Multiparty Secure Computation over Multivariate Polynomials

Dana Dachman-Soled, Tal Malkin,
Mariana Raykova, Moti Yung

Results

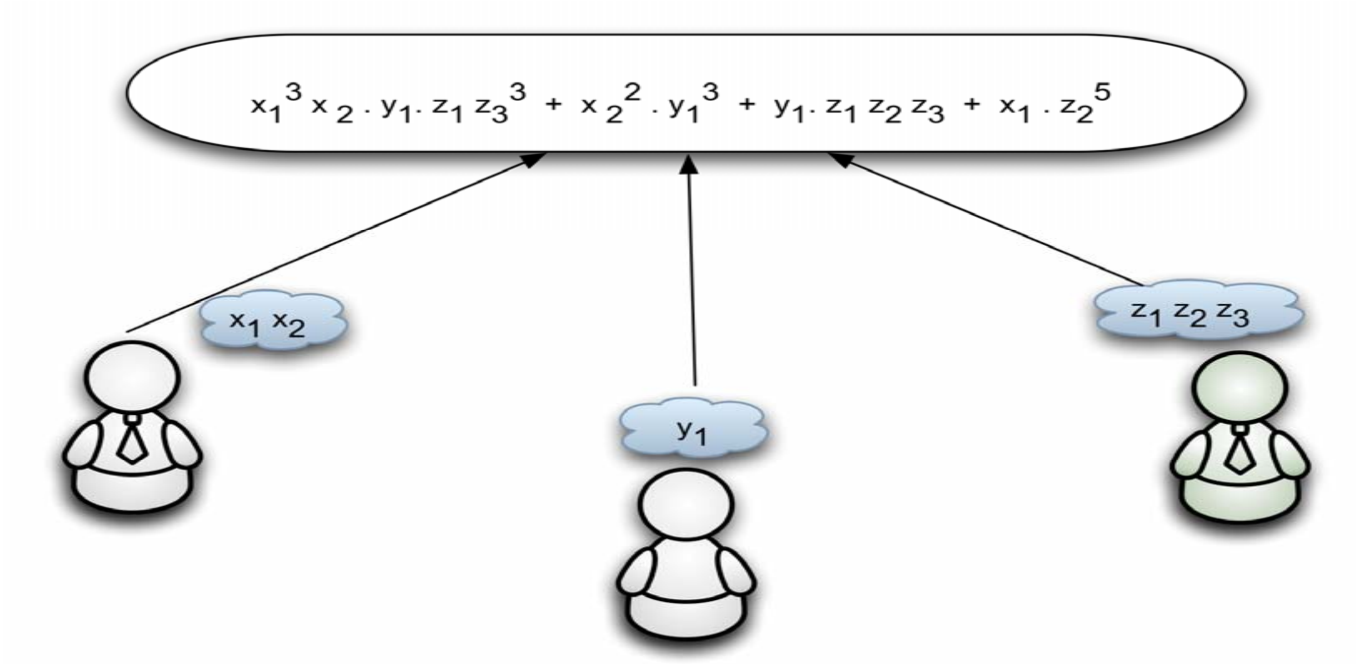
- Multiparty computation protocol for functionalities that can be represented as multivariate polynomials
- Security against malicious majority
- Black box techniques; Proofs in the standard model
- *Hardness Assumption*: Decisional Composite Residuosity (threshold Paillier encryption)
- High efficiency of communication

Applications

- Multi Party “Set Intersection” (efficient without ZK proofs
- Multi Party “Oblivious Polynomial Evaluation”
- Linear Algebra Operations, Statistics, etc. (these are efficiently represented as multi variate polynomial).

Model

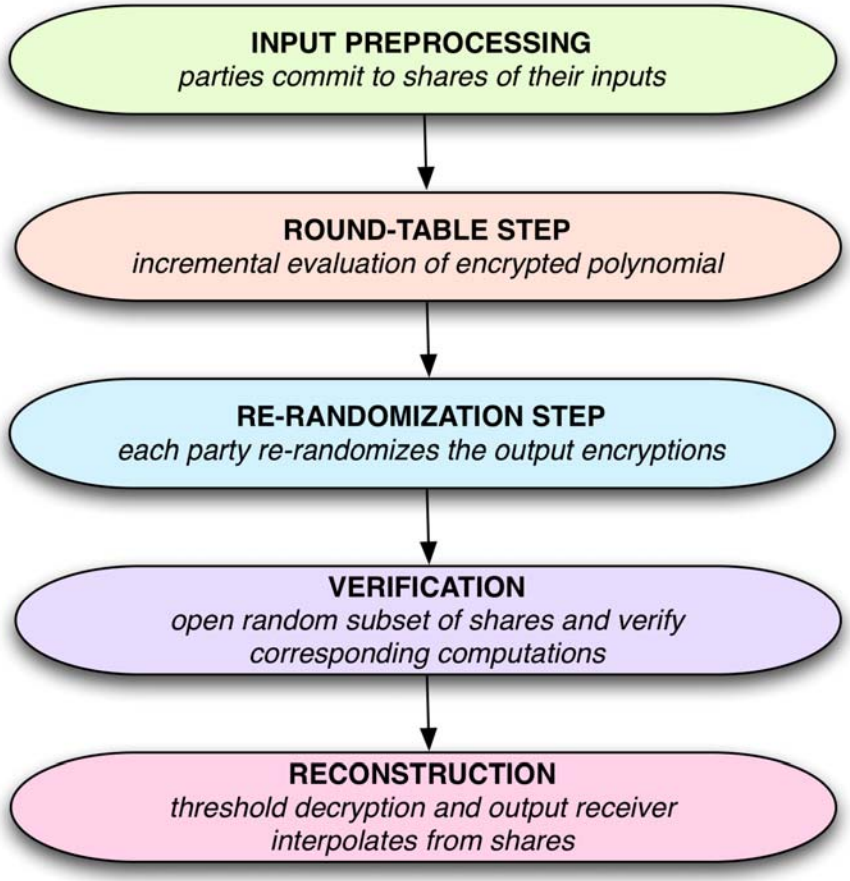
- Each party contributes a subset of the variables of the multivariate polynomial


$x_1^3 x_2 . y_1 . z_1 z_3^3 + x_2^2 . y_1^3 + y_1 . z_1 z_2 z_3 + x_1 . z_2^5$
$x_1 x_2$
y_1
$z_1 z_2 z_3$

Techniques

- Polynomial code commutativity between polynomial evaluation and Reed-Solomon (Shamir SS) codes
- Incremental encrypted polynomial evaluation - round-table evaluation of polynomial
- Polynomial interpolation over encrypted data- vector homomorphic property on both plaintext and randomness
- Zero knowledge proofs for languages of encrypted shares – homomorphic encryption + cut-and-choose technique

Protocol



INPUT PREPROCESSING
parties commit to shares of their inputs

ROUND-TABLE STEP
incremental evaluation of encrypted polynomial

RE-RANDOMIZATION STEP
each party re-randomizes the output encryptions

VERIFICATION
open random subset of shares and verify corresponding computations

RECONSTRUCTION
threshold decryption and output receiver interpolates from shares

Application – Multiparty Set Intersection

- Each party except output receiver represents its set X_i as a polynomial $P_{xi}(x)$ (set elements are poly zeros)
- For each set element of the output receiver the parties evaluate

$$r * \Sigma_i P_{xi}(x) + x$$

- Inputs:
  - each party expect output receiver - *coefficients for its polynomial and input for randomness r*
  - output receiver – *one of its inputs for each execution and input for randomness r*
- Optimizations applied on main protocol

Summary & Complexity

- Two types of communication complexity
  - Broadcast communication – input commitments and verification; *may be much smaller than the polynomial representation*
  - Round-table communication (*between two parties only*) – all intermediate messages (we only employ a constant number of round-table rounds)
  - This is very efficient. This is a new model and way to employ many of interesting multiparty problems securely.