From SPDZ to SPD$\mathbb{Z}_{2^k}$

Fabian Schmid, IAIK

28th November 2019

Contents

A brief history

- The Millionaires’ Problem (two-party)
  - First proposed by Andrew Yao (1982) for Boolean circuits
- Secret sharing based (multi-party)
  - Further introduction of new protocols since then

An intuition on secret sharing

P_i wants to share secret $s \in \mathbb{F}_q$ among n parties.

- Additive sharing:
  - Distribute random shares s_i such that $\sum_{j=0}^{n} s_j = s$
  - Not robust in the general case, sufficient for MPC

Arithmetic on secret shares

Suppose we have the shared secrets x and y

- Performing addition:
  - Every party P_i has the shares x_i and y_i
  - Everyone adds their shares together $z_i = x_i + y_i$

$$z = \sum^n z_j = \sum^n x_j + \sum^n y_j = x + y$$

Arithmetic on secret shares

Suppose we have the shared secrets x and y

- Performing multiplication:
  - Does $z_i = x_i \cdot y_i$ also hold?

Arithmetic on secret shares

- Introduction of beaver triples a_i, b_i, c_i
  - Only $c = a \cdot b$ is known
  - We now create and open $\alpha_i = (x_i - a_i)$ and $\beta_i = (y_i - b_i)$
  - Everyone computes $z_i = c_i + \alpha b_i + \beta a_i$, one party also adds $\alpha \cdot \beta$
  - Hence $\sum^n z_j = c + \alpha b + \beta a + \alpha\beta = xy$

What is SPDZ?

- Preprocessing based MPC protocol
  - Sacrificing
  - Zero-Knowledge Proofs of Plaintext Knowledge
  - MACs

The many faces of SPDZ

- SPDZ2 - earlier MAC checks possible and better performance
- MASCOT - Oblivious Transfer based preprocessing
- Overdrive - Making SPDZ Great Again

Challenges of SPD$\mathbb{Z}_{2^k}$

- Information theoretically secure MAC
- MASCOT variant in $\mathbb{Z}_{2^k}$
- Adaptation of online phase

Protocol	Message space	Stat. security	Input cost (kbit)	Triple cost (kbit)
Ours	$\mathbb{Z}_{2^{32}}$	26	3.17	79.87
	$\mathbb{Z}_{2^{64}}$	57	12.48	319.49
	$\mathbb{Z}_{2^{128}}$	57	16.64	557.06
MASCOT	32-bit field	32	1.06	51.20
	64-bit field	64	4.16	139.26
	128-bit field	64	16.51	360.44

Improving the online phase

- SPDZ works in a finite field
- The integers modulo 2^k $\mathbb{Z}_{2^k}$ form a Ring
- Modern CPUs also work with integers mod 2^k
    - Many tricks and advantages in this domain.
- Significant speedup for secure comparison and bit decomposition