# WPEC 2024 — Call for Abstracts (Talk Proposals)

**NIST Workshop on Privacy-Enhancing Cryptography 2024**

- **Workshop date and place:** **2024-Sep-26–28**, Virtual
- **Submission deadline:** **2024-Jul-22**, 23:59:59 Anywhere on Earth (UTC–12)
- **Main featured topic:** **P**rivate **S**et **I**ntersection (PSI)
- **Workshop webpage:** https://csrc.nist.gov/events/2024/wpec2024
- **Email address for submissions or questions:** wpec2024@nist.gov

The NIST **W**orkshop on **P**rivacy-**E**nhancing **C**ryptography (WPEC) 2024 will bring together multiple perspectives of PEC stakeholders. The 3-days virtual workshop is organized for sharing insights about PEC capabilities, use-cases, real-world deployment, initiatives, challenges and opportunities, and the related context of privacy & auditability. The program will aim for two main themes/scopes (specific and broad), aiming for about 50% time for each, as follows:

- **Private Set Intersection (PSI):** for a deep dive into this specific technique, exploring its technicalities, readiness, feasibility, applicability, variants, and broader context.
- **Other PEC techniques:** for a broader perspective of PEC (including FHE, MPC, and ZKP, and possible combinations with other privacy-enhancing technologies).

WPEC 2024 is organized within the scope of the NIST Privacy-Enhancing Cryptography (PEC) project. It will host technical and positioning talks, and panel discussions, in a learning and collaborative environment. The presentations will be recorded and made available online. The gathering of reference material is intended as informative for future characterization of PEC techniques, listing of potential use-cases, and the matching between PEC capabilities and real-world privacy & auditability challenges. Attendance is free but requires registration (details in the workshop webpage). Participation in any capacity (speaker, panelist, moderator, attendee) requires abiding to the Code of Conduct for NIST Conferences.

External proposals for talks are welcomed by email, using the provided PDF form and instructions. All submissions will be reviewed, and an acceptance or rejection decision will be sent by email. The review phase may include asking submitters to refine their proposals for better alignment with the thematic and logistical needs of the workshop. The overall selection, which will also include invited talks or panels, will prioritize the creation of a high-quality balanced program, aligned with the workshop goals.

## Welcomed topics for presentation proposals

The workshop welcomes highly-technical crypto material, and also less-technical inter-disciplinary perspectives about PEC development and integration. Some welcomed topics:

1. **Private Set Intersection** (and variants)
2. **Other PEC tools** (e.g., ZKP, FHE, MPC, specially-featured signatures/encryption)
3. **Pairing-based PEC** (distinctive features of crypto based on bilinear maps)
4. **Post-quantum PEC** (examples, and differences from pre-quantum solutions)
5. **Systematization of PEC knowledge** (techniques, applications, and related context)
6. **PEC integration with various technologies** (e.g., artificial intelligence, blockchain, digital identity, federated learning, quantum information, navigation, networking)
7. **PEC for combined privacy and auditability** (challenges and opportunities)
8. **PEC need and adoptability** (e.g., fulfilled, urgent, emerging, envisioned)
9. **Specific PEC perspectives** (from Academia, Industry, Government, and Community)
10. **PEC specification, deployment, and standardization** (challenges & achievements)
11. **Other PEC initiatives** (e.g., of characterization, development, education)

## Suggested references with additional context:

- NIST Privacy-Enhancing Cryptography (PEC) project: https://csrc.nist.gov/projects/pec
- National Strategy to Advance Privacy-Preserving Data Sharing and Analytics: https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Strategy-to-Advance-Privacy-Preserving-Data-Sharing-and-Analytics.pdf

**Supporting references:** Submitted abstracts should include references to publicly available reference materials, which can depend on the submission source/scope. For example:

- **Academia:** supported on peer-reviewed publications on cryptography and privacy.
- **Industry:** referencing publicly documented use-cases, deployments or initiatives.
- **Government:** relating to public agencies and governance at federal/state/local levels.
- **Community:** based on researched challenges and applicability of PEC for individuals, community members, local groups, and non-governmental organizations.