БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Листопад Н. И. Модели оптимальной маршрутизации в компьютерных сетях // Труды БГТУ. Сер. VI, Физико-математические науки и информатика. 2006. Вып. XVI. С. 130–132.

2. Листопад Н. И., Матрук Аль Даллаен А., Копачев А. Г. Модели обеспечения живучести компьютерных сетей при оптимальной маршрутизации информационных потоков // Информатика. 2006. Вып. 4. С. 39–48.

3. Листопад Н. И., Величкевич И. О. Методы балансировки трафика в IP сетях // Докл. БГУИР. 2010. № 7 (53). С. 18–24.

4. Листопад Н. И., Величкевич И. О. Оптимальная маршрутизация информационных потоков с учетом параметров QOS // Докл. БГУИР. 2012. № 4 (66). С. 111–116.

5. Girlich E., Kovalev M. M., Listopad N. I. Optimal choice of the capacities of telecommunication networks to provide QoS-routing. Magdeburg, 2009.

6. A Scalable Approach to QoS-Aware Self-adaptation in Service-Oriented Architectures / V. Cardellini [et al.] // Proc. of 6th Intern. ICST Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness, Q Shine 2009 and 3rd Intern. Workshop on Advanced Architectures and Algorithms for Internet Delivery and Applications, AAA-IDEA 2009 (Las Palmas, Gran Canaria, Nov. 23–25, 2009). Berlin ; Heidelberg ; New York, 2009. P. 431–447.

7. Listopad N. I., Kopachev A. G., Matruk A. A. Quality of Service at the Computer Networks Based on Internet // Системні дослідження та інформаційні технології. 2006. № 4. С. 71–76.

8. Dijkstra E. W. A note on two problems in connexion with graphs // Numerische Mathematik. 1959. Vol. 1. P. 269–271.

Поступила в редакцию 14.10.2014.

Николай Измайлович Листопад – доктор технических наук, профессор, заведующий кафедрой информационных радиотехнологий факультета радиотехники и электроники УО «Белорусский государственный университет информатики и радиоэлектроники», директор Учреждения «Главный информационно-аналитический центр Министерства образования Республики Беларусь».

Юрий Иосифович Воротницкий – кандидат физико-математических наук, доцент, заведующий кафедрой телекоммуникаций и информационных технологий факультета радиофизики и компьютерных технологий БГУ, начальник Центра информационных технологий БГУ.

Ахмед Абдулазиз Хайдер – аспирант кафедры информационных радиотехнологий факультета радиотехники и электроники УО «Белорусский государственный университет информатики и радиоэлектроники». Научный руководитель – Н. И. Листопад.

УДК 003.26:51:004(075.8)

Т. В. ГАЛИБУС, Г. В. МАТВЕЕВ

ВЕРИФИКАЦИЯ ПАРАМЕТРОВ МОДУЛЯРНОГО РАЗДЕЛЕНИЯ СЕКРЕТА

Предложены метод верификации модулярной схемы разделения секрета в кольце полиномов и алгоритм проверки дилера, исключающий возможность распределения некорректных данных. Алгоритм является модификацией метода Фельдмана и основан на вычислительной сложности решения задачи дискретного логарифмирования. В отличие от существующих алгоритмов верификации для модулярных схем в кольце целых чисел наш метод автоматически гарантирует верификацию как промежуточного значения секрета, так и порогового значения *t*. Тем самым завершено построение криптостойкой верифицируемой пороговой схемы разделения секрета. Попутно проанализированы методы верификации параметров схем разделения секрета в кольце целых чисел.

Ключевые слова: разделение секрета; метод Фельдмана; модулярные параметры; верификация разделения секрета; пороговые схемы.

We construct a verification scheme for the polynomial modular secret sharing and propose a dealer verification algorithm that guarantees the correctness of the distributed data. We compare the constructed algorithm with the same for the integer modular secret sharing scheme. Our method is the modification of Feldman's verifiable secret sharing scheme and is based on the complexity of discrete logarithm computation. The proposed method guarantees the verification of all modular (t, k)-threshold secret sharing scheme parameters including the intermediate secret value and the threshold value t. We construct the Feldman verification in the univariate polynomial ring over F_q and provide conditions on the size of the finite field in which the scheme is constructed. Our algorithm constructs the verifiable cryptographically secure or perfect modular secret sharing scheme.

Key words: secret sharing; Feldman method; modular parameters; secret sharing verification; threshold schemes.

Схемы разделения секрета (СРС) лежат в основе многих криптографических протоколов в распределенных системах. Разделение секрета применяется для совместных конфиденциальных вычислений [1], шифрования на основе атрибутов [2] и электронного защищенного голосования [3]. Важной задачей в разделении секрета является построение таких схем, с помощью которых пользователи могут проверить корректность секрета и тем самым не допустить обман со стороны остальных участников и дилера. Такие схемы строятся на основе протоколов с нулевым разглашением [4]. В схемах верифицируемого разделения секрета (СВРС) дилер распределяет информацию о секретном значении среди участников таким образом, что для честных пользователей гарантируется получение ими значения секрета, а для нечестных – невозможность восстановить секрет.

СВРС позволяет честным пользователям, т. е. тем, которые следуют протоколу восстановления секрета, проверить корректность частичных секретов при их распределении и восстановлении исходного

секрета. Верификация разделения секрета лежит в основе криптографического протокола совместных конфиденциальных вычислений (СКВ) [1].

В основе верификации схем разделения секрета лежит подход Фельдмана [5], который основывается на свойстве гомоморфности односторонней функции дискретного логарифма. Позже Беналоу [3] предложил еще один подход. Первоначально оба эти метода применялись лишь для верификации параметров пороговой схемы Шамира.

В последние годы получили развитие методы верификации для модулярного разделения секрета, что обусловлено быстродействием модулярного алгоритма восстановления [6], адаптивными свойствами таких схем [7] и возможностью включить верификацию для произвольных структур доступа [8]. Изучением данного вопроса занимались Ифтене [9], Кьонг и др. [10], Кайя и Сельджук [11]. В их работах предложены алгоритмы верификации для модулярных пороговых схем Миньотта [12] и Асмуса – Блюма [1] в кольце целых чисел. Общий недостаток данных методов верификации модулярных схем – их применимость лишь в кольце целых чисел, что в силу отсутствия совершенной модулярной схемы в этом кольце [13] делает их неприменимыми на практике. Алгоритмы верификации всех существующих модулярных СВРС служат для проверки лишь промежуточного значения секрета, что ограничивает возможности участников по верификации основного значения и не позволяет исключить обман со стороны дилера.

Преимуществом полиномиальных схем модулярного разделения секрета является их теоретико-информационная криптостойкость: полиномиальная модулярная схема, в общем случае – совершенная, а в пороговом – идеальная [7]. Еще одно преимущество полиномиальных схем по сравнению с целочисленными – их расширенные возможности по генерации параметров: в качестве исходного поля используется любое поле F_p, а количество параметров зависит от степеней модулей участников в $F_p[x]$, что позволяет построить множество схем даже для небольших простых p.

В связи с вышесказанным верификация полиномиальной модулярной схемы является актуальной задачей. Нами предлагается верификация всех параметров разделения секрета, т. е. дилер публикует секретные параметры полностью, включая основной секрет, зашифрованные односторонней функцией верификации. Предлагаемый подход избавляет от необходимости громоздкой верификации интервала промежуточного секрета, как это сделано в работе [11].

Пороговая модулярная схема разделения секрета в кольце $F_p[x]$

Пороговая полиномиальная модулярная СРС была предложена в работах [14], [7] и принята в качестве стандарта в Республике Беларусь (СТБ 34.101.60). Данная схема позволяет разделить секретное значение $s(x) \in F_p[x]$. Промежуточный секрет $S(x)$ (t, k)-пороговой модулярной полиномиальной схемы выбирается так, что $\deg S(x) < tn$, где t – порог; n – общая степень модулей участников. Разделение секрета можно начать с генерации значения $S(x)$.

Фаза дилера (алгоритм разделения):

1) случайным образом выбирается промежуточное значение секрета $S(x) \in F_p[x]$ с условием

$$\deg S(x) < tn;$$

2) случайным образом выбираются попарно различные неприводимые $m_i(x)$, $i = 1, \ldots, k$, и $p(x)$ с ограничением $\deg m_i(x) = \deg p(x) = n$. В работе [8] указан способ выбора параметров t, k, n, p;

3) дилером публикуются $m_i(x)$, $p(x)$, а $s(x) = S(x) \bmod p(x)$ назначается в качестве секрета схемы;

4) дилером по секретным каналам участников отправляются их частичные секреты: $s_i(x) = S(x) \bmod m_i(x)$;

5) дополнительно, для ускорения вычислений на фазе восстановления секрета, дилером заранее вычисляются и публикуются значения:

$$M_A(x) = \prod_{j=i_1}^{i_t} m_j(x), \text{ где } A = \{i_1, \ldots, i_t\} \text{ – подмножество } t \text{ участников;}$$

$$M_{A\setminus\{i\}}(x) = \frac{M_A(x)}{m_i(x)};$$

$$M'_{A,\,i} = \left(M_A(x) / m_i(x)\right)^{(-1)} \bmod m_i(x), \forall i \in A.$$

Фаза участников (алгоритм восстановления):

участники из подмножества A обмениваются частичными секретами $s_i(x)$, $i \in A$, и находят значение секрета $s(x)$:

$$u_i = s_i M'_{A,i} M_{A\setminus\{i\}}, \forall i \in A;$$

$$S(x) = \sum_{i \in A} u_i \bmod M_A;$$

$$s(x) \equiv S(x) \bmod p(x).$$

Отметим, что вычисления в кольце многочленов аналогичны вычислениям в кольце целых чисел. Но в силу того, что в кольце многочленов все участники равноправны, т. е. обладают частичными секретами одинакового размера, построенная пороговая схема является идеальной [7].

Верификация полиномиальной пороговой схемы разделения секрета

Пусть заданы параметры (t, k)-пороговой модулярной схемы:

$$m_1(x), m_2(x), \ldots, m_k(x), p(x), S(x), s(x) \in F_p[x].$$

При этом $s(x) = S(x) \bmod p(x)$, т. е. $S(x) = p(x)\, q(x) + s(x)$.

Обобщая известный метод верификации Фельдмана [5], предлагается поступить следующим образом. Пользователю, т. е. обладателю полинома $s_i(x)$, $i = 1, 2, \ldots, k$, фактически необходимо проверить условие

$$S(x) = m_i(x)q(x) + s_i(x), \text{ т. е. } s_i(x) = S(x) \bmod m_i(x),$$

при том, что полином $S(x)$ остается скрытым. Для построения соответствующего протокола воспользуемся следующим известным фактом. Условие $S(x) = m_i(x)\, q(x) + s_i(x)$ эквивалентно системе уравнений $S(\beta_j) = s_i(\beta_j)$, $j = 1, 2, \ldots, n$, где $\beta_1, \beta_2, \ldots, \beta_n$ – корни многочлена $m_i(x)$. Известно, что все они попарно различны и принадлежат полю F_{p^n}, так как многочлен $m_i(x)$ неприводим. Эти условия полностью определяют полином $s_i(x)$, если известны величины $s_i(\beta_j)$, $j = 1, 2, \ldots, n$, и тем самым верифицируется частичный секрет пользователя.

Остается только провести эту верификацию так, чтобы пользователь не получал никакой информации, кроме априорной, о полиноме $S(x)$. Для этого можно поступить следующим образом. Возьмем достаточно большую циклическую группу $G = <g>$, порожденную элементом g, в которой задача дискретного логарифмирования является вычислительно трудной. Поскольку мы отождествляем поле F_p с множеством $\{0, 1, \ldots, p - 1\}$, то корректно определена степень g^x в случае, когда $x \in F_p$. Определим сначала g^x в случае, когда $x \in F_{p^n}$. С этой целью можно поступить следующим образом. Выберем какой-нибудь базис $b_1, b_2, \ldots, b_n$ расширения F_{p^n}/F_p. Тогда

$$x = \alpha_1 b_1 + \alpha_2 b_2 + \ \ldots\ + \alpha_n b_n, \alpha_i \in F_p, \forall x\, F_{p^n}.$$

Определим g^x следующим образом:

$$g^x = g^{\alpha_1 b_1 + \alpha_2 b_2 + \ldots + \alpha_n b_n} = \left(g^{b_1}\right)^{\alpha_1} \left(g^{b_2}\right)^{\alpha_2} \ldots \left(g^{b_n}\right)^{\alpha_n}.$$

Здесь элементы g^{b_i} имеют формальный смысл, их можно рассматривать как порождающие элементы изоморфных циклических групп.

Пусть теперь $S(x) = s_0 + s_1 x + \ldots + s_\gamma x^\gamma$, $\gamma < nt$.

Дилер публикует значения g^{s_0}, g^{s_1}, …, g^{s_γ}. Конечно, при этом поле F_p должно быть достаточно большим, с тем чтобы задача вычисления дискретных логарифмов $s_0, s_1, \ldots, s_\gamma$ была вычислительно трудной.

Теперь проверку условия вида $s_i(x) = S(x) \bmod m_i(x)$ можно заменить проверкой условий вида $S(\beta_j) = s_i(\beta_j)$, $j = 1, 2, \ldots, n$, где $\beta_1, \beta_2, \ldots, \beta_n$ – корни многочлена $m_i(x)$. Последнее условие эквивалентно условию

$$g^{s_0} \left(g^{s_1}\right)^{\beta_j} \left(g^{s_2}\right)^{\beta_j^2} \ldots = g^{S(\beta_j)} = g^{s_i(\beta_j)}.$$

Таким образом, предложенная верификация состоит в проверке этих условий каждым участником $i = 1, 2, \ldots, k$ и ее следует проводить по всем корням каждого полинома $m_i(x)$.

Поскольку в зашифрованном виде публикуются отдельные значения для всех коэффициентов $S(x)$, то протокол автоматически гарантирует проверку условия $\deg S(x) < nt$ и верификацию порогового значения t. Также отпадает необходимость в громоздкой проверке принадлежности промежутку [11] и передаче дополнительных параметров для ее осуществления.

Таким образом, предложенная схема верификации параметров полиномиального порогового разделения секрета исключает возможность распределения некорректных данных. Это является преимуществом верификации разделения секрета в кольце полиномов по сравнению с кольцом целых чисел.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Cramer R., Damgard I., Nielsen J. Multiparty Computation from Threshold Homomorphic Encryption // LNCS. 2001. Vol. 2045. P. 280–300.

2. Bethencourt J., Sahai A., Waters B. Ciphertext-policy attribute-based encryption // Proc. of IEEE Symposium on Security and Privacy. California, 2007. P. 321–334.

3. Benaloh J. Secret sharing homomorphisms: keeping shares of a secret secret // LNCS. 1987. Vol. 263. P. 251–260.

4. Blum M., Feldman P., Micali S. Non Interactive Zero-Knowledge and Its Applications // Proc. of the 20th ACM Symposium on Theory of Computing. ISSN for Comp. Machinery. New York, 1988. P. 103–112.

5. Feldman P. A practical scheme for non-interactive verifiable secret sharing // IEEE Symposium on Foundations of Computer Science. Washington, 1987. P. 427–437.

6. Asmuth C. A., Bloom J. A modular approach to key safeguarding // IEEE Transactions on Information Theory. 1983. Vol. 29. P. 156–169.

7. Galibus T., Matveev G., Shenets N. Some structural and security properties of the modular secret sharing // Proc. of SYNASC'08. Los Alamitos, 2009. P. 197–200.

8. Galibus T., Matveev G. Generalized Mignotte Sequences in Polynomial Rings // ENTCS. 2007. Vol. 186.

9. Iftene S. Secret sharing schemes with applications in security protocols: technical report TR 07-01 / University Alexandru Ioan Cuza of Iasi, Faculty of Computer Science. Iasi, 2007.

10. A non-interactive modular verifiable secret sharing scheme / L. Qiong [et al.] // Proc. of ICCCAS'05. Hong Cong, 2005. P. 84–87.

11. Kaya K., Selcuk A. Verifiable Secret Sharing Scheme Based on the Chinese Remainder Theorem // LNCS. 2008. Vol. 5365. P. 288–305.

12. Mignotte M. How to share a secret // LNCS. 1982. Vol. 149. P. 371–375.

13. Quisquater M., Preneel B., Vandewalle J. On the security of the threshold scheme based on the Chinese remainder theorem // LNCS. 2002. Vol. 2274. P. 199–210.

14. Галибус Т. В. Разделение секрета над полиномиальными кольцами // Вестн. БГУ. Сер. 1, Физика. Математика. Информатика. 2006. № 2. С. 97–100.

Поступила в редакцию 12.11.2014.

Татьяна Васильевна Галибус – кандидат физико-математических наук, доцент кафедры информационных систем управления факультета прикладной математики и информатики БГУ.

Геннадий Васильевич Матвеев – кандидат физико-математических наук, доцент кафедры высшей математики факультета прикладной математики и информатики БГУ.

УДК 517.938:925

B. S. KALITINE

ON THE PSEUDO-STABILITY OF SEMIDYNAMICAL SYSTEMS

Введено свойство псевдоустойчивости как необходимое условие орбитальной устойчивости замкнутых инвариантных множеств полудинамических систем на произвольном метрическом пространстве. Приведена классификация устойчивоподобных свойств в форме диаграммы, которая отражает взаимоотношения псевдоустойчивости и равномерной псевдоустойчивости с известными характеристиками качественной теории устойчивости полудинамических систем (инвариантность, устойчивость, притяжение и их модификации). Установлена связь между понятием псевдоустойчивости и определением первого интеграла полудинамической системы. Сформулированы критерии псевдоустойчивости в форме достаточных условий с использованием определенно положительных и знакопостоянных функций Ляпунова. Даны комментарии к результатам на иллюстративных примерах.

Ключевые слова: полудинамическая система; положительно инвариантное множество; устойчивость; псевдоустойчивость; первый интеграл; функция Ляпунова.

Pseudo-stability property is introduced as a necessary condition of the orbital stability of closed positively invariant sets of semidynamical systems defined on an arbitrary metric space. We give a classification of stability-like properties in the form of a diagram. The diagram reflects the relationship between pseudo-stability and uniform pseudo-stability with known characteristics of qualitative stability theory of motion of semidynamical systems (invariance, stability, attraction and their modifications). We establish particular connection between the pseudo-stability notion and first integrals of semidynamical systems. The criteria of pseudo-stability are formulated and sufficient conditions for this property with positive definite and semidefinite Lyapunov functions are provided. We also give comments on the results with a number of illustrating examples.

Key words: semidynamical system; positively invariant set; stability; pseudo-stability; first integral; Lyapunov function.

Overview of results

Over the past 50 years development of the qualitative theory of dynamical systems has contributed greatly to the generation of methods of topological dynamics with respect to objectives of stability theory of movement [1]. In V. I. Zubov monograph [2] author presents the research methods for problems of the stability theory of dynamical systems $(X, \mathbb{R}, \pi)$ defined on a metric space (X, d). The author gives the basics of direct Lyapunov's method and lays the foundation of qualitative study of the structure of closed invariant sets' neighbourhoods in terms of their stability properties. In [3–5] authors introduce an interesting idea of splitting