ИССЛЕДОВАНИЕ СИММЕТРИЧНОЙ СХЕМЫ ЦИФРОВОЙ ПОДПИСИ, РАЗРАБОТАННОЙ НА БАЗЕ АЛГОРИТМА «ГОСТ Р 34.12-2015»

Бабенко Л.К.[1], Санчес Россель Х.А.[2]

В современном мире широкое распространение получили электронные цифровые подписи, которые служат для предотвращения изменения содержимого передаваемого сообщения и подтверждения подлинности отправителя. В настоящее время для этих целей используют ассиметричные схемы подписи. Ассиметричные схемы на сегодняшний день обладают высокой криптографической стойкостью, однако, нет гарантий, что в будущем они не будут взломаны, так как нет теоретического доказательства невозможности решения задач дискретного логарифмирования в группе точек эллиптической кривой. В свою очередь криптографическая стойкость симметричной схемы цифровой подписи зависит от стойкости блочного шифра, используемого в схеме, поэтому они являются более надежными. В работе приводятся результаты серии экспериментальных исследований по установлению взаимосвязи между количеством подписываемых групп в симметричной схеме цифровой подписи и быстродействием программной реализации. В качестве базового шифра в рассматриваемой схеме использовался симметричный блочный алгоритм шифрования «Кузнечик» (ГОСТ Р 34.12–2015). Приведена информация об экспериментальных стендах и условиях проведения экспериментальных исследований. В ходе работы получена и проанализирована адекватная математическая модель в виде линейного полинома.

***Ключевые слова**: криптография, цифровая подпись, симметричное шифрование, вычислительный эксперимент, математическая модель.*

DOI: 10.21681/2311-3456-2018-2-52-58

Введение

В настоящее время все более широкое распространение получают такие средства компьютерной криптографии, как электронные цифровые подписи, которые можно разделить на две группы, исходя из принципа их работы: симметричные и ассиметричные схемы ЭЦП [1, 2, 4, 7, 10, 12, 16]. По историческим причинам в практических целях используются ассиметричные схемы, так как в эпоху развития концепции цифровой подписи не было достаточно стойких классических алгоритмов шифрования [11, 17, 18], на которых базируются симметричные схемы.

Ассиметричные схемы подписи являются достаточно криптостойкими, однако, нет гарантий, что в будущем они не будут взломаны, так как нет теоретического доказательства не решаемости задачи дискретного логарифмирования в группе точек эллиптической кривой [13-15]. Более надежными в данном случае представляются симметричные цифровые подписи [8], так как их криптостойкость зависит только от стойкости шифра, входящего в их основу.

В работах [5, 6] описывается симметричная схема цифровой подписи, работающая на базе блочного шифра «Кузнечик» [3, 9].

Схема, подробна описанная в этих работах, состоит из трех основных частей: алгоритма формирования ключа, а так же алгоритмов подписи и проверки хэш-блока массива данных.

Ключом схемы является n_k-битовый блок данных представленный как

$$X_j, X = (X_1, X_2, ..., X_{2n_G}), \left| X_j \right| = n. \quad (1)$$

Параметр n_k, косвенно варьируемый в приведенных ниже опытах, связан с уравнением (1) следующей зависимостью:

$$X = \Gamma_{2n_g}(i, K_s) \quad (2)$$

где i – порядковый номер подписи, n_G - число групп, равное

$$n_G = \lceil \frac{n}{n_T} \rceil. \quad (3)$$

Алгоритмы подписи и проверки хэш-блока массива данных в рассматриваемой схеме реализованы по принципу Диффи и Хеллмана с модификации битовых групп.

1 Бабенко Людмила Климентьевна, доктор технических наук., профессор, Южный Федеральный Университет, Таганрог, Россия. E-mail: blk@tsure.ru

2 Санчес Россель Хосе Агустин, Южный Федеральный Университет, Таганрог, Россия и Боливарианский Военный университет, Каракас, Боливарианская Республика Венесуэла. E-mail: jasroda@gmail.com

Таблица1
Конфигурация тестовых стендов

	Стенд 1	Стенд 2	Стенд 3	Стенд 4
Материнская плата	Supermicro, X9DR3-F, Версия BIOS American Megatrends Inc. 1.1, 03.10.2012	Asus M5A99X Evo, версия BIOS American Megatrends Inc. 01.06.2011	MacBook Pro 17» начало 2011	MacBook Pro 17» начало 2011
Процессор	AMD A10-5750M APU with Radeon(tm) HD Graphics 2.50 GHz	QuadCore AMD FX-4100, 4154 MHz	Core i7, 2.3 ГГц, Hyper-Threading включён, всего 8 логических процессора (семейство Sandy Bridge)	Core i7, 2.3 ГГц, Hyper-Threading включён, всего 8 логических процессора (семейство Sandy Bridge)
ОЗУ	8 Гб	2 x 4Gb DDR3 1333 MHz	8 Гб	8 Гб
Жесткий диск	256 Gb SSD	Non-SSD 1TB	512 Гб SSD	512 Гб SSD
ОС	Windows 8	Windows 7 x64	Mac OS X Lion 10.7.5	Mac OS X Lion 10.7.5

Модифицирование заключаются в подписи целых наборов бит:

Пусть $n \leq n_{k..}$ Расширение n в n_k –битные блоки осуществляется процедурой

$$Y = P_{n \to nK}(X).$$

Тогда функция «односторонней криптографической прокрутки» блока T размером n бит k раз определяется рекурсивной функцией:

$$R_k(T) = \begin{cases} T, k = 0, \\ E_{P_{n \to n_k}(R_{k-1}(T))}(X), k \succ 0.' \end{cases} \quad (4)$$

где X – случайный n-битовый блок информации.

В настоящей работе приводится исследование этой схемы методами вычислительного эксперимента с целью ее дальнейшей оптимизации.

Описание экспериментального оборудования и условий проведения экспериментов

Для проведения опытов использовались четыре тестовых стенда, характеристики которых приведены ниже (табл. 1).

Для реализации использовались библиотеки libgcc_s_dw2-1.dll, libstdc++-6.dll, libwinpthread-1.dll, Qt5Cored.dll, Qt5Guid.dll, Qt5Widgetsd.dll. В рамках программы использованы расширения стандартных unit64_t до 128 и 256 бит. Сборка программы осуществлялась с библиотеками Qt 5.7.0 под компилятор «MinGW». Для генерации ключа использовался криптостойкий генератор, интегрированный в программу. Программа позволяет варьировать параметры подписи с целью ее дальнейшей оптимизации.

Для получения математической модели применялись экспериментально-статические методы расчёта и анализа. Для определения уравнения регрессии, отражающего влияние параметров цифровой подписи на быстродействие схемы была разработана программная среда. Графические интерфейсы программ приведены на рисунках 1 и 2.

Опыты проводились поочередно для каждого из тестовых стендов (табл. 1). Кодировались четыре сообщения в порядке, соответствующем номерам опытов (табл. 2).

Первоначально была проведена серия однофакторных исследований:

а) при постоянных значениях параметров i и L варьировался параметр n_T;

б) при постоянном значении параметра n_T варьировался параметр L.

Результаты опытов представлены в виде таблиц (табл. 3, 4) и графиков (рис. 3, 4).

Таблица 2
Подписываемые сообщения

№ Опыта	Сообщение
1	49515544706d516375762e29626a202a547c277d25627d286437447b73
2	3342373c724f535f4f6b3f743568587a485a253c792f6d387a21443169
3	3 другом d72273f50573f4d6721762765495a645f4a5628796e792c3a73286e сообщения45
4	6b6f2f2b523b6d5f743b4f7467376b3a743165745b5b334e4c74505f59

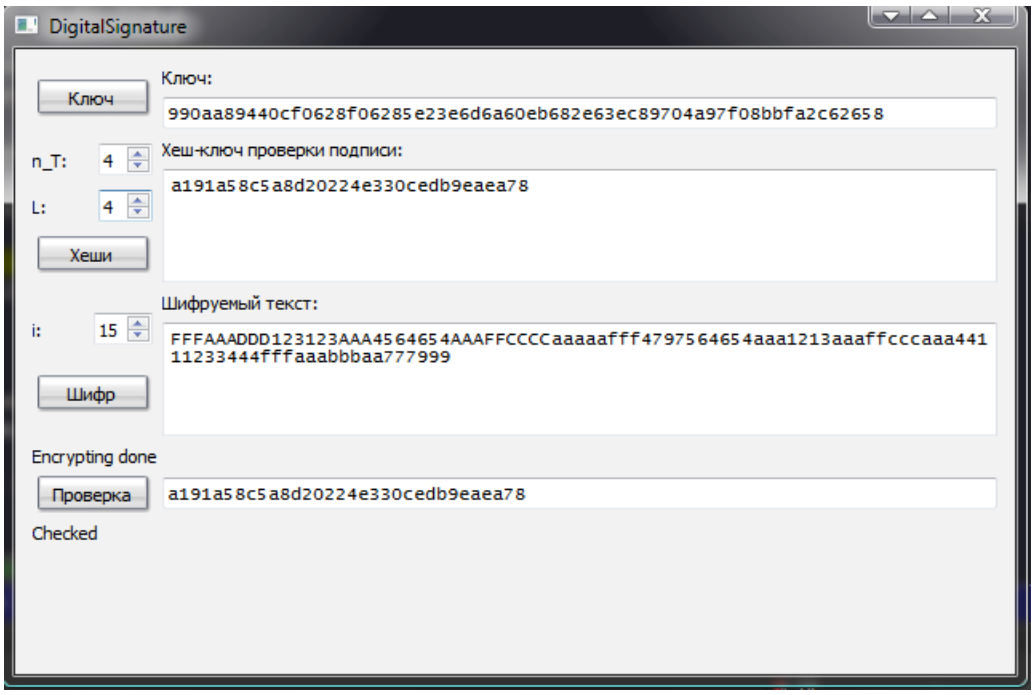

***Рис. 1**. Интерфейс программной реализации симметричной схемы цифровой подписи на базе блочного шифра «Кузнечик»*

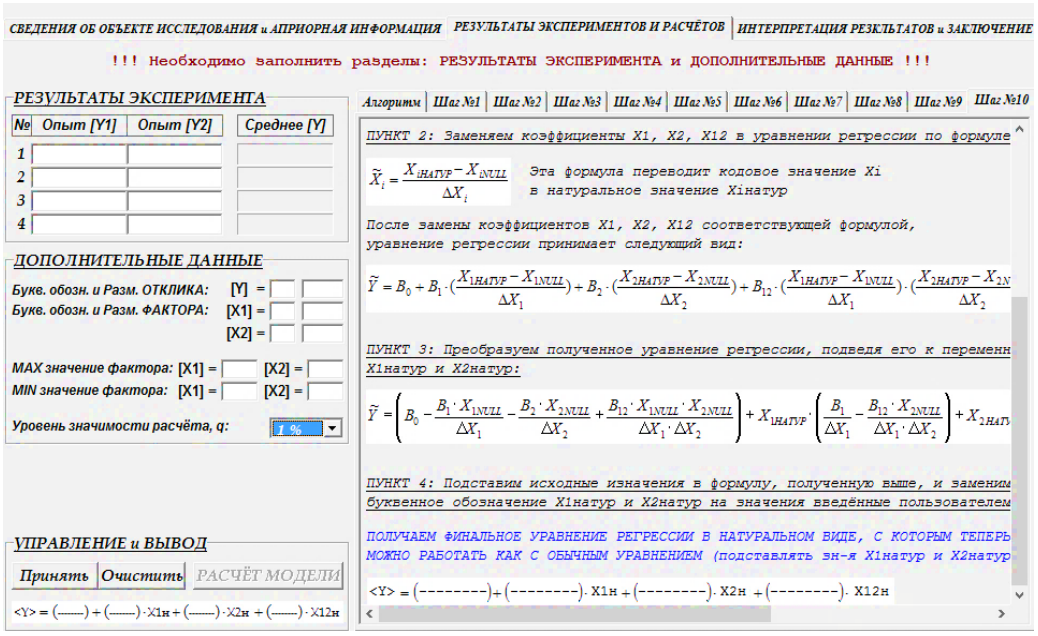

***Рис. 2**. Интерфейс программы расчета финального уравнения регрессии в натуральном виде*

Таблица 3

Результаты исследований t=f(n_T)

i=1, *L*=1		Время шифрования, с	Время хэширования, с	Время проверки, с	Суммарное время *t*, с
№	*n_T*				
1	2	1,204	0,302	0,301	1,807
2	4	3,002	0,753	0,75	4,505
3	6	8,673	2,168	2,166	13,007
4	8	25,489	6,384	6,372	38,245
5	10	83,122	20,808	20,786	124,716

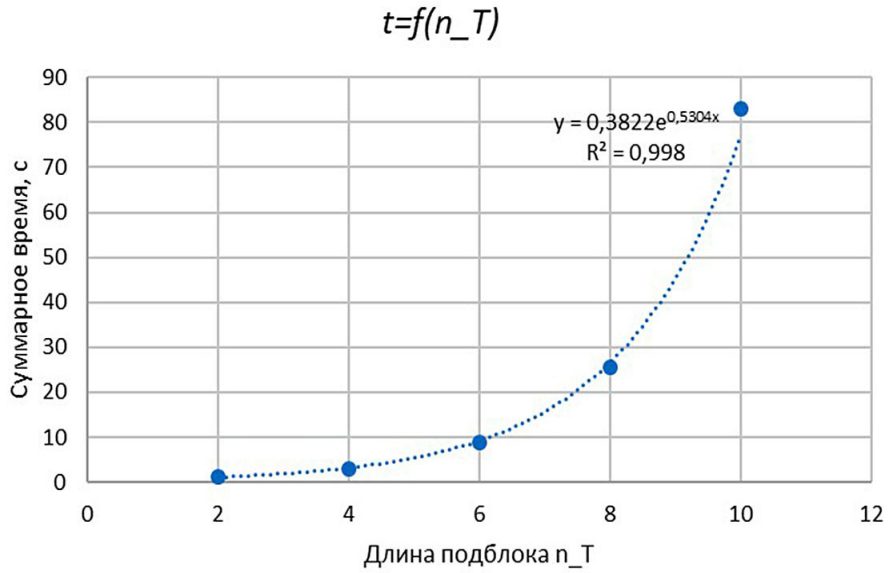

***Рис. 3**. График зависимости функции t=f(n_T)*

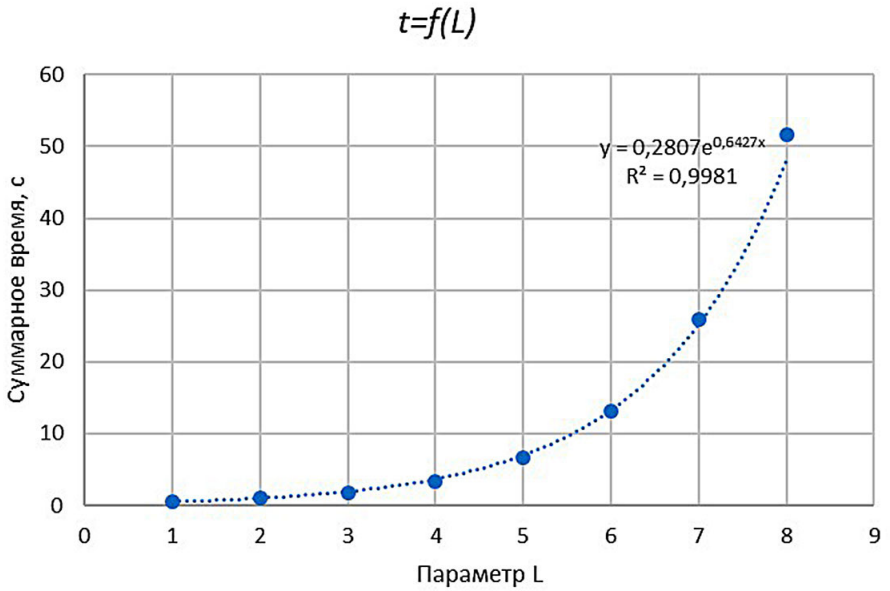

***Рис. 4**. График зависимости функции t=f(L)*

Таблица 4
Результаты исследований t=f(L)

n_T=2			Время полученного шифрования, с	Время хэширования, с	Время проверки, с	Суммарное время t, с
№	*L*	*i*				
1	1	1	1,204	0,302	0,301	0,602333
2	2	3	2,411	0,303	0,302	1,002333
3	3	7	4,818	0,302	0,301	1,807
4	4	15	2,411	0,302	0,301	3,411667
5	5	31	19,267	0,302	0,301	6,323333
6	6	63	38,529	0,302	0,301	13,044
7	7	127	77,092	0,302	0,302	25,89867
8	8	255	154,132	0,301	0,302	51,57833

Таблица 5

Матрица планирования эксперимента

№ Опыта	Факторы		$\tilde{x}_1\tilde{x}_2$	Функция отклика
	n_T –длина подблока (x_1)	L - фактор подписи (x_2)		Суммарное время t, с (y)
1	6 (+1)	4 (+1)	(+1)	60,5457
2	2 (-1)	4 (+1)	(–1)	0,2699
3	6 (+1)	1 (–1)	(–1)	60,5457
4	2 (-1)	1 (–1)	(+1)	0,2699

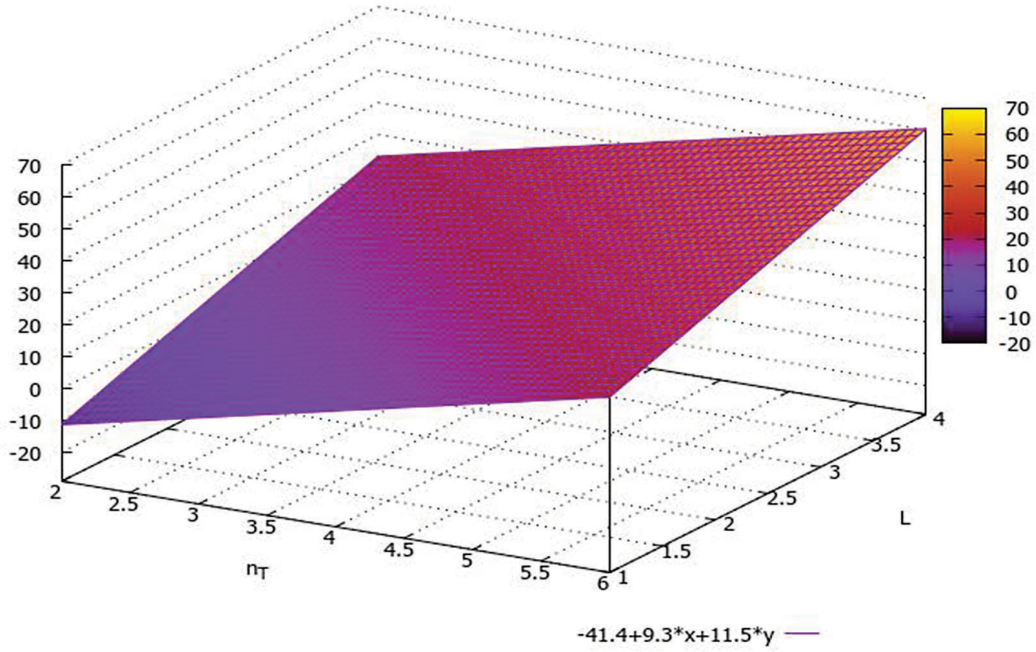

Рис. 5. *Поверхность отклика уравнения (6)*

Для определения уравнений регрессии использован полнофакторный эксперимент.

Матрица планирования эксперимента с усреднёнными экспериментальные результаты, построенная на основании однофакторных исследований приведены в табл. 5.

Предполагаемая математическая модель принята линейной с эффектом взаимодействия между факторами (5):

$$\hat{y} = b_0\tilde{x}_0 + b_1\tilde{x}_1 + b_2\tilde{x}_2 + b_{12}\tilde{x}_1\tilde{x}_2 \qquad (5)$$

На основании приведенных исследований была получена адекватная математическая модель в виде линейного полинома:

$$t = -41.3693 + 9.3183n\_T + 11.5013L \qquad (6)$$

Графически уравнение (6) представлено на рисунке 5.

Таким образом, полученная математическая модель отражает взаимосвязь между суммарным временем процесса создания и проверки реализованной симметричной схемы цифровой подписи, числом бит в подписываемых группах (n_T), а также значением фактора количества подписей (L). Модель позволяет подобрать оптимальную комбинацию параметров, в зависимости от предъявляемых требований ко времени.

Рецензент*: Макаревич Олег Борисович, профессор, доктор технических наук, профессор кафедры Безопасность информационных технологий Южного федерального университета, Таганрог, Россия. E-mail: mak@tsure.ru*

Работа поддержана грантом РФФИ № 18-07-01347А

Литература

1. А.Г. Ростовцев, Е.Б. Маховенко, Теоретическая криптография – СПб.: АНО НПО «Профессионал», 2005. – 480 с.
2. Бабенко Л.К. Ищукова Е.А. Сидоров И.Д. Параллельные алгоритмы для решения задач защиты информации. М.: Горячая линия Телеком, 2014. 304 с.
3. Бабенко Л.К., Ищукова Е.А., Ломов И.С. Математическое моделирование криптографического алгоритма «Кузнечик» // Информационное противодействие угрозам терроризма. 2015. № 24. С. 166–176.
4. Бабенко Л.К., Санчес Россель Х.А. Анализ новых российских криптографических алгоритмов с целью их интеграции в инфокоммуникационные структуры Боливарианской Республики Венесуэла // Информатизация и связь. 2016. № 2. С. 117-120.
5. Бабенко Л.К., Санчес Россель Х.А. Верификация безопасности протокола электронной цифровой подписи с помощью AVISPA // Вопросы кибербезопасности. 2017 №2. С. 45-52.
6. Бабенко Л.К., Санчес Россель Х.А. Разработка и реализация симметричной схемы цифровой подписи на базе алгоритма шифрования «КУЗНЕЧИК» // Фундаментальные исследования. – 2017. – № 11-1. – С. 20-23
7. Бабенко Людмила Климентьевна, Ищукова Евгения Александровна, Маро Екатерина Александровна, Сидоров Игорь Дмитриевич, Кравченко Павел Павлович Развитие криптографических методов и средств защиты информации // Известия ЮФУ. Технические науки. 2012. №4 С.40-50.
8. Березин Б.В., Дорошкевич П.В. Цифровая подпись на основе традиционной криптографии // Защита информации. – М.: МП «Ирбис-II»,1992. – вып. 2. – С. 93–98.
9. Ищукова Е. А., Кошуцкий Р. А., Бабенко Л. К. Разработка и реализация высокоскоростного шифрования данных с использованием алгоритма Кузнечик // Auditorium. 2015. №4 (8)Научная библиотека
10. Резник, С.А. Методы и средства верификации для комбинированного анализа протоколов безопасности / С.А. Резник, И.В. Котенко // Защита информации. Инсайд - 2009. - №3. - С. 56-72.
11. Санчес Россель Х.А. Анализ государственного стандарта шифрования России Гост 28147-89 с целью его интеграции в инфокоммуникационные структуры Боливарианской республики Венесуэла / Россель. Хосе. Санчес // Международный научно-исследовательский журнал. — 2015. — №9 (40) Часть 2. — С. 86—88.
12. Санчес Россель Х.А. Сравнительный анализ старого и нового стандартов РФ на криптографическую функцию хэширования // Международный научно-исследовательский журнал. — 2016. — № 3 (45) Часть 2. — С. 38—40.
13. Чеканов С. Г. Разработка, реализация и анализ криптографического протокола цифровой подписи на основе эллиптических кривых // Вестник ЮУрГУ. Серия: Математическое моделирование и программирование. 2013. №2 С.120-127.
14. Чеканов, С.Г. Криптографические протоколы: основные свойства и уязвимости / С.Г. Чеканов // Вестник ЮУрГУ - 2013. - №2. –Т.6. - С. 120-127.
15. Черемушкин А. В. Автоматизированные средства анализа протоколов // ПДМ. Приложение. 2009. №1 С.34-36.
16. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – Пер. с англ.: М.: Издательство ТРИУМФ, 2002 – 816 с.
17. Babenko L., Ischukova E., Maro E. GOST Encryption Algorithm and Approaches to its Analysis // Theory and Practice of Cryptography Solutions for Secure Information Systems, IGI Global book series Advances in Information Security, Privacy, and Ethics (AISPE) Book Series, Published in the United States of America by Information Science Reference. 2013. P. 34–61.
18. Babenko L.K., Ishchukova E.A., Maro E.A. Research about Strength of GOST 2814789 Encryption Algorithm // Proceedings of the 5th international conference on Security of information and networks (SIN 2012), ACM, New York, NY, USA. P. 80–84.

INVESTIGATION OF THE SYMMETRIC DIAGRAM OF THE DIGITAL SIGNATURE DEVELOPED ON THE BASIS OF THE ALGORITHM «GOST R 34.12-2015»

Babenko L.K.[3], Jose A. Sanchez R.[4]

In the modern world electronic digital signatures are widely used, which serve to prevent the content of the transmitted message from changing and to confirm the authenticity of the sender. At present, asymmetric signature schemes are used for these purposes. Asymmetric schemes today have high cryptographic stability, however, there are no guarantees that in the future they will not be hacked, since there is no theoretical proof of the impossibility of solving discrete logarithm problems in the group of points of an elliptic curve. In turn, the cryptographic stability of a symmetric digital signature scheme depends on the robustness of the block cipher used by the circuit, so they are more reliable. The paper presents the results of a series of experimental studies on establishing the relationship between the number of subscribed groups in a symmetrical digital signature scheme and the speed of software implementation. As a basic cipher in the

3 Liudmila Babenko, Dr.Sc., professor, Southern Federal University, Taganrog, Russia. E-mail: blk@tsure.ru

4 Jose A. Sanchez, Southern Federal University, Taganrog, Russia end Universidad Militar Bolivariana de Venezuela, Caracas, Republica Bolivariana de Venezuela. E-mail: jasroda@gmail.com

scheme under consideration, we used the symmetric block encryption algorithm «Grasshopper» (GOST R 34.12–2015). The information on experimental stands and conditions of carrying out of experimental researches is given. In the course of the work, an adequate mathematical model in the form of a linear polynomial was obtained and analyzed.

***Keywords**: cryptography, digital signature, symmetric encryption, computational experiment, mathematical model.*

References

1. A.G. Rostovcev, E.B. Mahovenko, Teoreticheskaya kriptografiya – SPb.: ANO NPO «Professional», 2005. – 480 s.
2. Babenko L.K. Ishchukova E.A. Sidorov I.D. Parallel'nye algoritmy dlya resheniya zadach zashchity informacii. M.: Goryachaya liniya Telekom, 2014. 304 s.
3. Babenko L.K., Ishchukova E.A., Lomov I.S. Matematicheskoe modelirovanie kriptograficheskogo algoritma «Kuznechik» // Informacionnoe protivodejstvie ugrozam terrorizma. 2015. № 24. S. 166–176.
4. Babenko L.K., Sanches Rossel' H.A. Analiz novyh rossijskih kriptograficheskih algoritmov s cel'yu ih integracii v infokommunikacionnye struktury Bolivarianskoj Respubliki Venesuehla // Informatizaciya i svyaz'. 2016. № 2. S. 117-120.
5. Babenko L.K., Sanches Rossel' H.A. Verifikaciya bezopasnosti protokola ehlektronnoj cifrovoj podpisi s pomoshch'yu AVISPA // Voprosy kiberbezopasnosti. 2017 №2. S. 45-52.
6. Babenko L.K., Sanches Rossel' H.A. Razrabotkai realizaciya simmetrichnoj skhemy cifrovoj podpisi na baze algoritma shifrovaniya «KUZNECHIK» // Fundamental'nye issledovaniya. – 2017. – № 11-1. – S. 20-23
7. Babenko Lyudmila Kliment'evna, Ishchukova Evgeniya Aleksandrovna, Maro Ekaterina Aleksandrovna, Sidorov Igor' Dmitrievich, Kravchenko Pavel Pavlovich Razvitie kriptograficheskih metodov i sredstv zashchity informacii // Izvestiya YUFU. Tekhnicheskie nauki. 2012. №4 S.40-50.
8. Berezin B.V., Doroshkevich P.V. Cifrovaya podpis' na osnove tradicionnoj kriptografii // Zashchita informacii. – M.: MP «Irbis-II»,1992. – vyp. 2. – S. 93–98.
9. Ishchukova E. A., Koshuckij R. A., Babenko L. K. Razrabotka i realizaciya vysokoskorostnogo shifrovaniya dannyh s ispol'zovaniem algoritma Kuznechik // Auditorium. 2015. №4 (8)Nauchnaya biblioteka
10. Reznik, S.A. Metody i sredstva verifikacii dlya kombinirovannogo analiza protokolov bezopasnosti / S.A. Reznik, I.V. Kotenko // Zashchita informacii. Insajd - 2009. - №3. - S. 56-72.
11. Sanches Rossel' H.A. Analiz gosudarstvennogo standarta shifrovaniya Rossii Gost 28147-89 s cel'yu ego integracii v infokommunikacionnye struktury bolivarianskoj respubliki venesuehla / Rossel'. Hose. Sanches // Mezhdunarodnyj nauchno-issledovatel'skij zhurnal. — 2015. — №9 (40) CHast' 2. — S. 86—88.
12. Sanches Rossel' H.A. Sravnitel'nyj analiz starogo i novogo standartov RF na kriptograficheskuyu funkciyu hehshirovaniya // Mezhdunarodnyj nauchno-issledovatel'skij zhurnal. — 2016. — № 3 (45) CHast' 2. — S. 38—40.
13. CHekanov S. G. Razrabotka, realizaciya i analiz kriptograficheskogo protokola cifrovoj podpisi na osnove ehllipticheskih krivyh // Vestnik YUUrGU. Seriya: Matematicheskoe modelirovanie i programmirovanie. 2013. №2 S.120-127.
14. CHekanov, S.G. Kriptograficheskie protokoly: osnovnye svojstva i uyazvimosti / S.G. CHekanov // Vestnik YUUrGU - 2013. - №2. –T.6. - S. 120-127.
15. CHeremushkin A. V. Avtomatizirovannye sredstva analiza protokolov // PDM. Prilozhenie. 2009. №1 S.34-36.
16. SHnajer B. Prikladnaya kriptografiya. Protokoly, algoritmy, iskhodnye teksty na yazyke Si. – Per. s angl.: M.: Izdatel'stvo TRIUMF, 2002 – 816 s.
17. Babenko L., Ischukova E., Maro E. GOST Encryption Algorithm and Approaches to its Analysis // Theory and Practice of Cryptography Solutions for Secure Information Systems, IGI Global book series Advances in Information Security, Privacy, and Ethics (AISPE) Book Series, Published in the United States of America by Information Science Reference. 2013. P. 34–61.
18. Babenko L.K., Ishchukova E.A., Maro E.A. Research about Strength of GOST 2814789 Encryption Algorithm // Proceedings of the 5th international conference on Security of information and networks (SIN 2012), ACM, New York, NY, USA. P. 80–84.