# STPPA #2 Intro:

## Brief comments on PEC and STPPA

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

Presentation* on April 19, 2021 @ Virtual meeting
**S**pecial **T**opics on **P**rivacy and **P**ublic **A**uditability (STPPA) event #2
Hosted by the **P**rivacy-**E**nhancing **C**ryptography (PEC) project @ NIST/ITL/CSD/CTG

* 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 presentation

1. **The PEC project**
   - 1.1 Goals
   - 1.2 PEC tools
   - 1.3 Webpage and activities

2. The **STPPA** series
   - 2.1 The series
   - 2.2 Today's schedule (event #2)
   - 2.3 Video-conference logistics

# This presentation

1. **The PEC project**
   - 1.1 Goals
   - 1.2 PEC tools
   - 1.3 Webpage and activities
2. The **STPPA** series
   - 2.1 The series
   - 2.2 Today's schedule (event #2)
   - 2.3 Video-conference logistics

# 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.

# 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 ≈ primitives, protocols, techniques, technologies)

# Example PEC tools

**ZKP**

**Z**ero-**K**nowledge **P**roofs

**SMPC**

**S**ecure **M**ulti**p**arty **C**omputation

**HE**

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

**FE**

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

**GRS**

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

**SE**

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

**PIR**

**P**rivate **I**nformation **R**etrieval

**PSI**

**P**rivate **S**et **I**ntersection

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

# Example PEC tools

**ZKP**

**Z**ero-**K**nowledge **P**roofs

**SMPC**

**S**ecure **M**ulti**p**arty **C**omputation

Today's event

**HE**

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

**FE**

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

**GRS**

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

**SE**

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

~~Today's event~~*

**PIR**

**P**rivate **I**nformation **R**etrieval

**PSI**

**P**rivate **S**et **I**ntersection

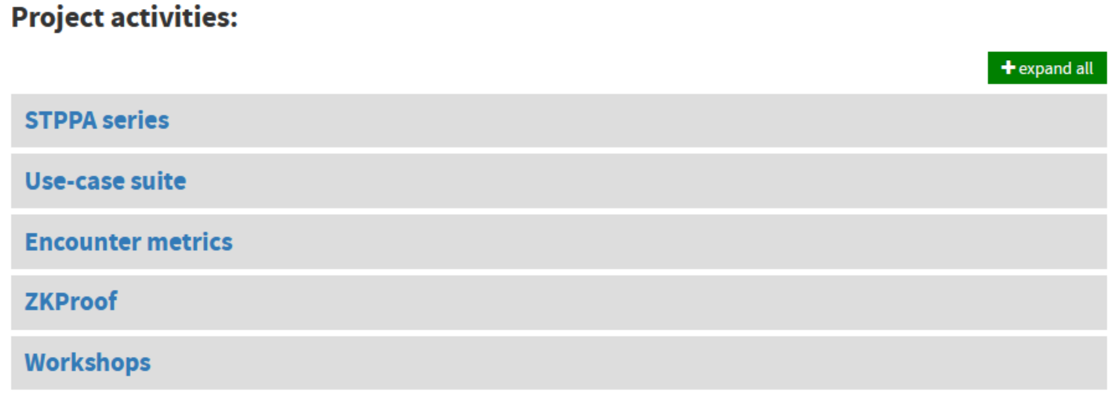
Today's event

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

* Slide adjustment after the event, based on schedule change.

# PEC webpage

https://csrc.nist.gov/projects/pec/ showcases the ongoing PEC activities ... and other links



Project activities:

STPPA series

Use-case suite

Encounter metrics

ZKProof

Workshops

Webpage within the NIST Computer Security Resource Center (CSRC)

# This presentation

1. **The PEC project**
   - 1.1 Goals
   - 1.2 PEC tools
   - 1.3 Webpage and activities

2. The **STPPA** series
   - 2.1 The series
   - 2.2 Today's schedule (event #2)
   - 2.3 Video-conference logistics

# Special Topics on Privacy and Public Auditability (STPPA)

**Series of half-day events:**

- **Talks+panel:** on interconnected topics related 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

# Today's event: STTPA #2 (April 19, 2021)

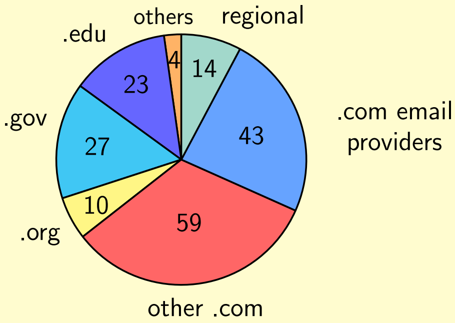
(Eastern Daylight Time: UTC-4)

- 13:00–13:15: **Intro: STPPA and PEC.**
- 13:15–13:55: **A Brief Overview of Private Set Intersection.**
  Mike Rosulek (Oregon State University)
- 13:55–14:55: **Secure computation on datasets.**
  Steve Lu (Stealth Software Technologies) and Rafail Ostrovsky (UCLA)
- 14:55–15:10: Break
- 15:20–16:00: **Panel: PEC for privacy and public auditability.**
  Panelists: All speakers. Moderators: the PEC team.

Note: this slide has been adjusted after the event, to reflect a schedule adjustment.

# 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:** 180 (excluding speakers and hosts).



Note: this slide has been adjusted after the event, to reflect the latest registration statistics.

# Thank you for your attention!

**We hope you enjoy today's talks and panel.**

We welcome feedback/questions about ongoing PEC activities:

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