Секция 2

МАТЕМАТИЧЕСКИЕ МЕТОДЫ КРИПТОГРАФИИ

УДК 519.7

МНОГОЧЛЕНЫ НАД ПРИМАРНЫМИ КОЛЬЦАМИ ВЫЧЕТОВ С МАЛЫМ РАССТОЯНИЕМ ЕДИНСТВЕННОСТИ

А. В. Аборнев, Д. Н. Былков

Пусть $F(x)$ — унитарный многочлен степени m над кольцом $R = \mathbb{Z}_{2^n}$. Через $L_R(F)$ будем обозначать множество всех линейных рекуррентных последовательностей над R с характеристическим многочленом $F(x)$ [1]. Каждой последовательности u из $L_R(F)$ сопоставим последовательности $u_0, \ldots, u_{n-1}$, получающиеся из двоичного разложения

$$u(i) = u_0(i) + 2u_1(i) + \ldots + 2^{n-1}u_{n-1}, u_s(i) \in \{0,1\}, s = 0, \ldots, n-1;\ i \geqslant 0. \qquad (1)$$

При правильном выборе многочлена $F(x)$ последовательности u_s обладают рядом важных для криптографии свойств: большим периодом, высоким рангом, хорошими частотными характеристиками. Одним из наименее изученных параметров является *расстояние единственности*.

Определение 1. Назовем расстоянием единственности многочлена $F(x)$ и обозначим через $\mathrm{Ud}(F)$ минимум натуральных чисел l, таких, что для любых двух рекуррент $u, v \in L_R(F), u \neq v$, верно соотношение

$$u_{n-1}[\overline{0, l-1}] \neq v_{n-1}[\overline{0, l-1}];$$

если же таких натуральных l не существует, то будем писать $\mathrm{Ud}(F) = \infty$.

А. А. Нечаевым выдвинута

Гипотеза 1. Параметр $\mathrm{Ud}(F)$ зависит линейно от величины mn.

В настоящее время эта гипотеза не доказана, но и не опровергнута. Первым шагом в продвижении этой гипотезы стал результат А. А. Варфоломеева о расстоянии единственности многочлена $x^2 - x - 1 \in \mathbb{Z}_{2^n}[x]$ (устные сообщения). В дальнейшем второму из авторов удалось частично подтвердить гипотезу 1 в случае, когда многочлен $F(x) \in \mathbb{Z}_4$ является трехчленом [2]. В частности, справедлива

Теорема 1. Пусть $F(x) = x^m - x - 1$, тогда $\mathrm{Ud}(F) = 3m$.

Далее $n = 2, R = \mathbb{Z}_4$. Конечность параметра $\mathrm{Ud}(F)$ означает, что начальный вектор $u[\overline{0, m-1}]$ последовательности $u \in L_R(F)$ однозначно определяется по отрезку $u_1[\overline{0, \mathrm{Ud}(F)-1}]$. Обширные вычислительные эксперименты на ЭВМ показали существование многочленов $F(x) \in R[x]$ со свойством $\mathrm{Ud}(F) = 2m$.

Для таких многочленов А. А. Нечаевым предложен способ построения подстановки ψ_F, действующей на множестве $T = \mathbb{Z}_2^m$. В этом случае отрезок $u[\overline{0, m-1}]$ однозначно задается отрезком $u_1[\overline{0, 2m-1}]$. Для каждого $t \in T$ зададим последовательность $u \in L_R(F)$ по правилу $u_0[\overline{0, m-1}] = t,\ u_1[\overline{0, m-1}] = \overline{0}$. В соответствии со сказанным выше отрезок $u_1[\overline{0, 2m-1}]$ однозначно определяет начальный вектор

$u[\overline{0,m-1}]$, а значит, и элемент t. Так как $u_1[\overline{0,m-1}] = \overline{0}$, то $t = u_0[\overline{0,m-1}]$ однозначно определяется отрезком $u_1[\overline{m,2m-1}]$. Зададим подстановку ψ_F равенством $\psi_F(t) = u_1[\overline{m,2m-1}]$.

Достоинством таких подстановок является возможность их эффективной реализации на современных микропроцессорах. Отметим, что некоторые координатные функции ψ_F имеют степень нелинейнсти 2. Рассмотрим узел блочного шифра с r раундами и набором раундовых ключей $k = (k_1, \ldots, k_r) \in T^r$, построенный на основе подстановки ψ_F. Исходное сообщение $x \in T$ преобразуется согласно равенству

$$y = S_k(x) = \psi_F(\ldots \psi_F(\psi_F(x + k_1) + k_2) \ldots + k_r).$$

Зададим группу подстановок $G = \{g_t : g_t(x) = x \oplus t,\ x, t \in T\}$. Тогда $S_k \in (\psi_F G)^r$. В ходе экспериментов установлено, что в ряде случаев множество подстановок $\psi_F G$ порождает знакопеременную группу подстановок. Построены примеры, когда уже при $k = m$ данный узел является стойким к методу дифференциального анализа.

Тривиальными примерами многочленов с расстоянием единственности $2m$ являются многочлены $F(x)$, такие, что $F(x) \equiv x^m + 1 \pmod 2$. Однако пока не обосновано существование нетривиальных многочленов со свойством $\mathrm{Ud}(F) = 2m$ произвольной степени m. Важным шагом в этом направлении является

Теорема 2. Пусть $m = 2^k + s$, $k \in \mathbb{N}$, s нечетно, $F(x) = F_0(x) + 2F_1(x)$ — двоичное разложение многочлена $F(x)$, $F_0(x) \equiv (x+1)^m \pmod 2$ и $(F_1(x) + x^s, x + 1) = 1$. Тогда $\mathrm{Ud}(F) \in \{2m, \infty\}$.

Пусть $R = \mathbb{Z}_{p^2}$, $p > 2$ — простое число, $\Gamma(R) = \{a \in R : a^p = a\}$ — p-адическое координатное множество. Известно [1], что каждый элемент $a \in R$ однозначно представляется в виде $a = a_0 + pa_1, a_0, a_1 \in \Gamma(R)$. Аналогично (1) каждую линейную рекуррентную последовательность $u \in L_R(F)$ можно представить в виде

$$u(i) = u_0(i) + pu_1(i), \quad u_0(i), u_1(i) \in \Gamma(R), \quad i \geqslant 0.$$

Параметр $\mathrm{Ud}(F)$ определяется так же, как и в двоичном случае. Серия экспериментов на ЭВМ показала, что результат теоремы 1 справедлив для $p = 3$, $m \in \overline{2,9}$; $p = 5$, $m \in \overline{2,5}$. Экспериментально показано существование многочленов с расстоянием единственности $2m$. Такие многочлены также позволяют задавать подстановки на множестве $\mathbb{Z}_p^m$. Степень нелинейности координатных функций соответствующих подстановок равна p.

ЛИТЕРАТУРА

1. *Kurakin V. L., Kuzmin A. S., Mikhalev A. V., and Nechaev A. A.* Linear Recurring Sequences over Rings and Modules // J. Math. Sci. 1995. V. 76. No. 6. P. 2793–2915.
2. *Былков Д. Н.* Расстояние единственности семейства координатных последовательностей, полученных усложнением линейных рекуррент над кольцом Галуа //Прикладная дискретная математика. 2008. № 2. С. 5–7.

УДК 519.7

О РАСШИРЕНИЯХ ОТОБРАЖЕНИЙ, СОХРАНЯЮЩИХ СВОЙСТВО ИДЕНТИФИЦИРУЕМОСТИ[1]

Л. Н. Андреева

Пусть $A = \{0, 1, \ldots, k-1\}$, $k \geqslant 2$, n — натуральное число, Q — множество всех отображений $q\colon A^n \to A^n$ и для каждого отображения q в Q определены функции $q_i\colon A^n \to A$, $i = 1, 2, \ldots, n$, так, что $q(x) = q_1(x)q_2(x)\ldots q_n(x)$ для всех x в A^n, т. е. $q = q_1q_2\ldots q_n$. Пусть также $B = \{i_1, i_2, \ldots, i_{|B|}\} \subseteq \{1, \ldots, n\}$, $i_1 < i_2 < \ldots < i_{|B|}$ и $a[B] = a_{i_1}a_{i_2}\ldots a_{i_{|B|}}$ для любого вектора $a = a_1a_2\ldots a_n$.

Говорят, что отображение q в Q *идентифицируется на* B, если для любого отображения $t \in Q$ из $q[B] = t[B]$ следует $q = t$.

По определению, если отображение q в Q идентифицируется на B, то оно идентифицируется и на любом множестве $F \subseteq \{1, \ldots, n\}$, таком, что $B \subseteq F$.

Построим отображение $g\colon A^{n+1} \to A^{n+1}$ как расширение отображения q следующим образом. Возьмём произвольную функцию $\sigma\colon A \to A$ и элемент $j \in \{1, \ldots, n+1\} \setminus B$ и положим $g_j(x_1, \ldots, x_j, \ldots, x_{n+1}) = \sigma(x_j)$, $g_i(x_1, \ldots, x_j, \ldots, x_{n+1}) = q_i(x_1, \ldots, x_{j-1}, x_{j+1}, \ldots, x_{n+1})$ для всех $i \neq j$. Пусть наконец $D = B \cup \{j\}$.

Теорема 1. Отображение q идентифицируется на B, если и только если отображение g идентифицируется на D. Отображение g не идентифицируется на множестве $\{1, \ldots, n+1\} - \{j\}$.

Доказательство. Пусть отображение q идентифицируется на B. Предположим, что его расширение g не идентифицируется на D. Тогда найдётся такое отображение $t' : A^{n+1} \to A^{n+1}$, что $t'[D] = g[D]$ и $g \neq t'$, и для $t \in Q$, полученного из t' вычёркиванием j-й компоненты, будет $q[B] = t[B]$ и $q \neq t$, что противоречит идентифицируемости q на B. Следовательно, g идентифицируется на D.

Обратно, пусть отображение g идентифицируется на D. Предположим, что q не идентифицируется на B. Тогда найдётся такое отображение $t\colon A^n \to A^n$, что $t[B] = q[B]$ и $q \neq t$. Построим расширение t' для t, положив $t'_j = g_j$, и как результат получим $g[D] = t'[D]$ и $g \neq t'$, что противоречит идентифицируемости g на D. Следовательно, q идентифицируется на B.

Пусть g' — такое расширение отображения q, что $g'_j(x) = \sigma'(x_j) \neq \sigma(x_j) = g_j(x)$. Тогда $g_1g_2\ldots g_{j-1}g_{j+1}\ldots g_{n+1} = g'_1g'_2\ldots g'_{j-1}g'_{j+1}\ldots g'_{n+1}$ и $g \neq g'$, т. е. отображение g не идентифицируется на множестве $\{1, \ldots, n+1\} - \{j\}$. ■

Пусть далее $V \subseteq Q$ есть множество всех инволюций на A^n, т. е. подстановок $q\colon A^n \to A^n$ со свойством инволютивности: $\forall x, y \in A^n(q(x) = y \Rightarrow q(y) = x)$. Непосредственно проверяется, что если расширение g инволюции $q \in V$ построено с помощью подстановки $\sigma\colon A \to A$, то $g \in V$, т. е. расширение инволюции по подстановке является инволюцией; в этом случае теорема 1 остаётся в силе, если в её формулировке вместо отображений в Q рассматриваются инволюции в V. Таким образом, для любой инволюции $q \in V$ можно построить $k!(n+1)$ различных инволюций, являющихся расширениями инволюции q, сохраняющими свойство идентифицируемости последней.

Эти результаты могут быть использованы в инволюционных схемах разделения секрета [1], когда в множество участников схемы вводится новый участник и требуется,

[1]Работа выполнена в рамках реализации ФЦП «Научные и научно-педагогические кадры инновационной России» на 2009–2013 гг. (гос. контракт № П1010).

чтобы неавторизованные множества новой схемы включали в себя неавторизованные множества прежней схемы.

В этой связи, а также в связи с криптоанализом инволюционных шифров [2, 3] представляет интерес следующий тест идентифицируемости произвольной инволюции.

Теорема 2. Инволюция $q \in V$ идентифицируется на B, если и только если для любых x и y в A^n, $x \neq y$, выполняется $q(x)[B] \neq q(y)[B]$.

Доказательство. Необходимость. Пусть инволюция q идентифицируется на B. Предположим, что в A^n найдутся такие x и y, что $x \neq y$ и $q(x)[B] = q(y)[B]$. Построим инволюцию $t \in V$, $t \neq q$, такую, что $q(x) = t(y)$ и $q(y) = t(x)$, а на остальных элементах в A^n инволюции t и q совпадают. Тогда $t(y)[B] = q(x)[B] = q(y)[B] = t(x)[B]$. Имеем $t[B] = q[B]$ и $t \neq q$, что противоречит идентифицируемости q на B.

Достаточность. Пусть для любых x и y в A^n, где $x \neq y$, выполняется $q(x)[B] \neq \neq q(y)[B]$. Предположим, что инволюция q не идентифицируется на B. Тогда в Q найдется инволюция t, что $t \neq q$ и $q[B] = t[B]$. Если же $t \neq q$, то в A^n найдутся такие x и y, что $x \neq y$, $q(x) = t(y)$ и $q(y) = t(x)$. Следовательно, $q(x)[B] = t(x)[B] = q(y)[B] = = t(y)[B]$, что противоречит условию. ■

ЛИТЕРАТУРА

1. *Андреева Л. Н.* Инволюционные схемы разделения секрета // Вестник Томского госуниверситета. Приложение. 2007. № 23. С. 99.
2. *Андреева Л. Н.* К криптоанализу шифров инволюционной подстановки // Вестник Томского госуниверситета. Приложение. 2005. № 14. С. 43–44.
3. *Андреева Л. Н.* К криптоанализу инволютивных шифров с частично известными инволюциями // Вестник Томского госуниверситета. Приложение. 2006. № 17. С. 109–112.

УДК 004.056.55

ДОКАЗУЕМО БЕЗОПАСНАЯ ДИНАМИЧЕСКАЯ СХЕМА ГРУППОВОЙ ПОДПИСИ

А. В. Артамонов, П. Н. Васильев, Е. Б. Маховенко

В ряде прикладных задач для защиты сообщений от фальсификации требуется выполнение следующих условий:

— возможности создания электронной цифровой подписи одним лицом от имени группы лиц;
— невозможности идентификации автора такой подписи проверяющей стороной;
— возможности раскрытия автора подписи уполномоченным лицом.

Этим условиям удовлетворяют схемы групповой подписи. В зависимости от решаемой прикладной задачи к ним могут быть предъявлены дополнительные требования:

— возможность добавления новых членов в группу без необходимости изменения открытого ключа группы;
— возможность отзыва права подписи у определенных членов группы.

Анализ современных схем групповой подписи позволил выделить признаки, по которым такие схемы можно классифицировать и сравнивать, а на их основе построить обобщенную классификационную схему схем групповой подписи [1]. По совокупности этих признаков, в частности свойств безопасности, обеспечиваемых схемой, эффективности процедур формирования, проверки и раскрытия подписи, ее длины, а также

набору криптографических предположений следует выделить схему BBS [2]. Ее безопасность основана на предоставлении в подписи знания решения задачи SDH (Strong Diffie — Hellman): пары $(A, x) \in G_1 \times \mathbb{Z}_p$, такой, что $A^{x+\gamma} = g_1$, где $\langle g_1 \rangle = G_1$ — циклическая группа простого порядка p; $\gamma \in \mathbb{Z}_p$ — секретный ключ выпускающего менеджера группы. Схема BBS является наиболее гибкой и расширяемой. Но ни она, ни более поздние и совершенные ее модификации BS VLR [2] и XSGS [3] не обладают полнотой сразу по всем характеристикам: функциональности, безопасности, эффективности.

Предлагается динамическая доказуемо безопасная схема групповой подписи, построенная на основе схемы BBS, с возможностью отзыва права подписи у заданного члена группы с определенного момента времени. Чтобы обеспечить возможность интерактивного добавления в группу новых членов, в схему внедрен протокол Join, по аналогии с XSGS [3]. Для этого потребовалось изменить состав ключей членов группы: ключом является тройка $(A, x, y) \in G_1 \times \mathbb{Z}_p^2$, где $A^{x+\gamma} = g_1 h^y$, $h \in G_1$ — элемент открытого ключа группы, и соответствующим образом адаптировать алгоритмы формирования и проверки подписи. Предложена спецификация и самого протокола Join.

Для обеспечения полной анонимности [4] в схеме BBS CPA-стойкая схема линейного шифрования заменена модифицированной CCA2-стойкой линейной схемой Крамера — Шоупа [5]. Это позволило доказать безопасность предложенной схемы по требованиям динамической модели BSZ [4]. Согласно этим требованиям, возможности нарушителя моделируются предоставлением ему доступа к различным оракулам. При доказательстве свойств предполагается, что:

— с помощью атакующего, который умеет с ненулевой вероятностью нарушать некоторое свойство безопасности, строится новый алгоритм, решающий сложную по предположению задачу. Из этого следует, что такого атакующего не может быть;
— имеется возможность откатить алгоритм атакующего на некоторый шаг и сформировать для него новое окружение, например изменить ответ случайного оракула.

В схеме BBS применим механизм отзыва права подписи, основанный на динамических аккумуляторах [2]. Его недостаток в том, что ранее сгенерированные подписи после отзыва перестают быть корректными. Неясно также, как вынудить всех субъектов одновременно обновить локальные копии ключей, а выпускающего менеджера — всю базу данных членов группы, без которой раскрывающий менеджер не сможет раскрыть новые подписи. Все описанные проблемы носят временнòй характер.

Предлагается решать эти проблемы путем введения в схему доверенного субъекта, который выполняет различные проверки, ограничивающие возможности других субъектов, а следовательно, и потенциальных нарушителей, и заверяет обычной подписью временные метки первого ключа группы, известной части каждого членского сертификата и каждой групповой подписи. Таким образом, процесс формирования подписи стал интерактивным, так как теперь в нем принимает участие удостоверяющий центр. В этом случае проверяющий может использовать для проверки актуальный на момент создания подписи открытый ключ группы. Также новый субъект отвечает за синхронизацию всех остальных субъектов при проведении отзыва и не позволяет оставить базы данных группы в рассогласованном состоянии.

Предложенная система эффективно применима, если количество отзываемых пользователей незначительно, так как в этом случае все операции, требующие значительного времени на их выполнение, являются достаточно редкими. При этом количество отозванных пользователей никак не сказывается на сложности выполнения основных операций: формировании, проверке, раскрытии подписи и проверке правильности ее

раскрытия. Трудоемкость механизма отзыва инкапсулируется внутри группы и не делегируется третьей стороне по отношению к группе, а следовательно, и к организации.

ЛИТЕРАТУРА

1. *Васильев П. Н., Артамонов А. В., Маховенко Е. Б.* Классификационная схема групповых подписей для построения распределенных приложений // Научно-технические ведомости СПбГПУ. СПб.: Изд-во Политехнического университета, 2010. С. 71–77.
2. *Shacham H.* New paradigms in signature schemes // `http://hovav.net/dist/thesis.pdf`, 2005.
3. *Delerablee C. and Pointcheval D.* Dynamic fully anonymous short group signatures // LNCS. 2006. V. 4341. P. 193–210.
4. *Bellare M., Shi H., and Zang C.* Foundations of group signatures: the case of dynamic groups // LNCS. 2005. V. 3376. P. 136–153.
5. *Shacham H.* A Cramer — Shoup encryption scheme from the linear assumption and from progressively weaker linear variants // http://eprint.iacr.org/2007/074.pdf.

УДК 519.7

АЛГЕБРАИЧЕСКИЙ КРИПТОАНАЛИЗ ОДНОРАУНДОВОГО S-AES[1]

Р. И. Воронин

Advanced Encryption Standard (AES) — симметричный алгоритм блочного шифрования, принятый в США в качестве стандарта шифрования. AES проектировался как алгоритм, который может эффективно противостоять различным методам криптоанализа. Но в 2002 г. Николя Куртуа и Йозеф Пипджик высказали предположение о возможности алгебраической атаки на шифры с подобной AES структурой [1]. Алгебраическая атака нацелена на анализ уязвимости в математических частях алгоритма и использование его внутренних алгебраических структур. Однако об эффективности такой атаки мало что известно.

В работе исследуется применимость алгебраической атаки к упрощенному варианту S-AES, разработанному в [2]. Длина шифруемого блока и ключа равна 16 битам. Число раундов шифрования равно двум. Для анализа используются соотношения, подобные тем, которые получены в [1] для AES. Точнее, для S-блоков шифра выполнено

$$\forall x \neq 0 \quad 1 = x * y,$$
$$\forall x \quad x = y * x^2,$$
$$z = Ay \oplus b,$$

где x, z — входной и выходной векторы S-блока длины 4; y — обратный вектор к x в поле $\mathrm{GF}(2^4)$ с порождающим многочленом $\lambda^4 + \lambda + 1$; A — некоторая фиксированная матрица и b — фиксированный вектор. С помощью данных уравнений строится система относительно битов открытого текста p, шифртекста c и ключа шифрования k, полностью описывающая процесс шифрования одноразундового S-AES:

$$\sum_{i,j=0}^{15} \alpha_{ijm} p_i c_j \oplus \sum_{i,j=0}^{15} \alpha_{ijm} p_i k_j \oplus \sum_{i,j=0}^{15} \alpha_{ijm} k_i c_j \oplus \sum_{i,j=0}^{15} \alpha_{ijm} k_i k_j \oplus \sum_{i=0}^{15} \beta_{im} p_i \oplus \sum_{i=0}^{15} \beta_{im} k_i \oplus \gamma_m = 0,$$

где $m = 0, \ldots, 31$; $\alpha_{ijm}, \beta_{im}, \gamma_m \in \{0, 1\}$ определяются только структурой шифра и не зависят от выбранных значений p, c, k.

[1]Исследование выполнено при поддержке РФФИ (проект № 11-01-00997).

По сравнению с ранее предложенными в [1, 3, 4] атаками, наш подход отличается использованием двух различных пар открытых текстов/шифртекстов (p, c) и (p', c') при одном и том же ключе k, что позволяет получить систему из небольшого числа уравнений, а именно

$$\sum_{i,j=0}^{15} \alpha_{ijm}(p_i \oplus p'_i)(c_j \oplus c'_j) \oplus \sum_{i,j=0}^{15} \alpha_{ijm}(p_i \oplus p'_i)k_j \oplus \sum_{i,j=0}^{15} \alpha_{ijm}k_i(c_j \oplus c'_j) \oplus \sum_{i=0}^{15} \beta_{im}(p_i \oplus p'_i) = 0, \quad (1)$$

$m = 0, \ldots, 31$, которая является линейной относительно неизвестных битов ключа. Система содержит 32 уравнения с 16 неизвестными.

Будем говорить, что вектор длины 16 обладает дефектом, если при разбиении его на четыре подвектора длины 4 хотя бы один из них является нулевым.

Теорема 1. Пусть ключ k случаен и фиксирован. Тогда верны предложения:

(i) При случайном равновероятном выборе открытых текстов p, p' система уравнений (1) непротиворечива с вероятностью 0,6074.

(ii) При фиксированном p', таком, что $p' \oplus k$ не имеет дефекта, и случайном равновероятном выборе открытого текста p система уравнений (1) непротиворечива с вероятностью 0,7725.

Однако непротиворечивость системы еще не означает существования единственного решения. Использование столь небольшого количества уравнений позволяет в конкретных случаях проанализировать фактическую эффективность алгебраической атаки. Например, для ключа $k = 1010111111001000$ и $p' = 0110010101010101$ найдено 44 747 (68,28 %) открытых текстов p, таких, что система (1) имеет единственное решение — ключ k.

Ранее анализ упрощенного варианта AES проводился в [3, 4]. В [3] для анализа слегка измененного S-AES используются соотношение (15) и соотношения, полученные с помощью таблицы истинности S-блоков. В общей сложности один раунд шифра описывается системой из 150 уравнений с 24 переменными. После преобразования системы к линейному виду она содержит 3600 уравнений с 2324 неизвестными. Для проанализированной в [3] пары открытого текста и шифртекста алгоритм выдаёт в качестве решения 4 ключа, любой из которых является подходящим для данной пары.

В [4] проведён анализ шифра, аналогичного S-AES, с S-блоками по 3 бита. Анализ заключается в переборе всех 4 194 304 возможных квадратичных уравнений относительно переменных S-блока, выборе тех из них, которые выполняются при всех значениях входных битов S-блока и битов выхода. Найдена система из 16 383 линейно зависимых уравнений. Из неё выбрана некоторая более удобная для анализа подсистема. После преобразования подсистемы к линейному виду получена система из 392 уравнений с 164 неизвестными. В [4] приводится её решение.

Система относительно двухраундового S-AES содержит 96 квадратичных уравнений с 32 неизвестными. Использование двух различных пар открытых текстов/шифртекстов сокращает количество мономов с 232 до 160, что позволяет более эффективно применять методы, разработанные для подобных систем.

ЛИТЕРАТУРА

1. *Courtois N. and Pieprzyk J.* Cryptanalysis of Block Ciphers with Overdefined Systems of Equations // LNCS. 2002. V. 2501. P. 267–287.

2. *Mohammad M., Edward S., and Stephen W.* A simplified AES algorithm and its linear and differential cryptanalyses. // Cryptologia. 2003. No. 27. P. 148–177.

3. *Kleiman E.* The XL and XSL attacks on Baby Rijndael // Ms. Thesis. Iowa SU, USA, 2005.
4. *Бабенко Л. К., Маро Е. А.* Алгебраический анализ упрощенного алгоритма шифрования Rijndael // Известия ЮФУ. Технические науки. Тематический выпуск «Информационная безопасность». Таганрог: Изд-во ТТИ ЮФУ, 2009. №11 (100). С. 187–199.

УДК 512.62

ДИОФАНТОВОСТЬ ДИСКРЕТНОГО ЛОГАРИФМА

С. Ю. Ерофеев

Дискретный логарифм является важным математическим понятием в криптографии. Существует множество криптографических протоколов, основанных на трудности его нахождения. Достаточно упомянуть протокол разделения секретного ключа Диффи и Хеллмана, протоколы Масси — Омуры и Эль Гамаля. Многие протоколы аутентификации и цифровые подписи также имеют в основе дискретный логарифм.

Цель данной работы — дать представление дискретного логарифма в $\mathbb{Z}_p$ как диофантова множества, а также выписать явное представление соответствующего диофантова многочлена. Тогда проблема нахождения дискретного логарифма будет эквивалентна проблеме нахождения решения диофантова многочлена. Поскольку по знаменитой теореме Ю. В. Матиясевича (решение 10-й проблемы Гильберта) проблема существования решения произвольного диофантова уравнения алгоритмически неразрешима [1 – 3], указанная задача вычислительно трудна.

Определение 1. Множество $S \subseteq Z^n$ является диофантовым, если существует многочлен D с целыми коэффициентами, такой, что

$$\langle a_1, \ldots, a_n \rangle \in S \Longleftrightarrow \exists x_1, \ldots, x_m \{D(a_1, \ldots, a_n, x_1, \ldots, x_m) = 0\}.$$

Определение 2. Функция $f : \mathbb{Z}^n \to \mathbb{Z}$ является диофантовой, если ее график $\Gamma_f = \{(f(b_1, \ldots, b_n), b_1, \ldots, b_n) : (b_1, \ldots, b_n) \in \operatorname{dom} f\}$ является диофантовым множеством.

Теорема 1. Пусть даны $i, p, n \in \mathbb{N}$, p простое. Тогда если следующая система уравнений имеет решение в натуральных числах в оставшихся аргументах, то $n^k \equiv i \pmod{p}$:

$$\begin{cases} x^2 - (a^2-1)y^2 = 1, \\ u^2 - (a^2-1)v^2 = 1, \\ s^2 - (b^2-1)t^2 = 1, \\ v^2 = ry^2, \\ b = 1 + 4yo = a + qu, \\ s = x + cu, \\ t = k + 4(d-1)y, \\ y = k + e - 1, \\ (x - y(a-n) - m)^2 = (f-1)^2(2an - n^2 - 1)^2, \\ m + g = 2an - n^2 - 1, \\ w = n + h = k + l, \\ a^2 - (w^2-1)(w-1)^2 z^2 = 1, \\ m = i + pj. \end{cases}$$

Верно и обратное: если $n^{k'} \equiv i \pmod p$ для некоторого $k' \in \mathbb{N}$, то эта система уравнений имеет решение в натуральных числах, причем $k \equiv k' \pmod{p-1}$.

Следствие 1. Дискретный логарифм в $\mathbb{Z}_p$ является диофантовой функцией.

Заметим, что данное представление может быть основанием протоколов разделения ключа, аутентификации, цифровой подписи и т. п. Кроме того, оно может быть использовано с целью организации атаки на дискретный логарифм.

ЛИТЕРАТУРА

1. *Матиясевич Ю. В.* Диофантовость перечислимых множеств // Докл. АН СССР. 1970. Т. 191. № 2. С. 279–282.
2. *Матиясевич Ю. В.* Диофантово представление перечислимых предикатов // Изв. АН СССР. Сер. математ. 1971. № 35. С. 3–30.
3. *Davis M.* Hilbert's Tenth Problem is Unsolvable // Amer. Math. Monthly. 1973. V. 80. No. 3. P. 233–270.

УДК 512.54, 512.62, 519.7

ПОСТРОЕНИЕ ОДНОСТОРОННИХ ФУНКЦИЙ НА ОСНОВЕ НЕРАЗРЕШИМОСТИ ПРОБЛЕМЫ ЭНДОМОРФНОЙ СВОДИМОСТИ В ГРУППАХ

С. Ю. Ерофеев, В. А. Романьков

Односторонние функции — неотъемлемая часть криптографических схем и протоколов. Теоретически их существование до сих пор не установлено. В работах Л. А. Левина [1, 2] представлена универсальная функция, являющаяся односторонней, если существует хотя бы одна односторонняя функция.

Предлагается схема построения односторонней функции в группе с разрешимой проблемой равенства и неразрешимой проблемой эндоморфной сводимости, а также протокол аутентификации на ее основе.

Говорят, что в эффективно заданной группе G разрешима проблема эндоморфной сводимости, если существует алгоритм, определяющий по любой паре элементов $g, f \in G$, является ли f эндоморфным образом элемента g.

Существование группы G с разрешимой проблемой равенства и неразрешимой проблемой эндоморфной сводимости установлено в работах В. А. Романькова [3, 4]. А именно доказано, что указанным свойством обладают свободные метабелевы группы M_n достаточно большого ранга n и свободные нильпотентные группы N_{rc} достаточно большого ранга r и ступени нильпотентности $c \geqslant 9$.

В общих чертах схема выглядит следующим образом. В группе G выбирается элемент g, эндоморфные значения которого в фиксированной циклической подгруппе $\langle f \rangle$ кодируются наборами целых чисел $\alpha \in \mathbb{Z}^m$. Это позволяет определить функцию $\varphi : \mathbb{Z}^m \to \mathbb{Z}$. Свойства группы G позволяют рассматривать φ как одностороннюю. Для аутентификации фиксируется открытое значение $g \in M_n$ и публикуется значение $\varphi(g)$ для секретного $\varphi \in \operatorname{End} G$, $\varphi \leftrightarrow \alpha \in \mathbb{Z}^m$. Сессионная аутентификация заключается в выборе $\psi \in \operatorname{End} G$ и публикации $h = \psi(\varphi(g))$. При ответе «0» объявляется ψ и проверяется равенство для $\varphi(g)$. При ответе «1» объявляется $\varphi \circ \psi$ и проверяется равенство для g.

Однако в указанной схеме, предложенной в работе Д. Григорьева и В. Шпильрайна [5] и основанной на идее В. А. Романькова, имеется существенная слабость.

Для ее надежности требуется неразрешимость проблемы эндоморфизма для образов, в частности для $\varphi(G)$.

Основным результатом настоящей работы является следующая теорема.

Теорема 1. В свободной метабелевой группе M_n достаточно большого ранга неразрешима проблема двукратной эндоморфной сводимости.

Теорема позволяет ликвидировать указанную слабость протокола аутентификации.

ЛИТЕРАТУРА

1. *Levin L. A.* One-way Functions and Pseudorandom Generators // Combinatorica. 1987. V. 7. No. 4. P. 357–363.
2. *Левин Л. А.* Односторонние функции // Проблемы передачи информации. 2003. Т. 39. № 1. С. 103–117.
3. *Романьков В. А.* Об уравнениях в свободных метабелевых группах // Сибирский математический журнал. 1979. Т. 20. № 3. С. 671–673.
4. *Романьков В. А.* О неразрешимости проблемы эндоморфной сводимости в свободных нильпотентных группах и в свободных кольцах // Алгебра и логика. 1977. Т. 16. № 4. С. 457–471.
5. *Grigoriev D. and Shpilrain V.* Zero-knowledge authentication schemes from actions on graphs, groups, or rings // Ann. Pure Appl. Logic. 2010. No. 162. P. 194–200.

УДК 004.056.55

РЕАЛИЗАЦИЯ НА ПЛИС ШИФРА FAPKC[1]

Д. С. Ковалев, В. Н. Тренькаев

Существует немного асимметричных шифров (RSA, El-Gamal, ECC), которые используются на практике. Основным их недостатком является низкое быстродействие. При этом потребность в быстродействующих шифрах с небольшой длиной ключа остается. В частности, это актуально для устройств с ограниченными ресурсами. В работе исследуется автоматный ассиметричный шифр FAPKC (Finite Automata Public Key Cryptosystem) [1 – 3] на пригодность к практическому использованию.

В шифре FAPKC используются обратимые с задержкой автоматы, т. е. автоматы, у которых входное слово восстанавливается по выходному с задержкой на несколько тактов работы, а также автоматы с конечной памятью, значение выходного символа для которых зависит от значений конечного количества входных и выходных символов в предыдущие такты работы. Закрытый ключ состоит из двух обратимых автоматов A и B (нелинейного с задержкой 0 и линейного с задержкой τ соответственно), обратные к которым могут быть построены с полиномиальной сложностью. Открытый ключ есть последовательная композиция автоматов A и B при известном начальном состоянии. При этом по выбранному состоянию композиции вычисляются начальные состояния A и B. При шифровании к открытому тексту добавляются произвольные τ символов. Шифртекст есть реакция автомата открытого ключа в выбранном начальном состоянии на «расширенное» входное слово. Таким образом, длина шифртекста увеличивается на τ символов по сравнению с открытым текстом. При расшифровании сначала находится реакция β автомата, обратного к B, в его начальном состоянии

[1]Работа выполнена в рамках реализации ФЦП «Научные и научно-педагогические кадры инновационной России» на 2009–2013 гг. (гос. контракт № П1010).

на зашифрованное слово. Исходный открытый текст получается как реакция автомата, обратного к A, в его начальном состоянии на входное слово β. Стойкость FAPKC основана на сложности решения задачи декомпозиции нелинейного обратимого с задержкой автомата с конечной памятью.

Цель данной работы — изучение вопросов эффективности аппаратной реализации шифра FAPKC на базе программируемых логических интегральных схем (ПЛИС). Проведены исследования по выявлению зависимости количества используемых ресурсов и производительности ПЛИС от параметров шифрсистемы (длины ключа, размерности линейного пространства, задержки шифрующего автомата, стойкости к различным атакам), а также сравнение ПЛИС-реализаций шифров FAPKC и RSA.

В частности, в САПР Xilinx WebPack ISE реализован оценочный вариант шифра FAPKC на ПЛИС Spartan-3 XC3S1500, для которого выявлена зависимость ресурсоемкости и быстродействия от задержки, величина которой изменялась от 32 до 160. Оказалось, что увеличение задержки, а следовательно, длины ключа существенно влияет (в сторону увеличения) только на число используемых ресурсов ПЛИС, в то время как максимальная рабочая частота ПЛИС убывает незначительно. Проведено сравнение шифра RSA-1024 [4] с вариантом FAPKC той же стойкости, результатом которого является утверждение о том, что использование шифра FAPKC предпочтительней как с точки зрения производительности, так и с точки зрения числа используемых ресурсов. При этом коэффициент эффективности ПЛИС-реализации FAPKC (отношение производительности к количеству используемых ресурсов) на порядок лучше этого показателя для RSA. В целом, проведённые исследования показывают, что шифр FAPKC, реализованный на ПЛИС, пригоден для использования на практике и по сравнению с RSA имеет существенно более высокое быстродействие и меньшую ресурсоемкость.

ЛИТЕРАТУРА

1. *Bao F. and Igarashi Y.* Break Finite Automata Public Key Cryptosystem // LNCS. 1995. No. 944. P. 147–158.
2. *Dai Z. D., Ye D. F., and Lam K. Y.* Weak Invertibility of Finite Automata and Cryptanalysis on FAPKC // LNCS. 1998. No. 1514. P. 227–241.
3. *Tao R. J.* Finite Automata and Application to Cryptography. Tsinghua University Press and Springer, 2008.
4. *Wollinger T., Guajardo J., and Paar C.* Cryptography on FPGAs: State of the art implementations and attacks // ACM Trans. Embedded Computing Systems. 2004. V. 3. Iss. 3. P. 534–574.

УДК 003.26

БЕЗОПАСНОСТЬ РЕЖИМОВ ШИФРОВАНИЯ ГОСТ 28147-89

И. А. Кукало

Отечественный алгоритм криптографического преобразования ГОСТ 28147-89 является единственным алгоритмом симметричного шифрования, разрешенным к использованию на территории РФ. Стандарт ГОСТ 28147-89 определяет алгоритм шифрования $E : K \times \{0,1\}^{64} \to \{0,1\}^{64}$, три режима симметричного шифрования $SE = (k, \varepsilon, D)$ с соответствующими уравнениями шифрования ε и расшифрования D, а также режим выработки имитовставки. С момента опубликования и перевода стандарта на английский язык в отечественной и зарубежной литературе появилось боль-

шое количество работ, посвященных анализу криптостойкости *алгоритма* шифрования ГОСТ 28147-89. Однако оценка криптостойкости *режимов* шифрования, определенных в стандарте, до настоящего времени не проводилась, хотя, согласно [1], данная задача является актуальной для современной криптографии.

Согласно [2], основным показателем криптостойкости режимов шифрования является возможность адаптивной атаки по выбранным открытым текстам (IND-CPA). Данный показатель ориентирован на практическую оценку безопасности режима шифрования [3] против злоумышленника с ограниченными ресурсами.

Пусть $SE = (k, \varepsilon, D)$ — произвольный режим шифрования [2] и A — злоумышленник, который передает специальной подпрограмме-оракулу (ППО) множество пар сообщений $(M_{0,1}, M_{1,1}), \ldots, (M_{0,q}, M_{1,q})$ одинаковой длины. ППО возвращает злоумышленнику набор шифртекстов $C_1, \ldots, C_q$ в соответствии с экспериментами:

— для $\mathrm{Exp}_{SE}^{\text{ind-cpa-1}}$ элемент C_i является шифртекстом сообщения $M_{1,i}$, $1 \leqslant i \leqslant q$;
— для $\mathrm{Exp}_{SE}^{\text{ind-cpa-0}}$ элемент C_i является шифртекстом сообщения $M_{0,i}$, $1 \leqslant i \leqslant q$.

Определение 1. Определим возможность адаптивной атаки по выбранным открытым текстам как

$$\mathrm{Adv}_{SE}^{\text{ind-cpa}}(A) = \Pr[\mathrm{Exp}_{SE}^{\text{ind-cpa-1}}(A) = 1] - \Pr[\mathrm{Exp}_{SE}^{\text{ind-cpa-0}}(A) = 1],$$

где $\Pr[\mathrm{Exp}_{SE}^{\text{ind-cpa-1}}(A) = 1]$ — вероятность события, при котором злоумышленник A считает, что ППО зашифровал сообщения $M_{1,i}$ для эксперимента $\mathrm{Exp}_{SE}^{\text{ind-cpa-1}}(A)$; $\Pr[\mathrm{Exp}_{SE}^{\text{ind-cpa-0}}(A) = 1]$ — вероятность события, при котором злоумышленник A считает, что ППО зашифровал сообщения $M_{1,i}$ для эксперимента $\mathrm{Exp}_{SE}^{\text{ind-cpa-0}}(A)$.

Режим шифрования является безопасным при $\mathrm{Adv}_{SE}^{\text{ind-cpa}}(A) \to 0$. Определены значения $\mathrm{Adv}_{SE}^{\text{ind-cpa}}$ для всех режимов работы ГОСТ 28147-89, обеспечивающих конфиденциальность обрабатываемой информации. Модель злоумышленника A определяется количеством σ запросов к ППО. Безопасность алгоритма шифрования определяется показателем псевдослучайности функции шифрования $\mathrm{Adv}_{E}^{\text{prf}}(B)$ [2]. Теоретические результаты приведены в табл. 1.

Таблица 1

Теоретические характеристики криптостойкости отечественных режимов шифрования

Название режима шифрования	Теоретическое значение $\mathrm{Adv}_{SE}^{\text{ind-cpa}}$
Простой замены	1
Гаммирования	$\mathrm{Adv}_{\text{GOST}}^{\text{prf}}(B) + 2\sigma^2/2^{64}$
Гаммирования с обратной связью	$\mathrm{Adv}_{\text{GOST}}^{\text{prf}}(B) + \sigma^2/2^{64}$

Практические значения $\mathrm{Adv}_{SE}^{\text{ind-cpa}}$ приведены в табл. 2 и рассчитываются при допущении, что наилучшей атакой на алгоритм шифрования в ГОСТ является атака, основанная на парадоксе дней рождения [1].

Значение σ соответствует количеству блоков данных, зашифрованных ППО, и позволяет определить продолжительность сессии защищенного обмена данными в системах криптографической защиты информации. Таким образом,

— для режима простой замены безопасным является шифрование данных размером в один блок, т. е. 64 бита, или 8 байт;

— для режима гаммирования безопасным является шифрование данных размером 2^{31} блоков, т. е. 16 Гбайт;
— для режима гаммирования с обратной связью безопасным является шифрование данных размером $\sqrt{2^{64}/3}$ блоков, т. е. $\approx 18{,}475$ Гбайт.

Таблица 2

Практические характеристики криптостойкости отечественных режимов шифрования

Название режима шифрования	Практическое значение $\mathrm{Adv}_{SE}^{\text{ind-cpa}}$	Значение σ, обеспечивающее криптостойкость
Простой замены	1	1
Гаммирования	$\leqslant 4\sigma^2/2^{64}$	$\leqslant 2^{31}$
Гаммирования с обратной связью	$\leqslant 3\sigma^2/2^{64}$	$\leqslant \sqrt{2^{64}/3}$

ЛИТЕРАТУРА

1. *Bellare M. and Rogaway P.* Introduction to Modern Cryptography. 2005. `http://cseweb.ucsd.edu/~mihir/cse207/w-se.pdf`
2. *Goldwasser S. and Bellare M.* Lecture Notes on Cryptography. 2001. `http://cseweb.ucsd.edu/~mihir/papers/gb.pdf`
3. *Katz J. and Yehuda L.* Introduction to Modern Cryptography. Boca Raton: Chapman& Hall/CRC, 2008.

УДК 519.7

О ВЫБОРЕ СЛАЙДОВЫХ ПАР В КОРРЕЛЯЦИОННОМ МЕТОДЕ КРИПТОАНАЛИЗА ШИФРА KeeLoq

О. Н. Лебедева

KeeLoq — блочный шифр, широко используемый в системах бесключевого удалённого доступа. Шифр был разработан профессором Г. Каном и запатентован Южно-Африканской компанией «Nanoteq» в середине 80-х. В 1995 г. фирма «MICROCHIP» приобрела KeeLoq у фирмы «Nanoteq» вместе с лицензионными правами.

Алгоритм KeeLoq [1] имеет 64-битный ключ и осуществляет шифрование 32-битных блоков открытого текста. В нём используются два регистра сдвига: один — длины 64 без функции обратной связи (для выработки подключа), другой — регистр сдвига длины 32 с нелинейной функцией обратной связи NLF от пяти переменных (непосредственно для шифрования). Блок открытого текста помещается в текстовый регистр. Шифртекстом является состояние регистра после 528 циклов с использованием регистра ключа. Пусть $V_n = \mathrm{GF}_2^n$ — множество всех n-битных слов; $Y^{(i)} = (y_{31}^{(i)}, \ldots, y_0^{(i)}) \in \in V_{32}$ и $K^{(i)} = (k_{63}^{(i)}, \ldots, y_0^{(i)}) \in V_{63}$ — соответственно состояния текстового регистра и регистра ключа после i тактов. Каждый цикл шифрования может быть описан следующим образом:

— вычисление очередного бита: $\varphi = NLF(y_{31}^{(i)}, y_{26}^{(i)}, y_{20}^{(i)}, y_9^{(i)}, y_1^{(i)}) \oplus y_{16}^{(i)} \oplus y_0^{(i)} \oplus k_0^{(i)}$;
— сдвиг состояния текстового регистра: $R^{(i+1)} = (\varphi, y_{31}^{(i)}, \ldots, y_1^{(i)})$;
— сдвиг состояния регистра ключа: $K^{(i+1)} = (k_0^{(i)}, k_{63}^{(i)}, \ldots, k_1^{(i)})$.

Первый криптоанализ KeeLoq был опубликован только в феврале 2007 г. А. Богдановым [1]. Эта атака основана на слайдовой технике и линейном приближении нелинейной булевой функции, использующейся в KeeLoq. Криптоанализ имеет временную

сложность 2^{52} и требует 16 Гбайт памяти. Позднее Богданов обновил свой метод, используя алгебраический криптоанализ для нахождения первых 16 битов ключа [2]. Улучшение привело к уменьшению временной сложности до $2^{50,6}$.

В работе [1] Богданов описывает следующие шаги. Для каждого подключа $K' = (k_{15}, \ldots, k_0)$ и случайного 32-битного входа $I_0 \in V_{32}$ с помощью парадокса дней рождения угадывается промежуточный шифртекст $O_0 \in V_{32}$ после 64 циклов шифрования. Такая пара (I_0, O_0) называется *слайдовой парой*. Используя периодическую структуру ключа, в KeeLoq генерируются другие пары $(I_i, O_i) \in (V_{32})^2, i = 1, \ldots, N-1$. Для успешной атаки их число должно быть около 2^8. Для каждого такого набора пар получаются линейные соотношения для неизвестных битов ключа с высокой вероятностью в связи с тем, что нелинейная функция обратной связи, использующаяся в KeeLoq, не является 2-устойчивой. Таким образом, можно определить $(k_{47}, \ldots, k_{16})$ бит за битом. После этого решается треугольная система линейных уравнений для оставшихся битов ключа $(k_{63}, \ldots, k_{48})$.

Отметим, что в методе А. Богданова для каждого подключа $K' = (k_{15}, \ldots, k_0)$ по сути происходит полный перебор всевозможных пар (кандидатов на первую слайдовую пару (I_0, O_0)) из случайного подмножества мощности 2^{16} множества всех двоичных векторов длины 32 и для каждой такой пары (I_0, O_0) выполняется корреляционный криптоанализ.

В данной работе предлагается на каждом шаге корреляционной атаки использовать найденные биты ключа для отсеивания неподходящих пар, а именно можно найти вероятностное соотношение между битами из правильной слайдовой пары и битами ключа, проверка которого позволяет для части неправильных пар остановить выполнение корреляционного криптоанализа уже на этом шаге. В этом соотношении используется линейное приближение нелинейной функции NLF, выполняющееся с вероятностью $5/8$.

Например, связь бита $y_0^{(64)}$ с битами на 16-м раунде выражается так:

$$y_0^{(64)} = y_{31}^{(33)} = NLF(y_{31}^{(32)}, y_{26}^{(32)}, y_{20}^{(32)}, y_9^{(32)}, y_1^{(32)}) \oplus y_{16}^{(32)} \oplus y_0^{(32)} \oplus k_{32} =$$
$$= y_1^{(32)} \oplus y_9^{(32)} \oplus y_{16}^{(32)} \oplus y_0^{(32)} \oplus k_{32} = y_{17}^{(16)} \oplus y_{25}^{(16)} \oplus y_{31}^{(17)} \oplus y_{16}^{(16)} \oplus k_{32} =$$
$$= y_{17}^{(16)} \oplus y_{25}^{(16)} \oplus (NLF(y_{31}^{(16)}, y_{26}^{(16)}, y_{20}^{(16)}, y_9^{(16)}, y_1^{(16)}) \oplus y_{16}^{(16)} \oplus y_0^{(16)} \oplus k_{16}) \oplus y_{16}^{(16)} \oplus k_{32}.$$

Таким образом, после того как будут найдены k_{16} и k_{32} на первом шаге корреляционной атаки, для отсеивания неправильных слайдовых пар используются биты ключа $(k_{16}, k_{15}, \ldots, k_0)$ и k_{32}.

На каждом шаге корреляционной атаки используется дополнительное соотношение для битов входного и выходного текста, что позволяет останавливать криптоанализ с вероятностью $5/8$ для каждой пары, которая не удовлетворяет полученным соотношениям. Следующая таблица иллюстрирует этот процесс.

Шаг	0	1	2	...	15	16
Количество слайдовых пар	2^{32}	2^{31}	2^{30}	...	2^{17}	2^{16}
Найденные биты ключа	$k_{15}, \ldots, k_0$	k_{16}, k_{32}	k_{17}, k_{33}	...	k_{30}, k_{46}	k_{31}, k_{47}

Во второй строке указано количество пар, для которых будет выполняться следующий шаг корреляционного анализа. Например, изначально понадобится перебор 2^{32} пар. Затем находятся биты ключа k_{16} и k_{32} на первом шаге корреляционной атаки, которые используются в соотношении между $y_0^{(64)}$ и битами шифртекста после 16 циклов. Значит, можно не рассматривать пары, не удовлетворяющие этому соотношению.

Следовательно, число пар, для которых будет выполняться следующий шаг криптоанализа, сократится до 2^{31}, и т. д.

При выборе другого приближения нелинейной функции NLF можно добиться повышения вероятности нахождения правильной слайдовой пары.

В дальнейшем необходимо определить параметры улучшенного метода криптоанализа: временную сложность, требуемую память и т. д.

ЛИТЕРАТУРА

1. *Bogdanov A.* Cryptanalysis of the KeeLoq Block cipher // `http://eprint.iarc.org/2007/055`, 2007.
2. *Bogdanov A.* Attack on the KeeLoq Block Cipher and Authentication System // `http://rfidsec07.etsit.uma.es/slides/papers/paper-22.pdf`, 2007.

УДК 519.7

О НЕВОЗМОЖНЫХ УСЕЧЁННЫХ РАЗНОСТЯХ XSL-АЛГОРИТМОВ БЛОЧНОГО ШИФРОВАНИЯ

М. А. Пудовкина

Идея использовать невозможные разности, т. е. разности с нулевой вероятностью, для определения ключа шифрования была предложена Л. Р. Кнудсеном [1] при анализе алгоритма блочного шифрования DEAL. Позже невозможные разности применялись для атак на алгоритмы блочного шифрования Skipjack [2], MISTY1 [3], AES [4], ARIA [5] и др.

Пусть $X^{\times} = X\backslash\mathbf{0}$; $S(X)$ — множество всех подстановок на множестве X; V_t — множество всех t-мерных векторов над $\mathrm{GF}(2)$; $m = d \cdot q$; $\tilde{s}_0, \ldots, \tilde{s}_{q-1} \in S(V_d)$; $H_d \in \in \left\{V_d, \mathrm{GF}(2^d)\right\}$; $\tilde{\alpha} \in V_d$; нелинейное преобразование $s : V_m \to V_m$ есть $s = (\tilde{s}_{q-1}, \ldots, \tilde{s}_0)$, где $\tilde{s}_i \in S(V_d)$; линейное преобразование $a : H_d^q \to H_d^q$ в стандартном базисе задаётся как

$$(\alpha_{q-1,i}, \ldots, \alpha_{0,i})\,\mathbf{a} = \left(\alpha'_{q-1,i}, \ldots, \alpha'_{0,i}\right),$$

где $\mathbf{a} = (a_{ij})$ — обратимая $(q \times q)$-матрица над $\mathrm{GF}(2)$ $(\mathrm{GF}(2^d))$; $\mathbf{a}^{-1} = \mathbf{b} = (b_{ij})$;

$$A^{(j)} = \{i \in \{0, ..., q-1\} : a_{ji} > 0\}, \quad B^{(j)} = \{i \in \{0, ..., q-1\} : b_{ji} > 0\}.$$

В работе рассматриваются алгоритмы блочного шифрования с раундовой функцией $g_\beta : V_m \to V_m$, заданной как $\alpha^{g_\beta} = (\alpha \oplus \beta)^{sa}$ для всех $\beta, \alpha \in V_m$, и $f_{(k_1,\ldots,k_j)} = = g_{k_1} \ldots g_{k_j}$ — j-раундовая функция зашифрования. Предполагается, что раундовые ключи $k_1, \ldots, k_l$ выбираются случайно и равновероятно из V_m.

Зафиксируем номера координат $\{j_1, \ldots, j_c\} \subset \{0, \ldots, q-1\}$, $j_1 < \ldots < j_c$. Положим

$$\Lambda(j_1, \ldots, j_c) = \{\alpha \in H_d^q : \tilde{\alpha}_{j_t} \neq 0,\ t = 1, \ldots, c\}.$$

Множество разностей $(\Lambda(j_1, \ldots, j_c), \Lambda(i_1, \ldots, i_{t'}))$ называется невозможной усечённой разностью для преобразования $v \in S(V_m)$, если для любых векторов $\alpha \in \in \Lambda(j_1, \ldots, j_c)$, $\beta \in \Lambda(i_1, \ldots, i_{t'})$ выполняется равенство $p_{\alpha,\beta}(v) = 0$, где

$$p_{\alpha,\beta}(v) = 2^{-m} \cdot |\{\lambda \in V_m : (\lambda \oplus \alpha)^v \oplus \lambda^v = \beta\}|.$$

В этом случае при $v = f_{(k_1,\ldots,k_j)}$ будем использовать обозначение

$$\Lambda(j_1, \ldots, j_c) \not\twoheadrightarrow_j \Lambda(i_1, \ldots, i_{t'}).$$

Покажем, что для большого класса XSL-алгоритмов блочного шифрования существуют 3-раундовые невозможные разности.

Утверждение 1. Пусть $\mathbf{a}$ — такая произвольная обратимая $(q \times q)$-матрица над полем GF(2) (GF(2^d)), что по крайней мере один элемент в столбце $a_t^{\downarrow}$ или $b_t^{\downarrow}$ равен нулю для некоторого $t \in \{0, \ldots, q-1\}$. Тогда существует 3-раундовая невозможная усечённая разность $\Lambda(i) \not\twoheadrightarrow_3 \Lambda(j)^a$ для некоторых $i, j \in \{0, \ldots, q-1\}$.

Таким образом, для любой обратимой матрицы $\mathbf{a}$ над полем GF(2) в алгоритме шифрования XSL существует 3-раундовая усечённая невозможная разность, а значит, и просто 3-раундовая невозможная разность. Это следует из того, что если все элементы матрицы $\mathbf{a}$ равны единице, то она является необратимой. Приведём условия, при которых существуют 4-раундовые невозможные усечённые разности.

Утверждение 2. Пусть $i, j \in \{0, \ldots, q-1\}$. Пусть также для всех $\tilde{\alpha}_t'' \in V_d^{\times}$, $t \in A^{(i)}$, $c \in \{0, \ldots, q-1\}$ не выполняются одновременно следующие равенства:

1) $\bigoplus\limits_{t \in A^{(i)}} \tilde{\alpha}_t'' a_{tc} = \tilde{0}$ для всех $c \notin B^{(j)}$;

2) $\bigoplus\limits_{t \in A^{(i)}} \tilde{\alpha}_t'' a_{tc} \neq \tilde{0}$ для всех $c \in B^{(j)}$.

Тогда $\Lambda(i) \not\twoheadrightarrow_4 \Lambda(j)^a$.

Следствие 1. Пусть $i, j \in \{0, ..., q-1\}$. Пусть также для всех $\tilde{\beta}_t'' \in V_d^{\times}$, $t \in B^{(j)}$, $c \in \{0, ..., q-1\}$ не выполняются одновременно следующие равенства:

1) $\bigoplus\limits_{t \in B^{(i)}} \tilde{\beta}_t'' \cdot b_{tc} = \tilde{0}$ для всех $c \notin A^{(i)}$;

2) $\bigoplus\limits_{t \in B^{(i)}} \tilde{\beta}_t'' \cdot b_{tc} \neq \tilde{0}$ для всех $c \in A^{(j)}$.

Тогда $\Lambda(i) \not\twoheadrightarrow_4 \Lambda(j)^a$.

Приведены примеры 4-раундовых усечённых разностей для некоторых алгоритмов блочного шифрования. Отметим, что утверждения 3, 4, 5 работы [6] являются следствием п. 1 утверждения 2.

ЛИТЕРАТУРА

1. *Knudsen L. R.* DEAL — A 128-bit Block Cipher // Technical Report Department of Informatics. University of Bergen, Norway, 1998.
2. *Biham E., Biryukov A., and Shamir A.* Cryptanalysis of Skipjack Reduced to 31 Rounds Using Impossible Differentials // LNCS. 1999. V. 2595. P. 12–23.
3. *Dunkelman O. and Keller N.* An Improved Impossible Differential Attack on MISTY1 // LNCS. 2008. V. 5350. P. 441–454.
4. *Lu J., Dunkelman O., Keller N., and Kim J.* New Impossible Differential Attacks on AES // LNCS. 2008. V. 5365. P. 279–293.
5. *Li R., Sun B., Zhang P., and Li C.* New Impossible Differential Cryptanalysis of ARIA // Cryptology ePrint Archive, Report 2008/227. `http://eprint.iacr.org/2008/227`
6. *Li R., Sun B., and Li C.* Impossible Differential Cryptanalysis of SPN Ciphers // Cryptology ePrint Archive, Report 2010/307. `http://iacr.org/2010/307`