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

NO TRUSTED SERVER REQUIRED

GUARANTEED CHEATER DETECTION

IMPLEMENTATION INCLUDED

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