# STPPA#3 Welcome

Cryptographic Technology Group
**N**ational **I**nstitute of **S**tandards and **T**echnology

Presentation* on July 06, 2021 @ Virtual meeting

**S**pecial **T**opics on **P**rivacy and **P**ublic **A**uditability (STPPA) event #3

Hosted by the **P**rivacy-**E**nhancing **C**ryptography (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 **c**ryptography (that can be) used to **e**nhance **p**rivacy.

**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 $\approx$ 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**
**Z**ero-
**K**nowledge
**P**roofs

**SMPC**
**S**ecure
**M**ulti**p**arty
**C**omputation
Previous event

**HE**
**H**omomorphic
**E**ncryption
(Full or Additive)
**Today**

**FE**
**F**unctional
**E**ncryption
(Inc. ABE & IBE)

**GRS**
**G**roup and
**R**ing
**S**ignatures

**SE**
**S**earchable
**E**ncryption
(Symm./PKI)
**Today**

**PIR**
**P**rivate
**I**nformation
**R**etrieval
**Today**

**PSI**
**P**rivate
**S**et
**I**ntersection
Previous event

Legend. Inc: Including. ABE: attribute-based encryption. IBE: identity-based encryption. Symm/pub: symmetric-key of public-key based.

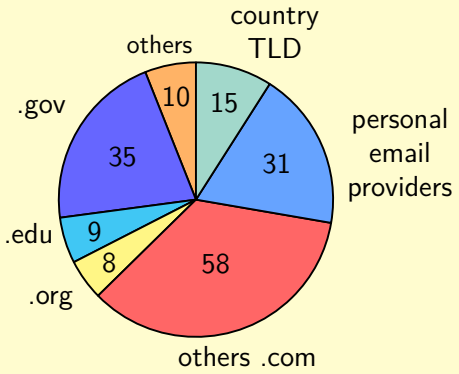
# Today's event: STTPA#3 (July 06, 2021)

(Eastern Daylight Time: UTC-4)

- 13:30–13:40: ***STPPA#3 Welcome.***
- 13:40–14:20: ***Puncturable Pseudorandom Sets and Private Information Retrieval with Near-Optimal Online Bandwidth and Time.***
  Elaine Shi (Carnegie Mellon University)
- 14:20–15:00: ***An Overview of Encrypted Databases.***
  Seny Kamara (Brown University)
- 15:00–15:10: Break
- 15:10–15:50: ***Private AI: Machine Learning on Encrypted Data.***
  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


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