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.

Уравнения гаммообразования автомата A описываются системой уравнений $F_{m,n} = a$, где $f_i(x_1,\dots,x_n)$ есть i-я выходная функция автомата: $f_i(x_1,\dots,x_n) = f(h^i(x_1,\dots,x_n))$, $i=1,\dots,m$. Гамма и последовательность $\{f_i(x_1,\dots,x_n)\}$ выходных функций автомата являются чисто периодическими, длины их периодов совпадают и являются делителями числа 2^n.

Пусть длины их периодов равны 2^t, где $1 < t \leqslant n$. Оценим сложность определения начального состояния генератора методом формального кодирования по известному периоду гаммы, то есть по отрезку длины 2^t. Следовательно, требуется определить $\dim\langle F_{2\tau,n}\rangle$ и $|M(F_{2\tau,n})|$, где $\tau = 2^{t-1}$.

Пусть r — натуральное число, $W = \{w_i\}$ — чисто периодическая последовательность над V_r с длиной периода $2\tau = 2^t$, где $\tau > 1$, $m_W(\lambda)$ — минимальный многочлен (над $GF(2)$) последовательности W. Длину периода периодической последовательности W обозначим $\operatorname{per} W$.

Последовательность W *компенсированная*, если $w_1 \oplus \dots \oplus w_{2\tau} = u_r$, где u_r — нуль пространства V_r.

Теорема 1. $m_W(\lambda)=(\lambda\oplus 1)^s$, где $\tau+1\leqslant s\leqslant 2\tau-\varepsilon(W)$ и $\varepsilon(W)=1$ $(=0)$, если W — компенсированная (не компенсированная); при этом $s=\tau+1$, если $w_i \oplus w_{i+\tau} = \alpha$ при $\alpha \neq u_r$ и при всех $i=1,\dots,\tau$.

Следствие 1. $\dim\langle F_{2\tau,n}\rangle \geqslant \tau+1$.

Для автомата A обозначим чисто периодические последовательности: $W(h) = \{h^i(u_n)\}$ — последовательность состояний при начальном состоянии u_n; $f(W(h)) = \{f(h^i(u_n))\}$ — соответствующая ей выходная последовательность; $f(H) = \{f(h^i)\}$ — последовательность выходных функций, $i = 0,1,2,\dots$

На периоде последовательности $W(h)$ определим порядковый номер вектора $\gamma \in V_n$ (обозначим его $n(\gamma)$): $n(u_n) = 0$, $n(\gamma)$ — наименьшее натуральное число t, такое, что $h^t(u_n) = \gamma$. Для монома x^δ степени $d > 0$, где $\delta \in V_n$, определим многочлен $\psi_\delta(\lambda) = \overset{\oplus}{_{\gamma\leqslant\delta}}\lambda^{\nu(\gamma)}$ над $GF(2)$, где $\nu(\gamma)$ – наименьший неотрицательный вычет числа $n(\gamma)$ по $\bmod(2\tau)$; $\leqslant$ есть стандартный частичный порядок на V_n. Многочлен $\psi_\delta(\lambda)$ назовем *A-многочленом монома* x^δ.

Обозначим $g = h^\tau$. Заметим, подстановка g состоит из τ циклов длины $2^n/\tau$.

Лемма 1.

а) Моном x^δ степени $d > 0$ не содержится в $M(f(H)) \Leftrightarrow$ A-многочлен $\psi_\delta(\lambda)$ монома x^δ либо нулевой, либо аннулирующий для последовательности $f(H)$.

б) Если $\psi_\delta(\lambda)$ аннулирует последовательность $f(H)$ и $\gamma \leqslant \delta$ для $\gamma,\delta \in V_n$, то и $g(\gamma) \leqslant \delta$.

Для монома x^δ обозначим: $U_n(x^\delta) = \{\xi \in M_n\colon x^\delta \leqslant \xi\}$; $\overline{U}_n(x^\delta) = M_n \backslash U_n(x^\delta)$. При любом δ из V_n множество $\overline{U}_n(x^\delta)$ не содержит монома x^{e_n} и множество $U_n(x^\delta)$ не пусто и образует в M_n подрешётку, изоморфную решётке $M_{n-\|\delta\|}$, где $\|\delta\|$ — вес вектора δ.

Обозначим также: $M_n(\gamma,\beta) = (U_n(x^\gamma) \cap \overline{U}_n(x^\beta)) \cup (U_n(x^\beta) \cap \overline{U}_n(x^\gamma))$, где $\gamma,\beta \in V_n$.

Теорема 2. Множество $M(f(H))$ содержит $M(f(x_1,\dots,x_n))$ и все мономы степени $d > 0$ из $\bigcup\limits_{\gamma\in V_n} M_n(\gamma, g(\gamma))$ с ненулевым A-многочленом.

Теорема 3. Если $\operatorname{per} f(H) = 2^n$, то $|M(f(H))| \geqslant 2^{n-1}$ и при случайном равновероятном выборе h из класса всех полноцикловых подстановок математическое ожидание оценивается как $E|M(f(H))| \geqslant 2^n - (1{,}5)^n + (1{,}25)^n$.

Выводы

1) Последовательность выходных функций генератора гаммы, построенного на основе полноцикловой подстановки множества состояний V_n, имеет высокую линейную сложность Λ, а именно $2^{n-1}+1 \leqslant \Lambda \leqslant 2^n$.

2) Для порядка множества мономов на периоде последовательности выходных функций генератора верны оценки: $2^{n-1} \leqslant |M(f(H))| \leqslant 2^n - 1$. При $n \to \infty$ и при случайном равновероятном выборе функции переходов h из класса всех полноцикловых подстановок множества V_n математическое ожидание величины $|M(f(H))|/(2^n-1)$ стремится к 1.

3) Сложность T_n определения начального состояния методом формального кодирования оценивается как $TL(2^{n-1}) < T_n < TL(2^n)$, где $TL(m)$ — сложность решения над $GF(2)$ системы линейных уравнений размера $m \times m$.

ЛИТЕРАТУРА

1. *Фомичёв В. М.* Дискретная математика и криптология. М.: ДИАЛОГ-МИФИ, 2003.
2. *Shamir A., Patarin J., Courtois N., and Klimov A.* Efficient Algorithms for solving Overdefined Systems of Multivariate Polynomial Equations // Eurocrypt'2000. Springer. LNCS. 2001. V. 1807.

УДК 65.012.810(075.8)

АВТОМАТИЗИРОВАННЫЕ СРЕДСТВА АНАЛИЗА ПРОТОКОЛОВ[1]

А. В. Черемушкин

Приведем примеры средств автоматизированного анализа криптографических протоколов, которые в настоящее время можно отнести к наиболее эффективным, и рассмотрим математические аспекты работы этих систем. Подчеркнем, что данные средства позволяют не только проверять заданные свойства протоколов, но и находить конкретные атаки на протоколы в случае, когда эти свойства не выполнены. Поскольку информация о конкретных механизмах работы этих систем не всегда доступна, то при их оценке будем опираться только на те сведения, которые опубликованы в печати.

AVISPA

Программный продукт AVISPA появился в начале осени 2005 года. Разработка данного средства проводилась в рамках единого европейского проекта, в котором участвовали LORIA-INRIA (Франция), ETH Цюрих (Швейцария), университет г. Генуя (Италия), Siemens AG (Германия).

Архитектура AVISPA допускает анализ протокола одним из четырех выходных модулей (TA4SP, SATMC, OFMC, CL-AtSe). Спецификация протокола, основанная на ролевом представлении, записывается на языке высокого уровня HLPSL, а затем транслируется во внутренний язык IF. Проверяемые свойства записываются в терминах темпоральной логики. Модуль TA4SP реализует технику, основанную на построении древовидных автоматов и развитую для систем автоматического доказательства. Строится верхняя аппроксимация древовидного автомата, реализующего систему переписывания термов, которая описывает максимальные знания нарушителя. Исследование свойства конфиденциальности теперь сводится к проверке наличия в этом множестве терма, содержащего секрет. Модули SATMC, OFMC, CL-AtSe осуществляют верификацию методом проверки на модели (model checking). Протокол представля-

[1]Работа выполнена при поддержке гранта Президента РФ НШ № 4.2008.10.