4. *Александрович А. Е., Бородакий Ю. В., Чуканов В. О.* Проектирование высоконадежных информационно-вычислительных систем. М.: Радио и связь, 2004.
5. *Коваленко И. Н., Кузнецов Н. Ю.* Методы расчета высоконадежных систем. М.: Радио и связь, 1988.
6. *Половко А. М., Маликова И. М.* Сборник задач по теории надежности. М.: Советское радио, 1972.
7. *Половко А. М., Гуров С. В.* Основы теории надежности. СПб.: БХВ-Петербург, 2006.
8. *Майерс Г.* Надежность программного обеспечения. М.: Мир, 1980.
9. *Боэм Б., Браун Дж., Каспар Х. и др.* Характеристики качества программного обеспечения. М.: Мир, 1981.
10. *Тейер Т., Липов М., Нельсон Э.* Надежность ПО. М.: Мир, 1981.
11. *Липаев В. В.* Надежность программных средств. М.: СИНТЕГ, 1998.

REFERENCES:

1. *Azymshin I. M., Chukanov V. O.* Analysis of safety of software // Bezopasnost Informatsionnykh Tekhnology. 2014. № 1. P. 45–47.
2. *Chukanov V. O.* Nadezhnost programmnogo obespecheniya i apparatnykh sredstv sistem peredachi dannykh atomnykh elektrostantsy: Uchebnoye posobiye. M.: MEPhI, 2008.
3. *Gurov V. V., Chukanov V. O.* Osnovy teorii i organizatsii EVM. M.: BINOM. Laboratoriya znany, 2012.
4. *Aleksandrovich A. E., Borodaky Yu. V., Chukanov V. O.* Proyektirovaniye vysokonadezhnykh informatsionno-vychislitelnykh sistem. M.: Radio i svyaz, 2004.
5. *Kovalenko I. N., Kuznetsov N. Yu.* Metody rascheta vysokonadezhnykh sistem. M.: Radio i svyaz, 1988.
6. *Polovko A. M., Malikova I. M.* Sbornik zadach po teorii nadyozhnosti. M.: Sovetskoye radio, 1972.
7. *Polovko A. M., Gurov S. V.* Osnovy teorii nadyozhnosti. SPb.: BKhV-Peterburg, 2006.
8. *Myers G.* Software reliability. M.: Mir, 1980
9. *Boem B., Braun Dzh., Kaspar Kh. i dr.* Kharakteristiki kachestva programmnogo obespecheniya. M.: Mir, 1981.
10. *Teyer T., Lipov M., Nelson E.* Nadezhnost PO. M.: Mir, 1981.
11. *Lipayev V. V.* Nadezhnost programmnykh sredstv. M.: SINTEG, 1998.

E. B. Aleksandrova, E. A. Kuznetsova

User Revocation and Joining in the Lattice-based VLR Group Signature

Key words: lattice-based group signature, verifier local revocation, joining

Modified lattice-based VLR group signature is proposed, allowing user's signature revocation and joining the new group member. This new scheme guarantees selfless anonymity and traceability.

Е. Б. Александрова, Е. А. Кузнецова

ОТЗЫВ И ДОБАВЛЕНИЕ ПОЛЬЗОВАТЕЛЯ В РЕШЕТОЧНОЙ VLR-СХЕМЕ ГРУППОВОЙ ПОДПИСИ

В ряде прикладных областей для защиты информации требуется анонимное подтверждение ее достоверности. Для решения этой задачи используются специальные схемы цифровой подписи, обеспечивающие анонимность подписывающего, – групповые подписи [1].

Важными составляющими протокола групповой подписи являются процедуры отзыва права подписи и добавления пользователя в группу. Наиболее эффективным вариантом отзыва является отзыв, локальный для проверяющего (verifier local revocation, VLR). В таких схемах сообщения, содержащие информацию об отозванных членских сертификатах, обрабатываются только проверяющими. Основным преимуществом VLR-схем групповой подписи является

то, что выпускаемые записи отзыва никак не привязаны к используемым ключам. Тем самым они позволяют отзывать не право подписи у члена группы, как при отзыве с динамическим накоплением, а сами подписи, им сформированные.

Одной из перспективных альтернатив «традиционным» алгебраическим структурам, используемым для построения схем групповой подписи, являются решетки. Первая попытка интеграции решеток в механизм групповых подписей была предпринята в работе [2]. Протокол, построенный в целом по шаблонам схемы BMW, использует модель со случайным оракулом. Дальнейшее развитие данная схема получила в работе [3]. Основной особенностью этого протокола является малый размер цифровой подписи. Схема обеспечивает анонимность (причем возможно обеспечение полной CCA-анонимности) и отслеживаемость.

Однако оба эти протокола не предоставляют достаточной функциональности, поскольку не обладают наиболее востребованными свойствами схем групповой подписи: возможностью отзыва подписи и добавления нового участника в группу без изменения существующих параметров криптосистемы. Поэтому основой данного исследования стал протокол, предложенный в работе [4]. Указанный протокол предоставляет возможность для организации необходимых функций. Кроме того, защита строится на задаче SIVP (short integer solution problem: для данной m-мерной решетки, образованной базисом, равномерно распределенным над $(\mathbf{Z}_q)^{n\times m}$, найти кратчайший вектор с ρ-нормой), в отличие от более ранних протоколов, безопасность которых основана на задаче LWE (learning with errors).

Основу схемы составляет интерактивный протокол, позволяющий предоставить проверяющему доказательство того, что подписывающий является сертифицированным членом группы (то есть владеет ключом подписи) и что ключ отсутствует в списке отозванных.

Для данного протокола механизм отзыва будет выглядеть следующим образом. Для секретного ключа каждого из пользователей рассмотрим первый блок x_0, соответствующий корню «дерева бонсай» (см., например, работу [5]), и положим маркер отзыва равным $A_0x_0 \pmod q$ из $(\mathbf{Z}_q)^n$. При правильном выборе параметров значение маркера будет равномерно распределено над $(\mathbf{Z}_q)^n$. Пользователю предлагается вычислить значение функции c_0 по схеме обязательств COM [6] от случайного вектора r_0 из $(\mathbf{Z}_q)^m$. Далее, в зависимости от целей проверяющего, пользователь передает либо значение r_0, либо $r_0 + x_0$. В первом случае можно проверить честность вычисления значения c_0, во втором — содержится ли ключ пользователя в списке RL отозванных: для всех u_i из RL должно выполняться неравенство $c_0 \neq \mathrm{COM}(A_0(r_0 + x_0) - u_i \bmod q)$. Таким образом, если сертификат у пользователя отозван, то найдется такое i, что $A_0x_0 \pmod q = u_i$. Процедура добавления пользователя в группу по новому идентификатору изменяет ключ подписи пользователя и ключ отзыва менеджера группы.

Модифицированная схема обладает свойствами «чужой» анонимности, отслеживаемостью, возможностью отзыва членства. В то же время является простой, поскольку основывается на доказательстве знания «все-в-одном» с использованием парадигмы Фиата — Шамира, и эффективной: для параметра безопасности n и числа пользователей N открытый ключ группы и подпись имеют длину порядка $O(n^2 \log N)$.

СПИСОК ЛИТЕРАТУРЫ:

1. *Chaum D., Heyst van E.* Group signatures // Proceedings of Eurocrypt 1991. Springer-Verlag. Apr. 1991. P. 257–265.
2. *Gordon S. D., Katz J., Vaikuntanathan V.* A group signature scheme from lattice assumptions. URL: https://eprint.iacr.org/2011/060.pdf.

3. *Laguillaumie F., Langlois A., Libert B., Stehle D.* Lattice-based group signatures with logarithmic signature size. URL: http://eprint.iacr.org/2013/308.pdf.
4. *Langlois A., Ling S., Nguyen K., Wang H.* Lattice-based group signature scheme with verifier-local revocation // Public Key Cryptography – PKC2014. Springer, 2014. LNCS. Vol. 8383. P. 345–361.
5. *Cash D., Hofheinz D., Kiltz E., Peikert C.* Bonsai trees, or How to delegate a lattice basis. URL: http://www.cc.gatech.edu/~cpeikert/pubs/bonsai.pdf.
6. *Kawachi A., Tanaka K., Xagawa K.* Concurrently secure identification schemes based on the worst-case hardness of lattice problems // ASIACRYPT. Springer, 2008. LNCS. Vol. 5350. P. 372–389.

REFERENCES:

1. *Chaum D., Heyst van E.* Group signatures // Proceedings of Eurocrypt 1991. Springer-Verlag. Apr. 1991. P. 257–265.
2. *Gordon S.D., Katz J., Vaikuntanathan V.* A group signature scheme from lattice assumptions. URL: https://eprint.iacr.org/2011/060.pdf.
3. *Laguillaumie F., Langlois A., Libert B., Stehle D.* Lattice-based group signatures with logarithmic signature size. URL: http://eprint.iacr.org/2013/308.pdf.
4. *Langlois A., Ling S., Nguyen K., Wang H.* Lattice-based group signature scheme with verifier-local revocation // Public Key Cryptography – PKC2014. Springer, 2014. LNCS. Vol. 8383. P. 345–361.
5. *Cash D., Hofheinz D., Kiltz E., Peikert C.* Bonsai trees, or How to delegate a lattice basis. URL: http://www.cc.gatech.edu/~cpeikert/pubs/bonsai.pdf.
6. *Kawachi A., Tanaka K., Xagawa K.* Concurrently secure identification schemes based on the worst-case hardness of lattice problems // ASIACRYPT. Springer, 2008. LNCS. Vol. 5350. P. 372–389.

V. M. Barbashov, V. G. Ivanenko, N. S. Trushkin

Experiment-Calculated Estimate of a LSIC Operation Reliability in order to Ensure Safety of Information under Radiation Influence

Key word: criteria-based membership function, Brower automat, topological probabilistic models

In this paper digital systems safety operation prediction methods under radiation influence, founded on Brower digital automate and a digital systems operation estimate topological probabilistic models, is considered.

В. М. Барбашов, В. Г. Иваненко, Н. С. Трушкин

РАСЧЕТНО-ЭКСПЕРИМЕНТАЛЬНАЯ ОЦЕНКА НАДЕЖНОСТИ ФУНКЦИОНИРОВАНИЯ БИС ДЛЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ВОЗДЕЙСТВИИ РАДИАЦИИ

Создание сложных систем БИС, устойчивых к воздействию радиационных дестабилизирующих факторов, на сегодняшний день невозможно без активного использования логического моделирования, обеспечивающего необходимую адекватность описания и точность расчетов. При этом реальный характер радиационного поведения сложной электронной системы определяется конкретным соотношением радиационно-чувствительных параметров ее элементов и учетом влияния их статистического разброса. Соотношение между функцией распределения плотности вероятности разброса и критериальной функцией принадлежности (КФП) определяет, в конечном итоге, целесообразность использования функционально-логических моделей радиационного поведения БИС применительно к каждому конкретному случаю [1].