Sub-linear Zero-Knowledge Argument for Correctness of a Shuffle

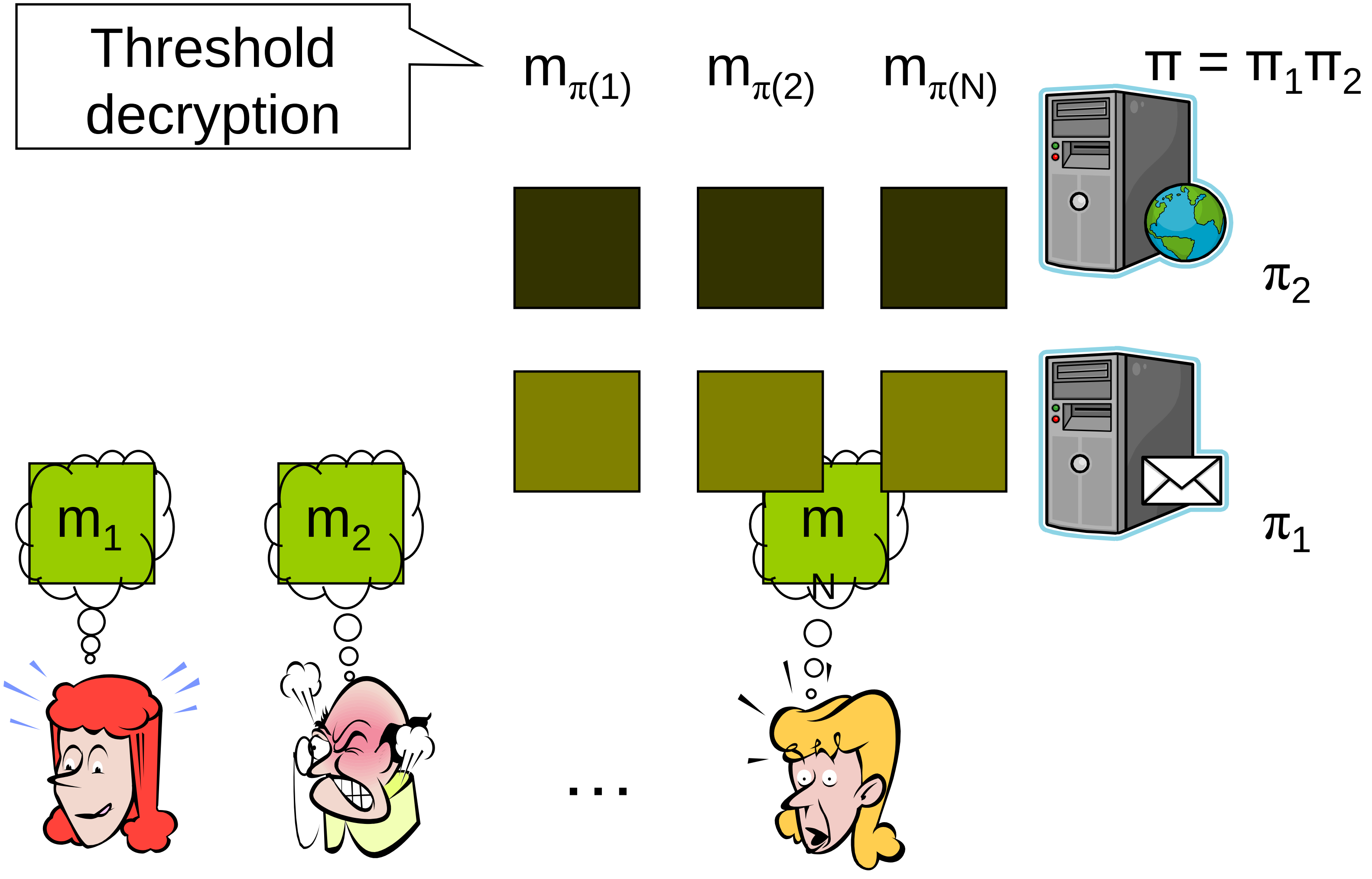
Jens Groth
University College London

Yuval Ishai
Technion and University of California Los Angeles

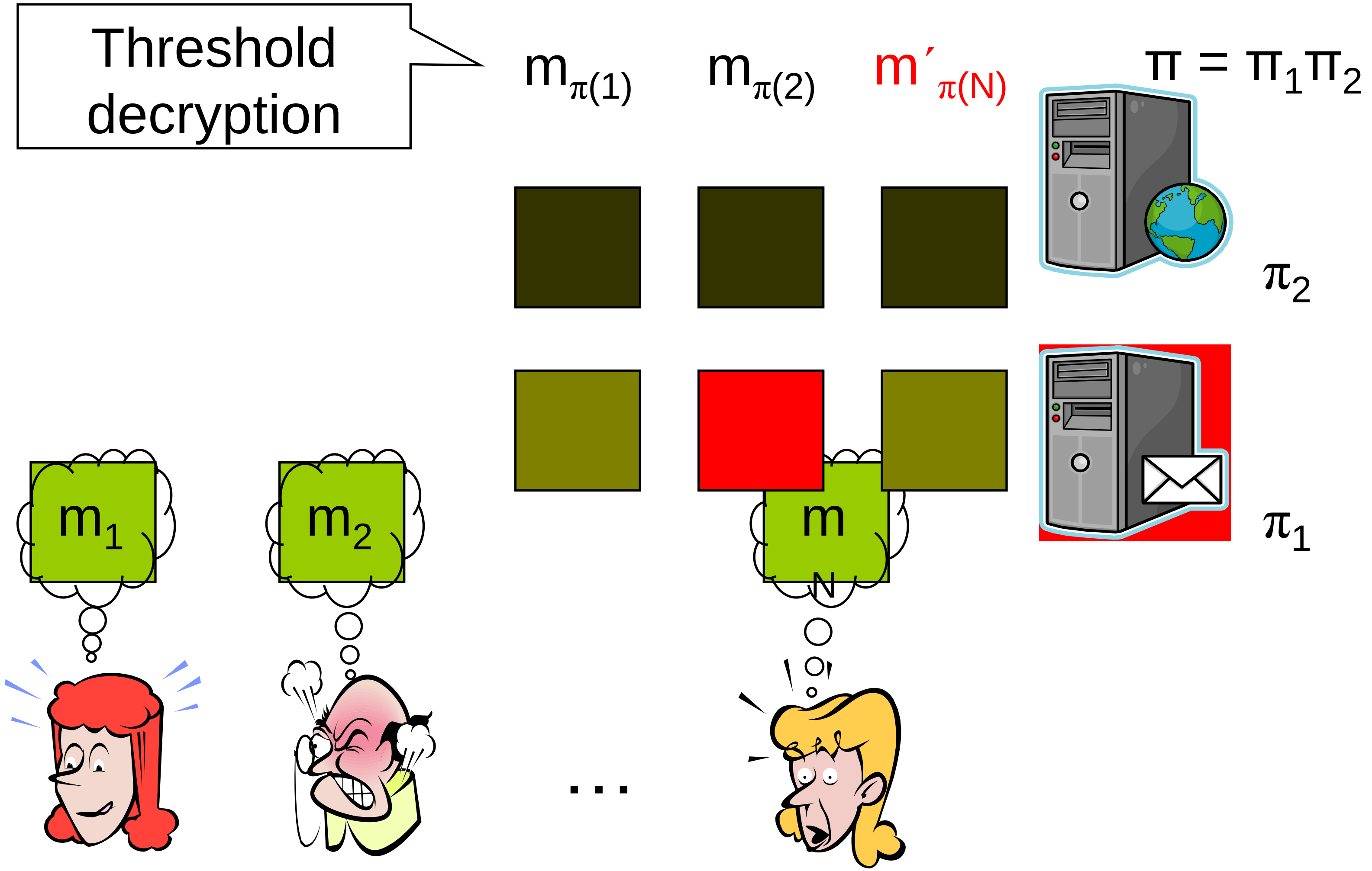
Initial question

- Kilian 92 gave sub-linear size zero-knowledge argument for SAT
- Not practical though
  (SAT statement, PCP theorem, ...)
- Is there a practical sub-linear zero-knowledge argument?
- Yes! We will give sub-linear shuffle argument

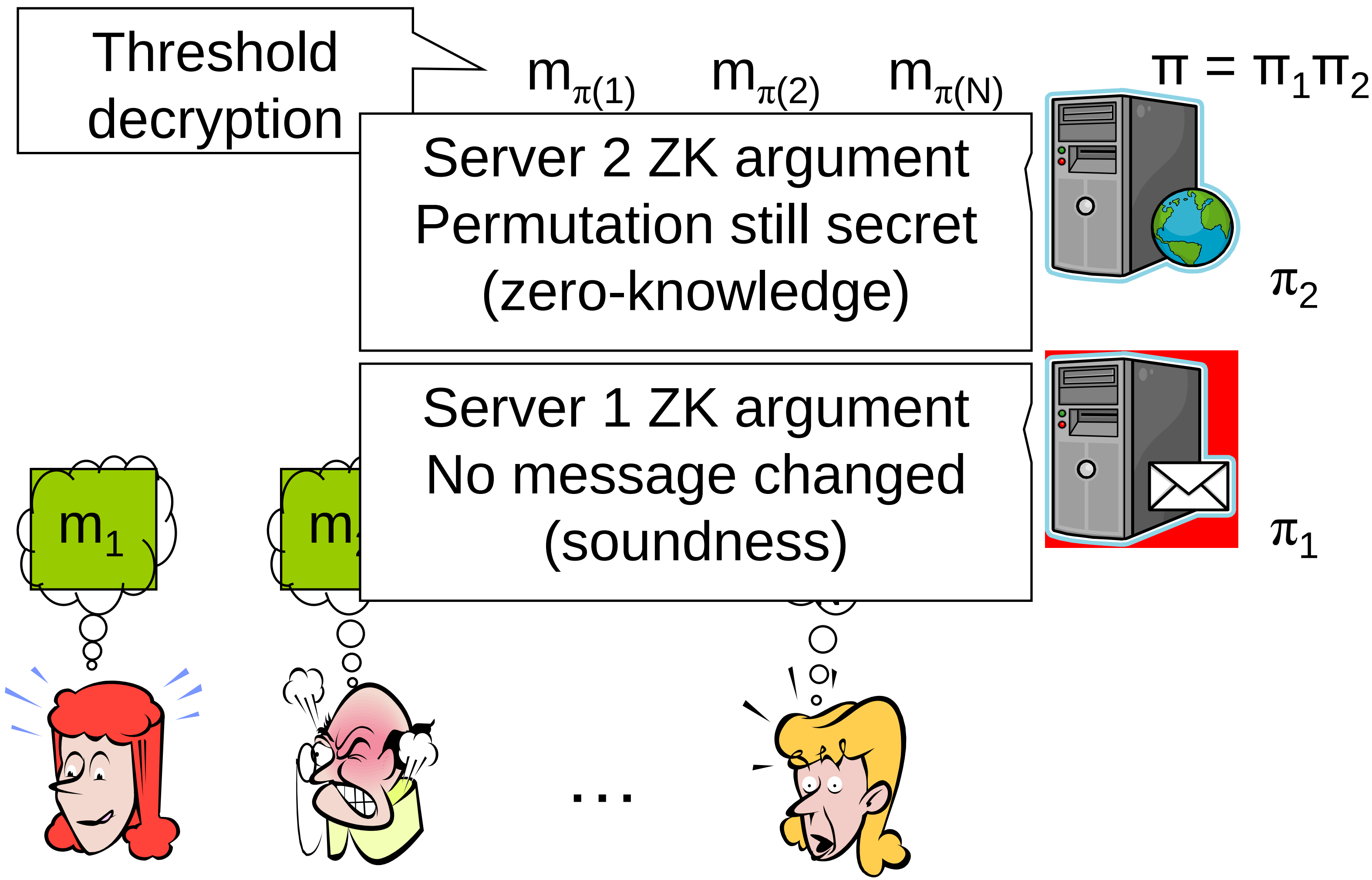
Mix-net: Anonymous message broadcast



Problem: Corrupt mix-server



Solution: Zero-knowledge argument



ElGamal encryption

Setup: Group G of prime order q with generator g

Public key: $pk = y = g^x$

Encryption: $E_{pk}(m; r) = (g^r, y^r m)$

Decryption: $D_x(u,v) = vu^{-x}$

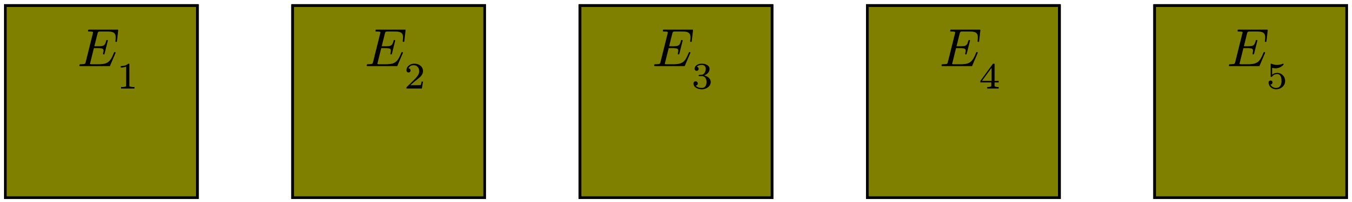
Homomorphic:

$$E_{pk}(m; r) \times E_{pk}(M; R) = E_{pk}(mM; r+R)$$

Re-randomization:

$$E_{pk}(m; r) \times E_{pk}(1; R) = E_{pk}(m; r+R)$$

Shuffle



- Input ciphertexts $e_1,\ldots,e_N$
- Permute to get $e_{\pi(1)},\ldots,e_{\pi(N)}$
- Re-randomize them $E_i = e_{\pi(i)} \times E_{pk}(1;R_i)$
- Output ciphertexts $E_1,\ldots,E_N$

Zero-knowledge shuffle argument

Statement: $(pk, e_1, \ldots, e_N, E_1, \ldots, E_N)$

Zero-knowledge:
Nothing but truth revealed;
permutation is secret

Sound:
Shuffle is correct

Prover

Verifier

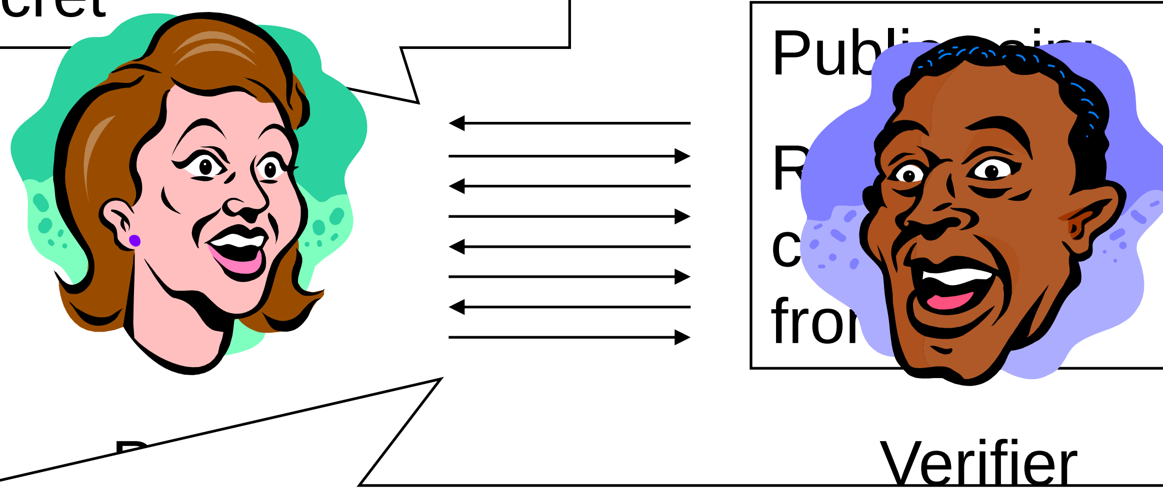
√

Public coin honest verifier zero-knowledge

Setup: (G,q,g) and common random string

Statement: $(pk, e_1, \ldots, e_N, E_1, \ldots, E_N)$

Honest verifier zero-knowledge
Nothing but truth revealed;
permutation secret

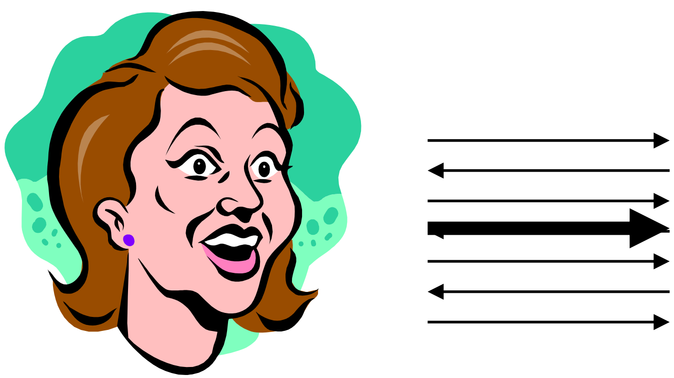


Can convert to standard zero-knowledge argument

Non-interactive zero-knowledge argument

Setup: (G,q,g) and common reference string

Statement: $(pk, e_1, \ldots, e_N, E_1, \ldots, E_N)$



Fiat-Shamir 86:

Compute challenges using cryptographic hash-function

Prover

Verifier

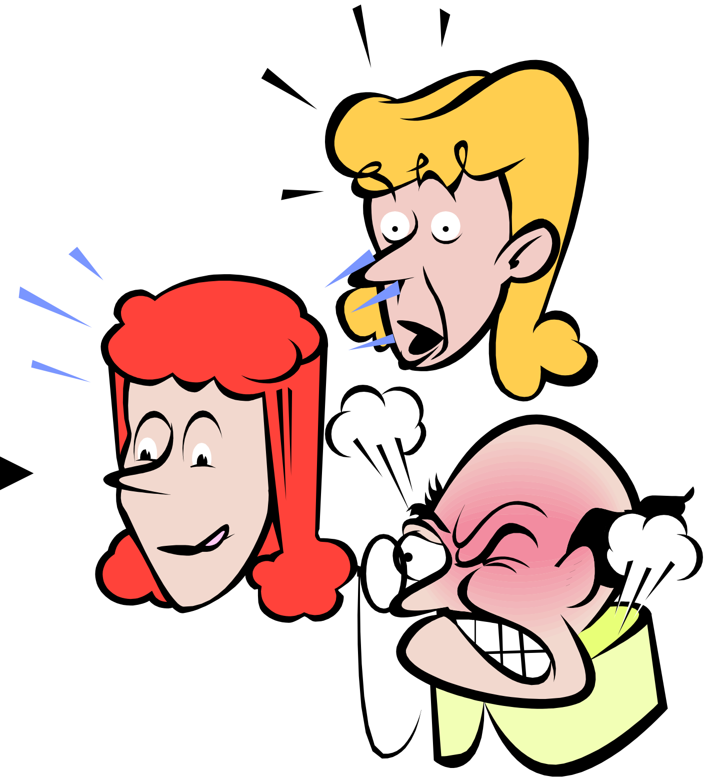
Anybody

Non-interactive zero-knowledge argument

Setup: (G,q,g) and common reference string

Statement: $(pk, e_1, \ldots, e_N, E_1, \ldots, E_N)$

Prover



History

• Cut-and-choose	O(Nks) bits
• Abe 99 (Abe-Hoshino 01)	O(N log(N)k) bits
• Furukawa-Sako 01 (Furukawa 05, Groth-Lu 07)	O(Nk) bits
• Neff 01 (Groth 03)	O(Nk) bits
• Others	O(Nk) bits
• This work	$O(N^{2/3}k)$ bits

Our contribution

- 7-move public coin honest verifier zero-knowledge argument for correctness of shuffle in common random string model
- Communication: $O(m^2+N/m)k$ bits
  Prover computation: $O(mN)$ expos
  Verifier computation: $O(N)$ expos

Previous
$O(N)k$
$O(N)$
$O(N)$

Fiat-Shamir heuristic:
Prover only computes once

Concrete example

- Back-of-envelope estimates
- ElGamal over elliptic curve (256 bit)
- Shuffle N = 100,000 ciphertexts (88Mbits)
- m = 10
- Optimized with multi-exponentiation, batch-verification, etc.
- Estimated cost

		Groth 03
Communication	8 Mbits	77 Mbits
Prover comp.	143 sec.	18 sec.
Verifier comp.	5 sec.	14 sec.

Tools

- Inspired by [IKO07] we will not use full-blown PCPs
- Pedersen commitment to multiple messages

$$ck = (g; h_1; \ldots; h_n)$$

$$\text{commit}_{ck}(m_1; \ldots; m_n; r) = g^r \prod_{i=1}^{n} h_i^{m_i}$$

- Batch verification using Schwartz-Zippel lemma

$$\text{poly}_1(x; y; \ldots; z) = \text{poly}_2(x; y; \ldots; z)$$

with probability at most d/q

HVZK shuffle argument

Setup: $(G; q; g; ck)$

Statement: $pk; \left\{e_{ij}\right\}_{i;j=1}^{m;n}; \left\{E_{ij}\right\}_{i;j=1}^{m;n}$ where $N = mn$

$\text{commit}_{ck}(\pi)$ →

$s_1; \dots; s_m; t_1; \dots; t_n \leftarrow \mathbb{Z}_q$ ←

$a_{ij} := s_i t_j$

HVZK $\prod_{i;j=1}^{m;n} e_{ij}^{a_{ij}} = E_{pk}(1; R) \prod_{i;j=1}^{m;n} E_{ij}^{a_{\pi(ij)}}$

Prover

Verifier

HVZK shuffle argument

Prover | Verifier

$$\text{commit}_{ck}(\pi) \longrightarrow$$

$$\longleftarrow s_1,\ldots,s_m,t_1,\ldots,t_n \leftarrow \mathbb{Z}_q$$

Schwartz-Zippel lemma implies

$$\forall i,j : m_{ij} = M_{\pi^{-1}(ij)}$$

or else only probability 2/q of polynomial equality

$$\sum_{i,j=1}^{m,n} \log(m_{ij}) s_i t_j = \sum_{i,j=1}^{m,n} \log(M_{\pi^{-1}(ij)}) s_i t_j$$

HVZK shuffle argument

Setup: (G, q, g, ck)

Statement: $pk, \{e_{ij}\}_{i,j=1}^{m,n}, \{E_{ij}\}_{i,j=1}^{m,n}$ where $N = mn$

Prover

Verifier

$\text{commit}_{ck}(\pi)$ $\longrightarrow$

$\longleftarrow$ $s_1, \ldots, s_m, t_1, \ldots, t_n \leftarrow \mathbb{Z}_q$

$a_{ij} := s_i t_j$

$c \leftarrow \text{commit}_{ck}(\ldots, a_{\pi(ij)}, \ldots)$

$\text{HVZK}\left(\text{commitment to } \alpha_{ij} \text{ so } \alpha_{ij} = a_{\pi(ij)}\right)$

$$\text{HVZK}\left(\prod_{i,j=1}^{m,n} e_{ij}^{a_{ij}} = E_{pk}(1; R) \prod_{i,j=1}^{m,n} E_{ij}^{\alpha_{ij}}\right)$$

The second HVZK argument

Setup: (G, q, g, ck)

Statement: $pk, A_1, \dots, A_m, E, \{E_{ij}\}_{i,j=1}^{m,n}$ where $N = mn$

$$A_1 = \text{commit}_{ck}(\alpha_{11}, \dots, \alpha_{1n}; r_1)$$

$$\vdots$$

$$A_m = \text{commit}_{ck}(\alpha_{m1}, \dots, \alpha_{mn}; r_m)$$

$$c = \text{commit}_{ck}(\dots, \alpha_{ij}, \dots)$$

$$\text{HVZK} \left(E = E_{pk}(1;R) \prod_{i,j=1}^{m,n} E_{ij}^{\alpha_{ij}} \right)$$

Main idea

$$A_1 = \mathrm{commit}_{ck}(\alpha_{11}, \ldots, \alpha_{1n}; r_1)$$
$$\vdots$$
$$A_m = \mathrm{commit}_{ck}(\alpha_{m1}, \ldots, \alpha_{mn}; r_m)$$

$$\mathrm{HVZK}\left(E = \prod_{i,j=1}^{m,n} E_{ij}^{\alpha_{ij}}\right)$$

$$D_{11} := \prod_{j=1}^{n} E_{1j}^{\alpha_{1j}} \quad \cdots \quad D_{1m} := \prod_{j=1}^{n} E_{mj}^{\alpha_{1j}}$$
$$\vdots \qquad\qquad \vdots$$
$$D_{m1} := \prod_{j=1}^{n} E_{1j}^{\alpha_{mj}} \quad \cdots \quad D_{mm} := \prod_{j=1}^{n} E_{mj}^{\alpha_{mj}}$$

$$c_1, \ldots, c_m \leftarrow \mathbb{Z}_q$$

$$\prod_{i=1}^{m} A_i^{c_i} = \mathrm{commit}_{ck}\left(\sum_{i=1}^{m} c_i \alpha_{i1}, \ldots, \sum_{i=1}^{m} c_i \alpha_{in}\right) \qquad \prod_{i,j} E_{ij}^{\alpha_{ij}} = \prod_{i=1}^{n} D_{ii}$$

$$\prod_{j=1}^{n} E_{\ell j}^{\sum_{i=1}^{m} c_i \alpha_{ij}} = \prod_{i=1}^{n} D_{i\ell}^{c_i}$$

$$\prod_{i=1}^{n}\left(\prod_{j=1}^{n} E_{\ell j}^{\alpha_{ij}}\right)^{c_i} = \prod_{i=1}^{n} D_{i\ell}^{c_i}$$

Schwartz-Zippel lemma implies

$$\forall i, \ell : D_{i\ell} = \prod_{j=1}^{n} E_{\ell j}^{\alpha_{ij}}$$

Argument for correct shuffle of ElGamal ciphertexts

- Honest verifier zero-knowledge
- Argument of knowledge
- Random string model
- 7-moves
- Public coin
- Cost

Communication	$O(m^2+N/m)k$ bits
Prover computation	$O(mN)$ expos
Verifier computation	$O(N)$ expos

- Generalizations
  - Homomorphic cryptosystems (e.g. Paillier)
  - 8-move zero-knowledge argument of knowledge for correctness of a shuffle in plain model

Future work: Beyond shuffling

- Can generalize techniques to arithmetic circuits.

  Public coin honest verifier zero-knowledge argument for arithmetic circuit over $\mathbf{Z}_q$ of size $O(|C|^{2/3}k)$

Thanks

Questions?