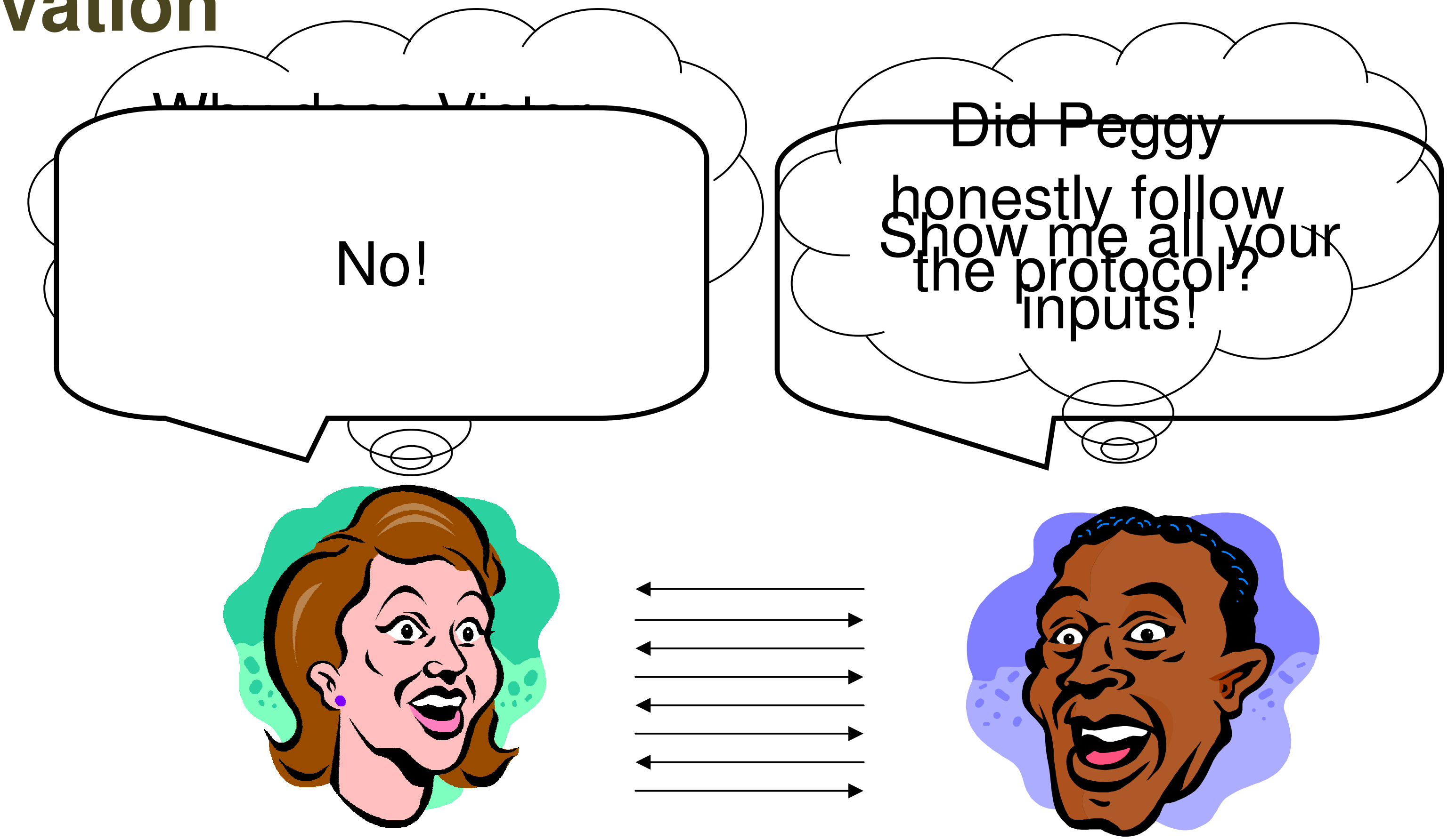
Linear Algebra with Sub-linear Zero-Knowledge Arguments

Jens Groth

University College London

Motivation



Peggy

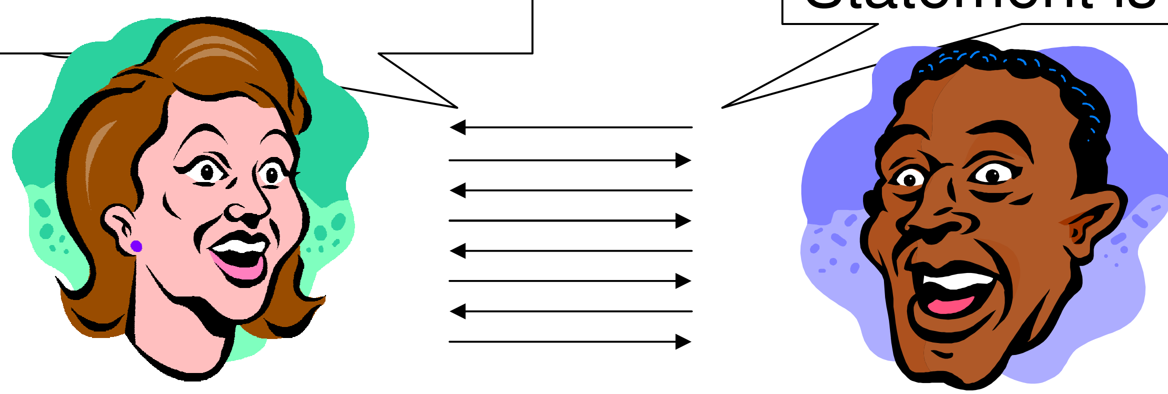
Victor

Zero-knowledge argument

Statement

Zero-knowledge:
Nothing but truth revealed

Soundness:
Statement is true



Prover

Verifier

√

Statements

- Mathematical theorem: 2+2=4
- Identification: I am me!
- Verification: I followed the protocol correctly.

- Anything: X belongs to NP-language L

Our contribution

- Perfect completeness
- Perfect (honest verifier) zero-knowledge
- Computational soundness
  - Discrete logarithm problem
- Efficient

Rounds	Communication	Prover comp.	Verifier comp.
$O(1)$	$O(\sqrt{N})$ group elements	$\omega(N)$ expos/mults	$O(N)$ mults
$O(\log N)$	$O(\sqrt{N})$ group elements	$O(N)$ expos/mults	$O(N)$ mults

Which NP-language L?

Circuit Satisfiability!

Anonymous Proxy
Group Voting!

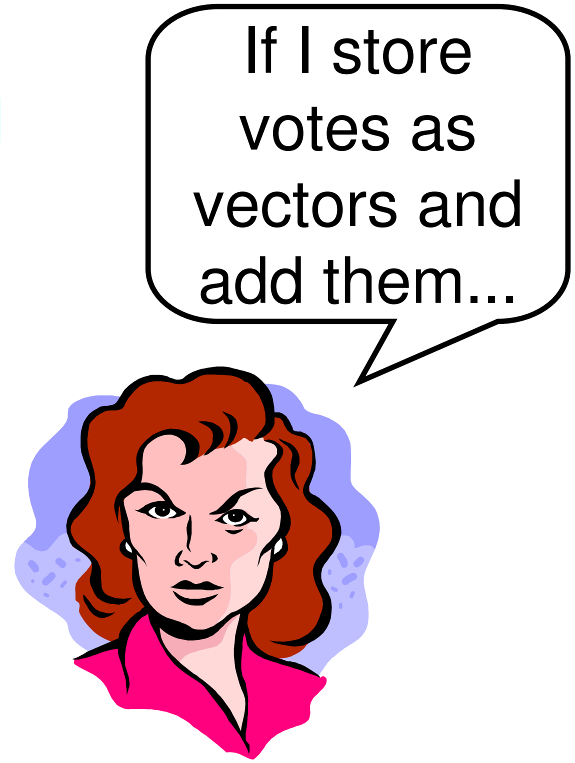
George the
Generalist

Sarah the
Specialist

Linear algebra

$$\begin{bmatrix} a & b \end{bmatrix} \begin{bmatrix} c & d \\ e & f \end{bmatrix} = \begin{bmatrix} g & h \end{bmatrix}$$

George the Generalist



Sarah the Specialist

Statements

$$\exists \vec{x}, \vec{y} \in Z_p^n \;\; \exists A, B \in Mat_{n \times n}(Z_p):$$

$$0 = xy^T \quad AB = I \quad \vec{x}A + \vec{y}B = 2\vec{x}$$

Rounds	Communication	Prover comp.	Verifier comp.
O(1)	O(n) group elements	$\omega(n^2)$ expos	$O(n^2)$ mults
O(log n)	O(n) group elements	$O(n^2)$ expos	$O(n^2)$ mults

Levels of statements

Circuit satisfiability

$$\det(B) = \pm z \quad B = \pi(A) \quad \mathrm{trace}(A) = z$$

$$0 = xy^T \quad AB = I \quad \vec{x}A + \vec{y}B = 2\vec{x}$$

$$z = \sum_{i=1}^{m} \vec{x}_i * \vec{y}_i$$

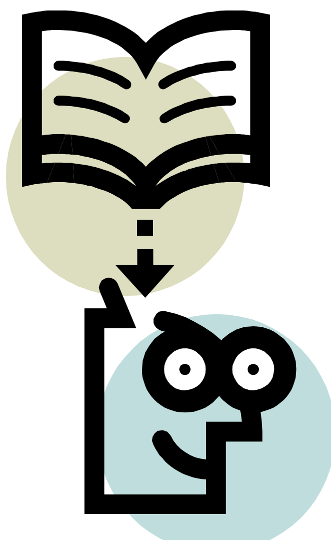
$$z = \vec{x} * \vec{y}$$

Known

Reduction 1

Circuit satisfiability

$$\det(B) = \pm z \quad B = \pi(A) \quad \mathrm{trace}(A) = z$$



See paper

Reduction 2

$$\det(B) = \pm z \quad B = \pi(A) \quad \mathrm{trace}(A) = z$$

$$0 = xy^T \quad AB = I \quad \vec{x}A + \vec{y}B = 2\vec{x}$$

Example:

$$\mathrm{trace}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{bmatrix} 1 & 1 \end{bmatrix}\left(\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \circ \begin{bmatrix} a & b \\ c & d \end{bmatrix}\right)\begin{bmatrix} 1 \\ 1 \end{bmatrix}$$

Reduction 3

$$0 = xy^T \quad AB = I \quad \vec{x}A + \vec{y}B = 2\vec{x}$$

$$z = \sum_{i=1}^{m} \vec{x}_i * \vec{y}_i$$

commit $\longrightarrow$

$s \leftarrow Z_p$

Peggy

Victor

Pedersen commitment

$$\mathrm{commit}(x_1, \ldots, x_n; r) = h^r \prod_{i=1}^{n} g_i^{x_i}$$

- Computationally binding
  - Discrete logarithm hard
- Perfectly hiding
- Only 1 group element to commit to n elements
- Only n group elements to commit to n rows of matrix

Computational soundness

Perfect zero-knowledge

Sub-linear size

Pedersen commitment

$$\text{commit}(\vec{x}\,;r) = h^r \prod_{i=1}^{n} g_i^{x_i}$$

- Homomorphic

$$\text{commit}(\vec{x};*)\text{commit}(\vec{y};*) = \text{commit}(\vec{x}+\vec{y};*)$$

- So

$$\prod_{i=1}^{m} c_i^{s^i} = \text{commit}\left(\sum_{i=1}^{m} s^i \vec{x}_i\,;*\right)$$

Example of reduction 3

$$X\vec{y}^T = \vec{0}^T$$

commit →

$s \leftarrow Z_p$ ←

$$\left(\sum_{i=1}^{n} s^i \vec{x}_i\right)\vec{y}^T = 0$$

Reduction 4

$$z = \sum_{i=1}^{m} \vec{x}_i * \vec{y}_i$$

$$z = \vec{x} * \vec{y}$$

$\xrightarrow{\text{commit}}$

$\xleftarrow{s \leftarrow Z_p}$

$$\mathrm{commit}\left(\sum_{i=1}^{m} s^{i}\vec{x}_i \,; *\right) \qquad \mathrm{commit}\left(\sum_{i=1}^{m} s^{m-i}\vec{y}_i \,; *\right)$$

Product

$$
\begin{array}{lllll}
 & s^2\vec{y}_1 \; + & s^1\vec{y}_2 \; + & s^0\vec{y}_3 & \\
s^1\vec{x}_1 & s^3\vec{x}_1 * \vec{y}_1 & s^2\vec{x}_1 * \vec{y}_2 & s^1\vec{x}_1 * \vec{y}_3 & s^1 \sum \vec{x}_i * \vec{y}_{i+2} \\
+s^2\vec{x}_2 & s^4\vec{x}_2 * \vec{y}_1 & s^3\vec{x}_2 * \vec{y}_2 & s^2\vec{x}_2 * \vec{y}_3 & s^2 \sum \vec{x}_i * \vec{y}_{i+1} \\
+s^3\vec{x}_3 & s^5\vec{x}_3 * \vec{y}_1 & s^4\vec{x}_3 * \vec{y}_2 & s^3\vec{x}_3 * \vec{y}_3 & \\
 & s^5 \sum \vec{x}_{i+2} * \vec{y}_i & s^4 \sum \vec{x}_{i+1} * \vec{y}_i & & s^3 z
\end{array}
$$

Example of reduction 4

- Statemen
- Peggy →
- Peggy ←
- New state

Soundness:
For the s^m parts to match for random s it must be that

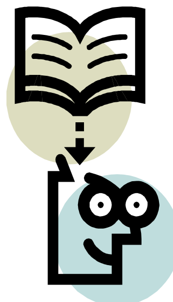
$$z = \sum_{i=1}^{m} \vec{x}_i * \vec{y}_i$$

$$\mathrm{commit}\left(\sum_{i=1}^{m} s^i \vec{x}_i ;*\right) \qquad \mathrm{commit}\left(\sum_{i=1}^{m} s^{m-i} \vec{y}_i ;*\right)$$

$$\mathrm{commit}(z;*)^{s^m} \prod_{l \neq m} \mathrm{commit}\left(\sum_{i+j=l} \vec{x}_i * \vec{y}_j ;*\right)^{s^l}$$

Reducing prover's computation

- Computing diagonal sums requires $\omega(mn)$ multiplications
- With 2log m rounds prover only uses $O(mn)$ multiplications

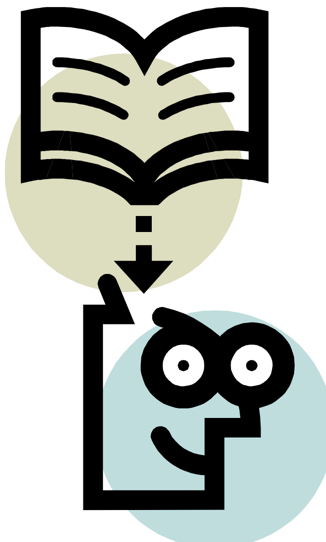


Rounds	Comm.	Prover comp.	Verifier comp.
2	2m group	m^2n mult	4m expo
2log m	2log m group	4mn mult	2m expo

Basic step

$$z = \vec{x} * \vec{y}$$

Known



Rounds	Communication	Prover comp.	Verifier comp.
3	2n elements	2n expos	n expos

Conclusion

	Rounds	Comm.	Prover comp.	Verifier comp.
$z = \vec{x} * \vec{y}$	3	2n group	2n expo	n expo
$z = \sum \vec{x}_i * \vec{y}_i$	5	2n+2m group	m^2n mult	4m+n expo
$z = \sum \vec{x}_i * \vec{y}_i$	2log m+3	2n group	4mn mult	2m+n expo
Upper triangular	6	4n group	n^3 add	5n expo
Upper triangular	2log n+4	2n group	$6n^2$ mult	3n expo
Arithmetic circuit	7	$O(\sqrt{N})$ group	$O(N\sqrt{N})$ mult	$O(N)$ mult
Arithmetic circuit	log N + 5	$O(\sqrt{N})$ group	$O(N)$ expo	$O(N)$ mult
Binary circuit	7	$O(\sqrt{N})$ group	$O(N\sqrt{N})$ add	$O(N)$ mult
Binary circuit	log N + 5	$O(\sqrt{N})$ group	$O(N)$ mult	$O(N)$ mult