СХЕМА ПОСТ-КВАНТОВОЙ АГРЕГИРОВАННОЙ ПОДПИСИ НА ОСНОВЕ ТЕОРИИ АЛГЕБРАИЧЕСКОГО КОДИРОВАНИЯ

Макаров А.О.[1]

Агрегированные подписи позволяют объединять индивидуальные подписи различных подписантов для различных сообщений в единую подпись, которая затем может быть использована для проверки любого из подписанных сообщений. При этом размер результирующей агрегированной подписи меньше суммарного размера индивидуальных подписей. Подписи данного типа могут быть использованы с целью уменьшения размера передаваемых сообщений в ряде приложений, таких как протоколы защищённой маршрутизации (SBGP) или инфраструктура закрытых ключей.

Однако большинство современных схем подписи основываются на предположении о сложности задач дискретного логарифмирования и факторизации, что делает их нестойкими перед квантовым противником, способным на эффективное выполнение квантового алгоритма факторизации Шора. Учитывая возможность появления квантового компьютера, способного на эффективное выполнение данного алгоритма, задача построения пост-квантовых схем подписи встаёт наиболее остро. Одной из групп схем пост-квантовых подписей являются подписи на основе теории алгебраического кодирования, которым и посвящена данная статья.

***Целью** данной работы является построение схемы пост-квантовой последовательной агрегированной подписи на основе теории алгебраического кодирования.*

***Метод** исследования: построение пост-квантовой агрегированной подписи с использованием односторонней подстановки с секретом на основе задач алгебраического кодирования, анализ теоретических и практических атак для полученной схемы, представление параметров схемы, сравнение предложенной схемы подписи с существующими схемами.*

***Результат** работы: схема пост-квантовой агрегированной подписи на основе теории алгебраического кодиро-вания, рекомендуемые параметры схемы. Параметр стойкости схемы составляет 80 бит, схема обладает полной агрегацией, т.е. размер подписи не увеличивается с ростом числа подписантов.*

***Ключевые слова:** криптография на основе теории кодирования, схема электронной подписи CFS, агрегированная подпись, пост-квантовая криптография.*

DOI: *10.21681/2311-3456-2019-2-69-76*

Введение

Системам обеспечения безопасности часто приходится иметь дело с электронными подписями, выработанными различными пользователями для различных сообщений. Например, в инфраструктуре открытых ключей (PKI) цепочка сертификатов содержит n подписей различных центров сертификации (CA) на n различных закрытых ключах. Аналогичная ситуация при использовании протокола SBGP — каждый узел сети получает список из n подписей, соответствующих определенному пути длины n в сети. Каждый узел подписывает собственный сегмент пути в сети, и итоговый список из n+1 подписи передаётся следующему узлу. В результате число подписей, сопровождающих сообщение при передаче, линейно растёт с числом пройденных узлов. Обе описанных системы могли бы получить выигрыш при использовании алгоритма “сжатия” списка электронных подписей для разных сообщений, подписанных различными сторонами. Для уменьшения размеров итоговых подписей, как правило, используются так называемые схемы агрегированных подписей [1], позволяющих преобразовать различные индивидуальны электронные подписи в единую подпись, которая затем может быть использована для проверки любого из подписанных сообщений.

Большинство современных схем подписи (включая агрегированные) основываются на предположении о сложности задач факторизации больших чисел и нахождения дискретного логарифма. Однако, принимая во внимание возможность появления в ближайшем будущем эффективного квантового компьютера, наиболее остро встаёт задача разработки пост-квантовых схем подписи.

Главным эффектом появления квантового компьютера является практическая эффективная реализация алгоритма Шора [2], позволяющего решать задачи дискретного логарифмирования и факторизации за полиномиальное время, и алгоритма Гровера [3], позволяющего производить поиск в множестве из N элементов за $N^{1}/_{2}$. В то время как алгоритм Гровера оказывает лишь линейное влияние на стойкость криптосистем (фактически необходимо удвоение длины симметричных ключей для сохранения исходного уровня стойкости), возможность эффективного применения алгоритма Шора делает такие криптосистемы как RSA и ECDSA нестойкими, сводя экспоненциальную сложность атак к полиномиальной. Именно поэтому в настоящий момент идёт активное создание и исследование пост-квантовых ассиметричных криптосистем.

Одной из групп вычислительно сложных квантовых задач являются задачи на основе теории алгебраического

1 Макаров Артём Олегович, аспирант кафедры «Криптология и кибербезопасность», НИЯУ «МИФИ», Москва, Россия. E-mail: zma.94@mail.ru

кодирования. В основе сложности данных задач лежит частный случай задачи нахождения скрытой подгруппы (Hidden Subgroup Problem), для которой не известно существования эффективного квантового алгоритма или возможного эффективного применения алгоритмов Гровера и Шора. Отличительной особенностью данной группы задач является факт того, что криптосистемы, построенные на их основе, являются легко реализуемыми и легко вычислимыми, так как большинство вычислений в них сводятся к матричным операциям, которые могут быть эффективно выполнены как на стандартных процессорах, так с использованием FPGA [4]. Электронные подписи на основе задач теории кодирования обладают небольшим размером, относительно других пост-квантовых схем подписи. Всё это делает криптосистемы на основе теории кодирования одним из наиболее вероятных кандидатов на роль пост-квантовых асимметричных криптосистем.

В данной статье представлено расширение существующей пост-квантовой схемы подписи Parallel-CFS, построенной на основе задач теории кодирования, для получения последовательной агрегированной подписи. Представленная схема является первой описанной агрегированной схемой подписи на основе задач теории кодирования.

Последовательные агрегированные подписи

Основная идея, лежащая в основе агрегации подписей: имея n различных электронных подписей для n различных сообщений, выработанных n различными пользователями, иметь возможность преобразовать данные подписи в единую электронную подпись, размеры которой меньше размеров объединённых индивидуальных подписей. Полученная подпись может быть использована для проверки подписи для каждого из n сообщений.

Опишем формальное определение схемы агрегированной электронной подписи. Схемой агрегированной подписи называется четвёрка алгоритмов — Генерация ключей, Подпись, Агрегация и Агрегированная проверка подписи.

Генерация ключей: имея на вход параметр l, получить пару ключей (PK_i,SK_i) для каждого пользователя u_i,i $\in$ {1..n}.

Подпись: имея на вход сообщение M и секретный ключ SK, получить подпись σ для сообщения M.

Агрегация: имея на вход сообщения M_1,..,M_n, открытые ключи PK_1,...,PK_n и подписи σ_1,...,σ_n соответствующих сообщений, получить агрегированную подпись σ.

Агрегированная проверка подписи: имея на вход сообщения M_1,...,M_n, открытые ключи PK_1,...,PK_n и агрегированную подпись σ, проверить её верность для всех сообщений, и в случае успеха вернуть 1, иначе — 0.

В соответствии с введенными определениями выделяют следующие типы агрегированных подписей: общие (General) агрегированные подписи и последовательные (Sequential) агрегированные подписи [1].

При использовании общих электронных подписей каждый пользователь u_i независимо подписывает собственное сообщение M_i с использованием ключа SK_i и получает подпись σ_i. Затем любой стороной (в том числе и не участвующей в процедуре подписи сообщений) используется алгоритм агрегации, на вход которого подаётся n подписей σ_1,...,σ_n, которые агрегируются в единственную подпись σ. Заметим, что агрегация может происходить последовательно — подписи σ_1 и σ_2 могут быть агрегированы в подпись σ_{12}, которая затем может быть агрегирована с подписью σ_3 с целью получения подписи σ_{123} и так далее. Подписи данного типа могут быть получены без взаимодействия между пользователями в процессе подписания.

В последовательных подписях агрегация может быть получена только в процессе подписания очередного сообщения пользователем. Иными словами, алгоритмы Агрегации и Подписи объединяются в единый алгоритм Агрегированной Подписи. Каждый пользователей u_i с помощью ключа SK_i производит подпись своего сообщения M_i с использованием текущего значения агрегированной подписи σ_{i-1} для получения новой агрегированной подписи σ_i. Таким образом, подписанты должны последовательно взаимодействовать между собой в процессе формирования агрегированной подписи, путём передачи агрегированной подписи.

Для оценки качества агрегации подписей вводится понятие коэффициента сжатия подписи:

$$r = 1 - \frac{|\sigma_{ag}|}{n|\sigma|}, \quad (1)$$

где $|\sigma_{ag}|$ — размер агрегированной подписи, $|\sigma|$ — размер индивидуальной подписи, n — число подписантов. Схема агрегированной схемы называется оптимальной при r=1-1/n или говорят, что схема обеспечивает полную агрегацию.

Схема электронной подписи CFS

Первая асимметричная криптосистема на основе теории алгебраического кодирования была предложена МакЭлисом [5]. Единственной [6] известной стойкой схемой подписи на основе криптосистемы МакЭлиса является схема электронной подписи Куртуа-Файниаса-Сендриера [7] (CFS). Стойкость данной схемы сводится к стойкости криптосистемы МакЭлиса, которая в свою очередь основана на предположении о сложности решения задачи декодирования двоичного кода Гоппы. В данном разделе представлено описание схемы CFS и её модификации.

Для начала дадим формальное описание криптосистемы Нидерайдера, которая является основой для построения схемы электронной подписи CFS.

Генерация ключей. Выбрать параметры m и t, n=2m. Пусть Γ(g,S) двоичный код Гоппы, заданный полиномом g F_{2^m}) степени t и с поддержкой S, где S — перестановка элементов F_{2^m}). Описанный код может исправлять до t ошибок. Пусть H систематическая mt×n матрица проверки кода Γ(g,S). H является открытым ключом, g и S образуют закрытый ключ.

Зашифрование. Для зашифрования открытого текста p он преобразуется в ошибку e_p длины n и веса Хэмминга не более чем t, используя обратимое отображение φ_t. С использованием открытого ключа H вычисляется $s=H\times e^T$, p — синдром, соответствующий ошибке e_p, являющийся шифртекстом.

Расшифрование. Для расшифрования шифртекста s необходимо применить алгоритм декодирования синдрома s для получения ошибки e_p. Открытый текст вос-

станавливается с помощью вычисления обратного преобразования φ_t^{-1} от ошибки e_p.

Классическое описание схемы Нидерайдера содержит использование двух матриц для «усложнения» структура матрицы H. На практике использование этим матриц не является необходимым: перестановочная матрица n×n задаётся использованием поддержки S, а обратимая mt×n матрица не является необходимой, если H представлена в систематичекой форме.

Теперь приступим к описанию схемы CFS. Схема подписи CFS [7] использует принцип “hash-and-sign”, при котором сначала вычисляется хэш от подписываемого сообщения, а затем производится подпись для полученного хэш значения. Хэш-функция, используемая в CFS, имеет выход в mt бит. Подписываемое сообщение хэшируется, а затем рассматривается как шифртекст в схеме Нидерайдера. Однако расшифрованы могут быть только шифртексты, соответствующие синдромам ошибок веса не более t. Это означает, что только $\binom{2^m}{t} \approx \frac{2^m}{t!}$ из 2^m возможных синдромов могут быть расшифрованы как шифртексты. Иными словами, только один из t! документов может быть подписан, что делает использование данного подхода сложно реализуемым для практического применения. Однако существуют два метода преодоления данной проблемы — использование счётчика, как части подписываемого сообщения, и осуществление полного декодирования. Оба метода, однако, требуют в среднем t! операций расшифрования схемы Нидерайдера.

Атаки на схему электронной подписи CFS

Существует два основных типа атак на схему CFS — атака на восстановление ключа, целью которой является восстановление закрытого ключа из открытого, и поделка подписи, при которой пытаются создать верную подпись для сообщения без использования закрытого ключа. Атаки на восстановление ключа на схему МакЭлиса традиционно менее эффективны, чем атаки на декодирование [8], однако недавние достижения в построении алгоритмов различимости кодов Гоппы может привести к появлению новых атак. На текущий момент нет известных реализуемых атак данного типа, поэтому далее будут описаны атаки на декодирование, которые в контексте схем подписи являются атаками на подделку подписи. Для подделки CFS подписи атакующему необходимо найти корректную пару документ/подпись и таким образом решить вычислительную задачу декодирования синдрома: найти вектор ошибки, соответствующий заданному синдрому, имеющий при этом вес, меньше заданного. В отличие от обычной Задачи Декодирования (Syndrome Decoding, SD) необходимо найти любой вектор ошибки из многих.

Формальное описание данной проблемы выглядит следующим образом: для параметров n,t,r,N, двоичной r×n матрицы H, множества двоичных векторов $S=\{S_i \in \{0,1\}^r\}, i \in \{1,N\}$ найти двоичный вектор ошибки e с весом Хэмминга не более t, такой что: $\exists i \in \{1..N\}: H \times e^T = S_i$. Данная задача часто носит название декодирование одного из многих синдромов (One out of Many Syndrome Decoding, OMSD).

Наиболее эффективными практическими атаками на декодирование одного из многих синдромов являются атака на декодирование информационного множества (Information Set Decoding, ISD) и атаки на основе обобщенного алгоритма дней рождений (Generalized Birthday Algorithm, GBA), позволяющие проводить атаки сложностью порядка $2^{\frac{mt}{2}}$ и $2^{\frac{mt}{3}} \log_2(2^{\frac{mt}{3}})$ соответственно [9].

Схема электронной подписи Parallel-CFS

Использование атаки на основе обобщенного алгоритма дней рождений даёт снижение асимптотической стойкости CFS с $2^{\frac{mt}{2}}$ до $2^{\frac{mt}{3}} \log_2(2^{\frac{mt}{3}})$ по сравнению с использованием атаки на декодирование информационного множества, которая использовалась авторами CFS при изначальном анализе схемы. Атака на основе обобщенного алгоритма дней рождений оставляет схему асимптотически стойкой, однако требует существенного пересмотра её параметров для обеспечения требуемого уровня стойкости. Увеличение параметров m и t приводит к значительному росту в размере открытых ключей (размер которых является экспонентой от t). При линейном увеличении параметров для обеспечения необходимой стойкости схема становится не применима в практическом смысле. Для решения данной проблемы была предложена модификация схемы CFS — Параллельная схема CFS (Parallel-CFS) [9].

Для получения подписи сообщения вместо вычисления одного хэш значения (с использованием функции h) для сообщения D, используются два хэш значения (с использованием двух различных хэш-функций h_1 и h_2) и параллельная подпись обоих значений h_1 (D) и h_2 (D). Таким образом, для осуществления атаки необходимо подделать две подписи для обоих хэш-функций. В то же время эти две поддельные подписи должны быть для одного и того же документа D. Обобщенно используется i различных хэш-функций для получения i параллельных подписей одного сообщения, где i параметр схемы.

Использование CFS со счётчиком невозможно для использования в параллельной схеме CFS [9]. Таким образом, для применения в параллельном CFS используется схема CFS на основе полного декодирования. Пусть δ наименьшее целое число, такое что $\binom{n}{t+\delta} > 2^{mt}$. Тогда произвольный синдром может быть декодирован (с высокой вероятностью) в ошибку веса не более t+δ. При использовании данного метода подписант проходит по всем ошибкам Φ δ (i) веса δ и пытается декодировать синдром

$$s = h(D) + H \times \varphi_\delta(i)^T. \quad (2)$$

Когда декодируемый синдром получен для заданного индекса i_0 необходимо найти открытый текст

$$p'_{i0}: H \times \varphi_t(p'_{i_0})^T = s_{i_0} = h(D) + H \times \varphi_\delta(i_0)^T. \quad (3)$$

Подписью является значение

$$p_{i_0} = \varphi_{t+\delta}^{-1}(\varphi(p'_{i_0}) + \varphi_\delta(i_0)), \quad (4)$$

т.е. открытый текст соответствующий ошибке веса t+δ Для проверки подписи необходимо проверить верность равенства $H \times \varphi_{t+\delta}(p_{i_0})^T = h(D)$.

Возможна модификация Алгоритма Дней Рождений для нахождения нескольких решений, т.е. обобщение его на случай атаки на схему Parallel-CFS. Основной идеей является получения большого числа верных подписей для хэш значения первой хэш-функции h_1 и использова-

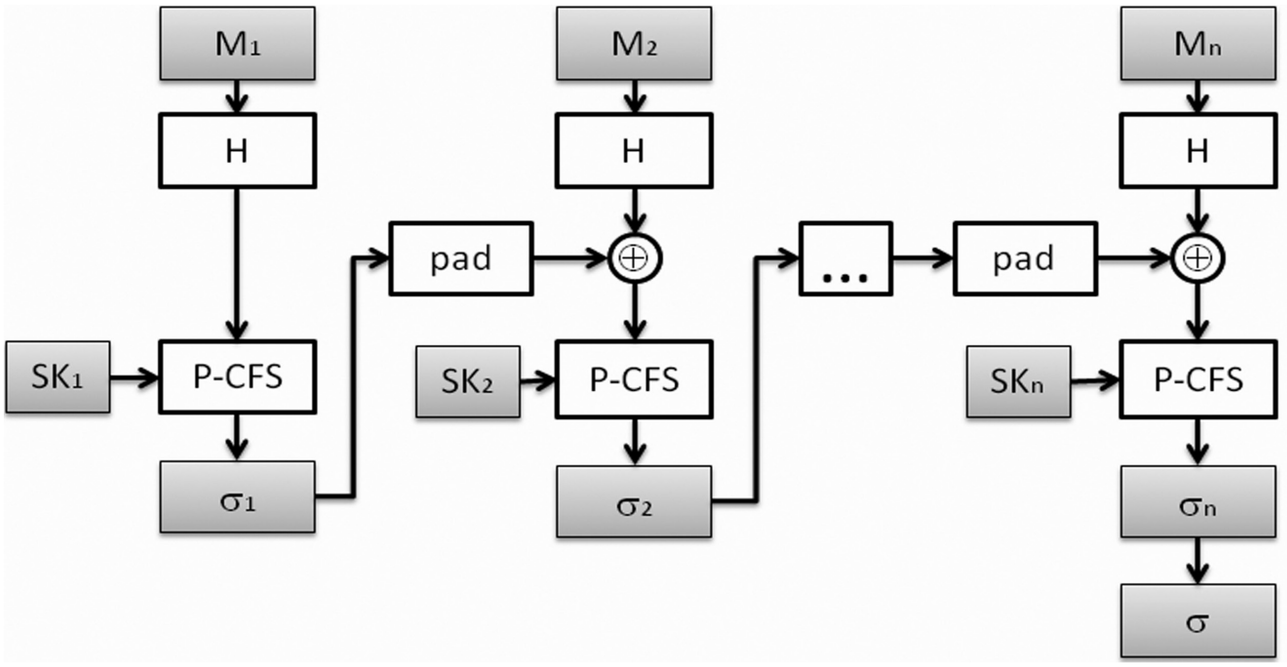

Рис.1. Схема получения агрегированной подписи APCFS

ние полученных решений как возможных подписей для второй хэш-функции h_2. Используя техники описанные в [9, 10] можно получить последовательную атаку на схему P-CFS сложностью LlogL для $L = 2^{\frac{2^{i}-1}{2^{i+1}}mt}$, где m,t,i — параметры схемы.

Схема агрегированной электронной подписи APCFS

В данном разделе представлено формальное описание предлагаемой схемы пост-квантовой агрегированной подписи. В качестве основы для построения схемы используется параллельная схема CFS [7], к которой применяется принцип последовательной агрегации, аналогичный схеме MQSAS [11], а именно построения агрегированной подписи с использованием произвольной подстановки [12]. Схема получила название Агрегированной Параллельной Подписи CFS — APCFS.

Генерация ключей: Выбрать параметры m и t, n=2^m, $i, \delta: \binom{n}{n+\delta} > 2^{mt}$, и i криптографических хэш-функции $h_1,...,h_i$. Пусть Γ(g,S) двоичный код Гоппы, заданный полиномом $g \in \mathbb{F}_2^{2^m}$ степени t и поддержкой S, где S — перестановка элементов $\mathbb{F}_2^{2^m}$. Пусть H систематическая mt× n матрица проверки кода Γ(g,S) является открытым ключом, g и S образуют закрытый ключ.

Агрегированная подпись. Имея подпись σ_{n-1} сообщений $D_1,...,D_{n-1}$, открытые ключи $H_1,...,H_{n-1}$, получить агрегированную подпись для сообщений $D_1,...,D_n$ (рис.1). Сначала производится проверка агрегированной подписи σ_{n-1}. В случае её верности для сообщения D вычисляются i хэш значений

$$h^{(n)} = h_1(D_n)||h_2(D_n)||\dots||h_i(D_n), \quad (5)$$

к которым побитно прибавляется подпись

$$\sigma_{n-1}: h_{\oplus}^{(n)} = h^{(n)} \oplus \sigma_{n-1} = h_{\oplus_1}^{(n)}||h_{\oplus_2}^{(n)}||\dots||h_{\oplus_i}^{(n)}. \quad (6)$$

Если длина вектора σ_{n-1} меньше длины $h^{(n)}$, то σ_{n-1} дополняется с помощью дополнения PKCS#7. Затем используется алгоритм декодирования кодов Гоппы схемы CFS с полным декодированием для получения i ошибок $e_1^{(n)},\dots,e_i^{(n)}$ веса не более t+δ, таких что $H\times e_i^T = h_{\oplus_i}^{(n)}$. Подписью является

$$\sigma = \sigma_n = \phi_{t+\delta}^{-1}\left(e_1^{(n)}\right)||\dots||\phi_{t+\delta}^{-1}\left(e_i^{(n)}\right). \quad (7)$$

Агрегированная проверка подписи. Имея сообщения $D_1,...,D_n$, агрегированную подпись $\sigma=\sigma_n = p_1^n||...||p_{in}$, открытые ключи $H_1,...,H_n$ для k=n,...,t последовательно вычисляются (рис.2):

$$h_{\oplus j}^{k} = H\times \phi_{t+\delta}\left(p_j^{(k)}\right), j = 1,..,i, \quad (8)$$

$$\sigma_{i-1} = unpad(h_{\oplus 1} \oplus h_1(D_k)||\dots||h_{\oplus i} \oplus h_i(D_k)), \quad (9)$$

где unpad операция удаления PKCS#7 дополнения. В конце производится проверка σ_0=?0.

Для демонстрации корректности схемы без потери общности зафиксируем i=2. При осуществлении проверки подписи, в случае если хотя бы одна подпись в цепочке будет неверна, итоговое значение σ_0 будет отлично от нуля, так как в случае неверной подписи $\sigma = p_1^{(j)}||p_2^{(j)}$ данная подпись не даст равенства

$$h_{\oplus 2}^{(j)} = H\times\phi_{t+\delta}\left(p_2^{(j)}\right)\ \sigma_{j-1} = p_1^{(j-1)}||p_2^{(j-1)}, \quad (10)$$

что впоследствии даст неверное значение $\sigma_{(j-1)}=p_1^{(j-1)}||p_2^{(j-1)}$. Таким образом, равенство σ_0=0 возможно только в случае верных подписей σ_j,j={1,..,n}.

При формировании каждой новой подписи каждым подписантом могут быть использованы техники сжатия подписи, описанные в [7]. Таким образом, каждая агрегированная подпись σ_j будет иметь меньший размер. При максимальном сжатии операция проверки усложняется на незначительное число матричных операций в матрице H, что не оказывает значительного влияния на скорость проверки подписи.

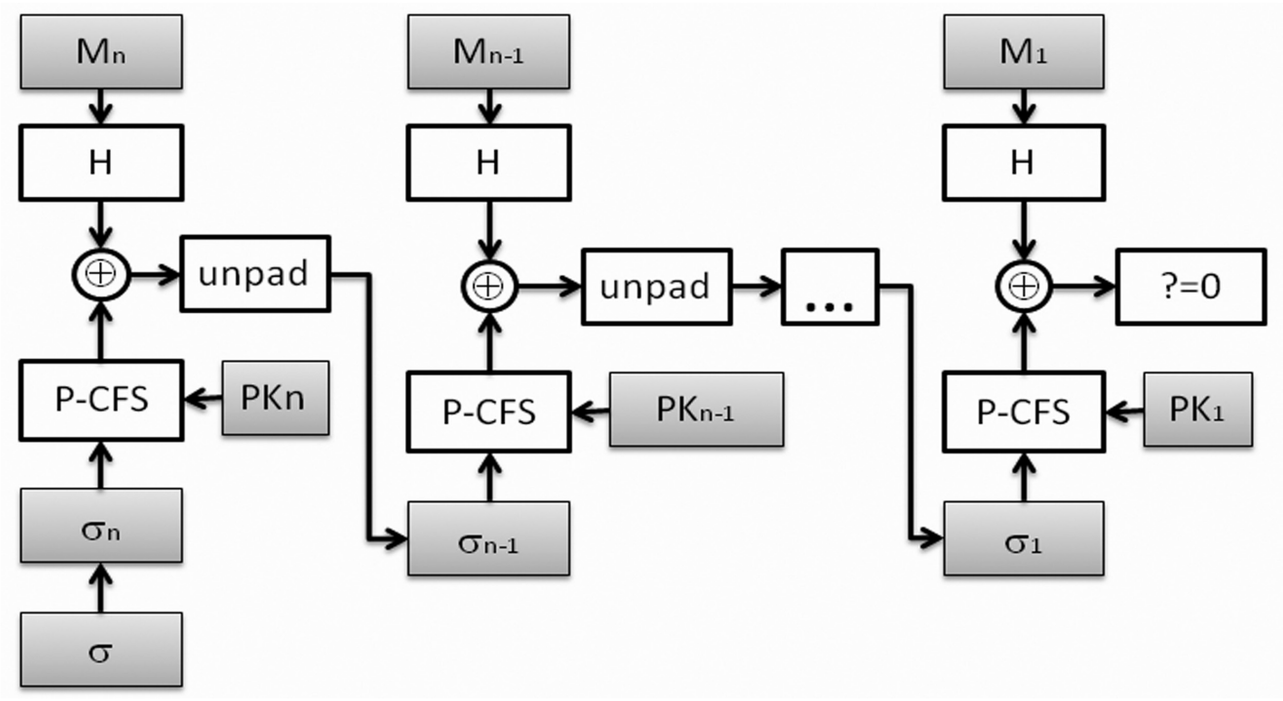

Рис.2. Схема проверки агрегированной подписи APCFS

Теоретическая стойкость агрегированной электронной подписи APCFS

Рассмотрим теоретическую стойкость полученной схемы. Для начала опишем формальное определение используемой модели для определения теоретической стойкости, которая может быть сведена к стойкости схемы Нидерайдера как односторонней функции. Функция зашифрования N схемы Нидерайдера с параметрами m,t является стойкой односторонней функцией, такой, что для любых злоумышленников, моделируемых вероятностной полиномиальной машиной Тьюринга, вычислительно сложно найти прообраз x для заданного значения y=N(x). Преимущество противника A против функции N определяется как:

$$Adv_N(A) = \Pr[y \leftarrow \{0,1\}^{mt}, x \leftarrow A|\, N(x) = y] \leq \epsilon \quad (11)$$

для пренебрежимо малой функции ϵ. Односторонняя функция называется (θ, ϵ) стойкой, если не существует эффективного алгоритма A, выполняемого время не более θ, который способен получить верную подпись с вероятностью больше чем ϵ. Предполагая (θ', ϵ') стойкость функции N, схема APCFS последовательной агрегированной подписи является (θ, ϵ) стойкой против создания новой подписи при адаптивной атаке с доступом к оракулу агрегированной подписи, причём для всех (θ, ϵ):

$$(iq_s + q_H + 1)\epsilon' \geq \epsilon; \quad (12)$$
$$\theta \leq \theta' - (4kq_H + 4ikq_s + 7 - 1).$$

Доказательство теоремы аналогично доказательству теоремы из [12]: злоумышленник запрашивает у оракула агрегированной подписи не более q_S подписей, выполняет не более q_H операций хэширования, используя время не более θ и получает верную подпись с вероятностью не более ϵ. Число пользователей при последовательной агрегации не превосходит k. Таким образом, получаем теорему аналогичную [12] с умноженным на i значением q_S, так как при каждом запросе, злоумышленник фактически получает i подписей. Описанное константное умножение не влияет на теоретическую асимптотическую стойкость. Таким образом, показана теоретическая стойкость схемы APCFS, при использовании предположения о стойкости схемы Нидерайдера.

Практическая стойкость агрегированной электронной подписи APCFS

Практическая стойкость схемы сводится к стойкости единичной схемы Parallel-CFS против наилучшей практической атаки, так как фактически схема является итеративном применением схемы Parallel-CFS с использованием различных ключей. Нетрудно видеть, что использование схемы APCFS эквивалентно n независимым подписям различных сообщений различными подписантами, и сложность атаки эквивалентна сложности атаки на создание поддельной подписи для произвольного подписанта, так как одновременная атака на несколько ключевых пар не даст преимущество по сравнению с атакой на одну ключевую пару. Таким образом, сложность практической атаки на схему APCFS с параметрами m,t можно оценивать как

$$\min\left[2^{\frac{mt}{3}}\log_2\left(2^{\frac{mt}{3}}\right), L\log_2 L\right], \quad (13)$$

для $L = 2^{\frac{2^i-1}{2^{i+1}}mt}$, где m,t,i — параметры схемы.

Параметры схемы APCFS

Предлагаемые параметры схемы подписи APCFS представлены в таблице 1. Заметим, что схема APCFS является оптимальной, и коэффициент сжатия не зависит от изменения параметров.

Производительность APCFS на одном ядре Intel Xeon W3670 3.20GHz составляет порядка одной подписи в секунду, что является приемлемым значением, при использовании в реальных системах [13].

Таблица 1.

Параметры (m,t,δ,i)	Параметр стойкости, бит	Размер открытого ключа	Размер подписи, бит	Число двоичных операций для осуществления подписи
(20,8,2,2)	75	20 MB	196	$2^{16,3}$
(20,8,2,3)	81	20 MB	294	$2^{16,9}$
(18,2,2,2)	76	5 MB	162	$2^{19,5}$
(18,2,2,3)	83	5 MB	288	2^{20}
(19,9,2,2)	80	10,7 MB	209	$2^{19,5}$
(19,9,2,3)	87	10,7 MB	309	2^{20}
(16,10,2,2)	75	1,2 MB	180	$2^{22,8}$
(16,10,2,3)	82	1,2 MB	270	$2^{23,4}$

В таблице 2 представлено сравнение подписи APCFS с агрегированной подписью MQSAS и подписью на основе RSA. На рисунке 3 представлено сравнение размеров подписей MQSAS и APCFS при различном числе подписантов.

Таблица 2.

Сравнение подписи APCFS с подписью MQSAS и RSA

Название схемы (параметры)	Параметр стойкости, бит	Размер открытого ключа	Размер индивидуальной подписи	Размер агрегированной подписи (20 подписантов)
APCFS (16,10,2,3)	82,5	1,2 MB	270 бит	270 бит
APCFS (19,9,2,2)	80,5	10,7 MB	206 бит	206 бит
MQSAS (96,65,2,2,2)	80	55,7 kB	102 бит	254 бит
MQSAS (96,5,6,6,2)	80	55,7 kB	114 бит	570 бит
RSA (1024,17)	80	256 B	1024 бит	–

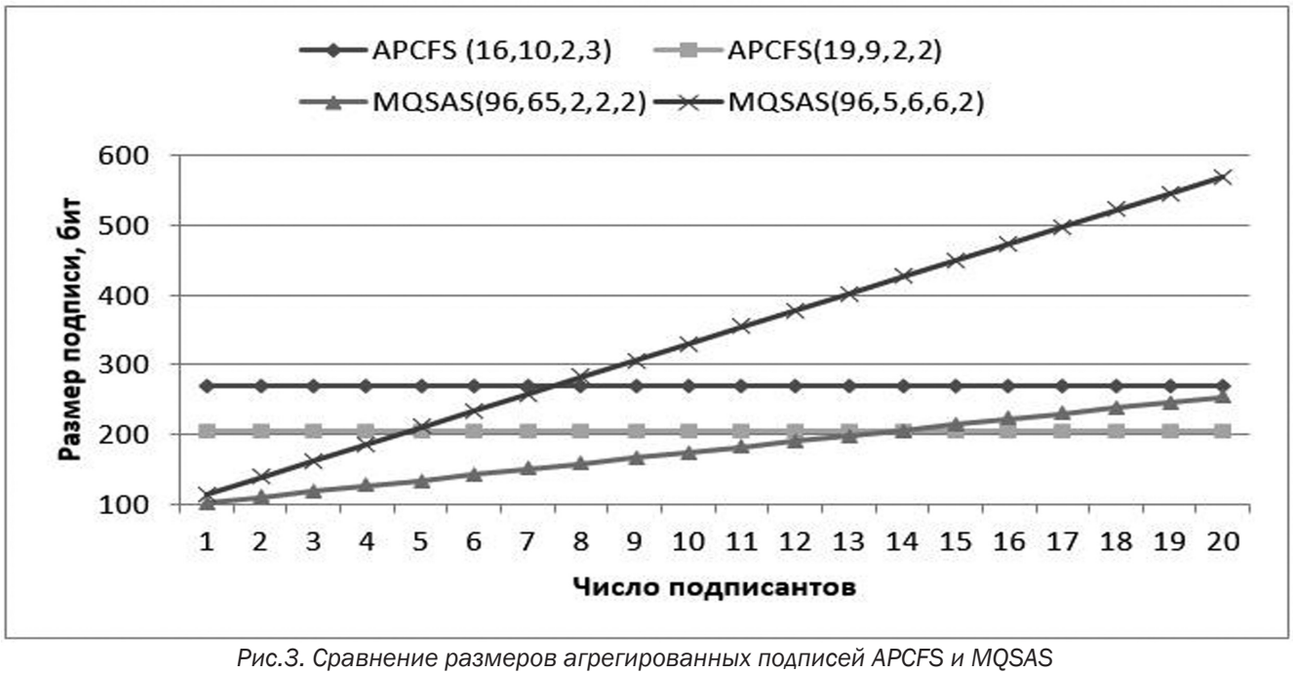

Рис.3. Сравнение размеров агрегированных подписей APCFS и MQSAS

Как видно из сравнения, схема APCFS обеспечивает такой же уровень стойкости, как и MQSAS, однако имеет меньший размер агрегированной подписи, при определённых параметрах. В то же время стоит отметить, что размер открытого ключа схемы APCFS значительно больше, чем в схеме MQSAS (на несколько порядков), что ограничивает применение данной схемы на встраиваемых устройствах, для которых большой размер ключей может стать критичным.

Выводы

В статье была описана первая схема агрегированной подписи на основе теории кодирования — APCFS. Рассмотрены существующие практические атаки на схемы подписи на основе теории алгебраического кодирования применительно к предлагаемой схеме. Рассмотрена теоретическая стойкость схемы, сведённая к стойкости функции зашифрования криптосистемы Нидерайдера.

Представленная схема обладает малым размером подписи, однако низкой скоростью подписи (порядка одной секунды) и имеет достаточно большой размер ключей. Параметр стойкости схемы составляет 80 бит.

Описанная схема, в отличии от других известных пост-квантовых схем, обладает полной агрегацией, т.е. не увеличивает свой размер с ростом числа подписантов и позволяет получить преимущество в размерах под-

писи уже при 8 подписантах по сравнению со схемой MQSAS.

Описанные в данной статье результаты могут быть использованы для реализации схемы пост-квантовой агрегированной подписи при переходе к пост-квантовым криптосистемам.

Научный руководитель: *Варфоломеев Александр Алексеевич, кандидат технических наук, доцент, МГТУ им.Н. Э. Баумана, Москва, Россия. E-mail: a.varfolomeev@mail.ru*

Литература

1. Boneh D. A Survey of Two Signature Aggregation Techniques / Boneh D., Gentry C., Lynn B., Shacham H. // CryptoBytes. – 2003. – Vol. 6, № 2.
2. Shor P. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer // SIAM Journal on Scientic and Statistical Computing. – 1997. – Vol. 26, № 5. – pp. 1484–1509.
3. Grover L. A fast quantum mechanical algorithm for database search // Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing. – 1996. – pp. 212–219.
4. Wang W. FPGA-based Key Generator for the Niederreiter Cryptosystem Using Binary Goppa Codes / Wang W., Szefer J., Niederhagen R. // Cryptographic Hardware and Embedded Systems CHES 2017. Lecture Notes in Computer Science. – 2017. – pp. 253-274.
5. McEliece R. A public-key cryptosystem based on algebraic coding theory // DSN Progress Report. – 1978. – Vol 42. – pp. 114–116
6. Bernstein D. Post-Quantum Cryptography / Bernstein D., Buchmann J., Dahmen E. // Springer-Verlag Berlin Heidelberg. – 2009. – 245 p.
7. Courtois N. How to Achieve a McEliece-Based Digital Signature Scheme / Courtois N., Finiasz M., Sendrier N. // Advances in Cryptology — ASIACRYPT 2001. Lecture Notes in Computer Science. – 2001. – Vol. 2248. – pp. 157–174.
8. Faugere J. Algebraic cryptanalysis of mcEliece variants with compact keys / Faugere J., Otmani A., Perret L., Tillich J. // Advances in Cryptology – EUROCRYPT 2010. Lecture Notes in Computer Science. – 2010. – Vol. 6110. – pp. 279–298.
9. Finiasz M. Parallel-CFS Strengthening the CFS McEliece-Based Signature Scheme // Selected Areas in Cryptography - 17th International Workshop. – 2011. – pp. 159–170.
10. Finiasz M. Security bounds for the design of code-based cryptosystems // Finiasz M., Sendrier N. / Advances in Cryptology – ASIACRYPT 2009. Lecture Notes in Computer Science. – 2009, Vol. 5912, pp. 88–105.
11. Bansarkhani R. MQSAS - A Multivariate Sequential Aggregate Signature Scheme / Bansarkhani R., Mohamed M., Albrecht Petzoldt A. // International Conference on Information Security. – 2016. – 19 p.
12. Lysyanskaya A. Sequential Aggregate Signatures from Trapdoor Permutations / Lysyanskaya A., Micali S., Reyzin L., Shacham H. // EUROCRYPT 2004: Advances in Cryptology. – 2004. – pp. 74–90.
13. Landais G. CFS Software Implementation / Landais G., Sendrier N. // Cryptology ePrint Archive. – 2012. – 15 p.

APCFS – POST-QUANTUM CODE BASED AGGREGATE SIGNATURE SCHEME

Makarov A.O.[2]

Abstract. *Aggregate signatures allow to compress n signatures on n different messages from n distinct users into one aggregate signature. This signature with the public keys can be used as signature for any of the signed messages and can convince the verifier every user signed his own message. At the same time, the size of aggregate signature should be less than the size of combined individual signatures. Signature schemes of this type can improve efficiency of numerous applications like SBGP protocol of secure Internet routing and PKI.*

On the other hand, most of proposed aggregate signature schemes based on assumption that Discrete log and Factorization problems are hard for attacker. At the same time, these problems are known to be efficiently solvable by quantum computer performing Shor algorithm. Considering the possibility of efficient quantum computer in the next few decades the problem of building post-quantum signatures schemes becomes urgent. Code-based signatures schemes are known as one of the candidates for post-quantum signatures.

This article presents code-based sequential aggregate signature scheme APCFS as extension of Parallel-CFS signature scheme. The proposed aggregation technique of individual Parallel-CFS signatures allows to achieve full signature aggregation, such that the size of aggregate signature is the same as the size of individual Parallel-CFS signature. By doing this we create the first code-based signature scheme of this kind.

Keywords: *code based cryptography, CFS signature, aggregate signature, post-quantum cryptography.*

References

1. Boneh D., Gentry C., Lynn B., Shacham H. A Survey of Two Signature Aggregation Techniques. CryptoBytes, 2003, vol. 6, no. 2.
2. Shor P. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. SIAM Journal on Scientic and Statistical Computing, 1997, vol. 26, no. 5, pp. 1484–1509.

2 Artyom Makarov, Department of Cryptology and Cybersecurity, NRNU MEPhI, Moscow, Russia. E-mail: zma.94@mail.ru

3. Grover L. A fast quantum mechanical algorithm for database search. Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing, 1996, pp. 212–219.
4. Wang W., Szefer J., Niederhagen R. FPGA-based Key Generator for the Niederreiter Cryptosystem Using Binary Goppa Codes. Cryptographic Hardware and Embedded Systems CHES 2017. Lecture Notes in Computer Science, 2017, pp. 253-274.
5. McEliece R. A public-key cryptosystem based on algebraic coding theory. DSN Progress Report, 1978, vol 42, pp. 114–116.
6. Bernstein D., Buchmann J., Dahmen E. Post-Quantum Cryptography. Springer-Verlag Berlin Heidelberg, 2009, 245 p.
7. Courtois N., Finiasz M., Sendrier N. How to Achieve a McEliece-Based Digital Signature Scheme. Advances in Cryptology — ASIACRYPT 2001. Lecture Notes in Computer Science, 2001, vol. 2248, pp. 157–174.
8. Faugere J., Otmani A., Perret L., Tillich J. Algebraic cryptanalysis of mcEliece variants with compact keys. Advances in Cryptology – EUROCRYPT 2010. Lecture Notes in Computer Science, 2010, vol. 6110, pp. 279–298.
9. Finiasz M. Parallel-CFS Strengthening the CFS McEliece-Based Signature Scheme. Selected Areas in Cryptography - 17th International Workshop, 2011, pp. 159–170.
10. Finiasz M., Sendrier N. Security bounds for the design of code-based cryptosystems. Advances in Cryptology – ASIACRYPT 2009. Lecture Notes in Computer Science, 2009, vol. 5912, pp. 88–105.
11. Bansarkhani R., Mohamed M., Albrecht Petzoldt A. MQSAS - A Multivariate Sequential Aggregate Signature Scheme. International Conference on Information Security, 2016, 19 p.
12. Lysyanskaya A., Micali S., Reyzin L., Shacham H. Sequential Aggregate Signatures from Trapdoor Permutations. EUROCRYPT 2004: Advances in Cryptology, 2004, pp. 74–90.
13. Landais G., Sendrier N. CFS Software Implementation. Cryptology ePrint Archive, 2012, 15 p.