СПИСОК ЛИТЕРАТУРЫ:

1. *Balakrishnan G.* Wysinwyx: what you see is not what you execute. PhD thesis. Madison. WI. USA, 2007. Adviser-Reps Thomas.
2. *Cousot P., Cousot R.* Abstract interpretation: a unified lattice model for static analysis of programs by construction or approximation of fixpoints // Conference Record of the Fourth Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages. P. 238–252. Los Angeles. California, 1977. ACM Press. New York. NY.
3. *Fahringer T., Scholz B.* Advanced Symbolic Analysis for Compilers. Springer-Verlag, New York. Inc. Secaucus. NJ. USA, 2003.
4. *Станкевичус А.* Инструментальное средство проверки безопасности кода, предназначенного для исполнения в ГРИД-сетях // Безопасность информационных технологий. 2009. № 1. С. 58–61.

Е. Б. Маховенко, Н. Г. Сюсюгина

АНАЛИЗ КРИПТОСИСТЕМ НА СКРЫТЫХ ОТОБРАЖЕНИЯХ ПОЛЕЙ НЕЧЕТНЫХ ХАРАКТЕРИСТИК

Параметрами алгоритма являются: конечное поле $\mathbf{F} = \mathbf{F}_q$, где q — степень простого числа, n — степень расширения поля $\mathbf{F}$, d — степень секретного полинома $\rho(x)$, а также другие параметры для модификаций алгоритма: l — число исключаемых открытых полиномов для HFE- (добавляемых случайных полиномов для HFE+), v — число новых переменных для HFEv. В качестве характеристик алгоритма рассмотрим время генерации ключевой пары (t_{gen}), скорость шифрования (v_{enc}) и расшифрования (v_{dec}), а также сложность наилучшего алгоритма вскрытия ($diff$, F_4).

В работах [1–3], посвященных алгоритму HFE, рассматривается только зависимость стойкости алгоритма от параметров, причем выбор параметров алгоритма осуществляется исключительно эмпирически. Для нахождения оптимального набора параметров представляется целесообразным оценить все прямые зависимости и далее применить методы теории принятия решений. Выявленные прямые зависимости представлены в таблице 1.

Таблица 1.

y	x	$y(x)$	Параметры	Коэффициент корреляции
Генерация ключевой пары (t_{gen})	q	$y = a+b*\ln x$, $n = 25$, $d = 2$	$a = 2{,}5146$; $b = 0{,}8817$	0,9198
Зашифрование (v_{enc})		$y = a+b*\ln x$, $n = 25$, $d = 2$	$a = 0{,}1026$; $b = 0{,}0254$	0,9228
Расшифрование (v_{dec})		$y = a+b*\ln x$, $n = 25$, $d = 2$,	$a = -0{,}5758$; $b = 0{,}9045$;	0,9834
		$y = a*e^{b*x}$, $n = 25$, $d = 40$	$a = 2{,}1285$; $b = 3{,}2*10^{-3}$	0,9952
Генерация ключевой пары (t_{gen})	n	$y = a*x^{b}*e^{c*x}$, $q = 7$, $d = 2$	$a = 7*10^{-5}$; $b = 3{,}2088$; $c = 0{,}0278$	0,9988
Зашифрование (v_{enc})		$y = a+b*x^4$, $q = 7$, $d = 2$	$a = -0{,}0116$; $b = 4{,}1*10^{-5}$	0,9977
Расшифрование (v_{dec})		$y = a_i*x^{9-i}$, $i = 0$ч9, $q = 7$, $d = 2$	$a_0 = -0{,}47$, $a_1 = -0{,}106$, $a_2 = 1{,}03*10^{-5}$, $a_i = 0$, i=3ч9	0,9942
		$y = a*e^{b*x}$, $q = 7$, $d = 40$	$a = 4{,}4576$; $b = 6{,}3*10^{-3}$	0,9893

Генерация ключевой пары (t_{gen})	d	$y = a+b*\ln x$, $q = 7$, $n = 25$	$a = 3{,}4167$; $b = 0{,}7816$	0,9851
Зашифрование (v_{enc})		$y = a+b*\ln x$, $q = 7$, $n = 25$	$a = 0{,}5164$; $b = 0{,}0073$	0,9964
Расшифрование (v_{dec})		$y = a*x^b$, $q = 7$, $n = 25$	$a = 2{,}1285$; $b = 6$	0,9941

Наиболее трудоемким шагом в процессе расшифрования является нахождение корней секретного полинома степени d в расширенном поле. При $d = 2$ уравнение решается по алгоритму нахождения корней квадратного уравнения, сложность которого — $O((\log q^n)^3)$. При $d \geq 2$ в общем случае необходимо применять алгоритмы Берлекэмпа и Кантора—Цассенхауза [4, 5], сложность которых оценивается, соответственно, $O(d^3 + q^n kd)$, где k — число неприводимых сомножителей полинома, и $O((d\ln d + \ln q^n)d(\ln d)^2 \ln\ln d)$. Для минимизации скорости расшифрования был выбран параметр $d = 2$.

Для нахождения набора параметров $(q, n, d) = (q, n, 2)$ был применен метод многокритериальной оптимизации Парето [6]. Были приняты следующие критерии:

$diff \geq 2^{128}$; $t_{gen} \rightarrow \min$; $v_{enc} \rightarrow \min$; $v_{dec} \rightarrow \min$.

С помощью пакета Mathematica 6.0.3 были построены графики зависимостей характеристик от параметров и найдено множество Парето. Оптимальный набор параметров: $(q, n, d) = (53, 43, 2)$.

Характеристики алгоритма при таких значениях параметров представлены в таблице 2 (AMD Turion(tm) 64 X2 Mobile Technology TL-60 2.00 GHz).

Таблица 2.

Длина сообщения	240 бит (30 байт)
Время генерации ключей	44,187 с
Скорость шифрования	161 бит/с
Скорость расшифрования	20 бит/с
Размер открытого ключа	30 Кб
Размер закрытого ключа	15 Кб

СПИСОК ЛИТЕРАТУРЫ:

1. *Patarin J.* Hidden Field Equations (HFE) and Isomorphisms of Polynomials (IP): Two new families of asymmetric algorithms // Eurocrypt'96. Lecture Notes in Computer Science. Springer-Verlag, 1996. Vol. 1070. P. 33–46.
2. *Jiang X., Ding J., Hu L.* Kipnis-Shamir's attack on HFE revisited. URL: eprint.iacr.org/2007/203.pdf.
3. *Baena J., Clough C., Ding J.* Square-Vinegar signature scheme // PQCrypto 2008. LNCS. Springer, Heidelberg, 2008. Vol. 5299. P. 17–30.
4. *Василенко О. Н.* Теоретико-числовые алгоритмы в криптографии. М.: МЦНМО, 2003.
5. *Лидл Р., Нидеррайтер Г.* Конечные поля: В 2-х томах. Т. 1. Пер. с англ. М.: Мир, 1988.
6. *Подиновский В. В., Ногин В. Д.* Парето-оптимальные решения многокритериальных задач. М.: Наука, 1982.