March 14, 2024

R&D in Cyber Security Group
Ministry of Electronics and Information Technology
New Delhi 110003

Comment on the Cryptography Roadmap

Thank you for the opportunity to comment on the draft Cryptography Roadmap. I am an applied cryptography, privacy, and technology policy researcher. My work has applied novel cryptographic techniques to yield privacy-enhancing solutions to problems of policy interest including public elections, auctions, content moderation, and surveillance. I design and implement efficient classical protocols that are not only deployable today but also resist future quantum attacks. In this comment, I draw on academic cryptographic research to provide suggestions on the draft Roadmap.

Certification and Standardisation

- [*Short-Term*] In order to increase public trust, cryptographic primitives should be certified and standardised via an open and transparent process that invites submissions from all stakeholders. Allegations of interference in the process by motivated parties can severely undermine confidence in the resulting standard.[1]
- [*Medium-Term*] Quantum-resistant Key Encapsulation[2] and Homomorphic Encryption[3] could also be considered for certification and standardisation.

Randomness

- [*Medium-Term*] A verifiable, decentralised randomness beacon[4] would combine multiple high-entropy sources to produce verifiable public randomness. Such a decentralised beacon would be easier to trust and could be a collaborative effort by stakeholders across government, industry, academia, and civil society.

---

[1] Hales, Thomas C. "The NSA back door to NIST." *Notices of the AMS* 61.2 (2013): 190-192.

[2] NIST Post-Quantum Cryptography Standardization (https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization).

[3] Homomorphic Encryption Standard (https://homomorphicencryption.org/standard/).

[4] Examples include a deployment by the League of Entropy (https://drand.love/).

Quantum-Resistant Classical Constructions of Cryptographic Primitives

- [*Short-Term*] Concretely efficient quantum-resistant classical constructions of many otherwise well-studied cryptographic primitives (e.g., Oblivious Transfer) remain understudied. Such constructions would improve the security and performance of many novel cryptographic protocols that rely on these primitives.

Applications of Privacy-Enhancing Technologies (PETs)

- [*Medium-Term*] State of the art PETs including Private Information Retrieval[5] and Multiparty Private Set Operations[6] have significantly improved in performance over the past decade and are viable for many applications. Their use in government and industry could be encouraged by funding further research.
- [*Long-Term*] Applications of PETs that increase privacy and accountability in our public life should be explored. For example, governmental procurement processes could use distributed private-bid publicly verifiable auctions.[7] Cryptographic end-to-end verifiability[8] could increase trust in our elections. Encouraging processing of homomorphically encrypted user data could increase security and privacy for all. Secure multiparty computation could offer viable solutions to many sensitive multi-stakeholder problems of trust.

I hope the R&D in Cyber Security Group finds my suggestions valuable.

Sincerely,

Anunay Kulshrestha
Doctoral Candidate in Computer Science
Center for Information Technology Policy
Princeton University[9]

---

[5] Henzinger, Alexandra, et al. "One Server for the Price of Two: Simple and Fast Single-Server Private Information Retrieval." *32nd USENIX Security Symposium*. 2023.
[6] Kulshrestha, Anunay, and Jonathan Mayer. "Estimating Incidental Collection in Foreign Intelligence Surveillance: Large-Scale Multiparty Private Set Intersection with Union and Sum." *31st USENIX Security Symposium*. 2022.
[7] Kulshrestha, Anunay, et al. "Cryptographically secure multiparty computation and distributed auctions using homomorphic encryption." *Cryptography* 1.3 (2017): 25.
[8] Examples include ElectionGuard (https://www.electionguard.vote/).
[9] All expressed views are personal.