УДК 681.3.06

Г.З. ХАЛІМОВ, д-р техн. наук, Є.В. КОТУХ, канд. техн.наук,
Ю.О. СЕРГІЙЧУК, О.С. МАРУХНЕНКО

АНАЛІЗ СКЛАДНОСТІ РЕАЛІЗАЦІЙ КРИПТОСИСТЕМИ НА ГРУПІ СУДЗУКІ

Криптографія з відкритим ключем будується на труднощах розв'язання математичних проблем, які дуже часто, але не виключно, виникають з теорії чисел. На початку 80-х років було запропоновано застосування групових теоретичних проблем для криптографії (Wagner і Magyarik [1], Wagner [2], Magliveras [3]). Зокрема в роботах Magliveras та ін. були зроблені пропозиції для криптографічних схем на основі спеціальних розкладених кінцевих груп (так звані логарифмічні сигнатури) [3]. Крім того, відомі інші криптографічні дослідження Gonzarlez Vasco, Steinwandt, Birget, Bohliet і ін. Ці розкладання як математичні об'єкти цікаві самі по собі. Наприклад, работа Hajors про гіпотезу Міньковського показує, що для абелевих груп цей вид розкладання виникає при вивченні багатовимірних покриттів (див. [4]).

Прикладами криптосистем з відкритим ключем є MST1, MST2, MST3. Актуальним завданням їх реалізації є побудова коротких логарифмічних сигнатур. Логарифмічні сигнатури, як особливий тип групових розкладів представляються в якості основних компонентів деяких криптографічних ключів. Науковий інтерес пов'язан з пошуком логарифмічних сигнатур в кінцевих групах (такі розкладання існують для вирішуваних, симетричних і знакозмінних груп), оцінкою їх практичної можливості і секретності.

В роботі розглянуто основні реалізації криптосистем на групах і аналіз оцінки складності обчислень.

Визначення та властивості логарифмічних сигнатур

Основні позначення, визначення та основні факти про логарифмічні сігнатури, накриття для кінцевих груп і їх породжені відображення представимо на основі опису в [4].

Нехай ς – кінцева абстрактна група. Визначимо ширину ς як позитивне ціле число $w = \lceil \log|\varsigma| \rceil$. Позначимо через $\varsigma^{[\mathbf{Z}]}$ сукупність усіх кінцевих послідовностей елементів ς і відобразимо елементи $\varsigma^{[\mathbf{Z}]}$ як однорядкові матриці із записами в ς. Нехай $X = [x_1, x_2 \ldots, x_r]$ і $Y = [y_1, y_2 \ldots, y_s]$ будуть двома елементами в. $\varsigma^{[\mathbf{Z}]}$

Визначимо $X \cdot Y = [x_1y_1, x_1y_2, \ldots, x_1y_s, x_2y_1, x_2y_2, ..., x_2y_s, ..., x_ry_1, x_ry_2, ..., x_ry_s]$.

Замість запису $X \cdot Y$ можемо записати $X \otimes Y$ як звичайний тензорний добуток матриць або для короткого написання залишимо XY. Якщо $X = [x_1, \ldots, x_r] \in \varsigma^{|\mathbf{Z}|}$, позначимо через $\bar{X}$ елемент $\sum_{i=1}^{r} x_i$ у груповому кільці $\mathbf{Z}\varsigma$.

Нехай $\alpha = [A_1, A_2, ...A_s]$ – послідовність $A_i \in \varsigma^{|\mathbf{Z}|}$, така, що $\sum_{i=1}^{s} |A_i|$ обмежена поліномом в $\log|\varsigma|$. Нехай

$$\bar{A}_1 \cdot \bar{A}_2 \cdots \bar{A}_s = \sum_{g \in \varsigma} a_g g \,, a_g \in \mathbf{Z} \,.$$

Нехай S – підмасив ς. Тоді, можемо сказати, що α є:

(i) накриттям для ς (або S), якщо $a_g > 0$ для всіх $g \in \varsigma$ ($g \in S$);

(ii) логарифмічною сігнатурою для $\varsigma(S)$, якщо $a_g = 1$ для кожного $g \in \varsigma$ ($g \in S$).

Нехай α буде накриттям.

Визначимо $\lambda_{\min} := \min\{a_g : g \in \varsigma\}$, $\lambda_{\max} := \max\{a_g : g \in \varsigma\}$ та $\lambda := \lambda_{\max} / \lambda_{\min}$. Співвідношення λ визначає степінь однорідності α. Говоримо, що α – однорідне накриття, якщо $\lambda = 1$. Зокрема, логарифмічна сігнатура є однорідним накриттям.

Зверніть увагу, що якщо $\alpha = [A_1, ... A_s]$ є логарифмічною сігнатурою для ς, тоді кожний елемент $y \in \varsigma$ може бути однозначно виражений як добуток вигляду

$$y = q_1 \cdot q_2 \cdots q_{s-1} \cdot q_s, \; q_i \in A_i. \tag{1}$$

Зазвичай, для загальних накриттів, що факторизуються (1) не унікальне й проблема пошуку розкладення для даного $y \in \varsigma$, у загальному випадку, є обчислювально неможливою.

Нехай $\alpha = [A_1, ... A_s]$ – накриття для ς з $r_i = |A_i|$. Тоді A_i називаються блоками від α і вектором $(r_1, ..., r_s)$ блока довжин r_i і класу α. Визначимо довжину α як ціле число $\ell = \sum_{i=1}^{s} r_i$. Однорідне накриття $\alpha = [A_1, ... A_s]$ класу $(r, r, ..., r)$ називається $[s, r]$-мережею. Говоримо, що α є нетривіальним, якщо $s \geq 2$ й $r_i \geq 2$ для $1 \leq i \leq s$, у протилежному випадку α є тривіальним. Позначимо через $C(\varsigma)$ і $\Lambda(\varsigma)$ відповідні подання накриттів і логарифмічних сігнатур групи ς.

Нехай $\Gamma = \{(\varsigma_\ell, \alpha_\ell)\}_{\ell \in T}$ – сімейство пар, індексоване за допомогою параметра безпеки ℓ, де ς_ℓ – групи загальної презентації, α_ℓ – особливе накриття для ς_ℓ довжини полінома, який дорівнює ℓ. Вважаємо, що Γ – просте, якщо імовірнісний алгоритм поліноміального часу виконання A, за якого для кожного $g \in \varsigma_\ell$, A приймає (α_ℓ, g) вхідні й вихідні дані факторизації $\varphi(g)$ від g відносно α_ℓ з переважною імовірністю успіху. Або вважаємо, що Γ – випадкове, якщо для будь-якого імовірнісного алгоритму поліноміального часу виконання A, імовірність того, що A успішне у факторизації випадкового елемента g від ς, є незначною.

Для кінцевих груп є елементи $\{(\varsigma_\ell, \alpha_\ell)\}_\ell$, для яких факторизація вважається складною. Для прикладу, нехай q – проста степінь числа, для якого проблема дискретного логарифмування в мультиплікативній групі кінцевого поля F_q вважається складною. Нехай $2^{\ell-1} \leq q - 1 < 2^\ell$ і нехай ς_ℓ буде раніше згаданою мультиплікативною групою F_q^*. Нехай f – генератор ς_ℓ. Якщо $\alpha_\ell = [A_1, A_2, ... A_\ell]$, де $A_i = [1, f^{2^{i-1}}]$, тоді α_ℓ – накриття ς_ℓ й факторизація стосовно α_ℓ зводиться до розв'язання проблеми дискретного логарифмування для ς_ℓ.

Нехай $\alpha = [A_1, A_2, ... A_s]$ – накриття групи ς. Нехай $g_0, g_1, ..., g_s \in \varsigma$ і розглянемо $\beta = [B_1, B_2, ... B_s]$ з $B_i = g_{i-1}^{-1} A_i g_i$ для спеціального випадку, де $g_0 = 1$ й $g_s = 1$, тоді β називається багатошаровим накриттям від α. Зверніть увагу, що β також є накриттям для ς.

Нехай $\alpha = [A_1, A_2, ... A_s]$ – накриття класу $(r_1, r_2, ..., r_s)$ для ς з $A_i = [a_{i,1}, a_{i,2}, ..., a_{i,r_i}]$ і нехай $m = \prod_{i-1}^{s} r_i$. Нехай $m_1 = 1$ і $m_i = \prod_{j=1}^{i-1} r_j$ для $i = 2, ..., s$. Позначимо τ як канонічну бієкцію від $\mathbf{Z}_{r_1} \oplus \mathbf{Z}_{r_2} \oplus \cdots \oplus \mathbf{Z}_{r_s}$ на $\mathbf{Z}_m$, тобто

$$\mathbf{Z}_{r_1} \oplus \mathbf{Z}_{r_2} \oplus \cdots \oplus \mathbf{Z}_{r_s} \to \mathbf{Z}_m$$

$$\tau(j_1, j_2, ..., j_s) := \sum_{i=1}^{s} j_i m_i$$

Використовуючи τ, можемо визначити сюр'єктивне відображення $\breve{\alpha}$, породжене α:

$$\breve{\alpha}: \mathbf{Z}_m \to \varsigma$$

$$\breve{\alpha}(x) := a_{1,j_1} \cdot a_{2,j_2} \cdots a_{s,j_s}$$

де $(j_1, j_2, ..., j_s) = \tau^{-1}(x)$. Оскільки τ й τ^{-1} ефективно обчислювані, то відображення $\breve{\alpha}(x)$ також ефективно обчислюване.

З іншого боку, з даним накриттям α і елементом $y \in \varsigma$, щоб визначити будь-який елемент $x \in \breve{\alpha}^{-1}(y)$, необхідно отримати кожне з можливих розкладень класу для y і визначити показники $j_1, j_2, ..., j_s$ такі, що $y = a_{1,j_1} \cdot a_{2,j_2} \cdots a_{s,j_s}$. Це можливо тільки якщо α – просте. Оскільки вектор $(j_1, j_2, ..., j_s)$ визначено, то $\breve{\alpha}^{-1}(y) = \tau(j_1, j_2, ..., j_s)$ може бути ефективно обчислено.

Два накриття α й β вважатимуться еквівалентними, якщо $\breve{\alpha} = \breve{\beta}$.

Приклад

Наведемо приклад за участю α й β для змінної групи A_5. Класи α й β дорівнюють (5,2,6) і (3,4,5) і $|A_5| = 5 \cdot 2 \cdot 6 = 3 \cdot 4 \cdot 5 = 60$ відповідно. У табл. 1 блоки α й β подані вертикально. Щоб ефективно обчислити τ^{-1} й τ, прикладемо канонічні логарифмічні сігнатури τ_α й τ_β адитивної групи $\mathbf{Z}_{60}$ вліво від α і вправо від β. Відповідні класи τ_α й τ_β дорівнюють (5,2,6) і (3,4,5) лише для α й β.

Таблиця 1

Дві логарифмічні сігнатури від A_5

	τ_α	α
	$\mathbf{Z}_{60}$	A_5
$x_1 \to$	0	(1)(2)(3)(4)(5)
	1	(1 2 5 3 4)
	2	(1 5 4 2 3)
	3	(1 3 2 4 5)
	4	(1 4 3 5 2)
$x_2 \to$	0	(1 2 5 3 4)
	5	(2 4) (3 5)
$x_3 \to$	0	(1 3 5 4 2)
	10	(13) (24) (5)
	20	(1)(2)(3)(4)(5)
	30	(15)(23)(4)
	40	(132)(4)(5)
	50	(123)(4)(5)

A_5

β	τ_β	
A_5	$\mathbf{Z}_{60}$	
(1)(2)(345)	0	$\leftarrow y_1$
(1)(2)(354)	1	
(1)(2)(3)(4)(5)	2	
(1)(23)(45)	0	$\leftarrow y_2$
(1)(253)(4)	3	
(1)(243)(5)	6	
(1)(2)(3)(4)(5)	9	
(124)(3)(5)	0	$\leftarrow y_3$
(1)(235)(4)	12	
(13)(2)(45)	24	
(1 5 3 4 2)	36	
(1 4 3 2 5)	48	

Тепер можемо продемонструвати, як на практиці обчислити $\breve{\alpha}: \mathbf{Z}_{60} \to A_5$. Будь-який елемент $x \in \mathbf{Z}_{60}$ можна однозначно записати як суму елементів τ_α, використовуючи тільки один елемент з кожного блоку. Визначення цієї декомпозиції x містить у собі «жадібний» вибір компонентів, одного з кожного блоку, послідовно з нижнього блоку до верхнього й, по суті, визначає $\tau^{-1}(x) = (j_1, j_2, j_3)$. Якщо x_i є елементами A_5 відповідними j_i, то обчислюємо $\breve{\alpha}(x) = x_1 x_2 x_3$. Зокрема, якщо $x = 47$, маємо: 47=40+5+2 і компоненти $j_1 = 2$, $j_2 = 5$ і

$j_3 = 40$, елементи, що вказують $x_1 = (15423)$ $x_2 = (24)(35)$ і $x_3 = (132)$ від A_5. Тоді можемо обчислити: $\breve{\alpha}(47) = x_1 x_2 x_3 = (15423) \cdot (24)(35) \cdot (132) = (125)$.

Якщо розкладемо $y = \breve{\alpha}(x)$ відносно другої логарифмічної сігнатури β, то отримаємо $y = y_1 y_2 y_3$. З елементів y_i отримуємо відповідні елементи адитивної τ_β і формуємо суму. Для окремого випадку, $y = (125) = y_1 y_2 y_3 = (354) \cdot (253) \cdot (124)$ відповідними компонентами τ_β є 1,3,0.

Таким чином, $\breve{\beta}^{-1}((125)) = 1 + 3 + 0 = 4$. Необхідно зазначити у даному прикладі, що α й β належать до класу простих логарифмічних сігнатур, але β, насправді, суперпроста. Ми не пояснюватимемо, як ефективно отримати розкладення $y = y_1 y_2 y_3$, для цього дивіться [6].

Коли група, яка лежить в основі, обрана правильно, бієкція $\breve{\alpha}\breve{\beta}^{-1}$ може використовуватися як криптографічне перетворення з ключем (α, β) у симетричній криптосистемі PGM [8, 9] або як криптографічні примітиви в інших системах.

Опис криптосистеми *MST₃*

Розглянемо структуру криптосистеми MST_3 [4]. Нехай ς – кінцева неабелева група з нетривіальним центром $\mathbf{Z}$, таким, що ς не розкладаються над $\mathbf{Z}$. Також припустимо, що $\mathbf{Z}$ є досить великим, таким, що пошук перебором у $\mathbf{Z}$ є обчислювально нездійсненним.

Криптографічна гіпотеза, що є основою для криптосистеми, полягає в тому, що якщо $\alpha = [\mathrm{A}_1, \mathrm{A}_2, ..., \mathrm{A}_s] := (a_{i,j})$ – випадкове накриття для «великого» підмасива S в ς, то пошук розкладення $g = a_{1j_1} a_{2j_2} \cdots a_{sj_s}$ для будь-якого елемента $g \in S$ відносно α є невирішуваною проблемою.

Генерація ключових даних

Аліса обирає велику групу ς, описану раніше й генерує:

(1) проста логарифмічна сігнатура $\beta = [B_1, B_2, ..., B_s] := (\mathrm{b}_{ij})$ класу $(\mathrm{r}_1, \mathrm{r}_2, ..., \mathrm{r}_s)$ для $\mathbf{Z}$;

(2) випадкове накриття $\alpha = [\mathrm{A}_1, \mathrm{A}_2, ..., \mathrm{A}_s] := (a_{i,j})$ такого самого класу, як і β для деякої підмножини J від ς, такого, що $\mathrm{A}_1, ..., \mathrm{A}_s \subseteq \varsigma \setminus \mathbf{Z}$.

Потім вона обирає $t_0, t_1 ..., t_s \in \varsigma \setminus \mathbf{Z}$ й обчислює:

(3) $\breve{\alpha} = [\tilde{\mathrm{A}}_1, \tilde{\mathrm{A}}_2, ..., \tilde{\mathrm{A}}_s]$, де $\tilde{A}_i = t_{i-1}^{-1} A_i t_i$ для $i = 1, ..., s$;

(4) $\gamma := (h_{ij}) = (b_{ij} \tilde{a}_{ij})$.

Аліса публікує свій відкритий ключ $(\alpha = (a_{ij}), \gamma = (h_{ij}))$, а $(\beta = (\mathrm{b}_{ij}), (\mathrm{t}_0, ..., \mathrm{t}_s))$ – зберігає як свій закритий ключ.

Шифрування

Якщо Боб хоче відіслати повідомлення $x \in \mathbf{Z}_{|Z|}$ для Аліси, то він:

(1) обчислює $y_1 = \breve{\alpha}(x)$ і $y_2 = \breve{\gamma}(x)$;

(2) посилає Алісі $y = (y_1 y_2)$.

Дешифрування

Тепер, коли Аліса знає y_2:

$$y_2 = \breve{\gamma}(x) = b_{1j_1}\tilde{a}_{1j_1} \cdot b_{2j_2}\tilde{a}_{2j_2} \cdots b_{sj_s}\tilde{a}_{sj_s} = b_{1j_1}t_0^{-1}a_{1j_1}t_1 \cdots b_{sj_s}t_{s-1}^{-1}a_{sj_s}t_s =$$
$$= b_{1j_1}b_{2j_2} \cdots b_{sj_s}t_0^{-1}a_{1j_1}a_{2j_2} \cdots a_{sj_s}t_s = \breve{\beta}(x).t_0^{-1}\breve{\alpha}(x)t_s = \breve{\beta}(x).t_0^{-1}y_1t_s,$$

вона може обчислити $\breve{\beta}(x) = \mathrm{y}_2 t_s^{-1}y_1^{-1}t_0$.

Аліса відновлює x з $\breve{\beta}(x)$, використовуючи $\breve{\beta}^{-1}$, який ефективно обчислюємо, оскільки β – проста.

Особливості реалізації криптосистеми MST_3 на Судзукі 2-групах

В реалізації MST_3 запропонована Судзукі 2-група з порядком q^2. Використовуючи позначення Хігмана [5], Судзукі 2-група з порядком q^2 буде позначена як $A(\mathrm{m},\theta)$. Нехай $q = 2^m$ з $3 \le m \in N$ є таким, що поле F_q має нетривіальний автоморфізм θ непарного порядку. Тут мається на увазі, що m не є степенем 2. Тоді групи $A(\mathrm{m},\theta)$ існують.

Насправді, якщо ми визначаємо $\varsigma := \{S(a,b) \mid a,b \in \mathrm{F}_q\}$, де $S(a,b) = \begin{pmatrix} 1 & 0 & 0 \\ a & 1 & 0 \\ b & a^\theta & 1 \end{pmatrix}$ є матрицею 3×3 над полем F_q, це показує, що група ς ізоморфна $A(\mathrm{m},\theta)$. Отже, ς має порядок q^2 і маємо

$$Z := \mathbf{Z}(\varsigma) = \Phi(\varsigma) = \varsigma' = \Omega_1(\varsigma) = \{S(0,b) \mid b \in \mathrm{F}_q\}$$

Оскільки центр $\mathbf{Z}(\varsigma)$ є елементарною абелевою групою порядку q, він може бути ідентифікований з адитивною групою поля F_q. Крім того, фактор-група $\varsigma / \Phi(\varsigma)$ є елементарна абелева група порядку q. Тоді легко перевірити, що множення двох елементів у ς здійснюється відповідно до правила

$$S(a_1,b_1)S(a_2,b_2) = S(a_1+a_2, b_1+b_2+a_1^\theta a_2).$$

Обернений елемент знаходиться за формулою

$$S(a,b)^{-1} = S(a, b+a^{\theta+1}).$$

Алгоритм роботи системи для шифрування має такі етапи [6].

Генерація ключових даних:

1. Обрати велику групу $G = A(m,\theta),\ q = 2^m$.

2. Згенерувати логарифмічну сігнатуру, що факторизується:
$\beta = [B_1,...,B_s] = (b_{i,j}) = (S(0, b_{i,j}.b))$ типа $(r_1,...,r_s)$, где $b_{i,j}.b \in F_q$.

3. Згенерувати випадкове накриття $\alpha = [A_1,...,A_s] = (a_{i,j}) = (S(a_{i,j}.a, a_{i,j}.b))$ того ж типу, що й β, де $a_{i,j}.a \in F_q / \{0\}, a_{i,j}.b \in F_q$.

4. Згенерувати випадкові значення $t_0, t_1, ..., t_s \in G$, матрицю випадкових бітів $\sigma = [q \times q]$.

5. Побудувати гомоморфізм f:$G \to Z$, визначений як $f(S(a,b))=S(0,g(a))$ (в даній реалізації було використано множення на випадкову бітову матрицю $f(a) = a^\sigma$).

6. Обчислити $\gamma = [H_1,...,H_s] = (h_{i,j}) = (S(h_{i,j}.a, h_{i,j}.b))$, де $h_{i,j} = t_{i-1}^{-1} * a_{i,j} * t_i * b_{i,j} * f(a_{i,j})$.

7. Відкритий ключ – $[\alpha, \gamma]$, приватний ключ – $[\beta, (t_0, t_1, ..., t_s), f]$ та додаткові дані, необхідні для факторизації β.

Шифрування повідомлення m:

1. Створити елемент $\chi = S(0, m) \in G$
2. Згенерувати випадкове число $R \in Z$
3. Обчислити криптограму $y_1 = \alpha'(R) * \chi$, $y_2 = \gamma'(R) * \chi$.

Зауваження: для зменшення розмірів шифротексту достатньо зберігати $(y_{1.a}, y_{1.b}, y_{2.b})$, при розшифруванні складова $y_{2.a}$ може бути відновлена за формулою $y_{2.a} = y_{1.a} \oplus t_{0.a} \oplus t_{S.a}$

Розшифрування:

1. Обчислити $\beta'(R) = f(y_1)^{-1} * y_1^{-1} * t_0 * y_2 * t_S^{-1}$.
2. Виконати факторізацію $R = \beta'^{-1}(R)$.
3. Обчислити $\alpha'(R)$.
4. Відновити $m = y_{1.b} \oplus \alpha'(R)_{.b}$.

Тестування шифрування виконано на комп'ютері з ОС Ubuntu 16.04, процесором Intel® Core™ i7-4702MQ CPU @2,20 GHz, 12 ГБ ОЗП, результати представлено в табл. 2, 3.

Таблиця 2

Витрати на шифрування/розшифрування в кінцевому полі 128 біт

Класи розбиття	Час генерації ключових даних, мс	Розмір приватного ключа, байт	Розмір публічного ключа, байт	Час зашифрування 100 КБайт, мс	Час розшифрування 100 КБайт, мс
128[2] →64[4]	56	78830	39761	4749	2711
64[4] →32[16]	59	111726	75217	2388	1487
32[16] →16[256]	169	671918	590609	1205	888

Таблиця 3

Витрати на шифрування/розшифрування в кінцевому полі 256 біт

Класи розбиття	Час генерації ключових даних, мс	Розмір приватного ключа, байт	Розмір публічного ключа, байт	Час зашифрування 100 КБайт, мс	Час розшифрування 100 КБайт, мс
256[2] →128[4]	57	249630	128593	14811	7911
128[4]→ 64[16]	106	361502	248657	7540	4196
64[16] →32[256]	798	2193054	1967569	3782	2318

Порівняння з направленим шифруванням з RSA алгоритмом представлено в табл. 4.

Таблиця 4

Витрати на шифрування/розшифрування за RSA алгоритмом

Розрядність ключових параметрів, біт	Час генерації ключових даних, мс	Розмір приватного ключа, байт	Розмір публічного ключа, байт	Час зашифрування 100 КБайт, мс	Час розшифрування 100 КБайт, мс
512	3,368	342	92	66,987	641,277
1024	8,685	632	160	117,947	2116,400
2048	63,658	1214	292	243,887	9853,580
4096	707,645	2373	548	591,868	64250,400

Висновки

1. Для оптимізації витрат щодо розміру приватного та публічного ключів, часу зашифрування та розшифрування необхідно здійснити підбір класу розбиття логарифмічної сігнатури на блоки. Часові витрати можна зменшити в декілька разів. Використання кінцевого поля 128, 256 бітів достатньо для забезпечення найвищого класу захисту по класифікації криптосистем.

2. При обчисленні в кінцевому полі 2048 та 4096 бітів час зашифрування та розшифрування RSA алгоритмом в десятки разів більше в порівнянні з криптосистемою MST_3, але забезпечує суттєву економію витрат щодо розміру приватного та публічного ключів.

Список літератури:

1. N.R. Wagner and M. R. Magyarik. A Public Key Cryptosystem Based on the Word Problem // Advances in Cryptology. Proceedings of CRYPTO 1984, pp. 19-36, edited by G. R. Blakley and D. Chaum, Lecture Notes in Computer Science 196. Berlin: Springer, 1985.

2. N.R. Wagner. Searching for Public-Key Cryptosystems // In Proceedings of the 1984 Symposium on Security and Privacy (SSP ’84), pp. 91-98. Los Alamitos, CA: IEEE Computer Society Press, 1990.

3. S.S. Magliveras. A Cryptosystem from Logarithmic Signatures of Finite Groups // Proceedings of the 29th Midwest Symposium on Circuits and Systems, pp. 972-975. Amsterdam: Elsevier Publishing Company, 1986.

4. W. Lempken, S.S. Magliveras, Tran van Trung and W. Wei. A public key cryptosystem based on non-abelian finite groups // J. of Cryptology, 22(2009), 62-74.

5. G. Higman, Suzuki 2-groups.Ill. J. Mathematic. 1963. V.7. P.79-96.

6. Pavol Svaba. Covers and logarithmic signatures of finite groups in cryptography : Dissertation. Bratislava : Slowakische Republik, 2011.

Харківський національний
університет радіоелектроніки

Надійшла до редколегії 15.03.2018