DOI: 10.58254/viti.5.2024.20.227

УДК 003.26:519.688

канд. техн. наук Яковлєв С. В. ORCID: 0000-0002-5647-5043 (НТУУ «КПІ ім. Ігоря Сікорського»)
Кріпака І. А. (ННФТІ НТУУ «КПІ ім. Ігоря Сікорського»)

МЕТОДИ УСІЧЕННЯ ЦИФРОВОГО ПІДПИСУ ДЛЯ СХЕМ ТИПУ ЕЛЬ-ГАМАЛЯ ТА ДСТУ 4145-2002

Усічення цифрового підпису має важливе значення для реалізації криптографічних систем для малоресурсних пристроїв, зокрема у системах, де підписи зберігаються довгий час, але перевіряються відносно нечасто, таких як апаратні журнали аудиту чи сховища захищених документів. Скорочення підпису також може бути використане у тих випадках, коли обмежено пам’ять для представлення чи зберігання самого підпису (наприклад, у QR-кодах). У відкритих джерелах запропоновано методи усічення підпису для стандартів ECDSA та EdDSA.

У цій роботі запропоновано метод усічення цифрових підписів для класичної схеми Ель-Гамаля та деяких її узагальнень, які ґрунтуються на модулярній арифметиці. Запропоновані методи не вимагають зміни процедури підписування, а тому застосовні до довільних існуючих реалізацій схеми Ель-Гамаля; відновлення цифрового підпису відбувається завдяки збільшенню обчислювальних витрат з боку сторони, яка перевіряє підпис. Також запропоновано метод усічення цифрового підпису для національного стандарту ДСТУ 4145-2002; у цьому методі враховано особливості арифметики еліптичних кривих, на яких ґрунтується стандарт.

Запропоновані методи дозволяють ефективно реалізовувати усічення підписів типу Ель-Гамаля (особливо відчутно для підписів ДСТУ 4145-2002), відкидаючи до 32 бітів, але складність перевірки починає швидко зростати зі збільшенням частини підпису, що відкидається. Втім, для обраних меж довжини відкинутої частини запропоновані алгоритми мають відносно ефективну реалізацію і тому можуть бути використані для зменшення довжини підписів у протоколах для малоресурсних пристроїв.

Ключові слова: *цифровий підпис, схема Ель-Гамаля, еліптичні криві, ДСТУ 4145-2002.*

S. Yakovliev, I. Kripaka. Methods of digital signature truncation for El-Gamal-type signatures and for DSTU 4145-2002.

Digital signature truncation is important for implementing cryptographic systems for low-resource devices, particularly in systems where signatures are stored for a long term but are checked relatively infrequently. Among such systems we can mention hardware audit logs or secure document repositories. Signature truncation can also be used in cases where memory is limited to represent or store the signature itself (for example, in QR codes). Signature truncation methods for ECDSA and EdDSA standards were proposed in public sources.

This paper proposes a method of truncation of digital signatures for the classical El-Gamal scheme and some of its generalizations, which are based on modular arithmetic. The proposed methods do not require any alternations in the signing procedure, and are therefore applicable to arbitrary existing implementations of the El-Gamal scheme; the restoration of a digital signature occurs at the expense of an increase in computational costs on the part of the party verifying the signature. A digital signature truncation method for the national standard DSTU 4145-2002 is also proposed; this method takes into account the properties of the arithmetic of elliptic curves, on which the standard is based.

The proposed methods make it possible to effectively implement the truncation of signatures of the El-Gamal type (especially noticeable for DSTU 4145-2002 signatures), discarding up to 32 bits of signature, but the complexity of the verification increases rapidly with the increase in the discarded part of the signature. However, for selected limits of the length of the discarded part, the proposed algorithms have a relatively efficient implementation and therefore can be used to reduce the length of signatures in protocols for low-resource devices.

Keywords: *digital signature, El-Gamal scheme, elliptic curves, DSTU 4145-2002.*

Постановка завдання. Проблема скорочення підпису має велике значення в легкій криптографії для малоресурсних пристроїв, зокрема у системах, де підписи зберігаються довгий час, але перевіряються відносно нечасто (наприклад, в апаратних журналах аудиту чи сховищах захищених документів). Також скорочення підпису має значення у тих випадках, коли обмежено пам’ять для представлення самого підпису, наприклад, у QR-кодах. У таких ситуаціях було б бажано, щоб підпис скорочувався на стороні підписника без безпосередньої зміни алгоритму, – можливо, завдяки додатковим обчисленням на стороні перевіряючого. Також очевидною вимогою скороченого алгоритму підпису виступає збереження та незначне

зменшення стійкості, оскільки зловмисник може певним чином маніпулювати невідомою частиною підпису.

Нині відомі методи, направлені на скорочення розміру цифрового підпису для деяких типів схем цифрового підпису. Зокрема, був запропонований ефективний метод для скорочення підписів схем ECDSA та EdDSA, які побудовані на еліптичних кривих над простими полями. У цій роботі запропоновано аналогічні методи для класичних та узагальнених схем Ель-Гамаля, а також для національного стандарту цифрового підпису ДСТУ 4145-2002.

Аналіз публікацій за темою дослідження. Однією з основних сучасних схем цифрового підпису є *схема Ель-Гамаля* [3]. Наведемо її короткий опис, необхідний для викладення подальшого матеріалу.

1) Загальні параметри: p – велике просте число, g – елемент великого порядку q за модулем p. Особистим ключем виступає число $x \in \mathbb{Z}_q$, відкритим ключем – число $y = g^x \bmod p$. Використовується також геш-функція $H : \{0,1\}^* \to \mathbb{Z}_q^*$.

2) Постановка підпису описується таким алгоритмом:

– нехай k – випадково згенероване одноразове число, $k \in \mathbb{Z}_q^*$, $H(m)$ – геш-значення вхідного повідомлення m, $H(m) \in \mathbb{Z}_q^*$;
– обчислюються значення $r = g^k \bmod p$, $s = k^{-1}(H(m) - rx) \bmod q$;
– підписом повідомлення m є пара чисел (r, s);

3) Перевірка підпису виконується за співвідношенням:

$$y^r \cdot r^s \stackrel{?}{\equiv} g^{H(m)} \pmod p.$$

Якщо воно виконується, то підпис вважається вірним, інакше підпис невірний.

Варто зазначити, що довжина підпису у схемі Ель-Гамаля складає $\lceil log_2 q \rceil + \lceil log_2 p \rceil$ бітів. До прикладу, якщо обрати p як 1024-бітове число, а q як 160-бітове, то довжина підпису буде складати 1024 + 160 = 1184 бітів.

Алгебраїчні співвідношення, які лежать у основі схеми Ель-Гамаля, можуть бути замінені на інші, що дозволяє генерувати інші схеми зі збереганням основних властивостей. Значну частину таких схем можна описати у формальний спосіб, який одержав назву *узагальненої схеми Ель-Гамаля* [4]. Такі схеми задаються параметрами A, B, C, які визначаються як певні функції від чисел $H(m)$, s, r. Постановка підпису відбувається аналогічно до класичної схеми, причому параметр s знаходиться зі співвідношення $Ak \equiv B + Cx \pmod q$. Перевірка підпису виконується за співвідношенням $r^A \stackrel{?}{\equiv} g^B y^C \pmod p$.

Зауважимо також, що схеми Ель-Гамаля (і класичну, й узагальнену) можна перевизначити на інших алгебраїчних структурах із мультиплікативною операцією, наприклад, на еліптичних кривих.

У роботі [1] було розглянуто три можливих методи скорочення підписів у схемах типу Ель-Гамаля.

1. Схема із використанням функції компресії.

У цьому підході пропонується робити скорочення параметрів завдяки деякій функції компресії. Найбільш вдала реалізація цього методу, на нашу думку, викладена у стандарті цифрового підпису DSA [5], де значення r, s обчислюються за формулами

$$r = (g^k \bmod p) \bmod q, \qquad s = k^{-1}(H(m) + xr) \bmod q,$$

а перевірочне співвідношення має такий вид:

$$r \stackrel{?}{\equiv} \left(\left(g^{H(m)s^{-1} \bmod q} \cdot y^{rs^{-1} \bmod q}\right) \bmod p\right) \bmod q.$$

Перевагою цього методу є його довжина підпису, яка складає $2\lceil log_2 q \rceil$ бітів. До прикладу, якщо обрати p як 1024-бітове число, а q як 160-бітове, то довжина підпису DSA буде складати 320 бітів проти 1184 бітів у класичній схемі Ель-Гамаля. Але варто зазначити, що застосування цього методу до схем типу Ель-Гамаля вимагає їхньої значної алгоритмічної перебудови, фактично – побудови нової схеми цифрового підпису.

2. Фіксування частини підпису.

У цьому підході для зменшення підпису фіксується частина параметру r: $r = r_0 \| const$, де r_0 – обчислювана частина підпису, $const$ – зафіксована частина підпису, яка є загальним параметром схеми. Щоб отримати такий підпис, генеруються випадкові значення k доти, доки r не матиме потрібної форми. Сам підпис при цьому буде мати форму (r_0, s) та, відповідно, мати скорочену довжину. Альтернативно можна фіксувати частину параметру s.

Зауважимо, що цей підхід вимагає суттєвого збільшення ресурсних витрат у сторони, яка підписує, і тому для малопотужних пристроїв цей метод слабко застосовний.

3. Відкидання частини підпису.

Основна ідея цього методу полягає в скороченні частини s підпису. Величина s представляється як $s = s_0 \| s_1$, сам підпис буде мати форму (r, s_0), а частина s_1 буде відновлюватись під час перевіряння підпису. На противагу попередньому способу, тут обчислювальне навантаження збільшується на стороні, яка перевіряє підпис.

Саме цей метод розглядався у [1] як основний, але Томас Порнін [2] незалежно дослідив такий метод та запропонував його ефективну реалізацію для схем цифрового підпису ECDSA/EdDSA.

Метою цієї роботи є розробка ефективних методів усічення цифрового підпису для схем типу Ель-Гамаля, зокрема для національного стандарту цифрового підпису ДСТУ 4145-2002.

Виклад основного матеріалу дослідження. Сформулюємо методи усічення підпису для класичної схеми Ель-Гамаля та його узагальнених варіантів на основі відкидання частини підпису.

Спочатку необхідно обмежити доцільну величину скорочення підпису: очевидно, що ми не можемо відкинути дуже велику кількість бітів s, тому що тоді втратиться залежність з бітами секретного ключа x та одноразового ключа k і підпис стане уразливим до атак відновлення ключа та підробки. Будемо вважати, що кількість t бітів підпису, які відкидаються, лежить в межах $8 \leq t \leq 32$, і що сторони заздалегідь домовляються про конкретне значення t.

Представимо частину s як $s = s_0 \| s_1 = s_0 + s_1 2^n$, де $n = \lceil log_2 q \rceil - t$, s_0 – частина підпису, що залишається, а s_1 – частина, що відкидається. Підписом у такому випадку буде пара (r, s_0).

Для відновлення підпису під час перевіряння метод верифікації потребує алгоритму ефективного знаходження можливих кандидатів разом із перевіркою на правильність перевірочного співвідношення. Застосуємо для такої задачі алгоритм великих та малих кроків (BSGS [6]), який повертає відповідь у форматі $s_1 = i + jI$, $i \in \{1, \dots I\}$, $j \in \{1, \dots J\}$, а параметри I та J визначаються налаштуваннями алгоритму BSGS.

З перевірочного співвідношення схеми Ель-Гамаля одержуємо:

$$y^r \cdot r^{s_0 + s_1 2^n} \stackrel{?}{\equiv} g^{H(m)} \ (mod\ p),$$
$$y^r \cdot r^{s_0 + i2^n} \stackrel{?}{\equiv} g^{H(m)} r^{jI \cdot 2^n} \ (mod\ p).$$

Останнє співвідношення дозволяє адаптувати алгоритм BSGS для нашої задачі.

Алгоритм 1: знаходження значення s_1 для відновлення усіченого підпису в класичній схемі Ель-Гамаля.

1. Встановити $J = 2^{t/2}$, $I = 2^{t/2-1}$.
2. Для j від 0 до J обчислюємо значення $U_j = g^{H(m)} \cdot r^{-jI\,2^n} \ mod\ p$.
3. Для i від 0 до I обчислюємо значення $V_i = y^r \cdot r^{s_0 + i\,2^n}$.
4. Шукаємо збіги між множинами $\{U_j\}$ та $\{V_i\}$. Кожен збіг $U_i = V_j$ формує кандидата на відновлений підпис $s = s_0 + (i + Ij)2^n$, якого вже перевіряємо за основним перевірочним співвідношенням схеми Ель-Гамаля. Якщо збігів не виявлено, підпис вважається невірним.

В аналогічний спосіб будується алгоритм усічення цифрового підпису для узагальненої схеми Ель-Гамаля. Зауважимо, що аналітична форма величин U_j, V_i визначається через параметри узагальненої схеми; приклади таких співвідношень для різних варіантів узагальнених схем наведено у таблиці 1. Варто додати, що у таблиці параметри, позначені як «довільні», не повинні залежати від s, інакше наведений метод вимагатиме уточнення та додаткової адаптації.

Алгоритм відновлення та перевіряння усіченого цифрового підпису в узагальненій схемі Ель-Гамаля повністю повторює Алгоритм 1, за винятком інших формул для обчислення значень U_j, V_i.

Таблиця 1

Формули обчислення величин U_j, V_i для деяких варіантів узагальнених схем Ель-Гамаля із різними параметрами A, B, C

Параметри	**Перевірочне співвідношення**	U_j	V_i
$A = s,\ B = m,\ C = -r$	$r^s = g^m y^{-r}$	$g^m r^{-(jI2^n)}$	$y^r r^{(s_0+i2^n)}$
$A = s,\ B,\ C$ — довільні	$r^s = g^B y^C$	$g^B y^C r^{-(jI2^n)}$	$r^{(s_0+i2^n)}$
$A = -s,\ B,\ C$ — довільні	$r^{-s} = g^B y^C$	$g^B y^C r^{(jI2^n)}$	$r^{-(s_0+i2^n)}$
$B = s,\ A,\ C$ — довільні	$r^A = g^s y^C$	$g^{(s_0+jI2^n)} y^C$	$r^A g^{-(i2^n)}$
$B = -s,\ A,\ C$ — довільні	$r^A = g^{-s} y^C$	$g^{-(s_0+jI2^n)} y^C$	$r^A g^{(i2^n)}$
$C = s,\ A,\ B$ — довільні	$r^A = g^B y^s$	$g^B y^{(s_0+jI2^n)}$	$r^A y^{i2^n}$
$C = -s,\ A,\ B$ — довільні	$r^A = g^B y^{-s}$	$g^B y^{-(s_0+jI2^n)}$	$r^A y^{i2^n}$
$A = rs,\ B = m,\ C = const = c$	$r^{rs} = g^m y^c$	$g^m y^c r^{-(rjI2^n)}$	$r^{r(s_0+i2^n)}$
$A = ms,\ B,\ C$ — довільні	$r^{ms} = g^B y^C$	$g^B y^C r^{-(mjI2^n)}$	$r^{m(s_0+i2^n)}$

Національний стандарт цифрового підпису ДСТУ 4145-2002 [7] описує схему цифрового підпису типу Ель-Гамаля на основі еліптичних кривих у формі Веєрштраса над полями F_{2^m} характеристики 2, що суттєво відрізняє його від алгоритмів ECDSA та EdDSA. Використовуються еліптичні криві у формі $y^2 + xy = x^3 + ax^2 + b$, де a, b є параметрами.

Деталі та нюанси арифметики еліптичних кривих над простими полями та полями характеристики 2 можна знайти, наприклад, у [8].

Наведемо необхідні для подальшого викладення відомості про схему ДСТУ 4145-2002.

1) цифровий підпис D має вид $D = (r \parallel s)$, де s, r – частини цифрового підпису;

2) головне співвідношення для перевірки підпису має вид $R = sP + rQ$, де Q – відкритий ключ (точка на еліптичній кривій), P – базова точка кривої, R – спеціально обчислена на основі підписаного повідомлення точка еліптичної кривої;

3) алгоритм перевіряння цифрового підпису складається з таких кроків:

а) відновити значення r та s з підпису D;

б) обчислити точку $R \coloneqq sP + rQ$, $R = (x_R, y_R)$;

в) обчислити елемент поля $y = hx_R$, де h є елементом поля, одержаним із геш-значення $H(M)$ повідомлення M, яке перевіряється;

г) перетворити елемент поля y у число r';

д) перевірити рівність $r \stackrel{?}{=} r'$.

Як і для класичної схеми Ель-Гамаля, будемо робити усічення частини s. Знову покладаємо $s = \mathrm{s}_0 + \mathrm{s}_1 2^n$, де $s_1 - t$-бітова частина, що відкидається. Підписом у такому випадку, буде $D = (r \parallel s_0)$.

Процедура перевіряння підпису ґрунтується на пошуку оригінального значення s_1; для цього необхідно перебудувати сам алгоритм перевіряння підпису.

Алгоритм 2: перевіряння усіченого підпису ДСТУ 4145-2002.

1. Відновити точки еліптичної кривої R з відомого значення r (алгоритм 3).
2. Застосувати модифікований алгоритм BSGS (алгоритм 4) для пошуку s_1.
3. Перевірити знайдені точки та кандидати у s_1 головним перевірочним співвідношенням. Підпис вважається правильним, якщо хоча б одне співвідношення виконалось.

Для відновлення точки R використовується такий алгоритм.

Алгоритм 3: відновлення точки еліптичної кривої R з відомого значення r

Вхід: – r: частина підпису за ДСТУ 4145-2002;
– a, b: параметри використаної еліптичної кривої;
– h: геш-значення вхідного повідомлення ($h = H(M)$).

Вихід: точки еліптичної кривої R та $-R$.

1. Обчислити $x_R = r \cdot h^{-1}$ у скінченному полі.
2. Розв'язати рівняння $y^2 + xy = x^3 + ax^2 + b$ зі значенням $x = x_R$ для одержання двох значень y_R. Дві пари (x_R, y_R) формують обидві точки R та $-R$.

Для пошуку кандидатів у скорочену частину підпису використовується такий алгоритм.

Алгоритм 4: знаходження значення s_1 для відновлення усіченого підпису у схемі ДСТУ 4145-2002.

Вхід: – r, s_0: частини усіченого підпису за ДСТУ 4145-2002;
– P, Q, R: базова точка кривої, відкритий ключ та відновлена точка R;
– t:довжина відкинутої частини підпису.

Вихід: відновлене значення s_1.

1. Встановити $I = 2^{t/2}, J = 2^{t/2-1}$.
2. Для j від 0 до $J - 1$ обчислити точки $U_j = s_0 P + jI(2^n P) + rQ$. Зберегти координати x обчислених точок.
3. Для i від 0 до $I - 1$ обчислити точки $V_i = R - i(2^n P)$. Зберегти координати x обчислених точок.
4. Шукаємо збіги між збереженими x-координатами точок U_j та V_i. Кожен збіг дає кандидата $s_1 = i + Ij$. Якщо збігів не виявлено, підпис вважається невірним.

Зауважимо, що $U_{j+1} = U_j + (I \cdot 2^n)P$ та $V_{i+1} = V_i - 2^n P$, отже, послідовності точок U та V можуть бути просто обчислені звичайним додаванням із передобчисленими точками.

Алгоритм 4 може знайти двох можливих кандидатів у s_1, якщо йому на вхід замість правильної точки R подати $(-R)$ – іншу точку, яка відповідає значенню r. Це можливо, оскільки перевіряючий не знає, яка саме точка з цих двох була використана під час генерування цифрового підпису. З іншого боку, для формування підпису використовується тільки x-координата точки R, яка збігається у R та $(-R)$. Втім, перевіряючий, якщо він має якісь сумніви, може перевірити головні співвідношення для кожної точки:

$$R = s_0 P + s_1(2^n)P + rQ, \qquad -R = s_0 P + s_1(2^n)P + rQ,$$

і якщо одне з них буде виконуватись, приймати підпис як вірний.

У таблиці 2 наведено оцінки ефективності запропонованого алгоритму відновлення усіченого підпису порівняно з повним перебором.

Таблиця 2

Порівняння кількості операцій алгоритмів відновлення усіченого цифрового підпису та повного перебору

t	Складність звичайного (повного) перебору s_1	Складність алгоритмів 1 та 4
8	$2^8 = 256$	$I + J = 24$
16	$2^{16} = 65536$	$I + J = 384$
24	$2^{24} = 16777216$	$I + J = 6144$
32	$2^{32} = 4294967296$	$I + J = 98304$

Запропоновані методи дозволяють ефективно реалізовувати усічення підписів типу Ель-Гамаля на певну кількість бітів (не дуже велику для класичної схеми Ель-Гамаля, але доволі суттєву для ДСТУ 4145-2002), але складність перевірки починає швидко зростати зі збільшенням частини підпису, що відкидається. Втім, для обраних меж довжини відкинутої частини t запропоновані алгоритми мають відносно ефективну реалізацію і тому можуть бути використані для зменшення довжини підписів у протоколах для малоресурсних пристроїв. Варто зауважити, що такий метод можна комбінувати із методом № 2 (фіксуванням частини r), але при цьому суттєво зросте навантаження на підписника, що може бути неприйнятним для певних випадків, і необхідно провадити ретельний аналіз ризиків безпеки, пов'язаних зі зниженням стійкості такого цифрового підпису.

Висновки. У роботі було запропоновано метод скорочення цифрового підпису для схем типу Ель-Гамаля. Були розглянуті класична схема Ель-Гамаля та її узагальнений багатопараметричний варіант. Також був запропонований метод усічення для цифрових підписів ДСТУ 4145-2002 з урахуванням особливостей арифметики еліптичних кривих, на якій ґрунтується цей стандарт. Запропоновані методи не змінюють процедуру постановки підпису; обчислений підпис скорочується шляхом відкидання певних бітів. Це дозволяє застосовувати запропоновані методи у реалізаціях криптографічних систем на малоресурсних пристроях, зокрема використовувати вже існуючі реалізації без змін. Для перевіряння усіченого підпису використовується відновлення на основі алгоритму великих та малих кроків, який дозволяє розв'язувати таку задачу із високою ефективністю.

Напрямками подальших досліджень є пошук границі для довжини усікання підпису, за якої підпис ще можна вважати практично стійким до відомих атак, а також пошук методів усікання інших типів цифрового підпису (наприклад, RSA).

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. L. Akhmetzyanova, E. Alekseev, A. Babueva, S. Smyshlyaev. On Methods of Shortening ElGamal-type Signatures. Cryptology ePrint Archive, Paper 2021/148. URL: https://eprint.iacr.org/2021/148.

2. Pornin T. Truncated EdDSA/ECDSA Signatures. Cryptology ePrint Archive, Paper 2022/938. URL: https://eprint.iacr.org/2022/938.

3. ElGamal T. A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms // IEEE transactions on information theory. 1985. Т. 31. № 4. P. 469–472.

4. Schneier B. Applied Cryptography: Protocols, Algorthms, and Source Code in C. 20th Anniversary Edition. John Wiley & Sons, 2015. 784 p. ISBN 978-1-119-09672-6.

5. FIPS PUB 186-5:2019. Standards Federal Information Processing. Digital Signature Standard (DSS). URL: https://doi.org/10.6028/NIST.FIPS.186-5.

6. Menezes A. J., Van Oorschot P. C., Vanstone S. A. Handbook of Applied Cryptography. CRC Press, 1996. 816 p. ISBN 0-8493-8523-7.

7. ДСТУ 4145-2002. Національний стандарт України. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевірка.

8. Chen L. et al. Recommendations for discrete logarithm-based cryptography: Elliptic curve domain parameters. 2023. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-186.pdf.