Math-Net.Ru

Общероссийский математический портал

А. М. Гуселев, Применение теории решеток к анализу схем цифровой подписи,
Матем. вопр. криптогр., 2018, том 9, выпуск 4, 73–84

DOI: <https://doi.org/10.4213/mvk269>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и
согласны с пользовательским соглашением

<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 54.198.67.100

26 апреля 2023 г., 17:31:22

**Применение теории решеток
к анализу схем цифровой подписи**

А. М. Гуселев

*Технический комитет по стандартизации
«Криптографическая защита информации» (ТК 26), Москва*

Получено 18.IV.2018

Аннотация. Проведен анализ четырех атак на определенную в стандарте ГОСТ Р 34.10-2012 схему цифровой подписи. Для этих атак, использующих аппарат теории решеток, получены верхние асимптотические границы вероятности успешной реализации. На основании полученных численных оценок делается вывод о том, что рассмотренные методы анализа, основанные на использовании теории решеток, не способны понизить оценки стойкости схемы цифровой подписи, определенной в стандарте ГОСТ Р 34.10-2012.

Ключевые слова: схема цифровой подписи, теория решеток, подделка цифровой подписи

Application of the lattice theory to the analysis of digital signature schemes

A. M. Guselev

*Technical committee for standardization “Cryptography and security mechanisms”
(TC 26), Moscow*

Abstract. With the use of lattice theory four attacks on digital signature schemes described in the national standard GOST R 34.10-2012 are analysed. These attacks are based on the lattice theory. Upper asymptotic bounds for the probability of successful implementation are obtained. A conclusion is made that the considered attacks are unable to lower the security estimate of the Russian standardized signature scheme.

Key words: digital signature scheme, lattice theory, digital signature forgery

Citation: *Mathematical Aspects of Cryptography*, 2018, v. 9, № 4, pp. 73–84 (Russian)

© Академия криптографии Российской Федерации, 2018 г.

Введение

В настоящее время существует несколько хорошо изученных подходов к анализу схем цифровой подписи. Так, если подписываемое сообщение обрабатывается с помощью хэш-функции, при подделке цифровой подписи применяются методы, связанные с построением коллизий хэш-функций. Если объектом атаки является секретный ключ подписи, то могут использоваться методы решения задач факторизации или дискретного логарифмирования, в зависимости от математических структур, лежащих в основе схемы подписи. Далее основное внимание уделяется схемам, где такой структурой является подгруппа простого порядка группы точек эллиптической кривой, в частности схемам, определенным в стандартах ECDSA [11] и ГОСТ Р 34.10-2012 [14] (далее схема ГОСТ). Для указанных схем подписи здесь рассматриваются методы анализа, основанные на теории решеток.

Впервые аппарат теории решеток при анализе схем подписи был использован в 1997 году в [7], где описан метод анализа схемы DSA (версии схемы ECDSA, использующей подгруппу простого порядка мультипликативной группы поля вычетов [11]). Впоследствии вышел ряд работ по этой тематике. Так, в [12] для восстановления секретного ключа схем DSA и ECDSA использован LLL-алгоритм [6], в [2] — решетки Лагранжа, а в [9] схема DSA анализировалась в случае, когда для ее реализации используется подгруппа, порядок которой мал по сравнению с порядком базового поля вычетов. См. также [1, 3, 5, 10].

Наиболее актуальной в настоящее время является работа Д. Пулакиса [13]. В ней описаны методы восстановления секретного ключа и разового секретного значения (эффемерного ключа), используемых в схемах DSA и ECDSA, когда эти ключи или элементы, обратные к ним по модулю используемой подгруппы, являются «достаточно маленькими» по сравнению с ее мощностью. Автору не известны работы, в которых аппарат теории решеток применяется к анализу отечественной схемы цифровой подписи ГОСТ.

Ниже приводятся результаты исследования перспектив использования аппарата теории решеток при анализе стойкости схемы подписи ГОСТ. На основе результатов [13] и теории решеток построено четыре метода анализа, которые применимы к вариантам обобщенной схемы подписи Эль-Гамала [4], в частности к схемам DSA, ECDSA и ГОСТ. Для схемы ГОСТ получены оценки вероятности успешной реализации этих методов. Основным итогом заключается в том, что схема подписи ГОСТ является стойкой по отношению к рассмотренным методам анализа. Методы анализа, предложенные в настоящей работе, будем называть *MV-атаками*, поскольку они основаны на алгоритме Д. Миццианцио и П. Вульгариса [8].

1. Обобщенная схема цифровой подписи Эль-Гамала на эллиптических кривых

Схема подписи ГОСТ и схема ECDSA — это варианты обобщенной схемы Эль-Гамала [4], использующие операции в подгруппе простого порядка q группы точек эллиптической кривой E над конечным полем $\mathbb{F}_p$, где p — простое число. В схеме подписи Эль-Гамала на эллиптических кривых в подгруппе простого порядка выбирается точка P — один из открытых параметров схемы. Секретный ключ — это элемент $d \in \{1, \dots, q-1\}$, выбираемый случайно равномерно. По элементу d вычисляется точка эллиптической кривой $Q = dP$ — открытый ключ проверки подписи. Тогда (p, E, P, q, Q) — открытые параметры схемы, а d — секретный. Для построения цифровой подписи ([14]) под сообщением m вычисляется значение хэш-функции

$$e = (m) \in \{1, \dots, q-1\},$$

случайно равномерно выбирается эфемерный ключ $k \in \{1, \dots, q-1\}$ и вычисляются

$$kP = (x, y), \quad r \equiv x \pmod{q}.$$

Для обобщенной схемы Эль-Гамала уравнение подписи имеет вид

$$a \equiv (bd + ck) \pmod{q}, \tag{1}$$

набор параметров a , b и c может быть любой перестановкой элементов e , r и s , они могут принимать как положительные, так и отрицательные значения; пара (r, s) — подпись под сообщением m .

Обобщенная схема Эль-Гамала позволяет получить 12 схем подписи, различающихся уравнением подписи. Так, схема ГОСТ — это вариант обобщенной схемы Эль-Гамала с $(a, b, c) = (s, r, e)$, т. е. уравнение подписи имеет вид

$$s \equiv (rd + ke) \pmod{q}.$$

В случае схемы ECDSA используется набор $(a, b, c) = (e, -r, s)$, т. е. уравнение подписи имеет вид

$$s \equiv k^{-1}(e + dr) \pmod{q}.$$

Аналогичное уравнение подписи используется в схеме подписи DSA.

2. Теоретическое обоснование MV-атак

В основе MV-атак лежат следующие утверждения из [8] и [13].

Теорема 1 ([8]). Пусть $\mathcal{L}$ — n -мерная решетка в $\mathbb{R}^n$ и вектор $\mathbf{y} \in \mathbb{R}^n$. Существует детерминированный алгоритм, который при $n \rightarrow \infty$ позволяет за $2^{2n+o(n)}$ двоичных операций вычислить такой вектор $\mathbf{v} \in \mathcal{L}$, что для каждого $\mathbf{t} \in \mathcal{L}$ имеет место неравенство $\|\mathbf{v} - \mathbf{y}\| \leq \|\mathbf{t} - \mathbf{y}\|$.

Эта теорема обосновывает существование указанного алгоритма.

Теорема 2 ([13]). Пусть $q > 2$ — простое число, n, A_i, B_i , $i = 1, \dots, n$, — такие числа, что

$$n \leq \log_2 \log_2 q - 1 \quad \text{и} \quad 2^{i-1} q^{i/(n+1)} < A_i < 2^i q^{i/(n+1)}.$$

Тогда система сравнений

$$y_i + A_i x + B_i \equiv 0 \pmod{q}, \quad i = 1, \dots, n, \quad (2)$$

имеет по крайней мере одно такое решение

$$\mathbf{v} = (x, y_1, \dots, y_n) \in \{0, \dots, q-1\}^{n+1},$$

что

$$\|\mathbf{v}\| < \frac{1}{16} q^{n/(n+1)}. \quad (3)$$

Лемма 1 ([13]). Пусть заданы простое число $q > 2$, целое положительное число $n \leq \log_2 \log_2 q - 1$, такие неотрицательные числа A_i , что

$$2^{i-1} q^{i/(n+1)} < A_i < 2^i q^{i/(n+1)},$$

и $B_i \in \{1, \dots, q-1\}$, $i = 1, \dots, n$. Если $\mathcal{L} \subset \mathbb{Z}^{n+1}$ — решетка, базисом которой являются строки квадратной матрицы

$$J = \begin{pmatrix} -1 & A_1 & A_2 & \cdots & A_n \\ 0 & q & 0 & \cdots & 0 \\ 0 & 0 & q & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & q \end{pmatrix},$$

то для каждого вектора $\mathbf{v} \in \mathcal{L} \setminus \{0\}$ имеет место неравенство

$$\|\mathbf{v}\| > \frac{1}{8} q^{n/(n+1)}.$$

Если система (2) имеет решение, удовлетворяющее условию (3), то алгоритм из теоремы 1, примененный к вектору $(0, B_1, \dots, B_n)$ и решетке из леммы 1, даст вектор, первой координатой которого является x . Трудоемкость алгоритма составляет $O((\log_2 q)^2)$ двоичных операций.

Теорема 2 является основой для построения алгоритмов восстановления секретных долговременного и эфемерного ключей и содержит условия, при выполнении которых можно найти секретные параметры схемы подписи, решая соответствующую систему сравнений.

Перейдем непосредственно к описанию MV-атак.

3. MV-атаки на обобщенную схему Эль-Гамала

3.1. Атака MV-1

Целью атаки MV-1 является восстановление секретного ключа подписи в обобщенной схеме Эль-Гамала.

Пусть выполняются условия теоремы 2, при этом зафиксирован параметр

$$n \leq \log_2 \log_2 q - 1$$

и известно $t \leq n$ подписей (r_j, s_j) под сообщениями m_j , $j = 1, \dots, t$, вычисленных по обобщенной схеме Эль-Гамала.

Перепишем уравнение (1) подписи обобщенной схемы Эль-Гамала в виде

$$k_j + db_j c_j^{-1} - a_j c_j^{-1} \equiv 0 \pmod{q}, \quad j = 1, \dots, t. \quad (4)$$

Введем обозначения

$$C_j \equiv b_j \cdot c_j^{-1} \pmod{q},$$

$$D_j \equiv -a_j \cdot c_j^{-1} \pmod{q}$$

и перепишем уравнение (4) в виде

$$k_j + C_j d + D_j \equiv 0 \pmod{q}, \quad j = 1, \dots, t. \quad (5)$$

Приведем алгоритм восстановления секретного ключа обобщенной схемы Эль-Гамала.

АЛГОРИТМ АТАКА MV-1

Вход: t подписанных сообщений (m_j, r_j, s_j) , $j = 1, \dots, t$.

Выход: ключ подписи d .

1. Вычисляются значения $C_j \equiv b_j \cdot c_j^{-1} \pmod{q}$, $D_j \equiv -a_j \cdot c_j^{-1} \pmod{q}$.

2. Выбираются такие числа A_i , что

$$2^{i-1}q^{i/(n+1)} < A_i < 2^i q^{i/(n+1)}, \quad i = 1, \dots, n.$$

3. **Если** существуют такие $i = 1, \dots, n$ и $j = 1, \dots, t$, что выполняются неравенства $2^{i-1}q^{i/(n+1)} < C_j < 2^i q^{i/(n+1)}$, **то**

4. для этих i, j полагается $A_i = C_j$ (если таких пар i, j более одной, то выбирается пара с наибольшим j).

5. Вычисляются $B_{ij} \equiv A_i D_j C_j^{-1} \pmod{q}$, $i = 1, \dots, n$, $j = 1, \dots, t$.

6. Пусть M — множество всех отображений $\mu: \{1, \dots, n\} \rightarrow \{1, \dots, t\}$, $|M| = t^n$. Для каждого $\mu \in M$ вычисляются все такие значения x_μ , что вектор $\mathbf{v}_\mu = (x_\mu, y_{1,\mu(1)}, \dots, y_{n,\mu(n)})$ является решением системы

$$y_i + A_i x + B_{i,\mu(i)} \equiv 0 \pmod{q}, \quad i = 1, \dots, t, \quad (6)$$

и удовлетворяет условию $\|\mathbf{v}_\mu\| < q^{n/(n+1)}/16$.

7. Для каждого $\mu \in M$ проверяется, является ли какое-либо из вычисленных значений x_μ секретным ключом d .

Уравнения (6) получены из (5) умножением на $C_j^{-1}A_i$:

$$k_j C_j^{-1} A_i + d A_i + C_j^{-1} D_j A_i \equiv 0 \pmod{q}, \quad j = 1, \dots, t, \quad i = 1, \dots, n,$$

и переобозначениями $x = d$, $y_{ij} = k_j C_j^{-1} A_i$, $B_{ij} = C_j^{-1} D_j A_i$.

При тех же предположениях, что в [13], трудоемкость атаки MV-1 составляет $O((\log_2 q)^2((\log_2 q)^{\log_2 t} + (\log_2 \log_2 q)^4))$ двоичных операций и $O((\log_2 q)^{1+\log_2 t})$ операций в группе точек эллиптической кривой.

Для применения к конкретной схеме подписи атаку MV-1 можно адаптировать за счет выбора значений C_j и D_j . В частности, для схемы ГОСТ равенства (4) примут вид

$$k_j + dr_j e_j^{-1} - s_j e_j^{-1} \equiv 0 \pmod{q},$$

а для схемы ECDSA — вид

$$k_j - dr_j s_j^{-1} - s_j^{-1} e_j \equiv 0 \pmod{q}.$$

Согласно теореме 2 атаку MV-1 можно применять для восстановления секретного ключа d , если существует такое $\mu \in M$, для которого выполняется неравенство

$$\|(d, k_{1\mu(1)}, \dots, k_{n\mu(n)})\| < \frac{1}{16} q^{n/(n+1)}, \quad (7)$$

где $k_{ij} \equiv k_j C_j^{-1} A_i \pmod{q}$, $i = 1, \dots, n$, $j = 1, \dots, t$.

Оценим вероятность выполнения неравенства (7) для ключа d схемы ГОСТ, считая, что d выбирается случайно и равновероятно из интервалов $2^{254} < q < 2^{256}$ или $2^{508} < q < 2^{512}$. Эти интервалы рекомендованы в стандарте ГОСТ Р 34.10-2012.

Для схемы ГОСТ неравенство (7) можно переписать в виде

$$\left\| \left(d, A_1 k_{\mu(1)} r_{\mu(1)} e_{\mu(1)}^{-1}, \dots, A_n k_{\mu(n)} r_{\mu(n)} e_{\mu(n)}^{-1} \right) \right\| < \frac{q^{n/(n+1)}}{16}. \quad (8)$$

Для его выполнения необходимо, чтобы каждая компонента вектора в (8), приведенная по модулю q (в частности первая), не превышала $q^{n/(n+1)}/16$. Заметим, что в данном случае рассматривается полученное из теоремы 2 условие (8), достаточное для применения атаки MV-1.

Из предположения о случайности и равновероятности распределения d на $\{1, \dots, q-1\}$ следует, что вероятность выполнения условия (8) не превосходит

$$\frac{1}{q-1} \frac{q^{n/(n+1)}}{16} \approx \frac{1}{16q^{1/(n+1)}}.$$

Сначала рассмотрим случай $2^{254} < q < 2^{256}$. Тогда

$$\log_2 \log_2 q \geq \log_2 \log_2 2^{254} \approx 7.99$$

и $n \leq 7.99 - 1$, т. е. $n \leq 6$.

При $n = 1$ вероятность выполнения условия (8) не больше

$$\frac{1}{16q^{1/2}} = \frac{1}{2^{131}} \approx 10^{-39.4},$$

и с ростом n верхняя оценка этой вероятности возрастает, например при $n = 6$ оценка имеет вид

$$\frac{1}{16q^{1/7}} = \frac{1}{2^{4+254/7}} \approx 10^{-12.1}.$$

(Отметим, что если считать, что все компоненты вектора (8) независимы и имеют равновероятное распределение на $\{1, \dots, q-1\}$, то верхняя оценка вероятности существенно уменьшится, примет вид

$$\left(\frac{1}{16q^{1/(n+1)}} \right)^{n+1} = \frac{1}{16q} < 10^{-77.6}$$

и перестанет зависеть от n .)

Аналогично, если $2^{508} < q < 2^{512}$, то $\log_2 \log_2 2^{508} \approx 8.99$, следовательно, $n \leq 8.99 - 1$, т.е. $n \leq 7$, и в качестве грубых верхних оценок вероятности выполнения неравенства (8) получаем

$$\frac{1}{16q^{1/2}} = \frac{1}{2^{258}} \approx 10^{-77.7} \quad \text{при } n = 1$$

и

$$\frac{1}{16q^{1/8}} = \frac{1}{2^{4+508/8}} \approx 10^{-20.3} \quad \text{при } n = 7.$$

(Как и выше, если считать, что все компоненты вектора (8) независимы и имеют равновероятное распределение на $\{1, \dots, q-1\}$, то верхняя оценка вероятности существенно уменьшится, примет вид

$$\left(\frac{1}{16q^{1/(n+1)}} \right)^{n+1} = \frac{1}{16q} < 10^{-154}$$

и перестанет зависеть от n .)

3.2. Атака MV-2

В этом подразделе рассматривается атака, целью которой является восстановление элемента, обратного по модулю q к секретному ключу обобщенной схемы подписи Эль-Гамала. После нахождения такого элемента для определения секретного ключа подписи остается обратить его по модулю q . Такую атаку будем называть атакой MV-2.

По своей сути атака MV-2 является модификацией атаки MV-1 и, соответственно, для ее реализации необходимы схожие начальные условия.

Преобразуем систему сравнений (5), домножив ее на $d^{-1} \pmod{q}$:

$$d^{-1}k_j + C_j + D_j d^{-1} \equiv 0 \pmod{q}, \quad j = 1, \dots, t.$$

Отсюда получаем систему

$$d^{-1}k_j D_j^{-1} A_i + d^{-1} A_i + C_j D_j^{-1} A_i \equiv 0 \pmod{q}, \quad j = 1, \dots, t, \quad (9)$$

которую можно рассматривать как систему сравнений от неизвестных $y_{i,j} = d^{-1}k_j D_j^{-1} A_i$ и $x \equiv d^{-1} \pmod{q}$. Решив эту систему относительно x , можно найти значение элемента, обратного по модулю q к секретному ключу подписи.

Трудоемкость атаки MV-2 совпадает трудоемкостью атаки MV-1.

Согласно теореме 2 атаку MV-2 можно применять для анализа схемы ГОСТ, если выполняется неравенство

$$\|(d^{-1} \pmod{q}, k_{1\mu(1)}, \dots, k_{n\mu(n)})\| < \frac{q^{n/(n+1)}}{16}, \quad (10)$$

где

$$k_{ij} = d^{-1}k_j D_j^{-1} A_i \equiv d^{-1}k_j s_j e_j^{-1} A_i \equiv (k_j e_j^{-1} r_j + d^{-1}k_j^2) A_i \pmod{q},$$

$$i = 1, \dots, n, \quad j = 1, \dots, t.$$

Оценки вероятности выполнения неравенства (10) совпадают (для соответствующих значений параметров) с оценками вероятности выполнения неравенства (7), вычисленными в подразделе 3.1.

Отличительная особенность атак MV-1 и MV-2 состоит в том, что их можно реализовать даже по одному подписанному сообщению, удовлетворяющему заданным требованиям, т. е. при $t = 1$. Для применения атак MV-3 и MV-4, описанных ниже, необходимо, чтобы выполнялось условие $t \geq 2$.

Вместе с тем, поскольку для успешной реализации атак MV-1 и MV-2 необходимо, чтобы секретный ключ формирования подписи d удовлетворял сформулированным выше условиям, схемы подписи могут считаться стойкими относительно данных атак весь срок эксплуатации секретного ключа d , не удовлетворяющего условиям их применимости.

Ниже представлено еще две атаки, применение которых возможно в любой момент эксплуатации схемы подписи независимо от предварительного выбора длительного секретного ключа.

3.3. Атака MV-3

В этом подразделе рассматривается атака, целью которой является восстановление эфемерного ключа, использованного для формирования подписи под фиксированным сообщением в обобщенной схеме Эль-Гамала. Хорошо известно, что восстановление эфемерного ключа приводит к восстановлению долговременного секретного ключа. Далее такую атаку будем называть атакой MV-3.

Пусть дано $t \geq 2$ подписанных сообщений, полученных способом, описанным в подразделе 3.1. Если зафиксировать одно из сравнений в системе (5) (без ограничения общности будем считать, что зафиксировано сравнение с номером t), то можно из него выразить d :

$$d \equiv -C_t^{-1}(k_t + D_t) \pmod{q},$$

а затем подставить полученное выражение в оставшиеся сравнения системы:

$$k_j - C_j C_t^{-1} k_t - C_j C_t^{-1} D_t + D_j \equiv 0 \pmod{q}, \quad j = 1, \dots, t-1.$$

Если положить $-C_j C_t^{-1} \equiv \tilde{C}_j \pmod{q}$, $-C_j C_t^{-1} D_t + D_j \equiv \tilde{D}_j \pmod{q}$, то эта система примет вид

$$k_j \tilde{C}_j^{-1} A_i + k_t A_i + \tilde{C}_j^{-1} \tilde{D}_j A_i \equiv 0 \pmod{q}, \quad j = 1, \dots, t-1. \quad (11)$$

Решая систему сравнений (11) относительно неизвестных $y_{i,j} = k_j \tilde{C}_j^{-1} A_i$ и $x = k_t$, можно получить значение эфемерного ключа, использованного при формировании подписи под сообщением с номером t .

Трудоемкость атаки MV-3 совпадает с трудоемкостью атаки MV-1.

Чтобы применить атаку MV-3 к схеме ГОСТ, необходимо в системе сравнений (11) провести соответствующие замены параметров $\tilde{C}_j$ и $\tilde{D}_j$. Согласно теореме 2 атаку MV-3 можно применять для анализа схемы ГОСТ, если выполняется неравенство

$$\|(k_t, k_{1\mu(1)}, \dots, k_{n\mu(n)})\| < \frac{q^{n/(n+1)}}{16}, \quad (12)$$

где $k_{ij} = -k_j(r_j^{-1}e_j)(r_t^{-1}e_t)A_i \pmod{q}$, $i = 1, \dots, n$, $j = 1, \dots, t-1$.

Оценки вероятности выполнения неравенства (12) совпадают (при соответствующих значениях параметров) с оценками вероятности выполнения неравенства (7), вычисленными в подразделе 3.1.

3.4. Атака MV-4

В этом подразделе рассматривается атака, целью которой является восстановление элемента, обратного по модулю q к эфемерному ключу k , использованному для формирования подписи под фиксированным сообщением в обобщенной схеме Эль-Гамала. Чтобы определить использованный эфемерный ключ, необходимо обратить по модулю q элемент, полученный в результате применения этой атаки. Далее будем ее называть атакой MV-4.

По своей сути атака MV-4 является модификацией атаки MV-3 и отличается от нее домножением каждого сравнения системы (11) на элемент $k_t^{-1} \pmod{q}$ и соответствующей перестановкой коэффициентов.

Итак, систему

$$k_t^{-1}k_j + \tilde{C}_j + \tilde{D}_j k_t^{-1} \equiv 0 \pmod{q}, \quad j = 1, \dots, t,$$

можно преобразовать в систему вида

$$k_t^{-1}k_j \tilde{D}_j^{-1} A_i + k_t^{-1} A_i + \tilde{C}_j \tilde{D}_j^{-1} A_i \equiv 0 \pmod{q}, \quad j = 1, \dots, t. \quad (13)$$

Решив систему сравнений (13) от неизвестных

$$y_{i,j} = k_t^{-1}k_j \tilde{D}_j^{-1} A_i \quad \text{и} \quad x = k_t^{-1} \pmod{q},$$

можно найти элемент $k_t^{-1} \pmod{q}$.

Трудоемкость атаки MV-4 совпадает с трудоемкостью атаки MV-1.

Чтобы применить атаку MV-4 к схеме ГОСТ, необходимо в системе сравнений (13) провести соответствующие замены для параметров $\tilde{C}_j$ и $\tilde{D}_j$. Согласно теореме 2 атаку MV-4 можно применять для анализа схемы ГОСТ, если выполняется неравенство

$$\|(k_t^{-1} \pmod{q}, k_{1\mu(1)}, \dots, k_{n\mu(n)})\| < \frac{q^{n/(n+1)}}{16}, \quad (14)$$

где

$$k_{ij} \equiv k_t^{-1}k_j \tilde{D}_j^{-1} A_i = r_j e_j^{-1} r_t^2 e_t^{-1} d k_t^{-1} k_j + \\ + r_j e_j^{-1} r_t e_t^{-1} k_j - r_j d e_j^{-1} k_t^{-1} k_j - k_t^{-1} k_j^2 \pmod{q},$$

$$i = 1, \dots, n, \quad j = 1, \dots, t.$$

Оценки вероятности выполнения неравенства (14) совпадают (при соответствующих значениях параметров) с оценками вероятности выполнения неравенства (7), вычисленными в подразделе 3.1.

Список литературы

- [1] Blake I. F., Garefalakis T., “On the security of the digital signature algorithm”, *Des. Codes Cryptogr.*, **26**:1–3 (2002), 87–96.
- [2] Draziotis K., Poulakis D., “Lattice attacks on DSA schemes based on Lagrange’s algorithm”, *Lect. Notes Comput. Sci.*, **8080**, 2013, 119–131.
- [3] Faugere J.-L., Goyet C., Renault G., “Attacking (EC)DSA given only an implicit hint”, *SAC 2012*, *Lect. Notes Comput. Sci.*, **7707**, 2013, 252–274.
- [4] Horster P., Michels M., Petersen H., “Generalized El-Gamal signature schemes for one message block”. In: “*Proc. 2nd Int. Workshop on IT-Security*”, 1994, 66–81.
- [5] Howgrave-Graham N. A., Smart N. P., “Lattice attacks on digital signature schemes”, *Des. Codes Cryptogr.*, **23** (2001), 283–290.
- [6] Lenstra A. K., Lenstra H. W. Jr., Lovasz L., “Factoring polynomials with rational coefficients”, *Math. Ann.*, **261** (1982), 513–534.
- [7] Goldwasser S., Bellare M., Micciancio D., “‘Pseudo-random’ number generation within cryptographic algorithms: the DSS case”, *Lect. Notes Comput. Sci.*, **1294**, 1997, 277–291.
- [8] Micciancio D., Voulgaris P., “A deterministic single exponential time algorithm for most lattice problems based on Voronoi cell computations”, *SIAM J. Comput.*, **42**:3 (2013), 1364–1391.
- [9] Nguyen P., Shparlinski I. E., “The insecurity of the digital signature algorithm with partially known nonces”, *J. Cryptology*, **15** (2002), 151–176.
- [10] Nguyen P., Shparlinski I. E., “The insecurity of the elliptic curve digital signature algorithm with partially known nonces”, *Des. Codes Cryptogr.*, **30**:2 (2003), 201–217.
- [11] *National Institute of Standards and Technology (NIST). Digital signature standard*, FIPS Publication 186., May 1994.
- [12] Poulakis D., “Some lattice attacks on DSA and ECDSA”, *Appl. Algebra Eng., Commun. and Comput.*, **22** (2011), 347–358.
- [13] Poulakis D., “New lattice attacks on DSA schemes”, *J. Math. Cryptology*, **10**:2 (2016), 135–144.
- [14] *Национальный стандарт Российской Федерации. ГОСТ Р 34.10-2012. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи*, М.: Федеральное агентство по техническому регулированию и метрологии, 2012.