Свойства некоторых режимов шифрования при использовании TWIN-конструкции с блочным шифром «Магма»

Гузаирова Д.М.

ООО «СФБ Лаб»

Рускрипто'22

23 марта 2022

Diana.Guzairova@sfblaboratory.ru

Нагрузка на ключ

Режим шифрования позволяет обрабатывать на одном ключе **ограниченный** объем данных

Превышение этого объема приводит к атакам – нарушению конфиденциальности и/или целостности (бесключевое чтение, навязывание, получение информации об открытом тексте по зашифрованному и т.д.)

Нагрузка на ключ

Режим шифрования позволяет обрабатывать на одном ключе **ограниченный** объем данных

Превышение этого объема приводит к атакам – нарушению конфиденциальности и/или целостности (бесключевое чтение, навязывание, получение информации об открытом тексте по зашифрованному и т.д.)

Нагрузка на ключ

CTR, CBC, OFB, CFB [ГОСТ 34.13-2018]

Максимально допустимое количество блоков открытого текста, обрабатываемых на одном ключе (по парадоксу дней рождения),

$$N_{\max} \leq \sqrt{2^n \cdot \pi_{\text{enc}}} = 2^{n/2} \cdot \sqrt{\pi_{\text{enc}}},$$

π_{enc} – максимально допустимое значение вероятности эффективного применения методов криптографического анализа.

Рекомендации по стандартизации Р 1323565.1.005-2017

Допустимые объемы материала для обработки на одном ключе при использовании некоторых вариантов режимов работы блочных шифров в соответствии с ГОСТ Р 34.13-2015

Как шифровать больше на одном ключе?

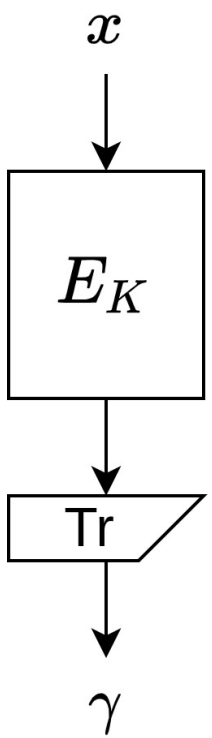
1. Конструирование специальных режимов (CTR-ACPKM и т.д.)
2. Использование псевдослучайных **функций** (PRF) вместо псевдослучайных **подстановок** (PRP)
   - Специально сконструированные PRF
   - PRF из PRP

Как шифровать больше на одном ключе?

1. Конструирование специальных режимов (CTR-ACPKM и т.д.)
2. Использование псевдослучайных **функций** (PRF) вместо псевдослучайных **подстановок** (PRP)
   - Специально сконструированные PRF
   - PRF из PRP

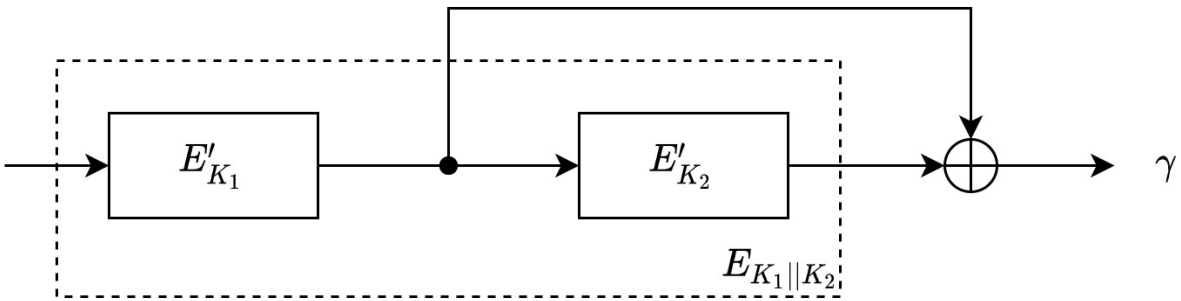
Способы построения PRF из PRP

1. Усечение выхода шифра



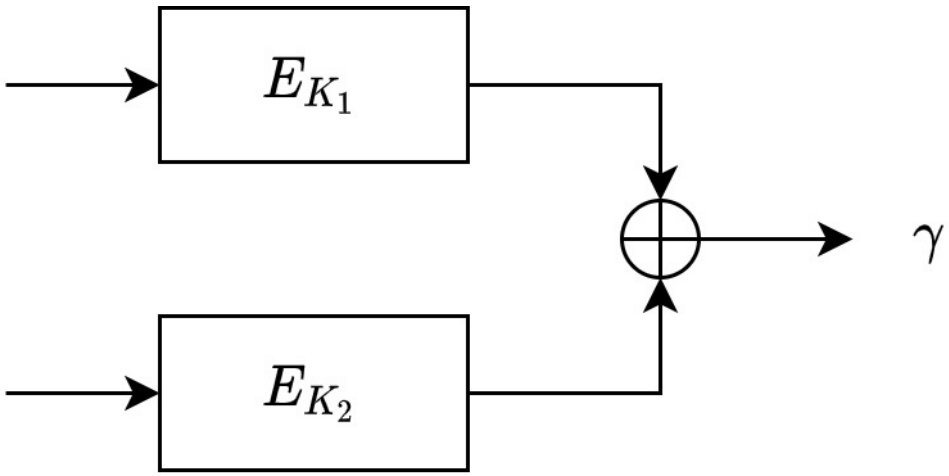
Способы построения PRF из PRP

2. «Зацепление» с внутренним состоянием шифра



Способы построения PRF из PRP

3. Суммирование выходов блочного шифра (разные ключи)



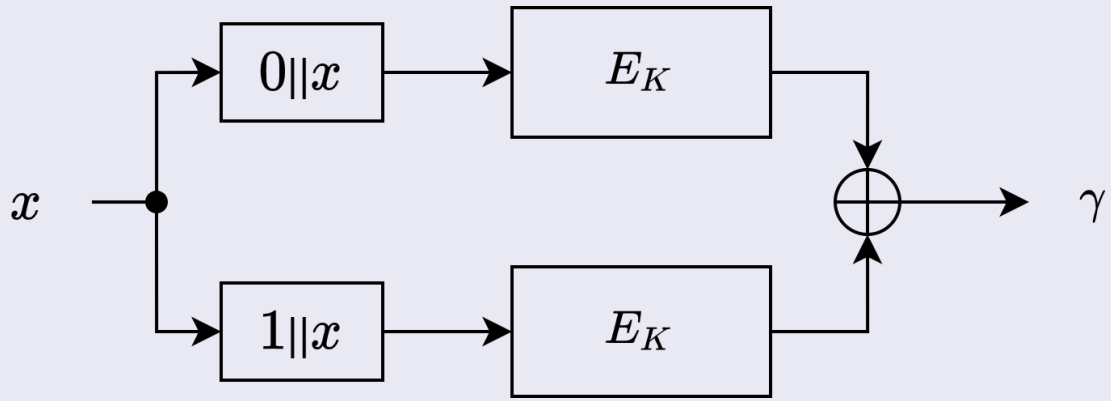
TWIN-конструкция

4. Суммирование нескольких выходов блочного шифра,

один ключ и разные блоки

$$\mathrm{TWIN} : V^{n-1} \to V^n$$

$$\mathrm{TWIN}[\mathrm{E}_K](x) = \mathrm{E}_K(0||x) \oplus \mathrm{E}_K(1||x)$$



Lucks S.

The Sum of PRPs Is a Secure PRF, EUROCRYPT 2000

TWIN-конструкция

4. Суммирование нескольких выходов блочного шифра,

один ключ и разные блоки

Достоинства

- НЕ требует изменений в блочном шифре
  - лучше, чем специально сконструированные PRF
- Параллельное выполнение
  - лучше, чем «зацепление»
- Высокая стойкость
  - лучше, чем при усечении выхода

Недостатки

- Снижение скорости работы вдвое
- Размерность входа снижается на один бит

Использование в режимах шифрования

Замена шифра E_K на TWIN[E_K] в режимах CTR и GCM порождает:

- CTR2E
- GCM2E

Режим CTR2E

Вход

– ключ $K \in V^k$

– уникальный вектор инициализации $IV \in V^{n/2-1}$ (синхропосылка)

– открытый текст (ОТ) $P = P_1 || \ldots || P_l$

Выход

– шифртекст (ШТ) $C = \gamma \oplus P = C_1 || \ldots || C_l$

Режим CTR2E

Вход

– ключ $K \in V^k$

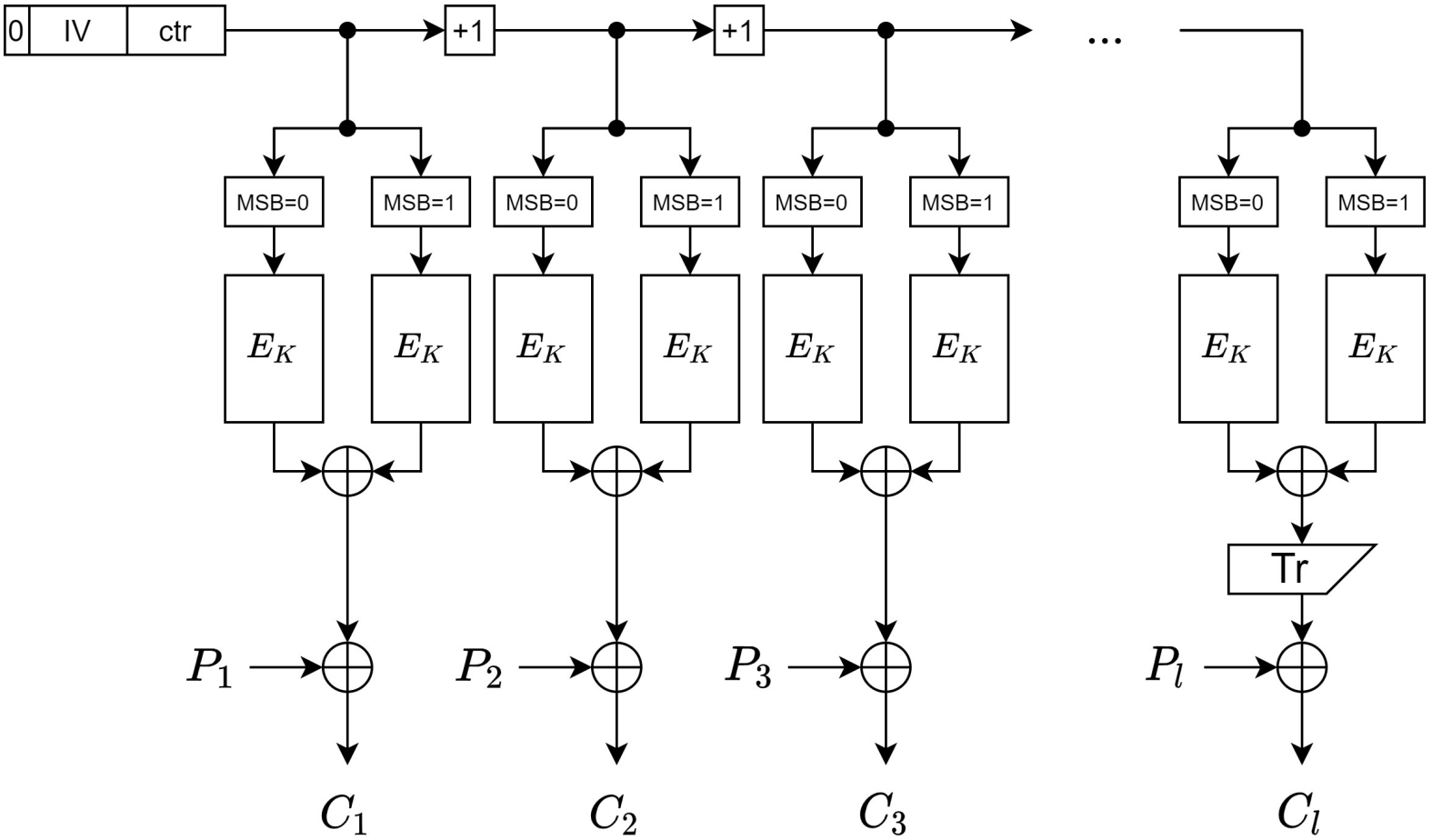
– уникальный вектор инициализации $IV \in V^{n/2-1}$ (синхропосылка)

– открытый текст (ОТ) $P = P_1 || \ldots || P_l$

Выход

– шифртекст (ШТ) $C = \gamma \oplus P = C_1 || \ldots || C_l$

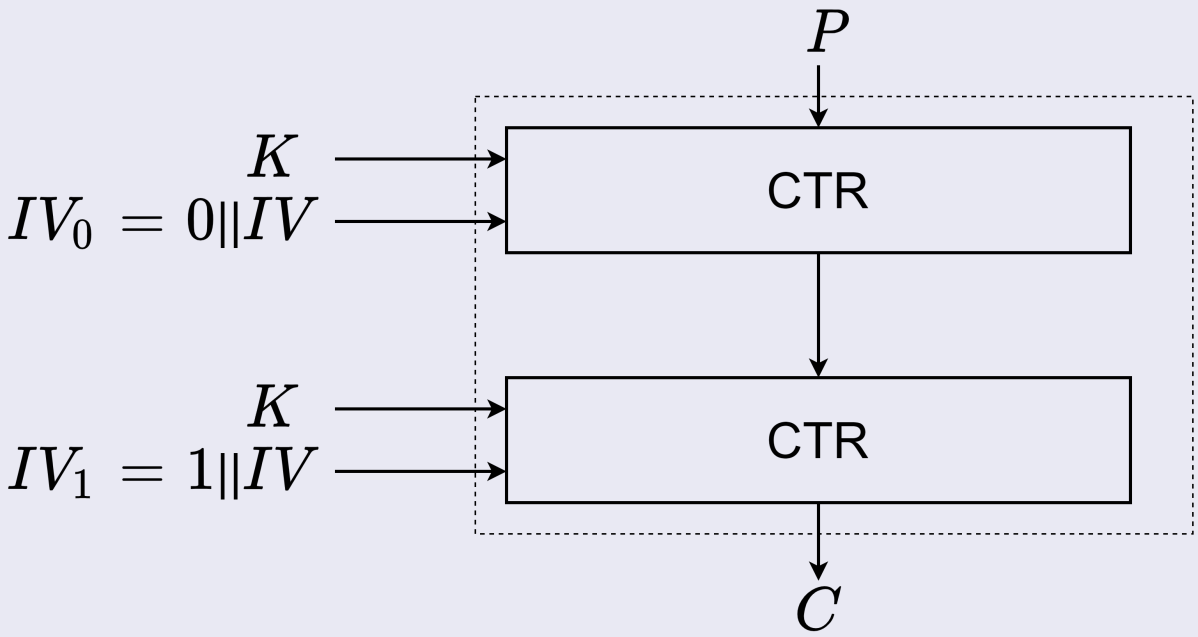
Режим CTR2E



$$\gamma_i = \mathsf{E}_K(0||IV||ctr_i) \oplus \mathsf{E}_K(1||IV||ctr_i)$$

Режим CTR2E

Режим CTR2E можно построить на основе стандартизированного режима шифрования CTR



$$C = \mathrm{CTR}_{K,IV_1}\left(\mathrm{CTR}_{K,IV_0}\left(P\right)\right), \quad IV_0 \neq IV_1$$

Режим GCM2E

Вход

– ключ $K \in V^k$

– уникальный вектор инициализации $IV \in V^{n/2-1}$

– открытый текст $P = P_1 || \ldots || P_m$

– имитозащищаемые данные $A_1 || ... || A_r$

Выход

– шифртекст (ШТ) $C = \gamma \oplus P = C_1 || \ldots || C_l$

– имитовставка T

Режим GCM2E

Вход

– ключ $K \in V^k$

– уникальный вектор инициализации $IV \in V^{n/2-1}$

– открытый текст $P = P_1 || \ldots || P_m$

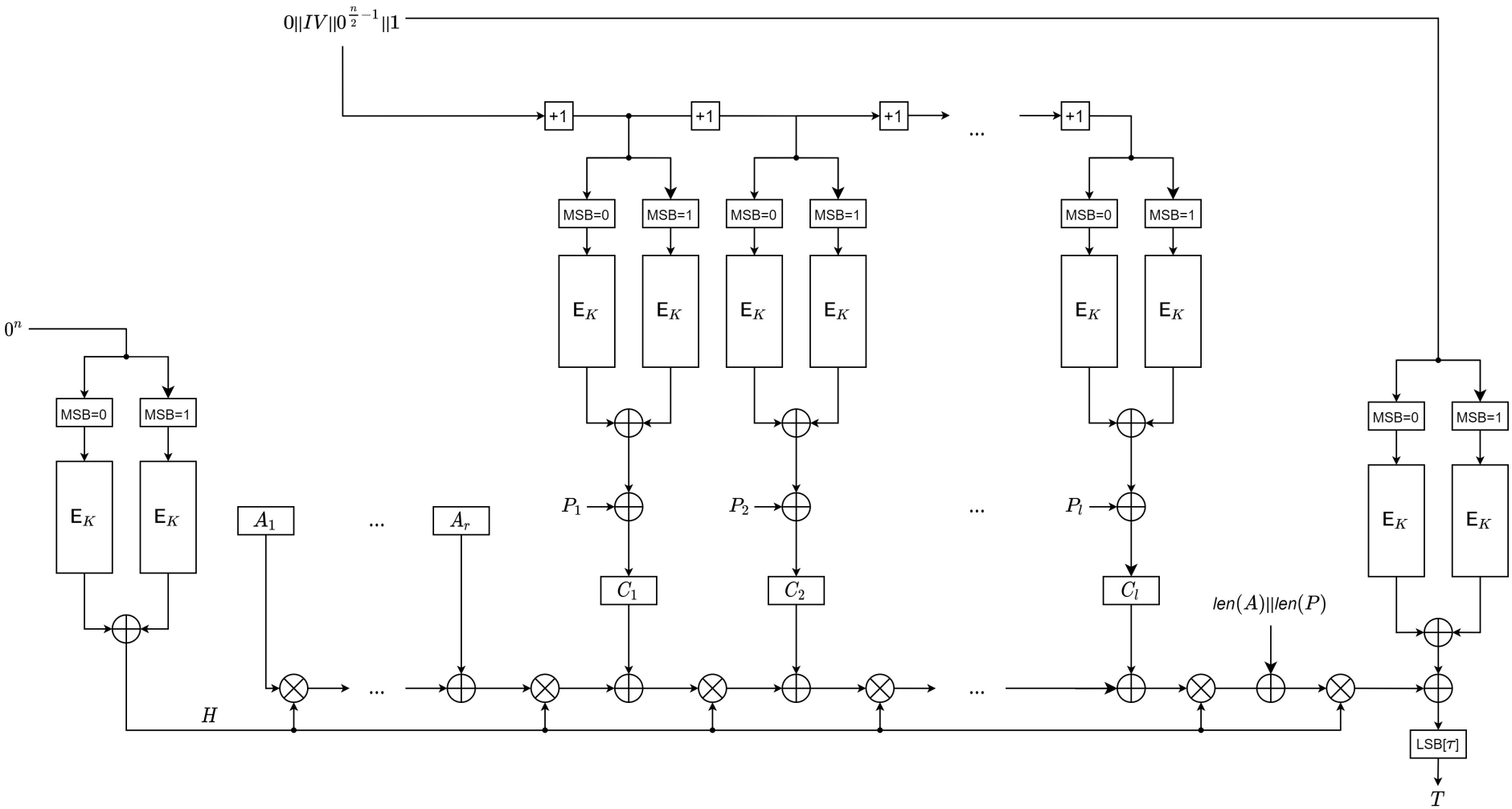
– имитозащищаемые данные $A_1 || ... || A_r$

Выход

– шифртекст (ШТ) $C = \gamma \oplus P = C_1 || \ldots || C_l$

– имитовставка T

Режим GCM2E


$0||IV||0^{\frac{n}{2}-1}||1$
+1
MSB=0
MSB=1
E_K
0^n
A_1
A_r
P_1
P_2
P_l
C_1
C_2
C_l
H
$len(A)||len(P)$
LSB[τ]
T

Обоснование стойкости

Используем математический аппарат теории ***доказуемой стойкости***:

- задаем целевое свойство безопасности
- определяем модель противника
- определяем сложную «базовую задачу»

$\Rightarrow$ выполняем редукцию (сведéние) – показываем, что нарушение целевого свойств безопасности системы в рамках заданной модели противника **невозможно** без решения базовой задачи.

Свойства безопасности

Модель priv (IND-CPNA)

Неотличимость шифртекстов от последовательности реализаций равновероятных и независимых случайных величин (абсолютно стойкого шифра) при атаке с адаптивно выбираемыми открытыми текстами и неповторяющимися синхропосылками

$$\mathrm{Adv}_{\mathsf{F}}^{\mathrm{priv}}(\mathcal{A}) = \left|\mathsf{Pr}(K \xleftarrow{R} V^k : \mathcal{A}^{\mathsf{F}(\cdot)} \Rightarrow 1) - \mathsf{Pr}(\mathcal{A}^{\$(\cdot)} \Rightarrow 1)\right|$$

Модель противника

Модель priv (IND-CPNA)

Противник $\mathcal{A}$ – произвольный алгоритм, который:

- знает ШТ к q адаптивно выбираемым ОТ (длина до l блоков)
- обладает вычислительными ресурсами – t операций

Свойства безопасности

Модель auth (SUF-CMA)

Вероятность навязывания сообщения

$$\mathrm{Adv}_{\mathsf{F}}^{\mathrm{auth}}(\mathcal{A}) = \mathsf{Pr}(K \xleftarrow{R} V^k : \mathcal{A}^{\mathsf{E}_K(\cdot),\mathsf{D}_K(\cdot)} \text{ forges})$$

Общие определения

Модель auth (SUF-CMA)

Противник $\mathcal{A}$ – произвольный алгоритм, который:

- знает ШТ и имитовставки к q адаптивно выбираемым ОТ
- выполняет ν попыток навязывания
- обладает вычислительными ресурсами – t операций

Свойства безопасности

Для режима CTR2E доказывается свойство конфиденциальности в модели priv (IND-CPNA)

Для режима GCM2E доказывается свойство конфиденциальности и целостности в модели priv (IND-CPNA) и auth (SUF-CMA) соответственно

Обоснование стойкости

Базовая задача (PRP-CPA)

Блочный шифр E со случайно выбранным секретным ключом неотличим от случайной подстановки

$$\mathrm{Adv}_{\mathsf{E}}^{PRP-CPA}(\mathcal{A}) = \Big|\Pr(K \xleftarrow{R} V^k : \mathcal{A}^{\mathsf{E}_K(\cdot)} \Rightarrow 1) - \Pr(\pi \xleftarrow{R} \mathrm{Perm}(V^n) : \mathcal{A}^{\pi(\cdot)} \Rightarrow 1)\Big|$$

Обоснование стойкости

Будем пользоваться оценкой

Оценка стойкости TWIN–конструкции

$$\mathrm{Adv}^{PRF}_{\mathrm{TWIN}[\pi]}(\sigma) \leq \frac{\sigma}{2^n} + \frac{3\sigma\sqrt{\sigma}}{2^n\sqrt{2^n}}$$

Dai W., Hoang V.T., Tessaro S.

Information-theoretic Indistinguishability via the Chi-squared Method

CRYPTO 2017

Обоснование стойкости

Оценка стойкости CTR2E

$$\mathrm{Adv}^{\mathrm{priv}}_{\mathrm{CTR2E[E]}}(q, l, t) \leq \mathrm{Adv}^{PRP}_{\mathrm{E}}(2 \cdot q \cdot l, t') + \frac{ql}{2^n} + \frac{3ql\sqrt{ql}}{2^n\sqrt{2^n}}$$

В эвристическом предположении о стойкости блочного шифра

$$\mathrm{Adv}^{\mathrm{priv}}_{\mathrm{CTR2E[E]}}(q, l, t) \lessapprox \frac{t}{2^k} + \frac{ql}{2^n} + \frac{3ql\sqrt{ql}}{2^n\sqrt{2^n}} \approx \frac{ql}{2^n}$$

Обоснование стойкости

Оценка стойкости GCM2E

$$\mathrm{Adv}^{\mathrm{priv}}_{\mathsf{GCM2E}[\mathsf{E}_K]}(t,q,\sigma) \le \mathrm{Adv}^{PRP}_{\mathsf{E}_K}\left(t', 2\cdot\sigma'\right) + f(\sigma') \approx \frac{\sigma'}{2^n}$$

$$\mathrm{Adv}^{\mathrm{auth}}_{\mathsf{GCM2E}[E_K]}(t,q,\sigma,\nu) \le \mathrm{Adv}^{PRP}_{\mathsf{E}_K}\left(t', 2\cdot\sigma''\right) + f(\sigma'') + \frac{\nu\,(l+1)}{2^\tau}$$

$$f(\sigma) = \sigma\cdot 2^{-n} + 3\sigma^{\frac{3}{2}}\cdot 2^{-\frac{3}{2}n}$$

$$\sigma' = \sigma + q + 1$$

$$\sigma'' = \sigma + q + \nu + 1$$

Результат

Максимально допустимое количество блоков ОТ $N_{\max} \leq q \cdot l$, обрабатываемых на одном ключе,

$$N_{\max} = 2^n \cdot \pi_{\mathrm{enc}} \text{ для CTR2E,}$$

$$N_{\max} = \min\left(2^n \cdot \pi_{\mathrm{enc}},\ 2^n \cdot \left(\pi_{\mathrm{mac}} - \frac{l}{2^\tau}\right)\right) \text{ для GCM2E,}$$

π_{enc} – максимально допустимое значение вероятности эффективного применения методов криптографического анализа,

π_{mac} – максимально допустимое значение вероятности однократного навязывания сообщения.

Результат

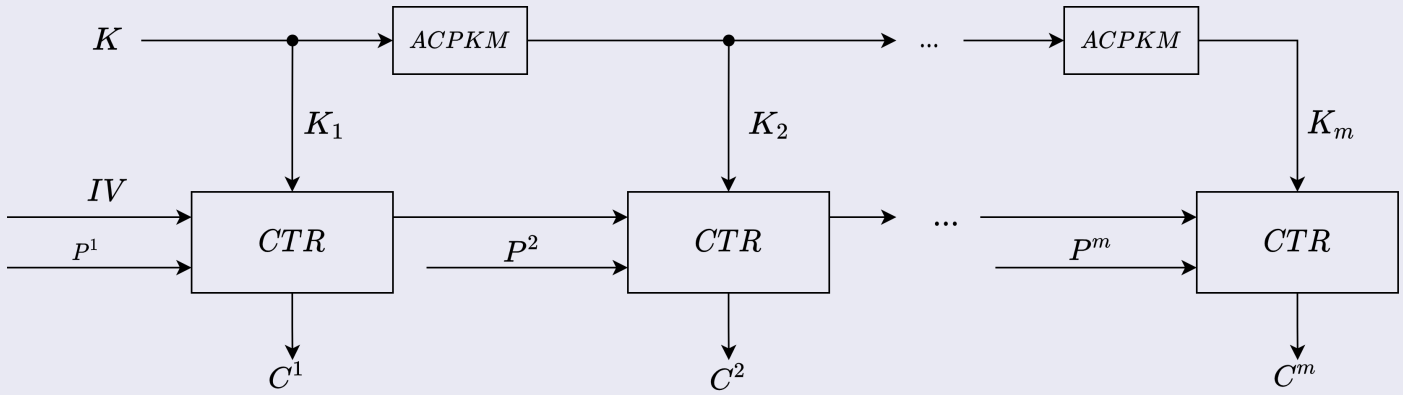
$\Rightarrow$ нагрузка на ключ НЕ зависит от парадокса ДР

$$N_{\max} = \sqrt{2^n \cdot \pi_{\text{enc}}} \text{ (CTR, CBC, OFB, CFB)}$$

$$N_{\max} = 2^n \cdot \pi_{\text{enc}} \text{ (CTR2E)}$$

Сравнение с CTR-ACPKM

Режим CTR-ACPKM



На входе

– Ключ $K \in V^k$

– Синхропосылка IV

– Открытый текст $P = P^1||P^2||...||P^m, \quad P^i = P^i_1||...||P^i_{l_i}$

На выходе

– Шифртекст $C = C^1||C^2||...||C^m, \quad C^i = C^i_1||...||C^i_{l_i}$

Рекомендации по стандартизации Р 1323565.1.017—2018

Криптографические алгоритмы, сопутствующие применению алгоритмов блочного шифрования

Сравнение с CTR-ACPKM

Оценка стойкости режима CTR-ACPKM

$$\mathrm{Adv}^{\mathrm{priv}}_{CTR-ACPKM_N}(t, \sigma = \sigma_1 + ... + \sigma_m) \leq$$

$$m \cdot \mathrm{Adv}^{PRP-CPA}_{E}(t') + \frac{(\sigma_1 + s)^2 + ... + (\sigma_{m-1} + s)^2 + (\sigma_m)^2}{2^{n+1}}$$

N – размер секции в блоках

l – длина в блоках одного сообщения

$m = \left[\frac{l}{N}\right]$ – количество секций в одном сообщении

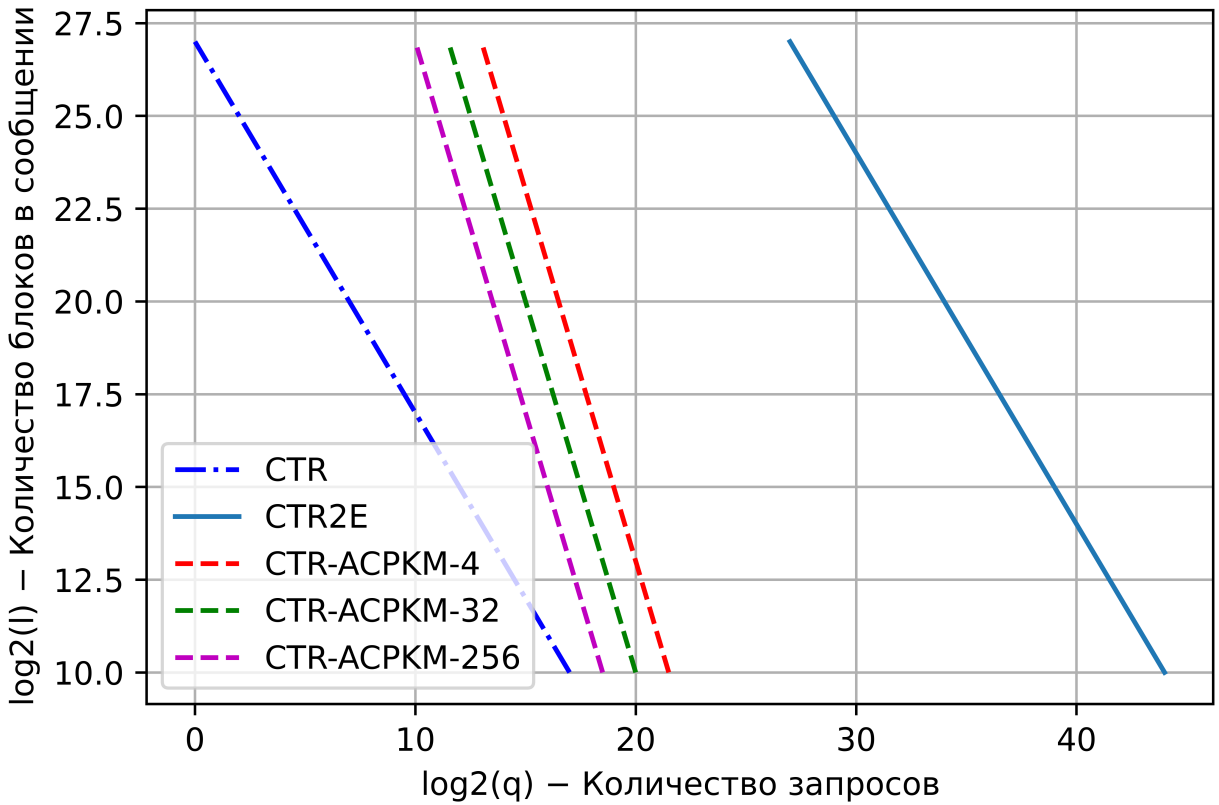
k – размерность ключа

n – размерность обрабатываемого блока, $s = \left[\frac{k}{n}\right]$

Liliya Akhmetzyanova, Evgeny Alekseev, Stanislav Smyshlyaev

Security bound for CTR-ACPKM internally re-keyed encryption mode – 2018

Сравнение с CTR-ACPKM



- Меньше секция у CTR-ACPKM – больше допустимая нагрузка на ключ
- CTR2E – за счет потери скорости допустимая нагрузка на ключ **многократно** больше

TWIN[Магма]

Дополнительное преимущество TWIN:

- не возникает более эффективных атак **на восстановление ключа**
- существующие атаки (скорее всего) становятся сложнее или перестают работать

Атаки на блочный шифр «Магма»

Блочный шифр «Магма» – ГОСТ 34.12-2018

Размер ключа $k = 256$, размер блока $n = 64$ бита

Материал (q)	Трудоемкость (t)	Метод
$\pi_{\text{enc}} \cdot 2^{32}$	$\pi_{\text{enc}} \cdot 2^{224}$	[1]
$\pi_{\text{enc}} \cdot 2^{64}$	$\pi_{\text{enc}} \cdot 2^{192}$	[2]

Таблица: Атаки на блочный шифр «Магма»

[1] Isobe T.

A Single-Key Attack on the Full GOST Block Cipher – 2012

[2] Dinur I., Dunkelman O., Shamir A.

Improved Attacks on Full GOST – 2012

Атаки на TWIN[Магма] – без усечения по числу раундов

Атака (использование свойства «точка отражения»)

$$2^{192} \cdot 2^{32} \cdot 2^{64} = 2^{290} > 2^{256}$$

Атака (использование свойства «фиксированная точка»)

$$2^{128} \cdot 2^{64} \cdot 2^{64} = 2^{256}$$

$\Rightarrow$ хуже полного перебора!

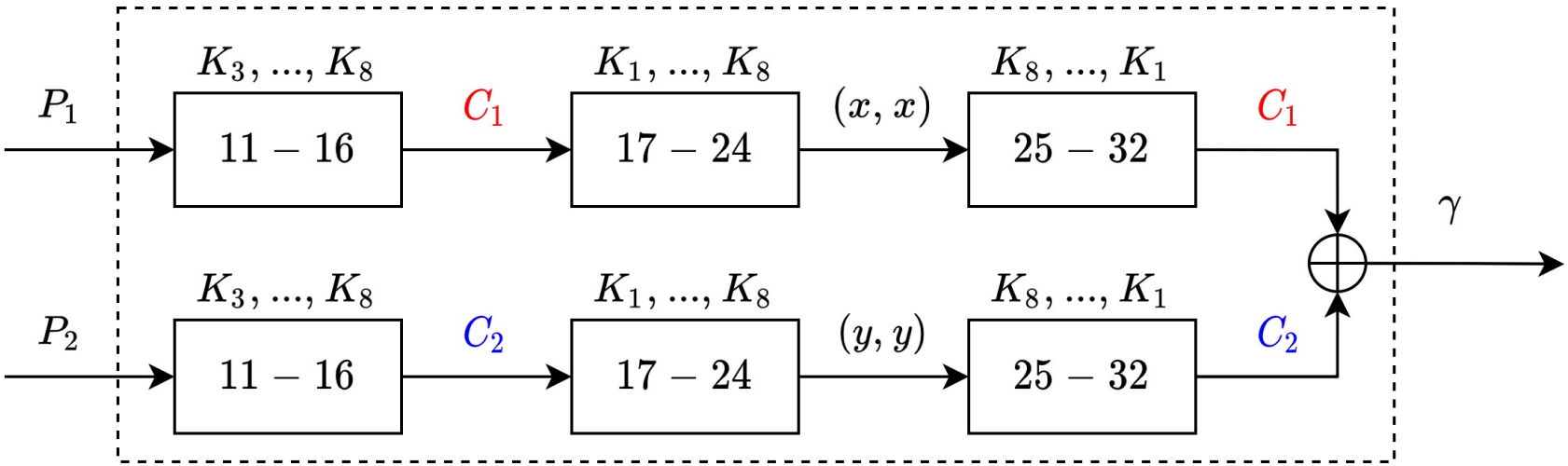
Атаки на TWIN[Магма] – 24 раунда

Рассматривались атаки на первые и последние 24 раунда, использующие:

- одну/две «точки отражения»
- одну/две «фиксированных точки»
- сдвиговые свойства
- комбинации этих свойств

НЕ удалось построить метод лучше тотального опробования!

Атака на TWIN[Магма] – 22 последних раунда



При каждой паре вход-выход надеемся на две «точки отражения»:

- опробуем C_1 и однозначно определяем C_2

$$P_1 = \mathsf{E}_{K_3,\ldots,K_8}(C_1) \text{ и } P_2 = \mathsf{E}_{K_3,\ldots,K_8}(C_2)$$

- атакуем 6 раундов (2^{96} операций) $\Rightarrow$ 2^{64} ключей $K_3, \ldots, K_8$
- опробуем (x, x) – 2^{32} операций $\Rightarrow$ вычисляем K_1, K_2
- проверяем 2^{96} ключей на двух иных парах вход-выход

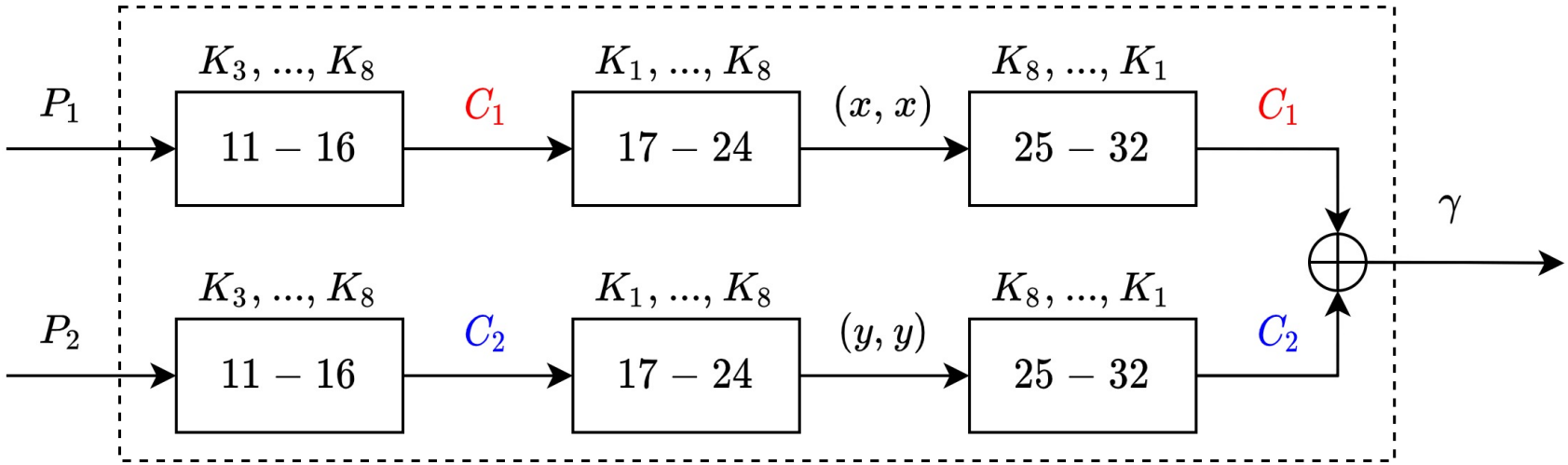
Атака на TWIN[Магма] – 22-а последних раунда

Атака – две точки отражения:

$$t = \underbrace{\pi_{\text{enc}} \cdot 2^{64}}_{\text{пары вход-выход}} \cdot \underbrace{2^{64}}_{\text{опробование } C_1} \cdot \left(\underbrace{2^{96} + 2^{96}}_{\text{атака на 6 раундов}} + \underbrace{2^{64} \cdot 2^{32}}_{\text{определение } K_1, K_2} \right)$$

$$t \approx \pi_{\text{enc}} \cdot 2^{224}$$

$$q = \pi_{\text{enc}} \cdot 2^{64} \leq 2^{63}$$



Заключение

- Способ перехода от PRP к PRF – TWIN-конструкция: $\mathrm{TWIN}(x) = \mathrm{E}_K(0|x) \oplus \mathrm{E}_K(1|x)$
- Использование TWIN в CTR и GCM $\Rightarrow$ CTR2E и GCM2E
- Для CTR2E и GCM2E получены оценки стойкости – на одном ключе можно шифровать порядка 2^n, а не $2^{n/2}$ блоков
- Существующие атаки на восстановление ключа «Магмы» неэффективны против TWIN[Магма]
  - Удалось построить метод только на 22 раунда TWIN[Магма] из 32
- Потенциально: использование TWIN с шифром, усеченным по числу раундов, позволяет обеспечить приемлемые скоростные характеристики

Заключение

- Способ перехода от PRP к PRF – TWIN-конструкция: $\mathrm{TWIN}(x) = \mathrm{E}_K(0|x) \oplus \mathrm{E}_K(1|x)$
- Использование TWIN в CTR и GCM $\Rightarrow$ CTR2E и GCM2E
- Для CTR2E и GCM2E получены оценки стойкости – на одном ключе можно шифровать порядка 2^n, а не $2^{n/2}$ блоков
- Существующие атаки на восстановление ключа «Магмы» неэффективны против TWIN[Магма]
  - Удалось построить метод только на 22 раунда TWIN[Магма] из 32
- Потенциально: использование TWIN с шифром, усеченным по числу раундов, позволяет обеспечить приемлемые скоростные характеристики

Заключение

- Способ перехода от PRP к PRF – TWIN-конструкция: $\mathrm{TWIN}(x) = \mathrm{E}_K(0|x) \oplus \mathrm{E}_K(1|x)$
- Использование TWIN в CTR и GCM $\Rightarrow$ CTR2E и GCM2E
- Для CTR2E и GCM2E получены оценки стойкости – на одном ключе можно шифровать порядка 2^n, а не $2^{n/2}$ блоков
- Существующие атаки на восстановление ключа «Магмы» неэффективны против TWIN[Магма]
  - Удалось построить метод только на 22 раунда TWIN[Магма] из 32
- Потенциально: использование TWIN с шифром, усеченным по числу раундов, позволяет обеспечить приемлемые скоростные характеристики

Заключение

- Способ перехода от PRP к PRF – TWIN-конструкция: $\mathrm{TWIN}(x) = \mathrm{E}_K(0|x) \oplus \mathrm{E}_K(1|x)$
- Использование TWIN в CTR и GCM $\Rightarrow$ CTR2E и GCM2E
- Для CTR2E и GCM2E получены оценки стойкости – на одном ключе можно шифровать порядка 2^n, а не $2^{n/2}$ блоков
- Существующие атаки на восстановление ключа «Магмы» неэффективны против TWIN[Магма]
  - Удалось построить метод только на 22 раунда TWIN[Магма] из 32
- Потенциально: использование TWIN с шифром, усеченным по числу раундов, позволяет обеспечить приемлемые скоростные характеристики

Заключение

- Способ перехода от PRP к PRF – TWIN-конструкция: $\mathrm{TWIN}(x) = \mathrm{E}_K(0|x) \oplus \mathrm{E}_K(1|x)$
- Использование TWIN в CTR и GCM $\Rightarrow$ CTR2E и GCM2E
- Для CTR2E и GCM2E получены оценки стойкости – на одном ключе можно шифровать порядка 2^n, а не $2^{n/2}$ блоков
- Существующие атаки на восстановление ключа «Магмы» неэффективны против TWIN[Магма]
  - Удалось построить метод только на 22 раунда TWIN[Магма] из 32
- Потенциально: использование TWIN с шифром, усеченным по числу раундов, позволяет обеспечить приемлемые скоростные характеристики

Благодарю за внимание!

Обоснование стойкости CTR2E

Редукция – основные шаги доказательства

Шаг 1. Сводим стойкость CTR2E к стойкости псевдослучайной функции TWIN (к неотличимости TWIN от случайной функции)

$$\mathrm{Adv}^{\mathrm{priv}}_{\mathsf{CTR2E[E]}}(q, l, t) \leq \mathrm{Adv}^{PRF}_{\mathsf{TWIN[E]}}(q, l, t')$$

Обоснование стойкости CTR2E

Редукция – основные шаги доказательства

Шаг 2. Сводим стойкость TWIN[E_K] к стойкости TWIN[π] и стойкости блочного шифра E (неравенство треугольника)

$$\mathrm{Adv}^{PRF}_{\mathsf{TWIN[E]}}(q, l, t) \leq \mathrm{Adv}^{PRF}_{\mathsf{TWIN}[\pi]}(q \cdot l) + \mathrm{Adv}^{PRP}_{\mathsf{E}}(2 \cdot q \cdot l, t')$$

Обоснование стойкости GCM2E–конфиденциальность

Редукция – основные шаги доказательства

Шаг 1. Сводим стойкость GCM2E с блочным шифром E к стойкости GCM2E с использованием случайной подстановки

$$\mathrm{Adv}^{\mathrm{priv}}_{\mathsf{GCM2E[E]}}(q, l, t) \leq \mathrm{Adv}^{PRP}_{\mathsf{E}_K}\left(2\left(q + ql + 1\right), t'\right) + \mathrm{Adv}^{\mathrm{priv}}_{\mathsf{GCM2E}[\pi]}\left(q, l, t''\right)$$

Обоснование стойкости GCM2E–конфиденциальность

Редукция – основные шаги доказательства

Шаг 2. Сводим стойкость GCM2E[π] к стойкости TWIN[π]

$$\mathrm{Adv}^{\mathrm{priv}}_{\mathsf{GCM2E}[\pi]}\left(q, l, t''\right) \leq \mathrm{Adv}^{PRF}_{\mathsf{TWIN}[\pi]}(q, l, t'')$$

Обоснование стойкости GCM2E–конфиденциальность

$$\mathrm{Adv}^{\mathrm{priv}}_{\mathsf{GCM2E[E]}}(q, l, t) \leq \mathrm{Adv}^{PRP}_{\mathsf{E}_K}\left(2\sigma', t'\right) + \frac{\sigma'}{2^n} + \frac{3\sigma'\sqrt{\sigma'}}{2^n\sqrt{2^n}} \quad \sigma' = \sigma + q + 1$$

Обоснование стойкости GCM2E–целостность

Редукция – основные шаги доказательства

Шаг 1. Сводим стойкость GCM2E с блочным шифром к стойкости GCM2E с использованием случайной подстановки

$$\mathrm{Adv}^{\mathrm{auth}}_{\mathsf{GCM2E[E]}}\left(t,q,\sigma,\nu\right) \leq \mathrm{Adv}^{PRP}_{\mathsf{E}_K}\left(\sigma',t'\right) + \mathrm{Adv}^{\mathrm{auth}}_{\mathsf{GCM2E}[\pi]}\left(t',q,\sigma,\nu\right)$$

Обоснование стойкости GCM2E–целостность

Редукция – основные шаги доказательства

Шаг 2. Сводим стойкость GCM2E[π] к стойкости TWIN[π] и к сумме вероятностей коллизий в точке

$$\mathrm{Adv}^{\mathrm{auth}}_{\mathsf{GCM2E}[\pi]}\left(q, l, t''\right) \leq \mathrm{Adv}^{\mathit{PRF}}_{\mathsf{TWIN}[\pi]}(q, l, t'') + \frac{\nu\left(r + l + 1\right)}{2^{\tau}}$$