STPPA #7 Welcome and Introduction

Presented* at STPPA 7:

Special **T**opics on **P**rivacy and **P**ublic **A**uditability, Event #**7**

2025-Jan-16th, from Gaithersburg (Maryland, USA)

https://csrc.nist.gov/events/2025/stppa7

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

Welcome to STPPA#7

The 7^{th} Event of the **S**pecial **T**opics on **P**rivacy and **P**ublic **A**uditability.

Today we are looking forward to **learn** about three exquisite types of encryption:

- **Timelock** Encryption
- **Witness** Encryption
- **Deniable** Encryption

Welcome to STPPA#7

The $\mathbf{7}^{\text{th}}$ Event of the **S**pecial **T**opics on **P**rivacy and **P**ublic **A**uditability.

Today we are looking forward to **learn** about three exquisite types of encryption:

- **Timelock** Encryption
- **Witness** Encryption
- **Deniable** Encryption

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

Outline

1. **The NIST-PEC-STPPA Context**

2. **Today's Event: STPPA #7**

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

1. **The NIST-PEC-STPPA Context**

2. **Today's Event: STPPA #7**

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 name and address plate (source: nist.gov)

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 (**≈ 7000 **persons):** Laboratories $\rightarrow$ Divisions $\rightarrow$ Groups

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

National Institute of Standards and Technology

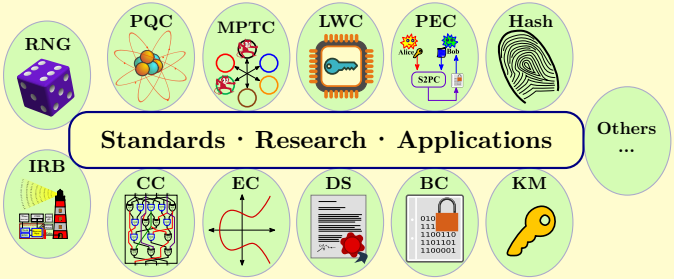
- **Non-regulatory** federal agency (@ U.S. Dept. Commerce)
- **Mission:** ... innovation ... industrial competitiveness ... measurement science, standards, and technology ... economic security ... quality of life.
- **NIST (≈ 7000 persons):** Laboratories $\rightarrow$ Divisions $\rightarrow$ Groups

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

ITL INFORMATION TECHNOLOGY LABORATORY $\rightarrow$ **Computer Security Division (CSD)**

$\rightarrow$ **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



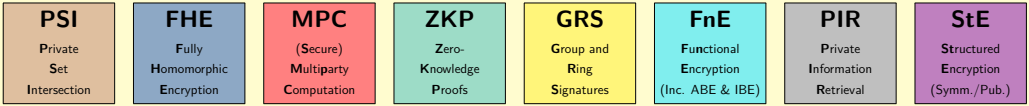
BC = Block Ciphers
CC = Circuit Complexity
DS = Digital Signatures
EC = Elliptic Curves
IRB = Interoperable Randomness Beacons
KM = Key Management
LWC = Lightweight Cryptography
MPTC = Multi-Party Threshold Cryptography
PEC = Privacy-Enhancing Cryptography
PQC = Post-Quantum Cryptography
RNG = Random-Number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

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

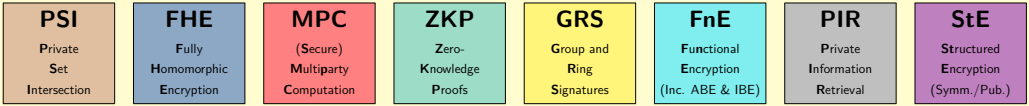


Legend: ABE: attribute-based encryption. IBE: identity-based encryption. Symm./pub.: symmetric-key or public-key based.

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

Privacy-Enhancing Cryptography (PEC) [NIST Project]

- **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.

- **Activities supporting creation of reference material:**
  - **As organizer:** STPPA series; Threshold Call (with MPTC); WPEC 2024.
  - **As collaborator/participant:** Nat'l Strategies; ZKProof; HES.
  - **Occasional writeups:** Encounter metrics; privacy blogpost; ...

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 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 = **a**ttribute-**b**ased **e**ncryption. auth. = **auth**entication. 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. ZKP = **z**ero-**k**nowledge **p**roof.

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

Various NIST Series of Crypto Talks

- **NIST Crypto Reading Club:** crypto-club-questions@nist.gov
  https://csrc.nist.gov/projects/crypto-reading-club

- **NIST PQC Seminar:** pqc-seminars@nist.gov
  https://csrc.nist.gov/projects/post-quantum-cryptography/workshops-and-timeline/pqc-seminars

- **Special Topics on Privacy and Public Auditability:** pec-stppa@nist.gov
  https://csrc.nist.gov/projects/pec/stppa

- (Upcoming) **Threshold Crypto Seminar:** threshold-crypto@nist.gov
  Once the Threshold Call final version is released in 2025

See "Other NIST-hosted presentations/workshops" list at https://csrc.nist.gov/projects/crypto-reading-club

Outline

1. The NIST-PEC-STPPA Context

2. **Today's Event: STPPA #7**

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.

STPPA7 Schedule: Half-day virtual event (12:00–16:00 EST)

- 12:00–12:15: Intro: ***STPPA #7 Welcome and Introduction.***
- 12:15–13:00: Invited talk 1: ***Timelock Encryption: An Overview and Retrospective.***
  Kelsey Melissaris (Aarhus University, Denmark) and Yolan Romailler (Randamu Inc, Switzerland & USA)
- 13:00–13:45: Invited talk 2: ***Witness Encryption: Theory and Practice.***
  Sanjam Garg (UC Berkeley, USA)
- 13:45–14:30: Break (45 min)
- 14:30–15:15: Invited talk 3: ***The Multiple Faces of Deniability.***
  Rafail Ostrovsky (UCLA, USA)
- 15:15–16:00: Panel: ***STPPA7 Panel.*** All speakers.

Updates and details at https://csrc.nist.gov/events/2025/stppa7

Why this set of topics for today's event?

{Timelock, Witness, Deniable} Encryption

- Expand the **diversity** of topics/concepts covered by the STPPA series.
- Showcase challenges and opportunities related to **advanced cryptography**.
- Promote reflection on **applications for privacy and public auditability**.

Why this set of topics for today's event?

{Timelock, Witness, Deniable} Encryption

- Expand the **diversity** of topics/concepts covered by the STPPA series.
- Showcase challenges and opportunities related to **advanced cryptography**.
- Promote reflection on **applications for privacy and public auditability**.

The PEC team


Luís Brandão


René Peralta


Angela Robinson

- thanks the speakers for their participation.
- wishes a PEC-insightful STPPA7 to everyone.

Why this set of topics for today's event?

{Timelock, Witness, Deniable} Encryption

- Expand the **diversity** of topics/concepts covered by the STPPA series.
- Showcase challenges and opportunities related to **advanced cryptography**.
- Promote reflection on **applications for privacy and public auditability**.

The PEC team


Luís Brandão


René Peralta


Angela Robinson

- thanks the speakers for their participation.
- wishes a PEC-insightful STPPA7 to everyone.

Disclaimer: *It is assumed that the opinions expressed in this event are those of the speakers. The selection of STPPA7 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.*

Logistic notes for good workshop functioning

- **Code of Conduct:** Participation in STPPA7 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 workshop webpage
- **Text/chat:** Should be limited to only PEC/workshop-related matters. Can be used for comments about the presentations.
- **Q&A:** Questions and comments from the audience are encouraged:
  - Some may be relayed during the Q&A periods after the talks.
  - Speakers can also follow up in the chat, after the talk.
  - Virtually-raised hands may be selected for an oral comment (which will be recorded)

Thank you for your attention!

STPPA #7 Welcome and Introduction

Notes presented at **S**pecial **T**opics on **P**rivacy and **P**ublic **A**uditability, Event #**7** 2024

January 16, 2025, from Gaithersburg (Maryland, USA) — luis.brandao@nist.gov

Useful links

- **STPPA7 Webpage:** https://csrc.nist.gov/events/2025/stppa7
- **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