УДК 004.056.5

к.т.н. Чевардін В.Є. (ВІТІ)
к.т.н. Самойлов І.В. (ВІТІ)
Толстих В.А. (ВІТІ)
Пономарьов О.А. (ВІТІ)

СТІЙКИЙ МЕТОД ГЕНЕРАЦІЇ ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ ДО КВАНТОВОГО КРИПТОАНАЛІЗУ

Визначені загрози квантового криптоаналіза для алгоритмів генерації ключів. Отримані оцінки часу необхідного для квантового криптоаналізу симетричних та несиметричних криптосистем. Розглянуто стандартизований генератор псевдовипадкових послідовностей (ПВП) на основі еліптичних кривих, наведена його модель. Для вдосконалення генератору ПВП взято канонічну форму еліптичної кривої. Запропоновано метод генерації ПВП на основі ізоморфних перетворень еліптичної кривої та отримані оцінки його стійкості.

Чевардин В.Е., Самойлов И.В., Толстих В.А., Пономарев А.А. Стойкий метод генерации псевдослучайных последовательностей к квантовому криптоанализу. *Определены угрозы квантового криптоанализа для алгоритмов генерации ключей. Полученные оценки времени, необходимого для квантового криптоанализа симметричных и несимметричных криптосистем. Рассмотрены стандартизированный генератор псевдослучайных последовательностей на основе эллиптических кривых, приведена его модель. Для усовершенствования генератора псевдослучайных последовательностей взята каноническая форма эллиптической кривой. Предложен метод генерации на основе изоморфных преобразований эллиптической кривой и полученные оценки его устойчивости.*

V. Chevardin, I. Samoylov, V. Tolstuh, A. Ponomarev The secure pseudorandom sequence generation method to quantum cryptanalysis. *The threats of quantum cryptanalysis for key generation algorithms are identified. Received estimates of the time required for quantum cryptanalysis of symmetric and asymmetric cryptosystems. A standardized deterministic random bit generator (DRBG) based on elliptic curves is considered, and its model is given. To improve the DRBG, the canonical form of the elliptic curve is taken. A method is proposed for generating an elliptic curve on the basis of isomorphic transformations and estimates of its stability obtained.*

Ключеві слова: *генератор псевдовипадкових послідовностей, еліптична крива, ізоморфні перетворення еліптичної кривої, квантовий комп'ютер.*

1. Постановка проблеми та актуальність дослідження

Одну з найважливіших завдань забезпечення конфіденційності, цілісності та доступності інформації в сучасних комп'ютерних системах відіграє криптографія. І слід зауважити, що для безпечної роботи розподілених в просторі інформаційних систем основну роль грають асиметричні криптосистеми. Прикладами таких криптосистем, є RSA з відкритим ключем довжиною 1024 біта, який використовується практично у всіх сучасних інфраструктурах відкритих ключів, алгоритми Ель Гамаля, асиметричні алгоритми, що використовують арифметику еліптичних кривих, що використовуються у фінансовій сфері та електронний документообіг [1]. У зв'язку з цим, методи криптоаналізу асиметричних криптосистем користуються особливою увагою, так як дозволяють оцінити потенційну загрозу злому широко поширених крипто алгоритмів [2]. Однак, часто виникає питання: чи достатній запас має сучасний криптографічні алгоритми і що необхідно робити в разі різкого зростання обчислювальних можливостей сучасного умовного криптоаналитика? У зв'язку з чим, при розробці нових криптографічних алгоритмів і використанні існуючих часто виникає необхідність оцінки їх стійкості в умовах існуючих можливостей і на перспективу. З іншого боку, останнім часом часто виникає також питання, особливо це стосується для такої області як Інтернет речей (Internet of Things), а як можна використовувати криптографічні алгоритми з максимальною компактністю при реалізації і необов'язково високою стійкістю, а лише достатньою для захисту інформації на певному проміжку часу. Такі методи сьогодні прийнято називати легковагова криптографія (Lightweight Cryptography). У першому і в другому випадку, виникає необхідність, по-перше, в оцінці можливої обчислювальної потужності в світі, хоча б на найближче десятиліття, по-друге, в розробці нових алгоритмів криптозахисту. Особливо, це стосується генераторів криптографічних ключів, як основний елемент будь-якого сучасна криптосистеми.

У зв'язку з цим, актуальним питанням є пошук та розробка нових алгоритмів генерації ПВП підвищеної стійкості з урахуванням сучасних і перспективних можливостей потенційного криптоаналитика щодо злому відомих генераторів ПВП.

2. Аналіз загроз квантового криптоаналізу для генерації криптографічних ПВП

Для криптоанализа відомого алгоритму RSA сьогодні використовують методи на основі розкладання великого цілого числа на множники. За сучасним вимогам для алгоритму RSA повинно використовуватися досить велика модульне значення N, де $N = p*q$. Довжина H повинна бути не менше 2048 біт, а значення співмножників р і д повинні бути великими простими числами довгої 1024 біта. До певного часу, без використання квантових алгоритмів, злом таких криптосистеми вважався практично неможливим. Найбільш ефективною для розкладання алгоритмів значення N довжини до +1024 біт сьогодні вважаються метод Ферма, метод (p-1) Поларда, метод ρ-Поларда, метод (p+1) Вільямса та інші [3]. Так, метод факторизації p-1 Поларда дозволив знайти розкладання для таких чисел як $10^{243} – 4*10^{121} – 1$ (M. Tervooren,13.09.2012), $5^{323} + 2^{323}$ (P. Jammes, 06.04.2012), $2^{2098} + 1$ (P. Zimmermann, 28.09.2005) та інші [4, 5, 6]. В роботі Полларда запропоновано виконувати просіювання не в кільці цілих чисел, як в методі квадратичного решета, а в алгебраїчному числовому полі. Це дозволило зменшити складність від 1/2 в методі квадратичного решета до 1/3 в решеті числового поля [3, 6]. За загальними оцінками криптоанализа на основі методу факторизації цей алгоритм вимагає часу порядку $N^{1/3}$.

В основу алгоритмів розв'язання складних теоретичних завдань, таких як факторизація цілого числа, дискретний логарифм в простому полі, дискретний логарифм в групі точок еліптичної кривої закладена фундаментальна здатність інформаційних одиниць квантових комп'ютерів (кубітів) приймати кілька значень одночасно і перебувати в стані „заплутаності" [4, 7]. Це дозволяє проводити обчислення в умовах економії кубітів і отримувати величезну перевагу в обчислювальної швидкості в порівнянні з класичними комп'ютерами, які здатні за один такт процесора виконувати одну 32-розрядну 64-якої розрядна операція. В основу алгоритмів розв'язання складних теоретичних завдань, таких як факторизация цілого числа, дискретний логарифм в простому полі, дискретний логарифм в групі точок еліптичної кривої закладена фундаментальна здатність інформаційних одиниць квантових комп'ютерів (кубітів) приймати кілька значень одночасно і перебувати в стані „заплутаності" [7]. Це дозволяє проводити обчислення в умовах економії кубітів і отримувати величезну перевагу в обчислювальної швидкості в порівнянні з класичними комп'ютерами, які здатні за один такт процесора виконувати одну 32-розрядну або 64-розрядну операцію.

Найбільший інтерес сьогодні викликали можливості квантового комп'ютеру з декількома сотнями логічних кубітів, які здібні здійснити злам криптографічних систем з відкритим ключем. Запропонований Шором алгоритм [7], використовуючи можливості квантового комп'ютерів, здатний вирішувати завдання факторизації числа і дискретного логарифмування за поліноміальний час. Цей результат заснований на використанні квантового паралелізму і зведення задачі до пошуку періоду деякої функції. Розглянемо сутність алгоритму Шора.

Нехай, необхідно розкласти на множники деяке число N, яке використовується в якості модуля для операцій шифрування і розшифрування в криптосистемі RSA. Функція шифрування представлена виразом:

$$F_N(x)=a^x \bmod N, \qquad (1)$$

де $N = p*q$, p і q – великі прості числа, які згідно алгоритму тримаються у секреті.

Для подання числа N необхідно обирати довільне ціле число $a < N$.

Функція (1) є циклічною з періодом П у разі, якщо N – просте, період такої функцій буде обмежений зверху значенням $r = N – 1$. В інших випадках r буде меншим. Визначити простоту N можна швидкими методами визначення простоти N.

Для функції (1) значення періоду зациклення буде r, справедливо наступне:

$$f_N(x + r) = f_N(x) \quad (2)$$

підставимо до рівняння значення функції f_N:

$$a^{(x+r)} mod\ N = a^{(x)} mod\ N, \quad (3)$$

звідки

$$a^r = 1\ mod\ N. \quad (4)$$

Обчислення значення r з виразу (4) є завданням дискретного логарифмування, в даному випадку, на підставі a.

Розкладання числа N на співмножники знаходиться наступним чином.

Якщо r парне, з виразу (4) отримаємо наступне рівняння:

$$(a^{r/2} - 1)(a^{r/2} + 1) = 0\ mod\ N. \quad (5)$$

Оскільки ліва частина ділиться на N, то його співмножники повинні мати спільні з N дільники, які обчислюються за алгоритмом Евкліда (пошуку найбільшого загального дільника). Якщо r непарне або множник в лівій частині вироджується в нуль, слід вибрати інше значення a. Вирішення цього завдання за поліноміальний час невідомо.

За алгоритмом Шора пропонується використовувати квантовий комп'ютер з двома квантовими регістрами довжини n. Причому $M = 2^n > N$, $M \sim N^2$. Результати аналізу відомих робіт [6 – 9] дозволили спрогнозувати потенційну можливість криптоаналитика майбутнього, на основі яких були проведені розрахунки часу, необхідного для криптоаналізу симетричних (табл. 1) та несиметричних криптографічних систем (табл. 2).

Таблиця 1

Ресурси для квантового рішення задачі пошуку ключа симетричної криптосистеми

Криптоаналіз симетричних криптосистем			
Довжина ключа [біти]	Число кубітів	Квантовий час [секунди(роки)]	Середній класичний час [секунди(роки)]
k	*n*	$(\pi/4)\sqrt{2k}$	
57	57	$2.8*10^8$ (9 р.)	$6.39*10^{16}(206*10^7$ р.)
82	82	$1.93*10^{12}(62258$ р.)	$3.03*10^{24}(97*10^{15}$ р.)
113	113	$1.06*10^{17}(34*10^8$ р.)	$9.20*10^{33}(296*10^{24}$ р.)
129	129	$2.76*10^{19}(89*10^{10}$ р.)	$6.03*10^{38}(194*10^{29}$ р.)
258	258	$5.03*10^{38}(162*10^{30}$ р.)	$2.05*10^{77}(66*10^{68}$ р.)

Таблиця 2

Ресурси для квантового рішення задач факторизації та ECDLP

Факторизація			ECDLP			
Довжина числа N [біти]	Число кубітів	Квантовий час [секунди(роки)]	Довжина числа N [біти]	Число кубітів	Квантовий час [секунди(роки)]	Класичний час [секунди(роки)]
n	*2n*	$4n^3$	n	*f(n)*	$360n^3$	
512	1024	$0.54*10^9$(17р.)	110	700	$0.5*10^9$(16р.)	$6.39*10^{16}(206*10^7$р.)
1024	2048	$4.3*10^9$(138р.)	163	1000	$1.6*10^9$(51р.)	$3.03*10^{24}(977*10^{15}$р.)
2048	4096	$34*10^9$(1096р.)	224	1300	$4.0*10^9$(129р.)	$9.20*10^{33}(296*10^{24}$р.)
3072	6114	$120*10^9$(3870р.)	256	1500	$6.0*10^9$(193р.)	$6.03*10^{38}(194*10^{29}$р.)
15360	30720	$1.5*10^{13}(48*10^4$р.)	512	2800	$50*10^9$(1612р.)	$2.05*10^{77}(66*10^{68}$р.)

З урахуванням наведених можливостей квантового криптоаналізу деякі криптографічні системи, особливо це стосується несиметричних криптосистем, стають уразливими. А враховуючі, що сучасні стандарти [11] побудовані з використанням асиметричних криптопримітивів виникає загроза практично більшості систем криптографічного захисту інформації. Розглянемо деякі найбільш відомі генератори ПВП та оцінимо їх уразливість.

Стандартизованими способами генерації ПВП є генератори ПВП, які називаються Deterministic random bit generator (DRBG) [9 – 11]. У рекомендаціях стандарту наведені різні способи генерації ПВП на основі геш-функцій, блочно-симетричних алгоритмів шифрування [11]. Особливе місце серед усіх алгоритмів займають генератори на основі теоретико-складної задачі математики – дискретному логарифмуванні в групі точок еліптичної кривої (ЕК) (рис. 1).

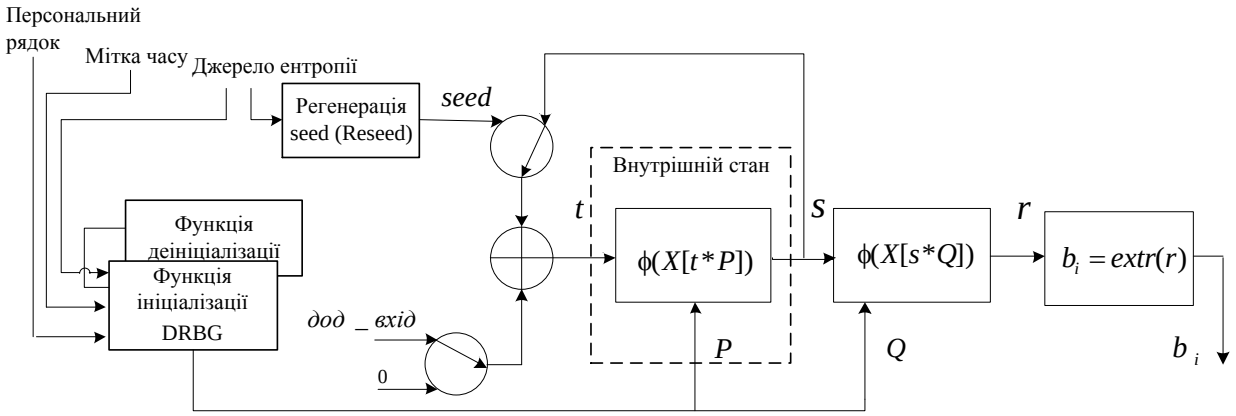

Рис. 1. Функціональна модель генератора Dual_EC_DRBG

Для оцінки стійкості генераторів ПВП згідно [11] введені показники:

– стійкість до відтворення (backtracking resistance),

– стійкість до передбачення (prediction resistance),

– криптографічна стійкість (security strength),

– число кроків до зациклення генератору, показник який визначає величину періоду ПВП. Для генераторів (рис. 1) число кроків до зациклення складається з двох значень: періоду зациклення та передперіоду. Для спрощення подання результатів ми будемо використовувати показник числа кроків до зациклення генератору.

Нехай значення *NT* – число кроків до зациклення стандартизованого генератору. Значення *NT* показує кількість різноманітних значень внутрішнього стану генератору, яке також визначає потужність простору вхідних значень, *s* для другого множення $s*Q$ та визначає стійкість до зламу генератора ПВП.

Враховуючи, що внутрішній стан генератора є значенням $X[t_i * P]$, яке для кривої (1) не перебільшує $n/2$, а період ПВП в цьому випадку буде визначений значенням *NT* тобто числом значень t_i. Значення t_i отримуються з виразу $X[t_i * P]$, тобто їх кількість буде не більше $n/2$.

Збільшення числа внутрішніх станів без витрат часу є загально відомою проблемою, яка набуває більшої актуальності в умовах бурхливого розвитку квантових комп'ютерів. У зв'язку з цим, розробка нових методів генерації ПВП на основі відомої стандартизованої моделі генераторів за рахунок використання відомого підходу до збільшення числа внутрішніх станів генератора на основі ізоморфних трансформацій еліптичної кривої є одним з можливих шляхів подальшого розвитку криптографічних генераторів цього класу.

3. Необхідні для вирішення завдання положення теорії еліптичних кривих

Гладкою (неособливою) еліптичною кривою порядка *n* над полем F_p називається множина точок $(X, Y), X, Y \in F_p$, які задовольняють рівнянню $F(X,Y) = 0$, де $F(X,Y)$ багаточлен ступені[1] *m* з коефіцієнтами з F_p. Така крива не повинна мати особливих точок, в яких $\frac{\partial F}{\partial X} \neq 0, \frac{\partial F}{\partial Y} \neq 0$.

[1] Ступінь багаточлена є максимальна степінь одночленів, з яких він складається.

Множина точок еліптичної кривої разом з точкою на нескінченності з операцією додавання[2] є абелевою групою.

Для кожної еліптичної кривої обчислюється дискримінант $\Delta(E)$ та *j*-інваріант. Для криптографічних цілей використовують лише криві с $\Delta(E) \neq 0$, $j \neq \{0, 12^3\}$. Вимога $j \neq \{0, 12^3\}$ дозволяє позбавитись використання суперсингулярних кривих.

Нормальною формою еліптичної кривої на над полем F_p, називається крива виду:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \quad (6)$$

Коли коефіцієнти a_1, a_2, a_3 дорівнюють нулю, крива (6) може бути представлена в канонічній формі (або скороченій формі Веєрштрасса):

$$y^2 = x^3 + a_4x + a_6,\ a_4, a_6 \in F_p. \quad (7)$$

Лінійна ізоморфна трансформація координат цієї кривої в канонічній формі задається формулами:

$$y = u^3\bar{y} + su^2\bar{x} + t,\ x = u^2\bar{x} + r,\ u \neq 0,\ r, s, t \in \{0, ..., p-1\}.$$

Лінійна ізоморфна трансформація не змінює значення інваріанту, тобто всі ізоморфні криві мають однаковий інваріант. Коли трансформація має параметри $u = \{1, ..., p-1\}, r = 0, s = 0, t = 0$ ($a_1 = 0, a_2 = 0, a_3 = 0$) крива залишається в канонічній формі.

В такому випадку лінійна ізоморфна трансформація для кривої (7) має вид:

$$y = u^3\bar{y},\ x = u^2\bar{x},\ u = \{1, ..., p-1\}. \quad (8)$$

Враховуючи конструктивні особливості існуючих підходів до побудови генераторів ПВП на основі еліптичної кривої [11], розглянемо новий метод формування ПВП на основі ізоморфних трансформацій канонічної форми еліптичної кривої в канонічну.

4. Метод генерації ПВП на основі ізоморфних трансформацій точок ЕК. Нехай базова еліптична крива задана у канонічній формі, E_p. Ізоморфні трансформації цієї кривої подані виразом (8). Для опису алгоритму генерації зафіксуємо наступні операції: отримання ізоморфної базової точки $P_i = \varphi_i(P)$, отримання раундової точки кривої, $f(P_{i-1}, P_i) = P' = t_i * P_i$, перетворення координати X в бітову послідовність, $r_i = \phi(X[P_i])$, компресія бітової послідовності в блок біт $b_i = extr(r_i)$ (один біт) згідно [11].

Початок алгоритму.

Встановлюється початковий стан генератора: характеристика *p* поля Галуа, коефіцієнти базової кривої, базові точки *P* й *Q*, довжина ПВП.

Крок 1. Для забезпечення стійкості до передбачення скалярне число отримуємо на основі секретного числа *seed*, $(seed, n) = 1$. Число *t* визначається:

$$t = \omega'^{seed} \bmod n, \quad (9)$$

де *t* – генератор групи Z_n, *n* – порядок циклічної групи точок *P* й *Q* (просте число), ω' – генератор групи Z_n, *seed* – секретне число.

Крок 2. Обчислення значення раундового скаляра t_i наступним чином:

$$t_i = t * t_{i-1} \bmod n. \quad (10)$$

Крок 3. Обчислення значення u_i:

$$u_i = \omega^{2i} \bmod p, \quad (11)$$

де ω – генератор групи Z_p, *p* – характеристика поля Галуа.

---

[2] $P_{i-1}(x_{i-1}, y_{i-1}) + Q_j\ (x_{Q_j}, y_{Q_j}) = P_i\left(\frac{y_{i-1} - y_{Q_j}}{x_{i-1} - x_{Q_j}} - x_{Q_j} - x_{i-1}, -y_{Q_j} + \frac{y_{i-1} - y_{Q_j}}{x_{i-1} - x_{Q_j}}(x_{Q_j} - x_i)\right)$.

Крок 4. Розрахунок значень координат ізоморфної точки P_i: $x_{P_i} = u_i^{\,2}\bar{x} \bmod p$, $y_{P_i} = u_i^{\,3}\bar{y} \bmod p$.

Крок 5. Розрахунок значення внутрішнього стану генератора:

$$r_i = X[t_i \underset{scalmull}{*} P_i] = X[t_i \underset{scalmull}{*} \varphi_i(P)]. \quad (12)$$

Крок 6. Отримання бітового блока (біт) з послідовності r_i:

$$b_i = extr(r_i). \quad (13)$$

Кінець алгоритму.

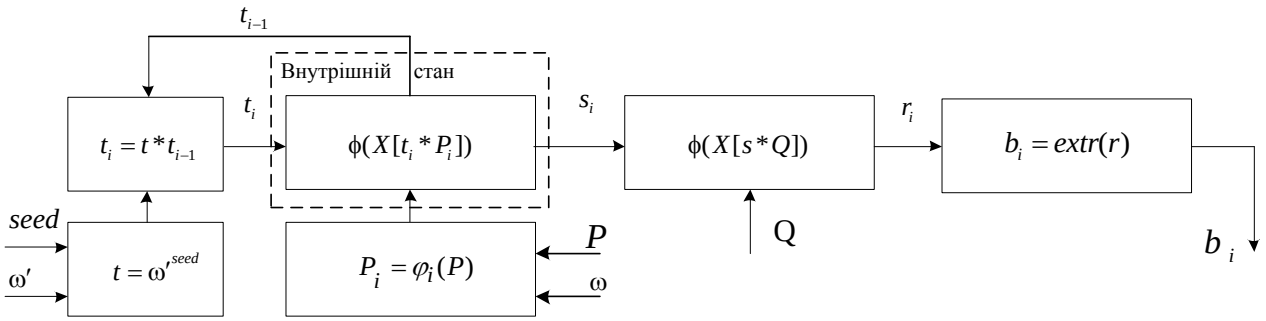

Рис. 2. Модель модифікованого генератора Dual_EC_DRBG

Підставимо в вираз (13) вирази (8 – 12) отримаємо загальний вираз генератора:

$$r_i = \phi(X\left[\phi\left(X\left[\omega'^{seed} * t_{i-1} (\bmod n) \underset{scalmull}{*} (\omega^{4i} * X_P (\bmod p), \omega^{6i} * Y_P (\bmod p))\right]\right) \underset{scalmull}{*} Q\right]). \quad (14)$$

5. Оцінка виграшу розробленого методу генерації ПВП у порівнянні з існуючим стандартизованим підходом. Враховуючи граничні значення числа ізоморфізмів ЕК у канонічній формі, $NT = 1/2(p-1)$, число внутрішніх станів модифікованого генератора Dual_EC_DRBG визначено:

$$NT = 1/2(p-1) * n, \quad (15)$$

де n – порядок циклічної групи точок кривої, p – характеристика поля Галуа.

Скаляр t_i пробігає усі елементи Z_n, внаслідок чого $P_i = t_i * P$, $P_i \in E^i{}_p$ (E_p^i – ізоморфна група). Параметр u_i пробігає усі значення від'ємників у полі, число яких NT. У такому випадку, період послідовності значень $X[P_i] = X[t_i * \varphi_i(P)]$, які потрапляють у якості скалярів на вхід $s*Q = X[P_i]*Q$, буде дорівнювати *NT*. Період ПВП у такому випадку буде дорівнювати *NT*.

Для передбачення наступного блоку біт на виході генератору нападнику необхідно обчислити значення $s_i * Q$, для чого йому необхідно отримати точку P_i' й скаляр t_i. Для цього йому необхідно здійснити пошук параметра t, який використовується в скалярному добутку $\omega'^{seed} * t_{i-1} (\bmod n) \underset{scalmull}{*} P_{\varphi_i}$. Для t_i необхідно знайти значення *seed*. Враховуючи, що ω' – генератор Z_n, число генераторів дорівнює $n_{\omega'} = \varphi_{Oiler}(\varphi_{Oiler}(n))$. Наприклад, для забезпечення стійкості до передбачення генератора ПСП еквівалентної значенню 2^{256} необхідно використовувати циклічну групу точок, порядок якої є 257-бітним числом. Більш детальний аналіз стійкості запропонованого методу буде проведено в подальшій роботі.

Висновки

Таким чином, при широкому розповсюдженні квантових комп'ютерів рішення задачі ECDLP буде можливо за 51 рік, коли існуючі можливості дозволяють її вирішити приблизно за 10^{15} років. Слід врахувати, що одна з складнощів використання квантового комп'ютеру це проведення аналізу та вимірів різних квантових станів, що накладає суттєві обмеження на таку крипто аналітичну систему. Значення часу рішення задачі факторизації для інших параметрів алгоритмів наведені в таблицях 1 та 2. В таких умовах, одним з варіантів рішення наукового завдання було обрано збільшення періоду генераторів ПВП з метою отримання запасу стійкості генераторів ПВП до зростаючих можливостей квантових комп'ютерів в світі. Було запропоновано метод генерації ПВП на основі відомого підходу з використанням ізоморфних перетворень еліптичних кривих. Отриманий метод дозволив у $1/2(p-1)$ разів збільшити число внутрішніх станів стандартизованного генератора, що дозволяє підвищити стійкість генератора ПВП пропорційно характеристики поля p. При фіксованому значенні числа внутрішніх станів стандартизованного генератора розроблений генератор дозволяє скоротити бітову довжину характеристики p поля та підвищити його швидкодію. В подальшому, підхід до використання ізоморфних перетворень може бути застосований для побудови алгоритмів генерації криптографічних ключів в легковагової криптографії, в криптографічних системах, які використовуються в інформаційно-телекомунікаційних системах критичної інфраструктури.

ЛІТЕРАТУРА

1. Thurimella R. Cryptography for Cyber Security and Defense: Information Encryption and Cyphering / R. Thurimella and L. C. Baird III // IGI Global, 2009, chapter title: „Network Security".

2. Богданов А.Ю. Квантовые алгоритмы и их влияние на безопасность современных классических криптографических систем / Богданов А.Ю. Кижватов И.С // РГГУ ФЗИ (2005) – С. 18.

3. Bai S. Better polynomials for GNFS / Bai, S., Bouvier, C., Kruppa, A., Zimmermann, P. // Mathematics of Computation 85. – 2016. – P. 861 – 873.

4. Shor P. W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer // Foundations of Computer Science : Conference Publications. – 1997. – P. 1484 – 1509.

5. Web: https://members.loria.fr/PZimmermann/records/Pminus1.html

6. Валиев К.А. Квантовые компьютеры и квантовые вычисления/ Валиев К.А.// Физико-технологический институт РАН (2004) – С. 37.

7. Shor P. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, in Proc./ Shor P.W. // IEEE Computer Society Press 1994. – P. 31.

8. Kaliski Jr. B. S. A pseudo-random bit generator based on elliptic logarithms / B. S. Kaliski Jr. // Advances in Cryptology: Proceedings of Crypto '86 (Lecture Notes in Computer Science, vol. 263), Springer-Verlag, New York, 1987, pp. 84 – 103.

9. Impagliazzo R. Pseudo-random generation from one-way functions / R. Impagliazzo, L. Levin, and M. Luby // Proceedings of the 21st Annual ACM Symposium on Theory of Computing, ACM, New York, 1989, pp. 12 – 24.

10. Gjøsteen K. Comments on Dual-EC-DRBG/NIST SP 800-90, Draft December 2005 / Kristian Gjøsteen // March 16, 2006.

11. NIST Special Publication 800-90A. Recommendation for Random Number Generation Using Deterministic Random Bit Generators / Elaine Barker, John Kelsey // Computer Security Division Information Technology Laboratory National Institute of Standards and Technology. – January 2012.