International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 09 | Sept - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

Evolution of SIM and ESIM Security: Authentication, Fraud, and Emerging Defenses

Arya Dhanesh
Department of Computer Science and Engineering(Cyber Security)
Vimal Jyothi Engineering College
Chemperi, Kannur
Email: koroth.arya@gmail.com

Jyothika K
Department of Computer Science and Engineering(Cyber Security)
Vimal Jyothi Engineering College
Chemperi, Kannur
Email: jyothikavineesh@gmail.com

Malavika Jayaraj
Department of Computer Science and Engineering(Cyber Security)
Vimal Jyothi Engineering College
Chemperi, Kannur
Email: malavikajayaraj4@gmail.com

Nevin Jose Antony
Department of Computer Science
Vimal Jyothi Engineering College
Chemperi, Kannur
Email:nevinjose@gmail.com

Ms.Anu Treesa George
Assistant Professor
Department of Computer Science
Vimal Jyothi Engineering College
Chemperi, Kannur
Email:anuvellackallil@vjec.ac.in

***Abstract*—The transition of Subscriber Identity Module (SIM) technology from traditional physical cards to embedded SIMs (eSIMs) has brought significant advances in flexibility, scalability, and device interoperability within the telecommunications ecosystem, but it has simultaneously introduced critical challenges in terms of security and fraud prevention. Early research beginning in the early 2000s concentrated on vulnerabilities in GSM authentication mechanisms, demonstrating how attackers could exploit weaknesses in algorithms such as COMP128 to clone SIM cards and impersonate legitimate users. As mobile networks evolved into UMTS, LTE, and eventually 5G, studies revealed that although cryptographic protocols improved, attackers still leveraged human and organizational weaknesses, such as poorly implemented authentication checks by carriers, to perform SIM-swap fraud and account takeovers. In recent years, eSIM technology and GSMA's Remote SIM Provisioning (RSP) standard have enabled seamless subscription management and expanded use in the Internet of Things (IoT), but they have also widened the attack surface through new threats such as unauthorized provisioning and profile hijacking. This review analyzes research from 2002 onwards, emphasizing how early foundational works on cloning and authentication flaws paved the way for current investigations into eSIM security, large-scale fraud detection, and advanced defense frameworks. It highlights not only technical contributions but also socio-technical dimensions of fraud, concluding that although substantial progress has been made in protocol security, scalable fraud detection, and blockchain-based provisioning, there remains a persistent lack of real-time, user-centric defenses that empower individuals to counter hijacking attempts effectively.**

***Index Terms*—GSM security, SIM cloning, eSIM, Remote SIM Provisioning (RSP), SIM-swap fraud, telecom fraud detection, anomaly detection, blockchain security, post-quantum cryptography.**

I. Introduction

From the early days of GSM networks in the late 1990s and early 2000s, the security of SIM cards has been at the center of mobile communication security research. According to preliminary research, the security of authentication algorithms like COMP128 was less robust than expected, allowing hackers to obtain secret keys and duplicate SIM cards. This allowed for the creation of cloned identities that could be used fraudulently and illegallyThese flaws soon showed that mobile communication security required comprehensive attention to implementation techniques, carrier procedures, and fraud monitoring, and was not just a cryptographic issue. Stronger encryption standards and mutual authentication were introduced as the industry moved to UMTS and LTE networks, improving resistance to direct cryptographic attacks. However, adversaries changed their strategies to use signaling protocols like SS7 and social engineering to persuade mobile operators to transfer service to attacker-controlled SIMs, thus initiating SIM-swap fraud. The advent of eSIMs and the GSMA's Remote SIM Provisioning (RSP) framework has introduced a new paradigm in subscription management that allows consumers and IoT devices to remotely switch carriers and manage multiple profiles. While these capabilities promise scalability and flexibility, they also present new risks such as unauthorized provisioning, large-scale IoT exploitation, and sophisticated profile hijacking. Reviewing two decades of research provides a comprehensive picture of how threats evolved, how technical and organizational responses emerged, and what gaps remain in ensuring secure and fraud-resilient SIM and eSIM ecosystems.

II. Literature Survey

TABLE I
COMPARISON OF KEY SECURITY PROTOCOL VERIFICATION PAPERS

Ref	Name	Advantages	Disadvantages
[1]	A Logic of Authentication	• Introduced BAN logic to formalize reasoning about authentication protocols • Detected subtle design flaws and suggested improvements	• Operates at abstract level, not linked to real implementations • Cannot detect cryptographic weaknesses or low-level issues
[2]	Using Encryption for Authentication in Large Networks	• Proposed practical authentication protocols using both symmetric and public-key cryptography • Highlighted decentralized authentication without full reliance on central authority	• Protocols provided only illustrative, not fully engineered solutions • Did not address broader attacks like traffic analysis
[3]	Formal Verification of Consumer Remote SIM Provisioning Mutual Authentication	• Applied BAN logic to eSIM Remote SIM Provisioning (RSP) protocols • Proved mutual authentication under well-defined assumptions • Suggested enhancements using blockchain and cloud-based methods	• Dependent on assumptions of BAN logic; limited expressiveness • Identified but did not mitigate certain vulnerabilities
[4]	DEEPSEC: Deciding Equivalence Properties in Security Protocols	• First exact decision procedure for trace equivalence and bisimilarity (bounded sessions) • Scales better than previous tools and supports broader primitives	• Guarantees only in bounded session settings • Still computationally heavy for complex protocols
[5]	Automated Analysis and Verification of TLS 1.3 (0-RTT, Resumption, Delayed Auth)	• Comprehensive symbolic analysis of TLS 1.3 draft-10 using Tamarin • Verified secrecy, PFS, and authentication across multiple handshake modes • Discovered potential impersonation attack in resumption	• Analysis tied to draft-10, later changes required re-analysis • Focused only on symbolic model, not full computational proofs
[6]	A Comprehensive Symbolic Analysis of TLS 1.3	• Built most complete symbolic model of TLS 1.3 draft-21 • Verified secrecy, authentication, PFS, and downgrade resilience with Tamarin • Provided annotated specification for transparency	• Model tied to draft-21, risk of outdated results if spec changes • Could not fully guarantee strong authentication in all cases
[7]	A Study of Emerging Trends in SIM Swapping Crime	• Analyzed global SIM swap cases and trends • Proposed countermeasures including stronger authentication and awareness	• Lacks formal verification framework • Focused more on policy recommendations than technical solutions
[8]	Securing SIM Toolkit-Based Mobile Money Apps Against SIM Swap Using Location Data	• Novel defense model using user location to detect fraudulent SIM swaps • Lightweight approach with minimal computational overhead	• Effectiveness depends on accurate location data • Privacy concerns around storing user location
[9]	Timestamps in Key Distribution Protocols	• Prevents replay of compromised keys • Replaces handshake with simpler timestamp check	• Relies on reasonably synchronized clocks • Private key compromise still breaks security
[10]	Downgrade Resilience in Key-Exchange Protocols	• Prevents attackers from forcing weaker cryptographic algorithms during communication. • Ensures secure negotiation of protocols, maintaining confidentiality and integrity.	• Increases protocol complexity, making implementation harder. • May lead to incompatibility issues with older systems that only support weaker algorithms.

TABLE II
COMPARISON TABLE

Ref.	Name	Advantages	Disadvantages
[11]	The EMV Standard: Break, Fix, Verify	• Formal symbolic model enables detection of subtle protocol flaws • Identifies real-world attacks such as PIN bypass and offline fraud • Suggests verifiable improvements that strengthen EMV security	• Complexity of EMV specification makes verification challenging • Some flaws require major infrastructure changes • Still vulnerable to implementation-specific issues
[12]	Understanding the Implications of SIM Card Swap Fraud in India	• Highlights severe risks of SIM-swap attacks in financial and social domains • Raises awareness on legal, technical, and preventive measures • Provides real-world case studies to illustrate impact	• Prevention heavily depends on telecom provider security • Victims often face irreversible financial and reputational damage • Limited legal enforcement and awareness in India
[13]	Verified Models and Reference Implementations for the TLS 1.3 Standard Candidate	• Provides both symbolic and computational proofs for TLS 1.3 • RefTLS offers high-assurance, formally analyzed implementation • Addresses downgrade, replay, and cross-protocol attacks	• Verification excludes some low-level implementation details • Proofs become obsolete as drafts evolve • Legacy TLS versions still introduce vulnerabilities
[14]	Toward Post-Quantum Digital Certificate for eSIM	• Introduces PQC-based digital certificates for eSIM authentication • Ensures resilience against quantum adversaries • Facilitates smooth migration from classical PKI	• Larger key/signature sizes increase communication overhead • Limited practical deployments so far • Transition requires industry-wide adoption
[15]	The Applied Pi Calculus: Mobile Values, New Names, and Secure Communication	• Extends π-calculus with functions and equations for realistic modeling • Provides strong foundations for analyzing security protocols • Basis of widely used tools like ProVerif	• Reasoning and proofs can be complex • Abstract models may not capture all practical attack vectors • Requires expertise in formal methods to apply effectively

A. Timestamps in Key Distribution Protocols [9]

It has long been acknowledged that a key component of secure network communication is key distribution. The generation and sharing of session keys in earlier systems depended on a reliable authentication server; nevertheless, it was discovered that these techniques were susceptible to replay attacks in the event that the keys were compromised. Researchers implemented timestamps in key distribution systems to solve this problem. By eliminating the need for additional handshake procedures and guaranteeing the freshness of session keys, timestamps improve security and efficiency. This technique has been effectively used in both public key and symmetric systems, and it has impacted the development of contemporary authentication methods and secure key management frameworks like PKI and Kerberos.

B. Automated Analysis and Verification of TLS 1.3: 0-RTT, Resumption and Delayed Authentication [5]

The automated verification of TLS 1.3 by Cremers, Horvat, Hoyland, Scott, and van der Merwe focused on delayed authentication and 0-RTT resumption. Understanding complicated relationships between various key exchange modalities remains a difficulty because previous publications only examined limited handshake instances or older versions of TLS. The authors developed a thorough model of TLS 1.3 using the Tamarin prover, which covered several concurrent sessions and different handshake techniques including PSK and PSK-DHE. Important characteristics including confidentiality, authentication, and handshake consistency were validated by their analysis. More significantly, it exposed a vulnerability to client impersonation when PSK resumption was coupled with delayed authentication. In addition to pointing out possible dangers, these results offered

insightful advice that helped TLS 1.3 be improved throughout standardization process.

C. DEEPSEC: Deciding Equivalence Properties in Security Protocols [4]

Beyond reachability analysis, Cheval, Kremer, and Rakotonirina tackled the topic of confirming equivalency qualities in security protocols. They established decidability for bounded-session protocols under subterm convergent rewriting systems and provided novel complexity results for labeled bisimilarity, trace equivalence, and static equivalence. Their method permits richer classes of cryptographic primitives and protocol behaviors while avoiding approximations.

When compared to earlier tools like APTE, SPEC, and AKISS, the authors' process showed notable performance gains in the tool DEEPSEC. DEEPSEC demonstrated scalability across a wide range of benchmarks, including both traditional authentication procedures and sophisticated systems such as e-voting techniques and mobile network protocols. By providing accurate and effective techniques for examining privacy and indistinguishability properties, this study advanced the theory and practice of protocol verification.

D. A Comprehensive Symbolic Analysis of TLS 1.3 [6]

Cremers, Horvat, Hoyland, Scott, and van der Merwe presented a symbolic verification of TLS 1.3, offering one of the most detailed analyses prior to the protocol's standardization. Unlike earlier works that covered only selected handshake modes, their study modeled all handshake variants, including PSK, PSK-DHE, resumption, and 0-RTT. Using the Tamarin prover, they provided formal guarantees for properties such as secrecy, forward secrecy, authentication, and key uniqueness.

The study also uncovered an unexpected behavior affecting strong authentication guarantees in some implementations. A novel contribution of this work was an annotated TLS 1.3 specification that explicitly mapped modeled elements to their formal representation, increasing transparency and reproducibility. This research significantly strengthened confidence in TLS 1.3's design and influenced both the academic community and the IETF working group.

E. A Logic of Authentication [1]

Burrows, Abadi, and Needham introduced a formal logic for reasoning about authentication protocols, aiming to address the challenges of protocol design and verification. Many early authentication schemes suffered from redundancies and subtle flaws, despite their apparent simplicity. The authors proposed a logic that represents the beliefs of principals and the evolution of those beliefs through communication steps, enabling a precise understanding of authentication goals and assumptions.

Their system was used to examine popular protocols including X.509 and Needham–Schroeder, successfully identifying flaws and making recommendations for enhancements. One of the first systematic methods for assessing authenticity was offered by this work, which had an impact on decades of later protocol correctness research. By emphasizing the value of logical reasoning in protocol verification, it laid the groundwork for formal approaches in security.

F. The Applied Pi Calculus: Mobile Values, New Names, and Secure Communication [15]

An important expansion of the traditional pi calculus, the Applied Pi Calculus was introduced by Abadi, Blanchet, and Fournet. It was created to handle values, functions, and cryptographic operations for communication and concurrent reasoning. The applied pi calculus offers a richer framework for simulating actual security procedures than the pure pi calculus, which just transmits atomic names. The applied pi calculus permits structured values and equations. The methodical development of syntax, semantics, equivalencies, and proving strategies has been made possible by this formalism. The use of this work in protocol verification tools like ProVerif, which can automatically assess the security of cryptographic protocols, is one of its most significant results. Their work established the foundation for a cohesive, adaptable, and useful framework that is still actively applied in secure communication research.

G. The EMV Standard: Break, Fix, Verify [11]

A formal symbolic study of the EMV standard, the international protocol for smartcard-based payments, was carried out by Basin, Sasse, and Toro-Pozo. They created the first thorough symbolic model of EMV, encompassing its various authentication techniques, verification modes, and transaction kinds, using the Tamarin verification tool. Their investigation uncovered serious weaknesses in Visa's contactless payment system, such as a fraudulent offline transaction attack that tricks the terminal and a PIN bypass attack that permits unlawful high-value transactions without knowing the PIN. They illustrated the usefulness of these flaws with a proof-of-concept Android application. Additionally, they suggested simple enhancements to terminal implementations that can stop these assaults without requiring modifications to cards that are currently in use. Their findings highlight the importance of rigorous formal analysis in financial security protocols, ensuring that real-world systems match their intended security guarantees.

H. Verified Models and Reference Implementations for the TLS 1.3 Standard Candidate [13]

Bhargavan, Blanchet, and Kobeissi analyzed TLS 1.3, the next-generation transport security protocol, which was designed to address known vulnerabilities in TLS 1.2 and

improve performance. Their work combined symbolic verification using ProVerif, computational proofs using CryptoVerif, and a formally analyzed reference implementation called RefTLS. By studying TLS 1.3 across 18 drafts, they reconstructed both known and new vulnerabilities, including issues in early designs of 0-RTT authentication and cross-protocol weaknesses when TLS 1.3 interacts with TLS 1.2. Their computational proof for TLS 1.3 Draft-18 demonstrated strong security guarantees under standard cryptographic assumptions, while the RefTLS implementation showcased how verified protocol models can directly influence secure software development. This methodology bridged the gap between theoretical analysis and real-world implementations, contributing to the finalization of a robust TLS 1.3 standard.

I. Downgrade Resilience in Key-Exchange Protocols [10]

Configurable key-exchange protocols like TLS, SSH, IPsec, and ZRTP are frequently subject to downgrade attacks. Bhargavan, Brzuska, Fournet, Green, Kohlweiss, and Zanella-Be´guelin tackled this persistent problem. These protocols are susceptible to adversaries who coerce peers into negotiating weaker modes since they frequently offer several cryptographic algorithms and protocol versions. The authors created a methodology to examine the resilience of protocols through their negotiating sub-protocols and put forth a formal definition of downgrade security. In addition to providing design patterns to fortify protocols against such threats, their investigation uncovered both known and new downgrade flaws, proving that TLS up to version 1.2 is not downgrade secure. Notably, their research helped TLS 1.3 become much more resilient by influencing the addition of required downgrade protections. This study advances our knowledge of the need to carefully combine robust downgrade protection mechanisms with configurability and agility in cryptographic systems.

J. Formal Verification of Consumer Remote SIM Provisioning Common Mutual Authentication using BAN Logic [3]

The security of Remote SIM Provisioning (RSP) protocols is examined in this study with an emphasis on mutual authentication between the Subscription Manager Data Preparation+ (SM-DP+) server and the embedded Universal Integrated Circuit Card (eUICC). The authors explicitly confirm that the Common Mutual Authentication protocol meets its stated security objectives using Burrows-Abadi-Needham (BAN) logic. The study contributes to the safe deployment of eSIM in mobile and IoT ecosystems by highlighting flaws and offering solutions through blockchain integration, cloud-based authentication, and automated verification mechanisms, all while proving the accuracy of the technology.

K. Understanding the Implications of SIM Card Swap Fraud in India: A Comprehensive Study [12]

In India, SIM swap fraud occurs when hackers deceive mobile service providers into moving victims' numbers to phony SIM cards. This paper examines this phenomenon. It highlights the shortcomings of the legal frameworks under the Indian Penal Code and IT Act by reviewing actual incidents that resulted in significant financial losses and identity theft. Preventive measures like strong passwords, two-factor authentication, and legislative reforms are highlighted in the study. It draws attention to the growing need for more public awareness and more robust telecom protections in India's cyber environment by providing case studies and preventive measures.

L. Securing SIM Toolkit-Based Mobile Money Applications Against SIM Swap Attacks Using User Location Data [8]

In response to the increasing frequency of SIM swap attacks on mobile money systems, this study introduces a novel location-based verification technique. By comparing the locations of SIM swap requests with those of previous transactions or connectivity points using the Haversine formula, the program detects anomalies when the indicated trip speed exceeds acceptable thresholds. The experimental results show little computational overhead (0.16 seconds per request), ensuring a viable deployment. By lessening the impact of identity theft and social engineering threats, the strategy improves mobile money security, particularly in areas like Sub-Saharan Africa where these services are popular.

M. Using Encryption for Authentication in Large Networks of Computers [2]

Needham and Schroeder's seminal work introduces encryption-based authentication systems for dispersed computer networks. It discusses methods for establishing authenticated interactive communication, authenticated mail exchange, and digital signatures. Both public-key and traditional (symmetric) encryption techniques are taken into account. Threats including replay, impersonation, and message tampering are addressed by the protocols, which are made for decentralized contexts without the need for a central authority. The paper laid foundational concepts in network authentication and remains influential in modern cryptographic protocol design.

N. A Study of the Emerging Trends in SIM Swapping Crime and Effective Countermeasures [7]

This study examines the global patterns of SIM switching offenses, which increased during the COVID-19 pandemic. It divides assaults into three phases: exploitation of compromised accounts, fake SIM duplication, and theft of personal data. The report draws attention to weaknesses in subscriber authentication processes, particularly as eSIM deployment increases. By looking at incidents from throughout the world, it suggests countermeasures include public awareness campaigns, coop-

eration between telcos and financial institutions, and stricter identification verification for SIM re-issuance. The results highlight SIM swapping as a dynamic cyberthreat that calls for coordinated policy and technical solutions.

O. Toward Post-Quantum Digital Certificate for eSIM [14]

This study examines the weaknesses of the Elliptic Curve Digital Signature Algorithm (ECDSA)-based eSIM authentication systems that are vulnerable to quantum computing attacks. The need to move toward Post-Quantum Cryptography (PQC) is emphasized, with special attention paid to NIST-selected algorithms including Dilithium, Falcon, and SPHINCS+. The article highlights the research need in implementing post-quantum certificates specifically to eSIM authentication while reviewing the literature on post-quantum certificates in networking protocols such as X.509 PKI, TLS, and QUIC.The authors offer a framework for mutual authentication between mobile clients and core networks, assess certificate verification performance, and describe a design plan to replace pre-quantum digital signatures with PQC algorithms in eSIMs.

III. Conclusion

A definite trajectory in the development of SIM and eSIM security research can be seen in the literature studied over the course of two decades. The majority of early research in the 2000s concentrated on GSM vulnerabilities, such as weaknesses in authentication algorithms like COMP128 that made large-scale fraud and practical SIM cloning possible. These pioneering research showed that mobile communication systems were immediately and visibly threatened by cryptographic flaws. Research found that as networks switched to UMTS and LTE, adversaries adjusted by taking advantage of signaling flaws like SS7 and using social engineering strategies to carry out SIM-swap attacks using lax carrier authentication protocols, even as cryptographic safeguards improved.

With the introduction of eSIM technology and the GSMA's Remote SIM Provisioning (RSP) standard, the attack surface expanded significantly. Recent research highlights vulnerabilities in provisioning protocols, access control mechanisms, and authentication frameworks, suggesting that while eSIM enhances flexibility, it requires stronger assurance frameworks to prevent profile hijacking and unauthorized provisioning. Parallel to these protocol-level investigations, a growing body of work has focused on fraud detection, moving from statistical anomaly detection in the early 2000s to modern machine learning and graph neural network models that can analyze large-scale, dynamic datasets. Blockchain-based provisioning and IoT-focused frameworks represent emerging solutions aimed at increasing auditability and resilience in distributed deployments.

The assessment emphasizes that user-facing, real-time defensive mechanisms are still lacking in spite of these developments. Most proposed solutions strengthen carrier-side authentication, backend fraud detection, or protocol-level resilience, but end users remain vulnerable to immediate threats such as SIM-swap fraud and hijacking attempts. Future research must therefore bridge this gap by designing integrated frameworks that combine strong cryptographic protocols, scalable detection systems, and effective user notification mechanisms. Such developments will be critical to ensuring the secure evolution of SIM and eSIM ecosystems in the 5G and post-quantum communication era.

References

[1] M. Burrows, M. Abadi, and R. Needham, "A logic of authentication," *ACM Trans. Comput. Syst.*, vol. 8, no. 1, p. 18–36, Feb. 1990. [Online]. Available: https://doi.org/10.1145/77648.77649

[2] R. M. Needham and M. D. Schroeder, "Using encryption for authentication in large networks of computers," *Commun. ACM*, vol. 21, no. 12, p. 993–999, Dec. 1978. [Online]. Available: https://doi.org/10.1145/359657.359659

[3] J. K. Lastre, Y. Ko, H. Kwon, B. Kim, and I. You, "Formal verification of consumer remote sim provisioning common mutual authentication using ban logic," in *2025 1st International Conference on Consumer Technology (ICCT-Pacific)*, 2025, pp. 1–4.

[4] V. Cheval, S. Kremer, and I. Rakotonirina, "Deepsec: Deciding equivalence properties in security protocols theory and practice," in *2018 IEEE Symposium on Security and Privacy (SP)*, 2018, pp. 529–546.

[5] C. Cremers, M. Horvat, S. Scott, and T. van der Merwe, "Automated analysis and verification of tls 1.3: 0-rtt, resumption and delayed authentication," in *2016 IEEE Symposium on Security and Privacy (SP)*, 2016, pp. 470–485.

[6] C. Cremers, M. Horvat, J. Hoyland, S. Scott, and T. van der Merwe, "A comprehensive symbolic analysis of tls 1.3," in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '17. New York, NY, USA: Association for Computing Machinery, 2017, p. 1773–1788. [Online]. Available: https://doi.org/10.1145/3133956.3134063

[7] M. Kim, J. Suh, and H. Kwon, "A study of the emerging trends in sim swapping crime and effective countermeasures," in *2022 IEEE/ACIS 7th International Conference on Big Data, Cloud Computing, and Data Science (BCD)*, 2022, pp. 240–245.

[8] C. Cheruyot, R. Kouame, and H. Inaba, "Securing sim toolkit-based mobile money applications against sim swap attacks using user location data," 10 2024, pp. 100–104.

[9] D. E. Denning and G. M. Sacco, "Timestamps in key distribution protocols," *Commun. ACM*, vol. 24, no. 8, p. 533–536, Aug. 1981. [Online]. Available: https://doi.org/10.1145/358722.358740

[10] K. Bhargavan, C. Brzuska, C. Fournet, M. Green, M. Kohlweiss, and S. Zanella-Be´guelin, "Downgrade resilience in key-exchange protocols," in *2016 IEEE Symposium on Security and Privacy (SP)*, 2016, pp. 506–525.

[11] D. Basin, R. Sasse, and J. Toro-Pozo, "The emv standard: Break, fix, verify," 06 2020.

[12] S. Bhavana, D. Doreen Hephzibah Miriam, and C. Rene Robin, "Understanding the implications of sim card swap fraud in india: A comprehensive study," in *2024 International Conference on Communication, Computing and Internet of Things (IC3IoT)*, 2024, pp. 1–8.

[13] K. Bhargavan, B. Blanchet, and N. Kobeissi, "Verified models and reference implementations for the tls 1.3 standard candidate," in *2017 IEEE Symposium on Security and Privacy (SP)*, 2017, pp. 483–502.

[14] Q. Khan, S. Purification, R. Cheruiyot, J. Kim, J. Kim, and S.-Y. Chang, "Toward post-quantum digital certificate for esim," in *2024 Silicon Valley Cybersecurity Conference (SVCC)*, 2024, pp. 1–3.

[15] M. Abadi, B. Blanchet, and C. Fournet, "The applied pi calculus: Mobile values, new names, and secure communication," *J. ACM*, vol. 65, no. 1, Oct. 2017. [Online]. Available: https://doi.org/10.1145/3127586