Если в структуре доступа СРС есть незаменимые участники, т. е. те, которые входят во все разрешённые коалиции, то основная идея СРС — восстановление секрета в отсутствие каких-либо участников — не работает. Незаменимость участника означает, что, какова бы ни была доля секрета, выдаваемая этому участнику, без его участия в восстановлении секрета не обойтись. Незаменимые участники фактически обладают теми же правами, что и дилер, хранитель секрета, и ассоциируются с ним. Они обладают «правом вето», т. е. без них ничего не решится. Итак, для разделения незаменимых участников необходимо, чтобы был цикл, содержащий по отдельности каждого из этих двух участников. Этим доказано

Утверждение 1. В матроиде, соответствующем СРС, нет незаменимых участников тогда и только тогда, когда для любых $x \neq y$ существует разделяющий их цикл C, т. е. $x \notin C$, $y \in C$.

Назовём такие матроиды разделяющими.

Матроид назовем почти пороговым, если все его циклы имеют мощность n, но, возможно, не все его n-элементные подмножества — циклы. Путём комбинаторных рассуждений доказано

Утверждение 2. Для мощностей цикла 1, 2 и 3 связного почти порогового непорогового матроида не существует.

Разграничение доступа к информации в компьютерных системах естественным образом, путём рассмотрения битовых строк, приводит к бинарным матроидам, т. е. матроидам, реализующимся как векторные над полями характеристики два. На этом пути удаётся построить связный почти пороговый непороговый матроид с мощностью цикла 4. Рассмотрением фактор-групп группы кода СРС получена обобщающая

Теорема 1. Бинарные связные разделяющие почти пороговые матроиды исчерпываются матроидами, соответствующими кодам Рида — Маллера первого порядка.

ЛИТЕРАТУРА

1. Доктрина информационной безопасности [Электронный ресурс]. `http://www.rg.ru/oficial/doc/min_and_vedom/mim_bezop/doctr.shtm`.
2. Введение в криптографию / под общ. ред. В. В. Ященко. СПб.: Питер, 2001. 288 с.
3. *Медведев Н. В., Титов С. С.* Почти пороговые схемы разделения секрета на эллиптических кривых // Доклады ТУСУРа. 2011. №1(23). С. 91–96.
4. *Гайдамакин Н. А.* Разграничение доступа к информации в компьютерных системах. Екатеринбург: Изд-во Урал. ун-та, 2003. 328 с.
5. *Медведев Н. В., Титов С. С.* О топологии эллиптических кривых // Тр. Ин-та математики и механики УрО РАН. 2012. Т. 18. №1. С. 242–250.
6. *Логачев О. А., Сальников А. А., Ященко В. В.* Булевы функции в теории кодирования и криптологии. М.: МЦНМО, 2004. 470 с.

УДК 681.326; 531.19

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ГЕНЕРАТОРА СЛУЧАЙНЫХ ЧИСЕЛ НА ОСНОВЕ ТРЁХЗНАЧНОЙ ЛОГИКИ

Е. Л. Столов

В последнее время созданы простые физические устройства, реализующие трёхзначную логику [1], что стимулирует разработку физических схем, работающих

в этой логике. Физические генераторы случайных последовательностей дают пример устройств, применение в которых k-значных логик увеличивает производительность устройства. Подобного рода схемы используются при генерации криптографических ключей. Как правило, требуется, чтобы выходная последовательность имела равномерное распределение, поскольку из него можно получить любое другое распределение стандартным образом.

Рассмотрим схему, представленную на рис. 1. Здесь F — комбинационная схема (блок) с двумя входами и одним выходом, работающая в трёхзначной логике, то есть входные и выходные сигналы принадлежат множеству $M = \{0, 1, 2\}$. Число блоков может быть произвольным, а способ их соединения вытекает из рисунка. Функционирование блока F определено следующим образом:

$$c = F(a, b), \quad \forall a, b \ (c \neq a, c \neq b). \tag{1}$$

Равенства (1) задают значения функции для неравных аргументов. Если аргументы совпадают, то $F(0, 0) = 1, F(1, 1) = 2, F(2, 2) = 0$. Функцию F можно заменить любой функцией вида $\sigma(F(\sigma(a), \sigma(b))$, где σ — любая перестановка чисел 0, 1, 2.

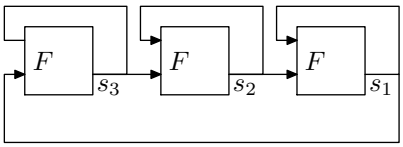

Рис. 1. Пример генератора случайных последовательностей, реализованного на трёх блоках

Схема работает следующим образом. В начальный момент времени на входах блоков находятся произвольные сигналы из множества M. Каждый из блоков срабатывает через случайный момент времени и изменяет свой выход. В результате вся схема переходит в режим хаотического генератора. Состоянием схемы (генератора) в момент времени t является набор выходов всех блоков в этот момент. Таких состояний конечное число, и каждое из них получает некоторый номер.

Для исследования свойств предложенного устройства нужно сделать дополнительные предположения. Будем следовать модели, предложенной в работе [2], где рассмотрена модель генератора, работающего в двоичной логике:

1) время срабатывания блока является случайной величиной, имеющей экспоненциальное распределение с одним параметром λ;
2) никакие два блока не могут сработать одновременно;
3) времена срабатывания блоков являются независимыми случайными величинами.

Обозначим через $S(t)$ состояние генератора в момент времени t. В этом случае $S(t)$ есть марковский процесс, и поведение системы описывается уравнениями Эрланга

$$\frac{dP(t)}{dt} = P(t)A,$$

где A — постоянная матрица, а компонента $P_n(t)$ есть вероятность того, что в момент времени t генератор находится в состоянии с номером n (см., например, [3]). Из определения функции F и способа соединения блоков следует, что в схеме отсутствуют состояния, из которых схема не сможет выйти. Состояния вида $(a, a, \ldots, a)$, $a \in M$, являются недостижимыми, поэтому исключим их из рассмотрения.

Теорема 1. Марковский процесс имеет единственное финальное распределение вероятностей, и на выходе каждого блока сигнал имеет равномерное распределение.

Даются оценки интервала времени между двумя съёмами сигналов, обеспечивающего независимость этих сигналов.

Подробное изложение представленных результатов можно найти в [4].

ЛИТЕРАТУРА

1. *Sheng L., Yong-Bin K., and Lombardi F.* CNTFET-Based Design of Ternary Logic Gates and Arithmetic Circuits // IEEE Trans. Nanotechnology. 2011. V. 10. No. 2. P. 217–225.
2. *Кузнецов В. М., Песошин В. А., Столов Е. Л.* Марковская модель цифрового стохастического генератора // АиТ. 2008. № 9. С. 62–68.
3. *Хинчин А. Я.* Работы по математической теории массового обслуживания. М.: Физматгиз, 1963. 236 с.
4. *Столов Е. Л.* Математическая модель генератора случайных чисел на основе трёхзначной логики // Прикладная дискретная математика. 2012. № 2(12). С. 43–49.

УДК 519.7

ОДНОРАЗОВАЯ КОЛЬЦЕВАЯ ПОДПИСЬ И ЕЁ ПРИМЕНЕНИЕ В ЭЛЕКТРОННОЙ НАЛИЧНОСТИ

Г. О. Чикишев

Кольцевая подпись (*ring signature*) [1] позволяет участнику группы подписывать сообщения от имени всей группы (указывая для проверки вместо своего открытого ключа ключи всех участников группы). Проверяющий уверен, что использован один из секретных ключей, но чей именно — он не знает. В работе мы вводим новый вид кольцевой подписи, наделяя её свойством одноразовости: в случае повторного использования одного и того же секретного ключа личность его автора будет раскрыта (иными словами, анонимно подписать можно лишь одно сообщение).

Такое свойство востребовано во многих областях: электронные выборы (каждый участник может проголосовать только один раз), цифровые деньги (электронные монеты можно потратить лишь единожды) и т. д. Продемонстрируем применение алгоритма в сфере открытых электронных транзакций на примере децентрализованной p2p-валюты Bitcoin [2]. Это решение позволяет участнику совершать полностью неотслеживаемый платёж (что на данный момент невозможно в Bitcoin), открыто публикуя детали операций по переводу и получению средств.

Алгоритм одноразовой кольцевой подписи состоит из нескольких этапов:

— **GEN** — генерация ключей. Каждый участник готовит два закрытых ключа $0 < x, y < N$ и публикует два открытых ключа $P_x = xQ_x$ и $P_y = yQ_y$ электронной подписи ECDSA.

— **RING-SIG** — создание кольца подписей. Алиса готовит $n-1$ «подделку» чужих подписей ECDSA (m_i, A_i, β_i), применяя технику «2-parameter forgery» [3]:

$$A_i = u_i Q_x + v_i P_{x_i}; \quad \beta_i = -\mathcal{H}(A_i) \cdot v_i^{-1} \bmod N; \quad m_i = u_i \cdot \beta_i \bmod N,$$

и выбирает такое m_{i_s}, чтобы все m_i рекуррентно замкнулись в кольцо

$$z_{i_0} = \mathcal{H}\left(m, m_{i_0+n-1} \oplus \mathcal{H}(m, m_{i_0+n-2} \oplus \mathcal{H}(m, \cdots \oplus \mathcal{H}(m, m_{i_0} \oplus z_{i_0}) \cdots))\right) \qquad (1)$$

для произвольно выбранного $i_0 \in \{1, \ldots, n\}$.