УДК 621. 391:519.2:519.7

Д.В. Іваненко

Харківський національний університет радіоелектроніки, Харків

КЛАСИФІКАЦІЯ АТАК СПЕЦІАЛЬНОГО ВИДУ НА ЕНЕРГОСПОЖИВАННЯ

Досліджуються атаки спеціального виду, розглядається класифікація атак спеціального виду на енергоспоживання. Досліджується можливість реалізації таких атак: простий аналіз енергоспоживання, кореляційний аналіз енергоспоживання та диференційний аналіз, на криптосистему з відкритим ключем. Аналіз проводиться на криптосистемі NTRU, на якій були реалізовані атаки спеціального виду на енергоспоживання.

Ключові слова: *алгоритм, поліном, атака спеціального виду, NTRU, SPA, CPA, DPA.*

Вступ

В цій статі розглянуто класифікацію атак спеціального виду на енергоспоживання з метою ознайомлення з можливими атаками та вияву можливих вразливостей, на які потрібно звернути увагу та враховувати при реалізації алгоритму.

Схожі атаки були добре відомі ще у 1980-х роках, але отримали широке розповсюдження тільки після публікації Полом Кохером у 1996 році [1]. Атаки спеціального виду не схожі на «класичні» атаки, які спрямовані на математичну модель алгоритму. Атаки спеціального виду направлені на конкретну реалізацію, серед параметрів якої є час виконання операції, енергоспоживання, електромагнітне випромінювання, звукові коливання та інше, але в той же час вони суттєво ефективніші. На цей час більшість реалізованих на практиці успішних атак використовують слабкість у реалізації та розміщенні механізмів криптоалгоритмів.

З цього виникає задача дослідження атак спеціального виду та дослідження реалізації алгоритмів на наявність можливих вразливостей. В статті розглядаються атаки спеціального виду на енергоспоживання, здійснюється аналіз цих атак та пошук можливих вразливостей. Всі атаки розглядаються на прикладі криптосистеми NTRU, як одної з найбільш перспективних сучасних систем.

Криптосистема з відкритим ключем NTRU

Наш вибір, криптосистема з відкритим ключем NTRU, є не випадковим. Останнім часом NTRU отримує все більше розповсюдження [2], саме NTRU займе лідируючу позицію у випадку створення квантового комп'ютера, забезпечуючи велику швидкість при невеликому розмірі ключа, алгоритм підтримує високий рівень безпеки [3].

Розглянемо криптосистему NTRU [4], яка представляє собою поліноміальне кільце R. Множина Z[X] є множиною всіх поліномів з набором цілих коефіцієнтів. Представимо кільце R, кільце усічених многочленів, як Z[X]/(XN-1). Елемент у цьому кільці R позначимо як

$$a(X) = \sum_{i=0}^{N-1} a_i X^i ,$$

цей елемент можна привести до вигляду:

$$a(X)=[a_0,a_1,\ldots,a_{N-1}].$$

Головною математичною операцією під час зашифрування та розшифрування у алгоритмі NTRU є добуток двох поліномів a(X) та b(X), результат цього добутку позначимо поліном c(X), де

$$c_к = \sum_{i+j\equiv k \bmod N} a_i b_j ,$$

при $X^N \equiv 1 \bmod (X^N-1)$.

Зниження полінома a(X) за modq , при $a(X) \in R$ та цілому q, буде мати наступний вигляд:

$$a(X) \bmod q := \sum_{i=0}^{N-1} (a_i \bmod q) X^i .$$

У подальшому поліном a(X) будемо позначати a. Також позначимо інверсію поліному f(X) mod q, як $f^{-1}(X) \bmod q$, та визначимо наступний вираз – $f(X)* f^{-1}(X) \equiv 1 \bmod q$, задовольняючи вираз.

Алгоритм NTRU включає в себе три відкритих параметри (N, p, q), де N, p, q – цілі, та p, q взаємно прості при тому, що p значно менше від q. Процедура генерації ключа починається з вибору випадкового $F \in R$ та вираховування f:=1+pF. У випадку, якщо f не має зворотного елемента за mod q, то потрібно обрати інший F та повторити процедуру. Далі необхідно вибрати другий поліном $g \in R$, який буде зворотній за mod q. Таким чином, f – це секретний ключ, а h - відкритий ключ, який потрібно обчислити з наступного виразу: $h:=pf^{-1} *g \bmod q$.

Позначимо повідомлення через m. При шифруванні відправник випадково вибирає поліном $r \in R$, потім обчислює значення шифр-тексту e:=r*h+m mod q. Для розшифрування e, отримувач обчислює a:=f*e modA q, де modA q значить, що коефіцієнти зсуваються на інтервал [A,A+q-1] після приведення за mod q. Значення A зумовлено прос-

тою формулою залежно від інших параметрів. Потім отримувач відновлює текст за формулою – m:=a modp.

Обчислення операції згортання

Домінуючою операцією в шифровані та розшифруванні NTRU є обчислення операції згортання r*h mod q та f*e mod q. Крім того на практиці це e+ pF*e mod q. Коефіцієнти поліномів h та e розподілені майже випадково, одby вибирає r та F так, що результат операції згортання r*h та F*e може мати більш низку обчислювальну складність. Береться зальний прийом, тобто використовується бінарні або тернарні коефіцієнти, $r_i,F_i \in \{0,1\}$ або $\{-1,0,1\}$, і фіксується число не нульових коефіцієнтів у r та F [8, 13]. Потім обчислення операції згортання може бути обчислено за dN-операції, де N загальне число коефіцієнтів поліноме та d – число не нульових коефіцієнтів. Алгоритм 1 представляє собою оптимізований алгоритм обчислення t=a*c modq, де зниження за модулем mod N пересуває в індексі обчислення по масиву t за рахунок додаткової пам'яті (t_N,.., t_{2N-1}). В цьому алгоритмі, $a \in R$ є бінарним поліномом з d ненульовими коефіцієнтами та $c \in R$ – загальним поліномом. Бінарний поліном a представляє собою масив b, у якому позначено ненульові положення d. Наприклад, $a(X)=1+x^3+x^6=[1,0,0,1,0,0,1,0]$ для N=8 буде мати наступний вигляд b=[0,3,6].

Алгоритм 1 – Обчислення операції згортання [5].

Вхідне: b (масив, який представляє собою не нульові значення бінарного поліному a(X)); c(X)(поліном).

Вихідне: t(x).

1. for $0 \le j < 2N$ do
2. $t_j \leftarrow 0$ //з t_N до t_{2N-1} : тимчасовий буфер
3. end for
4. for $0 \le j < d$ do
5. for $0 \le k < N$ do
6. $t_{k+b[j]} \leftarrow t_{k+b[j]} + c_k$
7. end for
8. end for
9. for $0 \le j < N$ do
10. $t_j \leftarrow (t_j + t_{j+N}) \bmod q$
11. end for

Класифікація атак спеціального виду на енергоспоживання

Атаки спеціального виду на енергоспоживання класифікуються на [7]: простий аналіз енергоспоживання (simple power analysis, далі SPA), диференціальний аналіз енергоспоживання (differential power analysis, далі DPA) [8] та кореляційний аналіз енергоспоживання (correlation power analysis, далі CPA) [9]. При SPA, зловмисник напряму спостерігає потужність енергоспоживання, яка потрібна для звичайного виконання операції, без використання статистичних методів. У свою чергу DPA та CPA збирають деякі сліди енергоспоживання від виконання криптографічних операції при використанні деякого секретного ключа та проводять їх статистичний аналіз. При атаці DPA, зловмисник робить припущення про біт невідомого ключа слідкуючи за частинами слідів енергоспоживання по деякому внутрішньому значенню регістра. Насамперед від цього і залежить припущення зловмисника, та перевіряє, як змінюється значення цієї частини. Атака CPA представляє собою більш вдосконалений метод, ніж DPA, її аналіз оснований на вирахуванні кореляційних коефіцієнтів між слідами енергоспоживання та значенням регістру.

SPA на NTRU

В цьому розділі спробуємо детальніше розглянути атаку SPA на алгоритм NTRU. Завданням атаки є спостерігання за виконанням операції згортання F*e mod q. Тим самим зловмисник намагається відновити значення масиву b (див. алгоритм 1), яке необхідно тримати у секреті.

Атака SPA на NTRU починається з визначення результату згортання. Потім обчислюються відмінності процедури обчислення для (x+y) та x+0 (або 0+y), таким чином SPA відрізняє енергоспоживання частин для (x+y) та x+0, де x та y не нульові цілі числа.

Наприклад, процесор може реалізувати доповнення так, що він не явно виконає умовний оператор для випадку, коли одним з двох операндів x та y буде нуль. Потім доповнення x+0 або y+0 може бути замінено копією у пам'яті без реального доповнення. Якщо обидва операнда не нульові, процесор виконує нормальне доповнення.

Після цього припущення потрібно буде проаналізувати безпеку NTRU.

Контролюючи вхідний поліном c, зловмисник може додати до всіх коефіцієнтів c деякі не нульові значення. Потім N додавань у лініях 5 -7(див. алгоритм 1) для j=0 буде мати вигляд $0+c_k$ ($c_k \neq 0$), тому що усі значення t_j були встановленні як 0. При j=1, перше доповнення N-(b[1]-b[0]) буде мати вигляд $c_{k+(b[1]-b[0])}+c_k$, де обидва операнда не нульові. Проте наступне доповнення b[1]-b[0] має вигляд $0+c_k$, яке зловмисник може відрізнити від не нульового доповнення. Звідси зловмисник зможе одержати значення b[1]-b[0] з визначеним місцем розташування, де модель енергоспоживання була змінена. Ця процедура може бути застосована до всіх схожих операцій для j, де зловмисник може вирахувати кожне значення b[1]-b[0] при j=l (0<l<d). Таким чином, злов-

миснику залишається знайти вихідне b[0] шляхом перебору.

Розглянемо для більшої наочності цей алгоритм з наступними параметрами: N=8 та d=4. Тут Z та A – споживана потужність для x+0 (або y+0) та x+y, відповідно. Послідовність Z та A записується в порядку виконання з ліва на права:

j=0:	Z	Z	Z	Z	Z	Z	Z	Z
j=1:	A	A	A	A	A	Z	Z	Z
j=0:	A	A	A	A	A	A	A	Z
j=0:	Z	A	A	A	A	A	Z	Z.

Зловмисник може відновити b[1]-b[0]=3, b[2]-b[1]=1, b[3]-b[2]=2, це бінарне значення полінома b, який можна представити у вигляді $a(X)=X^m(1+X^3+X^4+X^6)$ для деякого невід'ємного повідомлення m. У подальшому значення m може бути легко знайдено шляхом повного перебору.

Спробуємо запропонувати метод, спрямований на протидію SPA атаці. Простою мірою протидії можна назвати ліквідацію всіх доповнень з нулями. Можливим рішенням також може бути заміна встановленого t (у рядку 2, див. алгоритм 1) на $t_j \leftarrow x$ для деякого не нульового значення x, та відняти x від t_j після головного циклу(лінії 4-8, див. алгоритм 1). Оптимальним вибором x можна назвати при x=q, що заощадить віднімання після головного циклу.

Однак, фіксування значення t може призвести до вразливості від інших видів атак. Наприклад, вважатимемо, що зловмисник розпочав алгоритм встановлення всіх коефіцієнтів c(X) як 2^w-q, де w розмір слова процесора. Якщо t_j були встановлені як q, (лінії 5-7 див. алгоритм 1) при j=0 буде встановлено 2^w у інтервалі $t_{b[0]}$ до $t_{b[0]+N-1}$, таким чином при 0 буде переповнення або перенесення. Тепер зловмисник може розпочати атаку SPA використовуючи частину слідів енергоспоживання, що залишилась, при $j \geq 1$.

Таким чином потрібно використовувати деяку рандомізацію як протидію атаці SPA.

Висновок. Таким чином зловмисник, спостерігаючи за потужністю енергоспоживання, яке використовується при виконанні операції, робить припущення відносно значення масиву b за рахунок контролю вхідного c(X). Тобто зловмисник падає на вхід відоме c(X) та спостерігаючи за енергоспоживанням робить припущення відносно b. Саме під масивом b маємо на увазі не нульові значення a(X), тобто знаючи b можна відтворити a(X).

CPA на NTRU

Розглянемо можливість реалізації атаки CPA на секретний ключ NTRU підчас операції розшифрування, використовуючи експериментальні результати реалізації атаки на Tmoke Sky [11].

Основне завдання DPA та CPA полягає у тому, що доки пристрій виконує деякі операції, зловмисник спостерігає за найменшими змінами у енергоспоживанні між відповідними операндами та значеннями регістрів. Зловмисник використовує ці зміни, які з'являються у регістрі при обчислені операції згортання (див. алгоритм 1, рядок 6), для здобуття корисної інформації.

Для аналізу отриманих результатів зловмиснику можуть допомогти наступні методи - це код Хеммінга та відстань Хеммінга. Під кодом Хеммінга [6] маємо на увазі аналіз енергоспоживання, з метою знаходження залежностей набору біт у сигналі даних. Інший метод, відстань Хеммінга, це аналіз енергоспоживання з метою знаходження залежностей між значенням регістру до та після виконання операції згортання.

Було обрано відстань Хеммінга тому, що цей метод підходить для опису енергоспоживання, яке використовується у [12]. Далі позначимо HW(x)- код Хеммінга від x, а HD(x,y) – визначимо як відстань Хеммінга від x до y.

Мета атаки полягає у пошуку вихідного значення b[1]-b[0], b[2]-b[1],…, b[d-1]-b[d-2] у послідовному порядку. Після початку операції згортання, зловмисник слідкує за поведінкою процесу обчислення. На рис. 1 зображено приклад атаки для N=8, d=4, b=[1,4,5,7]. Розглянемо ітерації для j=0 та j=1. При додаванні відбувається відносний зсув з індексом t для c_0, значення регістру для b[1]-b[0] для цього прикладу буде дорівнюватися 4-1=3. Завдання зловмисника полягає у пошуку безпосередньо цього значення.

Поліном S, який використовується для атаки, представимо у вигляді множини $c^1, c^2,\ldots, c^S$ та множини $P^1, P^2,\ldots, P^S$, під множиною ^{P} має на увазі відповідні сліди енергоспоживання, які були залишені пристроєм при виконані операції над $c^1, c^2,\ldots, c^S$. Далі зловмисник робить припущення щодо значення b[1]-b[0] при w>1, та вираховує для кожного значення відстані Хеммінга $D^l=HD(c_w^l, c_w^l + c_0^l)$ при $1 \leq l \leq S$.

Наступний крок – це перевірка на наявність якої-небудь кореляції між D^l та P^l. Для вирішення цієї мети обчислимо коефіцієнт кореляції Пірсона, який допоможе виявити зміни між D^l та P^l:

$$P_{P,D}^t = \frac{\sum_{t=1}^{S}(P^l - \overline{P})\cdot(D^l - \overline{D})}{\sqrt{\sum_{t=1}^{S}(P^l - \overline{P})^2 \cdot \sum_{t=1}^{S}(D^l - \overline{D})^2}}, \qquad (1)$$

де $\overline{P}$ та $\overline{D}$ середнє значення P^l та D^l, взяте у S випадках, відповідно. Відмітимо, що (1) може бути обчислена незалежно для кожного відповідного шагу t між слідами енергоспоживання. У випадку наявнос-

ті значимої кореляції між P^l та D^l для деякого t означає, що b[1]-b[0]=w коректне припущення, та це t відповідає моменту, коли $c_{b[1]-b[0]}+c_0$ обчислюється. Тому завдання зловмисника полягає у знаходженні максимально вихідного w.

Після знаходження значення b[1]-b[0], значення b[2]-b[1] можна знайти аналогічним методом. Таким чином, зловмисник робить припущення w для b[2]-b[1] та використовує кореляцію між енергоспоживанням та

$$HD=(c_{b[1]-b[0]+w}+c_w, c_{b[1]-b[0]+w}+c_w+c_0)$$

Після знаходження всіх відповідних зсувів

b[1]-b[0],…, b[d-2]-b[d-1]

останнім завданням буде знаходження вихідного b[0] методом перебору.

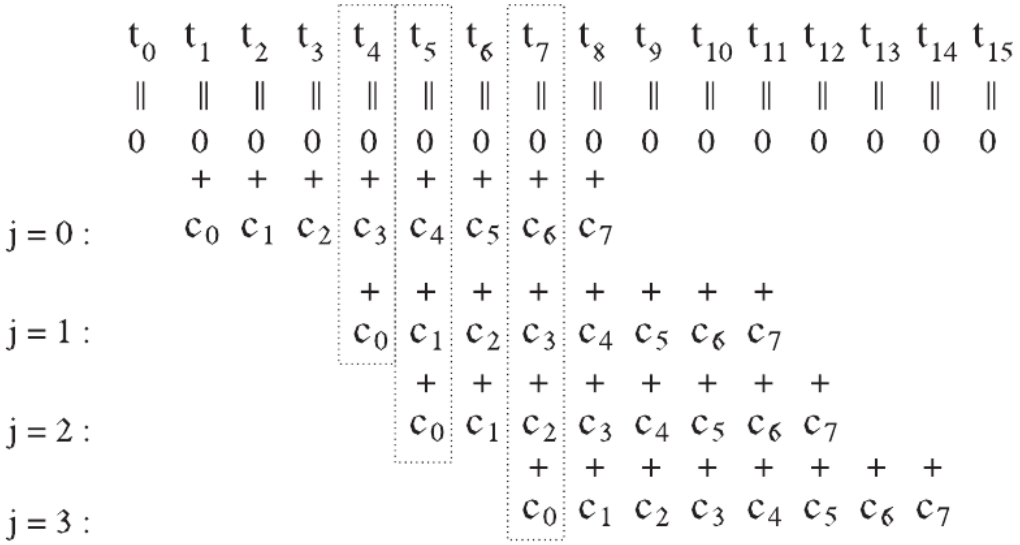

Рис. 1. Приклад алгоритму згортання з параметрами (N=8,d=4,b=[1,4,5,7]). Кожний прямокутник показує мету аналізу

Висновок. Таким чином, зловмисник, аналізуючи отриманні дані за допомогою відстані Хеммінга та коефіцієнта кореляції Пірсона, відновлює масив b, що допоможе отримати інформацію про a(X).

Експериментальні результати реалізації атаки спеціального виду на енергоспоживання

Атака була реалізована на платформу Tmoke Sky [11], яка використовує MSP430F157 процесор. MSP430F157 працює на 8 MHz з використанням 10 KB RAM та 48 KB флеш пам'яті. Операції згортання були реалізовані на NesC мові, та використовувалися наступний набір параметрів (N,d,p,q)= (251,48,2,197) згідно з [10]. Аналіз був продемонстрований за допомогою MathLab на 1000 слідів енергоспоживання, отриманих при операції розшифрування 1000 різних шифр-текстів e(X), та фіксованому невідомому поліномі F(x). Сліди енергоспоживання були отримані на частоті дискретизації у 200MHz, використовуючи осцилограф змішаних сигналів (MSO) Agilent 54830D [12].

Розглянемо експериментальні результати атаки на b[1]-b[0]. На рис. 2 зображена кореляція між енергоспоживанням та HD(c_w, c_w+c_0) для всіх можливих припущень w=1,…, 250. Горизонтальні та вертикальні осі представлені у вигляді точок перебору та коефіцієнтів кореляції Пірсона, які пов'язані з кожною з цих точок, відповідно. Побудуємо разом 250 кривих та до кожної кривої прив'яжемо значення w. Зазначимо, що фрагменти зі слідами енергоспоживання будуть більш довгими. «Пік», що з'явився між t=500 та t=600, значить, що c_w+c_0 обчислюється близько до цієї точки.

Також можна вибрати найбільше можливе вихідне w з 250 варіантів, з допомогою якого ідентифікується «пік».

Рис. 3 показує максимальне значення коефіцієнтів кореляції для кожного w. На графіку максимум дорівнює w=3 при значенні 0,4198, який є чітко помітний у порівнянні зі значеннями інших w. Звідси можна сказати, що в цьому випадку значення b[1]-b[0]=3. Всі інші значення b[l]-b[l-1] можуть бути знайдені використовуючи аналогічний підхід.

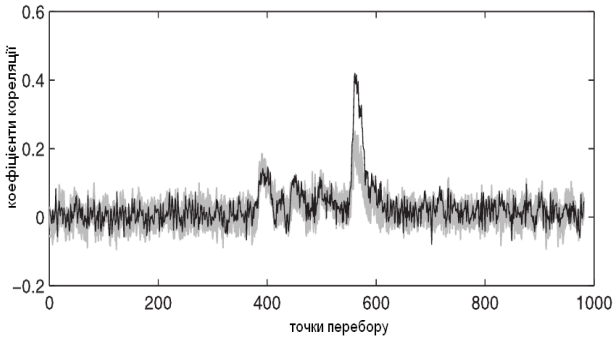

Рис. 2. Кореляція між енергоспоживанням та відстанню Хеммінга на всі можливі припущення

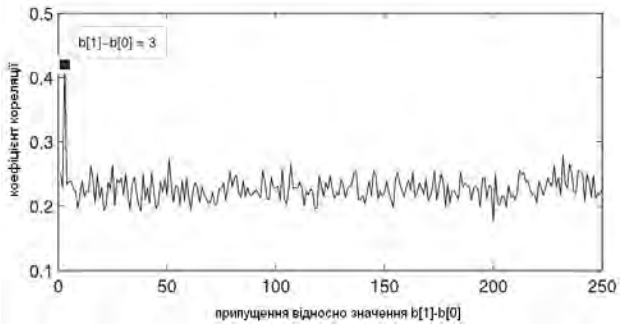

Рис. 3. Максимум кореляції для кожного можливого припущення

Висновки

У даній статті було розглянута класифікація атак спеціального виду на енергоспоживання та проаналізована можливість реалізації цих атак на криптосистему з відкритим ключем. Було розглянуто дві атаки: CPA та SPA, реалізація цих атак була направлена на відновлення секретного ключа NTRU. Проаналізувавши атаки CPA та SPA, можна сказати, що зловмисник теоретично відновить секретний ключ з високою імовірністю

Також в статті було розглянуто експериментальні результати реалізації атак виду CPA на операцію згортання алгоритму NTRU з такими параметрами (N,d,p,q)= (251,48,2,197), у результаті проведення атаки було відновлено перший елемент в масиві b та стало зрозуміло, що інші, наступні всі елементи, можна знайти аналогічним методом. Хоча атака CPA є можливою для цієї реалізації та реалізувавши атаку можна відновити секретний ключ, потрібно звернути увагу та враховувати те, що атаки спеціального виду більш направлені на певну апаратну та програмну реалізацію алгоритму. Наприклад, якщо користувач реалізує які-небудь методи протидії, тоді зловмиснику буде визначити або відновити секретний ключ.

Список літератури

1. Kocher P.C. Timing attacks on implementations of Diffie-Hellmann, RSA, DSS, and other systems / P.C. Kocher // Advances in Cryptology. CRYPTO '96 : сборник. – Springer, 1996. – Т. 1109. – С. 104-113.

2. Security Innovation's NTRUEncrypt Adopted as X9 Standard for Data Protection / Security Innovation is privately held and is headquartered in Wilmington, MA USA. [Електронний ресурс]. – Режим доступу до ресурсу: www/URL:http://www.businesswire.com/news/home/20110411005309/en/Security-Innovation %E2%80%99s-NTRUEncrypt-Adopted-X9-Standard-Data.

3. Іваненко Д.В. Порівняльний аналіз сучасних асиметричних криптосистем / Д.В. Іваненко, О.В. Сєвєрінов // Системи управління, навігації та зв'язку. – К.: ДП «ЦНДІ НІУ», 2012. – С. 61-64.

4. Hostein J. NTRU: A new high speed public key cryptosystem / J. Hostein, J. Pipher, J. Silverman // Preprint; presented at the rump session of Crypto 96.

5. Hoffstein J. Optimizations for NTRU / J.Hoffstein, J. Silverman // Proc. Public-Key Cryptography and Computational Number Theory, 2000.

6. Hoffstein J. Random small hamming weight products with applications to cryptography / J. Hoffstein, J. Silverman // Discrete Applied Mathematics. – 2003. – Vol. 130. – P. 37-49.

7. Kocher P. Timing attacks on implementation of Diffe-Hellman, RSA, DSS and other systems/ P. Kocher // Advances in Cryptology. – Crypto 96, LNCS. – Springer, 1996. – Vol. 1109. – P. 104-113.

8. Kocher P. Differential power analysis / P. Kocher, J. Jaffe, B. Jun // Advances in Cryptology. – Crypto 99, LNCS. – Springer, 1999. – Vol. 1666. – P .388-397.

9. Brier E. Correlation power analysis with a leakage model / E. Brier, C. Clavier, F. Olivier // Cryptographic Hardware and Embedded Systems. – CHES 2004, LNCS. – Springer, 2004. – Vol. 3156. – P. 16-29.

10. Howgrave-Graham N. Choosing parameter sets for NTRUEncrypt with NAEP and SVES-3 / N. Howgrave-Graham, J. Silverman, W. Whyte // CT-RSA 2005, LNCS. – Springer, 2005. – Vol. 3376. – P. 118-135.

11. Tmote Sky hardware description. [Електронний ресурс]. – Режим доступу до ресурсу: WWW/URL: http://www.sentilla. com/pdf/eol/tmote-sky-datasheet.pdf.

12. Texas Instruments, MSP430F157 Mixed Signal Microcontroller, 2005.

13. Bailey D.V. NTRU in constrained devices / D.V. Bailey, D. Coffin, A. Elbirt, J.H. Silverman, A.D. Woodbury // Cryptographic Hardware and Embedded Systems. – CHES 2001, LNCS. – Springer, 2001. – Vol. 2162. – P. 262–272.

Надійшла до редколегії 1.09.2012

Рецензент: д-р техн. наук, проф. І.Д. Горбенко, Харківський національний університет радіоелектроніки, Харків.

КЛАССИФИКАЦИЯ АТАК СПЕЦИАЛЬНОГО ВИДА НА ЭНЕРГОПОТРЕБЛЕНИЕ

Д.В. Иваненко

Исследуется атаки специального вида, рассматривается классификация атак специального вида на энергопотребление. Исследуется возможность реализации таких атак: простой анализ энергопотребление, корреляционный анализ энергопотребление и дифференциальный анализ энергопотребление, на криптосистему с открытым ключом. Анализ проводился на криптосистеме NTRU, на которой были реализованы атаки специального вида на энергопотребление.

Ключевые слова: *алгоритм, полином, атака специального вида, NTRU, SPA, CPA, DPA.*

THE CLASSIFICATION OF SIDE CHANNEL ATTACKS FROM OF CONSUMPTION

D.V. Ivanenko

We study a side channel attack is considered a classification of side channel attacks on power. The possibility of the realization of such attacks: simple power analysis, correlation analysis and differential power analysis, the public-key cryptosystem. The analysis was performed on the cryptosystem NTRU, which have been implemented a side channel attacks.

Keywords: *algorithm, polynomial, attack of the special kind, NTRU, SPA, CPA, DPA.*