STPPA #8 Welcome and Introduction

Presented* from Gaithersburg (Maryland, USA), 2025-Sep-18

Special **T**opics on **P**rivacy and **P**ublic **A**uditability, Event #**8**

https://csrc.nist.gov/events/2025/stppa8

Event organized by the Privacy-Enhancing Cryptography (PEC) project at NIST-ITL-CSD-CTG

* Presented by Luís Brandão (At NIST as a Foreign Guest Researcher, Contractor from Strativia)

Welcome to STPPA #8

The **8**th Event of the **S**pecial **T**opics on **P**rivacy and **P**ublic **A**uditability.

We are gathering to **to learn** and **recall** insights about implementations of:

- **Private Set Intersection (PSI)**
- **Zero-Knowledge Proof (ZKP)**
- **Threshold BLS Signatures (T-BLS)**

This brief presentation gives context and sets expectations about the half-day virtual event.

Outline

1. **The NIST-PEC-STPPA Context**
2. **PEC Topics in STPPA #8**
3. **Webinar Logistics**

NIST = **N**ational **I**nstitute of **S**tandards and **T**echnology.
PEC = **P**rivacy-**E**nhancing **C**ryptography.
STPPA = **S**pecial **T**opics on **P**rivacy and **P**ublic **A**uditability.

Outline

NIST = **N**ational **I**nstitute of **S**tandards and **T**echnology.
PEC = **P**rivacy-**E**nhancing **C**ryptography.
STPPA = **S**pecial **T**opics on **P**rivacy and **P**ublic **A**uditability.

National Institute of Standards and Technology

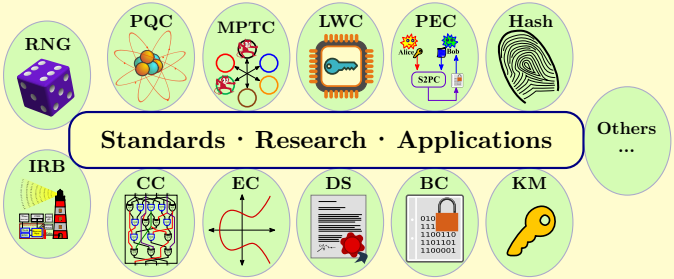
- **Non-regulatory** federal agency (@ U.S. Dept. Commerce)
- **Mission:** ... innovation ... industrial competitiveness ... measurement science, standards, and technology ... economic security ... quality of life.
- **NIST:** Laboratories → Divisions → Groups

NIST name and address plate (source: nist.gov)

INFORMATION TECHNOLOGY LABORATORY → **Computer Security Division (CSD)**

→ **Cryptographic Technology Group (CTG):** *research, develop, engineer, and produce guidelines, recommendations and best practices for cryptographic algorithms, methods, and protocols.*

Various projects in the “Crypto” Group



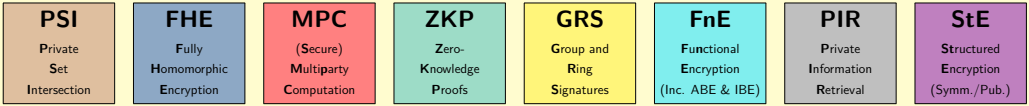
BC = Block Ciphers
CC = Circuit Complexity
DS = Digital Signatures
EC = Elliptic Curves
IRB = Interoperable Randomness Beacons
KM = Key Management
LWC = Lightweight Cryptography
MPTC = Multi-Party Threshold Cryptography
PEC = Privacy-Enhancing Cryptography
PQC = Post-Quantum Cryptography
RNG = Random-Number Generation
...

- **Standardization and guidelines:** PQC, LWC, RBG, ...
- **Exploratory (advanced cryptography): PEC**, MPTC, ...
- **Research and applications:** circuit complexity, randomness beacons, ...

More details at https://www.nist.gov/itl/csd/cryptographic-technology

Privacy-Enhancing Cryptography (PEC)

- **Program scope:** Accompany the progress of PEC; promote PEC reference material.
  (PEC $\approx$ non-standardized advanced crypto used/usable for privacy applications)



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

- **Various interactions support the gathering of reference material:**
  - **STPPA series:** Special Topics on Privacy and Public Auditability
  - **WPEC 2024:** NIST Workshop on PEC (including **The First PSI Day**)
  - **Threshold Call** (with MPTC): to form a body of reference material (including, FHE, ZKP)

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

Special Topics on Privacy and Public Auditability (STPPA)

Series of half-day events with talks and a panel conversation

Event 08 (2025-Sep-18): PSI, ZKP, Threshold BLS Signatures
Event 07 (2025-Jan-16): {Timelock, Witness, Deniable} Encryption
Event 06 (2023-Jul-25): FHE, MPC, ZKP, ABE, and others
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., differential privacy, and video time-auth.

Legend: ABE = attribute-based encryption. auth. = authentication. FHE = fully-homomorphic encryption. IBE = Identity-based encryption. MPC = (secure) multiparty computation. PIR = private information retrieval. PSI = private set intersection. rand. = randomness. ZKP = zero-knowledge proof.

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

Outline

NIST = **N**ational **I**nstitute of **S**tandards and **T**echnology.
PEC = **P**rivacy-**E**nhancing **C**ryptography.
STPPA = **S**pecial **T**opics on **P**rivacy and **P**ublic **A**uditability.

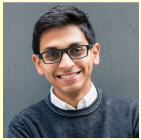
STPPA #8's Theme: Experimenting with PEC implementations

Featuring three speakers/topics:

PSI

Ni Trieu

ZKP



Pratyush Mishra

T-BLS

Sourav DAS

Legend: PSI = **P**rivate **S**et **I**ntersection. ZKP = **Z**ero-**K**nowledge **P**roof. T-BLS = **T**hreshold **BLS** Signatures.

The PEC team thanks the speakers, and wishes a PEC-insightful STPPA#8 to everyone.

The PEC team:

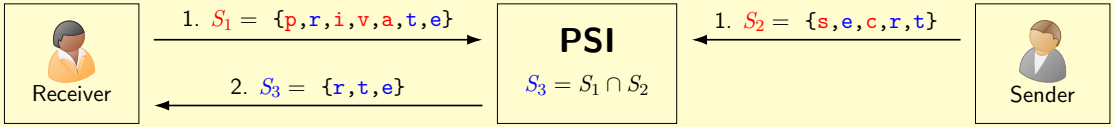
Luís Brandão

René Peralta

Angela Robinson

Private-Set Intersection (PSI)

Obtain the intersection of two sets, without disclosing the non-intersecting elements.



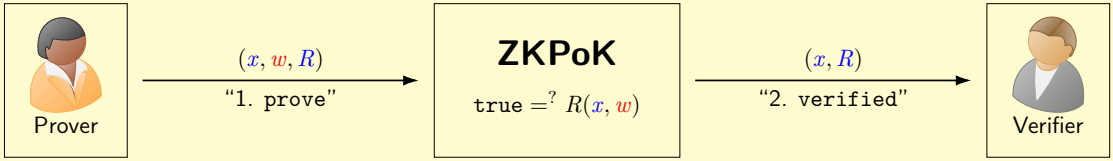
(The middle box is an abstraction; there is no actual intermediary)

- **Insecure:** Compare **hashes** (usual non-cryptographer's intuition)
- **Secure:** Compare **Oblivious-PRF** outputs (PRF = **P**seudo**r**andom **f**unction)

- **Generalizations:** Circuit-PSI (only learn $f(S_3)$), multi-party (≥ 2), ...
- Check "**The First PSI day**" organized within WPEC 2024 (NIST workshop)

Zero-Knowledge Proof of Knowledge (ZKPoK)

Prove knowledge of a secret w (witness) *related* (via a relation R) to a public statement (**x**).



(The middle box is an abstraction; there is no actual intermediary)

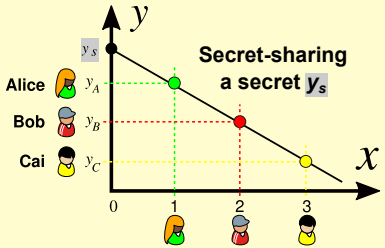
Example: prove knowledge of a private key corresponding to a public key.

Many nuances/concepts:

- **What is achieved:** Transferable versus deniable; Proof versus argument; ...
- **Method:** General versus special purpose; ...
- **How it is achieved:** Succinctness and efficiency; trusted setup versus transparent; ...

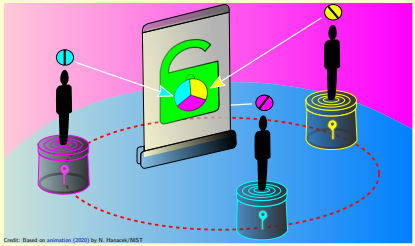
Threshold Signature

Secret-sharing:

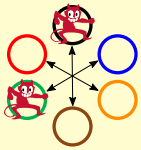


Splits the key into secret shares

Multi-party computation (MPC)



Operates without recombining the key



Participation threshold: the operation needs k parties in agreement

Corruption threshold: system secure even if f parties are malicious

Outline

NIST = **N**ational **I**nstitute of **S**tandards and **T**echnology.
PEC = **P**rivacy-**E**nhancing **C**ryptography.
STPPA = **S**pecial **T**opics on **P**rivacy and **P**ublic **A**uditability.

STPPA #8: Special Topics on Privacy and Public Auditability, Event 8

Theme: Experimenting with implementations of some PEC primitives

- 10:00–10:20: ***STPPA #8 Welcome and Introduction.***
- 10:20–11:20: ***Implementing PSI: From Elliptic Curves to Oblivious Transfer and Distance-Aware Extensions.*** Ni Trieu (Arizona State University, USA)
- 11:30–12:30: ***How to Program ZKPs.*** Pratyush Mishra (University of Pennsylvania, USA)
- 12:30–13:30: Lunch Break
- 13:30–14:30: ***A Deep Dive Into the Threshold BLS Signature Scheme.*** Sourav Das (University of Illinois Urbana-Champaign; Category Labs, USA)
- 14:40–15:30: ***STPPA8 Panel.*** All speakers.

(All times are in EDT = UTC -4)

Updates and details at https://csrc.nist.gov/events/2025/stppa8

Logistic notes for good workshop functioning

- **Code of Conduct:** Participation in STPPA #8 requires abiding to the Code of Conduct for NIST conferences: https://www.nist.gov/pao/code-conduct-nist-conferences

- **Slide-decks and presentation videos:** Will be published on the event webpage
- **Text/chat:** Should be limited to only PEC/workshop-related matters. Can be used for comments about the presentations.

Disclaimer: *The opinions expressed in this event are those of the speakers. The selection of STPPA #8 talks, and the publication of related media and metadata, should not be construed as indicating any preference, indication of suitability, recommendation or endorsement by NIST about the discussed technology, identified entities, equipment, materials, or expressed ideas.*

STPPA #8 Online Registrations

- **Virtual registrations:*** **160**

  (Not counting 3 speakers, 3 hosts, 4 in-person attendees)

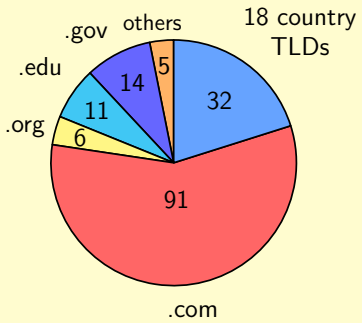
  Across 33 countries: US (78); IN (18); DE (12), UK (6), CA (5), And 28 other countries (37).

- **Live attendees: 111** (101 virtual;† 3 hosts; 3 speakers; 4 in-person attendees).

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

- **Questions:** Attendees can use the virtual Q&A.

Per registered email address:



* Slide Updated after the event (from 140 to 160), to account for registrations on the day of the event. † As reported by ZoomGov (a partial attendance counts as 1).

Legend: CA = Canada; DE = Germany; IN = India; PL = Poland; Q&A = Questions and answers; TLD = Top-Level Domain; UK = United Kingdom; US = United States.

Thank you for your attention!

STPPA #8 Welcome and Introduction

Notes presented at **S**pecial **T**opics on **P**rivacy and **P**ublic **A**uditability, Event #**8**

September 18, 2025, from Gaithersburg (Maryland, USA) — luis.brandao@nist.gov

Useful links

- **STPPA8 Webpage:** https://csrc.nist.gov/events/2025/stppa8
- **PEC-STPPA Contact:** pec-stppa@nist.gov
- **PEC Website:** https://csrc.nist.gov/projects/pec
- **Subscribe to the PEC-Forum:** https://csrc.nist.gov/projects/pec/email-list