My title goes here*

And there can be a subtitle

Firstname Lastname

DD.MM.YYYY · Conference for Things 2099 · or other info

* Some acknowledgments?

Slide Title

- edit title using ctrl-P
- add new textfield with F10
- change name and title for the footer in the document properties ctrl-shift-P
- use \hl command to **highlight**

Multiparty PCG for Authenticated Triple

Achieving $O(\log(N))$ communication size

Practical MPC

2021 12 12

Authenticated Triples Functionality

- Parties $P_1, \ldots, P_m$
- Each P_i holds $x^i[j], y^i[j], z^i[j], m_x^i[j], m_y^i[j], m_z^i[j], \Delta^j$ for $j \in \{0, \ldots, N-1\}$
- Constraint 1: $\forall j \in [N]$,

$$(\sum_{i \in [m]} x^i[j]) \cdot (\sum_{i \in [m]} y^i[j]) = (\sum_{i \in [m]} z^i[j])$$

- Constraint 2: $\forall j \in [N], \forall a \in \{x, y, z\}$,

$$(\sum_{i \in [m]} a^i[j]) \cdot (\sum_{i \in [m]} \Delta^i) = (\sum_{i \in [m]} m_a^i[j])$$

Building Blocks

- Semi-Honest Ring-LPN OLE
- Malicious LPN sVOLE (Wolverine)
- FLIOP

Idea:

1. Run SH-OLE to get **unauthenticated** triples
2. Run Wolverine to get MAC (deg-3)
3. Run FLIOP to check consistency

Building Blocks

- Semi-Honest Ring-LPN OLE
- Malicious LPN sVOLE (Wolverine)
- FLIOP

Requirements:

- Communication Complexity: $O(\log N)$

Idea:

1. Run SH-OLE to get **unauthenticated** triples
2. Run Wolverine to get MAC (deg-3)
3. Run FLIOP to check consistency

Step 1: **Unauthenticated** Triples

Ring-LPN parameters:

- Ring $R = \mathbb{Z}_p[X]/f(X)$, $\deg f = N$
- $\vec{a} = (a_0, ..., a_{c-1})$
- $\vec{e} = (e_0, ..., e_{c-1})$ where each e_i is t-regular
- Isomorphism Map: $M : \mathbb{Z}_p^N \to \mathbb{Z}_p^N$

Step 1a: Each P_i generates $\{x^i[j], y^i[j]\}_{j \in [N]}$ as follows:

- Samples $\vec{e^i}, \vec{f^i}$ from t-regular distribution
- Define $x^i := M \cdot \langle \vec{a}, \vec{e^i} \rangle$, $y^i := M \cdot \langle \vec{a}, \vec{f^i} \rangle$

Step 1b: Each pairwise P_i, P_j computes $\vec{e^i} \otimes \vec{f^j}$:

- Interpret results as a len-$2N$ truth table
- Sum of $(ct)^2$-point functions
- Use 2-DPF $(ct)^2$ times

A In-depth Look of 2-DPF

P_i

$s_{0,0}$ $s_{0,0}$