# Threshold Zero-Knowledge Proofs based on MPC


Jules Maire

Sorbonne Université – CNRS

# Motivation

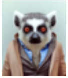
- a first paradigm for building threshold zero-knowledge proofs based on MPC
  ☞ threshold signatures from any NP relation
- the equivalence of MPC in the Head paradigm for **multi-prover & threshold**
  ☞ Ishai et al. (STOC 2007) with 1 prover vs 1 verifier
- NIST call for post-quantum threshold signatures

# Roadmap

- System and security model
- Black-box construction
- A construction with VSS-BGW
- Threshold signatures

# $(n, k)$-Threshold Signature

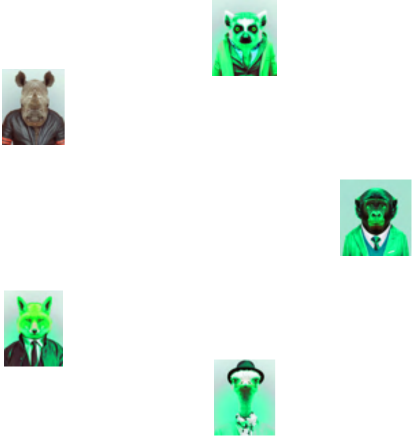
- $n$ users have a share of the signing/secret key
- at least $k \leq n$ users can sign a message
- at most $t < k$ users can be corrupted





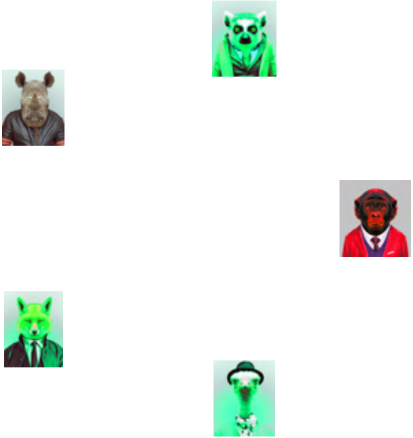
# $(n, k)$-Threshold Signature

- $n$ users have a share of the signing/secret key
- at least $k \leq n$ users can sign a message
- at most $t < k$ users can be corrupted



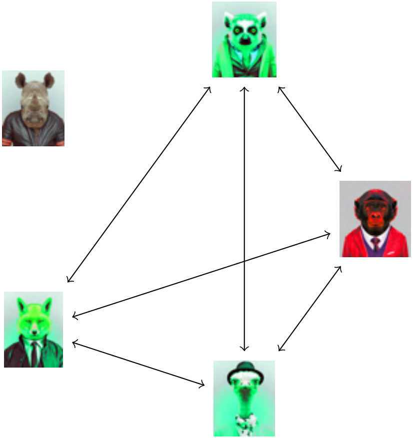
# $(n, k)$-Threshold Signature

- $n$ users have a share of the signing/secret key
- at least $k \leq n$ users can sign a message
- at most $t < k$ users can be corrupted



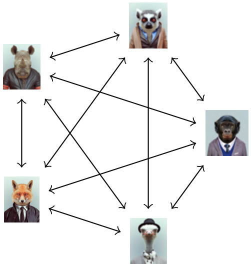
# $(n, k)$-Threshold Signature

- $n$ users have a share of the signing/secret key
- at least $k \leq n$ users can sign a message
- at most $t < k$ users can be corrupted



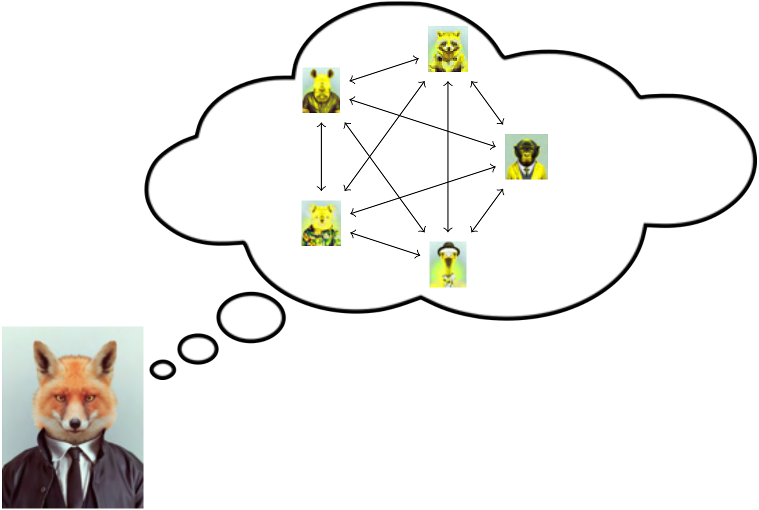
# Secure Multi-Party Computation (MPC)

- 1st model: **malicious setting** with robust security (for provers)
- 2nd model: **semi-honest setting** (for parties in heads)



# Secure Multi-Party Computation (MPC)

- 1st model: **malicious setting** with robust security (for provers)
- 2nd model: **semi-honest setting** (for parties in heads)



# Secret Sharing Schemes

- any $(n, t)$-threshold secret sharing (for provers)

  ☞ Shamir secret sharing $[\![s]\!]^t = \{[\![s]\!]^t_1 := p(1), \ldots, [\![s]\!]^t_n := p(n)\}$ with $p(x)$ degree $t$ and $p(0) = s$

- any linear secret sharing (for parties in the heads)

  ☞ additive secret sharing $[\![s]\!] = \{[\![s]\!]_1, \ldots, [\![s]\!]_n\}$ s.t. $s = \sum_{i=1}^{n} [\![s]\!]_i$

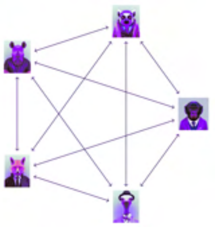
# Participants

- $k$ provers/signers $\mathcal{P}_1, \ldots, \mathcal{P}_k$
- 1 verifier $\mathcal{V}$
- an adversary $\mathcal{A}$ that may corrupt up to $t$ provers ($t < k$)
- assume that $k \geq \beta(t)$ for some $\beta : \mathbb{N} \to \mathbb{N}$

# Threshold Zero-Knowledge Proof (TZKP)

$F : x \rightarrow y$ a public one-way function (AES, syndrome decoding, ...)

- $\mathcal{P}_1, \ldots, \mathcal{P}_k$ hold $[\![x]\!]^t$ (i.e. $\mathcal{P}_i$ has $[\![x]\!]_i^t$)
- $\mathcal{V}$ knows $y$ (public)
- $k$ provers want to prove the *conjoint* knowledge of $x$ to $\mathcal{V}$



$\xrightarrow{\text{Commitments}}$

$\xleftarrow{\text{Challenge 1}}$

$\xrightarrow{\text{Response 1}}$

$\vdots$

$\xleftarrow{\text{Challenge } r}$

$\xrightarrow{\text{Response } r}$

# Threshold Zero-Knowledge Proof (TZKP)

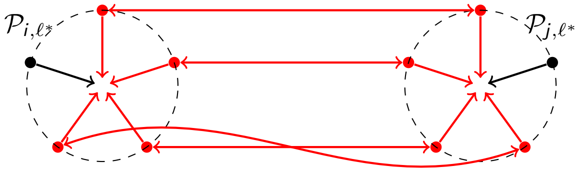
## Security Proofs

- **Completeness:** Pr[$\mathcal{V}$ accepts | at least $t+1$ provers hold a valid share]$= 1$
  ☞ perfect *t*-robustness
- **Soundness:** Pr[$\mathcal{V}$ accepts | less than $t+1$ provers hold a valid share]$\leq \epsilon$
  ☞ perfect correctness
- **Zero-knowledge:** $\mathcal{V}$ learns nothing on the secret
  ☞ *t*-privacy

# Overview of provers computation in TZKP


- secure per-to-per channel
- broadcasting authenticated channel

# Verification System in TZKP




- challenge $\ell^*$ for opening all-but-one party
- $\mathcal{V}$ chooses a subset of $t+1$ provers and checks the computation

# Black-box construction

- $\mathcal{R}^{t,k}(x, w_1, \ldots, w_k)$ a generalized NP-relation for multi-witness (threshold).
- Leads to a **general construction of a TZKP system** $\Pi_{\mathcal{R}^{t,k}}$ **for any NP-relation** $\mathcal{R}^{t,k}$ which makes a black-box use of an MPC protocol $\Pi_f$ for a related multi-party functionality $f$.

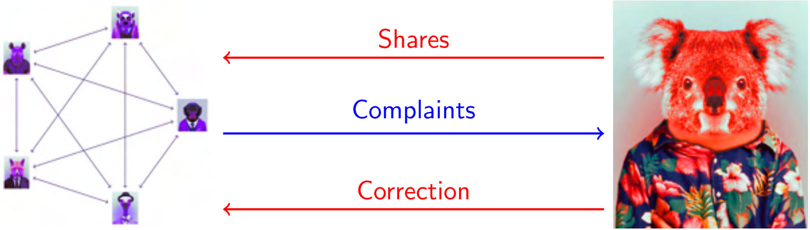
## Theorem - Informal

Let $\Pi_f$ realizes the $k$-party functionality $f$ such that $\Pi_f$ is **perfect** $t$-**robust**, and $t$-**private** in the malicious setting with an adversary corrupting up to $t$ provers. Then our Protocol $\Pi_{\mathcal{R}^{t,k}}$ is a TZKP for the NP-relation $R^{t,k}$.

# Verifiable Secret Sharing

a (possibly corrupted) dealer shares $s$ with $F(x)$ of degree $t$.

1. Dealer sends shares from bivariate polynomial of degree $t$ in both variables $S(x,y) \in \mathbb{F}[x,y]$ with $F(x) = S(x,0)$




2. They hold a shares from a $t$-threshold secret sharing (or dealer cheated and is fired)

**However... no guarantee on $s$**

# Construction based on BGW

1. provers shared secrets from $t$-Shamir secret sharing $([\![a]\!]^t, [\![b]\!]^t)$

   ☞ BGW protocol for multiplicative relations

2. in BGW some communication

   ☞ VSS to communicate with each other

3. after VSS provers shared a word of distance at most $t$ from a code of length $k$ and dimension $2t+1$

   ☞ when $k \geq \beta(t) \geq 4t+1$, code can correct up to $t$ errors

4. Reed-Solomon decoding algorithm

   ☞ $[\![ab]\!]^t$

**perfect $t$-robust protocol $\Pi$**

# Proof of Π

**Theorem - proved by Lindell**

Let $\beta(t) = 3t + 1$. Then, VSS-BGW sub-protocol is $t$-secure in the presence of an adversary corrupting up to $t$ provers.

informally, a protocol is *secure* if its real-world behavior can be simulated in the ideal model

**Theorem**

Let $\beta(t) = 3t + 1$. Then Π is a TZKP in the VSS-BGW-hybrid model.

# Threshold (post-quantum) signatures

- Multi-round Fiat Shamir for multi-prover
- Signature size: factor between $\approx k$ and $k^2$ compared to MPCitH based signatures

☞ **A new system/security model for threshold multi-prover ZKP**

☞ **A first versatile framework based on MPC for building threshold signatures from any one-way function**