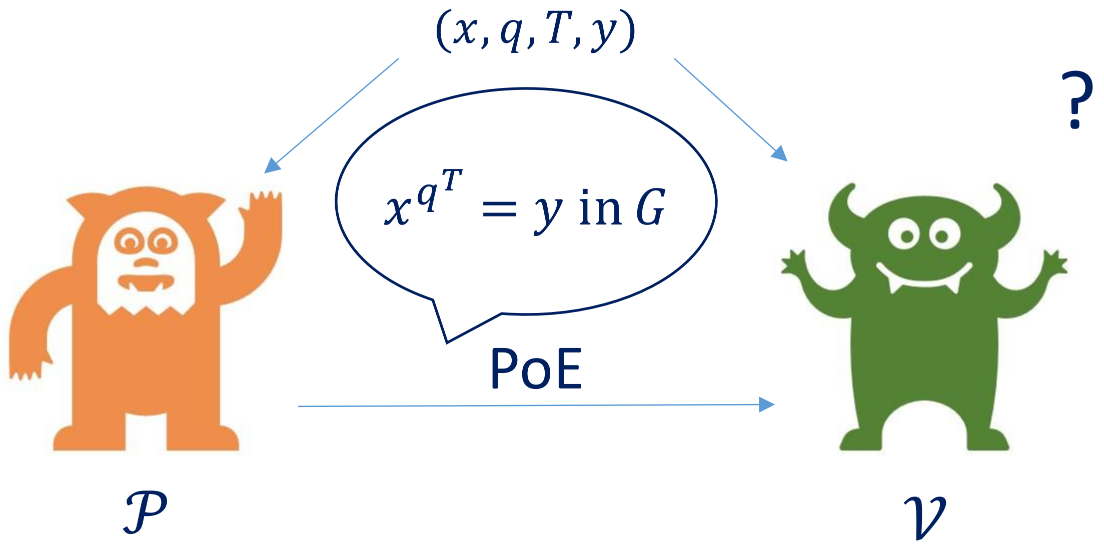
European Research Council
Established by the European Commission

Practical Statistically-Sound Proofs of Exponentiation in any Group

Charlotte Hoffmann[1], Pavel Hubáček[2], Chethan Kamath[3], Karen Klein[4], Krzysztof Pietrzak[1]

[1]Institute of Science and Technology Austria
[2]Charles University, Faculty of Mathematics and Physics
[3]Tel Aviv University
[4]ETH Zurich

Proofs of Exponentiation



- If $\mathrm{ord}(G)$ is known: $\mathcal{P}$ and $\mathcal{V}$ compute $e \coloneqq q^T \bmod \mathrm{ord}(G)$ and x^e.
- Otherwise: $\mathcal{P}$ performs T sequential exponentiations
$$x \to x^q \to x^{q^2} \to x^{q^3} \to \cdots \to x^{q^T}$$
  and sends a *Proof of Exponentiation* (PoE) to $\mathcal{V}$.
- Cost of computing and verifying the proof $\ll T$.

PoE Applications

- Verifiable Delay Functions (VDFs) [BBBF18, Pie19, Wes20]:
  - Verifiable: given a proof, everyone can efficiently and soundly verify correctness of the result
  - Delay: can't be computed faster than a given time parameter T even with parallelization
  - Function: unique output
- Time- and Space-Efficient Arguments for NP [BHR+21]:
  - PoEs as building blocks in polynomial commitment scheme

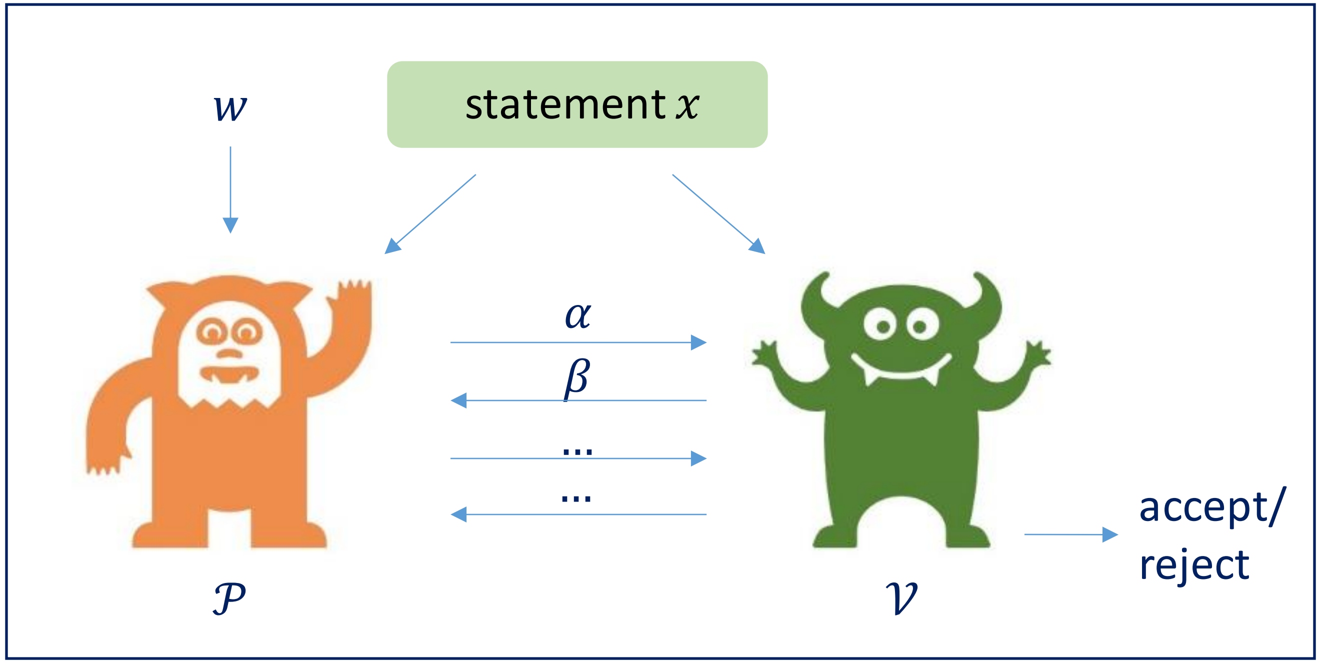
Plan

1. PoE Constructions and Properties
2. Technical Overview: Our PoE

Plan

1. **PoE Constructions and Properties**
2. Technical Overview: Our PoE

Interactive Protocols



- **Completeness:** If statement is true, $\mathcal{V}$ accepts with probability 1
- **Soundness:** If statement is false, $\mathcal{V}$ rejects with high probability

- **Statistical Soundness:** Cheating $\mathcal{P}$ is computationally unbounded
- **Computational Soundness:** Cheating $\mathcal{P}$ is polynomially bounded

Overview of PoEs

(x, y, q, T) s.t. $x^{q^T} = y$

Wesolowski [Wes20]	Pietrzak [Pie19]	Block et al. [BHR+21]
 $\$$ g		$, g_{2,1}, \dots, g_{\lambda,1}$ $\$, \$, \dots, \$$ $, g_{2,2}, \dots, g_{\lambda,2}$ … 
1 grp elem		grp elements
Adaptive Root Assumption	Statistically sound in some grps/ Low Order Assumption	Statistically sound in **any** group

<u>Our Contribution</u>: Statistically-sound PoE that reduces proof size of [BHR+21] by almost one order of magnitude for q of a special form

Why Statistical Soundness for PoEs?

- Polynomial Commitment [BHR+21]: Statistical knowledge soundness
- VDFs: Soundness holds even if group order known by prover
- Class groups: Low-order assumption not well studied/understood
- RSA groups: Need to sample safe primes and prove that a modulus is product of safe primes

Technical Overview

Plan

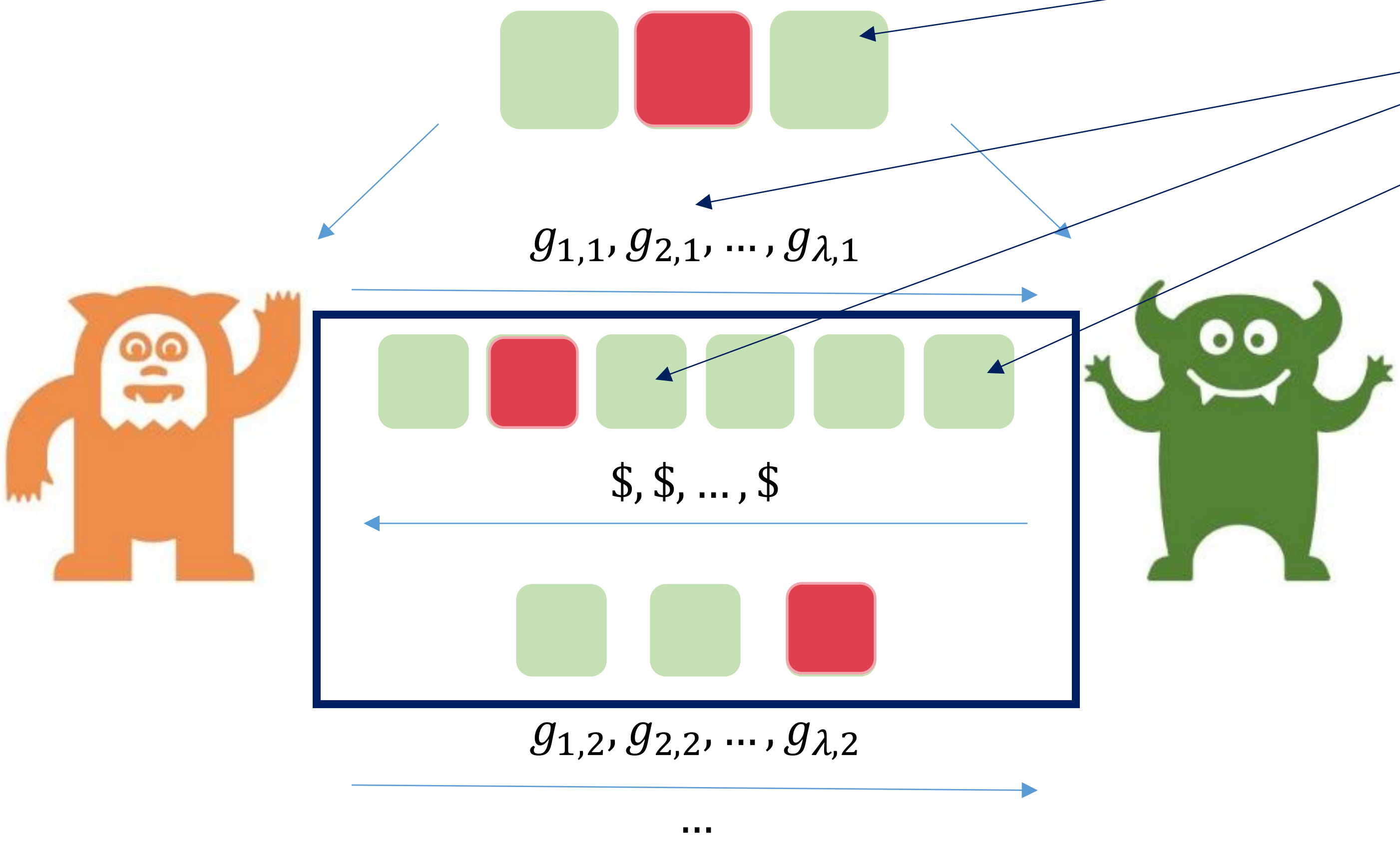
1. PoE Constructions and Properties
2. **Technical Overview:**
    1. PoE construction of [BHR+21]
    2. Our work: Reduce complexity

One Round of [BHR+21] PoE

$x_i^{q^T} = y_i$

$g_{i,1} = x_i^{q^{T/2}}$

$g_{i,1}^{q^{T/2}} = y_i$



[BHR+21] PoE – Main Idea

Want: Reduce the number of statements to λ

$x_1{}^{q^{T/2}} = y_1$ | $x_2{}^{q^{T/2}} = y_2$ | … | $x_k{}^{q^{T/2}} = y_k$ | $x_{2\lambda}{}^{q^{T/2}} = y_{2\lambda}$

$r \leftarrow \{0,1\}^{2\lambda}$

$r_k = 1$ w/ probability $1/2$

$$\left(\prod_{i\in[2\lambda]} x_i^{r_i}\right)^{q^{T/2}} = \prod_{i\in[2\lambda]} y_i^{r_i}$$

If at least one of the initial statements is wrong, the new statement

Goal: Reduce this number

$$\underbrace{\prod\ldots=\prod\ldots \quad \prod\ldots=\prod\ldots \quad \quad \quad \quad \prod\ldots=\prod\ldots}_{\lambda \text{ times}}$$

$\Rightarrow$ At least one of the statements is wrong with probability at least $1 - 2^{-\lambda}$.

Our Construction – First Step

$^{1}/_{2}$

$$\prod_{i\in m} x_i^{r_i q^T} = \prod_{i\in m} y_i^{r_i}$$

$r_i \in \{0,1\}$

Pr[new statement wrong] $\geq 1/2$

$r_i \in \{0,1,\ldots,R\}$

$$\prod_{i\in m} x_i^{r_i q^T} = \prod_{i\in m} y_i^{r_i}$$

$r_i \in \{0,1,\ldots,R\}$

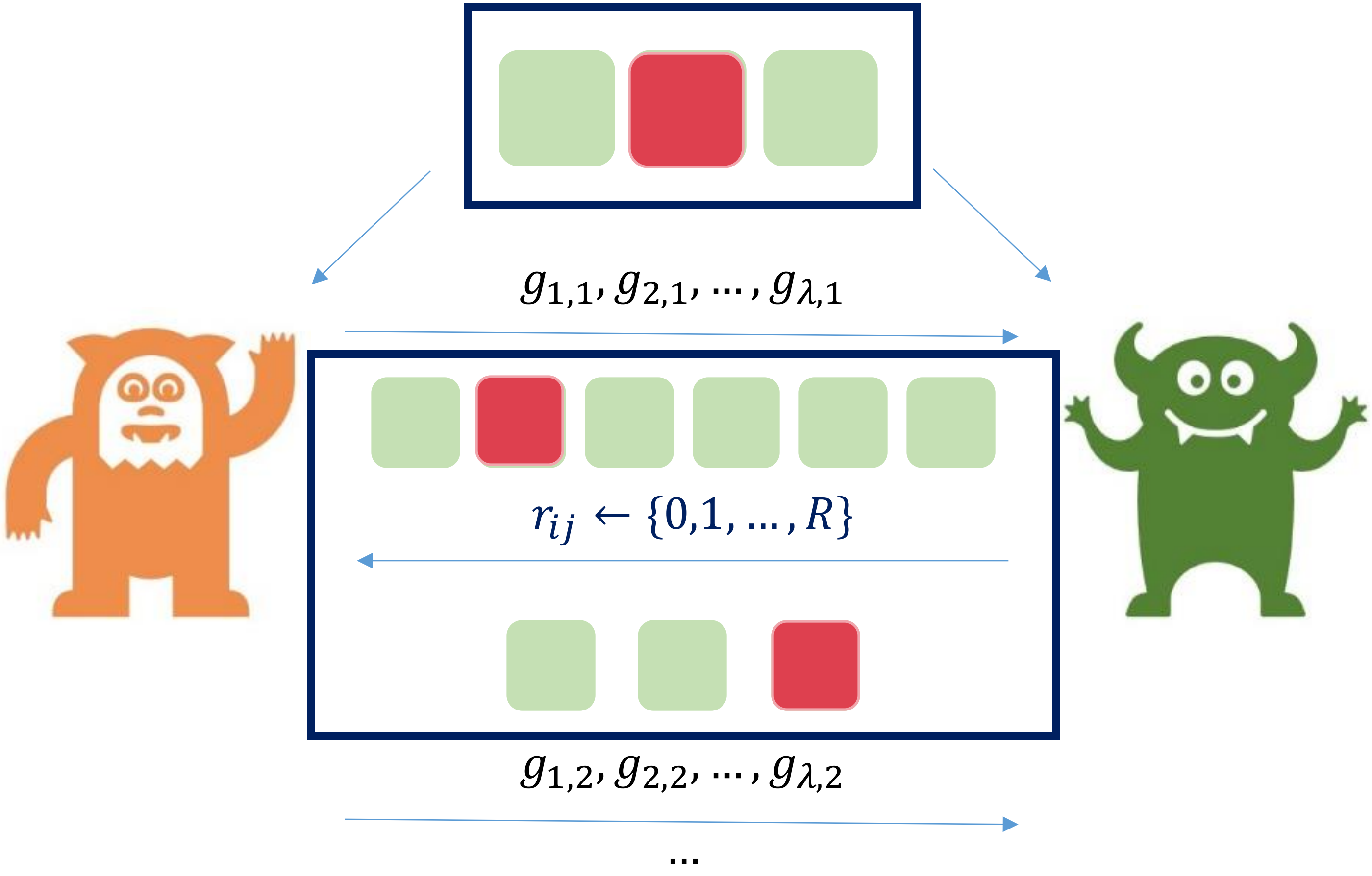
$\boxed{\Pr[\text{new statement wrong}] \geq 1/2}$

Due to low order elements [BBF18, BP00]:

$$x_k{}^{q^T} = \alpha y_k \xrightarrow{\mathrm{ord}(\alpha)\,\mid\, r_k} x_k{}^{r_k q^T} = y_k{}^{r_k}$$

$$\Pr[\mathrm{ord}(\alpha) \mid r_k] = 1/\mathrm{ord}(\alpha)$$

Our Construction – First Step



Our Construction – Second Step

$q := \prod_{p<B \text{ prime}} p$

$C := \log T \log B$

$x_1^{q^{T-C}} = \tilde{y}_1$ $x_2^{q^{T-C}} = \tilde{y}_2$ $x_k^{q^{T-C}} = \alpha \tilde{y}_k$ $x_\lambda^{q^{T-C}} = \tilde{y}_\lambda$

compute $\tilde{y}_i^{q^C} = y_i \; \forall i \in [\lambda]$

If α has low order: $x_k^{q^{T-C}} = \alpha \tilde{y}_k \xrightarrow{\mathrm{ord}(\alpha) \mid q^C} (\alpha \tilde{y}_k)^{q^C} = \tilde{y}_k^{q^C} = y_k = x_k^{q^T}$

$\Rightarrow$ Reduce proof size of [BHR+21] from $\lambda \log T$ to $\lambda \log T / \log B$

Our Construction – Basic Protocol

$$q := \prod_{p_i < B \text{ prime}} p_i$$

$$\rho := \lambda / \log B$$

$\boxed{x_i^{q^{T-C}} = \tilde{y}_i}$

α

$g_{1,1}, g_{2,1}, \dots, g_{\rho,1}$

$r_{ij} \leftarrow \{0,1,\dots,R\}$

$g_{1,1}, g_{2,1}, \dots, g_{\rho,1}$

…

compute $\tilde{y}_i^{q^C} = y_i \; \forall i \in [\rho]$

Statistical Soundness:

- If $\mathrm{ord}(\alpha) \mid q^C \Rightarrow \mathcal{V}$ obtains correct result y_i
- Else $\Rightarrow$ α has sufficiently high order $\Rightarrow \mathcal{V}$ rejects after interactive phase w.h.p.

On Parameters q and B

$$q := \prod_{p<B \text{ prime}} p$$

- [BHR+21]: q has to be large to ensure soundness of polynomial commitment: $q \gg 2^{n\, poly(\lambda)}$
- VDFs: Can adjust the cost of the initial exponentiation by adjusting time parameter T

<u>Example</u>

Set $\lambda = 80, \mathrm{T} = 2^{32}, B = 521 \Rightarrow q \approx 2^{703}$

Proof size drops from $\lambda \log T = 2560$ to $\lambda \log T \,/\, \log B = 284$ group elements

$\Rightarrow$ 655 KB to 74 KB

Comparison

Cost of Verifying λ PoEs

Verifier's complexity increases

PoE	Statistically Sound?	Verifier's Complexity	Proof Size
[Wes20]	no	$\log T + \lambda^2$	1
[Pie19]	in some groups	$\lambda \log T + \lambda^2 + \log q$	$\log T$
[BHR+21]	yes	$\lambda^2 \log T + \lambda \log q$	$\lambda \log T$
Our work w/o recursion	yes	$\lambda^2 \log T / \log B + \lambda \log q \log T / \log B$	$\lambda \log T / \log B$
Our work w/ recursion	yes	$\lambda^2 \log T / \log B + \lambda \log q \log\log T / \log B$	$\lambda(\log T / \log B + 1)$

Solve via recursion and batching

Questions?