УДК 004.056.53

Ю. В. Горобець
Я. В. Іванчук

МЕТОД ВИЗНАЧЕННЯ ВРАЖЕНОСТІ КРИПТОСИСТЕМ

Вінницький національний технічний університет

Анотація

Запропоновано метод визначення враженості криптосистеми ECDSA до атак по побічним каналам на основі системних преривань. Розроблений підхід ідентифікації типу враженості на основі градчастих атак, який показав, що при наявності загальних бітів у ефемерних ключах, можна відновити приватний ключ відправника, при наявності необхідної кількості повідомлень, в залежності від кількості загальних бітів.

Ключові слова: градчастий метод, спільні біти, ділення по модулю, детермінована сигнатура, криптосистеми.

Abstract

A method for determining the vulnerability of cryptosystem ECDSA to attacks on side channels based on system interrupts is proposed. A method has been developed to identify the type of attack based on lattice attacks, which showed that if there are common bits in ephemeral keys, you can recover the sender's private key, if you have the required number of messages, depending on the number of common bits..

Keywords: lattice, shared bits, modular inverse, deterministic signature, cryptosystems

Вступ

Криптосистема – це реалізація криптографічних методів та їх інфраструктури для надання послуг інформаційної безпеки [1]. Криптосистеми перетворюють вихідні дані в нечитабельну форму, використовуючи ключі шифрування і розшифрування, що у свою чергу дозволяє забезпечувати конфіденційність інформації. В основі будь-якої системи шифрування є наявність інформації обміну даними про відкритий текст тільки у відправника і отримувача [2].

Метою роботи є розробка методу визначення враженості криптосистем до атак по побічним каналам на основі підходу системних переривань.

Результати дослідження

Для ідентифікації можливого потенційно небезпечного виду криптоатаки на приватний ключ, що базується алгоритмі шифрування DSA (ECDSA), необхідно проаналізувати математичний опис цього алгоритму [3].

Для використання ECDSA алгоритму, відправник обирає еліптичну криву E на кінцевому полі $\mathbb{F}_p$, точка $P \in E(\mathbb{F}_p)$ з простим порядком q розміром як мінімум 160 бітів. Відповідно відповідності до FIPS 186-3 бінарна довжина простого числа p має бути в множині $\{160, 224, 256, 512\}$. Крім того, для деякого випадкового вибраного $a \in \{1, ..., q-1\}$ обчислюється $Q = aP$. Публічний ключ відправника це (E, p, q, P, Q) і приватний ключ a. Також, відправник обирає хеш функцію $h: \{0,1\}^* \to \{0, ..., q-1\}$. Щоб підписати повідомлення m, відправник обирає випадкове число $k \in \{1, ..., q-1\}$, яке і є ефемерним ключем і обчислює $kP = (x, y)$ (де x та y розглядаються як цілі числа у діапазоні $\{0, ..., p-1\}$. Далі, обчислюється сигнатура повідомлення m, а саме пара чисел (r, s):

$$r = x \bmod q; \quad s = k^{-1}(h(m) + ar) \bmod q. \tag{1}$$

Для верифікації повідомлення, отримувач обчислює:

$$u_1 = s^{-1}h(m) \bmod q, \quad u_2 = s^{-1}r \bmod q, \quad u_1P + u_2Q = (x_0, y_0). \tag{2}$$

Сигнатура (1) валідна тоді і тільки тоді, коли $r = x_0 \bmod p$. Безпека цих криптосистем опирається на припущення, щоб єдиний спосіб підробити підпис – це або відновити приватний ключ a, або підробити ефемерний ключ k. Таким чином, параметри цих криптосистем вибрані таким чином, щоб

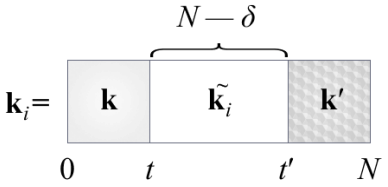
обчислення дискретних логарифмів є обчислювально нездійсненим.

Для здійснення потенційно-небезпечної криптоатаки зловмисником, що призведе до відкриття приватного ключа відправника, можна заблокувати деякі біти регістру або пам'яті, що містять значення ефемерного ключа k, при цьому саме значення заблокованих бітів, зловмиснику невідомо [4]. Припустимо, що зловмиснику вдалось зібрати n кількість зашифрованих повідомлень m_i (i=1, …, n) з відповідними сигнатурами (r_i, s_i), такими що всі відповідні ефемерні ключі k_i поділяють загалом δ бітів між більш значущими (MSB) та меншзначущими (LSB) бітами незалежно від поточної кількості повідомлень i. Таким чином, вони будуть відповідати наступній залежності для всіх i=1, ..., n:

$$k_i = k + 2^t \tilde{k}_i + 2^{t'} k', \tag{3}$$

де $0 \le k < 2^t, 0 \le k' < 2^{N-t'}, \delta = \mathrm{N} - t' + t, 0 \le k_i < 2^{N-\delta}$, k та k' загальні для всіх k_i.

На рисунку 1 зображена схема розміщення бітів у ефемерному ключі:



k – числове значення загальних більш значущих бітів (MSB), k' – числове значення загальних менш значущих бітів (LSB), $\tilde{k}_i$ - це числове значення поточних бітів, t – кількість загальних більш значущих бітів, t' – кількість загальних менш значущих бітів

Рисунок 1. Розрахункова схема ефемерного ключа

Слід зауважити, що значення змінних $k_i, k, \tilde{k}_i, k'$ невідомі. У n-ої кількості рівнянь (2), що визначають підпис:

$$\begin{cases} m_1 + ar_1 - s_1 k_1 \equiv 0 \pmod q; \\ m_2 + ar_2 - s_2 k_2 \equiv 0 \pmod q; \\ \dots \\ m_n + ar_n - s_n k_n \equiv 0 \pmod q, \end{cases} \tag{4}$$

де m_i – це повідомлення, a – це приватний ключ відправника, r_i – числове значення першої частини сигнатури, s_i – числове значення другої частини сигнатури, k_i – ефемерний ключ, i-індекс повідомлення.

Якщо в системі рівнянь (4) замінити параметри m_i, r_i, s_i на значення (3) і виключити загальні змінні k та k', тоді отримаємо:

$$\begin{cases} (s_1^{-1} m_1 - s_2^{-1} m_2) + a(s_1^{-1} r_1 - s_2^{-1} r_2) - 2^t (\tilde{k}_1 - \tilde{k}_2) \equiv 0 (\mathrm{mod}\, q); \\ (s_1^{-1} m_1 - s_3^{-1} m_3) + a(s_1^{-1} r_1 - s_3^{-1} r_3) - 2^t (\tilde{k}_1 - \tilde{k}_3) \equiv 0 (\mathrm{mod}\, q); \\ \dots \\ (s_1^{-1} m_1 - s_n^{-1} m_n) + a(s_1^{-1} r_1 - s_n^{-1} r_n) - 2^t (\tilde{k}_1 - \tilde{k}_n) \equiv 0 (\mathrm{mod}\, q). \end{cases} \tag{5}$$

Нехай $\alpha_i, \beta_i, \kappa_i \in Z$ є такими, що:

$$\begin{cases} \alpha_i := 2^{-t} (s_1^{-1} m_1 - s_i^{-1} m_i) \bmod q; \\ \beta_i := 2^{-t} (s_1^{-1} r_1 - s_i^{-1} r_i) \bmod q; \\ \kappa_i := \tilde{k}_1 - \tilde{k}_i. \end{cases} \tag{6}$$

Тоді, система рівнянь **Error! Reference source not found.** приймає наступний вигляд:

$$\begin{cases} \alpha_2 + a\beta_2 - k_2 \equiv 0 \pmod q; \\ \alpha_3 + a\beta_3 - \kappa_3 \equiv 0 \pmod q; \\ \alpha_n + a\beta_n - \kappa_n \equiv 0 \pmod q, \end{cases} \tag{7}$$

де a, κ_i і α_i, β_i – значення відомих та невідомих аргументів відповідно.

Тоді систему розв'язків можна представити у наступному вигляді:

$$L = \{(x_0, x_1, ..., x_n) \in \mathbb{Z}^{n+1} \mid x_0\alpha_i + x_1\beta_i - x_i \equiv 0 \,(\mathrm{mod}\, q)\}, \tag{8}$$

що утворює $(n+1)$ мірну маска-матрицю, натягнуту на вектори-стрічки базисної матриці:

$$M = \begin{pmatrix} 1 & 0 & \alpha_2 & \dots & \alpha_n \\ 0 & 1 & \beta_2 & \dots & \beta_n \\ 0 & 0 & q & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & q \end{pmatrix}. \tag{9}$$

Для знаходження короткого вектору у матриці **Error! Reference source not found.**, можуть бути застосовані LLL або BKZ алгоритми. Якщо система рівнянь **Error! Reference source not found.** має розв'язок (визначення значення короткого вектора $\bar{\upsilon}_0$ з елементами $v_0 = (1, a, \kappa_2, \kappa_3, ..., \kappa_n)$, що і буде тотожним елементом системи розв'язків **Error! Reference source not found.**, тоді і буде отримано значення приватного ключа *a* відправника [1-4].

Висновки

Розроблений у методі визначення враженості криптосистем підхід порядку отримання доступу до ключів повідомлень доводить, що алгоритм ECDSA є вразливим до криптоатак по побічним каналам, у випадку коли ефемерні ключі кожного зашифрованого повідомлення мають спільні біти у менш та/або більш значущих розрядах, що призводить до повної компроментації ступеню захисту даного типу криптосистеми.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone, *Handbook of applied cryptography*. 1996.

2. N. A. Howgrave-Graham and N. P. Smart, "Lattice Attacks on Digital Signature Schemes," *Des. Codes, Cryptogr.*, vol. 23, no. 3, 2001, doi: 10.1023/A:1011214926272.

3. Іванчук Я. В. Порівняльний аналіз HTTP1 та HTTP2 протоколів / Я. В. Іванчук, Ю. В. Горобець // Матеріали конференції «Молодь в науці: дослідження, проблеми, перспективи (МН-2021)», Вінниця, 2021. [Електронний ресурс]. - Режим доступу: https://conferences.vntu.edu.ua/index.php/mn/mn2021/paper/viewFile/13131/11029.

4. Kvyetnyy R. N. Algorithm for increasing the stability level of cryptosystems / R. N. Kvyetnyy, Y. V. Ivanchuk, A. A. Yarovyi, Y. V. Horobets // Inforrnation Technology and lmplementation (Satellite): Conference Proceedings. December 02, 2021, Kyiv, Ukraine / Taras Shevchenko National University ofKyiv and [etc]. – Kyiv: – 2021. 85-88 p.

Горобець Юрій Володимирович — аспірант кафедри комп`ютерних наук, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: ysparrow@ysparrow.com

Іванчук Ярослав Володимирович – д-р техн. наук, доцент, професор кафедри комп'ютерних наук, Вінницький національний технічний університет, Вінниця, e-mail: ivanchuck@ukr.net.

Horobets Yurii V. — graduate student of computer science department Vinnytsia National Technical University, Vinnytsia, Ukraine, email: ysparrow@ysparrow.com.

Ivanchuk Yaroslav V. — Dr. Sc. (Eng.), Professor of the Computer Science Department, Vinnytsia National Technical University, Vinnytsia, e-mail: ivanchuck@ukr.net.