Information Processing Letters ••• (••••) •••–•••

Contents lists available at ScienceDirect

Information Processing Letters

www.elsevier.com/locate/ipl

Improved reconstruction of RSA private-keys from their fraction

Shigeyoshi Imai, Kaoru Kurosawa *

Ibaraki University, Japan

ARTICLE INFO

Article history:
Received 3 July 2012
Accepted 19 February 2015
Available online xxxx
Communicated by D. Pointcheval

Keywords:
Cryptography
RSA
Attack
Erasure

ABSTRACT

In PKCS#1 standard, (p, q, d, d_p, d_q, q_p) is used as a private-key of RSA. Heninger and Shacham showed a method which can reconstruct $\mathsf{SK} = (p, q, d, d_p, d_q)$ from a random δ fraction of their bits. It succeeds with high probability for small e when $\delta \geq 0.27$.
In this paper, we show how to reduce the search range of a certain parameter k, which is a bottleneck of Heninger–Shacham attack. The bigger δ, the better our method is. More precisely, the search range of k is reduced from e to $2e\left(1 - \frac{1}{2-\delta}\right)$.

1. Introduction

RSA is the most popular public-key cryptosystem. Its public-key is $N = pq$ and e, where p and q are large primes. The secret-key is d such that

$$ed = 1 \bmod (p-1)(q-1). \tag{1}$$

In PKCS#1 standard, it is recommended to use a redundant tuple (p, q, d, d_p, d_q, q_p) as a private-key in order to allow for a fast Chinese Remainder type decryption process, where

$$d_p = d \bmod p - 1$$

$$d_q = d \bmod q - 1$$

$$q_p = q^{-1} \bmod p$$

Motivated by cold boot attack [2], Heninger and Shacham showed a method which can reconstruct $\mathsf{SK} = (p, q, d, d_p, d_q)$ from a random δ fraction of their bits [3]. It succeeds with high probability for small e when $\delta \geq 0.27$.

The reason why e must be small is as follows. From Eq. (1), it holds that

$$ed = 1 + k(p-1)(q-1)$$

for some k. The method of Heninger and Shacham first finds this k by exhaustive search over $1 \leq k \leq e-1$. Hence e must be small. In particular, it is so even for large δ.

In this paper, we show how to reduce the search range of k. The bigger δ, the better our method is. More precisely, the search range of k is reduced from e to $2e\left(1 - \frac{1}{2-\delta}\right)$.

2. Heninger and Shacham attack

Let $a[i]$ denote the i-th bit of a positive integer a, where $a[0]$ denotes the least significant bit of a. Define $a[0, i-1]$ as

$$a[0, i-1] = a \bmod 2^i.$$

In RSA, the following equations hold:

$$N = pq, \tag{2}$$

$$ed = 1 + k(p-1)(q-1), \tag{3}$$

* Corresponding author.
E-mail address: kurosawa@mx.ibaraki.ac.jp (K. Kurosawa).

http://dx.doi.org/10.1016/j.ipl.2015.02.013
0020-0190/

$$ed_p = 1 + k_p(p-1), \tag{4}$$

$$ed_q = 1 + k_q(q-1). \tag{5}$$

Assume that we know δ fraction of $\mathsf{SK} = (p, q, d, d_p, d_q)$. In Heninger–Shacham attack, we first determine the value k of Eq. (3). Since we have $0 < k < e\frac{d}{\phi(N)} < e$, we can determine the correct k by exhaustive search over $0 < k < e$.

For each k', we define

$$\tilde{d}(k') \equiv \lfloor \frac{1 + k'(N+1)}{e} \rfloor. \tag{6}$$

As Boneh, Durfee, Frankel observe [1], when k' equals k, this gives an approximation for d:

$$0 \le \tilde{d}(k) - d \le k(p+q)/e < p + q.$$

In particular, when p and q are balanced, we have $p + q < 3\sqrt{N}$, which means that $\tilde{d}(k)$ agrees with d on their $\lfloor n/2 \rfloor - 2$ most significant bits.

Hence we enumerate $\tilde{d}(1), \cdots, \tilde{d}(e-1)$ and check which of these agrees, in its more significant half, with the known bits of $\tilde{d}$. Provided that $\delta\frac{n}{2} \gg \lg e$, there will be just one value of k' for which $\tilde{d}(k')$ matches; that value is k.

Once k is found, we can compute k_p, k_q of Eqs. (4) and (5) as follows. It holds that [3]

$$k_p + k_q = k(N-1) + 1 \bmod e \tag{7}$$

$$k_p k_q = -k \bmod e \tag{8}$$

Hence k_p is a solution of the following quadratic equation.

$$x^2 - (k(N+1)+1)x - k = 0 \bmod e.$$

When e is a prime, it has two roots. When e has m distinct primes, it has 2^m roots. One of them is the correct value of k_p. The value of k_q is automatically derived from k_p by using Eq. (7).

Next since p, q are prime, we have $p[0] = q[0] = 1$. In general, suppose that we have a partial solution $p[0, i-1]$, $q[0, i-1]$, $d[0, i-1]d_p[0, i-1]$, $d_q[0, i-1]$ of level i. Heninger and Shacham derived four linear equations on five unknown variables $p[i]$, $q[i]$, $d[i]$, $d_p[i]$, $d_q[i]$.[1]

Their method then creates all possible solutions $p[0, i]$, $q[0, i]$, $d[0, i]d_p[0, i]$, $d_q[0, i]$ of level $i+1$ by appending $p[i]$, $q[i]$, $d[i]$, $d_p[i]$, $d_q[i]$ to $p[0, i-1]$, $q[0, i-1]$, $d[0, i-1]d_p[0, i-1]$, $d_q[0, i-1]$ and prunes the incorrect ones by checking the validity of the available relation. In this way, their method can reconstruct p, q, d, d_p, d_q if $\delta \ge 0.27$ for small e.

3. How to avoid exhaustive search on k

The method of Heninger and Shacham [3] works when e is small because it includes the exhaustive search on k of Eq. (3), where $1 \le k \le e-1$. This is so even if large fraction of SK is known. In this section we propose a method which reduces this search range of k.

[1] We assume that $k = k_p = k_q = 1 \bmod 2$ for simplicity.

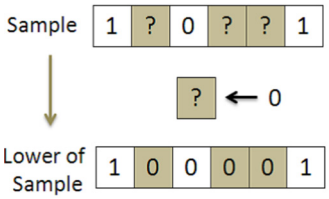

Fig. 1. How to derive the lower bound.

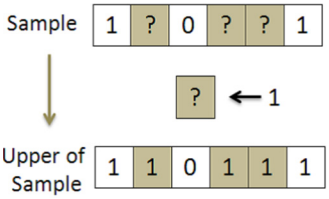

Fig. 2. How to derive the upper bound.

From Eq. (3), we have

$$k = \frac{ed-1}{N-(p+q)+1}. \tag{9}$$

In the above equation, some bits of p, q, and d are unknown.

First we derive lower bounds on p, q, and d. This is done by simply substituting 0s into their unknown bits (see Fig. 1). In this way, we can obtain lower bounds on p, q, and d. Let denote them by p_L, q_L, and d_L.

Similarly we can derive upper bounds on p, q, and d. This is done by simply substituting 1s into their unknown bits (see Fig. 2). Let denote them by p_U, q_U, and d_U.

By substituting p_L, q_L, and d_L into Eq. (9), we can compute a lower bound k as follows.

$$k_L = \frac{ed_L - 1}{N-(p_L+q_L)+1}. \tag{10}$$

Similarly, by substituting p_U, q_U, and d_U into Eq. (9), we can compute an upper bound on k as follows.

$$k_U = \frac{ed_U - 1}{N-(p_U+q_U)+1}. \tag{11}$$

Therefore we see that

$$k_L \le k \le k_U.$$

Further suppose that $p < q < 2p$. Then it is easy to see that

$$2\sqrt{N} < p + q < 3\sqrt{N}.$$

Define

$$k'_L = \frac{ed_L - 1}{N - 2\sqrt{N} + 1}$$

$$k'_U = \frac{ed_U - 1}{N - 3\sqrt{N} + 1}$$

Then we obtain that

$$k'_L \le k \le k'_U.$$

Please cite this article in press as: S. Imai, K. Kurosawa, Improved reconstruction of RSA private-keys from their fraction, Inf. Process. Lett. (2015), http://dx.doi.org/10.1016/j.ipl.2015.02.013

Table 1
$T =$ (new search range/previous search range).

$\downarrow e \rightarrow \delta$	0.27	0.4	0.5	0.6	0.7
$2^{16}+1$	0.47	0.38	0.32	0.23	0.16
$2^{30}+1$	0.46	0.37	0.32	0.24	0.18
$2^{40}+1$	0.47	0.38	0.31	0.24	0.18
$2^{50}+1$	0.46	0.37	0.32	0.24	0.18

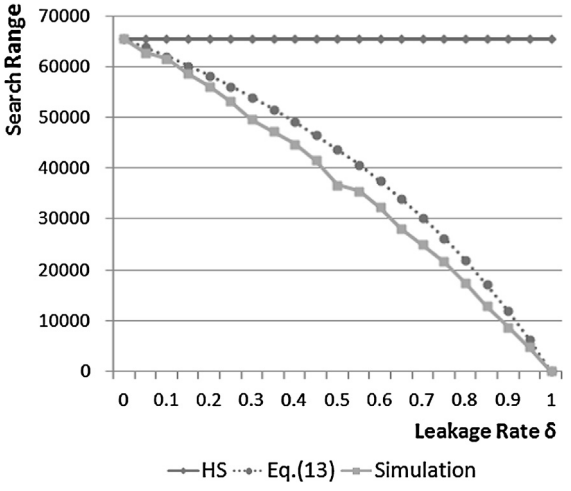

Fig. 3. Comparison for $e = 2^{16}+1$.

Finally define

$$k''_L = \max\{k_L, k'_L\}$$
$$k''_U = \min\{k_U, k''_U\}$$

Then we have

$$k''_L \le k \le k''_U.$$

This means that the search range of k is reduced to the above from $1 \le k \le e-1$. Hence we define the reduced ratio as follows.

$$T = \frac{k''_U - k''_L}{e}. \tag{12}$$

4. Formula on the search range

In this section, we derive a formula on the search range of the proposed method. Suppose that N and d are n-bit long. Let $d[i]$ denote the ith bit of d, where $d[n-1]$ is the most significant bit. If $d[n-1]$ is unknown, then $d_U - d_L \approx 2^n$. If $d[n-1]$ is known and $d[n-2]$ is known, then $d_U - d_L \approx 2^{n-1}$. Therefore

$$E[d_U - d_L] \approx 2^n\delta + 2^{n-1}\delta(1-\delta) + \cdots$$

Hence

$$\begin{aligned} E[T] &= E[k''_U - k''_L]/e \\ &\approx E[d_U - d_L]/N \\ &\approx E[d_U - d_L]/2^n \\ &\approx (\delta + 2^{-1}\delta(1-\delta) + \cdots) \\ &= (1-\delta)/(1-2^{-1}\delta) \\ &= 2\left(1 - \frac{1}{2-\delta}\right) \end{aligned}$$

We then have a formula on the search range of the proposed method as

$$E[k''_U - k''_L] \approx 2e\left(1 - \frac{1}{2-\delta}\right) \tag{13}$$

Simulation. Suppose that $|N| = 1024$ and δ fraction bits of p, q, d are known. Table 1 shows the average of T over 100 simulations. Fig. 3 shows a comparison for $e = 2^{16}+1$.

From Table 1 and Fig. 3, we can see that the bigger δ is, the better our method is. We can also see that Eq. (13) is a good approximation.

References

[1] D. Boneh, G. Durfee, Y. Frankel, An attack on RSA given a small fraction of the private key bits, in: Asiacrypt 1998, 1998, pp. 25–34.
[2] J. Alex Halderman, Seth D. Schoen, Nadia Heninger, William Clarkson, William Paul, Joseph A. Calandrino, Ariel J. Feldman, Jacob Appelbaum, Edward W. Felten, Lest we remember: cold boot attacks on encryption keys, in: USENIX Security Symposium 2008, 2008, pp. 45–60.
[3] N. Heninger, H. Shacham, Reconstructing RSA private keys from random key bits, in: CRYPTO 2009, 2009, pp. 1–17.

Please cite this article in press as: S. Imai, K. Kurosawa, Improved reconstruction of RSA private-keys from their fraction, Inf. Process. Lett. (2015), http://dx.doi.org/10.1016/j.ipl.2015.02.013