УДК 519.6

РАЗРАБОТКА И РЕАЛИЗАЦИЯ СИММЕТРИЧНОЙ СХЕМЫ ЦИФРОВОЙ ПОДПИСИ НА БАЗЕ АЛГОРИТМА ШИФРОВАНИЯ «КУЗНЕЧИК»

Бабенко Л.К., Санчес Россель Х.А.

ФГАОУ ВПО «Южный федеральный университет», Таганрог, e-mail: blk@ya.ru, jasroda@mail.ru

Настоящая статья посвящена разработке и реализации симметричной схемы цифровой подписи на базе блочного алгоритма шифрования «Кузнечик». Первыми на возможность создания симметричной схемы ЭЦП указали исследователи Диффи и Хеллман, однако в то время, когда они разрабатывали свою схему подписи, не было достаточно стойких классических алгоритмов шифрования, поэтому их идея не получила большого распространения. В работе описан новый российский стандарт шифрования ГОСТ Р 34.10-2012, описаны алгоритмы реализации цифровой подписи, основанные на схеме Диффи и Хеллмана с модификацией битовых групп, предложенной Б.В. Березиным и П.В. Дорошкевичем, которая позволяет обойти ряд классических недостатков подобных схем цифровой подписи. Приведена информация о технических параметрах реализации предлагаемой схемы цифровой подписи.

Ключевые слова: криптография, цифровая подпись, симметричное шифрование, Кузнечик, блочный шифр

DEVELOPMENT AND IMPLEMENTATION OF THE SYMMETRIC DIAGRAM OF THE DIGITAL SIGNATURE ARE BASED ON THE ALGORITHM OF THE «KUZNETCHIK» ENCRYPTION

Babenko L.K., Sanches Rossel Kh.A.

Federal State Autonomous Educational Institution of Higher Professional Education Southern Federal University, Taganrog, e-mail: blk@ya.ru, jasroda@mail.ru

This present paper reports on the results of the development and implementation of a symmetric digital signature scheme on the basis of a block encryption algorithm «Grasshopper». First the possibility of creating a symmetric digital signature scheme, proposed the researchers Diffie and Hallman, but at the time when they developed their signature scheme was not enough proof of the classical encryption algorithms, so the idea has not received wide acceptance. The paper describes a new Russian encryption standard GOST R 34.10-2012 are described and the algorithms for the implementation of digital signature scheme based on Diffie and Hellman with the modification of bit groups proposed by B.V. Berezin, and V.P. Doroshkevich, which avoids a number of classical shortcomings of such schemes a digital signature. The information on technical parameters of implementation of the proposed digital signature scheme is provided.

Keywords: cryptography, digital signature, symmetric encryption, Grasshopper, block cipher

В настоящее время повсеместно используются асимметричные схемы цифровой подписи. В Российской Федерации действующим стандартом такой цифровой подписи является ГОСТ Р 34.10-2012 [1].

Как показали предыдущие исследования [2], ассиметричные схемы являются достаточно криптостойкими, однако, нет гарантий, что в будущем такие ЭЦП не будут взломаны, так как нет теоретического доказательства того, что задачи дискретного логарифмирования в группе точек эллиптической кривой, на которых они базируются, не могут быть решены.

Таким образом, перспективным направлением представляется работа над созданием и исследованием симметричных схем цифровой подписи, использующих «классические» блочные шифры в своей основе.

Первыми на возможность создания симметричной схемы ЭЦП указали исследователи Диффи и Хеллман [3], однако в то время, когда они занимались этим вопросом, не было достаточно стойких классических алгоритмов шифрования, поэтому их идея не получила большого распространения. Сегодня же существует достаточное количество блочных шифров, обладающих высокой криптостойкостью [4–6]. В частности, в июне 2015 г. в РФ утвержден новый стандарт в области криптозащиты ГОСТ Р 34.12-2015, который описывает шифр «Кузнечик», представляющий собой *sp*-сеть [7, 8].

Согласно ГОСТ Р 34.12-2015 128-битный блок информации на входе шифруется следующим образом:

$$E_{k1,\ldots,k10}(a) = X[K_{10}]LSX[K_9]\ldots X[K_2]LSX[K_1](a). \quad (1)$$

Для дешифрования используются те же преобразования, которые применяют в обратном порядке:

$$D_{k1,...k10}(a) = X[K_1]S^{-1}L^{-1}X[K_2]...S^{-1}L^{-1}X[K_9]S^{-1}L^{-1}X[K_{10}](a)\,. \quad (2)$$

Схема цифровой подписи Диффи и Хеллмана в своей основе содержит три алгоритма:

1. Алгоритм G выработки ключевой пары:

$$K_S = (K_0, K_1) = R. \quad (3)$$

2. Алгоритм S выработки цифровой подписи для бита t ($t \in 0, 1\}$):

$$s = S(t) = K_t. \quad (4)$$

3. Алгоритм V проверки подписи для нашего t:

$$V(t,s,K_C) = \begin{cases} 1, E_S(X_t) = C_t \\ 0, E_S(X_t) \neq C_t \end{cases}. \quad (5)$$

где K_C – ключ для проверки, который вычисляется по формуле (6) в виде результата двух процедур шифрования по алгоритму E_k:

$$K_C = (C_0, C_1), \quad (6)$$

где $C_0 = E_{K0}(X_0)$, $C_1 = E_{K1}(X_1)$, блоки X_0 и X_1 известны всем участникам обмена информацией.

Помимо отсутствия надежного шифра распространению схемы Диффи и Хеллмана помешал ряд существенных недостатков, которыми эта схема обладала, среди которых можно выделить то, что алгоритм ЭЦП поддерживает возможность подписи только одного бита, а также в процессе подписи рассекречивается половина ключа.

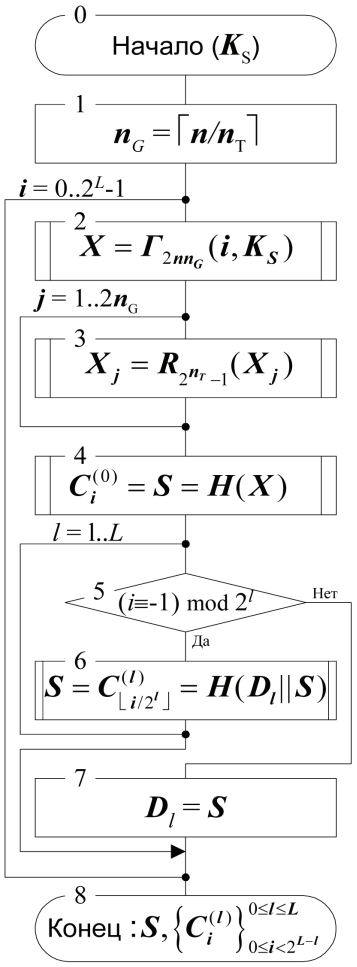

Рис. 1. Алгоритм получения ключа проверки ЭЦП

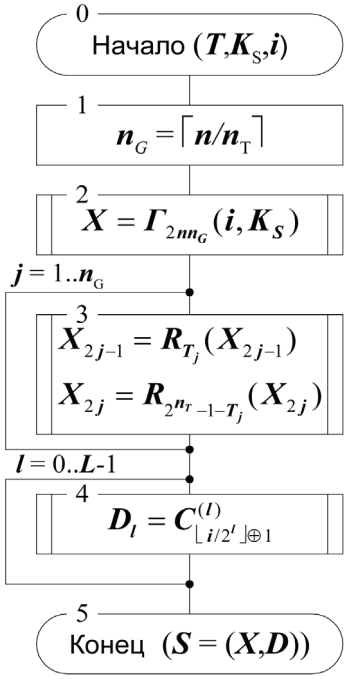

Рис. 2. Алгоритм подписи хэш-кода массива данных

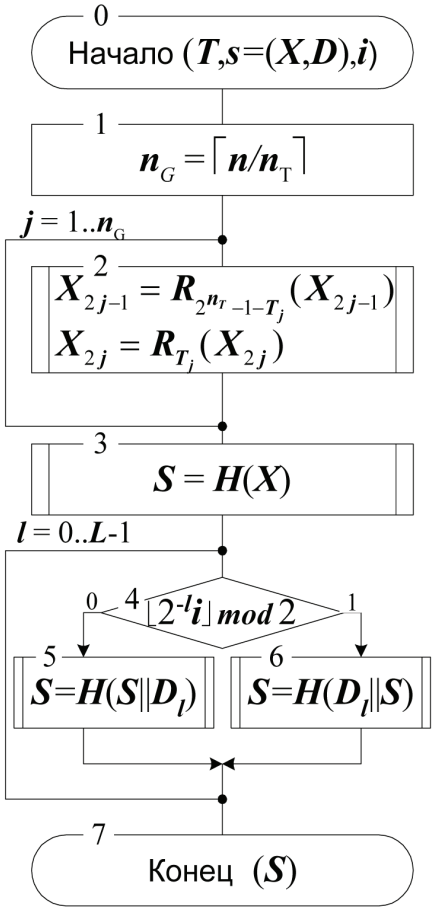

Рис. 3. Алгоритм проверки подписи хэш-блока

Для преодоления этих недостатков предлагается использовать модификацию битовых групп, предложенную Б.В. Березиным и П.В. Дорошкевичем [9].

Модифицирование заключается в подписи целых наборов бит и осуществляется следующим образом: пусть $n \le n_k$ и расширение n в n_K-битовые блоки осуществляется процедурой $Y = P_{n \to nK}(X)$, $|X| = n$, $|Y| = n_K$, тогда функция «односторонней криптографической прокрутки» блока T размером n бит k раз определяется рекурсивной функцией

$$R_k(T) = \begin{cases} T, k = 0, \\ E_{P_{n \to n_k}(R_{k-1}(T))}(X), k \succ 0, \end{cases} \qquad (7)$$

где X – случайный n-битовый блок информации.

Функция осуществляет k раз процедуры:

1) расширение n блока T до размерности n_k,

2) на полученном T зашифровать блок информации X,

3) результат второго пункта внести T.

Ниже приведены алгоритмы симметричной схемы цифровой подписи, использующей в качестве алгоритма шифрования блочный шифр «Кузнечик».

Ключ формируется с помощью генератора псевдослучайных кодов.

Схемы алгоритмов цифровой подписи представлены на рис. 1–3.

Данная схема была реализована программным путем на языке высокого уровня C++ (рис. 4).

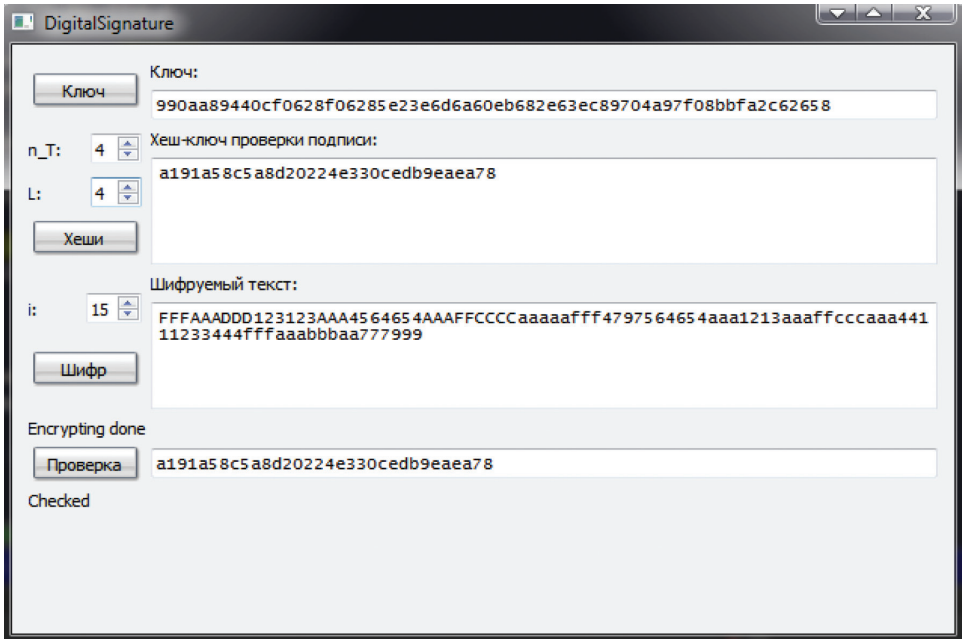

Рис. 4. Программная реализация, где: n_T – длина подблока; L – фактор подписи; i – входной параметр

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.

Так, например, при параметрах $n\_T = 2$, $L = 1$, $I = 1$ время проверки подписи на тестовом стенде (таблица) занимает 1018 миллисекунд.

Характеристики тестового стенда

Материнская плата	Supermicro, X9DR3-F, Версия BIOS American Megatrends Inc. 1.1, 03.10.2012
Процессор	AMD A10-5750M APU with Radeon(tm) HD Graphics 2.50 GHz
ОЗУ	8 Гб
Жесткий диск	256 Gb SSD
ОС	Windows 8

Таким образом, данная схема имеет следующие достоинства:

1. Механизмы выработки, получения и проверки ключей и подписи работоспособны и достаточно просты.

2. Для подписи бита t необходимо по отношению к s решить $E_s(X_t) = C_t$, т.е. это невозможно, если неизвестен ключ.

3. Так как алгоритм криптостойкий и $t \in \{0,1\}$, поэтому подобрать подходящий к подписи t не представляется возможным.

4. Только стойкость шифра оказывает влияние на ЭЦП.

Работа выполнена при поддержке гранта Минобрнауки № 2.6264.2017/8.9.

Список литературы

1. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. ГОСТ Р 34.10-2012. – М.: Стандартинформ, 2012. – 33 с.

2. 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.

3. Diffie W., Hellman M.E. New Directions in cryptography// IEEE Trans. Inform. Theory, IT-22, vol 6 (Nov. 1976). – P. 644–654.

4. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. ГОСТ 28147-89. – М.: Госстандарт СССР, 1989. – 28 с.

5. Информационная технология. Криптографическая защита информации. Блочные шифры. ГОСТ Р 34.12–2015. – М.: Стандартинформ, 2015. – 25 с.

6. Sanchez Rossel Jose Agustin. Analysis of public encryption standard russian gost 28147-89 with a view to its integration in information and communication patterns of the Bolivarian Republic of Venezuela // Международный научно-исследовательский журнал. – 2015. – № 9(40), ч. 2. – С. 86–88.

7. Бабенко Л.К., Ищукова Е.А., Ломов И.С. Математическое моделирование криптографического алгоритма «Кузнечик» // Информационное противодействие угрозам терроризма. – 2015. – № 24. – С. 166–176.

8. Санчес Россель Хосе Агустин. Исследование нового российского алгоритма криптографических преобразований «Кузнечик» // Теоретические и практические проблемы развития современной науки сборник материалов IX Международной научно-практической конференции. – 2015. – С. 33–35.

9. Березин Б.В., Дорошкевич П.В. Цифровая подпись на основе традиционной криптографии // Защита информации. – М.: МП «Ирбис-II»,1992. – вып. 2. – С. 93–98.