УДК 004.056.55; 004.052.3

Карпінський М.П., Дубчак Л.О., Карпінський В.М.

СИСТЕМА ДЛЯ ПРОВЕДЕННЯ КРИПТОАНАЛІЗУ

Описано математичну основу для оцінки ризику витоку інформації про приватний ключ під час часового аналізу сучасних методів піднесення до степеня за модулем. Запропоновано можливі методи протидії. Результати даного дослідження можуть бути корисними для дослідження імовірності ризику успішної атаки аналізу енергоспоживання. Табл.1, Літ.7

Часовий аналіз (Timing Analysis – TA) - один з найпростіших, з точки зору застосування, методів проведення аналізу побічних каналів витоку інформації (Side Channel Attaks – SCA) для атаки криптографічних засобів захисту інформації. Такий тип атак може бути дуже ефективний, коли зловмисник має доступ до засобів шифрування [1, 2, 7]. Тому розробка методів протидії (контрзаходів), для зменшення ризику витоку конфіденційної інформації - дуже важливе та актуальне завдання.

Для дослідження шляху проведення ТА можна розглянути часовий аналіз виконання операції піднесення до степеня за модулем (медулярне експоненціювання) $f(n) = x^n \pmod m$, яка є базовою у використовуваних на даний час асиметричних криптосистемах типу RSA. Як відомо, цю операцію можна здійснити декількома способами. Найпростішим є бінарний метод з напрямком зчитування бітів зліва направо. Загальний час виконання алгоритму здійснення медулярного експоненціювання [2, 3]:

$$T(n) = t_i + c_i + \lceil \log n \rceil \cdot r_i + H(n) \cdot s_i, \qquad (1)$$

де t – час, витрачений процесором на переведення показника у двійкову систему числення, c – на просте присвоєння, r - піднесення до квадрату за модулем, s - множення за модулем, H(n) – вага Хемінга, $\lceil \log n \rceil$ - довжина бінарного зображення n.

Відповідно до цієї математичної моделі, біти експоненти впливають на значення часу t_i.

Оскільки прийнято вважати, що в умовах часового аналізу зловмисник може виміряти час здійснення шифрування повідомлення, то загальний час виконання алгоритму будь-якого методу модулярного експоненціювання в загальному записується з урахуванням впливу помилки вимірювання та відстані передачі.

Для реалізації часової атаки криптоаналітик на ідентичному комп'ютері проводить аналогічне до реального експоненціювання і обчислює часи $\tilde{T}_{i,k-1,0}$ та $\tilde{T}_{i,k-1,1}$ (табл.1).

В даній таблиці стовпчик, де є найменша різниця часів ΔT, відповідає значенню біта експоненти, що аналізується. Тобто криптоаналітик може знайти значення n_{k-1} [5, 6].

Будуючи аналогічні різниці часів зловмисник може знайти послідовність бітів експоненти для будь-якого методу. Нижче наведено шлях знаходження різниці між реальним та отриманим часами для кожного з розглянутих методів.

Таблиця 1

Різниці реального та отриманого часів для значень біта 0 та 1

Значення біта дорівнює 0	Значення біта дорівнює 1
$T_1 - \tilde{T}_{1,k-1,0}$	$T_1 - \tilde{T}_{1,k-1,1}$
$T_2 - \tilde{T}_{2,k-1,0}$	$T_2 - \tilde{T}_{2,k-1,1}$
$T_3 - \tilde{T}_{3,k-1,0}$	$T_3 - \tilde{T}_{3,k-1,1}$
…	…

Нехай j_0 - деяке значення j (порядковий номер біта у представленні експоненти) у відповідному алгоритмі та $g = \begin{cases} 0, \text{для експоненти } 0 \\ 1, \text{для експоненти } 1 \end{cases}$.

Звідси, зловмисник може обчислити для бінарного методу відповідний час:

$$\tilde{T}_{i,j_0,g} = t_i + c_i + \sum_{j=k-1}^{j_0+1} (r_{i,j} + s_{i,j}) + (r_{i,j_0} + \tilde{s}_{i,j_0,g}) \qquad (2)$$

А звідси відповідно:

$$\Delta T_i = e_i + \sum_{j=j_0-1}^{0} (r_{i,j} + s_{i,j}) + (s_{i,j_0} + \tilde{s}_{i,j_0,g}) \qquad (3)$$

Якщо $\tilde{s}_{i,j_0,g}$ визначене правильно, то $\tilde{s}_{i,j_0,g} \equiv s_{i,j_0}$. Звідси слідує, що

$$\Delta T_i = e_i + \sum_{j=j_0-1}^{0} (r_{i,j} + s_{i,j}) . \qquad (4)$$

Проте, на практиці $\tilde{s}_{i,j_0,g} \neq s_{i,j_0}$, а це означає, що правильно визначити $\tilde{s}_{i,j_0,g}$ дуже важко. Саме тому необхідно оцінити ймовірність успіху атаки.

Дисперсія випадкової змінної $T - \tilde{T}_{j_0,g}$ обчислюється з наступними умовами:

1. g визначене правильно (тобто правильно знайдене n_j), тоді дисперсія:

$$\sigma^2(\Delta T) = \sigma^2(e) + j_0\sigma^2(r) + \frac{1}{2} j_0\sigma^2(s) . \qquad (5)$$

Якщо припустити, що операції піднесення до квадрату та множення еквівалентні (а в більшості прикладних імплементацій так воно і є), тобто $r = s$, тоді:

$$\sigma^2(\Delta T) = \sigma^2(e) + \frac{3}{2} j_0\sigma^2(s) . \qquad (6)$$

2. g визначене неправильно, тоді можливі два випадки:

а) $\begin{cases}\tilde{s}_{i,j_0,g} \neq 0 \\ s_{i,j_0} \neq 0\end{cases}$, тоді:

$$\sigma^2(\Delta T) = \sigma^2(e) + \left(\frac{3}{2}j_0 + 2\right)\sigma^2(s). \quad (7)$$

б) $\left[\begin{cases}s_{i,j_0} \neq 0 \\ \tilde{s}_{i,j_0,g} = 0\end{cases}\right.$, звідси:
$\left.\begin{cases}\tilde{s}_{i,j_0,g} \neq 0 \\ s_{i,j_0} = 0\end{cases}\right.$

$$\sigma^2(\Delta T) = \sigma^2(e) + \left(\frac{3}{2}j_0 + 1\right)\sigma^2(s). \quad (8)$$

Ця дисперсія може бути використана як критерій правильності припущення бітів експоненти, оскільки колонка таблиці різниць часів з правильним припущенням має розкид на $\sigma^2(s)$ нижчий, ніж інші колонки значень. Тобто, рівень похибки вимірювання залежить від кількості вимірювань. Тому необхідно оцінити ризик витоку конфіденційної інформації під час проведення часового аналізу розглянутих методів модулярного експоненціювання.

Припустимо, що r, c та s рівномірно розподілені. Нехай $N(\mu_r, \sigma^2_r)$ – розподіл r, а $N(\mu_c, \sigma^2_c)$, $N(\mu_s, \sigma^2_s)$ - розподіли змінних c та s, відповідно.

Крім того, нехай $N(\mu_0, \sigma^2_0)$ – розподіл очікуваного значення ΔT.

Відповідно до аналізу ризику витоку конфіденційної інформації, проведеного в [3, 4]:

$$P(S^2_W > S^2_V) \approx \Phi\left(\frac{\sigma_s}{\sigma_0}\frac{\sqrt{K}}{2}\right), \quad (9)$$

де $\Phi\left(\frac{\sigma_s}{\sigma_0}\frac{\sqrt{K}}{2}\right)$ - площа під стандартною нормальною кривою від $-\infty$ до Z.

Звідси можна записати:

$$\frac{\sigma_s}{\sigma_0} = \sqrt{\frac{\sigma^2_s}{\frac{3}{2}j_0\sigma^2_s}} = \sqrt{\frac{2}{3j_0}}. \quad (10)$$

Ризик витоку конфіденційної інформації для бінарного методу можна оцінити як:

$$P(S^2_W > S^2_V) \approx P\left(Z > -\sqrt{\frac{K}{6j_0}}\right). \quad (11)$$

Зі збільшенням K, ймовірність успіху атаки також збільшується. Очевидно також, що ризик витоку конфіденційної інформації зростає у відповідності до кількості правильно визначених бітів, оскільки ентропія зменшується.

Отримані теоретичні результати можуть використовуватись:

a) для побудови аналогічних імовірнісних моделей для сучасних методів модулярного експоненціювання;
b) при дослідженні ризику витоку конфіденційної інформації при DPA.

На підставі проведених досліджень можна сформулювати два основні підходи для зменшення ризику витоку конфіденційної інформації під час здійснення часового аналізу:

- збільшення помилки вимірювання $\sigma^2(e)$ шляхом внесення випадкових обчислень, щоб зменшити можливість правильного визначення біт таємного ключа;
- зменшення K - кількості повідомлень, зашифрованих одним ключем, для зменшення ймовірності ризику витоку конфіденційної інформації до значення 0,5.

Література

1. Muir J. Techniques of Side Channel Cryptanalysis // A thesis presented to the University of Waterloo in fulfillment of the thesis requirement for the degree of Master of Mathematics in Combinatorics and Optimization, Waterloo, Ontario, Canada, 2001.
2. Васильцов І.В., Васильків Л.О. Стійкість сучасних алгоритмів модулярного експоненціювання до часового аналізу // Науково-технічний журнал „Захист інформації". - №1. - 2005. – С. 54-69.
3. Seong-Min H., Sang-Yeop O., Hyunsoo Y. New Modular Multiplication Algorithms for Fast Modular Exponentiation. – Spring-Verlag, 1998.
4. Vasyltsov I., Vasylkiv L., Vasylkiv N., Chyrka M. Investigation of Modern Exponentiation Algorithms // Proceedings of the International Conference TCSET'2004 "Modern Problems of Radio Engineering, Telecommunications and Computer Science" (24-28 February 2004, Lviv-Slavsko, Ukraine). – Lviv: Publishing House of Lviv Polytechnic National University. – 2004. – Pp. 291-293.
5. Biham E., Shamir A. Differential Cryptanalysis of the Data Encryption Standard, Springer-Verlag, 1993.
6. Karpinskyy M., Vasyltsov I., Vasylkiv L.: Estimation of the Secret Information Leakage Risk during Timing Analysis of Binary Modular Exponentiation Method // Proceedings of the 2-nd International Conference ACSN–2005 "Advanced Computer Systems and Networks: Design and Application" (21-23 September 2005, Lviv, Ukraine). – Lviv: Publishing House of Lviv Polytechnic National University. – 2005. – Pp. 132-135.
7. Зайчук А.В. Основные пути утечки информации и несанкционированного доступа в корпоративных сетях // Науково-технічний журнал "Захист інформації". – 2003. – № 4. – С. 19-24.