WPEC 2026 — Call for Talk Proposals

NIST Workshop on Privacy-Enhancing Cryptography 2026

- **Workshop date and place:** **2026-Oct-26–29**, Virtual
- **Submission deadline:** **2026-Sep-14**, Anywhere on Earth (UTC−12)
- **Workshop webpage:** https://csrc.nist.gov/events/2026/wpec2026
- **Email address for talk proposals (submissions):** wpec2026-submit@list.nist.gov
- **Email address for inquiries or comments:** wpec2026@nist.gov

Scope. The NIST **W**orkshop on **P**rivacy-**E**nhancing **C**ryptography (WPEC) 2026 will bring together multiple perspectives of PEC stakeholders, for sharing insights about PEC capabilities, use-cases, real-world deployment, initiatives, challenges and opportunities, and the related context of privacy & auditability. The workshop will aim to:

- Host the 2nd Private Set Intersection (PSI) Day
- Feature techniques for and applications of encrypted search.
- Showcase the broader PEC perspective of techniques, applications and initiatives.

Organization. WPEC 2026 is organized within the scope of the NIST Privacy-Enhancing Cryptography (PEC) program. This 2nd edition of WPEC is organized as a 4-day virtual workshop that will host technical and positioning talks, and conversations, 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.

Talk proposals: Submit by email, using the PDF form and instructions published in the workshop webpage. After a period of review, an acceptance or rejection decision will be sent by email (aimed for 2026-Sep-28). 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 may also include invited talks or panels, will prioritize the creation of a high-quality balanced program, aligned with the workshop goals.

Participation. Attendance is free but requires online registration (details in the workshop webpage). Participation in any capacity (speaker, panelist, moderator, attendee) requires abiding by the Code of Conduct for NIST Conferences. Registration and attendance are limited to humans. Automated bots, AI agents, or similar tools may not participate in the workshop. The organizers reserve the right to remove any participant/tool believed to violate this policy.

Topics for presentation proposals. The workshop welcomes technical PEC material, and also less-technical inter-disciplinary perspectives about PEC development and integration. In any case, the presentations should be tailored to a technical audience not necessarily expert in the presentation topic. There is preference for presentations with a context of privacy-preserving/enhancing applications. Example welcome topics:

- **Technical PEC tools:**
  1. **Private Set Intersection** (and variants)
  2. **Encrypted Search** (tools and applications)
  3. **Other PEC tools** (e.g., ZKP, FHE, MPC, PIR, privacy-oriented signatures)
  4. **Special encryption: IB, AB, functional, witness, etc.** (privacy-related apps)
  5. **Post-quantum PEC** (alternatives to quantum-vulnerable PEC solutions)
- **Broader perspectives:**
  1. **Systematization of PEC knowledge** (techniques, applications, and context)
  2. **PEC integration with various technologies** (e.g., artificial intelligence, blockchain, digital identity, federated learning, quantum information, navigation, networking)
  3. **PEC for combined privacy and auditability** (challenges and opportunities)
  4. **PEC need and adoptability** (e.g., fulfilled, urgent, emerging, envisioned)
  5. **Specific PEC perspectives** (from Academia, Industry, Government, and Community)
  6. **PEC specification, deployment, and standardization** (challenges & achievements)
  7. **Other PEC initiatives** (e.g., of characterization, development, education)

Supporting references. Talk proposals should include references to publicly available material, which can depend on the source and scope of the submission. For example:

- **Academia:** supported by 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 research challenges and applicability of PEC for individuals, community members, local groups, and organizations.