# STPPA#6 Welcome and Introduction

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

Presented* on July 25th, 2023 @ Virtual meeting

**S**pecial **T**opics on **P**rivacy and **P**ublic **A**uditability (STPPA) event #6

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 author and should not be construed as official views of NIST. (Slides updated on 2023-July-27).

# Outline

1. High-level context: PEC, MPTC, STPPA

2. Today's STPPA#6 (topics, schedule, statistics, logistics)

3. Online resources

# Outline

1. High-level context: PEC, MPTC, STPPA

2. Today's STPPA#6 (topics, schedule, statistics, logistics)

3. Online resources

# Two NIST-Crypto projects related to today's event

(i.e., projects in the Cryptographic Technology Group at NIST)

- **PEC:** "**privacy-enhancing cryptography**" (advanced features/functionalities)
- **MPTC:** "**multi-party threshold cryptography**" (threshold schemes for crypto primitives)

# Two NIST-Crypto projects related to today's event

(i.e., projects in the Cryptographic Technology Group at NIST)

- **PEC:** "**privacy-enhancing cryptography**" (advanced features/functionalities)
- **MPTC:** "**multi-party threshold cryptography**" (threshold schemes for crypto primitives)

**The "Threshold Call" (from MPTC+PEC):**

*NIST First Call for Multi-Party Threshold Schemes*

[see NISTIR 8214C] to gather **reference material** for public analysis ...

aiming for **recommendations** (in a 1st phase), including about PEC.

# The Privacy-Enhancing Cryptography (PEC) project

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

[emphasis on non-standardized tools]

| **FHE** | **MPC** | **ZKP** | **FnE** | **PSI** | **GRS** | **PIR** | **StE** |
|---|---|---|---|---|---|---|---|
| **F**ully **H**omomorphic **E**ncryption | (**S**ecure) **M**ulti**p**arty **C**omputation | **Z**ero-**K**nowledge **P**roofs | **Fun**ctional **E**ncryption (Inc. ABE & IBE) | **P**rivate **S**et **I**ntersection | **G**roup and **R**ing **S**ignatures | **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.

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

# 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***.
2. Promote development of **reference material**.
3. **Exploratory work** to assess potential for recommendations, standardization; ....

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

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

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 06 (2023-Jul-25):** FHE, MPC, ZKP, ABE, PAKE, threshold crypto

**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.

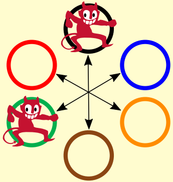
https://csrc.nist.gov/projects/pec/stppa

**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. PAKE = **p**assword-**a**uthenticated **k**ey-**e**xchange. PIR = **p**rivate **i**nformation **r**etrieval. PSI = **p**rivate **s**et **i**ntersection. rand. = **rand**omness.

# Multi-Party Threshold Cryptography: NIST project

**Cryptographic primitives:** Signing Encryption KeyGen Hashing etc.

**Threshold schemes (for cryptographic primitives):**

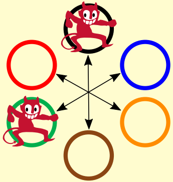


https://csrc.nist.gov/projects/threshold-cryptography

# Multi-Party Threshold Cryptography: NIST project

**Cryptographic primitives:** Signing Encryption KeyGen Hashing etc.

**Threshold schemes (for cryptographic primitives):**



1. Split (**secret-share**) the secret/private-key across multiple parties.
2. Use **MPC** to perform needed operation (with split key), e.g., sign.

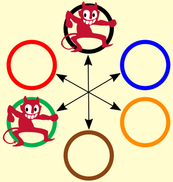
   (MPC = secure multiparty computation ... or call it “Threshold Cryptography”)

https://csrc.nist.gov/projects/threshold-cryptography

# Multi-Party Threshold Cryptography: NIST project

**Cryptographic primitives:** Signing Encryption KeyGen Hashing etc.

**Threshold schemes (for cryptographic primitives):**



1. Split (**secret-share**) the secret/private-key across multiple parties.
2. Use **MPC** to perform needed operation (with split key), e.g., sign.

   (MPC = secure multiparty computation … or call it “Threshold Cryptography”)

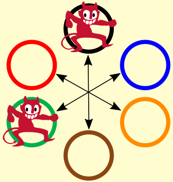
- **“Threshold” ($f$):** Operation is secure if number of corrupted parties is $\leq f$.
- **Decentralized** trust about key **(not reconstructed)**: avoids single-point of failure.

https://csrc.nist.gov/projects/threshold-cryptography

# Multi-Party Threshold Cryptography: NIST project

**Cryptographic primitives:** Signing Encryption KeyGen Hashing etc.

**Threshold schemes (for cryptographic primitives):**



1. Split (**secret-share**) the secret/private-key across multiple parties.
2. Use **MPC** to perform needed operation (with split key), e.g., sign.

   (MPC = secure multiparty computation … or call it "Threshold Cryptography")

- **"Threshold" ($f$):** Operation is secure if number of corrupted parties is $\leq f$.
- **Decentralized** trust about key **(not reconstructed)**: avoids single-point of failure.

Primitives featured in today's event are of interest to the **NIST Threshold Call**

https://csrc.nist.gov/projects/threshold-cryptography

# Outline

1. High-level context: PEC, MPTC, STPPA

2. Today's STPPA#6 (topics, schedule, statistics, logistics)

3. Online resources

# STPPA#6 technical scope

**Theme:** Community Efforts on Advanced Cryptographic Techniques.

**Featured topics:** FHE, MPC, ZKP, ABE, PAKE, threshold crypto, ...

**Why these topics?**

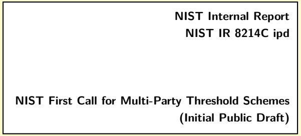
# STPPA#6 technical scope

**Theme:** Community Efforts on Advanced Cryptographic Techniques.

**Featured topics:** FHE, MPC, ZKP, ABE, PAKE, threshold crypto, ...

**Why these topics?**

1. ***PEC tools* of interest** in upcoming NIST report on "Privacy Enhancing Cryptography"
2. **NIST Call for Multi-Party Threshold Schemes**
   Scope of submissions includes FHE, ZKP, MPC, ABE, ...
   (NISTIR 8214C ipd ... revised version is upcoming)



**NIST Internal Report**
**NIST IR 8214C ipd**

**NIST First Call for Multi-Party Threshold Schemes**
**(Initial Public Draft)**

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

# STPPA#6 Schedule (July 25th, 2023)

(Eastern Daylight Time: UTC-4)

- **09:30**–10:00: **STPPA#6 welcome and introduction**

---

- **10:00**–10:30: Talk on **HomomorphicEncryption** efforts on **f**ully-**h**omomorphic **e**ncryption (FHE)
- 10:30–11:00: Talk on **MPC Alliance** efforts on **s**ecure **m**ulti**p**arty **c**omputation (MPC)

---

- **11:15**–11:45: Talk on **ZKProof** efforts on **z**ero-**k**nowledge **p**roofs (ZKP)
- 11:45–12:15: Talk on **ETSI** efforts on **a**ttribute-**b**ased **e**ncryption (ABE)

---

- **12:45**–13:15: Talk on **CFRG** efforts on various advanced cryptographic techniques
- 13:15–13:45: Talk on **ISO/IEC** efforts on **f**ully-**h**omomorphic **e**ncryption (FHE)

---

- **14:00**–15:00$^+$: **Panel conversation** with all the speakers

**Event details:** https://csrc.nist.gov/events/2023/stppa6 **Contact email:** pec-stppa@nist.gov

For future PEC-related announcements, join the PEC forum: https://csrc.nist.gov/projects/pec/email-list

# Video-conference Webinar (registrations and logistics)

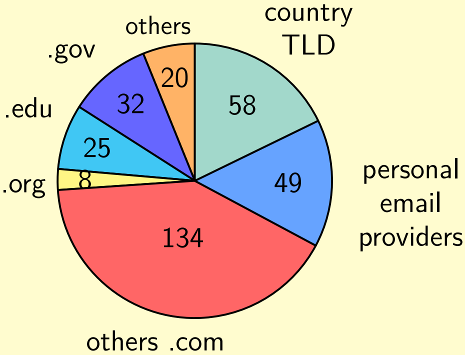
- **Virtual registrations:** 326*
  (Not counting speakers and hosts)

  **Across 32 countries:** US (199); UK (19), IN (18); CA (16), NL (13), DE (11), SG (6), ...

- **Audio and video:** 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 after the event (from 301 to 326), to account for additional registrations during the event. Not counting the external invited speakers (7) and host/welcomer/chairs (5).

Legend: CA = Canada; DE = Germany; IN = India; Q&A = Questions and answers; SG = Singapore; TLD = top-level domain; UK = United Kingdom; US = United States.

# Outline

1. High-level context: PEC, MPTC, STPPA

2. Today's STPPA#6 (topics, schedule, statistics, logistics)

3. Online resources

# Online resources

We welcome feedback/questions about ongoing PEC activities:

- STPPA resources: https://csrc.nist.gov/projects/pec/stppa
- PEC website: https://csrc.nist.gov/projects/pec
- Join the PEC forum: https://csrc.nist.gov/projects/pec/email-list
- Email: (PEC project) crypto-privacy@nist.gov; (STPPA) pec-stppa@nist.gov
- The PEC team: Luís Brandão, René Peralta, Angela Robinson

**Enjoy today's STPPA event!** **Thank you for your attention!**