ISSN 1991-3494

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ
ҰЛТТЫҚ ҒЫЛЫМ АКАДЕМИЯСЫНЫҢ

Х А Б А Р Ш Ы С Ы

ВЕСТНИК

НАЦИОНАЛЬНОЙ АКАДЕМИИ НАУК
РЕСПУБЛИКИ КАЗАХСТАН

THE BULLETIN

OF THE NATIONAL ACADEMY OF SCIENCES
OF THE REPUBLIC OF KAZAKHSTAN

1944 ЖЫЛДАН ШЫҒА БАСТАҒАН
ИЗДАЕТСЯ С 1944 ГОДА
PUBLISHED SINCE 1944

2

АЛМАТЫ
АЛМАТЫ
ALMATY

2015

НАУРЫЗ
МАРТ
MARCH

«Вестник Национальной академии наук Республики Казахстан». ISSN 1991-3494
Собственник: РОО «Национальная академия наук Республики Казахстан» (г. Алматы)
Свидетельство о постановке на учет периодического печатного издания в Комитете информации и архивов Министерства культуры и информации Республики Казахстан **№5551-Ж**, выданное 01.06.2006 г.

Периодичность: 6 раз в год
Тираж: 2000 экземпляров

Адрес редакции: 050010, г. Алматы, ул. Шевченко, 28, ком. 219, 220, тел. 272-13-19, 272-13-18.
www: nauka-nanrk.kz, bulletin-science.kz

Адрес типографии: ИП «Аруна», г. Алматы, ул. Муратбаева, 75

Bulletin of the National Academy of Sciences of the Republic of Kazakhstan.
ISSN 1991-3494

Owner: RPA "National Academy of Sciences of the Republic of Kazakhstan" (Almaty)
The certificate of registration of a periodic printed publication in the Committee of Information and Archives of the Ministry of Culture and Information of the Republic of Kazakhstan N 5551-Ж, issued 01.06.2006

Periodicity: 6 times a year
Circulation: 2000 copies

Editorial address: 28, Shevchenko str., of. 219, 220, Almaty, 050010, tel. 272-13-19, 272-13-18,
http://nauka-nanrk.kz /, http://bulletin-science.kz

Address of printing house: ST "Aruna", 75, Muratbayev str, Almaty

BULLETIN OF NATIONAL ACADEMY OF SCIENCES
OF THE REPUBLIC OF KAZAKHSTAN
ISSN 1991-3494
Volume 2, Number 354 (2015), 198 – 204

EVALUATION OF SUSTAINABLE METHODS OF MODULAR EXPONENTIATION BASED ON PROBABILISTIC APPROXIMATION

A. K. Shaikhanova[1], A. D. Zolotov[2], E. M. Mukhametov[2], M. P. Karpinski[3]

[1]Kazakh National Technical University after K. I. Satpayev, Almaty, Kazakhstan;
[2]Semey State University named after Shakarim, Kazakhstan;
[3]University of Bielsko-Biala, Poland.
E-mail: Igul7@mail.ru,azol64@mail.ru, eldos_sports@mail.ru,mpkarpinski@gmail.com

Key words: time complexity, space complexity, modular exponentiation, binary method, β method, sliding window method.

Abstract. There are various parameters of analysis of computer system as a whole, but the main criterion for evaluating its security subsystem information is resistant to attacks. To ensure trouble-free and efficient operation of the subsystem that runs on RSA cryptographic algorithm, it is necessary to investigate the basic parameters of the algorithms for modular exponentiation. Traditionally it is accepted to estimate the degree of complexity of the algorithm in terms of resources used by the main computer: CPU time and memory. In this regard, such things as the time complexity of the algorithm complexity and volume are considered. A comparative study of the operations of the binary method, β-ary method and sliding window method of a modular exponentiation with reading exponent bits "left to right" and "right to left" is conducted. Studied in this paper stability criteria to the analysis time are sufficient and necessary in the construction of modern computer systems with distributed access.

УДК 004.74.76.2

ОЦЕНКА УСТОЙЧИВОСТИ МЕТОДОВ МОДУЛЯРНОГО ЭКСПОНЕНЦИРОВАНИЯ НА ОСНОВЕ ВЕРОЯТНОСТНЫХ ПРИБЛИЖЕНИЙ

А. К. Шайханова[1], А. Д. Золотов[2], Е. М. Мухаметов[2], М. П. Карпинский[3]

[1] Казахский национальный технический университет им. К. И. Сатпаева, Алматы, Казахстан;
[2] Государственный университет им. Шакарима города Семей, Казахстан;
[3] Техническо-гуманитарная академия г. Бельско-Бяла, Польша

Ключевые слова: временная сложность, объемная сложность, модулярное экспоненциирование, бинарный метод, β-арный метод, метод скользящего окна.

Аннотация. Существуют различные параметры анализа работы компьютерной системы в целом, но основным критерием оценки ее подсистемы защиты информации является устойчивость к атакам. Для обеспечения безотказной и результативной работы этой подсистемы, которая работает по криптоалгоритмам RSA, необходимо исследовать основные параметры алгоритмов выполнения модулярного экспоненцирования. Традиционно принято оценивать степень сложности алгоритма по объему используемых им основных ресурсов компьютера: процессорного времени и оперативной памяти. В связи с этим рассматриваются такие понятия, как временная сложность и объемная сложность алгоритма. Проведено сравнительное исследование операций бинарного метода, β-арного метода и метода скользящего окна медулярного экспоненцирования со считыванием бит экспонентов «слева направо» и «справа налево». Исследованные в данной статье критерии устойчивости к временному анализу, являются достаточными и необходимыми при построении современных компьютерных систем с распределением доступа.

Введение. Проведем имитационное моделирование осуществления злоумышленником временной анализ. Поскольку принято считать, что злоумышленник может измерить время осуществления шифрования сообщения, то время выполнения алгоритма любого метода модулярного экспоненцирования в общем записывается с учетом влияния ошибки измерения времени шифрования и расстояния передачи.

Постановка задачи. Для реализации временной атаки криптоаналитик на идентичном компьютере проводит аналогичное реального экспоненцирования и вычисляет время $\widehat{T}_{i,k-1,0}$ и $\widehat{T}_{i,k-1,1}$ (для каждого метода «слева направо») или $\widehat{T}_{i,0,0}$ и $\widehat{T}_{i,0,1}$ (для каждого метода «справа налево», соответственно) для экспонент 0 и 1 (i - номер проведенного вычисления) [1, 4].

Методика. После этого он может построить таблицу различий между реальным и полученным временами (таблица 1) [2].

Таблица 1 – Различия реального и полученного времен при осуществлении временного анализа

Значение текущего бита равно 0	Значение текущего бита равно 1
$T_1 - \hat{T}_{1,k-1,0}$	$T_1 - \hat{T}_{1,k-1,1}$
$T_2 - \hat{T}_{2,k-1,0}$	$T_2 - \hat{T}_{2,k-1,1}$
$T_3 - \hat{T}_{3,k-1,0}$	$T_3 - \hat{T}_{3,k-1,1}$
...	...

В данной таблице колонка, где есть маленькая разница времени ΔT, соответствующая значению бита экспоненты, анализируется. То есть криптоаналитик может найти значение n_{n-2} для каждого метода «слева направо» или n_1 при считывании битов «справа налево».

Получая аналогичные разницы времени, злоумышленник может найти последовательность битов экспоненты для любого метода.

Результаты. Пусть j_0 – некоторое значение j (порядковый номер бита в представлении экспоненты) в соответствующем алгоритме и $g = \begin{cases} 0, \text{для экспоненты } 0 \\ 1, \text{для экспоненты } 1 \end{cases}$.

Следует отметить, что $\hat{s}_{i,j_0,g} > 0$ для β-арного метода «слева направо», поскольку он не зависит от n_j и $\hat{s}_{i,j_0,g} = \begin{cases} 0, g = 0 \\ > 0, g = 1 \end{cases}$ – время осуществления умножения в β-арном методе «справа налево», когда $n_j = 1$.

Обозначим через binLTR, binRTL – бинарный метод модулярного экспоненцирования «слева направо» и «справа налево», соответственно, βLTR - β-арный метод со считыванием бит «слева направо», βRTL - β-арный метод «справа налево», а *sw*LTR и*sw*RTL - метод скользящего окна «слева направо» и «справа налево», соответственно.

Злоумышленник может вычислить для бинарного, β-арного методов и метода скользящего окна соответствующие времена [5]:

$$\widehat{T}_{i,j_0,g\ \text{binLTR}} = t_i + c_i + \sum_{j=k-1}^{j_0+1} (r_{i,j} + s_{i,j}) + (r_{i,j_0} + \hat{s}_{i,j_0,g}), \quad (1)$$

$$\widehat{T}_{i,j_0,g\ \text{binRTL}} = t_i + c_i + b_i + \sum_{j=0}^{j_0-1} (r_{i,j} + s_{i,j}) + (r_{i,j_0} + \hat{s}_{i,j_0,g}), \quad (2)$$

$$\widehat{T}_{i,j_0,g_{\beta LTR}} = t_i + 2c_i + (\beta - 1)s_i + \sum_{j=k-1}^{j_0+1} (d_{i,j} + s_{i,j}) + (d_{i,j_0} + \hat{s}_{i,j_0,g}), \quad (3)$$

$$\widehat{T}_{i,j_0,g\,\beta\,RTL} = t_i + (\beta+1)c_i + b_i + \sum_{\substack{j=0 \\ n_j=1}}^{j_0-1} d_{i,j} + \sum_{\substack{j=0 \\ n_j=1}}^{j_0-1} (d_{i,j} + s_{i,j}) + (d_{i,j_0} + \widehat{s}_{i,j_0,g}), \quad (4)$$

$$\hat{T}_{i,j_0,g\ SWLTR} = t_i + b_i + (2^{w-1} + p_{j_0})s_i + (p_{j_0}+1)c_i + p_{j_0}q_i + \sum_{j=k-1}^{j_0} s_{i,j} + \sum_{\substack{j=k-1 \\ n_{ji}=0}}^{j_0+1} c_{i,j} + \hat{c}_{i,j_0,g}, \quad (5)$$

$$\hat{T}_{i,j_0,g\ SWRTL} = t_i + b_i + (2^{w-1} + 2 + p_{j_0})c_i + (3\cdot 2^{w-1} + p_{j_0})s_i + p_{j_0}d_i + p_{j_0}q_i + \sum_{\substack{j=0 \\ n_j=0}}^{j_0-1} s_{i,j} + \hat{s}_{i,j_0,g}. \quad (6)$$

А отсюда, соответственно, разница измеренного и вычисленного времени $\Delta T = T_i - \hat{T}_i$ для каждого из исследуемых методов модулярного экспоненцирования с учетом времени e_i, затраченного на прохождение сигналом по каналу связи:

$$\Delta T_{i\,binLTR} = e_i + \sum_{j=j_0-1}^{0} (r_{i,j} + s_{i,j}) + (s_{i,j_0} - \widehat{s}_{i,j_0,g}), \quad (7)$$

$$\Delta T_{i\,binRTL} = e_i + \sum_{j=j_0+1}^{k-1} (r_{i,j} + s_{i,j}) + (s_{i,j_0} - \widehat{s}_{i,j_0,g}), \quad (8)$$

$$\Delta T_{i\beta\,LTR} = e_i + \sum_{j=j_0-1}^{0} (d_{i,j} + s_{i,j}) + (s_{i,j_0} - \widehat{s}_{i,j_0,g}), \quad (9)$$

$$\Delta T_{i\beta_{RTL}} = e_i + \sum_{j=j_0+1}^{k-1} d_{i,j} + \sum_{\substack{j=j_0+1 \\ n_j=1}}^{k-1} s_{i,j} + (s_{i,j_0} - \widehat{s}_{i,j_0,g}), \quad (10)$$

$$\Delta T_{i\ SWRTL} = e_i + (p-p_{j_0})c_i + (p-p_{j_0})s_i + (p-p_{j_0})d_i + (p-p_{j_0})q_i + \sum_{j=j_0+1}^{k-1} s_{i,j} + (s_{i,j_0} - \hat{s}_{i,j_0,g}). \quad (11)$$

Если $\widehat{s}_{i,j_0,g}$ определено правильно, то $\widehat{s}_{i,j_0,g} \equiv s_{i,j_0}$. Отсюда следует, что $\Delta T_{i\,\mathrm{binLTR}} = \mathrm{e_i} + \sum_{j=j_0-1}^{0} (r_{i,j} + s_{i,j})$, $\Delta T_{i\,\mathrm{binRTL}} = \mathrm{e_i} + \sum_{j=j_0+1}^{k-1} (r_{i,j} + s_{i,j})$ (для бинарного метода), $\Delta T_{i\beta_{LTR}} = e_i + \sum_{j=j_0-1}^{0} (d_{i,j} + s_{i,j})$ и $\Delta T_{i\,\beta RTL} = e_i + \sum_{j=j_0+1}^{k-1} d_{i,j} + \sum_{\substack{j=j_0+1 \\ n_j=1}}^{k-1} s_{i,j}$ (для β-арного метода).

Для метода скользящего окна, если $c_{i,j_0} \equiv \hat{c}_{i,j_0,g}$, то $\Delta T_{iSWRTL} = e_i + (p-p_{j_0})(s_i + c_i + d_i + q_i) + \sum_{j=j_0+1}^{k-1} s_{i,j}$ (при считывании бит «справа налево») и $\Delta T_{iSWLTR} = e_i + (p-p_{j_0})(s_i + c_i + q_i) + \sum_{j=j_0-1}^{0} s_{i,j} + \sum_{\substack{j=j_0-1 \\ n_j=0}}^{0} c_{i,j}$ («слева направо»).

Однако на практике $\hat{s}_{i,j_0,g} \neq s_{i,j_0}$ или $c_{i,j_0} \neq \hat{c}_{i,j_0,g}$, а это значит, что правильно

определить $\hat{s}_{i,j_0,g}$ или $\hat{c}_{i,j_0,g}$ очень трудно. Именно поэтому необходимо оценить вероятность успеха атаки.

Применяя методы теории вероятности [2, 6], сначала вычислим дисперсию случайной переменной $T-\hat{T}_{j_0,g}$ со следующими условиями:

1) g определено правильно (то есть правильно найден n_j), тогда дисперсии для каждого из исследуемых методов [6]:

$$\sigma^2(\Delta T)_{binLTR}=\sigma^2(e)+j_0\sigma^2(r)+\frac{1}{2}j_0\sigma^2(s), \tag{12}$$

$$\sigma^2(\Delta T)_{binRTL}=\sigma^2(e)+(k-j_0-1)\sigma^2(r)+\frac{1}{2}(k-j_0-1)\sigma^2(s), \tag{13}$$

$$\sigma^2(\Delta T)_{\beta LTR}=\sigma^2(e)+j_0\sigma^2(d)+j_0\sigma^2(s), \tag{14}$$

$$\sigma^2(\Delta T)_{\beta RTL}=\sigma^2(e)+(k-j_0-1)\sigma^2(d)+\frac{1}{2}(k-j_0-1)\sigma^2(s), \tag{15}$$

$$\sigma^2(\Delta T)_{SWLTR}=\sigma^2(e)+(p-p_{j_0})(\sigma^2(s)+\sigma^2(c)+\sigma^2(q))+j_0\sigma^2(s)+\frac{1}{2}j_0\sigma^2(c), \tag{16}$$

$$\sigma^2(\Delta T_i)_{SWRTL}=\sigma^2(e)+(p-p_{j_0})(\sigma^2(s)+\sigma^2(c)+\sigma^2(d)+\sigma^2(q))+\frac{1}{2}(k-j_0-1)\sigma^2(s). \tag{17}$$

Если предположить, что операции возведения в квадрат и умножения эквивалентны (а в большинстве прикладных реализаций так оно и есть), то есть $r = s$, а также, что время, затраченное на выполнение операции $z=z^{\beta} \bmod m$ равно $(\beta-1)s$, то:

$$\sigma^2(\Delta T)_{binLTR}=\sigma^2(e)+\frac{3}{2}j_0\sigma^2(s), \tag{18}$$

$$\sigma^2(\Delta T)_{binRTL}=\sigma^2(e)+\frac{3}{2}(k-j_0-1)\sigma^2(s), \tag{19}$$

$$\sigma^2(\Delta T)_{\beta LTR}=\sigma^2(e)+\beta j_0\sigma^2(s), \tag{20}$$

$$\sigma^2(\Delta T)_{\beta RTL}=(k-j_0-1)(\beta-\frac{1}{2})\sigma^2(s). \tag{21}$$

2) g определено неправильно, тогда возможны два случая:

а) $\begin{cases}\hat{s}_{i,j_0,g}\neq 0\\ s_{i,j_0}\neq 0\end{cases}$ (для бинарного и β-арного методов)

или $\begin{cases}c_{i,j_0}\neq 0\\ \hat{c}_{i,j_0,g}\neq 0\end{cases}$ (для метода скользящего окна),

тогда [105]:

$$\sigma^2(\Delta T)_{binLTR}=\sigma^2(e)+\left(\frac{3}{2}j_0+2\right)\sigma^2(s), \tag{22}$$

$$\sigma^2(\Delta T)_{binRTL}=\sigma^2(e)+\left(\frac{3}{2}(k-j_0-1)+2\right)\sigma^2(s), \tag{23}$$

$$\sigma^2(\Delta T)_{\beta LTR} = (\beta+1)(j_0+2)\sigma^2(s), \quad (24)$$

$$\sigma^2(\Delta T)_{\beta RTL} = \sigma^2(e) + ((k-j_0-1)(\beta-\frac{1}{2})+2)\sigma^2(s), \quad (25)$$

$$\sigma^2(\Delta T)_{SW\ LTR} = \sigma^2(e) + (p-p_{j_0})(\sigma^2(s)+\sigma^2(c)+\sigma^2(q)) + j_0\sigma^2(s) + (\frac{1}{2}j_0+2)\sigma^2(c), \quad (26)$$

$$\sigma^2(\Delta T)_{SW\ RTL} = \sigma^2(e) + (p-p_{j_0})(\sigma^2(s)+\sigma^2(c)+\sigma^2(d)+\sigma^2(q)) + (\frac{1}{2}(k-j_0-1)+2)\sigma^2(s). \quad (27)$$

б) $\left[\begin{cases} s_{i,j_0} \neq 0 \\ \hat{s}_{i,j_0,g} = 0 \end{cases}\right.$ (для бинарного метода и β-арного метода «справа налево»)
$\left.\begin{cases} \hat{s}_{i,j_0,g} \neq 0 \\ s_{i,j_0} = 0 \end{cases}\right.$

или $\left[\begin{cases} c_{i,j_0} = 0 \\ \hat{c}_{i,j_0,g} \neq 0 \end{cases}\right.$ (для метода скользящего окна). Отсюда:
$\left.\begin{cases} c_{i,j_0} \neq 0 \\ \hat{c}_{i,j_0,g} = 0 \end{cases}\right.$

$$\sigma^2(\Delta T)_{binLTR} = \sigma^2(e) + \left(\frac{3}{2}j_0+1\right)\sigma^2(s), \quad (28)$$

$$\sigma^2(\Delta T)_{binRTL} = \sigma^2(e) + \left(\frac{3}{2}(k-j_0-1)+1\right)\sigma^2(s), \quad (29)$$

$$\sigma^2(\Delta T)_{\beta RTL} = \sigma^2(e) + ((\beta-\frac{1}{2})(k-j_0-1)+1)\sigma^2(s), \quad (30)$$

$$\sigma^2(\Delta T)_{SWRTL} = \sigma^2(e) + (p-p_{j_0})(\sigma^2(s)+\sigma^2(c)+\sigma^2(d)+\sigma^2(q)) + (\frac{1}{2}(k-j_0-1)+1)\sigma^2(s). \quad (31)$$

Дисперсия $\sigma^2(\Delta T)$ может быть использована в качестве критерия правильности предположения бит экспоненты, так столбец таблицы 2.4 разницы времени с правильным предположением имеет разброс на $2\sigma^2(s)$ для β-арного метода «слева направо», $\sigma^2(s)$ и $2\sigma^2(s)$ для бинарного метода и β-арного метода «справа налево», $\sigma^2(c)$ для метода скользящего окна «слева направо» и на $2\sigma^2(c)$ для метода скользящего окна «справа налево» ниже, чем другие столбики значений. То есть, уровень погрешности измерения времени выполнения алгоритма модулярного экспоненцирования зависит от количества измерений. Поэтому необходимо оценить риск утечки секретной информации во время проведения временного анализа рассмотренных методов модулярного экспоненцирования.

Обсуждение. В зависимости риска утечки секретной информации от j_0 для бинарного, β-арного методов и метода скользящего окна, где количество экспериментов равно 100 и экспонента имеет длину 1024 бит, показаны на рисунке 2 и рисунке 2, соответственно [7].

Из рисунков 1 и 2 следует, что риск утечки секретной информации наименьший в случае применения в асимметричной криптосистеме типа RSA β-арного метода «слева направо» или метода скользящего окна «слева направо».

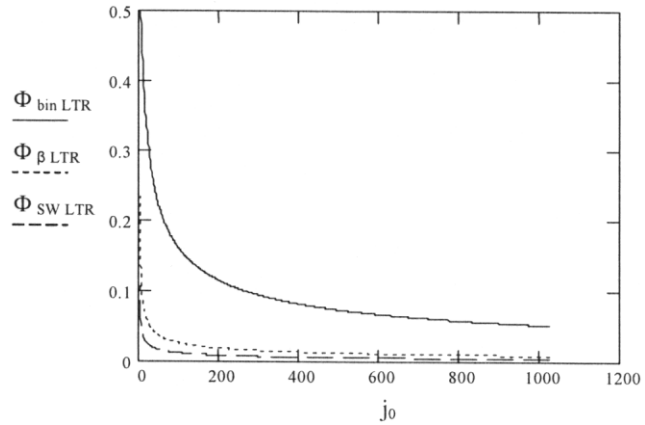

Рисунок 1 –Зависимость риска утечки секретной информации от j_0 в случае считывания битов экспоненты «слева направо»

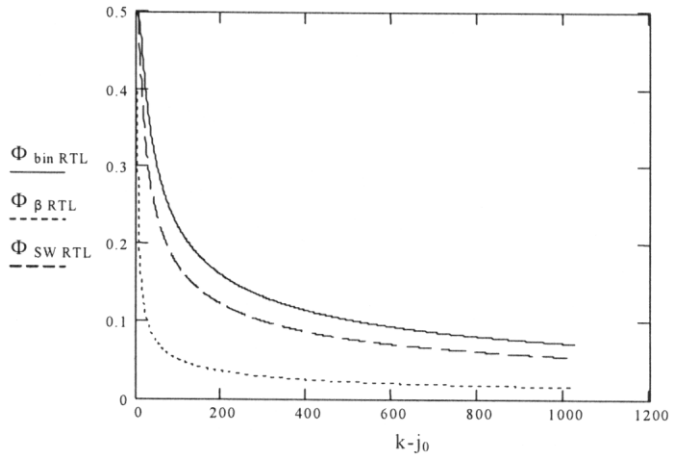

Рисунок 2 – Зависимость риска утечки секретной информации от j_0 в случае считывания битов экспоненты «справа налево»

Заключение. Таким образом, для уменьшения риска утечки секретной информации при осуществлении временного анализа можно предложить следующие пути:

1) увеличение ошибки измерения путем внесения случайных вычислений, чтобы уменьшить возможность правильного определения бит секретного ключа;

2) уменьшение количества сообщений, зашифрованных одним ключом, для уменьшения вероятности риска утечки секретной информации.

Исследованные в данной статье критерии устойчивости к временному аналізу являются достаточными и необходимыми при построении современных компьютерных систем с распределением доступа.

ЛИТЕРАТУРА

[1] Bellezza A. Countermeasures against side-channel attacks for elliptic curve cryptosystems. In: Cryptology ePrint Archive, 2001/103. http://citeseer.ist.psu.edu/bellezza01countermeasures.html.

[2] Biham E., Shamir A. Differential fault analysis of secret key cryptosystems. In: Kaliski B.S. Jr (ed) CRYPTO'97. 17th annual international cryptology conference on advances in cryptology, Santa Barbara, CA, August 1997. Lecture notes in computer science, vol 1294. Springer, Heidelberg, pp 513-525

[3] Конвенция о киберпреступности CETS.No 185. Комитет Конвенции о киберпреступности (T-CY), Страсбург. 2001. http://conventions.coe.int/Treaty/en/Treaties/html/185.htm.

[4] Горбенко И.Д., Горбенко Ю.И. Прикладная криптология. Форт, Харьков. 2012. 458 с.

[5] Kshetri N., Murugesan S. EU and US Cybersecurity Strategies and Their Impact on Businesses and Consumers. Computer 10 (46) 2013: 84-88

[6] Kurose J.F., Ross K.W. Computer networking: A top-down approach, 6th edn. Addison-Wesley, Boston. 2011. 354 p.

[7] Mangard S., Oswald E., Popp Power analysis attacks: Revealing the secrets of smart cards. Springer, Berlin. 2007. 458 p.

[8] Молдовян А.А., Молдовян Н.А., Советов Б.А. Криптография. Санкт-Петербург. Изд-во LAN. 2000. 325 с.

REFERENCES

[1] Bellezza A. *Countermeasures against side-channel attacks for elliptic curve cryptosystems*. In: Cryptology ePrint Archive, 2001/103. http://citeseer.ist.psu.edu/bellezza01countermeasures.html.

[2] Biham E., Shamir A. *Differential fault analysis of secret key cryptosystems*. In: Kaliski B.S. Jr (ed) CRYPTO'97. 17th annual international cryptology conference on advances in cryptology, Santa Barbara, CA, August 1997. Lecture notes in computer science, vol 1294. Springer, Heidelberg, pp 513-525

[3] *Convention on Cybercrime CETS* No 185 The Cybercrime Convention Committee (T-CY), Strasbourg. **2001.**ttp://conventions.coe.int/Treaty/en/Treaties/html/185.htm. (in Russ.).

[4] Gorbenko I.D., GorbenkoY.I. Applied cryptology. Fort. Kharkiv. 2012. 458p. (in Russ.).

[5] Kshetri N., Murugesan S. *EU and US Cybersecurity Strategies and Their Impact on Businesses and Consumers*. Computer 10 (46) 2013: 84-88

[6] Kurose J.F., Ross K.W. *Computer networking: A top-down approach*, 6th ed. Addison-Wesley, Boston. **2011**. 354 p.

[7] Mangard S., Oswald E., Popp. *Power analysis attacks: Revealing the secrets of smart cards*. Springer, Berlin. **2007**. 458 p.

[8] Moldovyan A.A., Moldovyan N.A., Sovyetov B.A. C*ryptography*. LAN ,Saint Petersburg. **2000.** 325p. (in Russ.).

ЫҚТИМАЛДЫҚ ЖАҚЫНДАУЛАР НЕГІЗІНДЕ МОДУЛЯРЛЫ ЭКСПОНЕНЦИРЛЕУ ӘДІСТЕРІНІҢ ТҰРАҚТЫЛЫҚ БАҒАСЫ

А.К.Шайханова[1], А.Д. Золотов[2], Е.М. Мухаметов [2], М.П. Карпинский[3]

[1] Қ. И. Сәтбаев атындағы Қазақ ұлттық техникалық университеті, Алматы, Қазақстан;
[2] Шәкәрім атындағы мемлекеттік университет, Семей, Қазақстан;
[3] Бельско-Бяла қаласының Технико-гуманитарлық академиясы, Польша

Тірек сөздер: уақыт күрделілігі, көлемді күрделілігі, модулярлы экспоненцирлеу, сыңарлы әдіс, β-лы әдіс,сырғымалы терезе әдісі.

Аннотация. Жалпы алғанда, компьютерлік жүйелер жұмысының әртүрлі анализ параметрлері болады, бірақ оның ақпаратының қауіпсіздік жүйесінің бағалау критерийінің негізгісі – шабуылдарға тұрақтылығы болып табылады. RSA криптоалгоритмдары арқылы жұмыс істейтін мына жүйенің нәтижелі жұмысын және тоқтамауын қамтамасыз ету үшін, модулярды экспоненцирлеудің неізгі алгоритм параметрлерін қарастыру қажет. Процессорлы уақытты және жедел жады сияқты компьютерлік ресурстарының қолданатын көлемі бойынша алгоритмнің күрделілік деңгейін дәстүрлі бағалау қабылданған. Осыған орай, алгоритмнің уақыт күрделілігі мен көлемдік күрделілік деген ұғымдар қарастырылған. «Солдан оңға» және «оңнан солға» битэкспонента есебімен модулярды экспоненцирлеудің сырғымалы терезе әдісі және бинарлы әдісінің, β-лы әдісінің салыстыру зерттеулері келтірілген. Берілген мақалада зерттелген уақыт анализине байланысты тұрақтылық критерийі заманауи компьютерлік жүйелердің құрастырылуы жеткілікті және қажет болып табылады.

Поступила 20.03.2015 г.

Publication Ethics and Publication Malpractice
in the journals of the National Academy of Sciences of the Republic of Kazakhstan

For information on Ethics in publishing and Ethical guidelines for journal publication see http://www.elsevier.com/publishingethics and http://www.elsevier.com/journal-authors/ethics.

Submission of an article to the National Academy of Sciences of the Republic of Kazakhstan implies that the described work has not been published previously (except in the form of an abstract or as part of a published lecture or academic thesis or as an electronic preprint, see http://www.elsevier.com/postingpolicy), that it is not under consideration for publication elsewhere, that its publication is approved by all authors and tacitly or explicitly by the responsible authorities where the work was carried out, and that, if accepted, it will not be published elsewhere in the same form, in English or in any other language, including electronically without the written consent of the copyright-holder. In particular, translations into English of papers already published in another language are not accepted.

No other forms of scientific misconduct are allowed, such as plagiarism, falsification, fraudulent data, incorrect interpretation of other works, incorrect citations, etc. The National Academy of Sciences of the Republic of Kazakhstan follows the Code of Conduct of the Committee on Publication Ethics (COPE), and follows the COPE Flowcharts for Resolving Cases of Suspected Misconduct (http://publicationethics.org/files/u2/New_Code.pdf). To verify originality, your article may be checked by the Cross Check originality detection service http://www.elsevier.com/editors/plagdetect.

The authors are obliged to participate in peer review process and be ready to provide corrections, clarifications, retractions and apologies when needed. All authors of a paper should have significantly contributed to the research.

The reviewers should provide objective judgments and should point out relevant published works which are not yet cited. Reviewed articles should be treated confidentially. The reviewers will be chosen in such a way that there is no conflict of interests with respect to the research, the authors and/or the research funders.

The editors have complete responsibility and authority to reject or accept a paper, and they will only accept a paper when reasonably certain. They will preserve anonymity of reviewers and promote publication of corrections, clarifications, retractions and apologies when needed. The acceptance of a paper automatically implies the copyright transfer to the National Academy of Sciences of the Republic of Kazakhstan.

The Editorial Board of the National Academy of Sciences of the Republic of Kazakhstan will monitor and safeguard publishing ethics.

Правила оформления статьи для публикации в журнале смотреть на сайте:

www:nauka-nanrk.kz

bulletin-science.kz

Редакторы *М. С. Ахметова, Д. С. Аленов, Т. А. Апендиев*
Верстка на компьютере *Д. Н. Калкабековой*

Подписано в печать 14.04.2015.
Формат 60x881/8. Бумага офсетная. Печать – ризограф.
18,9 п.л. Тираж 2000. Заказ 2.