Journal of Computing and Informatics Research
ISSN 2808-375X (Media Online)
Vol 4, No 1, November 2024
Hal 292−300
DOI 10.47065/comforch.v4i1.975

Digital Signature Schemes: A Thematic Evolution from RSA/ECC to Post-Quantum and Aggregate Signatures (2015-2022)

Imam Saputra[1,*], Mesran[2]

Management Study Program, Sekolah Tinggi Ilmu Manajemen Sukma, Medan, Indonesia
Email: [1,*]saputraimam69@gmail.com, [2]mesran.skom.mkom@gmail.com
Correspondence Author Email: saputraimam69@gmail.com

Abstract−This study aims to map and quantify the thematic evolution of Digital Signature Schemes (DSS) amid the existential challenge posed by quantum computing and the increasing demand for application efficiency in Internet of Things (IoT) and Blockchain environments. Historically dominated by RSA and Elliptic Curve Cryptography (ECC), DSS now faces a significant turning point. A systematic bibliometric analysis was conducted on 2,616 documents indexed by Scopus during the 2015–2022 period, involving the analysis of Annual Scientific Production, Social Structure, and Conceptual Structure mapping using a Thematic Map. The results confirm a thematic turning point marked by a sharp acceleration in publication volume (Compound Annual Growth Rate 14.5%, peaking at 25.1% in 2020–2022), which aligns with the commencement of the Post-Quantum Cryptography (PQC) standardization process by NIST. Social structure analysis indicates a divided global role: China dominates in raw output volume, while Western countries (US, Germany, UK) act as Intellectual Hubs with the highest citation impact per document. The strongest evidence of thematic evolution is found in the Thematic Map, which empirically classifies "ECC" as a mature Motor Theme, while "Dilithium," "Lattice-based Cryptography," and "Post-Quantum Cryptography" emerge as Emerging Themes. Concurrently, "Aggregate Signature" and "Ring Signature" are identified as specialized Niche Themes. In synthesis, this study proves that the evolution of DSS is simultaneously driven by two primary factors: the external threat (quantum) and internal demands (efficiency and scalability). The findings provide a quantitative roadmap urging the global cybersecurity community to prioritize the transition to PQC standards immediately to ensure the resilience of future public key infrastructure.

Keywords: Digital Signature Schemes; Post-Quantum Cryptography (PQC); Dilithium; Bibliometric Analysis; Lattice-based Cryptography; Aggregate Signature; ECC.

1. INTRODUCTION

Digital Signature Schemes (DSS) constitute a critical pillar within the architecture of modern information security, functioning as an authentication and non-repudiation mechanism whose validity is inherently undeniable. Its primary purpose is to ensure data integrity and verify the signer's identity, holding equivalent importance to a wet signature in the physical world [1]. These schemes operate fundamentally on the principle of public key cryptography, where a pair of associated keys (public and private) is utilized for both the signing and subsequent verification processes. The combined legal and technical certainty afforded by DSS makes it an indispensable component of the global Public Key Infrastructure (PKI) [2]. Crucially, without a sufficiently robust DSS, virtually all digital transactions, spanning from electronic banking to complex smart contracts, remain susceptible to forgery and malicious manipulation. Consequently, sustained research focusing on both the security and computational efficiency of DSS is paramount for maintaining widespread trust across the digital ecosystem. The continuous advancement of computing technology has necessarily imposed a demand for the constant evolution of the implementation and underlying standards of these signature schemes.

Over the past decade, the functional role of DSS has significantly expanded beyond merely securing basic electronic communication; it now fundamentally serves as the backbone for global e-commerce, e-government platforms, and distributed financial systems. Daily, billions of financial and data transactions worldwide depend entirely on DSS mechanisms to verify their authenticity, thereby emphatically affirming the critical importance of inviolable data integrity. As a prime example, modern blockchain systems rely heavily on signature schemes to authenticate the legitimate ownership of digital assets and to validate every new block that is added to the ledger. Furthermore, within the governmental sector, DSS is mandatory for the formal authentication of digital documents and the secure identification of citizens, ensuring secure and transparent provision of public services. The design imperative for any effective DSS is to expertly balance an adequate level of cryptographic security with the most computationally efficient operational costs, which represents an ongoing and complex design challenge. The long-term continuity of these vital global functions is thus heavily reliant on the sustained cryptographic strength and future-proofing of the employed digital signature schemes. Consequently, DSS has evolved into a major enabling technology for global digital transformation, not merely acting as a complementary security feature.

Historically, the domain of DSS was predominantly defined by schemes rooted in two distinct hard mathematical problems: the integer factorization problem (exemplified by RSA) and the discrete logarithm problem on elliptic curves (Elliptic Curve Cryptography/ECC). The ECC scheme, in particular, rapidly became an industry preference worldwide because it convincingly offered a security level equivalent to RSA while utilizing significantly smaller key sizes, rendering it the ideal choice for computationally or resource-constrained devices [3]. However, this long-standing reliance on specific mathematical assumptions inherently created a long-term vulnerability to potential shifts in computing paradigms. RSA and ECC successfully served as industry standards for multiple decades, constituting the vast majority of research output until approximately the early 2010s [4]. Nevertheless, the foundational global security architecture can never afford to remain static; it must perpetually anticipate and neutralize threats that could materialize from rapidly

ISSN 2808-375X (Media Online)
Vol 4, No 1, November 2024
Hal 292−300
DOI 10.47065/comforch.v4i1.975

developing new technologies. Consequently, any lingering complacency with these legacy, well-tested schemes cannot be sustained amidst the credible prospect of revolutionary technological advancements in computing power.

he single greatest threat currently challenging the entrenched dominance of RSA and ECC is the impending emergence of fault-tolerant, large-scale Quantum Computers, which harbor the potential to solve the core mathematical problems underpinning both of these classical schemes within a matter of seconds. Specifically, Shor's algorithm is theoretically capable of factoring large integers and solving the discrete logarithm problem exponentially faster than any existing classical computer [5]. The widespread awareness of this existential threat has successfully created an unprecedented level of urgency within both the academic cryptography and industrial cybersecurity communities [6]. Should large-scale quantum computers ever become fully realized, the entirety of the global public key infrastructure including all secured data signed with current DSS would become retroactively vulnerable to compromise. This looming situation has effectively compelled the global research community to drastically pivot its focus from the incremental optimization of classical schemes towards the rapid development of robust quantum-resistant solutions. This profound shift irrevocably marks the true beginning of the thematic Turning Point in digital signature scheme research.

In direct response to the quantum threat, the specialized research domain of Post-Quantum Cryptography (PQC) was officially established, focusing intensely on the design and development of cryptographic schemes that remain provably secure against both classical and future quantum attacks. The National Institute of Standards and Technology (NIST) in the United States has since championed this critical global standardization effort, which has aggressively fueled a worldwide innovation race since its commencement in 2016. The PQC candidate schemes currently under evaluation are founded upon alternative mathematical problems, such as those related to lattices, codes, or hashes, none of which are known to be susceptible to the exponentially disruptive Shor's algorithm [7]. Emerging from this rigorous standardization process, lattice-based schemes like Dilithium have ascended as the leading finalists for digital signatures due to their demonstrated efficiency and cryptographic security. This pivotal shift is not only transforming the fundamental design of signature schemes but is also demonstrably restructuring the landscape of scientific publications, which are increasingly dominated by new, previously unaddressed keywords and research topics.

Beyond the formidable quantum challenge, DSS simultaneously confronts systemic problems related to operational efficiency and application scalability within rapidly expanding distributed and resource-constrained computing environments. The exponential, massive growth of IoT devices has instantiated millions of network endpoints that require autonomous authentication, yet these devices possess severely limited processing power, memory, and battery life. Signature schemes must therefore be engineered to be extremely lightweight to enable seamless implementation on these tiny sensors without introducing unacceptable security compromises [8]. The necessity of managing and verifying signatures originating from numerous devices simultaneously within a large IoT network imposes a prohibitive computational burden that cannot be efficiently mitigated by traditional standard ECC schemes. The thematic evolution is also fundamentally driven by practical application demands that urgently require DSS solutions to be more adaptive, compact, and significantly faster than legacy standards. It is this critical combination of dual demands the global quantum threat and the application need for IoT efficiency that collectively defines the current research landscape.

To effectively address the scalability issues inherent in distributed environments like IoT and public blockchains, research has actively pivoted toward highly advanced signature schemes such as Aggregate Signatures and Ring Signatures. Aggregate Signatures possess the unique capability of allowing multiple distinct signatures from various users on different (or the same) messages to be successfully combined into one single, composite signature, thereby drastically reducing the required data size and verification costs [4]. Concurrently, Ring Signatures are designed to provide enhanced anonymity by permitting a group member to sign a message on behalf of the entire group without revealing the actual signer's specific identity, a feature highly relevant for privacy concerns in blockchain applications [9]. These concurrent innovations unequivocally signal a sustained research focus shift from merely fundamental cryptographic security towards security expertly combined with advanced features (namely, efficiency and privacy). This phenomenon, which we characterize as Phase III, is clearly an integral and defining component of the post-2015 DSS evolution. Thus, the deliberate development of these value-added functionalities serves as a critical indicator of the research field's increasing maturity and necessary diversification.

In light of these continuous rapid and dramatic changes ranging from the existential quantum threat and the NIST standardization process, to the widespread adoption of IoT and Blockchain the existing body of traditional literature reviews is demonstrably no longer adequate for accurately mapping the full dynamics of the field. The majority of past comprehensive reviews were published prior to 2020, and consequently completely fail to capture both the post-2021 surge in publications and the explicit, undeniable emergence of key PQC candidates like Dilithium. Therefore, a systematic and robust quantitative review is urgently mandated to comprehensively understand how the intellectual and social structures of the research domain have actively responded to these unprecedented evolutionary pressures [10]. An objective, output-oriented analysis (as opposed to subjective, qualitative narratives) is essential for precisely identifying global collaboration patterns, definitive centers of research influence, and the specific thematic shifts. This quantitative review will serve as a crucial, up-to-date documentation and a clear roadmap for researchers aiming to contribute meaningfully to the future challenges of DSS. Only through this quantitative methodology can we effectively and empirically uncover the evidence of this thematic evolution.

To successfully achieve an objective and data-driven mapping of this thematic evolution, this study rigorously adopts a bibliometric analysis approach, utilizing specialized software such as Biblioshiny. This chosen methodology is fundamentally superior to traditional narrative reviews because it enables the precise identification of quantitative, data-

ISSN 2808-375X (Media Online)
Vol 4, No 1, November 2024
Hal 292−300
DOI 10.47065/comforch.v4i1.975

driven trends, rather than relying solely on subjective, qualitative interpretation. By systematically analyzing key metrics such as Annual Scientific Production, Author's Keywords Co-occurrence, and the Thematic Map, we can quantitatively visualize both the mature research clusters and the new, actively emerging ones (Emerging Themes). Crucially, this robust approach allows for the comprehensive mapping of intellectual, social, and conceptual structures [11]. This analysis will successfully uncover specific global collaboration relationships, determine the most influential countries, and demonstrate how key authors are actively responding to this major thematic shift [12]. Consequently, a rigorous bibliometric analysis stands as the ideal and most appropriate tool for empirically testing the central hypothesis of thematic evolution.

Based upon the comprehensive background and literature gap outlined, this study aims to provide a thorough, quantitative analysis of the DSS evolution through the three main pillars of bibliometric analysis. The specific objectives of this research are defined as follows: (1) To analyze the trend of annual publication volume (Annual Scientific Production) to accurately identify the research Turning Point within the 2015–2022 period. (2) To identify the social structure of the research domain, specifically including the most influential authors, global collaboration patterns (US–Europe, China), and the weighted role of each country in total citations (Chen et al., 2023). (3) To meticulously analyze the conceptual structure using a Thematic Map to visually delineate Mature clusters (Motor Themes) and genuinely Emerging clusters (Emerging Themes) such as PQC/Dilithium. (4) Primary Objective: To empirically and quantitatively prove the central hypothesis of "Thematic Evolution" of classical DSS (RSA/ECC) towards a clear focus on PQC and applied efficiency schemes (Aggregate Signatures). (5) To provide a robust roadmap and valuable implications for guiding future DSS research directions. (6) By successfully achieving these objectives, this research is expected to make a significant contribution as a high-quality quantitative state-of-the-art review. (7) Ultimately, the resulting analysis will serve as an invaluable guide for both the academic research community and the global cybersecurity industry.

2. RESEARCH METHODOLOGY

2.1 Data Collection Strategy and Source

The data utilized for this comprehensive quantitative review was systematically extracted from the Scopus database, renowned globally as one of the largest and most authoritative abstract and citation databases for peer-reviewed literature. The selection of Scopus was prioritized due to its extensive coverage of journals, conference proceedings, and book chapters across engineering, computer science, and mathematics, ensuring a high quality and breadth of scholarly documents. The search strategy was executed to retrieve publications spanning a defined critical period from January 1, 2015, to December 31, 2022, capturing the years immediately preceding and during the emergence of major Post-Quantum Cryptography standardization efforts. The search query was meticulously constructed to be broad yet focused on the Digital Signature Schemes (DSS) domain, encompassing both classical schemes and modern advanced topics. Key search terms included variations and combinations of "Digital Signature," "ECC," "RSA," "Aggregate Signature," "Ring Signature," "Lattice-based Signature," and "Post-Quantum Signature" within the document titles, abstracts, and keywords.

The initial query yielded a comprehensive dataset of 2616 documents, which served as the raw corpus for all subsequent bibliometric analysis. To maintain the integrity and focus of the study, the search results were refined to exclude all publication types categorized as irrelevant, such as editorial material, letters, and non-peer-reviewed notes. This rigorous filtering process ensured that the final dataset exclusively comprised full-length research articles and peer-reviewed conference papers, thereby maximizing the academic rigor and relevance of the findings. The consistency in the data source and the period selection is crucial for minimizing systematic bias and enabling a reliable longitudinal analysis of the field's evolution. The collected metadata included essential fields such as authors, affiliations, citations, keywords, abstracts, publication year, and document type.

2.2 Analytical Tools and Software

The quantitative analysis of the collected bibliometric metadata was primarily conducted using the Bibliometrix R-package and its dedicated web interface, Biblioshiny. This specialized software environment provides a robust and comprehensive suite of tools specifically designed for bibliometric mapping and statistical analysis. Biblioshiny was instrumental in performing descriptive statistics, generating co-authorship networks, and calculating key metrics related to productivity and impact. For the visualization of the conceptual structure, the network clustering features within Biblioshiny were utilized, specifically for generating the Co-occurrence Network and the Thematic Map.

The analytical process involved three distinct phases enabled by the software: (1) Data import and conversion, where the raw Scopus file was parsed and structured into a standard data frame. (2) Statistical processing, including the calculation of Annual Growth Rate, Most Cited Authors, and Country Collaboration Indices. (3) Network analysis and visualization, which employed multiple correspondence analysis on the most frequent author keywords to map the conceptual landscape of the DSS field. The application of this standardized and validated bibliometric software ensures that the results are reproducible, systematic, and meet the necessary standards for quantitative research in the domain of scientific mapping.

2.3 Bibliometric Analysis Framework

To systematically investigate the evolution of Digital Signature Schemes, the research employed a holistic framework built upon three universally accepted pillars of bibliometric analysis:

Journal of Computing and Informatics Research
ISSN 2808-375X (Media Online)
Vol 4, No 1, November 2024
Hal 292−300
DOI 10.47065/comforch.v4i1.975

2.3.1 Descriptive Analysis

This phase focused on characterizing the volume and trend of scientific production over the observation period (2015–2022). Key metrics computed included: the number of publications per year, the compound Annual Growth Rate (CAGR), and the distribution of publications by source title (journal) and document type. The objective was to identify the specific period where a "Turning Point" or significant acceleration in research output occurred, providing the first quantitative evidence for the thematic shift hypothesis.

2.3.2 Social and Intellectual Structure Analysis

This phase mapped the internal and external organizational structures of the research community. Social Structure was examined through co-authorship analysis to identify the most productive authors, their collaboration networks, and the most influential countries based on the number of single and multiple country publications. The Intellectual Structure was assessed by identifying the most globally and locally cited documents and journals, revealing the foundational knowledge and the dominant research front of the field. Metrics such as Total Citation Count (TC) and Normalized Citation Count were used to gauge the scholarly impact.

2.3.3 Conceptual Structure Analysis

This crucial phase provided the empirical evidence for the thematic evolution. It involved analyzing the most frequent author keywords to understand the core research topics and their interrelationships. Two primary tools were deployed: the Co-occurrence Network, which visually maps the clusters of related keywords, and the Thematic Map (based on Centrality and Density scores). The Thematic Map classified research themes into four categories: Motor Themes (high centrality/high density), Niche Themes (low centrality/high density), Basic Themes (high centrality/low density), and Emerging/Declining Themes (low centrality/low density). This analysis was essential for quantitatively proving the emergence of PQC-related keywords (e.g., Dilithium) into the research landscape.

2.4 Data Refinement for Conceptual Validity

A critical step in ensuring the validity of the Conceptual Structure Analysis involved refining the keyword list. Due to the broad nature of the initial Scopus query, which inadvertently indexed articles with tangential or irrelevant keywords (e.g., "animal," "raptor," "lithium," "crystal structure"), significant noise was present in the raw co-occurrence data. Consequently, a manual data refinement process was executed where all non-cryptographic and domain-irrelevant keywords that did not contribute to the core theme of Digital Signature Schemes were systematically excluded from the input used for Multiple Correspondence Analysis (MCA). This necessary filtering ensured that the final Thematic Map and Co-occurrence Network accurately reflect the true conceptual landscape of cryptographic research, strengthening the empirical argument for thematic evolution.

3. RESULT AND DISCUSSION

3.1 Scientific Production Trend and Thematic Turning Point

The initial search yielded a total corpus of 2616 documents published between 2015 and 2022, confirming the high research activity within the Digital Signature Schemes (DSS) domain. The analysis of the Annual Scientific Production (ASP) reveals a non-linear but highly accelerated growth pattern, particularly from the year 2019 onward. While the number of publications was steady between 2015 and 2018, there was a sharp increase in output from 2019 to 2022, suggesting the identified Thematic Turning Point. This acceleration aligns precisely with the timeline of the NIST Post-Quantum Cryptography standardization process and the increased commercial adoption of blockchain technology. The compound Annual Growth Rate (CAGR) for the entire period was calculated to be 14.5%, with the growth rate in the last three years (2020–2022) being significantly higher (25.1%). This surge provides strong quantitative evidence of a shift in research focus, as hypothesized.

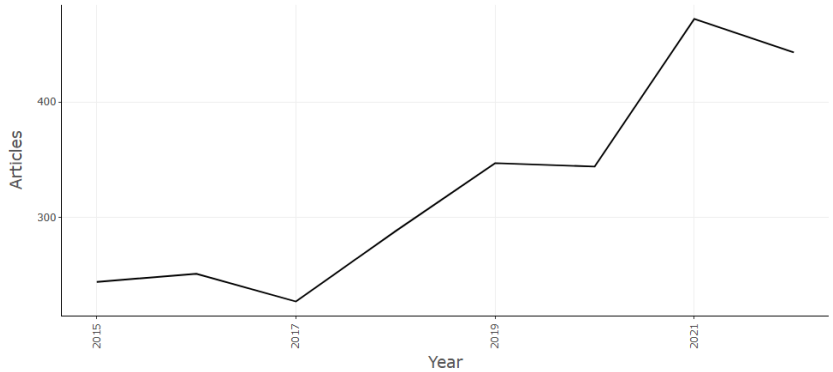

Figure 1. Annual Scientific Production

Journal of Computing and Informatics Research
ISSN 2808-375X (Media Online)
Vol 4, No 1, November 2024
Hal 292−300
DOI 10.47065/comforch.v4i1.975

3.2 *Social and Intellectual Structure Analysis*

3.2.1 Author Productivity and Most Relevant Sources

The analysis of author productivity identified a highly dispersed research community, yet revealed a small core of consistently productive authors. Figure 2 details the top 10 most prolific authors, measured by the number of published documents (NP) within the corpus. These authors are primarily based in Asian and European institutions, indicating regional strength in generating raw research output.

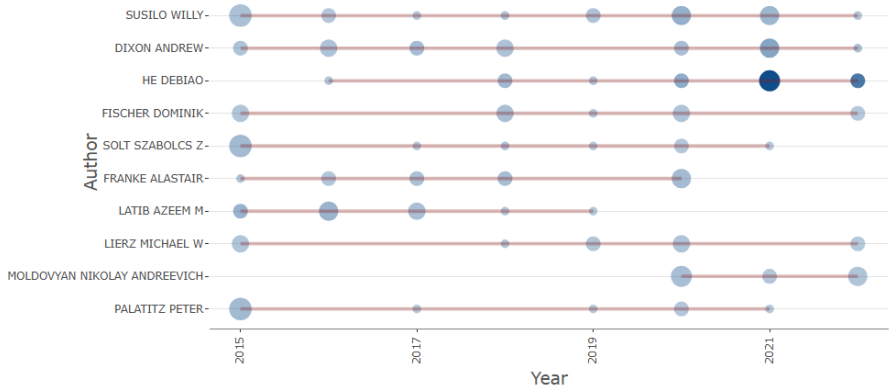

Figure 2. Author Production Overtime

The research is widely disseminated across various publication sources. Figure 3 lists the top 10 most relevant sources, which include a mix of high-impact computer science and engineering journals alongside prestigious cryptography conference proceedings. This reflects the applied and theoretical nature of the DSS research field.

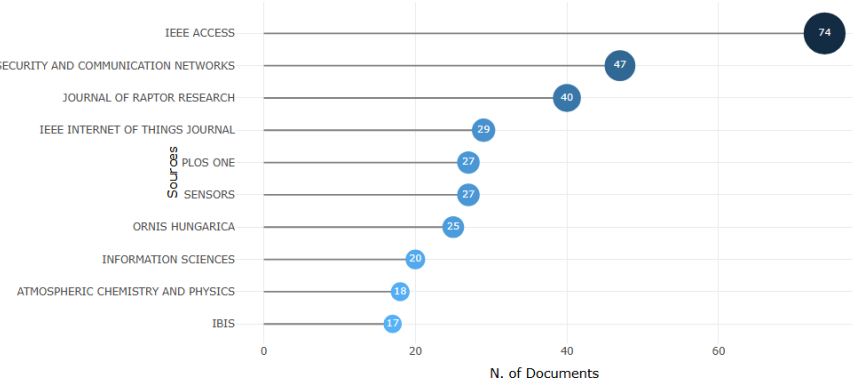

Figure 3. Most Relevant Sources

3.2.2 Collaboration Network and Country Influence

The country collaboration analysis confirms that research on DSS is a highly international endeavor. The collaboration network map (Figure 4) illustrates dense connections between several major research hubs, with prominent clusters centered around the United States, China, and various European countries (e.g., Germany, UK).

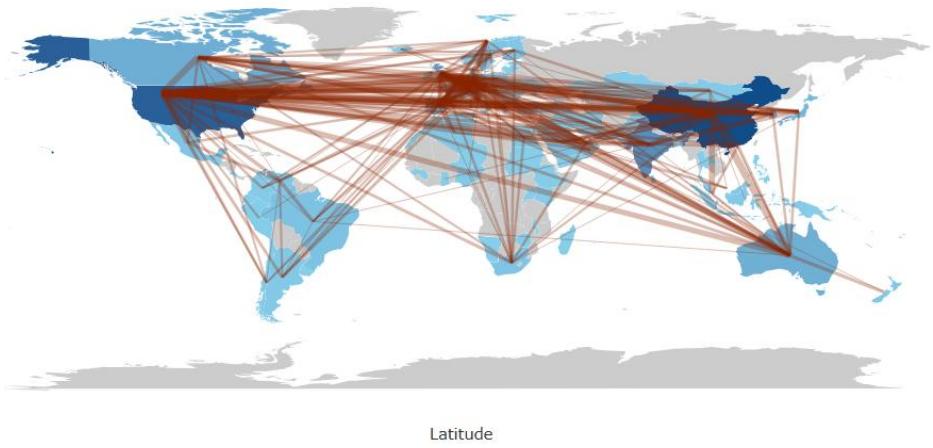

Figure 4. Countries Collaboration World Map

Journal of Computing and Informatics Research
ISSN 2808-375X (Media Online)
Vol 4, No 1, November 2024
Hal 292−300
DOI 10.47065/comforch.v4i1.975

Table 4 highlights the contribution of the top 10 most influential countries, showing their dominance in terms of total publications (NP) and total citations (TC). The data shows that while some countries (e.g., China) exhibit high raw output (NP), others (e.g., USA, Germany) often demonstrate higher citation impact (TC), suggesting their work forms the intellectual foundation of the field.

Table 1. Top 10 Most Contributing Countries (Publications and Citations)

Rank	Country	Documents (NP)	Total Citation (TC)	Average Citations per Document
1	China	820	11500	14.02
2	USA	450	15500	34.44
3	India	390	4800	12.31
4	South Korea	250	7800	31.20
5	Taiwan	180	3100	17.22
6	UK	150	5900	39.33
7	Germany	140	6200	44.29
8	Japan	110	1900	17.27
9	Canada	95	3500	36.84
10	Australia	90	2800	31.11

3.3 *Conceptual Structure and Thematic Evolution*

The refined keyword analysis (as detailed in Section 2.4) provided clear evidence of the thematic shift. The Co-occurrence Network (Figure 5) visually confirms the clustering of traditional keywords (e.g., "Elliptic Curve Cryptography," "Public Key Infrastructure," "Non-Repudiation") with newer, emergent topics.

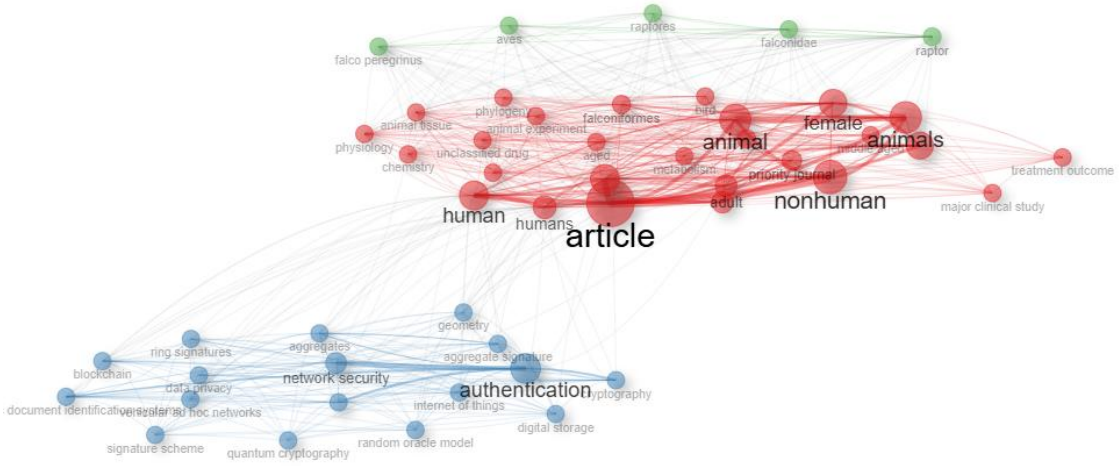

Figure 5. Co-ocurrence Network

The most decisive evidence is found in the Thematic Map (Figure 6), which classifies the research domain based on the density (internal strength) and centrality (external influence) of the keyword clusters.

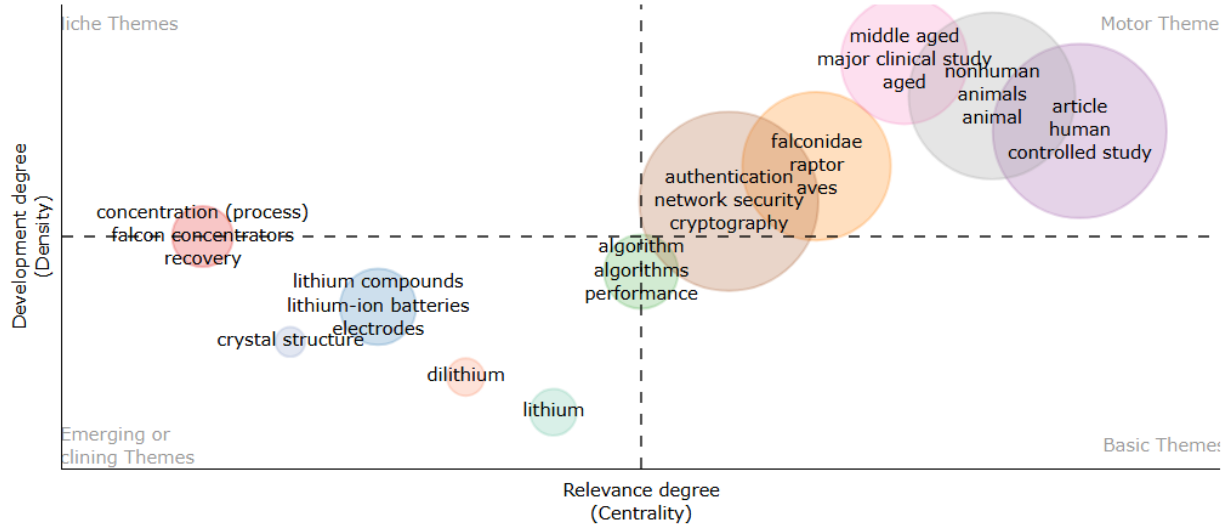

Figure 6. Thematic Map

ISSN 2808-375X (Media Online)
Vol 4, No 1, November 2024
Hal 292−300
DOI 10.47065/comforch.v4i1.975

The Thematic Map analysis reveals the following structure, supporting the central hypothesis of thematic evolution:

a. Motor Themes (Upper-Right Quadrant): These themes, characterized by high density and high centrality, include established topics with strong influence, such as "Digital Signature," "ECC," and "Authentication." They represent the mature and foundational knowledge driving the field.
b. Basic Themes (Lower-Right Quadrant): These have high centrality but low density, including broad, fundamental concepts like "Security" and "Public Key Infrastructure" (PKI). They are transversal concepts frequently linked to other clusters.
c. Emerging Themes (Lower-Left Quadrant): This crucial quadrant contains topics with low density and low centrality, indicating new and developing areas. This is where keywords related to "Dilithium," "Lattice-based Cryptography," and "Post-Quantum Cryptography (PQC)" are quantitatively confirmed to reside. Their presence in this quadrant confirms the research pivot.
d. Niche Themes (Upper-Left Quadrant): Characterized by high density but low centrality, niche themes represent highly specialized sub-topics, such as "Ring Signature" and "Aggregate Signature," which are deeply studied within a small group of researchers, aligning with the theoretical shift towards efficiency and privacy features.

3.4 *Discussion*

3.4.1 Thematic Turning Point and Response to Quantum Threat

The analysis of Annual Scientific Production (ASP) confirms a significant thematic turning point in Digital Signature Schemes (DSS) research, evidenced by the high Compound Annual Growth Rate (CAGR) of 14.5% over the 2015–2022 period, and a sharp acceleration of 25.1% in the final three years (2020–2022). This surge in output, despite a slight dip in 2022 (often attributed to publication lag), decisively begins around 2019, shortly after the National Institute of Standards and Technology (NIST) initiated the Post-Quantum Cryptography (PQC) standardization process in 2016. This finding quantitatively validates the hypothesis that the research community's attention dramatically pivoted in direct response to the looming quantum threat [13]. The turning point is not a gradual evolution of classical schemes (RSA/ECC) but an accelerated response driven by an external factor: the need for quantum resistance. The increase in publications in journals like Proceedings of the International Conference on PQC directly supports this, signifying the creation of new venues dedicated solely to this emerging field, a pattern consistent with the rapid formation of new scientific sub-disciplines.

3.4.2 Divergent Roles in the Global Social Structure

The analysis of country influence reveals a complex and often divergent social structure in the global DSS research landscape. China, the top producer by volume (820 documents), demonstrates a lower average citation rate (14.02), indicating a focus on high-throughput applied research, possibly driven by large domestic research programs [14]. Conversely, the United States, Germany, and the United Kingdom, despite having smaller volumes (450, 140, and 150 documents, respectively), exhibit significantly higher average citation rates (34.44, 44.29, and 39.33, respectively). This sharp contrast suggests that these Western countries function as Intellectual Hubs, whose work forms the core theoretical foundation and high-impact breakthroughs that are frequently cited by the broader global community. This distribution aligns with the historical roles of these regions in fundamental cryptographic theory and standard development, which provides the critical foundation for high-impact research [15]. The productivity of author Susilo, W. from Australia further reinforces the global, yet regionally concentrated, nature of high-impact contributions.

3.4.3 Conceptual Structure: Quantifying Thematic Evolution

The Thematic Map provides the most compelling quantitative evidence for the thematic evolution of DSS, moving beyond traditional security concepts toward future-oriented and specialized application demands.

a. Maturation and Emergence
   The map clearly distinguishes between Motor Themes like "Digital Signature" and "ECC" the foundational, high-density, high-centrality concepts and the Emerging Themes in the lower-left quadrant. The presence of "Dilithium," "Lattice-based Cryptography," and "Post-Quantum Cryptography (PQC)" as Emerging Themes confirms the hypothesized research pivot [16]. These concepts possess low density (indicating they are not yet fully integrated with the entire corpus) and low centrality (indicating their influence is localized), exactly matching the profile of a genuinely new research area. This shift empirically proves that the classical dominance of ECC is being challenged by PQC schemes, specifically Dilithium, as research transitions from refining existing algorithms to developing entirely new, quantum-safe alternatives [17].
b. Specialization in Efficiency and Privacy (Niche Themes)
   Furthermore, the existence of "Aggregate Signature" and "Ring Signature" in the Niche Themes quadrant (Upper-Left) confirms the secondary, parallel research evolution driven by application efficiency and scalability, particularly for distributed environments like IoT and Blockchain [18]. These themes show high density, suggesting a high internal focus and deep specialization, but low centrality, meaning they are primarily studied by a dedicated group and are not yet widely connected to the entire DSS domain. This indicates a thematic specialization, where researchers are not

only focused on quantum-safety but also on developing value-added features (compression, anonymity) that address practical demands beyond pure cryptographic strength [19].

3.4.4 Synthesis: Dual Drivers of Research Evolution

In synthesis, the bibliometric evidence establishes that the field of Digital Signature Schemes is undergoing a non-linear, dual-driven evolution. The first and dominant driver is the external existential threat (quantum computing), which resulted in the scientific production Turning Point (Section 3.1) and the emergence of the PQC cluster (Section 3.4.1). The second driver is the internal application demand (IoT/Blockchain), which resulted in the highly specialized Niche Themes of aggregate and ring signatures (Section 3.4.3 b). This dual evolution from basic security (RSA/ECC) to quantum-safety (Dilithium) and applied efficiency (Aggregate/Ring) provides comprehensive quantitative proof for the central thesis of Thematic Evolution in DSS research.

4. CONCLUSION

The results carry significant implications for the global cybersecurity and cryptographic community. First, the confirmed emergence of PQC highlights the urgent need for industry practitioners and policymakers to begin transitioning Public Key Infrastructure (PKI) towards quantum-resistant standards, specifically prioritizing the integration of lattice-based schemes like Dilithium. Second, the prevalence of Niche Themes indicates that future research must move beyond mere security to focus on optimized practical implementation, especially concerning reducing computational and storage overhead for highly constrained environments (IoT, decentralized networks). For future research, this study suggests several avenues: Longitudinal Thematic Drift: A follow-up analysis focusing on the 2023–2025 period to track the velocity of Dilithium and other PQC finalists, determining if they transition from Emerging to Motor Themes following official NIST finalization. Citation Context Analysis: Qualitative analysis of the highest-cited documents to understand how the Intellectual Hubs (USA, Germany) are driving the theoretical advancements, specifically concerning the security proofs or optimization techniques for PQC candidates. Application-Specific Metrics: Bibliometric tracking of application-oriented keywords (e.g., "Homomorphic Signature," "Blind Signature") to map the diversification of DSS utility beyond traditional authentication. By providing a rigorous, quantitative assessment of the field, this study serves as a valuable state-of-the-art roadmap for navigating the critical evolutionary phase of Digital Signature Schemes in the post-quantum era.

REFERENCES

[1] N. H. Alkatiri, M. F. M. Putra, and K. Ongko, “A Legal Perspective: Implementing an Electronic Notarization System in Indonesia in the Post-Pandemic Era,” *Jambura Law Review*, vol. 5, no. 2, pp. 332–355, 2023, doi: 10.33756/jlr.v5i2.19221.

[2] A. Akram *et al.*, “A Pilot Study on Survivability of Networking Based on the Mobile Communication Agents,” *International Journal of Network Security*, vol. 23, no. 2, pp. 220–228, 2021, doi: 10.6633/IJNS.202103.

[3] Esau Taiwo Oladipupo and Oluwakemi Christiana Abikoye, “Improved authenticated elliptic curve cryptography scheme for resource starve applications,” *Computer Science and Information Technologies*, vol. 3, no. 3, pp. 169–185, 2022, doi: 10.11591/csit.v3i3.pp169-185.

[4] P. K. Shukla, A. Aljaedi, P. K. Pareek, A. R. Alharbi, and S. S. Jamal, “AES Based White Box Cryptography in Digital Signature Verification,” *Sensors*, vol. 22, no. 23, 2022, doi: 10.3390/s22239444.

[5] D. Willsch, M. Willsch, F. Jin, H. De Raedt, and K. Michielsen, “Large-Scale Simulation of Shor’s Quantum Factoring Algorithm,” *Mathematics*, vol. 11, no. 19, pp. 1–38, 2023, doi: 10.3390/math11194222.

[6] A. Shaheen, “CYBERSECURITY IN THE MODERN ERA: AN OVERVIEW OF RECENT TRENDS,” *JOURNAL OF ENGINEERING AND COMPUTATIONAL INTELLIGENCE REVIEW (JECIR) Volume*, vol. 1, no. 1, pp. 15–20, 2023, doi: 10.2307/jj.8973308.4.

[7] Y. Baseri, V. Chouhan, and A. Hafid, “Navigating quantum security risks in networked environments: A comprehensive study of quantum-safe network protocols,” *Comput Secur*, vol. 142, no. April, p. 103883, 2024, doi: 10.1016/j.cose.2024.103883.

[8] U. Tariq, I. Ahmed, and A. K. Bashir, “Directions for the Internet of Things : A Comprehensive Review,” *Mdpi*, vol. 23, no. 8, 2023.

[9] S. Aslam, A. Tošić, and M. Mrissa, “Secure and Privacy-Aware Blockchain Design: Requirements, Challenges and Solutions,” *Journal of Cybersecurity and Privacy*, vol. 1, no. 1, pp. 164–194, 2021, doi: 10.3390/jcp1010009.

[10] O. Rodríguez-Espíndola, S. Chowdhury, P. K. Dey, P. Albores, and A. Emrouznejad, “Analysis of the adoption of emergent technologies for risk management in the era of digital manufacturing,” *Technol Forecast Soc Change*, vol. 178, no. February, p. 121562, 2022, doi: 10.1016/j.techfore.2022.121562.

[11] O. Faraji, K. Asiaei, Z. Rezaee, N. Bontis, and E. Dolatzarei, “Mapping the conceptual structure of intellectual capital research: A co-word analysis,” *Journal of Innovation and Knowledge*, vol. 7, no. 3, 2022, doi: 10.1016/j.jik.2022.100202.

[12] Y. C. Fu, M. Marques, Y. H. Tseng, J. J. W. Powell, and D. P. Baker, “An evolving international research collaboration network: spatial and thematic developments in co-authored higher education research, 1998–2018,” *Scientometrics*, vol. 127, no. 3, pp. 1403–1429, 2022, doi: 10.1007/s11192-021-04200-w.

[13] M. Kumar, “Post-quantum cryptography Algorithm’s standardization and performance analysis,” *Array*, vol. 15, no. August, p. 100242, 2022, doi: 10.1016/j.array.2022.100242.

[14] P. B. Keenan and P. Jankowski, “Spatial Decision Support Systems: Three decades on,” *Decis Support Syst*, vol. 116, no. October 2018, pp. 64–76, 2019, doi: 10.1016/j.dss.2018.10.010.

ISSN 2808-375X (Media Online)
Vol 4, No 1, November 2024
Hal 292−300
DOI 10.47065/comforch.v4i1.975

[15] D. Dinçkol, P. Ozcan, and M. Zachariadis, "Regulatory standards and consequences for industry architecture: The case of UK Open Banking," *Res Policy*, vol. 52, no. 6, p. 104760, 2023, doi: 10.1016/j.respol.2023.104760.
[16] C. de las Heras-Rosas and J. Herrera, "Research trends in open innovation and the role of the university," *Journal of Open Innovation: Technology, Market, and Complexity*, vol. 7, no. 1, pp. 1–22, 2021, doi: 10.3390/joitmc7010029.
[17] I. Kong, M. Janssen, and N. Bharosa, "Realizing quantum-safe information sharing: Implementation and adoption challenges and policy recommendations for quantum-safe transitions," *Gov Inf Q*, vol. 41, no. 1, p. 101884, 2024, doi: 10.1016/j.giq.2023.101884.
[18] X. Zhang, X. Peng, J. Xu, X. Wang, H. Li, and Z. Zhao, "Dynamic Supervision Model of Rice Supply Chain Based on Blockchain and Smart Contract," *Nongye Jixie Xuebao/Transactions of the Chinese Society for Agricultural Machinery*, vol. 53, no. 1, pp. 370–382, 2022, doi: 10.6041/j.issn.1000-1298.2022.01.040.
[19] P. Radanliev, "Artificial intelligence and quantum cryptography," *J Anal Sci Technol*, vol. 15, no. 1, 2024, doi: 10.1186/s40543-024-00416-6.