THE LAST DECADE OF THE RSA CRYPTOSYSTEM

Abderrahmane Nitaj

University of Caen Normandy, France

Caen, France

February 5, 2025

Contents

Contents

Nov. 2024

NIST Special Publication 800
NIST SP 800-131Ar3 ipd

Transitioning the Use of Cryptographic Algorithms and Key Lengths

Initial Public Draft

Elaine Barker
Allen Roginsky

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-131Ar3.ipd

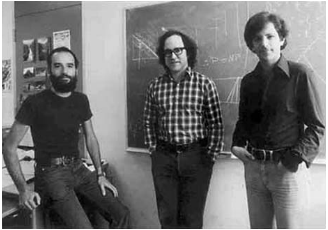
Table 2: Quantum-vulnerable digital signature algorithms

Digital Signature Algorithm Family	Parameters	Transition
ECDSA [FIPS186]	112 bits of security strength	***Deprecated*** after 2030 ***Disallowed*** after 2035
	≥ 128 bits of security strength	***Disallowed*** after 2035
EdDSA [FIPS186]	≥ 128 bits of security strength	***Disallowed*** after 2035
RSA [FIPS186]	112 bits of security strength	***Deprecated*** after 2030 ***Disallowed*** after 2035
	≥ 128 bits of security strength	***Disallowed*** after 2035

Member-only story

Shock News: SHA-256, ECDH, ECDSA and RSA Not Approved by ASD in Australia for 2030

The RSA Cryptosystem



- Invented in 1978 by Rivest, Shamir and Adleman.
- The most widely used asymmetric cryptosystem.
- Many applications such as encryption and digital signatures.

RSA®
The Security Division of EMC

https://www.nist.gov

An official website of the United States government Here's how you know

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE

Official UTC(NIST) Time
22:32:01
heure d'été d'Europe centrale (UTC+2)

Search NIST

Topics | Publications | Labs & Major Programs | Services & Resources | News & Events | About NIST

Nom DNS	www.nsrl.nist.gov
Nom DNS	www.pscr.gov
Nom DNS	ciks.cbt.nist.gov

Informations sur la clé publique

Algorithme	RSA
Taille de la clé	2048
Exposant	65537
Module	B8:67:0C:01:FC:19:40:F1:2A:0E:8D:AD:0C:4C:B7:7C:55:5A:1C:8D:12:CE:B1:FF:55:F5:...

Divers

Numéro de série	02:AD:4C:E5:B8:69:63:68:A7:40:9B:E0:F3:62:2E:14
Algorithme de signature	SHA-256 with RSA Encryption
Version	3
Télécharger	PEM (cert) PEM (chain)

Empreintes numériques

SHA-256	C1:C3:B3:AF:3D:5B:BF:54:B1:2D:E2:AF:1B:F5:FB:F8:67:0B:E5:69:19:CB:0B:C5:0C:F0:...
SHA-1	DC:4F:53:91:F9:F8:C3:6A:B4:4D:4D:47:43:DF:28:F2:98:51:BD:FA

The RSA Cryptosystem

Key Generation

1. Generate two large primes p and q of the same bit size.
2. Compute $N = pq$ and $\phi(N) = (p-1)(q-1)$.
3. Choose a random e with $1 \leq e \leq \phi(N)$ such that $\gcd(e, \phi(N)) = 1$.
4. Compute $d \equiv e^{-1} \pmod{\phi(N)}$.
5. Publish the public key (N, e).
6. The private key is (N, d).

Encryption

1. Compute $c \equiv m^e \pmod{N}$.
2. Send the ciphertext c.

Decryption

1. Compute $m \equiv c^d \pmod{N}$.

The RSA Cryptosystem

Key Generation

1. Generate two large primes p and q of the same bit size.
2. Compute $N = pq$ and $\phi(N) = (p-1)(q-1)$.
3. Choose a random e with $1 \leq e \leq \phi(N)$ such that $\gcd(e, \phi(N)) = 1$.
4. Compute $d \equiv e^{-1} \pmod{\phi(N)}$.
5. Publish the public key (N, e).
6. The private key is (N, d).

Encryption

1. Compute $c \equiv m^e \pmod{N}$.
2. Send the ciphertext c.

Decryption

1. Compute $m \equiv c^d \pmod{N}$.

The RSA Cryptosystem

Key Generation

1. Generate two large primes p and q of the same bit size.
2. Compute $N = pq$ and $\phi(N) = (p-1)(q-1)$.
3. Choose a random e with $1 \leq e \leq \phi(N)$ such that $\gcd(e, \phi(N)) = 1$.
4. Compute $d \equiv e^{-1} \pmod{\phi(N)}$.
5. Publish the public key (N, e).
6. The private key is (N, d).

Encryption

1. Compute $c \equiv m^e \pmod{N}$.
2. Send the ciphertext c.

Decryption

1. Compute $m \equiv c^d \pmod{N}$.

RSA: The hard problems

The equations

$$N = pq, \qquad \phi(N) = (p-1)(q-1) = N + 1 - (p+q),$$
$$ed - k\phi(N) = 1, \qquad c \equiv m^e \pmod{N}.$$

The Integer Factorization Problem

Let $N = pq$ be an RSA modulus with unknown factorization. The Integer Factorization Problem is to find p and q.

The Key Equation Problem

Given $N = pq$ and e satisfying $ed - k\phi(N) = 1$. Find d, k and $\phi(N)$.

The RSA Problem

Given $N = pq$, e and c. Find an integer $m \in \mathbb{Z}_N^*$ such that

$$m^e \equiv c \pmod{N}.$$

RSA: The hard problems

The equations

$$N = pq, \qquad \phi(N) = (p-1)(q-1) = N + 1 - (p+q),$$
$$ed - k\phi(N) = 1, \quad c \equiv m^e \pmod{N}.$$

The Integer Factorization Problem

Let $N = pq$ be an RSA modulus with unknown factorization. The Integer Factorization Problem is to find p and q.

The Key Equation Problem

Given $N = pq$ and e satisfying $ed - k\phi(N) = 1$. Find d, k and $\phi(N)$.

The RSA Problem

Given $N = pq$, e and c. Find an integer $m \in \mathbb{Z}_N^*$ such that

$$m^e \equiv c \pmod{N}.$$

RSA: The hard problems

The equations

$$N = pq, \qquad \phi(N) = (p-1)(q-1) = N + 1 - (p+q),$$
$$ed - k\phi(N) = 1, \qquad c \equiv m^e \pmod{N}.$$

The Integer Factorization Problem

Let $N = pq$ be an RSA modulus with unknown factorization. The Integer Factorization Problem is to find p and q.

The Key Equation Problem

Given $N = pq$ and e satisfying $ed - k\phi(N) = 1$. Find d, k and $\phi(N)$.

The RSA Problem

Given $N = pq$, e and c. Find an integer $m \in \mathbb{Z}_N^*$ such that

$$m^e \equiv c \pmod{N}.$$

RSA: The hard problems

The equations

$$N = pq, \qquad \phi(N) = (p-1)(q-1) = N + 1 - (p+q),$$
$$ed - k\phi(N) = 1, \quad c \equiv m^e \pmod{N}.$$

The Integer Factorization Problem

Let $N = pq$ be an RSA modulus with unknown factorization. The Integer Factorization Problem is to find p and q.

The Key Equation Problem

Given $N = pq$ and e satisfying $ed - k\phi(N) = 1$. Find d, k and $\phi(N)$.

The RSA Problem

Given $N = pq$, e and c. Find an integer $m \in \mathbb{Z}_N^*$ such that

$$m^e \equiv c \pmod{N}.$$

Some variants of the RSA Cryptosystem

1. KMOV, based on elliptic curves, 1991: Modulus $N = pq$, key equation $ed - k(p+1)(q+1) = 1$.
2. Takagi RSA, 1998: Modulus $N = p^r q$, key equation $ed - k(p-1)(q-1) = 1$.
3. Prime Power RSA, 1998: Modulus $N = p^r q^s$, key equation $ed - kp^{r-1}q^{s-1}(p-1)(q-1) = 1$.
4. LUC, KKT cryptosystems, 1993: Modulus $N = pq$, key equation $ed - k\left(p^2-1\right)\left(q^2-1\right) = 1$.
5. RSA with Gaussian integers, 2002: Modulus $N = PQ$, key equation $ed - k\left(|P|^2-1\right)\left(|Q|^2-1\right) = 1$.
6. Generalization of KMOV and Edwards curves: Modulus $N = p^r q^s$, key equation $ed - kp^{r-1}q^{s-1}(p+1)(q+1) = 1$.
7. Cubic Pell curve 2018, 2024: Modulus $N = pq$, key equation $ed - k\left(p^2+p+1\right)\left(q^2+q+1\right) = 1$.

Contents

Shor's algorithm

Facts

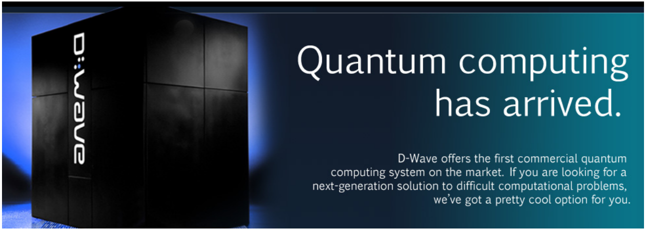
- Presented by Peter Shor in 1994.
- Complexity of factorization on a classical computer

$$\mathcal{O}\left(e^{c\ln(n)^{\frac{1}{3}}\ln\ln(n)^{\frac{2}{3}}}\right).$$

- Complexity of factorization on a quantum computer

$$\mathcal{O}\left((\ln(n))^2(\ln\ln(n))^2\ln\ln\ln(n)\right).$$

Consequences of Shor's algorithm



Vulnerability to quantum computers

- The RSA cryptosystem and its variants: vulnerable.
- The Diffie-Hellman key exchange protocol: vulnerable.
- The El Gamal Cryptosystem: vulnerable.
- The elliptic curve cryptosystems and protocols: vulnerable.
- Digital Signature Algorithm (DSA):vulnerable.
- Elliptic Curve Digital Signature Algorithm (ECDSA):vulnerable.

Reduction to Order Finding

- **INPUT :** A positive integer n.
  1. Choose an integer x at random with $2 \le x \le n-1$.
  2. Compute the order r of x modulo n, that is
     the smallest $r \ge 1$ such that $x^r \equiv 1 \pmod{n}$.
  3. Compute $\gcd\left(n, x^{r/2}-1\right)$.
- **OUTPUT :** A factor of n.
- The quantum part is Step 2.
- The (quantum) polynomial time: $O\left((\log n)^3\right)$.

Example

- $n = 3301033176670071726715065074773$; $x = 2457121578798 1$.
- Then $r = 550172196111676677823842611058$ with $r \approx n^{0.97}$.
- $\gcd\left(n, x^{r/2}+1\right) = 1136942909517 4399$ and
  $\gcd\left(n, x^{r/2}-1\right) = 290342914234027$.

Reduction to Order Finding

- **INPUT :** A positive integer n.
  1. Choose an integer x at random with $2 \le x \le n-1$.
  2. Compute the order r of x modulo n, that is

     the smallest $r \ge 1$ such that $x^r \equiv 1 \pmod{n}$.
  3. Compute $\gcd\left(n, x^{r/2}-1\right)$.
- **OUTPUT :** A factor of n.
- The quantum part is Step 2.
- The (quantum) polynomial time: $O\left((\log n)^3\right)$.

Example

- $n = 330103317667007172671506507473$; $x = 24571215787981$.
- Then $r = 55017219611167667823842611058$ with $r \approx n^{0.97}$.
- $\gcd\left(n, x^{r/2}+1\right) = 1136942909517439\!9$ and

  $\gcd\left(n, x^{r/2}-1\right) = 290342914234027$.

中国人的进攻
Zhōngguó rén de jìngōng

第 47 卷 第 5 期 计 算 机 学 报 Vol. 47 No. 5
2024 年 5 月 CHINESE JOURNAL OF COMPUTERS May 2024

基于 D-Wave Advantage 的量子退火公钥密码攻击算法研究

王 潮 王启迪 洪春雷 胡巧云 裴 植
(上海大学特种光纤与光接入网重点实验室 上海 200444)

摘 要 D-Wave 专用量子计算机的原理量子退火凭借独特的量子隧穿效应可跳出传统智能算法极易陷入的局部极值,可视为一类具有全局寻优能力的人工智能算法. 本文研究了两类基于量子退火的 RSA 公钥密码攻击算法(分解大整数 $N=pq$):一是将密码攻击数学方法转为组合优化问题或指数级空间搜索问题,通过 Ising 模型或 QUBO 模型求解,提出了乘法表的高位优化模型,建立新的降维公式,使用 D-Wave Advantage 分解了 200 万整数 2269753. 大幅度超过普渡大学、Lockheed Martin 和富士通等实验指标,且 Ising 模型系数 h 范围缩小了 84%,系数 J 范围缩小了 80%,极大地提高了分解成功率,这是一类完全基于 D-Wave 量子计算机的攻击算法;二是基于量子退火算法融合密码攻击数学方法优化密码部件的攻击,采用量子退火优化 CVP 问题求解,通过量子隧穿效应获得比 Babai 算法更近的向量,提高了 CVP 问题中光滑对的搜索效率,在 D-Wave Advantage 上实现首次 50 比特 RSA 整数分解. 实验表明,在通用量子计算机器件进展缓慢情况下,D-Wave 表现出更好的现实攻击能力,且量子退火不存在 NISQ 量子计算机 VQA 算法的致命缺陷贫瘠高原问题:算法会无法收敛且无法扩展到大规模攻击.

关键词 RSA; D-Wave; 量子退火; CVP; 量子隧穿; 整数分解; 量子计算
中图法分类号 TP309 **DOI 号** 10.11897/SP.J.1016.2024.01030

The Chinese attack, 2024

Quantum Annealing Public Key Cryptographic Attack Algorithm Based on D-Wave Advantage

WANG Chao WANG Qi-Di HONG Chun-Lei HU Qiao-Yun PEI Zhi

(*Key Laboratory of Specialty Fiber Optics and Optical Access Networks, Shanghai University, Shanghai* 200444)

Analysis of the attack

- D Wave Advantage: 5000 qubits, 2 million variables, unknown price.
- Based on quantum annealing: combinatorial optimization problems, not on Shor's algorithm.
- Factor an integer up to 2^{50}.
- Far from $2^{2048} \approx \left(2^{50}\right)^{41}$.

中国万岁
Zhōngguó wànsuì

TSINGHUA SCIENCE AND TECHNOLOGY
ISSN 1007-0214 22/28 pp1270–1282
DOI: 10.26599/TST.2024.9010028
Volume 30, Number 3, June 2025

A First Successful Factorization of RSA-2048 Integer by D-Wave Quantum Computer

Chao Wang, Jingjing Yu, Zhi Pei*, Qidi Wang, and Chunlei Hong

Abstract: Integer factorization, the core of the Rivest–Shamir–Adleman (RSA) attack, is an exciting but formidable challenge. As of this year, a group of researchers' latest quantum supremacy chip remains unavailable for cryptanalysis. Quantum annealing (QA) has a unique quantum tunneling advantage, which can escape local extremum in the exponential solution space, finding the global optimal solution with a higher probability. Consequently, we consider it an effective method for attacking cryptography. According to Origin Quantum Computing, QA computers are able to factor numbers several orders of magnitude larger than universal quantum computers. We try to transform the integer factorization problem in RSA attacks into a combinatorial optimization problem by using the QA algorithm of D-Wave quantum computer, and attack RSA-2048 which is composed of a class of special integers. The experiment factored this class of integers of size 2^{2048}, $N=p\times q$. As an example, the article gives the results of 10 RSA-2048 attacks in the appendix. This marks the first successful factorization of RSA-2048 by D-Wave quantum computer, regardless of employing mathematical or quantum techniques, despite dealing with special integers, exceeding $2^{1061}-1$ of California State University. This experiment verifies that the QA algorithm based on D-Wave is an effective method to attack RSA.

	N ($N=p\times q$)	p	q
1	2344221089529646655151068154361983197810258179973 6611246976521590191893224135789025070678051976867 3493065933323317287750867313641112828898759744515 6040874014601593498699047621427064008681742558153 8170373870259313066583768903697048280641467367411 5899391004146113560115133979780382186697097472478 6872772467600158490577052523497666938289546423287 1732123454572174833964467804115311936850586791492 8449735609052294298924389262041881744905437550809 7262165283165093027743111302874592959317102563951 8249955921255776393078247519734666509055776152948 5013603452022242275599644386533529497325415067214 38058592990053089448078211591	15310849387051152934318398 2 6945810375548166939018931 86 0902798006004492850911092 72 5780710664273360703216936 01 5622744330985806196000996 63 9054102790231481525239396 50 0716155960774135164693214 66 4864549214045683424972165 91 9614393540648442582007387 32 4342415272089894881983294 00 8201158253359215854823896 11 993667849543	15310849387051152934318398 2 6945810375548166939018931 86 0902798006004492850911092 72 5780710664273360703216936 01 5622744330985806196000996 63 9054102790231481525239396 50 0716155960774135164693214 66 4864549214045683424972165 91 9614393540648442582007387 32 4342415272089894881983294 00 8201158253359215854823896 11 993667849537

Analysis of the attack

- D-Wave 2000Q: 2000 qubits, 15 000 000 \$.
- Quantum annealing: based combinatorial optimization problems, not Shor's algorithm.
- Factor an integer $N = pq \approx 2^{2048}$.

	N ($N=p\times q$)	p	q
1	2344221089529646655151068154361983197810258179973 6611246976521590191893224135789025070678051976867 3493065933323317287750867313641112828898759744515 6040874014601593498699047621427064008681742558153 8170373870259313066583768903697048280641467367411 5899391004146113560115133979780382186697097472478 6872772467600158490577052523497666938289546423287 1732123454572174833964467804115311936850586791492 8449735609052294298924389262041881744905437550809 7262165283165093027743111302874592959317102563951 8249955921255776393078247519734666509055776152948 5013603452022242275599644386533529497325415067214 38058592990053089448078211591	1531084938705115293431839822 6945810375548166939018931866 0902798006004492850911092722 5780710664273360703216936011 5622744330985806196000996633 9054102790231481525239396500 0716155960774135164693214666 4864549214045683424972165911 9614393540648442582007387322 4342415272089894881983294000 8201158253359215854823896111 993667849543	1531084938705115293431839822 6945810375548166939018931866 0902798006004492850911092722 5780710664273360703216936011 5622744330985806196000996633 9054102790231481525239396500 0716155960774135164693214666 4864549214045683424972165911 9614393540648442582007387322 4342415272089894881983294000 8201158253359215854823896111 993667849537

Analysis of the attack

- D-Wave 2000Q: 2000 qubits, 15 000 000 $\$$.
- Quantum annealing: based combinatorial optimization problems, not Shor's algorithm.
- Factor an integer $N = pq \approx 2^{2048}$.
- $|p-q| < 10 \Longrightarrow q = \text{PrevPrime}\left(\sqrt{N}\right),\ p = \text{NextPrime}\left(\sqrt{N}\right)$.

Contents

Wiener's attack, 1990

The RSA equation

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

Wiener's attack, 1990

f $d < \frac{1}{3}N^{\frac{1}{4}}$ then $\frac{k}{d}$ is among the convergents of the continued fraction expansion of $\frac{e}{N}$ and the factorization of $N = pq$ can be found.

The method

- $\frac{k}{d} \approx \frac{e}{N}$.
- The continued fraction algorithm.

Wiener's attack, 1990

The RSA equation

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

Wiener's attack, 1990

If $d < \frac{1}{3}N^{\frac{1}{4}}$ then $\frac{k}{d}$ is among the convergents of the continued fraction expansion of $\frac{e}{N}$ and the factorization of $N = pq$ can be found.

The method

- $\frac{k}{d} \approx \frac{e}{N}$.
- The continued fraction algorithm.

Wiener's attack, 1990

The RSA equation

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

Wiener's attack, 1990

If $d < \frac{1}{3}N^{\frac{1}{4}}$ then $\frac{k}{d}$ is among the convergents of the continued fraction expansion of $\frac{e}{N}$ and the factorization of $N = pq$ can be found.

The method

- $\frac{k}{d} \approx \frac{e}{N}$.
- The continued fraction algorithm.

Coppersmith's lattice based attack

Polynomial equation

Given a multivariate polynomial f and a modulus N, find a solution $(x_1, \ldots, x_n)$ of the equation

$$f(x_1, \ldots, x_n) \equiv 0 \pmod{N}.$$

Coppersmith's method

1. Lattices.
2. The LLL algorithm.
3. Jochemz-May strategy.
4. Howgrave-Graham's method.
5. Gröbner basis or resultant computation techniques.

Boneh and Durfee attack, 1999

The RSA equation

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

Boneh-Durfee's attack, 1999

If $d < N^{0.292}$, then the factorization of $N = pq$ can be found.

The method

- $k(N+1-x) \equiv 1 \pmod{e}$, where $x = p + q$.
- Lattice reduction techniques and Coppersmith's method for finding small roots of modular polynomial equations.

Boneh and Durfee attack, 1999

The RSA equation

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

Boneh-Durfee's attack, 1999

If $d < N^{0.292}$, then the factorization of $N = pq$ can be found.

The method

- $k(N+1-x) \equiv 1 \pmod{e}$, where $x = p + q$.
- Lattice reduction techniques and Coppersmith's method for finding small roots of modular polynomial equations.

Boneh and Durfee attack, 1999

The RSA equation

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

Boneh-Durfee's attack, 1999

If $d < N^{0.292}$, then the factorization of $N = pq$ can be found.

The method

- $k(N+1-x) \equiv 1 \pmod{e}$, where $x = p + q$.
- Lattice reduction techniques and Coppersmith's method for finding small roots of modular polynomial equations.

Contents

Factoring algorithms with the General Number Field Sieve

The RSA equation: $N = pq$

Name	Decimal size of N	Year	Authors
RSA-576	174	2003	Franke et al.
RSA200	200	2005	Bahr et al.
RSA768	232	2013	Kleinjung et al.
RSA-240	240	2019	Boudot et al.
RSA-250	250	2020	Boudot et al.

Boneh and Durfee attack, 1999

The RSA equation: $ed - (p-1)(q-1)k = 1.$

Main attacks: One can factor $N = pq$

1. Wiener 1990: If $d < \frac{1}{3}N^{0.25}$.
2. Boneh Durfee 1998: If $d < N^{0.292}$.

Improvements

- Partial prime attacks: p and q share their least significant bits (LSBs).
- Partial prime attacks: p and q share their most significant bits (LSBs).
- Partial prime attacks: MSBs or LSBs of p is known.
- Partial key attacks: MSBs or LSBs of d is known.

Boneh and Durfee attack, 1999

The RSA equation: $ed - (p-1)(q-1)k = 1.$

Main attacks: One can factor $N = pq$

1. Wiener 1990: If $d < \frac{1}{3}N^{0.25}$.
2. Boneh Durfee 1998: If $d < N^{0.292}$.

Improvements

- Partial prime attacks: p and q share their least significant bits (LSBs).
- Partial prime attacks: p and q share their most significant bits (LSBs).
- Partial prime attacks: MSBs or LSBs of p is known.
- Partial key attacks: MSBs or LSBs of d is known.

Boneh and Durfee attack, 1999

The RSA equation: $ed - (p-1)(q-1)k = 1.$

Main attacks: One can factor $N = pq$

1. Wiener 1990: If $d < \frac{1}{3}N^{0.25}$.
2. Boneh Durfee 1998: If $d < N^{0.292}$.

Improvements

- Partial prime attacks: p and q share their least significant bits (LSBs).
- Partial prime attacks: p and q share their most significant bits (LSBs).
- Partial prime attacks: MSBs or LSBs of p is known.
- Partial key attacks: MSBs or LSBs of d is known.

Achieving the upper bound 0.292 for $N \geq 2^{1000}$

Year	Bound	Condition	Time	Authors
2000	0.265	–	45 minutes	Boneh, Durfee
2002	0.277	–	2,5 hours	Durfee
2021	0.28	–	?	Miller, Narayanan
2023	0.285	–	1 month	Li, Zheng, Qi
2023	0.292	18 MSBs of p	1 month	Li, Zheng, Qi
2024	0.292	14 MSBs of $p+q$	23 hours	Feng, Liu, Nitaj, Pan*

* Y. Feng, Z., Liu, A. Nitaj, Y. Pan: Practical Small Private Exponent Attacks against RSA, Cryptology ePrint Archive, Paper 2024/1331, 2024

Contents

Murru and Saetton variant of RSA

- Proposed by Murru and Saetton in 2018.
- Modulus $N = pq$.
- A parameter: $r \in \mathbb{Z}/N\mathbb{Z}$, cubic non-residue modulo p, q, and N.
- The arithmetic operations are performed on the ring

$$\mathbb{Z}/N\mathbb{Z}[t]/\left(t^3 - r\right) = \left\{a_0 + a_1 t + a_2 t^2,\ a_i \in \mathbb{Z}/N\mathbb{Z}\right\}.$$

- The generalized Euler totient function

$$\psi(N) = \left(p^2 + q + 1\right)\left(q^2 + q + 1\right).$$

- Public key: (N, e, r).
- Private key: (N, d, p, q, r).
- Key equation $ed - k\psi(N) = 1$.

Murru and Saetton variant of RSA

- Public key (N, e, r).
- Private key (N, d, p, q, r) with $ed \equiv 1 \pmod{\psi(N)}$.
- To encrypt a message $(m_1, m_2) \in (\mathbb{Z}/N\mathbb{Z})^2$, compute

$$(c_1, c_2) \equiv (m_1, m_2)^e \pmod{N}.$$

- To decrypt $(c_1, c_2) \in (\mathbb{Z}/N\mathbb{Z})^2$, compute

$$(m_1, m_2) \equiv (c_1, c_2)^d \pmod{N}.$$

Murru and Saetton variant of RSA

RSA vs Murru and Saetton variant

- Modulus $N = pq$
- Public exponent e
- Private exponent d
- Euler's function $\phi(N) = (p-1)(q-1)$
- Ring $\mathbb{Z}/N\mathbb{Z}$
- Encryption $c \equiv m^e \pmod N$
- Decryption $m \equiv c^d \pmod N$
- Key equation $ed - k(p-1)(q-1) = 1$.

- Modulus $N = pq$
- Public exponent e, non-cubic residue r
- Private exponent d
- Euler's generalized function $\psi(N) = \left(p^2+p+1\right)\left(q^2+q+1\right)$.
- Ring $\mathbb{Z}/N\mathbb{Z}$
- Encryption $c \equiv m^e \pmod N$ on the Pell curve
- Decryption $m \equiv c^d \pmod N$ on the Pell curve
- Key equation $ed - k\left(p^2+p+1\right)\left(q^2+q+1\right) = 1$.

Seck and Nitaj variant of RSA

Key generation

- Proposed by Seck and N. in 2024.
- Modulus $N = pq$.
- The generalized Euler totient function is $\psi(n)$ with one of the values

$$\begin{aligned}
\psi_1(N) &= p^{2(r-1)}q^{2(s-1)}\left(p^2+p+1\right)\left(q^2+q+1\right),\\
\psi_2(N) &= p^{2(r-1)}q^{2(s-1)}(p-1)^2(q-1)^2,\\
\psi_3(N) &= p^{2(r-1)}q^{2(s-1)}\left(p^2+p+1\right)(q-1)^2,\\
\psi_4(N) &= p^{2(r-1)}q^{2(s-1)}(p-1)^2\left(q^2+q+1\right).
\end{aligned}$$

- Public key: (N, e).
- Private key: (N, d_i, p, q), $i = 1, 2, 3, 4$ with $e_i d_i \equiv 1 \pmod{\psi_i(N)}$.
- Key equations $ed_i - k\psi_i(N) = 1$.

Seck and Nitaj variant of RSA

Encryption

- Public key (N, e).
- Private key (N, d, p, q) with $ed \equiv 1 \pmod{\psi(N)}$.
- To encrypt a message $(m_1, m_2) \in (\mathbb{Z}/N\mathbb{Z})^2$, compute $a \equiv \frac{1-m_1^3}{m_2^3} \bmod N$.
- Compute the ciphertext

$$(c_1, c_2, c_3) \equiv e \cdot (m_1, m_2, 0) \pmod{N},$$

on the curve with the equation $x^3 + ay^3 + a^2z^3 - 3axyz \equiv 1 \pmod{N}$.

Seck and Nitaj variant of RSA

Decryption

- Private key: (N, d_i, p, q) with $ed_i \equiv 1 \pmod{\psi_i(N)}$, $i = 1, 2, 3, 4$.
- Ciphertext $(c_1, c_2, c_3) \in (\mathbb{Z}/N\mathbb{Z})^3$.
- Find the four solutions a_j, $j = 1, 2, 3, 4$, of the equation $c_1^3 + ac_2^3 + a^2c_3^3 - 3ac_1c_2c_3 \equiv 1 \pmod N$.
- Let $\mathcal{R}^3(p)$ be the set of cubic residues modulo p. For $i = 1, 2, 3, 4$, set

$$D = \begin{cases} d_1 & \text{if } a_i \notin \mathcal{R}^3(p) \text{ and } a_i \notin \mathcal{R}^3(q), \\ d_2 & \text{if } a_i \in \mathcal{R}^3(p) \text{ and } a_i \in \mathcal{R}^3(q), \\ d_3 & \text{if } a_i \notin \mathcal{R}^3(p) \text{ and } a_i \in \mathcal{R}^3(q), \\ d_4 & \text{if } a_i \in \mathcal{R}^3(p) \text{ and } a_i \notin \mathcal{R}^3(q), \end{cases}$$

- Compute $(m_1, m_2, m_3) \equiv D \cdot (c_1, c_2, c_3) \pmod N$ on the curve with the equation $x^3 + a_iy^3 + a_i^2z^3 - 3a_ixyz \equiv 1 \pmod N$.
- The plaintext is the triple (m_1, m_2, m_3) with $m_3 = 0$.

Seck and Nitaj variant of RSA

Security

- Public key (N, e).
- Private key (N, d, p, q).
- Euler's generalized: $\psi(N) = \left(p^2 + q + 1\right)\left(q^2 + q + 1\right)$.
- Public message: $(c_1, c_2, c_3) \in (\mathbb{Z}/N\mathbb{Z})^3$.
- Hard problem: Solve $ed - k\psi(N) = 1$.
- Hard problem: Solve $c_1^3 + ac_2^3 + a^2c_3^3 - 3ac_1c_2c_3 \equiv 1 \pmod{N}$
  This is equivalent to factoring (à la Rabin)

Contents

Conclusion

Le roi est mort, vive le roi

- RSA deprecated by 2030
- RSA disallowed by 2035
- 45 years of applications
- 45 years of attacks
- Future? Academic interest

- Crystals-Kyber KEM: FIPS 203 Module-LatticeBased Key-Encapsulation Mechanism Standard
- Crystals-Dilithium: FIPS 204 Module-LatticeBased Digital Signature Standard
- SPHINCS+:FIPS 205 Stateless HashBased Digital Signature Standard
- Falcon: FIPS 206 FFT-Over-NTRULattice-Based Digital Signature Standard
- Installation before 2030.

Thank you – Merci

Source: Medium