Qwen

Beyond Backdoors: A Protocol Blueprint for Cryptographic Sovereignty in Mobile Communications

The Philosophical Imperative: Why Verifiable Telecom Hardware is Non-Negotiable

The impetus for the VensaSIM project is rooted not merely in technical obsolescence but in a profound philosophical critique of modern power structures and their embodiment in opaque, proprietary technology. This initiative extends the core tenets of the Cypherpunk movement into the critical domain of telecommunications, arguing that true digital freedom cannot exist without verifiable control over the fundamental hardware of one's digital identity. The analysis of this imperative draws heavily from recent articulations by figures like Vitalik Buterin and Bunnie Huang, who frame the issue in terms of power dynamics, trust, and the necessity of common knowledge as a precondition for a secure society.

The central thesis, articulated by Vitalik Buterin in his announcement of the Vensa open-silicon initiative, is that technology profoundly shapes power dynamics [3]. He identifies a spectrum of risk, ranging from the digital divide, where unequal access to technology exacerbates inequality, to the more acute danger of technology being actively weaponized against users [3] [17]. This latter risk is encapsulated in the concept of "weaponized interdependence," a term coined by scholars Henry Farrell and Abraham Newman [4] [17]. It describes a situation where actors with control over critical network infrastructures—such as the SIM card, which serves as the primary authentication token for mobile networks—can exploit their central position to exert political coercion or engage in surveillance [3] [55]. When a technology becomes a de facto chokepoint, the power asymmetry between the controller of the chokepoint and the users becomes starkly apparent [12]. The SIM card exemplifies this perfectly; it authenticates a user to the network, yet the user has no insight into its internal cryptographic operations or the algorithms governing its security [9]. This inherent opacity creates a dynamic where power naturally skews away from the individual and toward the entity controlling the black box [12] [28].

Buterin’s solution is a direct inversion of this model: the pursuit of openness and verifiability [59]. Openness allows for public scrutiny, while verifiability enables the creation of "common knowledge of security." This is a crucial distinction from reputation-based trust, which relies on an individual's faith in a specific vendor. Such trust is fragile, as the threat model often involves complex systems with numerous closed-source dependencies, where the compromise of any single component can undermine the entire stack [78]. Common knowledge, in contrast, is a shared understanding among a wide group of people—including those who inherently distrust the vendor—that a system is secure [59]. The Vensa project is thus positioned not just as a technical endeavor to make silicon cheaper or more accessible, but as a strategic intervention to rebalance power by giving users agency over the foundational hardware of their digital lives [82]. This philosophy directly challenges the long-standing principle of "security through obscurity," demonstrating its failure as a sustainable security strategy.

Complementing this high-level vision are the practical approaches developed by hardware security expert Bunnie Huang. Huang's work, seen in projects like the Precursor smartwatch and Betrusted router, is dedicated to building systems where every component, down to the silicon, can be independently verified [71]. The core principles derived from this work provide a blueprint for achieving the ideals espoused by Buterin. These include the use of fully open-source toolchains for design and manufacturing to eliminate hidden dependencies on proprietary software, modular designs that isolate critical components like secure enclaves to minimize the attack surface, and the application of physical verification techniques such as reverse engineering and side-channel analysis to validate a device's behavior [38] [76]. For the VensaSIM project, these lessons are paramount. Even in a software-focused proof-of-concept, the protocol design should anticipate these architectural patterns. The demonstration could simulate how a hypothetical VensaSIM chip would interact with a network, emphasizing secure key storage and attestable operations, thereby mirroring the robust security models found in mature hardware security products.

This entire framework is a direct continuation of the ideological lineage of the Cypherpunk movement, which emerged in the early 1990s through the collaborative efforts of activists like Eric Hughes, Timothy C. May, and John Gilmore [7]. Their writings, most notably "A Cypherpunk's Manifesto" by Hughes and "The Crypto Anarchist Manifesto" by May, laid out a clear agenda for using cryptography to reclaim privacy and individual autonomy from both state and corporate overreach [6] [18] [19]. The manifestos advocate for privacy as a necessary social good in an open society and express a deep skepticism of centralized systems that create dependency [35] [82]. They view technology not as neutral but as a powerful political tool whose design choices have profound social

consequences [59]. The modern concept of Self-Sovereign Identity (SSI) builds upon this foundation, arguing that individuals should own and control their own identity data rather than ceding it to centralized authorities [82]. VensaSIM represents a natural extension of SSI principles from the digital realm of the internet to the physical world of telecommunications. By empowering users to select their own cryptographic primitives for authentication, it shifts the locus of control from network operators and chip manufacturers to the individual user. This ideological coherence provides a powerful narrative, distinguishing VensaSIM from incremental improvements on flawed standards and grounding it in a long history of activism for digital rights and freedoms.

Anatomy of the Black Box: A Deep Dive into SIM, UICC, and eSIM Architecture

The VensaSIM project is predicated on the assertion that incumbent SIM technologies are fundamentally incompatible with the principles of openness, transparency, and user sovereignty. These systems, while enabling global communication, operate as opaque "black boxes" whose security relies on secrecy and trust in proprietary vendors, a model that history has repeatedly shown to be fragile and insufficient. A detailed examination of the Universal Integrated Circuit Card (UICC), the underlying authentication protocols, and the newer eSIM standard reveals why a clean-slate approach is not only desirable but necessary.

The modern SIM card is officially known as a UICC, a miniature computer embedded in a plastic card [20]. Its architecture includes a central processing unit (CPU), read-only memory (ROM), random-access memory (RAM), and electrically erasable programmable read-only memory (EEPROM) [20]. It runs a specialized operating system, most commonly Java Card, which manages applications and enforces security policies [20]. While technologically sophisticated, this complexity introduces significant opacity. The exact algorithms used for authentication, key generation, and data storage are proprietary secrets held by chip manufacturers such as Thales and Infineon [20]. Users and even network operators cannot inspect the code running on the card to verify its integrity or check for vulnerabilities. This black-box nature is a critical security weakness, as successful attacks on SIM cards often require extensive and difficult reverse engineering processes to uncover hidden flaws [9] [71]. The entire security posture of the system rests on the assumption that the vendor is both honest and competent—a deeply fragile basis for trust in a globally interconnected environment.

The standard authentication process in cellular networks has evolved significantly but remains tethered to legacy principles. In GSM networks, the process relied on the COMP128 algorithm, which was later found to have serious weaknesses that allowed for the recovery of the subscriber's secret key (Ki) with relatively low computational effort [9] [15]. This was eventually superseded by the Milenage suite, a more robust set of algorithms designed for 3G, 4G, and 5G networks [15]. Despite its improved cryptographic design, Milenage does not solve the fundamental problem of the black box. The implementation details remain proprietary, and the potential for subtle implementation flaws or hidden backdoors persists. Research has demonstrated that even with strong algorithms, side-channel attacks that analyze power consumption or electromagnetic emissions during cryptographic operations can be used to extract keys from SIM cards [71]. Furthermore, the threat is not limited to theoretical vulnerabilities; real-world examples, such as a flaw in some YubiKeys caused by a defective random number generator leading to nonce reuse, have shown how poor implementation can break even well-regarded cryptographic schemes like ECDSA [44]. This underscores that the threat model is rarely a single catastrophic failure but the accumulation of weaknesses across the entire software and hardware stack. The reliance on a closed, unverifiable platform ensures that such vulnerabilities will remain undetected until exploited.

The introduction of the eSIM standard was intended to address the physical inconvenience of plastic SIM cards by enabling remote provisioning of carrier profiles [23]. However, the eSIM does not represent a fundamental shift towards transparency and sovereignty; it is, at its core, a "digital black box." The embedded Universal Integrated Circuit Card (eUICC) still runs proprietary firmware on a closed, non-verifiable platform. While it offers greater flexibility in switching carriers, the cryptographic primitives it employs remain opaque and are almost certainly based on the same legacy standards as traditional SIMs, such as Milenage. The eSIM ecosystem is also dominated by a small number of large providers, creating new forms of vendor lock-in under a different guise [20]. Therefore, the eSIM represents an evolutionary improvement in convenience and logistics, but it fails to address the core philosophical and security issues of the underlying technology. It maintains the status quo of relying on trust in opaque, proprietary systems rather than building a foundation of verifiable security. For a project focused on user sovereignty, the eSIM is not a solution but another iteration of the same flawed paradigm.

Feature	Traditional SIM/UICC	eSIM (Embedded UICC)
Form Factor	Physical plastic card [20]	Embedded chip soldered onto the device's motherboard [23]
Provisioning	Manual insertion of a physical card [20]	Remote provisioning via Over-the-Air (OTA) download [23]
Platform Model	Closed, proprietary [20]	Closed, proprietary [20]
Verifiability	Not verifiable; source code and algorithms are secret [20]	Not verifiable; source code and algorithms are secret [20]
Vendor Lock-in	Carrier-dependent physical card [20]	Carrier profiles can be changed remotely, but the underlying platform remains controlled [20]
Security Model	Relies on "security through obscurity" and trust in the vendor [20]	Relies on "security through obscurity" and trust in the vendor [20]

The Crypto-Sovereignty Thesis: An Analysis of Elliptic Curve Trust

The most technically innovative aspect of the VensaSIM proposal is its core mechanism for achieving cryptographic sovereignty: allowing users to select from a list of vetted elliptic curves or define their own. This feature is a direct and forceful response to a crisis of confidence in the integrity of standardized cryptography, triggered by events that revealed how cryptographic building blocks themselves could be weaponized. This section analyzes the controversy surrounding NIST-standardized curves, presents transparent alternatives, and outlines the path to truly sovereign cryptographic construction.

The foundational issue stems from the Dual_EC_DRBG (Dual Elliptic Curve Deterministic Random Bit Generator) scandal, a canonical example of a covert backdoor engineered into a cryptographic standard [42]. In June 2013, disclosures by Edward Snowden revealed that the National Security Agency (NSA) had intentionally inserted a vulnerability into this pseudorandom number generator, which was proposed for inclusion in the NIST SP 800-90 standard [2] [47]. The backdoor's existence was possible because the algorithm's specification included two constants (points P and Q on an elliptic curve) whose relationship was known only to the NSA [1]. Anyone possessing this secret relationship could predict the output of the random number generator, thereby breaking the security of any system that used it for key generation or encryption [47]. This incident shattered public trust in the integrity of US government-backed cryptographic standards, proving that a powerful actor could embed a covert channel into a global

standard, compromising the confidentiality of countless communications worldwide [69]. It stands as a stark warning of the dangers of weaponized interdependence applied to the very foundations of digital security.

In stark contrast to the opaque origins of Dual_EC_DRBG, several widely used elliptic curves have been constructed using transparent methods that satisfy the "nothing-up-my-sleeve" principle. This principle dictates that the parameters of a cryptographic primitive should be derived from simple, well-known mathematical constants to prove they were not chosen to create a hidden weakness. Two prominent examples are secp256k1 and Curve25519.

Property	secp256k1	Curve25519
Primary Use Case	Bitcoin, Ethereum [44]	TLS 1.3, Signal Protocol, many other secure protocols [43]
Parameter Origin	Derived from the fractional parts of the square roots of small integers (2, 3, 5). [53]	Parameters are based on the integer -336144, chosen to maximize performance. [43]
Design Philosophy	Focus on simplicity and efficiency in point addition.	Focus on maximum speed and resistance to side-channel attacks. [43]
Adoption	Widely adopted in blockchain and cryptocurrency ecosystems.	Widely adopted in major internet security protocols. [43]
"Nothing-Up-My-Sleeve" Status	High; the derivation process is simple and transparent.	High; the parameters were generated through a clear, documented process. [43]

By offering these or other similarly vetted curves, VensaSIM moves away from a reliance on potentially compromised standards and toward a model of cryptographic self-determination. This empowers users to choose primitives that have undergone intense public scrutiny and are considered highly trustworthy by the cryptographic community.

The ultimate expression of this philosophy is the "user-defined curve" feature. While theoretically powerful, it carries significant risks if implemented naively. A malicious or uninformed user could define a curve with hidden weaknesses, rendering the system insecure. Therefore, a responsible implementation must provide guidance and validation. The VensaSIM protocol should incorporate a function that validates a user-provided curve against a checklist of established security criteria, drawing from academic resources like the SafeCurves project [48]. These criteria include ensuring the curve is not anomalous, that its order is prime, that it resists twist attacks, and that its parameters follow a verifiable generation process. By providing this validation layer, the system can empower users with genuine choice while protecting them from common cryptographic pitfalls, representing a true path toward cryptographic sovereignty.

The Ecosystem Landscape: A Review of Adjacent Technologies and Precedents

To chart a viable course for VensaSIM, it is essential to learn from existing projects and communities that have grappled with similar challenges of transparency, decentralization, and user control. The landscape of open-source telecommunications and hardware security provides valuable precedents in both technical architecture and development philosophy. Projects like Osmocom offer a model for deconstructing and rebuilding the telecom stack from the ground up, while hardware security keys like YubiKey demonstrate the architectural principles required to build a trusted hardware root of trust.

The Open Source Mobile Communications (Osmocom) project, and specifically its sysmoUSIM product line, represents a grassroots effort to create a fully open-source cellular network infrastructure [20]. Sysmocom aims to provide transparency at every layer, from base station emulation software (like OpenBTS) to subscriber identity modules (SIMs) like the sysmoUSIM-SJS1 [20]. The key lesson from Osmocom is the power of decomposition. Instead of treating the telecom stack as a monolithic, black-box system, Osmocom breaks it down into independent, interoperable components that can be individually scrutinized and audited by the community [20]. This approach leverages the collective intelligence of developers worldwide to find and fix bugs, fostering a culture of continuous improvement and public accountability. For VensaSIM, this suggests a strategy of designing a clean-slate protocol that can be implemented in a modular fashion, adhering to open specifications wherever possible to ensure interoperability with the wider ecosystem. While Osmocom works within the constraints of existing, albeit flawed, standards, its commitment to transparency provides a powerful proof-of-concept for what is possible when the telco stack is treated as public utility software.

A more mature parallel can be found in the world of hardware security keys, exemplified by products like the YubiKey, Nitrokey, and Ledger. These devices have achieved widespread adoption precisely because they embody a clear and compelling architectural model for user-centric security. The first and most critical principle is isolation: private keys never leave the secure element of the device [33]. All cryptographic operations, including signing, are performed internally, making it physically impossible for the private key to be exposed to the host computer or any network. Second is attestation. Devices like the YubiKey implement open protocols such as FIDO/U2F and CTAP/FIDO2, which allow them to cryptographically prove their own identity and integrity to a third party, such as a web service [34] [64]. This provides a verifiable guarantee that the operation

is being performed by a genuine, unmodified device. Finally, they succeed by implementing open standards, which fosters interoperability and allows for external validation and auditing [34].

VensaSIM can adopt this hardware-first mindset. The protocol should be designed to facilitate features like secure key storage and attestation, positioning it as the cryptographic engine for future open-hardware devices envisioned by initiatives like Vensa. The software proof-of-concept can serve as a reference implementation of this protocol, demonstrating how a client would securely generate keys, sign challenges, and provide verifiable evidence of its actions. By focusing on the architecture of trust—the principles of key isolation and attestable execution—rather than regulatory compliance, which is a concern for later stages of development, VensaSIM can align itself with the most successful precedents in modern hardware security.

Synthesis & Recommendations for a VensaSIM Proof-of-Concept

The preceding analysis establishes a clear and compelling case for VensaSIM as a philosophically coherent and technically necessary project. Grounded in the Cypherpunk tradition of advocating for individual sovereignty through cryptography, it directly confronts the power imbalances created by opaque, proprietary telecommunications infrastructure [6] [82]. The critique of incumbent SIM/UICC and eSIM technologies as unverifiable black boxes is substantiated by their reliance on security through obscurity and a history of documented vulnerabilities [9] [20]. The project's core innovation—cryptographic sovereignty through user-selectable elliptic curves—is a direct and justified response to the documented backdoor in the Dual_EC_DRBG standard, which proved that even foundational cryptographic primitives could be weaponized [42] [47]. To translate this vision into a successful hackathon project, the following recommendations outline a strategic approach focused on demonstrating the viability of the core protocol in a software proof-of-concept, explicitly rejecting backward compatibility in favor of an idealistic "north star" prototype.

For the proof-of-concept, the primary focus must be on the software protocol, as hardware implementation is outside the scope of a short-term hackathon project [3]. The goal is to prove the idea is sound today, ready for future integration with open-hardware platforms. The recommended technology stack should prioritize rapid development and

reliability. Python is an excellent choice due to its rich ecosystem of mature, audited cryptographic libraries like `cryptography` or `ecdsa`. Alternatively, Go or Rust could be used to showcase performance (Go) or memory safety (Rust), respectively. The PoC should not attempt to simulate the entire Java Card environment of a UICC; instead, it should be a focused library or script that exposes a simple API for the core cryptographic functions. This API should allow for the generation of keypairs on a specified elliptic curve, receiving a challenge from a simulated network, deterministically signing that challenge, and returning the resulting signature for verification.

The Minimal Viable Protocol (MVP) should be a clean-slate challenge-response mechanism, deliberately avoiding mimicry of existing, flawed standards. Its steps would be: 1. **Curve Advertisement:** The client (the VensaSIM PoC) advertises a list of supported elliptic curves (e.g., secp256k1, Curve25519). 2. **Challenge Generation:** The network selects a curve from the client's list and generates a random, unpredictable challenge message. 3. **Deterministic Signing:** The client uses its private key associated with the selected curve to generate a deterministic signature for the challenge. Following RFC 6979 is critical here to prevent nonce-related vulnerabilities that could expose the private key [80]. 4. **Signature Verification:** The network verifies the received signature against the client's pre-provisioned public key, which would be loaded securely via an out-of-band channel.

The strategic arguments for pitching this project must emphasize its visionary, non-compromising nature. The pitch should frame VensaSIM not as an incremental improvement but as a paradigm shift. Key talking points should include:

- **A Clean-Slate Alternative:** We are not attempting to patch a broken system; we are demonstrating what a truly secure, transparent, and sovereign authentication protocol looks like from the ground up.
- **User Control, Not Vendor Lock-In:** Unlike traditional SIMs or eSIMs, our model places the choice of cryptographic primitive directly in the hands of the user, protecting them from backdoors, opaque standards, and coercive interdependence.
- **Proven Through Code:** Our software proof-of-concept is a working, executable demonstration of the core protocol's feasibility. This proves the idea is viable now, serving as a blueprint for future open-hardware implementations.
- **Ideological Clarity:** We are guided by a clear philosophy of digital sovereignty and radical transparency, rejecting the pragmatic compromises of "good enough" security for the sake of backward compatibility.

By focusing on this idealistic vision, the VensaSIM project positions itself as a catalyst for change, challenging the incumbents to catch up to a new standard of security and user empowerment.

Reference

1. A Security Analysis of the NIST SP 800-90 Elliptic Curve ... https://www.researchgate.net/publication/220336742_A_Security_Analysis_of_the_NIST_SP_800-90_Elliptic_Curve_Random_Number_Generator
2. 求转正]斯诺登Dual EC DRBG伪随机后门事件综述-付费问答 https://bbs.kanxue.com/thread-183751-1.htm
3. Securing the Silk Road https://academic.oup.com/book/61829/chapter/546892163
4. A digital cold war in Africa? Capitalist multiplicity ... https://www.tandfonline.com/doi/full/10.1080/01436597.2025.2546668
5. (PDF) Alignment Statecraft and Alignment Dilemma https://www.researchgate.net/publication/396144430_Alignment_Statecraft_and_Alignment_Dilemma_The_Causes_of_Hedging_Under_US-China_Competition_in_Latin_America's_Digital_Infrastructure
6. A Cypherpunk'S Manifesto: Eric Hughes | PDF | Cryptography https://www.scribd.com/document/404968941/A-CYPHERPUNK-docx
7. 密码朋克简介原创 https://blog.csdn.net/u013669912/article/details/140896426
8. Evaluating NUMS Elliptic Curve Cryptography for IoT ... https://www.researchgate.net/publication/326383457_IoT-NUMS_Evaluating_NUMS_Elliptic_Curve_Cryptography_for_IoT_Platforms
9. Smartphones as Practical and Secure Location Verification ... https://www.researchgate.net/publication/269197156_Smartphones_as_Practical_and_Secure_Location_Verification_Tokens_for_Payments
10. Aaa | PDF | Computer Networking | Security Engineering https://www.scribd.com/document/388518204/aaa
11. Universal Digital Identity in Africa: Biometric Surveillance, ... https://www.researchgate.net/publication/

398818474_Universal_Digital_Identity_in_Africa_Biometric_Surveillance_Data_Sovereignty_and_Eschatological_Risks

12. Should We Trust a Black Box to Safeguard Human Rights? https://escholarship.org/content/qt1k39n4t9/qt1k39n4t9_noSplash_7bfe8ba12645c1bcbff08127590df5c1.pdf
13. Cryptography-based privacy-preserving large language models https://link.springer.com/article/10.1007/s10462-025-11466-6
14. (PDF) Research on the Digital Sovereignty System Based ... https://www.researchgate.net/publication/398995143_Research_on_the_Digital_Sovereignty_System_Based_on_the_DIKWP_Framework_Starting_from_the_Semantics_of_Quan
15. Infrastructural insecurity: geopolitics in the standardization ... https://journals.sagepub.com/doi/10.1177/1329878X231225748
16. Yubico Authenticator - App Store https://apps.apple.com/ua/app/yubico-authenticator/id1497506650?mt=12
17. Evaluating Assumptions About the Role of Cyberspace in ... https://www.researchgate.net/publication/372492368_Evaluating_Assumptions_About_the_Role_of_Cyberspace_in_Warfighting_Evidence_from_Ukraine
18. Cypherpunk ideology: objectives, profiles, and influences ... https://www.tandfonline.com/doi/full/10.1080/24701475.2021.1935547
19. THE TECHNICAL AND IDEOLOGICAL ROOTS OF BITCOIN https://www.researchgate.net/publication/394283688_FROM_CYBERPUNK_TO_CYPHERPUNK_THE_TECHNICAL_AND_IDEOLOGICAL_ROOTS_OF_BITCOIN
20. Sysmocom - S.F.M.C. GMBH: Sysmousim User Manual | PDF https://www.scribd.com/document/476316094/sysmousim-manual
21. Book 7 - Mobile Forensics - European Union https://ec.europa.eu/programmes/erasmus-plus/project-result-content/9d82c6b2-d28c-441a-b165-e73b1a87736f/FORC%20Book%207.pdf
22. Message Authentication and Provenance Verification for ... https://dl.acm.org/doi/10.1145/3607194
23. The Road to Trustworthy 6G: A Survey on Trust Anchor ... https://ieeexplore.ieee.org/iel7/8782661/10008219/10042484.pdf
24. Message Authentication and Provenance Verification for ... https://dl.acm.org/doi/pdf/10.1145/3607194
25. Cyber Attack Prediction: From Traditional Machine Learning to ... https://ieeexplore.ieee.org/iel8/6287639/10820123/10909100.pdf

26. Cross-Domain Opportunities in Cyber Threat Intelligence https://ieeexplore.ieee.org/iel8/6287639/10820123/11222578.pdf
27. A Survey on Trust Anchor Technologies https://ieeexplore.ieee.org/iel7/8782661/8901158/10042484.pdf
28. Cyber Threat Susceptibility Assessment for Heavy-Duty ... https://ieeexplore.ieee.org/iel8/8782711/10774192/10921673.pdf
29. Ten Years of Asset Administration Shell https://ieeexplore.ieee.org/iel8/6287639/6514899/11072423.pdf
30. Digital Transformation https://digitalreality.ieee.org/wp-content/uploads/2025/09/DRI_White_Paper_-_Digital_Transformation_-_Final_25March21.pdf
31. A Novel Machine Learning-Optimized Framework https://ieeexplore.ieee.org/iel8/6287639/10820123/11264542.pdf
32. DiVerify: Hardening Identity-Based Software Signing with ... https://arxiv.org/pdf/2406.15596
33. Yubikey PIV "The smartcard cannot perform the requested ... https://stackoverflow.com/questions/73102834/yubikey-piv-the-smartcard-cannot-perform-the-requested-operation
34. Protocol-level Attacks and Defenses to Advance IoT Security https://theses.hal.science/tel-05019219v1/file/145708_CASAGRANDE_2024_archivage.pdf
35. Follow the (Electronic) Money: How Bitcoin and Blockchain ... https://www.researchgate.net/publication/347801072_Follow_the_Electronic_Money_How_Bitcoin_and_Blockchain_Technology_Are_Shaking_the_System
36. 259 - AVIONICS, AEROSPACE AND DEFENSE ... https://de.scribd.com/document/142763797/259-AVIONICS-AEROSPACE-AND-DEFENSE-ACRONYMS-AND-ABBREVIATIONS-Januar-2011
37. Standardizing Bad Cryptographic Practice https://dl.acm.org/doi/10.1145/3133956.3134040
38. Detecting Information Flow Security Vulnerabilities by ... https://ieeexplore.ieee.org/iel8/32/11207080/11082015.pdf
39. Private, Verifiable, and Auditable AI Systems https://arxiv.org/html/2509.00085v1
40. A comprehensive review of current trends, challenges, and ... https://www.sciencedirect.com/science/article/pii/S0167404825000471
41. Authenticated Encryption Schemes: A Systematic Review https://ieeexplore.ieee.org/iel7/6287639/6514899/09695453.pdf
42. Dual EC: A Standardized Back Door https://www.researchgate.net/publication/308734228_Dual_EC_A_Standardized_Back_Door

43. Topgun: An ECC Accelerator for Private Set Intersection https://dl.acm.org/doi/full/10.1145/3603114
44. SECP256k1, NIST256p, NIST521p and LLL https://www.researchgate.net/publication/369069505_Research_on_Elliptic_Curve_Crypto_System_with_Bitcoin_Curves_-_SECP256k1_NIST256p_NIST521p_and_LLL
45. (PDF) Crypto - How the Code Rebels Beat the Government https://www.academia.edu/4903458/Crypto_How_the_Code_Rebels_Beat_the_Government_Saving_Privacy_in_the_Digital_Age
46. RFC 9380: Hashing to Elliptic Curves | Request PDF https://www.researchgate.net/publication/373687315_RFC_9380_Hashing_to_Elliptic_Curves
47. Dual_EC_DRBG事件后，NIST何以维持密码标准化国际地位 https://www.secrss.com/articles/61076
48. Safe curves for elliptic-curve cryptography https://www.researchgate.net/publication/389801482_Safe_curves_for_elliptic-curve_cryptography
49. UC San Diego Electronic Theses and Dissertations https://escholarship.org/content/qt27g0s74r/qt27g0s74r.pdf
50. Cyber security | PDF | Key (Cryptography) | Encryption https://www.scribd.com/document/975775211/Cyber-security
51. Faster Constant-time Evaluation of the Kronecker Symbol ... https://www.researchgate.net/publication/375807639_Faster_Constant-time_Evaluation_of_the_Kronecker_Symbol_with_Application_to_Elliptic_Curve_Hashing
52. Proceedings of International Conference on Wireless ... https://link.springer.com/content/pdf/10.1007/978-981-15-1002-1.pdf
53. SECURWARE 2014, The Eighth International Conference ... https://www.academia.edu/16705928/SECURWARE_2014_The_Eighth_International_Conference_on_Emerging_Security_Information_Systems_and_Technologies
54. Untitled - Springer Link https://link.springer.com/content/pdf/10.1057%2F9781137386694.pdf
55. (PDF) Red Territory: Forging Infrastructural Power https://www.researchgate.net/publication/344778253_Red_Territory_Forging_Infrastructural_Power
56. OSF _ Weaponized Interdependence in a Bipolar World_ ... https://www.scribd.com/document/979929540/OSF-Weaponized-Interdependence-in-a-Bipolar-World-How-Economic-Forces-and-Security-Interests-Shape-the-Global-Reach-of-U-S-and-Chinese-Cloud-Data

57. (PDF) Editor KevinnDaimi Associate Editors https://www.academia.edu/40120883/Editor_KevinnDaimi_Associate_Editors

58. the weaponization of economic interdependence https://www.researchgate.net/publication/394013971_THE_WEAPONIZATION_OF_ECONOMIC_INTERDEPENDENCE_SANCTIONS_FINANCIAL_STATECRAFT_AND_THE_FRAGMENTATION_OF_THE_GLOBAL_ECONOMIC_ORDER

59. A Verification Framework for Secure Group Messaging https://hal.science/tel-05455122v1/file/main.pdf

60. [The Crypto Anarchist Manifesto, Timothy C. May ... https://www.linkedin.com/posts/drsyl_reminder-this-is-growing-exponentially-activity-7266749161583071233-Eqai

61. What We Can Learn from Crypto's Anti-Hero https://hackernoon.com/what-we-can-learn-from-cryptos-anti-hero-302f6346c524

62. Digital Currency Governance Consortium White Paper Series https://www3.weforum.org/docs/WEF_Digital_Currency_Governance_Consortium_White_Paper_Series_2021.pdf

63. EverCrypt: A Fast, Verified, Cross-Platform Cryptographic ... https://www.researchgate.net/publication/343340372_EverCrypt_A_Fast_Verified_Cross-Platform_Cryptographic_Provider

64. Web Authentication: An API for accessing Public Key ... https://www.w3.org/TR/webauthn-2/

65. Enhancing System Security and Privacy with Trusted ... https://escholarship.org/content/qt5jn4k4m1/qt5jn4k4m1_noSplash_1e939a192058d8bbc085e660ab10077d.pdf

66. Computer Network Security - Springer Link https://link.springer.com/content/pdf/10.1007/978-3-319-65127-9.pdf

67. Josephy IT Rechtsinformatiker GbR: Blockchain Ethereum https://www.researchgate.net/profile/Ralf_Josephy2/publication/333134039_Projektvorschlag_17_-_Blockchain-Ethereum_-_2019-05-15/links/5d0374bc92851c874c651311/Projektvorschlag-17-Blockchain-Ethereum-2019-05-15.pdf

68. Cross-Network Weaponization in the Semiconductor Supply ... https://academic.oup.com/isq/article-pdf/68/1/sqae003/60442245/sqae003.pdf

69. U.S.-CHINA TECHNOLOGICAL “DECOUPLING” https://carnegie-production-assets.s3.amazonaws.com/static/files/Bateman_US-China_Decoupling_final.pdf

70. Analysing WTO Governance of Data Flows https://www.scirp.org/pdf/blr_3302402.pdf

71. Side-Channel based Reverse Engineering for ... https://www.researchgate.net/publication/237134490_Side-Channel_based_Reverse_Engineering_for_Microcontrollers
72. Comprehensive Cyber Security Index | PDF | Authentication https://www.scribd.com/document/673543560/CyBOK-v1-1-0-6
73. 9.4 Release Notes | Red Hat Enterprise Linux | 9 https://docs.redhat.com/en/documentation/red_hat_enterprise_linux/9/html-single/9.4_release_notes/index
74. 9.4 Release Notes | Red Hat Enterprise Linux | 9 https://docs.redhat.com/de/documentation/red_hat_enterprise_linux/9/html-single/9.4_release_notes/index
75. https://packages.debian.org/trixie/amd64/allpackag... https://packages.debian.org/trixie/amd64/allpackages?format=txt.gz
76. CyBOK v1.1.0-3 | PDF | Operating System https://www.scribd.com/document/673543684/CyBOK-v1-1-0-3
77. Comments on Dual-EC-DRBG/NIST SP 800-90, Draft ... https://www.researchgate.net/publication/228960119_Comments_on_Dual-EC-DRBGNIST_SP_800-90_Draft_December_2005
78. Maksym Grinenko - Bitcoin and the Japanese Retail Investor https://www.academia.edu/42765007/Maksym_Grinenko_Bitcoin_and_the_Japanese_Retail_Investor
79. Finding Satoshi - The Real Story Behind Mysterious Bitcoin https://www.scribd.com/document/919795534/Finding-Satoshi-The-Real-Story-Behind-Mysterious-Bitcoin-Ivy-McLemore-WeLib-org
80. How to sign and verify signature with ecdsa in python https://stackoverflow.com/questions/34451214/how-to-sign-and-verify-signature-with-ecdsa-in-python
81. Hashing to Elliptic Curves Through Cipolla–Lehmer–Müller's ... https://link.springer.com/article/10.1007/s00145-024-09490-w
82. Sovereignty, privacy, and ethics in blockchain-based identity ... https://pmc.ncbi.nlm.nih.gov/articles/PMC7701220/