

О неотделимости анализа функции внутренней смены ключа от анализа режима шифрования

А. Бахарев, К. Царегородцев

¹АО «НПК «Криптонит», Новосибирский государственный университет, Новосибирск, Россия

²АО «Актив-софт», МГУ им. М.В. Ломоносова, Москва, Россия

XV симпозиум «Современные тенденции в криптографии»

Содержание

- 1 Введение
- 2 Определения и обозначения
- 3 О невозможности отделения схемы шифрования от функции смены ключа
- 4 Моделирование утечки информации
- 5 Пример: анализ CTR-TWIN

Мотивация

Большинство режимов шифрования допускают зашифрование ограниченного количества блоков открытого текста на одном ключе (см. «парадокс дней рождения»):

$$\sqrt{|\text{множество открытых текстов}|}.$$

¹Kiryukhin, “AEAD-mode MXP – Beyond the Birthday Bound without Loss of Efficiency”.

²Гузаирова, “Свойства некоторых режимов шифрования при использовании TWIN-конструкции с блочным шифром «Магма»”.

³Abdalla and Bellare, “Increasing the Lifetime of a Key: A Comparative Analysis of the Security of Re-keying Techniques”.

⁴Akhmetzyanova et al., “On Internal Re-keying”.

Мотивация

Большинство режимов шифрования допускают зашифрование ограниченного количества блоков открытого текста на одном ключе (см. «парадокс дней рождения»):

$$\sqrt{|\text{множество открытых текстов}|}.$$

Для преодоления «корневой» оценки можно использовать следующие подходы:

- замена используемого блочного шифра на псевдослучайную функцию (например, режим MXP^1 , TWIN -конструкция²)
- внешнее преобразование ключа³;
- внутреннее преобразование ключа⁴.

¹Kiryukhin, “AEAD-mode MXP – Beyond the Birthday Bound without Loss of Efficiency”.

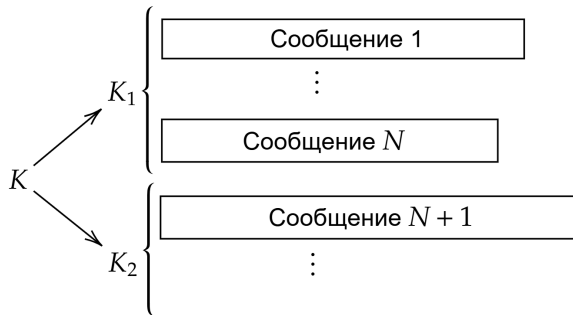
²Гузаирова, “Свойства некоторых режимов шифрования при использовании TWIN -конструкции с блочным шифром «Магма»”.

³Abdalla and Bellare, “Increasing the Lifetime of a Key: A Comparative Analysis of the Security of Re-keying Techniques”.

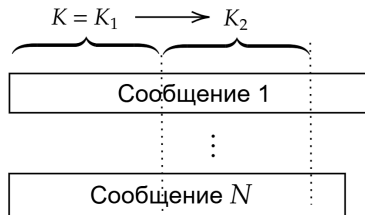
⁴Akhmetzyanova et al., “On Internal Re-keying”.

Внешняя vs внутренняя смены ключа

Внешнее преобразование



Внутреннее преобразование



Внешняя vs внутренняя смены ключа

- Внешняя смена ключа: возможен **раздельный** анализ режима шифрования и механизма внешнего преобразования ключа⁵.

⁵ Abdalla and Bellare, “Increasing the Lifetime of a Key: A Comparative Analysis of the Security of Re-keying Techniques”.

⁶ Цыпышев, *Стойкость ключевого генератора АСРКМ и режимов шифрования с внутренним обновлением ключа*.

⁷ Алексеев, “О невозможности построения универсального внутреннего преобразования ключа” 

Внешняя vs внутренняя смены ключа

- Внешняя смена ключа: возможен **раздельный** анализ режима шифрования и механизма внешнего преобразования ключа⁵.
- Внутренняя смена ключа (далее: ВСК), В.Н. Цыпышев⁶: возможен ли аналогичный результат?
- Е.К. Алексеев, Sibescrypt'25⁷: пример стойкого режима шифрования, который при встраивании в него **любой** функции ВСК становится нестойким.

⁵Abdalla and Bellare, “Increasing the Lifetime of a Key: A Comparative Analysis of the Security of Re-keying Techniques”.

⁶Цыпышев, *Стойкость ключевого генератора АСРКМ и режимов шифрования с внутренним обновлением ключа*.

⁷Алексеев, “О невозможности построения универсального внутреннего преобразования ключа” 

Внешняя vs внутренняя смены ключа

- Внешняя смена ключа: возможен **раздельный** анализ режима шифрования и механизма внешнего преобразования ключа⁵.
- Внутренняя смена ключа (далее: ВСК), В.Н. Цыпышев⁶: возможен ли аналогичный результат?
- Е.К. Алексеев, Sibescrypt'25⁷: пример стойкого режима шифрования, который при встраивании в него **любой** функции ВСК становится нестойким.
- Результат свидетельствует о **невозможности** отделения анализа функции ВСК и режима шифрования.

⁵Abdalla and Bellare, “Increasing the Lifetime of a Key: A Comparative Analysis of the Security of Re-keying Techniques”.

⁶Цыпышев, *Стойкость ключевого генератора АСРКМ и режимов шифрования с внутренним обновлением ключа*.

⁷Алексеев, “О невозможности построения универсального внутреннего преобразования ключа” 

Постановка задачи

- Анализ функции ВСК невозможен в отрыве от режима шифрования.
- Допустим ли такой анализ: проанализировать режим шифрования с идеальной функцией ВСК (случайный оракул), а затем подставить вместо идеальной функции ВСК какую-либо «реальную» функцию (зашифрование констант, хэш-функция, детерминированный экстрактор энтропии, ...)?

⁸Алексеев, “О невозможности построения универсального внутреннего преобразования ключа” 

Постановка задачи

- Анализ функции ВСК невозможен в отрыве от режима шифрования.
- Допустим ли такой анализ: проанализировать режим шифрования с идеальной функцией ВСК (случайный оракул), а затем подставить вместо идеальной функции ВСК какую-либо «реальную» функцию (зашифрование констант, хэш-функция, детерминированный экстрактор энтропии, ...)?
- Контрпример `sibescrypt'25`⁸ **не запрещает** априори такую возможность, т.к. приведенный режим шифрования ломается даже с идеальной функцией ВСК.

⁸Алексеев, “О невозможности построения универсального внутреннего преобразования ключа” 

Постановка задачи

- Анализ функции ВСК невозможен в отрыве от режима шифрования.
- Допустим ли такой анализ: проанализировать режим шифрования с идеальной функцией ВСК (случайный оракул), а затем подставить вместо идеальной функции ВСК какую-либо «реальную» функцию (зашифрование констант, хэш-функция, детерминированный экстрактор энтропии, ...)?
- Контрпример `sibescrypt'25`⁸ **не запрещает** априори такую возможность, т.к. приведенный режим шифрования ломается даже с идеальной функцией ВСК.
- Если так тоже нельзя: можно ли сделать хоть что-то, чтобы упростить себе жизнь?

⁸Алексеев, “О невозможности построения универсального внутреннего преобразования ключа” 

Основные результаты работы

- Такой анализ не допустим: здесь тоже можно построить контрпример; строится стандартным образом⁹.
- Построенный режим шифрования не детектирует смену ключа с помощью «идеальной» функции, но улавливает смену ключа с помощью любой компактно описываемой и эффективно вычислимой¹⁰ функции ВСК; когда он детектировал замену ключа, то принудительно ломает сам себя.

⁹Canetti, Goldreich, and Halevi, “The Random Oracle Methodology, Revisited”; Maurer, Renner, and Holenstein, “Indifferentiability, Impossibility Results on Reductions, and Applications to the Random Oracle Methodology”.

¹⁰читай: любой разумной

Основные результаты работы

- Такой анализ не допустим: здесь тоже можно построить контрпример; строится стандартным образом⁹.
- Построенный режим шифрования не детектирует смену ключа с помощью «идеальной» функции, но улавливает смену ключа с помощью любой компактно описываемой и эффективно вычислимой¹⁰ функции ВСК; когда он детектировал замену ключа, то принудительно ломает сам себя.
- Можно ли упростить жизнь? Да, можно: анализ можно свести к рассмотрению действия схемы шифрования с функцией ВСК к одной секции (но при этом необходимо сузить определение до «допустимых» схем шифрования).

⁹Canetti, Goldreich, and Halevi, “The Random Oracle Methodology, Revisited”; Maurer, Renner, and Holenstein, “Indifferentiability, Impossibility Results on Reductions, and Applications to the Random Oracle Methodology”.

¹⁰читай: любой разумной

Основные результаты работы

- Такой анализ не допустим: здесь тоже можно построить контрпример; строится стандартным образом⁹.
- Построенный режим шифрования не детектирует смену ключа с помощью «идеальной» функции, но улавливает смену ключа с помощью любой компактно описываемой и эффективно вычислимой¹⁰ функции ВСК; когда он детектировал замену ключа, то принудительно ломает сам себя.
- Можно ли упростить жизнь? Да, можно: анализ можно свести к рассмотрению действия схемы шифрования с функцией ВСК к одной секции (но при этом необходимо сузить определение до «допустимых» схем шифрования).
- Для примера применили методологию к режиму шифрования **CTR-TWIN** (базовая функция ВСК из режима **АСРКМ** заменяется на **TWIN**-конструкцию).

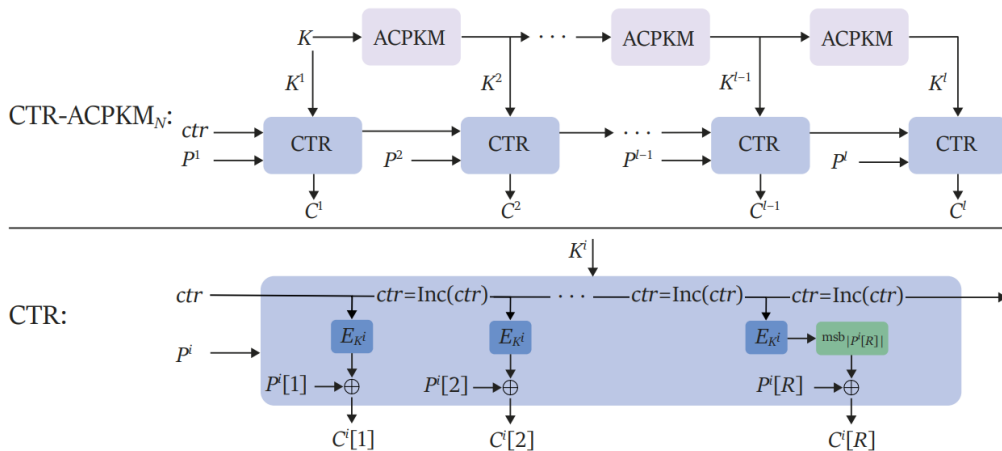
⁹Canetti, Goldreich, and Halevi, “The Random Oracle Methodology, Revisited”; Maurer, Renner, and Holenstein, “Indifferentiability, Impossibility Results on Reductions, and Applications to the Random Oracle Methodology”.

¹⁰читай: любой разумной

Содержание

- 1 Введение
- 2 Определения и обозначения
- 3 О невозможности отделения схемы шифрования от функции смены ключа
- 4 Моделирование утечки информации
- 5 Пример: анализ CTR-TWIN

Режим CTR-ACPKM¹¹



¹¹Ahmetzyanova, Alekseev, and Smyshlyaev, *Security Bound for CTR-ACPKM Internally Re-keyed Encryption Mode*.

Используемые модели безопасности

- **IND-CPNA**: базовая модель безопасности для схем шифрования, задачей противника является отличить выход схемы от случайных битов.
- **IND-CPNA'**: главное отличие от **IND-CPNA** состоит в том, что противник дополнительно в начале эксперимента получает значение производного ключа $RK(K)$; моделирует обработку одной секции схем шифрования с функцией ВСК (производный ключ не должен раскрывать много информации об исходном).
- **IND-CPNA-RO**: модель безопасности для схем шифрования с функцией ВСК, в которой функция ВСК заменяется на случайный оракул **ROM**; противнику также дается доступ к **ROM**.
- **Ext** с одним и d производными ключами: рассмотрим позднее.

Модель IND-CPNA: формально

$\text{Exp}_{\text{SE}}^{\text{IND-CPNA-}b}(\mathcal{A})$	$\mathcal{O}_{\text{enc}}^b(IV, M)$
$K \xleftarrow{\mathcal{U}} \{0,1\}^k$	if $(IV \in IVs) : \text{return } \perp$
$IVs \leftarrow \emptyset$	$CT \leftarrow \text{SE.Enc}_K^{IV}(M)$
$b' \xleftarrow{\$} \mathcal{A}^{\mathcal{O}_{\text{enc}}^b}$	if $(b = 0) : CT \xleftarrow{\mathcal{U}} \{0,1\}^{ CT }$
return b'	$IVs \leftarrow IVs \cup \{IV\}$
	return CT

$$\begin{aligned} \text{InSec}_{\text{SE}}^{\text{IND-CPNA}}(t, q, \mu, \sigma) &= \max_{\mathcal{A} \in \mathcal{A}(t, q, \mu, \sigma)} \text{Adv}_{\text{SE}}^{\text{IND-CPNA}}(\mathcal{A}) = \\ &= \max_{\mathcal{A} \in \mathcal{A}(t, q, \mu, \sigma)} \left| \mathbb{P} \left[\text{Exp}_{\text{SE}}^{\text{IND-CPNA-1}}(\mathcal{A}) \rightarrow 1 \right] - \mathbb{P} \left[\text{Exp}_{\text{SE}}^{\text{IND-CPNA-0}}(\mathcal{A}) \rightarrow 1 \right] \right|, \end{aligned}$$

t — ограничение на вычислительные ресурсы, число запросов к $\mathcal{O}_{\text{enc}}^b$ не более q , максимальная/суммарная длины запросов не превышает μ/σ блоков.

Содержание

- 1 Введение
- 2 Определения и обозначения
- 3 О невозможности отделения схемы шифрования от функции смены ключа
- 4 Моделирование утечки информации
- 5 Пример: анализ CTR-TWIN

Идеализация случайного оракула

$\text{Exp}_{\text{SE}'[\text{RK}]}^{\text{IND-CPNA-RO-}b}(\mathcal{A})$	$\mathcal{O}_{\text{enc}}^b(\text{IV}, M)$	$\mathcal{O}_{\text{ro}}(x)$
$K \xleftarrow{\mathcal{U}} \{0, 1\}^k$	if $(\text{IV} \in \text{IVs})$: return $\perp$	return $F(x)$
$F \xleftarrow{\mathcal{U}} \{f: \{0, 1\}^k \rightarrow \{0, 1\}^k\}$	$\text{CT} \xleftarrow{\$} \text{SE}'[F].\text{Enc}_K^{\text{IV}}(M)$	
$\text{IVs} \leftarrow \emptyset$	if $(b = 0)$: $\text{CT} \xleftarrow{\mathcal{U}} \{0, 1\}^{ \text{CT} }$	
$b' \xleftarrow{\$} \mathcal{A}^{\mathcal{O}_{\text{enc}}^b}$	$\text{IVs} \leftarrow \text{IVs} \cup \{\text{IV}\}$	
return b'	return CT	

$\text{InSec}_{\text{SE}'[\text{RK}]}^{\text{IND-CPNA-RO}}(t, q_{\text{ro}}, q, \mu, \sigma)$ определяется аналогично $\text{InSec}_{\text{SE}}^{\text{IND-CPNA}}(t, q, \mu, \sigma)$, кроме дополнительного ограничения q_{ro} на количество вызовов случайного оракула, идеализирующего функцию смены ключа.

Режим шифрования SE_{td}

$$\text{Encode: } (\{0, 1\}^*)^2 \rightarrow \{0, 1\}^*, \text{ Decode: } \{0, 1\}^* \rightarrow (\{0, 1\}^*)^2 \cup \{\perp\}, \\ \forall (x, y) \in (\{0, 1\}^*)^2 \quad \text{Decode}(\text{Encode}(x, y)) = (x, y).$$

Режим шифрования SE_{td}

$$\text{Encode: } (\{0, 1\}^*)^2 \rightarrow \{0, 1\}^*, \text{ Decode: } \{0, 1\}^* \rightarrow (\{0, 1\}^*)^2 \cup \{\perp\},$$
$$\forall (x, y) \in (\{0, 1\}^*)^2 \quad \text{Decode}(\text{Encode}(x, y)) = (x, y).$$

Пусть схема $SE'[RK]$ стойкая в $IND\text{-}CPNA\text{-}RO$ (например, $CTR\text{-}ACPKM$). Построим на основе SE' модифицированную схему SE_{td} следующим образом:

- Первый этап $SE_{td}.Enc$ совпадает с $CT \leftarrow SE'.Enc_K^{IV}(M)$.
- На втором этапе $SE_{td}.Enc$ запускается алгоритм-различитель $\mathcal{D}^O$, где O , вычисляет функцию RK (случайную функцию в случае $IND\text{-}CPNA\text{-}RO$).
 - ▶ Если $\mathcal{D}^O(M) = 0$, то $(CT, R) \leftarrow SE_{td}.Enc_K^{IV}(M)$, где $R \xleftarrow{\mathcal{U}} \{0, 1\}^k$.
 - ▶ Если $\mathcal{D}^O(M) = 1$, то $(CT, K) \leftarrow SE_{td}.Enc_K^{IV}(M)$.

Режим шифрования SE_{td}

$$\text{Encode: } (\{0, 1\}^*)^2 \rightarrow \{0, 1\}^*, \text{ Decode: } \{0, 1\}^* \rightarrow (\{0, 1\}^*)^2 \cup \{\perp\}, \\ \forall (x, y) \in (\{0, 1\}^*)^2 \quad \text{Decode}(\text{Encode}(x, y)) = (x, y).$$

Пусть схема $SE'[RK]$ стойкая в $IND\text{-}CPNA\text{-}RO$ (например, $CTR\text{-}ACPKM$). Построим на основе SE' модифицированную схему SE_{td} следующим образом:

- Первый этап $SE_{td}.Enc$ совпадает с $CT \leftarrow SE'.Enc_K^{IV}(M)$.
- На втором этапе $SE_{td}.Enc$ запускается алгоритм-различитель $\mathcal{D}^O$, где O , вычисляет функцию RK (случайную функцию в случае $IND\text{-}CPNA\text{-}RO$).
 - ▶ Если $\mathcal{D}^O(M) = 0$, то $(CT, R) \leftarrow SE_{td}.Enc_K^{IV}(M)$, где $R \xleftarrow{\mathcal{U}} \{0, 1\}^k$.
 - ▶ Если $\mathcal{D}^O(M) = 1$, то $(CT, K) \leftarrow SE_{td}.Enc_K^{IV}(M)$.
- $SE_{td}.Dec$ отбрасывает второй элемент пары в шифртексте и расшифровывает с помощью алгоритма $SE'.Dec$ первый элемент пары.

Компактность и эффективная вычислимость

Пусть RK задается программой $\pi_{RK} \in \{0, 1\}^*$ на универсальной машине Тьюринга и требует не более τ_{RK} шагов для вычисления ответа на любом $K \in \{0, 1\}^k$,

$$\mu_{RK} = |\text{Encode}(\pi_{RK}, 1^{\tau_{RK}})|_n.$$

Компактность и эффективная вычислимость

Пусть RK задается программой $\pi_{RK} \in \{0, 1\}^*$ на универсальной машине Тьюринга и требует не более τ_{RK} шагов для вычисления ответа на любом $K \in \{0, 1\}^k$,

$$\mu_{RK} = |\text{Encode}(\pi_{RK}, 1^{\tau_{RK}})|_n.$$

Опишем подробнее алгоритм-различитель $\mathcal{D}^O(M)$:

- M подается на вход алгоритму Decode : если декодирование возвращает $\perp$, то $\mathcal{D}^O(M) = 0$, в противном случае результат интерпретируется как пара $\text{Decode}(M) = (\pi, 1^\tau)$, где
 - ▶ π : программа для универсальной машины Тьюринга;
 - ▶ 1^τ : ограничение на количество тактов в унарной записи.

Если пара не может быть интерпретирована подобным образом, то декодирование возвращает ошибку $\perp$.

Компактность и эффективная вычислимость

Пусть RK задается программой $\pi_{RK} \in \{0, 1\}^*$ на универсальной машине Тьюринга и требует не более τ_{RK} шагов для вычисления ответа на любом $K \in \{0, 1\}^k$,

$$\mu_{RK} = |\text{Encode}(\pi_{RK}, 1^{\tau_{RK}})|_n.$$

Опишем подробнее алгоритм-различитель $\mathcal{D}^O(M)$:

- M подается на вход алгоритму **Decode**: если декодирование возвращает $\perp$, то $\mathcal{D}^O(M) = 0$, в противном случае результат интерпретируется как пара $\text{Decode}(M) = (\pi, 1^\tau)$, где
 - ▶ π : программа для универсальной машины Тьюринга;
 - ▶ 1^τ : ограничение на количество тактов в *унарной записи*.

Если пара не может быть интерпретирована подобным образом, то декодирование возвращает ошибку $\perp$.

- $\mathcal{D}$ выбирает случайный элемент $x \xleftarrow{\mathcal{U}} \{0, 1\}^k$, после чего не более чем за τ шагов получает $\text{res} \leftarrow \pi(x)$.
 - ▶ Если $\text{res} = \perp$ или $\text{res} \notin \{0, 1\}^k$, то $\mathcal{D}$ возвращает 0.
 - ▶ Если $\mathcal{O}(x) = \text{res}$, то $\mathcal{D}^O(M) = 1$, иначе 0.

Результаты анализа SE_{td}

Теорема

Зададим параметры $\mu \geq \mu_{RK} = |\text{Encode}(\pi_{RK}, 1^{\tau_{RK}})|_n$, $q \geq 1$, $p = \lceil \frac{\mu}{\ell} \rceil$. Тогда для схемы SE_{td} и $t' = t + n(\sigma + ps) \approx t$ выполняются следующие неравенства:

$$\text{InSec}_{SE_{td}[RK]}^{\text{IND-CPNA-RO}}(t, q_{ro}, q, \mu, \sigma) \leq \frac{p(q\ell)^2}{2^{n+1}} + \frac{q(q_{ro} + 1) + p - 1}{2^k} + p \cdot \text{InSec}_E^{\text{PRP}}(t', \sigma_1),$$

$$\text{InSec}_{SE_{td}}^{\text{IND-CPNA}}(t, q, \mu, \mu) \geq 1 - 2^{-n(\mu_{RK}-1)} \approx 1.$$

Вывод: если доказано, что режим «хороший» при моделировании RK как случайного оракула, то это не дает гарантий, что режим останется хорошим для конкретной функции RK .

Содержание

- 1 Введение
- 2 Определения и обозначения
- 3 О невозможности отделения схемы шифрования от функции смены ключа
- 4 Моделирование утечки информации**
- 5 Пример: анализ CTR-TWIN

В сухом остатке

- 1 Есть схемы шифрования, которые «плохим образом» взаимодействуют с функцией смены ключа.

В сухом остатке

- 1 Есть схемы шифрования, которые «плохим образом» взаимодействуют с функцией смены ключа.
- 2 Это взаимодействие может быть более или менее грубым (детектирование любой смены ключа, даже с помощью идеального случайного оракула; детектирование смены ключа только с помощью эффективно вычислимой функции).

В сухом остатке

- 1 Есть схемы шифрования, которые «плохим образом» взаимодействуют с функцией смены ключа.
- 2 Это взаимодействие может быть более или менее грубым (детектирование любой смены ключа, даже с помощью идеального случайного оракула; детектирование смены ключа только с помощью эффективно вычислимой функции).
- 3 Совместное рассмотрение схемы шифрования и встраиваемой в нее функции смены ключа до некоторой степени неизбежно.

- 1 Есть схемы шифрования, которые «плохим образом» взаимодействуют с функцией смены ключа.
- 2 Это взаимодействие может быть более или менее грубым (детектирование любой смены ключа, даже с помощью идеального случайного оракула; детектирование смены ключа только с помощью эффективно вычислимой функции).
- 3 Совместное рассмотрение схемы шифрования и встраиваемой в нее функции смены ключа до некоторой степени неизбежно.
- 4 Что в таком случае можно сделать для минимальной «модульности» доказательства? возможно ли сведение к более простым моделям?

ВСК-схема $SE'_\ell[SE, RK, RIV]$

Схема шифрования, которая строится на основе трех объектов:

- базовая схема шифрования SE ;
- функция (внутренней) смены ключа RK ;
- функция смены вектора инициализации RIV .

ВСК-схема имеет определенный вид (см. далее), не всякая схема шифрования с функцией ВСК является ВСК-схемой (по нашему определению).

ВСК-схема $SE'_\ell[SE, RK, RIV]$

$SE'.KGen()$

$K \xleftarrow{\$} SE.KGen$
return K

$SE'.Enc_K^{IV}(M)$

$(M_1, \dots, M_s) \leftarrow \text{Split}_\ell(M)$
 $K' \leftarrow K$
for $1 \leq i \leq s$
 $C_i \leftarrow SE.Enc_{K'}^{IV}(M_i)$
 $IV \leftarrow RIV(IV)$
 $K' \leftarrow RK(K')$
endfor
return $(C_1 \parallel \dots \parallel C_s)$

$SE'.Dec_K^{IV}(CT)$

$(C_1, \dots, C_s) \leftarrow \text{Split}_\ell(CT)$
 $K' \leftarrow K$
for $1 \leq i \leq s$
 $M_i \leftarrow SE.Dec_{K'}^{IV}(C_i)$
 $IV \leftarrow RIV(IV)$
 $K \leftarrow RK(K')$
endfor
return $(M_1 \parallel \dots \parallel M_s)$

- **CTR-АСРКМ**: ВСК-схема (нет «памяти» между сменами ключей, перезапускается по новой).
- Пример в Алексеев, “О невозможности построения универсального внутреннего преобразования ключа”: не ВСК-схема (есть «память» между сменами ключей).
- Пример SE_{td} : ВСК-схема; но «ломается» уже на одной секции.

Как моделируют утечку информации о ключе?

- IND-KM¹² для изучения стойкости режима CTR-CPKM.
- Модели для сильных экстракторов энтропии¹³.
- Модели, предложенные в рамках формализации атак по побочным каналам¹⁴.

¹²Ahmetzyanova, Alekseev, Oshkin, et al., “On the Properties of the CTR Encryption Mode of Magma and Kuznyechik Block Ciphers with Re-keying Method Based on CryptoPro Key Meshing”; Ahmetzyanova, Alekseev, and Smyshlyaev, *Security Bound for CTR-ACPKM Internally Re-keyed Encryption Mode*.

¹³Koenig and Maurer, “Generalized Strong Extractors and Deterministic Privacy Amplification”.

¹⁴Kalai and Reyzin, “A Survey of Leakage-Resilient Cryptography”; Micali and Reyzin, “Physically Observable Cryptography”; Standaert et al., “Leakage Resilient Cryptography in Practice”.

Модель Ext

- Модель Ext: противник не может отличить $(d + 1)$ -й ключ в цепочке ключей, формируемых с помощью функции-экстрактора F , от случайного равновероятного ключа K' ...
- даже в условиях доступа противника к «косвенной информации» об исходном и промежуточных ключах K_i , $1 \leq i \leq d$.
- Доступ к косвенной информации формализуется с помощью адаптивного доступа противника к функции утечки $\text{Leak}_{K_i}^b(\cdot)$.
- Модель IND-KM является частным случаем модели Ext.
- Модель Ext является аналогом модели LROB¹⁵.

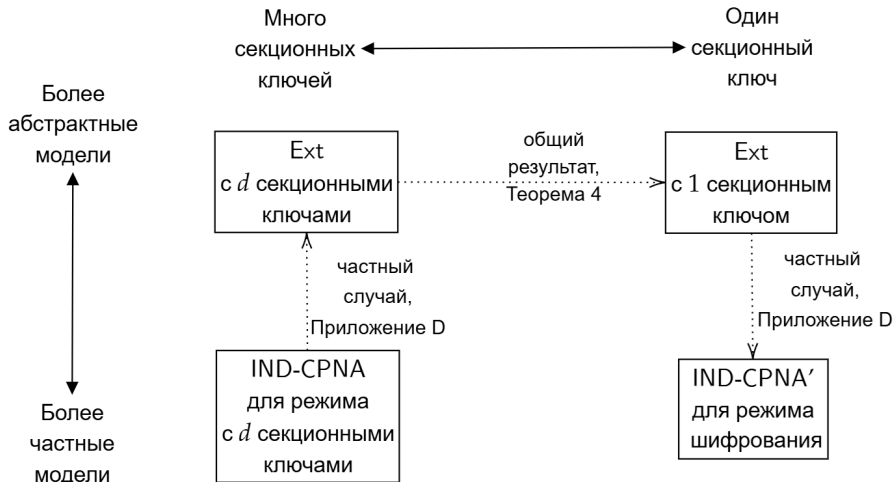
¹⁵Abdalla, Belaïd, et al., “Robust Pseudo-Random Number Generators with Input Secure Against Side-Channel Attacks”.

Модель IND-CPNA'

- Модель IND-CPNA'¹⁶: противник получает производный ключ и должен отличить «честный» оракул зашифрования от оракула, выдающего случайные биты; аналог моделей IND-KM и стандартной IND-CPNA с «дополнительной информацией» в виде ключа K' .
- Основная идея: производный ключ «похож» на случайную строку и не дает почти никакой информации противнику.
- Рассматриваем обработку только ОДНОЙ секции.

¹⁶по сути формализация идеи, изложенной в Akhmetzyanova et al., “On Internal Re-keying”

Взаимосвязь моделей в работе



Зачем так сложно?

- Более абстрактное $\Rightarrow$ понятнее, что является существенным для сведения к более простому случаю (отделение контрпримера из Алексеев, “О невозможности построения универсального внутреннего преобразования ключа” от АСРКМ и TWIN).
- Есть надежда, что с помощью более абстрактной модели Ext удастся в будущем уловить и другие атаки по побочным каналам.
- Есть надежда, что стойкость режимов типа OMAC тоже можно изложить в предложенной парадигме с помощью tweakable MAC.

Содержание

- 1 Введение
- 2 Определения и обозначения
- 3 О невозможности отделения схемы шифрования от функции смены ключа
- 4 Моделирование утечки информации
- 5 Пример: анализ CTR-TWIN

Режим CTR-TWIN

- Аналог CTR-ACPKM с заменой функции смены ключа RK на сумму значений подстановки в двух неравных точках.

$$\begin{aligned}\mathbb{K} &= \{0, 1\}^k, \mathbb{M} = \mathbb{C} = \{0, 1\}^{<n2^{n/2}}, \mathbb{IV} = \{0, 1\}^{n/2} \setminus \{1^{n/2}\}, RIV(IV) = IV, \\ RK(K) &= E_K(C_{000}) \oplus E_K(C_{001}) \parallel \dots \parallel E_K(C_{110}) \oplus E_K(C_{111}), \\ \text{Enc}_K^{IV}(X) &= \text{Dec}_K^{IV}(X) = \text{CTR}_K^{IV}(X).\end{aligned}$$

- Основная идея: сумма подстановок в разных точках больше «похожа» на случайную функцию, чем простое применение подстановки...
- А значит, ключевое множество имеет меньше предсказуемой структуры.
- Для оценки стойкости CTR-TWIN в модели IND-CPNA достаточно исследовать свойства режима при зашифровании **одной секции**, т.е. в модели IND-CPNA'.

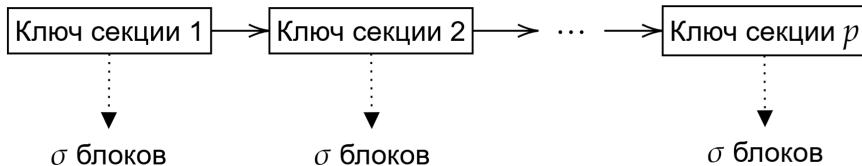
Основные шаги доказательства

- 1 Стандартный шаг: заменяем все вхождения E_K на применение случайной подстановки π .
- 2 Отделяем действие подстановки π на 8 выделенных точках $C_{b_1 b_2 b_3}$ от действия на всех остальных точках области определения: меняем π на независимую π' .
- 3 При такой замене преимущество вырастает не более чем на статистическое расстояние между распределениями; а оно мало.
- 4 Независимая π' доступна противнику только как XOR на четырех (в общем случае s) парах точек; XOR подстановки в парах точек «похож» на случайную функцию¹⁷.

¹⁷Dai, Hoang, and Tessaro, “Information-Theoretic Indistinguishability via the Chi-Squared Method”; Urivskiy, Borodin, and Rybkin, “Finding Distinguishers for Pseudorandom Number Generators Based on Permutations”; Гузаирова, “Свойства некоторых режимов шифрования при использовании TWIN-конструкции с блочным шифром «Магма»”.

Стало ли лучше?

- Для демонстрации рассмотрим равномерную нагрузку на все ключи; значение p задает число смен ключа, σ задает нагрузку на один производный ключ.

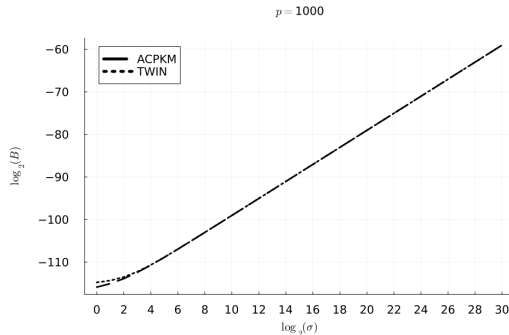
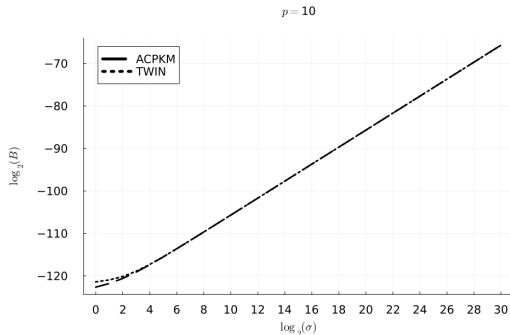


- Получаем следующие верхние оценки на преимущество в модели IND-CPNA:

$$B_{\text{АСРКМ}}(p, \sigma) \approx \frac{(p-1)(\sigma + s)^2 + \sigma^2}{2^{n+1}}, B_{\text{TWIN}} \approx p \cdot \left(\frac{\sigma^2 + 24}{2^{n+1}} + \Delta(2^{n+1}, \sigma, 2s) \right),$$

слагаемое $\Delta(\dots)$ отвечает за статистическое расстояние при замене $\pi \rightarrow \pi'$.

Стало ли лучше?



Сравнение верхних оценок для блочного шифра «Кузнечик», логарифмический масштаб осей, 10 ключей (слева) и 1000 ключей (справа).

Лучше не стало, а почему?

- Доминирует слагаемое $p\sigma^2$ из «парадокса» на одном ключе.
- Наибольшее потенциальное сжатие множества производных ключей происходит за счет **итерирования** случайного отображения, в то время как **размер базового множества** ключей играет второстепенную роль.
- С точки зрения конкретных атак¹⁸ ключи в АСПКМ имеют особенность: различные блоки ключа не могут быть равны друг другу. При итерировании функции **TWIN** также существуют особенности: так, например, никакой блок ключа не может быть равен 0^n .
- Теоретически **TWIN** может быть чуть-чуть предпочтительнее: получаемое ключевое множество больше по размеру и менее структурировано. Фактически **TWIN** чуть «тяжелее» с точки зрения вычислений, преимущества на умеренных объемах неочевидны.

¹⁸Dunkelman, Ghosh, and Lambooi, *Attacking the IETF/ISO Standard for Internal Re-keying CTR-ACPKM*; Миронкин, “О некоторых вероятностных характеристиках алгоритма выработки ключа «CRYPTOPRO KEY MESHING»”.

Заключение

- 1 Пример схемы шифрования с внутренней сменой ключа, стойкой при моделировании функции смены ключа с помощью случайного оракула, но не являющейся стойкой при замене случайного оракула на любую компактно описываемую и быстро вычисляемую функцию.
- 2 Абстрактная модель [Ext](#), позволяющая сводить изучение систем с несколькими производными ключами к системам с одним производным ключом.
- 3 Класс ВСК-схем, для которых работает доказательство в модели [Ext](#).
- 4 Пример анализа в модели для режима [CTR-TWIN](#).

СПАСИБО ЗА ВНИМАНИЕ!

`a.bakharev@g.nsu.ru`

`kirill94_12@mail.ru`

Список литературы I



Abdalla, M., S. Belaïd, et al. “Robust Pseudo-Random Number Generators with Input Secure Against Side-Channel Attacks”. In: *Applied Cryptography and Network Security (ACNS 2015)*. Vol. 9092. Lecture Notes in Computer Science. Cham: Springer International, 2015, pp. 635–654.



Abdalla, M. and M. Bellare. “Increasing the Lifetime of a Key: A Comparative Analysis of the Security of Re-keying Techniques”. In: *ASIACRYPT 2000*. Vol. 1976. Lecture Notes in Computer Science. 2000, pp. 546–559.



Ahmetzyanova, L. R., E. K. Alekseev, I. B. Oshkin, et al. “On the Properties of the CTR Encryption Mode of Magma and Kuznyechik Block Ciphers with Re-keying Method Based on CryptoPro Key Meshing”. In: *Матем. вопр. криптогр.* 8.2 (2017), pp. 39–50. DOI: 10.4213/mvk222. URL: <http://mi.mathnet.ru/mvk222>.



Ahmetzyanova, L. R., E. K. Alekseev, and S. V. Smyshlyaev. *Security Bound for CTR-ACPKM Internally Re-keyed Encryption Mode*. Cryptology ePrint Archive, Paper 2018/950. 2018. URL: <https://eprint.iacr.org/2018/950>.

Список литературы II

-  Akhmetzyanova, L. et al. “On Internal Re-keying”. In: *SSR 2020*. Vol. 12529. Lecture Notes in Computer Science. 2020, pp. 23–45.
-  Canetti, R., O. Goldreich, and S. Halevi. “The Random Oracle Methodology, Revisited”. In: *Journal of the ACM (JACM)* 51.4 (2004), pp. 557–594.
-  Dai, W., V. T. Hoang, and S. Tessaro. “Information-Theoretic Indistinguishability via the Chi-Squared Method”. In: *Advances in Cryptology – CRYPTO 2017*. Vol. 10403. Lecture Notes in Computer Science. Springer, 2017, pp. 497–523.
-  Dunkelman, O., S. Ghosh, and E. Lambooi. *Attacking the IETF/ISO Standard for Internal Re-keying CTR-ACPKM*. Cryptology ePrint Archive, Paper 2023/230. 2023. URL: <https://eprint.iacr.org/2023/230>.
-  Kalai, Y. T. and L. Reyzin. “A Survey of Leakage-Resilient Cryptography”. In: *Providing Sound Foundations for Cryptography: On the Work of Shafi Goldwasser and Silvio Micali*. 2019, pp. 727–794.
-  Kiryukhin, V. “AEAD-mode MXP – Beyond the Birthday Bound without Loss of Efficiency”. In: *CTCrypt’25*. 2025.

Список литературы III

-  Koenig, R. and U. Maurer. “Generalized Strong Extractors and Deterministic Privacy Amplification”. In: *IMA International Conference on Cryptography and Coding*. Vol. 3796. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer, 2005, pp. 322–339.
-  Maurer, U., R. Renner, and C. Holenstein. “Indifferentiability, Impossibility Results on Reductions, and Applications to the Random Oracle Methodology”. In: *Theory of Cryptography (TCC 2004)*. Vol. 2951. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer, 2004, pp. 21–39.
-  Micali, S. and L. Reyzin. “Physically Observable Cryptography”. In: *Theory of Cryptography (TCC 2004)*. Vol. 2951. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer, 2004, pp. 278–296.
-  Standaert, F.-X. et al. “Leakage Resilient Cryptography in Practice”. In: *Towards Hardware-Intrinsic Security: Foundations and Practice*. Berlin, Heidelberg: Springer, 2010, pp. 99–134.

Список литературы IV

-  Urivskiy, A., M. Borodin, and A. Rybkin. “Finding Distinguishers for Pseudorandom Number Generators Based on Permutations”. In: *Journal of Computer Virology and Hacking Techniques* 16.4 (2020), pp. 295–303.
-  Алексеев, Е. К. “О невозможности построения универсального внутреннего преобразования ключа”. In: *Sibecrypt’25*. 2025.
-  Гузаирова, Д. “Свойства некоторых режимов шифрования при использовании TWIN-конструкции с блочным шифром «Магма»”. In: *Рускрипто’22*. 2022.
-  Миронкин, В. О. “О некоторых вероятностных характеристиках алгоритма выработки ключа «CRYPTOPRO KEY MESHING»”. In: *Проблемы информационной безопасности. Компьютерные системы* 4 (2015), pp. 140–146.
-  Цыпышев, В. Стойкость ключевого генератора АСРКМ и режимов шифрования с внутренним обновлением ключа. Семинар «Математические методы криптографического анализа». 20 февраля 2023 г. 2023.