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).