неизвестного перехода $s - x/y \to p$. Требуется путем проведения простого условного эксперимента с автоматом A определить неизвестные (секретные) переходы.

Восстановление функции выходов. Пусть для $a \in X$ значение функции $\varphi_s(a)$ неизвестно. Поскольку функция φ_s есть биекция, то образ символа a относительно φ_s вычисляется как разность множеств Y и $\{y : y = \varphi_s(x), x \in X \backslash \{a\}\}$.

Восстановление функции переходов. Отметим, что начальный идентификатор для любого состояния s автомата, предъявленного для эксперимента (после восстановления функции выходов), может быть построен как $id(s) = \{x/y : x \in X, y = \varphi_s(x)\}$.

Шаг 1. $L := S$, т. е. автомат A может находиться в любом из своих состояний.

Шаг 2 (построение установочного слова). Найти входной символ x, такой, что существуют два состояния s и s' из L, для которых $\varphi(s, x) \neq \varphi(s', x)$. Подать на автомат A входной символ x и пронаблюдать выходной символ y. Найти состояния из L, стартуя из которых автомат A может выдавать y, т. е. построить множество $N = \{s : s \in L, y = \varphi_s(x)\}$. Построить множество Q преемников состояний из N по символу x. Если существует $s \in N$, соответствующее начальному состоянию секретного перехода $s - x/y \to p$, то перейти на Шаг 1. Если $|Q| \neq 1$, то $L := Q$ и перейти на Шаг 2.

Шаг 3 (построение переводящего слова). Найти и подать на A входное слово, переводящее автомат из состояния $q \in Q$, причем $|Q| = 1$, в неизвестное состояние k, соответствующее финальному состоянию секретного перехода $s - x/y \to p$.

Шаг 4 (восстановление неизвестного состояния). На автомат A подать входной символ a и пронаблюдать выходной символ b. $ID_k := ID_k \cup a/b$. Если $|ID_k| = |X|$, то состояние $k := p$, где p такое, что $id(p) = ID_k$, т. е. переход $s - x/y \to p$ восстановлен. Если существуют невосстановленные переходы, то перейти на Шаг 1.

ЛИТЕРАТУРА

1. *Кудрявцев В. Б., Алешин С. В., Подколзин А. С.* Введение в теорию автоматов. М.: Наука, 1985. 320 с.
2. *Бабаш А. В., Шанкин Г. Н.* Криптография. М.: СОЛОН-Р, 2002. 512 с.
3. *Грунский И. С., Козловский В. А.* Синтез и идентификация автоматов. Киев: Наукова думка, 2004. 245 с.

УДК 519.725; 519.816; 519.712.6

ПРОТОКОЛ АРГУМЕНТА ЗНАНИЯ СЛОВА КОДА ГОППЫ И ОШИБКИ ОГРАНИЧЕННОГО ВЕСА

В. Е. Федюкович

Рассматривается задача проверки утверждения об ошибке в искаженном кодовом слове кода Гоппы. Дополнительным условием является предоставление проверяющей стороне минимально необходимой информации о структуре кода, кодовом слове и весе ошибки. Рассматриваются интерактивные протоколы (interactive proof system) и протоколы доказательства знания (proof of knowledge) значений, из которых получены экземпляры привязки (commitment). Произвольный Доказывающий, который не знает компонентов кодового слова и коэффициентов полинома Гоппы, удовлетворяющих проверяемым условиям, имеет только ничтожную вероятность успешно завершить протокол с честным Проверяющим.

Рассматриваются протоколы аргумента, в которых как Проверяющий, так и Доказывающий располагают только полиномиальными ресурсами. Рассматривается схема

запрос – ответ, в которой запросом является значение переменной некоторого полинома над конечным полем, а проверяемым условием — равенство нулю этого полинома.

Рассматриваются условия, эквивалентные определению кодового слова кода Гоппы и утверждению о верхней границе веса ошибки. Также рассматриваются проверочные полиномы, в которых компоненты кодового слова и коэффициенты полинома Гоппы заменяются ответами Проверяющего.

Полученный протокол имеет свойство полноты (completeness), свойство корректности (soundness) в предположении о сложности задачи поиска логарифма в конечной группе, является аргументом знания кодового слова и полинома Гоппы, имеет специальное свойство нулевого разглашения в модели с честным проверяющим (special honest verifier zero knowledge). Ошибка корректности протокола экспоненциально мала, параметром безопасности является количество бит в двоичном представлении порядка группы.

Протокол для слова кода Гоппы, полинома Гоппы и ошибки ограниченного веса

Общая информация Проверяющего и Доказывающего: порядок q и пара элементов группы (h, f), дополнительные значения $\{a_j\}_{j=1\ldots N}$, искаженное кодовое слово $\{w_j\}_{j=1\ldots N}$, экземпляры привязки к коэффициентам полинома $\{V_k\}_{k=0\ldots T}$ и к компонентам кодового слова $\{W_j\}_{j=1\ldots N}$, верхняя граница веса ошибки S.

Информация Доказывающего: коэффициенты полинома $\{g_k\}$ и дополнительные значения $\{\theta_k\}$, компоненты кодового слова $\{b_j\}$ и дополнительные значения $\{\varphi_j\}$, такие, что $V_k = h^{g_k} f^{\theta_k}$, $W_j = h^{b_j} f^{\varphi_j}$ и $g(z) = \sum_{k=0}^{T} z^k g_k$, $\sum_{j=1}^{N} \frac{b_j}{z-a_j} \equiv 0 \pmod{g(z)}$, $|\{j \mid b_j \neq w_j\}| \leqslant S$.

Доказывающий демонстрирует знание значений $\{b_j\}$ и $\{g_k\}$, из которых были получены экземпляры привязки $\{W_j\}$ и $\{V_k\}$, а также справедливость утверждения о весе ошибки.

1) Проверяющий выбирает запрос $d \in \mathbb{F}_q$ и пересылает его Доказывающему.
2) Доказывающий выбирает $\{\alpha_k, \zeta_k\}_{k=0\ldots T}$, $\{\beta_j, \eta_j\}_{j=1\ldots N}$, $\{\mu_t\}_{t=0\ldots N}$, $\{\tau_s\}_{s=0\ldots S} \in \mathbb{F}_q$, получает коэффициенты $\{r_t\}$, $\{p_s\}$, экземпляры привязки $\{U_k\}$, $\{Q_j\}$, $\{R_t\}$, $\{P_s\}$:

$$\sum_{j=1}^{N}(yb_j + \beta_j)\sum_{k=1}^{T}(yg_k + \alpha_k)\frac{d^k - a_j^k}{d - a_j}\prod_{i=1, i\neq j}^{N}\sum_{m=0}^{T}(yg_m + \alpha_m)a_i^m = \sum_{t=0}^{N} y^t r_t,$$

$$\prod_{j=1}^{N}(yb_j + \beta_j - yw_j) = \sum_{s=0}^{S} y^s p_s,$$

$$U_k = h^{\alpha_k} f^{\zeta_k}, \qquad Q_j = h^{\beta_j} f^{\eta_j}, \qquad R_t = h^{r_t} h^{\mu_t}, \qquad P_s = h^{p_s} h^{\tau_s}.$$

Доказывающий пересылает $\{U_k\}, \{Q_j\}, \{R_t\}, \{P_s\}$ Проверяющему.
3) Проверяющий выбирает запрос $c \in \mathbb{F}_q$ и пересылает его Доказывающему.
4) Доказывающий получает ответы и пересылает их Проверяющему:

$$\Psi_k = cg_k + \alpha_k, \qquad \Theta_k = c\theta_k + \zeta_k, \qquad \Omega_j = cb_j + \beta_j, \qquad \Phi_j = c\varphi_j + \eta_j,$$

$$\Delta = \sum_{t=0}^{N} c^t \mu_t, \qquad \Delta' = \sum_{s=0}^{S} c^s \tau_s.$$

5) Проверяющий получает значения проверочных полиномов:

$$\Gamma = \sum_{j=1}^{N} \Omega_j \sum_{k=1}^{T} \Psi_k \frac{d^k - a_j^k}{d - a_j} \prod_{i=1, i\neq j}^{N} \sum_{m=0}^{T} \Psi_m a_i^m, \qquad \Gamma' = \prod_{j=1}^{N} (\Omega_j - cw_j).$$

Проверяющий рассматривает демонстрацию как убедительную, если

$$h^{\Psi_k} f^{\Theta_k} V_k^{-c} = U_k \ \wedge \ h^{\Omega_j} h^{\Phi_j} W_j^{-c} = Q_j \ \wedge \ h^{\Gamma} f^{\Delta} \prod_{t=0}^{N} R_t^{-c^t} = 1 \ \wedge \ h^{\Gamma'} f^{\Delta'} \prod_{s=0}^{S} P_s^{-c^s} = 1.$$

УДК 519

СЛОЖНОСТЬ МЕТОДА ФОРМАЛЬНОГО КОДИРОВАНИЯ ПРИ АНАЛИЗЕ ГЕНЕРАТОРА С ПОЛНОЦИКЛОВОЙ ФУНКЦИЕЙ ПЕРЕХОДОВ

В. М. Фомичев

Обозначим: M_n — множество всех мономов, зависящих от переменных $x_1, \ldots, x_n$; $M_{n,d}$ — подмножество всех мономов степени d, где $0 \leqslant d \leqslant n$. На M_n имеется частичный порядок: $x_{j_1} \cdot \ldots \cdot x_{j_d} \leqslant x_{s_1} \cdot \ldots \cdot x_{s_l} \Leftrightarrow \{j_1, \ldots, j_d\} \subseteq \{s_1, \ldots, s_l\}$. Решётка M_n изоморфна решётке V_n двоичных n-мерных векторов, при этом изоморфизме вектору $\delta = (\delta_1, \ldots, \delta_n) \in V_n$ соответствует моном $x^\delta = x_1^{\delta_1} \cdot \ldots \cdot x_n^{\delta_n} \in M_n$, где $x_j^{\delta_j} = x_j$ при $\delta_j = 1$ и $x_j^{\delta_j} = 1$ при $\delta_j = 0$, $1 \leqslant j \leqslant n$.

Систему уравнений $f_i(x_1, \ldots, x_n) = a_i$, $i = 1, \ldots, m$, заданную полиномами над $GF(2)$, обозначим $F_{m,n} = a$. Левая часть системы определяет отображение $V_n \to V_m$, правая часть $a = (a_1, \ldots, a_m) \in V_m$.

Обозначим: $M(f)$ — множество мономов ненулевой степени полинома $f(x_1, \ldots, x_n)$, $M(F_{m,n}) = \bigcup_{i=1}^{m} M(f_i(x_1, \ldots, x_n))$ — множество мономов ненулевой степени системы всех координатных полиномов $F_{m,n}$. Для полинома $f(x_1, \ldots, x_n)$ (для системы $F_{m,n}$) над $GF(2)$ величину $|M(f)|$ ($|M(F_{m,n})|$) называют *весом полинома* f (*весом системы* $F_{m,n}$), обозначается $wp(f)$ ($wp(F_{m,n})$).

При решении системы уравнений $F_{m,n} = a$ методом формального кодирования каждый ненулевой моном из $M(F_{m,n})$ заменяется новой переменной: $x_{j_1} \ldots x_{j_s} = z_j$, после чего система уравнений $F_{m,n} = a$ преобразуется в линейную систему $L_{m,\nu} = a$ от переменных $z_1, \ldots, z_\nu$, то есть $L_{m,\nu}$ – система m булевых линейных полиномов от ν переменных, где $\nu = wp(F_{m,n})$. Система линейных уравнений $L_{m,\nu} = a$ решается известными методами. При решении совместной системы достаточно рассмотреть лишь максимальную подсистему из μ линейно независимых уравнений, где $\mu = \dim \langle F_{m,n} \rangle$ — размерность линейной оболочки системы полиномов $F_{m,n}$ (число линейно независимых строк матрицы $L_{m,\nu}$). Сложность решения совместной системы уравнений полиномиально зависит от μ и ν. Например, метод Гаусса решения системы уравнений над полем имеет сложность порядка $\max\{\mu, \nu\} \cdot (\min\{\mu, \nu\})^2$ операций поля.

Рассмотрим генератор двоичной гаммы, моделируемый автономным автоматом $A = (V_n, V_1, h, f)$, где V_n — множество состояний; V_1 — выходной алфавит; f — функция выходов; h — функция переходов, реализующая полноцикловую подстановку множества V_n.