Pairing-Based Non-interactive Zero-Knowledge Proofs

Jens Groth
University College London

Based on joint work with Amit Sahai

Agenda

- Motivation
  - Zero-knowledge proofs useful when designing schemes
- Modules with bilinear maps
  - Generalizes groups with pairings
- Non-interactive proofs for modules with bilinear maps
  - Witness-indistinguishable
  - Zero-knowledge in some cases
- Efficient non-interactive privacy-preserving proofs that can be used in groups with pairings

Groups with bilinear map

- $Gen(1^k)$ generates (p,G,H,T,e,g,h)
- G,H,T finite cyclic groups of order p
- Bilinear map $e: G \times H \to T$
  - $e(g^a,h^b) = e(g,h)^{ab}$
- $G = \langle g \rangle$, $H = \langle h \rangle$, $T = \langle e(g,h) \rangle$
- Deciding group membership, group operations, and bilinear map efficiently computable
- Choices:
  - Order p prime or composite, $G = H$ or $G \neq H$, etc.

Constructions in bilinear groups

$y \in \mathbf{Z}_p$
$x \in G$

$a,c \in G,\ h \in H,\ b,d \in \mathbf{Z}_p$

$t = b+yd \pmod{p}$

$t_G = x^y a^y c^t$

$t_T = e(t_G, h^b)$

Non-interactive proof for correctness

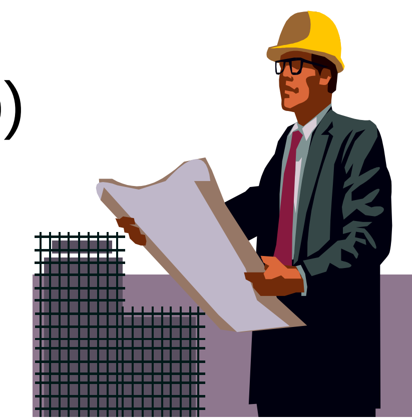
Yes, here is a proof.

Are the constructions correct? I do not know your secret x, y.

$$t = b+yd \pmod{p}$$

$$t_G = x^y a^y c^t$$

$$t_T = e(t_G, c t_G^b)$$



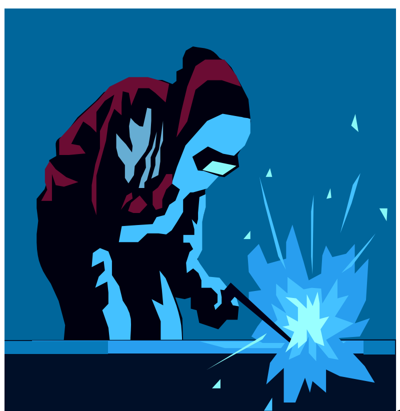
$$\pi$$

Non-interactive zero-knowledge proof

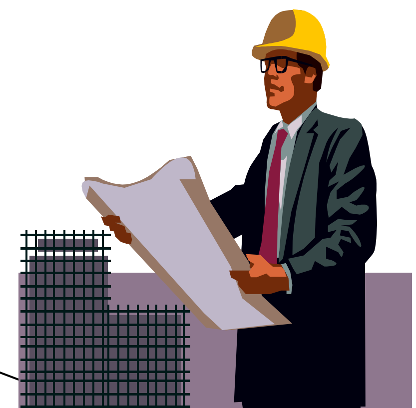
Witness for statement being true

Common reference string

Statement



Proof: π



Zero-knowledge:
Nothing but truth revealed

Soundness:
Statement is true

Verifiably encrypted signature

- ElGamal encryption of Boneh-Boyen signature

$$(h^r, y^r s) \quad \text{such that} \quad e(vg^m, s) = e(g,h)$$

- Statement: y,c,d,v,m
- Witness: r,s such that $c = h^r$, $d = y^r s$, $e(vg^m,s)=e(g,h)$
- Non-interactive zero-knowledge proof convinces verifier but keeps witness r,s private

Applications of non-interactive zero-knowledge proofs

- Verifiable encryption
- Ring signatures
- Group signatures
- Voting
- Digital credentials
- E-cash
- …

Module

- An abelian group (A,+,0) is a $\mathbf{Z}_p$-module if $\mathbf{Z}_p$ acts on A such that for all $r,s \in \mathbf{Z}_p$ $x,y \in A$:
  - $1x = x$
  - $(r+s)x = rx + sx$
  - $r(x+y) = rx + ry$
  - $(rs)x = r(sx)$
- If p is a prime, then A is a vector space
- Examples:

  $\mathbf{Z}_p$, G, H, T, G^2, H^2, T^4 are $\mathbf{Z}_p$-modules

Modules with bilinear map

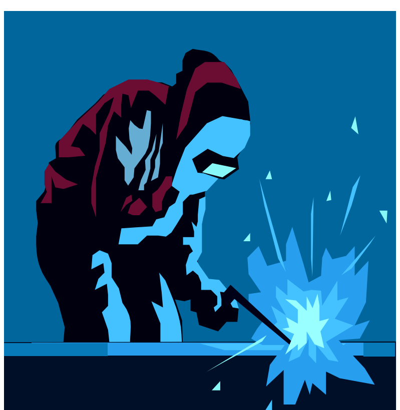
- We will be interested in finite $\mathbf{Z}_p$-modules A, B, T with a bilinear map f: $A \times B \to T$
- Examples:
  - e: $G \times H \to T$ $\quad (x,y) \to e(x,y)$
  - exp: $G \times \mathbf{Z}_p \to G$ $\quad (x,y) \to x^y$
  - exp: $\mathbf{Z}_p \times H \to H$ $\quad (x,y) \to y^x$
  - mult: $\mathbf{Z}_p \times \mathbf{Z}_p \to \mathbf{Z}_p$ $\quad (x,y) \to xy \pmod p$

Equations in modules with bilinear map

- Given $f: A \times B \to T$ we are interested in equations

$$\sum f(a_j,y_j) + \sum f(x_i,b_i) + \sum m_{ij} f(x_i,y_j) = t$$

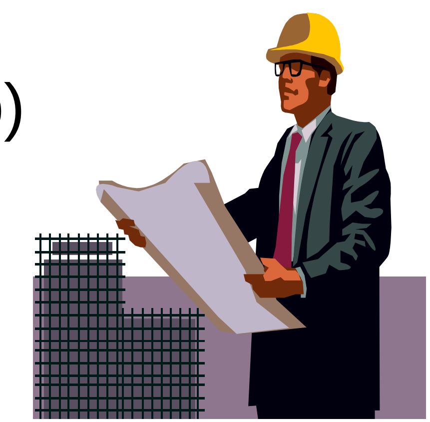
- Examples



$t = b+yd \pmod{p}$

$t_G = x^y a^y c^t$

$t_T = e(t_G, c t_G{}^b)$



Equations in modules with bilinear map

- Given $f: A \times B \rightarrow T$ we are interested in equations

$$\sum f(a_j, y_j) + \sum f(x_i, b_i) + \sum m_{ij} f(x_i, y_j) = t$$

- Define $\mathbf{x} \cdot \mathbf{y} = \sum f(x_i, y_i)$
- Rewrite equations as

$$\mathbf{a} \cdot \mathbf{y} + \mathbf{x} \cdot \mathbf{b} + \mathbf{x} \cdot M\mathbf{y} = t$$

Statements and witnesses

- Setup: (p, A, B, T, f)
- Statement: N equations of the form $(\mathbf{a}_i, \mathbf{b}_i, M_i, t_i)$ with the claim that there exists $\mathbf{x}$, $\mathbf{y}$ such that for all i:

$$\mathbf{a}_i \cdot \mathbf{y} + \mathbf{x} \cdot \mathbf{b}_i + \mathbf{x} \cdot M_i\mathbf{y} = t_i$$

- Witness: $\mathbf{x} \in A^m$, $\mathbf{y} \in B^n$ that satisfy all equations

Non-interactive proofs

- Common reference string: $K(p,A,B,T,f) \rightarrow \sigma$
- Prover: $P(\sigma,\{(\mathbf{a}_i,\mathbf{b}_i,M_i,t_i)\}_i,\mathbf{x},\mathbf{y}) \rightarrow \pi$
- Verifier: $V(\sigma,\{(\mathbf{a}_i,\mathbf{b}_i,M_i,t_i)\}_i,\pi) \rightarrow$ accept/reject

- Completeness:
  Given witness $\mathbf{x}$,$\mathbf{y}$ for simultaneous satisfiability of equations the prover outputs accepting proof π
- Soundness:
  If statement is false, i.e., no such $\mathbf{x}$,$\mathbf{y}$ exists, then impossible to construct accepting π

Privacy

- Zero-knowledge:
  Proof π reveals nothing about **x**, **y**
- Witness-indistinguishability:
  Proof π does not reveal which witness **x**, **y** out of many possible witnesses was used

- Zero-knowledge implies witness-indistinguishability
- Witness-indistinguishability weaker than ZK
  - May leak partial information (e.g. all witnesses have $x_1 = 0$)
  - May leak entire witness when only one witness exists

Witness-indistinguishability

- Simulated common reference string: $S(p,A,B,T,f) \rightarrow \sigma$
  – Computationally indistinguishable from real CRS
- On simulated common reference string σ:
  – Given any satisfiable statement $\{(\mathbf{a}_i,\mathbf{b}_i,M_i,t_i)\}_i$ and any two possible witnesses $\mathbf{x}_0,\mathbf{y}_0$ or $\mathbf{x}_1,\mathbf{y}_1$ the proofs using either witness have identical probability distributions

$$
\begin{aligned}
& \{ P(\sigma,\{(\mathbf{a}_i,\mathbf{b}_i,M_i,t_i)\}_i,\mathbf{x}_0,\mathbf{y}_0) \rightarrow \pi \} \\
= \quad & \{ P(\sigma,\{(\mathbf{a}_i,\mathbf{b}_i,M_i,t_i)\}_i,\mathbf{x}_1,\mathbf{y}_1) \rightarrow \pi \}
\end{aligned}
$$

Modules and maps defined by setup and CRS

- Modules with linear and bilinear maps

$$\begin{array}{ccccc} A & \times & B & \xrightarrow{f} & T \\ i_C \downarrow\uparrow p_A & & i_D \downarrow\uparrow p_B & & i_W \downarrow\uparrow p_T \\ C & \times & D & \xrightarrow[F]{} & W \end{array}$$

- Non-trivial: $p_A(i_C(x)) = x$, $p_B(i_D(y)) = y$, $p_T(i_W(z)) = z$
- Commutative:

$$F(i_C(x),i_D(y)) = i_W(f(x,y))$$
$$f(p_A(c),p_B(d)) = p_T(F(c,d))$$

A simple equation

- Want to prove $\exists x \in A\ \exists y \in B$: $f(x,y) = t$
- The prover computes $c = i_C(x)$ and $d = i_D(y)$
- The verifier checks $F(c,d) = i_W(t)$

- Completeness:

$$
\begin{array}{ccccc}
x & , & y & \xrightarrow{f} & t \\
i_C \downarrow & & i_D \downarrow & & i_W \downarrow \\
i_C(x) & , & i_D(y) & \xrightarrow[F]{} & i_W(t)
\end{array}
$$

Soundness

- Soundness:

$$
\begin{tikzcd}
p_A(c) & , & p_B(d) \arrow[r, "f"] & t \\
c \arrow[u, "p_A"'] & , & d \arrow[u, "p_B"'] \arrow[r, "F"'] & i_W(t) \arrow[u, "p_T"']
\end{tikzcd}
$$

- Given proof c,d define $x = p_A(c)$ and $y = p_B(d)$ to get a solution to the equation $f(x,y) = t$

Sets of equations

- Define $i_C(\mathbf{x}) = (i_C(x_1),\ldots,i_C(x_m))$ similar for $i_D(\mathbf{y})$
- Define $p_A(\mathbf{c}) = (p_A(c_1),\ldots,p_A(c_n))$ similar for $p_B(\mathbf{d})$
- Define $\mathbf{c} \bullet \mathbf{d} = F(c_1,d_1)+\ldots+F(c_n,d_n)$

- Want to prove $\exists \mathbf{x} \in A^m \ \exists \mathbf{y} \in B^n$ satisfying N equations of the form $\mathbf{a} \cdot \mathbf{y} + \mathbf{x} \cdot \mathbf{b} + \mathbf{x} \cdot M\mathbf{y} = t$
- Prover with $\mathbf{x},\mathbf{y}$ can compute $\mathbf{c} = i_C(\mathbf{x})$, $\mathbf{d} = i_D(\mathbf{y})$
- Verifier checks for each equation

$$i_C(\mathbf{a}) \bullet \mathbf{d} + \mathbf{c} \bullet i_D(\mathbf{b}) + \mathbf{c} \bullet M\mathbf{d} = i_W(t)$$

Completeness and soundness

$$
\begin{array}{ccccccc}
\mathbf{a}, \mathbf{x} & & \mathbf{b}, \mathbf{y} & \cdot & t \\
A & \times & B & \to & T \\
i_C \downarrow\uparrow p_A & & i_D \downarrow\uparrow p_B & & i_W \downarrow\uparrow p_T \\
C & \times & D & \to & W \\
i_C(\mathbf{a}), \mathbf{c} & & i_D(\mathbf{b}), \mathbf{d} & \bullet & i_W(t)
\end{array}
$$

- Completeness comes from linearity, bilinearity and the commutative property $F(i_C(x),i_D(y)) = i_W(f(x,y))$
- Soundness comes from linearity, bilinearity, non-triviality $p_A(i_C(a)) = a$, $p_B(i_D(b)) = b$, $p_T(i_W(t)) = t$ and the commutative property $f(p_A(c),p_B(d)) = p_T(F(c,d))$

Example

- Modules with linear and bilinear maps

$$\begin{array}{ccccccc} & x & & y & e & t & \\ & G & \times & H & \rightarrow & T & \\ i_C \downarrow\uparrow p_A & & i_D \downarrow\uparrow p_B & & i_W \downarrow\uparrow p_T & & \\ & G^2 & \times & H^2 & \rightarrow & T^4 & \\ & (1,x) & & (1,y) & E & (1,1,1,t) & \end{array}$$

- $p_A(c,x) = c^{-\alpha}x$, $p_B(d,y) = d^{-\beta}y$, $p_T(u,v,w,t) = u^{-\alpha\beta}v^{-\alpha}w^{-\beta}t$
- $E((c,x),(d,y)) = (e(c,d),e(c,y),e(x,d),e(x,y))$
- Commutative:

$$E(i_C(x),i_D(y)) = i_W(e(x,y))$$
$$e(p_A(c,x),p_B(d,y)) = p_T(E((c,x),(d,y)))$$

Witness-indistinguishable?

- The example has no privacy at all
- Given $i_C(\mathbf{x}) = ((1,x_1),\ldots,(1,x_m))$ and $i_D(\mathbf{y}) = ((1,y_1),\ldots,(1,y_n))$ easy to compute $\mathbf{x}$, $\mathbf{y}$

- What if in the general case i_A, i_B, i_W are one-way functions and p_A, p_B, p_T are hard to compute?
- Still not witness-indistinguishable
- Given two witnesses $(\mathbf{x}_0, \mathbf{y}_0)$ and $(\mathbf{x}_1,\mathbf{y}_1)$ it is easy to test whether $i_C(\mathbf{x}) = i_C(\mathbf{x}_0)$ and $i_D(\mathbf{y}) = i_D(\mathbf{y}_0)$

Randomization

- No deterministic witness-indistinguishable proofs
- Need to randomize the maps $\mathbf{x} \to \mathbf{c}$, $\mathbf{y} \to \mathbf{d}$

- Common reference string: $\mathbf{u} \in C^{\underline{m}}$, $\mathbf{v} \in D^{\underline{n}}$
such that $p_A(\mathbf{u}) = \mathbf{0}$ and $p_B(\mathbf{v}) = \mathbf{0}$
- Compute $\mathbf{c} = i_C(\mathbf{x}) + R\mathbf{u}$ and $\mathbf{d} = i_D(\mathbf{y}) + S\mathbf{v}$
with random $R \leftarrow \mathrm{Mat}_{m \times \underline{m}}(\mathbf{Z}_p)$, $S \leftarrow \mathrm{Mat}_{n \times \underline{n}}(\mathbf{Z}_p)$
- Observe: $p_A(\mathbf{c}) = p_A(i_C(\mathbf{x})+R\mathbf{u}) = p_A(i_C(\mathbf{x})) = \mathbf{x}$

- Example:If $u = (g,g^{\alpha})$ then $c = i_C(x)u^r = (g^r,g^{\alpha r}x)$

Soundness

- Common reference string: $\mathbf{u} \in C^{\underline{m}}$, $\mathbf{v} \in D^{\underline{n}}$ such that $p_A(\mathbf{u}) = \mathbf{0}$ and $p_B(\mathbf{v}) = \mathbf{0}$
- Compute $\mathbf{c} = i_C(\mathbf{x}) + R\mathbf{u}$ and $\mathbf{d} = i_D(\mathbf{y}) + S\mathbf{v}$
- For each equations $\mathbf{a} \cdot \mathbf{y} + \mathbf{x} \cdot \mathbf{b} + \mathbf{x} \cdot M\mathbf{y} = t$ somehow (next slide) compute proof $\boldsymbol{\pi} \in D^{\underline{m}}$, $\boldsymbol{\phi} \in C^{\underline{n}}$
- Verifier checks $i_C(\mathbf{a}) \bullet \mathbf{d} + \mathbf{c} \bullet i_D(\mathbf{b}) + \mathbf{c} \bullet M\mathbf{d} = i_W(t) + \mathbf{u} \bullet \boldsymbol{\pi} + \boldsymbol{\phi} \bullet \mathbf{v}$
- Soundness – apply projections to get $\mathbf{a} \cdot p_B(\mathbf{d}) + p_A(\mathbf{c}) \cdot \mathbf{b} + p_A(\mathbf{c}) \cdot Mp_B(\mathbf{d}) = t + 0 + 0$
- So $\mathbf{x} = p_A(\mathbf{c})$ and $\mathbf{y} = p_B(\mathbf{d})$ satisfies all equations

Completeness

- Common reference string: $\mathbf{u} \in C^{\underline{m}}$, $\mathbf{v} \in D^{\underline{n}}$
- Compute $\mathbf{c} = i_C(\mathbf{x}) + R\mathbf{u}$ and $\mathbf{d} = i_D(\mathbf{y}) + S\mathbf{v}$ with random $R \leftarrow Mat_{m \times \underline{m}}(\mathbf{Z}_p)$, $S \leftarrow Mat_{n \times \underline{n}}(\mathbf{Z}_p)$
- For each equations $\mathbf{a} \cdot \mathbf{y} + \mathbf{x} \cdot \mathbf{b} + \mathbf{x} \cdot M\mathbf{y} = t$ can use proof $\phi = S^T i_C(\mathbf{a}) + S^T M^T (i_C(\mathbf{x}) + R\mathbf{u})$, $\pi = R^T i_D(\mathbf{b}) + R^T M i_D(\mathbf{y})$
- Verification always works when $\mathbf{x}$, $\mathbf{y}$ satisfy equations

$$
\begin{aligned}
& i_C(\mathbf{a}) \bullet \mathbf{d} + \mathbf{c} \bullet i_D(\mathbf{b}) + \mathbf{c} \bullet M\mathbf{d} \\
&= i_C(\mathbf{a}) \bullet (i_D(\mathbf{y}) + S\mathbf{v}) + (i_C(\mathbf{x}) + R\mathbf{u}) \bullet i_D(\mathbf{b}) + (i_C(\mathbf{x}) + R\mathbf{u}) \bullet M(i_D(\mathbf{y}) + S\mathbf{v}) \\
&= i_W(t) + \phi \bullet \mathbf{v} + \mathbf{u} \bullet \pi
\end{aligned}
$$

Witness-indistinguishability

- Simulated common reference string hard to distinguish from real common reference string
- Simulated common reference string: $\mathbf{u} \in C^{\underline{m}}$, $\mathbf{v} \in D^{\underline{n}}$ such that $C = \langle u_1,\ldots,u_{\underline{m}} \rangle$ and $D = \langle v_1,\ldots,v_{\underline{n}} \rangle$
- Compute $\mathbf{c} = i_C(\mathbf{x}) + R\mathbf{u}$ and $\mathbf{d} = i_D(\mathbf{y}) + S\mathbf{v}$ with random $R \leftarrow Mat_{m \times \underline{m}}(\mathbf{Z}_p)$, $S \leftarrow Mat_{n \times \underline{n}}(\mathbf{Z}_p)$
- On simulated common reference string **c** and **d** are perfectly hiding **x**, **y**
- Indeed, for any **x**, **y** we get uniformly random **c**, **d**

Example

- Common reference string includes
  $u_1 = (g, g^{\alpha})$, $u_2 = (g^{\rho}, g^{\alpha\rho+\delta})$, $v_1 = (h, h^{\beta})$, $v_2 = (h^{\sigma}, h^{\beta\sigma+\varepsilon})$
  - Real CRS: $\delta = 0$, $\varepsilon = 0$
  - Simulated CRS: $\delta \neq 0$, $\varepsilon \neq 0$
  - Indistinguishable: DDH in both G and H
- To commit to x pick $(r_1, r_2) \leftarrow Mat_{1\times 2}(\mathbf{Z}_p)$ and set
  $c = (c_1, c_2) = i_C(x) u_1^{r_1} u_2^{r_2} = (1, x)\,(g, g^{\alpha})^{r_1}\,(g^{\rho}, g^{\alpha\rho+\delta})^{r_2}$
  $= (g^{r_1+\rho r_2}, g^{\alpha(r_1+\rho r_2)} g^{\delta r_2} x)$
- On real CRS we get ElGamal encryption of x
  - $p_A(c) = c_1^{-\alpha} c_2 = x$ when $\delta = 0$
- On simulated CRS perfectly hiding x
  - $c = (c_1, c_2)$ random since u_1, u_2 linearly independent

Witness-indistinguishability

- The commitments **c** and **d** do not reveal **x** and **y** when using a simulated common reference string
- But maybe the proofs π, ϕ reveal something
- Let us therefore randomize the proofs as well
- For each equation we will pick π, ϕ uniformly at random among solutions to verification equation $i_C(\mathbf{a}) \bullet \mathbf{d} + \mathbf{c} \bullet i_D(\mathbf{b}) + \mathbf{c} \bullet M\mathbf{d} = i_W(t) + \mathbf{u} \bullet \pi + \phi \bullet \mathbf{v}$
- Given witness $\mathbf{x}_0$, $\mathbf{y}_0$ or $\mathbf{x}_1$, $\mathbf{y}_1$ we have uniformly random **c**, **d** and for each equation independent and uniformly random proofs π,ϕ

Randomizing the proofs

- Given $\mathbf{u},\mathbf{v},\mathbf{c},\mathbf{d}$ and a proof π,ϕ such that
  $i_C(\mathbf{a})\bullet\mathbf{d} + \mathbf{c}\bullet i_D(\mathbf{b}) + \mathbf{c}\bullet M\mathbf{d} = i_W(t) + \mathbf{u}\bullet\pi + \phi\bullet\mathbf{v}$
- Then there are other possible proofs
  $i_C(\mathbf{a})\bullet\mathbf{d} + \mathbf{c}\bullet i_D(\mathbf{b}) + \mathbf{c}\bullet M\mathbf{d} = i_W(t) + \mathbf{u}\bullet(\pi-\mathbf{v}) + (\phi+\mathbf{u})\bullet\mathbf{v}$
- More generally for any $T\in \mathrm{Mat}_{\underline{n}\times\underline{m}}(\mathbf{Z}_p)$
  $i_C(\mathbf{a})\bullet\mathbf{d}+\mathbf{c}\bullet i_D(\mathbf{b})+\mathbf{c}\bullet M\mathbf{d} = i_W(t) + \mathbf{u}\bullet(\pi-T^T\mathbf{v}) + (\phi+T\mathbf{u})\bullet\mathbf{v}$
- We may also have $H\in \mathrm{Mat}_{\underline{m}\times\underline{n}}(\mathbf{Z}_p)$ such that $\mathbf{u}\bullet H\mathbf{v} = 0$
- Then we have
  $i_C(\mathbf{a})\bullet\mathbf{d}+\mathbf{c}\bullet i_D(\mathbf{b})+\mathbf{c}\bullet M\mathbf{d} = i_W(t) + \mathbf{u}\bullet(\pi+H\mathbf{v}) + \phi\bullet\mathbf{v}$

Randomizing the proofs

- Given $\mathbf{u},\mathbf{v},\mathbf{c},\mathbf{d}$ and for each equation $\boldsymbol{\pi},\boldsymbol{\phi}$ such that

  $$i_C(\mathbf{a})\bullet\mathbf{d} + \mathbf{c}\bullet i_D(\mathbf{b}) + \mathbf{c}\bullet M\mathbf{d} = i_W(t) + \mathbf{u}\bullet\boldsymbol{\pi} + \boldsymbol{\phi}\bullet\mathbf{v}$$

- Randomize each proof $\boldsymbol{\pi},\boldsymbol{\phi}$ as

  $$\boldsymbol{\pi}' = \boldsymbol{\pi} - T^T\mathbf{v} + H\mathbf{v} \qquad \boldsymbol{\phi}' = \boldsymbol{\phi} + T\mathbf{u}$$

- T is chosen at random from $Mat_{\underline{n}\times\underline{m}}(\mathbf{Z}_p)$
- H chosen at random in $Mat_{\underline{m}\times\underline{n}}(\mathbf{Z}_p)$ such that $\mathbf{u}\bullet H\mathbf{v}=0$
- We still have correct verification for each equation

  $i_W(t) + \mathbf{u}\bullet\boldsymbol{\pi}' + \boldsymbol{\phi}\bullet\mathbf{v}' = i_W(t) + \mathbf{u}\bullet(\boldsymbol{\pi}-T^T\mathbf{v}+H\mathbf{v}) + (\boldsymbol{\phi}+T\mathbf{u})\bullet\mathbf{v}$

  $= i_W(t) + \mathbf{u}\bullet\boldsymbol{\pi} + \mathbf{u}\bullet\mathbf{v} = i_C(\mathbf{a})\bullet\mathbf{d} + \mathbf{c}\bullet i_D(\mathbf{b}) + \mathbf{c}\bullet M\mathbf{d}$

Witness-indistinguishability

- On simulation common reference string we now have perfect witness-indistinguishability; given $\mathbf{x}_0$, $\mathbf{y}_0$ or $\mathbf{x}_1$, $\mathbf{y}_1$ satisfying the equations we get the same distribution of commitments **c**, **d** and proofs
- Actually, every **x**, **y** satisfying all equations gives uniform random distribution on **c**, **d** and proofs
- Proof:
  – We already know **c**, **d** are uniformly random
  – For each equation $\boldsymbol{\phi}' = \boldsymbol{\phi} + T\mathbf{u}$ random since $C = \langle \mathbf{u} \rangle$
  – For each equation $\boldsymbol{\pi}' = \boldsymbol{\pi} - T^T\mathbf{v} + H\mathbf{v}$ uniformly random over $\boldsymbol{\pi}'$ satisfying $i_C(\mathbf{a})\bullet\mathbf{d}+\mathbf{c}\bullet i_D(\mathbf{b})+\mathbf{c}\bullet M\mathbf{d}=i_W(t)+\mathbf{u}\bullet\boldsymbol{\pi}'+\boldsymbol{\phi}'\bullet\mathbf{v}$ due to H uniformly random over $\mathbf{u}\bullet H\mathbf{v}=0$ and $D = \langle \mathbf{v} \rangle$

The setup and common reference string

- Setup and common reference string describes non-trivial linear and bilinear maps that commute

$$
\begin{array}{ccccc}
A & \times & B & \xrightarrow{f} & T \\
i_C \downarrow\uparrow p_A & & i_D \downarrow\uparrow p_B & & i_W \downarrow\uparrow p_T \\
C & \times & D & \xrightarrow[F]{} & W
\end{array}
$$

- Common reference string also describes **u**, **v**
- Real CRS: $p_A(\mathbf{u}) = \mathbf{0}$, $p_B(\mathbf{v}) = \mathbf{0}$
- Simulated CRS: $C = \langle \mathbf{u} \rangle$, $D = \langle \mathbf{v} \rangle$

The proof system

- Statement: N equations of the form

$$\mathbf{a} \cdot \mathbf{y} + \mathbf{x} \cdot \mathbf{b} + \mathbf{x} \cdot M\mathbf{y} = t$$

- Witness: $\mathbf{x}$, $\mathbf{y}$ satisfying all N equations
- Proof: $\mathbf{c} = i_C(\mathbf{x}) + R\mathbf{u}$ and $\mathbf{d} = i_D(\mathbf{y}) + S\mathbf{v}$

  For each equation $\mathbf{a} \cdot \mathbf{y} + \mathbf{x} \cdot \mathbf{b} + \mathbf{x} \cdot M\mathbf{y} = t$

  set $\boldsymbol{\phi} = S^T i_C(\mathbf{a}) + S^T M^T (i_C(\mathbf{x}) + R\mathbf{u}) + T\mathbf{u}$

  and $\boldsymbol{\pi} = R^T i_D(\mathbf{b}) + R^T M i_D(\mathbf{y}) - T^T\mathbf{v} + H\mathbf{v}$
- Verification: For each eq. $\mathbf{a} \cdot \mathbf{y} + \mathbf{x} \cdot \mathbf{b} + \mathbf{x} \cdot M\mathbf{y} = t$

  check $i_C(\mathbf{a}) \bullet \mathbf{d} + \mathbf{c} \bullet i_D(\mathbf{b}) + \mathbf{c} \bullet M\mathbf{d} = i_W(t) + \mathbf{u} \bullet \boldsymbol{\pi} + \boldsymbol{\phi} \bullet \mathbf{v}$

Size of NIWI proofs

Each equation constant cost.
independently of number of public constants and secret variables.
NIWI proofs can have sub-linear size compared to statement!

Cost of each variable/equation	Subgroup Decision	DDH in both groups	Decision Linear
Variable in G, H or $\mathbf{Z}_p$	1	2	3
Pairing product	1	8	9
Multi-exponentiation	1	6	9
Quadratic in $\mathbf{Z}_p$	1	4	6

Zero-knowledge

- Are the NIWI proofs also zero-knowledge?
- Proof is zero-knowledge if there is a simulator that given the statement can simulate a proof
- Problem: The simulator does not know a witness
- Zero-knowledge in special case where all N equations are of the form $\mathbf{a} \cdot \mathbf{y} + \mathbf{x} \cdot \mathbf{b} + \mathbf{x} \cdot M\mathbf{y} = 0$
- Now the simulator can use $\mathbf{x} = \mathbf{0}$, $\mathbf{y} = \mathbf{0}$ as witness

A more interesting special case

- If $A = \mathbf{Z}_p$ and $T = B$ then possible to rewrite
$$\mathbf{a} \cdot \mathbf{y} + \mathbf{x} \cdot \mathbf{b} + \mathbf{x} \cdot M\mathbf{y} = t$$
as
$$\mathbf{a} \cdot \mathbf{y} + (-1)\cdot t + \mathbf{x} \cdot \mathbf{b} + \mathbf{x} \cdot M\mathbf{y} = 0$$
- Using $c_0 = i_C(-1) + 0\mathbf{u}$ as a commitment to $x_0 = -1$ we can give NIWI proofs with witness $(x_0,\mathbf{x}),\mathbf{y}$
- Soundness on a real CRS shows that for each equation we have
$$\mathbf{a} \cdot \mathbf{y} - 1\cdot t + \mathbf{x} \cdot \mathbf{b} + \mathbf{x} \cdot M\mathbf{y} = 0$$

A more interesting special case

- Simulated CRS generation:
  Setup CRS such that $i_C(-1) = i_C(0) + \boldsymbol{\tau}^T\mathbf{u}$ for $\boldsymbol{\tau} \in \mathbf{Z}_p^m$
- Simulating proofs:
  Give NIWI proofs for equations of the form
  $$\mathbf{a} \cdot \mathbf{y} - x_0 \cdot t + \mathbf{x} \cdot \mathbf{b} + \mathbf{x} \cdot M\mathbf{y} = 0$$
- In NIWI proofs interpret $c_0 = i_C(0) + \boldsymbol{\tau}^T\mathbf{u}$ as a commitment to $x_0 = 0$, which enables the prover to use the witness $\mathbf{x} = \mathbf{0}$, $\mathbf{y} = \mathbf{0}$ in all equations
- Zero-knowledge:
  Simulated proofs using $x_0 = 0$ are uniformly distributed just as real proofs using $x_0 = -1$ are

Size of NIZK proofs

Cost of each variable/equation	Subgroup Decision	DDH in both groups	Decision Linear
Variable in G, H or $\mathbf{Z}_p$	1	2	3
Pairing product (t=1)	1	8	9
Multi-exponentiation	1	6	9
Quadratic in $\mathbf{Z}_p$	1	4	6

Summary

- Modules with commuting linear and bilinear maps

$$\begin{array}{ccccc} A & \times & B & \xrightarrow{f} & T \\ i_C \downarrow\uparrow p_A & & i_D \downarrow\uparrow p_B & & i_W \downarrow\uparrow p_T \\ C & \times & D & \xrightarrow[F]{} & W \end{array}$$

  Randomized commitments and proofs in C, D
- Efficient NIWI and NIZK proofs that can be used when constructing pairing-based schemes

Open problems

- Modules with bilinear maps useful elsewhere?
  - Groups: Simplicity, possible to use special properties
  - Modules: Generality, many assumptions at once
  - What is the right level of abstraction?
- Other instantiations of modules with bilinear map?
  - Known constructions based on groups with bilinear map
  - Other ways to construct them?