Intro to WPEC 2024 and the First PSI Day

Presented[*] at WPEC 2024:

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

2024-Sep-24th, from Gaithersburg (Maryland, USA)

https://csrc.nist.gov/events/2024/wpec2024

* Luís Brandão: At NIST as a Foreign Guest Researcher (non-employee), Contractor from Strativia.
Joint work with René Peralta and Angela Robinson.

Welcome to WPEC 2024

NIST **W**orkshop on **P**rivacy-**E**nhancing **C**ryptography 2024

We are looking forward to the sharing of insights about

Privacy-Enhancing Cryptography (PEC):

PSI, FHE, MPC, ZKP ...

during this 3-day virtual workshop!

PSI = **P**rivate-**S**et **I**ntersection. **FHE** = **F**ully-**H**omomorphic **E**ncryption.
MPC = Secure **M**ultiparty **C**omputation. **ZKP** = **Z**ero-**K**nowledge **P**roofs.

Welcome to WPEC 2024

NIST **W**orkshop on **P**rivacy-**E**nhancing **C**ryptography 2024

We are looking forward to the sharing of insights about

Privacy-Enhancing Cryptography (PEC):

PSI, FHE, MPC, ZKP ...

during this 3-day virtual workshop!

PSI = **P**rivate-**S**et **I**ntersection. **FHE** = **F**ully-**H**omomorphic **E**ncryption.
MPC = Secure **M**ulti**p**arty **C**omputation. **ZKP** = **Z**ero-**K**nowledge **P**roofs.

This presentation provides context and sets basic expectations about the workshop.

Outline

1. **On NIST Crypto Projects (including PEC)**

2. **The Workshop (WPEC 2024)**

NIST = **N**ational **I**nstitute of **S**tandards and **T**echnology.

PEC = **P**rivacy-**E**nhancing **C**ryptography.

WPEC = NIST **W**orkshop on **P**rivacy-**E**nhancing **C**ryptography.

Outline

1. **On NIST Crypto Projects (including PEC)**

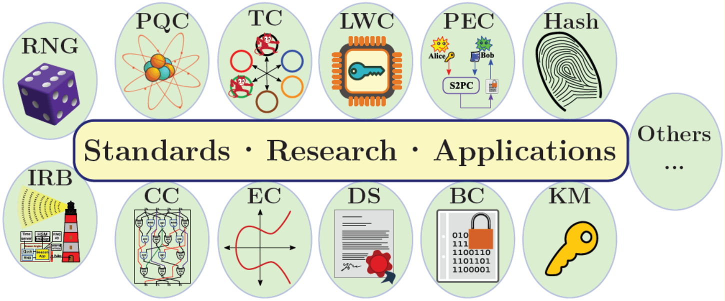
2. **The Workshop (WPEC 2024)**

NIST = **N**ational **I**nstitute of **S**tandards and **T**echnology.

PEC = **P**rivacy-**E**nhancing **C**ryptography.

WPEC = NIST **W**orkshop on **P**rivacy-**E**nhancing **C**ryptography.

Activities in the “Crypto” Group



- Public documentation: FIPS; Special Publications (SP 800); NIST Reports (IR).
- International cooperation: government, industry, academia, standardization bodies.

Legend: **BC** = **B**lock **C**iphers. **CC** = **C**ircuit **C**omplexity. **Crypto** = **Crypto**graphy. **DS** = **D**igital **S**ignatures. **EC** = **E**lliptic **C**urves. **FIPS** = **F**ederal **I**nformation **P**rocessing **S**tandards. **IR** = **I**nternal or **I**nteragency (denoting that the public NIST report was developed internally at NIST or in an interagency collaboration, respectively. **IRB** = **I**nteroperable **R**andomness **B**eacons. **KM** = **K**ey **M**anagement. **LWC** = **L**ight**w**eight **C**rypto. **PEC** = **P**rivacy-**E**nhancing **C**rypto. **PQC** = **P**ost-**Q**uantum **C**rypto. **RNG** = **R**andom-**N**umber **G**eneration. **SP 800** = **S**pecial **P**ublications in Computer Security. **TC** = [Multi-Party] **T**hreshold **C**rypto).

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

Intro: NIST has various Crypto Projects

- **PQC:** [standardization] "**post-quantum**" signatures and key-encapsulation
- **LWC:** [standardization] "**lightweight**" **A**uth. **E**nc. w/ **A**ssoc. **D**ata, and hashing

Legend: **AEAD** = **A**uth[enticated] **E**nc[ryption] w[ith] **A**ssoc[iated] **D**ata. **CTG** = **C**ryptographic **T**echnology **G**roup. **LWC** = **L**ightweight **C**ryptography. **MPTC** = **M**ulti-**P**arty **T**hreshold **C**ryptography. **NIST** = **N**ational **I**nstitute of **S**tandards and **T**echnology. **PEC** = **P**rivacy-**E**nhancing **C**ryptography. **PQC** = **P**ost-**Q**uantum **C**ryptography.

Intro: NIST has various Crypto Projects

- **PQC:** [standardization] "**post-quantum**" signatures and key-encapsulation
- **LWC:** [standardization] "**lightweight**" **A**uth. **E**nc. w/ **A**ssoc. **D**ata, and hashing
- **PEC:** [exploratory] "**privacy-enhancing**" (advanced) features/functionalities
- **MPTC:** [exploratory] "**multi-party threshold**" schemes for crypto primitives
- **...** (various other projects in the NIST "Crypto group" [CTG])

Legend: **AEAD** = **Auth**[enticated] **Enc**[ryption] **w**[ith] **Assoc**[iated] **D**ata. **CTG** = **C**ryptographic **T**echnology **G**roup. **LWC** = **L**ight**w**eight **C**ryptography. **MPTC** = **M**ulti-**P**arty **T**hreshold **C**ryptography. **NIST** = **N**ational **I**nstitute of **S**tandards and **T**echnology. **PEC** = **P**rivacy-**E**nhancing **C**ryptography. **PQC** = **P**ost-**Q**uantum **C**ryptography.

Intro: NIST has various Crypto Projects

- **PQC:** [standardization] "**post-quantum**" signatures and key-encapsulation
- **LWC:** [standardization] "**lightweight**" **A**uth. **E**nc. w/ **A**ssoc. **D**ata, and hashing
- **PEC:** [exploratory] "**privacy-enhancing**" (advanced) features/functionalities
- **MPTC:** [exploratory] "**multi-party threshold**" schemes for crypto primitives
- **...** (various other projects in the NIST "Crypto group" [CTG])

Throughout this workshop (WPEC 2024),
we are focused on the "Exploratory" approach

Legend: **AEAD** = **Auth**[enticated] **Enc**[ryption] **w**[ith] **Assoc**[iated] **D**ata. **CTG** = **C**ryptographic **T**echnology **G**roup. **LWC** = **L**ight**w**eight **C**ryptography. **MPTC** = **M**ulti-**P**arty **T**hreshold **C**ryptography. **NIST** = **N**ational **I**nstitute of **S**tandards and **T**echnology. **PEC** = **P**rivacy-**E**nhancing **C**ryptography. **PQC** = **P**ost-**Q**uantum **C**ryptography.

On the PEC and MPTC projects

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

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

On the PEC and MPTC projects

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

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

PEC: Privacy-Enhancing Cryptography

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

MPTC: Multi-Party Threshold Cryptography

- *Threshold Schemes* for diverse Cryptographic Primitives

On the PEC and MPTC projects

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

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

PEC: Privacy-Enhancing Cryptography

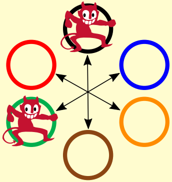
- Crypto (that can be) used to enhance privacy [emphasis on non-standardized tools].

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

MPTC: Multi-Party Threshold Cryptography

- *Threshold Schemes* for diverse Cryptographic Primitives



On the PEC and MPTC projects

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

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

PEC: Privacy-Enhancing Cryptography

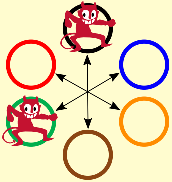
- Crypto (that can be) used to enhance privacy [emphasis on non-standardized tools].

PSI	**FHE**	**MPC**	**ZKP**	**GRS**	**FnE**	**PIR**	**StE**
Private **S**et **I**ntersection	**F**ully **H**omomorphic **E**ncryption	(**S**ecure) **M**ultiparty **C**omputation	**Z**ero- **K**nowledge **P**roofs	**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.

MPTC: Multi-Party Threshold Cryptography

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



Privacy-Enhancing Cryptography (PEC) [NIST Project]

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

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

Privacy-Enhancing Cryptography (PEC) [NIST Project]

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

Privacy-Enhancing Cryptography (PEC) [NIST Project]

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

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

- **Later (a goal for some time): A NIST Report about PEC.**
  Should emerge from diverse informed perspectives (including WPEC). Topics: relevant focuses (PEC tools); pre-vs-post quantum; apps; best practices; subsequent processes ...

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

Outline

1. **On NIST Crypto Projects (including PEC)**

2. **The Workshop (WPEC 2024)**

NIST = **N**ational **I**nstitute of **S**tandards and **T**echnology.

PEC = **P**rivacy-**E**nhancing **C**ryptography.

WPEC = NIST **W**orkshop on **P**rivacy-**E**nhancing **C**ryptography.

The PEC team wishes you a PEC-insightful workshop

Luís Brandão

René Peralta

Angela Robinson

WPEC 2024: NIST **W**orkshop on **P**rivacy-**E**nhancing **C**ryptography 2024

The workshop participants include 30 other speakers, and 750$^+$ registered participants

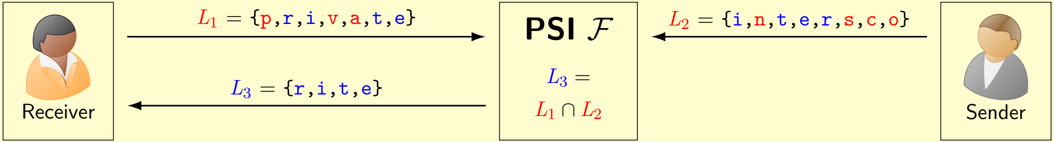
Workshop mindset / hopes

- To foster a **learning and collaborative environment** about PEC (perspectives from academia, industry, and gov, shared with a public audience)
- To hear examples of PEC **applications** (real and conceivable) for the real world
- To encourage **reflection**: PEC for public good; social responsibility on PEC use/dev. ...
- To gain **insights** useful for future **characterization** of PEC techniques
- To promote **matching** of PEC **capabilities** and real-world **challenges**
- To disseminate PEC **knowledge**, including to non-cryptographers.

PEC = Privacy-Enhancing Cryptography

WPEC 2024 sessions

- **1st Day (Sep 24th): The First PSI Day: PSI** (morning); **More PSI** (afternoon)



Receiver

$L_1 = \{\texttt{p},\texttt{r},\texttt{i},\texttt{v},\texttt{a},\texttt{t},\texttt{e}\}$

$L_3 = \{\texttt{r},\texttt{i},\texttt{t},\texttt{e}\}$

PSI $\mathcal{F}$

$L_3 = L_1 \cap L_2$

$L_2 = \{\texttt{i},\texttt{n},\texttt{t},\texttt{e},\texttt{r},\texttt{s},\texttt{c},\texttt{o}\}$

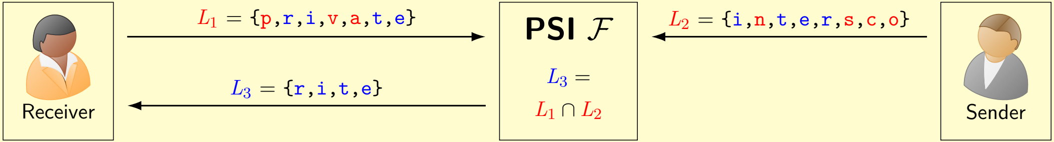
Sender

Two parties compute the intersection of their sets, without disclosing the non-intersecting elements.

WPEC 2024 sessions

- **1st Day (Sep 24th): The First PSI Day: PSI** (morning); **More PSI** (afternoon)

  For a dive into Private-Set Intersection, exploring its technicalities, readiness, feasibility, applicability, variants, and broader context. 10 talks and 1 slot for open comments.



Receiver

$L_1 = \{\texttt{p,r,i,v,a,t,e}\}$

$L_3 = \{\texttt{r,i,t,e}\}$

PSI $\mathcal{F}$

$L_3 = L_1 \cap L_2$

$L_2 = \{\texttt{i,n,t,e,r,s,c,o}\}$

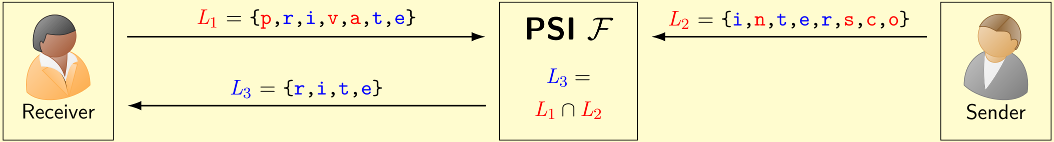
Sender

Two parties compute the intersection of their sets, without disclosing the non-intersecting elements.

WPEC 2024 sessions

- **1st Day (Sep 24th): The First PSI Day: PSI** (morning); **More PSI** (afternoon)

  For a dive into Private-Set Intersection, exploring its technicalities, readiness, feasibility, applicability, variants, and broader context. 10 talks and 1 slot for open comments.

  Receiver

  $L_1 = \{\mathtt{p},\mathtt{r},\mathtt{i},\mathtt{v},\mathtt{a},\mathtt{t},\mathtt{e}\}$

  $L_3 = \{\mathtt{r},\mathtt{i},\mathtt{t},\mathtt{e}\}$

  PSI $\mathcal{F}$

  $L_3 = L_1 \cap L_2$

  $L_2 = \{\mathtt{i},\mathtt{n},\mathtt{t},\mathtt{e},\mathtt{r},\mathtt{s},\mathtt{c},\mathtt{o}\}$

  Sender

  Two parties compute the intersection of their sets, without disclosing the non-intersecting elements.

- **2nd Day (Sep 25th): PEC in Gov** (morning); **FHE** (afternoon)
- **3rd Day (Sep 26th): MPC** (morning); **ZKP** (afternoon)

WPEC 2024 Brief Stats

Tally of Speakers/Talks (across 37 time slots):

- **24** speakers in **20** accepted talk proposals; **12** speakers in **10** invited talks
- PEC-team / moderated: **4** day intros and workshop closing / **3** slots of open comments;

WPEC 2024 Brief Stats

Tally of Speakers/Talks (across 37 time slots):

- **24** speakers in **20** accepted talk proposals; **12** speakers in **10** invited talks
- PEC-team / moderated: **4** day intros and workshop closing / **3** slots of open comments;

Time slots

- Most talks have **25-min slots**
- Three tutorials (overview talks) have **40-min slots**: FHE, MPC, ZKP
- Some **briefer slots** for intros and some comments
- **Small break** (5–10 min) inside each session; **long break** (≈1 hour) between sessions

WPEC 2024 Brief Stats

Tally of Speakers/Talks (across 37 time slots):

- **24** speakers in **20** accepted talk proposals; **12** speakers in **10** invited talks
- PEC-team / moderated: **4** day intros and workshop closing / **3** slots of open comments;

Time slots

- Most talks have **25-min slots**
- Three tutorials (overview talks) have **40-min slots**: FHE, MPC, ZKP
- Some **briefer slots** for intros and some comments
- **Small break** (5–10 min) inside each session; **long break** (≈1 hour) between sessions

Participants:

- ≈ 750 registered participants before the workshop (less will be live online)
- Stats will be published after the workshop (Countries, Acad/Gov/Industry/Personal, ...)

WPEC 2024 Schedule of Day 1 (The First PSI Day)

- 1a0: 09:20–09:30: ***Welcoming Remarks.*** Matt Scholl

Morning Session (1a): Private Set Intersection (PSI)

- 1a1: 09:30–09:45: ***Intro to WPEC and The PSI Day.*** Luís Brandão
- 1a2: 09:45–10:10: ***Spotlight on PSI for Small Sets.*** Mike Rosulek
- 1a3: 10:10–10:35: ***Actively Secure PSI in the Client-Server Setting.*** Yunqing Sun
- 1a4: 10:45–11:10: ***Circuit-PSI and Applications.*** Seongkwang Kim
- 1a5: 11:10–11:35: ***Private Collection Matching Protocols.*** Kasra Edalatnejad
- 1a6: 11:35–12:00: ***Vole-PSI: Fast PSI from the LPN Assumption.*** Peter Rindal

Afternoon Session (1b): More PSI

- 1b1: 13:00–13:25: ***Paths Toward PSI Standardization and a New Approximate PSI.*** Steve Lu
- 1b2: 13:25–13:50: ***Multiparty PSI and Beyond.*** Ni Trieu
- 1b3: 13:50–14:15: ***Structure-Aware PSI from Function Secret Sharing.*** Gayathri Garimella
- 1b4: 14:25–14:50: ***Unbalanced PSI: Apps, Constructions, and Combinations with PIR.*** Christian Weinert
- 1b5: 14:50–15:15: ***Asymmetric PSI and Its Leakage: ... the MIGP Protocol.*** Evgenios Kornaropoulos
- 1b6: 15:15–15:40: ***Closing of The PSI Day.*** PEC team and PSI speakers

Some abbreviations to fit titles in the slide.

Updates and details at https://csrc.nist.gov/events/2024/wpec2024

WPEC 2024 Schedule of Day 2

Morning Session (2a): Privacy-Enhancing Cryptography (PEC) in Government

- 2a1: 09:20–09:45: ***The Role of PEC in Recent and Upcoming U.S. National Strategies.*** Angela Robinson
- 2a2: 09:45–10:10: ***Measur. Demog. Disparities w/ Group-wise PSI: A Fed-Gov Case Study.*** Tomo Lazovich
- 2a3: 10:10–10:35: ***The US PETs Lab — Making Privacy Tech. Accessible In Gov.*** C. Mitchell and G. Howarth
- 2a4: 10:45–11:10: ***NSF PDaSP: [...] Use-case/App-Driven Translational Research in Privacy.*** James Joshi
- 2a5: 11:10–11:35: ***NIH Workshop on Homomorphic Encryption and PETs.*** S. Chen and J. Pollock
- 2a6: 11:35–12:00: ***Privacy-Preserving Data Sharing across Financial Institutions.*** K. Rohloff and A. Alexandru

Afternoon Session (2b): Fully-Homomorphic Encryption (FHE)

- 2b1: 13:00–13:40: ***Overview of Fully Homomorphic Encryption.*** Daniele Micciancio
- 2b2: 13:40–14:05: ***Practical and Affordable FPGA-based FHE.*** Rashmi Agrawal
- 2b3: 14:05–14:30: ***Practical Perf. of CKKS and Encrypted Training and Inference...*** D. Stehlé and J. Shin
- 2b4: 14:40–15:05: ***Decentralized FHE Computer and its Applications.*** Gurgen Arakelov
- 2b5: 15:05–15:30: ***Security Guidelines for Implementing FHE.*** Erin Hales
- 2b6: 15:30–15:40: ***Brief Comments on FHE.*** PEC team and FHE speakers

Some abbreviations to fit titles in the slide.

Updates/details at https://csrc.nist.gov/events/2024/wpec2024

WPEC 2024 Schedule of Day 3

Morning Session (3a): Secure Multi-Party Computation (MPC)

- 3a1: 09:20–09:30: ***NIST Threshold Call: Notes on the Upcoming Second Public Draft.*** Luís Brandão
- 3a2: 09:30–10:10: ***The Many Facets of MPC.*** Benny Pinkas
- 3a3: 10:10–10:35: ***Optimizing ML MPC from System & Theoretical Perspectives.*** Yongqin Wang
- 3a4: 10:45–11:10: ***Graphiti: Secure Graph Computation Made More Scalable.*** Bhavish Raj Gopal
- 3a5: 11:10–11:35: ***Signs of life for secure multi-party computation in protecting data.*** Dan Bogdanov
- 3a6: 11:35–12:00: ***Lightning comments about PEC.*** Attendees

Afternoon Session (3b): Zero-Knowledge Proofs (ZKP)

- 3b1: 13:00–13:40: ***ZKPs: Technical Challenges, Apps., and Real-world Deployment.*** T. Silde and A. Takahashi
- 3b2: 13:40–14:05: ***Verifiable Decryption from Learning with Rounding.*** Emil A.H. Olaisen
- 3b3: 14:05–14:30: ***On Anonymous Credentials.*** Anna Lysyanskaya
- 3b4: 14:40–15:05: ***Provably Forgotten Signatures: Adding Privacy to Digital Identity.*** Wayne Chang
- 3b5: 15:05–15:30: ***Making BBS Anonymous Credentials eIDAS 2.0 Compliant.*** A. Dumanois and J. Traoré
- 3b6: 15:30–15:40: ***WPEC 2024 Closing Remarks.*** PEC team

Some abbreviations to fit titles in the slide.

Updates and details at https://csrc.nist.gov/events/2024/wpec2024

Logistic notes for good workshop functioning

- **Code of Conduct:** Participation in WPEC 2024 requires abiding to the Code of Conduct for NIST conferences: https://www.nist.gov/pao/code-conduct-nist-conferences
- **Text/chat:** limited to only PEC/workshop-related matters.
- **Q&A:** For each talk, we may relay a few (but not all) comments / questions from the audience. Speakers can also follow up in the chat, after their talk.
- **Slide-decks and videos:** will be published on the workshop webpage
- **Mute your audio**, unless when giving a presentation, or in particular moments where your name is called out to speak up some question/comment (particular times).

Other 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

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

Thank you for your attention!

Intro to WPEC 2024 and the First PSI Day

Notes presented at NIST **W**orkshop on **P**rivacy **E**nhancing **C**ryptography 2024

September 24, 2024, from Gaithersburg (Maryland, USA) — luis.brandao@nist.gov

Useful links

- **WPEC 2024 Webpage:** https://csrc.nist.gov/events/2024/wpec2024
- **WPEC 2024 Contact:** wpec2024@nist.gov
- **PEC Website:** https://csrc.nist.gov/projects/pec
- **Subscribe to the PEC-Forum:** https://csrc.nist.gov/projects/pec/email-list
- **Subscribe to the MPTC-Forum:** https://csrc.nist.gov/projects/threshold-cryptography/email-list