STPPA#3 Welcome

Cryptographic Technology Group
National Institute of Standards and Technology

Presentation* on July 06, 2021 @ Virtual meeting
Special Topics on Privacy and Public Auditability (STPPA) event #3
Hosted by the Privacy-Enhancing Cryptography (PEC) project

* Luís Brandão — Foreign Guest Researcher at NIST (Contractor via Strativia).
Opinions expressed here are from the speaker and are not to be construed as official views of NIST.
This short presentation

1. The PEC project

2. The STPPA series

3. PEC tools

4. Today’s event

5. Resources
The Privacy-Enhancing Cryptography (PEC) project

▶ A project within the NIST Cryptographic Technology Group (CTG).
▶ **PEC**: broadly refers to cryptography (that can be) used to enhance privacy.

Goals:

1. Accompany the progress of emerging PEC tools [emphasis on non-standardized tools]
2. Develop reference material that can support the use of crypto to enable privacy.
3. Preliminary work on evaluating the potential for standardization of PEC tools.

(Tools ≈ primitives, protocols, techniques, technologies)

https://csrc.nist.gov/projects/pec/
Special Topics on Privacy and Public Auditability (STPPA)

Series of half-day events with talks and/or panel(s)

- Emphasis on privacy-enhancing cryptography (PEC) tools
- Topics relating to privacy and public auditability

Goal: convey basic technical background, incite curiosity, suggest research questions and discuss applications.

Recurring: Various events this year will cover the role of diverse PEC tools

https://csrc.nist.gov/projects/pec/stppa
Example PEC tools

- **ZKP**
  - Zero-Knowledge Proofs

- **SMPC**
  - Secure Multiparty Computation

- **HE**
  - Homomorphic Encryption (Full or Additive)

- **FE**
  - Functional Encryption (Inc. ABE & IBE)

- **GRS**
  - Group and Ring Signatures

- **SE**
  - Searchable Encryption (Symm./PKI)

- **PIR**
  - Private Information Retrieval

- **PSI**
  - Private Set Intersection

Today’s event: STTPA#3 (July 06, 2021)

- 13:30–13:40: **STTPA#3 Welcome.**

  
  Elaine Shi (Carnegie Mellon University)

- 14:20–15:00: **An Overview of Encrypted Databases.**
  
  Seny Kamara (Brown University)

- 15:00–15:10: Break

  
  Kristin Lauter (Facebook AI Research)

- 15:50–16:30+: **Panel: PEC for privacy and public auditability.**
  
  Panelists: All speakers. Moderators: the PEC team.
Video-conference logistics/registrations

- **Video:** Audio and video are being recorded (will later be online; will inform by email).

- **Questions:** Attendees can write questions using the Q&A on Webex (to consider as time permits).

- **Webex registrations:** 166 (excluding speakers and hosts).

Note: data updated after the event, to include registrations received during the event.
PEC webpage resources

**PEC webpage**

https://csrc.nist.gov/projects/pec/

**STPPA subpage**

https://csrc.nist.gov/projects/pec/stppa

---

**Project activities:**

- STPPA series
- PEC use-case suite
- Encounter metrics
- ZKProof collaboration
- Workshops

---

Below is a list of past or scheduled events, with links to further details.

- Event 04 (2021-Sep/Oct tentative)
- Event 03 (2021-July-06) @ Virtual event
- Event 02 (2021-April-19) @ Virtual event
- Event 01 (2020-January-27) @ NIST Gaithersburg

Webpage within the NIST Computer Security Resource Center (CSRC)
Thank you for your attention!

Enjoy today’s STPPA event

We welcome feedback/questions about ongoing PEC activities:

- Join the PEC forum: https://csrc.nist.gov/Projects/pec/email-list
- PEC project email: crypto-privacy@nist.gov
- STPPA specific email: pec-stppa@nist.gov
- PEC website: https://csrc.nist.gov/projects/pec
- STPPA resources: https://csrc.nist.gov/projects/pec/stppa
- The PEC team: Luís Brandão, René Peralta, Angela Robinson