WPEC 2026 Welcome and Introduction

Presented* at WPEC 2026:

NIST Workshop on Privacy Enhancing Cryptography

2026-Oct-26, from Maryland, USA

https://csrc.nist.gov/events/2026/wpec2026



* Luís Brandão: Foreign Guest Researcher (contractor) at NIST Cryptographic Technology Group.
Expressed opinions are from the speaker. Based on joint work with René Peralta and Angela Robinson.

Welcome to WPEC 2026

The NIST **W**orkshop on **P**rivacy-**E**nhancing **C**ryptography 2026

We look forward to the sharing of insights



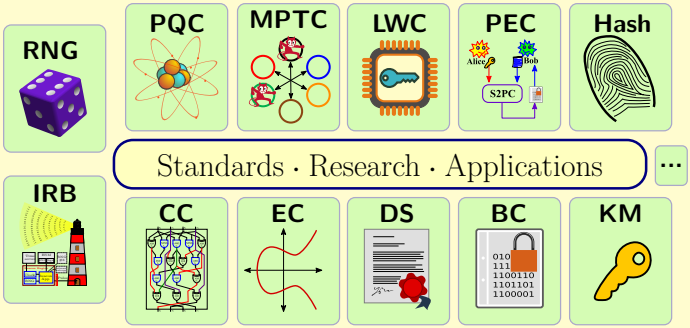
- **6 sessions in 3 days**
- **Welcome remarks**
- **21 talks**
- **22 speakers**
- **400$^+$ registrants**

Presentation Outline

1. **NIST-Crypto Intro**
2. A Workshop on PEC: FHE, PSI, ZKP, ...
3. Workshop Schedule and Logistics

FHE = Fully-Homomorphic Encryption.
NIST = National Institute of Standards and Technology.
PEC = Privacy-Enhancing Cryptography.
PSI = Private Set Intersection.
ZKP = Zero-Knowledge Proof.

Activities in the “Crypto” Group



Legend:

AES = Advanced Encryption Standard.
BC = Block Ciphers. **CC** = Circuit Complexity.
DS = Digital Signatures. **EC** = Elliptic Curves.
FIPS = Federal Information Processing Standards.
IR = Internal or Interagency Report (i.e., public technical report, developed internally or in an interagency collaboration).
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.
SHA = Secure Hash Algorithm.
SP 800 = Special Publications in Computer Security.

- **Public documentation:** FIPS; Special Publications (SP 800); NIST Reports (IR).
- **Standardization initiatives**, e.g., PQC, LWC, AES, SHA, ...
- **Exploratory programs**, e.g., PEC and MPTC.

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

On the PEC and MPTC Programs

Exploratory work to assess potential for recommendations, and standardization processes.

PEC: Privacy-Enhancing Cryptography

- Crypto (that can be) used to enhance privacy [emphasis on non-standardized tools].

FHE	PSI	ZKP	MPC	GRS	FnE	PIR	StE
Fully Homomorphic Encryption	Private Set Intersection	Zero-Knowledge Proofs	(Secure) Multiparty Computation	Group and Ring Signatures	Functional Encryption (Inc. ABE & IBE)	Private Information Retrieval	Structured Encryption (Symm./Pub.)

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

MPTC: Multi-Party Threshold Cryptography

- *Threshold Schemes* for diverse Cryptographic Primitives
- The NIST Threshold Call also considers FHE, ZKP and gadgets.



Main approach: promote development of **reference material**.

NIST Privacy-Enhancing Cryptography (PEC)

Cryptography usable to **enhance privacy**
(emphasis on non-standardized tools)

Focus at WPEC 2026: **FHE** **PSI** **ZKP**

Multi-Party Computation (MPC) and Threshold schemes
Fully-Homomorphic Encryption (FHE)
Private Set Intersection (PSI) / Operations (PSO)
Zero-Knowledge Proof (ZKP)
STPPA (series of talks)
PEC use-case suite
PEC tools

Goals

1. Accompany the progress of **emerging *PEC tools***
2. Promote development of PEC **reference material**
3. **Exploratory work** to assess potential for recommendations, standardization; ...

Various Public Workshops

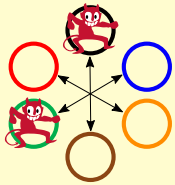
- **STPPA series:** Special Topics on Privacy and Public Auditability
- **WPEC:** Workshops on Privacy-Enhancing Cryptography: 2024, 2026

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

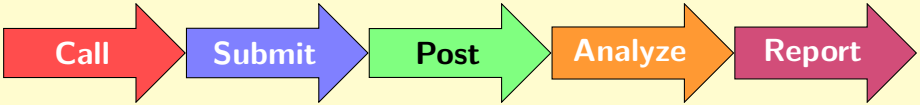
Multi-Party Threshold Cryptography (MPTC)

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.



NIST Threshold Call: Establishes a process to gather reference materials



A public call for threshold schemes, to form a body of reference material

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

60 Submissions in the Previews Phase (2026)

	Sign	PKE	Symmetric	KeyGen	**FHE**	**ZKPoK**	Gadgets
NIST specified	**N1**	**N2**	**N3**	**N4**			
Special others	**S1**	**S2**	**S3**	**S4**	**S5**	**S6**	**S7**

Adamas S2	Amber S2	ark-pq S6	ATMACA N1	Axolotl N1 S7	BAM N1 N4	CGGMP N1 N4 S2 S7	Classic Schnorr N1 N4	Coord MPC S7	DKLs N1 N4 S7
DUOV S1 S4	FaFROST N1	FROST N1	Gargos N1	Haystack N1	Hermine S1 S4	Holocron N2	Kettle S1	Kryptallage S4 S5	KU N1
LaTSEC S1 S7	LaZer S6	LEAST S1 S4	Lemur S1	LoTRS S1	Menshen/(T)CL N1	Mithril N1 N4	MOZI S5 S7	MPC-MINIONS N1 N4	PANTHERIA S5
Pilaf S1	PiVer S7	PQarrots S1 S2 S4	Quorus N1 N4	RedETA N1 N4	Schmivitz S6 S7	SmallWood S6	SplitForge N1 N4 S2	Stoats N1 N4 S1 S4 S7	Symphony N3 S7
TALH N1 S1	TalonG/P-DualTS S1	TALUS N1 N4	Tanuki S1	TapTop/Robot S1	tBLS S1	TECLA N1	Teddy N1	THE-CLASH N1	Thimza S1
THQC N2	Threshcon N3	(Threshold-)CL S2	TORTL N4	Trout++ N1	TSitH S1	Tulva S5	Twig N1	Vinaigrette S1 S4	Zama S4 S5 S6

https://csrc.nist.gov/projects/threshold-cryptography/tcall-1

Coverage of Categories in the Threshold Call

NIST Signatures (N1)

Threshold EdDSA/Schnorr

- Classic Schnorr
- FaFROST
- FROST
- Gargos
- RedETA
- Axolotl
- Teddy

Threshold ECDSA

- BAM
- CGGMP
- KU
- RedETA
- SplitForge
- TECLA
- THE-CLASH
- Trout++
- Twig
- DKLs
- Menshen/(T)CL
- Stoats

Threshold PQ Signatures

- Haystack
- Mithril
- Quorus
- SplitForge
- TALUS
- ATMACA
- TALH

Symmetric (N3/S3)

- MPC-MINIONS
- Symphony
- Threshcon

Each name may appear in more than one category, since it may have proposed more than one crypto-system.

Non-NIST Signatures (S1)

Quantum-vulnerable (QV)

- tBLS
- Pilaf
- Stoats
- TapTop/Robot

Post-Quantum (PQ)

- Hermine
- LEAST
- Lemur
- LoTRS
- PQarrots
- Tanuki
- Vinaigrette
- DUOV
- Kettle
- LaTSEC
- TALH
- TalonG/P-DualTS
- Thimza
- TSitH

KeyGen (N4/S4)

Quantum-vulnerable (QV)

- BAM
- CGGMP
- Classic Schnorr
- RedETA
- SplitForge
- DKLs
- Stoats
- TORTL

Post-Quantum (PQ)

- Mithril
- Quorus
- SplitForge
- TALUS
- TORTL
- Hermine
- LEAST
- PQarrots
- Vinaigrette
- Zama
- DUOV
- Kryptallage

PKE/KEM (N2/S2)

- Amber
- CGGMP
- PQarrots
- SplitForge
- Adamas
- (Threshold-)CL
- Holocron
- THQC

FHE (S5)

- PANTHERIA
- Zama
- Kryptallage
- MOZI
- Tulva

ZKP (S6)

- LaZer
- Schmivitz
- SmallWood
- Zama
- ark-pq

Gadgets (S7)

- CGGMP
- Coord MPC
- MPC-MINIONS
- PiVer
- Schmivitz
- Symphony
- Axolotl
- DKLs
- LaTSEC
- MOZI
- Stoats

Note there is no category for PSI

Presentation Outline

1. NIST-Crypto Intro
2. **A Workshop on PEC: FHE, PSI, ZKP, ...**
3. Workshop Schedule and Logistics

FHE = Fully-Homomorphic Encryption.
NIST = National Institute of Standards and Technology.
PEC = Privacy-Enhancing Cryptography.
PSI = Private Set Intersection.
ZKP = Zero-Knowledge Proof.

The PEC Team Wishes You a PEC-Insightful Workshop



Luís Brandão



René Peralta



Angela Robinson

WPEC 2026: NIST **W**orkshop on **P**rivacy-**E**nhancing **C**ryptography 2026

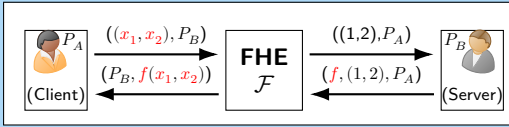
The workshop participants include speakers and registered participants

Workshop Mindset and Hopes

1. To foster a **learning and collaborative environment** about PEC
2. To hear examples of PEC **applications** (real and conceivable) for the real world
3. To gain **insights** useful for future **characterization** of PEC techniques

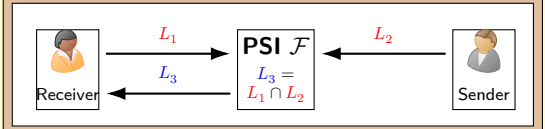
Topics Featured at WPEC 2026

Fully-Homomorphic Encryption (FHE)



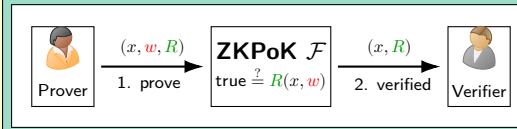
Compute over encrypted data

Private Set Intersection (PSI)



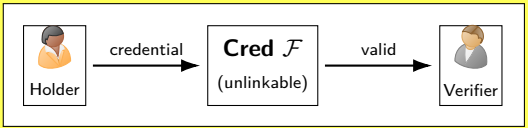
Find intersection, without disclosing the original sets

Zero-Knowledge Proof (ZKP)



Prove knowledge or correctness, revealing no secrets

Privacy-Preserving Digital Credentials



Prove authenticity, with unlinkability

Informal depiction of "Ideal Functionalities". Real implementations do not rely on $\mathcal{F}$.

FHE Webpage in the PEC Website



Fully-Homomorphic Encryption (FHE)

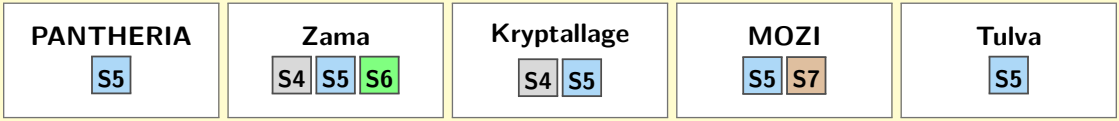
Fully-Homomorphic Encryption (FHE) allows computation of arbitrary functions over encrypted data, without knowing the secret key. This is a Privacy-Enhancing Cryptography (PEC) tool, alongside with Multi-Party Computation (MPC), Zero-Knowledge Proofs (ZKP), Private-Set Intersection (PSI), and others. The NIST PEC program is accompanying FHE developments and initiatives toward future useful standards.

+ expand all

- **FHE Applications**
- **FHE Info Sources**
- **FHE Conceptualization**
- **FHE Techniques**

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

FHE in the NIST Threshold Call (S5)



Also using FHE: Holocron. **Also using HE:** BAM, CGGMP, RedETA, (Threshold-)CL, Menshen/(T)CL, MOZI, SplitForge, TapTop/Robot, TECLA, THE-CLASH, Trout++. Example HE schemes: Paillier, CL, ElGamal.

Various considerations

- **Arithmetic:** integers, approximate reals, and switching between schemes.
- **Threshold designs:** specialized protocols and generic asynchronous compilers.
- **Security:** varying corruption thresholds; security with abort or robustness.
- **Building blocks:** key generation, bootstrapping, noise control, and ZKP.
- **Applications:** confidential smart contracts, private analytics, encrypted Ascon.

https://csrc.nist.gov/projects/threshold-cryptography/tcall-1

ZKP Webpage in the PEC Website



Zero-Knowledge Proof (ZKP)

Zero-Knowledge Proof (ZKP) is an important Privacy-Enhancing Cryptography (PEC) technique. It enables proving the truthfulness of a mathematical statement, without revealing information that may have been useful in finding said truthfulness and is not apparent in the statement.

+ expand all

ZKP in the NIST Threshold Call

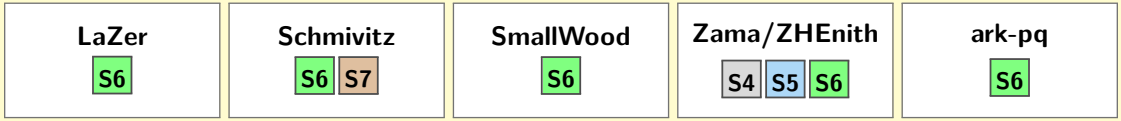
ZKP Applications

ZKP related talks hosted by NIST

Past NIST-PEC collaboration with ZKProof

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

ZKP in the NIST Threshold Call (S6)



Also using ZKP: Adamas, Axolotl, BAM, CGGMP, (Threshold-)CL, FaFROST (IA), Gargos, Holocron, LEAST, LoTRS, Menshen/(T)CL, MOZI, PiVer, SplitForge, TALUS, Teddy, TECLA, THE-CLASH, TORTL, Trout++, Twig. Optional use or in consideration: Kryptallage, PANTHERIA, tBLS, THQC, Tulva+.

Various considerations

- **Statements:** lattice relations, key/signature knowledge, ciphertext validity.
- **Techniques:** lattice-based and hash-based arguments; VOLE-in-the-Head.
- **Security:** post-quantum constructions, including options without trusted setup.
- **Integration:** proof libraries and gadgets for threshold and FHE protocols.
- **Tradeoffs:** proof size, prover time, and verifier time.

https://csrc.nist.gov/projects/threshold-cryptography/tcall-1

PSI Webpage in the PEC Website



Private Set Intersection (PSI) and other Private Set Operations (PSO)

Private Set Intersection (PSI) enables two (or more) parties, each with a private set, to identify which are the common elements across the sets, while not revealing information about the non-common elements. For example, two persons with privates lists of contacts can use PSI to determine which contacts they have in common. This is a very special case of Multiparty Computation (MPC), with well-known feasible solutions.

+expand all

- **PSI/PSO Applications**
- **PSI/PSO Info Sources**
- **PSI/PSO Conceptualization**
- **PSI/PSO Techniques**

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

What to Do About PSI / PSO?

PSI = Private Set Intersection
PSO = Private Set Operation

Done so far

- WPEC 2024 and 2026: Host the **First and Second PSI Days**
- STPPA series: Events #2 and #8 featured PSI

Idea: Should we do a "Call for PSO: models and implementation"?

- A paper specifying a system model, and a protocol (solution)
- Open-source implementation, and experimental evaluation report

Many nuances

- Post-quantum security, Two-party and Multi-party, ...
- Small sets, Large sets, Symmetric/Asymmetric sizes
- With committed inputs/outputs
- Approximate/Fuzzy/Circuits/**Pick-your-favorite-version** PSI/PSO

This is an idea in consideration (aligned with an earlier PEC Use-Case Suite idea)



Presentation Outline

1. NIST-Crypto Intro
2. A Workshop on PEC: FHE, PSI, ZKP, ...
3. **Workshop Schedule and Logistics**

FHE = Fully-Homomorphic Encryption.
NIST = National Institute of Standards and Technology.
PEC = Privacy-Enhancing Cryptography.
PSI = Private Set Intersection.
ZKP = Zero-Knowledge Proof.

Guidelines for Virtual Participation

- **Code of Conduct for NIST conferences:**
  https://www.nist.gov/pao/code-conduct-nist-conferences



- **Recording:** Audio-visual recording is allowed only by the hosts, for later posting on the webpage. Slide-decks (PDF) will also be posted.
- **Humans only**
  - **Text/chat:** Limited to topics related to the workshop and crypto.
  - **Q&A:** For each talk, we may relay a few comments / questions from the audience. Speakers can also follow up in the chat, after their talk.
- **Audio:** Oral question/comment implies consent for audio recording/posting.

WPEC 2026 Day 1 (Oct 26): FHE

Times are in EDT (UTC -4)

Session 1a — Morning

- 10:05–10:10: Welcoming Remarks by the NIST Computer Security Division
- **Talk 101**. 10:10–10:30: [W]PEC intro and PEC @ Threshold Call
- **Talk 1a1**. 10:30–11:25: Fully Homomorphic Encryption Benchmarking and Beyond

  Short break
- **Talk 1a2**. 11:35–12:00: (Fully-Homomorphically) Encrypted Neural Networks Without Overflows
- **Talk 1a3**. 12:00–12:25: Differentially Private Machine Learning under Fully Homomorphic Encryption

Session 1b — Afternoon

- **Talk 1b1**. 13:00–13:25: Mímir: A Stateless Private Search Engine
- **Talk 1b2**. 13:25–13:50: Privacy-Enhancing Cryptology in the Swedish Public Administration

(Edit note: displayed time slots were corrected after the presentation)

WPEC 2026 Day 2 (Oct 27): PSI

Times are in EDT (UTC -4)

Session 2a — Morning

- 10:00–10:05: Login and day intro
- **Talk 2a1**. 10:05–10:30: Post-Quantum Private Set Intersection for Small Sets
- **Talk 2a2**. 10:30–10:55: Private Set Intersection on Noisy Identifiers
- **Talk 2a3**. 10:55–11:20: Fuzzy Private Set Intersection for Real-World Datasets

Short break

- **Talk 2a4**. 11:35–12:00: Approximate Private Set Intersection
- **Talk 2a5**. 12:00–12:25: Outsourced PSI: Primitives, Properties, and Future Directions

Session 2b — Afternoon

- **Talk 2b1**. 13:30–13:55: Actively Secure Dishonest-Majority Table Join
- **Talk 2b2**. 13:55–14:20: Practical Two-Party Secret-Shared Joins for SQL Analytics

Short break

- **Talk 2b3**. 14:35–15:00: Communication-Efficient Private Join and Compute over Distributed Sets
- **Talk 2b4**. 15:00–15:25: Privacy-Preserving Proximity Testing from Geometric Fuzzy Matching

(Edit note: displayed time slots were corrected after the presentation)

WPEC 2026 Day 3 (Oct 28): ZKP and Credentials

Times are in EDT (UTC -4)

Session 3a — Morning

- 10:00–10:05: Login and day intro
- **Talk 3a1**. 10:05–10:55: Recent Advances in Zero-Knowledge Proofs and SNARKs

  Short break
- **Talk 3a2**. 11:10–11:35: Threshold Lattice-Based Zero-Knowledge Proofs
- **Talk 3a3**. 11:35–12:00: Doxxing-Proof Authentic Digital Media

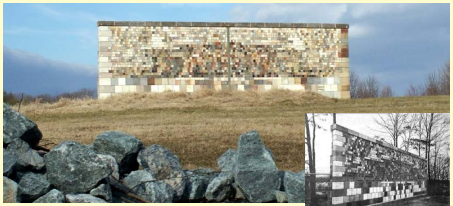
Session 3b — Afternoon

- **Talk 3b1**. 13:10–13:35: Private Sealed-bid Auctions at Scale
- **Talk 3b2**. 13:35–14:00: Private Delegation of Proofs on Non-Revocation for Anonymous Credentials
- **Talk 3b3**. 14:00–14:25: Rate-Limited Tokens (Anonymous Credentials)

(Edit note: displayed time slots were corrected after the presentation)

Thank You for Participating

NIST-PEC wishes an insightful workshop to everyone.



The NIST Stone Test Wall

Come place or study a new "block" in the "wall" of Crypto Reference Materials

"*Constructed [in **1948**] to study the **performance of stone subjected to weathering**. It contains 2352 individual samples of stone, of which 2032 are domestic stone from 47 [U.S.] states, and 320 are stones from 16 foreign countries.*"

Thank You for Your Attention!


WPEC Event


PEC Program


PEC Forum


MPTC Program


Threshold Call

WPEC 2026 Welcome and Introduction

Presented at WPEC 2026 | October 26, 2026

NIST **W**orkshop on **P**rivacy **E**nhancing **C**ryptography

luis.brandao@nist.gov

Index of Slides

1. WPEC 2026 Welcome and Introduction
2. Welcome to WPEC 2026

1. NIST-Crypto Intro

3. Presentation Outline
4. Activities in the "Crypto" Group
5. On the PEC and MPTC Programs
6. NIST Privacy-Enhancing Cryptography (PEC)
7. Multi-Party Threshold Cryptography (MPTC)
8. 60 Submissions in the Previews Phase (2026)
9. Coverage of Categories in the Threshold Call

2. A Workshop on PEC: FHE, PSI, ZKP, ...

10. Presentation Outline
11. Wishes of a PEC-insightful workshop
12. Workshop Mindset and Hopes
13. Topics Featured at WPEC 2026
14. FHE Webpage in the PEC Website
15. FHE in the NIST Threshold Call (S5)
16. ZKP Webpage in the PEC Website
17. ZKP in the NIST Threshold Call (S6)
18. PSI Webpage in the PEC Website
19. What to Do About PSI / PSO?

3. Workshop Schedule and Logistics

20. Presentation Outline
21. Guidelines for Virtual Participation
22. WPEC 2026 Day 1 (Oct 26): FHE
23. WPEC 2026 Day 2 (Oct 27): PSI
24. WPEC 2026 Day 3 (Oct 28): ZKP and Credentials
25. Thank You for Participating
26. Thank You for Your Attention!
27. Index of Slides
28. Production Notes

Slide-Production Notes

- **Source language:** LaTeX. **Compiler:** LuaLaTeX / LuaHBTeX 1.24.0.
- **TeX distribution (various packages):** TeX Live 2026.
- **Document class:** `ltx-talk` 0.4.7. **Fonts:** Latin Modern {Sans, Roman, Mono, Math}
- **PDF-file a11y/navigation:** bookmarks, tagging, acronym-hover tooltips, PDF/{A-4,UA-2}.
- **Externally obtained cliparts (free):** */<id> = `https://www.clker.com/clipart-<id>.html`


*/green-and-purple-dice


*/10264


*/11092


*/crypto-chip


*/2380


*/1775


*/3712


*/encryption


*/3855


*/paper-writing

(Edit note: Slide added after the presentation)