Digital Security of Subscriber Identity Modules: Evolution, Emerging Threats, and Futureproofing for 5G, IoT, and the Quantum Era

Dr Zulkharnain Muhammad[1], Dr Ali Ahmed Alqudaihi[2]

[1,2]Electrical Engineering Technology Department, College of Applied Industrial Technology (CAIT), Jazan University, 45142, Saudi Arabia

ABSTRACT:

The Subscriber Identity Module (SIM) has been the cornerstone of mobile network security, providing a trusted anchor for subscriber identity and authentication. However, the evolution of mobile technology, driven by the advent of 5G, the Internet of Things (IoT), and the need for device miniaturization, has necessitated a transformation of the SIM from a physical form factor to embedded (eSIM) and integrated (iSIM) solutions. This transition has altered the security landscape, introducing new benefits and complexities. While eSIM and iSIM technologies offer enhanced tamper resistance and remote provisioning capabilities, they also present novel attack surfaces, such as remote provisioning exploits and firmware vulnerabilities. Moreover, the contemporary threat landscape encompasses sophisticated social engineering attacks, like SIM swapping, and architectural weaknesses inherent to the 5G ecosystem, such as the security paradox of network slicing. As the industry looks ahead to the post-quantum era, the computational demands of post-quantum cryptography pose significant challenges for resource-constrained SIMs. Strategies for a secure transition include the development of lightweight post-quantum protocols, the adoption of crypto-agility, and a hybrid approach combining classical and post-quantum algorithms. Future research must address the security of inter-operator protocols, the optimization of post-quantum algorithms for constrained devices, and the secure lifecycle management of iSIMs. The SIM's role as a trusted identity anchor remains critical in the evolving mobile landscape, necessitating a holistic, ecosystem-wide approach to security.

KEYWORDS : Subscriber Identity Module (SIM)- 5G- Internet of Things (IoT)- Embedded SIM (eSIM)- Integrated SIM (iSIM)- Post-quantum cryptography- Network slicing- Authentication- UICC

1. Introduction

The Subscriber Identity Module (SIM) stands as the foundational secure element in mobile telecommunications, providing a trusted anchor for identity and authentication in cellular networks. The SIM, or more accurately the Universal Integrated Circuit Card (UICC), is a specialized integrated circuit designed to securely store the International Mobile Subscriber Identity (IMSI) number and its associated key, known as the Authentication Key (Ki).[1] These credentials are paramount for authenticating a subscriber on mobile networks, from traditional mobile phones to tablets and laptops. The security architecture of the SIM card has been meticulously defined and maintained by key standards bodies, including the European Telecommunications Standards Institute (ETSI) and the 3rd Generation Partnership Project (3GPP), establishing a robust framework of trust that has underpinned mobile network security for decades.[2]

However, the traditional physical SIM is undergoing a profound transformation. This change is driven by the demands of contemporary mobile technology, most notably the advent of 5G, the exponential growth of the Internet of Things (IoT), and the increasing need for device miniaturization and efficiency.[3] The shift from a removable physical form factor to embedded (eSIM) and integrated (iSIM) solutions has been a direct response to these market forces. Concurrently, the digital threat landscape has become more complex and sophisticated, encompassing procedural attacks like social engineering as well as emerging, existential threats from technologies such as quantum computing.[5] This confluence of technological evolution and a dynamic threat environment necessitate a comprehensive reassessment of the SIM's role and its security model. While the core principles of identity and authentication remain, the methods of ensuring their integrity must evolve to meet these new challenges.

This report provides a detailed analysis of the SIM's security evolution. The first contribution is a comparative study of the security architectures and trade-offs inherent to physical SIM, eSIM, and iSIM technologies. The second is a detailed dissection of the contemporary threat landscape, moving beyond traditional cryptographic attacks to include procedural vulnerabilities, software flaws, and architectural weaknesses. The third is a forward-looking examination of security requirements for the 5G era, with a particular focus on network slicing, and the critical need to future-proof SIM technology for the post-quantum era. The remainder of this paper is structured to follow this analytical progression, offering a holistic perspective on the past, present, and future of SIM security.

2. Foundational Security Architecture of UICC-Based SIMs

The security of a traditional SIM card is built on a foundation of both hardware and protocol design, governed by well-established international standards. An understanding of this foundational architecture is essential for appreciating the advancements and vulnerabilities of modern SIM form factors.

2.1 Hardware and Logical Structure

A SIM card is, at its core, a type of smart card, which is an integrated circuit (IC) chip mounted on a plastic card body.[1] The entire physical unit is technically known as a Universal Integrated Circuit Card (UICC), and the SIM itself is the primary application running on this platform.[1] The hardware architecture of a SIM card is designed according to the ISO 7816 standard, which dictates its physical, electrical, and logical characteristics.[7] The functional modules of the chip include a microprocessor (CPU) for all computations, a Program Memory (ROM) that stores the operating system and pre-installed applications, a Working Memory (RAM) for temporary data, and a Data Memory (EEPROM) that holds variable information such as phonebooks, SMS messages, and crucial security keys.[8]

The security-critical information stored in the EEPROM includes a unique serial number, the Integrated Circuit Card Identification (ICCID), and the International Mobile Subscriber Identity (IMSI).[1] The IMSI is a globally unique number that identifies the subscriber and is composed of three parts: the Mobile Country Code (MCC), the Mobile Network Code (MNC), and the Mobile Identification Number (MSIN).[1] Most importantly, the SIM securely stores the Authentication Key (Ki), a secret key used to identify and authenticate the subscriber to the network.[1] The ISO 7816 standard also defines the electrical contacts and the serial communication channel (I/O) that facilitate communication between the SIM and the mobile device.[7]

2.2 The GSM Authentication and Key Agreement (AKA) Protocol

The central security function of the SIM is performed through the challenge-response protocol known as Authentication and Key Agreement (AKA).[1] This process is initiated when a mobile device attempts to connect to an operator's network. The sequence of events is as follows:

1. **Request and Initial Identification:** When a mobile device powers on, it obtains the IMSI from the SIM card and sends it to the mobile operator's network, requesting access and authentication. A PIN code on the SIM card may be required before the IMSI is released.[1]
2. **Network Challenge:** The operator's network searches its database for the IMSI and retrieves its associated Ki. The network then generates a random number (RAND) and signs it with the Ki, computing a Signed Response 1 (SRES1) and an encryption key (Kc).[1]
3. **SIM Card Computation:** The network sends the RAND to the mobile device, which forwards it to the SIM card. The SIM card, using its own securely stored copy of the Ki, signs the RAND to produce a Signed Response 2 (SRES2) and the same encryption key (Kc).[1]
4. **Verification and Session Encryption:** The mobile device transmits SRES2 back to the network. The network compares its computed SRES1 with the received SRES2. If the two values matches, the SIM is successfully authenticated, and the mobile device is granted access to the network. The session key Kc is then used to encrypt all subsequent communications between the mobile device and the network, ensuring the confidentiality of data transmitted over the air.[1]

This AKA process, with its reliance on a shared secret key (Ki) that never leaves the SIM card, forms the robust cryptographic foundation of cellular security.

3. The Evolving SIM Form Factor: From Physical to Integrated

The physical SIM card, despite its foundational security model, presented limitations in a world of ever-smaller, sealed, and remotely managed devices. The industry's strategic shift to embedded and integrated form factors has fundamentally altered the security landscape, introducing new benefits and complexities.

3.1 From Physical SIM to Embedded SIM (eSIM)

The embedded SIM (eSIM), or eUICC, is a programmable SIM chip that is soldered directly onto a device's Printed Circuit Board (PCB).[3] This permanent integration eliminates the need for physical swapping, enabling remote management of subscriber profiles through an Over-the-Air (OTA) protocol defined by the GSMA.[10]

This shift to the eSIM offers significant security advantages over the traditional physical SIM. The eSIM is more **tamper-resistant** because it cannot be physically removed or easily stolen from the device, which dramatically reduces the risk of SIM cloning.[11] Traditional SIM cloning required an attacker to physically extract the Ki, a process made much more difficult by the

eSIM's embedded nature.[11] The GSMA's Remote SIM Provisioning (RSP) security model is a critical enabler of this security paradigm.[13] It mandates that carrier profiles, which contain the critical authentication keys, are provided in an encrypted format that can only be decrypted and installed by the eUICC itself.[13] The keys (Ki, OPc) are decoded

inside the chip, preventing them from ever being exposed to the outside world, a key difference from the traditional model where an attacker with physical access could attempt to dump them.[13]

However, the transition to remote provisioning introduces a new attack surface. The OTA provisioning system, which consists of the Subscription Manager (SM) and the Local Profile Assistant (LPA) software on the device, becomes a potential point of compromise.[12] A security flaw in the LPA software or the secure channel protocol could potentially be exploited to perform profile hijacking or other remote-based attacks.[12]

3.2 The Integrated SIM (iSIM) and the SoC Revolution

The integrated SIM (iSIM) represents the logical conclusion of the SIM's evolution. It embeds the entire SIM functionality directly into a device's System-on-Chip (SoC), eliminating the need for a separate physical component or chip entirely.[3] This streamlines manufacturing, simplifies the Bill of Materials (BoM), and provides a compact solution ideal for space-constrained devices like IoT sensors and wearables.[3]

The iSIM's architecture elevates tamper resistance to its highest level. The SIM functionality operates within a secure enclave, referred to as a Tamper-Resistant Element (TRE) or Trusted Execution Environment (TEE), which is isolated from the main application processor.[4] This deep integration reduces the physical attack surface to a minimum and provides a robust, hardware-based root of trust. By eliminating the physical connections and dedicated interfaces of a separate SIM chip, the risk of hardware-based attacks, such as probing or side-channel analysis, is significantly reduced.[14]

Despite these advances, the iSIM introduces new complexities. The tight integration into the SoC increases the complexity of the chip's design and manufacturing process.[16] Furthermore, because the iSIM relies on firmware and is not physically replaceable, vulnerabilities in the device's main firmware or the secure enclave itself could potentially expose sensitive data.[12] This makes secure lifecycle management and reliable over-the-air updates critical for addressing future vulnerabilities in a device that cannot be physically serviced.[16]

SIM Type	Physical Form Factor	Provisioning	Tamper Resistance	Primary Attack Vectors	Key Security Standard
Traditional SIM	Removable Plastic Card (UICC)	Physical	Low	SIM Swapping, Cloning, Legacy Software Exploits	3GPP
eSIM	Soldered Chip (eUICC)	Remote (RSP)	High	Remote Provisioning Exploits, Firmware Flaws	GSMA SGP.24
iSIM	Integrated into SoC (TRE/TEE)	Remote (RSP)	Very High	Firmware Flaws, Side-Channel Attacks, Lifecycle Management	GSMA SGP.32, Trust Connectivity Alliance

4. A Contemporary Threat Landscape Analysis

The evolution of the SIM has been accompanied by a parallel evolution of cyber threats. Modern attacks often exploit procedural and software-level vulnerabilities, demonstrating that a secure hardware component is insufficient without an equally robust ecosystem of policies, processes, and software.

4.1 Social Engineering and Procedural Attacks: The Rise of SIM Swapping

SIM swapping, also known as "port-out fraud" or "port jacking," is a non-technical attack that has emerged as a significant threat to digital identity.[5] Instead of exploiting a cryptographic weakness in the SIM card itself, attackers leverage social engineering to trick mobile carrier employees into transferring a victim's phone number to a new SIM card under the attacker's control.[5] This is typically accomplished by presenting stolen Personal Identifiable Information

(PII) or forged IDs. Once the swap is complete, all calls and SMS-based Multi-Factor Authentication (MFA) codes are routed to the attacker's device, providing a gateway to high-value accounts such as email, banking, and social media.[5]

The prevalence and financial impact of this attack have been staggering. In 2024, the U.K. saw a 1,055% increase in SIM swap cases, while the U.S. reported nearly $50 million in losses in 2023 due to such scams.[5] The attack has escalated from a consumer threat to a critical enterprise concern, as exemplified by the January 2024 hack of the U.S. Securities and Exchange Commission's X account, which was enabled by a SIM swap that bypassed "extra security" measures on the victim's account.[5] The continued reliance on SMS-based MFA for access to critical corporate tools and networks makes remote workers particularly vulnerable.[5] The fact that an attack on the human element of a telecommunications company can lead to such widespread financial and reputational damage highlights that the security of a digital identity is only as strong as the weakest link in the entire chain.

To combat this threat, a multi-layered approach is required. Technical countermeasures include transitioning away from SMS-based MFA to more secure app-based authenticators or FIDO2-compliant hardware security tokens.[5] Procedural safeguards are equally critical, such as implementing carrier-level account PINs, mandating supervisor approval for SIM-related changes, and providing comprehensive security awareness training to educate employees on how to recognize and resist social engineering tactics.[5] Recognizing the severity of this systemic issue, the FCC has implemented new rules requiring wireless providers to adopt secure authentication methods that accommodate a diverse range of customer needs, making the problem a matter of regulatory compliance.[17]

4.2 Baseband and Application-Level Exploits

While SIM swapping exploits human vulnerabilities, other attack vectors target the complex software and hardware of the mobile ecosystem. The baseband chipset, a physically separated system with its own CPU and operating system, handles all cellular network functions.[18] Although this separation prevents user applications from directly manipulating cellular traffic, it does not protect the system from memory corruption attacks launched from a malevolent tower.[18] This vulnerability exposes a fundamental design assumption that a phone receives well-formed and accurate information from the network, an assumption that is no longer valid in an era of cheap, portable fake base stations.[18]

The **Simjacker** exploit (CVE-2019-16256) illustrates a software vulnerability on the SIM itself. This attack works by exploiting a weakness in a legacy UICC library called the S@T Browser.[19] An attacker sends a specially formatted binary text message to the victim's handset, which contains a set of commands to be executed by the vulnerable software environment on the UICC. The S@T Browser, with access to a subset of SIM Toolkit commands, can then be

instructed to exfiltrate the device's location and International Mobile Equipment Identity (IMEI) to the attacker without the user's knowledge.[19] This attack is particularly noteworthy because it is OS-agnostic and does not require the attacker to have the SIM key.[19] This exploit demonstrates how the addition of non-core, un-sandboxed software features to a secure element can introduce a new and significant attack surface, proving that the security of the entire system is dependent on every component, no matter how obscure.

5. Security in the 5G and IoT Ecosystem

The transition to 5G and the proliferation of IoT devices introduce a new set of security requirements and challenges. While the 5G standard builds in significant security enhancements over previous generations, its new architectural paradigms also create a paradox where logical security features can give rise to new systemic vulnerabilities.

5.1 5G: New Security by Design Features

The 5G standard was developed with a "security by design" philosophy, incorporating several key features to address long-standing threats in 2G, 3G, and 4G networks.[21] One of the most significant improvements is the

enhanced subscriber identity protection. Unlike previous generations that transmitted the IMSI in the clear over the air, 5G protects the confidentiality of the initial Non-Access Stratum (NAS) messages and conceals the subscriber's identity using public/private key pairs.[21] This new identity, the Subscription Concealed Identifier (SUCI), makes it impossible for attackers to trace user equipment over the radio interface, effectively protecting against IMSI catchers and man-in-the-middle attacks.[21]

Furthermore, 5G supports **unified authentication** (EAP) across different access network types, such as WLAN, allowing for secure re-authentication of a device as it moves between different networks.[21] It also introduces user plane integrity checking, which ensures that user traffic is not modified during transit, and provides access-agnostic authentication, strengthening the overall security posture.[21]

5.2 The Security Paradox of 5G Network Slicing for IoT

Network slicing is a cornerstone of the 5G architecture, enabling the creation of multiple virtual, logically separate networks that share the same underlying physical infrastructure.[23] This functionality allows for the customization of performance, Quality of Service (QoS), and security policies for specific use cases, such as industrial control systems or medical devices.[23] On the surface, this segmentation appears to offer a way to contain security threats by

isolating traffic.

However, a closer look reveals a security paradox. While network slicing provides logical segmentation, the shared physical resources create a critical new attack surface.[24] An attacker who gains a foothold in one vulnerable slice can potentially move laterally to other slices, distributing malware and compromising a large portion of the IoT ecosystem.[24] This vulnerability defeats the very purpose of segmentation and highlights a major weakness in the distributed, shared-resource model of 5G.

The open, decentralized architecture of 5G also relies on Application Programming Interfaces (APIs) for communication between services, creating new attack vectors.[26] Misconfigured settings, which are common in complex IoT deployments, can be exploited to install malware.[24] This architectural shift from a centralized, tightly controlled network to a decentralized, API-driven one fundamentally alters the security challenge. It means that while 5G has successfully addressed lower-layer protocol vulnerabilities, it has simultaneously introduced higher-level, systemic weaknesses that demand a new, ecosystem-wide approach to security.

5.3 The Role of the SIM in a 5G/IoT Context

In this new, complex network environment, the SIM-based identity remains a critical anchor of trust. The evolution to tamper-resistant eSIM and iSIM technologies is a direct response to the massive scalability requirements of IoT deployments.[4] The iSIM, in particular, with its deep integration into the SoC's secure enclave, is uniquely positioned to serve as a hardware-based root of trust in a world of fragmented and potentially untrusted network slices. It provides a robust and efficient identity management solution that can be securely provisioned and managed at scale, serving as the linchpin for a zero-trust architecture in a network where every node is a potential point of vulnerability.

6. Future-Proofing for the Post-Quantum Era

Beyond the current threats, a new, existential challenge looms: the advent of practical quantum computing. The ability of these machines to perform computations exponentially faster than classical computers poses a severe threat to current public-key cryptosystems like RSA and Elliptic Curve Cryptography (ECC).[6]

6.1 The Impending Quantum Threat

The threat posed by quantum computers is not theoretical; it has given rise to the "harvest now, decrypt later" threat model.[29] In this model, adversaries collect today's encrypted communications, anticipating that future quantum computers will be able to break the

encryption and expose the data.[29] This impending security failure has mobilized governments, industry stakeholders, and standards bodies like NIST to accelerate the development and deployment of Post-Quantum Cryptography (PQC).[6] PQC algorithms, which are based on mathematical problems believed to be difficult for both classical and quantum computers to solve, are designed to replace the vulnerable cryptographic schemes currently in use.[30]

6.2 Implementation Challenges on Resource-Constrained SIMs

The transition to PQC presents a particularly acute challenge for resource-constrained devices like SIM cards. PQC algorithms are significantly more computationally demanding and often have larger key and signature sizes compared to their classical counterparts.[28] Research has demonstrated that while high-performance servers can implement these algorithms with a negligible performance impact, resource-constrained embedded devices experience a one-order-of-magnitude increase in processing time.[29] These overheads include increased computational latency, higher memory utilization, and greater energy consumption.[30] The following table provides a comparison of PQC performance metrics on resource-constrained devices, based on empirical evaluations.

Metric	CRYSTALS-Kyber (KEM)	CRYSTALS-Dilithium (Signature)	Falcon (Signature)
Computational Latency (Level 5)	**Best performance**, significantly faster than other KEMs on constrained hardware.	**Good performance**, with times increasing by approximately one order of magnitude compared to servers.	**Good performance**, comparable to Dilithium on constrained hardware.
Memory Utilization	Higher than classical ciphers; requires careful optimization.	Higher than classical ciphers; a key design challenge for constrained platforms.	Higher than classical ciphers; optimization is critical for embedded systems.
Key/Signature Size	Larger than classical RSA/ECC; can impact bandwidth and storage.	Larger than classical RSA/ECC; can impact bandwidth and storage.	Larger than classical RSA/ECC; can impact bandwidth and storage.
Power Consumption (Raspberry Pi)	Consumes more power than classical ciphers; Dilithium5 is 2.97% higher than RSA-4096.	Consumes more power than classical ciphers; Falcon-1024 is 3.00% lower than RSA-4096.	Consumes more power than classical ciphers; Falcon-1024 is 3.00% lower than RSA-4096.

6.3 Strategies for a Secure Transition

A straightforward "drop-in replacement" of cryptographic algorithms is not a viable strategy for SIM cards. Instead, a more nuanced approach is required. One solution is the development of **lightweight PQC protocols** specifically designed for resource-constrained environments, such as the proposed lightweight PQ-FLAT protocol for SIM cards.[27]

The most critical long-term strategy for SIM technology is the adoption of **crypto-agility**. This principle requires that cryptographic functionalities, including algorithms and key schemes, can be updated or replaced without the need for significant changes to the rest of the system.[32] For a device with a non-replaceable iSIM, this is an essential design consideration. An agile architecture, secured by a robust, post-quantum update mechanism, is the only way to ensure that a device's core security component can be continuously updated to protect against evolving threats and future cryptographic breakthroughs.[32] An interim measure to address the immediate threat is a **hybrid approach**, which combines a classical algorithm with a new PQC scheme to provide an extra layer of protection while minimizing performance penalties.[32]

7. Conclusion

The Subscriber Identity Module has undergone a fundamental transformation, evolving from a physically based, static secure element to a dynamic, remotely managed, and fully integrated component. This evolution has addressed classic physical vulnerabilities, such as cloning and theft, by embedding the secure element within the device. However, this has simultaneously introduced new attack surfaces in the form of remote provisioning systems and complex software layers. The contemporary threat landscape is multifaceted, encompassing sophisticated social engineering attacks that exploit human trust and architectural vulnerabilities inherent to the new 5G ecosystem, such as the paradox of network slicing.

Looking ahead, the challenges of 5G are a preview of what is to come in 6G, where a more distributed, AI-driven architecture will further expand the attack surface and demand a holistic, ecosystem-wide approach to security.[26] Securing future networks will require a paradigm shift that integrates security from a foundational SIM-based identity to the network core, leveraging technologies like AI for threat detection, blockchain for decentralized trust, and a zero-trust architecture.[26]

Based on this analysis, several critical open research questions remain to be addressed:

- How can inter-operator protocols and the network core be secured against attacks, particularly those that exploit the shared physical infrastructure of network slicing?
- What are the most effective and efficient lightweight PQC algorithms for mass-market

deployment on resource-constrained devices, and how can their performance overheads be minimized without compromising security?

- How can the lifecycle management of iSIMs, which are not physically replaceable, be made secure and reliable at scale to ensure uninterrupted service and address future vulnerabilities throughout a device's long operational lifetime?

Continued research in these areas is essential to ensure that the SIM card retains its role as the trusted, secure anchor of identity in the next generation of mobile and connected devices.

References

1. SIM card - Wikipedia, accessed September 10, 2025, https://en.wikipedia.org/wiki/SIM_card
2. Secure Elements (Smart Cards) - ETSI, accessed September 10, 2025, https://www.etsi.org/technologies/smart-cards
3. The Differences between SIM, eSIM and iSIM - Telit Cinterion, accessed September 10, 2025, https://www.telit.com/blog/sim-vs-esim-vs-isim/
4. Integrated SIM (iSIM) for IoT connectivity - IDEMIA, accessed September 10, 2025, https://www.idemia.com/integrated-sim-isim
5. What Is SIM Swapping? Attack, Definition, Prevention | Proofpoint US, accessed September 10, 2025, https://www.proofpoint.com/us/threat-reference/sim-swapping
6. Toppan and NICT Establish World's First Technology for Equipping Smart Card Systems with Post-Quantum Cryptography Selected by NIST | 2022, accessed September 10, 2025, https://www.nict.go.jp/en/press/2022/10/26-1.html
7. Smart Card Technical Introduction, accessed September 10, 2025, http://downloads.acs.com.hk/technology/462-01-smart-card-technical-introduction.pdf
8. QuecDevZone - Quectel, accessed September 10, 2025, https://python.quectel.com/doc/Application_guide/en/network-comm/sim/SIM-card-hardware-structure.html
9. About Smart Cards : Introduction : Standards - Secure Technology Alliance, accessed September 10, 2025, https://www.securetechalliance.org/smart-cards-intro-standards/
10. ST4SIM: What is an eSIM? - STMicroelectronics, accessed September 10, 2025, https://www.st.com/content/st_com/en/ecosystems/st4sim-cellular-connectivity/back-to-basics.html
11. eSIM vs. Physical SIM: Which One Is More Secure - Blog - WorldSIM, accessed September 10, 2025, https://www.worldsim.com/blog/esim-more-secure-than-physical-sim
12. SIM Types and Security: eSIM, iSIM, and Traditional SIMs Explained - P1 Security, accessed September 10, 2025, https://www.p1sec.com/blog/understanding-sim-types-security-risks-attacks-and-penetration-testing

13. Remote SIM provisioning - Wikipedia, accessed September 10, 2025, https://en.wikipedia.org/wiki/Remote_SIM_provisioning
14. iSIM vs eSIM: 5 Key Differences - floLIVE, accessed September 10, 2025, https://flolive.net/blog/esim-vs-isim-the-touchless-sim/
15. iSIM (integrated SIM): definition, benefits, perspective - Thales, accessed September 10, 2025, https://www.thalesgroup.com/en/markets/digital-identity-and-security/mobile/connectivity/isim
16. What is an iSIM? How it works, pros/cons, and differences between iSIM and embedded SIM, accessed September 10, 2025, https://flolive.net/blog/glossary/what-is-an-isim/
17. FCC Announces Effective Compliance Date for SIM Swapping Item ..., accessed September 10, 2025, https://www.fcc.gov/consumer-governmental-affairs/fcc-announces-effective-compliance-date-sim-swapping-item
18. CELLULAR BASEBAND SECURITY - GT Digital Repository, accessed September 10, 2025, https://repository.gatech.edu/bitstreams/8cb73e2d-184d-41a3-8069-1d21d48ccc9a/download
19. Simjacker - Wikipedia, accessed September 10, 2025, https://en.wikipedia.org/wiki/Simjacker
20. Lookout Simjacker, accessed September 10, 2025, https://www.lookout.com/documents/threat-reports/us/lookout-simjacker-tg-us.pdf
21. Securing the 5G Era - GSMA, accessed September 10, 2025, https://www.gsma.com/solutions-and-impact/technologies/security/securing-the-5g-era/
22. Understanding what a 5G SIM is and its benefits - Thales, accessed September 10, 2025, https://www.thalesgroup.com/en/markets/digital-identity-and-security/mobile/secure-elements/5g-sim
23. 5G and IoT for businesses: Benefits and use cases | A1 Digital, accessed September 10, 2025, https://www.a1.digital/knowledge-hub/5g-and-iot-new-opportunities-for-companies/
24. Cybersecurity Risks of Network Slicing for IoT | IoT For All, accessed September 10, 2025, https://www.iotforall.com/cybersecurity-risks-of-network-slicing-for-iot
25. Security Threats, Requirements and Recommendations on Creating ..., accessed September 10, 2025, https://www.mdpi.com/2079-9292/13/10/1860
26. Cybersecurity Challenges and Pitfalls in 6G Networks - ICS-FORTH, accessed September 10, 2025, https://users.ics.forth.gr/~zarras/files/HOLISTIC_2025_Cybersecurity.pdf
27. Proposed post-quantum secure protocol for SIM card with private ..., accessed September 10, 2025, https://www.researchgate.net/figure/Proposed-post-quantum-secure-protocol-for-SIM-card-with-private-key_fig2_362987875
28. A Deep Dive into Post-Quantum Cryptography - PixelPlex, accessed September 10, 2025, https://pixelplex.io/blog/post-quantum-cryptography/

29. A Practical Performance Benchmark of Post-Quantum Cryptography Across Heterogeneous Computing Environments - MDPI, accessed September 10, 2025, https://www.mdpi.com/2410-387X/9/2/32
30. POSTER: Post-Quantum Cipher Power Analysis in Lightweight Devices - NSF Public Access Repository, accessed September 10, 2025, https://par.nsf.gov/servlets/purl/10423194
31. (PDF) Navigating the Quantum Era: Exploring Lightweight Quantum-Resistant Cryptography - ResearchGate, accessed September 10, 2025, https://www.researchgate.net/publication/388735768_Navigating_the_Quantum_Era_Exploring_Lightweight_Quantum-Resistant_Cryptography
32. Crypto-agility for smart cards - NIST Computer Security Resource Center, accessed September 10, 2025, https://csrc.nist.gov/csrc/media/Events/2025/crypto-agility-workshop/documents/presentations/s6-christophe-giraud-presentation.pdf
33. Drivers and needs to define security for 6G - Ericsson, accessed September 10, 2025, https://www.ericsson.com/en/reports-and-papers/white-papers/6g-security-drivers-and-needs
34. 6G Technology Risks: Security Threats, Cybersecurity Challenges & Solutions | ECCU, accessed September 10, 2025, https://www.eccu.edu/blog/understanding-the-risks-of-6g-technology-the-next-cybersecurity-challenge/
35. Security, trust and privacy - 6G Technologies - Nokia, accessed September 10, 2025, https://www.nokia.com/bell-labs/research/6g-networks/6g-technologies/security-and-trust/