Succinct Diophantine-Satisfiability Arguments

Patrick Towa[1,*] and Damien Vergnaud[2,3]

1: ETH zürich

2: institut universitaire de France

3: SORBONNE UNIVERSITÉ

* Work done while at IBM Research – Zurich and ENS and PSL Research University

Diophantine Equations

Multivariate polynomial equations with

- coefficients in $\mathbb{Z}$
- solutions in $\mathbb{Z}$

$$\sum_{\boldsymbol{i} \in \mathbb{N}^\nu} \underbrace{a_{\boldsymbol{i}}}_{= 0 \text{ for all but finitely many } \boldsymbol{i}} x_1^{i_1} \cdots x_\nu^{i_\nu} = 0$$

Diophantine Equations

Multivariate polynomial equations with

- coefficients in $\mathbb{Z}$
- solutions in $\mathbb{Z}$

$$\sum_{\boldsymbol{i} \in \mathbb{N}^{\nu}} \underbrace{a_{\boldsymbol{i}}}_{= 0 \text{ for all but finitely many } \boldsymbol{i}} x_1^{i_1} \cdots x_{\nu}^{i_{\nu}} = 0$$

DPRM Theorem [1970]: satisfiability of Diophantine equations is undecidable
(negative answer to Hilbert's tenth problem)

Diophantine Equations – Relevance

Problems that can be encoded as Diophantine equations:

- Circuit–SAT, 3–SAT
- Graph coloring
- Hamiltonian cycle
- ILP

Diophantine Equations – Relevance

Problems that can be encoded as Diophantine equations:

- Circuit–SAT, 3–SAT
- Graph coloring
- Hamiltonian cycle
- ILP

- Proving knowledge of
  - RSA signatures $(x^e - k\,N\, - y = 0)$
  - (EC)DSA signatures
- Verifiable shuffling of two lists $(x_i)_i$ and (y_i)
  $\boldsymbol{y} = \boldsymbol{U}\,\boldsymbol{x},$ with $\boldsymbol{U}$ a permutation matrix

- Many more…

Arguments for NP in $\mathbb{Z}_p$ vs $\mathbb{Z}$

- Solutions to certain problems (e.g. ILP) may not be a priori bounded

Arguments for NP in $\mathbb{Z}_p$ vs $\mathbb{Z}$

- Solutions to certain problems (e.g. ILP) may not be a priori bounded

- Most problems can be naturally encoded as Diophantine equations

  $\Rightarrow$ no overheard from the reduction to an NP-complete problem

Hidden-Order Groups

- Used to argue over integers
- Typically Z_N^* for $N = pq$ or ideal-class groups
- Assumptions: $\approx$ strong RSA; difficult to compute small-order elements (except for elements of order 2)

Integer Commitments

Pedersen

$G = < g >$ of public prime order p

Damgård and Fujisaki

G of hidden order $\leq 2^{b_G}$

Integer Commitments

Pedersen

$G = < g >$ of public prime order p

$h \leftarrow_\$ G^*$

Damgård and Fujisaki

G of hidden order $\leq 2^{b_G}$

$h \leftarrow_\$ G;\ \alpha \leftarrow_\$ [0; 2^{b_G+\lambda}]; g \leftarrow h^\alpha$

$g \in < h >$ crucial for Hiding

Integer Commitments

Pedersen

$G = < g >$ of public prime order p

$h \leftarrow_{\$} G^*$

To commit to $x \in \mathbb{Z}_p$: $C \leftarrow g^x h^r$ for $r \leftarrow_{\$} \mathbb{Z}_p$

Damgård and Fujisaki

G of hidden order $\leq 2^{b_G}$

$h \leftarrow_{\$} G;\ \alpha \leftarrow_{\$} [0; 2^{b_G+\lambda}]; g \leftarrow h^{\alpha}$

To commit to $x \in \mathbb{Z}$: $C \leftarrow g^x h^r$ for $r \leftarrow_{\$} [0; 2^{b_G+\lambda}]$

Integer Commitments

Pedersen

$G = < g >$ of public prime order p

$h \leftarrow_{\$} G^*$

To commit to $x \in \mathbb{Z}_p$: $C \leftarrow g^x h^r$ for $r \leftarrow_{\$} \mathbb{Z}_p$

To open C with (x, r): $C = g^x h^x$?

Damgård and Fujisaki

G of hidden order $\leq 2^{b_G}$

$h \leftarrow_{\$} G;\ \alpha \leftarrow_{\$} [0; 2^{b_G+\lambda}]; g \leftarrow h^\alpha$

To commit to $x \in \mathbb{Z}$: $C \leftarrow g^x h^r$ for $r \leftarrow_{\$} [0; 2^{b_G+\lambda}]$

To open C with (x, r): $C^2 = (g^x h^r)^2$?

To allow for efficient proofs of knowledge of openings

Integer Commitments

Damgård and Fujisaki

G of hidden order $\leq 2^{b_G}$

$$h \leftarrow_\$ G;\ \alpha \leftarrow_\$ [0; 2^{b_G+\lambda}]; g \leftarrow h^\alpha$$

Proof on the parameters with $\{0,1\}$ as challenge space ⇒ size $\Omega(b_G \log^2 \lambda)$ bits

New Scheme

G of hidden order $\leq 2^{b_G}$

$$h \leftarrow_\$ G;\ \alpha \leftarrow_\$ [0; 2^{b_G+\lambda}]; g \leftarrow h^\alpha$$

Proof on the parameters with $[0; \lambda^{\log \lambda}]$ as challenge space ⇒ size $O(b_G)$ bits

Only guarantees that $g^2 \in < h^2 >$

Integer Commitments

Damgård and Fujisaki

G of hidden order $\leq 2^{b_G}$

$h \leftarrow_\$ G;\ \alpha \leftarrow_\$ [0; 2^{b_G+\lambda}]; g \leftarrow h^\alpha$

Proof on the parameters with $\{0,1\}$ as challenge space $\Rightarrow$ size $\Omega(b_G \log^2 \lambda)$ bits

For n integers, $\Omega(n b_G \log^2 \lambda)$

New Scheme

G of hidden order $\leq 2^{b_G}$

$h \leftarrow_\$ G;\ \alpha \leftarrow_\$ [0; 2^{b_G+\lambda}]; g \leftarrow h^\alpha$

Proof on the parameters with $[0; \lambda^{\log \lambda}]$ as challenge space $\Rightarrow$ size $O(b_G)$ bits

Only guarantees that $g^2 \in <h^2>$

For n integers, $O(b_G + \log n)$

Integer Commitments

Damgård and Fujisaki

G of hidden order $\leq 2^{b_G}$

$h \leftarrow_{\$} G;\ \alpha \leftarrow_{\$} [0; 2^{b_G+\lambda}]; g \leftarrow h^{\alpha}$

To commit to $x \in \mathbb{Z}$: $C \leftarrow g^x h^r$ for $r \leftarrow_{\$} [0; 2^{b_G+\lambda}]$

To open C with (x, r): $C^2 = (g^x h^r)^2$?

New Scheme

G of hidden order $\leq 2^{b_G}$

$h \leftarrow_{\$} G;\ \alpha \leftarrow_{\$} [0; 2^{b_G+\lambda}]; g \leftarrow h^{\alpha}$

To commit to $x \in \mathbb{Z}$: $C \leftarrow (g^x h^r)^2$ for $r \leftarrow_{\$} [0; 2^{b_G+\lambda}]$

To open C with (x, r): $C^2 = (g^x h^r)^4$?

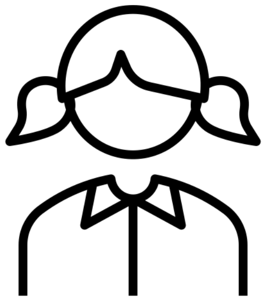
Arguing Knowledge of Dlogs in Hidden-Order Groups

$G = \langle g \rangle$ of hidden order $\leq 2^{b_G}$

$g = h^{\alpha}$

$k \leftarrow_{\$} ?$

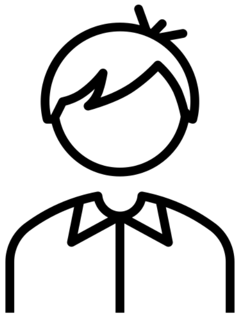
$t \leftarrow h^{k}$



t →

← c

r →



$c \leftarrow ?$

$r \leftarrow k - c\,\alpha$

(over $\mathbb{Z}$)

$h^{r} g^{c} = t?$

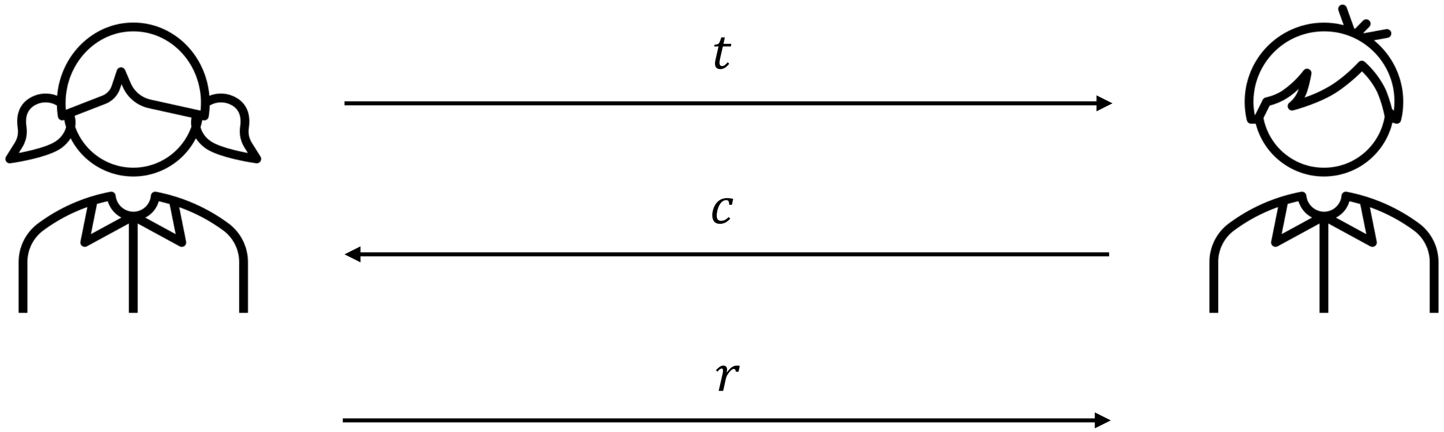
Arguing Knowledge of Dlogs in Hidden-Order Groups

$G = \langle g \rangle$ of hidden order $\leq 2^{b_G}$

$g = h^{\alpha}$

$k \leftarrow_{\$} ?$

$t \leftarrow h^{k}$



$c \leftarrow \{\mathbf{0}, \mathbf{1}\}$

$r \leftarrow k - c\,\alpha$

$h^{r} g^{c} = t?$

$g^{c_1 - c_2} = h^{r_2 - r_1}$

$c_1 - c_2 \in \{-1, 1\}$

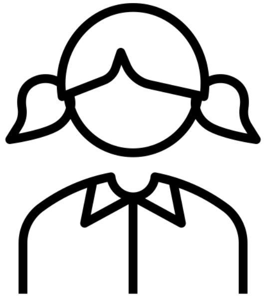
Arguing Knowledge of Dlogs in Hidden-Order Groups

$G = \langle g \rangle$ of hidden order $\leq 2^{b_G}$

$g = h^{\alpha}$

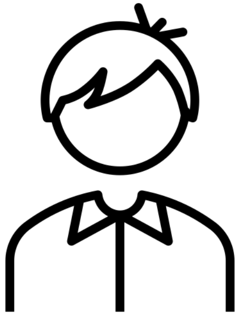
$k \leftarrow_{\$} ?$

$t \leftarrow h^{k}$



t →

← c



$c \leftarrow [\mathbf{0}, \lambda^{\log \lambda}]$

$r \leftarrow k - c\,\alpha$

r →

$h^{r} g^{c} = t?$

$g^{c_1 - c_2} = h^{r_2 - r_1}$

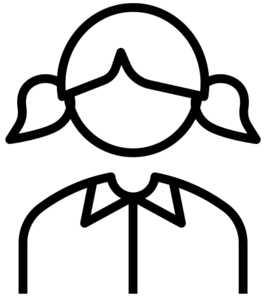
Arguing Knowledge of Dlogs in Hidden-Order Groups

$G = < g >$ of hidden order $\leq 2^{b_G}$

$g = h^{\alpha}$

$k \leftarrow_{\$} ?$

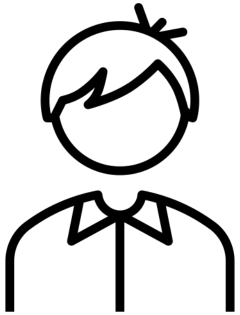
$t \leftarrow h^k$



t

c

r



$c \leftarrow [\mathbf{0}, \lambda^{\mathbf{log}\,\lambda}]$

$r \leftarrow k \; - c\, \alpha$

$h^r g^c = t?$

if $c_1 - c_2 | \, r_2 - r_1$ $\quad\quad$ $\left(h^{(r_2 - r_1)/(c_1 - c_2)}\, g^{-1}\right)^{c_1 - c_2} = 1_G$

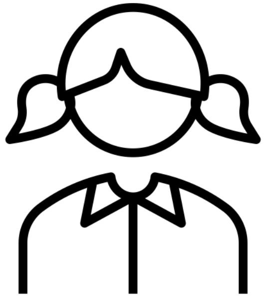
Arguing Knowledge of Dlogs in Hidden-Order Groups

$G = < g >$ of hidden order $\leq 2^{b_G}$

$g = h^{\alpha}$

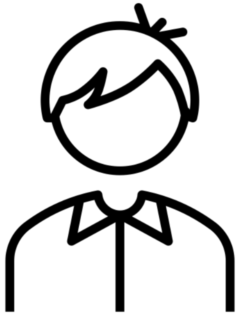
$k \leftarrow_{\$} ?$

$t \leftarrow h^{k}$



$t \longrightarrow$

$\longleftarrow c$



$c \leftarrow [\mathbf{0}, \lambda^{\mathbf{log}\,\lambda}]$

$r \leftarrow k - c\,\alpha$

$r \longrightarrow$

$h^{r} g^{c} = t?$

$$\left(h^{(r_2 - r_1)/(c_1 - c_2)}\, g^{-1}\right)^{c_1 - c_2} = 1_G$$

could be of order 2

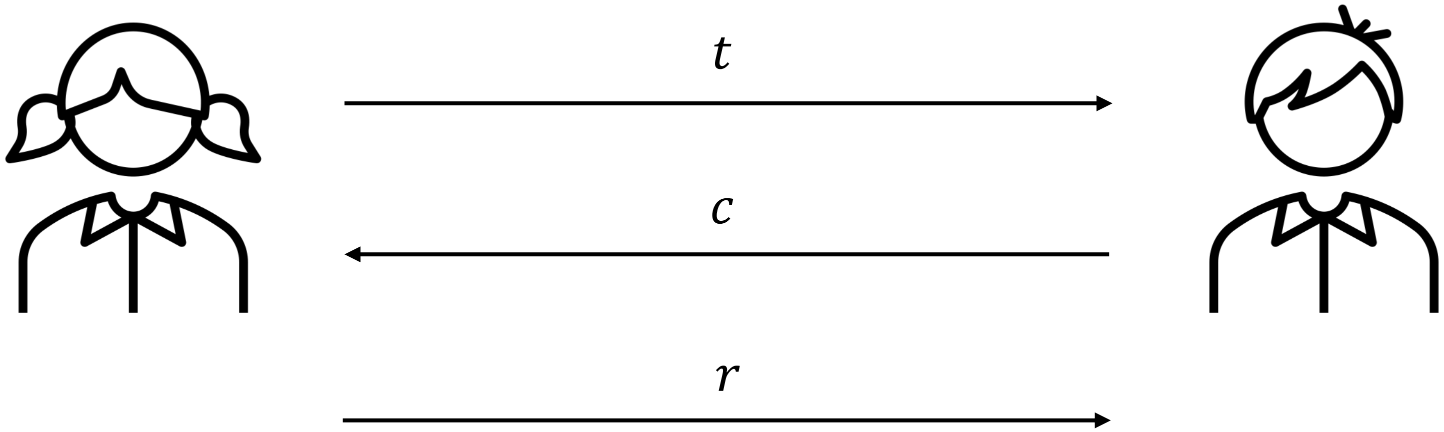
Arguing Knowledge of Dlogs in Hidden-Order Groups

$G = < g >$ of hidden order $\leq 2^{b_G}$

$g = h^{\alpha}, |\alpha| \leq 2^{b_G+\lambda}$

$k \leftarrow_{\$} ?$

$t \leftarrow h^k$



$c \leftarrow [\mathbf{0}, \lambda^{\mathbf{log}\,\lambda}]$

$r \leftarrow k - \underbrace{c\,\alpha}_{|\cdot| \leq 2^{b_G+\lambda}\lambda^{\log \lambda}}$

$h^r g^c = t?$

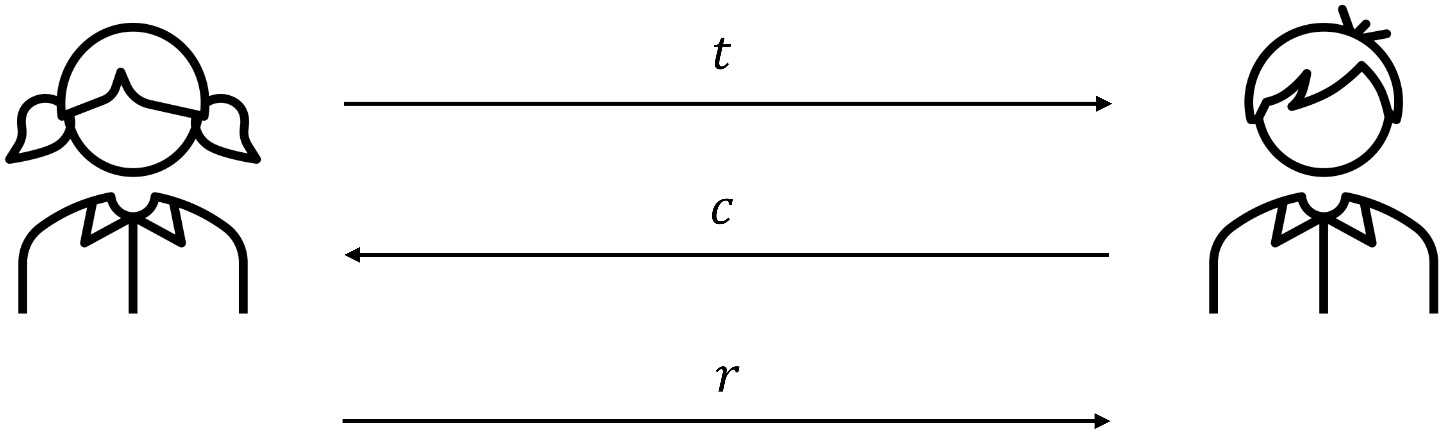
Arguing Knowledge of Dlogs in Hidden-Order Groups

$G = \langle g \rangle$ of hidden order $\le 2^{b_G}$

$g = h^{\alpha}, |\alpha| \le 2^{b_G+\lambda}$

$k \leftarrow_{\$} ?$

$t \leftarrow h^{k}$



$c \leftarrow [\mathbf{0}, \lambda^{\log\lambda}]$

$r \leftarrow k - \underbrace{c\,\alpha}_{|\cdot| \le 2^{b_G+\lambda}\lambda^{\log\lambda}}$

$h^{r} g^{c} = t?$

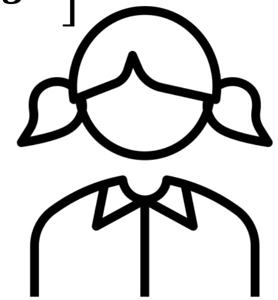
Arguing Knowledge of Dlogs in Hidden-Order Groups

$G = \langle g \rangle$ of hidden order $\leq 2^{b_G}$

$g = h^{\alpha}, |\alpha| \leq 2^{b_G+\lambda}$

$k \leftarrow_{\$} [\mathbf{0}; \mathbf{2^{\lambda}} \mathbf{2}^{b_G+\lambda} \lambda^{\log \lambda}]$

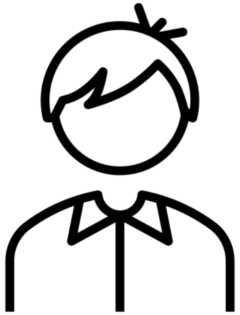
$t \leftarrow h^k$



t →

← c

r →

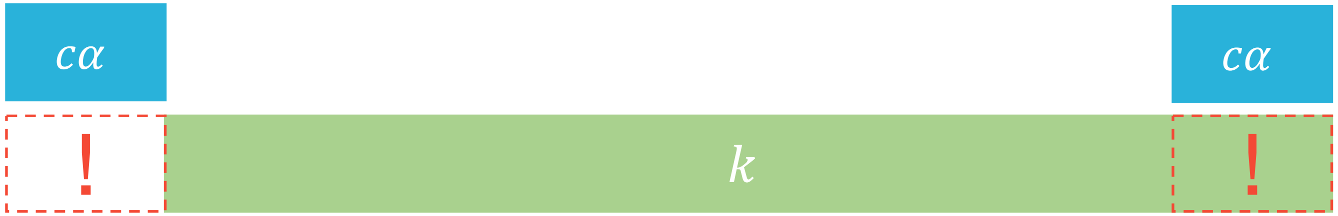


$c \leftarrow [\mathbf{0}, \lambda^{\log \lambda}]$

$r \leftarrow k - c\,\alpha$

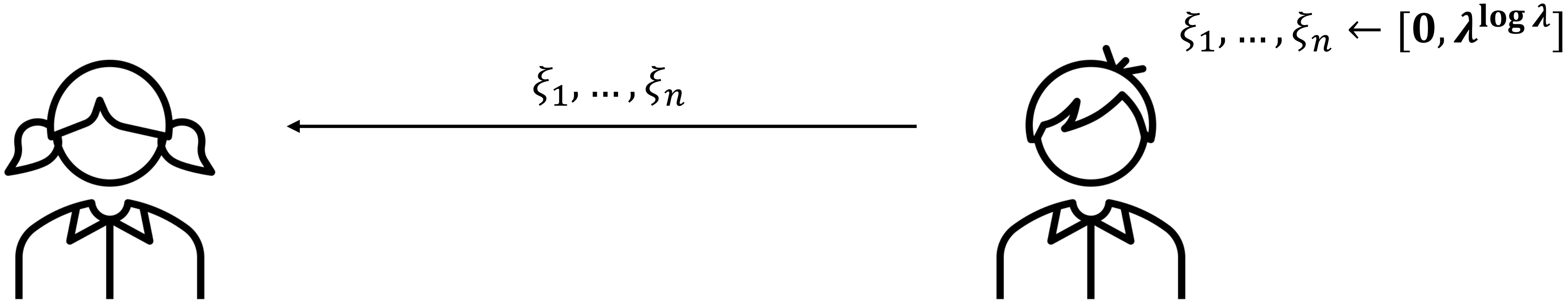
$|\cdot| \leq 2^{b_G+\lambda} \lambda^{\log \lambda}$ (bound on $c\,\alpha$)

$h^r g^c = t?$



Arguing Knowledge of Dlogs in Hidden-Order Groups

$g_1 = h^{\alpha_1}; \ldots; g_n = h^{\alpha_n}$

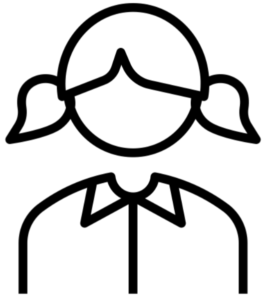


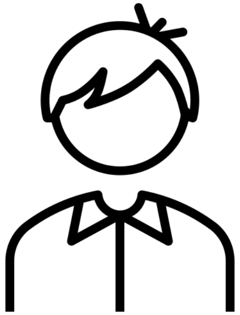
use $\xi_1\alpha_1 + \cdots + \xi_n\alpha_n$ as witness for $g_1^{\xi_1} \cdots g_n^{\xi_n}$

Inner-Product Argument over the Integers

$g_{1/2}, h_{1/2} \in \langle f \rangle$

$$C = \left(g_1^{a_1} g_2^{a_2} h_1^{b_1} h_2^{b_2} f^r\right)^2 \text{ and } \langle \boldsymbol{a}, \boldsymbol{b} \rangle = z$$

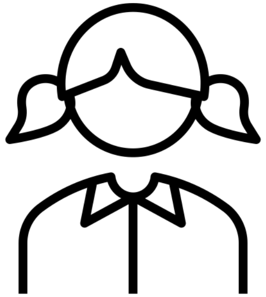


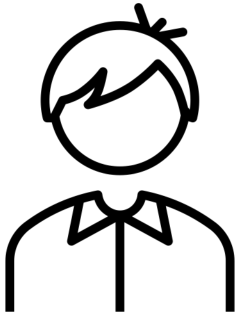


Inner-Product Argument over the Integers

$g_{1/2}, h_{1/2}, e \in < f >$

$$C = \left(g_1^{a_1} g_2^{a_2} h_1^{b_1} h_2^{b_2} e^{<\boldsymbol{a},\boldsymbol{b}>} f^r\right)^2$$

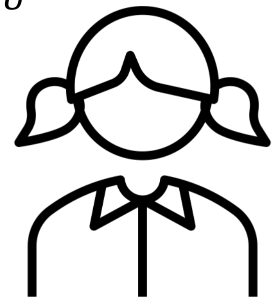


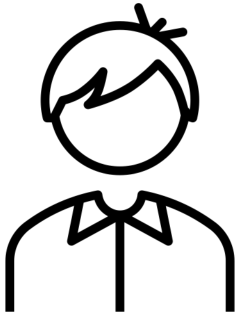


Inner-Product Argument over the Integers

$$C = \left(g_1^{a_1} g_2^{a_2} h_1^{b_1} h_2^{b_2} e^{\langle \mathbf{a},\mathbf{b} \rangle} f^{r}\right)^2$$

$U \leftarrow g_1^{a_2} h_2^{b_1} e^{a_2 b_1} f^{r_U}$



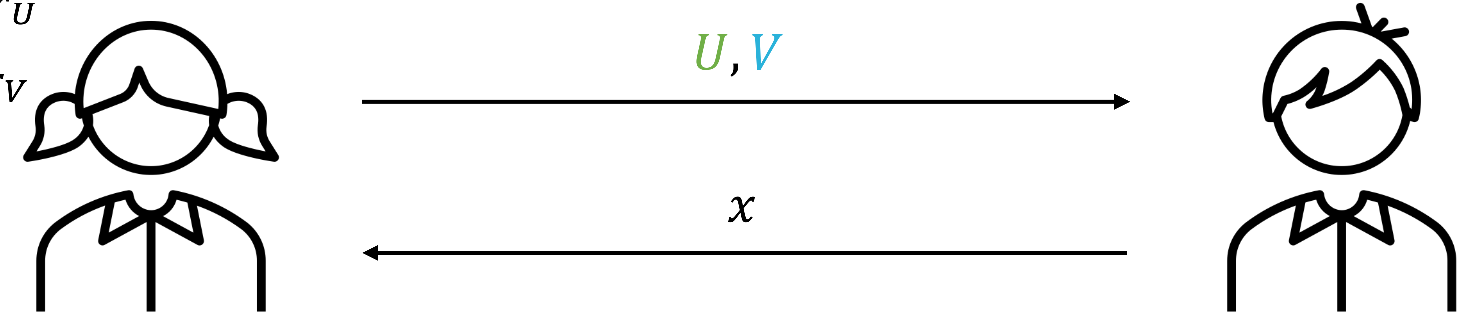


Inner-Product Argument over the Integers

$$C = \left(g_1^{a_1} g_2^{a_2} h_1^{b_1} h_2^{b_2} e^{<\mathbf{a},\mathbf{b}>} f^r\right)^2$$

$U \leftarrow g_1^{a_2} h_2^{b_1} e^{a_2 b_1} f^{r_U}$

$V \leftarrow g_2^{a_1} h_1^{b_2} e^{a_1 b_2} f^{r_V}$



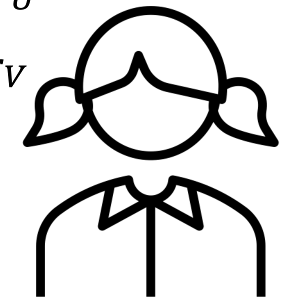
$x \leftarrow [\mathbf{0}, \boldsymbol{\lambda}^{\mathbf{log}\,\lambda}]$

Inner-Product Argument over the Integers

$$C = \left(g_1^{a_1} g_2^{a_2} h_1^{b_1} h_2^{b_2} e^{<\mathbf{a},\mathbf{b}>} f^{r}\right)^2$$

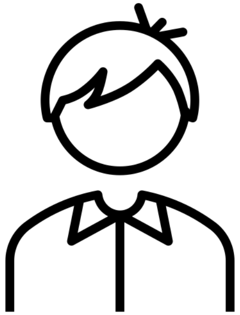
$U \leftarrow g_1^{a_2} h_2^{b_1} e^{a_2 b_1} f^{r_U}$

$V \leftarrow g_2^{a_1} h_1^{b_2} e^{a_1 b_2} f^{r_V}$



U, V →

← x



$x \leftarrow [\mathbf{0}, \boldsymbol{\lambda}^{\mathbf{log}\,\lambda}]$

$a \leftarrow a_1 + x a_2$

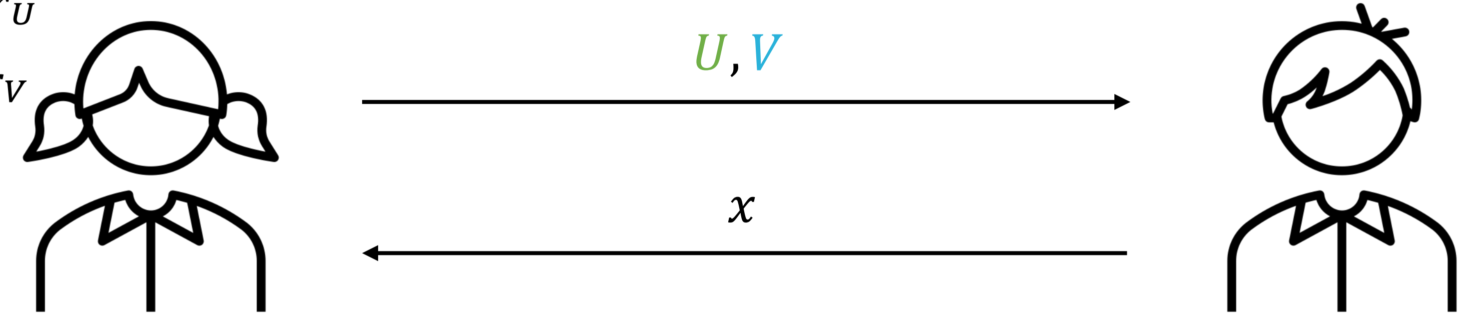
$b \leftarrow x b_1 + b_2$

Half the size of (a_1, a_2) and (b_1, b_2)!

Inner-Product Argument over the Integers

$$C = \left(g_1^{a_1} g_2^{a_2} h_1^{b_1} h_2^{b_2} e^{\langle \mathbf{a},\mathbf{b}\rangle} f^{r}\right)^2$$

$$U \leftarrow g_1^{a_2} h_2^{b_1} e^{a_2 b_1} f^{r_U}$$
$$V \leftarrow g_2^{a_1} h_1^{b_2} e^{a_1 b_2} f^{r_V}$$



$$x \leftarrow [\mathbf{0}, \boldsymbol{\lambda}^{\log \lambda}]$$

$$a \leftarrow a_1 + x a_2$$
$$b \leftarrow x b_1 + b_2$$
$$t \leftarrow r_V + r\,x + r_U x^2$$

$$\left((g_1^x g_2)^a (h_1 h_2^x)^b e^{ab} f^t\right)^4 = \left(U^{x^2} C^x V\right)^2$$

Recurse!

Inner-Product Argument over the Integers

$$\left((g_1^x g_2)^a (h_1 h_2^x)^b e^{ab} f^t\right)^4 = \left(U^{x^2} C^x V\right)^2$$

$$\underbrace{\begin{matrix} 1 & 1 & 1 \\ x_1 & x_2 & x_3 \\ x_1^2 & x_2^2 & x_3^2 \end{matrix}}_{\boldsymbol{X}} \quad \begin{matrix} \nu_1 \\ \nu_2 \\ \nu_3 \end{matrix} \quad = \quad \begin{matrix} 0 \\ 1 \\ 0 \end{matrix}$$

Inner-Product Argument over the Integers

$$\left((g_1^x g_2)^a (h_1 h_2^x)^b e^{ab} f^t\right)^4 = \left(U^{x^2} C^x V\right)^2$$

$$\begin{pmatrix} 1 & 1 & 1 \\ x_1 & x_2 & x_3 \\ x_1^2 & x_2^2 & x_3^2 \end{pmatrix} \begin{pmatrix} \nu_1 \\ \nu_2 \\ \nu_3 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$$

Even if x_1, x_2 and x_3 are pairwise distinct, there may not be a sol. in $\mathbb{Z}$!

Inner-Product Argument over the Integers

$$\left((g_1^x g_2)^a (h_1 h_2^x)^b e^{ab} f^t\right)^4 = \left(U^{x^2} C^x V\right)^2$$

$$\begin{matrix} 1 & 1 & 1 \\ x_1 & x_2 & x_3 \\ x_1^2 & x_2^2 & x_3^2 \end{matrix} \quad \begin{matrix} \nu_1 \\ \nu_2 \\ \nu_3 \end{matrix} \quad = \quad \begin{matrix} 0 \\ 1 \\ 0 \end{matrix}$$

$$\boldsymbol{X} \operatorname{ajd} \boldsymbol{X} = \det \boldsymbol{X} \; \boldsymbol{I}_3$$

Inner-Product Argument over the Integers

$$\left((g_1^x g_2)^a (h_1 h_2^x)^b e^{ab} f^t\right)^4 = \left(U^{x^2} C^x V\right)^2$$

$$\boldsymbol{X} \operatorname{ajd} \boldsymbol{X} = \det \boldsymbol{X} \ \boldsymbol{I_3}$$

$$\left(g_1^{a_{C,1}} g_2^{a_{C,2}} h_1^{b_{C,1}} h_2^{b_{C,2}} e^{z_C} f^{r_C}\right)^4 = C^{2 \det \boldsymbol{X}}$$

Inner-Product Argument over the Integers

$$\left((g_1^x g_2)^a (h_1 h_2^x)^b e^{ab} f^t\right)^4 = \left(U^{x^2} C^x V\right)^2$$

$$\boldsymbol{X} \operatorname{ajd} \boldsymbol{X} = \det \boldsymbol{X} \; \boldsymbol{I_3}$$

$$\left(g_1^{a_{C,1}} g_2^{a_{C,2}} h_1^{b_{C,1}} h_2^{b_{C,2}} e^{z_C} f^{r_C}\right)^4 = C^{2 \det \boldsymbol{X}}$$

$2 \det \boldsymbol{X}$ must divide all the exponents of the l.h.s. under the assumptions on G

Inner-Product Argument over the Integers

$$\left((g_1^x g_2)^a (h_1 h_2^x)^b e^{ab} f^t\right)^4 = \left(U^{x^2} C^x V\right)^2$$

$$\boldsymbol{X}\,\mathrm{ajd}\,\boldsymbol{X} = \det \boldsymbol{X}\ \boldsymbol{I_3}$$

$$\left(g_1^{a_{C,1}} g_2^{a_{C,2}} h_1^{b_{C,1}} h_2^{b_{C,2}} e^{z_C} f^{r_C}\right)^4 = C^2$$

Inner-Product Argument over the Integers

$$\left((g_1^x g_2)^a (h_1 h_2^x)^b e^{ab} f^t\right)^4 = \left(U^{x^2} C^x V\right)^2$$

$$\boldsymbol{X}\,\mathrm{ajd}\,\boldsymbol{X} = \det \boldsymbol{X}\ \boldsymbol{I_3}$$

$$\left(g_1^{a_{C,1}} g_2^{a_{C,2}} h_1^{b_{C,1}} h_2^{b_{C,2}} e^{z_C} f^{r_C}\right)^4 = C^2$$

Similarly for U and V

Inner-Product Argument over the Integers

$$\left((g_1^x g_2)^a (h_1 h_2^x)^b e^{ab} f^t\right)^4 = \left(U^{x^2} C^x V\right)^2$$

$$\boldsymbol{X} \operatorname{ajd} \boldsymbol{X} = \det \boldsymbol{X} \ \boldsymbol{I_3}$$

$$\left(g_1^{a_{C,1}} g_2^{a_{C,2}} h_1^{b_{C,1}} h_2^{b_{C,2}} e^{z_C} f^{r_C}\right)^4 = C^2$$

$$1_G = g_1^{p_{g_1}(x)} g_2^{p_{g_2}(x)} h_1^{p_{h_1}(x)} h_2^{p_{h_2}(x)} e^{p_e(x)} f^{p_f(x)}$$

Inner-Product Argument over the Integers

$$\left((g_1^x g_2)^a (h_1 h_2^x)^b e^{ab} f^t\right)^4 = \left(U^{x^2} C^x V\right)^2$$

$$\boldsymbol{X} \operatorname{ajd} \boldsymbol{X} = \det \boldsymbol{X}\ \boldsymbol{I_3}$$

$$\left(g_1^{a_{C,1}} g_2^{a_{C,2}} h_1^{b_{C,1}} h_2^{b_{C,2}} e^{z_C} f^{r_C}\right)^4 = C^2$$

must be 0 under the assumptions on G

$$1_G = g_1^{p_{g_1}(x)} g_2^{p_{g_2}(x)} h_1^{p_{h_1}(x)} h_2^{p_{h_2}(x)} e^{p_e(x)} f^{p_f(x)}$$

Inner Products for Diophantine Satisfiability

$$\boldsymbol{a_L} \circ \boldsymbol{a_R} = \boldsymbol{a_O} \text{ and } \boldsymbol{W_L a_L} + \boldsymbol{W_R a_R} + \boldsymbol{W_O a_O} = \boldsymbol{W_V} \underbrace{\boldsymbol{v}}_{\text{Committed integers}} + \boldsymbol{C}$$

(over $\mathbb{Z}$)

Procedure for Polynomial-Degree Reduction

$$2\,x^3 + xy\; - 1 = 0$$

Procedure for Polynomial-Degree Reduction

$$2\,x^3 + xy \; - 1 = 0$$

$$u \leftarrow x^2;\; v \leftarrow xy;\; w \leftarrow ux$$

Procedure for Polynomial-Degree Reduction

$$2\,x^3 + xy - 1 = 0$$

$$u \leftarrow x^2;\; v \leftarrow xy;\; w \leftarrow ux$$

$$\underbrace{(u - x^2)^2 + (v - xy)^2 + (w - ux)^2}_{\text{Hadamard}} + \underbrace{(2w + v - 1)^2}_{\text{Linear}} = 0$$

Procedure for Polynomial-Degree Reduction

$$2\,x^3 + xy\ - 1 = 0$$

$$u \leftarrow x^2;\ v \leftarrow xy;\ w \leftarrow ux$$

$$\underbrace{(u\ - x^2)^2 + (v\ - xy)^2 + (w\ - ux)^2}_{\text{Hadamard}} + \underbrace{(2w + v\ - 1)^2}_{\text{Linear}} = 0$$

$$\boldsymbol{a_L} \circ \boldsymbol{a_R} = \boldsymbol{a_O} \text{ and } \boldsymbol{W_L a_L} + \boldsymbol{W_R a_R} + \boldsymbol{W_O a_O} = \boldsymbol{W_V}\, \boldsymbol{v} + \boldsymbol{C}$$

Proving Diophantine-Satisfiability

- Damgård and Fujisaki gave a proof that x_1, x_2, x_3 committed in C_1, C_2, C_3 satisfy $x_1 x_2 = x_3$

- $\sum_{\boldsymbol{i} \in \mathbb{N}^\nu} a_{\boldsymbol{i}}\, x_1^{i_1} \cdots x_\nu^{i_\nu}$ of total degree δ which requires $M(\nu, \delta)$ multiplications $\Rightarrow 2\, \underbrace{M(\nu, \delta)}_{\leq \binom{\nu+\delta}{\delta} - \nu - 1} + 1$ commitments and $M(\nu, \delta)$ consistency args.

- Communication complexity $\Omega\left(\binom{\nu+\delta}{\delta}(\underbrace{\ell}_{\text{max bit length of sol.}} + b_G)\right)$

Arguing Diophantine Satisfiability

- With our commitments, polynomial-degree reduction algorithm and inner-product argument over the integers

$\Rightarrow$ args. of size $O(\delta\ell + \min(\nu,\delta)\log(\nu+\delta)b_G + \underbrace{H}_{\text{Height of the polynomial}})$ bits

vs. $\Omega\left(\binom{\nu+\delta}{\delta}(\ell + b_G)\right)$

Arguing Diophantine Satisfiability

- Can such arguments be aggregated?

- Can the verification time (~ linear in the bit length of the witness) be reduced (e.g. to log)?