Composition with Knowledge Assumptions

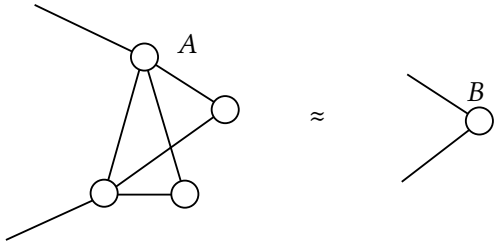
Thomas Kerber
papers@tkerber.org

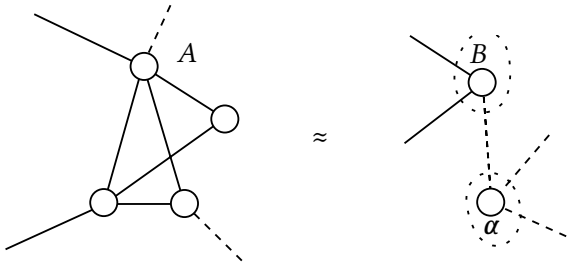
Aggelos Kiayias
akiayias@ed.ac.uk

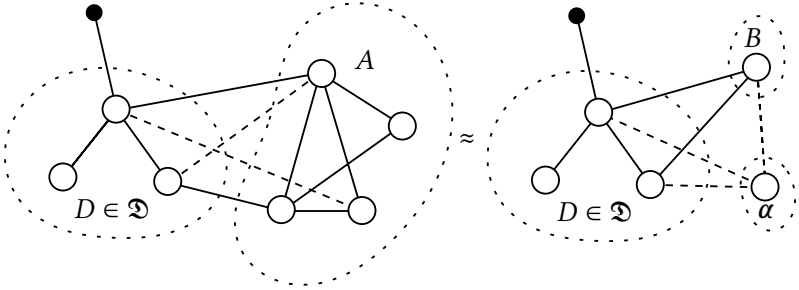
Markulf Kohlweiss
mkohlwei@ed.ac.uk

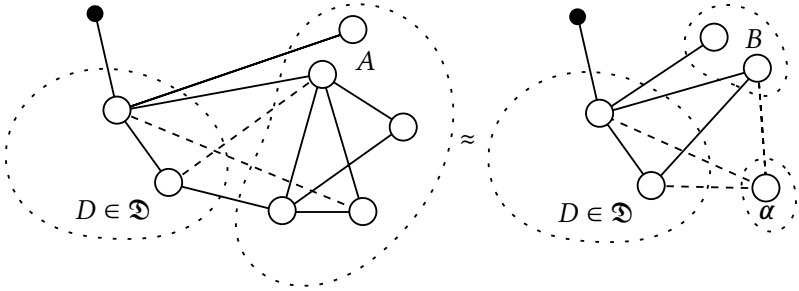
The University of Edinburgh & IOHK

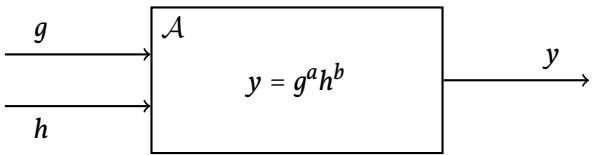
- Knowledge assumptions are useful
- Compositional security proofs are useful
- They conflict

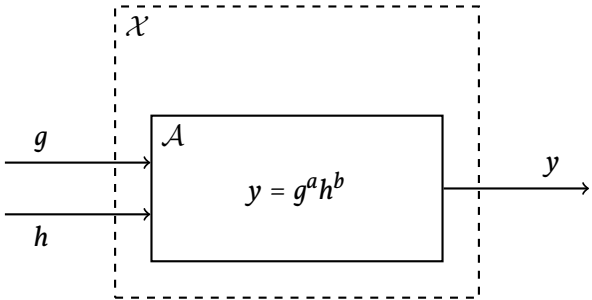

A
≈
B

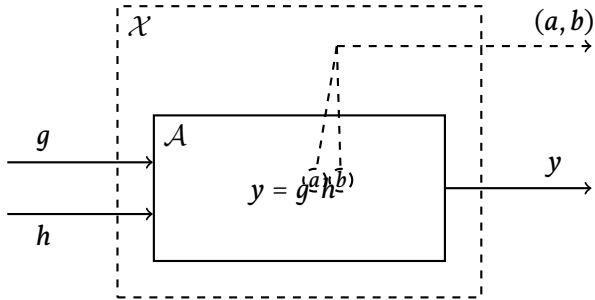

A
≈
B
α


A
$D \in \mathfrak{D}$
≈
B
$D \in \mathfrak{D}$
α


A
$D \in \mathfrak{D}$
≈
B
$D \in \mathfrak{D}$
α


g
h
A
$y = g^a h^b$
y


$\mathcal{X}$
$\mathcal{A}$
g
h
$y = g^a h^b$
y


$\mathcal{X}$
(a, b)
g
$\mathcal{A}$
$y = g^{(a,b)}h$
y
h

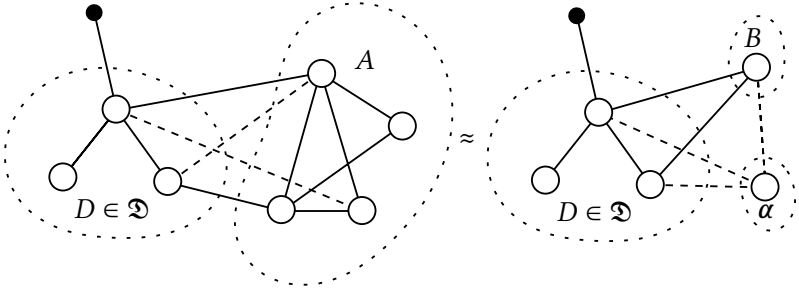
$$\tau \equiv \mathbb{0} \mid \mathbb{1} \mid \tau_1 + \tau_2 \mid \tau_1 \times \tau_2 \mid \tau^* \mid [\mathfrak{K}_{\mathrm{pp}}] \mid \langle \mathfrak{K}_{\mathrm{pp}}, I \rangle$$

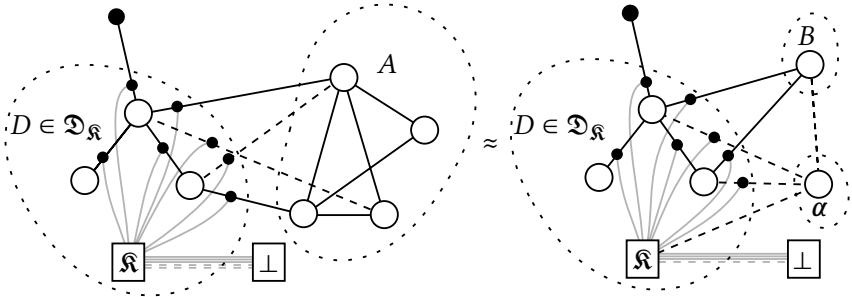
$$E \equiv \top \mid \mathsf{inj}_1(E) \mid \mathsf{inj}_2(E) \mid (E_1, E_2) \mid \varepsilon \mid E_1 :: E_2 \mid [E]_{\mathfrak{K}_{\mathrm{pp}}} \mid \langle E_1, E_2 \rangle^I_{\mathfrak{K}_{\mathrm{pp}}}$$

$$\vdash \top : \mathbb{1} \qquad \frac{\vdash x : \tau_1}{\vdash \mathsf{inj}_1(x) : \tau_1 + \tau_2} \qquad \frac{\vdash x : \tau_2}{\vdash \mathsf{inj}_2(x) : \tau_1 + \tau_2}$$

$$\frac{\vdash x : \tau_1 \qquad \vdash y : \tau_2}{\vdash (x, y) : \tau_1 \times \tau_2} \qquad \vdash \varepsilon : \tau^* \qquad \frac{\vdash x : \tau \qquad \vdash \vec{x} : \tau^*}{\vdash x :: \vec{x} : \tau^*}$$

$$\frac{\vdash x : X_{\mathrm{pp}} \qquad \vdash w : W_{\mathrm{pp}} \qquad (x, w) \in \mathcal{R}_{\mathrm{pp}}(I)}{\vdash \langle x, w \rangle^I_{\mathfrak{K}_{\mathrm{pp}}} : \langle \mathfrak{K}_{\mathrm{pp}}, I \rangle} \qquad \frac{\vdash x : X_{\mathrm{pp}}}{\vdash [x]_{\mathfrak{K}_{\mathrm{pp}}} : [\mathfrak{K}_{\mathrm{pp}}]}$$


A
$D \in \mathfrak{D}$
≈
B
$D \in \mathfrak{D}$
α



Example, where $y = g^a h^b$:

- Original: $(1, [y]_{\mathfrak{K}_{\mathrm{pp}}}) \colon 2 \times [\mathfrak{K}_{\mathrm{pp}}]$
- Lifted: $(1, \langle y, (g, a) :: (h, b) :: \varepsilon \rangle^{\{g,h\}}_{\mathfrak{K}_{\mathrm{pp}}}) \colon 2 \times \langle \mathfrak{K}_{\mathrm{pp}}, \{g, h\} \rangle$
- Recorded: $\langle y, (g, a) :: (h, b) :: \varepsilon \rangle^{\{g,h\}}_{\mathfrak{K}_{\mathrm{pp}}} \colon \langle \mathfrak{K}_{\mathrm{pp}}, \{g, h\} \rangle$
- Queried: $y \colon X_{\mathrm{pp}} \mapsto (g, a) :: (h, b) :: \varepsilon \colon W_{\mathrm{pp}}(X_{\mathrm{pp}})$

$$A \overset{\varepsilon_1,\alpha,\mathfrak{D}}{\rightarrowtail} B \wedge B \overset{\varepsilon_2,\beta,\mathfrak{D}\alpha}{\rightarrowtail} C \implies A \overset{\varepsilon_1+\varepsilon_2,\alpha\beta,\mathfrak{D}}{\rightarrowtail} C$$

$$A \overset{\varepsilon,\alpha,\mathfrak{D}\mathbf{C}}{\rightarrowtail} B \implies \mathbf{C}A \overset{\varepsilon,\alpha,\mathfrak{D}}{\rightarrowtail} \mathbf{C}B$$

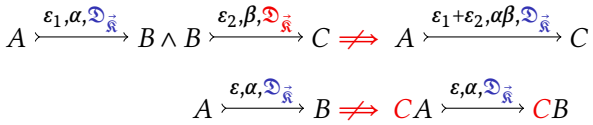
Statements slightly simplified for clarity.

Where $\vec{\mathfrak{K}}_1$, $\vec{\mathfrak{K}}_2$ are disjoint sets of knowledge assumptions:

$$\left[\begin{array}{ccc} A & \overset{\varepsilon_1,\alpha,\mathfrak{D}_{\vec{\mathfrak{K}}_1}}{\rightarrowtail} & B \\ & \wedge & \\ B & \overset{\varepsilon_2,\beta,\mathfrak{D}_{\vec{\mathfrak{K}}_2}}{\rightarrowtail} & C \end{array}\right] \implies A \overset{\varepsilon_1+\varepsilon_2,\vec{\mathfrak{K}}_2(\alpha)\beta,\mathfrak{D}_{\vec{\mathfrak{K}}_1\cup\vec{\mathfrak{K}}_2}}{\rightarrowtail} C$$

$$A \overset{\varepsilon,\alpha,\mathfrak{D}_{\vec{\mathfrak{K}}}}{\rightarrowtail} B \implies \forall C \in \mathrm{RespNet}_{\vec{\mathfrak{K}}}\colon \vec{\mathfrak{K}}(C)A \overset{\varepsilon,\gamma,\mathfrak{D}_{\vec{\mathfrak{K}}}}{\rightarrowtail} \vec{\mathfrak{K}}(C)B$$

Statements slightly simplified for clarity.


$A \overset{\varepsilon_1,\alpha,\mathfrak{D}_{\vec{\mathfrak{K}}}}{\rightarrowtail} B \wedge B \overset{\varepsilon_2,\beta,\mathfrak{D}_{\vec{\mathfrak{K}}}}{\rightarrowtail} C \not\Longrightarrow A \overset{\varepsilon_1+\varepsilon_2,\alpha\beta,\mathfrak{D}_{\vec{\mathfrak{K}}}}{\rightarrowtail} C$
$A \overset{\varepsilon,\alpha,\mathfrak{D}_{\vec{\mathfrak{K}}}}{\rightarrowtail} B \not\Longrightarrow CA \overset{\varepsilon,\alpha,\mathfrak{D}_{\vec{\mathfrak{K}}}}{\rightarrowtail} CB$

- Groth16 is composable in the AGM.
- Special-case composition permits composing with a setup ceremony.
- Many practical questions remain:
  - Which schemes are simulation extractable?
  - Is the current practice of freely re-using curve pairs and universal setups safe?