Zheng and Kang *Cybersecurity (2024)7:74*
https://doi.org/10.1186/s42400-024-00289-7

Cybersecurity

SURVEY

Open Access

Lattice-based cryptanalysis of RSA-type cryptosystems: a bibliometric analysis

Mengce Zheng[1,2*] and Hao Kang[1]

Abstract

The RSA (Rivest–Shamir–Adleman) cryptosystem is a widely used public-key cryptographic algorithm in information systems and computer applications. With the advancement of lattice theory, a technique known as the lattice-based method has emerged as a significant threat to RSA and its variants. This paper aims to conduct a bibliometric analysis of publications in the field of lattice-based attacks on RSA-type cryptosystems. The analysis is based on a dataset of relevant publications retrieved from Scopus and utilizes visualization tools such as CiteSpace and VOSviewer for a thorough overview. In order to understand the research developmental trajectory, we analyze the publication trends over the years, explore cooperation networks at various levels, including country/region, institution, and author, and assess the extent of collaboration, contribution, and productivity within the field. Additionally, author co-citation network and reference co-citation clustering are utilized to enable the identification of significant research achievements, cutting-edge developments, and structural framework. Furthermore, we conduct detailed analysis from a keyword perspective to identify research hotspots and emerging trends. The findings contribute to the existing body of knowledge on lattice-based cryptanalysis of RSA-type cryptosystems. Moreover, this bibliometric analysis serves as a valuable resource for identifying fruitful areas for further exploration and guides future research efforts.

Keywords Bibliometric analysis, Visualization, Cryptanalysis, Attack, RSA, Lattice

Introduction

The study of lattices traces its roots back to the eighteenth century, gaining computational significance in the early 1980s as a powerful tool for breaking cryptosystems (Lagarias and Odlyzko 1985). This historical evolution has tightly interwoven lattice theory with cryptology (Nguyen and Stern 2001). From a cryptographic design standpoint, the complexity of lattice hard problems becomes instrumental in creating public-key cryptographic schemes (Ajtai and Dwork 1997). Conversely, in cryptographic analysis, lattice reduction algorithms and the techniques for solving lattice hard problems serve as tools to assess the security of both lattice-based and classical public-key cryptographic algorithms (Joux and Stern 1998).

The RSA cryptosystem invented by Rivest et al. (1978), holds a prominent position in public-key encryption and digital signatures across diverse domains like information security, e-commerce, and finance. Its key generation chooses two large prime numbers p and q, calculates the modulus $N = pq$, randomly selects an integer e coprime to $\varphi(N)$, and calculates $d \equiv e^{-1} \bmod \varphi(N)$. The public and private key pairs are bundled as (N, e) and (p, q, d), respectively. One uses $c = m^e \bmod N$ to encrypt a plaintext m, and another uses $c^d \bmod N$ in decrypting the corresponding ciphertext. Two integers e and d are sometimes called the public and private exponents. Its security relies on the presumed computational infeasibility of the large integer factorization problem, with no absolutely effective attacks discovered to date. However,

*Correspondence:
Mengce Zheng
mczheng@zwu.edu.cn; mengce.zheng@gmail.com
[1] College of Information and Intelligence Engineering, Zhejiang Wanli University, Ningbo, China
[2] Advanced Cryptography and System Security Key Laboratory of Sichuan Province, Chengdu, China

under specific conditions or with additional information, efficient lattice-based attacks can break RSA within polynomial time complexity.

The pioneering work on lattice-based cryptanalysis of RSA-type cryptosystems was introduced by Coppersmith (1997). Coppersmith (1996b, 1996a) employed the LLL lattice reduction algorithm (Lenstra et al. 1982) to address modular and integer polynomial equations, ingeniously transforming attacks on the RSA cryptosystem into finding short vectors in some lattices. Effective in attack scenarios with small exponents or partial leakage of prime factors, this method has become integral to assessing RSA's security and enhancing RSA-type public-key algorithms.

Coppersmith (1997) originally developed this method for univariate/bivariate polynomial equations, and it can be generalized to handle multivariate cases. The similar core idea is to construct a lattice where each row encodes the coefficients of certain generated shift polynomials. After performing lattice reduction, a set of multivariate polynomials is obtained that share the desired root over the integers. These polynomials can be solved using Gröbner basis computation or resultant computation. This root will lead to the recovery of key information of RSA-type cryptosystems.

We informally overview the general strategy using lattice reduction to find small roots of multivariate polynomial equations. The lattice-based solving strategy involves the following stages.

1. *Polynomial Equation Derivation* One starts by deriving multivariate polynomial equation to be solved $f(x_1, \ldots, x_n)$ from target RSA-type cryptosystem. The corresponding roots $(x_1^\star, \ldots, x_n^\star)$ are closely related to its private key information.
2. *Shift Polynomial Generation* One generates a set of shift polynomials $g_i(x_1, \ldots, x_n)$ using the given multivariate polynomial and estimated upper bounds $X_1, \ldots, X_n$. These shift polynomials are designed to share a common root modulo a known modulus.
3. *Lattice Construction* The coefficient vectors of shift polynomials with upper bounds $g_i(X_1x_1, \ldots, X_nx_n)$ are converted into row vectors to form a lattice basis matrix. The LLL algorithm is then employed to reduce this lattice, producing the first few reduced vectors.
4. *Polynomial Transformation* These reduced vectors are transformed into integer polynomials $h_i(x_1, \ldots, x_n)$. For the system to be solvable, these polynomials must be algebraically independent.
5. *Root Extraction* If the integer polynomials are confirmed to be algebraically independent, one can solve the system using several trivial methods, thereby extracting the desired roots $(x_1^\star, \ldots, x_n^\star)$.

It is notable that this strategy is heuristic because there is no guarantee that the integer polynomials derived from lattice reduction will be algebraically independent. However, it is a common assumption in lattice-based attacks that these polynomials do exhibit algebraic independence, enabling the effective recovery of the common root.

After Coppersmith's seminal work, numerous lattice-based attacks on RSA-type cryptosystems have been investigated and presented. Hence, conducting a bibliometric analysis is crucial to understanding the field's development trends and research hotspots, especially for new researchers.

Bibliometric analysis, using statistical and analytical methods, explores quantity, quality, citation patterns, and more to understand the developmental trends, research hotspots, and academic influence in a particular research field. It quantifies various aspects such as country/region, institution, author, citation count, and keyword, providing researchers with an objective and comprehensive analysis while minimizing subjective bias. This approach allows for a revealing exploration of the developmental trajectory of a research area. Additionally, visualization tools like CiteSpace and VOSviewer can transform abstract data, such as collaborative relationships, knowledge structures, research hotspots, and emerging trends, into intuitive visual representations. These tools offer researchers a clearer understanding of the studied field. This paper utilizes bibliometric analysis and visualization techniques to comprehensively study the literature related to lattice-based cryptanalysis of RSA-type cryptosystems.

The structure of the paper is organized as follows. Section 2 introduces data acquisition process and visualization methods employed in this work. Section 3 presents the bibliometric analysis results in seven major aspects, including publication, country/region, institution, author collaboration network, author co-citation network, highly cited references, and reference co-citation clustering. These results summarize the development trends, collaboration relationships, and primary achievements. Section 4 reveals specific research hotspots and emerging trends through the analysis of keywords and related information. Section 5 offers a concluding summary and outlines potential future work. Unlike previous literature reviews (Boneh 1999; Mumtaz and Luo 2019), we vividly present research hotspots and emerging trends, aiding researchers in understanding the field's structural framework and providing valuable research directions.

Data acquisition and visualization methods

Data acquisition

To initiate our bibliometric analysis, we carefully choose a literature database. Scopus (https://www.scopus.com/), known for its authority and optimal trade-off, is our selected database. The two keywords "lattice" and "RSA" guide our literature search from 1996 to 2023. Moreover, we identify five influential papers, i.e., (Coppersmith 1996a, b, 1997; Howgrave-Graham 1997; Boneh and Durfee 2000) in lattice-based cryptanalysis of RSA-type cryptosystems. Extracting citations from these publications helps us gather unretrieved literature pertinent to our research target, and finally ensures the relevance of publications to our research objectives through rigorous manual inspection. This meticulous process results in a consolidated dataset of 400 relevant publications.

Visualization methods

Bibliometric analysis enables the quantification of information within literature datasets, with CiteSpace and VOSviewer providing visualizations of the derived results. Developed by Chen (2006), CiteSpace is a powerful tool for bibliometric analysis, creating visual knowledge maps like co-occurrence and cooperation network maps. We utilize CiteSpace to construct a reference co-citation clustering map, elucidating the knowledge structure and evolutionary trends in the field of lattice-based cryptanalysis of RSA-type cryptosystems.

VOSviewer developed by van Eck and Waltman (2010), is used to analyze and visualize keyword co-occurrence relationships, showcasing the structure of research hotspots. Because the keyword co-occurrence map made by VOSviewer lacks an integration of the time element, the burst detection function in CiteSpace complementarily reveal the emerging trends in the field of lattice-based cryptanalysis of RSA-type cryptosystems.

Results

Analysis of publication outputs

To gauge the field's development and knowledge accrual over time, examining the yearly publication count in lattice-based cryptanalysis of RSA-type cryptosystems is insightful. Figure 1 illustrates the annual publication count and corresponding cumulative results from 1996 to 2023.

The literature in this domain originated in 1996, marked by two pivotal contributions from Coppersmith. He introduced a method for solving small roots of a univariate modular polynomial equation (Coppersmith 1996b) and small roots of a bivariate integer polynomial equation (Coppersmith 1996a). Coppersmith's innovative idea connected the security analysis of RSA to the problem of finding approximately short lattice vectors. This transformation emphasized the significance of the lattice-based method in cryptographic attacks against RSA.

Following this inception, research in this field has burgeoned, with researchers increasingly focusing on it, though the overall output remained modest. The initial stage (1996–2006) witnessed an annual count of no more than 10 publications, averaging 7 publications yearly, totaling less than 80 papers, indicative of gradual growth. Since 2007, there has been a swift and peaked growth in literature, reaching its zenith in 2009 with 28 publications. The publication trend has been jagged since, averaging 19 publications annually, marking the development stage (2007-present). This stage reveals an accelerated

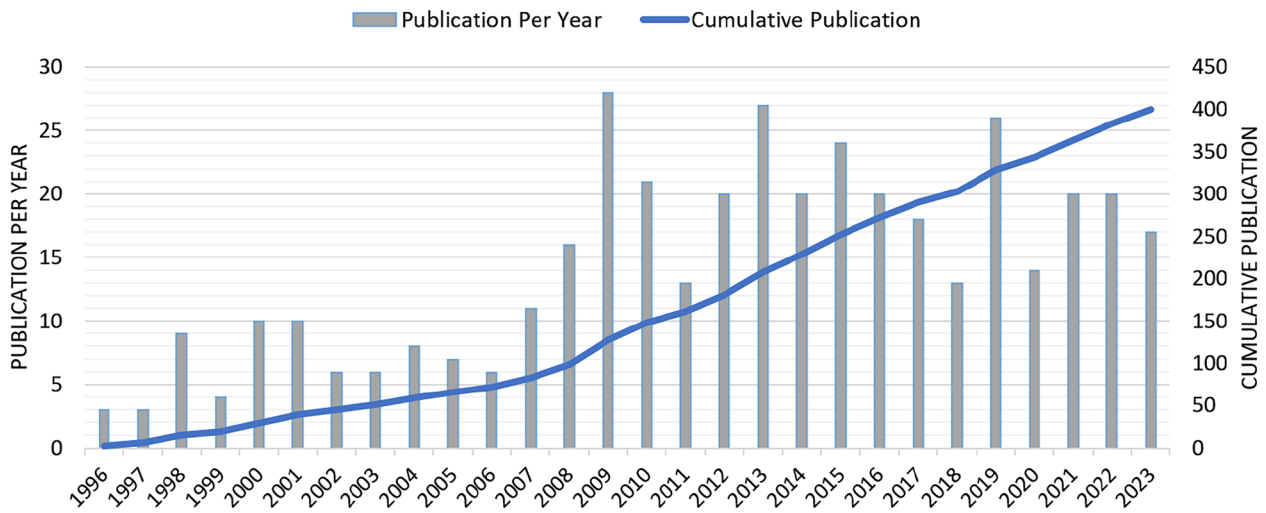


Fig. 1 The annual publication count and cumulative results in lattice-based cryptanalysis of RSA-type cryptosystems from 1996 to 2023

and heightened interest in lattice-based cryptanalysis of RSA-type cryptosystems, showcasing a considerable rise in overall annual publications compared to the initial stage.

Analysis of countries/regions and institutions

Analysis of country/region publication

The analysis of country/region publication is helpful to explore the spatial distribution in the field of lattice-based cryptanalysis of RSA-type cryptosystems. The collected dataset spans 39 countries/regions in terms of geographical distribution. We list the top 10 countries/regions based on publications in Table 1.

In Table 1, China ranks first with 102 publications (25.50%), followed by France (72 publications, 18.00%), Japan (56 publications, 14.90%) and the United States (51 publications, 12.75%). It is worth noting that although the total number of publications in the United States ranks fourth, the total number of citations (that is 2809) is far higher than that of other countries/regions. France (1243 citations) and Germany (1236 citations) also contribute significantly. Assessing TC and AC values, the United States, France, and Germany emerge as important contributors to the field's research.

Analysis of country/region cooperation

Visualizing the cooperation network map effectively illustrates the cooperation patterns among countries/regions. In Fig. 2a (Parameter settings: type of analysis: co-authorship; unit of analysis: countries/regions; as shown in counting method: full counting), colorful nodes represent countries/regions, with larger nodes indicating more publications. The lines between the nodes represent cooperative relationships between countries/regions, with China, France, and the United States being the most connected countries, reflecting the broader cooperation between them. Additionally, the width of the lines symbolizes the cooperation intensity between different countries/regions. To better illustrate the extent of cooperation, we adjust the threshold **Min.strength**, resulting in Fig. 2b. It is observed that China demonstrates high-intensity cooperation with countries like the United States and Japan. Similarly, it reveals high-intensity cooperation between France with countries like Malaysia and Australia. Moreover, there is more high-intensity cooperation between countries/regions in Europe and Asia, while there are fewer in the Americas. Therefore, strengthening cooperation across continents, particularly in the Americas, is recommended for advancing lattice-based cryptanalysis of RSA-type cryptosystems.

Table 1 Top 10 countries/regions based on publications

Rank	Country/region	Publications	Percent	TC	AC
1	China	102	25.50%	472	4.63
2	France	72	18.00%	1243	17.26
3	Japan	56	14.90%	414	7.39
4	The US	51	12.75%	2809	55.08
5	India	42	10.50%	385	9.17
6	Germany	33	8.25%	1236	37.46
7	Malaysia	26	6.50%	120	4.62
8	Australia	21	5.25%	260	12.38
9	Taiwan	13	3.25%	258	19.85
10	Canada	11	2.75%	383	34.82

TC the total citations of a country/region, *AC* the average citations per publication for a country/region

Analysis of institution cooperation

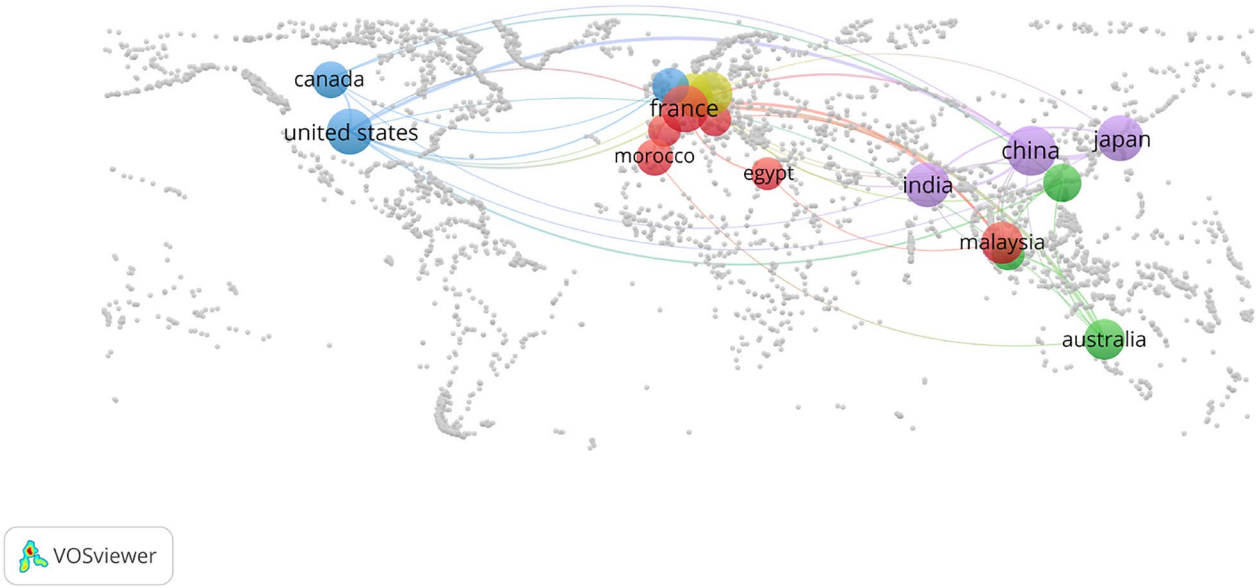
The top 10 institutions contributing to this field are listed in Table 2, which include the University of Tokyo (33 publications) and the Chinese Academy of Sciences (32 publications) having more than 30 publications. Among these, 5 institutions are located in China, reflecting the country's significant involvement in lattice-based cryptanalysis of RSA-type cryptosystems. The rest 5 institutions are located in Japan, Malaysia, France and India.

Figure 3 (Parameter settings: years per slice: 1; node type: institution) displays an institution cooperation network map, revealing a concentrated cooperation pattern.

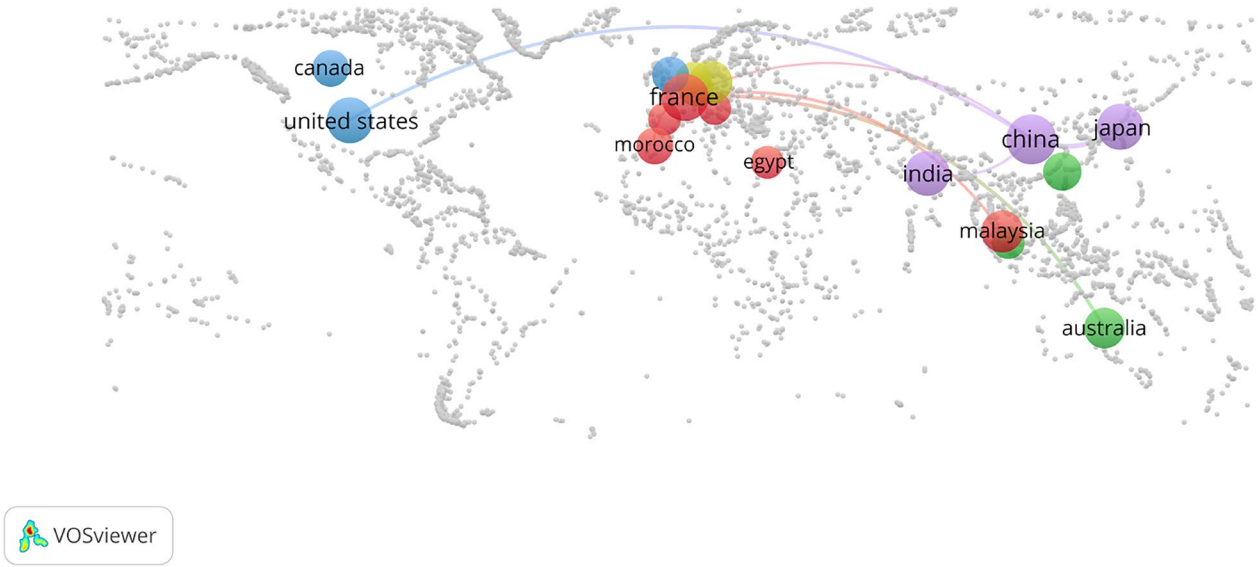
Through this institution cooperation network map, it is observed that the cooperation of institutions is relatively concentrated, indicating that a certain cooperative relationship has been formed between various institutions. Among them, the University of Tokyo (centrality 0.03), the Chinese Academy of Sciences (centrality 0.04), Université de Caen Normandie (centrality 0.03) and École Normale Supérieure (centrality 0.02) have higher centrality, indicating widespread cooperation and important roles in the institution cooperation network. These institutions play crucial roles in advancing lattice-based cryptanalysis of RSA-type cryptosystems.

Analysis of author collaboration and author co-citation

Analyzing authors in the literature provides insights into core research strengths and the degree of correlation among authors in this research field. Figure 4 (Parameter settings: years per slice: 1; node type: author; pruning: pathfinder, pruning sliced networks and pruning the merged network) illustrates the collaboration network of authors in this field. It is observed that the author nodes exhibit a local cluster phenomenon, indicating that certain authors prefer collaborating with specific peers. Table 3 shows the top 10 core authors and their affiliated institutions. Among them, Nitaj leads with 31



(a) Basic cooperation network map of countries/regions.



(b) High-intensity cooperation network map of countries/regions.

Fig. 2 The cooperation network maps of countries/regions in lattice-based cryptanalysis of RSA-type cryptosystems

publications, followed by Kunihiro (28 publications), Sarkar (27 publications) and May (21 publications).

Price (1963) suggesting half of publications on a topic stem from a group of highly productive authors (equaling to the square root of the total authors), guides the following analysis. According to Price's Law, the minimum number of core authors in a certain field is calculated as $m = 0.749 \times \sqrt{n_{\max}}$. Here, $n_{\max}$ is the number of publications by the most productive author, yielding $m = 0.749 \times \sqrt{31} \approx 4.17$. Therefore, authors with 4 or more papers are deemed core authors. In total, 61 core authors, contributing 275 publications (68.75% of the total), align with the 50% standard of Price's Law. This suggests the establishment of a relatively stable core

Table 2 Top 10 institutions based on publications

Rank	Institution	Publications	Centrality	Country/region
1	The University of Tokyo	33	0.03	Japan
2	Chinese Academy of Sciences	32	0.04	China
3	Universiti Putra Malaysia	24	0.01	Malaysia
4	Université de Caen Normandie	23	0.03	France
5	École Normale Supérieure	16	0.02	France
6	Tsinghua University	13	0.01	China
7	University of Chinese Academy of Sciences	13	0	China
8	Shandong University	12	0	China
9	Indian Statistical Institute	11	0	India
10	University of Science and Technology of China	10	0	China

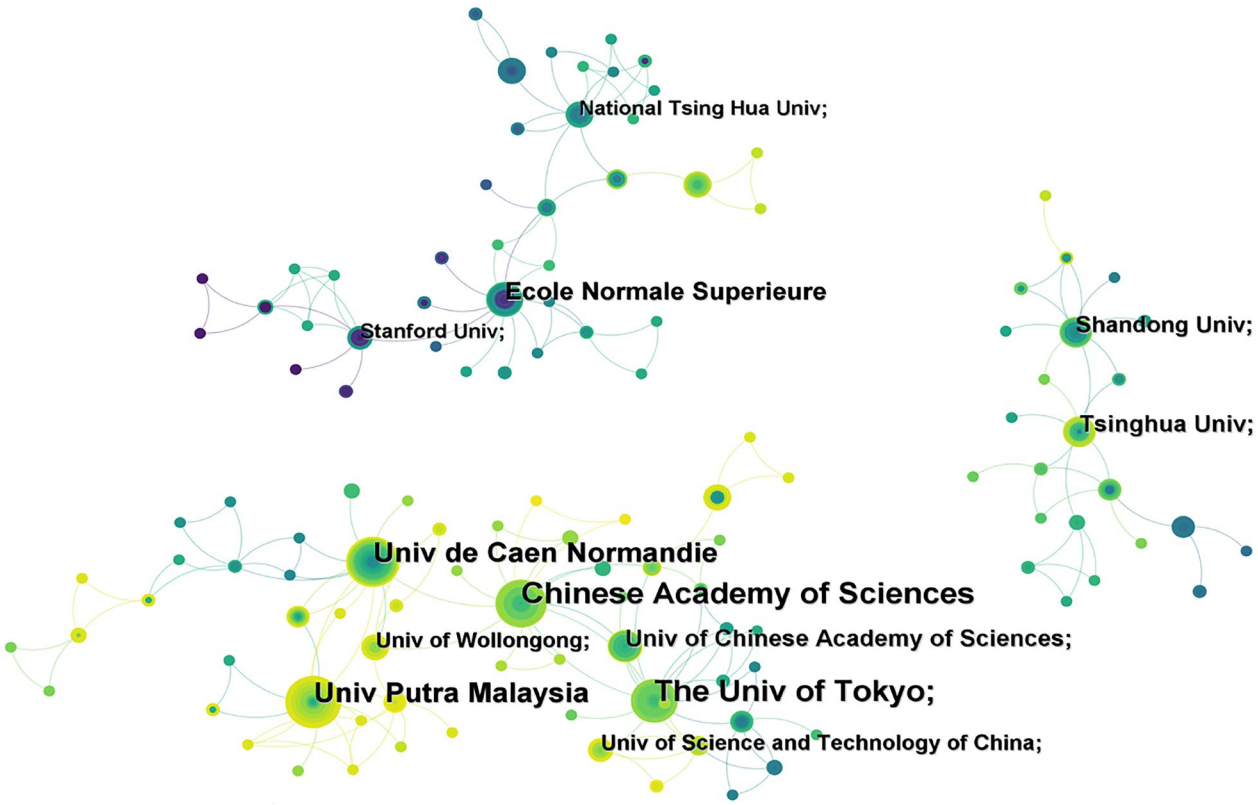


Fig. 3 The cooperation network map of institutions in lattice-based cryptanalysis of RSA-type cryptosystems

author group in lattice-based cryptanalysis of RSA-type cryptosystems.

White and Griffith (1981) extended the concept of co-citation proposed by Small (1973) to authors and proposed the concept of author co-citation analysis. This analysis identifies co-citation relationships when two or more authors are cited by one or more later publications simultaneously. Author co-citation analysis allows us to identify highly cited authors and understand the impactful research shaping this field. Figure 5 (Parameter settings: years per slice: 1; node type: cited author) presents the visualization map of author co-citation network. The purple outer ring indicates nodes with high centrality. Table 4 lists the top 10 co-cited authors and their highly cited references. Note that the highly cited references here are obtained by citation counts in our derived dataset, not citation counts in Scopus.

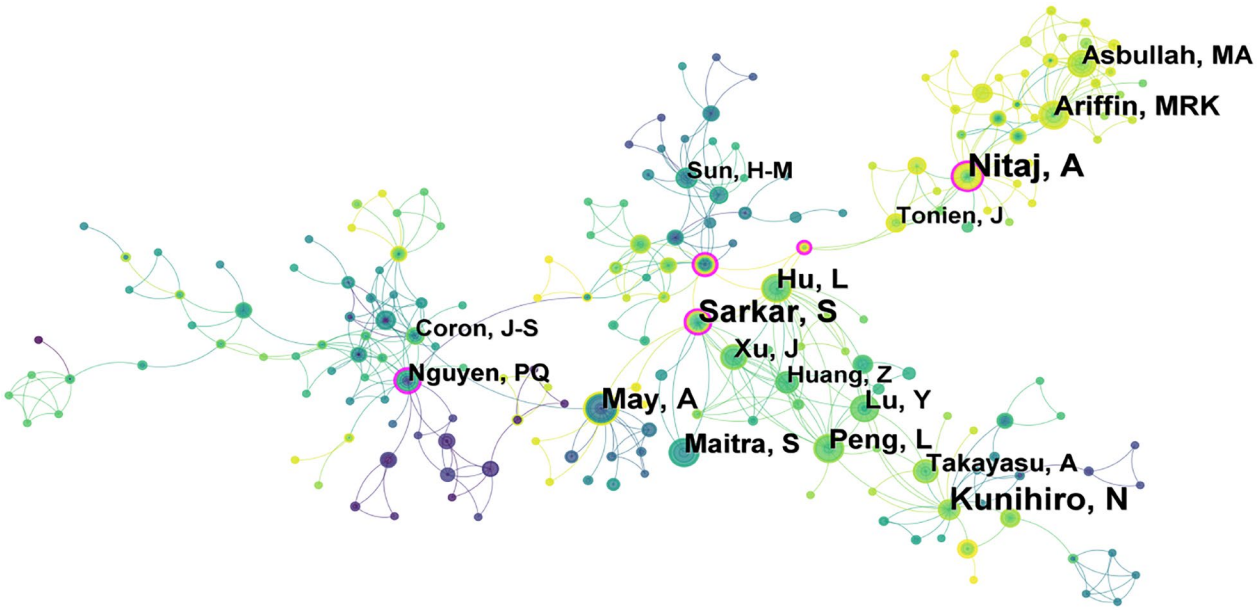


Fig. 4 The collaboration network map of authors in lattice-based cryptanalysis of RSA-type cryptosystems

Table 3 Top 10 core authors based on publications

Rank	Publications	Author	Institution	Country/region
1	31	Nitaj, Abderrahmane	Université de Caen	France
2	28	Kunihiro, Noboru	University of Tsukuba	Japan
3	27	Sarkar, Santanu	Indian Institute of Technology Madras	India
4	21	May, Alexander	Ruhr-University Bochum	Germany
5	18	Peng, Liqiang	Alibaba Group	China
6	18	Ariffin, Muhammad Rezal Kamel	Universiti Putra Malaysia	Malaysia
7	18	Hu, Lei	Chinese Academy of Sciences	China
8	16	Maitra, Subhamoy	Indian Statistical Institute	India
9	15	Xu, Jun	Chinese Academy of Sciences	China
10	14	Lu, Yao	The University of Tokyo	China

Institution: the latest institutions corresponding to relevant authors are listed

Coppersmith stands out as the most co-cited author, renowned for his groundbreaking work of solving small roots of univariate modular and bivariate integer polynomial equations (Coppersmith 1996b, a). His extensively cited reference (Coppersmith 1997) is an extended and improved version of the above work. It is worth mentioning that the LLL lattice reduction algorithm (Lenstra et al. 1982) adopted by Coppersmith was initially proposed by Lenstra et al., who holds the fourth position in Table 4. This algorithm marks the inception of polynomial-time solutions for the approximate shortest vector problem.

Subsequent advancements by Howgrave-Graham (1997) and Coron (2004) refined Coppersmith's original method for solving small roots of polynomial equations. May (2003) further extended it to address multivariate polynomial equations. Later, Jochemsz and May (2006) proposed a comprehensive strategy for extracting small solutions to modular and integer polynomial equations, introducing the so-called "basic strategy" and "extended strategy". Note that the mentioned method for solving multivariate polynomial equations is based on an empirical assumption that the reduced basis vectors of the LLL algorithm are algebraically independent. In general, this type of analysis improved by Howgrave-Graham, Coron and Jochemsz and May for Coppersmith's original method is collectively referred to as the lattice-based method. Surprisingly, the literature related to the lattice-based method is commonly associated with highly

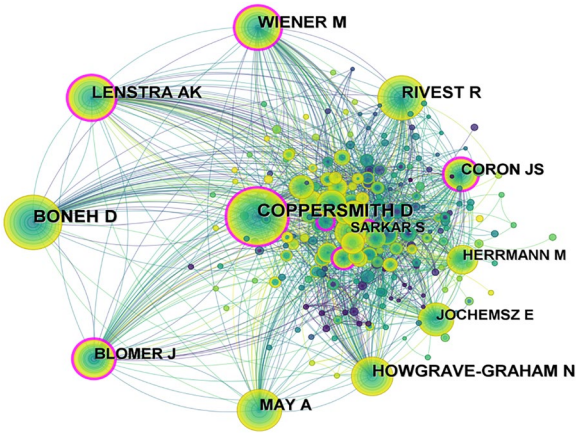


Fig. 5 The co-citation network map of authors in lattice-based cryptanalysis of RSA-type cryptosystems

co-cited authors like Coppersmith, Howgrave-Graham, Coron, Jochemsz and May.

Additionally, Rivest et al. (1978), positioned third in Table 4, are the inventors of the RSA cryptosystem. Under certain conditions, cryptanalysis of RSA-type cryptosystems can be transformed into the problem of finding small roots of polynomial equations. Accordingly, the lattice-based method efficiently solve this problem, resulting in small public exponent attack (Coppersmith 1996b), small private exponent attack (Boneh and Durfee 2000), partial key exposure attack (Blömer and May 2003) and so on. Among them, Boneh and Durfee (2000), the second-ranked in Table 4, increased the small private exponent attack boundary from Wiener's continued fraction-based attack $d < \frac{1}{3}N^{0.25}$ (Wiener 1990) to an improved result $d < N^{0.292}$. This remains the optimal attack bound to date, underscoring the pioneering role in the realm of lattice-based cryptanalysis of RSA-type cryptosystems.

Analysis of cited references

In bibliometrics, delving into the citation frequency and co-citation network of relevant literature offers an insightful exploration of the field's vital knowledge foundation and correlation degrees. While these methods proficiently uncover essential connections, they fall short in revealing the research frontiers and knowledge structure of the field. Price (1965) asserted in "Networks of Scientific Papers" that "the pattern of bibliographic references indicates the nature of the scientific research front," signifying the flow of the existing knowledge base towards the forefront of research.

Building on the above principle, on the basis of reference co-citation analysis, this paper uses CiteSpace to cluster the co-citation network map, so as to show the process of mapping the knowledge base of lattice-based cryptanalysis of RSA-type cryptosystems towards the research frontier, which can help scholars understand the research frontier and the overall structure of the field. The reference co-citation clustering map generated by CiteSpace is depicted in Fig. 6 (Parameter settings: years per slice: 4; node type: reference; pruning: pathfinder, pruning sliced networks and pruning the merged network). The modularity $= 0.742 > 0.3$, and

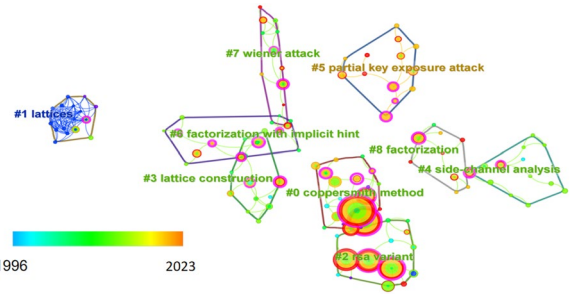


Fig. 6 The reference co-citation clustering map of publications in lattice-based cryptanalysis based on RSA-type cryptosystems

Table 4 Top 10 co-cited authors and their highly cited references

Rank	Frequency	Centrality	Author	Highly Cited Reference
1	349	0.14	Coppersmith, Don	Small solutions to polynomial equations, and low exponent RSA vulnerabilities
2	296	0.05	Boneh, Dan	Cryptanalysis of RSA with private key d less than $N^{0.292}$
3	233	0.08	Rivest, Ronald L	A method for obtaining digital signatures and public-key cryptosystems
4	230	0.18	Lenstra, Arjen K	Factoring polynomials with rational coefficients
5	201	0.07	Howgrave-Graham, Nicholas	Finding small roots of univariate modular equations revisited
6	195	0.12	Wiener, Michael J	Cryptanalysis of short RSA secret exponents
7	183	0.04	May, Alexander	New RSA vulnerabilities using lattice reduction methods
8	143	0.10	Blomer, Johannes	New partial key exposure attacks on RSA
9	118	0.12	Coron, Jean-Sébastien	Finding small roots of bivariate integer polynomial equations Revisited
10	108	0.06	Jochemsz, Ellen	A strategy for finding roots of multivariate polynomials with new applications in attacking RSA variants

a mean silhouette $= 0.959 > 0.5$, indicating that the structure is clear, and the clustering is well-founded.

In Fig. 6, each node symbolizes a reference, with its size indicative of the citation frequency. The color of the annual ring within the node signifies the time of citation, while the connections between nodes denote co-citation relationships. The connection color corresponds to the time it takes for a co-citation relationship to form. The presence of a purple outer ring designates high centrality, indicating a pivotal connecting role within the neighboring nodes. The reference co-citation clustering map reveals 9 clusters, which are sorted according to the number of nodes in each cluster. Clustering labels are extracted from the citing articles of nodes, which can represent the research frontier of this topic to a certain extent.

To enhance precision, we extensively refine and rename cluster labels from the title, keywords, and abstract of citing articles, as extracted by CiteSpace. The clustering map utilizes colors to delineate distinct time periods, facilitating a clearer depiction of the evolution of the research frontier in lattice-based cryptanalysis of RSA-type cryptosystems since 1996. Table 5 presents comprehensive information for each cluster.

Table 6 provides a list of the top 10 cited references. We next discuss each clustering in detail in chronological order.

Cluster 1, labeled "lattices," encompasses the discrete geometric structure of lattices, proving their broad utility in both cryptographic design and cryptanalysis. The unique geometric nature of lattices renders many lattice problems NP-hard, paving the way for the development of lattice-based cryptosystems with resistance against quantum attacks. The exploration of lattice hard problems and their complexities has led to breakthroughs in solving these challenges. The seminal LLL lattice reduction algorithm, introduced by Lenstra et al. (1982), stands as the most famous algorithm for approximating shortest lattice vectors.

The LLL lattice reduction algorithm has significantly contributed to advancing the security analysis of lattice-based and classical public key cryptographic algorithms. It serves as an important tool in lattice-based cryptanalysis, transforming the task of attacking public key cryptosystems into finding short lattice vectors. The fundamental concept involves leveraging the algebraic relationship between the public/private keys, along with given system parameters, to formulate lattice reduction problems. Algorithms like LLL or BKZ (Chen and Nguyen 2011) are then employed to solve these problems, offering widespread applications in cryptanalysis.

Cluster 0, identified as "Coppersmith method," is the primary approach in lattice-based cryptanalysis of RSA-type cryptosystems. This method broadly encompasses techniques for solving problems related to finding small solutions to modular/integer polynomial equations through lattice reduction algorithms.

The Coppersmith method involves deriving the modular or integer polynomial equations from the algebraic relationships inherent in RSA and its variants. By arranging the coefficient vectors appropriately and mapping them to a lattice basis matrix, the subsequent application of lattice reduction algorithms like LLL facilitates the extraction of short vectors in the lattice. If the output vectors are sufficiently short, the small roots of the corresponding equations can be efficiently solved using trivial methods such as resultant computation or Gröbner basis computation (Becker et al. 1993).

It is noteworthy that the term "Coppersmith method" always refers to an improved version, refined by Howgrave-Graham and others such as Howgrave-Graham (1997), Coron (2004), Blömer and May (2005), Jochemsz and May (2006), Coron (2007), Lu et al. (2015). Therefore, we use the term "lattice-based method" instead in this paper. Particularly in solving multivariate polynomial

Table 5 Reference co-citation clustering labels in lattice-based cryptanalysis of RSA-type cryptosystems

Cluster ID	Label	Size	Silhouette	Representative publications
0	Coppersmith method	21	0.960	Coppersmith (1997), Howgrave-Graham (1997), Jochemsz and May (2006)
1	Lattices	18	0.998	Stern (1998), Nguyen and Stern (2000, 2001)
2	RSA variant	14	0.918	Quisquater and Couvreur (1982), Collins et al. (1998), Takagi (1998)
3	Lattice construction	13	0.989	Aono (2009), Takayasu and Kunihiro (2014a), Lu et al. (2015)
4	Side-channel analysis	13	0.984	Sarkar and Maitra (2012), Kunihiro et al. (2014), Nemec et al. (2017)
5	Partial key exposure attack	13	0.932	Takayasu and Kunihiro (2014c, 2016, 2017)
6	Factorization with implicit hint	12	0.879	Sarkar and Maitra (2011), Peng et al. (2014), Lu et al. (2015)
7	Wiener attack	12	1.000	Blömer and May (2004), Nitaj (2008, 2009)
8	Factorization	9	0.952	May (2010), Nitaj and Rachidi (2015), Zheng et al. (2017)

Table 6 Top 10 cited references in reference co-citation clustering map

Rank	Frequency	Centrality	Title	Author	Year	Source
1	258	0.26	Small solutions to polynomial equations, and low exponent RSA vulnerabilities	Coppersmith, Don	1997	Journal of Cryptology
2	202	0.25	Factoring polynomials with rational coefficients	Lenstra, Arjen K	1982	Mathematische Annalen
3	149	0.20	Cryptanalysis of RSA with private key d less than $N^{0.292}$	Boneh, Dan	2000	IEEE Transactions on Information Theory
4	141	0.15	Cryptanalysis of short RSA secret exponents	Wiener, Michael J	1990	IEEE Transactions on Information Theory
5	139	0.09	A method for obtaining digital signatures and public-key cryptosystems	Rivest, Ronald L	1978	Communications of the ACM
6	96	0.18	Finding small roots of univariate modular equations revisited	Howgrave-Graham, Nicholas	1997	IMA International Conference on Cryptography and Coding 1997
7	63	0	New RSA vulnerabilities using lattice reduction methods	May, Alexander	2003	Doctoral Dissertation
8	47	0.23	Finding a small root of a bivariate integer equation; factoring with high bits known	Coppersmith, Don	1996	EUROCRYPT '96
9	47	0.05	Twenty years of attacks on the RSA cryptosystem	Boneh, Dan	1999	Notice of the AMS
10	45	0.03	A strategy for finding roots of multivariate polynomials with new applications in attacking RSA variants	Jochemsz, Ellen	2006	ASIACRYPT 2006

equations, ensuring the algebraic independence of the short vectors produced by the LLL algorithm poses a challenge. The lattice-based method often assumes this independence, making multivariate lattice-based cryptanalysis an empirical approach, necessitating validation through practical experimentation.

Cluster 7, identified as "Wiener attack," focuses on Wiener's continued fraction-based attack (Wiener 1990) and subsequent related work. This attack type aims to attack RSA and its variants using small private keys. Wiener asserted that if the private key $d < \frac{1}{3}N^{0.25}$, it becomes feasible to factor the modulus N in polynomial time, thereby compromising the RSA cryptosystem. Wiener's continued fraction-based method was extended to more attack scenarios like (Nitaj 2008; Nassr et al. 2022). Furthermore, Howgrave-Graham and Seifert (1999) combined Coppersmith method with Wiener attack, which resulted in a new attack on RSA. This entails small private key attack in scenarios where n many key pairs share the same RSA modulus N and Takayasu and Kunihiro (2014b) achieved an improved result. Moreover, such combined idea of Coppersmith method with Wiener attack has been used in (Blömer and May 2004; Bunder et al. 2017).

Cluster 2, labeled "RSA variants," explores modifications to the standard RSA cryptosystem to enhance efficiency while maintaining security. Typically, RSA operations involving modular operations are time-consuming, directly linked to the bit lengths of the public and private exponents, e and d. Opting for smaller exponents can boost efficiency but compromises security. To address this trade-off and optimize RSA performance for different applications, various RSA-type cryptosystems have been developed.

One such scheme, CRT-RSA, proposed by Quisquater and Couvreur (1982), leverages the Chinese remainder theorem during decryption or signature phases to reduce modulus size, thus improving operational efficiency. Another variant, Multi-Prime RSA (Collins et al. 1998), represents $N = p_1 p_2 \dots p_r$ in modulus form. Unlike standard RSA, it features smaller prime factors during key generation, enhancing the efficiency of prime number selection. Additionally, specialized arithmetic operations like those involving elliptic curves (Koyama et al. 1991), Gaussian domains (Elkamchouchi et al. 2002), and cubic fields (Murru and Saettone 2017) offer alternative avenues for designing RSA-type cryptosystems.

Cluster 3, identified as "lattice construction," holds core significance in lattice-based cryptanalysis. The keypoint of the lattice-based method lies in ingenious lattice constructions, matured over time to improve the upper bounds of solvable small roots and minimize attack conditions necessary for cryptanalysis. The focus

of subsequent work has shifted to constructing a lattice basis with better properties. Jochemsz and May (2006) offered a generic and concise strategy for constructing full-rank lattices.

However, when dealing with polynomial equations possessing special algebraic relations, the generic strategy may not be able to make full use of the special algebraic structure of polynomials, and thus cannot achieve the optimal attack performance. Consequently, most of the existing lattice-based cryptanalysis of RSA-type cryptosystems is not based on Jochemsz-May strategy. Such cryptanalysis target the specific algebraic structures of distinct cryptosystems, utilizing specialized lattice construction techniques to enhance the effectiveness of attacks.

Durfee and Nguyen (2000) introduced the variable substitution technique for analyzing RSA with unbalanced prime factors p and q. This technique introduces a new variable by scrutinizing the algebraic relationship between unknown variables, resulting in a more efficient lattice basis construction. Herrmann and May (2009) introduced the unravelled linearization technique, simplifying lattice construction and enhancing lattice-based cryptanalysis by digging implicit algebraic relations in unknown variables.

In order to address the imbalance in the upper bounds of small roots in multivariate polynomial equations, Takayasu and Kunihiro (2014a) proposed the equalization technique. This technique links lattice construction with the upper bounds of unknown variables, optimizing the lattice basis construction. Lu et al. (2015) proposed the exponential optimization technique for solving linear modular equations. Leveraging the special exponential structure of known modulus, this technique refines lattice construction, which is applied in lattice-based cryptanalysis of Prime Power RSA (Takagi 1998) and Common Prime RSA (Hinek 2006).

Recognizing that direct lattice reduction may not always yield desired results, Peng et al. (2015) proposed a two-step reduction technique. This technique divides the original lattice-based cryptanalysis into two stages. Firstly constructing a lower-dimensional lattice and utilizing lattice reduction to express the target variable as a linear combination of smaller variables. Subsequently, the algebraic relationship is further employed to construct a new polynomial equation, leading to improved attack results. This technique finds applications in cryptanalysis of Dual RSA (Sun et al. 2007) and cryptanalysis of RSA with implicitly related keys (Zheng et al. 2020).

Cluster 4, identified as "side-channel analysis," involves an attack method capable of extracting confidential information from cryptographic devices. Distinguishing itself from other attack techniques, this method does not exploit theoretical vulnerabilities in the cryptosystem but leverages the side channel information of systems running on the physical device. The so-called side channel information includes aspects like time information, energy consumption, electromagnetic leakage, and more.

In the context of lattice-based cryptanalysis of RSA-type cryptosystems, side-channel analysis like fault attack (Coron et al. 2009), timing attack (Kocher 1996), or differential power analysis (Kocher et al. 1999) can result in the partial leakage of prime factor bits or private key information. This facilitates the use of lattice-based cryptanalysis to compromise RSA and its variants. Hence, in specific scenarios, the combined threat of side-channel analysis and lattice-based cryptanalysis poses a significant risk to the security of RSA and its variants (Ma et al. 2020; Ueno and Homma 2023).

Cluster 8, identified as "factorization," focuses on a direct attack idea against RSA. If an attacker successfully factors the modulus $N = pq$, then the private exponent d can be calculated by the extended Euclidean algorithm according to the public exponent e, and hence cracks the RSA cryptosystem. The well-known number field sieve algorithm (Lenstra Jr et al. 1990) is state-of-the-art factorization approach, characterized by sub-exponential time complexity.

Beyond general factorization, the RSA modulus N can be factored in polynomial time when partial bits of the prime factors p and/or q are known. Rivest and Shamir (1985) successfully factored N with $\frac{2}{3}$ continuous bits of prime factor p. Coppersmith (1996a) later demonstrated that a $\frac{1}{2}$ fraction is sufficient to effectively factor N. However, the above attacks often require continuous leakage, which contrasts with the discrete bits obtained through practical side channel information. Herrmann and May (2008) addressed the attack scenario with given discrete leakage of one prime factor p, achieving factorization with approximately $\ln 2 \approx 70\%$ random bits of p. But the time complexity of the algorithm is exponentially in the number of unknown bit blocks.

Prime-Power RSA proposed by Takagi (1998), is a variant of RSA using modular form $N = p^r q$, $r \geq 2$. Boneh et al. (1999) provided lattice-based cryptanalysis for this variant and showed that N can be factored in polynomial time when given $\frac{1}{r+1}$ partial bits of p. Lu et al. (2013) extended it to the case of more unknown bit blocks, utilizing Herrmann-May's approach. Exploiting the special exponential structure of Prime Power RSA, Lu et al. (2015) further achieve the same results as Boneh et al. (1999) with a lower-dimensional lattice and higher efficiency. Lim et al. (2000) extended the modulus of Prime Power RSA to $N = p^r q^s$ and analyzed its factorization. Lu et al. (2017) further presented factoring attack under the leakage scenario of more unknown bit blocks. Later,

more improved factoring attacks (Wang et al. 2019; Zheng et al. 2023) have been studied.

Cluster 6, identified as "factorization with implicit hint," involves two ℓ-bit RSA moduli, $N_1 = p_1q_1$ and $N_2 = p_2q_2$. Specially, q_1 and q_2 are of $\alpha\ell$ bit-length, and the common bits shared by p_1 and p_2 are $t\ell$. The goal is to find the solvable condition on t and α that enables the efficient factorization of RSA moduli. This attack type was initially introduced by May and Ritzenhofen (2009). Recent known optimal results were presented by Lu et al. (2015) using the variable substitution technique. They pointed out that successful implicit factorization of two RSA moduli is achievable when $t > 2\alpha - 2\alpha^2$. Further improvements on the generalized implicit factorization problem were presented in (Wang et al. 2021; Feng et al. 2023) and cryptanalysis of RSA with implicitly related keys was studied by Zheng et al. (2020).

Cluster 5, identified as "partial key exposure attack," focuses on factorization of the modulus N or recovery of entire private key d given knowledge of partial exposure of private key or prime factors. Boneh et al. (1998) introduced this attack type, highlighting that in the most significant bits (MSBs) leakage scenario, if e is less than $N^{0.5}$ and partial MSBs of d is known, d can be recovered in polynomial time. In the least significant bits (LSBs) leakage scenario, with a small e, RSA can be broken when $\frac{\log_2 N}{4}$ bits of d is leaked. Takayasu and Kunihiro (2014c) provided improved attack results for MSBs/LSBs leakage scenarios using elaborate lattice construction techniques.

Beyond solely considering MSBs or LSBs leakage, Ernst et al. (2005) proposed lattice-based attacks in scenarios where both MSBs and LSBs are leaked. Besides, Sarkar (2011) studied cases with more unknown discrete bit blocks of d, revealing that a higher number of unknown bit blocks results in a less effective attack. Suzuki et al. (2020) further extended Takayasu-Kunihiro's attack to scenarios where both MSBs and LSBs are leaked simultaneously.

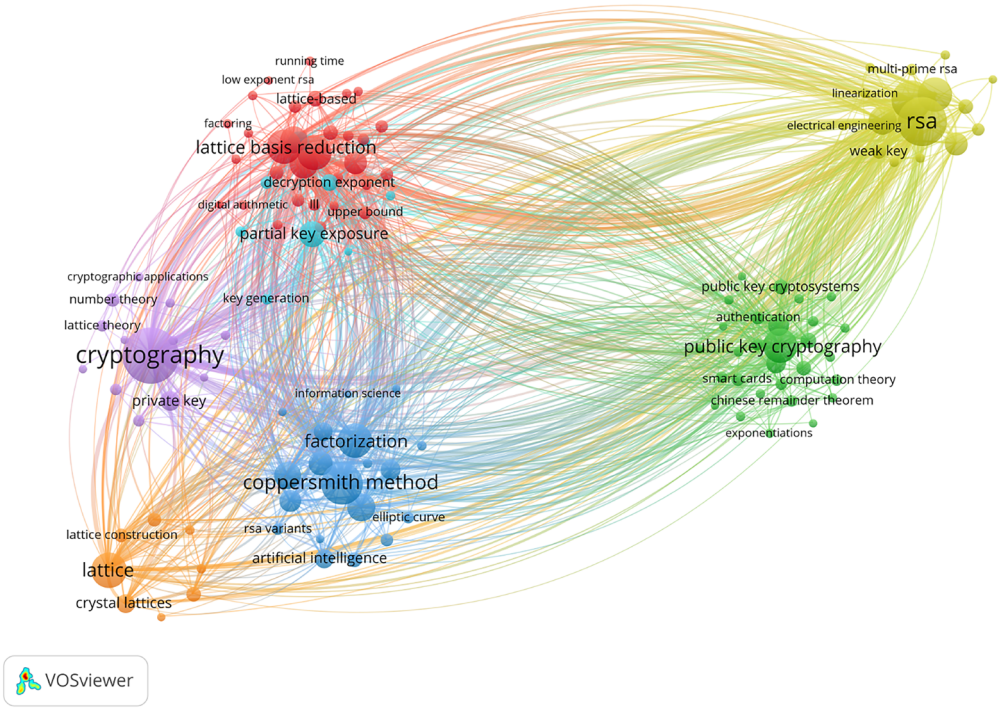
The partial key exposure attack is extensively investigated in lattice-based cryptanalysis of RSA variants like CRT-RSA and Common Prime RSA. Blömer and May (2003) proposed partial key exposure attack on CRT-RSA. The more effective partial key exposure attack was given by Takayasu and Kunihiro (2015). Recently, partial key exposure attack on CRT-RSA with small public exponent was studied by May et al. (2022) and Zhou et al. (2022) investigated extended partial key exposure attack on CRT-RSA with additive exponent blinding. Additionally, Zheng (2023) proposed partial key exposure attack on Common Prime RSA.

Hot research topics and emerging trends

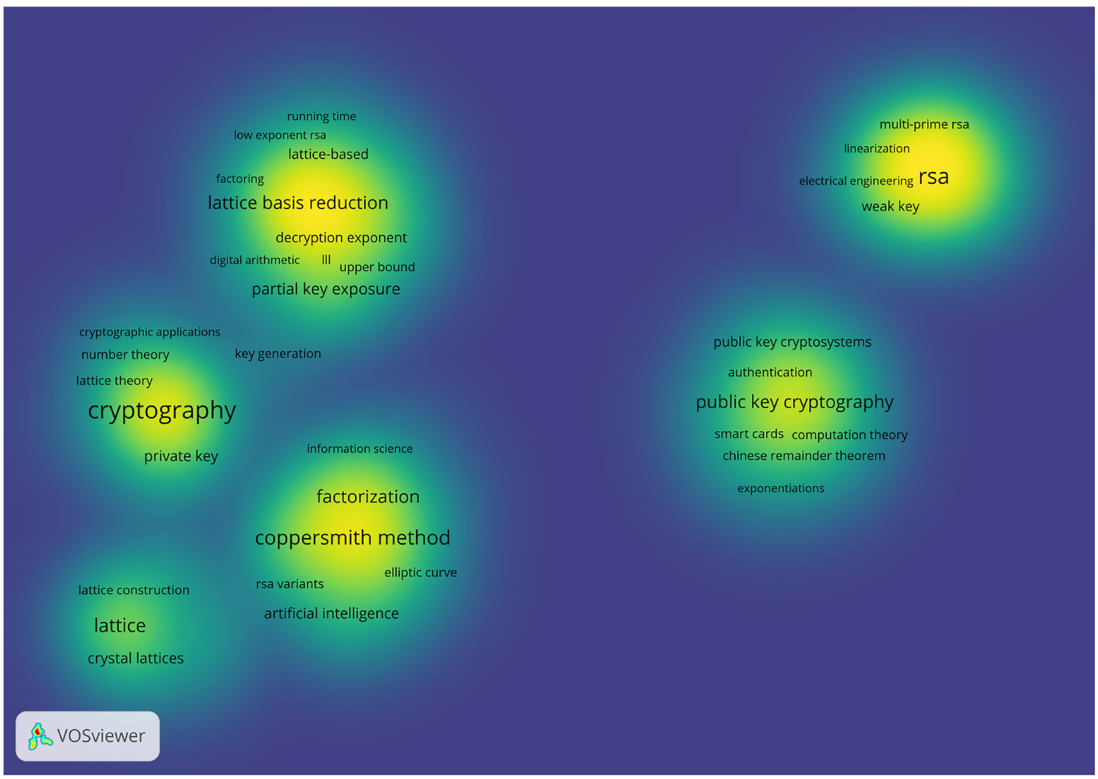
By scrutinizing the literature keywords within our dataset, we gain insights into the main topics and current research hotspots in lattice-based cryptanalysis of RSA-type cryptosystems. To facilitate this understanding, we utilize VOSviewer to construct a keyword co-occurrence network map, illustrated in Fig. 7. In Fig. 7a, distinct colors signify separate clusters, with larger nodes indicating higher occurrence frequencies. Figure 7b (Parameter settings: type of analysis: co-occurrence; unit of analysis: all keywords; counting method: full counting) employs brightness to denote varying occurrence frequencies. The high-frequency keywords for each cluster are detailed in Table 7, offering a glimpse into the prevalent research hotspots in this field.

Within the primary clusters, "cryptography", "lattice basis reduction", "RSA", "latice", and "Coppersmith method" exhibit the highest frequencies. However, gauging hot topics solely based on keyword frequencies falls short of capturing emerging trends in the academic realm. To address this, we employ the burst detection function of CiteSpace to scrutinize keywords, unveiling bursty topics within specific timeframes. In addition to the keyword time evolution map illustrated in Fig. 8 using VOSviewer, we reveal emerging trends in lattice-based cryptanalysis of RSA-type cryptosystems by incorporating the temporal dimension in Fig. 9 (Parameter settings: years per slice: 4; node type: keyword; pruning: pathfinder, pruning sliced networks and pruning the merged network.). To be specific, the top 20 keywords, distinguished by burst strength as detected by CiteSpace, are depicted. The blue segments denote the time intervals, with the red segments indicating burst periods.

We categorize three periods based on the various burst timeframes of the literature keywords, i.e., **Begin** and **End** in Fig. 9. In the beginning stage (1996–2007), keywords displaying the highest burst strength include "polynomials", "cryptography", "low exponent RSA", and "algorithms". These keywords are tied to early cryptographic attacks employing lattice reduction algorithms, particularly targeting low exponent RSA. Transitioning to the intermediate stage (2008–2015), keywords like "RSA", "weak key", "upper bound", and "RSA moduli" emerge with the highest burst strength. This phase aligns with subsequent efforts delving into weak keys within RSA implementations and maximizing upper bounds on vulnerable weak keys. In the current stage (2016–2023), keywords such as "Coppersmith method", "RSA cryptosystems", "RSA variants" and "lattice construction" exhibit notable burst strength. This signifies recent advancements exploring more attacks on RSA-type cryptosystems using the lattice-based method, coupled with improvements in lattice construction to enhance attack



(a) The network visualization map based on publication weights.



(b) The density visualization map based on publication weights.

Fig. 7 The keyword co-occurrence network map in lattice-based cryptanalysis of RSA-type cryptosystems

Table 7 High-frequency keywords for distinct cluster in keyword co-occurrence network map

Cluster ID	High-Frequency Keywords	Legend	Size
1	Lattice basis reduction, polynomial approximation, algorithms, polynomials		31
2	Public key cryptography, network security, side channel attack, public keys, authentication		29
3	Coppersmith method, factorization, rsa cryptosystems, rsa moduli, least significant bits, computer science		19
4	RSA, cryptanalysis, security of data, lll algorithm, continued fraction		16
5	Cryptography, private key, number theory, cryptanalyse, lattice attacks, lattice theory		13
6	Partial key exposure, most significant bit, decryption exponent, computational methods		9
7	Lattice, lattices, crt-rsa, lattice construction, polynomial-time algorithms		8

efficiency. It is worth noting that the latest cryptanalysis such as (Zheng et al. 2021; Shi et al. 2022; Nitaj et al. 2022) is centered around the RSA variant using Pell equation (Murru and Saettone 2017).

Moreover, we analyze the regional and institutional distribution of research activity related to the top 20 keywords listed in Fig. 9. We identify the regions that are most active in research related to the top 20 keywords in Table 8. This analysis highlights the regions where leading research in lattice-based cryptanalysis of RSA-type cryptosystems is concentrated. We also pinpoint the core institutions leading research in each of the top 20 keyword areas in Table 9, which include universities or research centers.

For new researchers entering the field of lattice-based cryptanalysis of RSA-type cryptosystems, selecting the suitable region and institution is essential. China, France, India, and Japan stand out for their leadership in cryptographic research, making it ideal for foundational studies and networking. Australia, Germany, UK, and USA combine academic rigor with industry collaboration, which is perfect for those interested in applied research. Emerging regions like Malaysia offer growing research opportunities, making them suitable for researchers looking to establish themselves in less saturated areas.

When choosing a suitable institution, it is important to align the research interests with the strengths of the institution. Chinese Academy of Sciences, École Normale Supérieure, and University of Tokyo specialize in deep theoretical exploration and algorithmic optimization, making it a great choice for those interested in foundational research. University College London and University of Paderborn focus on practical implementations, bridging the gap between theory and real-world applications. Université de Caen, University of Tokyo, and University of Wollongong are known for their generalization research, integrating cryptanalysis with extended RSA variants and generalized methods. Moreover, Chinese Academy of Sciences and Université de Caen provide excellent opportunities for international collaboration, making it ideal for those seeking a global perspective.

Conclusion and future work

We employ a bibliometric analysis, utilizing visualization tools CiteSpace and VOSviewer, to explore 400 publications related to lattice-based cryptanalysis of RSA-type cryptosystems from the Scopus database. The paper delivers a comprehensive review of the field's evolution over the past two decades.

The bibliometric analysis reveals the field's origins in 1996, with substantial growth from 2007 onward. Although annual publication trends exhibit fluctuations, the overall growth rate remains faster than before. The analysis of cooperation at the country/region and institution levels indicates that China is the leading producer, with significant publication outputs. Among the top 10 prolific institutions, half of them are Chinese. Despite China's dominance, the United States, France, and Germany hold significant influence in this field. Notably, the University of Tokyo, Chinese Academy of Sciences, Université de Caen Normandie, and École Normale Supérieure play pivotal roles in fostering inter-institutional cooperation.

The analysis of author reveals a stable core research force, with certain authors displaying a preference for collaborations with specific peers. Coppersmith emerges as the most frequently co-cited author, underscoring the pioneering role of his work in lattice-based cryptanalysis of RSA-type cryptosystems. Subsequently, Howgrave-Graham, Boneh, Coron, and May make further improvements to Coppersmith's foundation, advancing this research field.

Reference co-citation clustering outlines the progress in "Coppersmith method", "lattices", "RSA variant", "lattice construction", "side-channel analysis", "partial key exposure attack", "factorization with implicit hint", "Wiener attack" and "factorization". This succinctly captures the evolving trends and knowledge structure

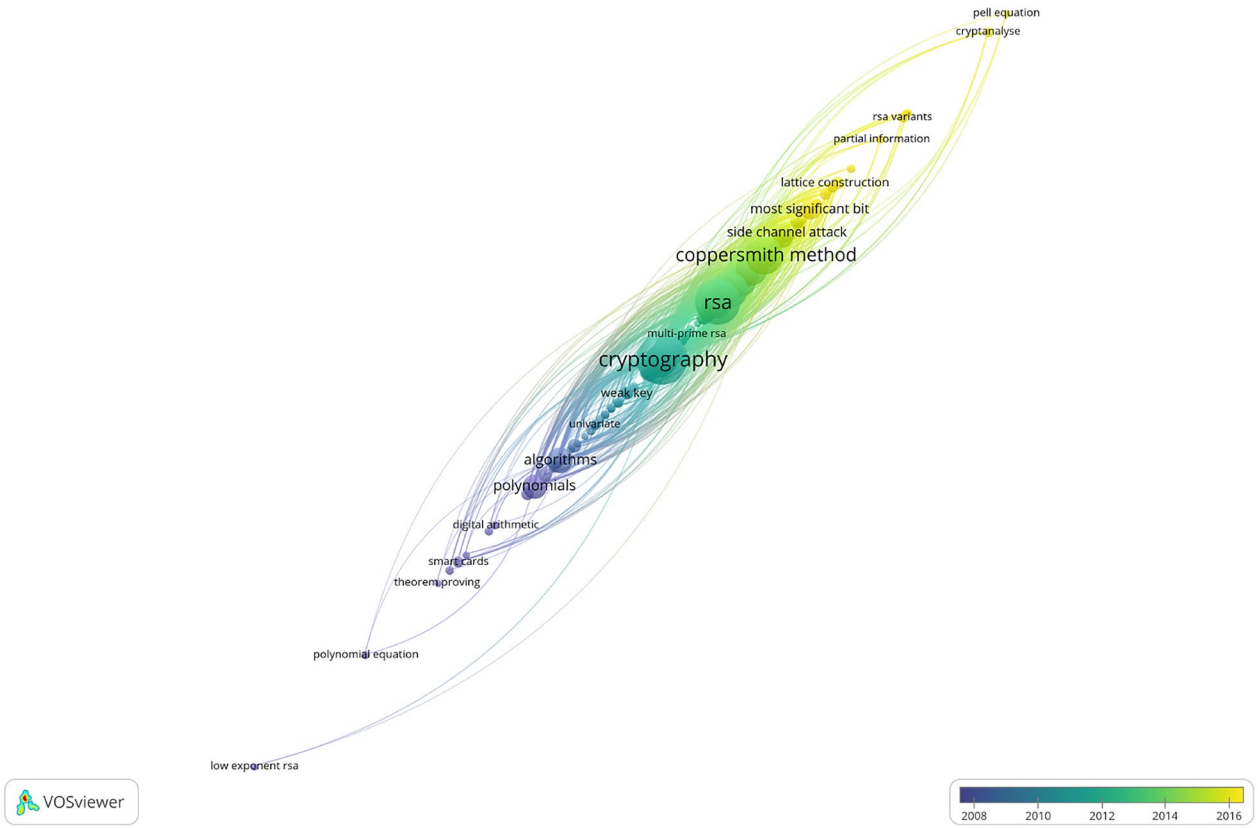


Fig. 8 The keyword time evolution map in lattice-based cryptanalysis of RSA-type cryptosystems

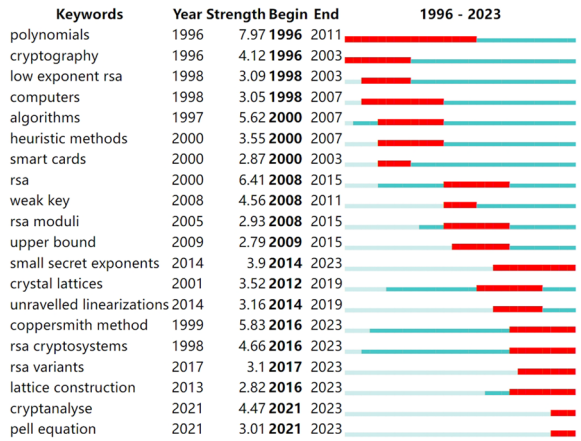


Fig. 9 Top 20 keywords based on burst strength

in this field, emphasizing the underlying study in the lattice-based method and various attacks under distinct scenarios. Future research might explore these areas, especially partial key exposure attack, side channel attack, and lattice construction in the context of Internet of Things, cloud computing, and machine learning.

Table 8 Top 3 regions based on the top 20 keywords listed in Fig. 9

Keyword	Top 3 Regions
polynomials	Japan, Germany, China
cryptography	China, France, Japan
low exponent rsa	USA, France, Germany
computers	Japan, USA, Australia
algorithms	China, Japan, France
heuristic methods	France, China, Germany
smart cards	France, Germany, UK
weak key	China, India, Germany
rsa moduli	China, France, India
upper bound	China, Japan, Canada
small secret exponents	Japan, Germany, India
crystal lattices	Japan, China, USA
unravelled linearizations	China, Japan, Germany
coppersmith method	France, China, Japan
rsa cryptosystems	China, France, Australia
rsa variants	China, France, Australia
lattice construction	Japan, China, India
cryptanalyse	China, India, Japan
pell equation	China, France, Malaysia

Table 9 Top 3 institutions based on the top 20 keywords listed in Fig. 9

Keyword	Top 3 Institutions
polynomials	Chinese Academy of Sciences, University of Paderborn, University of Luxembourg
cryptography	Chinese Academy of Sciences, University of Tokyo, École Normale Supérieure
low exponent rsa	Stanford University, Microsoft Research, École Normale Supérieure
computers	University of Tokyo, University of Wollongong, Shandong University
algorithms	University of Tokyo, Chinese Academy of Sciences, École Normale Supérieure
heuristic methods	Chinese Academy of Sciences, University of Paderborn, École Normale Supérieure
smart cards	École Normale Supérieure, University of Paderborn, University College London
weak key	Indian Statistical Institute, Shandong University, University of Paderborn
rsa moduli	Chinese Academy of Sciences, Indian Statistical Institute, University of Tokyo
upper bound	University of Tokyo, Shandong University, Kyushu University
small secret exponents	University of Tokyo, University of Paderborn, Chinese Academy of Sciences
crystal lattices	University of Tokyo, Chinese Academy of Sciences, National Institute of Advanced Industrial Science and Technology
unravelled linearizations	National University of Defense Technology, University of Tokyo, Chinese Academy of Sciences
coppersmith method	Chinese Academy of Sciences, University of Tokyo, Université de Caen
rsa cryptosystems	University of Wollongong, Université de Caen, Universiti Putra Malaysia
rsa variants	University of Wollongong, University of Tokyo, Chinese Academy of Sciences
lattice construction	University of Tokyo, Chinese Academy of Sciences, National Institute of Information and Communications Technology
cryptanalyse	Tokyo Institute of Technology, Zhejiang Wanli University, University of Science and Technology of China
pell equation	Université de Caen, Universiti Putra Malaysia, Zhejiang Wanli University

Besides, lattice-based attacks on novel RSA-type cryptosystems and recently proposed automated Coppersmith method (Meers and Nowakowski 2023) are worth exploring and studying.

Despite these insights, our analysis has certain limitations. The dataset is solely from Scopus, potentially missing few relevant sources. Subjectivity in reference selection and limitations in visualization tools like CiteSpace and VOSviewer are acknowledged. However, the widespread use of CiteSpace and VOSviewer across academic fields suggests their reliability and stability in generating results.

Acknowledgements
The authors would like to thank the anonymous reviewers for their detailed comments and impressive suggestions, which improved this paper in terms of both technical and editorial quality.

Author Contributions
MZ: Conceptualization, Methodology, Supervision, Writing—review and editing. HK: Investigation, Software, Visualization, Data curation, Writing—original draft.

Funding
This work was supported by the National Natural Science Foundation of China, Grant No. 62002335, Ningbo Natural Science Foundation, Grant No. 2021J174, Ningbo Young Science and Technology Talent Cultivation Program, Grant No. 2023QL007, and the Open Fund of Advanced Cryptography and System Security Key Laboratory of Sichuan Province, Grant No. SKLACSS-202315.

Availability of data and materials
The data are available on request from the corresponding author.

Declarations

Competing interests
All authors declare that they have no competing interests.

Received: 11 June 2024 Accepted: 3 September 2024
Published online: 12 December 2024

References

Ajtai M, Dwork C (1997) A public-key cryptosystem with worst-case/average-case equivalence. In: Leighton FT, Shor PW (eds) Proceedings of the twenty-ninth annual ACM symposium on the theory of computing, El Paso, Texas, USA, May 4–6, 1997, pp 284–293. ACM. Retrieved from https://doi.org/10.1145/258533.258604

Aono Y (2009) A new lattice construction for partial key exposure attack for RSA. In: Jarecki S, Tsudik G (eds) Public key cryptography—PKC 2009, 12th international conference on practice and theory in public key cryptography, Irvine, CA, USA, March 18-20, 2009. Proceedings, vol 5443. Springer, Berlin, pp 34–53. https://doi.org/10.1007/978-3-642-00468-1_3

Becker T, Weispfenning V, Kredel H (1993) Gröbner bases: a computational approach to commutative algebra, vol 141. Springer, Berlin

Blömer J, May A (2003) New partial key exposure attacks on RSA. In: Boneh D (ed) Advances in cryptology: CRYPTO 2003, 23rd annual international cryptology conference, Santa Barbara, California, USA, August 17–21, 2003, proceedings, vol 2729. Springer, Berlin, pp 27–43. https://doi.org/10.1007/978-3-540-45146-4_2

Blömer J, May A (2004) A generalized wiener attack on RSA. In: Bao F, Deng RH, Zhou J (eds) Public key cryptography: PKC 2004, 7th international workshop on theory and practice in public key cryptography, Singapore, March 1–4, 2004, vol 2947. Springer, Berlin, pp 1–13. https://doi.org/10.1007/978-3-540-24632-9_1

Blömer J, May A (2005) A tool kit for finding small roots of bivariate polynomials over the integers. In: Cramer R (ed) Advances in cryptology: EUROCRYPT 2005, 24th annual international conference on the theory and applications of cryptographic techniques, Aarhus, Denmark, May 22–26,

2005, proceedings, vol 3494. Springer, Berlin, pp 251–267. https://doi.org/10.1007/11426639_15
Boneh D (1999) Twenty years of attacks on the RSA cryptosystem. Not AMS 46(2):203–213
Boneh D, Durfee G (2000) Cryptanalysis of RSA with private key d less than $N^{0.292}$. IEEE Trans Inf Theory 46(4):1339–1349. https://doi.org/10.1109/18.850673
Boneh D, Durfee G, Frankel Y (1998) An attack on RSA given a small fraction of the private key bits. In: Ohta K, Pei D (eds) Advances in cryptology: ASIACRYPT '98, international conference on the theory and applications of cryptology and information security, Beijing, China, October 18–22, 1998, proceedings, vol 1514. Springer, Berlin, pp 25–34. https://doi.org/10.1007/3-540-49649-1_3
Boneh D, Durfee G, Howgrave-Graham N (1999) Factoring $N = p^r q$ for large r. In: Wiener MJ (eds) Advances in cryptology: CRYPTO '99, 19th annual international cryptology conference, Santa Barbara, California, USA, August 15–19, 1999, proceedings, vol 1666, pp 326–337. Springer. Retrieved from https://doi.org/10.1007/3-540-48405-1_21
Bunder MW, Nitaj A, Susilo W, Tonien J (2017) A generalized attack on RSA type cryptosystems. Theor Comput Sci 704:74–81. https://doi.org/10.1016/j.tcs.2017.09.009
Chen C (2006) CiteSpace II: detecting and visualizing emerging trends and transient patterns in scientific literature. J Assoc Inf Sci Technol 57(3):359–377. https://doi.org/10.1002/asi.20317
Chen Y, Nguyen PQ (2011) BKZ 2.0: better lattice security estimates. In: Lee DH, Wang X (eds) Advances in cryptology: ASIACRYPT 2011—17th international conference on the theory and application of cryptology and information security, Seoul, South Korea, December 4–8, 2011. Proceedings, vol 7073, pp 1–20. Springer. Retrieved from https://doi.org/10.1007/978-3-642-25385-0_1
Collins T, Hopkins D, Langford S, Sabin M (1998) Public key cryptographic apparatus and method (No. 5848159). (U.S. Patent 5848159)
Coppersmith D (1996a) Finding a small root of a bivariate integer equation; factoring with high bits known. In: Maurer UM (ed) Advances in cryptology: EUROCRYPT '96, international conference on the theory and application of cryptographic techniques, Saragossa, Spain, May 12–16, 1996, proceeding, vol 1070. Springer, pp 178–189. https://doi.org/10.1007/3-540-68339-9_16
Coppersmith D (1996b) Finding a small root of a univariate modular equation. In: Maurer UM (ed) Advances in cryptology: EUROCRYPT '96, international conference on the theory and application of cryptographic techniques, Saragossa, Spain, May 12–16, 1996, proceeding, vol 1070. Springer, Berlin, pp 155–165. https://doi.org/10.1007/3-540-68339-9_14
Coppersmith D (1997) Small solutions to polynomial equations, and low exponent RSA vulnerabilities. J Cryptol 10(4):233–260. https://doi.org/10.1007/s001459900030
Coron J (2004) Finding small roots of bivariate integer polynomial equations revisited. In: Cachin C, Camenisch J (eds) Advances in cryptology: EUROCRYPT 2004, international conference on the theory and applications of cryptographic techniques, Interlaken, Switzerland, May 2–6, 2004, proceedings, vol 3027. Springer, Berlin, pp 492–505. https://doi.org/10.1007/978-3-540-24676-3_29
Coron J (2007) Finding small roots of bivariate integer polynomial equations: a direct approach. In: Menezes A (ed) Advances in cryptology: CRYPTO 2007, 27th annual international cryptology conference, Santa Barbara, CA, USA, August 19–23, 2007, proceedings, vol 4622. Springer, Berlin, pp 379–394. https://doi.org/10.1007/978-3-540-74143-5_21
Coron J, Joux A, Kizhvatov I, Naccache D, Paillier P (2009) Fault attacks on RSA signatures with partially unknown messages. In: Clavier C, Gaj K (eds) Cryptographic hardware and embedded systems: CHES 2009, 11th international workshop, Lausanne, Switzerland, September 6–9, 2009, proceedings, vol 5747. Springer, Berlin, pp 444–456. https://doi.org/10.1007/978-3-642-04138-9_31
Durfee G, Nguyen PQ (2000) Cryptanalysis of the RSA schemes with short secret exponent from asiacrypt '99. In: Okamoto T (ed) Advances in cryptology—ASIACRYPT 2000, 6th international conference on the theory and application of cryptology and information security, Kyoto, Japan, December 3–7, 2000, proceedings, vol 1976, pp 14–29. Springer. Retrieved from https://doi.org/10.1007/3-540-44448-3_2
Elkamchouchi H, Elshenawy K, Shaban H (2002) Extended RSA cryptosystem and digital signature schemes in the domain of Gaussian integers. In: The 8th international conference on communication systems, 2002 (ICCS 2002), vol 1, pp 91–95
Ernst M, Jochemsz E, May A, de Weger B (2005) Partial key exposure attacks on RSA up to full size exponents. In: Cramer R (ed) Advances in cryptology: EUROCRYPT 2005, 24th annual international conference on the theory and applications of cryptographic techniques, Aarhus, Denmark, May 22–26, 2005, proceedings, vol 3494. Springer, Berlin, pp 371–386. https://doi.org/10.1007/11426639_22
Feng Y, Nitaj A, Pan Y (2023) Generalized implicit factorization problem. CoRR, arXiv:2304.08718, Retrieved from https://doi.org/10.48550/arXiv.2304.08718
Herrmann M, May A (2008) Solving linear equations modulo divisors: on factoring given any bits. In: Pieprzyk J (ed) Advances in cryptology: ASIACRYPT 2008, 14th international conference on the theory and application of cryptology and information security, Melbourne, Australia, December 7–11, 2008. proceedings, vol 5350, pp 406–424. Springer. Retrieved from https://doi.org/10.1007/978-3-540-89255-7_25
Herrmann M, May A (2009) Attacking power generators using unravelled linearization: when do we output too much? In: Matsui M (ed) Advances in cryptology: ASIACRYPT 2009, 15th international conference on the theory and application of cryptology and information security, Tokyo, Japan, December 6–10, 2009. Proceedings, vol 5912. Springer, Berlin, pp 487–504. https://doi.org/10.1007/978-3-642-10366-7_29
Hinek MJ (2006) Another look at small RSA exponents. In: Pointcheval D (ed) Topics in cryptology: CT-RSA 2006, the cryptographers' track at the RSA conference 2006, San Jose, CA, USA, February 13–17, 2006, proceedings, vol 3860. Springer, Berlin, pp 82–98. https://doi.org/10.1007/11605805_6
Howgrave-Graham N (1997) Finding small roots of univariate modular equations revisited. In: Darnell M (ed) Cryptography and coding, 6th IMA international conference, Cirencester, UK, December 17–19, 1997, proceedings, vol 1355. Springer, Berlin, pp 131–142. https://doi.org/10.1007/BFb0024458
Howgrave-Graham N, Seifert J (1999) Extending Wiener's attack in the presence of many decrypting exponents. In: Baumgart R (ed) Secure networking: CQRE (secure) '99, international exhibition and congress Düsseldorf, Germany, November 30–December 2, 1999, proceedings, vol 1740. Springer, Berlin, pp 153–166. https://doi.org/10.1007/3-540-46701-7_14
Jochemsz E, May A (2006) A strategy for finding roots of multivariate polynomials with new applications in attacking RSA variants. In: Lai X, Chen K (eds) Advances in cryptology: ASIACRYPT 2006, 12th international conference on the theory and application of cryptology and information security, Shanghai, China, December 3–7, 2006, proceedings, vol 4284, pp 267–282. Springer. Retrieved from https://doi.org/10.1007/11935230_18
Joux A, Stern J (1998) Lattice reduction: a toolbox for the cryptanalyst. J Cryptol 11(3):161–185. https://doi.org/10.1007/s001459900042
Kocher PC (1996) Timing attacks on implementations of Diffie–Hellman, RSA, DSS, and other systems. In: Koblitz N (ed) Advances in cryptology: CRYPTO '96, 16th annual international cryptology conference, Santa Barbara, California, USA, August 18–22, 1996, proceedings, vol 1109. Springer, Berlin, pp 104–113. https://doi.org/10.1007/3-540-68697-5_9
Kocher PC, Jaffe J, Jun B (1999) Differential power analysis. In: Wiener MJ (eds) Advances in cryptology: CRYPTO '99, 19th annual international cryptology conference, Santa Barbara, California, USA, August 15–19, 1999, proceedings, vol 1666, pp 388–397. Springer. Retrieved from https://doi.org/10.1007/3-540-48405-1_25
Koyama K, Maurer UM, Okamoto T, Vanstone SA (1991) New public-key schemes based on elliptic curves over the ring Z_n. In: Feigenbaum J (ed) Advances in cryptology: CRYPTO '91, 11th annual international cryptology conference, Santa Barbara, California, USA, August 11–15, 1991, proceedings, vol 576. Springer, Berlin, pp 252–266. https://doi.org/10.1007/3-540-46766-1_20
Kunihiro N, Shinohara N, Izu T (2014) Recovering RSA secret keys from noisy key bits with erasures and errors. IEICE Trans Fundam Electron Commun Comput Sci 97–A(6):1273–1284. https://doi.org/10.1587/transfun.E97.A.1273
Lagarias JC, Odlyzko AM (1985) Solving low-density subset sum problems. J ACM 32(1):229–246. https://doi.org/10.1145/2455.2461
Lenstra AK, Lenstra HW, Lovász L (1982) Factoring polynomials with rational coefficients. Math Ann 261(4):515–534

Lenstra AK, Jr, HWL, Manasse MS, Pollard JM (1990) The number field sieve. In: Ortiz H (eds) Proceedings of the 22nd annual ACM symposium on theory of computing, May 13–17, 1990, Baltimore, Maryland, USA, pp 564–572. ACM. Retrieved from https://doi.org/10.1145/100216.100295

Lim S, Kim S, Yie I, Lee H (2000) A generalized Takagi-cryptosystem with a modulus of the form $p^r q^s$. In: Roy BK, Okamoto E (eds) Progress in cryptology: INDOCRYPT 2000, first international conference in cryptology in India, Calcutta, India, December 10–13, 2000, proceedings, vol 1977. Springer, Berlin, pp 283–294. https://doi.org/10.1007/3-540-44495-5_25

Lu Y, Zhang R, Lin D (2013) Factoring multi-power RSA modulus $N = p^r q$ with partial known bits. In: Boyd C, Simpson L (eds) Information security and privacy: 18th Australasian conference, ACISP 2013, Brisbane, Australia, July 1–3, 2013. Proceedings, vol 7959. Springer, Berlin, pp 57–71. https://doi.org/10.1007/978-3-642-39059-3_5

Lu Y, Peng L, Zhang R, Hu L, Lin D (2015a) Towards optimal bounds for implicit factorization problem. In: Dunkelman O, Keliher L (eds) Selected areas in cryptography: SAC 2015—22nd international conference, Sackville, NB, Canada, August 12–14, 2015, revised selected papers, vol 9566. Springer, Berlin, pp 462–476. https://doi.org/10.1007/978-3-319-31301-6_26

Lu Y, Zhang R, Peng L, Lin D (2015b) Solving linear equations modulo unknown divisors: revisited. In: Iwata T, Cheon JH (eds) Advances in cryptology: ASIACRYPT 2015—21st international conference on the theory and application of cryptology and information security, Auckland, New Zealand, November 29–December 3, 2015, proceedings, part I, vol 9452. Springer, Berlin, pp 189–213. https://doi.org/10.1007/978-3-662-48797-6_9

Lu Y, Peng L, Sarkar S (2017) Cryptanalysis of an RSA variant with moduli $N = p^r q^l$. J Math Cryptol 11(2):117. https://doi.org/10.1515/jmc-2016-0025

Ma Z, Li B, Cai Q, Yang J (2020) Applications and developments of the lattice attack in side channel attacks. In: Zhou J et al (eds) Applied cryptography and network security workshops: ACNS 2020 satellite workshops, Aiblock, Aihws, Aiots, cloud s &p, sci, secmt, and Simla, Rome, Italy, October 19–22, 2020, proceedings, vol 12418. Springer, Berlin, pp 435–452. https://doi.org/10.1007/978-3-030-61638-0_24

May A (2003) New RSA vulnerabilities using lattice reduction methods (Doctoral dissertation, University of Paderborn). Retrieved from http://ubdata.uni-paderborn.de/ediss/17/2003/may/disserta.pdf

May A (2010) Using LLL-reduction for solving RSA and factorization problems. In: Nguyen PQ, Vallée B (eds) The LLL algorithm: survey and applications. Springer, Berlin, pp 315–348. https://doi.org/10.1007/978-3-642-02295-1_10

May A, Ritzenhofen M (2009) Implicit factoring: on polynomial time factoring given only an implicit hint. In: Jarecki S, Tsudik G (eds) Public key cryptography: PKC 2009, 12th international conference on practice and theory in public key cryptography, Irvine, CA, USA, March 18–20, 2009, proceedings, vol 5443. Springer, Berlin, pp 1–14. https://doi.org/10.1007/978-3-642-00468-1_1

May A, Nowakowski J, Sarkar S (2022) Approximate divisor multiples: factoring with only a third of the secret crt-exponents. In: Dunkelman O, Dziembowski S (eds) Advances in cryptology: EUROCRYPT 2022—41st annual international conference on the theory and applications of cryptographic techniques, Trondheim, Norway, May 30–June 3, 2022, proceedings, part III, vol 13277, pp 147–167. Springer. Retrieved from https://doi.org/10.1007/978-3-031-07082-2_6

Meers J, Nowakowski J (2023) Solving the hidden number problem for CSIDH and CSURF via automated coppersmith. In: Guo J, Steinfeld R (eds) Advances in cryptology: ASIACRYPT 2023—29th international conference on the theory and application of cryptology and information security, Guangzhou, China, December 4–8, 2023, proceedings, part IV, vol 14441. Springer, Berlin, pp 39–71. https://doi.org/10.1007/978-981-99-8730-6_2

Mumtaz M, Luo P (2019) Forty years of attacks on the RSA cryptosystem: a brief survey. J Discrete Math Sci Cryptogr 22(1):9–29. https://doi.org/10.1080/09720529.2018.1564201

Murru N, Saettone FM (2017) A novel RSA-Like cryptosystem based on a generalization of the rédei rational functions. In: Kaczorowski J, Pieprzyk J, Pomykala J (eds) Number-theoretic methods in cryptology: first international conference, nutmic 2017, Warsaw, Poland, September 11–13, 2017, revised selected papers, vol 10737. Springer, Berlin, pp 91–103. https://doi.org/10.1007/978-3-319-76620-1_6

Nassr DI, Anwar M, Bahig HM (2022) Improving small private exponent attack on the Murru–Saettone cryptosystem. Theor Comput Sci 923:222–234. https://doi.org/10.1016/j.tcs.2022.05.010

Nemec M, Sýs M, Svenda P, Klinec D, Matyas V (2017) The return of coppersmith's attack: practical factorization of widely used RSA moduli. In: Thuraisingham B, Evans D, Malkin T, Xu D (eds) Proceedings of the 2017 ACM SIGSAC conference on computer and communications security, CCS 2017, Dallas, TX, USA, October 30–November 03, 2017, pp 1631–1648. ACM. Retrieved from https://doi.org/10.1145/3133956.3133969

Nguyen PQ, Stern J (2000) Lattice reduction in cryptology: an update. In: Bosma W (ed) Algorithmic number theory, 4th international symposium, ants-iv, Leiden, The Netherlands, July 2–7, 2000, proceedings, vol 1838. Springer, Berlin, pp 85–112. https://doi.org/10.1007/10722028_4

Nguyen PQ, Stern J (2001) The two faces of lattices in cryptology. In: Silverman JH (ed) Cryptography and lattices, international conference, calc 2001, Providence, RI, USA, March 29–30, 2001, revised papers, vol 2146. Springer, Berlin, pp 146–180. https://doi.org/10.1007/3-540-44670-2_12

Nitaj A (2008) Another generalization of Wiener's attack on RSA. In: Vaudenay S (ed) Progress in cryptology: AFRICACRYPT 2008, first international conference on cryptology in Africa, Casablanca, Morocco, June 11–14, 2008, proceedings, vol 5023. Springer, Berlin, pp 174–190. https://doi.org/10.1007/978-3-540-68164-9_12

Nitaj A (2009) Cryptanalysis of RSA using the ratio of the primes. In: Preneel B (ed) Progress in cryptology: AFRICACRYPT 2009, second international conference on cryptology in Africa, Gammarth, Tunisia, June 21–25, 2009, proceedings, vol 5580. Springer, Berlin, pp 98–115. https://doi.org/10.1007/978-3-642-02384-2_7

Nitaj A, Rachidi T (2015) Factoring RSA moduli with weak prime factors. In: Hajji SE, Nitaj A, Carlet C, Souidi EM (eds) Codes, cryptology, and information security: first international conference, C2SI 2015, Rabat, Morocco, May 26–28, 2015, proceedings—in honor of Thierry Berger, vol 9084, pp 361–374. Springer. Retrieved from https://doi.org/10.1007/978-3-319-18681-8_29

Nitaj A, Ariffin MRBK, Adenan NNH, Lau TSC, Chen J (2022) Security issues of novel RSA variant. IEEE Access 10:53788–53796. https://doi.org/10.1109/ACCESS.2022.3175519

Peng L, Hu L, Xu J, Huang Z, Xie Y (2014) Further improvement of factoring RSA moduli with implicit hint. In: Pointcheval D, Vergnaud D (eds) Progress in cryptology—AFRICACRYPT 2014—7th international conference on cryptology in Africa, Marrakesh, Morocco, May 28–30, 2014, proceedings, vol 8469, pp 165–177. Springer. Retrieved from https://doi.org/10.1007/978-3-319-06734-6_11

Peng L, Hu L, Lu Y, Huang Z, Xu J (2015) Implicit factorization of RSA moduli revisited (short paper). In: Tanaka K, Suga Y (eds) Advances in information and computer security—10th international workshop on security, IWSEC 2015, Nara, Japan, August 26–28, 2015, proceedings, vol 9241, pp 67–76. Springer. Retrieved from https://doi.org/10.1007/978-3-319-22425-1_5

Price DJDS (1963) Little science, big science. Columbia University Press, New York. https://doi.org/10.7312/pric91844

Price DJDS (1965) Networks of scientific papers: the pattern of bibliographic references indicates the nature of the scientific research front. Science 149(3683):510–515. https://doi.org/10.1126/science.149.3683.510

Quisquater J-J, Couvreur C (1982) Fast decipherment algorithm for RSA public-key cryptosystem. Electron Lett 18(21):905–907. https://doi.org/10.1145/359340.359342

Rivest RL, Shamir A (1985) Efficient factoring based on partial information. In: Pichler F (ed) Advances in cryptology: EUROCRYPT '85, workshop on the theory and application of of cryptographic techniques, Linz, Austria, April 1985, proceedings, vol 219, pp 31–34. Springer. Retrieved from https://doi.org/10.1007/3-540-39805-8_3

Rivest RL, Shamir A, Adleman LM (1978) A method for obtaining digital signatures and public-key cryptosystems. Commun ACM 21(2):120–126. https://doi.org/10.1145/359340.359342

Sarkar S (2011) Partial key exposure: generalized framework to attack RSA. In: Bernstein DJ, Chatterjee S (eds) Progress in cryptology: INDOCRYPT 2011—12th international conference on cryptology in India, Chennai, India, December 11–14, 2011, proceedings, vol 7107, pp 76–92. Springer. Retrieved from https://doi.org/10.1007/978-3-642-25578-6_7

Sarkar S, Maitra S (2011) Approximate integer common divisor problem relates to implicit factorization. IEEE Trans Inf Theory 57(6):4002–4013. https://doi.org/10.1109/TIT.2011.2137270

Sarkar S, Maitra S (2012) Side channel attack to actual cryptanalysis: breaking CRT-RSA with low weight decryption exponents. In: Prouff E, Schaumont P (eds) Cryptographic hardware and embedded systems: CHES 2012—14th international workshop, Leuven, Belgium, September 9–12, 2012. proceedings, vol 7428, pp 476–493. Springer. Retrieved from https://doi.org/10.1007/978-3-642-33027-8_28

Shi G, Wang G, Gu D (2022) Further cryptanalysis of a type of RSA variants. In: Susilo W, Chen X, Guo F, Zhang Y, Intan R (eds) Information security: 25th international conference, ISC 2022, Bali, Indonesia, December 18–22, 2022, proceedings, vol 13640, pp 133–152. Springer. Retrieved from https://doi.org/10.1007/978-3-031-22390-7_9

Small H (1973) Co-citation in the scientific literature: a new measure of the relationship between two documents. J Am Soc Inf Sci 24(4):265–269. https://doi.org/10.1002/asi.4630240406

Stern J (1998) Lattices and cryptography: an overview. In: Imai H, Zheng Y (eds) Public key cryptography, first international workshop on practice and theory in public key cryptography, PKC '98, Pacifico Yokohama, Japan, February 5–6, 1998, proceedings, vol 1431, pp 50–54. Springer. Retrieved from https://doi.org/10.1007/BFb0054013

Sun H, Wu M, Ting W, Hinek MJ (2007) Dual RSA and its security analysis. IEEE Trans Inf Theory 53(8):2922–2933. https://doi.org/10.1109/TIT.2007.901248

Suzuki K, Takayasu A, Kunihiro N (2020) Extended partial key exposure attacks on RSA: improvement up to full size decryption exponents. Theor Comput Sci 841:62–83. https://doi.org/10.1016/j.tcs.2020.07.004

Takagi T (1998) Fast RSA-type cryptosystem modulo $p^k q$. In: Krawczyk H (eds) Advances in cryptology: CRYPTO '98, 18th annual international cryptology conference, Santa Barbara, California, USA, August 23–27, 1998, proceedings, vol 1462, pp 318–326. Springer. Retrieved from https://doi.org/10.1007/BFb0055738

Takayasu A, Kunihiro N (2014a) Better lattice constructions for solving multivariate linear equations modulo unknown divisors. IEICE Trans Fundam Electron Commun Comput Sci 97–A(6):1259–1272. https://doi.org/10.1587/transfun.E97.A.1259

Takayasu A, Kunihiro N (2014b) Cryptanalysis of RSA with multiple small secret exponents. In: Susilo W, Mu Y (eds) Information security and privacy: 19th Australasian conference, ACISP 2014, Wollongong, NSW, Australia, July 7–9, 2014, proceedings, vol 8544, pp 176–191. Springer. Retrieved from https://doi.org/10.1007/978-3-319-08344-5_12

Takayasu A, Kunihiro N (2014c) Partial key exposure attacks on RSA: achieving the Boneh–Durfee bound. In: Joux A, Youssef AM (eds) Selected areas in cryptography: SAC 2014—21st international conference, Montreal, QC, Canada, August 14–15, 2014, revised selected papers, vol 8781, pp 345–362. Springer. Retrieved from https://doi.org/10.1007/978-3-319-13051-4_21

Takayasu A, Kunihiro N (2015) Partial key exposure attacks on CRT-RSA: better cryptanalysis to full size encryption exponents. In: Malkin T, Kolesnikov V, Lewko AB, Polychronakis M (eds) Applied cryptography and network security: 13th international conference, ACNS 2015, New York, NY, USA, June 2–5, 2015, revised selected papers, vol 9092, pp 518–537. Springer. Retrieved from https://doi.org/10.1007/978-3-319-28166-7_25

Takayasu A, Kunihiro N (2016) Partial key exposure attacks on CRT-RSA: General improvement for the exposed least significant bits. In: Bishop M, Nascimento ACA (eds) Information security: 19th international conference, ISC 2016, Honolulu, HI, USA, September 3–6, 2016, proceedings, vol 9866, pp 35–47. Springer. Retrieved from https://doi.org/10.1007/978-3-319-45871-7_3

Takayasu A, Kunihiro N (2017) A tool kit for partial key exposure attacks on RSA. In: Handschuh H (eds) Topics in cryptology: CT-RSA 2017—the cryptographers' track at the RSA conference 2017, San Francisco, CA, USA, February 14–17, 2017, proceedings, vol 10159, pp 58–73. Springer. Retrieved from https://doi.org/10.1007/978-3-319-52153-4_4

Ueno R (2023) Homma N (2023) How secure is exponent-blinded RSA-CRT with sliding window exponentiation? IACR Trans Cryptogr Hardw Embed Syst 2:241–269. https://doi.org/10.46586/tches.v2023.i2.241-269

van Eck NJ, Waltman L (2010) Software survey: VOSviewer, a computer program for bibliometric mapping. Scientometrics 84(2):523–538. https://doi.org/10.1007/s11192-009-0146-3

Wang S, Qu L, Li C, Wang H (2019) Further improvement of factoring $N = p^r q^s$ with partial known bits. Adv Math Commun 13(1):121–135. https://doi.org/10.3934/amc.2019007

Wang S, Qu L, Li C, Fu S, Chen H (2021) Finding small solutions of the equation $bx - ay = z$ and its applications to cryptanalysis of the RSA cryptosystem. Adv Math Commun 15(3):441–469. https://doi.org/10.3934/amc.2020076

White HD, Griffith BC (1981) Author cocitation: a literature measure of intellectual structure. J Am Soc Inf Sci 32(3):163–171. https://doi.org/10.1002/asi.4630320302

Wiener MJ (1990) Cryptanalysis of short RSA secret exponents. IEEE Trans Inf Theory 36(3):553–558. https://doi.org/10.1109/18.54902

Zheng M (2023) Partial key exposure attack on common prime RSA. In: Ge C, Yung M (eds) Information security and cryptology: 19th international conference, inscrypt 2023, Hangzhou, China, December 9–10, 2023, revised selected papers, part II, vol 14527, pp 407–410. Springer. Retrieved from https://doi.org/10.1007/978-981-97-0945-8_27

Zheng M, Kunihiro N, Hu H (2017) Improved factoring attacks on multi-prime RSA with small prime difference. In: Pieprzyk J, Suriadi S (eds) Information security and privacy: 22nd Australasian conference, ACISP 2017, Auckland, New Zealand, July 3–5, 2017, proceedings, part I, vol 10342, pp 324–342. Springer. Retrieved from https://doi.org/10.1007/978-3-319-60055-0_17

Zheng M, Kunihiro N, Hu H (2020) Lattice-based cryptanalysis of RSA with implicitly related keys. IEICE Trans Fundam Electron Commun Comput Sci 103–A(8):959–968. https://doi.org/10.1587/transfun.2019EAP1170

Zheng M, Kunihiro N, Yao Y (2021) Cryptanalysis of the RSA variant based on cubic Pell equation. Theor Comput Sci 889:135–144. https://doi.org/10.1016/j.tcs.2021.08.001

Zheng M, Chen Z, Wu Y (2023) Solving generalized bivariate integer equations and its application to factoring with known bits. IEEE Access 11:34674–34684. https://doi.org/10.1109/ACCESS.2023.3264590

Zhou Y, van de Pol J, Yu Y, Standaert F (2022) A third is all you need: extended partial key exposure attack on CRT-RSA with additive exponent blinding. In: Agrawal S, Lin D (eds) Advances in cryptology: ASIACRYPT 2022—28th international conference on the theory and application of cryptology and information security, Taipei, Taiwan, December 5–9, 2022, proceedings, part IV, vol 13794, pp 508–536. Springer. Retrieved from https://doi.org/10.1007/978-3-031-22972-5_18

Publisher's Note