Taylor & Francis
Taylor & Francis Group

Journal of Discrete Mathematical Sciences and Cryptography

ISSN: 0972-0529 (Print) 2169-0065 (Online) Journal homepage: https://www.tandfonline.com/loi/tdmc20

Forty years of attacks on the RSA cryptosystem: A brief survey

Majid Mumtaz & Luo Ping

To cite this article: Majid Mumtaz & Luo Ping (2019) Forty years of attacks on the RSA cryptosystem: A brief survey, Journal of Discrete Mathematical Sciences and Cryptography, 22:1, 9-29, DOI: 10.1080/09720529.2018.1564201

To link to this article: https://doi.org/10.1080/09720529.2018.1564201

Published online: 27 Feb 2019.

Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 22 (2019), No. 1, pp. 9–29
DOI : 10.1080/09720529.2018.1564201

Forty years of attacks on the RSA cryptosystem : A brief survey

Majid Mumtaz *
Luo Ping
State Key Laboratory of Information Security
Institute of Software Systems and Engineering
School of Software
Tsinghua University
Beijing 100086
China

Abstract

RSA public key cryptosystem is the de-facto standard use in worldwide technologies as a strong encryption/decryption and digital signature scheme. RSA successfully defended forty years of attack since invention. In this study we survey, its past, present advancements and upcoming challenges that needs concrete analysis and as a counter measure against possible threats according to underlying algebraic structure. Past studies shows us some attacks on RSA by inspecting flaws on relax model using weak public/private keys, integer factorization problem, and some specific low parameter selection attacks. Such flaws can not hamper the security of RSA cryptosystem by at large, but can explore possible vulnerabilities for more deep understanding about underlying mathematics and improper parameter selection. We describe a brief survey of past findings and detail description about specific attacks. A comprehensive survey of known attacks on RSA cryptosystem shows us that a well implemented algorithm is unbreakable and it survived against a number of cryptanalytic attacks since last forty years.

Keywords: *RSA cryptanalysis, Lattice reduction attack, Coppersmith's method, Implementation attacks*

1. Introduction

The RSA (Rivest, Shamir, Adleman) public key cryptographic algorithm was invented in 1977 [1]. It is a well studied and implemented algorithm, extensively utilized in different domains [2, 3]. Cryptanalyst draw attention towards it's security and robustness. Two major hard

*E-mail: `maji16@mail.tsinghua.edu.cn`

open problems of RSA cryptosystem since birth are Integer Factorization Problem (IFP) and an RSA Problem (i.e. e^{th} root finding problem).

A dozens of RSA cryptanalysis techniques proposed in literature, but no one yet claim a total break of the underlying big number. Some attack on RSA are mathematical, factorization attack [4], low public/private key attacks, improper implementation attacks etc.). Most of them are based on relaxed models (a model in which some or preliminary guesses are known in advance) including known partial information, weak public/private exponents attacks etc. As computational power increases with the passage of time, more clever attacks are expected. Therefore, to strengthen the RSA security against any devastating attacks, the underlying algebraic characteristics need rigorous analysis that can resist all attacks on it. In this work, we consider a comprehensive study of past attacks on RSA especially based on lattice reduction techniques. The major functions in RSA are public/private key pair generation, encryption/decryption and digital signatures.

To understand the background, let $N = pq$ be the product of two large distinct primes p and q with equal bit-size. Further, let $1 < e < \varphi(N)$ with $gcd(e, \varphi(N)) = 1$ where, $\varphi(N) := \{1 < k < N \mid (k, N) = 1\}$ and $gcd(x, y)$ denotes the greatest common divisor of positive integers x and y, also φ denotes the Euler's totient function. Note that for large N, the $\varphi(N) = (p - 1)(q - 1)$. Also, let d be the multiplicative inverse of $e \ mod \ \varphi(N)$ represent as; $ed \equiv 1 \ mod \ \varphi(N)$. Now, the encryption of a plaintext $m \in \mathbb{Z}_N$, $gcd(m, N) = 1$, and the decryption of a ciphertext denotes as $c \in \mathbb{Z}_N$, $gcd(c, N) = 1$ can be calculated by the following relations $E(m) := m^e \ mod(N)$, and $D(c) := c^d \ mod(N)$ respectively. The relation between e and d yields the following RSA equation;

$$ed \equiv 1 \ mod \ \varphi(N) \Rightarrow ed - 1 = k.\varphi(N) \tag{1}$$

where, $k \in \mathbb{Z}$. Equation (1) is the key equation used for RSA cryptanalysis purpose. The correctness of RSA algorithm depends on Euler's theorem, which states that for every integer a is a co-prime with N and the equation $a^{\varphi(N)} \equiv 1 \ mod \ \varphi(N)$ holds.

$$m^{ed} \equiv m^{1+k.\varphi(N)} \equiv m(m^{\varphi(N)})^k \equiv m(1)^k \equiv m(mod \ N) \tag{2}$$

Thus, the equality in equation (2) shows that m is always correctly achieved.

1.1 *Study Approach and Objectives*

In this work we follow the survey approach presented by Kitchenham et al. [5]. He covers a comprehensive survey framework in a systematic way. We find the previous work since 1997, investigate the results, record the major attacks analogies according to their level of impacts, and open challenges. Our research objectives are:

1. To analyze several known Elementary, mathematical/algebraic attacks on RSA public/private key and possible weaknesses and security measures over the years.
2. To explore more about lattice reduction techniques (i.e. L^3, L^2) for multivariate polynomial equations and significant results, their impacts on lattices.
3. Current challenges and advances on RSA algebraic structure and possible improvements against known vulnerabilities.

To achieve above objectives, we explore most relevant information presented in state of the art journal articles, conferences, white papers (NIST, RSA etc.). We also explored digital resources, electronic databases including Springer, ScienceDirect, Google Scholar, IEEExplore, Webofknowledge, ACM Digital Library, HPC etc.

1.2 *Outline*

The outline of the paper is divided as follows. In section 2, we survey an integer factorization problem with respect to RSA perspective as it consider as an intractable hard problem since it's invention, specifically for larger key spaces. In section 3, we describe some known elementary attacks on RSA. In section 4, 5, and 6 we describe an inside of the RSA underlying mathematics, which explore more about relaxed RSA problems, solutions according to Coppersmith's based lattice reduction technique and than we describe challenges and possible future opportunities and finally in section 8, we conclude the paper.

2. Integer Factorization Problem (IFP)

Integer factorization problem (IFP) is an intractable number-theoretic problem. In RSA cryptosystem N is generally the product of two equal size big prime numbers chosen in a way no one can guess it or factorize using today's computation power. If the factorization of N is given, one can efficiently find d (a private exponent), then compute $\varphi(N)$ easily. Since e is already known therefore, it can easily break the RSA cryptosystem. As RSA cryptosystem is based on the intractability of the IFP, such mathematical problems are hard to solve in time polynomial, where such factorization attack attempts to break big modulus N into p and q prime factors, which is believe to be computationally infeasible for larger N. Whereas, short key space of RSA is always susceptible to factorization attack. For example, given the factorization of N, an adversary can easily construct $\varphi(N)$ out of which the private key $d = e^{-1} \; mod \; \varphi(N)$ can be deduced. IFP algorithms initiate since Euclid's time and in modern times 1980s to 1990s years when the more popular factorization algorithms developed especially the Quadratic Sieve [6], the Elliptic curve [7], and the General Number Field sieve (GNFS) [8, 9] algorithms. Among them the GNFS is the fastest algorithm, for more detail we refer the readers to [8]. In 2009 an effort had been made by using hundreds of machines to factorize 232-digits long number (RSA-768 bits) [10]. The GNFS algorithm compute the prime factorization of N and it's running time was $\exp(c(LogN)^{1/3}(LogLogn)^{2/3}))$ where, $c = (64/9)^{1/3} = 1.922999427$ denotes an arbitrary integer. Whereas, in special treatment of GNFS, the value of constant c = $(32/9)^{1/3}$ = 1.526285657 was used. GNFS is asymptotically faster algorithm among other existing one. The detail study about factorization algorithms are available in [7, 8]. Also, optimization problem on existing factorization algorithm is one of the challenging task.

3. Elementary Attacks on RSA

An elementary or basic attacks used to exploit the possible back holes in RSA algorithm. While deploying such an attack, an adversary try to guess some weak links such as whether implemented solution can accept vulnerable input to produce some error response. Such exploits are indirect algorithmic attacks based on deliberate system misuse [11]. A number of such elementary attacks are common modulus attack, blinding attack [12]. We briefly overview the attacks below.

3.1 *Common Modulus Attack*

RSA is a deterministic algorithm in which encryption procedure output the same ciphertext when we use same public key. Such characteristic assist an adversary to launch common modulus attack against RSA. Suppose a message M is encrypted twice using the same modulus $N = pq$ with different public keys $<e_1, N>$ and $<e_2, N>$ such that

$gcd(e_1, e_2) = 1$. If an adversary knows $C_1 = M^{e_1} mod\, N$ and $C_2 = M^{e_2} mod\, N$, then she can recover the original message M easily. For example an adversary knows e_1 and e_2 on the basis of this she deduce two integers a and b, such that $ae_1 + be_2 = 1$ using extended Euclidean algorithm to compute $C_1^a C_2^b \equiv M^{a.e_1} M^{b.e_2} \equiv M^{a.e_1 + b.e_2} \equiv M.$ An adversary could intercept the message and obtain the public key with the corresponding ciphertexts. To overcome such an attacks, try to avoid redundant modulus again and again.

3.2 *Blind signature attack*

A blind signature introduced by David Chaum [13] is a form of digital signature in which the content of a message disguised (blinded) before signing. The resulting blind signature publicly verify against the original unblinded message in a manner of a regular digital signature schemes. If RSA self-reducibility feature (which assure that all random ciphertexts are hard to decipher) [14] breached, an adversary can steal sensitive information about someone's valid signature [15]. A random padding schemes resist such attacks to protect individual's privacy and authenticity [16] in privacy-related protocols, where the signer and message authors are different entities. It's practical examples includes cryptography based election systems and digital cash schemes [17, 18]. Similar concept of blinding signature recently emerge on E-cash-lottery systems proposed by X. Sun et al. [19]. In their scheme the zero-knowledge proof and the blind signature combine together ingeniously on E-cash lottery schemes. In such lottery scheme, it is of highly anonymous that the lottery player must be honest. A dishonest player for example when the player spend or exchange bonus repeatedly the identity certainly be recognized. In this way one can avoid potential attack on such lottery schemes.

4. Weak Public Exponent Attack on RSA

RSA is insecure in some special cases, for example weak public exponent [20, 21, 22], as summarized in [23]. Breaking an RSA using a weak public exponent e is of special meaning as it achieves fast encryption. The minimum value of e is 3, and a recommended is $e = 2^{16} + 1 = 65537$. However, besides other attacks on RSA, attack employ through small e are far from total break. We describe some of the prominent attacks in subsections below.

4.1 *Message Recovery through Small Public Exponent attacks*

4.1.1 Hästad's Attack and Franklin-Reiter message recovery attack

Hästad first present a broadcast attack on low RSA public key by using Coppersmith's theorem [20]. Their results describe as a theorem statement below.

Theorem 1. *Suppose plaintext m is encrypted k times with the public keys* $<e,N_1>,<e,N_2>,\ldots,<e,N_k>$ *where,* $k \geq e$ *and* $N_1, N_2, \ldots, N_k$ *are pairwise relative prime number. Let* $N_0 = min\ (N_1, N_2, \ldots, N_k)$ *and* $N = \Pi_{i=1}^{k} N_i$. *If the plaintext m satisfy* $m < N_0$, *then an adversary Trudy can easily know* $c_i \equiv m^e \bmod (N_i)$ *and* $<e, N_i>$ *for* $i = 1, 2, \ldots, k$ *and she can compute the plain text m in time polynomial log*(*N*).

Such an attack only works with succinctly small *e* usually happen on broadcast applications. An extended result of Hästad attack describe by May et al. [24] is also known as Polynomial related message attack.

Another similar attack performed by Franklin and Reiter [25] to guess an encypted message. In their experiment authors sent several linearly related messages encrypted by using a single RSA key with low public exponent. They found a clever attack on same modulus based ciphertext, which is insecure as describe by Coppersmith [21]. Coppersmith's technique strengthened the Franklin-Reiter's attack by introducing a padding scheme [22]. The subsection (4.1.2) describes their attack briefly.

4.1.2 Coppersmith's short Pad attack to Recover message

Coppersmith's short pad attack also known as random padding attack. Coppersmith [21] perform this attack and recovers the plaintext which is encrypted by small *e*. Also, as standard RSA has proven insecure without any prior padding scheme. We describe Coppersmith's short pad attack output in theorem statement below.

Theorem 2. (*Coppersmith's short pad attack*). *Let <e, N> be a public key, and* $e = 3$. *Suppose* m_1, m_2 *satisfy the equation* $m_2 = m_1 + b$ *are encrypted using <3, N>. The attacker knows the two ciphertexts* c_1, c_2 *and public key, if* $|b| < N^{\frac{1}{9}}$, *it is possible to compute* m_1 *and* m_2 *in time polynomial log(N).*

When performing cryptanalaysis of padded plaintext like $m_1 = m + b$, where *b* is actually a random data appended at the end of plaintext make harder to attack on RSA. Also, it is recommended to generate strong random pad every time, if the public exponent is very small.

4.2 *Weak public exponent with common LSBs of primes*

An RSA cryptosystem [26] with modulus primes share a number of Least Significant Bits (LSBs) written as LSBs-RSA. Suppose, $N = pq$ be the modulus of LSBs-RSA, share the $\frac{1}{2} - \alpha$ least significant bits, i.e. $p - q = i.2^{\alpha}$ for some odd integer i and $\alpha > 1$, where i and $\alpha \in N$. Steinfeld et al. [27] first showed in early 2001 using BDF [28] attack on LSBs-RSA. They analyzed the complexity of the attack and described that weak public exponent, LSBs-RSA is inherently resistant to the partial key exposure attacks. According to their findings, BDF attack is less effective for LSBs-RSA with small e as compared with standard RSA. Whereas, LSBs-RSA with large size of e is more vulnerable then standard RSA. The work is further improved by Sun et al. [29] by reducing the cost of exhaustive search of k in LSBs-RSA. Where, k is some integer value use in RSA main equation (i.e. $ed = k\varphi(N) + 1$). The improvement depends on two cases as follows;

Case 1: $\gamma \leq min\{\beta, 2\alpha\} - \sigma$ and,

Case 2: $\gamma > min\{\beta, 2\alpha\} - \sigma$

In case 1, the cost of $k's$ exhaustive search is reduced in polynomial time therefore, complexity automatically increased. Whereas, in case 2 without searching k exhaustively, the complexity of LSBs-RSA are improved. The maximum of 2α, β in LSBs-RSA is considered vulnerable under BDF attack as modulus N proportionally increases.

5. Weak Private Exponent attacks on RSA

RSA is most secure for large value of modulus N. Therefore, cryptanalytic attacks are difficult to perform. To perform attacks on RSA some relax model (a model based on some prior known assumptions such as, a known weak private exponent or Some known approximate value of private exponent or either guessed known-ciphertexts or Some known approximation of primes p and q) require. Such known values use as a back-door, especially when RSA is implemented on low processing smart devices [12, 16]. To perform cryptanalysis on RSA, lattice reduction techniques (i.e. LLL, BKZ etc.) are most popular ingredients these days. Pioneer Coppersmith's found small inverse roots of univariate modular polynomial and a heuristic bivariate integer solution. In 2006 Jochemsz-May's [30] described a generic strategy to solve multivariate RSA polynomial equation. Later Herrman-May [31] employ unraveled linearization technique to obtain optimized lattice dimension. Currently in our findings, all multivariate approaches for lattice construction output only heuristic results. Lattice optimization is one of the open challenge in multivariate polynomials. Though, Jochemsz-May's work to construct a generic strategy for multivariate polynomials also, it optimizes lattice dimension with algebraic indepdendence assumption. A recent work done by Y. Lu et al. [32], summarize certain possible ways to construct lattices of RSA polynomials including unraveled linearization [33], exponent trick [34] and two-step [35] based lattice method. Later both tricks use for Multi-prime RSA [36, 37] and Dual RSA [38] respectively. Both schemes are out of scope in this work. Here, we describe more about unraveled linearization technique according to standard RSA perspective.

The most prominent result achieved by Boneh and Durfee using Howgrave-Graham's reformulation of Coppersmith's method [39, 40, 28]. They found small roots of bivariate polynomial equation and achieve best bound. Later Herrmann and May improves the lattice dimension using unraveled linearization technique [31] but their bound was less efficient than Coppersmith's bound. We summarize in Table 1 about Coppersmith's method and Herrmann-May unravalled linearization method for a comparison.

Table 1

Comparison about Coppersmith's Method and Unravlled Linearization Method

Coppersmith's Method	Unravalled Linearization
1) To analyze Polynomial Power generators.	1) To analyze Polynomial Power generators.
2) Complex for lattice construction.	2) Hybrid in nature based on lattices and Coppersmith's method.
3) Based on structured polynomial monomials set.	3) Based on similarity of polynomial coefficients.
4) Cryptanalytic tool for univariate and multivariate polynomials.	4) A cryptanalytic tool for linear equations only.
5) Usually Triangular Lattice dimensions shape degraded.	5) Always construct an optimized triangular lattice dimensions.

5.1 *Small Private Exponent attacks*

RSA security relies on hardness of searching the private key d, when the public key $<e, N>$ is given due to a trapdoor function. Where d denotes the trapdoor information. As small value of private exponent d plays significant role for speeding up the RSA signature generation but at the same instance if the factorization of n is possible then one can compute $\varphi(n)$ in order to find the value of private key d. If an adversary knows d, she can compute f inverse (f^{-1}), which is as easy as of computing the function f. We cover some attacks on small private exponents in subsections below.

5.1.1 Wiener's Attack

Wiener [41] in 1990's described that an adversary can easily break RSA, if the private exponent d is less than one-quarter of the length of modulus (i.e. $d < N^{1/4}$). He performed an attack on weak private exponents. Let (e, N) be a public key instance of RSA with balanced primes and let $d < \frac{1}{3}N^{\frac{1}{4}}$ be its corresponding private exponent. By substituting $\varphi(N) = N - p - q + 1$ into RSA key equation, we get $ed = 1 + k(N - p - q + 1)$ dividing both sides by dN and rearranging similar terms, he obtained $\left|\frac{e}{N} - \frac{k}{d}\right| = \left|\frac{1}{dN} - \frac{k(p+q-1)}{dN}\right| = \left|\frac{k(p+q-1)}{dN}\right| < \frac{1}{2d^2}$. Therefore, from continued fraction theorem, this followed that $c = \frac{k}{d}$ is one of the convergent in the continued fraction expansion of $\frac{e}{N}$. By their result $\varphi(N)$ is exposed since $\frac{1}{k} < 1$ and $\left\lfloor \frac{e}{c} \right\rfloor = \left\lfloor \frac{ed}{k} \right\rfloor = \left\lfloor \frac{1}{k} + \varphi(N) \right\rfloor = \varphi(N)$. Once φ is known, the modulus can easily be factored. As the number of convergent is polynomial in $log_2(N)$, computation run in time polynomial $log_2(N)$. Wiener observe the fact when the private exponent is smaller then $\frac{1}{3}N^{\frac{1}{4}}$ the modulus can easily be factored in time polynomial. In order to circumvent the attack, Wiener also proposed some solutions which adds multiple of $\varphi(n)$ to the public exponent e, i.e. to use $e' = e + i\varphi(n)$ for a large integer i. Also one can defeat the attack by using large value of e. According to Wiener's attack d provides no information as soon as $e > N^{3/2}$.

Variants of Continued Fraction attack: A number of attack described in literature are based on continued fraction, table 2 shows different variants of Wiener's attack on small private RSA exponent. [42, 43, 44, 45, 46] accordingly.

Table 2

Variants of Wiener's Continued fraction attack

Reference	Equation Used	Technique Used	Bounds
Verheul et al.[42]	$ed - k\varphi(N) = 1$	Continued fraction	$d <= rN^{0.25}$, where $r \approx 1/4$
Dujella et al. [43]	$ed - k\varphi(N) = 1$	Continued fraction	$d < 4.04(\sqrt[4]{N})$
A.N. et al. [44]	$eX - (p - u)\ (q - v)\ Y = 1$	Continued fraction	$d <= N^{0.292}$
Nitaj et al. [47]	$eX - \left(N - \left(up \pm \frac{q}{u}\right)\right) Y = Z$	Continued fraction and Coppersmith	$d <= N^{\frac{3}{4} - \varepsilon}$ where $\varepsilon > 0$
M. Bunder et al. [46]	$ex - (p^2 - 1)(q^2 - 1)\ y = z$	Continued fraction and Coppersmith	$d < \sqrt{\frac{2N^3 - 18N^2}{e}}$

5.1.2 Lattice Reduction Technique

Lattices in $\mathbb{Z}^n$ are the discrete points in n-dimensional space. For detail understanding about lattice theory one can read in [48]. Coppersmith's open the door of algebraic cryptanlaysis using lattice reduction technique to solve RSA polynomial equation. The main idea was of twofold:

- To convert the RSA polynomial equation into the problem of finding small solution of modular equation and then,
- By using Howgrave-Graham's reformulation of Coppersmith's technique to achieve a simplified result in the form of small inverse roots of the polynomial equation.

In mathematics, congruence based polynomial equation solution is consider a hard problem. Whereas, a non-congruence (*integer*) based polynomial equation solves with the help of known root finding method. To find small solutions of univariate polynomial equations, Coppersmith's theorem is utilized, which is based on high dimension lattices to look for all small integer solutions called roots of $f(x_0)$ the modular polynomial equation $f(x) \equiv 0(modN)$, and if $x_0 < N^{1/2}$ then x_0 solve it easily. The two most used techniques are Coppersmith's technique and Coron's lattice reduction technique, below we cover both.

5.1.3 CopperSmith's lattice reduction technique

Don Coppersmith proposed this technique in 1996 – 97. It finds small roots of univariate and a bivariate polynomial equation modulo a given integer on the basis of $LLL(L^3)$ [49] algorithm. LLL provides easy way to find the shortest vector over a lattice by reducing it within polynomial time. A number of reduction algorithms are available including LLL [49], BKZ [50] and L^2 [51]. Among them the fastest implementation of LLL algorithm is due to Nguyen and Stehl [51]. The time complexity is $O(c\delta^5 log^9 N)$, where c denotes a constant term. For visual representation of monomials Newton's polytope give us a convex hull points set of polynomials. The set notation form is; $\{(k_1, k_2, \ldots, k_n) \in N^n \mid x_1^{k_1}, x_2^{k_2}, \ldots, x_n^{k_n}$ is a monomial of $f(x_1, \ldots, x_n)$ with non-zero coefficients$\}$. Coppersmith's method statement as;

Theorem 3 *(Coppersmith's Univariate Theorem). Let $p(x)$ be a monic integer polynomial of degree i and N a positive integer of unknown factorization. One can find all integer solutions x_0 of $p(x_0) = 0(mod\ (N))$, such that $|x_0| < N^{\frac{1}{k}}$ in time polynomial $log(N)$ and k.*

According to theorem 3, let N be an integer of unknown factorization that has a divisor $b \geq N^{\beta}$, for $0 < \beta \leq 1$, and $f(x)$ be a univariate monic polynomial equation of degree k. One can find all the solutions x_0 of $f(x) = 0mod(b)$, by satisfying $|x_0| \leq cN^{\beta^{2/k}}$ in time polynomial in $log(N)$, guess the value of c and calculate the number of polynomial roots. A more comprehensive detail about this theorem can be found in [39]. Coppersmith's method mainly based on two major assumptions in a univariate polynomial case;

- The polynomial of univariate case over integer or modulo have only one small solution.
- And the polynomial obtained after LLL-reduction is the basis vector that assumes to be algebraically independent.

Though, both assumptions hold true but in some cases negative results were reported in [52]. After all, these assumptions greatly improves the security of RSA cryptosystem especially for exploiting the weak RSA private exponents. Normally, the value of δ assumed to be small enough so that LLL-algorithm can compute the small reduced basis within reasonable amount of time. The method later improved by Howgrave-Graham [40] using polynomial coefficients and modulus N together for matrix construction instead of relying coefficients as used by Coppersmith.

Though, both methods have equal complexity but Howgrave-Graham's technique is computationally efficient as well as simplify the process. Boneh and Durfee used Coppersmith technique to achieve best bound of polynomial equations. We describe Boneh and Durfee attack below.

Boneh and Durfee attack. The main result of their attack was that, N can be factored in time polynomial when $d \leq N^{0.292}$ on the basis of lattice reduction technique such as LLL algorithm.

Theorem 4. *Let $N = pq$ be the modulus of size n-bits where p, q are primes with $q < p < 2q$. Also, let $ed \equiv 1 \bmod \varphi(N)$ with $e \sim N^{\alpha}$ and $d \sim N^{\beta}$. If $d < N^{0.292}$, the modulus N can factor in time polynomial in $log(n)$.*

The problem solve with the help of Howgrave-Graham's lemma mentioned below;

Lemma 1. *Let $h(x, y) \in \mathbb{Z}(x, y)$ be a polynomial sum of at most w monomials. Suppose that*

1) $h(x_0, y_0) \equiv 0$ $(mod\ e^m)$ *for some integer $m > 0$ and (x_0, y_0) satisfies $x_0 < X$, $y_0 < Y$ and*
2) $\| h(x, y)\| < e^m / \sqrt{w}$.

Then, $h(x_0, y_0) = 0$ holds over the integers.

This lemma solves the small inverse problem easily. In bivariate case they found another polynomial $h(x, y)$ that has small roots as $f(x, y)$, which satisfy the conditions of above lemma especially $\|h(xX, yY)\|$ has small norm. They found the roots of $h(x, y)$ over the integers in order to solve the small inverse problem. The main idea was to construct the polynomial $h(x, y)$ as an integer linear combination of the polynomials called shift polynomials. Initially they calculated the weak bound $\delta \leq 0.284$ by plugging the maximum value $\tau = \frac{1}{2} - \beta$ in an inequality as: $3\beta^2 + 7\beta - \frac{7}{4} < 0$ then $\beta = \frac{7}{6} - \frac{1}{3}\sqrt{7} \approx 0.284.$ The bound of δ improve upto $\delta < 1 - \sqrt{2}/2,$ it gives considerable improvement as compared to Wiener's bound. Unfortunately, the determinants of sub-lattices are much difficult to compute as the matrices are no longer triangular though progressive matrix concept is used to obtained an improved bound of d i.e. $\delta \leq 0.292$. They also claim that their result can improve up to $\delta < 0.5$, this means the private key d should be smaller than $n^{0.5}$. How to improve the bound more then Boneh and Durfee's bound? is still an open problem.

5.1.4 Coron's lattice reduction technique

Coron's [53] described a more simplified technique to full rank lattice and construct an optimized triangular basis which derives the determinant with an improve bounds. For example, if the complexity of Coron's algorithm is $XY < W^{2/3\delta - \varepsilon}$ where, $XY \in \mathbb{Z}$, W is the lattice dimension and $\varepsilon > 0$ is chosen as fixed. Whereas, in Coppersmith's algorithm complexity relation is defined as $XY < W^{2/3\delta}$ that is slightly improve result then Coron's approach. In an experiment, when high or low order bits of $p\,(1/4 \log_2 n)$ is known in advance, Coron's approach found the factorization of RSA modulus. We describe Coron's theorem statement below;

Theorem 5 (Coron's Theorem). *Let $N = pq$ be the given modulus and high-order $(1/4 + \varepsilon)\log_2 n$ bits of p are known for any $\varepsilon > 0$. One can recover the factorization of n in time polynomial in $\log_n$.*

6. Large Private Exponent Attack

6.1 *$d > e$ a special case of BD attack*

A special case of Boneh and Durfee attack was studied by Luo et al. [54]. They studied RSA system with low public exponent less then private exponent i.e. $e < d$, under some constrained conditions. They solved the problem as stated below;

Theorem 6. *Let $N = pq$ be the modulus of n-bits where p, q are the primes with $q < p < 2q$. Also, let $ed \equiv 1 \bmod \varphi(N)$ with $e \sim N^{\alpha}$, $d \sim N^{\beta}$ and $d > e$. Then, if $d < N^{0.5}$ under algebraic independence assumption, the modulus N can be factored in time polynomial $\log(n)$.*

Open Question: How can improve the multivariate polynomial bound without the assumption of algebraic independence.

7. Challenges and advancements

RSA algebraic cryptanalysis research depends widely on Coppersmith's lattice reduction technique. In a univariate and bivariate polynomials Coppersmith's approach gives remarkable outcome where in multivariate polynomials results depends on heuristic outcome. The major challenges are Bound optimization, multivariate polynomial equation rigorous solution and Coppersmith's method limitations. We describe all of them briefly below.

7.1 *Bound Optimization*

RSA underlying algebraic structure of the polynomial further improve through optimization. In a univariate case, one needs to define an algebraic multiple of polynomials $f(x)$ that maximize the size of the root x_0. Whereas, in multivariate case choices are limited and it appears to be a complex optimization problem. In almost all applications of Coppersmith's method, the preliminary step is to choose either the modular polynomial equation or integer polynomial equation i.e. ($f(x_1, ..., x_m) = 0 \; mod \; b$ or $f(x_1, ..., x_m) = 0$). Whereas, in a univariate case, a function $f(x)$ is used to find an integer linear combination $f_1(x) = \Sigma_i \, a_i \cdot f_i(x)$, where $a_i \in \mathbb{Z}$ so that the root $f_1(x_0) = 0$ over some integer appears and then we can find the root by standard root finding method. In a bivariate polynomial case say $f_1(x, y)$ needs some algebraic multiples of $g_1(x, y)$, $g_n(x, y)$ and then find a polynomial $h(x, y) = \Sigma_i \, a_i g_i(x, y)$ by using LLL-reduction. Finally the roots (x_0, y_0) get by some resultant method. Also, Newton polytope play a central role to optimize the bounds. For example a polynomial equation $g(x, y) = xy - N$, where W is the dimension, $W = N$ denotes a full rank lattice. According to Newton's polytope, the line formed the points (0, 0) and (1, 1). When apply the Coppersmith's method, it yields the bound $XY \leq W^{1-\varepsilon} = N^{1-\varepsilon}$, where ε denotes small error term. It eliminate by brute-force technique and obtain an optimized bound. Bound optimization is one of the crucial task still needs more optimal way of solution.

7.2 *Multivariate polynomial equation for rigorous solution*

Multivariate polynomial equation is another challenging issue in RSA cryptanalysis. The results obtained from past studies are heuristic only. As roots are computed on the basis of resultant computation, one study describe negative outcome [52]. In bivariate case polynomial $f_1(x, y)$ does not lie in an ideal $< f >$ therefore, the resultant of f and f_1 can not equal to zero polynomial and bivariate case mostly can not fail. But for trivariate case it is difficult to achieve results every time. In trivariate case, the resultant obtained are bivariate, $r_1 = Res(f, g_1)$ and $r_2 = Res(f, g_2)$. Then, eventually the final resultant $R(r_1, r_2)$ combined together in a univariate form yields one coordinate of the roots with algebraically independence of f_1 and f_2. A study done by Bauer and Joux [55] proposed a mechanism of algebraic independence of polynomials. Their technique was based on an iterative application of Coppersmith's technique by choosing trivariate polynomial $p_1(x, y, z)$ and then constructs a polynomial $p_2(x, y, z)$ in a way p_2 does not fall on an Ideal $< p_1 >$. After that they use a Gröbner basis technique with an iteration of LLL reduction to obtain a third polynomial $p_3(x, y, z)$. The third polynomial also does not fall on an Ideal $< p_1, p_2 >$. Their approach though gives rigorous result but only for special shapes of trivariate polynomials that picked in advance. Whereas, in generic multivariate case still it incorporates a heuristic assumption and needs more fine grained approach to solve this open problem.

7.3 *Limitations of Coppersmith's Method*

Coppersmith's method is the promising direction towards cryptanalysis of small RSA exponents. It produced small solutions of polynomial equation in a constructive way within a pre-set boundaries. As it is running in time polynomial therefore, it produce number of polynomial solutions. Due to this one can limits the size of an interval in search space for finding specific solution within polynomial time. The most important part of Coppersmith's method is the enabling condition, which is bounded on the determinant of the lattice. The enabling condition mathematically represents as;

$$|\Lambda| \leq e^{m(n-1)}(n2^n)^{(1-n)/2} \tag{3}$$

where, $n = dim(\Lambda)$. Equation (3) enables LLL to produce a short vector over a lattice. Though in RSA (for small exponent case), it helps best when one selects a large key space instead of small keys. This is somewhat an inherent limitation of Coppersmith's approach.

To get an algebraic independence in multivariate case, it is unfortunate to get rigorous results unless liberalizing the norm criterion. As LLL outputted several vectors those somewhat logarithmically same. Therefore, it is hard to differentiate all of them easily until a concrete examination of the underlying geometry of the input/output lattices observed. This way we can differentiate the importance of shortest vector according to their length. Also the length obtained through enabling condition is actually quadratic in polynomial coefficients, but the requirement is a linear, say a linear functional on lattice Λ. Due to that it might loss some useful information. Therefore, the geometry of small variables should known in advance. Also by examining the algebraic independence of long and short vectors of certain ranges say 1000-bit RSA modulus can help to obtain rigorous solution. A study [56] shows that discarded long vectors also contains useful information. The study also concludes that long discarded vectors can also work in situation even when short vectors become fail or it might not be found. Though the ultimate goal of Coppersmith's approach is to increase the probability of occurrence of short vectors without considering long vectors. Such limitation aparent as research goes towards multivariate cases. Therefore, identify the sub-lattices having short vectors, as lattice dimension does not affect the sub-lattices. Though lattice dimension improved by Herrman-May [31], but their work was based on linear aspect of polynomials also they focused on short vectors and completely ignore the longer ones.

8. Conclusions

RSA proved to be a secure public key cryptography algorithm after four decades since 1977. No devastating attack hardly harm the security of RSA, though some insightful attacks discovered but all those illustrates only the negligence of the system designers pitfall. If the system is well implemented, it is widely trusted among internet community.

In this study we survey past literature in detail and categorized attacks on RSA into different sub-categories, those includes Integer factorization attacks, basic elementary attacks, weak public/private exponent attacks on the basis of lattice reduction technique with some popular results, challenges and advances. We conclude that redundant RSA modulus shouldn't be a good choice. A number of ways devise to protect RSA security including large value of public exponent enhances the speed and accuracy of the algorithm, also CRT-RSA is a good choice for resource intensive devices like smart cards. For messages, ciphertext can be protected by using randomized padding schemes. For fixed message, the probability becomes increased to break the security. A number of possible applications at low level to enterprise scale needs public key [57, 16] algorithm that can strengthen the systems security. As a final note, a well implemented RSA solution is still secure since last forty years and defeats all possible attacks.

Acknowlegment

This research is done at key laboratory of information security, Beijing and it was supported by the National Natural Science foundation of China under Grant No's. 90818021,9071803.

References

[1] R. L. Rivest, A. Shamir, L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, Communications of the ACM 21 (2) (1978) 120–126.

[2] G. Lokeshwari, S. Susarla, S. U. Kumar, A modified technique for reliable image encryption method using merkle-hellman cryptosystem and rsa algorithm, *Journal of Discrete Mathematical Sciences and Cryptography* 18 (3) (2015) 293–300. doi:10.1080/09720529.2014.968367.

[3] G. Iovane, A. Amorosia, E. Benedetto, G. Lamponi, An information fusion approach based on prime numbers coming from rsa algorithm and fractals for secure coding, *Journal of Discrete Mathematical Sciences and Cryptography* 18 (5) (2015) 455–479. doi:10.1080/09720529.2014.89 4311.

[4] O. Khadir, Algorithm for factoring some rsa and rabin moduli, *Journal of Discrete Mathematical Sciences and Cryptography* 11 (5) (2008) 537–543. doi:10.1080/09720529.2008.10698205.

[5] B. Kitchenham, R. Pretorius, D. Budgen, O. P. Brereton, M. Turner, M. Niazi, S. Linkman, Systematic literature reviews in software engineering–a tertiary study, *Information and Software Technology* 52 (8) (2010) 792– 805.

[6] C. Pomerance, The quadratic sieve factoring algorithm, in: Workshop on the Theory and Application of Cryptographic Techniques, Springer, 1984, pp. 169–182.

[7] H. W. Lenstra Jr, Factoring integers with elliptic curves, *Annals of mathematics* (1987) 649–673.

[8] A. K. Lenstra, H. W. Lenstra Jr, M. S. Manasse, J. M. Pollard, The number field sieve, in: Proceedings of the twenty-second annual ACM symposium on Theory of computing, ACM, 1990, pp. 564–572.

[9] A. K. Lenstra, H. W. Lenstra Jr, M. S. Manasse, J. M. Pollard, The number field sieve, in: The development of the number field sieve, Springer, 1993, pp. 11–42.

[10] T. Kleinjung, K. Aoki, J. Franke, A. Lenstra, E. Thomé, J. Bos, P. Gaudry, A. Kruppa, P. Montgomery, D. A. Osvik, et al., Factorization of a 768-bit rsa modulus, in: CRYPTO 2010, Vol. 6223, Springer, 2010, pp. 333–350.

[11] K. Gagneja, J. Singh, Survey and analysis of security issues on rsa algorithm for digital video data, *Journal of Discrete Mathematical Sciences*

and Cryptography 19 (1) (2016) 39–55. doi:10.1080/09720529.2015.1085730.

[12] H. Om, M. R. Reddy, Rsa based remote password authentication using smart card, *Journal of Discrete Mathematical Sciences and Cryptography* 15 (2-3) (2012) 105–111. doi:10.1080/09720529.2012.10698367.

[13] D. Chaum, Blind signature system, in: Advances in cryptology, Springer, 1984, pp. 153–153.

[14] R. L. Rivest, B. Kaliski, Rsa problem, in: Encyclopedia of cryptography and security, Springer, 2005, pp. 532–536.

[15] M. Bellare, C. Namprempre, D. Pointcheval, M. Semanko, The power of rsa inversion oracles and the security of chaum's rsa-based blind signature scheme, in: International Conference on Financial Cryptography, Springer, 2001, pp. 319–338.

[16] H. Om, S. Kumari, Comment and modification of rsa based remote password authentication using smart card, *Journal of Discrete Mathematical Sciences and Cryptography* 20 (3) (2017) 625–635. doi:10.1080/09720529.2014.932130.

[17] D. Pointcheval, J. Stern, Security arguments for digital signatures and blind signatures, *Journal of cryptology* 13 (3) (2000) 361–396.

[18] M. Burmester, E. Magkos, Towards secure and practical e-elections in the new era., Secure electronic voting 7 (2003) 63–76.

[19] X.-h. Sun, Study of a secure e-lottery scheme based on e-cash, in: Intelligent Computing and Intelligent Systems, 2009. ICIS 2009. IEEE International Conference on, Vol. 3, IEEE, 2009, pp. 195–197.

[20] J. Hastad, Solving simultaneous modular equations of low degree, *siam Journal on Computing* 17 (2) (1988) 336–341.

[21] D. Coppersmith, M. Franklin, J. Patarin, M. Reiter, Low-exponent rsa with related messages, in: International Conference on the Theory and Applications of Cryptographic Techniques, Springer, 1996, pp. 1–9.

[22] D. Coppersmith, Small solutions to polynomial equations, and low exponent rsa vulnerabilities, *Journal of Cryptology* 10 (4) (1997) 233–260.

[23] D. Boneh, et al., Twenty years of attacks on the rsa cryptosystem, Notices of the AMS 46 (2) (1999) 203–213.

[24] A. May, M. Ritzenhofen, Solving systems of modular equations in one variable: how many rsa-encrypted messages does eve need to know?, Lecture Notes in Computer Science 4939 (2008) 37–46.

[25] M. K. Franklin, A linear protocol failure for rsa with exponent three, Crypto'95 Rump Session, August.

[26] M. Bellare, P. Rogaway, The exact security of digital signatures-how to sign with rsa and rabin, in: International Conference on the Theory and Applications of Cryptographic Techniques, Springer, 1996, pp. 399–416.

[27] R. Steinfeld, Y. Zheng, On the security of rsa with primes sharing least-significant bits, Applicable Algebra in Engineering, Communication and Computing 15 (3) (2004) 179–200.

[28] D. Boneh, G. Durfee, Y. Frankel, An attack on rsa given a small fraction of the private key bits, in: AsiaCrypt, Vol. 98, Springer, 1998, pp. 25–34.

[29] H.-M. Sun, M.-E. Wu, H. Wang, J. Guo, On the improvement of the bdf attack on lsbs-rsa, in: Australasian Conference on Information Security and Privacy, Springer, 2008, pp. 84–97.

[30] E. Jochemsz, A. May, A strategy for finding roots of multivariate polynomials with new applications in attacking rsa variants, in: Asiacrypt, Vol. 6, Springer, 2006, pp. 267–282.

[31] M. Herrmann, A. May, Maximizing small root bounds by linearization and applications to small secret exponent rsa., in: Public Key Cryptography, Vol. 6056, Springer, 2010, pp. 53–69.

[32] Y. Lu, L. Peng, N. Kunihiro, Recent progress on coppersmith's lattice-based method: A survey, in: Mathematical Modelling for Next-Generation Cryptography, Springer, 2018, pp. 297–312.

[33] M. Herrmann, A. May, Attacking power generators using unravelled linearization: When do we output too much?, in: ASIACRYPT, Vol. 5912, Springer, 2009, pp. 487–504.

[34] N. Howgrave-Graham, Approximate integer common divisors, in: CaLC, Vol. 1, Springer, 2001, pp. 51–66.

[35] L. Peng, L. Hu, J. Xu, Z. Huang, Y. Xie, Further improvement of factoring rsa moduli with implicit hint, in: International Conference on Cryptology in Africa, Springer, 2014, pp. 165–177.

[36] T. Takagi, Fast rsa-type cryptosystem modulo p k q, in: Annual International Cryptology Conference, Springer, 1998, pp. 318–326.

[37] Y. Lu, R. Zhang, L. Peng, D. Lin, Solving linear equations modulo unknown divisors: revisited, in: International Conference on the Theory and Application of Cryptology and Information Security, Springer, 2015, pp. 189–213.

[38] H.-M. Sun, M.-E. Wu, W.-C. Ting, M. J. Hinek, Dual rsa and its security analysis, IEEE Transactions on Information Theory 53 (8) (2007) 2922– 2933.

[39] D. Coppersmith, Finding a small root of a univariate modular equation, in: Advances in cryptology—EUROCRYPT'96, Springer, 1996, pp. 155–165.

[40] N. Howgrave-Graham, Finding small roots of univariate modular equations revisited, in: IMA International Conference on Cryptography and Coding, Springer, 1997, pp. 131–142.

[41] M. J. Wiener, Cryptanalysis of short rsa secret exponents, IEEE Trans-ac-tions on Information theory 36 (3) (1990) 553–558.

[42] E. R. Verheul, H. C. van Tilborg, Cryptanalysis of 'less short'rsa secret exponents, Applicable Algebra in Engineering, Communication and Computing 8 (5) (1997) 425–435.

[43] A. Dujella, Continued fractions and rsa with small secret exponent, arXiv preprint cs/0402052.

[44] Y. Aono, A new lattice construction for partial key exposure attack for rsa., in: Public Key Cryptography, Springer, 2009, pp. 34–53.

[45] Y. Aono, Simplification of the lattice based attack of boneh and durfee for rsa cryptoanalysis, in: Computer Mathematics, Springer, 2014, pp. 15–32.

[46] M. Bunder, A. Nitaj, W. Susilo, J. Tonien, A generalized attack on rsa type cryptosystems, Theoretical Computer Science 1 (2017) 1–8. doi:10.1016/j.tcs.2017.09.009.

[47] A. Nitaj, A new vulnerable class of exponents in rsa, *JP Journal of Algebra, Number Theory and Applications* 21 (2) (2011) 203–220.

[48] L. Lovász, An algorithmic theory of numbers, graphs and convexity, SIAM, 1986.

[49] A. K. Lenstra, H. W. Lenstra, L. Lovász, Factoring polynomials with ra-tional coefficients, Mathematische Annalen 261 (4) (1982) 515–534.

[50] N. Gama, P. Nguyen, Predicting lattice reduction, Advances in Cryptology– EUROCRYPT 2008 (2008) 31–51.

[51] D. Stehlé, Floating-point lll: theoretical and practical aspects, in: The LLL Algorithm, Springer, 2009, pp. 179–213.

[52] J. Blömer, A. May, Low secret exponent rsa revisited, in: Cryptography and Lattices, Springer, 2001, pp. 4–19.

[53] J.-S. Coron, Finding small roots of bivariate integer polynomial equations revisited, in: International Conference on the Theory and Applications of Cryptographic Techniques, Springer, 2004, pp. 492–505.

[54] P. Luo, H. Zhou, D. Wang, Y. Dai, Cryptanalysis of rsa for a special case with $d > e$, Science in China Series F: Information Sciences 52 (4) (2009) 609–616.

[55] A. Bauer, A. Joux, Toward a rigorous variation of coppersmith's algorithm on three variables, in: Annual International Conference on the Theory and Applications of Cryptographic Techniques, Springer, 2007, pp. 361–378.

[56] S. D. Miller, B. Narayanan, R. Venkatesan, Coppersmith's lattices and" focus groups": an attack on small-exponent rsa, arXiv preprint arXiv:1708.09445.

[57] H. Zhao, Research on applying physical chaos generator to spacecraft information security, Science in China Series E: Technological Sciences 52 (5) (2009) 1463–1470.

Received March, 2018

Revised October, 2018