STPPA#5 Welcome and Introduction

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

Presented* on February 09, 2023 @ Virtual meeting

Special **T**opics on **P**rivacy and **P**ublic **A**uditability (STPPA) event #5

Hosted by the **P**rivacy-**E**nhancing **C**ryptography (PEC) project

* Luís Brandão (NIST/Strativia: Foreign Guest Researcher [non-employee] at NIST, contractor from Strativia). Expressed opinions are those of the speaker(s) and are not to be construed as official views of NIST. (Slides updated on 2023-Feb-13)

This short presentation

- **Context:** the PEC project; the STPPA series.
- **Today's event:** topic; schedule; webinar details
- **PEC online resources**

The Privacy-Enhancing Cryptography (PEC) project

- A project within the **NIST Cryptographic Technology Group** (@ Computer Security Division, Information Technology Lab).
- **PEC:** broadly refers to **cryptography** (that can be) used to **enhance privacy**.

[emphasis on non-standardized tools]

Goals:

1. Accompany the progress of **emerging *PEC tools*** (including research).
2. Develop **reference material** that can support the use of crypto to enable privacy.
3. **Exploratory work** on evaluating the potential for standardization of *PEC tools*.

ZKP	MPC	FHE	PSI	GRS	FnE	PIR	StE
Zero-**K**nowledge **P**roofs	(**S**ecure) **M**ultiparty **C**omputation	**F**ully **H**omomorphic **E**ncryption	**P**rivate **S**et **I**ntersection	**G**roup and **R**ing **S**ignatures	**Fu**nctional **E**ncryption (Inc. ABE & IBE)	**P**rivate **I**nformation **R**etrieval	**St**ructured **E**ncryption (Symm./Pub.)

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

Special Topics on Privacy and Public Auditability (STPPA)

Series of half-day events with talks and a panel conversation
https://csrc.nist.gov/projects/pec/stppa

Event 05 (2023-Feb-09): IBE, ABE, and broadcast encryption

Event 04 (2022-Nov-21): anonymous credentials, and blind signatures

Event 03 (2021-Jul-06): PIR, encrypted search, and FHE

Event 02 (2021-Apr-19): PSI, and MPC

Event 01 (2020-Jan-27): public rand., diff. privacy, and video time-auth.

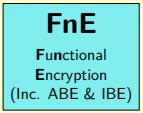
Legend: ABE = **a**ttribute-**b**ased **e**ncryption. auth. = **auth**entication. diff. = **diff**erential. FHE = **f**ully-**h**omomorphic **e**ncryption. IBE = **I**dentity-**b**ased **e**ncryption. MPC = (secure) **m**ulti**p**arty **c**omputation. PIR = **p**rivate **i**nformation **r**etrieval. PSI = **p**rivate **s**et **i**ntersection. rand. = **rand**omness.

STPPA#5 featured topics

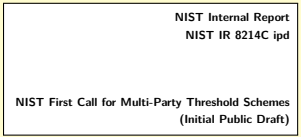
{identity-based, attribute-based, and broadcast} encryption

Why these topics?

1. ***PEC tools* of interest** in upcoming NIST report on "Privacy Enhancing Cryptography" (2023)



2. **NIST Call for Multi-Party Threshold Schemes**
   Subcategory 2.6 is for submission of IBE/ABE/...
   (Public comments open till 2023-Apr-10)



3. **Real world importance** (as today's speakers will tell us)

STPPA#5 schedule (February 09, 2023)

Featured topics: {identity-based, attribute-based, and broadcast} encryption

- 12:00–12:10: ***STPPA#5 Welcome*** (Eastern Standard Time: UTC-5)
- 12:10–13:00: ***Identity Based Encryption: an Overview***
  Dan Boneh (Stanford University)
- 13:00–13:50: ***Attribute-Based Encryption, Variants, and Pairing-Based Instantiations.***
  Melissa Chase (Microsoft Research)
- 13:50–14:10: Break
- 14:10–15:00: ***Attribute-Based and Broadcast Encryption from Lattices***
  Hoeteck Wee (NTT Research)
- 15:00–15:50: ***STPPA#5 Panel conversation on IBE, ABE and broadcast encryption***
  Panelists: the 3 speakers + Tanya Verma (Cloudflare). Moderators: the PEC team.

Event details: https://csrc.nist.gov/events/2023/stppa5

Video-conference logistics/registrations

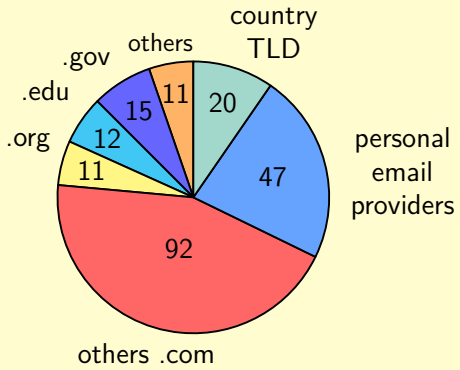
- **Virtual registrations:** 208*
  (Not counting speakers and hosts)

  29 declared countries: US (145); DE (10), CA (7), ...

- **Video:** Audio and video are being recorded (posting will be announced in the PEC-forum)

- **Questions:** Attendees can use the virtual Q&A (to be considered as time permits)

Per registered email address:



* Updated (from 191), after the event, to account for same-day registrations. Not counting speakers (4) and hosts (3).

PEC online

We welcome feedback/questions about ongoing PEC activities:

- Join the PEC forum: https://csrc.nist.gov/projects/pec/email-list
- Email: (PEC project) crypto-privacy@nist.gov; (STPPA) 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

Enjoy today's STPPA event!

Thank you for your attention!