FORTYTWO LABS
BRINGING IDEAS TO LIFE

MINISTRY OF
ELECTRONICS AND
INFORMATION TECHNOLOGY

www.isea.gov.in

HACKATHON 2026

Organized by

Indian Statistical Institute Kolkata in collaboration with Fortytwo labs

ZKP Based Multi System Attribute Verification

Event Structure:

Phase 1: Pre-Hackathon Training (23-27 February 2026)

Phase 2: Finals at ISI Kolkata (09-10 March, 2026)

Team Size: 2-4 members per team

Registration Here

Prize Pool:
Rs. 2,00,000/-

Deadlines:
15 February 2026

Guidelines for Hackathon 2026

Organized by

Indian Statistical Institute, Kolkata

In Collaboration with

Fortytwo Labs

INFORMATION SECURITY EDUCATION AND AWARENESS (ISEA) PHASE – III

Cryptography

Hackathon Details:

1. **Title:** ZKP Based Multi System Attribute Verification.
2. **Problem Statement:** Design and build a zero-knowledge proof (ZKP) system that allows a user to prove selected attributes (or predicates over attributes) to multiple independent verifiers across systems without revealing the underlying attributes and while preventing linkage across verifications.
3. **Delivery mechanism:**
   a) Design Document- protocol description, threat model, security/privacy claims.
   b) Working prototype (issuer, holder, verifier(s)) with automated demo script.
   c) Benchmarks & evaluation report (CPU, memory, network, proof sizes).
   d) Short video (3–5 min) demonstrating user flow and privacy guarantees.

Objectives (Examples teams can pick):

1. Design a protocol that supports selective disclosure of attributes and non-linkability across verifiers.
2. Implement a prototype ZKP construction (e.g., zk-SNARK or zk-STARK, or signature-based proofs like CL/Idemix or BBS+ with ZK) integrated with a simple credential issuer and two independent verifiers.
3. Measure prover time, verifier time, proof size, and end-to-end latency (mobile/desktop).
4. Evaluate privacy: show unlinkability under realistic threat models (honest-but-curious verifiers, partial collusion).
5. (Optional) Add revocation support while preserving unlinkability.

Potential Extensions:

1. Add decentralized identity (DID) / verifiable credential storage (e.g., W3C VC, JSON-LD).
2. Add selective revocation with accumulator-based or short-lived credentials.
3. Provide a formal proof sketch of unlinkability or simulation-based privacy.

Structure of Hackathon:

1. **Duration:** 24th January to 10th March, 2026.
2. **Team Structure:** The total participation in each team should be **2 to 4 persons** (Only the **team leader should register** through the online form and enter the names and details of the **other members** in that form).
3. **Prize Pool:** The winner of this event will receive prize money of **Rs. 200,000/-**.
4. **Phases:**
   a) **Phase I**: **Pre-Hackathon Training (23–25 February 2026)**: Introductory sessions on cryptographic foundations, ZKP concepts, tools, and implementation basics.
   b) **Phase II**: **Shortlisting (26–27 February 2026)**: Candidate selection from online applicant pools based on a preliminary and partially specified problem statement.
   c) **Phase III**: **Finalization (9–10 March 2026)**: Design, implementation, testing, and benchmarking of proposed solutions with continuous mentor support. Capture-the-Flag or challenge-based assessment aligned with security, privacy, and performance goals. Final presentations, expert evaluation, certification, and award distribution.

Literature and Resources:

1. Survey: A Survey on the Applications of Zero-Knowledge Proofs.
2. Attribute / credential literature: Anonymous and Linkable Scoped Credentials (2022) and general attribute-based credential surveys.
3. Example ZKP + credential systems (academic implementations & recent blockchain projects): see ZKP surveys for practical libraries.

Attack / Ethical Considerations:

Be explicit about threat models: which parties may collude, network adversary, and side channels from the client device. Do not attempt deanonymization or harvesting personal data; use synthetic or consented test attributes.

Contact Email: iseakolkata@gmail.com