УДК 004.056.5 Вестник УрФО № 2(32) / 2019, с. 18–24

Комарова А. В., Коробейников А. Г.

DOI: 10.14529/secur190203

КОМБИНИРОВАНИЕ ЗАДАЧ ТЕОРИИ РЕШЁТОК И ТЕОРИИ ЧИСЕЛ В СХЕМАХ, АЛГОРИТМАХ И ПРОТОКОЛАХ АУТЕНТИФИКАЦИИ

В настоящее время в современной криптографии достаточно остро стоит вопрос противодействия атакам, выполняемым на квантовом компьютере. В случае появления такого устройства криптографические протоколы, основанные на сложности решения задач факторизации (ЗФ), дискретного логарифмирования в конечном простом поле (ЗДЛКПП) и дискретного логарифмирования в группе точек эллиптической кривой (ЗДЛЭК) могут быть скомпрометированы за полиномиальное время. Ввиду вышесказанного актуальной темой исследований и разработок являются методы повышения безопасности существующих схем аутентификации. В статье рассматриваются возможные способы комбинирования нескольких трудно решаемых задач в одной схеме электронной подписи (ЭП). Отличительной особенностью предлагаемых схем является использование постквантовой задачи поиска короткого целочисленного решения, относящейся к теории решеток, что обеспечивает повышенный уровень криптографической стойкости. В работе проведена оценка параметров выработанных схем.

Ключевые слова: *криптография, постквантовая криптография, теория решеток, задача поиска короткого целочисленного решения, электронная подпись, аутентификация.*

Komarova A. V., Korobeynikov A. G.

THE COMBINATION OF THE LATTICE THEORY PROBLEM AND THE NUMBER THEORY PROBLEM IN THE AUTHENTICATION SCHEMES, ALGORITHMS AND PROTOCOLS

The issue of countering quantum computer attacks is quite acute in modern cryptography. In the case of emergence such a device, cryptographic protocols based on complexity of solving the factorization problem, discrete logarithms in finite simple field and the discrete logarithm on elliptic curve can be compromised in polynomial time. In view of the above, methods of improving the safety of combined authentication schemes are an important topic of research. The article considers possible ways of combining several difficult tasks in one electronic signature scheme. A distinctive feature of the proposed schemes is the use of post-quantum short integer solution problem related to the lattice theory. It provides a higher level of cryptographic strength. The paper assesses the parameters of the developed schemes.

Keywords: *cryptography, post-quantum cryptography, lattice theory, short integer solution problem, electronic signature, authentication.*

Введение. Концепция создания комбинированных схем может быть реализована различными методами [1]. Например, при помощи модификации существующих схем ЭП с элементами встраивания одной подписи в другую. Так можно добиться повышения уровня стойкости и понижения вероятности взлома модифицированных схем ЭП. Рассмотрим варианты комбинирования различных схем ЭП с постквантовой схемой на основе теории решеток Falcon [2]. В основе вычислительной сложности схемы Falcon лежит задача поиска короткого целочисленного решения (Short Integer Solution problem, SIS) [3].

Комбинирование схемы Falcon и схемы ЭП Эль-Гамаля. Сформируем алгоритм ФЭГ путем комбинирования схем ЭП Эль-Гамаля [4] и схемы ЭП Falcon [2]. Связь этих двух схем будет определяться по параметру **z**, который является числовым представлением части подписи **s** с учетом случайного вектора ошибок **e**. Создавая связь между схемами именно таким образом, можно добиться наибольшей независимости друг от друга сложно вычислимых задач, положенных в основу комбинируемых схем.

Процедура генерации ключей схемы ФЭГ:

• генерируются матрицы **A** и **B** по требованиям схемы Falcon [2];

• генерируются закрытый и открытый ключи, как схеме ЭП Эль-Гамаля.

Тогда закрытым ключом (*ЗК*) будут являться (x, **B**), а открытым ключом (*ОК*) - (y, **A**).

Процедура генерации подписи к сообщению M:

• генерируется битовая строка r = $\{0,1\}^{320}$ из некоторого случайного равномерного распределения;

• вычисляется значение $h = H(M \| r)$;

• вычисляется значение **c**, такое чтоб выполнялось условие $\mathbf{cA}^T = h$;

• с помощью матрицы **B** вычисляется $\mathbf{v} \in L_q^{\perp}(\mathbf{B})$ близкий к **c**;

• вычисляется разность **s = c - v**;

• генерируется случайный вектор ошибок **e** $(\vec{e} \in Z_q)$ с малыми коэффициентами;

• вычисляется **z = s + e**;

• вычисляется $z = (Compress(\mathbf{z}))$, $1 < z < q$;

• вычисляется значение $R \equiv a^z \bmod p$;

• вычисляется $S \equiv \dfrac{(h - xR)}{z} \bmod (p-1)$

Подписью являются (r, **s**, *R, S).*

Процедура проверки подписи к сообщению *M*:

• проверяется выполнимость условий: $0 < R < p-1$ и $0 < S < p-1$;

• вычисляется значение $h = H(M \| r)$;

• проверяется выполнимость условия $\|\mathbf{s}\| < \beta$;

• вычисляется значение $h' = \mathbf{sA}^T$. Если $h' \neq h$, то подпись отвергается.

• проверяется выполнение условия $y^R R^S \equiv a^h \bmod p$. Если сравнение выполняется, то подпись признается верной.

Можно показать, что созданная схема ФЭГ действительно основывается на сложности вычисления двух трудно решаемых математических задач: на ЗДЛКПП и на задаче SIS. Если нарушитель сумеет подобрать часть *ЗК x*, то, зная значения *h* и *R*, он может попытаться скомпрометировать часть подписи *S* из уравнения (1). Злоумышленник может вычислить $h - xR = D$, затем $Sz \equiv D \bmod (p-1)$, затем $Sz = D + (p-1)Q$, где $Q \in Z$, потом $z = \dfrac{D + (p-1)Q}{S}$ и далее подобрать целое *Q* и пытаться подменить значение *z*, но даже если ему это удастся, то для подделки второй части подписи (**s**) ему необходимо знать вектор ошибок **e** либо значение закрытого ключа **B**. Напротив, если нарушитель умеет решать постквантовые задачи за полиномиальное время, он может скомпрометировать часть подписи **s**, но, так как для поиска значения *x* ему необходимо решить ЗДЛКПП, модифицированная схема ФЭГ останется не подделан-

ной. Таким образом, взлом одной части схемы не позволяет произвести полное раскрытие всех параметров схемы ФЭГ.

Комбинирование Falcon и схемы ЭП Шнорра. Предлагается следующий алгоритм ЭП, реализованный путем синтеза схемы ЭП Шнорра [5] и схемы Falcon [2]. Назовем его ФАШ. Процедура генерации ключей алгоритма ФАШ состоит из генерации матриц **A** и **B** по требованиям схемы Falcon и генерации значений *x* и *y* как в схеме ЭП Шнорра. Таким образом, *ЗК* - (*x*, **B**), *ОК* - (*y*, **A**).

Рис. 1. Алгоритм формирования подписи ФАШ

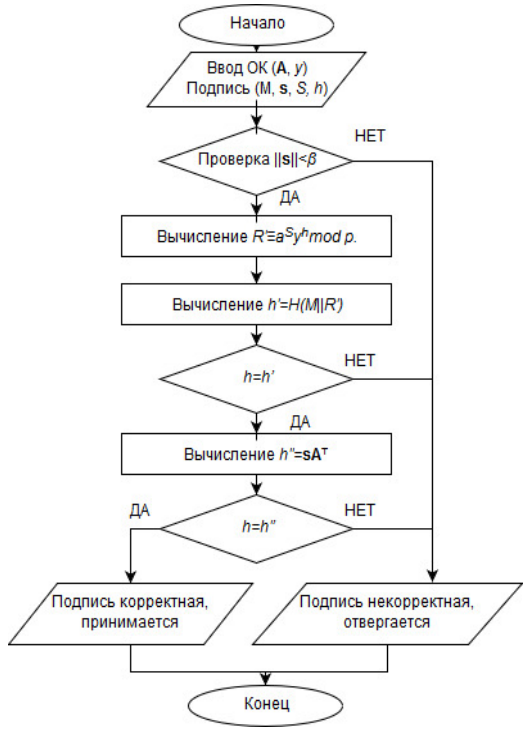

Рис. 2. Алгоритм проверки подписи ФАШ

Блок-схемы алгоритмов формирования подписи и проверки подписи разработанного алгоритма представлены на рисунках 1 и 2 соответственно.

Покажем, что предложенная схема действительно основывается на сложности решения двух трудных математических задач. Предположим, что нарушитель умеет решать ЗДЛКПП, тогда он может вычислить часть секретного ключа – значение *x*. Далее, подставляя все известные ему значения в уравнение $R' \equiv a^S y^h \bmod p$, злоумышленник может подобрать число *R'* равное числу *R*. Потом - из уравнения подобрать значение *k*, и таким образом, он может подделать *S* - часть подписи ФАШ. Однако знание параметров *k* и *x* никак не поможет подобрать вектор **v** близкий к вектору **c**, то есть, полностью схему взломать не удастся. С другой стороны, в случае, если злоумышленник смог решить задачу SIS, то есть подобрать такой вектор **v**, близкий к вектору c, чтоб выполнялись условия $h'' = h$ и $\|\mathbf{s}\| < \beta$, то он все равно не сможет полностью скомпрометировать схему ФАШ, так как знание параметров *h*, **v** и **B** никак не поможет при решении ЗДЛКПП. Отметим, что длина подписи данной схемы будет меньше, чем сумма длин исходных подписей.

Комбинирование схемы Falcon и ГОСТ Р 34.10-2012. Разработаем протокол аутентификации на основе комбинирования ЭП по ГОСТ 34.10-2012 [6] со схемой Falcon [2]. Данный протокол будет называться ФАГО (Таблица 1). В протоколе взаимодействуют два участника: участник *A* (подписывающий) и участник *B* (проверяющий).

В том случае, если злоумышленник умеет решать ЗДЛЭК, он может скомпрометировать первую часть подписи, то есть подобрать *d*, удовлетворяющее *d*P = Q*. Тогда нарушитель может попытаться подобрать значение *k* такое, чтобы выполнялось сравнение $k \equiv (\frac{z - td}{s}) \bmod q$, далее найти значение *t*, и таким образом взломать ГОСТ 34.10-2012, однако умение справляться с ЗДЛЭК никак не

Таблица 1

Протокол ФАГО

Участник А		**Участник В**
Генерация системных параметров		
• Генерирует простое число *p*, $p > 2^{255}$. • Выбирает ЭК *E*. • Выбирает целое число *m* - порядок группы точек ЭК *E*. • Отправляет запрос *Z* на генерацию значения q.		
	---[Z]-->	• Принимает *Z*. • Выбирает простое число *q*, и отправляет его участнику *A*.
• Принимает число *q*. • Проверяет выполнимость $m = nq,\ \ n \in N,\ \ n \geq 1$. Если условие не выполняется, то участнику *B* отправляется запрос на генерацию нового значения *q*.	<--[q]---	
	Если условие $m = nq,\ n \in Z,\ n \geq 1$ не выполняется ---[Z′]-->	• Принимает *Z′*. • Выбирает новое простое число *q*, и отправляет его участнику *A*.
• Выбирает точку $P \in E$, $P = (x_p, y_p)$, $P \neq 0,\ qP = 0$. • Генерирует *d*, $0 < d < q$. • Вычисляет $Q \in E$, $Q = (x_q, y_q)$, $d*P = Q$. Генерирует матрицы **A** и **B** по требованиям схемы Falcon. • Генерирует ЗК: (d, **B**). • Генерирует ОК: (Q, **A**). • Отправляет ОК (Q, **A**) участнику *B*.	<--[q]---	
	---[Q,A]-->	• Принимает (Q,A). • Формирует документ *M* и отправляет его числовую интерпретацию участнику *A*.
Генерация подписи		
• Принимает значение *M*. • Генерирует битовую строку $r = \{0,1\}^{320}$. • Вычисляет $h = H(M \| r)$ • Вычисляет **c**, $\mathbf{cA}^{\mathbf{T}} = h$. •Вычисляет $\mathbf{v} \in L_q^{\perp}(\mathbf{B})$, близкий к **c**. • Вычисляет **s = c - v**. • Вычисляет $a = (Compress(\mathbf{s}))$, $a < q$. • Вычисляет число $e \equiv a \bmod q$. Если $e = 0$, то считает $e = 1$. • Генерирует случайное *k*, $0 < k <$ q. • Вычисляет точку ЭК $C = k*P$, $C = (x_c, y_c)$. • Вычисляет $t \equiv x_c \bmod q$. Если $t = 0$, то возвращается к шагу генерации случайного *k*. • Вычисляет z: $z \equiv (td + ke) \bmod q$, если $z = 0$, то возвращается на шаг генерации случайного *k*. • Вычисляет двоичные векторы **t** и **z**. • Формирует подпись $\zeta = (\mathbf{t} \| \mathbf{z} \| \mathbf{s} \| \mathbf{r})$. • Отправляет участнику **B** подпись ζ.	<--[M]---	
Проверка подписи		

	---[ζ]-->	• Принимает ζ. • Вычисляет из него числа *t* и *z*. Если неравенства $0 < t < q$ и $0 < z < q$ не выполняются, то подпись считается неверной и участнику *A* отправляется запрос *N* для старта генерации новых системных параметров.
• Принимает N. *• Переходит к первому шагу генерации системных параметров.*	*Если неравенства $0 < t < q$ и $0 < z < q$ не выполняются* <--[N]---	
		• Вычисляет $h = H(M \| r)$. • Проверяет $\|\mathbf{s}\| < \beta$. Если условие не выполняется, то то подпись считается неверной и участнику *A* отправляется запрос *N* для старта генерации новых системных параметров.
• Принимает N. *• Переходит к первому шагу генерации системных параметров.*	*Если неравенство $\|\mathbf{s}\| < \beta$ не выполняется* <--[N]---	
		• Вычисляет значение $h' = \mathbf{s}\mathbf{A}^T$. • Если $h' \neq h$, то подпись считается неверной и участнику *A* отправляется запрос *N* для старта генерации новых системных параметров.
• Принимает N. *• Переходит к первому шагу генерации системных параметров.*	*Если $h' \neq h$* <--[N]---	
		• Вычисляет $a = (Compress(\mathbf{s}))$. • Вычисляет $e \equiv a \bmod q$. Если $e = 0$, то считает $e = 1$. • Вычисляет $v \equiv e^{-1} \bmod q$, $z_1 \equiv zv \bmod q$, $z_2 \equiv -tv \bmod q$. • Вычисляет точку ЭК $C' = z_1 * P + z_2 * Q$, $C' = (x_{c'}, y_{c'})$; • Вычисляет $t' \equiv x_{c'} \bmod q$. Если $t' \neq t$, то подпись считается неверной и участнику *A* отправляется запрос *N* для старта генерации новых системных параметров.
• Принимает N. *• Переходит к первому шагу генерации системных параметров.*	Если $t' \neq t$ <--[N]---	

		Если $t' = t$, то подпись признается подлинной и участнику *A* отправляется уведомление *Y* о том, что процесс его аутентификации прошел успешно.
• Принимает Y. *• Завершает процесс аутентификации.*	*<--[Y]---*	

влияет на умение решать задачу SIS, и параметр подписи **s** подделать не удастся. С другой стороны, при взломе схемы Falcon злоумышленник может подделать параметр подписи **s**, затем подделать значение a и заменить значение e, но далее для подделки параметра *t* нарушителю требуется решить ЗДЛЭК, что за полиномиальное время пока невозможно сделать. Длины ключей и подписи разработанных схем приведены в Таблице 2.

Выводы. В настоящей статье предлагаются схема и алгоритм ЭП и протокол аутентификации, обладающие повышенным уровнем безопасности, и базирующиеся на сложности вычисления нескольких трудно решаемых задач разного типа одновременно, одна из которых является постквантовой задачей SIS. Рассмотрены возможные виды атак на предложенные схемы. Проведена оценка параметров выработанных схем аутентификации.

Таблица 2

Оценка параметров разработанных схем

Схема	Длина ЗК, байт	Длина ОК, байт	Длина подписи, байт
Falcon512	4 097	897	690
Схема ЭП Эль-Гамаля	128	128	256
ФЭГ	4225	1025	946
Схема ЭП Шнорра	128	128	256
ФАШ	4225	1025	818
ГОСТ Р 34.10-2012	32	32	64
ФАГО	4129	929	754

Литература

1. Коробейников А.Г., Кутузов И.М. Алгоритм обфускации//Кибернетика и программирование. 2013. № 3. С. 1-8.

2. FALCON. - Режим доступа: https://falcon-sign.info, свободный (дата обращения: 05.06.2019).

3. Gentry C., Peikert C., Vaikuntanathan V. Trapdoors for hard lattices and new cryptographic constructions. In Richard E. Ladner and Cynthia Dwork, editors, 40th ACM STOC, p. - 197–206, Victoria, British Columbia, Canada, May 17-20, 2008. ACM Press. 7, 8, 11, 12, 13, 14.

4. Elgamal T. A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms // IEEE Trans. Inf. Theory / F. Kschischang — IEEE, 1985. — Vol. 31, Iss. 4. — P. 469–472. — ISSN 0018-9448 — doi:10.1109/TIT.1985.1057074.

5. Schnorr C.P. Efficient Identification and Signatures for Smart Cards.Advances in Cryptology - CRYPTO'89. Lecture Notes in Computer Science 435. — 1990. — С. 239 – 252.

6. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. ГОСТ 34.10-2012. – Госстандарт России. М., Стандартинформ. – 2013. – 18с.

References

1. Korobeynikov A. G., Kutuzov I. M. Obfuscation Algorithm [Algoritm obfuskacii] // Cybernetics and programming, 2013, № 3, P. 1-8.

2. FALCON. Available at: https://falcon-sign.info, free (accessed: 05.06.2019).

3. Gentry C., Peikert C., Vaikuntanathan V. Trapdoors for hard lattices and new cryptographic constructions. In Richard E. Ladner and Cynthia Dwork, editors, 40th ACM STOC, p. - 197–206, Victoria, British Columbia, Canada, May 17-20, 2008. ACM Press. 7, 8, 11, 12, 13, 14.

4. Elgamal T. A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms // IEEE Trans. Inf. Theory / F. Kschischang — IEEE, 1985. — Vol. 31, Iss. 4. — P. 469–472. — ISSN 0018-9448 — doi:10.1109/TIT.1985.1057074.

5. Schnorr C.P. Efficient Identification and Signatures for Smart Cards.Advances in Cryptology - CRYPTO'89. Lecture Notes in Computer Science 435. — 1990. — C. 239 – 252.

6. Information technology. Cryptographic protection of information. Processes of formation and verification of electronic digital signature. GOST 34.10-2012 [Informacionnaya tekhnologiya. Kriptograficheskaya zashchita informacii. Processy formirovaniya i proverki elektronnoj cifrovoj podpisi. GOST 34.10-2012]. Gosstandart Rossii. M., Standartinform, 2013, p. 18.

КОМАРОВА Антонина Владиславовна, аспирант факультета безопасности информационных технологий, Федерального государственного автономного образовательного учреждения высшего образования «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики», 197101, г. Санкт-Петербург, Кронверкский проспект, 49, E-mail: piter-ton@mail.ru

КОРОБЕЙНИКОВ Анатолий Григорьевич, доктор технических наук, профессор, заместитель директора по науке, Санкт-Петербургский филиал Федерального государственного бюджетного учреждения науки Института земного магнетизма, ионосферы и распространения радиоволн им. Н.В.Пушкова Российской академии наук. 199034, г. Санкт-Петербург, Менделеевская линия, 3, E-mail: korobeynikov_a_g@mail.ru

KOMAROVA Antonina, postgraduate student, St. Petersburg National Research University of Information Technologies, Mechanics and Optics. 197101, St. Petersburg, Russia. Kronverksky pr., 49. E-mail: piter-ton@mail.ru

KOROBEYNIKOV Anatoly, Dr.Sc., Professor, Deputy Director for Science, Pushkov Institute of Terrestrial Magnetism, Ionosphere and Radio Wave Propagation of the Russian Academy of Sciences (IZMIRAN). 199034, St. Petersburg, Russia, Mendeleevskaya liniya, 3, E-mail: korobeynikov_a_g@mail.ru