УДК 004.75

Гарасимович Г. В.,
Куц В. Ю.

МЕТОД ЗАХИСТУ ОПЕРАНДІВ МОДУЛЯРНОГО ЕКСПОНЕНЦІЮВАННЯ ВІД ЇХ РЕКОНСТРУКЦІЇ АНАЛІЗОМ ДИНАМІКИ СПОЖИВАННЯ ПОТУЖНОСТІ

METHOD FOR PROTECTION MODULAR EXPONENTIATION OPERANDS RECONSTRATION BY POWER ANALYSIS

Метою представлених в статті досліджень є аналіз небезпеки реконструкції операндів модулярного експоненціювання аналізом динаміки споживання потужності і розробка способів протидії. Показано, що ступінь модулярного експоненціювання, що є ключем алгоритмів RSA, El-Gamal, DSA може бути реконструйована тимчасовим аналізом споживаної потужності. Для протидії розроблений спеціальний алгоритм модулярного експоненціювання. Алгоритм не має умовних операторів і включає неправдиві операції, що утрудняють тимчасової аналіз потужності. Застосування запропонованого підходу збільшує на 25% час виконання модулярного експоненціювання.

Ключові слова: модулярне експоненціювання, аналіз динаміки споживання потужності, смарт-карти, криптографічні алгоритми, протоколи захисту даних, термінальні обчислювальні пристрої.

Бібл.: 6

The goal of presented by article research is to point out the potential vulnerabilities of modular exponentiation operands reconstruction by power dynamic analysis and to elaborate countermeasures. It has been shown that exponent of modular exponentiation which is secret key of RSA, El-Gamal and DSA can be reconstruction by timing power analysis. For countermeasure the special algorithm for modular exponentiation has been worked out. Proposed algorithm does not conditional operators use and include the false operators which inhibit to timing power analysis. It has been shown that implementation of proposed approach demand about 25% more time for modular exponentiation.

Key words: power analysis, smart cards, cryptographic algorithms, data security protocols, terminal computer devises.

Bibl.: 6

Актуальність теми дослідження. Динамічне поглиблення інформаційної інтеграції на основі комп'ютерних мереж відіграє домінуючу роль на сучасному етапі розвитку більшості сфер людської діяльності. Важливою умовою розширення інформаційної інтеграції є рішення проблеми ефективного захисту даних і розмежування прав доступу до інформації в комп'ютерних системах і мережах. Розширення використання комп'ютерних і мережевих технологій в сфері фінансової діяльності, для управління складними технічними системами, пов'язаними з техногенним ризиком вимагає забезпечення високої надійності захисту інформації в комп'ютерних системах управління і мережах. Таким чином, існує об'єктивна необхідність підвищення ефективності засобів захисту інформації з точки зору розширення сфер використання інтегрованих систем. З іншого боку, об'єктивно існує ряд факторів, що знижують надійність засобів захисту даних. Таким чином, наукова задача підвищення ефективності засобів

захисту інформації є важливою і актуальною для сучасного етапу розвитку інформаційних технологій.

Постановка проблеми. В останні роки, однією з найбільш потенційно небезпечних загроз інформаційній безпеці в системах комп'ютерного управління є несанкціонований доступ до даних за допомогою вимірювання і аналізу динаміки зміни параметрів роботи обчислювального пристрою під час реалізації ним програм [1]. Особливо актуальною є проблема захисту даних від їх реконструкції за допомогою вимірювання і аналізу динаміки зміни споживаної потужності. В сучасних комп'ютерних мережах значну частину термінальних пристроїв складають мікроконтролери, для яких вимір споживаної потужності і зіставлення її з командами, що виконуються, здійснюється відносно просто [1]. Разом з тим, такі термінальні пристрої підтримують мережеві протоколи захисту інформації, при реалізації яких використовуються секретні дані - ключі і паролі.

Сучасні технології дозволяють виконувати статистичну реконструкцію цих секретних даних на основі аналізу динаміки споживаної потужності [2]. Аналіз таких технологій свідчить про те, що вони найбільш ефективні для доступу до постійних компонентів систем захисту інформації - ключам і паролів. Це особливо небезпечно для механізмів захисту даних, ключі яких рідко змінюються. До таких механізмів, зокрема, відносяться алгоритми з відкритим ключем, найбільш поширеними з яких є RSA, El-Gamal, DSA. Зміна ключів при кожному сеансі роботи цього алгоритму принципово порушує концепцію відкритості ключів. Тому ключі згаданих алгоритмів найбільш уразливі для несанкціонованого доступу до них шляхом аналізу динаміки споживання потужності. Разом з тим, ці алгоритми лежать в основі мережевих протоколів інформаційної безпеки, тому втрата контролю над їх ключами загрожує серйозними порушеннями в роботі систем захисту інформації в мережах.

Таким чином, проблема захисту від реконструкції аналізом динаміки споживання потужності ключів алгоритмів, в основі яких лежить модулярне експоненціювання є важливою і актуальною на сучасному етапі розвитку технології захисту даних в мережах.

Аналіз останніх досліджень і публікацій. Базовою обчислювальною операцією при програмній реалізації великої кількості алгоритмів захисту інформації з відкритим ключем, в тому числі RSA, є модулярне експоненціювання $X^E \bmod M$, при $X, E < M$. Кількість n двійкових розрядів чисел X, E і M значно перевищує розрядність k процесора. Кожне з чисел X, E і M, можна представити у вигляді s слів, що складаються з k двійкових розрядів $(s=n/k)$, кожне з яких лежить в інтервалі від 0 до 2^k-1: $X=\{x_{s-1},\ldots,x_1,x_0\}$, $E=\{e_{s-1},\ldots,e_1,e_0\}$ і $M=\{m_{s-1},\ldots,m_1,m_0\}$, $\forall j\in\{0,...,s-1\}$, $0\le x_j,e_j,m_j\le 2^k-1$. Для вказання двійкових розрядів слів X, E і M використовуються позначення з двома індексами, наприклад $e_0=\{e_{0,k-1},e_{0,k-2},\ldots,e_{0,1},e_{0,0}\}$; $\forall l\in\{0,...,k-1\}$: $x_{j,l}$, $e_{j,l}$, $m_{j,l}\in\{0,1\}$:

$$X=\sum_{j=0}^{s-1} x_j\cdot 2^{j\cdot k}=\sum_{j=0}^{s-1}\sum_{l=0}^{k-1} x_{j,l}\cdot 2^{j\cdot(k-1)+l}, E=\sum_{j=0}^{s-1} e_j\cdot 2^{j\cdot k}=\sum_{j=0}^{s-1}\sum_{l=0}^{k-1} e_{j,l}\cdot 2^{j\cdot(k-1)+l},$$

$$M=\sum_{j=0}^{s-1} m_j\cdot 2^{j\cdot k}=\sum_{j=0}^{s-1}\sum_{l=0}^{k-1} m_{j,l}\cdot 2^{j\cdot(k-1)+l}$$

Процес модулярного експоненціювання зводиться до послідовного виконання $log_2E = n$ циклів, в кожному з яких здійснюється операція зведення в квадрат отриманого на попередньому циклі результату і, додатково, в залежності від поточного біта ступеня E, виконується операція множення. Виходячи

з порядку, в якому аналізуються розряди ступеня E, існує два різновиди модулярного експоненціювання: справа - наліво і зліва - направо.

При використанні алгоритмів, заснованих на модулярному експоненціюванні, в якості секретного ключа виступає код експоненти E, який практично не змінюється. Відповідно, основним завданням ставлячи під загрозу безпеку є отримання коду E. В якості побічної задачі виступає задача доступу до значення коду X або результату - $A=X^E \bmod M$ при невідомому, але постійному E [2]

Виділення недосліджених частин загальної проблеми. Як уже зазначалося, значну частину термінальних пристроїв мереж складають вбудовані мікроконтролери та мікропроцесори, що використовуються для збору даних або управління технологічним обладнанням. До 2005 року частина таких термінальних пристроїв становила до 60% [2], причому має місце тенденція її зростання з розвитком комп'ютерних та мережевих технологій, а також з розширенням сфер їх застосування.

Цей клас термінальних пристроїв підтримує протоколи захисту інформації в мережах, в процесі реалізації яких використовує постійні секретні параметри - паролі, ключі криптографічних алгоритмів. Для мікроконтролерів і мікропроцесорів щодо просто виміряти під час виконання програм динаміку споживаної потужності і зіставити її з виконуваними командами. Всі процесорні пристрої обчислювальної техніки побудовані на логічних вентилях, основною частиною яких є транзистори. Струми, що протікають через транзистори, залежать від їх робочих точок і змінюються стрибкоподібно при перемиканні вентилів. При цьому, величина споживаного струму залежить від значення бітів даних, які обробляються в поточний момент часу [3]. Для вимірювання струму, споживаного обчислювальним пристроєм, в його ланцюг харчування додається резистор, напруга на якому вимірюється високоточним цифровим мікровольтметром [3]. Дослідницькі цифрові мікровольтметри дозволяють проводити вимірювання з частотою дискретизації 1-2 ГГц. і точністю до 1мкВ. Промислові загальнодоступні зразки забезпечують частоту дискретизації 50 МГц і точність 5мВ.; Більшість мікроконтролерів, вбудованих мікропроцесорів і смарт-карт працює з тактовою частотою 20-50 МГц.

Судячи з результатів виконаного аналізу публікацій [2], що стосуються технологій реконструкції даних з використанням технологій SPA і DPA, в даний час не існує математичної моделі впливу бітів оброблюваної інформації на споживану потужність. Але, це вплив має місце і може бути виявлено статистичними методами, на яких побудована ідея DPA.

Постановка завдання. Таким чином, проведений аналіз показав, що базові алгоритми модулярного експоненціювання не забезпечують захисту від реконструкції коду експоненти E з використанням SPA. Метою роботи є створення способів захисту від відновлення коду експоненти E за результатами аналізу динаміки потужності, споживаної обчислювальним пристроєм в процесі виконання модулярного експоненціювання.

Метод протидії реконструкції коду експоненти аналізом часовим аналізом динаміки споживання потужності

Наведений аналіз відомих способів протидії реконструкції експоненти, що здійснюється з використанням SPA, показав, що вузловий проблемою є виключення можливості відстеження засобами SPA умовних операторів, що виконують

послідовне тестування розрядів E. Для захисту від SPA необхідно модифікувати алгоритм модулярного експоненціювання таким чином, щоб виключити з нього умовні оператори. В якості основи модифікованого алгоритму вибрано модулярне експоненціювання справа-наліво, оскільки воно не використовує постійних елементів і, відповідно, більш стійкий до DPA. Нижче представлена пропонована модифікація алгоритму модулярного експоненціювання:

1. $A[0] = 1$; $A[1]=1$; $S = X$; $y = 1$;
2. for ($j=0$; $j<s$; j++)
   2.1. for ($l=0$; $l<k$; l++)
   {
   2.1.1. $q = e_j \& y$;11
   2.1.2. $e_j = e_j >> 1$;
   2.1.3. $A[q] = S \cdot A[1] \bmod M$;
   2.1.4. $S = S \cdot S \bmod M$;
   }

Результат $A[1] = X^E \bmod M$.

У запропонованій модифікації відсутні умовні оператори, на кожному циклі виконується одна операція зведення в квадрат і множення, що не дозволяє засобами SPA визначити значення оброблюваного в цьому циклі розряду експоненти. Виняток умовних операторів виконано за рахунок введення паразитного операції множення, результат якого фіксується в A[0], а накопичення правильного результату здійснюється в A[1]. Цілком очевидно, що за рахунок введення паразитного операції множення, обчислювальна складність модулярного експоненціювання зростає на 25%.

В якості другого, ефективного способу протидії SPA-реконструкції експоненти E пропонується виконання модулярного експоненціювання з використанням адитивних ланцюжків.

Адитивним ланцюжком V довжиною L для позитивного цілого числа E називається послідовність $u_0,u_1,\ldots,u_s$ додатних чисел і пов'язана з ними послідовність: $w_1,w_2,\ldots,w_s$ пар $w_i=<i_1,i_2>$, $0 \le i_1, i_2 < i$, які мають наступні властивості:

1. $u_0 = 1$ и $u_L = E$;
2. $\forall u_i$, $1 \le i \le L$, $u_i = u_{i_1} + u_{i_2}$

Алгоритм модулярного експоненціювання $X^E \bmod M$ на основі адитивних ланцюжків має наступний вигляд:

1. $G[0] = X$;
2. for($j=1$; $j<=L$; j++) $G[j] = G[j_1] \cdot G[j_2] \bmod M$;

Результат: $G[L] = X^E \bmod M$.

Наприклад, для $E=12$, можна сформувати адитивний ланцюжок у вигляді багатьох чисел {1,2,3,6,12}, який відповідають пари: : $w_1=<0,0>$, $w_2=<0,1>$, $w_3=<2,2>$, $w_4=<3,3>$. Для тієї ж експоненти $E=12$, можна сформувати інший адитивний ланцюжок, який задається безліччю чисел {1,2,4,5,10,12}, яким відповідають пари: $w_1=<0,0>$, $w_2=<1,1>$, $w_3=<0,2>$, $w_4=<3,3>$, $w_5=<1,4>$. Відповідно до наведеного вище алгоритмом, обчислення X^{12} з використанням останньої ланцюжка виконується в наступній послідовності: G[0]=X;

$G[1]=G[0] \cdot G[0] \bmod M = X^2 \bmod M$;

$G[2]=G[1] \cdot G[1] \bmod M = X^4 \bmod M$;

$G[3]=G[0]\cdot G[2] \bmod M = X^5 \bmod M$;
$G[4]=G[3]\cdot G[3] \bmod M = X^{10} \bmod M$;
$G[5]=G[1]\cdot G[4] \bmod M = X^{12} \bmod M$.

Оскільки наведений алгоритм не містить умовних операторів, то часовий аналіз динаміки споживання потужності при його реалізації практично не дозволить відновити значення *E*, навіть, якщо вдасться відрізнити операції множення і зведення в квадрат. Оскільки для використовуваної на практиці розрядності *n* експоненти (близько 1024) варіантів її розкладання на адитивні ланцюжка існує дуже багато, то відновити конкретно використаний ланцюжок не представляється можливим за результатами аналізу динаміки споживаної потужності.

Ефективність використання адитивних ланцюжків при модулярному експоненціюванні, як засобу протидії SPA, визначається тим, що на практиці експонента *E*, будучи закритим ключем RSA абонента не змінюється . Це дозволяє згенерувати, з використанням випадкових чисел, адитивний ланцюжок, відповідно до якого скомпілювати програму, яка буде безпосередньо виконуватися.

Недоліком використання адитивних ланцюжків є необхідність в додатковому обсязі пам'яті для масиву *G* і зберігання пар *w*, які задають зв'язком компонентів ланцюжків. При цьому необхідний обсяг пам'яті визначається довжиною *L* ланцюжка. Якщо вважати, що середня кількість одиниць в n-розрядній експоненті *E* рівне *n / 2*, то нижня межа значення довжини *L* ланцюжка складає *n + log2n -2*. Для реалізації наведеного вище алгоритму потрібно зберігання відносно невеликого числа елементів масиву *G*: в принципі можна виконати алгоритм при зберіганні всього 2-х чисел зазначеного масиву. Для зберігання пар *w*, потрібний обсяг V_w пам'яті, який визначається формулою:

$$V_w = 2 \cdot (n + \log_2 n - 2) \cdot \left\lfloor \log_2 (n + \log_2 n - 2) \right\rfloor \quad (1)$$

Наприклад, для тих що часто зустрічаються в практиці застосування RSA значення n=1024, V_w = 2838 байт, що не перевищує об’єм вбудованої пам’яті більшості сучасних вбудованих мікроконтролерів.

Висновки. Проведені дослідження, спрямовані на розробку способів протидії відновленню експоненти, здійснюваного шляхом вимірювання та аналізу динаміки споживаної обчислювальної платформою потужності при модулярних експоненціюваннь дозволяють зробити висновки:

1. Операція модулярного експоненціювання лежать в основі ряду криптографічних алгоритмів, таких як RSA, El-Gamal, DSA, які широко використовуються в протоколах захисту інформації в мережах. Експонента зазначеної операції є частиною закритого ключа цих алгоритмів, який змінюється дуже рідко.

2. Найбільшу небезпеку для реконструкції експоненти представляє тимчасової аналіз споживання потужності обчислювальної платформою при виконанні на ній операції модулярного експоненціювання.

3. Ефективним способом протидії реконструкції експоненти тимчасовим аналізом споживання потужності є виняток умовних операторів. Запропоновано алгоритм, що задовольняє цій вимозі, що включає паразитні операції, які ускладнюють ефективний аналіз динаміки споживання потужності. Реалізація запропонованого алгоритму вимагає на 25% більше часу в порівнянні зі звичайним модулярним експоненціюванням.

4. Запропоновано підхід до вирішення завдання протидії тимчасового аналізу споживання потужності для реконструкції секретного коду експоненти. Підхід заснований на використанні технології модулярного експоненціювання на основі адитивних ланцюжків

Запропоновані способи протидії доступу до закритих ключів алгоритмів захисту інформації, в основі яких лежить операція модулярного експоненціювання, можуть бути ефективно використані для підвищення інформаційної безпеки комп'ютерних мереж.

Список використаних джерел.

1. Cohher P. Timing Attack on Implementations of Diffie-Hellman, RSA, DSS and other systems / P.Cohher. // Proceeding of Advances in Cryptology-"CRYPTO-96". LNCS-1882. Springer-Verlag. – 1996. - PP. 104-113.

2. Messerges T.S. Power Analysis Attacks of Modular Exponentiation in Smartcards. / T.S. Messerges., E.A. Dabbish, R.H. Sloan. // Proceeding of 1-th International Workshop "Cryptographic Hardware and Embedded Systems" (CHES-1999), LNCS-1717. Springer-Verlag. - 1999. - P. 145-157.

3. Akkar M.L. Power analysis, what is now possible. / M.L. Akkar., C. Bevan, P. Dischamp, D. Moyart. // Proceeding of International Workshop "Asiacrypt-2000". LNCS-1976. Springer-Verlag. - 2000. - P. 489-502.

4. Mayer-Sommer R. Smartly analyzing the simplicity and power of simple power analysis on smartcards. / R. Mayer-Sommer. // Proceeding of 2-th International Workshop "Cryptographic Hardware and Embedded Systems" (CHES-2000), LNCS-1965. Springer-Verlag. - 2000. - P. 78-92.

5. Kocher P. Differential Power Analysis. / P. Kocher, J. Jaffe, B. Jun. // Proceeding of CRYPTO'99 . - Springer-Verlag. - 1999. - PP.388-404.

6. Марковский А. П. Способ защиты ключей алгоритма ГОСТ 28.147-89 от реконструкции анализом динамики потребляемой мощности. / А. П. Марковский, О. А. Абабне, Ияд Мохд Маджид Ахмад Шахрури. // Вісник національного технічного університету України "КПІ". Інформатика, управління та обчислювальна техніка. – 2007. - № 46. - С.128-138.

ДОВІДКА ПРО АВТОРІВ

Куц Володимир Юрійович – доцент, кафедра обчислювальної техніки, Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського».

Kuts Volodymyr Yuriiovych – associate professor, Department of Computer Engineering, National Technical University of Ukraine "Igor Sikorsky Kyiv PolytechnicInstitute".

Гарасимович Галина Володимирівна – студентка, кафедра обчислювальної техніки, Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського».

Harasymovych Halyna Volodymyrivna - student, Department of Computer Engineering, National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute".

E-mail: harasymovych.hv@gmail.com

Harasymovych Halyna Volodymyrivna,
Kuts Volodymyr Yuriiovych

METHOD FOR PROTECTION MODULAR EXPONENTIATION OPERANDS RECONSTRATION BY POWER ANALYSIS

Topicality of the research. The dynamic intensification of information integration based on the computer networks takes a leading role at the present stage of development of most spheres of human activities. There is an objective need to increase the effectiveness of information security means in terms of expanding the scope of integrated systems. Thus, the scientific task aimed at increasing the effectiveness of information security means is important and topical for the current stage of information technologies development.

Problemstatement. Protection of the keys of algorithms, based on modular exponentiation, against reconstruction by power analysis is important and topical problem at the current stage of the development of technologies for data protection in networks.

Analysis of recent researches and publications. Modular exponentiation X^E mod M, where X, $E < M$ serves as the basic computing operation for the program realization of a large number of public key algorithms, including RSA.

Uninvestigated parts of general matters defining. Following the analysis of publications related to technologies of data reconstruction using SPA and DPA technologies, as of today there is no mathematical model of the impact of bits of the processing information on power consumption. But this impact can be detected by using static method on which the idea of DPA is based.

The research objective. Therefore, the analysis showed that the basic algorithms of modular exponentiation do not protect against reconstruction of the code of exponent $E$by using SPA. The purpose of the research is to create methods of protecting from the restoration of code of the exponent E following the analysis of power consumed by the computing device in the process of modular exponentiation.

Main body. The present analysis of the known methods of counteraction against the reconstruction of the exponent that is performed by using SPA has showed that the key problem is the lack of opportunity of tracking by SPA the conditional operators which perform consecutive testing of E.

Conclusions. Proposed methods of counteracting access to the closed keys of information protection algorithm, based on the operation of modular exponentiation, can be used in order to increase information security in computer networks.

Key words: power analysis, smart cards, cryptographic algorithms, data security protocols, terminal computer devises.