УДК 003.26.09:519.2

КРИПТОГРАФІЧНІ АТАКИ НА RSA НА ОСНОВІ ІНФОРМАЦІЇ З ПОБІЧНОГО КАНАЛУ

Є. Ю. Толмачов[a]

[1] *Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», НН Фізико-технічний інститут*

Анотація

Темою даної роботи є доповнення атак на основі інформації з побічних каналів на прикладі RSA. Більшість таких атак засновано на статистичних методах та фізичних вимірах інформації з побічних каналів, через що отриманий в результаті атаки ключ може мати помилки. Ціллю роботи є дослідження алгоритмів виправлення помилок в знайденому в результаті атаки ключі. В ході роботи розглянуто дві криптографічні моделі та алгоритми атаки на них. Теоретично виведено та підраховано ймовірність успіху атаки та її складність.

Ключові слова: RSA, криптоаналіз, атака за побічними каналами, виправлення помилок

Вступ

Криптографічні алгоритми на практиці завжди виконуються на фізичному пристрої. І під час виконання утворюють багато інформації про алгоритми не передбаченної з їхнього математичного опису. Атаки на основі цієї інформації можуть бути на багато швидші та ефективніші в порівнянні з атаками на основі суто математичного аналізу. Такі атаки називають атаками на побічні канали (Side Channel Attacks, надалі — SCA-атаки). В своїй роботі професор Університету Белфордшира Сонг Йан зібрав ряд SCA-атак на RSA[1]. Більша частина атак заснована на вимірах фізичних величин та статистичних методах аналізу отриманих величин. І в вимірах і при аналізі з використанням статистичних методів можуть виникати помилки. Але це не означає що з отриманого хибного ключа неможливо отримати істиний. В цій роботі досліджуватимуться атаки з виправленям помилок.

1. Модель 1

В обох моделях припускається що відбулася SCA-атака на RSA алгоритм за побічним каналом енергоспостереження або часу виконання. Відкритий ключ — (N, e). В результаті SCA-атаки криптоаналітик E знайшов ключ $\tilde{d}$ що може мати помилки і бути хибним.

Припущення моделі 1

Нехай модель 1 визначається наступним чином:

1. Атака проводиться на основі відкритого тексту

2. За спостереженням криптоаналітик E за інформацією про виконання операції

$$M = C^d \bmod N \tag{1}$$

$$\text{або} \quad S = (H(M))^d \bmod N, \tag{2}$$

де H — геш-функція, S — підпис, знаходить біти секретного ключа з деякою помилкою

$$\tilde{d} = \tilde{d}_\beta, \tilde{d}_{\beta-1}, \tilde{d}_{\beta-2}, ..., \tilde{d}_2, \tilde{d}_1, \tilde{d}_0, \quad \tilde{d}_i \in \{0, 1\} \tag{3}$$

3. Вважаємо, що

$$\tilde{d}_i = d_i \oplus \varepsilon_i,$$

де $d_i \in \{0, 1\}$ — істинне значення біту, $\varepsilon_i \in \{0, 1\}$ — випадкові незалежні величини. Нехай ймовірність помилки в кожному біті визначається таким чином: $Pr\{\varepsilon_i = 1\} = p$, $0 \le p \le \frac{1}{2}$, $i = \overline{0, \beta}$. Якщо $p = 0$, то помилок немає і $\tilde{d}$ — істиний ключ d. Якщо ж $p = \frac{1}{2}$, то з (3) знайти якусь інформацією про істиний ключ d неможливо.

4. Криптоаналітик E може перевірити чи є $\tilde{d}$ ключем без помилок чи ключем хибним підстановкою в рівняння (1) або (2).

Алгоритм атаки

Мета другої половини атаки — із ключа з помилками (3) знайти справжній ключ d. При цьому в (3) можливі $1, 2, ..., k, ...$ помилок.

Алгоритм 1. Алгоритм виправлення до k помилок
Вхід: $\tilde{d}$, N, M, C та k
1. Якщо $C^{\tilde{d}} = M \bmod N$
   2. $d = \tilde{d}$, алгоритм завершує роботу
3. Покласти $i = 1$
4. Поки $i \le k$
   5. Cm_i — всі булеві вектори розміру $|\tilde{d}|$ та ваги i
   6. Для всіх j з Cm_i
      7. $\tilde{d}' = \tilde{d} \oplus j$
      8. Якщо $C^{\tilde{d}'} = M \bmod N$

[a] mr_yevhenii.tolmachov@gmail.com

9. $d = \tilde{d}'$, алгоритм завершує роботу
10. $i = i + 1$
11. Повернути помилку, алгоритм завершує роботу

Вихід: d

В якості рівняння для перевірки істиності ключа окрім (1) можна використовувати рівняння (2).

Помилок в ключі може бути більше k, отже алгоритм має певну ймовірність успіху.

Аналіз алгоритму

Ймовірність успіху алгоритму 1 що виправляє до k помилок дорівнювати

$$\Pr\{\text{успіху}\} = \sum_{i=0}^{k} C_{\beta+1}^{i} \cdot p^i \cdot (1-p)^{\beta+1-i}$$

Ймовірність успіху при різних значеннях $(\beta+1, p, k)$ наведено у таблиці 3.

Складність виконання алгоритму 1 в найгіршому випадку в операціях множення за модулем N

$$2\beta \cdot \sum_{i=0}^{k} C_{\beta+1}^{i}$$

Складність при різних значеннях $(\beta+1, k)$ наведено у таблиці 2.

Складність виконання алгоритму 1 у середньому

$$2\beta \cdot \left(p_0 + \sum_{i=1}^{k} p_i \cdot \left(\sum_{j=0}^{i-1} C_{\beta+1}^{j} + \frac{1}{2} C_{\beta+1}^{i} \right) + \right.$$
$$\left. + \sum_{i=0}^{k} C_{\beta+1}^{i} \left(1 - \sum_{i=0}^{k} p_i \right) \right)$$
$$\text{де} \quad p_i = C_{\beta+1}^{i} \cdot p^i \cdot (1-p)^{\beta+1-i} \quad (4)$$

2. Модель 2

Розглянемо другу модель. Нехай криптоаналітик E знає не одне, а декілька рівнянь типу (1) та (2).

Припущення моделі 2

Нехай модель 2 визначається наступним чином:

$$M_i = C_i^d \bmod N, \quad i = \overline{1,r} \quad (5)$$
$$S_i = (H(M_i))^d \bmod N, \quad i = \overline{1,r} \quad (6)$$

І відповідно

$$\tilde{d}_j = \tilde{d}_\beta^{(j)}, \tilde{d}_{\beta-1}^{(j)}, \tilde{d}_{\beta-2}^{(j)}, ..., \tilde{d}_2^{(j)}, \tilde{d}_1^{(j)}, \tilde{d}_0^{(j)}$$
$$\tilde{d}_i^{(j)} \in \{0,1\}, \quad j = \overline{1,r} \quad (7)$$
$$\tilde{d}_i^{(j)} = d_i^{(j)} \oplus \varepsilon_i^{(j)},$$

де $d_i^{(j)} \in \{0,1\}$ — істинне значення біту, $\varepsilon_i^{(j)} \in \{0,1\}$ — випадкові незалежні величини. $Pr\{\varepsilon_i^{(j)} = 1\} = p$, $0 \le p \le \frac{1}{2}$, $\quad i = \overline{0,\beta}$, $\quad j = \overline{1,r}$.

Алгоритм атаки

Алгоритм 2. Алгоритм виправлення до k помилок для моделі 2.

Вхід: N, M, C, k та $\tilde{d}_j$, $j = \overline{1,r}$

1. Покласти $i = 0$
2. Поки $i \le \beta + 1$
3. $$\tilde{d}_i = \begin{cases} 1, & \sum_{j=0}^{r} \tilde{d}_i^{(j)} \ge \frac{r}{2}, \\ 0, & \sum_{j=0}^{r} \tilde{d}_i^{(j)} < \frac{r}{2}. \end{cases}$$
4. $i = i + 1$
5. Запустити алгоритм 1 з параметрами $\tilde{d}$, N, M, C та k

Вихід: d

Ця модель також може мати більше k помилок, тому атака на неї має певну ймовірність успіху.

Аналіз алгоритму

Ймовірність успіху алгоритму 2 що виправляє до k помилок дорівнює

$$\Pr\{\text{Успіху}\} = \sum_{i=0}^{k} C_{\beta+1}^{i} \cdot q^i \cdot (1-q)^{r-i},$$

$$\text{де} \qquad q = \sum_{i=0}^{\lfloor r/2 \rfloor} C_r^i \cdot p^{r-i} \cdot (1-p)^i$$

Ймовірність успіху при різних значеннях $(\beta+1, p, r, k)$ наведено у таблиці 3.

Складність виконання алгоритму 2 в найгіршому випадку

$$O\left(r \cdot (\beta+1)\right) \text{додавань} + O\left(2\beta \cdot \sum_{i=0}^{k} C_{\beta+1}^{i}\right) \text{множень}$$

Складність виконання алгоритму 2 в середньому

$$2\beta \cdot \left(q_0 + \sum_{i=1}^{k} q_i \cdot \left(\sum_{j=0}^{i-1} C_{\beta+1}^{j} + \frac{1}{2} C_{\beta+1}^{i} \right) + \right.$$
$$\left. + \sum_{i=0}^{k} C_{\beta+1}^{i} \left(1 - \sum_{i=0}^{k} q_i \right) \right) \text{множень},$$
$$r \cdot (\beta+1) \text{ додавань}$$
$$\text{де} \quad q_i = C_{\beta+1}^{i} \cdot q^i \cdot (1-q)^{\beta+1-i},$$
$$q = \sum_{i=0}^{r/2} C_r^i \cdot p^{r-i} \cdot (1-p)^i \quad (8)$$

Складністю додавань можна знехтувати. В такому разі в найгіршому випадку складність в операціях множеннях дорівнює складності алгоритму 1. Але ймовірність успіху буде значно більшою.

Результати експериментальних обчислень наведено у таблицях 1, 2 та 3.

Табл. 1. Ймовірність успіху атаки в моделі 2 при ймовірності помилки p, розмірі ключа $\beta+1$, наявності r вимірів для ключа та k виправлень

		$\beta+1=1024$		
		$p=0,3$		
$k=$	0	1	2	3
r = 2	$1,1438938809\cdot10^{-42}$	$1,1699143241\cdot10^{-40}$	$5,9774765272\cdot10^{-39}$	$2,0343074357\cdot10^{-37}$
r = 3	$6,7227728081\cdot10^{-13}$	$1,9775177856\cdot10^{-11}$	$2,9091660478\cdot10^{-10}$	$2,8540808852\cdot10^{-9}$
r = 4	$1,3384157622\cdot10^{-39}$	$1,2653104796\cdot10^{-37}$	$5,9759426222\cdot10^{-36}$	$1,8800033610\cdot10^{-34}$
r = 5	$1,2488322476\cdot10^{-14}$	$4,1860451836\cdot10^{-13}$	$7,0155393779\cdot10^{-12}$	$7,8385931854\cdot10^{-11}$
		$p=0,1$		
k =	0	1	2	3
r = 2	0,000033918705402	0,000384754607741	0,002197406769827	0,008434883233301
r = 3	0,358971478189710	0,726926226604388	0,915323477669561	0,979568386107535
r = 4	0,022464328728460	0,107893264477120	0,270172228996970	0,475479089860619
r = 5	0,624284944861740	0,918483456604817	0,987737281192155	0,998594811661171
		$\beta+1=2048$		
		$p=0,3$		
k =	0	1	2	3
r = 2	$1,3084932107\cdot10^{-84}$	$2,6634307410\cdot10^{-82}$	$2,7094541336\cdot10^{-80}$	$1,8366712549\cdot10^{-78}$
r = 3	$4,5195674229\cdot10^{-25}$	$2,6136848851\cdot10^{-23}$	$7,5562210166\cdot10^{-22}$	$1,4561111768\cdot10^{-20}$
r = 4	$1,7913567526\cdot10^{-78}$	$3,3691094124\cdot10^{-76}$	$3,1667995399\cdot10^{-74}$	$1,9835230937\cdot10^{-72}$
r = 5	$1,5595819826\cdot10^{-28}$	$1,0299378232\cdot10^{-26}$	$3,3999904255\cdot10^{-25}$	$7,4808361748\cdot10^{-24}$
		$p=0,1$		
k =	0	1	2	3
r = 2	0,000000001150479	0,000000024950278	0,000000271001738	0,000001966022905
r = 3	0,128860522153705	0,393031042044385	0,663680218328781	0,848447724060470
r = 4	0,000504646065220	0,004342853456381	0,018931932528906	0,055882732620855
r = 5	0,389731692381026	0,757059095744892	0,930080100184675	0,984385230057266

Табл. 2. Складність атаки для моделі 1, в операціях піднесення до степені

		$\beta+1=1024$		
$k=$	0	1	2	3
$C^i_{\beta+1}$	1	1025	524801	178957825
$2^{\lceil\log_2(C^i_{\beta+1})\rceil}$	2^1	2^{11}	2^{20}	2^{28}
$k=$	4	5	6	7
$C^i_{\beta+1}$	45723987201	9336909979905	1587289997740801	$2,310667533321111\cdot10^{17}$
$2^{\lceil\log_2(C^i_{\beta+1})\rceil}$	2^{36}	2^{44}	2^{51}	2^{58}
		$\beta+1=2048$		
$k=$	0	1	2	3
$C^i_{\beta+1}$	1	2049	2098177	1431657473
$2^{\lceil\log_2(C^i_{\beta+1})\rceil}$	2^1	2^{12}	2^{22}	2^{31}
$k=$	4	5	6	7
$C^i_{\beta+1}$	732293847553	299508757152257	12032894512403970	$2,9779114853401\cdot10^{22}$
$2^{\lceil\log_2(C^i_{\beta+1})\rceil}$	2^{40}	2^{49}	2^{57}	2^{65}

Табл. 3. Ймовірність успіху атаки в моделі 1 при ймовірності помилки p, розмірі ключа $\beta+1$ та k виправлень

$\beta + 1 = 1024$				
k =	0	1	2	3
p = 0.0001	0.90266379012	0.99510580643	0.99983468845	0.99999580181
p = 0.001	0.35897147818	0.72692622660	0.91532347766	0.97956838610
p = 0.01	$3.391870540 \cdot 10^{-5}$	0.00038475460	0.00219740676	0.00843488323
p = 0.1	$1.394214727 \cdot 10^{-47}$	$1.600248681 \cdot 10^{-45}$	$9.175533669 \cdot 10^{-44}$	$3.504292371 \cdot 10^{-42}$
k =	4	5	6	7
p = 0.0001	0.99999991464	0.99999999855	0.99999999997	0.99999999999
p = 0.001	0.99598331391	0.99933531118	0.99990516190	0.99998811743
p = 0.01	0.02451686169	0.05765548396	0.11450439995	0.19801406299
p = 0.1	$1.002876343 \cdot 10^{-40}$	$2.294043386 \cdot 10^{-39}$	$4.369102693 \cdot 10^{-38}$	$7.126137135 \cdot 10^{-37}$
$\beta + 1 = 2048$				
k =	0	1	2	3
p = 0.0001	0.81480191799	0.98169003962	0.99877274713	0.99993790430
p = 0.001	0.12886052215	0.39303104204	0.66368021832	0.84844772406
p = 0.01	$1.150478576 \cdot 10^{-9}$	$2.495027780 \cdot 10^{-8}$	$2.710017375 \cdot 10^{-7}$	$1.966022904 \cdot 10^{-6}$
p = 0.1	$1.943834705 \cdot 10^{-94}$	$4.442742209 \cdot 10^{-92}$	$5.074706870 \cdot 10^{-90}$	$3.862581050 \cdot 10^{-88}$
k =	4	5	6	7
p = 0.0001	0.99999747892	0.99999991457	0.99999999751	0.99999999993
p = 0.001	0.94300466831	0.98169824069	0.99488659043	0.99873767154
p = 0.01	$1.071935191 \cdot 10^{-5}$	$4.686441148 \cdot 10^{-5}$	0.00017118151	0.00053749538
p = 0.1	$2.203959280 \cdot 10^{-86}$	$1.005582173 \cdot 10^{-84}$	$3.821627647 \cdot 10^{-83}$	$1.244315288 \cdot 10^{-81}$

Висновки

В цій роботі розглянуто дві криптографічні моделі та атаки на них. Обраховано ймовірність успіху та складність атак. Із отриманих результатів можна зробити висновок, що за допомогою ключа з помилками при певних умовах можна за практичний час зі значущою ймовірністю відтворити істиний ключ. І при наявності у криптоаналітика декількох незалежних вимірів ключа з помилками можна значно покращити ймовірність виправлення помилок, при цьому витрати часу на алгоритм виправлення в найгіршому випадку майже не зміниться, а в середньому зменшиться.

Перелік використаних джерел

1. Yan Song Y. Cryptanalytic Attacks on RSA. — 2008. — P. 255 c. — Access mode: https://fdocuments.in/document/cryptanalytic-attacks-on-rsa.html?page=1.