Privacy-Preserving Multi-Party Reconciliation Secure in the Malicious Model

8th ACM International Workshop on Data Privacy Management 2013

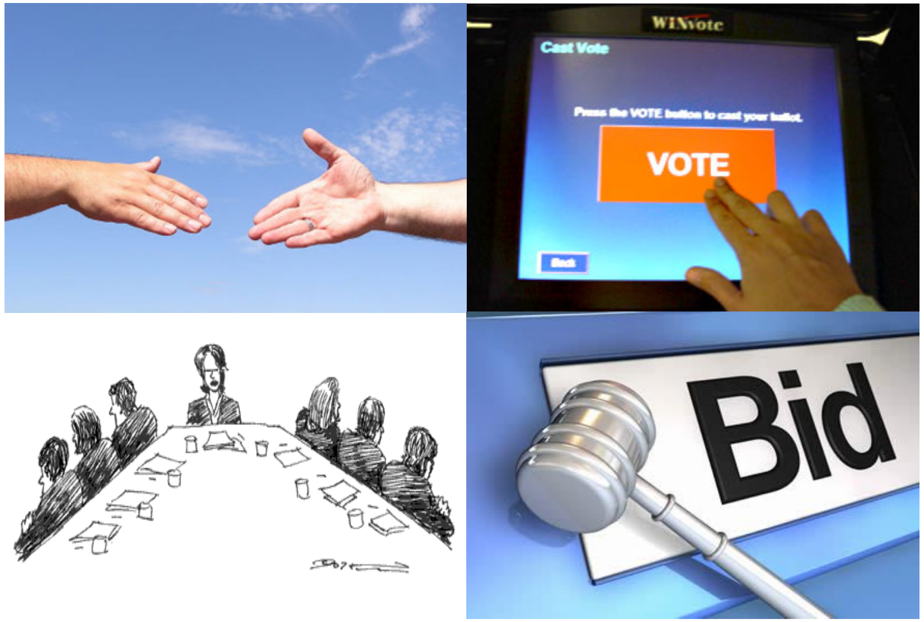
Georg Neugebauer[1], Lucas Brutschy[1], Ulrike Meyer[1] and Susanne Wetzel[2]

UMIC LuFG IT-Security, RWTH Aachen University[1]
Department of Computer Science, Stevens Institute of Technology[2]

12.09.2013

Overview

Fair and Privacy-Preserving Reconciliation



Borda Count Voting

Candidate	Points
Peter	3
Michael	2
Alice	1

Candidate	Points
Michael	3
Peter	2
Alice	1

Candidate	Points
Michael	3
Alice	2
Peter	1

Result	Points
Michael	8

Fair and Privacy-Preserving Reconciliation on Ordered Sets

Definition (MPROS)

- Secure multi-party computation protocol between n parties
- *Input:*
  - Ordered sets $S_1, \ldots, S_n$ of size k drawn from a common domain D
  - Ranking $rank_S(x_i) = k - i + 1$, $x_i \in S$
- *Fairness:*

$$f^{MR}(x) = \min\{\mathrm{rank}_{S_1}(x), \ldots, \mathrm{rank}_{S_n}(x)\}$$

$$f^{SR}(x) = \mathrm{rank}_{S_1}(x) + \ldots + \mathrm{rank}_{S_n}(x)$$

- *Output:*

$$X = \underset{x \in (S_1 \cap \ldots \cap S_n)}{\arg\max}\, f(x) \qquad t = \max_{x \in (S_1 \cap \ldots \cap S_n)} f(x)$$

Candidate	Points
Peter	3
Michael	2
Alice	1

MR

Candidate	Points
Michael	2
Peter	1
Alice	1

SR

Candidate	Points
Michael	8
Peter	6
Alice	4

MR

Result	Points
Michael	2

SR

Result	Points
Michael	8

Preliminaries

Basics

- Additively homomorphic cryptosystem (Threshold Paillier cryptosystem)
  - Compute the encrypted sum of two plaintexts given only the related ciphertexts
- Privacy-preserving multiset operations (Kissner et al.[1])
  - Represent multiset $S_i = \{s_{i,1}, \ldots, s_{i,k}\}$ as polynomial $f_i(x) = \prod_{j=1}^{k} \left(x - s_{i,j}\right)$
- Computation on encrypted polynomials, semi-honest adversary model

[1] L. Kissner and D. X. Song: **Privacy-Preserving Set Operations**, In *CRYPTO*, LNCS, 2005

Preliminaries

Basics

- Additively homomorphic cryptosystem (Threshold Paillier cryptosystem)
  - Compute the encrypted sum of two plaintexts given only the related ciphertexts
- Privacy-preserving multiset operations (Kissner et al.[1])
  - Represent multiset $S_i = \{s_{i,1}, \ldots, s_{i,k}\}$ as polynomial $f_i(x) = \prod_{j=1}^{k} \left(x - s_{i,j}\right)$
- Computation on encrypted polynomials, semi-honest adversary model

Privacy-Preserving Set Operations

- Let ϕ, γ denote enc. polys, g an unenc. poly, and s, r, F_i random unenc. polys
  - Multiset intersection: $\phi \times_h s +_h \gamma \times_h r$ — $\{a, b^2, c\} \cap \{b, c^3\} = \{b, c\}$
  - Multiset union: $\phi \times_h g$ — $\{a, b^2, c\} \cup \{b, c^3\} = \{a, b^3, c^4\}$
  - Multiset reduction: $\tilde{\sum}_{i=0}^{t} \gamma^{(i)} \times_h F_i \times_h r_i$ — $Rd_1(\{a, b^2, c\}) = \{b\}$

[1] L. Kissner and D. X. Song: **Privacy-Preserving Set Operations**, In *CRYPTO*, LNCS, 2005

MPROS Secure in the Semi-Honest Model

Reminder Definition

Fairness:

$$f^{MR}(x) = \min\left\{\mathrm{rank}_{S_1}(x), \dots, \mathrm{rank}_{S_n}(x)\right\} \qquad f^{SR}(x) = \mathrm{rank}_{S_1}(x) + \dots + \mathrm{rank}_{S_n}(x)$$

Output:

$$X = \underset{x \in (S_1 \cap \dots \cap S_n)}{\arg\max} f(x) \qquad t = \max_{x \in (S_1 \cap \dots \cap S_n)} f(x)$$

MPROS Functions[2]

- Minimum of ranks: $\bigcap_{i=1}^{n} \{s_{i1}, \dots, s_{il}\}$
  with round $1 \leq l \leq k$ and $S_i = \{s_{i1} > \dots > s_{ik}\}$
- Sum of ranks: $Rd_t\left(renc(S_1) \cup \dots \cup renc(S_n)\right) \cap \left(S_1 \cap \dots \cap S_n\right)$
  with $renc(S_i) = \left\{s^{rank_i(s)} | s \in S_i\right\}$ and $t = nk - 1, \dots, n - 1$

[2] G. Neugebauer, L. Brutschy, U. Meyer, S. Wetzel: **Design and Implementation of Privacy-Preserving Reconciliation Protocols**, 6th ACM International Workshop on Privacy and Anonymity in the Information Society, EDBT/ICDT 2013, Genoa, Italy, March 2013

How to Achieve Security in the Malicious Model

Security Model

- Semi-honest adversary: insider attacker that tries to infer as much (secret) information as possible, but follows the prescribed actions of the protocol
- Malicious adversary: insider attacker that can almost arbitrarily deviate from the protocol except refusal to participate, manipulation of its own input, and protocol abortion

Observations

- MPROS is based on privacy-preserving intersections, unions, and reductions of multisets that encode the ordered input sets of the n parties
- Privacy-preserving multiset operations are based on homomorphic additions and scalar multiplications

→ Use **ZKPK's** to prove correctness of computations involving **encryptions** of

- secret input sets
- chosen random polynomials
- intermediate computation results

Verifiable Set Operations

Zero-Knowledge Proofs of Knowledge

- We use ZKPK's based on a threshold version of the Paillier cryptosystem
- Previous work
  - Interactive Proof of Plaintext Knowledge
  - Interactive Proof of Correct Multiplication
  - Proof of a Subset Relation Using Verifiable Shuffles
  - Proof of Correct Threshold Decryption
- Novel work
  - Non-Interactive Proof of Plaintext Knowledge and Correct Multiplication
  - Proof of a Homomorphic Linear Equation

Polynomial Operations

- Proof of Correct Multiplication of Polynomials
- Proof of Arbitrary Linear Expressions of Polynomials

→ Enables verifiable set intersection, union, and reduction operations

Protocol Comparison (MR) - Semi-honest model (SHM) vs Malicious model (MM)

Same setting: $P_1, \ldots, P_n$, ordered sets $(S_i, <_i)$ chosen from a common domain D, pre-distributed keys, secure channels

1. Input Encryption

SHM Each party P_i encrypts and broadcasts its highest ranked input $\phi_{i,1} = E(x - d_{i,1})$

MM Each party P_i

1. Computes an encrypted shuffle $(\delta_{i,1}, \ldots, \delta_{i,k}, \ldots)$ of the domain D
2. Broadcasts the shuffle and a correctness proof $\Pi_{SHUFFLE,i}$

Each party P_i for $j \in \{1, .., n\}$

1. If $j \neq i$, verifies $\Pi_{SHUFFLE,j}$
2. Chooses random polynomial $r_{i,j,1}$ of degree 1
3. Computes and commits to $\rho_{i,j,1} = E_1(r_{i,j,1})$

Protocol Comparison (MR) - Semi-honest model (SHM) vs Malicious model (MM)

2. Set Intersection (Initially $t = k - 1$)

SHM Each party P_i

1. Chooses random polynomials $r_{i,j}$ of degree $k - t$
2. Calculates and broadcasts $\gamma_i = \tilde{\sum}_{j=0}^{n} (\phi_{j,k-t} \times_h r_{i,j})$
3. Calculates $\pi = \tilde{\sum}_{l=1}^{n} \gamma_i$

MM Each party P_i

1. Opens the commitment to $\rho_{i,j,k-t}$
2. Computes and broadcasts $\gamma_i = \left[\tilde{\sum}_{j=0}^{n} (\phi_{j,k-t} *_h r_{i,j,k-t})\right]_r$
3. Broadcasts a proof $\Pi_{\text{INTERSECT},i}$ that γ_i is correctly computed

Each party P_i

1. For $j \in \{1, .., n\} \setminus \{i\}$ verifies $\Pi_{\text{INTERSECT},j}$
2. Calculates $\pi = \sum_{i=1}^{n} \gamma_i$

Protocol Comparison (MR) - Semi-honest model (SHM) vs Malicious model (MM)

2. Set Intersection (Initially $t = k - 1$)

SHM Each party P_i

1. Chooses random polynomials $r_{i,j}$ of degree $k - t$
2. Calculates and broadcasts $\gamma_i = \tilde{\sum}_{j=0}^{n} (\phi_{j,k-t} \times_h r_{i,j})$
3. Calculates $\pi = \tilde{\sum}_{l=1}^{n} \gamma_i$

MM Each party P_i

1. Opens the commitment to $\rho_{i,j,k-t}$
2. Computes and broadcasts $\gamma_i = \left[\tilde{\sum}_{j=0}^{n} (\phi_{j,k-t} *_h r_{i,j,k-t})\right]_r$
3. Broadcasts a proof $\Pi_{\text{INTERSECT},i}$ that γ_i is correctly computed

Each party P_i

1. For $j \in \{1, .., n\} \setminus \{i\}$ verifies $\Pi_{\text{INTERSECT},j}$
2. Calculates $\pi = \sum_{i=1}^{n} \gamma_i$

3. Decryption

SHM All parties together perform a threshold decryption of π

MM All parties perform a malicious model threshold decryption of π

Protocol Analysis

Correctness

- We compute the same function as the semi-honest variants
- Assuming that the ZKPK's are difficult to forge, each party is forced to perform the correct computations

→ Correctness results in the semi-honest model also apply to our malicious model variant

Security / Privacy

- All parties only learn the optimal solution and the minimum of ranks value
- Security proof based on the simulation paradigm given in our paper

Results in Theory

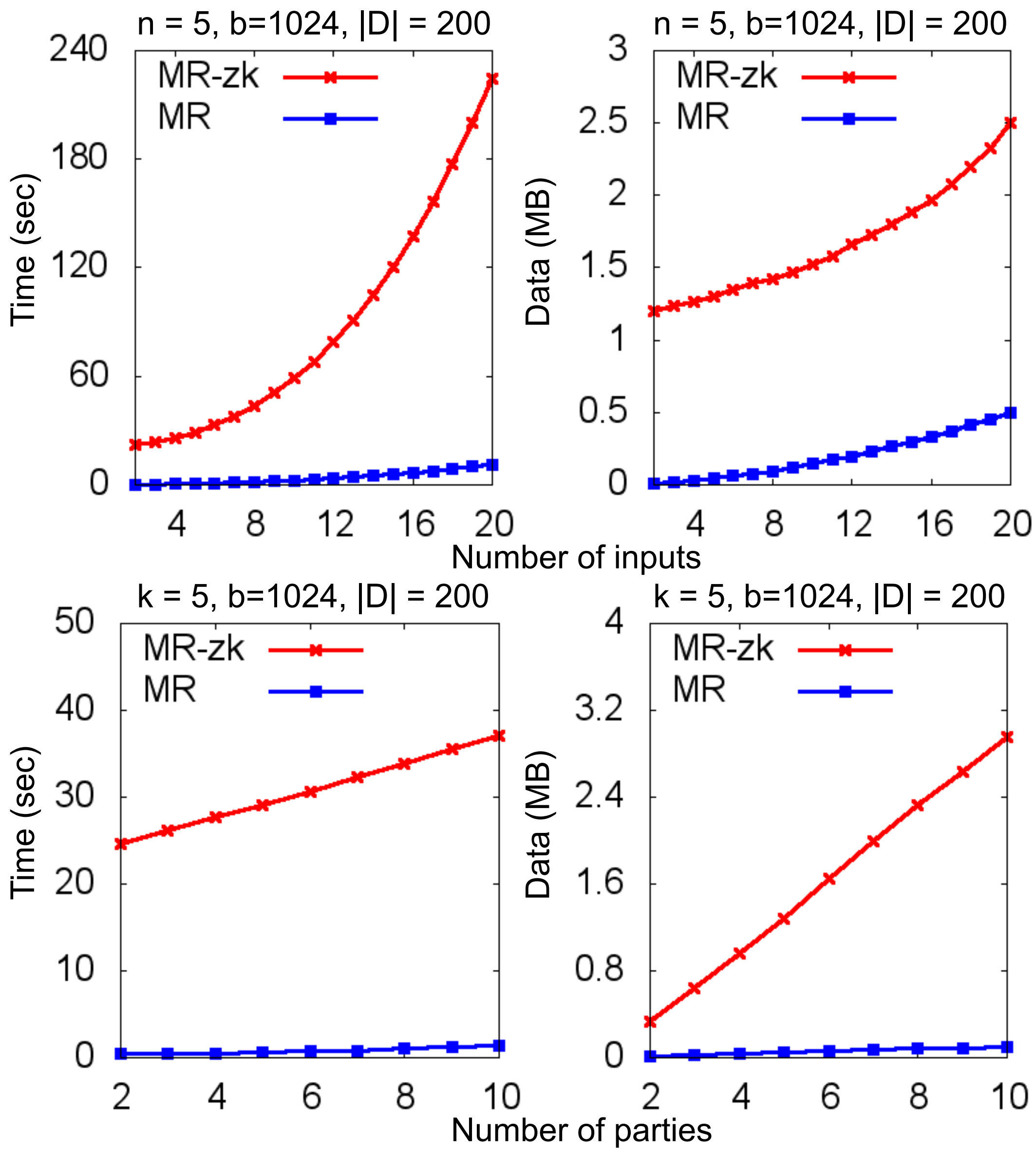
Problem	Model	Comp./Comm. Complexity
$MPROS^{MR}$	Semi-honest, standard model	$O\left(k^3 \cdot n \cdot b^3\right)$ $O\left(k^2 \cdot n \cdot b\right)$
	Malicious, random oracle model	$O\left(\left(\lvert D\rvert + k^3 \cdot n\right) \cdot n \cdot b^3\right)$ $O\left(\left(\lvert D\rvert + k^3 \cdot n\right) \cdot n \cdot b\right)$
$MPROS^{SR}$	Semi-honest, standard model	$O\left(k^6 \cdot n^4 \cdot b^3\right)$ $O\left(k^3 \cdot n^3 \cdot b\right)$
	Malicious, random oracle model	$O\left(\left(\lvert D\rvert + k^5 \cdot n^4\right) \cdot k \cdot n \cdot b^3\right)$ $O\left(\left(\lvert D\rvert + k^5 \cdot n^4\right) \cdot k \cdot n \cdot b\right)$

- n parties, k input elements, modulus with b bits
- Computation overhead: encryption, decryption and homomorphic operations
- Communication overhead: number of ciphertexts transmitted

Remarks

- All solutions polynomial-time bounded with respect to the number of parties n and inputs k

Results in Practice



Conclusion

Contributions

- New protocols for privacy-preserving reconciliation on ordered sets secure in the malicious model
- New ZKPK's to enable verifiable set operations
- First practical implementation and evaluation of MPROS protocols secure in the malicious model

Future research

- Development of a manifold library for privacy-preserving applications[3]
- Development of end-user (mobile) applications for privacy-preserving reconciliation

[3] G. Neugebauer, U. Meyer: **SMC-MuSe: A Framework for Secure Multi-Party Computation on MultiSets**, RWTH Aachen University, Technical Report, AIB-2012-16, December 2012.

Thank you for your attention!

Questions?