DOUDKIN A.A., GANCHENKO V.V., MARUSHKO E.E., CHARIN S.N. **Monitoring telemetry parameters of spacecraft target equipment using neural networks**

Neural network algorithms are proposed for monitoring target equipment on spacecraft telemetry data.

УДК 003.26:51:004(075.8)

Галибус Т.В.

ВЕРИФИКАЦИЯ ПОЛИНОМИАЛЬНОГО МОДУЛЯРНОГО РАЗДЕЛЕНИЯ СЕКРЕТА НАД ДВОИЧНЫМ ПОЛЕМ

В работе предлагается протокол верификации частичных секретов участников полиномиальной пороговой модулярной схемы разделения секрета. Верификация, т.е. проверка корректности разделения секрета, лежит в основе большинства криптографических протоколов в распределенных системах и позволяет исключить обман со стороны участников. В частности, такие схемы применяются для совместных конфиденциальных вычислений (MPC), шифрования на основе атрибутов (ABE) и электронного защищенного голосования (e-voting).

Ранее данную задачу для модулярного подхода решали Ифтене [5], Кайя и Сельджук [8], Кьонг и др.[6], В этих работах внимание уделено исключительно целочисленному разделению секрета [1], [7]. Однако, развивать модулярный подход, в силу его криптографической стойкости как показывает опыт [4], целесообразнее в полиномиальном кольце.

Один из способов верификации параметров полиномиальной схемы основывается на методе Фельдмана [2], и позволяет проверить параметры схем в кольцах $F_p[x]$, таких, что вычисление дискретного логарифма в поле F_p является достаточно трудоемким. Поэтому такое обобщение метода Фельдмана не совсем подходит для кольца $F_2[x]$, на котором построен стандарт разделения секрета СТБ 34.101.60. Для решения указанной задачи предлагается упрощенный протокол, который позволяет участникам при восстановлении исходного значения секрета взаимно верифицировать частичные секреты. Протокол работает при условии, что дилер корректно распределяет данные для проверки и восстановления. Протокол исключает обман со стороны участников схемы. Верификация основывается на опубликованных дилером проверочных значениях и ключах, при помощи которых участники восстановления проверяют частичные секреты друг друга. При этом, получить дополнительную информацию о секрете при помощи проверочных значений доказуемо невозможно, то есть гарантируется безопасность верификации.

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

Пусть k – число участников схемы и $1 \le t \le k$ – порог. (t, k)-пороговая модулярная полиномиальная схема позволяет раздать участникам частичные секреты таким образом, что секретное значение $s(x) \in F_p[x]$ могут найти лишь t-подмножества участников. Схема позволяет гарантировать защищенность секрета $s(x)$, такого, что $\deg s(x) < n$ при условии, что промежуточный секрет $S(x)$ выбирается так, что $\deg S(x) < tn$:

Распределение частичных секретов:

1) Случайным образом выбирается промежуточное значение секрета $S(x) \in F_p[x]$ с условием
$$\deg S(x) < tn.$$
2) Выбираются попарно различные неприводимые $p_i(x)$, $i = 1,..,k$ и $p(x)$, такие, что $\deg p_i(x) = \deg p(x) = n$.
3) Дилером публикуются $p_i(x)$, $p(x)$, а $s(x) = S(x) \bmod p(x)$ назначается в качестве секрета схемы.
4) Дилером отправляются частичные секреты участников $s_i(x) = S(x) \bmod p_i(x)$ по защищенным каналам связи.

Восстановление секрета:

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

$$u_i = s_i P'_{A,i} P_{A\setminus\{i\}}, \forall i \in A,$$
$$S(x) = \sum_{i \in A} u_i \bmod P_A,$$
$$s(x) \equiv S(x) \bmod p(x),$$

где:

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

$$P_{A\setminus\{i\}}(x) = \frac{P_A(x)}{p_i(x)};$$

$$P'_{A,i} = \left(\frac{P_A(x)}{p_i(x)}\right)^{-1} mod\ p_i(x),\ \forall i \in A.$$

Протокол проверки частичных секретов полиномиальной модулярной СРС над двоичным полем. Предлагается протокол проверки частичных секретов участников $s_i(x)$ при восстановлении секрета СРС в кольце $F_2[x]$. Поскольку мультипликативная группа конечного поля является циклической, то для всякого $S(x) \in F_2[x]$ и неприводимого $p(x) \in F_2[x]$, $\deg p(x) = n$, выполняется $(S(x))^d = S(x) mod\ p(x)$, при условии, что $d \equiv 1 mod\ (2^n - 1)$.

Исходными данными протокола являются:

1. Набор неприводимых полиномов в $F_2[x]$:
$$p(x), p_1(x), p_2(x), \ldots, p_k(x), \deg p(x) = \deg p_i(x) = n.$$
При этом $\left(MinDiv\left(2^n - 1\right)\right)^t \ge 2^n - 1$, где $MinDiv(a)$ – наименьший простой делитель натурального числа a.
2. Набор пар $\{e_i, d_i\}$, таких, что $e_i d_i \equiv 1 mod\ (2^n - 1)$, $i = 1,2,\ldots,k$.

Дополнительно к данным, необходимым для восстановления секрета, дилер публикует:

1. $D_1(x) = (S(x))^{d_1} mod\ p_1(x), D_2(x) = \left(S(x)\right)^{d_2} mod\ p_2(x),$
$\ldots, D_k(x) = \left(S(x)\right)^{d_k} mod\ p_k(x),$
которые служат для проверки частичных секретов участников.
2. $E_1 = g^{e_1}, E_2 = g^{e_2}, \ldots, E_k = g^{e_k}$, которые позволяют верифицировать проверочные ключи участников. При этом, $g \in G$ является порождающим элементом циклической группы достаточно большого порядка (а именно, не менее $2^n - 1$), в которой задача дискретного логарифмирования является вычислительно трудной.

Секретными данными участников, которые передаются по закрытым каналам, являются частичные секреты $s_i(x) = S(x) mod\ p_i(x)$ и проверочные ключи e_i.

Галибус Татьяна Васильевна, *доцент кафедры информационных систем управления Белорусского государственного университета. Беларусь, БГУ, 220013, г. Минск, пр. Независимости, 4.*

При восстановлении секрета участник предъявляет пару верифицируемых значений $\{e_i, s_i(x)\}$. Остальные участники протокола убеждаются в том, что:

$$(D_i(x))^{e_i} \equiv (S(x))^{d_i e_i} = S(x) \bmod p_i(x) = s_i(x),$$

$$g^{e_i} = E_i.$$

Построенный таким образом протокол верификации пороговой полиномиальной модулярной СРС работает про условии честности дилера, который корректно распределяет исходные и проверочные данные схемы. При этом, никакой участник не сможет предъявить неверные данные для проверки. Действительно, для того, чтобы подделать значение $s_i(x)$, ему также необходимо подобрать соответствующий ключ e_i, что невозможно сделать, поскольку это значение проверяется при помощи опубликованной дискретной экспоненты.

Обоснование стойкости протокола проверки. При публикации дилером дополнительных значений $\{D_i, E_i\}$ защищенность схемы может уменьшиться, поскольку при помощи этих данных участники могут попытатьсяполучить дополнительную информацию о значении $s(x)$. В частности, злоумышленник может попытаться сократить множество перебора значений $s(x)$. В самом деле,

$$s_i(x) = (D_i(x))^y \bmod p_i(x), y = 1,2,\ldots,k_i,$$

где k_i – порядок подгруппы, порожденной $D_i(x)$. Таким образом, частичный секрет $s_i(x)$ выбирается из множества мощности k_i. Для определения $s(x)$ требуется выбрать не менее t частичных секретов. Меньшее количество не дает информации о секрете в силу совершенности схемы [4]. Поскольку порядок подгруппы делит порядок группы, то для успешной атаки надо, чтобы $k_1 k_2 \ldots k_t < \left(MinDiv\left(2^n - 1\right)\right)^t$. А значит, для того чтобы отыскать секрет таким методом требуется перебрать не менее $\left(MinDiv\left(2^n - 1\right)\right)^t$ наборов $s_1(x) \cdot s_2(x) \ldots s_t(x)$. Однако, согласно условию (1) такой перебор не имеет смысла, поскольку значений основного секрета также $2^n - 1$. Таким образом, публикация значений $\{D_i\}$ не уменьшает защищенность схемы. Публикация $\{E_i\}$ не нарушает защищенность схемы при правильном выборе циклической группы.

Для того, чтобы определить, подходит ли набор неприводимых полиномов для построения протокола верификации, требуется проверить условие (1). Это зависит от факторизации чисел Мерсенна $2^n - 1$. Таблицы факторизации чисел такого вида известны, в частности, до $n < 1200$. Этого достаточно, чтобы удовлетворить условию (1). Очевидно, что наиболее подходящими для обеспечения стойкости опубликованных значений являются простые числа Мерсенна, т.е. числа вида $2^n - 1$, где n = 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1279 и т.д. (см. [9]). Размер исходного ключа при этом целесообразно выбирать не менее 128 бит, а значит, $n \geq 127$. Порядок циклической группы для генерации значений $\{E_i\}$, в которой задача нахождения дискретного логарифма является вычислительно трудной, при этом должен быть не менее $2^{127} - 1$.

Заключение. В работе предложен протокол верификации частичных секретов пороговой полиномиальной модулярной схемы. Обоснована его криптографическая стойкость, в частности, указано, что перебор с участием опубликованных проверочных значений не дает преимуществ в сравнении с перебором исходных данных схемы. Указаны условия, при которых секрет схемы остается защищенным независимо от опубликованных значений.

СПИСОК ЦИТИРОВАННЫХ ИСТОЧНИКОВ

1. Asmuth C.A., Bloom J. A modular approach to key safeguarding // IEEE Transactions on Information Theory. – 1983. – Vol. 29. – P. 156–169.
2. Feldman P. A practical scheme for non-interactive verifiable secret sharing // IEEE Symposium on Foundations of Computer Science – 1987 – P. 427-437.
3. Galibus T. Matveev G. Generalized Mignotte Sequences in Polynomial Rings // ENTCS – 2007. – Vol. 186.
4. Galibus T. Matveev G. Shenets N. Some structural and security properties of the modular secret sharing // Proc. of SYNASC'08. – IEEE Comp. soc. press, Los Alamitos – 2009 – P. 197-200.
5. 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. - 2007.
6. Kaya K., Selcuk A. A Verifiable Secret Sharing Scheme Based on the Chinese Remainder Theorem. // LNCS – 2008 – Vol.5365. – P.288-305.
7. Mignotte M. How to share a secret // Advances in cryptology – Eurocrypt'82, LNCS. – 1982. – P. 371–375.
8. Qiong L., Zhifang W., Xiamu N., Shenghe S. A non-interactive modular verifiable secret sharing scheme // Proc. of ICCCAS'05 – 2005 – Vol.1. – P. 84-87.
9. *The online encyclopedia of integer sequences: sequence* A000043 (*Mersenne primes)*, Available at: https://oeis.org/A000043 (accessed 19 November 2014).

Материал поступил в редакцию 23.12.14

GALIBUS T.V. **Verification of the participants of the polynomial modular secret sharing over the binary field**

We construct a verification of the shares of polynomial modular secret sharing in the case of the binary field. The verification is effective in the presence of honest dealer and malicious participants who wish to submit the false shares. The privacy of the verification is based on the perfectness of the threshold scheme and the hardness of discreet logarithm computation. We provide the restrictions on the degree of polynomials, field size and threshold that guarantee the privacy of the verification.

УДК 004.032.26,004.4

Ганченко В.В., Марушко Е.Е.

АРХИТЕКТУРА ПРОГРАММНОГО КОМПЛЕКСА ИДЕНТИФИКАЦИИ РЕЖИМОВ ФУНКЦИОНИРОВАНИЯ ПОДСИСТЕМ КОСМИЧЕСКИХ АППАРАТОВ

Введение. Программный комплекс (ПК) идентификации режимов функционирования подсистем космических аппаратов (КА) и детектирования нештатных и аварийных ситуаций является одним из основных структурных составляющих экспериментального образца нейросетевой системы мониторинга состояния и поведения подсистем космических аппаратов по телеметрическим данным (ЭО СМ СПКА) [1]. Основной его задачей является контроль за состоянием и режимами функционирования бортового оборудования на основе нейросетевых технологий