A Framework for Semi-Homomorphic Public Key Cryptosystems with Applications to MPC

Rikke Bendlin, Ivan Damgård,
Claudio Orlandi and Sarah Zakarias

Aarhus University

Results

- Definition of Semi-Homomorphic cryptosystems.
  - 7 examples including Paillier, Regev LWE, Subset Sum.
- Practical MPC protocol for computation mod p.
  - Based on any semi-homomorphic cryptosystem.
  - Secure against any number of actively corrupted parties.
- Offline phase: Efficiency similar to semi-honest solution.
- Online phase: No crypto, only linear computations mod p.

Semi-Homomorphic Cryptosystem

- Encryption: $c=E(x,r)$, integer x and randomness r.
- Decryption: If $|x|$ is small enough, $D(c)$ returns $x \bmod p$.
- Additively homomorphic: $E(x,r)+E(y,s) = E(x+y,r+s)$.
- Semantically secure.

MPC

Offline phase:

- ZK proofs for plaintext knowledge.
- Uses amortization techniques to get constant factor overhead [Cramer/Damgård '09].
- Produces “multiplication triples”, Beaver's Circuit randomization.

MPC - cont.

Online phase:

- Represents secret values using additive sharing and information theoretic MACs.
- Multiplication by using triples from offline phase.

Previous Practical Protocols for Dishonest Majority

- Boolean circuits :Yao Garbling, [Pinkas et al. '09], [Lindell/Pinkas '09].
- Arithmetic circuits: [Damgård/Orlandi tomorrow].

  Similar complexity in offline phase, much faster in online phase.

  DO construction assumes DL and passively secure multiplication protocol (in practical version Paillier).

  This work only needs Paillier, in general security of underlying cryptosystem.