Secure Multi-Party Computation of a Random Permutation

A Cryptographic Protocol

Step 1: Cooperatively generate a random permutation
Step 2: Reveal elements to chosen participants

---

**Featuring**

- Public-key cryptography
- Homomorphic encryption
- Zero-knowledge proofs
- Shamir's threshold scheme

**Applications**

- Secure on-line poker
- Drawing names from a hat

---

Ján Jerguš  Supervisor: Jozef Jirásek