УДК 004.056.55 DOI 10.17223/2226308X/13/20

АНАЛИЗ РЕЖИМОВ ШИФРОВАНИЯ ДЛЯ РЕАЛИЗАЦИИ В УСТРОЙСТВАХ RFID

К. Д. Царегородцев

Технология радиочастотной идентификации (RFID) описывает способы бесконтактной идентификации и аутентификации объектов с возможным обменом зашифрованными данными. В состав RFID-системы входит радио-метка и считывающее устройство. Основная функция RFID-меток — аутентификация с передачей небольшого объёма информации между меткой и считывателем (например, платежи). С учётом аппаратных ограничений изучены режимы шифрования, для которых на метке необходимо реализовать только алгоритм зашифрования блока текста. Рассмотрены режимы CTR, OFB, CFB, модифицированный режим CBC. Для модифицированного режима CBC получена верхняя оценка стойкости в соответствующей модели противника.

Ключевые слова: *доказуемая стойкость, RFID, режим шифрования.*

RFID-система состоит из двух взаимодействующих участников: метки (с записанными на ней наборами ключей) и считывателя. Необходимо передавать зашифрованную информацию как от считывателя к метке, так и от метки к считывателю. Дополнительно налагаются ограничения на метку: на ней реализован только алгоритм зашифрования блока текста (без расшифрования).

Будем рассматривать следующую стандартную модель LOR-неразличимости двух режимов шифрования [1]. На каждом шаге вычислений противник (являющийся вероятностной машиной Тьюринга) подаёт запросы на вход одного из двух оракулов: $\mathcal{O}_1$ или $\mathcal{O}_2$. Первый оракул реализует режим шифрования, используемый при передаче информации от метки к считывателю, второй оракул — режим шифрования, используемый при передаче информации от считывателя к метке. Оракулы используют один и тот же ключ, выбранный случайно равновероятно в начале эксперимента. Тем самым оракулы связаны друг с другом посредством общего ключа.

На каждом шаге противник даёт одному из оракулов (любому, на его выбор) два сообщения (одинаковой длины) для обработки:

$$\left(M^L = (m_1^L, \ldots, m_t^L),\ M^R = (m_1^R, \ldots, m_t^R)\right).$$

В эксперименте Left каждый из оракулов $\mathcal{O}_1$ и $\mathcal{O}_2$ зашифровывает сообщение M^L в своём режиме шифрования и возвращает вычисленный шифртекст. В эксперименте Right каждый из оракулов зашифровывает сообщение M^R и возвращает вычисленный шифртекст.

Задача противника — анализируя полученные шифртексты, суметь различить два эксперимента. Если противник «думает», что оракулы зашифровывают правые тексты (эксперимент Right), то он выдаёт 1, в противном случае — 0. Если противник способен с высокой вероятностью различать эксперименты Left и Right, то это означает, что он может восстанавливать частичную информацию об открытом тексте из шифртекста. Таким образом, преимущество противника $\mathcal{A}$ задаётся как разность вероятностей

$$\mathrm{Adv}(\mathcal{A}) = \mathsf{P}[\mathrm{Right}(\mathcal{A}) \to 1] - \mathsf{P}[\mathrm{Left}(\mathcal{A}) \to 1],$$

где $\mathsf{P}[X(\mathcal{A}) \to 1]$ — вероятность того, что противник, взаимодействуя с экспериментатором X, выдаст 1. Вероятность берётся по начальному выбору ключа, внутренних

выборах оракулов (случайные векторы инициализации) и случайным битам самого противника. Так, например, если противник не делает никаких запросов к оракулам и просто выдаёт результат подбрасывания случайной равновероятной монеты, то его преимущество $\mathrm{Adv}(\mathcal{A})$ равно нулю. Если противник идеально различает два эксперимента, то его преимущество равно 1.

Обозначим: q — общее число запросов к оракулам $\mathcal{O}_1$ и $\mathcal{O}_2$; m — максимальная длина одного запроса (в блоках); t — количество тактов вычислений противника; n — длина одного блока (в битах); k — длина используемого ключа; $\mathrm{Adv}^{LOR}_{\mathcal{O}_1,\mathcal{O}_2}(t,q,m)$ — максимально достижимое преимущество среди всех противников, работающих за время не более t и делающих суммарно не более q запросов, каждый из которых имеет длину не более m блоков.

Режимы шифрования CTR (гаммирования), OFB (гаммирования с обратной связью по выходу), CFB (гаммирования с обратной связью по шифртексту) [2] не требуют реализации алгоритма расшифрования на метке, поэтому могут использоваться непосредственно, без модификаций. Для этих режимов оракулы $\mathcal{O}_1$ и $\mathcal{O}_2$ совпадают.

Теорема 1 [3]. Для режима CTR имеем следующую оценку:

$$\mathrm{Adv}^{\mathrm{LOR}}_{\mathrm{CTR},\,\mathrm{CTR}}(t,q,m) \leqslant \frac{2q^2m^2}{2^n} + \frac{t+q+bqm}{2^{k-1}}.$$

Аналогичные оценки могут быть получены для режимов OFB и CFB (главный член имеет порядок $O((qm)^2/2^n)$ — оценка дней рождения [4]). При доказательстве используется предположение о PRP-стойкости используемого блочного шифра.

Отдельно рассмотрим режим CBC. Для расшифрования в режиме CBC требуется реализация алгоритма расшифрования блока текста, поэтому режим CBC при передаче сообщения от считывателя к метке был модифицирован следующим образом (обозначен далее как $\widehat{\mathrm{CBC}}$):

$$C_0 = \mathrm{IV}, \quad C_i = E_k^{-1}(C_{i-1} \oplus M_i),$$

где E_k^{-1} — алгоритм расшифрования блока текста; M_i — i-й блок открытого текста; C_i — i-й блок шифртекста. Заметим, что для расшифрования сообщения, зашифрованного по алгоритму $\widehat{\mathrm{CBC}}$, не требуется реализации алгоритма расшифрования блока текста.

Таким образом, у противника есть доступ к оракулу зашифрования по алгоритму CBC (оракул $\mathcal{O}_1$) и по алгоритму $\widehat{\mathrm{CBC}}$ (оракул $\mathcal{O}_2$) на одном и том же ключе k.

Основным результатом является следующая

Теорема 2. Для пары режимов CBC и $\widehat{\mathrm{CBC}}$ выполнена оценка

$$\mathrm{Adv}^{\mathrm{LOR}}_{\mathrm{CBC},\widehat{\mathrm{CBC}}}(t,q,m) \leqslant \frac{3q^2m^2}{2^n - qm} + \frac{t+q}{2^{k-1}}.$$

Доказательство основано на идее из работы [5]: если выходы двух оракулов могут быть промоделированы генератором, которому на вход подаются лишь длины сообщений (но не их содержание), то режим является LOR-стойким.

На первом шаге доказательства, используя свойство sPRP-стойкости блочного шифра (стандартное предположение, см., например, [6]), мы заменяем каждое вхождение блочного шифрования $E_k(x)$ и $E_k^{-1}(x)$ на применение случайной подстановки $\pi(x)$ и $\pi^{-1}(x)$ соответственно.

На втором шаге анализируем полученную конструкцию и показываем, что выходы обоих оракулов можно промоделировать без знания открытого текста. Итоговые оценки получаются из предположения, что множества, на которых вычисляются значения подстановок $\pi(x)$ и $\pi^{-1}(x)$, не пересекаются.

Полученная оценка близка к оптимальной для стандартного режима CBC: член вида $O((qm)^2/2^n)$ отражает тот факт, что для режима CBC всегда существует атака дней рождения, предполагающая возникновение коллизии для векторов инициализации IV.

ЛИТЕРАТУРА

1. *Katz J. and Lindell Y.* Introduction to Modern Cryptography, 2nd Ed. Chapman & Hall/CRC, 2014.
2. Межгосударственный стандарт ГОСТ 34.13-2018 Информационная технология (ИТ). Криптографическая защита информации. Режимы работы блочных шифров. М.: Стандартинформ, 2018.
3. *Ahmetzyanova L. R., Alekseev E. K., Oshkin I. B., 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 // Матем. вопр. криптогр. 2017. Т. 8. № 2. С. 39–50.
4. *Rogaway P.* Evaluation of Some Block Cipher Modes of Operation. 2011. `https://web.cs.ucdavis.edu/~rogaway/papers/modes.pdf`
5. *Wooding M.* New Proofs for Old Modes. IACR Cryptology ePrint Archive. 2008.
6. *Bellare M., Desai A., Jokipii E., and Rogaway P.* A concrete security treatment of symmetric encryption // Proc. 38th Ann. Symp. Foundations of Computer Science, IEEE, 1997. P. 394–403.

УДК 519.714.5 DOI 10.17223/2226308X/13/21

ОБ ОДНОМ ПОДХОДЕ К ПОСТРОЕНИЮ КРАТНО ТРАНЗИТИВНОГО МНОЖЕСТВА БЛОЧНЫХ ПРЕОБРАЗОВАНИЙ

И. В. Чередник

Пусть Ω — произвольное конечное множество; $\mathcal{B}(\Omega)$ — семейство всех бинарных операций, определённых на Ω; $x_1, \dots, x_n$ — переменные, принимающие значения из Ω; $*_1, \dots, *_k$ — общие символы бинарных операций. Фиксированный набор $W = (w_1, \dots, w_m)$ формул в алфавите $\{x_1, \dots, x_n, *_1, \dots, *_k\}$ при замене $*_1, \dots, *_k$ на произвольные бинарные операции $F_1, \dots, F_k \in \mathcal{B}(\Omega)$ соответственно реализует отображение $W^{F_1,\dots,F_k} \colon \Omega^n \to \Omega^m$. Исследованы криптографические свойства (биективность и кратная транзитивность) семейств блочных преобразований $\{W^{F_1,\dots,F_k} : F_1, \dots, F_k \in \mathcal{K}\}$, $\mathcal{K} \subset \mathcal{B}(\Omega)$, которые могут быть использованы при построении хэш-функций и блочных шифров.

Ключевые слова: *блочные преобразования, кратная транзитивность множества блочных преобразований, функциональная бинарная сеть.*

В последнее время при разработке систем защиты информации активно исследуется возможность использования неассоциативных алгебраических структур, особое место в таких исследованиях занимают квазигруппы. Например, в ряде схем поточных шифров, хеш-функций и др. [1 – 3] используются семейства блочных преобразований, реализуемых наборами «цепных» формул вида

$$C_a^*(x_1, \dots, x_n) = (a * x_1, (a * x_1) * x_2, \dots, ((a * x_1) * \dots) * x_n), \quad a \in \Omega,$$