УДК 681.3.06

ОЦІНКА ЗАХИЩЕНОСТІ АСИМЕТРИЧНИХ КРИПТОГРАФІЧНИХ ПЕРЕТВОРЕНЬ ВІД АТАК ТИПУ «ПОВНЕ РОЗКРИТТЯ»

І.Д. ГОРБЕНКО, І.Ф. АУЛОВ

Запропонована методика теоретичної оцінки рівня захищеності асиметричних криптографічних перетворень, яка дозволяє оцінити рівень стійкості асиметричних систем шифрування інформації з урахуванням досягнень в сфері криптоаналізу та обчислювальної техніки. Наводиться результати оцінки рівня захищеності асиметричних криптографічних перетворень від атак типу «повне розкриття» для відрізку часу.

Ключові слова: асиметричні криптосистеми, алгоритми факторизації, оцінка стійкості.

ВСТУП

Поняття інформаційної безпеки безпосередньо пов'язано з політичною, економічною, оборонною та іншими складовими національної безпеки держави. Сучасний інформаційний світ все більше зазнає шкоди від поширення комп'ютерної злочинності. Комп'ютерні злочинці наносять значні економічні збитки власникам комп'ютерних систем в разі отримання несанкціонованого доступу до цих систем. На сьогодні криптографічний захист інформації в Україні здебільшого використовується для захисту фінансово-кредитної сфери. Впровадження глобальної системи електронних платежів, електронних грошей, Інтернет-банкінгу потребує від держави впровадження та використання стандартів, використання яких задовольняло б загальновизнаному в світі рівню безпеки.

Використання асиметричних криптографічних перетворень пов'язано з цілою низкою задач: направленого шифрування, електронного цифрового підпису, протоколах розподілу загального секрету та встановлення ключів, протоколах, що забезпечують конфіденційність, цілісність інформації, що передається, автентичність взаємодіючих сторін, спостережливість в системі в цілому. Асиметричні криптографічні системи за рахунок використання пари ключів: відкритого та особистого володіють безумовною перевагою в тому, що немає необхідності в обміні особистими ключами, що значно підвищує загальний рівень захищеності системи.

Системи шифрування та підпису типу RSA, DSA в наш час піддаються критиці, проте широко використовуються на практиці, та є частинами міжнародних стандартів. В свою чергу системи реалізовані в групі точок еліптичної кривої мають більший рівень захищеності проте є більш складними в реалізації та мають менші показники по швидкодії. На сьогодні асиметричні криптографічні системи, реалізовані на основі перетворень в кільці цілих чисел, скінченому полі, групі точок еліптичної кривої не можуть гарантувати стійкість за умови появи квантових комп'ютерів. Перспективними в цьому плані можуть стати системи побудовані в кільці усічених поліномів, наприклад криптосистеми NTRU. Тому зараз є актуальною задачею порівняти рівень стійкості цих систем з урахуванням подальшого розвитку обчислювальної техніки, а також досягнень в криптографії.

1. ВИЗНАЧЕННЯ

Асиметричні криптоперетворення – це клас перетворень, властивістю яких є наявність пари ключів $K_{особ}$ та відповідного йому $K_{відкр}$. Необхідною умовою в асиметричних криптосистемах є не менше, ніж субекспоненційна складність вирішення задачі знаходження особистого ключа за умови знання відповідного йому відкритого, а також загальносистемних параметрів.

Асиметричні перетворення прийнято поділяти за їх математичними властивостями на наступні групи[1,2] :

– асиметричні перетворення в кільці цілих чисел (RSA);

– асиметричні перетворення в полі (DSA);

– асиметричні перетворення в групі точок еліптичної кривої (EC-DSA);

– асиметричні перетворення в кільці усічених поліномів (NTRUEncrypt, NTRUsign).

Для порівняння стійкості асиметричних криптографічних перетворень здебільшого користуються оцінками складності до знаходження особистого ключа.

Найбільш ефективнішою атакою для RSA є факторизація модуля перетворення за допомогою метода загального решета числового поля(GNFS). Цей метод має складність, яка оцінюється як:

$$O(e^{(1.9229+O(1))*\ln(n)^{1/3}*\ln(\ln(n))^{2/3}}). \qquad (1)$$

Аналогічну субекспоненційну складність має задача дискретного логарифму в полі для здійснення атаки на алгоритм DSA за допомогою метода загального решета числового поля(GNFS).:

$$O(e^{(1.9+O(1))*\ln(n)^{1/3}*\ln(\ln(n))^{2/3}}). \qquad (2)$$

Найбільшою – експоненційною складністю володіє задача дискретного логарифму в групі точок еліптичної кривої. Складність вирішення цієї задачі за допомогою методу ρ-Полларда оцінюється як:

$$O(\sqrt{\frac{\pi n}{4}} + O(\log n)). \quad (3)$$

Аналогічно, експоненційну складність має задача криптоаналізу в кільці усічених поліномів, вирішення задач пошуку найкоротшого та найближчого вектору, використовуючи алгоритм LLL (Lenstra, Lenstra and Lovasz), складність якого оцінюється як:

$$O(\sqrt{\frac{n}{2}} + O(\log n)). \quad (4)$$

Асиметричні криптосистеми в кільці цілих чисел, скінченому полі, групі точок еліптичної кривої детально розглянуті та вивчені [1-4], найбільший інтерес представляє асиметричні криптосистеми, засновані на математиці в кільці усічених поліномів, бо вони мають експоненційну складність криптоаналізу та вважаються стійкими до квантових алгоритмів криптоаналізу. Розглянемо принципи побудови такої системи на прикладі криптосистеми NTRUEncrypt [5]. NTRUEncrypt – це асиметрична криптографічна система, яка була розроблена математиками Дж. Хофстейном, Дж. Піфером та Дж. Сильверманом у 1996 році. Зараз ця криптосистема є запатентованою та права на неї належать компанії Security Innovation.

Параметри криптосистеми NTRUEncrypt:

– $R = (\boldsymbol{Z}/q\boldsymbol{Z})[X]/(X^N - 1)$ – кільце усічених многочленів в якому виконуються базові операції над поліномами;

– N – розмір усіченого кільця многочленів. елементами кільця є поліноми ступеня $N-1$ з цілими коефіцієнтами:

$$a = a_0 + a_1X + a_2X^2 + ... + a_{N-1}X^{N-1} \quad (5)$$

– модуль p ($p = 3$) – невелике ціле число, використовується при генерації ключів та при генерації «маскуючого» (blinding) поліному;

– модуль q ($q = 2^{11}$) – достатньо велике ціле число використовується для визначення усіченого кільця многочленів $(\boldsymbol{Z}/q\boldsymbol{Z})[X]/(X^N - 1)$. Модуль q обирається таким чином, щоб не мати спільних дільників з модулем p;

– індекс c – постійний коефіцієнт, який використовується в алгоритмі генерації «маскуючого» полінома r. Для кожного N, c – є постійним та обирається для зменшення кількості необхідних бітів виходу псевдовипадкового генератору;

– d_f, d_g – кількість 1 та -1 в особистому ключі користувача f та тимчасовому поліному g.

– (f,h) – особистий та відкритий ключі;

Алгоритм генерації ключової пари:

Вхід: N, q, p, d_f, d_g, c;

Вихід: Асиметрична пара (f ,h).

1. Встановити поліном $F = 0$.

2. Встановити $t = 0$.

3. Доки $t < d_f$ виконати наступні кроки

a. Згенерувати за допомогою випадкового генератора ціле число $i \bmod N$.

b. Якщо $F_i = 0$

i. Встановити $F_i = 1$

ii. Встановити $t = t + 1$

4. Встановити t=0. Доки $t < dF$ виконати наступні кроки

c. Згенерувати за допомогою випадкового генератора ціле число $i \bmod N$.

d. Якщо $F_i = 0$

iii. Встановити F_i= -1

iv. Встановити $t = t + 1$

5. Обчислити поліном $f = 1 + p*F$ в кільці $(\boldsymbol{Z}/q\boldsymbol{Z})[X]/(X^N - 1)$

6. Обчислити поліном: f^{-1} (f^{-1} такий що $f^{-1}*f = f*f^{-1} = 1$) в кільці $(\boldsymbol{Z}/q\boldsymbol{Z})[X]/(X^N - 1)$. Якщо f^{-1} не існує перейти до кроку 1.

7. Встановити поліном $g = 0$.

8. Встановити $t = 0$.

9. Доки $t < d_g + 1$ виконати наступні кроки

a. Згенерувати за допомогою випадкового генератора ціле число $i \bmod N$.

b. Якщо $g_i = 0$

i. Встановити $g_i = 1$

ii. Встановити $t = t + 1$

10. Встановити $t = 0$

11. Доки $t < d_g$ виконувати

a. Згенерувати за допомогою випадкового генератора ціле число i mod N.

b. Якщо $g_i = 0$

i. Встановити g_i = -1

ii. Встановити $t = t + 1$

12. Перевірити, що для g існує $g^{-1} \bmod q$, якщо ні перейти до кроку 8.

13. Обчислити поліном $h = f^{-1}*g*p$ in $(\boldsymbol{Z}/q\boldsymbol{Z})[X]/(X^N - 1)$

14. Вихід f, h.

Алгоритм зашифрування повідомлення:

Вхід: N, q, r, відкритий ключ одержувача h, представлення повідомлення у вигляді полінома m, поліном для «маскування» r.

Вихід: Зашифроване повідомлення – поліном e.

1. Обчислити поліном $e = r*h+m(\boldsymbol{Z}/q\boldsymbol{Z})[X]/(X^N-1)$.

2. Вихід зашифроване повідомлення – e.

Алгоритм розшифрування повідомлення:

Вхід: N, q, p особистий ключ одержувача f, зашифроване повідомлення e, коефіцієнт нижньої границі розшифрування A.

Вихід: Можливе повідомлення – поліном m', в деяких випадках $m \neq m$`.

1. Обчислити $a := f*e$ in $(\boldsymbol{Z}/q\boldsymbol{Z})[X]/(X^N - 1)$ з коефіцієнтами, приведеними за модулем з інтервалу $[A, A + q - 1]$.

2. Обчислити $m' = a \bmod p$

2. ТЕХНІЧНА БАЗА ДЛЯ ЗДІЙСНЕННЯ КРИПТОАНАЛІЗУ

Оцінку потужності сучасного стану обчислювальної техніки подамо, використовуючи наступні показники:

– кількість операцій с плаваючою точкою за секунду(FLoating point OPerations per Second, FLOPS);

– кількість інструкцій в секунду (Instructions per second, IPS Million Instructions per Second (MIPS));

– кількість інструкцій процесору за рік (MIPS-Year, 1 MIPS-Year).

Задачі криптоаналізу можуть вирішуватися з використанням різних комп'ютерних систем: суперкомп'ютерів, локальних мереж та мережі Інтернет, персонального комп'ютера, спеціалізованих обчислювальних процесорів, графічних карт. В сучасному світі найбільші обчислювальні потужності суперкомп'ютерів, що можуть бути використані для вирішення задач криптографії сконцентровані у США (рис. 1).

В якості апаратного засобу, що використовується для криптоаналізу, може бути використано графічну карту або процесор комп'ютера. За рахунок апаратного розпаралелювання графічні адаптери персональних комп'ютерів мають більшу потужність, отже є ефективнішими в порівнянні з центральним процессором. Спеціально для вирішення задач факторизації чисел ізраїльськими вченими під керівництвом Аді Шаміра було розроблено апаратні засоби TWINKLE та TWIRLE, які апаратно реалізують найбільш швидкі алгоритми факторизації. За результатами їх досліджень, час факторизації модуля довжиною 1024 біта становить приблизно рік та коштує 10 мільйонів доларів, що набагато менше, ніж використання суперкомп'ютеру, ціна якого становить близько 100 мільйонів доларів. В табл. 1 наведено данні щодо необхідної кількості років, для здійснення криптоаналізу RSA.

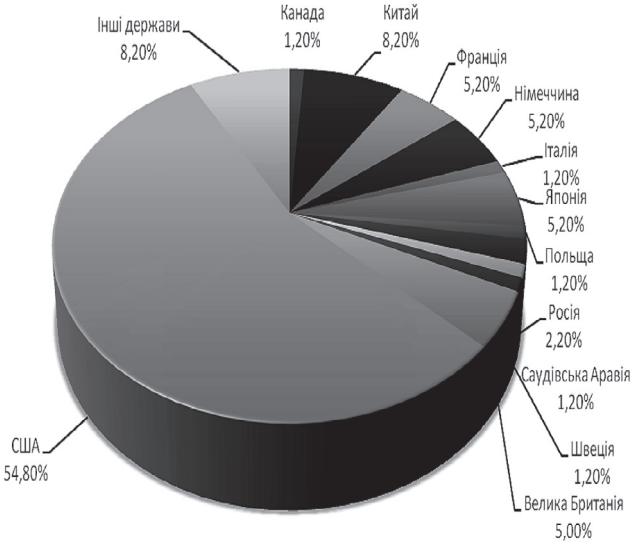

Рис. 1. Розподілення потужностей суперкомп'ютерів в світі

Існуючі квантові алгоритми для вирішення задач дискретного логарифму та факторизації, дозволяють вирішувати ці задачі за менший час, але за відсутності квантових комп'ютерів з заданою кількістю кубітів вирішення цих задач має експоненційний час. В табл. 2 наведені оцінки складності методів за умови існування квантового комп'ютера.

Таблиця 1

Оцінка вартості та часу криптоаналізу модуля RSA

Оцінка ціни криптоаналізу	Кількість/ Ціна тис. дол.	Потужн., Tflops	Кількість років, потрібних для криптоаналізу модуля RSA, біт					Об'єм пам'яті RAM/HDD, ТБ
			768	1024	2048	3072	15360	
Суперкомп'ютер (Tianhe-1A)	1/90000	2566	$7,8*10^{-3}$	1,93	$2,3*10^{9}$	$9,1*10^{15}$	$2,3*10^{55}$	0,229/1000
Апаратні засоби (TWIRL)	194/10000	12000	$8,3*10^{-4}$	1,03	$1,2*10^{9}$	$4,9*10^{15}$	$4,9*10^{55}$	Знаходиться в засобі
Розподілені комп'ютери мережі в Internet	73314/29325	2565	$3,9*10^{-3}$	4,83	$5,9*10^{9}$	$2,3*10^{16}$	$5,8*10^{55}$	100/1000
Звичайний комп'ютер	1/0,5	0,035	1140	$1,4*10^{6}$	$1,7*10^{16}$	$6,7*10^{21}$	$1,7*10^{61}$	0,002/1
Квантовий комп'ютер	1/-	-	$2*10^{-13}$	$42*10^{-9}$	4,08	$5,6*10^{7}$	$1,8*10^{49}$	Вимірюється в кубітах
Графічний адаптер	1/0,7	0,936	42,7	$5,3*10^{4}$	$6,4*10^{13}$	$2,5*10^{20}$	$6,3*10^{59}$	0,002/1

Таблиця 2

Порівняння квантових алгоритмів розв'язку проблеми логарифмування в групі точок ЕК та факторизації

Алгоритми факторизації (RSA)			Вирішення задачі дискретного логарифму в групі точок ЕК			Класичний алгоритм
n	≈ кількість кубітів	час	N	≈ кількість кубітів	час	час
	2n	$4n^3$		$f(n)$ $(f(n))$	$320n^3$	
512	1024	$0.54*10^{9}$	110	700(800)	$0.5*10^{9}$	C*
1024	2048	$4.3*10^{9}$	163	1000(1200)	$1.6*10^{9}$	$C*10^{8}$
2048	4096	$34*10^{9}$	224	1300(1600)	$4.0*10^{9}$	$C*10^{17}$
3072	6144	$120*10^{9}$	256	1500(1800)	$6.0*10^{9}$	$C*10^{22}$
15360	30720	$1.5*10^{13}$	512	2800(3600)	$50*10^{9}$	$C*10^{60}$

3. ІСНУЮЧІ ДОСЯГНЕННЯ КРИПТОАНАЛІЗУ

Для порівняльного аналізу існуючих асиметричних крипто алгоритмів є дуже важливим знати сучасні досягнення в криптоаналізі цих алгоритмів. Наведемо в табл. 3, існуючі досягнення в області криптоаналізу з зазначенням року, коли було здійснено криптоаналіз, довжини ключа, часу, який був витрачений на здійснення криптоаналізу, виміряний в MIPS-Year та необхідної пам'яті, яка була використана в процесі криптоаналізу[7].

Таблиця 3

Досягнення криптоаналізу

Рік	Довжина ключа, біт	Час, MIPS-Year	Пам'ять ОЗУ/ HDD, Гб
RSA			
1999	512	8000	0,064/2,3
2005	663	$0{,}128*10^6$	1/35
2009	768	$4*10^6$	5/1000
DSA			
2001	607	20000	0,256 /5
2011	907	$2{,}775*10^8$	1/35*
EC-DSA			
2001	109	13100	1/400
2009	112	36557	0,512/600
NTRU			
2009	$N = 167$	$2*10^6$	2/150

Практичні результати отримані в результаті здійснення криптоаналізу відповідних криптоперетворень надають можливість в подальшому використовувати їх для отримання оцінок для криптоаналізу цих перетворень.

Засновуючись на даних, отриманих в результаті експерименту, можна надати близьку оцінку щодо можливості криптоаналізу, використовуючи наведені співвідношення.

а) Оцінка часу криптоаналізу. Якщо відомий час t – необхідний для криптоаналізу алгоритму з довжиною ключа n, тоді час для довжини ключа m розраховується як:

$$t_m \approx t_n \frac{L[m]}{L[n]}, \qquad (6)$$

де L[v] – оцінка складності криптоаналізу алгоритму з довжиною ключа n, L[m] – оцінка складності алгоритму з довжиною ключа m.

Для асимметричного алгоритму типу RSA та DSA, вона дорівнює:

$$L[n,u,v] = O(e^{(v+O(1))*\ln(n)^u*\ln(\ln(n))^{1-u}}). \qquad (7)$$

Для алгоритму EC-DSA оцінка має вигляд:

$$L[n] = O(\sqrt{\frac{\pi n}{4}} + O(\log n)). \qquad (8)$$

В результаті специфіки арифметики в групі точок еліптичної кривої співвідношення (6) може бути надано у вигляді:

$$t_m = 10^{-5} \frac{\sqrt{n}}{l*\sqrt{m}M}, \qquad (9)$$

де n – довжина модуля, для якого необхідно знайти час, l – кількість операцій додавання/множення точки еліптичної кривої, M – кількість процесорів,m – довжина модуля перетворення, для якого час криптоаналізу відомий.

б) Оцінка необхідної пам'яті для виконання криптоаналізу (10).

$$Mem_m = Mem_n \sqrt{\frac{L[m]}{L[n]}}; \qquad (10)$$

в) Оцінка часу криптоаналізу для процесора.

$$t_{years} = \frac{t_m[MIPSYears]}{N[MIPS]} = \frac{t_m[MIPSYears]}{4N[MFLOPS]}, \qquad (11)$$

де t_m – час, необхідний для криптоаналізу в MIPS-Year, N – кількість операцій в секунду процесору (в MIPS (або MFLOPS)).

В 1965 році Гордон Мур на основі емпіричних даних зробив прогноз стосовно збільшення потужності обчислювальних пристроїв, який сформулював в наступний закон: «Кількість елементів, що розташовуються в корпусі мікросхеми, кожного року зростає вдвічі, разом з цим вдвічі зростає і кількість елементарних операцій, що може виконувати мікросхема.

На основі цього закону та емпіричних даних щодо криптоаналізу побудуємо криву (рис. 2), що відображає зростання обчислювальної потужності комп'ютерів та довжини відповідних параметрів, для яких буде виконана задача криптоаналізу, за наступними правилами:

– точку початку оберемо1965 рік, як рік, в якому було зроблено припущення Муром про експоненційне зростання можливостей обчислювальної техніки;

– потужність мікропроцесору в 1965 році приймемо за 1, при цьому з 1975 року ріст обчислювальної потужності процесорів став уповільнюватися та зростав в два рази за 2 роки;

– апроксимаційні оцінки криптоаналізу асиметричних перетворень були побудовані з використанням даних щодо фактично атакованих довжин модулів.

Засновуючись на побудованих графіках, можна зробити висновок, що при виконанні закону Мура в наступні 15-20 років стійкість RSA та DSA не буде забезпечуватися використанням більшого модуля перетворення, кожні два роки необхідно буде збільшувати модуль перетворення не менше, ніж в 2 рази. Цей графік використовує лише досягнення обчислювальної техніка та реальні результати здійснення успішних атак. Якщо врахувати ймовірності покращення криптоаналітичних атак, а також появу квантових комп'ютерів, то можна зробити висновок, що RSA та DSA криптографічні примітиви не будуть спроможні забезпечити рівень захисту, який вони мають зараз.

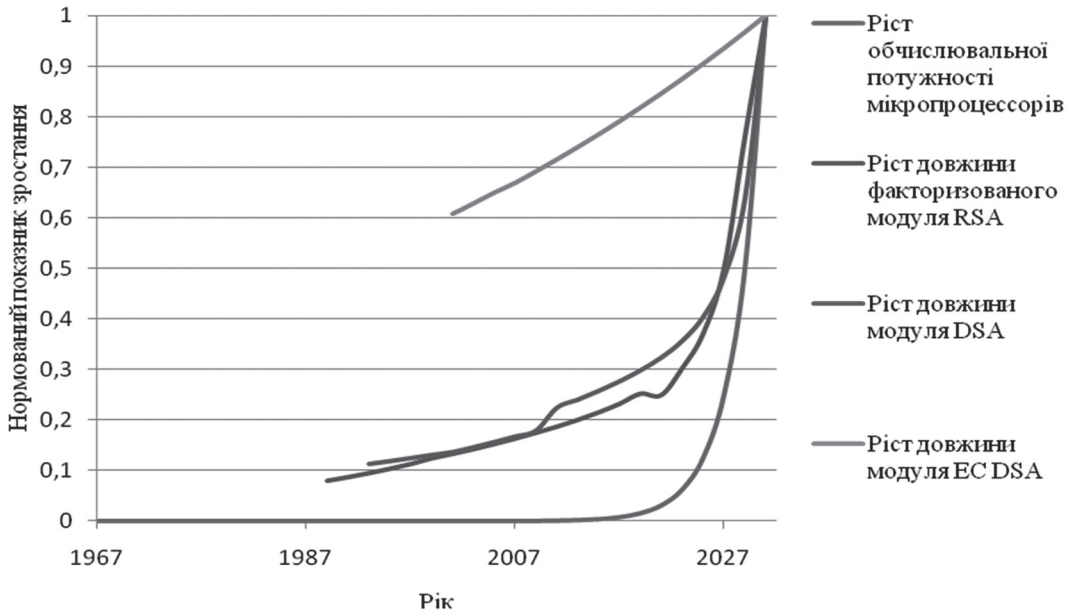

Рис. 2. Зростання обчислювальної можливості мікропроцесорної техніки, та довжини модуля різних криптографічних примітивів за роками

4. МЕТОДИКА ОБРАННЯ КЛЮЧОВИХ ПАРАМЕТРІВ

Як було вже показано для кожної криптосистеми, можна описати час та затрати, необхідні для здійснення вдалої атаки. За умови збереження сучасних тенденції розвитку обчислювальної техніки та методів криптоаналізу, використання рекомендацій з цієї методики дозволить забезпечити достатній рівень безпеки для використання криптографії в комерції.

Визначення довжини асиметричного ключа

Для визначення кількості обчислень IMY необхідних для криптоаналізу в конкретному році використовується наступна формула:

$$IMY(y) = 5*10^5 * 2^{12(y-s)/m} * 2^{t(y-s)/b}[MipsYears],$$

де $5*10^5$ кількість операцій, яка була необхідна для криптоаналізу DES; $2^{12(y-s)/m}$ – рівень зростання потужності процесорів з року s до року y; $2^{t(y-s)/b}$ – рівень зростання фінансових можливостей криптоаналітика.

Асиметричний ключ для перетворення в кільці цілих чисел для року y обирається згідно наступної формули:

$$\frac{L[2^k]}{IMY(y)*2^{12(y-1999)/r}} \geq \frac{L[2^{512}]}{10^4}, \qquad (12)$$

де $L[2^k]$ – довжина ключа в бітах; $2^{12(y-1999)/r}$ – рівень зростання потужності факторизації з 1999 року.

Асиметричний ключ для перетворення в групі точок еліптичної кривої обирається згідно правила:

$$\frac{2^{u/2}*u^2}{IMY(y)*C} \geq \frac{2^{109/2}*109^2}{2.2*10^6}. \qquad (13)$$

Використовуючи наведені співвідношення та результати криптоаналізу асиметричних криптографічних перетворень з табл. 4, надамо оцінку стійкості асиметричних криптографічних перетворень на наступні 30 років[8].

Використовуючи данні стандартів в області криптографічного захисту інформації щодо оцінки стійкості асиметричних криптографічних перетворень, наведемо оцінку стійкості для порівняння отриманих оцінок стійкості за допомогою апроксимацій результатів криптоаналізу з оцінками, наданими в стандартах. В табл. 5 наведені результати порівняння стійкості основних асимет-

Таблиця 4

Оцінка рівня стійкості асиметричних криптографічних перетворень, засновуючись на результатах попереднього криптоаналізу

Рік	Довжина ключа, біт			IMY, MipsYears	Нижня границя ціни	Необхідна кількість років на процесорі Pentium IV, 2 GHz
	RSA та DSA	EK	NTRU			
2010	1369	160	N = 263	$1,45*10^{12}$	$2,77*10^8$	$7,25*10^8$
2015	1613	154	N = 281	$2,07*10^{13}$	$3.92*10^8$	$1,03*10^{10}$
2020	1881	161	N = 317	$2.94*10^{14}$	$5.55*10^8$	$1,47*10^{11}$
2025	2174	169	N = 353	$4.20*10^{15}$	$7.84*10^8$	$2,10*10^{12}$
2030	2493	176	N = 401	$5.98*10^{16}$	$1.11*10^9$	$2,99*10^{13}$
2040	3214	191	N = 503	$1.22*10^{19}$	$2.22*10^9$	$6,08*10^{15}$

Таблиця 5

Порівняння стійкості стандартизованих крипто перетворень

Рівень стійкості, в бітах	Симетричні	Оцінка часу крипто аналізу, MIPS-years	Геш функції	Параметри асиметричних перетворень				
				DSA	RSA	EC-DSA	IBE (BF, BB1)	NTRU
До 2010 р. (мін. 80 біт стійкості)	2TDEA 3TDEA AES-128 AES-192 AES-256	10^9	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	Min.: L = 1024; N=160	Min.: k=1024	Min.: f=160	Min.: p = 512 q = 160	N=263 q=2048 d_f= 113
До 2030 р. (мін. 112 біт стійкості)	3TDEA AES-128 AES-192 AES-256	10^{17}	SHA-224, SHA-256, SHA-384, SHA-512	Min.: L = 2048 N = 224	Min.: k=2048	Min.: f=224	Min.: p = 1024 q = 224	N=401 q=2048 d_f= 113
Після 2030 (мін. 128 біт стійкості)	AES-128 AES-192 AES-256	10^{23}	SHA-256, SHA-384, SHA-512	Min.: L = 3072 N = 256	Min.: k=3072	Min.: f=256	Min.: p = 1536 q = 256	N=449 q=2048 d_f = 134
Рівень стійкості 192 біта	AES-192 AES-256	10^{41}	SHA-384, SHA-512	Min.: L = 7680 N = 384	Min.: k=7680	Min.: f=384	Min.: p = 3840 q = 384	N=677 q=2048 d_f= 153
Рівень стійкості 256 біта	AES-256	10^{63}	SHA-512	Min.: L = 15360 N = 512	Min.: k=15360	Min.: f=512	Min.: p = 7680 q = 512	N=1087 q=2048 d_f= 120

ричних перетворень DSA, RSA, EC-DSA(FIPS -186-3), NTRU (ANSI X9.98-2010), IBE (P1363-3), їх загальносистемні параметри та параметри ключів, а також надані оцінки щодо часу криптоаналізу цих перетворень. Відповідно до рівня стійкості асиметричних криптографічних перетворень наведені параметри симетричних шифрів та гешфункцій, використання яких буде забезпечувати відповідний рівень стійкості. В якості рівня стійкості використовується оцінка стійкості довжини ключа симетричного алгоритму (табл. 5)[6].

ВИСНОВКИ

Порівнюючи результати оцінки криптографічної стійкості асиметричних криптоперетворень, отримані за допомогою методики, заснованої на апроксимації даних, отриманих в результаті криптоаналізу та оцінок, наданих в стандартах, можна зробити наступні висновки:

– результати, отримані щодо довжин ключів та загальносистемних параметрів за допомогою методики апроксимацій, майже відповідають наведеним в стандартах значенням;

– менша оцінка щодо довжини параметрів EC-DSA табл. 4 пояснюється невеликою кількістю проведених експериментів, щодо криптоаналізу, а також великий розрив в роках між дослідженнями;

– методика та стандарти не враховують можливості щодо появи більш ефективного методу криптоаналізу, а також появи квантового комп'ютера, за допомогою якого можна здійснити криптоаналіз асиметричних перетворень DSA, RSA, EC-DSA, IBE(BF, BB1) за допомогою алгоритму Шора, який здатен зменшити стійкість цих перетворень до поліноміальної, та поставити під загрозу стійкість криптосистем, що використовують перераховані вище перетворення;

– виходячи з того, що перетворення в кільці (RSA), та полі (DSA) мають субекспоненційну складність крипто аналітичних атак, вони вже не в повній мірі відповідають вимогам стійкості[3];

– основною перевагою використання перетворень в групі точок еліптичної кривої є експоненційна стійкість до атак «повне розкриття», а також більша стійкість до можливих в майбутньому атак, наприклад за допомогою квантового комп'ютера;

– аналогічно до перетворень в групі точок еліптичної кривої, криптосистеми побудовані в кільці усічених поліномів мають експоненційну складність криптоаналізу, але при цьому для них невідомі атаки за допомогою квантового комп'ютера. Недоліком таких систем можна назвати недостатню їх вивченість [9-11].

В цілому, проведений аналіз можливостей щодо криптоаналізу асиметричних криптографічних перетворень показав, щоб гарантувати стійкість криптосистем, що використовують асиметричні криптоперетворення, необхідною умовою є використання рекомендованих стандартом FIPS-186-3 параметрів домену та довжин особистих ключів[3].

Література.

[1] ISO/IEC 15408: 2000 – Information technology – Security techniques – Evaluation criteria for IT security. Part 1-3.

[2] *Горбенко І.Д.* «Криптографічний захист інформації». Навч. посібник Харків, ХНУРЕ, 2004 р.

[3] FIPS-186-3 – Information Technology Laboratory – National Institute of Standards and Technology – Digital Signature Standard (DSS), 2006.

[4] A. Menezes, P. van Oorschot, S. Vanstone. Handbook of Applied Cryptography. — CRC-Press, 1996. — 816 p. — (Discrete Mathematics and Its Applications).

[5] Ntru Cryptosystems, The NTRUEncrypt Public Key Cryptosystem.

[6] ISO/IEC 18033-2,3,4 Information technology — Security techniques — Encryption algorithms — Part 2: Asymmetric ciphers, Part 3: Block ciphers, Part 4: Stream ciphers, 2005.

[7] Boneh, Dan (1999). «Twenty Years of attacks on the RSA Cryptosystem». Notices of the American Mathematical Society (AMS) 46 (2): 203–213.

[8] Arjen K. Lenstra, Eric R. Verheul: Selecting Cryptographic Key Sizes. J. Cryptology 14(4): 255-293 (2001).

[9] M. Ajtai, C. Dwork, A public-key cryptosystem with worst case/average case equivalence, Proc. 29th ACM Symposium on Theory of Computing, pp. 284.

[10] Joseph H. Silverman, Dimension-Reduced Lattices, Zero-Forced Lattices, and the NTRU Public Key Cryptosystem, NTRU Cryptosystems Technical Report 13, available at http://www.ntru.com.

[11] J. H. Silverman and W. Whyte, Estimating Decryption Failure Probabilities for NTRUEncrypt. Technical Report #18.

Надійшла до редколегії 25.04.2011

Аулов Іван Федорович, студент кафедри БІТ ХНУРЕ. Область наукових інтересів: дослідження принципів побудови, розгортання і аналізу стійкості криптографічнихсистем, заснованих на ідентифікаторах.

Горбенко Іван Дмитрович, д.т.н., професор, завідувач кафедри БІТ ХНУРЕ, головний конструктор АТ «Інститут інформаційних технологій». Область наукових інтересів: криптографічні системи та протоколи; проектування та розробка систем, комплексів та засобів криптографічного захисту інформації.

УДК 681.3.06

Оценка защищенности асимметрических криптографических преобразований от атак типа «полное раскрытие» / И.Д. Горбенко, И.Ф. Аулов // Прикладная радиоэлектроника: науч.-техн. журнал. – 2011. Том 10. № 2. – С. 176–182.

В статье рассмотрена методика оценки стойкости асимметрических криптографических преобразований. С помощью этой методики получены результаты оценки уровня их защищенности.

Ключевые слова: асимметрическая криптосистема, алгоритм факторизации, оценка стойкости.

Табл. 05. Ил.02. Библиогр.: 11 назв.

UDC 681.3.06

Assessment of security of asymmetric cryptographic transformations from attacks of "full disclosure" type / I.D. Gorbenko, I.F. Aulov // Applied Radio Electronics: Sci. Journ. – 2011. Vol. 10. № 2. – P. 176–182.

The paper considers methods of estimating the security of asymmetric cryptographic transformations. Using this methodology, results of assessing their security level are obtained.

Keywords: asymmetric cryptosystem, factoring algorithm, estimation security.

Tab. 05. Fig. 02. Ref.: 11 items.