УДК 621.391:519.2 **DOI:10.30837/rt.2021.2.205.09**

Є.В. КОТУХ, канд. техн. наук, О.В. СЄВЄРІНОВ, канд. техн. наук,
А.В. ВЛАСОВ, канд. техн. наук, Л.С. КОЗІНА, А. О. ТЕНИЦЬКА, К.О. ЗАРУДНА

МЕТОДИ ПОБУДОВИ ТА ВЛАСТИВОСТІ ЛОГАРИФМІЧНИХ ПІДПИСІВ

Вступ

У статті запропонований огляд властивостей перспективного напряму розвитку криптографічних систем на основі логарифмічних підписів і покриттів кінцевих груп, який належить до постквантової криптографії. Актуальний стан цього напряму й праці останніх років дають підстави припускати, що завдання факторизації елемента кінцевої групи в теорії побудови криптосистем на основі неабелевих груп з використанням логарифмічних підписів є обчислювально складні, що потенційно забезпечує необхідний рівень криптографічного захисту перед атаками, що використовують можливості квантових обчислень. У роботі наведено основні визначення логарифмічних підписів і покриттів кінцевих груп, їх класифікацію, властивості. У рамках аналізу підходів розглянуто практичні випадки використання властивостей логарифмічних підписів для забезпечення криптостійкості базових платформ для побудови криптосистем MST3.

Разом зі зростанням практичних можливостей використання квантових обчислень зростає загроза класичним схемам шифрування та електронного підпису, які використовують як основу класичні математичні проблеми, що долаються обчислювальними можливостями квантових комп'ютерів. Цей факт мотивує дослідження фундаментальних теорем, що стосуються математичних та обчислювальних аспектів постквантових криптосистем-кандидатів. У роботі представлено логарифмічні підписи як особливий тип факторизації в кінцевих групах, розглянуто їх властивості та методи побудови.

Нехай G – кінцева група. Логарифмічний підпис α для групи G є послідовністю підмножин $A_i \subseteq G$ виду $\alpha = [A_1, \ \dots, \ A_s]$, таких, що для кожного елемента g групи G є лише одна факторизація $(*)$ $g = a_q \cdot a_2 \cdot \ \dots \ \cdot a_s$, де $a_i \in A_i$ для $i = 1, \dots, s$. Множини A_i називають блоками. Розмір списку блоків позначають через $r_i := |A_i|$. Для спрощення ми називаємо елементи $A_i \cup \ \dots \ \cup A_s$ елементами логарифмічного підпису α . За певних умов ми розглядаємо впорядкування елементів блоку, тоді для $k_i = 0, \dots, r_i - 1$ позначаємо через a_{ik_i} кожний $(k_i + 1)$-й елемент блоку A_i. Вектор $(r_1, \dots, r_s)$ називають типом α, а

$$\ell(\alpha) = \sum_{i=1}^{s} r_i -$$

довжиною логарифмічного підпису. Множину логарифмічних підписів групи позначають через $\Lambda(G)$. Із визначення одержуємо певні властивості логарифмічних підписів. Через одноманітність факторизації (*) маємо $\prod_{i=1}^{s} r_i = |G|$, і тоді r_i ділить $|G|$ для всіх i. Це також показує, чому зазначені послідовності називають логарифмічними підписами. Логарифмічна функція перетворює добуток на суму, логарифмічні підписи скорочено відображають усі елементи групи довжини $r_1 \ + \ \dots \ + \ r_s$, де група містить у собі $r_1 \cdot \ \dots \ \cdot \ r_s$ елементів.

Якщо $e_G \in A_1 \cap \dots \ \cap A_s$, тоді ми можемо стверджувати, що α є нормалізованою. З огляду на одиничність факторизації ми навіть маємо $\bigcap_{i=1}^{s} A_i = \{e_G\}$ для нормалізованих логарифмічних підписів із більше ніж одним блоком. Легко помітити, що в абелевих $|A_i \cap A_j| \leq 1$ для $i \neq j$. У [1] доведено, що для $|G| = \prod_{j=1}^{t} p_j^{b_j}$ (p_j – просте число) є нижня границя довжини для будь-якого логарифмічного підпису групи G, одержаного таким чином:

$$\ell(\alpha) \geq \sum_{j=1}^{t} b_j \cdot p_j.$$

Логарифмічний підпис α називають мінімальним, якщо $\ell(\alpha)$ досягає нижньої границі, тобто кожен блок має простий ступінь або ступінь 4. У кількох статтях порушене питання існування мінімальних логарифмічних підписів у кінцевих полях [1, 2]. Було запропоновано мінімальні логарифмічні підписи для всіх кінцевих груп.

Приклад 1. Нехай $n \in \mathbb{N}$. Для циклічної групи $(\mathbb{Z}_{2^n}, +)$ послідовність виду $\alpha = \left[[0, 2^{n-1}], [0, 2^{n-2}], \ \ldots\ , \ [0,2], [0,1]\right]$ є нормалізованим логарифмічним підписом типу $(2, \ \ldots\ , 2)$. Обчислення факторизації елемента еквівалентне обчисленню його двійкового відображення, зокрема, якщо $n = 4$, $9 = 1001$ має факторизацію $2^3 + 0 + +0 + 2^0$.

Розглянемо можливість обчислення факторизації елемента групи для зазначеного логарифмічного підпису й певного елемента групи. Для прикладу, атака повним перебором за допомогою пошуку всіх можливих факторизацій, репрезентованих логарифмічним підписом $\alpha = [A_1, \ \ldots, \ A_s]$ групи G, становить $|G| \times (s-1)$ групових операцій у найгіршому випадку. Такий перебір знаходить правильну факторизацію для будь-якого логарифмічного підпису, але загалом неможливий. Приклад 1 показує, що для певних логарифмічних підписів легко обчислити факторизації. Для практичного використання в криптосистемах MST необхідно визначити логарифмічні підписи, для яких факторизація є обчислювально нездійсненною, а також підписи, для яких є ефективні алгоритми розкладання. Здебільшого, терміни «прості» й «складні» логарифмічні підписи вживають для позначення різниці між логарифмічними підписами, для яких відповідно обчислювально легко та складно одержати факторизації [3, 4]. Факторизація одного логарифмічного підпису становить постійний час, але коли ми вивчаємо питання ефективності обчислень для логарифмічних підписів, то розглядаємо сімейство (G_n, α_n) логарифмічних підписів $\alpha_n = \left[A_1^n, \ \ldots, \ A_{s_n}^n\right]$ груп G_n для $n \in \mathbb{N}$. Далі ми припускаємо, що $|G_n| \leq |G_{n+1}|$ і $\alpha_n \neq \alpha_m$ для $n \neq m$. Крім того, нехай одноманітний опис елементів G_n є таким, що $|g|_2 = \mu$ для всіх $g \in G_n$. Зауважуємо, що дає $\mu_n \geq log|G_n|$ для всіх $n \in \mathbb{N}$.

Робимо одне базове припущення: для зазначеного сімейства $(G_n, \ \alpha_n)$ є детермінований алгоритм поліноміального часу A, такий, що, маючи вхідні значення $(a_1, \ \ldots, \ a_{s_n})$ із $A_1^n \times \ \ldots \ \times A_{s_n}^n$, обчислює добуток $a_1 \cdot \ \ldots \ \cdot a_{s_n}$. Ми ідентифікуємо A з ін'єктованою функцією, що його обчислює.

Визначення 1. Для $n \in \mathbb{N}$ нехай α_n буде як у наведеному прикладі. Тоді сімейство $(G_n, \ \alpha_n)_{n \in \mathbb{N}}$ називають складним, якщо для кожного ймовірного алгоритму поліноміального часу A' для кожного позитивного полінома p і всіх істотно великих n маємо

$$pr\big(A'(g_n, \alpha_n) = A^{-1}(g_n)\big) < \frac{1}{p(\lceil log|G_n| \rceil)},$$

де g_n позначає випадковий елемент, одноманітно вибраний із G_n.

Для сімейства складних логарифмічних підписів $(G_n, \alpha_n)_{n \in \mathbb{N}}$ функція A визначає односторонню функцію, як зазначено в [5]. Серед логарифмічних підписів, що не є складними, ми визначаємо ті, які мають ефективні факторизації для всіх елементів групи.

Визначення 2. Для $n \in \mathbb{N}$ нехай a_n буде логарифмічним підписом групи G_n. Сімейство $(G_n, \alpha_n)_{n \in \mathbb{N}}$ називають простим, якщо є алгоритм A'', що, одержуючи на вході елементи $g_n \in G_n$ і α_n, обчислює факторизацію g_n щодо α_n за поліноміальний час.

Різницю між «нескладний» і «простий» уперше розглянуто в [6], і, на відміну від попередніх визначень (у яких ці два поняття еквівалентні), визначення є більш точним. Логарифмічний підпис, що не є ні простим, ні складним, може бути таким, для якого ми можемо ефективно знайти факторизацію для рівно половини групових елементів. Є алгоритм із заданими g і α_n, що випадково вгадує факторизацію з імовірністю $\frac{1}{|G_n|}$. Отже, алгоритм A' у другому

визначенні дає значно більший шанс знайти факторизацію, як і раніше менший, ніж $\frac{1}{p(\lceil log|G_n| \rceil)}$ (для будь-якого p). Алгоритм A' додатково одержує n на вхід для кодування групи G_n, такий, що A' обчислює G_n. Але твердження, що, маючи α_n на вході, гарантовано A' обчислює групу G_n, є не підтвердженими. Також припустимо, що для вхідних даних $(a_1, \ \dots, a_{s_n})$ алгоритм A знає, яку групову операцію застосовувати. Обчислення добутку елементів s_n, кожний із яких був випадково одноманітно вибраним із різних блоків a_n (щодо A), еквівалентне вибору випадкового елемента з G_n.

Відзначимо, що питання наявності варіантів для складних логарифмічних підписів залишається відкритим. Усі логарифмічні підписи, описані в літературі, репрезентовані простими [1 – 4, 7]. Криптосистеми MST використовують як складні, так і прості логарифмічні підписи для побудови криптосистем відкритого ключа. Криптосистема MST_1 ґрунтується на складних логарифмічних підписах; MST_3, у свою чергу, використовує прості логарифмічні підписи в елементарних абелевих 2-групах. Отже, нас цікавить структура простих логарифмічних підписів, а також груп, для яких можуть існувати логарифмічні підписи. Для подальшого аналізу груп важливими є три параметри. Для $n \in \mathbb{N}$ логарифмічний підпис $\alpha_n = [A_1^n, \ \dots, \ A_{s_n}^n]$ повністю описаний як

$$|\alpha_n| = \sum_{i=1}^{s} |A_i^n|$$

елементів із групи G_n. Можливо, є коротше репрезентування певних логарифмічних підписів, але загалом нам необхідний

$$\sum_{i=1}^{s} |A_i^n| \cdot \mu_n$$

біт, щоб виразити логарифмічний підпис, у якому елемент G_n репрезентований за допомогою μ_n біт. Нехай

$$r_n := max\{|A_i^n|, \ \dots, |A_{s_n}^n|\}.$$

Алгоритм факторизації A' у другому визначенні бере як вхідні дані елемент G_n і логарифмічний підпис α_n для певних $n \in \mathbb{N}$. Довжина цих вхідних даних дорівнює не більше за $(s_n \cdot r_n + 1) \cdot \mu_n$ біт.

Отже, ми пропонуємо використовувати три таких значення $(s_n, \ r_n, \ \mu_n)$ як параметри вимірювання ефективності алгоритму факторизації для α_n. Зазначимо, що ми одержуємо перші два параметри зі структури α_n, а третій параметр є незалежним від α_n та обумовлений лише репрезентуванням елементів G_n.

Зауваження . Для $n \in \mathbb{N}$ нехай (α_n) буде логарифмічним підписом у G_n. Якщо для всіх $g \in G_n$ факторизацію щодо α_n можна одержати за поліноміальний час із трьома параметрами s_n, r_n, μ_n, тоді сімейство $(\alpha_n)_n$ є простим.

Приклад 2. Візьмемо сімейство логарифмічних підписів у групі $G_n = \mathbb{Z}_{2^n}$ із прикладу 1. Три параметри ефективності дорівнюватимуть $s_n = n, r_n = 2, \mu_n = n$. Для заданого елемента $g \in \mathbb{Z}_{2^n}$ за допомогою його двійкового представлення $(g_1, \dots, \ g_n)$, де $g_i \in \{0,1\}$ – його факторизація, яка щодо α дорівнює $(g_1 \cdot 2^{n-1}, \dots, g_n \cdot 1)$, що одержано за допомогою не більше ніж n множень. Отже, маємо лінійний час у n. Тоді $(\alpha_n)_{n \in \mathbb{N}}$ є простою.

Перетворення логарифмічних підписів

Розглянемо певні перетворення логарифмічних підписів, зокрема такі, щоб факторизація щодо вихідного логарифмічного підпису була однаково ефективною щодо перетвореного логарифмічного підпису. Ідея полягає в тому, що алгоритм факторизації одного логарифмічного підпису в певному наборі дає алгоритм факторизації для всіх логарифмічних підписів цього набору. Наведемо стандартний підхід до класифікації логарифмічних підписів відповідно до структури блоків. Ми розглядаємо п’ять перетворень логарифмічних підписів, що не

змінюють властивостей належності до простих або складних логарифмічних підписів. Нехай $\alpha = [A_1, \dots, A_s]$ буде логарифмічним підписом групи G. Ми маємо справу з перетвореннями блоків $A_1, \dots,\ A_s$ логарифмічного підпису α на блоки $B_1, \dots, B_s$, які є результуючою послідовністю $\beta = [B_1, \dots, B_s]$ і також репрезентують логарифмічний підпис G.

Перетворення 1. Нехай φ буде автоморфізмом G і $B_i = \varphi(A_i)$ для $i = 1, \dots, s$. Тоді β також є логарифмічним підписом. І якщо $a_1 \cdot a_2 \cdot \ \dots \ \cdot a_3$ є факторизацією елементів $g \in G$, $\varphi(a_1) \cdot \varphi(a_2) \cdot \ \dots \ \cdot \varphi(a_s)$ є факторизацією $\varphi(g)$ щодо β.

Перетворення 2. Нехай $g_0, \dots, g_s$ будуть елементами групи G і $B_i = g_{i-1}^{-1} A_i g_i$ для $i = 1, \dots, s$. Тоді послідовність β також є логарифмічним підписом G, що називають трансляцією α. Якщо $g_0 = g_s = e_G$, β – сендвіч α. Зазначимо, що, якщо $a_1 \cdot a_2 \cdot \ \dots \ \cdot a_s$ є факторизацією елементів $g \in G$, $g_0^{-1} a_1 g_1 \cdot \ \dots \ \cdot g_{s-1}^{-1} a_s g_s$ є факторизацією $g_0^{-1} g g_s$ щодо β.
Необхідно пам'ятати, що в абелевих групах блоки трансляції β від α мають вигляд $B_i = A_i + h_i$ для елементів $h_1, \dots,\ h_s$ групи G, а отже будь-яка факторизація елемента $g \in G$ щодо α миттєво дає факторизацію $g + \sum_{i=1}^{s} h_i$ щодо β.

Перетворення 3. Для $i = 1, \dots, s$ нехай π_i буде перестановкою в S_{r_i} і $B_i = \left[a_{i\pi_i(1)}, \dots, a_{i\pi_i(r_i)}\right]$ для $j = 1, \dots, r_i$, тобто елементи блоку B_i – перестановка елементів блоку A_i. Тоді β також є логарифмічним підписом. І, якщо $a_{1k_1} \cdot a_{2k_2} \cdot \ \dots \ \cdot a_{sk_s}$ – факторизація елемента $g \in G$, $a_{1\pi_1(k_1)} \cdot a_{2\pi_2(k_2)} \cdot \ \dots \ \cdot a_{s\pi_s(k_s)}$ – факторизація g щодо β.

Перетворення 4. Тепер нехай G буде абелевою групою, π – перестановкою в S_s і $B_i = A_{\pi(i)}$, тобто $b_{ij} = a_{\pi(i)_j}$. Тоді послідовність β є логарифмічним підписом групи G. Її також називають перетворенням блочної перестановки α. Зазначимо, що якщо $a_{1i_1} + a_{2i_2} + \ \dots \ + a_{si_s}$ є факторизацією елемента $g \in G$ щодо α, $a_{\pi(1)(i_1)} \cdot a_{\pi(2)(i_2)} \cdot \ \dots \ \cdot a_{\pi(s)(i_s)}$ є факторизацією g щодо β. Крім того в неабелевих групах β може не бути логарифмічним підписом.

Перетворення 5. Для певних $j \in \{1, \dots, s-1\}$ нехай $B_j = A_j \cdot A_{j+1} = \left[x \cdot y | x \in A_j, y \in A_{j+1}\right]$ та $B_i = A_i$ для $i = 1, \dots, s-1$ і $i \neq j, j+1$. Послідовність $\beta = \left[B_1, \dots, B_{s-1}\right]$ є логарифмічним підписом, одержаним з α в результаті перетворення – злиття двох блоків. І, якщо $a_1 \cdot a_2 \cdot \ \dots \ \cdot a_s$ є факторизацією $g \in G$ щодо α, $a_1 \cdot \ a_{j-1} \cdot \ a \cdot a_{j+2} \dots \cdot a_s$, де $a = a_j \cdot a_{j+1}$, є факторизацією g щодо β. Зворотну операцію називають перетворенням розподілу. Для кожного з п'яти наведених перетворень ми описали, як факторизація елемента щодо логарифмічного підпису негайно приводить до факторизації щодо перетвореного логарифмічного підпису. Якщо ми розглядаємо ці перетворення для родин логарифмічних підписів (α_n), то легко помітити, що перемикання між алгоритмами факторизації (α_n) і перетвореннями (α_n) виконується за поліноміальний час, якщо перетворення є відомим або ефективно обчислюваним. Це справедливо й для нормалізації.

Визначення 3. Нехай (α_n) і (β_n) є родинами логарифмічних підписів для груп G_n з параметрами r_n, s_n, μ_n для (α_n). Тоді ми стверджуємо, що (α_n) перетворюється на (β_n), якщо (β_n) можна обчислити з (α_n) за допомогою перетворень 1 – 5 за поліноміальний час для r_n, s_n, μ_n. Зазначимо, що в такому разі кількість перетворень між (α_n) і (β_n) є кінцевою. $T -$ множина (α_n), визначена як $T(\alpha_n) = \{(\beta_n) | \beta_n\ \Lambda\ (G_n)$ і α_n перетвориться для всіх $n\}$.

Приклад 3. Візьмемо логарифмічний підпис $\alpha_n = \left[[0, 2^{n-1}], \dots, [0,2], [0,1]\right]$ групи $\mathbb{Z}_{2^n}$ із прикладу 1. Для $n > 4$ нехай

$$\beta_n = \left[[1,\ 5], [0,\ 1,\ 2,\ 3], [0,\ 8], [0,\ 16], \dots, [0, 2^{n-1}]\right]$$

І $\gamma_n = \left[\left[0,\ 1, 2, 3, \dots, \ 2^n - 1\right]\right]$. Тоді $(\beta_n) \in T(\alpha_n)$ і $(\gamma_n) \notin T(\alpha_n)$.

Визначення 4. Нехай $g_0 = 1$ і $g_i = \left(\prod_{j=1}^{i} a_{j1}\right)^{-1}$ для $i = 1, \ldots, s$. За допомогою трансляції α в $g_0, \ldots, g_s$ ми одержуємо логарифмічний підпис β, у якому

$$b_{i1} = g_{i-1}^{-1} a_{i1} g_i = \left(\left(\prod_{j=1}^{i-1} a_{j1}\right)^{-1}\right)^{-1} a_{i1} \left(\prod_{j=1}^{i} a_{j1}\right)^{-1} = \left(\prod_{j=1}^{i} a_{j1}\right) \cdot \left(\prod_{j=1}^{i} a_{j1}\right)^{-1} = 1,$$

тобто перший елемент у кожному блоці є нейтральним. Ми вважаємо β нормалізацією α.

В абелевих групах ми можемо нормалізувати логарифмічний підпис, застосовуючи трансляцію $B_i = A_i - a_{i1}$. Тоді перший елемент кожного блоку дорівнюватиме $a_{i1} - a_{i1} = 0$.

Інші класи мають стандартне позначення. Нехай G буде кінцевою групою. Ми називаємо точно-поперечним логарифмічний підпис $\alpha \in \Lambda(G)$, якщо такий ланцюг підгруп виду

$$e_G = G_0 < G_1 < \ldots < G_{s-1} < G_s = G,$$

якщо A_i є поперечною групи G_{i-1} у G_i, тобто $G_{i-1}A_i = G_i$ та $|G_{i-1}||A_i| = |G_i|$. Зазначимо, що блок $A_1 = G_1$ є підгрупою G. Відповідний клас позначають через ε. Якщо α є сендвічем точно поперечної логарифмічної групи, α називають поперечною. Клас поперечних логарифмічних підписів позначимо через T_{LS}.

Усі інші логарифмічні підписи належать до NT_{LS} – класу не поперечних логарифмічних підписів. Ми описуємо два підкласи NT_{LS}. Якщо жодний із блоків не є підмножиною (нетривіальною) підгрупи G, логарифмічний підпис є елементом TNT_{LS} – класу абсолютно непоперечних логарифмічних підписів. Клас TA_{LS} повністю аперіодичних логарифмічних підписів містить усі логарифмічні підписи, що не мають навіть періодичного блоку, тобто об'єднані підмножиною G. Отже, маємо $TA_{LS} \subseteq TNT_{LS} \subseteq NT_{LS}$ і $\varepsilon \subseteq T_{LS}$.

Необхідно пам'ятати, що властивість простоти для точно поперечних логарифмічних підписів породжується в певних групах.

Визначення 5. Нехай (α_n) – сімейство точних логарифмічних підписів, а тестування на належність підгрупи до групи G_n проведено за поліноміальний час μ_n. Тоді (α_n) є простим.

Для простішого читання опустимо індекс n. Нехай

$$e_G = G_0 < G_1 < \ldots < G_{s-1} < G_s = G$$

буде ланцюгом підгруп відповідних логарифмічних підписів $\alpha = [A_1, \ldots, A_s]$. Нехай $g \in G$. Є саме одна факторизація g і вона містить $a_1, \ldots, a_s$, де

$$g \cdot a_s^{-1} \cdot \ldots \cdot a_{k+1}^{-1} = a_1 \cdot \ldots \cdot a_k \in G_k$$

для $k = 1, \ldots, s-1$ та $a_1 \cdot \ldots \cdot a_s = g$. Наступний простий алгоритм знаходить факторизацію g щодо α. Алгоритм є детермінованим. Буде потрібно $O(r_n \cdot s_n)$ раундів, у кожному з яких необхідні одне множення, одне звернення й одне тестування на належність до підгрупи, виконувані за поліноміальний час μ_n, s_n, r_n. Крім того, зрозуміло, якщо μ_n, s_n, r_n є поліноміальними в $\lceil log|G_n| \rceil$ та (α_n) є простим сімейством нормалізованих точно поперечних логарифмічних підписів, тоді існує ефективний тест на належність до підгрупи для всіх підгруп G_i групи G_n: $g \in G_i$, лише якщо у факторизації $g = a_1 \cdot \ldots \cdot a_s$ одержуємо результат $a_{i+1} = \ldots = a_s = e_G$.

Можливо, непоперечні й навіть абсолютно непоперечні логарифмічні підписи є гарними варіантами, щоб бути складними. Проте, в [8] було доведено, що досить легко побудувати прості сімейства логарифмічних підписів для симетричних груп, що чергуються, які належать до класу TNT_{LS}. Отже, класи не мають критеріїв, щоб розрізняти прості й складні логарифмічні підписи.

Якщо немає ефективного тесту на належність до підгрупи для груп G_n, у цих групах також будуть складні логарифмічні підписи, що є поперечними. Очевидно, що для груп, для яких є ефективний тест на належність до підгрупи, точно поперечні логарифмічні підписи є простими. Для формалізації цього зауваження використовуємо наступне визначення.

Визначення 6. Для $n \in \mathbb{N}$ нехай P_n буде булевим предикатом, що можна застосовувати до будь-якого логарифмічного підпису групи G_n. Ми стверджуємо, що P є властивістю, яка породжує простоту для G_n, якщо всі сімейства $(\alpha_n)_{n\in\mathbb{N}}$ логарифмічних підписів (G_n), для яких правильне твердження: $P(\alpha_n)$ правдиве для всіх $n \in \mathbb{N}$, де n є простим.

Приклад 4. Переглянемо знову приклад 1. Для $n \in \mathbb{N}$ нехай P_n =«кожним блоком форми $[0, 2^i]$ для $0 \leq i \leq n''$». Тоді ми стверджуємо в прикладі 4, що P є властивістю породження простоти для $\mathbb{Z}_{2^n}$.

У групах, для яких є ефективний тест на належність до підгрупи, належність до поперечних логарифмічних підписів також є властивістю породження простоти.

Висновки

Криптосистеми MST використовують як складні, так і прості логарифмічні підписи для побудови криптосистем відкритого ключа. Криптосистема MST_3 використовує прості логарифмічні підписи в елементарних абелевих 2-групах. Цікавою задачею є дослідження всіх неабелевих груп з великим порядком в їх функціональних полях та структури простих логарифмічних підписів які можуть бути використані в таких групах. З огляду на результати конкурсів з побудови постквантовых криптосистем важливою задачею є квантовий криптоаналіз реалізацій криптосистем MST_3 та пошук вразливостей повязаних з побудовою логарифмічних підписів та груп, що використовуються у якості платформ для криптосистем.

Список літератури:

1. Gonzáles Vasco M. I. On minimal length factorizations of _nite groups / M. I. Gonzáles Vasco, M. Rotteler, R. Steinwandt // Experimental Mathematics. 2003. Vol. 12 (1). P. 1–12.
2. Singhi N. Minimal logarithmic signatures for _nite groups of Lie type / N. Singhi, N. Singhi, S. Magliveras // Designs, Codes and Cryptography. 2010. Vol. 55 (2). P. 243–260.
3. Magliveras S. New approaches to designing public key cryptosystems using one-way functions and trap-doors in nite groups / S. Magliveras, D. Stinson, T. van Trung // Journal of Cryptology. 2002. Vol. 15. P. 285–297.
4. Lempken W. A public key cryptosystem based on non-abelian _nite groups / W. Lempken, T. van Trung, S.S. Magliveras, W. Wei // Journal of Cryptology. 2009. Vol. 22 (1). P. 62–74.
5. Goldreich O. Foundations of Cryptography: Basic Tools / O. Goldreich // Cambridge University Press. 2001.
6. Nuss A. On group based public key cryptography [Electronic resource] : Phd thesis. Access mode : http://nbn-resolving.de/urn:nbn:de:bsz:21-opus-63659.
7. Blackburn S. R. Cryptanalysis of the MST 3 public key cryptosystem / S. R. Blackburn, C. Cid, C. Mullan // Journal of Mathematical Cryptology. 2009. Vol. 3 (4). P. 321–338.
8. Bohli J. Weak keys in MST / J. Bohli, M. I. Gonzáles Vasco, C. J. M. Martínez, R. Steinwandt // Designs, Codes and Cryptography. 2005. Vol. 37 (3). P. 509–524.
9. Caranti A. The round functions of cryptosystem PGM generate the symmetric group / A. Caranti, F. D. Volta // Designs, Codes and Cryptography. 2006. Vol. 38 (1). P. 147–155.
10. Magliveras S. Algebraic Properties of Cryptosystem PGM / S. Magliveras, N. D. Memon // Journal of Cryptology. 1992. Vol. 5 (3). P. 167–183.
11. Khalimov G. MST_3 Cryptosystem Based on a Generalized Suzuki 2-Groups [Electronic resource] / G. Khalimov, Y. Kotukh, S. Khalimova. Access mode : http://ceur-ws.org/Vol-2711/paper1.pdf
12. Khalimov G., Kotukh Y., Khalimova S. MST3 cryptosystem based on the automorphism group of the hermitian function field' // IEEE International Scientific-Practical Conference: Problems of Infocommunications Science and Technology, PIC S and T 2019 – Proceedings, 2019, pp. 865 – 868.
13. Khalimov G., Kotukh Y., Khalimova S. Encryption scheme based on the automorphism group of the Ree function field // 2020 7th International Conference on Internet of Things: Systems, Management and Security, IOTSMS 2020, 2020, 9340192.

Надійшла до редколегії 03.03.2021

Відомості про авторів:

Котух Євген Володимирович – канд. техн. наук, доцент, кафедра комп'ютерних наук, Сумський державний університет, Україна, e-mail: yevgenkotukh@gmail.com

Сєвєрінов Олександр Васильович – канд. техн. наук, доцент, доцент кафедри Безпеки інформаційних технологій, Харківський національний університет радіоелектроніки, Харків, Україна, e-mail: oleksandr.sievierinov@nure.ua

Власов Андрій Володимирович – канд. техн. наук, ст. дослідник, ст. викладач кафедри Безпеки інформаційних технологій, Харківський національний університет радіоелектроніки, Харків, Україна, e-mail: andrii.vlasov@nure.ua

Козіна Лідія Сергіївна – аспірантка, кафедра інформаційних технологій та програмної інженерії НУ «Чернігівська Політехника»

Теницька Альона Олексіївна – студентка, факультет Електроніки та інформаційних технологій, Сумський державний університет, Суми, Україна, e-mail: tenickajaalena@gmail.com

Зарудна Катерина Олександрівна – студентка, факультет електроніки та інформаційних технологій, Сумський державний університет, Суми, Україна, e-mail: zarudnayakatyaa@gmail.com