УДК 681.322.067

СИГНАТУРЫ КОНЕЧНЫХ ПОЛЕЙ ДЛЯ СИСТЕМ КОНТРОЛЯ УТЕЧЕК ДАННЫХ

Т.А. АНДРИЯНОВА, С.Б. САЛОМАТИН

Белорусский государственный университет информатики и радиоэлектроники
П. Бровки, 6, Минск, 220013, Беларусь

Поступила в редакцию 20 декабря 2016

Предложены схемы защиты информации в системах обнаружения утечек данных с использованием сигнатур и алгоритмов кодирования в конечных полях. Даны оценки вычислительной сложности и защищенности алгоритмов.

Ключевые слова: сигнатура, аутентификация, конечное поле, функция следа, кодовые структуры.

Введение

Системы обнаружения утечек данных (DLD-системы) широко используют кодовые конструкции для формирования сигнатур и в протоколах аутентификации [1, 2]. Наиболее широко известные системы и алгоритмы [3] могут превышать допустимые возможности в инфокоммуникационных системах с ограниченными ресурсами. Одним из альтернативных решений, позволяющим реализовать быстрые системы вычисления сигнатур и аутентификации с открытым ключом, является применение алгоритмов кодирования информации в конечных полях.

Кодовая система оператора следа и кода Рида-Соломона

Рассмотрим конечное поле $GF\left(q^m\right)$, где q – степень простого числа. Конечное поле $GF\left(q\right)$ является подполем $GF\left(q^m\right)$. Определим последовательность $A=\left(a_1, a_2,\cdots, a_n\right)$, состоящую из n различных элементов $GF\left(q^m\right)$.

Полиномиальная запись элементов S имеет вид

$$pol_a \Rightarrow \begin{cases} GF\left(q^m\right)[X] \to GF\left(q^m\right)^n \\ p(X) \to \left\{p(a_1),\cdots, p(a_n)\right\} \end{cases},$$

где $GF\left(q^m\right)[X]$ – множество одномерных полиномов с коэффициентами из $GF\left(q^m\right)$.

Конечное поле $GF\left(q^m\right)$ можно рассматривать как m-мерный вектор пространства над $GF\left(q\right)$. Любой элемент $\beta \in GF\left(q^m\right)$ может быть представлен в виде суммы

$$\beta = \sum_{i=1}^{m} b_i \gamma_i,$$

где $\gamma_1,\cdots,\gamma_m$ – базис $GF\left(q^m\right)$ над $GF\left(q\right)$, а $b_i \in GF\left(q\right)$.

Код Рида-Соломона (РС) размерности k, корректирующий $\lfloor (n-k)/2 \rfloor$ ошибок, можно определить как [4]

$$RS\{A\} \to \left\{ pol_a(f) \mid f \in GF(q^m)[X]; \deg(f) < k \right\}.$$

Оператор следа, отображающий $GF(q^m) \to GF(q)$, имеет вид

$$Tr(x) = x + x^q + \cdots + x^{q^{m-1}}, \ \forall x \in GF(q^m).$$

Используя функцию следа и операцию скалярного произведения, для любого базиса $\gamma_1, \cdots, \gamma_m$ можно определить дуальный (двойственный) базис как совокупность элементов $\gamma_1^*, \cdots, \gamma_m^*$, удовлетворяющих условию

$$Tr(<\gamma_i, \gamma_i^*>) = 1 \ \text{ и } \ Tr(<\gamma_i, \gamma_j^*>) = 0; \ i \neq j.$$

Функцию следа вектора $\mathbf{s} = (s_1, \cdots, s_n)$ определим как

$$Tr(\mathbf{s}) = (Tr(s_1), \cdots, Tr(s_n)).$$

Пусть $A = (a_1, \cdots, a_n)$, где $a_i \in GF(q)$, $i = 1, \cdots, n$. Тогда для всех $\mathbf{s} = pol_a(\mathbf{p})$, где

$$p(X) = \sum_{i=0}^{k-1} p_i X^i \in GF(q^m)[X],$$

справедливо свойство

$$Tr(\mathbf{s}) = pol_a(P),$$

где $P(X) = \sum_{i=0}^{k-1} Tr(p_i) X^i$.

Соответствующий код РС устойчив к воздействию оператора следа.

Исходные параметры. Конечное поле $GF(q^m)$, целые числа n, k, W, w, множество A, содержащее n элементов поля $GF(q)$.

Формирование ключей. Формируется полином $p(X)$ степени k со свойством: m коэффициентов $p_{k-1}, \cdots, p_{k-m}$ полинома образуют базис $GF(q^m)$ над $GF(q)$. После чего вычисляется вектор $\mathbf{s} = pol_a(\mathbf{p})$, принадлежащий коду РС. Формируется случайный вектор

$$\mathbf{t} = (t_1, \cdots, t_n) \in GF(q^m)^n,$$

имеющий точно W ненулевых координат.

Открытым ключом объявляется вектор $\mathbf{K} = \mathbf{s} + \mathbf{t}$ (или вектор $\mathbf{K}$, полученный в результате векторного представления числа $K = s^e$ типа логарифма, или $\mathbf{K} = f(\mathbf{s}, \mathbf{t})$ полученный в результате одностороннего функционального преобразования f) над $GF(q^m)$. Вектора $\mathbf{s}$ и $\mathbf{t}$ образуют секретный ключ.

Режим крипто-кодирования. Информационное сообщение $\mathbf{u} = (u_0, \cdots, u_{k-m-1})$ имеет длину $(k-m)$ и формируется над полем $GF(q)$. Сообщение кодируется $\mathbf{d} = pol_a(\mathbf{u})$. Случайным образом выбираются элемент $\alpha \in GF(q^m)$ и вектор $\mathbf{e}$ над $GF(q)$ длины n с w ненулевыми элементами. Закодированное сообщение имеет вид

$\mathbf{c} = \mathbf{d} + Tr(\alpha \mathbf{K}) + \mathbf{e},\ Tr(\cdot) GF(q^m) \to GF(q).$

Режим крипто-декодирования. Принимающая сторона укорачивает принятый текст, исключая элементы, расположенные на ненулевых позициях **t**. В результате образуется вектор $\mathbf{y}' = \mathbf{d}' + Tr(\alpha \mathbf{s}') + \mathbf{e}'$. Согласно свойству функция следа $Tr(\alpha \mathbf{s}') \in RS_k(\mathbf{s}')$ дает слово кода РС. Используя алгоритм интерполяции [4] можно получить полином $Q(X)$ степени $k-1$, такой, что

$pol_{a'}(Q) = \mathbf{d}' + Tr(\alpha \mathbf{s}')$ и $Q(X) = d(X) + P(X).$

Полином сообщения **u** имеет степень меньшую, чем $(k-m-1)$, следовательно, коэффициенты $Q(X)$ равны $q_i = Tr(\alpha p_i)$ для $i = k-m, \cdots, k-1$. Функция $Tr(\alpha p_i)$ для $i = k-m, \cdots, k-1$ позволяет получить *m* координат элемента α в двойственном базисе $p_{k-1}, \cdots, p_{k-m}$. Знание α дает полином *P*, коэффициенты которого равны $Tr(\alpha p_i)$ для $i = 0, \cdots, k-1$. Теперь можно выделить информационное сообщение

$u(X) = Q(X) - P(X).$

Характеристические последовательности третьего порядка

Пусть $F = GF(p)$, где *p* – простое число и

$f(x) = x^3 - ax^2 + bx - 1,\ a, b \in F$

полином над полем *F*.

Последовательность $\mathbf{s} = \{s_k\}$ является последовательностью третьего порядка с характеристическим полиномом $f(x)$ если ее элементы удовлетворяют следующему уравнению [5]:

$s_k = as_{k-1} - bs_{k-2} + s_{k-3},\ k \geq 3.$

Если **s** имеет начальное состояние $s_0 = 3,\ s_1 = a,\ s_2 = a^2 - 2b,$ тогда $\mathbf{s} = \{s_k\}$ – характеристическая последовательность, формируемая $f(x)$.

Предположим, что $\alpha_1, \alpha_2, \alpha_3$ представляют собой все три корня $f(x)$ в разделимом поле $f(x)$ над *F*. В соответствии с формулой Ньютона элементы последовательности **s** могут быть представлены в виде симметричной суммы корней *k*-й степени

$s_k = \alpha_1^k + \alpha_2^k + \alpha_3^k,\ k = 0, 1, \cdots$

Обозначим период $f(x)$ как $per\{f(x)\}$. Если $f(x)$ является неприводимым полиномом над полем *F*, то период последовательности $\mathbf{s}(f)$ равен $per\{f(x)\}$.

Характеристические последовательности имеют следующие свойства.

1. Пусть $f(x) = x^3 - ax^2 + bx - 1$ будет полином над F, $\alpha_1, \alpha_2, \alpha_3$ и представляют собой все три корня $f(x)$ в разделимом поле $f(x)$ над *F* и **s** – характеристическая последовательность и пусть

$f_k(x) = (x - \alpha_1^k)(x - \alpha_2^k)(x - \alpha_3^k),$

тогда справедливы следующие соотношения:

$f_k(x) = x^3 - s_k(a, b)x^2 + s_{-k}(a, b)x - 1$, где $s_{-k}(a, b) = s_k(b, a)$.

Заметим, что $f(x)$ и $f_k(x)$ имеют одинаковые периоды, если НОД$\left(per\{f(x)\}\right) = 1$. Если НОД$\left(per\{f(x)\}\right) = 1$, тогда $f(x)$ – неприводимый полином над *F*, только в том случае, если $f_k(x)$ неприводим над *F*.

2. Пусть $f(x) = x^3 - ax^2 + bx - 1$ будет полином над *F* и пусть **s** – характеристическая последовательность, формируемая $f(x)$, тогда для всех положительных целых *k* и *e*

$$s_k\left(s_e(a, b), s_{-e}(a, b)\right) = s_{ke}(a, b).$$

3. Пусть *k* фиксированное положительное число. Если НОД$\left(k, p^l - 1\right) = 1$, $l = 1, 2, 3$, тогда для любых $u, v \in F$ система уравнений

$$s_k(a, b) = u \text{ и } s_{-k}(a, b) = v$$

имеет единственное решение $(a, b) \in F \times F$. Другими словами, последовательности $s_k(a, b)$ и $s_{-k}(a, b)$ взаимно ортогональны в *F* относительно переменных *u*, *v*.

Введем обозначение $Q = p^2 + p + 1$. Положительное целое *r* называется лидером смежного класса по модулю *Q*, если *r* является положительным наименьшим целым числом в множестве $\left\{tp^l \bmod Q \mid l = 0, 1, 2\right\}$, где *t* – положительное целое.

Алгоритм быстрых вычислений

Пусть $\{s_k\}$ – характеристическая последовательность над *F* с характеристическим полиномом $f(x)$ и $\{s_{-k}\}$ ее взаимная последовательность. Тогда для любых положительных целых *n* и *m* имеем

$$s_{2n} = s_n^2 - 2s_{-n},\ s_n s_m - s_{n-m}s_{-m} = s_{n+m} - s_{n-2m},\ n \neq m.$$

Пусть $k = \sum_{i=0}^{r} k_i 2^{r-i}$ – двоичное представление числа *k*, $T_0 \neq k_0$, $T_j = k_j + 2T_{j-1}$, $1 \le j \le r$. В этом случае $T_r = k$.

Рекуррентные алгоритмы вычислений:

1) для $k_j = 0$

$$s_{T_j - 1} = s_{T_{j-1}} s_{T_{j-1}-1} - bs_{-T_{j-1}} + s_{-(T_{j-1}+1)},\ s_{T_j} = s_{T_{j-1}}^2 - 2s_{-T_{j-1}},\ s_{T_j+1} = s_{T_{j-1}} s_{T_{j-1}+1} - as_{-T_{j-1}} + s_{-(T_{j-1}-1)};$$

2) для $k_j = 1$

$$s_{T_j} = s_{T_{j-1}}^2 - 2s_{-T_{j-1}},\ s_{T_j+1} = s_{T_{j-1}} s_{T_{j-1}+1} - as_{-T_{j-1}} + s_{-(T_{j-1}-1)},\ s_{T_j+1} = s_{T_{j-1}+1}^2 - 2s_{-(T_{j-1}+1)}.$$

Схема распределения ключей

Режим формирования ключей.

1. *p* – простое число и $f(x) = x^3 - ax^2 + bx - 1$ – неприводимый полином над полем $GF(p)$ с периодом $Q = p^2 + p + 1$.

2. Пользователь А выбирает *e*, которое удовлетворяет неравенству $0 < e < Q$ и условию $\text{НОД}(e, Q) = 1$ и определяет *e* как свой секретный ключ.

3. Пользователь А вычисляет (s_e, s_{-e}) и определяет это значение как открытый ключ криптографической системы.

4. Пользователь Б выбирает *r*, которое удовлетворяет неравенству $0 < r < Q$ и условию $\text{НОД}(r, Q) = 1$ и определяет *r* как свой секретный ключ.

5. Пользователь Б вычисляет (s_r, s_{-r}) и определяет это значение как открытый ключ криптографической системы.

Режим установления общего секретного ключа

$$s_e(s_r, s_{-r}) = s_{er} = s_r(s_e, s_{-e})$$

и

$$s_{-e}(s_r, s_{-r}) = s_{-er} = s_{-r}(s_e, s_{-e}).$$

Общий ключ равен

$$(s_{er}, s_{-er}).$$

Пример. Пусть $p = 11, 1 f(x) = x^3 + 4x - 1$ – неприводим над полем $GF(11)$ и имеет период $133 = 7 \times 19$.

Пользователь А: выбирает $e = 9$ как свой секретный ключ. Открытый ключ

$$e_{\text{А}} = (s_9, s_{-9}) = (10, 6).$$

Пользователь Б: выбирает $r = 13$ как свой секретный ключ. Открытый ключ

$$e_{\text{Б}} = (s_{13}, s_{-13}) = (7, 1).$$

Установление общего секретного ключа

Пользователь А:

$$s_e(s_r, s_{-r}) = s_9(7, 1) = 8,$$

$$s_{-e}(s_r, s_{-r}) = s_{-9}(7, 1) = s_{124}(7, 1) = 5.$$

Ключ $= (8, 5)$.

Пользователь Б:

$$s_\kappa(s_y, s_{-y}) = s_{13}(10, 6) = 8, \; s_{-r}(s_e, s_{-e}) = s_{-13}(10, 6) = s_{120}(10, 6) = 5.$$

Ключ $= (8, 5)$.

Система распределения с открытым ключом

Система имеет два состояния: формирования ключей и установления общего ключа пользователей. В первом состоянии формируется двухуровневое ключевое пространство пользователей на основе кубического неприводимого полинома периода $P = (p^2 + p + 1)$ над полем $GF(p)$. Первый уровень содержит секретные ключи пользователей, второй уровень – открытые ключи системного взаимодействия. Ключи первого уровня представляют собой случайные числа, взаимно простые с числом *P*. Ключи второго уровня представляют собой пару элементов (s_k, s_{-k}) двух взаимных характеристических последовательностей, формируемых кубическим

полиномом. Пространство ключей представляет собой множества, состоящие из всех лидеров смежных классов модуля $p^2 + p + 1$ и всех неприводимых полиномов над полем $GF(p)$ степени 3 с периодом $p^2 + p + 1$.

Во втором состоянии формируется общий ключ пользователей на основе свойства характеристических последовательностей: $s_k(s_e(a, b), s_{-e}(a, b)) = s_{ke}(a, b)$, где k и e положительные целые числа. Алгоритмы системы реализуются с использованием техники быстрых вычислений.

Оценка уровня защитных свойств. Защитные свойства характеристических последовательностей и криптосистем на их основе базируются на трудности решения задачи дискретного логарифма в конечном поле $GF(p^3)$, где p – простое число. Вычислительная сложность быстрого алгоритма криптосистемы может быть приблизительно оценена зависимостью $L \log n$ модулярных операций умножений.

Заключение

Рассмотрены алгоритмы защиты данных в системах контроля утечек информации. Алгоритмы используют арифметику конечных полей и свойства односторонней функции при решении не полностью определенных уравнений в конечных полях. Алгоритмы поддерживают процедуры аутентификации и формирования сигнатурных последовательностей.

SIGNATURE OF FINITE FIELDS FOR DATA LEAKAGE DETECTION SYSTEMS

T.A. ANDRIJANOVA, S.B. SALOMATIN

Abstract

Schemes of information security and algorithm coding in finite fields for data leakage detection systems are considered. Complexity algorithms and level security are evaluated.

Keywords: signature, authentication, finite field, trace function, code structure.

Список литературы

1. *Panagiotis P.* // IEEE Transactions On Knowledge And Data Engineering. Vol. 22. №3. P. 2, 4-5.
2. San*dip A.K., Kulkarni S.V.* // Inter Journal of Advanced Research in Computer and Communication Engineering, Vol. 1. P 668-678.
3. *Stinson D.R.* Cryptography: Theory and Practice. Florida, 1995.
4. *Blahut R.E.* Algebraic Codes on Lines, Planes, and Curves. Cambridge, 2008.
5. *Chen L., Gong G.* Communication system security. Florida, 2012.