Google | Privacy & Data Protection Office

An update on Advanced Cryptography Standardization

August 17, 2019 @ HomomorphicEncryption.org Standards Meeting

Tancrède Lepoint
Google

PRIVATE COMPUTING

Many flavors of standardization

- ISO/IEC JTC 1 SC 27 *IT Security Techniques*.
    - Working Group 2 - Cryptography and security mechanisms.
        - Other WGs: Infosec management systems, sec. eval/testing/spec, sec. controls and services, identity management and *privacy technologies*.

Many flavors of standardization

- ISO/IEC JTC 1 SC 27 *IT Security Techniques*.
    - Working Group 2 - Cryptography and security mechanisms.
        - Other WGs: Infosec management systems, sec. eval/testing/spec, sec. controls and services, identity management and *privacy technologies*.
    - ISO/IEC 18033 Part 6 - Homomorphic encryption (published 2019-05)
        - 18033 “Encryption algorithms” (General, asym. enc, block/stream ciphers, IBE)

Many flavors of standardization

- ISO/IEC JTC 1 SC 27 *IT Security Techniques*.
  - Working Group 2 - Cryptography and security mechanisms.
    - Other WGs: Infosec management systems, sec. eval/testing/spec, sec. controls and services, identity management and *privacy technologies*.
  - ISO/IEC 18033 Part 6 - Homomorphic encryption (published 2019-05)
    - 18033 “Encryption algorithms” (General, asym. enc, block/stream ciphers, IBE)
    - **Does not include RLWE-based solution, only Paillier and (exponential) El-Gamal.**
    - **Include a "general model” for HE.**

Many flavors of standardization

- ISO/IEC JTC 1 SC 27 *IT Security Techniques*.
  - Working Group 2 - Cryptography and security mechanisms.
    - Other WGs: Infosec management systems, sec. eval/testing/spec, sec. controls and services, identity management and *privacy technologies*.
  - ISO/IEC 18033 Part 6 - Homomorphic encryption (published 2019-05)
    - 18033 "Encryption algorithms" (General, asym. enc, block/stream ciphers, IBE)
    - Does not include RLWE-based solution, only Paillier and (exponential) El-Gamal.
    - Include a general model for HE.
- IETF / IRTF
  - Internet Engineering Task Force (IETF): engineering and standards making.
  - Internet Research Task Force (IRTF): longer term research issues related to the Internet
    - Crypto Forum Research Group (CFRG) is a general forum for discussing and reviewing uses of cryptographic mechanisms, both for network security in general and for the IETF in particular.
      - RFCs: hash based signatures, AES-GCM-SIV
      - Active drafts RFCs: Hash to EC, VRFs, BLS signatures, OPRFs, Transition to PQC, Argon2, Kangaroo12, Hybrid PKE, etc.

Many standardization efforts

- NIST (US)
  - Competitions: one algorithm wins
    - AES (199X-199X), SHA3 (2007-2012)
  - Standardization efforts: one or more algorithms
    - **PQC (incl. LWE-based solutions)**, LWC
    - NIST conducted internal studies, published NISTIRs, workshops
  - Adoptions from other standards
    - E.g., ECDSA and RSA in FIPS 186 comes from X9.62 (now X9.142) and X9.31
    - CCM mode comes from IEEE 802.11
    - XTS-AES (disk encryption) comes from IEEE Std 1619-2007
  - Guideline standards and in-house dev
    - GCM, SP 800-131A (crypto transition), SP 800-57 (key management), SP 800-52 (TLS guidelines)
  - Held workshop on threshold encryption (MPC), expressed interest in ZKP

Open initiatives from the community

- Homomorphicencryption.org
  - 4 standard workshops since 2017 (~6 months)
  - Three white papers: http://homomorphicencryption.org/standard/
    - API/Utility, Security, and Applications
- Zkproof.org
  - Inspired from model of homomorphicencryption.org
  - 2 workshops since 2018
  - Three white papers: http://zkproof.org/documents.html
    - Security, Implementation, and Applications
- iDash competition
  - Since 2014
  - Track II: Secure Genotype Imputation using Homomorphic Encryption

- United Nations Handbook for Privacy-preserving Computation Technologies

Tomorrow in Santa Barbara!

1st Workshop on Advanced Cryptography Standardization

August 18, 2019.

Colocated with CRYPTO.

https://acs19.zkproof.org

- Representation of different standardization efforts.
- Slides will be put online after the talks.

Agenda

Luís Brandão (NIST) — A perspective on standardization of advanced cryptography at NIST

Kristin Lauter (Microsoft) — HomomorphicEncryption.org—a Community Effort

Ran Canetti (Boston University and Tel Aviv University) — Towards Standardizing Zero Knowledge.

Mariana Raykova (Google) — Advanced Cryptography on the Way to Practice.

Riad S. Wahby (Stanford) — An update on IETF standardization around elliptic curves.

Samuel Ranellucci (Unbound) — Standardizing Threshold Cryptography.

Karim Eldefrawy (SRI) — Computer-aided Verification and Software Synthesis for Secure Multi-Party Computation Protocols.

Panel with Hugo Krawczyk (Algorand Foundation), Dahlia Malkhi (Calibra), Eran Tromer (Columbia & TAU), Luís Brandão (NIST), Tanja Lange (Eindhoven University of Technology).

Tomorrow in Santa Barbara!

1st Workshop on Advanced Cryptography Standardization

August 18, 2019.

Colocated with CRYPTO.

https://acs19.zkproof.org

We're reaching the point where Advanced Crypto is fast enough for practice. Adoption by some companies is here.

- Representation of different standardization efforts.
- Slides will be put online after the talks.

Agenda

Luís Brandão (NIST) — A perspective on standardization of advanced cryptography at NIST

Kristin Lauter (Microsoft) — HomomorphicEncryption.org—a Community Effort

Ran Canetti (Boston University and Tel Aviv University) — Towards Standardizing Zero Knowledge.

Mariana Raykova (Google) — Advanced Cryptography on the Way to Practice.

Riad S. Wahby (Stanford) — An update on IETF standardization around elliptic curves.

Samuel Ranellucci (Unbound) — Standardizing Threshold Cryptography.

Karim Eldefrawy (SRI) — Computer-aided Verification and Software Synthesis for Secure Multi-Party Computation Protocols.

Panel with Hugo Krawczyk (Algorand Foundation), Dahlia Malkhi (Calibra), Eran Tromer (Columbia & TAU), Luís Brandão (NIST), Tanja Lange (Eindhoven University of Technology).

Tomorrow in Santa Barbara!

1st Workshop on Advanced Cryptography Standardization

August 18, 2019.

Colocated with CRYPTO.

https://acs19.zkproof.org

- Representation of different standardization efforts.
- Slides will be put online after the talks.

Formal verification and synthesis has not been studied for HE. I believe this would be a very interesting research direction.

Agenda

Luís Brandão (NIST) — A perspective on standardization of advanced cryptography at NIST

Kristin Lauter (Microsoft) — HomomorphicEncryption.org—a Community Effort

Ran Canetti (Boston University and Tel Aviv University) — Towards Standardizing Zero Knowledge.

Mariana Raykova (Google) — Advanced Cryptography on the Way to Practice.

Riad S. Wahby (Stanford) — An update on IETF standardization around elliptic curves.

Samuel Ranellucci (Unbound) — Standardizing Threshold Cryptography.

Karim Eldefrawy (SRI) — Computer-aided Verification and Software Synthesis for Secure Multi-Party Computation Protocols.

Panel with Hugo Krawczyk (Algorand Foundation), Dahlia Malkhi (Calibra), Eran Tromer (Columbia & TAU), Luís Brandão (NIST), Tanja Lange (Eindhoven University of Technology).

How to be (more) involved?

- ISO: Involvement in standard is mostly by country representatives
  - Sometimes, large projects can get a presence at ISO
  - Otherwise, little visibility in the overall community
  - Huge impact
- NIST: Guest Researcher Programs
  - visit NIST for an extended period of time
  - Publications, internal reports, participation to standardization process
- IRTF/CFRG: mailing list open to everyone
  - Help to review, help to propose new RFCs
- Cross company solutions for de-facto "standards”
- Homomorphicencryption.org and zkproof.org
  - Participate in the documents updates
  - Research to feed the different documents: new cryptanalysis, new applications
  - Development of production-ready libraries to make it easy to use by companies

Thank you

Privacy & Data Protection Office