Known–Plaintext–Only Attack on RSA–CRT with Montgomery Multiplication

Martin Hlaváč

Department of Algebra, Charles University in Prague,
Sokolovská 83, 186 75 Prague 8, Czech Republic
hlavm1am@artax.karlin.mff.cuni.cz

Abstract. The paper describes a new attack on RSA–CRT employing Montgomery exponentiation. Given the amount of so-called final subtractions during the exponentiation of a known message (not chosen, just known), it creates an instance of the well known Hidden Number Problem (HNP, [2]). Solving the problem reveals the factorization of RSA modulus, i.e. breaks the scheme.

The main advantage of the approach compared to other attacks [14,17] is the lack of the chosen plaintext condition. The existing attacks, for instance, cannot harm so-called Active Authentication (AA) mechanism of the recently deployed electronic passports. Here, the challenge, i.e. the plaintext, is jointly chosen by both parties, the passport and the terminal, thus it can not be conveniently chosen by the attacker. The attack described here deals well with such a situation and it is able to solve the HNP instance with 150 measurements filtered from app. 7000. Once the secret key used by the passport during AA is available to the attacker, he can create a fully functional copy of the RFID chip in the passport he observes.

A possible way to obtain the side information needed for the attack within the electromagnetic traces is sketched in the paper. Having no access to high precision measurement equipment, its existence has not been experimentally verified, yet. The attack, however, should be taken into account by the laboratories testing the resilience of (not only) electronic passports to the side channel attacks.

Keywords: RSA, Chinese Remainder Theorem, Montgomery exponentiation, Hidden Number Problem, side channel attack, electronic passport.

Introduction

Motivated by the recent deployment of the electronic passports, we study the security of it anti-cloning measure called Active Authentication (AA, [5]). As it is an RSA based challenge-response protocol, one can try to attack AA with the well-known Schindler's adaptive chosen plaintext attack [14] or Tomoeda's chosen plaintext attack [17]. It turns out, however, both of these approaches fail in this scenario due to their chosen plaintext condition as the plaintext used in AA is chosen jointly by both parties.

C. Clavier and K. Gaj (Eds.): CHES 2009, LNCS 5747, pp. 128–140, 2009.

In this paper we present a new side channel attack on RSA-CRT with Montgomery multiplication [10]. Being a known plaintext attack, it suits well the AA scenario. The side information that is available to the attacker is the same as in [17], i.e. the amount of the final subtractions during Montgomery exponentiation within one branch of the CRT computation (e.g. exponentiation $\mathbf{mod}\, p$). It is shown such information can be used to obtain modular approximations of one of the factors of the RSA modulus. The side information is stronger variant of the simple timing information used in [14].

The approximations suit perfectly as the input to the well-known Hidden Number Problem [2] which can be efficiently solved using lattice reduction techniques [9,4]. The attack presented using this side information is of independent merit and can be applied in other scenarios where the side information is available.

The existence of the side information in the electronic passport is yet to be proven, however. Our simple measurements show the square-and-multiply-always exponentiation can be identified very well in the electromagnetic trace surrounding the chip. More precise measurements are needed, however, to support the hypothesis that Montgomery multiplication is used and that the amount of the final subtractions is revealed.

As the existence of the side channel implies the insecurity of AA security measure, the attack should be taken into account by the testing laboratories. No further research is needed for this purpose. On the other hand, no theoretical guarantee is given in the paper that the attack always works. Further research is necessary for more theoretical results. The attack validity is supported by the experiments with the emulated side information. As the electronic passports are already deployed, we believe the attack should be made public at this stage already.

The paper is organized as follows. The electronic passport and AA are overviewed together with our simple electromagnetic measurements in Section 1. The RSA-CRT scheme with Montgomery multiplication is described in Section 2. Briefly overviewing the existing attacks, we elaborate the conversion to HNP here, as well. Remarks on HNP relevant to the scenario and the results of the experiments with the emulated observations are given in Section 3. Several possible directions for future research are suggested in Section 4.

1 e-Passport

The electronic passport is a modern travel document equipped with a RFID (Radio Frequency IDentification) chip compatible with ISO 14443 [7] (on the physical layer to the transport layer) and with ISO 7816 [8] (the application layer).

The chip contains digitally signed electronic copy of the data printed on the passport: the machine readable zone (MRZ) including the passport no., the photo of the holder, as well as the public and private key for the Active Authentication (AA) described in the next paragraph.

Algorithm 1. Active authentication

Parties: **T** ... terminal, **P** ... passport

1: **T:** generate random 8-byte value V
2: **T** $\rightarrow$ **P:** V
3: **P:** generate random 106-byte value U
4: **P:** compute $s = m^d \bmod N$, where $m =$"`6A`"$||U||w||$"`BC`", $w =$ `SHA-1`$(U||V)$ and d is the passport's secret AA key securely stored in the protected memory
5: **P** $\rightarrow$ **T:** s, U
6: **T:** verify $m = s^e \bmod N$, where e is the passport's public key stored in publicly accessible part of passport memory

1.1 Active Authentication

Besides the required security mechanisms in [6] such as the passive authentication and the basic access control (BAC), the e-passport can optionally employ cryptographically more sophisticated active authentication which aims to make the duplication virtually impossible for the attacker. The challenge-response protocol used in AA is shown in Algorithm 1.

As we can see, the formatted message m being signed by the passport is chosen jointly by the terminal and the passport, thus cannot be conveniently chosen by the attacker on the terminal side.

1.2 Electromagnetic Side Channel Leakage

As previously mentioned, the e-passport is compatible with ISO 14443 on the physical layer. To send the data to the terminal, the so-called near magnetic field is employed. Depending on the data being sent, the passport loads its antenna with a specific impedance circuit. Such an activity propagates in the surrounding magnetic field which is detected by the terminal. The reader is encouraged to see [3] for more details on the physical layer.

The question that is an interesting one to be asked in this scenario is whether the passport can fully control the emanation of the antenna. It is not only the special purpose circuit but also the other parts of the chip that load the antenna with their impedances. Especially, one should ask whether any of the cryptographic operations computed on the chip can be identified in the surrounding field.

During the early stages of the research, we presumed square-and-multiply algorithm with Montgomery exponentiation is employed during AA. This hypothesis is partly supported by the measurements shown on Figure 1. The ratio between the duration of two repetitive patterns corresponds to the execution duration of square and multiply operations and they appear in two series of 512 repetitions. This measurement does not reveal, however, whether the Montgomery multiplication is used. In case it is not, the attack described in the following text can still be employed in other implementations that make use of Montgomery multiplication.

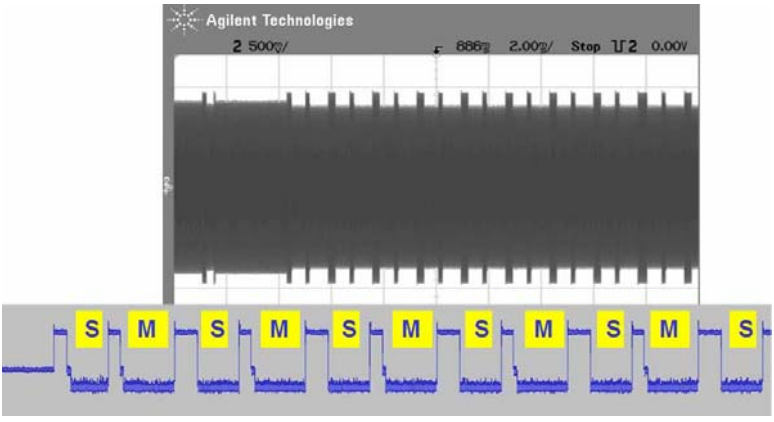

Fig. 1. Electromagnetic side channel measurement on an e-passport during the computation $s = m^d \bmod N$ within AA. The RFID chip on the passport is P5CD072 [13].

Since we presume square-and-multiply-always algorithm (see Algorithm 3) is used for exponentiation, the secret exponent d cannot be directly extracted from these measurements. We suspect however, it is possible to extract some information about the exponentiation if higher precision measurements are available. In fact, we believe the number of so-called final subtractions within the exponentiation $\bmod p$ can be revealed by this side channel. A method that is able to make use of such information and discloses the secret key d is described in the next section.

2 RSA–CRT with Montgomery Multiplication

Let N be the public RSA modulus and e be the public exponent. Let (p, q, d) satisfying $N = pq$, $d = e^{-1} \bmod \phi(N)$ be the corresponding private data.

Being given message m, the private RSA operation $m^d \bmod N$ is computed using Chinese Remainder Theorem as follows

$$s_p = (m_p)^{d_p} \bmod p \tag{1}$$

$$s_q = (m_q)^{d_q} \bmod q \tag{2}$$

$$s = ((s_q - s_p)\, p_{inv} \bmod q)\, p + s_p \tag{3}$$

where $d_p = d \bmod (p-1)$, $d_q = d \bmod (q-1)$, $m_p = m \bmod p$, $m_q = m \bmod q$ and $p_{inv} p = 1 \pmod q$. For our attack, we expect the exponentiation in (1) and (2) is computed employing the standard square-and-multiply-always algorithm with Montgomery representation of the integers (see Algorithm 3) with Montgomery constant $R = 2^{\lceil \frac{\log N}{2} \rceil}$.

One of the well-known countermeasures to prevent a simple SPA side channel attack on Algorithm 3 is the execution of the dummy multiplication in step 8.

Algorithm 2. Montgomery multiplication *mont()*

Input: $x, y \in Z_p$
Output: $w = xyR^{-1} \bmod p$

1: $s \leftarrow xy$
2: $t \leftarrow s(-p^{-1}) \bmod R$
3: $g \leftarrow s + tp$
4: $w \leftarrow g/R$
5: `if` $w > p$ `then`
6: $w \leftarrow w - p$ (final subtraction)
7: `return` w

Algorithm 3. Montgomery exponentiation *expmont()*

Input: $m, p, d\,(= (d_{n-1}e_{d-2} \ldots d_1 d_0)_2)$
Output: $x = m^d \bmod p$

1: $u \leftarrow mR \bmod p$
2: $z \leftarrow u$
3: `for` $i \leftarrow n-2$ `to` 0
4: $z \leftarrow mont(z, z, p)$
5: `if` $d_i == 1$ `then`
6: $z \leftarrow mont(z, u, p)$
7: `else`
8: $z' \leftarrow mont(z, u, p)$ (dummy operation)
9: `endfor`
10: $z \leftarrow mont(z, 1, p)$
11: `return` z

This prevents an attacker from distinguishing if the operation $mont(z, u, p)$ was executed or not. We will see, however, this countermeasure has no effect on our attack.

2.1 Schindler's Observation

In [14], Schindler demonstrated an interesting property of the Montgomery multiplication algorithm (Algorithm 1). Let x be a fixed integer in $\mathbb{Z}_p$ and B be randomly chosen from $\mathbb{Z}_p$ with uniform distribution. Then the probability that the final subtraction (step 6 in Algorithm 2) occurs during the computation $mont(x, B)$ is equal to

$$\frac{x \bmod p}{2R} \tag{4}$$

This observation allowed attacking RSA-CRT with an adaptive chosen plaintext timing attack.

2.2 Trick by Tomoeda et al.

In [17], the original Schindler's attack is modified to a chosen plaintext attack. All of the values are chosen in advance by the attacker, i.e. they are not required to be chosen during the attack.

With the probability of the final subtraction computation within one multiplication step given by Schindler (4), Tomoeda gave an estimate on the total number of final subtractions n_i during the whole exponentiation operation $(m_{p,i})^{d_p} \bmod p$, where $m_{p,i} = m_i \bmod p$. In fact, the approximation (5)

$$\frac{m_i R \bmod p}{p} \approx \frac{n_i - n_{min}}{n_{max} - n_{min}} \tag{5}$$

is given for $0 \leq i < k$ where $n_{max} = \max_{0 \leq i < k} n_i$ and $n_{min} = \min_{0 \leq i < k} n_i$ are the maximal and the minimal number of FS during k observations. To justify this approximation, the authors of [17] proposed experimental result similar to the one shown on Figure 2.

Being an approximation, we cannot expect (5) to be as tight as Schindler's high-precision (4). Instead, we can empirically measure minimal precision of (5) in bits. In section 2.4, we will see for 1024 bit modulus we can expect at minimum 4 bits with proper filtering of the measurements.

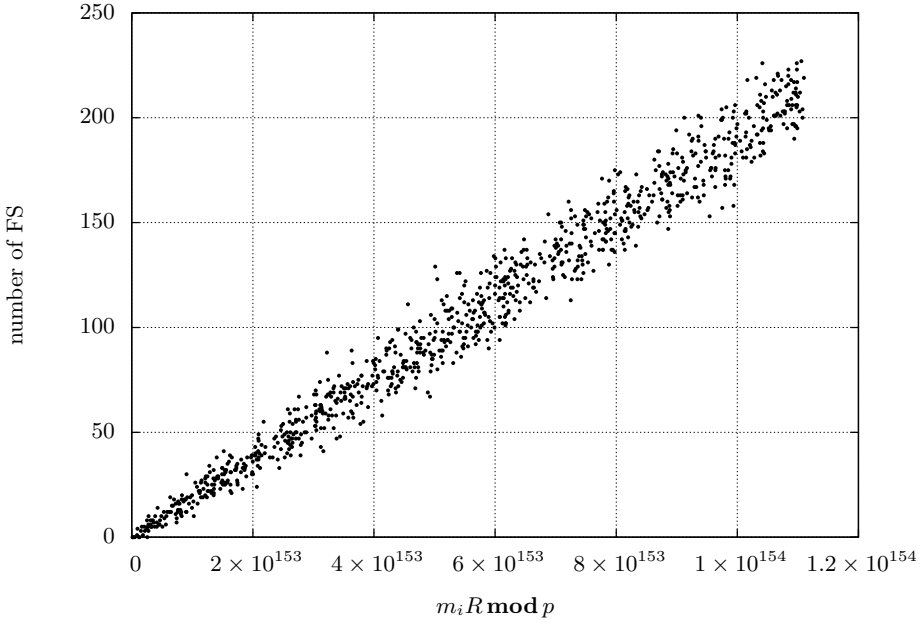

Fig. 2. The relationship between the *known* number of FS during the computation $(m_{p,i})^{d_p} \bmod p$ and the *unknown* value $m_i R \bmod p$. We see it is strongly linear and can be expressed as in (5).

In [17], the attack used 512 measurements (in case without the RSA blinding) to recover 512 bit long prime factor of N, i.e. one bit per measurement was used on average. We will see in section 2.4, however, that the average number of bits extracted per measurement and even their minimum can be much higher.

2.3 Conversion to HNP

Both approaches, Schindler's [14] and Tomoeda's [17], are chosen plaintext attacks on RSA–CRT with Montgomery exponentiation. They cannot be applied on AA in the e-passport scenario, however. As the plaintext (i.e. the formatted challenge) is generated jointly by the terminal and the e-passport, it cannot be conveniently chosen by the attacker.

The main contribution of this paper is the lack of the chosen plaintext condition while recovering the factorization of N. To do this we transform the problem of finding the secret factor of N to the well-known Hidden Number Problem (HNP, see [12]). Being given the approximation (5), we first realize there exists an integer k_i such that $m_i R \bmod p = m_i R - k_i p$. Consequently, we multiply (5) by N obtaining

$$m_i Rq - k_i N \approx \frac{n_i - n_{min}}{n_{max} - n_{min}} N \tag{6}$$

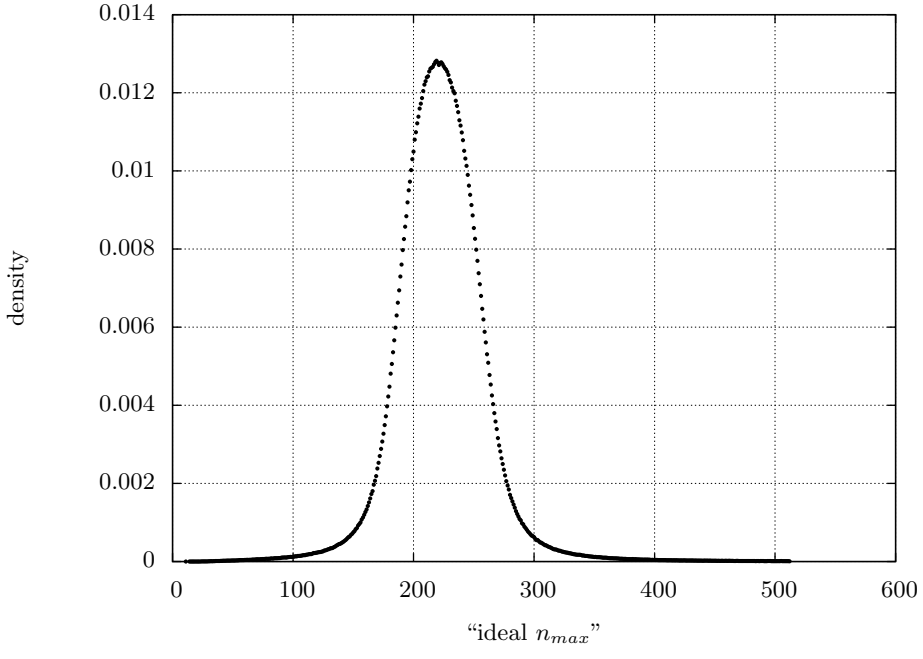

Fig. 3. The distribution of "ideal n_{max}" values computed from (6)

and we substitute $t_i = m_i R \bmod N$ and $u_i = \frac{n_i - n_{min}}{n_{max} - n_{min}} N$ for $0 \leq i < k$. We now have a "modular approximation" u_i of a known t_i-multiple of (hidden number) q, i.e.

$$t_i q + k'_i N - u_i \approx 0 \tag{7}$$

for suitable k'_i, $0 \leq i < k$.

Even if the values t_i and u_i were taken at random from $\mathbb{Z}_N$, it would hold

$$|t_i q - u_i|_N \leq \frac{N}{2} \tag{8}$$

(let us remind $|a|_N = \min_{k \in \mathbb{Z}}(a - kN)$).

However, we expect (7) to be a better approximation than the random one and we can measure its precision in bits and note it as l_i, i.e.

$$|t_i q - u_i|_N \leq \frac{N}{2} 2^{-l_i} \tag{9}$$

2.4 Approximation Precision and Filtering

During the one-time precomputation step we simulated the side channel measurements over 2^{12} RSA instances with 1024 bits long mudulus and 2^{12} random

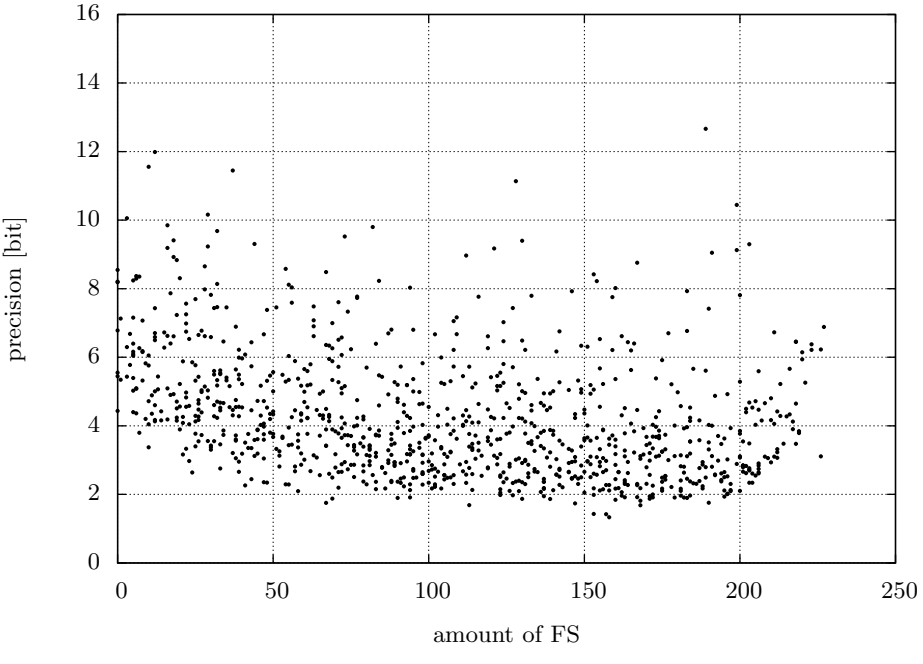

Fig. 4. The precision of the approximation in bits as a function of the amount of FS within the Montgomery exponentiation. During the attack, only the measurements with at most 4 FS are taken into account as their minimal precision is approximately 4 bits.

plaintexts for each instance. The minimal number of FS within the exponentiation **mod** p was 0 while the maximal was 290.

For each measurement we computed so-called "ideal n_{max}", the value for which the approximation (6) becomes equality with $n_{min} = 0$. The value was rounded to the nearest integer. The distribution of these values is shown on Figure 3. The value 224 being the most frequent candidate for "ideal n_{max}" value was used instead of the real value $n_{max} = \max_{0 \leq i < k} n_i$ during the following steps. This simple adjustment increased the minimal precision l_{min} by 0.5 bit and even by 1 bit within the filtered measurements described in the next paragraph.

The precision l_i of the i-th approximation u_i (see (9)) was measured as $l_i = -1 + \log N - \log |t_i q - u_i|_N$. The interesting relationship between these values and the number of FS is shown on Figure 4. We see the minimal precision of one single bit is obtained for approximately 150 final subtractions. However, focusing on the experiments with less than 5 final subtractions, the minimal precision jumps to 4 bits. For this reason during the simulated experiment we filter all of the measurements with 5 final subtractions or more resulting in 150 ($2^{7.2}$) suitable measurements from the total of 6797 ($2^{12.7}$) measurements conducted (simulated).

3 Hidden Number Problem

The Hidden Number Problem was first introduced in [2]. Being given k approximations

$$|t_i x - u_i|_N < \frac{N}{2^{l+1}} \tag{10}$$

with $t_i, u_i \in \mathbb{Z}_N$, $l \in \mathbb{N}$ known for $0 \leq i < k$, the task is to find the hidden number $x \in \mathbb{Z}_{N^{\frac{1}{2}}}$. In [2], the hidden number is a random unknown value from $\mathbb{Z}_N$, however, this is not the case in our scenario. Here, the hidden number is a factor of N with the expected size in order of $N^{\frac{1}{2}}$. The lattice we use to solve the HNP instance is adjusted for this purpose.

The usual technique to solve HNP is the employment of the lattices. The problem is converted to one of the well studied lattice problem, the Approximate Closest Vector Problem (ACVP). One constructs the lattice $\mathcal{L}$ spanned by the rows of the basis matrix

$$\mathbf{B} = \begin{pmatrix} N & 0 & \cdots & 0 & 0 \\ 0 & N & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & 0 \\ 0 & \cdots & 0 & N & 0 \\ t_0 & \cdots & \cdots & t_{k-1} & N^{\frac{1}{2}}/2^{l+1} \end{pmatrix} \tag{11}$$

and the vector $V = (u_0, \ldots, u_{k-1}, 0)$. The lattice vector

$$H = \left(t_0 x - \alpha_0 N, \ldots, t_{k-1} x - \alpha_{k-1} N, \frac{x N^{\frac{1}{2}}}{2^{l+1}} \right)$$

is the hidden vector for suitable $\alpha_0, \ldots, \alpha_{k-1} \in Z$, as its last coordinate reveals the hidden number x.

The hidden vector H belongs to lattice $\mathcal{L}$. It is unknown, however. The construction of lattice $\mathcal{L}$ and vector V yields existence of such $\alpha_0, \ldots, \alpha_{k-1}$ that $||H - V|| < \frac{N}{2^t}$. The first step in solving ACVP is finding an LLL-reduced basis of $\mathcal{L}$ using the LLL algorithm [9] or its BKZ variant [15] with the time complexity exponential on lattice dimension $k + 1$. Being given the reduced basis, the second step is using Babai's closest plane algorithm [1] to find a vector H' in $\mathcal{L}$ close to V. One can now hope the vector H' reveals the hidden number x in its last coordinate, i.e. H' is equal to hidden vector H or is "similar enough".

It is shown in [12] that the probability of recovering the hidden number using this approach is close to 1 if the precision l of the approximations is in order of $(\log N)^{1/2}$ and reasonable amount of approximations is given.

In our scenario with 1024-bit long modulus N, we would need 32 bit measurement precision in order to have the theoretical guarantee of success. As we have seen previously this would hardly be the case with the electromagnetic side channel which provides us with 4 bits at minimum, 7 bits on average. To overcome this limitation we can lower the imprecision of the approach introduced by Babai's algorithm by heuristically converting the ACVP to Unique-SVP, as shown in Appendix. More importantly, the lattice basis reduction algorithms behave much better in real-life situations than what is guaranteed in theory [4]. Next section shows it is possible in fact to recover the hidden number q in our scenario.

3.1 Experiments with Emulated Observations

We implemented the attack using NTL library [16]. The computing platform was 64-bit GNU/Linux Debian running on Opteron 244 with 2GB RAM.

We first emulated the side channel and extracted the number of final subtractions l_i within the Montgomery exponentiation $s_i = (m_{p,i})^{d_p} \bmod p$. As justified in Figure (4) only the measurements with at most 4 final subtractions were used in order to keep the approximation precision on an acceptable level. In fact, the minimal precision l_{min} within these measurements was 4.2 bits while it was as high as 7.2 bits on average. We have to note however, these values are not known during the attack, thus the lower bound has to be estimated. In order to collect 150 such measurements, the total number of 7000 measurement was emulated. In real life, the physical measuring of such a collection should be feasible in order of hours.

With the side information available, lattice $\mathcal{L}$ was constructed. The dimension of the lattice was 152, since the CVP problem was converted to Unique-SVP adding 1 to the original dimension. The parameter l approximating the minimal number of known bits was chosen from the set $\left\{\frac{7}{2} + \frac{t}{4}, t \in 0, \ldots, 19\right\}$, i.e. 20 lattices were constructed in parallel as the exact precisions l_i of the approximations are not known.

The lattices were first reduced with the basic LLL_XD variant of LLL algorithm implemented in NTL. Following, stronger G_BZK_XD reduction was run

with BlockSize initially set to 4 being increased by 2 to up to 20. After each BlockSize increase, the short vector of the reduced lattice was checked. In case it revealed the hidden number q, the attack was successful.

In the experiment with 150 simulated measurements, the attack was successful with parameter l equal to 9 and 9.5. The expensive lattice basis reduction steps took approximately 40 minutes each.

Five different scenarios with random RSA instances were emulated and experimented with. The RSA modulus was successfully factored in each of these instances.

4 Future Research

As mentioned several times, our main hypothesis—that the Montgomery multiplication is used and that the amount of final subtractions leaks—is to be verified. Furthermore, the resilience of other HW modules against this side channel attack in similar scenarios should be verified, as well. The probability of success of the attack under given circumstances is to be elaborated.

5 Conclusion

We presented new known plaintext side channel attack on RSA–CRT with Montgomery exponentiation in this paper. The lack of chosen plaintext condition greatly increases its applicability in the scenarios based on random formatting of the message being signed (probabilistic signature scheme). The existence of the side information we used was questioned. We urge the testing laboratories to verify it in the electronic passport scenario.

Acknowledgment

I would like to thank Dr. Rosa for pointing out [17] and for his guidance and the team of Prof. Lórencz at the department of computer science of FEE CTU in Prague for kindly providing their measurement results. Thanks also goes to the anonymous referees for their helpful comments.

References

1. Babai, L.: On Lovász' lattice reduction and the nearest lattice point problem (shortened version). In: Mehlhorn, K. (ed.) STACS 1985. LNCS, vol. 182, pp. 13–20. Springer, Heidelberg (1984)
2. Boneh, D., Venkatesan, R.: Hardness of computing the most significant bits of secret keys in Diffie-Hellman and related schemes. In: Koblitz, N. (ed.) CRYPTO 1996. LNCS, vol. 1109, pp. 129–142. Springer, Heidelberg (1996)
3. Finkenzeller, K.: RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification, 2nd edn. John Wiley & Sons, Chichester (2003)

4. Gama, N., Nguyen, P.Q.: Predicting lattice reduction. In: Smart, N.P. (ed.) EUROCRYPT 2008. LNCS, vol. 4965, pp. 31–51. Springer, Heidelberg (2008)
5. International Civil Aviation Organization (ICAO). Development of a Logical Data Structure – LDS for Optional Capacity Expansion Technologies, http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=39693
6. International Civil Aviation Organization (ICAO). Doc 9303, Machine Readable Travel Documents, http://www2.icao.int/en/MRTD/Pages/Doc9393.aspx
7. International Organization for Standardization. ISO/IEC 7816 – Identification cards – Contactless integrated circuit cards – Proximity cards, http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=39693
8. International Organization for Standardization. ISO/IEC 7816 – Identification cards – Integrated circuit(s) with contacts, http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=38770
9. Lenstra, A.K., Lenstra Jr., H.W., Lovász, L.: Factoring polynomials with rational coefficients. Mathematische Ann. 261, 513–534 (1982)
10. Montgomery, P.L.: Modular multiplication without trial division. Mathematics of Computation 44, 519–521 (1985)
11. Nguyên, P.Q.: Cryptanalysis of the Goldreich-Goldwasser-Halevi Cryptosystem from Crypto 1997. In: Wiener, M.J. (ed.) CRYPTO 1999. LNCS, vol. 1666, pp. 288–304. Springer, Heidelberg (1999)
12. Nguyen, P.Q., Shparlinski, I.: The insecurity of the Digital Signature Algorithm with partially known nonces. J. Cryptology 15(3), 151–176 (2002)
13. Philips Electronics N.V. P5CD072 – Secure Dual Interface PKI Smart Card Controller, http://www.nxp.com/acrobat_download/other/identification/sfs095412.pdf
14. Schindler, W.: A timing attack against RSA with the Chinese Remainder Theorem. In: Paar, C., Koç, Ç.K. (eds.) CHES 2000. LNCS, vol. 1965, pp. 109–124. Springer, Heidelberg (2000)
15. Schnorr, C.-P., Euchner, M.: Lattice basis reduction: Improved practical algorithms and solving subset sum problems. Math. Program. 66, 181–199 (1994)
16. Shoup, V.: NTL: A Library for doing Number Theory (2008), http://www.shoup.net/ntl/
17. Tomoeda, Y., Miyake, H., Shimbo, A., Kawamura, S.-i.: An SPA-based extension of Schindler's timing attack against RSA using CRT. IEICE Transactions 88-A(1), 147–153 (2005)

A Lattices

We give the definition of a full-rank lattice and overview several basic algorithmic problems associated with it in this section. We point out the state-of-the-art algorithms solving these problems, as well.

Let the set $\mathbf{B} = \{\mathbf{b}_0, \ldots, \mathbf{b}_{k-1}\}$ be a set of linearly independent vectors in $\mathbb{R}^k$. The lattice $\mathcal{L}$ spanned by the vectors in $\mathbf{B}$ is defined as $\mathcal{L} = \sum x_i \mathbf{b}_i, x_i \in \mathbb{Z}$. In such case, B is a basis of lattice L. A $k \times k$-type matrix over $\mathbb{R}$ whose rows are the vectors $\mathbf{b}_0, \ldots, \mathbf{b}_{k-1}$ is the called basis matrix of $\mathcal{L}$ and we will note it as $\mathbf{B}$, as well. The volume of a lattice $\mathcal{L}$ is defined as $\det \mathbf{B}$, where $\mathbf{B}$ is any basis of $\mathcal{L}$.

i-th successive Minkowski minimum $\lambda_i(\mathcal{L})$ of lattice $\mathcal{L}$ is the radius of the smallest sphere containing at least i linearly independent (non-zero) vectors of $\mathcal{L}$. Especially, we see the first Minkowski minimum is the length of the shortest non-zero lattice vector and we denote it as $\lambda(L)$. The ratio $\frac{\lambda_2(\mathcal{L})}{\lambda_1(\mathcal{L})}$ is called the gap of the lattice.

A.1 Problems

Two lattice problems that are interesting in scope of this paper are the Unique shortest vector problem (Unique-SVP) and the Closest vector problem (CVP). Being given the lattice and its gap, Unique-SVP problem is to find the shortest vector of the lattice. Analogically, CVP problem is to find closest lattice vector to a given non-lattice vector. Sometimes, CVP is viewed as a non-homogenic variant of SVP.

A.2 Solutions

The usual approach to solve Unique-SVP is the LLL algorithm [9] or one of its variants [15]. In [4], it is experimentally shown it is possible to solve Unique-SVP if the gap $\frac{\lambda_2}{\lambda_1}$ is at least 1.021^k with BKZ-20 variant of LLL algorithm.

One can try to solve CVP with Babais closest plane algorithm [Ba85], the experience shows, however, the heuristic conversion to Unique-SVP provides better results. We use the same technique as in [11], i.e. we construct lattice $\mathcal{L}'$ with the basis matrix $\mathbf{B}' = \begin{pmatrix} \mathbf{B} & 0 \\ V & 1 \end{pmatrix}$. As the lattices $\mathcal{L}$ and $\mathcal{L}'$ have the same determinant and approximately the same dimension, we can expect their respective shortest vectors to be approximately of the same size. Given the fact that the hidden vector H is in $\mathcal{L}$ and close to V (section 3), we see the vector $V-H$ is short and belongs to $\mathcal{L}'$. In fact, we can expect is to be the shortest vector of $\mathcal{L}'$. If the gap $\frac{\lambda_2}{\lambda_1}$ is sufficiently large, we can use the lattice basis reduction techniques and check if the short vector found reveals the hidden number x in $(k+1)$-st coordinate (follows from the construction of lattice L in section 3).