УДК 621.391:519.2 **DOI:10.30837/rt.2021.3.206.09**

Є.В. КОТУХ, канд. техн. наук, Т.О. ОХРІМЕНКО, канд. техн. наук,
О.Ф. ДЯЧЕНКО, канд. пед. наук, Н.Ю. РОТАНЬОВА, канд. пед. наук,
Л.С. КОЗІНА, Д.В. ЗЕЛЕНСЬКИЙ

КРИПТОАНАЛІЗ СИСТЕМ НА ОСНОВІ ПРОБЛЕМИ СЛОВА З ВИКОРИСТАННЯМ ЛОГАРИФМІЧНИХ ПІДПИСІВ

Стрімкий розвиток та досягнення у сфері квантових комп'ютерів сприяє розвитку криптосистем з відкритим ключем на основі математично складних або важко вирішуваних задач, адже загроза використання квантових алгоритмів для зламу сучасних традиційних криптосистем стає набагато реальнішою з кожним днем. Варто зазначити, що класичні математично складні проблеми факторизації цілих чисел та дискретних логарифмів більш не вважаються складними для квантових обчислень [1]. Десятки криптосистем були розглянуті та запропоновані з різних складних проблем теорії груп у 2000 -х роках [2 - 11].Одною з таких складних проблем є проблема слова [1]. Одна з перших реалізацій криптосистеми на основі проблеми слова була запропонована Магліверасом [5] з використанням логарифмічних підписів для кінцевих груп перестановок та надалі запропонована Лемпкеном та ін. для асиметричної криптографії з випадковими покриттями [2]. Новаторство цієї ідеї полягає у поширенні важко вирішуваної проблеми слова на велику кількість груп. Перша реалізація такої криптосистеми була запропонована для групи Сузукі під назвою MST_3. Кілька поліпшень MST_3 з групою Сузукі були зроблені в [12 - 13]. У 2010 р. Сваба та ін. [12] проаналізували всі опубліковані посилання на атаки на криптографію MST_3 та створили більш безпечну криптосистему $eMST_3$, додавши секретне гомоморфне покриття. У 2018 р. Т. ван Транг [14] запропонував загальний метод побудови сильних апериодичних логарифмічних сигнатур для абелевих р-груп, що є подальшим внеском у практичне застосування криптосистем MST_3.

У статті узагальнимо відомі результати криптоаналізу базових конструкцій криптосистеми MST_3 та визначимо рекомендації для напрямків покращення криптографічних властивостей конструкцій MST_3 та використання некомутативних груп у якості базових конструкцій.

Аналіз безпеки базової конструкції

У цьому розділі розглянуто попередні роботи, що присвячені безпеці MST_3, та зроблено деякі елементарні висновки щодо безпеки базової конструкції системи. Надалі для простоти будемо називати базову конструкцію платформою.

У [8] автори MST_3 дають стислий огляд безпеки схеми та дають атаку на криптосистему в пасивній моделі супротивника зі складністю приблизно q^2, коли використовуються Сузукі 2-групи, де $q = |Z| = |G/Z|$ (зауважимо, що q є експоненціальним параметром безпеки, тому атаки, які є поліноміальними за q, насправді мають експоненціальну складність). В роботі накладається додаткова умова на α, коли 2-групи Сузукі використовують як платформу для MST_3, а саме, що не повинно бути двох елементів набору A_i в одному класі суміжності Z. Оскільки ця умова виконується для переважної кількості ключів – ігноруємо її заради простоти.

Магліверас та співавтори [5] забезпечують кращу атаку складності $O(q)$. Вони стверджують, що їх атака застосовувана для платформи Сузукі 2-групи, але насправді їх атака працює для будь-якої платформи. В цій роботі автори далі показують, що MST_3 небезпечно, якщо β – це канонічний логарифмічний підпис (насправді їх атака не працює в цікавому окремому випадку, коли $d_i = 1$ для усіх i, так як їм потрібно, щоб сума векторів в підпросторі дорівнювала нулю, криптоаналіз покриває цей окремий випадок). Зауважимо, що можна запобігти атаці в [5]: або шляхом вибору $d_i = 1$ для усіх i, або створенням зведеного поперечного логарифмічного підпису (ATLS), який навряд чи буде канонічним. В попередній роботі автори давали визначення типів та особливостей генерації логарифмічних підписів. Автори MST_3 припускають [9], що випадково обране накриття α в кінцевій групі буде (з переважною ймовірністю) індукувати однобічну функцію $\breve{\alpha}$.

Це розумне припущення, але автори стверджують, що це припущення фактично не потрібне для встановлення безпеки MST_3 (в пасивній моделі). Гонсалес Васко та автори [3] дають переконливі докази того, що це останнє твердження невірне, показуючи, що коли α не індукує однобічну функцію, MST_3 небезпечна, якщо частка $|Z|/|J|$ є більшою. Потім вони наводять експериментальні докази того, що $|Z|/|J|$ – зазвичай доволі мала. В роботі показано, що рандомізована версія MST_3 небезпечна в сенсі нерозрізненості навіть для пасивних супротивників. Проблема генерації β глибоко не обговорюється в роботі [4], але припустимо, що β буде побудована як ATLS. Це найзагальніший з відомих, практичний метод для генерації слабких логарифмічних підписів для Z. Неперіодичні покриття типу (r_1, r_2) є надто ресурсномісткими з точки зору зберігання. Більш того, незрозумілими з огляду на безпеку є результати розкладання неперіодичного розбиття на логарифмічний підпис типу $(r_1, ..., r_s)$ для $s > 2$. Знову з міркувань зберігання кількість операцій злиття в конструкції ATLS має бути невеликою: об'єднання збільшує кількість елементів, які повинно бути збережено $|E_i||E_j| - (|E_i| + |E_j|)$ та тому невибіркове використання об'єднання може привести до експоненціальної вимоги до зберігання. З точки зору ефективності генерації ATLS типу $(2, 2, ..., 2)$ дуже приваблива. Однак це означає, що неможливо використовувати об'єднання для їх створення.

Попередні дослідження залишають відкритим питання про те, чи безпечно MST_3 на практиці, якщо запобігти канонічних поперечних логарифмічних підписів при генерації часткового ключа. Далі покажемо практичний криптоаналіз криптосистеми MST_3 в тому числі коли часткові ключі генеруються з використанням методу ATLS.

Звертаємо увагу, що хоча секретний ключ складається з простого логарифмічного підпису β та $s+1$ випадково генеровані елементи $\{t_0, ..., t_s\}$, $s-1$ елементи $t_1, ..., t_{s-1}$ насправді не потрібні: тільки β та t_0, t_s використовуються для дешифрування.

Зазначимо, що будь-який триплет форми $(\beta, g \cdot t_0, g \cdot t_s)$, де g є централізатором J (у тому числі, якщо $g \in Z$), може бути використаний для дешифрування шифртексту. Таким чином, існує багато еквівалентних секретних ключів. Задача криптоаналізу може бути спрощена при розгляді значно меншого класу відкритих та закритих ключів, чим у вихідному ви-

значенні. Це спрощення працює для усіх відповідних груп платформ, а не тільки для розглянутих вище Сузукі 2-груп.

Нехай (α,γ) буде відкритим ключем для MST_3 с $(\beta,(t_0,t_1,...,t_s))$ – відповідним секретним ключем. Запам'ятаємо, що $\alpha=[A_1,A_2,...,A_s]$ и $\beta=[B_1,B_2,...,B_s]$ та визначимо підмножини H_i через $\gamma=[H_1,H_2,...,H_s]$. Зазначимо, що алгоритм для отримання γ із закритого ключа передбачає, що $\gamma_{ij}=\beta_{ij}t_{i-1}^{-1}\alpha_{ij}t_i$. Визначимо елементи p_i,q_i та z_i через призначення $p_0=q_0=z_0=1$ та для $i\in\{1,2,...,s\}$ визначимо $p_i=\prod_{k=1}^{i}\alpha_{k1}, q_i=\prod_{k=1}^{i}\gamma_{k1}, z_i=\prod_{k=1}^{i}\beta_{k1}$.

Зауважимо, що факт того, що елементи β_{ij} знаходяться в центрі, передбачає, що

$$q_i=\prod_{k=1}^{i}\left(\beta_{k1}t_{k-1}^{-1}a_{k1}t_k\right)=z_it_0^{-1}p_it_i.$$

Визначимо $\alpha'=[A_1',A_2',...,A_s'],\gamma'=[H_1',H_2',...,H_s'],\beta'=[B_1',B_2',...,B_s']$ через

$$A_i'=p_{i-1}A_ip_i^{-1},$$
$$H_i'=q_{i-1}H_iq_i^{-1},$$
$$B_i'=z_{i-1}B_iz_i^{-1}.$$

Лема 1. Використовуємо позначене вище. Для усіх $i\in\{1,2,...,s\}$, перші елементи $\alpha_{i1}',\gamma_{i1}',\beta_{i1}'$ множин A_i',H_i',B_i' – усі дорівнюють одиниці.

Більш того, $\breve{\alpha}'(x)=\breve{\alpha}(x)p_s^{-1},\breve{\gamma}'(x)=\breve{\gamma}(x)q_s^{-1},\breve{\beta}'(x)=\breve{\beta}(x)z_s^{-1}$.

Зокрема, β' – логарифмічний підпис для Z та α' – покриття для деякої підмножини J' групи G.

Лема 2. Нехай (α,γ) буде відкритий ключ для MST_3 с $(\beta,(t_0,t_1,...,t_s))$ – відповідний закритий ключ. Визначимо α',γ' та β', як це зроблено раніше, та нехай $t_0'=t_1'=...=t_s'=t_0$. Тоді (α',γ') – публічний ключ для MST_3 із відповідним закритим ключем – $(\beta',(t_0',t_1',...,t_s'))$.

Доведення. Припустимо, що використовуємо α',β' та $t_0',t_1',...,t'$ для генерації відкритого ключа (α',δ), де $\delta=[D_1,D_2,...,D_s]$, тоді $\delta_{ij}=\beta_{ij}'(t_{i-1}')^{-1}\alpha_{ij}'t_i'$. Достатньо показати, що $\delta=\gamma'$, але

$$\delta_{ij}=\beta_{ij}'t_0^{-1}\alpha_{ij}'t_0=z_{i-1}\beta_{ij}z_i^{-1}t_0^{-1}\alpha_{ij}'t_0=z_{i-1}\beta_{ij}z_i^{-1}t_0^{-1}p_{i-1}\alpha_{ij}p_i^{-1}t_0$$
$$=\beta_{ij}z_{i-1}z_i^{-1}t_0^{-1}p_{i-1}\alpha_{ij}p_i^{-1}t_0=\beta_{ij}\beta_{i1}^{-1}t_0^{-1}p_{i-1}\alpha_{ij}p_i^{-1}t_0.$$

$t_0^{-1}p_{i-1}=z_{i-1}^{-1}q_{i-1}t_{i-1}^{-1}$ та $p_i^{-1}t_0=t_iq_i^{-1}z_i$.

Таким чином, $\delta_{ij}=\beta_{ij}\beta_{i1}^{-1}z_{i-1}^{-1}q_{i-1}t_{i-1}^{-1}\alpha_{ij}t_iq_i^{-1}z_i=\beta_{ij}q_{i-1}t_{i-1}^{-1}\alpha_{ij}t_iq_i^{-1}$.

З визначення z_i і, оскільки z_i є централом. Але $\gamma_{ij}'=q_{i-1}\gamma_{ij}q_i^{-1}=q_{i-1}\beta_{ij}t_{i-1}^{-1}\alpha_{ij}t_iq_i^{-1}$. Оскільки β_{ij} – є центром, маємо, що $\gamma_{ij}'=\delta_{ij}$, що та потрібно було довести.

Визначаємо проблему обмеження для MST_3 наступним чином. Вхід є відкритим ключем (α,γ) для MST_3 та випробуваний шифротекст (y_1,y_2). Відкритий ключ повинен мати додаткову властивість, що $\alpha_{i1}=\gamma_{i1}=1$ для $1\le i\le s$; відповідний закритий ключ повинен мати

властивість, що $t_0 = t_1 = ... = t_s$ та також, що $\beta_{i1} = 1$ для $1 \le i \le s$. Вихід є відкритим текстом p, що відповідає закритому (y_1, y_2).

Теорема 1. Існує скорочення поліноміального часу від проблеми OWE для MST_3 (для загальних ключів) до проблеми обмеженого OWE для MST_3 (дійсно, потрібен тільки один виклик оракла з обмеженим OWE).

Доведення. Нехай $O(\alpha, \gamma, y_1, y_2)$ буде ораклом для проблеми обмеженого OWE для MST_3. Показуємо, що цей оракл може бути використаний для вирішення проблеми OWE для MST_3 для загальних ключів.

Припустимо (α, γ) є (необмеженим) відкритим ключем із відповідним закритим ключем $(\beta, (t_0, t_1, ..., t_s))$. Нехай (y_1, y_2) випробуваним шифртекстом із відповідним повідомленням p. Припустимо, що отримаємо (α, γ) та (y_1, y_2). Визначимо (α', γ'), як це зроблено вище. Зауважимо, що α' та γ' може бути ефективно побудовано з α та γ з використанням тільки відкритої частини інформації. З Лем 1 та 2 (α', γ') є відкритим ключем із відповідним закритим ключем $(\beta', (t_0, t_0, ..., t_0))$, такі ключі задовольняють обмеженням. Визначимо $y_1' = y_1 p_s^{-1}$ та $y_2' = y_2 q_s^{-1}$. Зазначимо знову, що p_s та q_s визначені з використанням відкритої інформації, то що y_1' та y_2' можуть бути ефективно обчислені з отриманої інформації. Викликаємо оракла O на $(\alpha', \gamma', y_1', y_2')$ та отримаємо повідомлення p таке, що $(\alpha'(p), \gamma'(p)) = (y_1', y_2')$.

Тоді p – повідомлення, яке було нам необхідним, оскільки

$$\breve{\alpha}(p) = \breve{\alpha}'(p) p_s = y_1' p_s = y_1 p_s^{-1} p_s = y_1$$
$$\breve{\gamma}(p) = \breve{\gamma}'(p) \mathrm{q}_s = y_2' q_s = y_2 q_s^{-1} q_s = y_2 .$$

Практичні атаки на логарифмічні підписи

Нехай $m = 81$. Базової групою є Сузукі 2-група над полем F_q, де $q = 2^m$. Загальна атака потребує знаходження розміру q для успішності: фіксуємо $m = 81$, так, що ця загальна атака стає невідтворюваною. Зауважимо, що відкритий ключ вже доволі довгий, коли $m = 81$: у найбільш ефективному випадку розглянемо (дивиться приклад 1 нижче), нам потрібно більше 19 000 біт для зберігання елементів, які не є ідентифікаторами, в логарифмічних підписах α та γ. Методи суттєво не залежать від автоморфізму θ у визначенні Сузукі 2-групи, тому зафіксуємо θ такою, що дорівнює квадратичному автоморфізму в усіх експериментах.

Побудуємо логарифмічний підпис β та згенеруємо логарифмічні підписи типу $(r_1, r_2, ..., r_s)$, де $\prod_{i=1}^{s} r_i = 2^m$. Зауважимо, що цілі числа r_i повинні бути достатньо малими, щоб ефективно зберігати логарифмічні підписи. Першим кроком достатньо розглянути логарифмічні підписи, які мають додаткову властивість: елементи β_{i1} дорівнюють одиниці, тобто від самого початку генеруємо β з цією властивістю, та ніякий загал не втрачається під час генерації логарифмічних підписів таким чином.

У рамках задач криптоаналізу розглядаємо успішність атаки лише, якщо ми отримаємо дійсний закритий ключ після застосування невеликої кількості спроб вгадати t' за початкових умов для t як наслідок того, що β - бієктивне. Потім обираємо t' випадковим чином за цих умов.

Нагадаємо позначення $S(a,b)$ для елемента в Сузукі 2-групи, визначене в [2]. Спираючись на зауваження в [8], вважаємо, що $t = S(x,0)$, де $x \in \mathrm{F}_q$ невідомо, та тому обмежуємо припущення t' формою $S(y,0)$ для деяких $y \in \mathrm{F}_q$. Умови на t, які отримуємо, є F_2- лінійними умовами, тому легко обрати t', яке задовольняє цим умовам випадковим чином. Точні умови на t, які отримаємо, будуть залежати від кількості компонентів r_i типу β, що дорівнюють 2: коли таких компонентів багато, умова, яку отримаємо, слабкіше. З цієї причини приводимо ти випадки для ілюстрації методів. У прикладі 1 $r_i = 2$ для усіх i. У цьому випадку не знаходимо умов на t, але просто випадковий вибір невеликої кількості значень для t' призводить до успішної атаки. У прикладі 2 $r_i \neq 2$ для усіх i. У цьому випадку знаходимо, що кожна умова, яку отримаємо, обмежує t' такою невеликою кількістю можливостей, що можна провести незначний вичерпний пошук. Приклад 3 з приблизно половиною компонентів типу β, що дорівнює 2, ілюструє проміжний випадок. Тут кожна умова обмежує кількість можливостей для t' значно (приблизно до 2^{40} можливостей). Дуже небагато спроб вгадати t' можуть одночасно задовольняти двом з цих умов, тому поєднання двох умов дозволяє отримати еквівалентний закритий ключ шляхом незначного вичерпного пошуку.

Розглянемо приклад 1 для β типу $(2,2,...,2)$. У цьому випадку припускаємо, що β складається з 81 блоку довжиною 2. Такі логарифмічні підписи привабливі з точки зору ефективності: нам необхідно зберігати тільки 81 нетривіальний елемент в множині B_i, більш того, ці елементи формуються з базису Z, коли Z розглядається як 81-й мірний векторний простір над F_2 та обчислення з β можуть бути проведені з використанням простої лінійної алгебри (зауважимо, що це приклад канонічного логарифмічного підпису, як визначено в [8], однак атака, описана в цій статті, не працює в даному конкретному випадку).

Отримаємо відкриті й секретні ключі для MST_3 наступним чином. Довільно обираємо множину, що породжує $\{z_1,...,z_{81}\}$, для Z. Визначаємо елементи $d_{i2} \in \mathrm{F}_q$ через $z_i = S(0,d_{i2})$, таким чином елементи d_{i2} формують F_2 – базис для F_q. Обираємо $\beta = [B_1,...,B_{81}]$, де $B_i = \{1, S(0,d_{i2})\}$, потім генеруємо елементи $e_{i2}, f_{i2} \in \mathrm{F}_q$ випадковим чином та визначаємо $\alpha = [A_1,...,A_{81}]$, де $A_i = \{1, S(e_{i2}, f_{i2})\}$

Нехай $t = S(x,0)$, де $x \in \mathrm{F}_q$ – задано випадковим чином. Будуємо γ, як це описано у визначенні MST_3. Тобто, визначаємо

$$\gamma_{i2} = \beta_{i2} t^{-1} \alpha_{i2} t = S(0,d_{i2}) S(x, x^{\theta} x) S(e_{i2}, f_{i2}) S(x,0) =$$

$$= S(e_{i2}, d_{i2} + f_{i2} + e_{i2} x^{\theta} + e_{i2}^{\theta} x) =: S(e_{i2}, g_{i2})$$

і обираємо $\gamma = [C_1,...,C_{81}]$, де $C_i = \{1, \gamma_{i2}\}$.

Атака реалізується наступним чином. Нехай $t' = S(y,0)$ буде випадкова спроба вгадати t. Формуємо $b = [B_1,...,B_{81}]$, де $B_i = \{1, b_{i2}\}$ та b_{i2} задано як

$$b_{i2} = \gamma_{i2} t'^{-1} \alpha_{i2} t' = S(e_{i2}, g_{i2}) S(y, y^{\theta} y) S(e_{i2}, e_{i2}{}^{\theta} e_{i2} + f_{i2}) S(y,0)$$
$$= S(0, g_{i2} + f_{i2} + e_{i2} y^{\theta} + e_{i2}^{\theta} y)$$

Якщо множина $\{b_{i2}\}_{i=1}^{81}$ є лінійно незалежною, то $\tilde{b}$ є бієкцією, та з [9] випливає, що маємо еквівалентний секретний ключ. Якщо множина лінійно залежна, повторюємо цей процес з другою спробою здогадки t'. В роботі [12] цю атаку було згенеровано для 10 000 випадкових екземплярів MST_3. Результати наведені в табл. 1.

Середня кількість здогадок для t' перед тим, як знайти еквівалентний секретний ключ, склала приблизно 3,47. Таким чином, схема у цьому випадку небезпечна.

Таблиця 1

Експериментальні результати для Прикладу 1

Кількість здогадок t'	1	2	3	4	5	6	7	8	9
Частота	2829	2111	1429	1048	799	490	374	279	181
Кількість здогадок t'	10	11	12	13	14	15	16	17	18
Частота	133	98	66	47	31	26	19	11	5
Кількість здогадок t'	19	20	21	22	23	24	25	26	27
Частота	3	7	7	4	2	1	0	0	0

Розглянемо Приклад 2 для β типу $(8,64,64,...,64)$. Уданому випадку використовувані логарифмічні підписи складаються з одного блоку розміром 8 та тринадцять блоків розміром 64. Побудуємо β наступним чином. Виробляємо випадковий базис $\{z_1,...,z_{81}\}$ для Z.

Розглянемо ланцюжок підгруп $1 = Z_0 < Z_1 < ... < Z_{27} = Z$, де $Z_i = \langle z_1,...,z_{3i} \rangle$ для $1 \le i \le 27$. Формуємо поперечний логарифмічний підпис типу $(8,8,...,8)$ (з 27 блоками), чий i – й блок є поперечним для Z_{i-1} в Z_i, містить тотожність якості першого елементу. Потім випадковим чином поєднуємо 26 блоків розміром 8 по парах, щоб сформувати 13 блоків розміром 64. Шляхом передупорядковування блоків побудували ATLS $\beta = [B_1, B_2, \ldots, B_{14}]$ типу $(8,64,64,...,64)$ для Z. Визначимо елементи $d_{ij} \in F_q$ через $\beta_{ij} = S(0, d_{ij})$.

Генеруємо елемент $t = S(x,0)$, елементи $\alpha_{ij} = S(e_{ij}, f_{ij})$, елементи $\gamma_{ij} = S(e_{ij}, g_{ij})$ та накриття α та γ, як у Прикладі 1. Зокрема має місце рівність $g_{ij} = d_{ij} + f_{ij} + e_{ij}^{\theta} x + e_{ij} x^{\theta}$.

Атака відновлює секретний ключ безпосередньо невеликим вичерпним пошуком замість того, щоб вгадувати еквівалентний секретний ключ. З [12] витікає, що існує i та j таке, що $j \ge 2$ і $B_i \cdot b_{ij} = B_i$. Для i та j існує лише невелика кількість можливостей (з використанням незначного вичерпного пошуку); можемо припустити, що дійсний вибір для i та j відомий. Знаємо, що $d_{ij} = g_{ij} + f_{ij} + e_{ij}^{\theta} x + e_{ij} x^{\theta}$. Більш того, коли $B_i \cdot b_{ij} = B_i$, має місце рівність $d_{ij} + d_{ik} = d_{il}$ щонайменше $|B_i| - 2$ пар індексів k, l, де $2 \le k, l \le |B_i|$ та де j, k та l різні. Записуючи u_{ijkl} для $u_{ij} + u_{ik} + u_{il}$, отримаємо рівняння $g_{ijkl} + f_{ijkl} = e_{ijkl}{}^{\theta} x + e_{ijkl} x^{\theta}$.

Зазначимо, що елементи e_{ijkl}, f_{ijkl} та g_{ijkl} є відомими (формуючи частину відкритого ключа (α,γ)), але χ залишається невідомим. Для заданого $e\in \mathrm{F}_q$ відображення $\phi_e : \mathrm{F}_q \to \mathrm{F}_q$, задане за допомогою $x \mapsto e^o x + e x^o$ є F_2- лінійним відображенням. Більш того, коли $e\neq 0$, маємо, що ϕ_e є ядром розміру 2. Припустимо (у самому найкращому випадку), що e_{ijkl} не дорівнює нулю, отримаємо, що кожне таке рівняння виконується не більше ніж двома можливостями для χ (і ці варіанти легко обчислюються з використанням елементарної лінійної алгебри). Є менше 2^{18} варіантів для i, j, k та l. Як тільки ці вибори фіксовані, існує не більше 2 значень для χ, які задовольняють рівнянню. Таким чином, можемо відновити χ вичерпним пошуком, хоча 2^{20} можливостей (для кожної можливості для χ можемо побудувати b та перевірити, чи є $\tilde{b}$ бієкцією: ця перевірка може бути ефективно виконана для ATLS.). Зазначимо, що у цій атаці значним чином використовується той факт, що $|B_i|>2$, якщо $|B_i|=2$, то припустимих варіантів для j та k немає. Зазначимо також, що коли маємо правильне значення для i та j, той саме елемент χ буде знайдений щонайменше $|B_i|-2$ разів рішення рівняння при j та k, що змінюються за усіма можливими значеннями. Це спостереження можна використовувати для більш ефективного відновлення χ. Нарешті, зазначимо, що коли i правильно вгадується, множина B_i має властивість, що добуток його елементів повинен бути тотожнім (оскільки те саме вірно для будь-якого суміжного класу підгрупи Z порядку 4 або більше). Цю властивість можна використовувати для знаходження χ без необхідності вгадати j,k або l. Реалізуємо атаку з використанням SAGE на стандартному ПК, та в кожному запуску довільно обране секретне значення χ було повернено правильно протягом 30 хвилин. Таким чином, у цьому випадку криптосистема MST_3 також небезпечна.

Розглянемо приклад 3 для β типу $(2,2,...2,16,16,...,16)$. Нарешті, розглянемо випадок, коли β складається з 41 множини розмірів 2 та10 множин розміру 16. У цій ситуації рівняння не обмежує число можливостей для χ достатнім чином та тому об'єднуємо два рівняння для відновлення χ.

Побудуємо β, починаючи з ланцюжка підгруп $1=Z_0<Z_1<...<Z_{61}=Z$, де кожен Z_i має індекс 2 в Z_{i+1} при $0\le i\le 40$ та індекс 4 для $41\le i\le 60$. Формуємо випадковий поперечний логарифмічний підпис для цього ланцюжка (враховуючи тотожність як перший елемент в кожному поперечному): цей логарифмічний підпис буде складатися з 41 множини розмірів 2 та 20 множин розміру 4. Потім поєднуємо 20 множин розміру 4 в пари, щоб сформувати 10 множин розміру 16, де поєднання цих множин обирається випадковим чином. Результатом є ATLS $\beta=[B_1,B_2,...,B_{41},B_{42},...,B_{51}]$ того типу, який шукаємо. Потім обираємо t та α та будуємо, як і раніше, γ.

Таблиця 2

Експериментальні результати для прикладу 2

Номер можливих χ	0	1	2	4	8	16
Розподіл правильних індексів	0	579	386	33	2	0
Розподіл неправильних індексів	276	543	170	10	1	0

У даному випадку атака реалізується наступним чином. Визначимо підгрупу $H=\langle B_1,...,B_{41}\rangle$. Визначимо $\beta_{ij}=S(0,d_{ij})$ та $V=\langle d_{i2}:1\le i\le 41\rangle$. Зауважимо, що V має розмі-

рність 41 та $H=\{S(0,v):v\in V\}$. Зрозуміло, що образ $[B_{42},...,B_{51}]$ в Z/H є ATLS для Z/H та не містить блоків розмірами 2. Таким чином, можемо продовжувати аналогічно Прикладу 2, на цей раз працюючи в частці Z/H, щоб вивести рівняння, що x повинно задовольняти за модулем V. Використовуючи позначення з Прикладу 2, отримаємо рівняння виду $g_{ijkl}+f_{ijkl}+V=\phi_{e_{ijkl}}(x)$, де $\phi_{e_{ijkl}}$ є F_2- лінійним відображенням. У припущенні, що e_{ijkl} відмінний від нуля, рівняння цієї форми обмежує χ лежати в афінному підпросторі з розміром не більше 42, тому зменшили розмір вичерпного пошуку можливостей χ до 2^{42}. Але правильне припущення для i означає, що χ задовольняє хоча б $|B_i|-2\geq 2$ таких рівнянь, як j,k та l змінюються. Якщо правильно вгадуємо дві такі комбінації j,k та l, знаємо, що χ лежить в перетині двох афінних підпросторів розмірності не більше 42 (а саме, множини рішень, що відповідають двом рівнянням), та це зменшує кількість можливостей для χ до незначного числа. Дійсність кожної можливості для χ можна визначити, перевіривши бієкцію $\breve{b}$, як у прикладі 2.

Під час реалізації цієї ідеї створили 1 000 випадкових ATLS для Z/H. Для кожного ATLS обирали випадкову пару рівнянь, де індекси i,j,k та l були правильно вгадані, та обчислили розмір перетинів двох множин рішень. Зробили те саме, коли індекси були вгадані неправильно, щоб перевірити, що кількість можливостей для χ у цьому випадку не дуже велика. Записуємо результати в табл. 2.

Як видно з табл. 2, у будь-якому випадку число можливостей для χ невелике. Для перевірки необхідно менше 2^{20} пар рівнянь, та тому зазвичай очікуємо вичерпний пошук χ, розміром не більше 2^{24} (крім того, у цьому пошуку очікуємо, що знаходження χ буде відбуватися з відносно високою частотою, так як воно з'являється для кожної правильної пари рівнянь).

Висновки

Атаки на криптосистему MST_3 в її базовій конструкції призводять до її компрометації. Базовим елементом криптосистеми MST_3 є логарифмічні підписи – особливий вид факторизації. Методи генерації логарифмічних підписів суттєво впливають на безпеку конструкції. Зауважимо, що доки не буде винайдено метод створення безпечних слабких логарифмічних підписів, MST_3 небезпечна. Багато атак експлуатують проблеми базової конструкції з використанням Сузукі-2 груп. Більшість атак може буде імплементовано з використанням доступних обчислювачів. Водночас саме розуміння архітектури атаки стимулює спроби використання інших підходів до забезпечення потрібного рівня безпеки, на кшталт використання гомоморфного шифрування у якості додаткового елемента посилення конструкції [14], використання посилених логарифмічних підписів [15]. В останні роки, використовуючи обґрунтовані властивості неабелевих груп [16], результати робіт з пошуку кращих за характеристиками логарифмічних підписів [17], дослідникам вдалось запропонувати посилені конструкції криптосистеми MST_3 за рахунок застосування узагальнених груп [18], автоморфізмів груп [19, 20] та груп з посиленими параметрами безпеки [21]. Підсумовуючи, зауважимо, що доки не буде винайдено метод створення безпечних слабких логарифмічних підписів, MST_3 небезпечна.

Список літератури:

1. Kotukh Y., Khalimov G. Hard problems for non-abelian cryptography // 2021: Fifth International Scientific and Technical Conference "COMPUTER AND INFORMATION SYSTEMS AND TECHNOLOGIES", 2021, pp39-40, https://doi.org/10.30837/csitic52021232176

2. Lempken W. A public key cryptosystem based on non-abelian finite groups / W. Lempken, T. van Trung,

S.S. Magliveras, W. Wei // Journal of Cryptology. 2009. Vol. 22 (1). P. 62–74.

3. Gonzáles Vasco M. I. On minimal length factorizations of finite groups / M. I. Gonzáles Vasco, M. Rotteler, R. Steinwandt // Experimental Mathematics. 2003. Vol. 12 (1). P. 1–12.

4. Singhi N. Minimal logarithmic signatures for finite groups of Lie type / N. Singhi, N. Singhi, S. Magliveras // Designs, Codes and Cryptography. 2010. Vol. 55 (2). P. 243–260.

5. Magliveras S. New approaches to designing public key cryptosystems using one-way functions and trap-doors in finite groups / S. Magliveras, D. Stinson, T. van Trung // Journal of Cryptology. 2002. Vol. 15. P. 285–297.

6. Goldreich O. Foundations of Cryptography: Basic Tools // Cambridge University Press. 2001.

7. 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.

8. 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.

9. 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.

10.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.

11.Magliveras S. Algebraic Properties of Cryptosystem PGM / S. Magliveras, N. D. Memon // Journal of Cryptology. 1992. Vol. 5 (3). P. 167–183.

12.Mullan, Ciaran. Some Results in Group-Based Cryptography. (2011)//Thesis

13.Svaba P. and T. van Trung. Public key cryptosystem MST3 cryptanalysis and realization // Journal of Mathematical Cryptology. Vol.4. No.3. Pp.271–315,2010

14.Cong Y., Hong H., Shao J., Han S., Lin J. and Zhao S. A New Secure Encryption Scheme Based on Group Factorization Problem // IEEExplore, November 20, 2019 Digital Object Identifier 10.1109/ACCESS.2019.2954672 https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8907845

15.T. van Trung. Construction of strongly aperiodic logarithmic signatures // J. Math. Cryptol. Vol. 12. No. 1. Pp. 23-35, 2018

16.Kotukh Y., Severinov E., Vlasov O., Tenytska A., Zarudna E. Some results of development of cryptographic transformations schemes using non-abelian groups. Radiotekhnika. 2021. No. 204. P. 66–72. https://doi.org/10.30837/rt.2021.1.204.07

17.Kotukh E., Severinov O., Vlasov A., Kozina L., Tenytska A., Zarudna E. Methods of construction and properties of logariphmic signatures . *Radiotekhnika* 2021. No 205. P. 94–99. https://doi.org/10.30837/rt.2021.2.205.09

18.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

19.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.

20.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.

21.Khalimov G., Kotukh Y., Didmanidze I., Sievierinov O., Khalimova S., Vlasov A. Towards three-parameter group encryption scheme for MST3 cryptosystem improvement // 2021 Fifth World Conference on Smart Trends in Systems Security and Sustainability (WorldS4), 2021, pp. 204-211, doi: 10.1109/WorldS451998.2021.9514009.

Надійшла до редколегії 03.08.2021

Відомості про авторів:

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

Охріменко Тетяна Олександрівна – канд. техн. наук, докторант, старший науковий співробітник науково-дослідної лабораторії протидії кіберзагрозам в авіаційній галузі, Національний авіаційний університет, Київ, Україна. e-mail: t.okhrimenko@nau.edu.ua

Дяченко Оксана Федорівна – канд. пед. наук, доцент кафедри системного аналізу та інформаційних технологій, Маріупольський державний університет, Маріуполь, Україна. e-mail: o.dyachenko@mdu.in.ua

Ротаньова Наталія Юріївна – канд. пед. наук, доцент, доцент кафедри системного аналізу та інформаційних технологій, Маріупольський державний університет, Маріуполь, Україна. e-mail: n.rotaneva@mdu.in.ua

Козіна Лідія Сергіївна – здобувач вищої освіти, кафедра інформаційних та комп'ютерних систем, Національний університет "Чернігівська політехніка", Чернігів, Україна, e-mail: lidiia.kozina@gmail.com

Зеленський Данїїл Володимирович – здобувач вищої освіти, факультет комп'ютерних наук, Харківський національний університет радіоелектроніки, Харків, Україна.