Current trends in AI-Aided Cryptography

Tobias Höbbel[1][a],Sebastian Kavalir[1][b], Gero Knoblauch[2][c] and Dr. Alexander Wiesmaier[2][d]
[1]*Sopra Steria SE, Unterschweinstiege 2-14, Frankfurt (Main), Germany*
{*tobias.hoebbel2, sebastian.kavalir*}*@soprasteria.com*

[2]*Department of Computing, University of Applied Sciences Darmstadt, Germany*
{*gero.knoblauch, alexander.wiesmaier*}*@h-da.de*

Keywords: AI-aided Cryptography, Machine Learning for Cryptography, AI-aided Cryptanalysis, Side-channel Analysis, Cryptographic Hashing, Cryptographic Protocols, Post-Quantum Cryptography

Abstract: Research at the intersection of artificial intelligence (AI) and cryptography is expanding, but existing surveys often focus on specific techniques or provide only high-level overviews without cross-domain comparison. This paper presents a trend analysis across major subfields of AI-aided cryptography. We review 90 publications from 2021–2025 and complement them with call for papers from journals, conferences, and public tenders. The results show uneven coverage: cryptanalysis and hashing dominate, while protocols, encryption, and post-quantum cryptography are less explored. We outline emerging gaps and likely growth areas to support future research prioritization.

1 INTRODUCTION

Recent AI advances have sparked interest across many research domains. A key milestone was the development of new transformer architectures by (Vaswani et al., 2017). in Attention is All You Need, which underpins systems like ChatGPT.

AI in cryptography is not new and has been explored by authors such as (Rivest, 1993). Modern research is extending these ideas, applying AI in areas like pattern matching (Mitchell, 2014) and network intrusion detection (Park et al., 2023). This work provides an overview of past, current, and emerging approaches to AI-driven cryptography, highlighting its applications and potential.

While previous studies summarize AI-aided cryptography (Nitaj and Rachidi, 2023; Alani, 2019; Zolfaghari and Koshiba, 2022), they often omit a full overview and future trends instead focusing on certain topics and exploring them in detail or taking a more top level approach of the broader spectrum without depth. Accordingly, this study addresses the following research questions:

RQ1: What is the current state of AI-aided cryptography and which topics are covered?

RQ2: Which trends emerge from recent research and funding calls?

RQ3: How can the results of the literature review be systematically organized?

RQ4: Which topics are likely to gain relevance in the future?

RQ5: Which areas of AI-aided cryptography are underexplored?

These questions are addressed through a structured literature review, analysis of trends in publications and funding calls, and visualization of findings to identify research gaps and emerging topics.

The detailed contributions of this paper are summarized as follows:

- To assess the current state of AI-based cryptography, we analyzed 15 related papers addressing similar research questions. We identified a focus on the topics of cryptanalysis, side channel attacks, explainable AI and AI in the development of encryption and protocols.
- We created an overview of recent research topics in AI-aided cryptography using a systematic literature review (SLR), covering 90 papers published from 2021-2025 in total. Further analysis revealed

[a] https://orcid.org/0000-0000-0000-0000
[b] https://orcid.org/0000-0000-0000-0000
[c] https://orcid.org/0000-0000-0000-0000
[d] https://orcid.org/0000-0000-0000-0000

a downward trend in AI-aided cryptography publications. We pinpointed this trend to the recent COVID pandemic as well as rising geopolitical tensions.

- In addition to recent papers, we analyzed four funding databases and 117 conference call for papers to assess future research directions in AI-aided cryptography. We identify a strong research focus on AI-aided cryptanalysis, explainable AI and the use of Generative AI in the field of AI-aided cryptography that will continue to rise. In addition we identified a research gap in the topics of protocols, encryption, quantum cryptography, hashing and signatures due to their more application focused nature.

2 RELATED WORK

This chapter summarizes prior research on AI-aided cryptography and positions the present study within the existing literature.

2.1 Previous Work

Early work by (Rivest, 1993) already identified conceptual links between machine learning (ML) and cryptanalysis, suggesting that learning techniques could influence both attack strategies and cryptographic design. Since then, research at the intersection of AI and cryptography has expanded.

Several surveys examine AI applications in cybersecurity and cryptography from different perspectives (Alani, 2019), (Shara, 2020), (Meraouche et al., 2021), (Reddy et al., 2024), (Ofusori et al., 2024), and (Nitaj and Rachidi, 2023). These works discuss ML-based intrusion detection, neural-network-based cryptographic constructions, and AI-driven cryptanalysis while also addressing challenges such as integration complexity, computational cost, and explainability.

Other studies focus on specific subdomains. (Picek et al., 2023) provide a systematization of deep-learning-based side-channel attacks (SCAs), reviewing datasets, threat models, and methodological trends. (Singh et al., 2024a) analyze ML and optimization strategies in lightweight cryptanalysis. (Luo et al., 2023) survey deep hashing methods and their applications, highlighting their growing role in similarity retrieval and data protection contexts.

Research on AI-supported encryption and neural cryptography explores the use of neural networks and generative models for key generation, ciphertext transformation, and protocol design (Jyothi et al., 2022) and (Zolfaghari and Koshiba, 2022). Additional work investigates AI-driven security evaluation and broader cybersecurity implications, including ethical considerations and operational deployment challenges (Dinu et al., 2024).

Overall, prior literature either concentrates on specific techniques (e.g., SCAs, hashing, neural distinguishers) or provides broad overviews of AI in cybersecurity. However, a structured cross-domain trend analysis that systematically compares research distribution across cryptanalysis, hashing, encryption, protocols, and post-quantum cryptography remains limited.

2.2 Differentiation from Previous Work

Most of the aforementioned studies focus on individual research areas or emphasize technical depth within selected subfields. In contrast, this study provides a consolidated trend analysis across major domains of AI-aided cryptography.

By reviewing 90 publications from 2021–2025 and complementing them with conference call for papers and publicly funded research programs, this work integrates literature trends with forward-looking signals from funding and publication venues. This combined perspective enables identification of research concentration, emerging themes, and underexplored areas within the broader AI-aided cryptography landscape.

3 METHODOLOGY AND EXECUTION OF THE LITERATURE SEARCH

Given the expanding research at the intersection of artificial intelligence and cryptography, a systematic literature review (SLR) was conducted to identify and structure relevant contributions. The review follows established guidelines for transparent and reproducible literature analysis (Randolph, 2009) and aims to address RQ1 and RQ2 concerning the current state and emerging trends of AI-aided cryptography.

The review adopts a research-methods-oriented perspective (Cooper, 1988) to capture methodological developments across cryptanalysis, hashing, encryption, protocols, and post-quantum cryptography. Publications were categorized by research domain and analyzed chronologically for 2021–2025.

3.1 Inclusion and Exclusion Criteria

A rigorous selection process ensured that only relevant and methodologically sound publications were included. The criteria were adapted from (Kaur et al., 2023).

Inclusion Criteria Papers were included if they met all of the following conditions:

- Published between 2021 and 2025.
- Written in English.
- Publicly accessible as a full-text PDF.
- Minimum length of five pages.
- Provided a clear contribution involving the use of AI to support, analyze, or improve a cryptographic concept.
- Addressed at least one of the research questions defined in this study.
- For multiple published versions, only the most recent version was considered.

Exclusion Criteria Papers were excluded if they met any of the following:

- Non-English or non-scientific publications (e.g., posters, blogs, editorials).
- Duplicate works by the same authors or research groups.
- Papers shorter than five pages or lacking methodological detail.
- Works unrelated to cryptographic research.
- Purely practical AI applications without methodological or analytical contribution.
- Papers not available in full-text PDF form or behind restrictive paywalls.

3.2 Keyword Development and Search Strategy

Keywords were grouped into three thematic categories: AI-related terms, cryptography-related terms, and narrowing terms (Table 1). The search string was iteratively refined using Boolean operators and proximity constraints to ensure semantic linkage between AI and cryptographic concepts.

The primary search was conducted in Web of Science due to its structured metadata and filtering capabilities. Google Scholar was used as a complementary source to capture additional publications not indexed in major databases. The final query combined AI and cryptography terms with contextual filters to reduce noise and improve precision.

Table 1: Keywords for the Literature Search

AI	Cryptography	Narrowing terms
AI	crypto	analyzing
artificial intelligence	cryptoanalysis	assessing
CAD	cryptographic primitives	automation
DL	cryptographic protocols	design
deep learning	cryptographic schemes	developing
GAN	cryptographic systems	examining
generative adversarial network	cryptosystem	evolving
machine learning	cryptosystem	implementing
ML	cybersecurity	improving
natural language processing	hash	investigating
neural network	quantum cryptography	optimizing
computer-aided	signature	testing
computer vision	digital signature	validating
reinforcement learning		

3.3 Screening and Categorization Process

The combined search yielded 324 publications. These were screened by title, abstract, and full text, after which each publication was assigned to one of the following thematic categories:

- Cryptanalysis
- Hashing
- Encryption
- Protocols
- Post-quantum cryptography
- Peripheral
- Related work
- Signatures

After applying all screening and selection steps, the final dataset consisted of 90 publications. Table 2 summarizes the distribution across categories and data sources, while Table 4 in the Appendix documents the category assignment at publication level.

4 Processing of the Literature

To address RQ3, suitable methods for processing and interpreting the collected literature were identified by reviewing prior AI-focused systematic studies that included trend analysis components. In particular, the evaluation frameworks proposed by (Wiafe et al., 2020) and (Kaur et al., 2023) were considered due to their structured assessment of publication trends, geographic distribution, and thematic categorization.

Both approaches analyze research development over time and classify contributions by methodological and application-oriented criteria. Building on

Category	Total	Google Scholar	Web of Science	From References	Previously Known
Cryptanalysis	34	4	18	12	0
Encryption	5	0	2	3	0
Hashing	17	0	17	0	0
Protocols	4	0	3	1	0
Post-Quantum Crypto	2	0	2	0	0
Peripheral	12	5	5	2	0
Related Papers	15	2	6	0	7
Signatures	1	0	1	0	0
Total	**90**	**11**	**54**	**18**	**7**

Table 2: Overview of categories and number of papers per source.

these frameworks, the present study adopts a unified analysis scheme tailored to AI-aided cryptography.

Given the limited number of conference papers in the dataset, journal and conference publications were not analyzed separately. Instead, trend analysis focuses on:

- Publication year
- Country of origin
- Research area distribution

Additionally, publications are subdivided into thematic subcategories to identify more fine-grained developments within major domains such as cryptanalysis and hashing. Furthermore, thematic relationships between selected publications are discussed to illustrate methodological continuities within the field. Finally, methodological limitations are considered to contextualize the interpretation of the results and to derive directions for future work.

4.1 Distribution by Publication Year

Figure 1 shows all papers acquired during the SLR, sorted by year and research area. Only papers from 2021 to 2025 are considered. The research areas include AI applied to cryptanalysis, encryption, hashing, protocols, and post-quantum cryptography, with a marginal reference to this work.

The highest number of papers was in 2021, with 21 papers, while the lowest was 2025, with 7 papers. Most papers belong to AI-aided cryptanalysis, closely followed by hashing. The graph indicates a declining trend; however, this observation should be interpreted cautiously because the observation window is short (2021–2025) and may include short-term effects.

4.2 Distribution by Country of Origin

Figure 2 shows the distribution of papers by the country of the primary authors. The 76 in-scope papers are

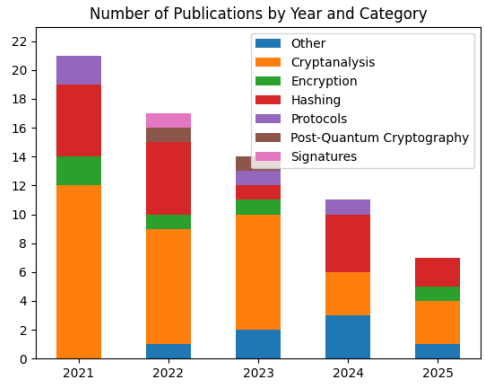


Figure 1: Papers based on publication year

sorted in descending order by frequency.

China leads with 36 papers, followed by India with 9 papers, and the Netherlands with 6 papers. At the lower end are Brazil, Colombia, Malaysia, Serbia, Taiwan, and Turkey, each with 1 publication in AI-aided cryptography. This absolute-count perspective is population- and funding-size dependent; a normalized indicator (e.g., publications per capita or per research expenditure) could lead to a different ranking.

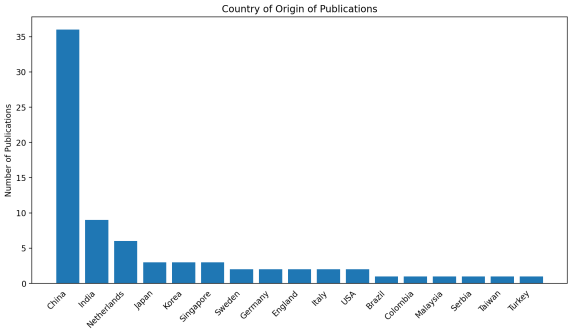


Figure 2: Papers based on country of origin

4.3 Distribution by Research Area

Figure 3 shows the distribution of papers by research area. The majority (54.0%) are in cryptanalysis, while the fewest (1.6%) are in signatures. Hashing accounts for 27.0%, encryption for 7.9%, protocols for 6.3% and post-quantum cryptography for 3.2%.

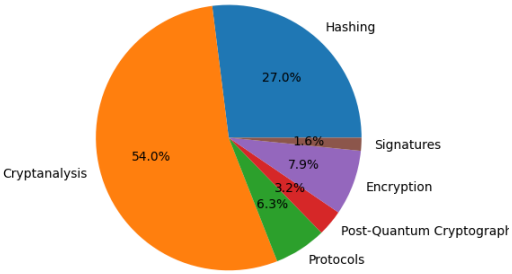


Figure 3: Distribution by research area

Figure 4 breaks these areas down into subcategories. This allows a more detailed view of topic distribution. Subcategories like model optimization (cryptanalysis), similarity retrieval (hashing), and explainability (cryptanalysis) already account for over 50% of all papers. This directly supports RQ1 by characterizing the current state of research concentration, and it informs RQ5 by highlighting underexplored areas such as signatures, protocols, and post-quantum cryptography.

4.4 Relationships Between Publications

This subsection outlines key thematic connections between selected publications to illustrate methodological continuities within AI-aided cryptography. Rather than providing a full citation-network analysis, representative research trajectories are highlighted.

A central development line originates from (Gohr, 2019), whose work on neural distinguishers for reduced-round Speck32/64 significantly influenced subsequent research in ML-based cryptanalysis. Later studies extended this approach by refining neural distinguishers, exploring related-key settings, and transferring ML techniques from differential to linear cryptanalysis (Benamira et al., 2021), (Bao et al., 2023), and (Hou et al., 2025). Collectively, these works demonstrate increasing methodological sophistication and improved key-recovery efficiency.

Another research trajectory concerns cipher identification and ensemble learning. (Yuan et al., 2023) and (Yuan et al., 2024) propose hybrid and multi-layer model combinations to improve block cipher identification stability and accuracy, reflecting a broader trend toward ensemble-based ML architectures in cryptanalysis.

In the area of side-channel analysis, (Lu et al., 2021) introduced end-to-end deep learning approaches for feature extraction from raw traces. Subsequent work emphasizes optimization of hyperparameters and model efficiency, indicating a shift from architecture-centric design toward training-strategy refinement (Perin et al., 2022).

Neural synchronization and generative approaches have also been explored for protocol design and encryption. Research on Tree Parity Machines and generative adversarial network (GAN)-based architectures demonstrates experimental applications of AI for key exchange and encryption construction (Sarkar, 2021), (Teodoro et al., 2022), (Kumar et al., 2024b), and (Ding et al., 2022a). While these approaches remain exploratory, they illustrate attempts to move AI from analytical to constructive cryptographic roles.

Finally, systematic analyses of deep-learning-based side-channel attacks highlight challenges such as overfitting and black-box complexity. Methodological refinements, including regularization strategies, indicate ongoing efforts to stabilize and generalize ML-based attack models (Picek et al., 2023), and (Rezaeezade and Batina, 2024).

4.5 Evaluation of the Results

The following subsection evaluates and interprets the processed literature review results.

Figure 1 shows a decreasing trend in total publications, suggesting declining relevance of AI-aided cryptography. However, anomalies from the COVID-19 pandemic may influence 2021-2022 publication numbers. In addition, the short time window, database selection, and possible publication delays mean this pattern may also reflect a temporary fluctuation rather than a stable long-term decline. (Rousseau et al., 2023) observed unexpected increases in 2021 and reduced collaborations between the USA and China due to geopolitical tensions, explaining the drop from 2021 to 2022.

Publication distribution by country (Figure 2) shows overrepresentation of Asian countries. China leads worldwide, partly due to state research funding, impacting both quantity and quality of publications (Hyland, 2023).

The distribution by research area (Figure 3) highlights cryptanalysis as the dominant area, followed by hashing. Many smaller cryptography research categories receive less attention but may become relevant. For example, explainability of DL-SCAs and new encryption methods using GAs and GANs represent emerging trends benefiting from AI.

4.6 Critical Review of the Literature Search

To assess the quality of this literature review and potential improvements, a critical analysis is conducted. (Randolph, 2009) recommends using the scoring table by (Boote and Beile, 2005). This evaluates literature across multiple categories on a scale of 1 (poor) to 3 (good).

In the work at hand, weaker ratings are mainly associated with limited historical contextualization and limited synthesis of related theoretical perspectives. Stronger ratings are associated with clear scope definition, terminology, structural organization, and transparent reporting of the search and categorization workflow. Overall, the review provides a solid baseline for trend analysis, while methodological depth can be improved in follow-up work.

Additional considerations include search database limitations and pandemic-related anomalies (Rousseau et al., 2023). The selected sources (Web of Science and Google Scholar) provide broad high-level coverage, but future iterations can strengthen reproducibility through extended cross-database validation. Future reviews should compare pre-COVID publications and investigate possible publication suppression due to security or competitive reasons. Digital signatures are now included in this review; however, they remain clearly underrepresented and should be expanded in future work.

In conclusion, the literature review yields meaningful trend insights for the defined research questions, but its findings should be interpreted together with the stated methodological boundaries. A natural extension is a dedicated future-work stream that broadens data sources, deepens theoretical synthesis, and expands underrepresented categories.

5 External Signals: Calls for Papers and Public Funding Priorities

To complement the literature review with forward-looking indicators, current calls for papers (CfPs) from security conferences and journals, as well as publicly funded research programs, were analyzed for the years 2025–2026.

A total of 117 security conferences and workshops were screened[1], with a focus on AI-related and cryptography-relevant topics. The CfPs largely emphasize AI-aided cryptanalysis, side-channel analysis, and computer-assisted cryptographic engineering. Explicit references to hashing and post-quantum cryptography appear less frequently. Overall, the thematic distribution of CfPs aligns with the publication trends identified in Section 4, particularly the strong focus on attack-oriented and evaluation-based research.

Journal calls, including special issues addressing generative AI in security contexts, further highlight increasing interest in AI-supported cryptographic evaluation and automation. Generative AI is frequently positioned as a tool for improving analysis, testing, and security assessment processes.

Searches for funded research programs related to AI-aided cryptography were conducted in the German Federal Funding Database[2] (FdB), the database of the National Coordination Center for Cybersecurity[3] (NKCS), and the Service Center for Electronic Research Funding Information[4] (ELFI). Recent calls emphasize post-quantum cryptography security, AI-supported security evaluation, and generative AI for cybersecurity operations. Compared with the broader publication landscape, funding priorities appear more mission-driven and implementation-oriented, focusing on secure deployment and operational resilience rather than exploratory method development.

Taken together, CfPs and funding programs reinforce the dominance of AI-aided cryptanalysis and growing interest in generative AI applications. At the same time, comparatively fewer explicit calls address AI-supported encryption design, protocol construction, or digital signatures, suggesting potential underexplored research areas.

6 Research Areas of Particular Relevance for Future Work

The following section presents the answers to RQ4 and RQ5 after processing the literature review. Particularly relevant papers are highlighted, based on the topics identified in section 5 and section 5, and the processed results presented in section 4, as important

[1] Using https://sec-deadlines.github.io/

[2] https://www.foerderdatenbank.de

[3] https://www.nkcs.bund.de

[4] https://www.elfi.info

for the future development of AI-aided cryptography. Subsequently, research gaps are identified and examined in more detail.

6.1 Particularly Relevant Works

This subsection highlights particularly relevant works in AI-aided cryptography. Relevance is determined by at least one of the following criteria: strong influence on subsequent studies, introduction of transferable methods adopted in later work, or representative contribution to an emerging trend identified in this review. These will be used in the following subsection to make more informed statements about research trends in AI-aided cryptography.

(Wang and Dubrova, 2021) were the first to combine DL classification features to perform DL-based side-channel attacks (SCA). They create a model using three classifiers trained on different points of a trace. Training data is generated using a profiling device, and the attack is performed with data from the targeted device. They test implementations using one, two, or all three classifiers to assess attack effectiveness. The third classifier performs best, using Hamming distance, optimized for hardware implementations. Tests with two classifiers show that any approach including the third classifier performs better than individually. Only the combination of classifiers one and two performs worse. Combining all three classifiers achieves the best results and requires about one-third fewer traces for a successful attack. They also test training all classifiers on a single attack point, which performs worse than using diversified points.

(Perin et al., 2026) investigate the explainability of DL-based SCAs. Although it is known that these approaches work with neural networks (NNs), the exact mechanism is unclear. They develop a framework for explainable DL-SCAs (ExDL-SCA) to understand which layers of the NN contribute and how they process relevant and irrelevant information. Their methodology trains a model for several epochs, collecting data from hidden layers to determine information content regarding the key. Experiments with various MLP and CNN architectures answer the "Where?" and "What?" questions. Irrelevant information is compressed, while uncompressed features are relevant. The "Where?" question is harder to answer due to limitations in the applied patching method, but it is assumed that share combination occurs after compression of irrelevant information. Future work will examine compression and generalization phases in more detail, as well as noise and irrelevant feature reduction.

Due to threats from cryptanalysis and quantum cryptography, (Singh et al., 2025) investigate a GA-GAN approach for securing cryptographic systems. Their work demonstrates that genetic algorithms (GA) can optimize NN architectures for encryption and decryption, while generative adversarial networks (GAN) increase system robustness under adversary scenarios. Random GAN architectures are generated, evaluated, and evolved using GA. The best GAN is trained with adversarial training, where Alice and Bob communicate while Eve interferes. Results show that encryption performance increases with generations, while Eve's ability to decrypt decreases. The authors claim resistance to Shor's and Grover's algorithms and near-immunity to cryptanalysis; however, this is presented as a study-specific result, and broader independent validation is subject to further research. Future work includes deeper NNs, improved optimization strategies for Eve, GA enhancements, integration with quantum-resistant algorithms, and application to image encryption.

6.2 Research Trends

This subsection addresses RQ4, which investigates which areas of AI-aided cryptography are particularly relevant. Area-level relevance is assessed by combining publication concentration, methodological influence on follow-up work, and signals from journals, conferences, and funding programs. Collected papers, calls for papers, and conferences from section 5 and section 5, and processed literature review results from section 4 are used.

The largest and numerically most significant topic is AI-aided cryptanalysis. It primarily focuses on model optimization and explainability of DL-SCAs. Both areas are equally relevant, although explainability is less represented. Model optimization advances the limits of feasible attacks by breaking more rounds of cryptographic algorithms or using smaller models. Explainability, as studied by (Perin et al., 2026), provides theoretical background and allows understanding countermeasure development. This is supported by journal and conference requirements and the public call for papers (Nationales Koordinierungszentrum für Cybersicherheit Deutschland, 2025) emphasizing contributions to cryptanalysis.

Another future-relevant area is the use of generative AI in cryptography. (Singh et al., 2025) use generative AI for encryption, (Ding et al., 2022b) for key generation, and (He et al., 2021) for cryptanalysis using GANs. Although the use of generative AI is limited compared to other methods, results are often remarkable. Generative AI is also encouraged in journals (Tennyson, 2024) and some conferences (see

Table 3).

Many works suggest future research focuses on foundational aspects (RQ2, section 9). Classic AI challenges remain: systems often need optimization in computational performance, models, and hyperparameters to handle larger datasets or calculations.

6.3 Research Gaps

This subsection addresses RQ5, identifying areas of AI-aided cryptography that are under- or unexplored. Collected papers, calls, and conferences from section 5 and section 5, and processed literature review results from section 4 are used.

From the distribution in Figure 3, protocols, encryption, and quantum cryptography receive little research attention. Irregular publication patterns in Figure 1 confirm this. Journal and paper requirements (see section 5) do not provide precise indications of relevance.

However, public calls (see section 5) for "Security of Implementations of Post-Quantum Cryptography Algorithms" (Nationales Koordinierungszentrum für Cybersicherheit Deutschland, 2025) request contributions on post-quantum algorithms, security measures, and security-by-design architectures using AI. Thus, these topics find practical application but remain largely unstudied in research.

7 Discussion

The findings reveal a structured research landscape within AI-aided cryptography. Current work is strongly concentrated on cryptanalysis and hashing, while encryption, protocols, post-quantum cryptography, and digital signatures receive comparatively limited attention. The dominance of cryptanalysis reflects AI's effectiveness as an analytical instrument, particularly in deep-learning-based side-channel attacks and neural distinguishers. Methodological refinement, including model optimization and explainability, indicates that the field is transitioning from proof-of-concept experimentation toward more systematic and robust attack frameworks. Generative approaches, especially GAN-based models, illustrate an emerging shift from purely analytical applications toward constructive cryptographic design. Although still exploratory, such approaches demonstrate AI's potential not only to evaluate but also to generate cryptographic mechanisms. Contrary to earlier expectations in the literature, quantum-related AI research appears less represented within the analyzed publication set. This discrepancy may result from the specialized and resource-intensive nature of post-quantum research or from publication timing effects. The comparatively low representation of AI-supported encryption design, protocol construction, and digital signatures suggests structural challenges. Security-critical domains require explainable, verifiable, and formally analyzable mechanisms, which can conflict with the black-box characteristics of many AI models. In addition, validating AI-generated cryptographic outputs often demands significant computational and theoretical resources. The overall publication volume between 2021 and 2025 appears moderate. External factors such as pandemic-related disruptions, geopolitical tensions, and reduced international collaboration may have influenced research output and publication visibility, particularly in security-sensitive domains. Taken together, the results suggest that AI-aided cryptography remains an emerging but consolidating field. While analytical applications currently dominate, generative and constructive approaches are gaining traction. Underrepresented areas may become increasingly relevant as explainability, robustness, and evaluation methodologies continue to mature.

8 Future Work

Future work should extend the observation window beyond 2025 and include periodic updates to reduce sensitivity to short-term publication effects. A broader database strategy and expanded keyword set, especially for signatures and other underrepresented topics, would improve coverage and reduce selection bias. In addition, citation-network analyses could complement the current qualitative relationship discussion with a more explicit structural view of topic evolution.

9 Conclusion

This work presents a comprehensive overview of AI-aided cryptography across major subfields and distinguishes itself from prior studies by combining literature trends with conference call for papers and publicly funded call analyses in one unified perspective. We find that AI methods can be applied to nearly every branch of cryptographic analysis and construction. Future developments will likely be shaped by deep-learning-based side-channel attacks, AI explainability, and generative models, all of which promise to influence the direction and progress of AI-aided cryptographic research. To achieve a more complete

understanding of the field, future studies should consider extending the research period. Additionally, the declining number of publications warrants further investigation to determine the underlying causes. Given increasing geopolitical tension and growing security demands in the digital sphere, AI-aided cryptography holds significant potential for enhancing information security and generating novel insights.

REFERENCES

Agate, V., Concone, F., De Paola, A., Ferraro, P., Re, G. L., and Morana, M. (2023). Bayesian Modeling for Differential Cryptanalysis of Block Ciphers: A DES Instance. *IEEE Access*, 11:4809–4820.

Alani, M. M. (2019). Applications of machine learning in cryptography: a survey. In *Proceedings of the 3rd International Conference on Cryptography, Security and Privacy*, ICCSP '19, page 23–27, New York, NY, USA. Association for Computing Machinery.

Bao, Z., Guo, J., Liu, M., Ma, L., and Tu, Y. (2022). Enhancing differential-neural cryptanalysis. In *Advances in Cryptology – ASIACRYPT 2022: 28th International Conference on the Theory and Application of Cryptology and Information Security, Taipei, Taiwan, December 5–9, 2022, Proceedings, Part I*, page 318–347, Berlin, Heidelberg. Springer-Verlag.

Bao, Z., Lu, J., Yao, Y., and Zhang, L. (2023). More insight on deep learning-aided cryptanalysis. In *Advances in Cryptology – ASIACRYPT 2023: 29th International Conference on the Theory and Application of Cryptology and Information Security, Guangzhou, China, December 4–8, 2023, Proceedings, Part III*, page 436–467, Berlin, Heidelberg. Springer-Verlag.

Barenghi, A., Carrera, D., Mella, S., Pace, A., Pelosi, G., and Susella, R. (2022). Profiled side channel attacks against the rsa cryptosystem using neural networks. *J. Inf. Secur. Appl.*, 66(C).

Benamira, A., Gerault, D., Peyrin, T., and Tan, Q. Q. (2021). A Deeper Look at Machine Learning-Based Cryptanalysis. In Canteaut, A. and Standaert, F.-X., editors, *Advances in Cryptology - EUROCRYPT 2021*, pages 805–835, Cham. Springer International Publishing.

Boote, D. N. and Beile, P. (2005). Scholars before researchers: On the centrality of the dissertation literature review in research preparation. *Educational Researcher*, 34(6):3–15.

Brunetta, C. and Picazo-Sanchez, P. (2022). Modelling cryptographic distinguishers using machine learning. *JOURNAL OF CRYPTOGRAPHIC ENGINEERING*, 12(2):123–135.

Chang, C.-C., Xu, S., Gao, K., and Chang, C.-C. (2024). Cryptanalysis of Dual-Stage Permutation Encryption Using Large-Kernel Convolutional Neural Network and Known Plaintext Attack. *CRYPTOGRAPHY*, 8(3).

Chen, Y., Long, Y., Yang, Z., and Long, J. (2025a). Parameter Adaptive Contrastive Hashing for multimedia retrieval. *NEURAL NETWORKS*, 182.

Chen, Y., Long, Y., Yang, Z., and Long, J. (2025b). Unsupervised random walk manifold contrastive hashing for multimedia retrieval. *COMPLEX & INTELLIGENT SYSTEMS*, 11(4).

Chong, B. Y. and Salam, I. (2021). Investigating Deep Learning Approaches on the Security Analysis of Cryptographic Algorithms. *Cryptography*, 5(4):30. Number: 4 Publisher: Multidisciplinary Digital Publishing Institute.

Christy, A. J. and Dhanalakshmi, K. (2022). Content-Based Image Recognition and Tagging by Deep Learning Methods. *WIRELESS PERSONAL COMMUNICATIONS*, 123(1):813–838.

Cintas-Canto, A., Kaur, J., Mozaffari-Kermani, M., and Azarderakhsh, R. (2023). ChatGPT vs. Lightweight Security: First Work Implementing the NIST Cryptographic Standard ASCON. arXiv:2306.08178 [cs].

Cooper, H. M. (1988). Organizing knowledge syntheses: A taxonomy of literature reviews. *Knowledge in Society*, 1(1):104–126.

Coyle, B., Doosti, M., Kashefi, E., and Kumar, N. (2022). Progress toward practical quantum cryptanalysis by variational quantum cloning. *PHYSICAL REVIEW A*, 105(4).

Ding, K., Chen, S., Yu, J., Liu, Y., and Zhu, J. (2022a). A New Subject-Sensitive Hashing Algorithm Based on MultiRes-RCF for Blockchains of HRRS Images. *ALGORITHMS*, 15(6).

Ding, Y., Tan, F., Qin, Z., Cao, M., Choo, K.-K. R., and Qin, Z. (2022b). DeepKeyGen: A Deep Learning-Based Stream Cipher Generator for Medical Image Encryption and Decryption. *IEEE Transactions on Neural Networks and Learning Systems*, 33(9):4915–4929.

Dinu, A., Vasile, P. C., and Georgescu, A. (2024). AI-driven solutions for cybersecurity: comparative analysis and ethical aspects. *ROMANIAN JOURNAL OF INFORMATION TECHNOLOGY AND AUTOMATIC CONTROL-REVISTA ROMANA DE INFORMATICA SI AUTOMATICA*, 34(3, SI):35–48.

Erkan, U., Toktas, A., Enginoğlu, S., Akbacak, E., and Thanh, D. N. H. (2022). An image encryption scheme based on chaotic logarithmic map and key generation using deep CNN. *Multimedia Tools and Applications*, 81(5):7365–7391.

Gohr, A. (2019). Improving Attacks on Round-Reduced Speck32/64 Using Deep Learning. In Boldyreva, A. and Micciancio, D., editors, *Advances in Cryptology - CRYPTO 2019*, pages 150–179, Cham. Springer International Publishing.

Golder, A., Bhat, A., and Raychowdhury, A. (2022). Exploration into the Explainability of Neural Network Models for Power Side-Channel Analysis. In *Proceedings of the Great Lakes Symposium on VLSI 2022*, GLSVLSI '22, pages 59–64, New York, NY, USA. Association for Computing Machinery.

Hawkes, S., Weinert, C., Almeida, T., and Mehrnezhad, M. (2024). Perceptual Hash Inversion Attacks on Image-

Based Sexual Abuse Removal Tools. *IEEE SECURITY & PRIVACY*.

He, W., Pan, S., Liao, M., Lu, D., Xing, Q., and Peng, X. (2021). A learning-based method of attack on optical asymmetric cryptosystems. *Optics and Lasers in Engineering*, 138:106415.

Hou, Z., Ren, J., and Chen, S. (2025). Improved machine learning-aided linear cryptanalysis: application to DES. *CYBERSECURITY*, 8(1).

Hu, F., Wang, H., and Wang, J. (2022). Multi-Leak Deep-Learning Side-Channel Analysis. *IEEE ACCESS*, 10:22610–22621.

Huo, Y., Qibing, Q., Dai, J., Zhang, W., Huang, L., and Wang, C. (2024). Deep Neighborhood-aware Proxy Hashing with Uniform Distribution Constraint for Cross-modal Retrieval. *ACM TRANSACTIONS ON MULTIMEDIA COMPUTING COMMUNICATIONS AND APPLICATIONS*, 20(6, SI).

Hussain, A., Li, H.-C., Ali, M., Wali, S., Hussain, M., and Rehman, A. (2022). An Efficient Supervised Deep Hashing Method for Image Retrieval. *ENTROPY*, 24(10).

Hyland, K. (2023). Enter the dragon: China and global academic publishing. *Learned Publishing*, 36(3):394–403. Publisher: John Wiley & Sons, Ltd.

Ito, A., Saito, K., Ueno, R., and Homma, N. (2021). Imbalanced Data Problems in Deep Learning-Based Side-Channel Attacks: Analysis and Solution. *IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY*, 16:3790–3802.

Jyothi, V. E., Latha, V. M., and Bharathi, D. S. B. (2022). Research on Artificial Intelligence Applications in Cryptography with an Analysis in Vulnerabilities Detection Management. *INTERNATIONAL JOURNAL OF EARLY CHILDHOOD SPECIAL EDUCATION*, 14(3):2446–2451. Num Pages: 6 Place: Eskisehir Publisher: Anadolu Univ Web of Science ID: WOS:000798019900034.

Kaur, R., Gabrijelčič, D., and Klobučar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. *Information Fusion*, 97:101804.

Kim, H., Lim, S., Kang, Y., Kim, W., Kim, D., Yoon, S., and Seo, H. (2023). Deep-Learning-Based Cryptanalysis of Lightweight Block Ciphers Revisited. *ENTROPY*, 25(7).

Kim, J., Picek, S., Heuser, A., Bhasin, S., and Hanjalic, A. (2025). Still Making Noise: Improving Deep-Learning-Based Side- Channel Analysis. *IEEE DESIGN & TEST*, 42(1):20–27.

Kubota, T., Yoshida, K., Shiozaki, M., and Fujino, T. (2021). Deep learning side-channel attack against hardware implementations of AES. *Microprocessors and Microsystems*, 87:103383.

Kumar, K., Tanwar, S., and Kumar, S. (2024a). MAN-C: A masked autoencoder neural cryptography based encryption scheme for CT scan images. *METHODSX*, 12.

Kumar, P., Rahman, M., Namasudra, S., and Moparthi, N. R. (2024b). Enhancing Security of Medical Images Using Deep Learning, Chaotic Map, and Hash Table. *MOBILE NETWORKS & APPLICATIONS*, 29(5, SI):1489–1503.

Kwon, D., Hong, S., and Kim, H. (2022). Optimizing Implementations of Non-Profiled Deep Learning-Based Side-Channel Attacks. *IEEE Access*, 10:5957–5967.

Lei, L., Guo, D., Shen, Z., and Wu, Z. (2023). Image hashing retrieval based on generative adversarial networks. *APPLIED INTELLIGENCE*, 53(8, SI):9056–9067.

Li, J., Sun, H., Du, Z., Wang, Y., Yuan, K., and Jia, C. (2025). A generic cryptographic algorithm identification scheme based on ciphertext features. *JOURNAL OF INFORMATION SECURITY AND APPLICATIONS*, 89:103984. Num Pages: 10 Place: Amsterdam Publisher: Elsevier Web of Science ID: WOS:001422909500001.

Li, X., Lei, W., Tang, W., Wang, Y., Yang, X., and Liao, X. (2024). Segmented Hash-Based Privacy-Preserving Image Retrieval Scheme in Cloud-Assisted IoT. *IEEE INTERNET OF THINGS JOURNAL*, 11(21):35250–35265.

Liao, M., Zheng, S., Pan, S., Lu, D., He, W., Situ, G., and Peng, X. (2021). Deep-learning-based ciphertext-only attack on optical double random phase encryption. *Opto-Electronic Advances*, 4(5):200016–12.

Liu, W., Li, W., Cao, X., Fu, Y., Wu, J., Liu, J., Chen, A., Zhang, Y., Wang, S., and Zhou, J. (2025). Full-Element Analysis of Side-Channel Leakage Dataset on Symmetric Cryptographic Advanced Encryption Standard. *Symmetry*, 17(5):769. Number: 5 Publisher: Multidisciplinary Digital Publishing Institute.

Lu, X., Zhang, C., Cao, P., Gu, D., and Lu, H. (2021). Pay Attention to Raw Traces: A Deep Learning Architecture for End-to-End Profiling Attacks. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pages 235–274.

Luo, X., Wang, H., Wu, D., Chen, C., Deng, M., Huang, J., and Hua, X.-S. (2023). A Survey on Deep Hashing Methods. *ACM TRANSACTIONS ON KNOWLEDGE DISCOVERY FROM DATA*, 17(1).

Meraouche, I., Dutta, S., Tan, H., and Sakurai, K. (2021). Neural Networks-Based Cryptography: A Survey. *IEEE ACCESS*, 9:124727–124740.

Meraouche, I., Dutta, S., Tan, H., and Sakurai, K. (2023). Learning asymmetric encryption using adversarial neural networks. *Engineering Applications of Artificial Intelligence*, 123:106220.

Mikhalev, V., Kopal, N., and Esslinger, B. (2025). Evaluating GPT-4's proficiency in addressing cryptography examinations. *CRYPTOLOGIA*, 49(2):170–185.

Mishra, G., Gupta, I., Murthy, S. V. S. S. N. V. G. K., and Pal, S. K. (2021). Deep Learning based Cryptanalysis of Stream Ciphers. *DEFENCE SCIENCE JOURNAL*, 71(4):499–506.

Mitchell, F. R. (2014). An Overview of Artificial Intelligence Based Pattern Matching in a Security and Digital Forensic Context. In Blackwell, C. and Zhu, H., editors, *Cyberpatterns: Unifying Design Patterns with Security and Attack Patterns*, pages 215–222. Springer International Publishing, Cham.

Mo, D., Wong, W. K., Liu, X., and Ge, Y. (2022). Concentrated hashing with neighborhood embedding for image retrieval and classification. *INTERNATIONAL JOURNAL OF MACHINE LEARNING AND CYBERNETICS*, 13(6):1571–1587.

Nationales Koordinierungszentrum für Cybersicherheit Deutschland (2025). German r&d institution is seeking partners for eu-horizon-cl3-2025-02-cs-eccc-05: Security of implementations of post-quantum cryptography algorithms - urgent.

Nie, X., Wang, B., Li, J., Hao, F., Jian, M., and Yin, Y. (2021). Deep Multiscale Fusion Hashing for Cross-Modal Retrieval. *IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY*, 31(1):401–410.

Nitaj, A. and Rachidi, T. (2023). Applications of Neural Network-Based AI in Cryptography. *Cryptography*, 7(3).

Ofusori, L., Bokaba, T., and Mhlongo, S. (2024). Artificial Intelligence in Cybersecurity: A Comprehensive Review and Future Direction. *APPLIED ARTIFICIAL INTELLIGENCE*, 38(1).

Pan, S., Liao, M., He, W., Zhang, Y., and Peng, X. (2021). Untrained neural network for cryptanalysis of a phase-truncated-Fourier-transform-based optical cryptosystem. *OPTICS EXPRESS*, 29(26):42642–42649.

Panwar, K., Singh, A., Kukreja, S., Singh, K. K., Shakhovska, N., and Boichuk, A. (2023). Encipher GAN: An End-to-End Color Image Encryption System Using a Deep Generative Model. *SYSTEMS*, 11(1).

Park, C., Lee, J., Kim, Y., Park, J.-G., Kim, H., and Hong, D. (2023). An Enhanced AI-Based Network Intrusion Detection System Using Generative Adversarial Networks. *IEEE Internet of Things Journal*, 10(3):2330–2345. Conference Name: IEEE Internet of Things Journal.

Park, S., Seo, A., Cheong, M., Kim, H., Kim, J., and Son, Y. (2025). Evaluating the Vulnerability of Hiding Techniques in Cyber-Physical Systems Against Deep Learning-Based Side-Channel Attacks. *Applied Sciences*, 15(13):6981. Number: 13 Publisher: Multidisciplinary Digital Publishing Institute.

Perin, G., Chmielewski, L., Batina, L., and Picek, S. (2021). Keep it Unsupervised: Horizontal Attacks Meet Deep Learning. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pages 343–372.

Perin, G., Karayalçin, S., Wu, L., and Picek, S. (2026). I know what your layers did: Layer-wise explainability of deep learning side-channel analysis. *IACR Communications in Cryptology*, 2(4).

Perin, G., Wu, L., and Picek, S. (2022). Exploring Feature Selection Scenarios for Deep Learning-based Side-channel Analysis. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pages 828–861.

Picek, S., Perin, G., Mariot, L., Wu, L., and Batina, L. (2023). SoK: Deep Learning-based Physical Side-channel Analysis. *ACM Comput. Surv.*, 55(11):227:1–227:35.

Randolph, J. (2009). A guide to writing the dissertation literature review. *Practical Assessment, Research, and Evaluation*, 14.

Reddy, M. K. J., Swaroop, A. S., Prasad, A. H., Nithin, D., and Singh, T. (2024). Artificial Neural Networks in Cryptography: Applications, Challenges, and Future Directions for Secure Systems. *Frontiers in Collaborative Research*, 2(1s):20–28. Number: 1s.

Rezaeezade, A. and Batina, L. (2024). Regularizers to the rescue: fighting overfitting in deep learning-based side-channel analysis. *Journal of Cryptographic Engineering*, 14(4):609–629.

Rijsdijk, J., Wu, L., Perin, G., and Picek, S. (2021). Reinforcement Learning for Hyperparameter Tuning in Deep Learning-based Side-channel Analysis. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pages 677–707.

Rivest, R. L. (1993). Cryptography and machine learning. In Goos, G., Hartmanis, J., Imai, H., Rivest, R. L., and Matsumoto, T., editors, *Advances in Cryptology — ASIACRYPT '91*, volume 739, pages 427–439. Springer Berlin Heidelberg, Berlin, Heidelberg. Series Title: Lecture Notes in Computer Science.

Rousseau, R., Garcia-Zorita, C., and Sanz-Casado, E. (2023). Publications during COVID-19 times: An unexpected overall increase. *Journal of Informetrics*, 17(4):101461.

Sang, Y., Sang, J., and Alam, M. S. (2022). Image encryption based on logistic chaotic systems and deep autoencoder. *Pattern Recognition Letters*, 153:59–66.

Sarkar, A. (2021). Deep Learning Guided Double Hidden Layer Neural Synchronization Through Mutual Learning. *NEURAL PROCESSING LETTERS*, 53(2):1355–1384.

Savic, D., Milic, P., and Mazinjanin, B. (2024). Cryptoanalysis of Simple Substitution Ciphers with Genetic Algorithms. *JOURNAL OF SCIENTIFIC & INDUSTRIAL RESEARCH*, 83(1):25–33.

Shan, X., Liu, P., Wang, Y., Zhou, Q., and Wang, Z. (2021). Deep Hashing Using Proxy Loss on Remote Sensing Image Retrieval. *REMOTE SENSING*, 13(15).

Shara, J. (2020). Some Applications of Machine Learning in Cryptography. 4(9).

Sharmila, F. M. and Karuppasamy, K. (2024). An effective cryptanalysis of DES for secure communication using hybrid cryptanalysis and deep neural network. *CONCURRENCY AND COMPUTATION-PRACTICE & EXPERIENCE*, 36(1).

Singh, A., Sivangi, K. B., and Tentu, A. N. (2024a). Machine Learning and Cryptanalysis: An In-Depth Exploration of Current Practices and Future Potential. *Journal of Computing Theories and Applications*, 1(3):257–272. Number: 3.

Singh, P., Pranav, P., Anwar, S., and Dutta, S. (2024b). Leveraging generative adversarial networks for enhanced cryptographic key generation. *CONCURRENCY AND COMPUTATION-PRACTICE & EXPERIENCE*, 36(22).

Singh, P., Pranav, P., and Dutta, S. (2025). A GA-GAN approach for next-generation cryptographic security

with a focus on quantum-resistant cryptography. *Discover Computing*, 28(1):82.

Staib, M. and Moradi, A. (2023). Deep Learning Side-Channel Collision Attack. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2023(3):422–444. Number: 3.

Tellez, F. and Ortiz, J. (2024). Comparing AI Algorithms for Optimizing Elliptic Curve Cryptography Parameters in e-Commerce Integrations: A Pre-Quantum Analysis. *INTERNATIONAL JOURNAL OF ADVANCED COMPUTER SCIENCE AND APPLICATIONS*, 15(6):1539–1553. Num Pages: 15 Place: West Yorkshire Publisher: Science & Information Sai Organization Ltd Web of Science ID: WOS:001277878600001.

Tennyson, S. (2024). Call For Papers: Special Issue on Security and Privacy of Generative AI.

Teodoro, A. A. M., Gomes, O. S. M., Saadi, M., Silva, B. A., Rosa, R. L., and Rodriguez, D. Z. (2022). An FPGA-Based Performance Evaluation of Artificial Neural Network Architecture Algorithm for IoT. *WIRELESS PERSONAL COMMUNICATIONS*, 127(2):1085–1116.

Ullah, F. and Pun, C.-M. (2023). Deep self-learning based dynamic secret key generation for novel secure and efficient hashing algorithm. *INFORMATION SCIENCES*, 629:488–501.

Vaswani, A., Shazeer, N., Parmar, N., Uszkoreit, J., Jones, L., Gomez, A. N., Kaiser, L., and Polosukhin, I. (2017). Attention is all you need. In *Proceedings of the 31st International Conference on Neural Information Processing Systems*, NIPS'17, page 6000–6010, Red Hook, NY, USA. Curran Associates Inc.

Wang, H. and Dubrova, E. (2021). Tandem Deep Learning Side-Channel Attack on FPGA Implementation of AES. *SN Computer Science*, 2(5):373.

Wang, J., Xu, S., Zheng, F., Lu, K., Song, J., and Shao, L. (2021). Learning Efficient Hash Codes for Fast Graph-Based Data Similarity Retrieval. *IEEE TRANSACTIONS ON IMAGE PROCESSING*, 30:6321–6334.

Wang, J., Zeng, Z., Chen, B., Wang, Y., Liao, D., Li, G., Wang, Y., and Xia, S.-T. (2024). Hugs Bring Double Benefits: Unsupervised Cross-Modal Hashing with Multi-granularity Aligned Transformers. *INTERNATIONAL JOURNAL OF COMPUTER VISION*, 132(8):2765–2797.

Wiafe, I., Koranteng, F. N., Obeng, E. N., Assyne, N., Wiafe, A., and Gulliver, S. R. (2020). Artificial Intelligence for Cybersecurity: A Systematic Mapping of Literature. *IEEE Access*, 8:146598–146612. Conference Name: IEEE Access.

Won, Y.-S., Han, D.-G., Jap, D., Bhasin, S., and Park, J.-Y. (2021). Non-Profiled Side-Channel Attack Based on Deep Learning Using Picture Trace. *IEEE ACCESS*, 9:22480–22492. Num Pages: 13 Place: Piscataway Publisher: Ieee-Inst Electrical Electronics Engineers Inc Web of Science ID: WOS:000617362300001.

Wu, L., Won, Y.-S., Jap, D., Perin, G., Bhasin, S., and Picek, S. (2021). Ablation Analysis for Multi-device Deep Learning-based Physical Side-channel Analysis. Publication info: Published elsewhere. IEEE Transactions on Dependable and Secure Computing.

Wu, Z., Qiao, K., Wang, Z., Cheng, J., and Zhu, L. (2024). Mixture Differential Cryptanalysis on Round-Reduced SIMON32/64 Using Machine Learning. *MATHEMATICS*, 12(9).

Xu, J.-X., Ren, Z.-A., Chen, Y.-P., Zhang, C.-H., and Wang, Q. (2022a). Optimal resource allocation of quantum digital signatures with machine learning. *Quantum Information Processing*, 21(9):338.

Xu, L., Zeng, X., Li, W., and Bai, L. (2022b). IDHashGAN: Deep Hashing With Generative Adversarial Nets for Incomplete Data Retrieval. *IEEE TRANSACTIONS ON MULTIMEDIA*, 24:534–545.

Yan, C., Gong, B., Wei, Y., and Gao, Y. (2021). Deep Multi-View Enhancement Hashing for Image Retrieval. *IEEE TRANSACTIONS ON PATTERN ANALYSIS AND MACHINE INTELLIGENCE*, 43(4):1445–1451.

Yap, T., Benamira, A., Bhasin, S., and Peyrin, T. (2023). Peek into the Black-Box: Interpretable Neural Network using SAT Equations in Side-Channel Analysis. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pages 24–53.

Yi, H. (2023). Machine Learning Method with Applications in Hardware Security of Post-Quantum Cryptography. *JOURNAL OF GRID COMPUTING*, 21(2).

Yuan, K., Huang, Y., Du, Z., Li, J., and Jia, C. (2024). A multi-layer composite identification scheme of cryptographic algorithm based on hybrid random forest and logistic regression model. *Complex & Intelligent Systems*, 10(1):1131–1147.

Yuan, K., Huang, Y., Li, J., Jia, C., and Yu, D. (2023). A Block Cipher Algorithm Identification Scheme Based on Hybrid Random Forest and Logistic Regression Model. *Neural Processing Letters*, 55(3):3185–3203.

Yuan, M., Qin, B., Li, J., Qian, J., and Xin, Y. (2021). Hidden multi-distance loss-based full-convolution hashing. *APPLIED SOFT COMPUTING*, 109.

Zhang, Q. and Li, J. (2022). Single Exposure Phase-Only Optical Image Encryption and Hiding Method via Deep Learning. *IEEE Photonics Journal*, 14(1):1–8.

Zhang, Q.-y., Zhao, X.-j., Zhang, Q.-w., and Li, Y.-z. (2022). Content-based encrypted speech retrieval scheme with deep hashing. *MULTIMEDIA TOOLS AND APPLICATIONS*, 81(7):10221–10242.

Zhu, L., Cui, H., Cheng, Z., Li, J., and Zhang, Z. (2021). Dual-Level Semantic Transfer Deep Hashing for Efficient Social Image Retrieval. *IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY*, 31(4):1478–1489.

Zhuang, X. and Yan, A. (2023). Deep-learning-based ciphertext-only attack on optical scanning cryptosystem. *OPTICS AND LASER TECHNOLOGY*, 157.

Zolfaghari, B. and Koshiba, T. (2022). AI Makes Crypto Evolve. *Applied System Innovation*, 5(4):75. Number: 4 Publisher: Multidisciplinary Digital Publishing Institute.

APPENDIX

Name	Relevant Topics
CASCASDE 2026	Machine learning attacks and countermeasures, Computer-aided cryptographic engineering, Automated and machine learning analysis frameworks for embedded systems
SAC 2025	Machine learning and cryptography: applications of machine learning to cryptography and Cryptanalysis and application of cryptanalytic techniques against machine learning algorithms.
AIHWS 2025	AI-assisted (hardware) design cycle, AI-based cryptanalysis
LightSEC 2025	AI for cryptography, Security and privacy implications of AI
AISec 2025	Security-related AI problems: Adaptive side-channel attacks, Secure multiparty computation and cryptographic approaches, AI approaches to trust and reputation, Vulnerability testing through intelligent probing (e.g. fuzzing)
CHES 2025/2026	Computer aided cryptographic engineering

Table 3: Conferences and workshops with AI topics in the area of cryptography (2025–2026), identified via the Security Deadlines list (https://sec-deadlines.github.io/).

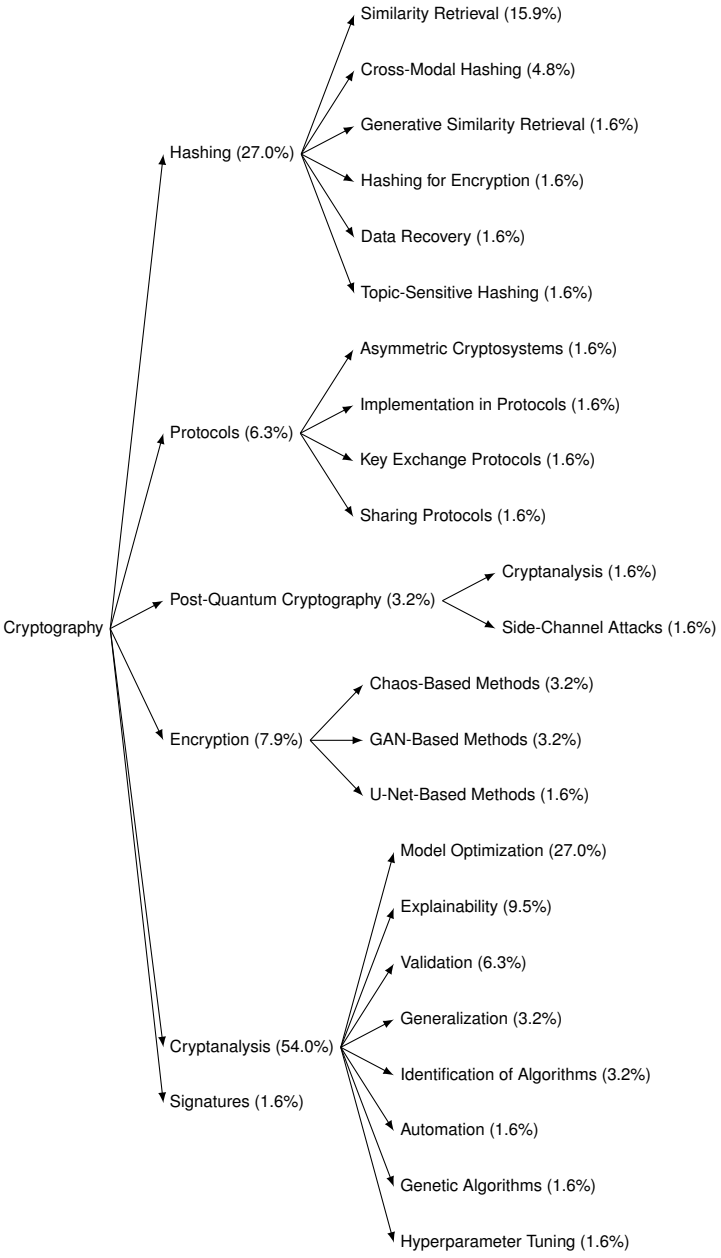


Figure 4: Breakdown of papers (2021–2025) into subcategories

Cryptanalysis	Hashing	Encryption	Protocols	Post-Quantum Cryptography	Signatures
(He et al., 2021)	(Nie et al., 2021),	(Erkan et al., 2022)	(Teodoro et al., 2022)	(Yi, 2023)	(Xu et al., 2022a)
(Kubota et al., 2021)	(Yan et al., 2021),	(Sang et al., 2022)	(Sarkar, 2021)	(Coyle et al., 2022)	
(Perin et al., 2021)	(Zhu et al., 2021),	(Zhang and Li, 2022)	(Meraouche et al., 2023)		
(Rijsdijk et al., 2021)	(Christy and Dhanalakshmi, 2022),	(Cintas-Canto et al., 2023)	(Kumar et al., 2024a)		
(Bao et al., 2022)	(Shan et al., 2021),	(Kumar et al., 2024b)			
(Benamira et al., 2021)	(Wang et al., 2021),	(Panwar et al., 2023)			
(Brunetta and Picazo-Sanchez, 2022)	(Xu et al., 2022b),	(Singh et al., 2024b)			
(Chong and Salam, 2021)	(Yuan et al., 2021),	(Tellez and Ortiz, 2024)			
(Ito et al., 2021)	(Ding et al., 2022a),	(Singh et al., 2025)			
(Liao et al., 2021)	(Hussain et al., 2022),				
(Lu et al., 2021)	(Lei et al., 2023),				
(Mishra et al., 2021)	(Mo et al., 2022),				
(Pan et al., 2021)	(Zhang et al., 2022),				
(Wang and Dubrova, 2021)	(Ullah and Pun, 2023),				
(Won et al., 2021)	(Hawkes et al., 2024),				
(Wu et al., 2021)	(Huo et al., 2024),				
(Barenghi et al., 2022)	(Li et al., 2024),				
(Golder et al., 2022)	(Wang et al., 2024),				
(Hu et al., 2022)	(Chen et al., 2025a),				
(Kwon et al., 2022)	(Chen et al., 2025b)				
(Perin et al., 2022)					
(Perin et al., 2026)					
(Yuan et al., 2023)					
(Zhuang and Yan, 2023)					
(Agate et al., 2023)					
(Bao et al., 2023)					
(Kim et al., 2023)					
(Savic et al., 2024)					
(Sharmila and Karuppasamy, 2024)					
(Staib and Moradi, 2023)					
(Yap et al., 2023)					
(Yuan et al., 2024)					
(Chang et al., 2024)					
(Kim et al., 2025)					
(Mikhalev et al., 2025)					
(Wu et al., 2024)					
(Hou et al., 2025)					
(Liu et al., 2025)					
(Li et al., 2025)					
(Park et al., 2025)					

Table 4: Papers and their assignment to categories