Ministry of Education and Science of Ukraine

ODESSA NATIONAL ACADEMY OF FOOD TECHNOLOGIES

International Competition of
Student Scientific Works

BLACK SEA SCIENCE 2018

PROCEEDINGS

April, 4, 2018

ODESSA, ONAFT 2018

Ministry of Education and Science of Ukraine

Odessa National Academy of Food Technologies

International Competition of Student Scientific Works

BLACK SEA SCIENCE 2018

Proceedings

April 4, 2018

Odessa, ONAFT 2018

Міністерство освіти і науки України

Одеська національна академія харчових технологій

Міжнародний конкурс студентських наукових робіт

BLACK SEA SCIENCE 2018

Матеріали

4 квітня 2018 року

Одеса, ОНАХТ 2018

UDC 001(262.5):378.4.091.27(08)
BBC 421D221
B64

Black Sea Science 2018: Proceedings of the International Competition of Student Scientific Works, April 4, 2018, Odessa / Odessa National Academy of Food Technologies; B. Yegorov, M. Mardar (editors-in-chief.) [*et al.*]. – Odessa: ONAFT, 2018. – 827 p.

Proceedings of International Competition of Student Scientific Works «Black Sea Science 2018» contain the works of winners of the competition.

The author of the work is responsible for the accuracy of the information.

ISBN 978-966-289-181-2 Odessa National Academy of Food Technologies

УДК 001(262.5):378.4.091.27(08)
ББК 421D221
В64

Black Sea Science 2018: Матеріали Міжнародного конкурсу студентських наукових робіт, 4 квітня 2018 р., Одеса / Одеська національна академія харчових технологій; Б. В. Єгоров, М. Р. Мардар (відп. ред.) [та ін.]. – Одеса: ОНАХТ, 2018. – 827 с.

Збірник включає матеріали робіт переможців Міжнародного конкурсу студентських наукових робіт «Black Sea Science 2018**».**

За достовірність інформації відповідає автор публікації.

ISBN 978-966-289-181-2 Одеська національна академія харчових технологій

Organizing committee:

Prof. Bogdan Yegorov, D.Sc., Rector of Odessa National Academy of Food Technologies, Head of the Committee

Prof. Maryna Mardar, D.Sc., Vice-Rector for Scientific and Pedagogical Work and International Relations of Odessa National Academy of Food Technologies, Deputy Head of the Committee

Prof. Stefan Dragoev, D.Sc., Vice-Rector on Research and Business Partnerships of University of Food Technologies (Bulgaria)

Prof. Baurzhan Nurakhmetov, D.Sc., First Vice-Rector of Almaty Technological University (Kazakhstan)

Prof. Andrzei Kowalski, Dr. habil., Director of Institute of Agricultural and Food Economics (Poland)

Dr. Olivera Djuragic, Ph.D., Director of Scientific Institute of Food Technology of University of Novi Sad (Serbia)

Prof. Mircea Bernic, Dr. habil., Vice-Rector on Research and Doctorate of Technical University of Moldova (Moldova)

Prof. Jacek Wrobel, Dr. habil., Rector of West Pomeranian University of Technology (Poland)

Prof. Michael Zinigrad, D.Sc., Rector of Ariel University (Israel)

Dr. Mei Lehe, PhD, Vice-President of Ningbo Institute of Technology, Zhejiang University (China)

Prof. Plamen Kangalov, Ph.D., Vice-Rector on Education of "Angel Kanchev" University of Ruse (Bulgaria)

Dr. Alexander Sychev, Ph.D., Assoc. Professor of Sukhoi State Technical University of Gomel (Belarus)

Dr. Hanna Lilishentseva, Ph.D., Assoc. Professor, Head of the Department of Merchandise of Foodstuff of Belarus State Economic University (Belarus)

Prof. Heinz Leuenberger, Ph.D., University of Applied Sciences and Arts Northwestern Switzerland (Switzerland)

Організаційний комітет:

Єгоров Богдан Вікторович – д.т.н., професор, ректор – Одеська національна академія харчових технологій – голова оргкомітету

Мардар Марина Ромиківна – д.т.н., професор, проректор з науково–педагогічної роботи та міжнародних зв'язків – Одеська національна академія харчових технологій – заступник голови оргкомітету

Драгоєв Стефан Георгієв– д.т.н., професор, проректор з наукової роботи і бізнес партнерства – Університет харчових технологій (Болгарія)

Нурахметов Бауржан Кумаргалієвич – д.т.н., професор, перший проректор – Алматинський технологічний університет (Казахстан)

Ковальські Анджей – доктор-хабілітат, професор, директор інституту економіки сільськогосподарської та харчової промисловості – Інститут сільськогосподарської та продовольчої економіки (Польща)

Дюрагіц Олівера – доктор, директор інституту харчових технологій – Університет в м. Нові Сад (Сербія)

Бернік Мірча – доктор-хабілітат, професор, проректор з наукової роботи та докторантури – Технічний університет Молдови (Молдова)

Вробель Яцек– доктор-хабілітат, професор, ректор – Західнопоморський технологічний університет (Польща)

Зініград Михаїл – доктор наук, професор, ректор – Аріельський університет (Ізраїль)

Лехе Мей – доктор, віце-президент – Технологічний інститут Нінбо Чжэцзянського університету (Китай)

Кангалов Пламен – професор, доктор, проректор з навчальної роботи – Русенський університет «Ангел Канчев» (Болгарія)

Сичев Олександр Васильович – к.т.н, доцент, проректор з навчальної роботи – Гомельський державний технічний університет ім. П. Й. Сухого (Білорусь)

Лілішенцева Анна Миколаївна – к.т.н, доцент, зав. кафедрою товарознавства продовольчих товарів – Білоруський державний економічний університет (Білорусь)

Леунбергер Хайнц – доктор, професор – Університет прикладних наук і мистецтв Північно-західної Швейцарії (Швейцарія)

INVESTIGATION OF CODE-BASED CRYPTOGRAPHIC TRANSFORMATIONS AND DIGITAL SIGNATURE SCHEMES

Author – Kiian A.
Supervisor – Svatovskyi I.
V. N. Karazin Kharkiv National University

The paper considers asymmetric crypto-transformations based on the use of algebraic block codes, analyzes the possibilities of using them to improve the confidentiality of information transmission, explores the principles of functioning and the existing contradictions, as well as the prospects for practical use of algorithms for the post-quantum period. A scheme for the formation and verification of the electronic digital signature CFS, as well as an alternative to this scheme, similar to it in terms of design characteristics, is described. Comparative characteristics of the considered algorithms of crypto-transformations are given, their potentially achievable indicators, advantages and disadvantages are analyzed in practical implementation.

ИССЛЕДОВАНИЕ КРИПТОГРАФИЧЕСКИХ ПРЕОБРАЗОВАНИЙ И СХЕМ ЦИФРОВОЙ ПОДПИСИ НА ОСНОВЕ ИСПОЛЬЗОВАНИЯ АЛГЕБРАИЧЕСКИХ КОДОВ

Автор – Киян А.С.
Руководитель – Сватовский И.И.
Харьковский национальный университет им. В. Н. Каразина

Введение

Электронная цифровая подпись (ЭЦП) является цифровым эквивалентом подписи (печати, штампа и пр.), наличие которого в сообщении позволяет с высокой точностью определить источник сообщения (документа) и юридически доказать, что, с определенной вероятностью, только он мог создать и подписать этот документ [1, 2].

С целью формирования ЭЦП на сегодняшний день используются различные криптографические механизмы и протоколы, в которых задача поиска секретного ключа по известному открытому ключу связана с решением известной и чрезвычайно сложной математической задачи(например, факторизации, дискретного логарифмирования, дискретного логарифмирования в группе точек эллиптической кривой). Однако квантовые вычисления позволяют существенно ускорить решение многих математических задач. Например, применение алгоритма Гровера позволяет найти за приемлемое время все простые множители в системе RSA, т. е. найти секретный ключ и/или подделать ЭЦП без знания секретного ключа [3].

Появление квантовых компьютеров, разработкой которых в настоящее время занимаются известные мировые компании такие, как Google, IBM и D-WaveSystems, способно в корне изменить представление об информационной безопасности. По этой причине Национальный Институт Стандартов и Технологий США (NIST) в конце 2016 года объявил открытый конкурс с целью принятия в течение пяти-семи лет новых пост-квантовых стандартов, в частности стандартов электронной цифровой подписи. Это обуславливает актуальность разработки, исследования и обоснования рекомендаций по практическому использованию новых криптосистем, устойчивых как к классическому, так и к квантовому криптоанализу [5, 7].

В настоящее время исследования в области пост-квантовой криптографии ведутся по пяти основным направлениям [5]. Одно из данных направлений основывается на использовании помехоустойчивого кодирования и, в частности, алгебраических блоковых кодов [6, 9]. При использовании подобных систем обеспечивается высокая скорость криптографического преобразования, стойкость к атакам, проводимым с использованием обычных и квантовых компьютеров, а также возможность дополнительного контроля возникающих ошибок [6, 9].

Объектом данного исследования являются теоретические основы, на которых базируется построение наиболее известных кодовых криптосистем Мак-Элиса и Нидеррайтера, а также схемы цифровой підписи CFS (Courtois, Finiasz, Sendrier) [4, 7, 8]. Предметом исследования, в свою очередь, являются алгоритмы функционирования вышеназванных систем, их достоинства и недостатки, а также возможности модификации для улучшения характеристик.

1. Исследование несимметричных криптографических преобразований с использованием алгебраических блоковых кодов

Для полноценного понимания функционирования схем электронной цифровой подписи, которые базируются на применении помехоустойчивого кодирования, необходимо рассмотреть принципы построение кодовых криптосистем, элементы которых используются для формирования подписи. В данной работе исследование будет ограничено рассмотрением криптографических систем Мак-Элиса и Нидеррайтера [4, 8].

1.1. Анализ принципов построения криптосистемы Мак-Элиса

В 1978 году Мак-Элисом (McEliece) была предложена первая криптосистема на алгебраических блоковых кодах[4]. В ее основе лежит маскирование быстрого правила декодирования посредством матричного умножения порождающей матрицы алгебраического блокового кода на случайные невырожденные матрицы (секретный ключ). Полученный результат (открытый ключ) представляет собой порождающую матрицу, имеющую вид случайно выбранных линейно независимых векторов. Злоумышленник, имеющий только открытый ключ, вынужден использовать сложный алгоритм неалгебраического декодирования. Уполномоченный пользователь, знающий секретный ключ, снимает действие маскирования и применяет быстрый алгебраический алгоритм декодирования [4].

Введем следующие обозначения. Зафиксируем конечное поле $GF(q)$. Пусть G – порождающая матрица алгебраического (n,k,d) кода над $GF(q)$, X – невырожденная $k \times k$ матрица с элементами из $GF(q)$, P и D – перестановочная и диагональная $n \times n$ матрицы.

Матрица $G_X = X \cdot G \cdot P \cdot D$ является открытым ключом, маскирующие матрицы X, P и D являются секретным ключом. Криптограммой является искаженное ошибкой e кодовое слово $c_X^* = I \cdot G_X + e$, причем вес Хемминга вектора ошибок удовлетворяет ограничению

$$w_h(e) \le t = \left\lfloor \frac{d-1}{2} \right\rfloor.$$

Вектор $c_X = I \cdot G_X$ является кодовым словом замаскированного кода, т.е. c_X принадлежит (n,k,d) коду с порождающей матрицей G_X, I – k-разрядный информационный вектор над $GF(q)$ [7].

Не зная матрицы X, P и D злоумышленник не может восстановить матрицу G и воспользоваться алгоритмом декодирования полиномиальной сложности. Из этих соображений величину $w_h(e)$ следует максимизировать. Например, при $w_h(e) = t$ обеспечивается наивысший уровень стойкости кодовой криптосистемы для заданных параметров n, k, q.

Уполномоченный пользователь, получив вектор c_X^*, строит вектор $\bar{c}^* = c_X^* \cdot D^{-1} \cdot P^{-1}$. Используя алгоритм полиномиальной сложности, он может декодировать вектор $\bar{c}^* = I' \cdot G + e'$, т.е. найти I'. Затем он вычисляет k-разрядный информационный вектор $I = I' X^{-1}$.

Таким образом, в криптосистеме Мак-Элиса основным средством маскировки линейного блокового *(n, k, d)* кода под линейный случайный код (код общего положения) являются матрицы *X, P, D*. Дополнительным секретным параметром, который можно использовать в случае кодов Гоппы, является многочлен Гоппы*G(x)*, или, в более широком смысле, вектор $Y = (Y_0, Y_1, \ldots, Y_{n-1})$ в случае альтернантных кодов [6]. Изменение шаблона не снижает конструктивных кодовых характеристик, т.е. с точки зрения криптографического преобразования не приведет к снижению безопасности. Однако знание вектора-шаблона $Y = (Y_0, Y_1, \ldots, Y_{n-1})$(или многочлена *G(x)*) является необходимым для правильного декодирования информационного сообщения, т.е. для корректного расшифрования на приемной стороне.

1.2. Изучение основ функционирования теоретико-кодовой схемы Нидеррайтера

Альтернативным примером криптосистем на кодах является схема Нидеррайтера [8]. Открытым ключом в этой криптосистеме есть матрица

$$H_X = X \cdot H \cdot P \cdot D, \qquad (1.2.1)$$

где H – проверочная матрица алгебраического (n, k, d) кода над $GF(q)$ (в оригинальной статье предлагалось использовать обобщенные коды Рида-Соломона), X – невырожденная $(n-k)\times(n-k)$ матрица с элементами из $GF(q)$ P и D – перестановочная и диагональная $n \times n$ матрицы (для двоичных кодов используется только матрица P).

Матрицы X, P и D (как и для криптосистемы Мак-Элиса) являются секретным ключом, который маскирует используемый алгебраический блоковый код под случайный код (код общего положения), т.е. открытый ключ (1.2.1) представляется злоумышленнику как

случайно сформированнаяпроверочная матрица некоторого линейного кода, для которого неизвестен алгоритм быстрого декодирования. Напротив, уполномоченный пользователь, знающий секретный ключ (матрицы X, P и D), может снять действие маскирующих матриц и воспользоваться быстрым алгоритмом декодирования алгебраического кода с проверочной матрицей H [7].

Криптограмма s_X представляет собой вектор длины $(n-k)$ и вычисляется по правилу

$$s_X = e \cdot H_X^T, \qquad (1.2.2)$$

где вектор e – вектор длины n и веса $w_h(e) \le t$, который несет конфиденциальную информацию (информационное сообщение, подлежащее зашифрованию). Наибольшая стойкость обеспечивается при $w_h(e) = t$.

Для расшифрования криптограммы s_X выполняются следующие действия. Уполномоченный пользователь (имеющий секретный ключ) находит одно из q^k решений выражения $s_X = c_X^* \cdot H_X^T$. Найденное решение является кодовым словом с ошибками

$$c_X^* = I \cdot G_X + e.$$

Далее, как и в схеме Мак-Элиса, уполномоченный пользователь строит вектор

$$\overline{c}^* = c_X^* \cdot D^{-1} \cdot P^{-1}$$

и декодирует полученное слово. Однако, вместо восстановления информационного слова I', он вычисляет кодовое слово $c' = I' \cdot G$, а затем и вектор ошибок $e' = \overline{c}^* - c'$. На последнем шаге производится вычисление вектора $e = e' \cdot P \cdot D$, который несет конфиденциальную информацию [8].

Расшифрование s_X может быть выполнено и по следующей схеме. Сначала заметим, что выражение (1.2.2) можно переписать в виде

$$s_X{}^T = H_X \cdot e^T. \qquad (1.2.2^*)$$

В этом случае, уполномоченный пользователь (имеющий матрицы X, P и D) для расшифрования криптограммы вычисляет вектор

$$s_X^{*T} = X^{-1} \cdot s_X{}^T = X^{-1} \cdot H_X \cdot e^T = H \cdot P \cdot D \cdot e^T = H \cdot \bar{e}^T,$$

значение которого зависит от вектора

$$\bar{e}^T = P \cdot D \cdot e^T.$$

Вектор $s_X^{*T} = H \cdot \bar{e}^T$ представляет собой синдром, вычисленный попроверочной матрице H алгебраического (n,k,d) кода, т.е. алгоритм быстрого (алгебраического) декодирования позволяет найти вектор $\bar{e}^T$.После этого уполномоченный пользователь снимает действие матриц маскирования P, D и находит вектор

$$e^T = D^{-1} \cdot P^{-1} \cdot \bar{e}^T = D^{-1} \cdot P^{-1} \cdot P \cdot D \cdot e^T.$$

Подводя итог, можно сказать, что в криптосистеме Нидеррайтера основным средством маскировки линейного кода под случайный код являются (как и в криптосистеме Мак-Элиса) матрицы *X, P, D*. Если использовать коды Гоппы, тогда многочлен *G(x)* может выступать дополнительным секретным параметром [8].

1.3. Сравнительный анализ криптосистем Мак-Элиса и Нидеррайтера

Проведя анализ особенностей рассмотренных систем, можно заметить, что у теоретико-кодовой схемы Мак-Элиса существует ряд преимуществ. Во-первых, это возможность совмещать криптографическое преобразование с контролем возникающих ошибок. Действительно, если при формировании криптограммы использовать случайный вектор ошибок *e*, веса *w(e)*< *t*, тогда появляется возможность одновременно с криптографическим преобразованием данных контролировать ошибки в пределах исправляющей способности. Во-вторых,следует обратить внимание на высокую скорость криптографического преобразования в схеме Мак-Элиса, которая на 3-5 порядков превосходит скорость шифрования в системе RSA (при сопоставимых показателях стойкости). Третье и, очевидно, одно из важнейших положительных свойств криптосистемы Мак-Элиса состоит в высокой устойчивости к квантовомукриптоанализу. По сравнению с другими несимметричными криптосистемами, например, с RSA, сложность квантовогокриптоанализа кодовой криптосистемы с увеличением ее параметров возрастает очень быстро. Фактически сложность криптоанализапри использовании квантовых алгоритмов сопо-

ставима с решением переборных задач поиска эквивалентных ключей симметричных шифров [5].

Стойкости криптосистем Мак-Элиса и Ниддерайтера эквивалентны и эффективную атаку на одну из схем можно легко трансформировать в атаку на другую схему. В этом смысле оценки стойкости криптосистемы Мак-Элиса справедливы и по отношению к криптосистеме Ниддерайтера. Другие характеристики этих криптосистем (скорость шифрования/расшифрования, объемы закрытого и открытого ключа) также сопоставимы.

Очевидным преимуществом теоретико-кодовой схемы Нидеррайтера по сравнению с криптосистемой Мак-Элиса является потенциальнобóльшая относительная скорость передачи данных.

Однако, несмотря на все преимущества рассмотренных схем, стоит выделить недостатки, с которыми сталкиваются разработчики при практическом их применении. Первой конструктивной проблемой являются значительные объемы ключевых данных. В связи с возможностью использования квантовых вычислительных систем эти объемы придется значительно увеличить (примерно в четыре раза). Ключи в кодовых схемах – это генераторные (порождающие и/или проверочные) матрицы линейного кода, которые должны выглядеть для злоумышленника как случайный набор линейно независимых векторов. Сжать или каким-то образом уменьшить этот набор не представляется возможным. В качестве второй проблемы можно выделить низкую относительную скорость передачи данных. Последняя проблема частично решается с использованием «гибридной» схемы, запатентованной в 2017 году [9, 10].

2. Анализ алгоритмов формирования электронной цифровой подписи, основанных на алгебраических кодах

2.1. Исследование схемы формирования ЭЦП CFS

Схема CFS, названная по инициалам своих создателей Courtois, Finiasz и Sendrier, является первым известным алгоритмом формирования и проверки ЭЦП с использованием алгебраических кодов, основана на криптосистеме Нидеррайтера. Оценка стойкости данного алгоритма против подделки подписи может быть сведена к оценке сложности решения задачи синдромного декодирования. Знание секретного ключа позволяет декодеру решить эту задачу для некоторой доли случайных кодовых слов. В алгоритме CFS реализован принцип, который заключается в многократном хешировании доку-

мента, рандомизированного счетчиком битовой длины *r*, пока не будет получен правильно выделенный синдром. Подписавшийся использует свой секретный ключ для определения соответствующего вектора ошибок. Вместе с текущим значением счетчика этот вектор ошибок используется в качестве подписи [7].

Алгоритм формирования подписи согласно данной схемы можно формализовано представить следующим образом:

Шаг 1. Хеширование открытого текста M, т.е. вычисление хеш-кода $h(M)$. Присваивание переменной i значения $i=1$;

Шаг 2. Вычисление хеш-кода $h(h(M)\|i)$, где $h(M)\|i$ – конкатенация (объединение) значений $h(M)$ и i, представленных в виде битовых последовательностей;

Шаг 3. Значение $h(h(M)\|i)$ интерпретируется как синдромная последовательность $s_X=(s_0,s_1,...,s_{n-k-1})$, вычисленная для некоторого (произвольного) кодового слова и вектора ошибок $e=(e_0,e_1,...,e_{n-1})$, т.е. предполагается выполнение равенства (1.2.2*) для соответствующего открытого ключа $H_X=X\cdot H\cdot P$;

Шаг 4.Вычисление значение вектора:

$$s_X^{*T}=X^{-1}\cdot s_X{}^T,$$

который (как предполагается) представляет собой синдром, вычисленный по проверочной матрице H алгебраического (n,k,d) кода, т.е. предполагается, что

$$s_X^{*T}=X^{-1}\cdot s_X{}^T=X^{-1}\cdot H_X\cdot e^T=H\cdot P\cdot e^T=H\cdot\overline{e}^T$$

и алгоритм быстрого декодирования позволит найти вектор $\overline{e}^T=P\cdot e^T$;

Шаг 5. Для синдромной последовательности s_X^* реализуется выполнение быстрого алгоритма декодирования:

если декодирование успешно – выводится найденный вектор ошибок $\overline{e}^T=P\cdot e^T$, который соответствует вектору s_X^*;

если декодирование не успешно – выдается сообщение о невозможности найти вектор ошибок $\overline{e}^T=P\cdot e^T$ для введенного вектора s_X^*. Присваивание переменной i значения $i=i+1$ и переход на Шаг 2;

Шаг 6. Вычисление вектора

$$e^T=P^{-1}\cdot\overline{e}^T=P^{-1}\cdot P\cdot e^T;$$

Шаг 7. Формирование ЭЦП по схеме CFS $Y=(e,i)$ для открытого текста M.

Таким образом, в результате выполнения рассмотренного алгоритма формирования ЭЦП по схеме CFS, вычисляется такое наименьшее положительное целое число i, для которого значение $h(h(M)\|i)$, интерпретируемое как синдромная последовательность $s_X=(s_0,s_1,...,s_{n-k-1})$, соответствует вектору ошибок $e=(e_0,e_1,...,e_{n-1})$, т.е. формально запишем:

$$Y=(e,i): H_X\cdot e^T=\left(h(h(M)\|i)\right)^T. \quad (30)$$

Задача вычисления вектора $e=(e_0,e_1,...,e_{n-1})$ по известному вектору $h(h(M)\|i)$ сопряжена с решением задачи декодирования (n,k,d) кода:

для уполномоченного пользователя (знающего секретный ключ) это вычислительно простая задача (полиномиальной сложности);

для злоумышленника (знающего только открытый ключ) это вычислительно сложная задача декодирования случайного кода (относящаяся к классу сложности NP-полных задач).

Для верификации (проверки правильности ЭЦП $Y=(e,i)$ сообщения M) необходимо убедится в том, является ли результат хеширования $h(h(M)\|i)$ синдромной последовательностью, вычисленной по вектору $e=(e_0,e_1,...,e_{n-1})$ (который интерпретируется как вектор ошибок)[10].

2.2. Изучение альтернативного алгоритма формирования цифровой подписи

Схема формирования и проверки ЭЦП, запатентованная в 2017 году, использует одностороннюю функцию из схемы Мак-Элиса. Для этого подписываемое информационное сообщение M (его сжатый образ) непосредственно связывается со значением c_X^* и только уполномоченный пользователь, знающий секретные матрицы X и P в $G_X=X\cdot G\cdot P$, сможет применить быстрый (полиномиальной сложности) алгоритм декодирования для нахождения векторов I и e. Эти вектора совместно со вспомогательной информацией (значение счетчика i) составляют подпись $Y=(I,e,i)$ сообщения M. Для проверки (верификации) подписи достаточно владеть открытым ключом (матрицей G_X) – для этого достаточно вычислить c_X^* и сравнить его с сжатым образом информационного сообщения. Таким образом, вычислить c_X^* по извест-

ным G_X, I и e (проверить ЭЦП) вычислительно легко (полиномиальная сложность), а найти I и e по известным G_X и c_X^* (сформировать ЭЦП) чрезвычайно сложно (NP-полная задача) [11].

Реализация предлагаемой схемы формирования и проверки ЭЦП осуществляется в соответствии со следующими алгоритмами.

1. Системные параметры: $m, t \in N$;

2. Генерация ключа: генерация пары ключей как в криптосистеме Мак-Элисана основе использования алгебраического кода из класса неприводимых кодов Гоппы. Для двоичного случая кодовые параметры связаны соотношениями: ($n = 2^m$, $k = n - mt$, $2t + 1$). Порождаются следующие матрицы:

матрица G: $k \times n$ – порождающая матрица алгебраического кода с исправляющей способностью t ошибок,

матрица X: $k \times k$- случайная обратимая матрица,

матрица P: $n \times n$- случайная матрица перестановок;

В случае применения недвоичных кодов используется также матрица D: $n \times n$- случайная диагональная матрица.

Открытый ключ: матрица $G_X = X \cdot H \cdot P \cdot D$ (для двоичного случая $G_X = X \cdot H \cdot P$) и число t(исправляющая способность кода).

Секретный ключ: матрицы X, P и, для недвоичного случая, матрица D Быстрый (полиномиальной сложности) алгоритм декодирования алгебраического кода.

Алгоритм декодирования позволяет по введенному кодовому слову с ошибками $c_X^* = (c*_0, c*_1, ..., c*_{n-1})$ в случае успеха декодирования найти вектор ошибок $e = (e_0, e_1, ..., e_{n-1})$ и вектор $I = (I_0, I_1, ..., I_{k-1})$, причем $c_X^* = I \cdot G_X + e$. В противном случае (если декодирование не удалось) алгоритм выдает отказ в декодировании вектора $c_X^* = (c*_0, c*_1, ..., c*_{n-1})$, т.е. по такой последовательности алгоритм не может найти вектор ошибок $e = (e_0, e_1, ..., e_{n-1})$ и вектор $I = (I_0, I_1, ..., I_{k-1})$.

3. Формирование подписи

Вход:

h – функция хеширования, которая применяется к входным данным x (аргументу функции) произвольной длины. Результатом хеширования является хеш-код $h(x)$ длины n кодовых символов (для двоичных кодов – n бит);

быстрый (полиномиальной сложности) алгоритм декодирования алгебраического кода, который применяется ккодовому слову с

ошибками $c_X^* = (c*_0, c*_1, ..., c*_{n-1})$. Предполагается, что в результате выполнения алгоритма декодирования возможны две ситуации:

если декодирование успешно – выводятся векторы $e = (e_0, e_1, ..., e_{n-1})$ и $I = (I_0, I_1, ..., I_{k-1})$, которые соответствует вектору $c_X^* = (c*_0, c*_1, ..., c*_{n-1})$;

если декодирование не успешно – выдается сообщение о невозможности найти векторы $e = (e_0, e_1, ..., e_{n-1})$ и $I = (I_0, I_1, ..., I_{k-1})$ для введенного вектора $c_X^* = (c*_0, c*_1, ..., c*_{n-1})$;

открытый текст M, для которого необходимо сформировать ЭЦП.

Выход:

ЭЦП Y для открытого текста M.

Предлагаемый алгоритм формирования ЭЦП (алгоритм представлен для общего случая недвоичных кодов, для двоичного случая матрица D не используется)[11]:

Шаг 1. Хешированиеоткрытого текста M, т.е. вычисление хеш-кода $h(M)$. Присваивание переменной i значения $i = 1$;

Шаг 2.Вычисление хеш-кода $h(h(M)\|i)$, где $h(M)\|i$ – конкатенация (объединение) значений $h(M)$ и i, представленных в виде двух последовательностей;

Шаг 3. Значение $h(h(M)\|i)$ интерпретируется как кодовое слово с ошибками $c_X^* = (c*_0, c*_1, ..., c*_{n-1})$, вычисленное для некоторых $I = (I_0, I_1, ..., I_{k-1})$ и $e = (e_0, e_1, ..., e_{n-1})$, причем $c = IG_X$, $c_X^* = c + e$, т.е. предполагается выполнение равенства (19) для соответствующего открытого ключа $G_X = X \cdot H \cdot P \cdot D$;

Шаг 4.Вычисление значения вектора

$$\bar{c}^* = c_X^* \cdot D^{-1} \cdot P^{-1},$$

который (как предполагается) представляет собой искаженное не более чем в t разрядах кодовое слово алгебраического (n, k, d) кода с порождающей матрицей G и его можно декодировать быстрым алгоритмом полиномиальной сложности, т.е. предполагается, что

$\bar{c}^* = c_X^* \cdot D^{-1} \cdot P^{-1} = (I \cdot G_X + e) \cdot D^{-1} \cdot P^{-1} = (I \cdot X \cdot H \cdot P \cdot D + e) \cdot D^{-1} \cdot P^{-1} = I \cdot X \cdot H + e \cdot D^{-1} \cdot P^{-1}$

и алгоритм быстрого декодирования позволит найти вектор $I' = I \cdot X$ посредством декодирования слова $\bar{c}^* = I' \cdot G + e'$, $e' = e \cdot D^{-1} \cdot P^{-1}$;

Шаг 5. Для слова $\bar{c}^* = I' \cdot G + e'$ реализуется выполнение быстрого алгоритма декодирования:

если декодирование успешно – выводятся найденные векторы $I' = I \cdot X$ и $e' = e \cdot D^{-1} \cdot P^{-1}$, которые соответствует вектору $\vec{c}^{*} = I' \cdot G + e'$;

если декодирование не успешно – выдается сообщение о невозможности найти векторы $I' = I \cdot X$ и $e' = e \cdot D^{-1} \cdot P^{-1}$ для введенного вектора $\vec{c}^{*}$. Присваивание переменной i значения $i = i + 1$ и переход на Шаг 2;

Шаг 6. Вычисление векторов

$$I = I' X^{-1} \text{ и } e = e' \cdot D \cdot P;$$

Шаг 7. Формирование ЭЦП $Y = (I, e, i)$ для открытого текста M.

Таким образом, в результате выполнения рассмотренного алгоритма формирования ЭЦП, вычисляется такое наименьшее положительное целое число i, для которого значение $h(h(M)\|i)$, интерпретируемое как кодовое слово с ошибками c_X^{*}, соответствует кодовому слову $c = IG_X$ и вектору ошибок e, т.е. формально запишем:

$$Y = (I, e, i) : IG_X + e = \left(h(h(M)\|i)\right). \qquad (2.2.1)$$

Задача вычисления векторов I и e по известному вектору $h(h(M)\|i)$ сопряжена с решением задачи декодирования (n, k, d) кода:

- для уполномоченного пользователя (знающего секретный ключ) это вычислительно простая задача (полиномиальной сложности);
- для злоумышленника (знающего только открытый ключ) это вычислительно сложная задача декодирования случайного кода (относящаяся к классу сложности NP-полных задач).

Для верификации (проверки правильности ЭЦП $Y = (I, e, i)$ сообщения M) необходимо убедится в том, является ли результат хеширования $h(h(M)\|i)$ кодовым словом с ошибками c_X^{*}, вычисленным по векторам I и e [11].

2.3.Сравнительная характеристика CFS и предлагаемой схемы

Как говорилось ранее, схема CFS базируется на криптосистеме Нидеррайтера, а в основу предложенной схемы был положен принцип, используемый в системе Мак-Элиса. Известно, что стойкость несимметричных криптосистем Мак-Элиса и Нидеррайтера эквивалентна. Таким образом, можно принять предположение о тождественности оценок стойкости соответствующих ЭЦП (по схеме CFS и по предлагаемой схеме),

Основные конструктивные характеристики предлагаемой схемы формирования и проверки ЭЦП сопоставимы с характеристиками ЭЦП по схеме CFS. При этом для высокоскоростных кодов (с $R = \frac{k}{n} > \frac{1}{2}$) объем ключевых данных схемы Нидеррайтера меньше, чем у схемы Мак-Элиса, а для низкоскоростных (с $R = \frac{k}{n} < \frac{1}{2}$) – наоборот, меньший объем ключей имеет схема Мак-Элиса. Схемы ЭЦП (предлагаемая и CFS) наследуют это свойство. Ввиду добавления в ЭЦП $Y = (I, e, i)$ вектора I битовая длина подписи больше, по сравнению со схемой CFS, на $2^m - m \cdot t$ бит.Объем ключевых данных в предлагаемой схеме определяется объемом ключевых данных несимметричной криптосистемы Мак-Элиса:

- битовая длина открытого ключа (число двоичных ячеек матрицы $G_X = X \cdot G \cdot P$)

$$l_{о.к.} = k \cdot n = (2^m - m \cdot t) \cdot 2^m;$$

- битовая длина закрытого ключа (число двоичных ячеек матрицы X плюс битовая длина n целых чисел в диапазоне $0,1,..,n-1$ для указания правила заполнения матрицы P)

$$l_{з.к.} = k^2 + n \cdot \lceil \log_2 n \rceil = (2^m - m \cdot t)^2 + 2^m \cdot m.$$

Также стоит отметить, что предлагаемая процедура верификации защищена от быстрой подделки подписи $Y = (I, e, i)$ на основе добавления произвольного кодового слова применяемого (n, k, d) кода. Так, если выбрать произвольное кодовое слово $\hat{c}$ используемого (n, k, d) кода с порождающей матрицей G_X, тогда можно попытаться подделать подпись $Y = (I, e + \hat{c}, i)$. Однако равенство (2.2.1)не будет выполняться:

$$Y = (I, e + \hat{c}, i) : IG_X + e + \hat{c} \neq \left(h(h(M) \| i)\right).$$

Это очевидное преимущество предлагаемой схемы ЭЦП дополнительно усилено введенной проверкой веса вектора e, которая предназначена для защиты от других гипотетических атак (например, одновременной подделки и вектора I и вектора e).

Анализируя полученные результаты, можно сделать вывод, что предлагаемая схема формирования ЭЦП являются реальной альтерна-

тивой первому известному алгоритму формирования подписи с использованием алгебраических кодов – CFS, поскольку их основные конструктивные характеристики сопоставимы. Кроме того, предлагаемая схема обладает достоинствами, отсутствующими у CFS (одновременное использование вектора I и вектора e).

Выводы

На основе проведенного анализа можно констатировать, что криптосистемы и схемы электронной цифровой подписи, основанные на алгебраическом кодировании, являются перспективным направлением для дальнейшего развития, поскольку предоставляют широкий спектр возможностей. Такими их достоинствами являются высокая скорость криптографического преобразования, стойкость к атакам, осуществленным на обычных и квантовых компьютерах, а также дополнительный контроль возникающих при передаче по каналу связи ошибок.

Во время проведения исследования были рассмотрены кодовые криптосистемы Мак-Элиса и Нидеррайтера, а также алгоритмы формирования и проверки ЭЦП на их основе. В частности, с использованием криптопреобразований по схеме Мак-Элиса была предложена модифицированная схема ЭЦП, которая по своим основным параметрам (длине ключей, длине подписей, стойкости) сопоставима с известной схемой CFS. Основным отличием предложенной схемы ЭЦП является способ формирования подписи: информационная последовательность (ее сжатый образ) интерпретируется не как синдром кодового слова, а как искаженное ошибками кодовое слово.

Применение предложенного способа позволяет получить весомое преимущество в том, что она позволяет защититься от быстрой подделки подписи на основе добавления произвольного кодового слова применяемого кода. Указанное преимущество дополнительно усилено введенной проверкой веса Хемминга, которая предназначена для защиты от других возможных атак на криптосистему, как, например, атаки одновременной подделки нескольких элементов подписи.

Список использованной литературы

1. Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone. Handbook of Applied Cryptography – CRC Press, 1997. – 794 p.

2. ArtoSalomaa. Public-Key Cryptography, Second, Enlarged Edition. – Springer-Verlag, Berlin, Heidelberg, New York, 1996. – 271 p.

3. Grover L. A fast quantum mechanical algorithm for database search. // Proceedings of the 28th annual ACM symposium on the theory of computing (STOC, 96). ACM Press, New York. – 1996. – P. 212–219.

4. McEliece R. J. A public-key cryptosystem based on algebraic coding theory. DSN Progress Report 42-44, Jet Propulsion Lab., Pasadena, CA, January-February, 1978. P. 114-116.

5. NISTIR 8105 DRAFT Report on Post-Quantum Cryptography. National Institute of Standards and Technology Internal, Report 8105, February 2016. – 15 p.

6. Морелос-Сарагоса Р. Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение / пер. с англ. В. Б. Афанасьева. – М.:Техносфера, 2006.

7. Bernstein, Daniel J., Buchmann, Johannes, and Dahmen, Erik. Post-Quantum Cryptography. – 2009, Springer-Verlag, Berlin-Heidleberg. – 245 p.

8. Niederreiter H. Knapsack-type cryptosystems and algebraic coding theory // Problem Control and Inform Theory, 1986, v. 15. P. 19-34.

9. Yu. V. Stasev, A. A. Kuznetsov. Asymmetric Code-Theoretical Schemes Constructed with the Use of Algebraic Geometric Codes // Cybernetics and Systems Analysis, Volume 41, Issue 3, May 2005, Pages 354-363.

10. Пат.116150 Україна, МПК(2017.01) H 03 M 13/00, H 03 M 13/19, G 06 F 21/72.Спосіб несиметричного криптографічного перетворення з використанням алгебраїчних блокових кодів / Кузнецов О.О., ПушкарьовА.І., СватовськийІ.І., Шевцов О. В, Кузнецов Т.Ю.; заявник та патентовласник Харківський національний університет імені В.Н.Каразіна.- № 201611744;заявл.21.11.2016; опубл. 10.05.2017, Бюл № 9.

11. А.А. Кузнецов, А.И. Пушкарев, И.И. Сватовский, А.В. Шевцов Несимметричные криптосистемы на алгебраических кодах для постквантового периода // Радиотехника, 2016, Вып. 186, с. 70-90.

12. Пат. 116152Україна, МПК(2017.01) H 03 M 13/00, H 03 M 13/19, G06 F 21/64, G 06 F 17/16. Спосіб формування та перевірки електронного цифрового підпису із використанням алгебраїчних блокових кодів / Кузнецов О.О., Пушкарьов А.І., Сватовський І.І., Шевцов О. В, Кузнецов Т.Ю.; заявник та патентовласник Харківський національний університет імені В.Н. Каразіна. – № 201611784; заявл. 21.11.2016; опубл. 10.05.2017, Бюл № 9.

Наукове видання

Міжнародний конкурс студентських наукових робіт

BLACK SEA SCIENCE 2018

Матеріали

Верстка – Н.М. Ковальчук

Формат 60х84/16. Гарнітура Times New Roman.
Умовно-друк. арк. 48,07. Тираж 300. Замовлення № 0518-105.

Видавництво і друкарня – Видавничий дім «Гельветика»
73034, м. Херсон, вул. Паровозна, 46-а, офіс 105
Телефон +38 (0552) 39 95 80
E-mail: mailbox@helvetica.com.ua
Свідоцтво суб'єкта видавничої справи
ДК № 4392 від 20.08.2012 р.