Composition in the Squirrel Prover

Jules Timmerman
Supervised by Charlie Jacomme

2024

Table of Contents

Protocols and security

- Protocols
- Indistinguishability
- Mechanized Provers

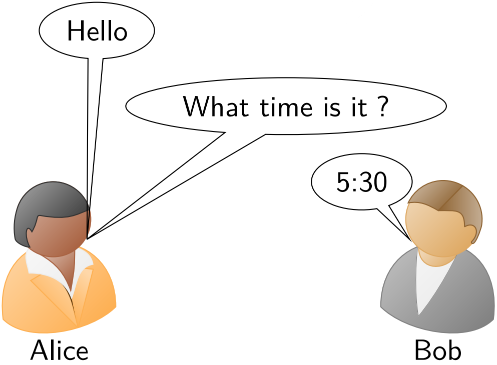
Composition

- What is composition ?
- Shared secrets

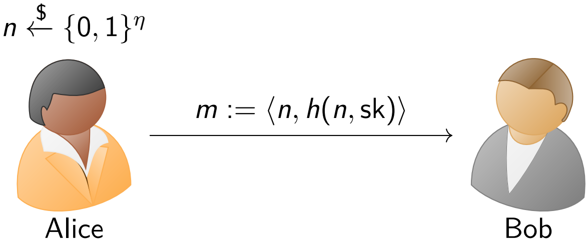
Using the result in Squirrel

- Bi-Deduction
- Final result

What is a protocol



Example protocol: Basic Hash



$n \xleftarrow{\$} \{0,1\}^{\eta}$

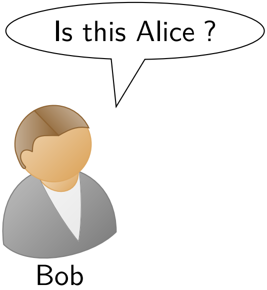
$m := \langle n, h(n, \mathsf{sk}) \rangle$

Alice

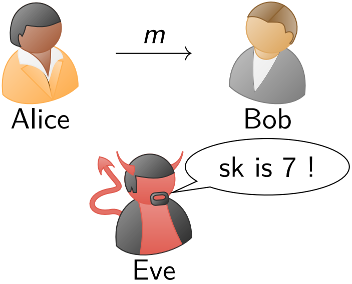
Bob

What is a “safe” protocol ?

Authentication

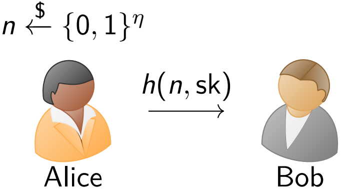


Key Secrecy



Indistinguishability

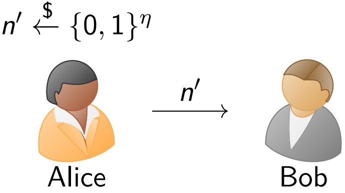
Side $b = 0$



$n \xleftarrow{\$} \{0,1\}^\eta$

$\xrightarrow{h(n, \mathsf{sk})}$

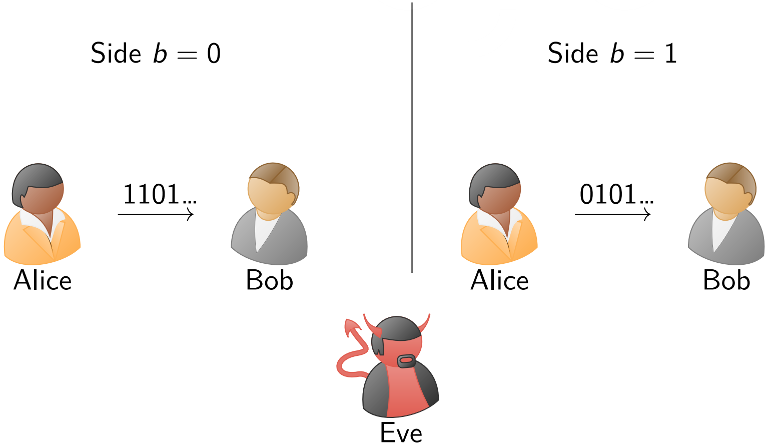
Side $b = 1$



$n' \xleftarrow{\$} \{0,1\}^\eta$

$\xrightarrow{n'}$

Indistinguishability



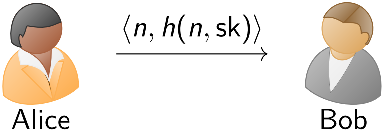
Side $b = 0$

Side $b = 1$

Example Cryptographic Reduction (PRF)

Side $b = 0$

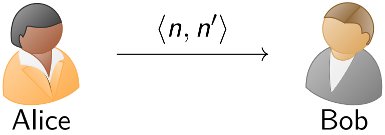
$n \xleftarrow{\$} \{0,1\}^\eta$



Side $b = 1$

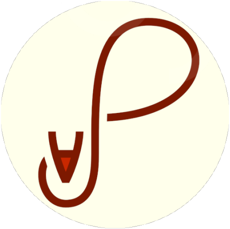
$n \xleftarrow{\$} \{0,1\}^\eta$

$n' \xleftarrow{\$} \{0,1\}^\eta$



Some Tools

- ProVerif
- Cryptoverif
- Tamarin
- EasyCrypt
- Squirrel



Squirrel

- Explicit randomness with tapes $\rho = (\rho_h, \rho_a)$
- Symbols: $\mathtt{enc}, \mathtt{dec}, h \ldots$
- Terms: λ-calculus
- Semantic: Random Variables $[\![t]\!]^{\eta,\rho}_{\mathbb{M}:\mathcal{E}}$
- Indistinguishability Predicate $\sim$

Protocols and security

- Protocols
- Indistinguishability
- Mechanized Provers

Composition

- What is composition ?
- Shared secrets

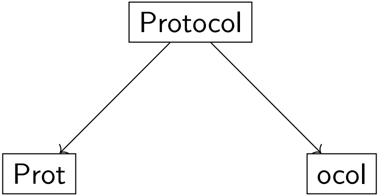
Using the result in Squirrel

- Bi-Deduction
- Final result

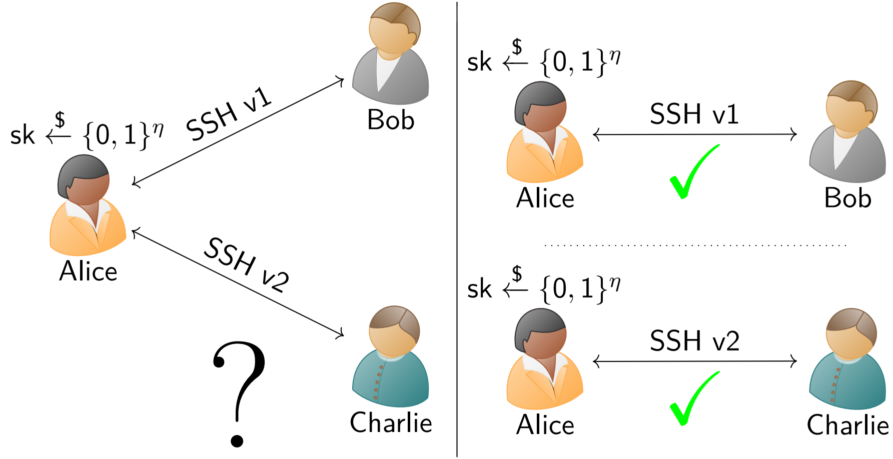
Composing protocols

$\boxed{\text{Protocol}}$

Composing protocols



Example: Multiple SSH

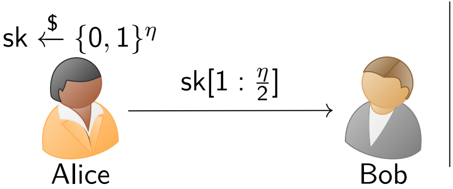


sk $\xleftarrow{\$} \{0,1\}^\eta$

SSH v1

SSH v2

Easy right ?



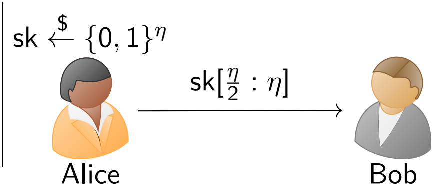
$\mathsf{sk} \xleftarrow{\$} \{0,1\}^\eta$

$\mathsf{sk}[1 : \frac{\eta}{2}]$

Alice

Bob

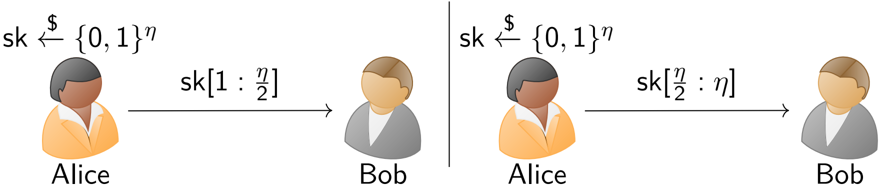
Easy right ?



$\mathsf{sk} \xleftarrow{\$} \{0,1\}^\eta$

$\mathsf{sk}[\frac{\eta}{2} : \eta]$

Easy right ?



$\mathsf{sk} \xleftarrow{\$} \{0,1\}^\eta$

$\mathsf{sk}[1 : \frac{\eta}{2}]$

Alice

Bob

$\mathsf{sk} \xleftarrow{\$} \{0,1\}^\eta$

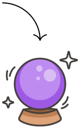
$\mathsf{sk}[\frac{\eta}{2} : \eta]$

Alice

Bob

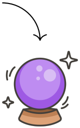
Solution: encapsulation [CCS20]

sk **usage**

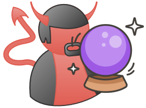


Solution: encapsulation [CCS20]

sk **usage**

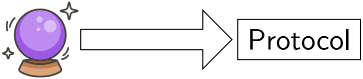


$\mathcal{O}$-indistinguishability



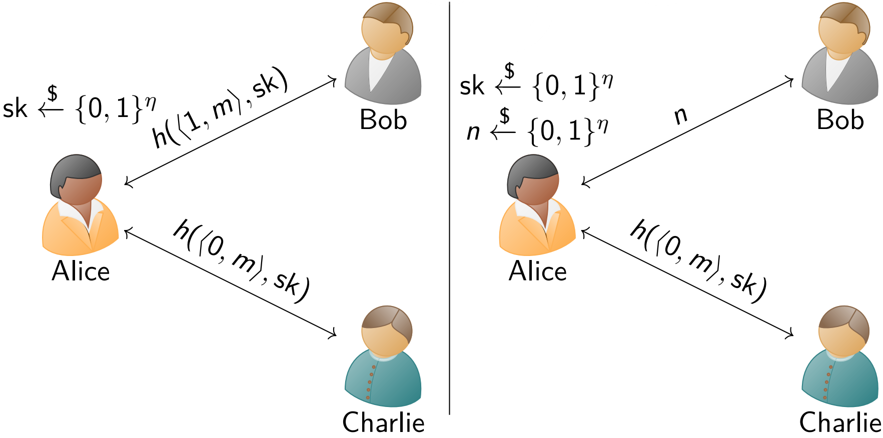
Eve

$\mathcal{O}$ -simulatability



Protocol

Example usage: prefixing messages


$\mathsf{sk} \xleftarrow{\$} \{0,1\}^\eta$
$h(\langle 1, m\rangle, sk)$
Bob
Alice
$h(\langle 0, m\rangle, sk)$
Charlie
$\mathsf{sk} \xleftarrow{\$} \{0,1\}^\eta$
$n \xleftarrow{\$} \{0,1\}^\eta$
n
Bob
Alice
$h(\langle 0, m\rangle, sk)$
Charlie

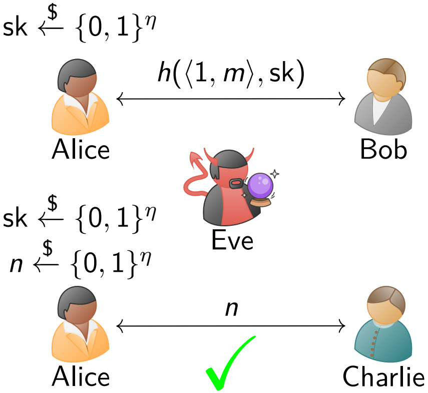
Example usage: using a “good” oracle

🔮 $= x \mapsto h(\langle 0, x \rangle, \mathsf{sk})$

Example usage: using a “good” oracle

$$🔮 = x \mapsto h(\langle 0, x \rangle, \mathsf{sk})$$

$\mathcal{O}$-indistinguishability

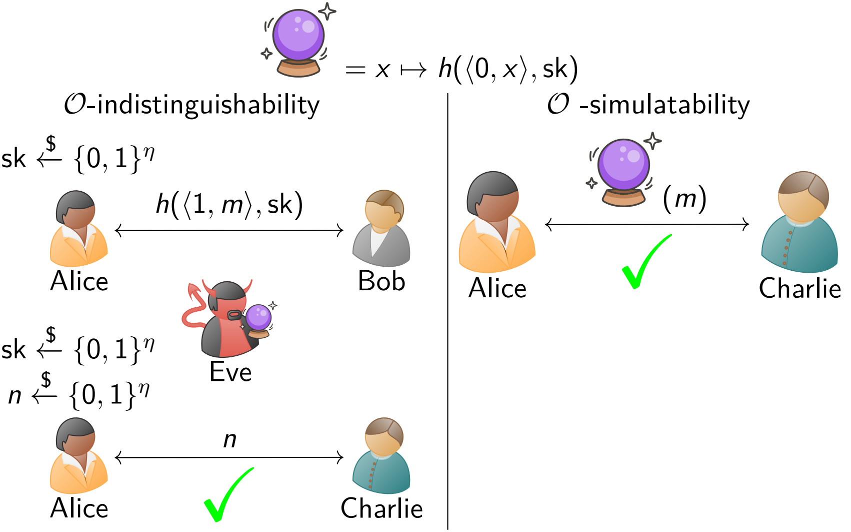


$\mathsf{sk} \xleftarrow{\$} \{0,1\}^\eta$

$\mathsf{sk} \xleftarrow{\$} \{0,1\}^\eta$

$n \xleftarrow{\$} \{0,1\}^\eta$

Example usage: using a “good” oracle



🔮 $= x \mapsto h(\langle 0, x \rangle, \mathsf{sk})$

$\mathcal{O}$-indistinguishability

$\mathsf{sk} \xleftarrow{\$} \{0,1\}^\eta$

Alice $\xleftrightarrow{h(\langle 1, m \rangle, \mathsf{sk})}$ Bob

Eve

$\mathsf{sk} \xleftarrow{\$} \{0,1\}^\eta$

$n \xleftarrow{\$} \{0,1\}^\eta$

Alice $\xleftrightarrow{n}$ Charlie ✓

$\mathcal{O}$ -simulatability

Alice $\xleftrightarrow{🔮(m)}$ Charlie ✓

Protocols and security
- Protocols
- Indistinguishability
- Mechanized Provers

Composition
- What is composition ?
- Shared secrets

Using the result in Squirrel
- Bi-Deduction
- Final result

Intuition

Bi-Deduction: $\#(u_0, u_1) \rhd_{\mathcal{G}} \#(v_0, v_1)$

Intuition

Bi-Deduction: $\#(u_0, u_1) \triangleright_{\mathcal{G}} \#(v_0, v_1)$

$$\begin{tikzcd}
u_0 \arrow[r, phantom, "\sim"] \arrow[d, "p"'] & u_1 \arrow[d, "p"] \\
v_0 \arrow[r, phantom, "\sim"] & v_1
\end{tikzcd}$$

Is it useful ?

Theorem (Overly Simplified Bi-Deduce)

$$\frac{\emptyset \rhd_{\mathcal{G}} u_\sharp}{u_0 \sim u_1}$$

Is it useful ?

Theorem (Overly Simplified Bi-Deduce)

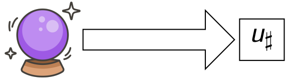
$$\frac{\emptyset \rhd_{\mathcal{G}} u_\sharp}{u_0 \sim u_1}$$

Example (Transitivity)

$$\frac{u_\sharp \rhd_{\mathcal{G}} v_\sharp \qquad u_\sharp, v_\sharp \rhd_{\mathcal{G}} w_\sharp}{u_\sharp \rhd_{\mathcal{G}} v_\sharp, w_\sharp}$$

Same vibe as $\mathcal{O}$ -simulatability

$u_\sharp$ $\mathcal{O}$ -simulatable



Bi-deduction $\emptyset \triangleright_{\mathcal{O}} u_\sharp$

$$\emptyset \Longrightarrow \boxed{u_\sharp}$$

Creating a rule

Theorem (Simplified Compositional Bi-Deduce)

$$CBD\,\frac{\emptyset \triangleright_{\mathcal{O}} w \qquad u, \lambda_{\mathcal{O}} \sim v, \lambda_{\mathcal{O}}}{u, w(u) \sim v, w(v)}$$

Conclusion and Future Works

- New way of doing proofs!
- Not implemented yet...
- Lots of corrolaries possible

Not simplified

Theorem (Bi-deduce)

$$\frac{\mathcal{E}, \Theta \vdash \mathit{Valid}(C_\sharp) \qquad \mathcal{E}, \Theta, C_\sharp, (\varphi_\sharp, \psi_\sharp) \vdash \emptyset \rhd_{\mathcal{G}} u_\sharp}{\mathcal{E}, \Theta \vdash u_0 \sim u_1}$$

Theorem (Compositional Bi-deduce)

$$\mathit{CBD}\,\frac{\begin{array}{cc}\mathcal{E}, \Theta \vdash \mathit{Valid}(C'_\sharp) & \mathcal{N}(w) \ \cap \ \mathcal{N}(u, v) = \{\mathsf{sk\ t}\} \\ \mathcal{E}, \Theta, C'_\sharp, (\varphi_\sharp, \psi_\sharp) \vdash \emptyset \rhd_{\mathcal{G}} w & \mathcal{E}, \Theta \vdash u, \lambda_{\mathcal{G}} \sim v, \lambda_{\mathcal{G}}\end{array}}{\mathcal{E}, \Theta \vdash u, w(u) \sim v, w(v)}$$