Ранее на РусКрипто. . .

Выводы доклада «Эффект плацебо в криптографии»:

Текущий уровень развития «доказуемой стойкости» в общем случае не позволяет делать обоснованные выводы о стойкости криптографического механизма лишь по значению величины Adv

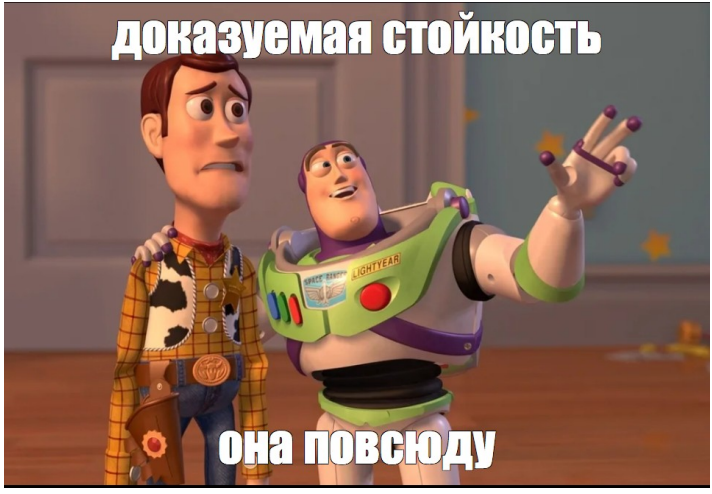
Показуемая стойкость в задаче обфускации криптографических исследований

Маршалко Григорй Борисович
Фомин Денис Бонславович

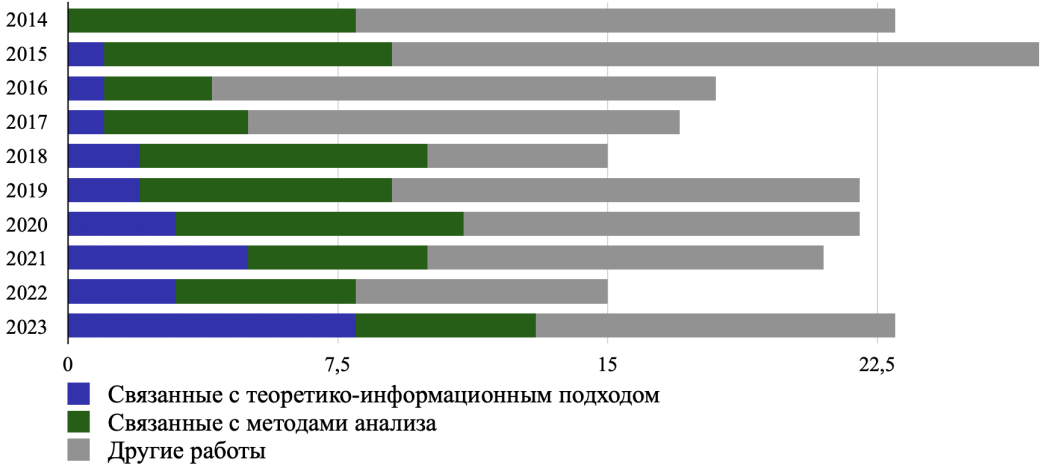
Академия криптографии Российской Федерации
Национальный исследовательский университет «Высшая школа экономики»

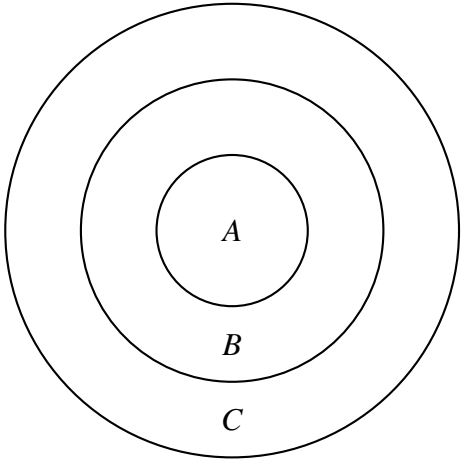
20 марта 2024 г.

Предисловие.

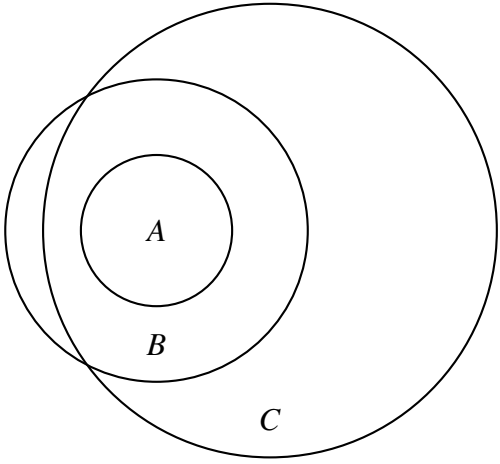


Работы, представленные на CTCrypt по тематикам





- A — Криптографические алгоритмы для которых предложены конкретные методы криптографического анализа
- B — Криптографические алгоритмы для которых показана их нестойкость в теоретико-информационной модели
- C — Нестойкие криптографические алгоритмы

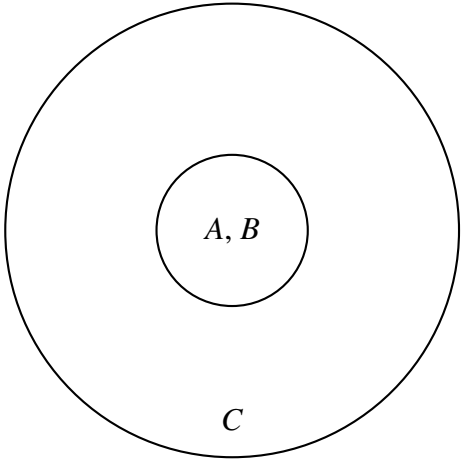


- A — Криптографические алгоритмы для которых предложены конкретные методы криптографического анализа
- B — Криптографические алгоритмы для которых показана их нестойкость в теоретико-информационной модели
- C — Нестойкие криптографические алгоритмы

- $A = C$, если бы была возможность перечислить все методы анализа
- Аналогично доказательству Колмогорова теоремы Гёделя о неполноте, можно показать, что $A \neq B$
- Теоретико-информационный подход использует тот же аппарат, что используется при построении методов криптографического анализа и имеет те же фундаментальные ограничения

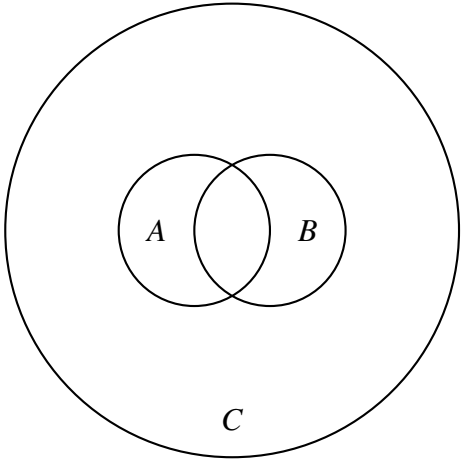
Курт Гёдель после выведения доказательства к теореме о неполноте, 1931 год

Хотелось бы, чтобы:



- A — Криптографические алгоритмы для которых предложены конкретные методы криптографического анализа
- B — Криптографические алгоритмы для которых показана их нестойкость в теоретико-информационной модели
- C — Нестойкие криптографические алгоритмы

Однако:

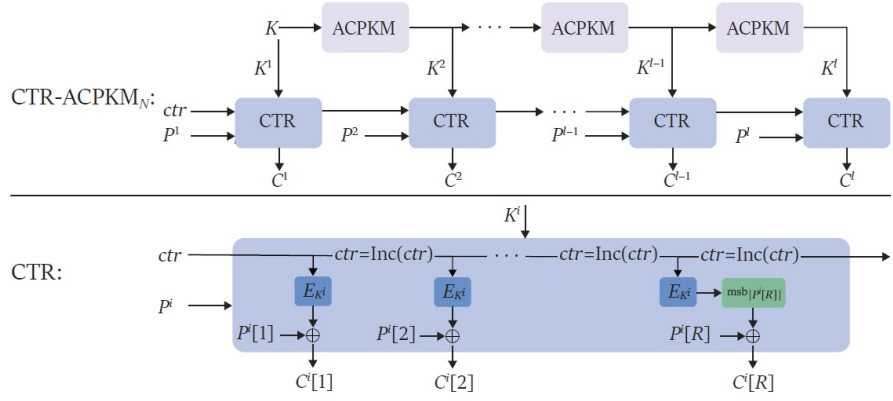


- A — Криптографические алгоритмы для которых предложены конкретные методы криптографического анализа
- B — Криптографические алгоритмы для которых показана их нестойкость в теоретико-информационной модели
- C — Нестойкие криптографические алгоритмы

Глава 1. Невозможность гарантирования стойкости решения с использованием только величины преобладания

На примере обоснования стойкости режима CTR-ACPKM покажем, что получение лишь только величины преобладания не позволяет говорить о стойкости итогового решения

CTR-ACPKM



Основной работой по исследованию свойств безопасности режима CTR-ACPKM считается работа [1], где были получены оценки на преобладание нарушителя $\mathsf{Adv}^{\text{IND-CPA}}_{\text{CTR-ACPKM}}$ в следующих предположениях:

- нарушитель действует в модели IND-CPA, в которой может адаптивно выбирать открытый текст и синхропосылки;
- вычислительные ресурсы нарушителя ограничены сверху некоторой величиной.

[1] L Akhmetzyanova и др. “Practical significance of security bounds for standardized internally re-keyed block cipher modes”. В: *Матем. вопр.крипт.* 10 (2019), с. 31—46.

В качестве «меры стойкости» используется значение преобладания, которое определяется следующей формулой:

$$\mathsf{Adv}^{\text{IND-CPA}}_{\text{CTR-ACPKM}}(\mathcal{A}) = \mathsf{P}(b' = 1 | b = 1) - \mathsf{P}(b' = 1 | b = 0).$$

Считается, что «чем ближе указанное значение к нулю, тем больше действия нарушителя похожи на случайное угадывание значения b».

Теорема ([2])

При выполнении условий реализации режима CTR-ACPKM*, для любого нарушителя $\mathcal{A}$, который обладает вычислительными ресурсами не превосходящими T, существует нарушитель $\mathcal{B}$ такой, что*

$$\mathsf{Adv}^{\text{IND-CPA}}_{\text{CTR-ACPKM}}(\mathcal{A}) \leq l \cdot \mathsf{Adv}^{\text{PRP-CPA}}_{E}(\mathcal{B}) + \frac{1}{2^{n+1}} \cdot \left(\sum_{i=1}^{l-1} (\sigma_i + d)^2 + \sigma_l^2 \right), \qquad (1)$$

где σ_i — количество блоков, зашифрованных на секционном ключе $K^{(i)}$. При этом, вычислительные ресурсы нарушителя $\mathcal{B}$ не превышают величины

$$T + c \cdot n \cdot \left(\sum_{i=1}^{l} \sigma_i + l \cdot d \right),$$

где константа c определяется моделью вычислений.

[2] Akhmetzyanova и др., “Practical significance of security bounds for standardized internally re-keyed block cipher modes”.

Рассмотрим первое слагаемое в формуле (1):

$$l \cdot \mathsf{Adv}_{E}^{\text{PRP-CPA}}(\mathcal{B})$$

Неформально: достаточно «нарушить свойство PRP-CPA» хотя бы для одного из l секционных ключей.

Снижение стойкости возможно, если есть возможность провести предварительные вычисления (как в методах балансировки время-память-данные) один раз, которые могут быть использованы для нарушения конфиденциальности для более, чем одного секционного ключа $K^{(i)}$, $i \in \{1, 2, \ldots, l\}$.

Действительно, пусть за одну элементарную операцию происходит опробование l секционных ключей $K^{(i)}$, $i \in \{1, 2, \ldots, l\}$. Тогда последовательно опробуя ключи шифрования с вероятностью 1, будет определен ключ $K^{(l)}$ с трудоемкостью:

$$\sum_{i=1}^{2^k} \left[\left(1 - \frac{i-1}{2^k}\right)^l - \left(1 - \frac{i}{2^k}\right)^l \right] \cdot i =$$

$$= 1 + \sum_{i=1}^{2^k-1} \left(1 - \frac{i}{2^k}\right)^l \approx 1 + \int_1^{2^k-1} \left(1 - \frac{i}{2^k}\right)^l di \approx 2^{k-l}.$$

Как и отметили выше — первое слагаемое в формуле (1) как раз говорит о потенциальном снижении стойкости в l раз.

Однако использование для каждого секционного ключа своего значения $IV^{(i)}$ не позволяет рассматривать такие методы криптографического анализа.

Несмотря на то, что потенциально возможно снизить оценку стойкости алгоритма блочного шифрования E, работающего в режиме CTR-ACPKM, в l раз, в настоящее время *не известны* методы анализа, позволяющие реализовать указанную угрозу в случае, *если не известны методы анализа более эффективные, чем тотальное опробование*.

Таким образом, формула (1) *занижает стойкость* для алгоритма «Кузнечик» в режиме CTR-ACPKM.

Для алгоритма «Магма» известны методы анализа, снижающие его практическую стойкость:

1. Метод отражения[3]
2. Метод Исобе[4]
3. Методы Динура-Данкельмана-Шамира[5]

[3] Orhun Kara. “Reflection Cryptanalysis of Some Ciphers.”. В: *INDOCRYPT*. Т. 5365. Lecture Notes in Computer Science. Springer, 2008, с. 294—307.

[4] Takanori Isobe. “A Single-Key Attack on the Full GOST Block Cipher.”. В: *J. Cryptol.* 26.1 (2013), с. 172—189.

[5] Itai Dinur, Orr Dunkelman и Adi Shamir. “Improved Attacks on Full GOST.”. В: *FSE*. Т. 7549. Lecture Notes in Computer Science. Springer, 2012, с. 9—28.

В приложении В (рекомендуемом) фиксированы следующие параметры для алгоритма «Магма»:

- $k = 256$, $n = 64$
- $m_{\max} \leq 2^{n/2-1} \cdot \frac{n \cdot N}{k+n} \approx 5.5 \cdot 10^{10}$ блоков
- $N \leq 1$ КБайт (128 блоков)
- $u \leq 4096$

При таких объемах материала вероятность появления неподвижной точки на одном секционном ключе (вероятность нарушения конфиденциальности):

$$p_0 = 2.84 \cdot 10^{-14}.$$

При таких объемах материала вероятность появления неподвижной точки на одном секционном ключе (вероятность нарушения конфиденциальности):

$$p_0 = 2.84 \cdot 10^{-14}.$$

Однако вероятность появления неподвижной точки (вероятность нарушения конфиденциальности) для режима целиком:

$$1.56 \cdot 10^{-3} \approx m_{\max} \cdot p_0.$$

Глава 2. Невозможность комбинирования с некоторыми методами анализа

Согласно рекомендации по стандартизации Р 1323565.1.017—2018:

Для средств криптографической защиты информации классов КС1, КС2 и КС3 (см. раздел 4 Р 1323565.1.012—2017), а также средств, которые не подпадают под действие [1], допустимым является использование следующих ограничений:

- *при использовании алгоритма блочного шифрования «Магма» объем преобразованной на одном секретном ключе информации не должен превышать 4 Мбайт (524 288 блоков);*
- *размер N одной секции режима CTR-ACKPM полагается равным 1 Кбайт (128 блоков).*

Из указанных ограничений следует, что число сообщений, которые могут быть обработаны на одном секретном ключе K, не должно превышать 4096. При этом длины сообщений дополнительно не ограничены.

Таким образом, авторы Р 1323565.1.017—2018 придерживались следующей парадигмы:

- ограничить количество информации, обрабатываемой на одном секционном ключе исходя из «нагрузки на ключ» и отсюда получить количество сообщений, которые можно обрабатывать на одном ключе
- ограничение на длину сообщений получить из формулы (1)

В приложении B (рекомендуемом) фиксированы следующие параметры для алгоритма «Кузнечик»:

- $k = 256$, $n = 128$
- $m_{\max} \leq 2^{n/2-1} \cdot \frac{n \cdot N}{k+n} \approx 5.5 \cdot 10^{10}$ блоков
- $N \leq 4$ КБайт (256 блоков)
- $u \leq 64$

Тогда на всем материале вероятность отличения выхода режима CTR-ACPKM от случайной подстановки равна:

$$p_1 = 1 - \left(1 - \frac{1}{2^{128}}\right)^{64 \cdot 256} \approx 1 - e^{-\frac{64 \cdot 256}{2^{128}}},$$

$$1 - (1 - p_1)^{m_0} \approx 1,$$

где

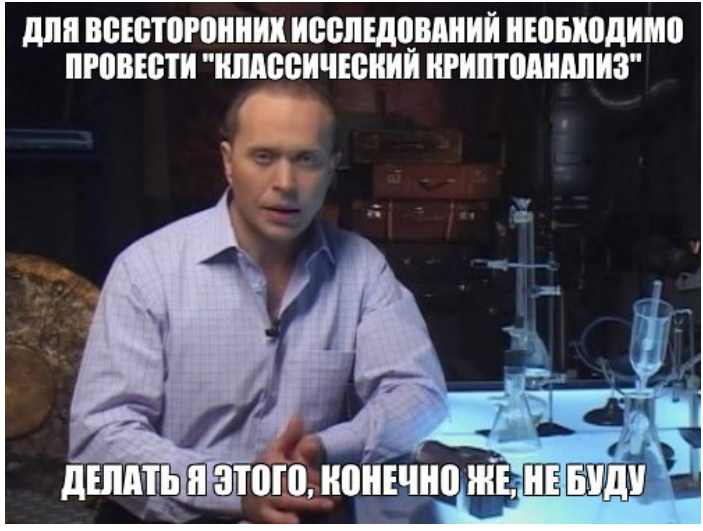
$$m_0 = 2^{n/2-1} \cdot \frac{N}{k+n}.$$

Такой подход по «комбинированию» методов криптографического анализа привел к тому, что с вероятностью 1 выход режима CTR-ACPKM может быть отличен от случайной равновероятной последовательности

Вывод:

При анализе криптографических алгоритмов необходимо рассматривать разные подходы к обоснованию стойкости

Глава 3. Что нам дают «классические методы» криптографического анализа?



- Из [6] следует коренная оценка на объем материала
- В работе [7] (которая, подтверждает полученные оценки) показано, что при достижении указанной границы нарушитель может получать пары x, y такие, что

$$E_K(x) = y,$$

что явно не следует из описания режима работы и [6]

[6] Liliya Akhmetzyanova и др. *Security of Multilinear Galois Mode (MGM)*. Cryptology ePrint Archive, Paper 2019/123. 2019.

[7] Alexey Kurochkin и Denis Fomin. “MGM beyond the birthday bound”. В: *Journal of Computer Virology and Hacking Techniques* (март 2023), с. 1—5.

Лишь некоторые примеры:

- В работе [8] предполагается, что нарушитель получает не полную информацию о пересылках в протоколе
- В работе [9] не рассматриваются методы, связанные с получением информации об открытом тексте, при совпадении шифртекстов

Таким образом, зачастую, удается гарантировать стойкость только в рассматриваемых формальных моделях, релевантность которых не обоснована

[8] Stefano Tessaro и Chenzhi Zhu. *Short Pairing-Free Blind Signatures with Exponential Security*. Cryptology ePrint Archive, Paper 2022/047. 2022.

[9] Yaobin Shen, Chun Guo и Lei Wang. *Improved Security Bounds for Generalized Feistel Networks*. Cryptology ePrint Archive, Paper 2020/285. 2020.

Но и это не все:

- Часто, из-за отсутствия корректного задания вероятностного пространства, используются необоснованные предположения о распределениях на множествах параметров и входных данных, что приводит к возможности построения методов анализа на практике
- Формальное описание моделей приводит к сложной верифицируемости результатов и наличия ошибок в доказательствах, которые обнаруживаются при «классическом» исследовании алгоритмов
- Некорректное обоснование «сведений», связанное с тем, что если получено значение преобладания, то алгоритм считается «абсолютно стойким»
- Наличие путаницы с понятиями «вероятности» и «преобладания»
- Не ясно как ограничивать значение преобладания

и т.д. и т.п.

Глава 4. А что мы доказываем то?

Согласно [10,11] утверждается, что

$$\mathsf{Adv}_E^{\mathrm{NCPA}}(q) = \max_{X \in M^{[q]}} \left\| \mathsf{Y} - \tilde{\mathsf{U}} \right\|, \tag{2}$$

где максимум берется по всем возможным наборам попарно различных открытых текстов объема q[12], а $\tilde{\mathsf{U}}$ — распределение вектора Y при реализации урновой схемы без возвращения.

[10] Shen, Guo и Wang, *Improved Security Bounds for Generalized Feistel Networks*.

[11] Valérie Nachef, Jacques Patarin и Emmanuel Volte. *Feistel Ciphers - Security Proofs and Cryptanalysis*. Springer, 2017, с. 1—309.

[12] Через $X^{[y]}$ обозначаем реализацию урновой схемы без возвращения, где вынимается y шаров из X

Заметим, что *при отсутствии конструктивных методов анализа* максимизация последней величины есть задача отличения двух распределений.

Пусть блочный шифр E есть композиция двух преобразований: шифра E_1, для которого с незначительной трудоемкостью с вероятностью 1 определяется его ключ, и случайно равновероятно выбранной подстановки $E_2 \xleftarrow{\mathsf{U}} \mathsf{P}(M)$, $E = E_1 \cdot E_2$. При этом подстановка E_2 выбирается известным нарушителю способом.

В этом случае очевидно, что статистическое расстояние будет равно 0, однако величина преобладания $\mathsf{Adv}_E^{\mathrm{NCPA}}(q)$ будет равна 1.

Таким образом, предложенный в данных работах подход *не позволяет говорить о стойкости алгоритмов шифрования*

Рассмотрим теперь $F_\kappa(x) = (E_\kappa(x), -x)$. В этом случае вероятность $\mathsf{P}\left(F_\kappa(x) = b\right)$ определяется как выбором ключа, так и x. Тогда

$$\begin{aligned}\mathsf{P}\left(F_\kappa(x) = b\right) &= \sum_{\kappa \in K} \mathsf{P}(\kappa) \cdot \mathsf{P}\left(F_\kappa(x) = b \middle| \kappa\right) = \\ &= \sum_{\kappa \in K} \mathsf{P}(\kappa) \cdot \left(\frac{1}{|Z|} \sum_{\gamma \in Z} \mathsf{M}\left[\phi_\gamma(F_\kappa) \middle| \kappa\right] \overline{\phi_\gamma(b)} \right) = \\ &= \frac{1}{|Z|} \sum_{\gamma \in Z} \left(\sum_{\kappa \in K} \mathsf{P}(\kappa) \mathsf{M}\left[\phi_\gamma(F_\kappa) \middle| \kappa\right] \right) \overline{\phi_\gamma(b)} = \frac{1}{|Z|} \sum_{\gamma \in Z} \mathsf{M}\phi_\gamma(F_\kappa) \overline{\phi_\gamma(b)},\end{aligned}$$

где ϕ_γ — характер соответствующей конечной абелевой группы Z, а $\mathsf{M}\phi_\gamma(F_\kappa)$ суть коэффициент корреляции.

Таким образом, гарантировав невозможность применения линейного метода криптографического анализа, гарантируем, что величина

$$\max_{X \in M^{[g]}} \left\| \mathsf{Y} - \tilde{\mathsf{U}} \right\|$$

будет мала и можем даже ее оценить.

Заключение


ВИДИШЬ КРИПТОАНАЛИЗ? И Я НЕТ
А ГОВОРЯТ, ЧТО ОН ЕСТЬ
memesmix.net

SEE YOU SPACE COWBOY...