Homomorphic UC Commitments in Minicrypt

Ivan Damgård, Bernardo David, Irene Giacomelli, Jesper Buus Nielsen
Aarhus University
Basic Structure

Setup: Cryptomania

Commit And Reveal:
Minicrypt
Related Works

• Up to this year:
  – Most efficient UC commitments required exponentiations in large groups [Lin11,BCPV13].

• Independent work in Eurocrypt 2014 [GIKW14]:
  – Optimal Rate.
  – Public key operations restricted to setup phase.
  – Relies specifically on [FY92] for encoding messages.
Our Work

• Many commitments from a fixed number of seed OTs of fixed length.

• Non-interactive commit and reveal phases requiring only a PRG and field arithmetic.

• Additive and multiplicative homomorphism.

• Constant rate even with constant size fields.
Applications

• Efficient Non-interactive UC zero-knowledge proof of knowledge for any NP relations. [DIK10]

Circuit C checking relation: \( C(x) = 1 \) if relation holds

Verify relations between commitments

Check opening of commitment to output R
Our New Tools

- General Packed Verifiable Secret Sharing:
  - Combined ideas from [FY92] and [BGW88].
  - Generalization of [CDM00] constructed from any LSSS.
  - Allows computation of linear functions and multiplications of shared secrets as in [BBDK00].
Basic Construction

• **Setup:**
  - Send t-out-of-n seeds for a PRG (e.g. [VZ12]) through OT as in [FJNNO13].
  - Run VSS in the head as in [IKOS09] with random strings as input and send the views one-time padded with the PRG outputs.

• **Commit:** Send the message one-time padded with a secret shared random string.

• **Reveal:** Send the shares for the random pad used for the commitment.
Thanks!