



Securing the Post-Quantum Digital World: A Bibliometric Mapping of Post-Quantum Cryptography and Cybersecurity Research

Elisha Mutize¹, Admire Mthombeni², Leonard Chitongo³

¹ Lecturer, Management Accounting and Finance Department, Walter Sisulu University, Mthatha Campus, South Africa. Email: emutize@wsu.ac.za

² Postdoctoral Research Fellow, Graduate School of Business and Leadership, University of KwaZulu-Natal, South Africa. Email: mthombeniA@ukzn.ac.za

³ Senior Lecturer Human Geography, Department of Biological and Environmental Sciences, Walter Sisulu University, Mthatha, South Africa. Email: Ichitongo@wsu.ac.za

ARTICLE INFO

Article History:

Received: May 11, 2026
Revised: September 02, 2026
Accepted: September 04, 2026
Available Online: September 30, 2026

Keywords:

Post-Quantum Cryptography
Cybersecurity
Quantum-Safe Security
Lattice-Based Cryptography
Blockchain
Internet of Things
Bibliometric Analysis
Science Mapping

ABSTRACT

As quantum computing progresses, longstanding security assumptions that form the foundations of today's digital infrastructure are being undermined, and new cryptographic mechanisms are needed that can resist attacks from a quantum computer. In this study, the bibliometric analysis of 1346 Web of Science Core Collection documents from 2015 to 2026 have been used to map the development, intellectual structure and emerging cybersecurity applications of post-quantum cryptography (PQC). Bibliometrix/Biblioshiny and VOSviewer were used to perform performance analysis and science mapping, including annual production, citation dynamics, author productivity, institutional and country contributions, source concentration, keyword co-occurrence, thematic positioning, and topic evolution. The results indicate that research has accelerated quickly, from less than 10 publications per year in 2015-2016 to 456 in 2025, and that 2026 is a partial indexing year. Citation influence is dominated by China and the United States, and the most visible affiliations include the Chinese Academy of Sciences, State University System of Florida, and Florida Atlantic University. IEEE Access is the leading publication outlet. Keyword and thematic analyses show that the field has moved from foundational cryptanalysis and mathematical constructions toward lattice-based cryptography, hardware acceleration, NIST standardization, CRYSTALS-Kyber/ML-KEM, authentication, blockchain, Internet of Things, and migration-oriented cybersecurity. The study further identifies a post-standardization shift from algorithm competition to implementation assurance, crypto-agility, interoperability, side-channel resilience, and sector-specific deployment. These findings provide an updated evidence base for researchers, cybersecurity practitioners, standards bodies, and organizations planning quantum-safe migration.



© 2026 The Authors, Published by iRASD. This is an Open Access article under the Creative Common Attribution Non-Commercial 4.0

Corresponding Author's Email: emutize@wsu.ac.za

1. Introduction

Public-key cryptography is embedded in almost every layer of modern digital life, including web authentication, software updates, virtual private networks, electronic payments, cloud platforms, identity systems, critical infrastructure, and Internet of Things (IoT) devices. Much of this security relies on mathematical problems such as integer factorization and discrete logarithms that are difficult for classical computers. Shor (1994), however, demonstrated that sufficiently capable quantum computers could solve these

problems in polynomial time, thereby undermining widely deployed RSA and elliptic-curve cryptography. The strategic implication is not that current systems are already broken, but that information requiring long-term confidentiality may be exposed to “harvest now, decrypt later” attacks and that large-scale cryptographic migration must begin before cryptographically relevant quantum computers become practical. Bauch et al. (2017) therefore frame post-quantum cryptography (PQC) as the development of cryptosystems intended to remain secure even when adversaries possess large quantum computers.

The policy and standards response have accelerated substantially. NIST’s 2016 report on PQC formally emphasized the need for quantum-resistant public-key algorithms and crypto-agility (Chen et al., 2016). After a multiyear international standardization process, NIST finalized FIPS 203 for ML-KEM, FIPS 204 for ML-DSA, and FIPS 205 for SLH-DSA in August 2024. In March 2025, NIST selected HQC as an additional key-encapsulation mechanism to diversify the mathematical foundations of the standardized portfolio (Alagic et al., 2025). By 2026, the focus shifted from selecting algorithms to migrating to an architecture and operating in a crypto-agile manner, with NIST guidance emphasizing the need to change and adapt cryptographic algorithms in software, hardware, firmware, protocols, and organizational infrastructures (Barker et al., 2026). This shift represents a critical shift in the research problem – it’s not just about whether there are quantum-resistant algorithms, but whether they can be securely deployed at scale in an efficient and interoperable way.

This magnified agenda is reflected in scientific literature. Early research focused almost exclusively on mathematical constructions and efficient implementations, such as lattice based, code based, hash based, multivariate based, and isogeny based. Hardware-oriented studies focused on FPGA and processor acceleration since PQC algorithms can handle larger keys, signatures, and workloads than conventional schemes (Kozziel et al., 2017; Nejatollahi et al., 2019). Lattice-based research gained momentum due to its performance and standardization potential, resulting in many studies on the multiplication of polynomials, acceleration of instruction set and embedded implementation (Bisheh-Niasar et al., 2021; Liu et al., 2019). Meanwhile, studies in the application domain investigated the introduction of quantum-safe security to IoT, edge devices, transport protocols, distributed energy systems and migration processes of organizations (Ahn et al., 2022; Cheng et al., 2017; Joseph et al., 2022; Liu et al., 2018).

Post-standardization literature has shifted more towards practical cybersecurity. A visible applied stream of hybrid and quantum-resistant Transport Layer Security (TLS), IPsec, blockchain platforms, healthcare systems, consumer devices, and enterprise migration frameworks are now available. Rubio García et al. (2024) demonstrated quantum-resistant TLS using PQC and quantum key distribution, while Lawo et al. (2024) reported PQC-secured IPsec tunnels. Hasan et al. (2024) proposed a structured enterprise migration framework based on cryptographic dependency analysis. More recent work studies digital-signature integration in TLS and PKI, quantum-safe blockchain, IoT authentication, side-channel leakage, and high-throughput hardware or GPU acceleration (Dai et al., 2025; Huang et al., 2024; Ma et al., 2024; Puneanyi & Bhat, 2025; Raavi et al., 2025). These developments indicate that PQC is becoming a systems-security and governance problem in addition to a cryptographic-design problem.

The rapid expansion and diversification of PQC research makes systematic mapping necessary. Bibliometric analysis is well suited to identifying growth patterns, leading contributors, source concentration, citation influence, intellectual structure, and emerging themes across large bodies of literature (Donthu et al., 2021). A recent Scopus-based study by Hasija et al. (2025) confirms strong interest in bibliometric assessment of PQC. Consequently, the contribution of the present study is not merely to repeat a general bibliometric overview. Instead, it provides an updated Web of Science-based map through 31 August 2026, captures the post-standardization period after FIPS 203-205 and the HQC selection, integrates Lotka’s and Bradford’s productivity laws, and explicitly interprets the transition from algorithmic foundations toward cybersecurity deployment, crypto-agility, hardware assurance, blockchain, IoT, authentication, and migration. This positioning is particularly important because publication counts alone cannot reveal whether the field is maturing toward implementable quantum-safe infrastructures.

The study therefore addresses four research questions. RQ1 examines how PQC research has evolved over time and how its citation profile has changed. RQ2 identifies the most productive and influential authors, sources, affiliations, and countries. RQ3 maps the dominant intellectual and thematic structures of literature. RQ4 identifies emerging cybersecurity applications and research priorities likely to shape the next phase of quantum-safe security. By combining descriptive performance indicators with science-mapping outputs, the paper offers a concise but comprehensive account of where PQC research has come from, where it is concentrated, and where it is moving.

RQ1: How has post-quantum cryptography and cybersecurity research evolved over time?

RQ2: Which authors, sources, affiliations, and countries dominate the field in productivity and influence?

RQ3: What are the dominant intellectual and thematic structures of post-quantum cryptography research?

RQ4: Which emerging cybersecurity applications and implementation priorities are shaping future research?

2. Conceptual Background and Related Literature

Post-quantum cryptography can be understood as classical cryptography against the adversary who may have quantum computers. Hence, it is different from quantum key distribution (QKD) which is based on quantum-physical mechanisms for key establishment. The primary driver of PQC is compatibility—quantum-resistant algorithms that can be executed on conventional computing and networking platforms, and in principle can be integrated into existing protocols and applications. The standardization process of NIST accelerated the work for several families of mathematics: lattices, codes, hashes, multivariate equations and isogenies. In the long run, lattice-based methods grew particularly prominent as they allow for very good security assumptions with relatively good practicality while introducing implementation complexity, memory size, physical leakage and interoperability issues.

It has also been demonstrated in the literature that the mathematical security is only one of the many layers of practical security. Nejatollahi et al. (2019) compiled the hardware and implementation issues of lattice-based cryptography, while Anastasova et al. (2021) and Bisheh-Niasar et al. (2021) illustrated the impact of implementation strategies and instruction-set acceleration on feasibility materially, respectively. Hardware performance is a current topic as embedded systems, IoT devices, smart meters, network appliances and high throughput servers have very different requirements. In the current bibliometric corpus, the increased attention on FPGA, processor architecture and side-channel research is the result of the understanding that even if an algorithm is mathematically correct its implementation may be inefficient or physically insecure, resulting in failure in the operational process.

Cybersecurity applications have increasingly become the medium between cryptographic standards and risk reduction in the real world. IoT is an early and persistent application domain because devices can be deployed for many years, and they often have limited resources (Cheng et al., 2017; Kumar, 2022). Digital signatures are also a major concern, as the public-key authentication is fundamental for software distribution, certificates, identity, and non-repudiation; Tan et al. (2022) demonstrate that the requirements for digital signatures in real-world applications impose different feasibility constraints on PQC candidates. As researchers incorporate PQC into TLS and IPsec and experiment with hybrid implementations that aim to minimize the risk of transition, transport and network security have gained traction. The research on blockchain is also growing as traditional signature assumptions are directly integrated into the transaction validation and consensus mechanisms (Abbas et al., 2025; Kim et al., 2024; Puneyani & Bhat, 2025).

Now the organisation migration issue has become a research theme by itself. Joseph et al. (2022) emphasize that the replacement of cryptography will be a multi-year process and will depend on many factors for application and device performance, compliance, implementation, and operation. In this context, Hasan et al. (2024) present a cryptographic

dependency analysis and prioritization approach. In addition, NIST's updated crypto-agility guidance highlights the importance of organizations having mechanisms to replace algorithms without disrupting operations (Barker et al., 2026). This means that today's PQC landscape is a shift from "which algorithms are quantum resistant?" to "how can quantum-resistant algorithms be securely deployed, governed, monitored, and replaced across complex digital ecosystems?"

In this context, bibliometric science mapping is useful as it provides an insight into the structure of that transition on a large scale. Performance analysis detects productive authors, institutions, countries and sources, while citation analysis reveals early intellectual influence, co-word mapping shows conceptual relationships, thematic maps differentiate well developed themes from emerging or peripheral ones, and trend-topic analysis shows how the vocabulary of the field evolves over time (Aria & Cuccurullo, 2017; Donthu et al., 2021). The use of Bibliometrix/Biblioshiny and VOSviewer is especially relevant as it allows for quantitative bibliometric indicators as well as network visualization (van Eck & Waltman, 2010).

3. Methodology

In this study, bibliometric performance analysis and science mapping were employed to analyze the literature on post-quantum cryptography in the Web of Science Core Collection. Web of Science was chosen because it includes bibliographic metadata, citation information, author affiliations, keywords, and source information all in a standardized format that is appropriate for replicable bibliometric analysis. The search was performed on 31st August 2026 with the following topic query: TS= ("post-quantum cryptograph*" OR "post quantum cryptograph*" OR "quantum-resistant cryptograph*" OR "quantum resistant cryptograph*" OR "quantum-safe cryptograph*"). The final merged source file submitted for analysis was already deduplicated with 1346 unique Web of Science records. The publication years observed in the final corpus were 2015-2026; thus, the manuscript presents the period that was observed in the provided data set, not the period that was arbitrarily chosen for the retrospective cut-off.

The selection workflow was carried out transparently according to the PRISMA approach (Page et al., 2021). The source file provided had been merged and deduplicated and so a pre-deduplication retrieval total could not be reconstructed without the invention of information. The flow diagram starts with the 1,346 records remaining in the final deduplicated WoS export, includes a bibliometric eligibility assessment, and indicates that all 1,346 records are included. There were no further exclusions made as the provided data set was prepared with the stipulated PQC search strategy. This allows for traceability and explicitly states the limitation of this approach in providing pre-processing counts from a final merged file.

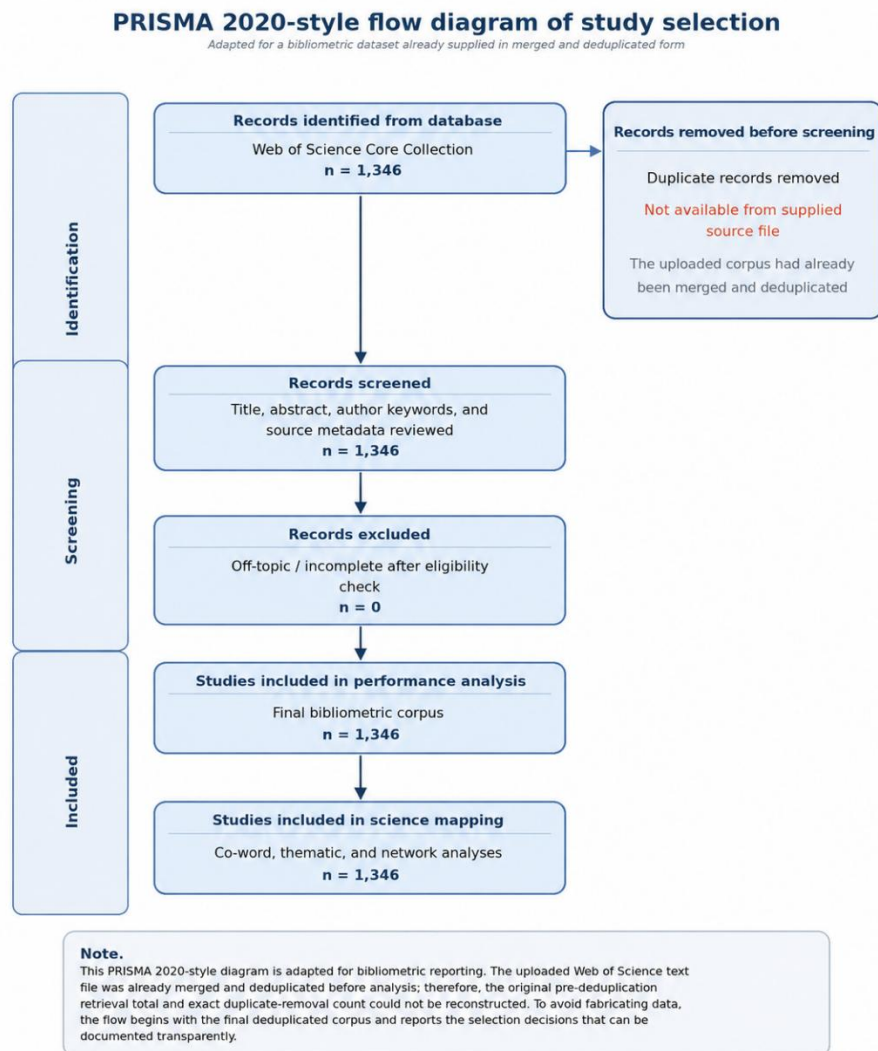
Bibliometrix/Biblioshiny was used for annual scientific production, citation trends, author productivity, source productivity, affiliations, country production, most cited countries, keyword frequencies, thematic mapping, trend topics, Lotka's law, and Bradford's law. Bibliometrix is an open-source R-based environment developed for comprehensive science mapping (Aria & Cuccurullo, 2017). VOSviewer was used for keyword co-occurrence visualization because it is specifically designed to construct and display bibliometric networks using similarity-based mapping (van Eck & Waltman, 2010). Lotka's law was used to assess the concentration of scientific productivity across authors Lotka (1926), whereas Bradford's law was used to examine concentration and dispersion across publication sources (Bradford, 1934).

The analysis was organized around four dimensions. First, temporal performance was assessed using annual scientific production and average article citations per year. Second, social and institutional structure was examined through productive authors, author productivity distribution, affiliations, and geographic production/citation patterns. Third, publication structure was assessed using most relevant sources and Bradford's law. Fourth, intellectual and conceptual structure was analyzed using the most relevant words, treemap, word cloud, thematic map, trend topics, and keyword co-occurrence network. Citation counts were treated as time-sensitive indicators of visibility rather than direct measures of research quality; recent documents naturally have shorter citation windows. The 2026

publication total was also interpreted cautiously because the search was conducted before the end of the calendar year and indexing delays can further depress the apparent output of the most recent year.

Table 1
Search Strategy and Analytical Protocol

Element	Specification
Database	Web of Science Core Collection
Search date	31 August 2026
Topic search	TS=("post-quantum cryptograph*" OR "post quantum cryptograph*" OR "quantum-resistant cryptograph*" OR "quantum resistant cryptograph*" OR "quantum-safe cryptograph*")
Observed publication period	2015-2026
Final records	1,346 unique records in the supplied merged/deduplicated export
Main tools	Bibliometrix/Biblioshiny and VOSviewer
Performance analyses	Annual production, citations, authors, affiliations, sources, countries, Lotka and Bradford laws
Science mapping	Keyword frequency, treemap, word cloud, thematic map, trend topics, keyword co-occurrence network



Source: Adapted from PRISMA 2020 (Page et al., 2021) for the present bibliometric study.

Figure 1: PRISMA-style Bibliometric Selection Flow for the Final Web of Science Corpus

Figure 1 documents the transparent selection logic used for the study. The analysis begins with the 1,346 records contained in the supplied merged and deduplicated Web of Science export and retains all of them after bibliometric eligibility assessment. The diagram

deliberately does not invent a pre-deduplication retrieval count because that information is not recoverable from the final merged file. This provides a reproducible basis for the subsequent performance and science-mapping analyses.

4. Results

4.1. Growth of the Field and Citation Dynamics

Figure 2 illustrates that there was a shift from a small specialist literature to a fast-growing research field. The number of publications did not exceed 10 per year in 2015 and 2016, grew to 34 in 2018 and 85 in 2020, and rapidly increased thereafter. Production increased to 140 documents in 2022, 172 in 2023, 268 in 2024, and 456 in 2025. The activity count in 2026 (32) is not considered a decline since the search was run on 31 August 2026 and there is a calendar truncation and indexing delay for the latest published year. The pattern of growth is similar to the one observed for PQC from the pre-standardization exploration phase to the phase of standardized algorithms and deployment-oriented cybersecurity research.

Table 2
Annual Scientific Production in the Final Corpus

Year	Documents
2015	9
2016	9
2017	10
2018	34
2019	44
2020	85
2021	87
2022	140
2023	172
2024	268
2025	456
2026	32

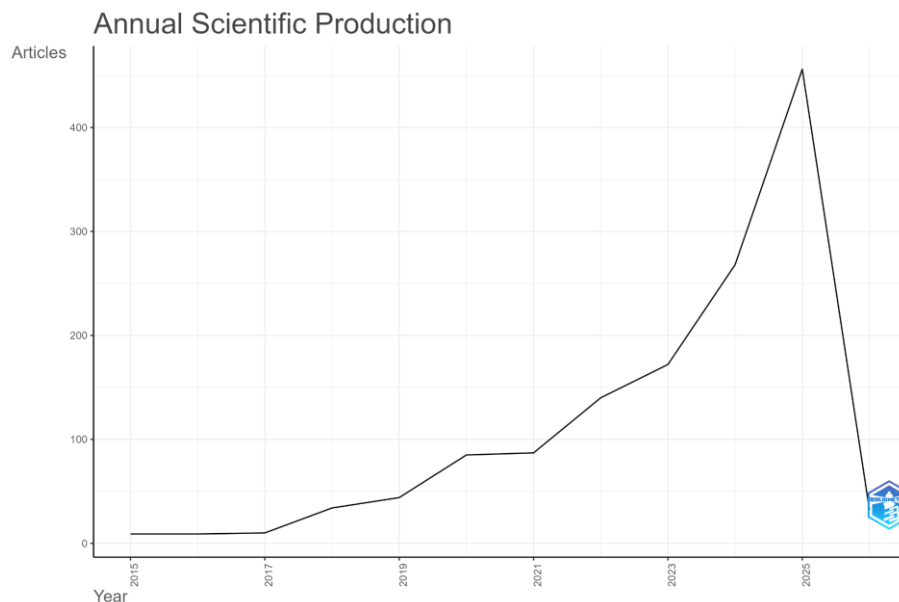


Figure 2: Annual Scientific Production in Post-quantum Cryptography Research

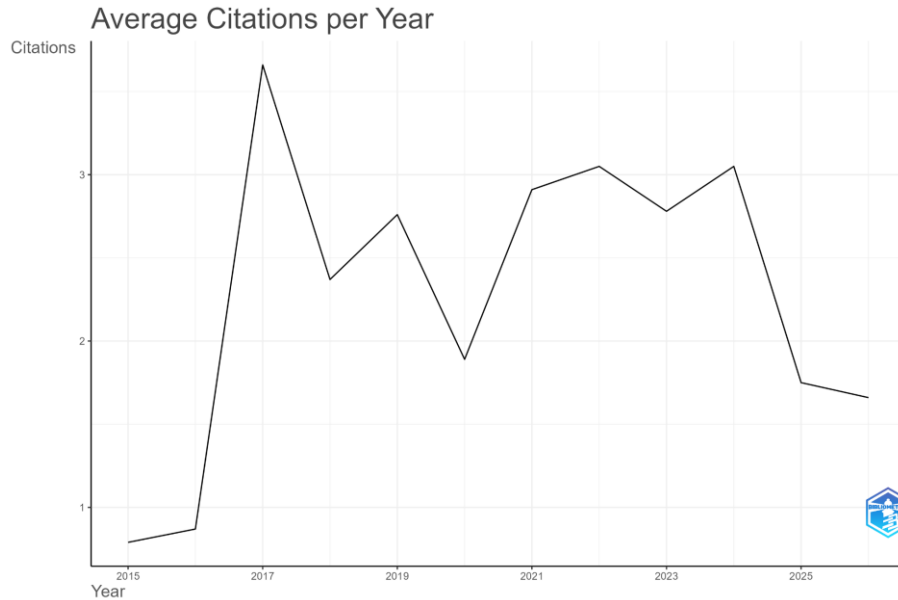


Figure 3: Average Article Citations per Year

The publication trend is complemented by the citation-rate profile in Figure 3. The higher normalized citation activity is seen around the earlier expansion phase (2017 and 2021-2024), which is since older cohorts have had more time to accumulate citations. The lower average for 2025 and 2026 is thus mostly attributable to a "citation-window effect" and not to a decline in scholarly importance. The 1,346 records received a total of 13,025 Web of Science citations, and the median was four citations per record. The combination of fast output growth and short citation windows further underscores the importance of taking raw citation rankings with a "grain of salt" when it comes to recent research.

4.2. Author productivity and Lotka's law

Figure 4 shows that there is a consistent set of recurring contributors. Azarderakhsh R has published the most documents (24), followed by Akleylek S (20), Kim S (20) and Kermani MM (18). Fourteen to fifteen papers were contributed by several other authors. These names are closely related to implementation, hardware acceleration, lattice-based cryptography, isogeny-based cryptography and security engineering, showing that the research on technical implementation has played a prominent role in the development of the field. The abbreviated names of the authors mean that the ranking should be interpreted with knowledge of possible author-name ambiguity, as with any bibliometric output using such names.

Table 3
Most Productive Author-name Entries

Author	Documents
Azarderakhsh R	24
Akleylek S	20
Kim S	20
Kermani MM	18
Debnath SK	15
Gaborit P	15
Seo H	15
Seo SC	15
Xie JF	15
Liu Z	14

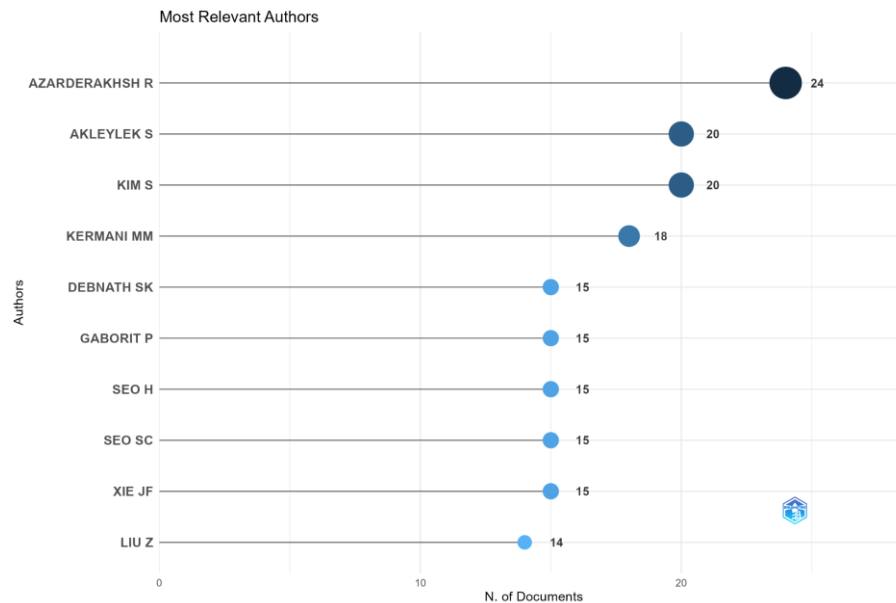


Figure 4. Most Relevant Authors

Figure 5 displays the Lotka distribution which indicates that author productivity is very skewed. Around 75.8% of author-name entries had only one document and around 12.9% had two, with decreasing percentages having more publications. The fitted exponent is 2.58 with $R^2 = 0.9731$; the fitted Kolmogorov-Smirnov p-value of 1 indicates good agreement between the observed and fitted distribution. Substantively, there is a widely distributed base of occasional contributors with a much smaller number of highly productive specialists, as is usual in rapidly growing technical areas.

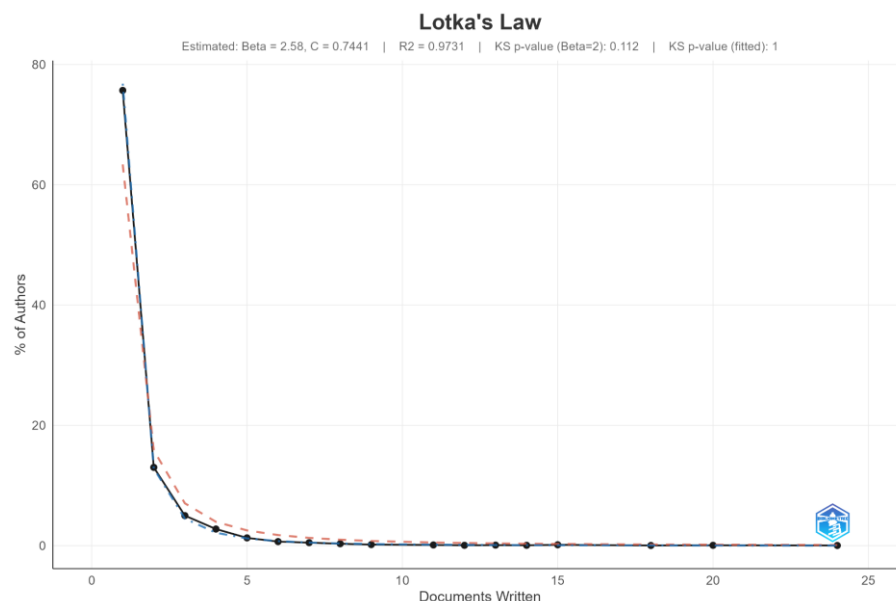


Figure 5: Lotka's Law of Scientific Productivity

4.3. Publication Sources and Bradford Concentration

IEEE Access is the dominant outlet with 125 documents, far ahead of the next sources. The rest of the top list includes circuits and systems, computer architecture, cryptographic engineering, embedded systems, and general cryptography journals. This outlet mix underlines the interdisciplinary nature of PQC; progress will require not just mathematical cryptography, but also hardware design, computer architecture, communications, embedded computing, and implementation of cybersecurity.

Table 4:
Most Relevant Publication Sources

Source	Documents
IEEE Access	125
IEEE Transactions on Circuits and Systems I- Regular Papers	41
IEEE Transactions on Computers	40
Designs, Codes and Cryptography	39
Electronics	37
Journal of Cryptographic Engineering	27
Cryptography	26
Applied Sciences-Basel	25
IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences	25
ACM Transactions on Embedded Computing Systems	24

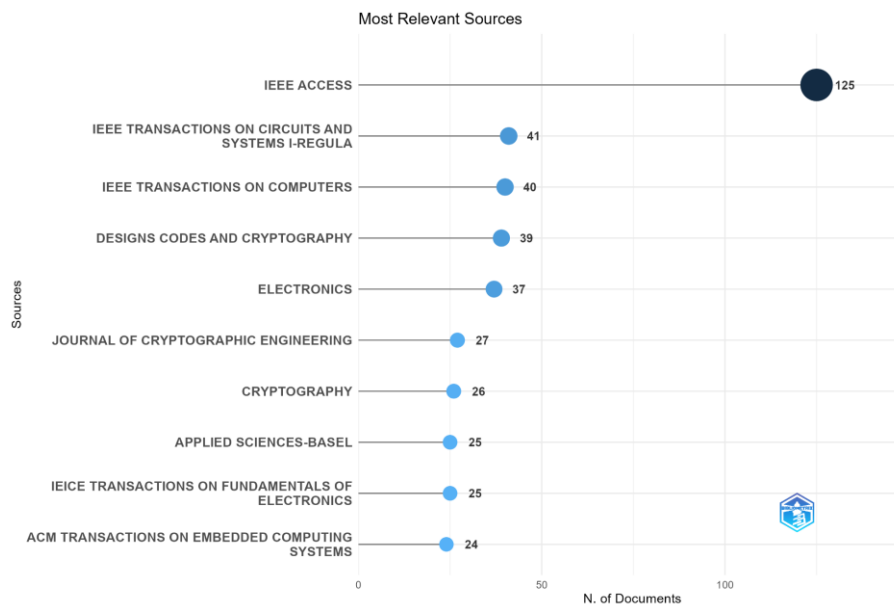


Figure 6. Most Relevant Sources

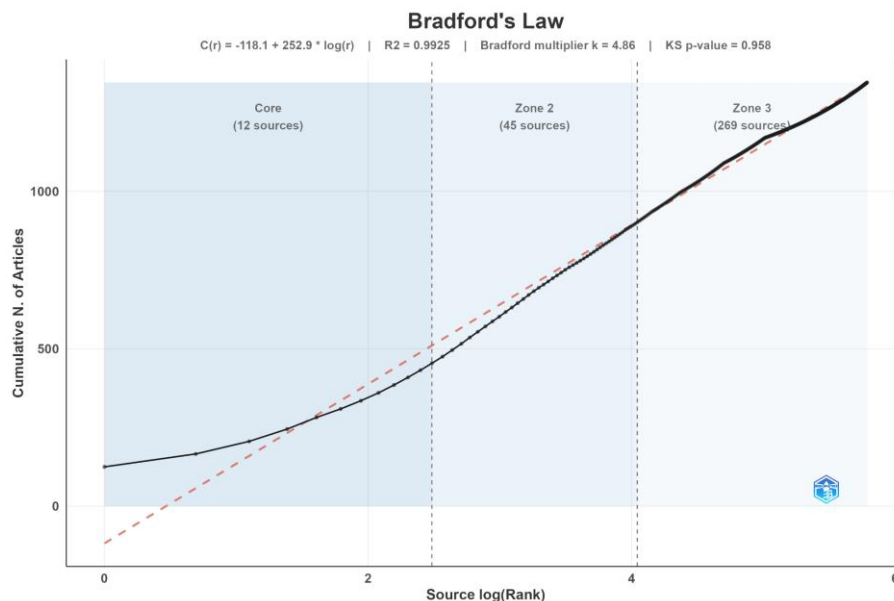


Figure 7: Bradford's Law Distribution of Sources

Bradford's law is a more meaningful interpretation of source concentration. The figure shows a core zone of 12 highly productive sources, a Zone 2 of 45 sources, and a long peripheral tail of 269 sources of Zone 3. The Bradford multiplier is 4.86 and the fitted

model has $R^2 = 0.9925$ with a KS p-value of 0.958. The finding is that the research in PQC has a distinguishable publication core, but literature is still scattered in neighbouring fields like networking, hardware, mathematics, IoT, information systems, and applied security.

4.4. Institutional and Geographic Structure

The affiliation ranking reveals high institutional concentration in China, the USA, India, South Korea and France. The Chinese Academy of Sciences is the top author with 84 articles, followed by the State University System of Florida with 63 articles. Others include Florida Atlantic University, the NIT System, Tsinghua University, and the University of Chinese Academy of Sciences. The distribution suggests that PQC has grown up around the institutional ecology of cryptography, hardware, communications, and computer-security.

Table 5
Most Relevant Affiliations

Affiliation	Articles
Chinese Academy of Sciences	84
State University System of Florida	63
Florida Atlantic University	37
National Institute of Technology (NIT System)	36
Tsinghua University	32
University of Chinese Academy of Sciences, CAS	32
Indian Institute of Technology System (IIT System)	28
Kookmin University	28
Centre National de la Recherche Scientifique (CNRS)	27
Nanjing University of Aeronautics and Astronautics	25

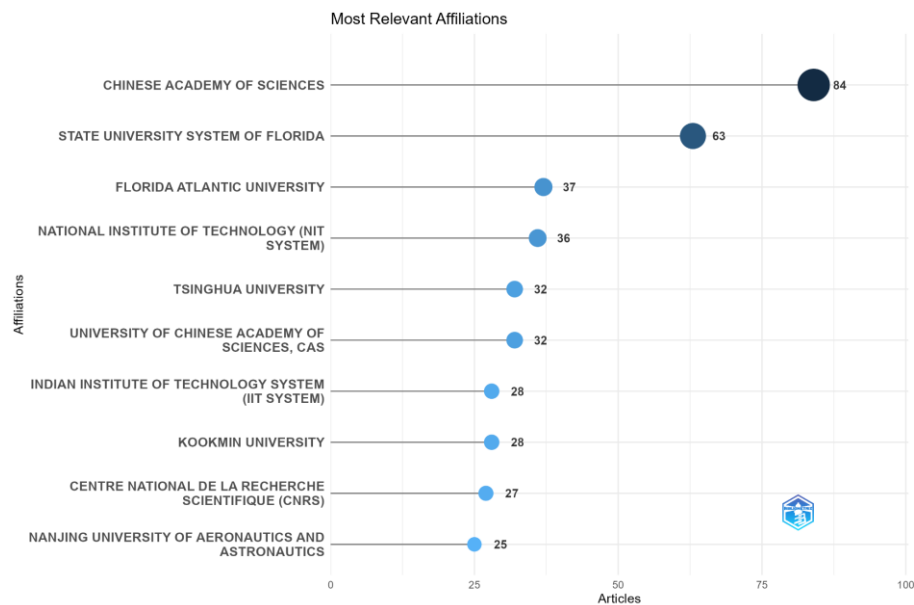


Figure 8. Most Relevant Affiliations

Country Scientific Production

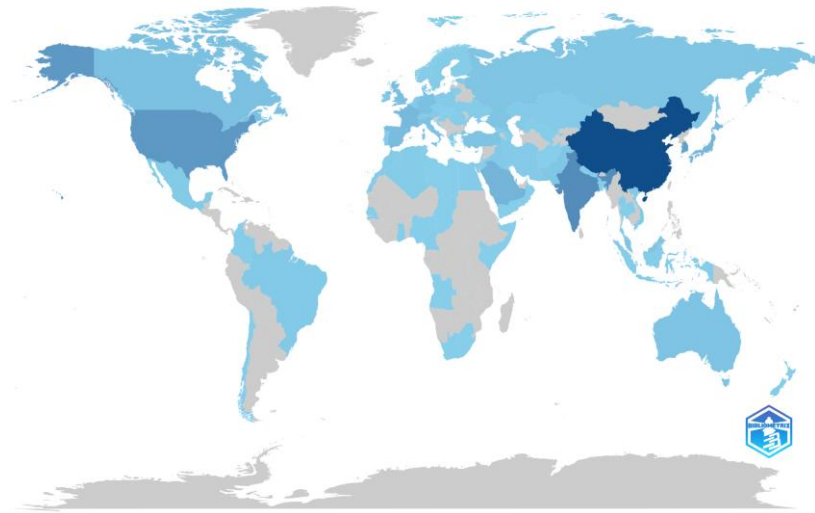


Figure 9: Country Scientific Production

The country-production map shows that there is widespread international involvement, but strong geographical asymmetry. China is the most active producer, with the United States and India also active. The second tier extends to Europe, East Asia, Canada, Australia and some of the emerging research economies. The diversity of participants shows the importance of the security services of quantum computers, and the fact that the participants are concentrated in a few countries demonstrates that the development of the quantum security market is still influenced by the availability of cryptographic know-how, hardware laboratories, cybersecurity courses, and standardization networks.

Table 6
Most Cited Countries

Country	Citations
China	3331
USA	2313
Korea	1029
India	1026
United Kingdom	458
Japan	341
Spain	295
Italy	275
France	271
Canada	260

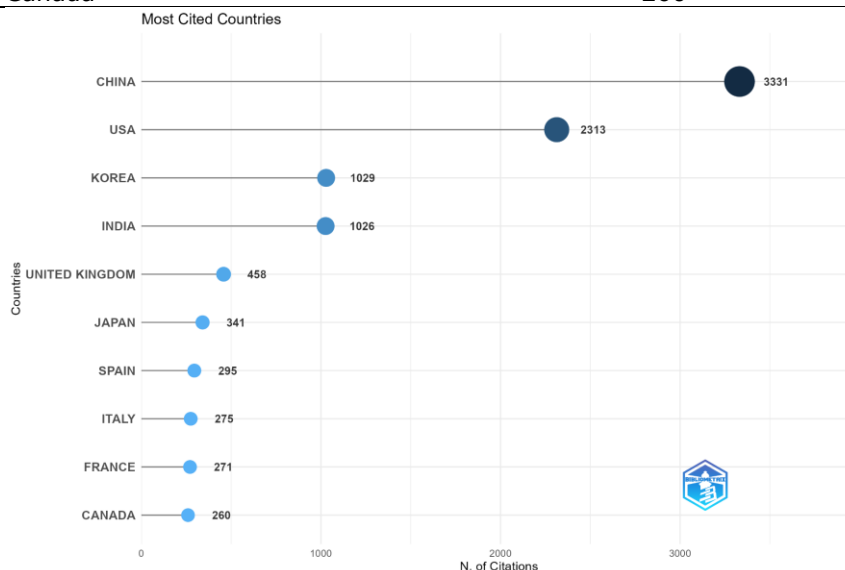


Figure 10: Most Cited Countries

Influence of citation is even more focused than geographic participation. The top countries for citations are China (3,331) and the United States (2,313). Korea and India have more than 1000 citations, while the United Kingdom, Japan, Spain, Italy, France and Canada rank in between. The finding validates that the field is early influenced by the interaction of systems in East Asia, North America, and select European systems. It also indicates that India has emerged as a big contributor both in output as well as citation visibility.

4.5. Influential documents and the intellectual base

The citation ranking shows that the intellectual base is anchored in implementation surveys, migration strategy, IoT security, FPGA acceleration, and efficient lattice/isogeny implementations. The most cited document in the data set is Nejatollahi et al. (2019), followed by Joseph et al. (2022). As can be seen, a work by Cheng et al. (2017) is among the most cited works, which shows that IoT security was early identified as a quantum-transition issue. In the body of knowledge of this field, several works by Koziel et al. (2017) are well cited that deal with practical isogeny and lattice implementations, thereby highlighting the importance of implementation engineering. The ranking also indicates a transition from algorithm feasibility to deployment and transition in which organizational migration and security are playing more of a role.

Table 7:
Ten Most Cited Documents in the Web of Science Corpus

Author(s)	Year	Document	Source	WoS citations
Nejatollahi et al.	2019	Post-Quantum Lattice-Based Cryptography Implementations: A Survey	Computing Surveys	199
Joseph et al.	2022	Transitioning organizations to post-quantum cryptography	Nature	189
Cheng et al.	2017	Securing the Internet of Things in a Quantum World	Ieee Communications Magazine	157
Koziel et al.	2017	Post-Quantum Cryptography on FPGA Based on Isogenies on Elliptic Curves	Ieee Transactions on Circuits and Systems I-Regular Papers	148
Anastasova et al.	2021	Fast Strategies for the Implementation of SIKE Round 3 on ARM Cortex-M4	Ieee Transactions on Circuits and Systems I-Regular Papers	146
Liu et al.	2019	Optimized Schoolbook Polynomial Multiplication for Compact Lattice-Based Cryptography on FPGA	Ieee Transactions on Very Large-Scale Integration (Vlsi) Systems	119
Bisheh-Niasar et al.	2021	Instruction-Set Accelerated Implementation of CRYSTALS-Kyber	Ieee Transactions on Circuits and Systems I-Regular Papers	110
Wang et al.	2021	Experimental authentication of quantum key distribution with post-quantum cryptography	Npj Quantum Information	106
Dam et al.	2023	A Survey of Post-Quantum Cryptography: Start of a New Race	Cryptography	103
Xin et al.	2020	VPQC: A Domain-Specific Vector Processor for Post-Quantum Cryptography Based on RISC-V Architecture	Ieee Transactions on Circuits and Systems I-Regular Papers	95

4.6. Keyword Structure and Thematic Positioning

The most frequent keywords are post-quantum cryptography (739), cryptography (218), security (208), lattice-based cryptography (134) and quantum computing (122). NIST is mentioned 97 times, which is a testament to the field-shaping influence of the standardization process. Another feature is the presence of blockchain, encryption and

Keyword	Occurrences
Post-quantum cryptography	739
cryptography	218
security	208
lattice-based cryptography	134
quantum computing	122
NIST	97
post-quantum cryptography (PQC)	86
encryption	81
blockchain	80
hardware	68



13

mathematical, hardware, protocol and application terms. It also suggests that the current PQC focus is more on embedding primitives as part of trustworthy systems.



Figure 13: Word Cloud of Dominant Keywords

The word cloud is an additional descriptive visualization, and not a stand-alone inferential result. Its visual hierarchy helps to emphasize the centrality of post-quantum cryptography, security, cryptography, lattice-based cryptography, quantum computing, NIST, blockchain, and authentication. Cloud is helpful because it helps to recognize the identity of the field right away: PQC research is at the same time mathematical, engineering-oriented, and cybersecurity-driven.

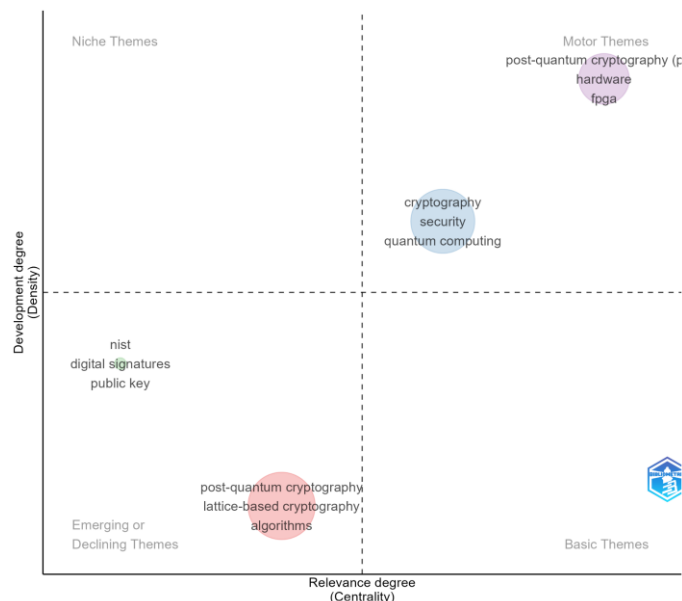


Figure 14: Thematic Map Based on Keyword Centrality and Density

The thematic map distinguishes between themes which are highly developed and central themes from themes which are less consolidated or emerging. The hardware-oriented PQC cluster, comprising post-quantum cryptography, hardware, and FPGA, dominates the upper-right motor-theme area, a cluster that is also larger than the other, encompassing cryptography-security-quantum computing. This means that implementation efficiency and hardware realization are not secondary issues but are main drives in the field. The lower-left emerging/declining region shows clusters of lattice-based cryptography, algorithms, NIST, digital signatures, and public key with lower density or centrality based on the mapping parameters used. The following positions are not mechanically understood as substantive decline. While the research is still going strong, older names can be moved into apparently weaker quadrants by lexical fragmentation, standard renaming, or by

changing from the generic “lattice-based cryptography” to the specific standardized names like ML-KEM and ML-DSA.

4.7. Topic Evolution and Co-occurrence Structure

The trend-topic analysis clearly shows a course of historical development. Previous studies focused on multivariate public-key cryptosystems, provable security, quantum cryptanalysis, oblivious transfer, computational complexity, McEliece, Rainbow, and isogeny-based cryptography. Around 2022-2023, cryptanalysis, lattice-based cryptography, hardware, and algorithms became prominent. The most prominent words in 2024 were post-quantum cryptography, cryptography, and security. The frontier shifted towards blockchain, authentication and CRYSTALS-Kyber in 2025. This series shows the evolution of the field from candidate families to standard lattice-based mechanisms and deployment in a specific domain.

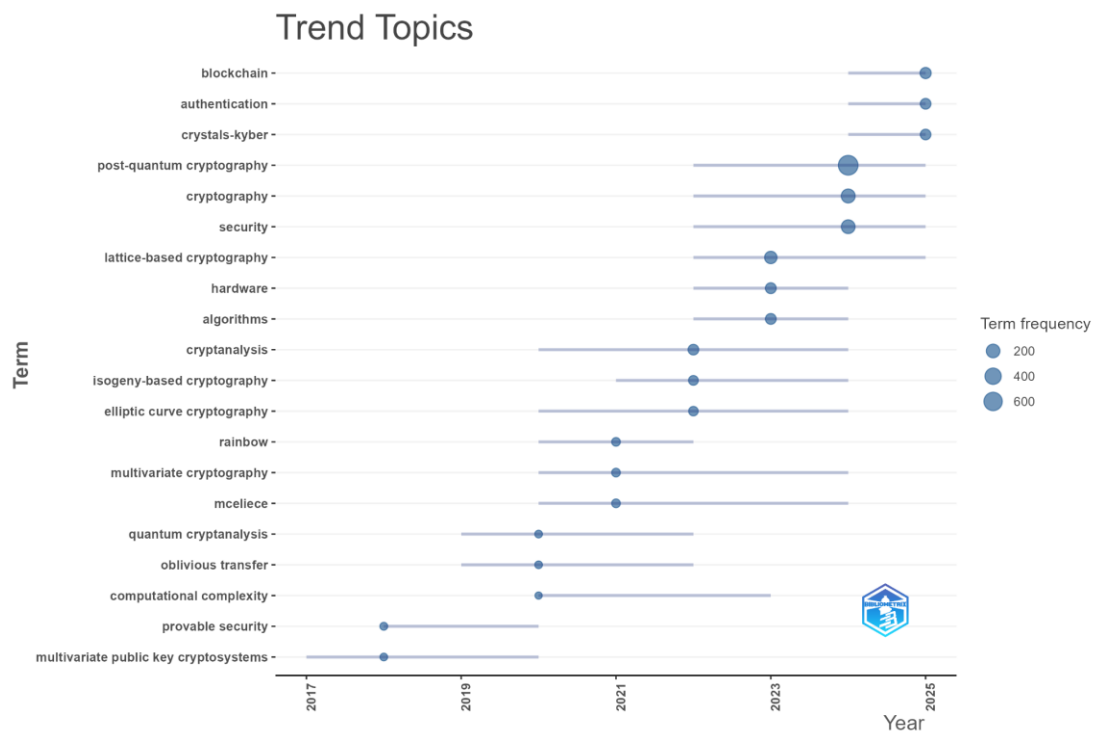


Figure 15. Trend Topics Across the Development of Post-quantum Cryptography Research

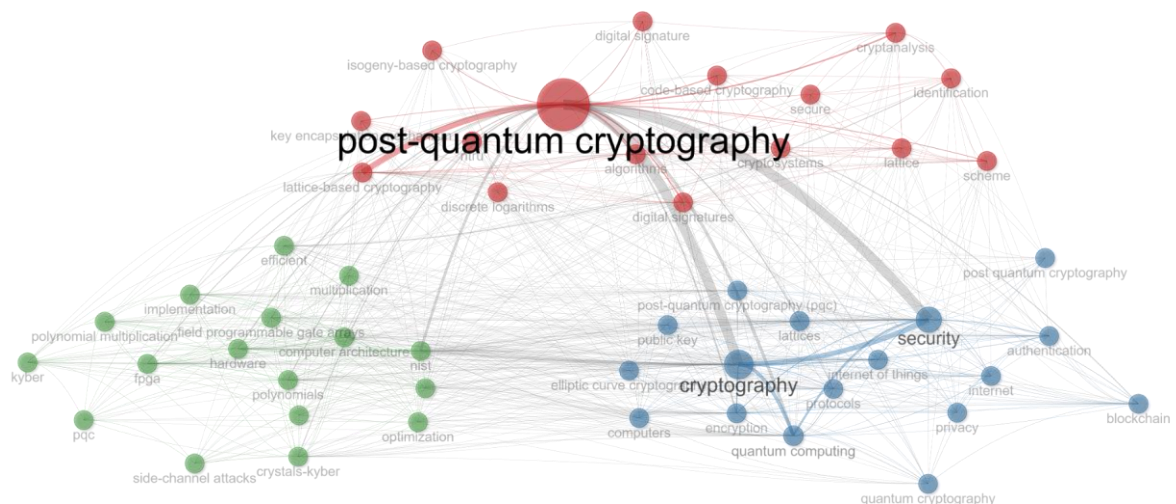


Figure 16: Keyword Co-occurrence Network

The co-occurrence network brings together thematic interpretation in three broad connected networks. One cluster focuses on post-quantum cryptography and its algorithmic/standardization terminology, a second cluster relates closely to security, cryptography, public-key mechanisms, and quantum-computing issues, and a third cluster is strongly associated with hardware implementation, FPGA, computer architecture, and efficiency. High connectivity between clusters indicates that these areas are not independent. In PQC research, mathematical security, system-level cybersecurity, and implementation performance are all becoming fundamental and must be addressed simultaneously. The network thus enables a systems approach to quantum-safe migration, where algorithmic, protocol, hardware and operational security practices are co-evolving.

5. Discussion

The results indicate that PQC has transitioned from a relatively small specialist field to a quickly expanding field in cybersecurity. The production curve is particularly telling production was in single digits in the mid-2010s but started to surge after 2022, reaching 456 records in 2025. This increase is in line with NIST's timeline for evaluating candidates and releasing FIPS 203, 204 and 205. The research incentive system seems to have been altered due to the standardization. Much of the literature prior to the finalization of the standards dealt with candidate algorithms, mathematical assumptions, cryptanalysis and comparative implementation. Post-standardization, literature has begun to focus on implementation of quantum-safe algorithms in practical systems, controlling the overhead of these algorithms, and mitigating migration risk.

This interpretation is backed up by the intellectual basis. Implementation surveys, FPGA and processor acceleration, IoT security and organizational transition are highly cited work. Nejatollahi et al. (2019) created a significant synthesis of implementation issues for lattice-based PQC, and Joseph et al. (2022) repackaged PQC as an organizational transition challenge. The high number of references to Cheng et al. (2017) and Liu et al. (2018) indicates that before standardization, concerns about IoT and edge-security dominated, with long-lived and resource-constrained devices being especially vulnerable to cryptographic obsolescence. Recent research takes the same reasoning and applies it to the realm of distributed energy resources, healthcare, blockchain, consumer devices and cloud-connected systems.

The distributions of the sources and authors show maturity and fragmentation. Just over 75% of the authors only appear in a single paper, and 269 sources fall into Bradford's third zone; a small number of highly productive authors and a small 12-source Bradford core indicate an identifiable research nucleus. This is common in an area that is at the intersection of cryptography, circuits, computer architecture, embedded systems, networking, IoT, blockchain, and cybersecurity. The benefit of diversity is that it enables rapid cross domain innovation, the drawbacks are that the evaluation criteria can become inconsistent. Throughput may be the focus of a hardware paper, latency may be the focus of an application paper, security reductions may be the focus of a cryptographic paper, and governance may be the focus of a migration paper. Future progress will need shared benchmarks that recognize and link these dimensions of progress together, as opposed to optimizing each dimension individually.

The keyword and thematic results reveal lattice-based cryptography as the predominant technical foundation but also indicate that the field's language is evolving. There are generic terms like lattice-based cryptography, algorithms and post-quantum cryptography as well as terms like blockchain and authentication that refer to applications. This change is in line with the standardization of ML-KEM and ML-DSA. However, as standardised names percolate through protocols and products, bibliometric analyses will need to increasingly normalize synonymous or transitional terminology (such as Kyber and ML-KEM, or Dilithium and ML-DSA) to prevent breaking a single technical lineage into multiple nodes of keywords.

Hardware is not a special implementation detail; it's a motor theme. The strong presence of FPGA, computer architecture, hardware, and implementation is indicative of the need for quantum-resistant security to be applicable to a variety of platforms. The studies related to polynomial multipliers, instruction-set acceleration, embedded processors and

GPU acceleration all show that performance engineering is now a first-class security requirement. Meanwhile, side-channel studies like Huang et al. (2024) and lightweight IoT cryptosystems like Ma et al. (2024) demonstrate that the assessment of acceleration should not be done in isolation and is coupled with physical leakage and implementation assurance. However, in the post-standardization world it will no longer be a question of whether an algorithm can be made to run, but rather if it can be made to run securely under realistic attack models and operational constraints.

The trend analysis also reveals the move towards application-layer cyber security. Authentication, CRYSTALS-Kyber and Blockchain are prominent in the latest period. This aligns with the efforts to incorporate quantum-safe protocols into Hyperledger Fabric, decentralized systems, TLS, PKI, and IPsec (Abbas et al., 2025). Hybrid designs are especially critical during the transition period when organizations can't change all classical cryptography at once. Rubio García et al. (2024) and Rubio García et al. (2025) demonstrate how PQC can be layered with existing security protocols and in some instances, QKD. Such methods are likely to gain more influence as migration moves from prototype to production systems.

The bibliometric results also bear significance to the novelty of the PQC mapping research itself. Starting with the year 2025, Hasija et al. (2025) already present a general bibliometric study of PQC based on Scopus. The present study, therefore, is valuable for its distinct database, more recent time, non-standardized angle, productivity-law analysis, and clear interpretation of implementation and migration to cybersecurity. This study does not suggest that the field has not been mapped before, rather it is offering an updated snapshot that is more deployment oriented. This is a more defensible and useful position for the researchers and practitioners who need to determine where new work can be useful.

6. Future Research Agenda

First, crypto-agility and migration engineering should be the focus of future research. There is a need for inventories of cryptographic dependencies, methods for algorithm substitution, hybrid transition methods and rollback strategies that maintain interoperability. Research needs to shift focus from one-time migration to measurable crypto-agility maturity models, which can be evaluated across industries and associated with software bills of materials (SBOMs), certificate infrastructures, hardware roots of trust, and enterprise risk management (ERM) (Barker et al., 2026; Hasan et al., 2024).

Secondly, more attention must be paid to implementation assurance. However, there are still ways to attack standardized algorithms, including side channels, weak randomness, faulty parameter handling, memory errors and insecure protocol integration. Future work should involve setting up repeatable leakage limits for microcontrollers, FPGA, CPU, GPU and trusted hardware, and reporting the leakage and the secure implementation overhead, power consumption, electromagnetic leakage, timing, and masking costs, and fault resistance. Security/Resource should be the objective, not simply throughput.

Third, the deployment in sectors should be strengthened. IoT, healthcare, smart grids, industrial control, cloud platforms, mobile devices and blockchain have unique constraints. Future standards (HQC/FALCON) should be evaluated in studies in the context of realistic message sizes, certificate chains, constrained memory, and intermittent connectivity, as well as lifecycle update requirements. The need for cross-layer experiments is particularly acute as algorithm benchmarks do not necessarily translate to application-level performance.

Fourth, hybrid and interoperable protocol design deserves systematic comparison. Classical-plus-PQC and PQC-plus-QKD configurations can minimise transition risk but are more complex and add new failure modes and larger messages. Research should involve comparisons of hybrid constructions with the same threat model and formal security analysis, as well as measuring handshake latency, bandwidth, state management, downgrade resistance, operational recoverability.

Fifth, evidence in the field is needed with respect to post-quantum blockchain and distributed systems. Feasibility has been demonstrated through current studies, but additional efforts are needed to increase signature size, expand states, improve consensus performance, increase validator throughput, facilitate key rotation, ensure smart-contract compatibility, and provide long-lived ledger verification. The same questions apply for archival signatures, electronic voting and digital identity: How long will the records be needed to be verifiable?

Finally, future bibliometric studies need to standardize terminology and explicitly differentiate between candidate names prior to standardization and candidate names after standardization. It is recommended to track Kyber/ML-KEM, Dilithium/ML-DSA, SPHINCS+/SLH-DSA and Falcon/FN-DSA as connected concepts. The longitudinal science mapping may then be able to assess if science moves from algorithm development to migration, compliance, product assurance and evidence of real-world incidents after 2026.

Table 9
Priority Agenda for Post-quantum Cybersecurity Research

Priority	Current gap	Recommended research direction
Crypto-agility and migration	Limited evidence on enterprise-wide replacement and dependency management	Develop measurable migration maturity models, cryptographic inventories, dependency graphs, hybrid transition strategies, and rollback mechanisms.
Implementation assurance	Performance studies often separated from physical-security evaluation	Benchmark timing, power, EM leakage, masking, fault resistance, randomness, and secure implementation overhead across platforms.
IoT and edge security	Resource constraints can make standardized PQC difficult to deploy	Evaluate ML-KEM/ML-DSA/SLH-DSA on constrained devices under realistic network, memory, energy, and updating conditions.
Network protocols	Hybrid designs add complexity and interoperability risks	Compare classical-PQC and PQC-QKD TLS/IPsec designs using consistent security and performance metrics.
Blockchain and digital identity	Signature and key growth can affect long-lived distributed systems	Study consensus, storage growth, key rotation, archival verification, and migration of legacy ledgers/identities.
Hardware acceleration	Throughput gains may increase side-channel exposure	Integrate acceleration with side-channel/fault countermeasures and report security-per-watt/security-per-area metrics.
Standards evolution	Terminology and algorithm names are changing after standardization	Track Kyber→ML-KEM, Dilithium→ML-DSA, SPHINCS+→SLH-DSA, and future HQC/FN-DSA adoption longitudinally.

7. Theoretical, Methodological, and Practical Implications

According to the study, PQC should be thought of more and more as a socio-technical transition than a small family of cryptographic algorithms. The bibliometric structure is related to mathematical security, hardware architecture, protocols, application domains and organizational migration. This systems perspective is also the reason why “security” and “hardware” are key topics in addition to lattice-based cryptography, and why recent areas like authentication and blockchain become prominent following standardization. Future conceptual efforts can thus be combined with cryptographic strength and implementation assurance, interoperability, lifecycle governance and migration readiness.

As for methodology, the paper shows the usefulness of the combination of performance analysis, Lotka and Bradford laws, citation geography, thematic maps, trend topics and co-word networks. There is no single bibliometric indicator that is sufficient. Publication counts provide evidence of growth, citation counts provide evidence of influence, and keyword maps provide evidence of conceptual organization—but are sensitive to terminology, and citation counts are biased by time. Analyses of this type, coupled with others, provide a more balanced picture of a rapidly changing technical area.

From a practical standpoint, the results show that it is not too soon for cyber security organizations to plan for a quantum-computing threat. The research frontier has already progressed to implementation, migration, hybrid protocols, side channel resilience, IoT, blockchain and crypto-agility. Security leaders should thus map their cryptographic exposures, list all the sensitive data that will be affected for a long time, and benchmark standardized PQC mechanisms and map out replacement routes. Researchers can help this by reporting deployment-oriented evidence instead of benchmarks that are based on algorithms.

8. Limitations

There are several limitations in this study. First, it relies on the Web of Science Core Collection; relevant papers indexed only in Scopus, IEEE Xplore, ACM Digital Library, arXiv, or other repositories may be omitted. Second, the search strategy intentionally uses broad PQC terminology and may under-retrieve papers that focus only on standardized algorithm names without explicitly using a post-quantum or quantum-resistant descriptor. Third, the source file provided for analysis was already merged and duplicated, so the pre-deduplication retrieval count could not be reconstructed for a conventional PRISMA duplicate-removal step. Fourth, citation counts favor older publications and should not be treated as direct measures of quality. Fifth, author and institution names may contain abbreviation or disambiguation issues. Finally, 2026 is an incomplete publication and citation year; its output should not be compared mechanically with full years. Future studies should combine multiple databases, apply controlled thesauri for standardized algorithm names, and replicate the mapping after additional post-standardization adoption data become available.

9. Conclusion

This bibliometric analysis traces the 1346 Web of Science articles related to post-quantum cryptography from the year 2015 to 2026 and reveals a field in rapid change. After 2021, the number of publications increased rapidly, reaching 456 in 2025. The literature is scattered and there are several core journals, institutions, and authors who provide visible intellectual leadership in cryptography, hardware, networking, IoT, blockchain, embedded systems, and cybersecurity. The top two countries in terms of citation influence are China and the United States, followed by Korea and India.

More important than growth statistics are conceptual evidence. The main terms used for lattice-based cryptography, security, quantum computing, hardware, NIST, blockchain, authentication, and CRYSTALS-Kyber, are the focus. The trend topics show a moving from multivariate cryptography, provable security, cryptanalysis, McEliece to isogeny-based work, lattice-based implementation, hardware, standardized algorithms, blockchain to authentication. Thematic and network analyses reveal that hardware and security are not side applications but are closely connected with the cryptographic core.

It is now a new era of post-quantum research agenda. However, the identification of quantum-resistant algorithms is no longer the main challenge. It is to deploy in a secure manner standardized mechanisms in real systems, with performance, interoperability, updatability and resilience to classical implementation attacks. Migration dependencies, hybrid protocols, IoT constraints, blockchain redesign, and lifecycle governance are likely to be the next areas of research in the context of crypto-agility and migration dependencies. This opens possibilities for cross-layer research, which links cryptographic design with systems security. The evidence suggests early, planned migration should be done in a structured way, instead of waiting for quantum risk to be immediate, for practitioners and policymakers.

References

- Abbas, S., Sultana, A., & Kaddoum, G. (2025). Quantum-Safe Blockchain in Hyperledger Fabric. *IEEE Networking Letters*, 7(1), 61-65.
<https://doi.org/https://doi.org/10.1109/LNET.2024.3522966>
- Ahn, J., Kwon, H.-Y., Ahn, B., Park, K., Kim, T., Lee, M.-K.,...Chung, J. (2022). Toward Quantum Secured Distributed Energy Resources: Adoption of Post-Quantum Cryptography (Pqc) and Quantum Key Distribution (Qkd). *Energies*, 15(3), .
<https://doi.org/https://doi.org/10.3390/en15030714>
- Alagic, G., Bros, M., Ciadoux, P., Cooper, D., Dang, Q., Dang, T.,...Smith-Tone, D. (2025). *Status Report on the Fourth Round of the Nist Post-Quantum Cryptography Standardization Process (Nist Ir 8545)*. <https://doi.org/10.6028/NIST.IR.8545>
- Anastasova, M., Azarderakhsh, R., & Kermani, M. M. (2021). Fast Strategies for the Implementation of Sike Round 3 on Arm Cortex-M4. *IEEE Transactions on Circuits and Systems I: Regular Papers*, 68(10), 4129-4141.
<https://doi.org/https://doi.org/10.1109/TCSI.2021.3096916>

- Aria, M., & Cuccurullo, C. (2017). Bibliometrix : An R-Tool for Comprehensive Science Mapping Analysis. *Journal of Informetrics*, 11(4), 959-975.
<https://doi.org/https://doi.org/10.1016/j.joi.2017.08.007>
- Barker, E., Chen, L., Cooper, D., Moody, D., Regenscheid, A., Souppaya, M.,...Barker, W. C. (2026). *Considerations for Achieving Crypto Agility: Strategies and Practices (Nist Cswp 39upd1)*. <https://doi.org/10.6028/NIST.CSWP.39-upd1>
- Bauch, J., Bernstein, D. J., de Valence, H., Lange, T., & Van Vredendaal, C. (2017). Short Generators without Quantum Computers: The Case of Multiquadratics. Annual International Conference on the Theory and Applications of Cryptographic Techniques,
- Bisheh-Niasar, M., Azarderakhsh, R., & Mozaffari-Kermani, M. (2021). Instruction-Set Accelerated Implementation of Crystals-Kyber. *IEEE Transactions on Circuits and Systems I: Regular Papers*, 68(11), 4648-4659.
<https://doi.org/https://doi.org/10.1109/TCSI.2021.3106639>
- Bradford, S. (1934). Sources of Information on Specific Subjects. *Engineering*, 10(4), .
<https://doi.org/https://doi.org/10.1177/016555158501000406>
- Chen, L., Jordan, S. P., Liu, Y. K., Moody, D., Peralta, R. C., Perlner, R. A., & Smith-Tone, D. (2016). *Report on Post-Quantum Cryptography (Nistir 8105)*.
<https://doi.org/10.6028/NIST.IR.8105>
- Cheng, C., Lu, R., Petzoldt, A., & Takagi, T. (2017). Securing the Internet of Things in a Quantum World. *IEEE Communications Magazine*, 55(2), 116-120.
<https://doi.org/https://doi.org/10.1109/MCOM.2017.1600522CM>
- Dai, R., Dong, J., Qiu, M., Dong, Z., Xiao, F., & Lin, J. (2025). Golf: Unleashing Gpu-Driven Acceleration for Falcon Post-Quantum Cryptography. *IEEE Transactions on Information Forensics and Security*, 20(8), 9441-9453.
<https://doi.org/https://doi.org/10.1109/TIFS.2025.3599681>
- Donthu, N., Kumar, S., Mukherjee, D., Pandey, N., & Lim, W. M. (2021). How to Conduct a Bibliometric Analysis: An Overview and Guidelines. *Journal of Business Research*, 133(09), 285-296. <https://doi.org/https://doi.org/10.1016/j.jbusres.2021.04.070>
- Hasan, K. F., Simpson, L., Baee, M. A. R., Islam, C., Rahman, Z., Armstrong, W.,...McKague, M. (2024). A Framework for Migrating to Post-Quantum Cryptography: Security Dependency Analysis and Case Studies. *IEEE Access*, 12(01), 23427-23450.
<https://doi.org/https://doi.org/10.1109/ACCESS.2024.3360412>
- Hasija, T., Ramkumar, K. R., Kaur, A., & Bali, M. S. (2025). Exploring the Landscape of Post Quantum Cryptography: A Bibliometric Analysis of Emerging Trends and Research Impact. *Journal of Big Data*, 12(9), 225.
<https://doi.org/https://doi.org/10.1186/s40537-025-01269-5>
- Huang, Z., Wang, H., Cao, B., He, D., & Wang, J. (2024). A Comprehensive Side-Channel Leakage Assessment of Crystals-Kyber in Iiot. *Internet of Things*, 27(10), .
<https://doi.org/https://doi.org/10.1016/j.iot.2024.101331>
- Joseph, D., Misoczki, R., Manzano, M., Tricot, J., Pinuaga, F. D., Lacombe, O.,...Hansen, R. (2022). Transitioning Organizations to Post-Quantum Cryptography. *Nature*, 605(05), 237-243. <https://doi.org/https://doi.org/10.1038/s41586-022-04623-2>
- Kim, H., Kim, W., Kang, Y., Kim, H., & Seo, H. (2024). Post-Quantum Delegated Proof of Luck for Blockchain Consensus Algorithm. *Applied Sciences*, 14(18), .
<https://doi.org/https://doi.org/10.3390/app14188394>
- Koziel, B., Azarderakhsh, R., Mozaffari Kermani, M., & Jao, D. (2017). Post-Quantum Cryptography on Fpga Based on Isogenies on Elliptic Curves. *IEEE Transactions on Circuits and Systems I: Regular Papers*, 64(1), 86-99.
<https://doi.org/https://doi.org/10.1109/TCSI.2016.2611561>
- Kumar, M. (2022). Post-Quantum Cryptography Algorithm's Standardization and Performance Analysis. *Array*, 15(9), .
<https://doi.org/https://doi.org/10.1016/j.array.2022.100242>
- Lawo, D. C., Abu Bakar, R., Cano Aguilera, A., Cugini, F., Imaña, J. L., Tafur Monroy, I., & Vegas Olmos, J. J. (2024). Wireless and Fiber-Based Post-Quantum-Cryptography-Secured Ipcsec Tunnel. *Future Internet*, 16(8), .
<https://doi.org/https://doi.org/10.3390/fi16080300>
- Liu, W., Fan, S., Khalid, A., Rafferty, C., & O'Neill, M. (2019). Optimized Schoolbook Polynomial Multiplication for Compact Lattice-Based Cryptography on Fpga. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, 27(10), 2459-2463.
<https://doi.org/https://doi.org/10.1109/tvlsi.2019.2922999>

- Liu, Z., Choo, K.-K. R., & Grossschadl, J. (2018). Securing Edge Devices in the Post-Quantum Internet of Things Using Lattice-Based Cryptography. *IEEE Communications Magazine*, 56(2), 158-162. <https://doi.org/https://doi.org/10.1109/MCOM.2018.1700330>
- Lotka, A. (1926). The Frequency Distribution of Scientific Productivity. *Journal of the Washington Academy of Sciences*, 16(12), 317-323.
- Ma, C., Shankar, A., Kumari, S., & Chen, C.-M. (2024). A Lightweight Brlwe-Based Post-Quantum Cryptosystem with Side-Channel Resilience for Iot Security. *Internet of Things*, 28(12), . <https://doi.org/https://doi.org/10.1016/j.iot.2024.101391>
- Nejatollahi, H., Dutt, N., Ray, S., Regazzoni, F., Banerjee, I., & Cammarota, R. (2019). Post-Quantum Lattice-Based Cryptography Implementations. *ACM Computing Surveys*, 51(6), 1-41. <https://doi.org/https://doi.org/10.1145/3292548>
- Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D.,...Moher, D. (2021). The Prisma 2020 Statement: An Updated Guideline for Reporting Systematic Reviews. *BMJ*, 372(01), . <https://doi.org/https://doi.org/10.1136/bmj.n71>
- Puneyani, V., & Bhat, K. V. (2025). Quantum-Resistant Blockchain Protocols for Secure Transactions. *IEEE Access*, 13(6), 108984-108991. <https://doi.org/https://doi.org/10.1109/ACCESS.2025.3581955>.
- Raavi, M., Khan, Q., Wuthier, S., Chandramouli, P., Balytskyi, Y., & Chang, S.-Y. (2025). Security and Performance Analyses of Post-Quantum Digital Signature Algorithms and Their Tls and Pki Integrations. *Cryptography*, 9(2), 1-38. <https://doi.org/https://doi.org/10.3390/cryptography9020038>
- Rubio García, C., Cano Aguilera, A., Stan, C., Vegas Olmos, J. J., Rommel, S., & Tafur Monroy, I. (2025). Enhanced Network Security Protocols for the Quantum Era: Combining Classical and Post-Quantum Cryptography, and Quantum Key Distribution. *IEEE Journal on Selected Areas in Communications*, 43(8), 2765-2781. <https://doi.org/https://doi.org/10.1109/JSAC.2025.3568011>
- Rubio García, C., Rommel, S., Takarabt, S., Vegas Olmos, J. J., Guilley, S., Nguyen, P., & Tafur Monroy, I. (2024). Quantum-Resistant Transport Layer Security. *Computer Communications*, 213(01), 345-358. <https://doi.org/https://doi.org/10.1016/j.comcom.2023.11.010>
- Shor, P. W. (1994). *Algorithms for Quantum Computation: Discrete Logarithms and Factoring* Proceedings 35th Annual Symposium on Foundations of Computer Science, <https://doi.org/10.1109/SFCS.1994.365700>
- Tan, T. G., Szalachowski, P., & Zhou, J. (2022). Challenges of Post-Quantum Digital Signing in Real-World Applications: A Survey. *International Journal of Information Security*, 21(8), 937-952. <https://doi.org/https://doi.org/10.1007/s10207-022-00587-6>
- van Eck, N. J., & Waltman, L. (2010). Software Survey: Vosviewer, a Computer Program for Bibliometric Mapping. *Scientometrics*, 84(8), 523-538. <https://doi.org/https://doi.org/10.1007/s11192-009-0146-3>