УДК 519.7

А.О. МАКАРОВ

Национальный исследовательский ядерный университет «МИФИ», Москва

СХЕМА ПОСЛЕДОВАТЕЛЬНОЙ АГРЕГИРОВАННОЙ ЭЛЕКТРОННОЙ ПОДПИСИ С ЛЕНИВОЙ ПРОВЕРКОЙ НА ОСНОВЕ ТЕОРИИ АЛГЕБРАИЧЕСКОГО КОДИРОВАНИЯ

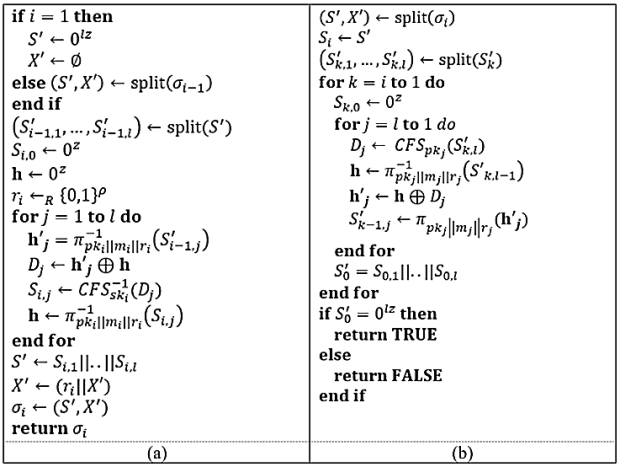
В работе представлена новая схема последовательной агрегированной электронной подписи с ленивой проверкой LARCFS: приводится её формальное описание, а также оценка теоретической стойкости в сведении к стойкости схемы электронной подписи CFS на основе кодов Гоппы.

Схемы последовательной агрегированной электронной подписи позволяют группе независимых подписантов сформировать единую подпись для множества сообщений, размеры которой меньше суммарного размера индивидуальных подписей. Свойство ленивой проверки схем последовательной агрегированной подписи позволяют не проверять текущую агрегированную подпись при формировании следующей, что увеличивает производительность процедуры формирования подписи.

Представим формальное описание схемы LARCFS. *Генерация ключей*. Параметры схемы – натуральные числа m, t, $n = 2^m$, δ, l, ρ, причем $\binom{n}{t+\delta} > 2^{mt}$, криптографические хэш-функции h_i, $i = 1, \dots, l$; двоичный код Гоппы $\Gamma(g, S)$, заданный многочленом $g \in \mathbb{F}_n$ степени t с определяющим множеством S. Пусть H систематическая $mt \times n$ матрица проверки кода $\Gamma(G, s)$. $pk = H$ является открытым ключом, (g, S, D_Γ) образует закрытый ключ, где D_Γ – алгоритм декодирования синдрома кода Γ. $\pi: K \times \{0,1\}^k \to \{0,1\}^k$ – идеальный шифр, где K – множество ключей идеального шифра.

Агрегированная подпись. Пусть m_i – сообщение, подписанное пользователем u_i. $pk = \{pk_1, \dots, pk_n\}$ – открытые ключи пользователей, σ_{i-1} — предыдущее значение агрегированной подписи. Для пользователя u_i процедура формирования подписи представлена на рис. 1 (a).

Агрегированная проверка. Пусть m_i – сообщение, подписанное пользователем $u_i \in U$. $pk = \{pk_1, \dots, pk_i\}$ – открытые ключи пользователей U, σ_i – агрегированная подпись, созданная пользователями для сообщений $\{m_j | \, 1 \le j \le i\}$. Подпись σ_i представляется в виде $\sigma = (S', X')$, где $X' = (r_i, || \dots || r_1)$, $|S'| = z$ бит, $|r_j| = \rho$ бит, $j \in \{1, \dots, i\}$. Дальнейший алгоритм вычисления представлен на рис. 1 (b).



if $i = 1$ **then**
  $S' \leftarrow 0^{lz}$
  $X' \leftarrow \emptyset$
else $(S', X') \leftarrow \text{split}(\sigma_{i-1})$
end if
$(S'_{i-1,1}, \dots, S'_{i-1,l}) \leftarrow \text{split}(S')$
$S_{i,0} \leftarrow 0^z$
$\mathbf{h} \leftarrow 0^z$
$r_i \leftarrow_R \{0,1\}^\rho$
for $j = 1$ **to** l **do**
  $\mathbf{h}'_j = \pi^{-1}_{pk_i||m_i||r_i}(S'_{i-1,j})$
  $D_j \leftarrow \mathbf{h}'_j \oplus \mathbf{h}$
  $S_{i,j} \leftarrow CFS^{-1}_{sk_i}(D_j)$
  $\mathbf{h} \leftarrow \pi^{-1}_{pk_i||m_i||r_i}(S_{i,j})$
end for
$S' \leftarrow S_{i,1}||\dots||S_{i,l}$
$X' \leftarrow (r_i||X')$
$\sigma_i \leftarrow (S', X')$
return σ_i

(a)

$(S', X') \leftarrow \text{split}(\sigma_i)$
$S_i \leftarrow S'$
$(S'_{k,1}, \dots, S'_{k,l}) \leftarrow \text{split}(S'_k)$
for $k = i$ **to** 1 **do**
  $S_{k,0} \leftarrow 0^z$
  for $j = l$ **to** 1 *do*
    $D_j \leftarrow CFS_{pk_j}(S'_{k,l})$
    $\mathbf{h} \leftarrow \pi^{-1}_{pk_j||m_j||r_j}(S'_{k,l-1})$
    $\mathbf{h}'_j \leftarrow \mathbf{h} \oplus D_j$
    $S'_{k-1,j} \leftarrow \pi_{pk_j||m_j||r_j}(\mathbf{h}'_j)$
  end for
  $S'_0 = S_{0,1}||\dots||S_{0,l}$
end for
if $S'_0 = 0^{lz}$ **then**
  return TRUE
else
  return FALSE
end if

(b)

Рис. 1. Алгоритм формирования (a) и проверки (b) агрегированной электронной подписи, где $CFS^{-1}_{sk_i}$ — вычисление подписи схемы CFS

Теоретическая стойкость схемы LARCFS может быть показана в игровой модели Белларе-Рогавея, аналогично доказанному для схемы LMQSAS [1]. Пусть функция проверки подписи схемы CFS [2] с использованием кодов Гоппы – (t', ϵ')-стойкая односторонняя функция с секретом. Тогда схема последовательной агрегированной электронной подписи LARCFS является $(t, q_H, q_\pi, z, \epsilon)$-стойкой для всех эффективных противников с временем работы не более t и преимуществом ϵ, делающих не более q_H запросов к случайному оракулу, не более q_π запросов к оракулу идеального шифра, для всех t', ϵ', z, где z – размер агрегируемой части агрегированной подписи, $m, t, l \in \mathbb{N}$ – параметры схемы:

$$\epsilon \leq \frac{q_H 2^{z+\rho}}{(2^z - q_\pi^2)(2^\rho - q_H^2)}\epsilon' + q_\pi^2/2^z,$$
$$t = t'/l.$$

Список литературы

1. Макаров А.О. Схема Постквантовой агрегированной подписи с ленивой проверкой на основе многомерных квадратичных многочленов//Безопасность Информационных Технологий, 2023, Т. 30, N 3, С. 30–50.

2. Courtois N.T., Finiasz M., Sendrier N. How to Achieve a McEliece-Based Digital Signature Scheme//Advances in Cryptology — ASIACRYPT 2001/ ed. C. Boyd. – Berlin, Heidelberg: Springer, 2001. – P. 157–174.