IS&C

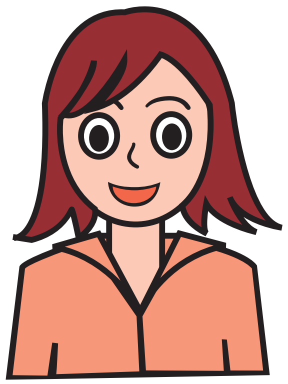
UNIVERSITÄT DES SAARLANDES

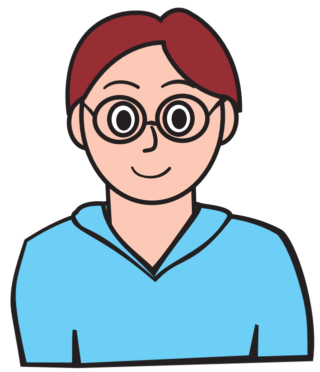
Improving Security Despite Compromise with Zero-knowledge

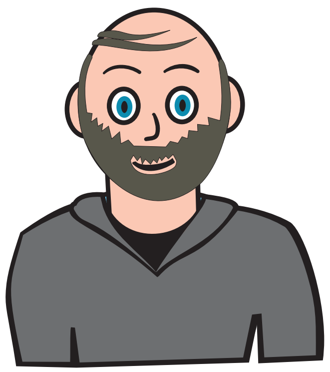
Cătălin Hrițcu (Saarland University)

Joint work with: Michael Backes, Matteo Maffei, and Dominique Unruh

A simple protocol

A: 

B: 

C: 

new m: Secret

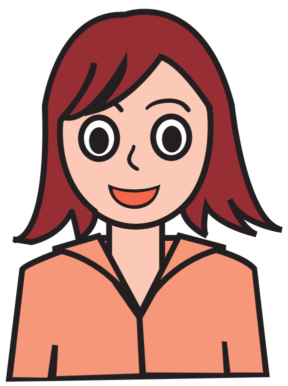
assume Authentic(m, B, C)

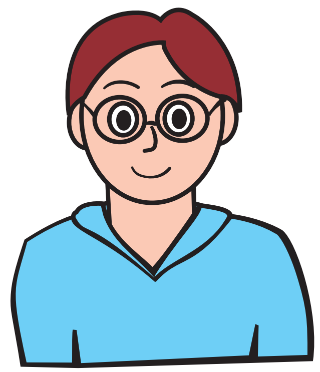
sign(enc((m,p),k_A^+), k_B^-)

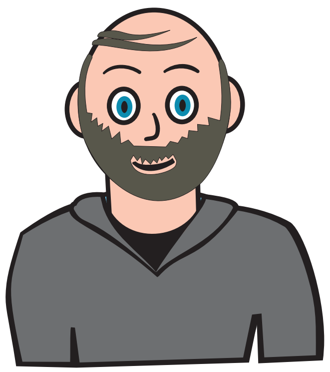
sign(enc(m,k_C^+), k_A^-)

assert Authentic(m, B, C)

A simple protocol

A: 

B: 

C: 

new m: Secret

assume Authentic(m, B, C)

$\xleftarrow{\text{sign(enc((m,p),}k_A^+\text{), }k_B^-\text{)}}$

$\xrightarrow{\text{sign(enc(m,}k_C^+\text{), }k_A^-\text{)}}$

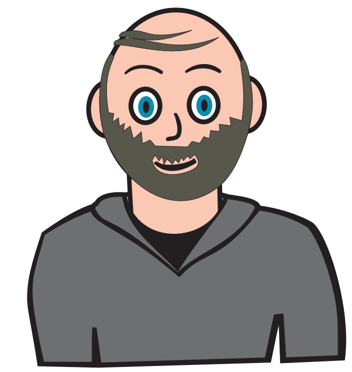
assert Authentic(m, B, C)

- This protocol is secure if all participants are honest (m is secret and authentic)

A simple protocol

A: 

B:

C: 

new m: Secret

assume Authentic(m, B, C)

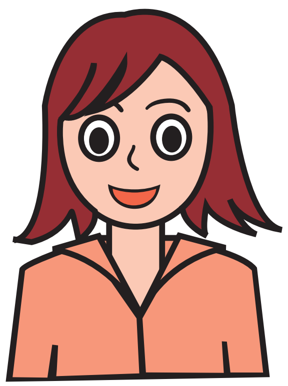
$\leftarrow$ sign(enc((m,p),k_A^+), k_B^-)

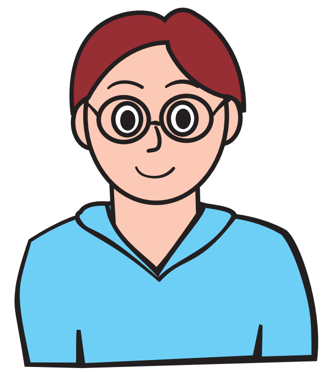
sign(enc(m,k_C^+), k_A^-) $\rightarrow$

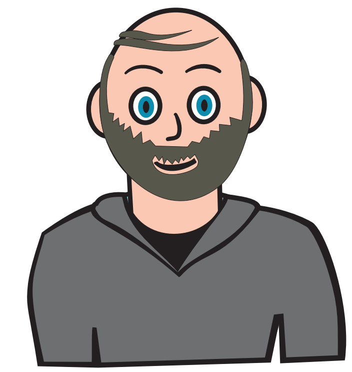
assert Authentic(m, B, C)

- This protocol is secure if all participants are honest (m is secret and authentic)
- **... but insecure if A is compromised (faking)**

Trying to strengthen the protocol

A: 

B: 

C: 

new m: Secret

assume Authentic(m, B, C)

forward

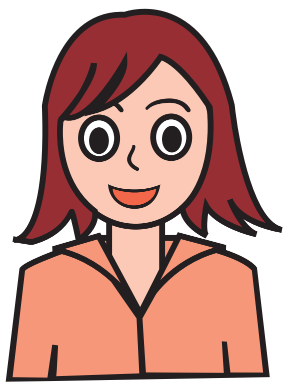
$\longleftarrow$ sign(enc((m,p),k_A^+), k_B^-)

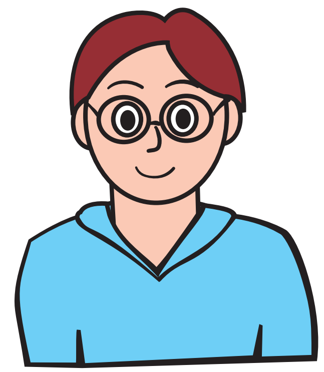
sign(enc(m,k_C^+), k_A^-), sign(enc((m,p),k_A^+), k_B^-) $\longrightarrow$

assert Authentic(m, B, C)

- C can check B's signature of "enc((m,p),k_A^+)"

Trying to strengthen the protocol

A: 

B: 

C: 

new m: Secret

assume Authentic(m, B, C)

forward

$\longleftarrow$ sign(enc((m,p),k_A^+), k_B^-)

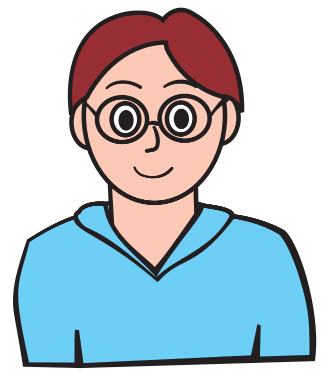
sign(enc(m,k_C^+), k_A^-), sign(enc((m,p),k_A^+), k_B^-) $\longrightarrow$

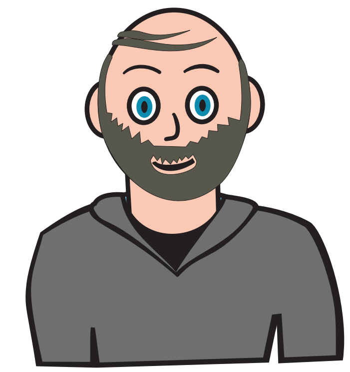
assert Authentic(m, B, C)

- C can check B's signature of "enc((m,p),k_A^+)"
- C cannot decrypt "enc((m,p),k_A^+)" in order to check m

Trying to strengthen the protocol

A: 

B: 

C: 

new m: Secret

assume Authentic(m, B, C)

sign(enc((m,p),k_A^+), k_B^-) ←

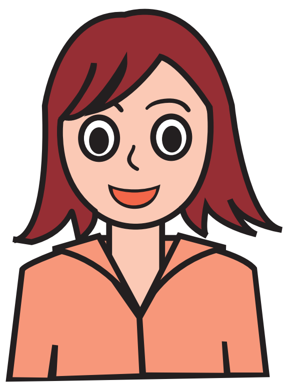
forward

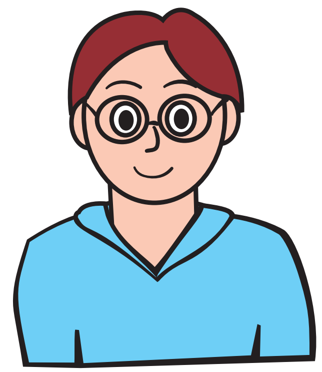
sign(enc(**m’**,k_C^+), k_A^-), sign(enc((m,p),k_A^+), k_B^-) →

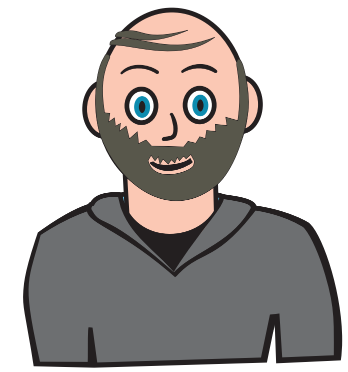
assert Authentic(m, B, C)

- C can check B’s signature of “enc((m,p),k_A^+)”
- C cannot decrypt “enc((m,p),k_A^+)” in order to check m
- **… still insecure if A comprised (substitution)**

Using zero-knowledge proofs

A: 

B: 

C: 

new m: Secret

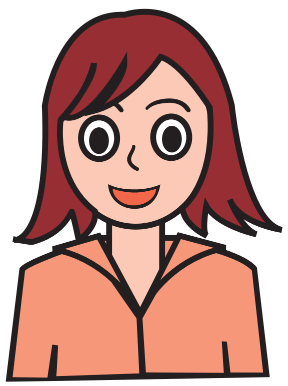
assume Authentic(m, B, C)

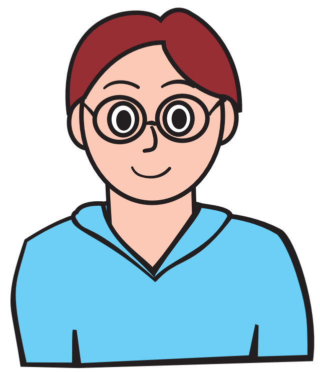
$\xleftarrow{\text{sign}(\text{enc}(m, k_A^+), k_B^-)}$

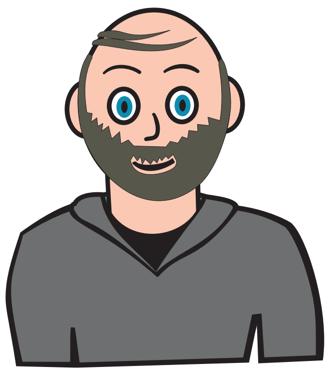
$\text{zk}_{3,2,S}(k_A^-, m, p; \text{sign}(\text{enc}(m, k_C^+), k_A^-), \text{sign}(\text{enc}((m, p), k_A^+), k_B^-))$ $\longrightarrow$

...

Using zero-knowledge proofs

A: 

B: 

C: 

new m: Secret

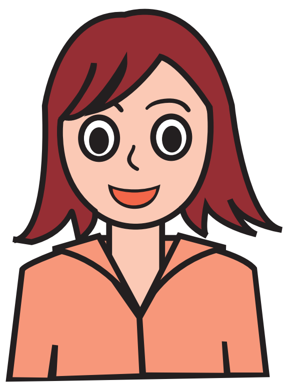
assume Authentic(m, B, C)

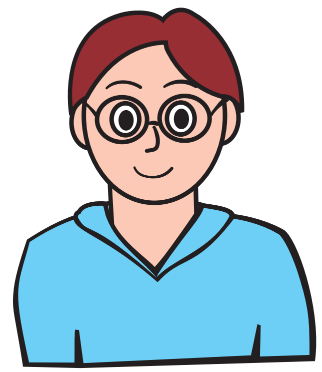
$$\xleftarrow{\text{sign}(\text{enc}(\text{m},\text{k}_{\text{A}}^{+}),\ \text{k}_{\text{B}}^{-})}$$

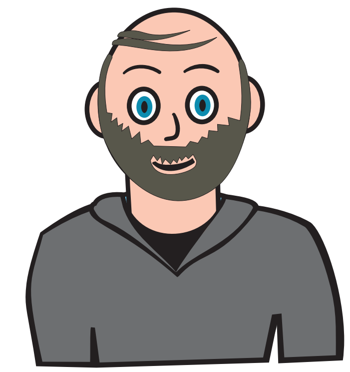
$$\text{zk}_{3,2,S}(\underbrace{k_A^-, m, p}_{\text{secrets}}; \underbrace{\text{sign}(\text{enc}(m, k_C^+), k_A^-), \text{sign}(\text{enc}((m,p), k_A^+), k_B^-)}_{\text{public values}})$$

...

Using zero-knowledge proofs

A: 

B: 

C: 

new m: Secret

assume Authentic(m, B, C)

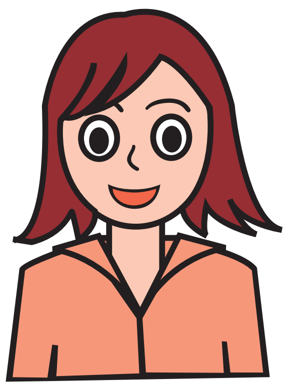
$\xleftarrow{\text{sign}(\text{enc}(m, k_A^{+}), k_B^{-})}$

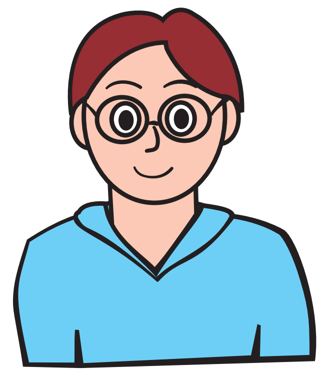
$\xrightarrow{\text{zk}_{3,2,S}(k_A^-, m, p;\ \text{sign}(\text{enc}(m, k_C^+), k_A^-), \text{sign}(\text{enc}((m, p), k_A^+), k_B^-))}$

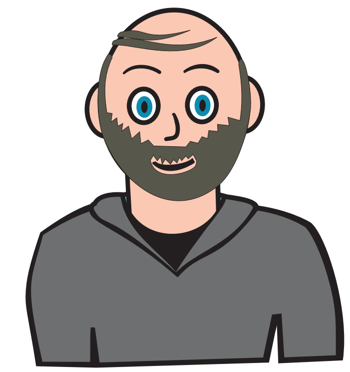
...

$$S = \text{check}(\beta_1, k_A^+) = \text{enc}(\alpha_2, k_C^+) \wedge \text{dec}(\text{check}(\beta_2, k_B^+), \alpha_1) = (\alpha_2, \alpha_3)$$

Using zero-knowledge proofs

A: 

B: 

C: 

new m: Secret

assume Authentic(m, B, C)

sign(enc(m,k_A^+), k_B^-)

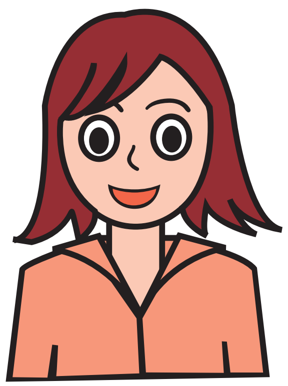
$\mathsf{zk}_{3,2,S}(k_A^-, m, p; \mathsf{sign}(\mathsf{enc}(m, k_C^+), k_A^-), \mathsf{sign}(\mathsf{enc}((m, p), k_A^+), k_B^-))$

...

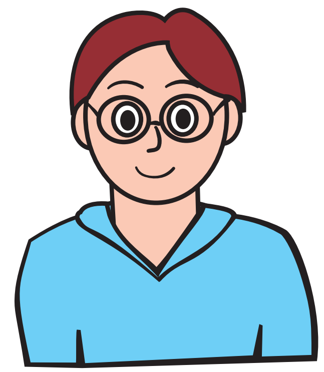
$$S = \mathsf{check}(\beta_1, k_A^+) = \mathsf{enc}(\alpha_2, k_C^+) \wedge \mathsf{dec}(\mathsf{check}(\beta_2, k_B^+), \alpha_1) = (\alpha_2, \alpha_3)$$

Using zero-knowledge proofs

A:



B:



C:

new m: Secret

assume Authentic(m, B, C)

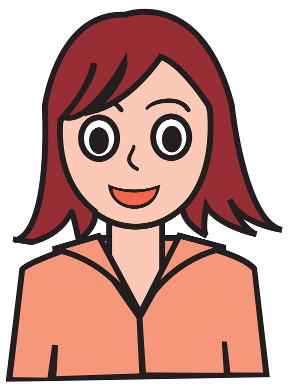
$\mathsf{sign}(\mathsf{enc}(m, k_A^+), k_B^-)$

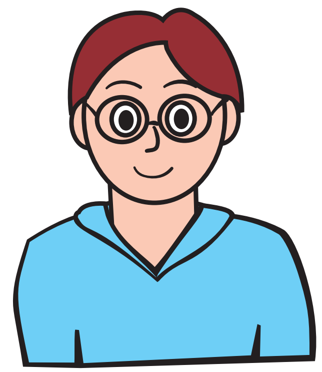
$$\mathsf{zk}_{3,2,S}(k_A^-, m, p; \mathsf{sign}(\mathsf{enc}(m, k_C^+), k_A^-), \mathsf{sign}(\mathsf{enc}((m, p), k_A^+), k_B^-))$$

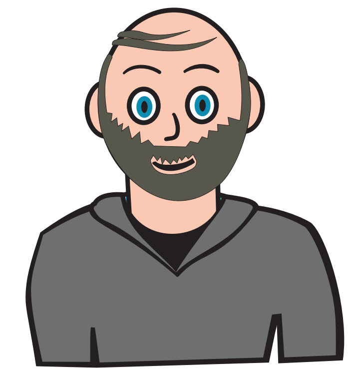
...

$$S = \mathsf{check}(\beta_1, k_A^+) = \mathsf{enc}(\alpha_2, k_C^+) \wedge \mathsf{dec}(\mathsf{check}(\beta_2, k_B^+), \alpha_1) = (\alpha_2, \alpha_3)$$

Using zero-knowledge proofs

A: 

B: 

C: 

new m: Secret

assume Authentic(m, B, C)

sign(enc(m,k_A^+), k_B^-)

$$\leftarrow$$

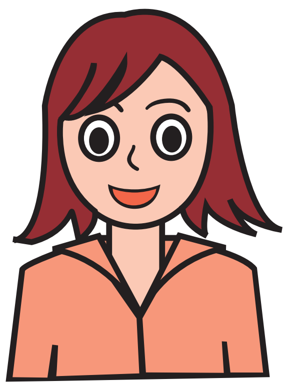
$$\mathsf{zk}_{3,2,S}(k_A^-, m, p; \mathsf{sign}(\mathsf{enc}(m, k_C^+), k_A^-), \mathsf{sign}(\mathsf{enc}((m,p), k_A^+), k_B^-))$$

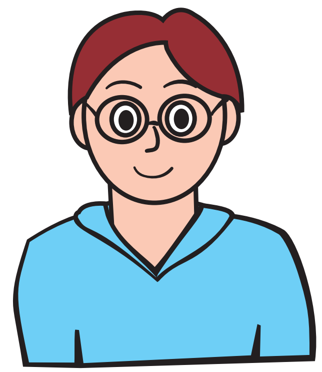
$$\rightarrow$$

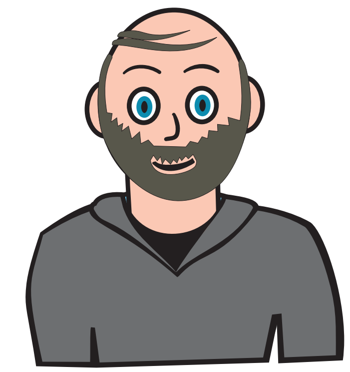
...

$$S = \mathsf{check}(\beta_1, k_A^+) = \mathsf{enc}(\alpha_2, k_C^+) \wedge \mathsf{dec}(\mathsf{check}(\beta_2, k_B^+), \alpha_1) = (\alpha_2, \alpha_3)$$

Using zero-knowledge proofs

A: 

B: 

C: 

new m: Secret

assume Authentic(m, B, C)

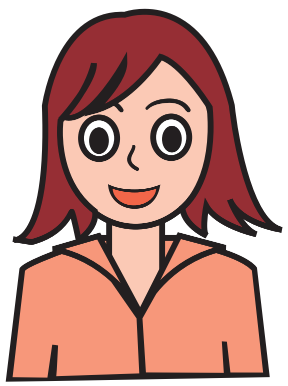
sign(enc(m,k_A^+), k_B^-)

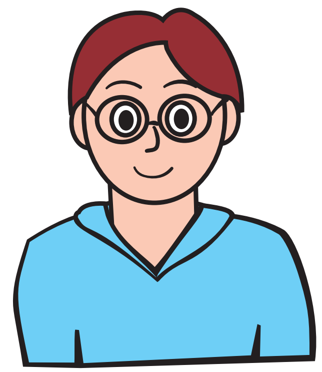
$$\mathsf{zk}_{3,2,S}(k_A^-, m, p; \mathsf{sign}(\mathsf{enc}(m, k_C^+), k_A^-), \mathsf{sign}(\mathsf{enc}((m,p), k_A^+), k_B^-))$$

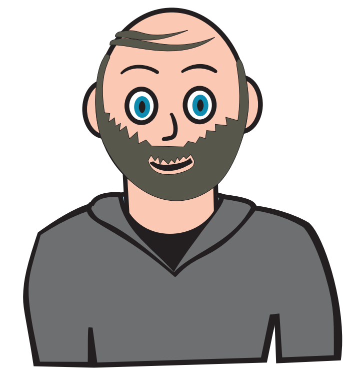
...

$$S = \mathsf{check}(\beta_1, k_A^+) = \mathsf{enc}(\alpha_2, k_C^+) \wedge \mathsf{dec}(\mathsf{check}(\beta_2, k_B^+), \alpha_1) = (\alpha_2, \alpha_3)$$

Using zero-knowledge proofs

A: 

B: 

C: 

new m: Secret

assume Authentic(m, B, C)

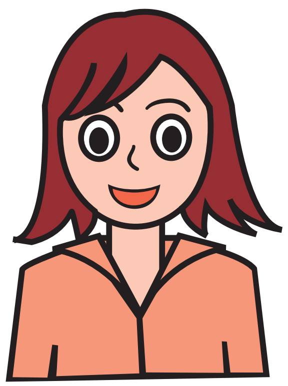
$\text{sign}(\text{enc}(m, k_A^+), k_B^-)$

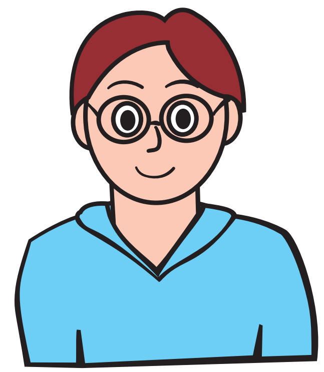
$$\text{zk}_{3,2,S}(k_A^-, m, p; \text{sign}(\text{enc}(m, k_C^+), k_A^-), \text{sign}(\text{enc}((m, p), k_A^+), k_B^-))$$

...

$$S = \text{check}(\beta_1, k_A^+) = \text{enc}(\alpha_2, k_C^+) \wedge \text{dec}(\text{check}(\beta_2, k_B^+), \alpha_1) = (\alpha_2, \alpha_3)$$

Using zero-knowledge proofs

A: 

B: 

C: 

new m: Secret

assume Authentic(m, B, C)

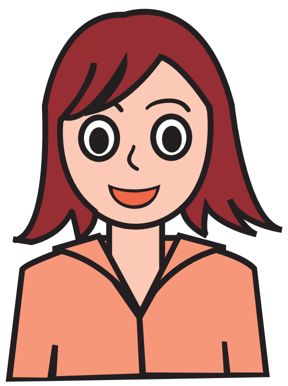
sign(enc(m,k_A^+), k_B^-)

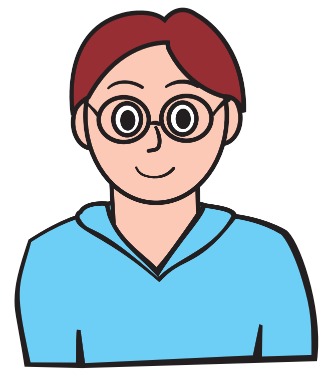
$$\mathsf{zk}_{3,2,S}(k_A^-, m, p; \mathsf{sign}(\mathsf{enc}(m, k_C^+), k_A^-), \mathsf{sign}(\mathsf{enc}((m, p), k_A^+), k_B^-))$$

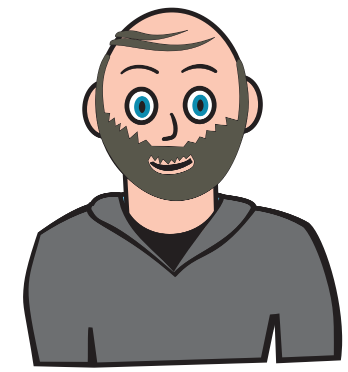
...

$$S = \mathsf{check}(\beta_1, k_A^+) = \mathsf{enc}(\alpha_2, k_C^+) \wedge \mathsf{dec}(\mathsf{check}(\beta_2, k_B^+), \alpha_1) = (\alpha_2, \alpha_3)$$

Using zero-knowledge proofs

A: 

B: 

C: 

new m: Secret

assume Authentic(m, B, C)

$\xleftarrow{\text{sign}(\text{enc}(m, k_A^+), k_B^-)}$

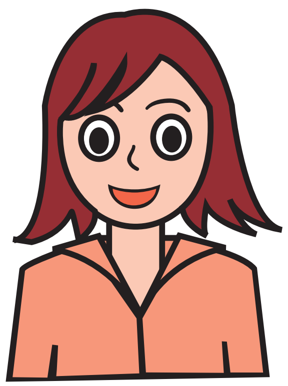
$$\text{zk}_{3,2,S}(k_A^-, m, p; \text{sign}(\text{enc}(m, k_C^+), k_A^-), \text{sign}(\text{enc}((m, p), k_A^+), k_B^-))$$

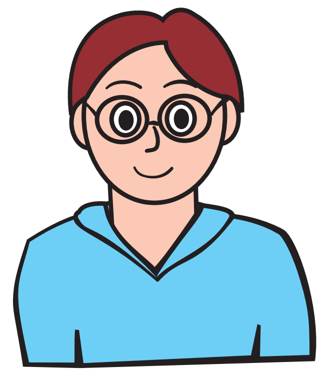
$\longrightarrow$

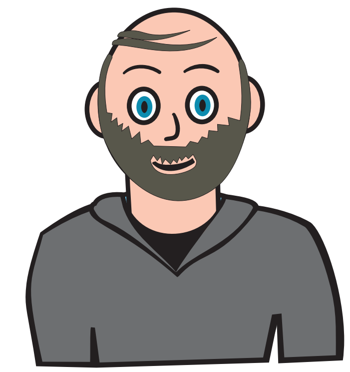
...

$$S = \text{check}(\beta_1, k_A^+) = \text{enc}(\alpha_2, k_C^+) \wedge \text{dec}(\text{check}(\beta_2, k_B^+), \alpha_1) = (\alpha_2, \alpha_3)$$

Using zero-knowledge proofs

A: 

B: 

C: 

new m: Secret

assume Authentic(m, B, C)

$\mathsf{sign}(\mathsf{enc}(m, k_A^{+}), k_B^{-})$

$$\mathsf{zk}_{3,2,S}(k_A^-, m, p; \mathsf{sign}(\mathsf{enc}(m, k_C^+), k_A^-), \mathsf{sign}(\mathsf{enc}((m,p), k_A^+), k_B^-))$$

...

$$S = \mathsf{check}(\beta_1, k_A^+) = \mathsf{enc}(\alpha_2, k_C^+) \wedge \mathsf{dec}(\mathsf{check}(\beta_2, k_B^+), \alpha_1) = (\alpha_2, \alpha_3)$$

- Symbolic abstraction of ZK (Dolev-Yao model) [Backes, Maffei & Unruh, S&P '08]

Goals

- General aim: to aid secure protocol design
- Automated translation
  - Preserve secrecy and authenticity if everybody is honest
  - Enforce authenticity even if some principals are compromised

Goals

- General aim: to aid secure protocol design
- Automated translation
  - Preserve secrecy and authenticity if everybody is honest
  - Enforce authenticity even if some principals are compromised
  - Use type system for authorization [Fournet et. al., CSF ’07]
    - We extended it to zero-knowledge [FCS-ARSPA-WITS ’08]
    - Also translate types
    - Prove that well-typing is preserved

$$\begin{aligned} \forall P\ \forall A.\ \ \Gamma \vdash P \ \Rightarrow\ \ & \langle\!\langle\, \Gamma \,\rangle\!\rangle \vdash \langle\!\langle\, P \,\rangle\!\rangle \wedge \\ & \langle\!\langle\, \Gamma \,\rangle\!\rangle \vdash \mathit{corrupt}(\,\langle\!\langle\, P \,\rangle\!\rangle\,, A) \end{aligned}$$