимущества

- Сходящийся процесс (т.к. модель строго расширяется)
- Экономия ресурсов: получить оценку стойкости (= построить сведение) можно силами малого числа специалистов
- Вера в стойкость остается только на уровне примитивов (блочный шифр, эллиптическая кривая)

Доказуемая стойкость

Определение релевантной модели противника → описание криптосистемы → построение сведения (= получение оценки стойкости) → уязвимость в расширенной модели → расширение модели → модификация системы → оценка стойкости → ...

Преимущества

- Сходящийся процесс (т.к. модель строго расширяется)
- Экономия ресурсов: получить оценку стойкости (= построить сведение) можно силами малого числа специалистов
- Вера в стойкость остается только на уровне примитивов (блочный шифр, эллиптическая кривая)

Есть нюансы

- Повышенные требования к примитивам (не сложность восстановления ключа, а сложность отличения блочного шифра от случайной перестановки) $\Rightarrow$ усложняется процесс разработки и анализа примитивов
- Неочевидные требования к высокоуровневым системам (например, неотличимость в том или ином смысле) $\Rightarrow$ сложнее объяснить некриптографам, что это и зачем

На практике: практически-ориентированная доказуемая стойкость

Удается получить конкретные значения, позволяющие оценить стойкост в конкретных условиях эксплуатации (количество обрабатываемых данных, длительность сеанса и т.п.).

TLS 1.3 draft-ietf-tls-tls13-27

«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.»

Исторические примеры

- Известно, что режим шифрования CBC не является стойким при предсказуемом IV $\Rightarrow$ атака BEAST на порядок использования CBC в протоколе TLS 1.0;
- Известно, что CBC не является стойким при больших объемах данных $\Rightarrow$ атака Sweet32 на режим CBC в протоколе TLS.
- Режим EAX доказуемо стойкий. При стандартизации в ANSI решили оптимизировать и получили EAX'(EAX-Prime), не получив для него оценки стойкости $\Rightarrow$ атака Иваты и коллег.

Основная сложность подхода

Необходимо выбрать релевантную модель противника, состоящую из

- Угрозы (определяет свойства безопасности исследуемой системы)
- Атаки (определяет возможности противника по атаке системы)
- Вычислительные ресурсы (определяет вычислительные мощности противника)

Модель должна учитывать возможности противника в реальных системах.

Основная сложность подхода

Необходимо выбрать релевантную модель противника, состоящую из

- Угрозы (определяет свойства безопасности исследуемой системы)
- Атаки (определяет возможности противника по атаке системы)
- Вычислительные ресурсы (определяет вычислительные мощности противника)

Модель должна учитывать возможности противника в реальных системах.

Примеры расширения моделей

- Кравчик в 2001 году доказал стойкость протокола TLS 1.2(«The Order of Encryption and Authentication for Protecting Communications»), однако в работах Водэнея («Password Interception in a SSL/TLS Channel») и Патерсона («Lucky Thirteen: Breaking the TLS and DTLS Record Protocols.») были приведены атаки по временному каналу, который не учитывался в модели Кравчика.
- В 2004 году Беллар и др. доказали стойкость протокола SSH BPP («Breaking and Provably Repairing the SSH Authenticated Encryption Scheme: A Case Study of the Encode-then-Encrypt-and-MAC Paradigm»). В 2009 году Патерсон и др. («Plaintext Recovery Attacks against SSH») осуществили атаку по побочному временному каналу на протокол SSH, используя возможность подавать сообщение на вход по частям, которая не учитывалась в модели Беллара.

Примеры расширения моделей

- Кравчик в 2001 году доказал стойкость протокола TLS 1.2(«The Order of Encryption and Authentication for Protecting Communications»), однако в работах Водэнея («Password Interception in a SSL/TLS Channel») и Патерсона («Lucky Thirteen: Breaking the TLS and DTLS Record Protocols.») были приведены атаки по временному каналу, который не учитывался в модели Кравчика.

- В 2004 году Беллар и др. доказали стойкость протокола SSH BPP («Breaking and Provably Repairing the SSH Authenticated Encryption Scheme: A Case Study of the Encode-then-Encrypt-and-MAC Paradigm»). В 2009 году Патерсон и др. («Plaintext Recovery Attacks against SSH») осуществили атаку по побочному временному каналу на протокол SSH, используя возможность подавать сообщение на вход по частям, которая не учитывалась в модели Беллара.

Все механизмы, описанные в созданных документах, анализировались с точки зрения доказуемой стойкости, если это вообще имело смысл.

Для части механизмов оценки получились тривиальным образом за счет того, что эти механизмы опирались на ранее стандартизированные ТК26 схемы, уже проанализированных с точки зрения доказуемой стойкости.

Некоторые механизмы потребовалось существенно менять. Наиболее яркий пример: механизмы выработки проверочных значений CVV, PVV и PIN-кода. В них неестественная западная конструкция, для которой не позволяла получить удовлетворительные оценки, была заменена на существенно более эффективную и стойкую.

Результаты

- Проведены переработка и обоснование стойкости для 7 групп механизмов платежных систем.
- Для выработанных решений получены законченные результаты в парадигме доказуемой стойкости.
- Применение полученных результатов позволяет сделать вывод о соответствии действующим требованиям.

Промежуточные выводы

- Строгие требования к проектам документов в ТК 26 по обоснованиям позволили получить базу оценок стойкости алгоритмов, благодаря которой проведение криптоанализа каждого из механизмов платежной системы оказалось возможным в сжатые сроки.

Результаты

- Проведены переработка и обоснование стойкости для 7 групп механизмов платежных систем.
- Для выработанных решений получены законченные результаты в парадигме доказуемой стойкости.
- Применение полученных результатов позволяет сделать вывод о соответствии действующим требованиям.

Промежуточные выводы

- Строгие требования к проектам документов в ТК 26 по обоснованиям позволили получить базу оценок стойкости алгоритмов, благодаря которой проведение криптоанализа каждого из механизмов платежной системы оказалось возможным в сжатые сроки.

CRYPTOPRO

Спасибо за внимание!

Вопросы?

- Материалы, вопросы, комментарии:
  - alekseev@cryptopro.ru
  - elistratov_aa@tc26.ru

«Использование алгоритмов согласования ключа и блочного шифрования при офлайновой проверке PIN»

Протокол

Терминал: ввод PIN

Терминал $\xleftarrow{\text{ICC Unpredictable Number(ICCUN)}\in V_{64},\ \text{Cert}_Y}$ Карта

Терминал: generate x, UKM, K = VKO(x, Y, UKM)

Терминал $\xrightarrow{xP,\ E_K^{CBC}(\text{ICCUN}||\text{PIN}-\text{block})}$ Карта

Карта блокируется после некоторого числа неудачных проверок PIN-кода (подряд/всего).

Угроза

Противник (возможно, с помощью собственного терминала) убеждает карту в том, что он знает PIN.

«Использование алгоритмов согласования ключа и блочного шифрования при офлайновой проверке PIN»

Протокол

Терминал: ввод PIN

Терминал $\xleftarrow{\text{ICC Unpredictable Number(ICCUN)}\in V_{64},\ \text{Cert}_Y}$ Карта

Терминал: generate x, UKM, K = VKO(x, Y, UKM)

Терминал $\xrightarrow{xP,\ E_K^{CBC}(\text{ICCUN}||\text{PIN}-\text{block})}$ Карта

Карта блокируется после некоторого числа неудачных проверок PIN-кода (подряд/всего).

Угроза

Противник (возможно, с помощью собственного терминала) убеждает карту в том, что он знает PIN.

В EMV предполагается шифрование с открытым ключом с помощью RSA. В РФ нет базового алгоритма, определяющего криптосистему с открытым ключом.

Решение

По аналогии с CMS в соответствии с Рекомендациями ТК 26:

- VKO на долговременном ключе карты и эфемерном ключе терминала;
- шифрование с помощью ГОСТ 28147-89.

ГОСТ 28147-89 используется в режиме CBC — режим шифрования, выбранный с учетом атак, учитывающих формат открытого текста, в отсутствие имитовставки.

В EMV предполагается шифрование с открытым ключом с помощью RSA. В РФ нет базового алгоритма, определяющего криптосистему с открытым ключом.

Решение

По аналогии с CMS в соответствии с Рекомендациями ТК 26:

- VKO на долговременном ключе карты и эфемерном ключе терминала;
- шифрование с помощью ГОСТ 28147-89.

ГОСТ 28147-89 используется в режиме CBC — режим шифрования, выбранный с учетом атак, учитывающих формат открытого текста, в отсутствие имитовставки.

Модель со случайным общим ключом

Методы, не основанные на свойствах VKO — поскольку Терминал использует эфемерный ключ, то для восстановления PIN у противника есть лишь 2 блока данных. Наилучший метод дешифрования для такого объема материала — полный перебор, который неосуществим на практике для 256-битного ключа.

Повторная пересылка

Наличие ICCUN не позволяет противнику передать для подтверждения PIN тот же блок данных, что передавался ранее честным образом. Накопление достаточного количества ”правильных” блоков невозможно при ограничениях, возникающих при использовании платежных карт.

Оценки стойкости VKO относительно атаки по открытым ключам в общем случае

Е.К. Алексеев, И.Б. Ошкин, В.О. Попов, С.В. Смышляев, «О криптографических свойствах алгоритмов, сопутствующих применению стандартов ГОСТ Р 34.11-2012 и ГОСТ Р 34.10-2012», Математические вопросы криптографии, 7:1 (2016), 5–38.

Стойкость основана на сложности решения распознавательной задачи Диффи-Хеллмана (DDH). Российские эллиптические кривые выбраны с учетом всех известных методов решения задачи DDH таким образом, что наилучший метод ее решения — ρ-метод Полларда.

Основной результат

При ограничениях, накладываемых порядком функционирования платежных систем, вероятность вскрытия PIN длины n цифр пассивным противником не превосходит:

$$10^{-n} + 10^{-9} + 10^{-43}.$$

«Использование режима имитозащиты алгоритма блочного шифрования при формировании прикладных криптограмм в платежных системах»

Формирование криптограмм для аутентификации данных, передаваемых между картой и эмитентом.

ГОСТ 28147-89 в режиме выработки имитовставки.

Режим выработки имитовставки по ГОСТ 28147-89 — это режим TCBC работы 16-раундовой версии шифра ГОСТ 28147-89. Общая оценка стойкости: P. Gazi, K. Pietrzak, S. Tessaro, Tight Bounds for Keyed Sponges and Truncated CBC, Cryptology ePrint Archive: Report 2015/053.

Дополнительная мера защиты: требование дополнения сообщений строго до 72 байт.

CRYPTOPRO

Основной результат

При ограничениях, накладываемых порядком функционирования платежных систем, вероятность успешного навязывания ложного сообщения не превосходит

$$10^{-6.3}.$$

«Использование алгоритмов блочного шифрования при формировании проверочного параметра платежной карты и проверочного значения PIN»: CVV

Входные параметры

- PAN (Personal Account Number) — номер карты (как правило, 12-16 цифр).
- ExpDate (Expiration Date) — срок действия карты (4 цифры в формате YYMM).
- SVC (Service Code) — сервисный код (3 цифры, может принимать только 6 значений: 000, 999, 200, 201, 220, 221).
- CVK — ключ для вычисления CVV (32 байта).

Выход

CVV (Card Verification Value) — проверочный параметр карты (3 цифры).

Процедура формирования проверочного параметра платежной карты CVV

1. $B_1 = (PAN||0\ldots0)$ — 64 бита;
2. $B_2 = (ExpDate||SVC||0\ldots0)$ — 64 бита;
3. $C = E_{CVK}(E_{CVK}(B_1) \oplus B_2)$, где $E_{CVK}(\cdot)$ —«Магма»;
4. $CVV = C \bmod 10^3$ — модульная децимализация.

Децимализация в зарубежных платежных системах

На Шаге 4 используется двухпроходная децимализация, разработанная компанией VISA.

Модель противника: поиск корректного значения CVV для некоторой целевой карты

известны значения параметров $q \leq 10^7$ карт, выпущенных эмитентом с помощью одного и того же ключа CVK, т.е. q наборов $(\mathrm{PAN}_1, \mathrm{ExpDate}_1, \mathrm{SVC}_1), \ldots, (\mathrm{PAN}_q, \mathrm{ExpDate}_q, \mathrm{SVC}_q)$; для этих карт известны соответствующие значения $\mathrm{CVV}_1, \ldots, \mathrm{CVV}_q$; ключ CVK не известен.

Угроза

противник находит корректное значение CVV для некоторой целевой карты с известными параметрами (PAN,ExpDate,SVC), для которой не известен соответствующий CVV.

Предположение о вычислительных ресурсах противника

$\approx 2^{128}$ операций шифрования алгоритма «Магма» в год.

В предположении стойкости шифра «Магма» в стандартной модели PRP-CPA методами доказуемой стойкости получен следующий результат.

Основной результат

Вероятность осуществления угрозы нахождения корректного значения CVV для некоторой целевой карты не превосходит

$$10^{-3} + 10^{-4.36} + 10^{-9.69}.$$

Замечание

Для двухпроходной децимализации VISA методами доказуемой стойкости не удается получить содержательную оценку.

Причина: статистическое расстояние между распределением модульной децимализации и равномерным в 10^{12} раз меньше статистического расстояния между распределением двухпроходной децимализации и равномерным.

«Использование алгоритмов блочного шифрования при формировании проверочного параметра платежной карты и проверочного значения PIN»: PVV

Входные параметры

- PAN (Personal Account Number) — номер карты (как правило, 12-16 цифр);
- PVKI — индекс ключа проверки PIN (цифра в интервале 0...6);
- PIN — 4 цифры (если PIN более 4 цифр, то 4 левые);
- PVK — ключ для вычисления PVV (32 байта).

Выход

PVV (PIN Verification Value) — проверочное значение PIN-кода (4 цифры).

Процедура формирования проверочного значения PIN-кода PVV

1. $\mathrm{TSP} = (\mathrm{PAN}|_{11}||\mathrm{PVKI}||\mathrm{PIN})$, где $\mathrm{PAN}|_{11}$ — первые 11 цифр номера карты;
2. $\mathrm{C} = \mathrm{E}_{\mathrm{PVK}}(\mathrm{TSP})$, где $\mathrm{E}_{\mathrm{PVK}}(\cdot)$ —«Магма»;
3. $\mathrm{PVV} = \mathrm{C} \bmod 10^4$ — модульная децимализация.

Децимализация в зарубежных платежных системах

На Шаге 3 используется двухпроходная децимализация, разработанная компанией VISA.

Модель противника I: поиск корректной пары (PIN, PVV) для некоторой целевой карты

известны значения параметров $q \leq 10^7$ карт, выпущенных эмитентом с помощью одного и того же ключа PVK, т.е. q наборов $(\mathrm{PAN}_1, \mathrm{PVKI}_1), \ldots, (\mathrm{PAN}_q, \mathrm{PVKI}_q)$; для этих карт известны корректные пары $(\mathrm{PIN}_1, \mathrm{PVV}_1), \ldots, (\mathrm{PIN}_q, \mathrm{PVV}_q)$; ключ PVK не известен.

Угроза

противник находит корректную пару (PIN, PVV) для некоторой целевой карты с известными параметрами (PAN, PVKI), для которой такая корректная пара не известна.

Предположение о вычислительных ресурсах противника

$\approx 2^{128}$ операций шифрования «Магма» в год

Модель противника II: поиск корректного значения PIN для некоторой целевой карты при известном PVV

известны значения параметров нескольких $q \leq 10^7$ карт, выпущенных эмитентом с помощью одного и того же ключа PVK, т.е. q наборов $(\mathrm{PAN}_1, \mathrm{PVKI}_1), \ldots, (\mathrm{PAN}_q, \mathrm{PVKI}_q)$; для этих карт известны корректные пары $(\mathrm{PIN}_1, \mathrm{PVV}_1), \ldots, (\mathrm{PIN}_q, \mathrm{PVV}_q)$; для некоторой целевой карты с известными параметрами $(\mathrm{PAN}, \mathrm{PVKI})$ известно корректное значение PVV; ключ PVK не известен.

Угроза

противник находит корректное значение PIN для целевой карты с известными параметрами $(\mathrm{PAN}, \mathrm{PVKI})$ и известным значением PVV.

Предположение о вычислительных ресурсах противника

$\approx 2^{128}$ операций шифрования «Магма» в год

CRYPTOPRO

Модель противника III: поиск корректного значения PIN для некоторой целевой карты при неизвестном PVV

известны значения параметров нескольких $q \leq 10^7$ карт, выпущенных эмитентом с помощью одного и того же ключа PVK, т.е. q наборов $(\mathrm{PAN}_1, \mathrm{PVKI}_1), \ldots, (\mathrm{PAN}_q, \mathrm{PVKI}_q)$; для этих карт известны корректные пары $(\mathrm{PIN}_1, \mathrm{PVV}_1), \ldots, (\mathrm{PIN}_q, \mathrm{PVV}_q)$; ключ PVK не известен.

Угроза

противник находит корректное значение PIN для целевой карты с известными параметрами $(\mathrm{PAN}, \mathrm{PVKI})$ и неизвестным значением PVV.

Предположение о вычислительных ресурсах противника

$\approx 2^{128}$ операций шифрования «Магма» в год

В предположении стойкости шифра «Магма» в стандартной модели PRP-CPA методами доказуемой стойкости получен следующий результат.

Основной результат

Вероятность осуществления угрозы нахождения корректной пары (PIN, PVV) для некоторой целевой карты не превосходит

$$10^{-4} + 10^{-4.96} + 10^{-8.63}.$$

Вероятность осуществления угрозы нахождения корректного значения PIN для некоторой целевой карты как при известном, так и при неизвестном PVV не превосходит

$$2 \cdot 10^{-4} + 10^{-4.96} + 10^{-8.63}.$$

«Использование режимов алгоритма блочного шифрования и имитозащиты в защищенном обмене сообщениями (ЗОС) между эмитентом и платежным приложением»

- Обеспечение целостности ЗОС между платежным приложением карты и эмитентом.
- Обеспечение конфиденциальности ЗОС между платежным приложением карты и эмитентом.
- Шифрование значений счетчиков при передаче эмитенту.

Для обеспечения целостности — ГОСТ 28147–89 в режиме выработки имитовставки с использованием блока подстановок из ГОСТ Р 34.12–2015 («Магма»).

Для обеспечения конфиденциальности — ГОСТ Р 34.12–2015 («Магма») в режиме простой замены.

Основной результат

Вероятность успеха противника при реализации угрозы подделки в стандартной модели MAC-CPA оценивается как

$$\mathrm{Adv}^{\text{MAC-CPA}}_{\mathrm{IM}_{\Gamma\mathrm{OCT}}}(\mathcal{A}) \leq 10^{-4.95}.$$

Вероятность успешного восстановления PIN-кода по результату его зашифрования отличается от априорно имеющейся вероятности его угадывания не более, чем на величину преимущества противника в стандартной модели PRP-CPA, которая оценивается как

$$\mathrm{Adv}^{\text{PRP-CPA}}_{\mathrm{E}_{\Gamma\mathrm{OCT}}}(\mathcal{A}) \leq 2^{-138}.$$

«Использование функции диверсификации для формирования производных ключей платежного приложения»

Порождение ключей, используемых на этапе процессинга:

- $\mathrm{IMK_{AC}} \xrightarrow{\mathrm{KDF}} \mathrm{MK_{AC}} \xrightarrow{\mathrm{KDF}} \mathrm{SK_{AC}}$
- $\mathrm{IMK_{SMI}} \xrightarrow{\mathrm{KDF}} \mathrm{MK_{SMI}} \xrightarrow{\mathrm{KDF}} \mathrm{SK_{SMI}}$
- $\mathrm{IMK_{SMC}} \xrightarrow{\mathrm{KDF}} \mathrm{MK_{SMC}} \xrightarrow{\mathrm{KDF}} \mathrm{SK_{SMC}}$
- $\mathrm{IMK_{IDN}} \xrightarrow{\mathrm{KDF}} \mathrm{MK_{IDN}}$

Порождение ключей, используемых на этапе персонализации:

- $\mathrm{KMC} \xrightarrow{\mathrm{KDF}(\cdot,\mathrm{label1})} \mathrm{K_{ENC}}$
- $\mathrm{KMC} \xrightarrow{\mathrm{KDF}(\cdot,\mathrm{label2})} \mathrm{K_{DEC}}$
- $\mathrm{KMC} \xrightarrow{\mathrm{KDF}(\cdot,\mathrm{label3})} \mathrm{K_{MAC}}$

Основная функция

Применяется функция KDF_GOSTR3411_2012_256, определенная в Рекомендациях по стандартизации Р 50.1.113-2016 «Криптографические алгоритмы, сопутствующие применению алгоритмов электронной цифровой подписи и функции хэширования».

Оценки стойкости KDF в общем случае

Е.К. Алексеев, И.Б. Ошкин, В.О. Попов, С.В. Смышляев, «О криптографических свойствах алгоритмов, сопутствующих применению стандартов ГОСТ Р 34.11-2012 и ГОСТ Р 34.10-2012», Математические вопросы криптографии, 7:1 (2016), 5–38.

Использование порожденных ключей

Вырабатываемые ключи используются для решения стандартных прикладных задач обеспечения конфиденциальности и целостности.

Рассматриваемая угроза

- "Классическая" угроза вскрытия мастер-ключей слишком слабая.
- Рассматривается более сильная и универсальная угроза — угроза отличения порождаемых ключей от ключей, порожденных случайно и независимо (модель PRF).

Модульность анализа

Дополнительное преимущество — при анализе протоколов, в которых используются порожденные ключи, допустимо будет считать их порожденными случайно и независимо.

CRYPTOPRO

Основной результат

При ограничениях (T, q, u), накладываемых порядком функционирования платежных систем, стойкость используемых механизмов:

$$\mathrm{Adv}^{\mathrm{PRF}}_{\mathrm{KDF}}(T, q, u) < 10^{-40}.$$