A Protocol for Online Mobile Payment

Asgeir Steine

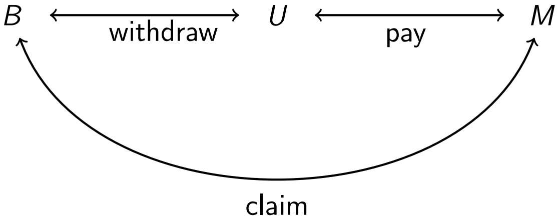
Plan:

- Mobile Online Payment
- Properties
- Blind Signatures
- Near Field Channel U <-> M
- Anonymous Online Channel B <-> U
- Protocol

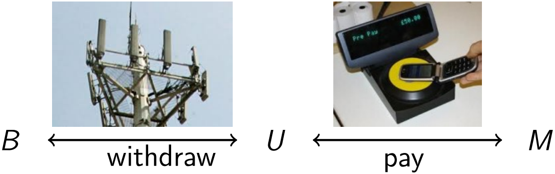
Mobile Online Payment

$$\begin{tikzcd} B \arrow[r, leftrightarrow, "\text{withdraw}"'] & U \arrow[r, leftrightarrow, "\text{pay}"'] & M \end{tikzcd}$$

Mobile Online Payment

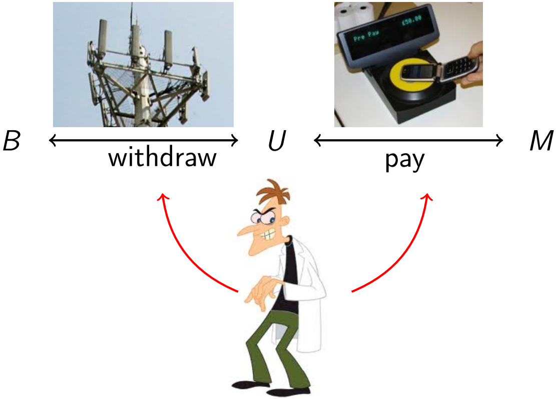


Mobile Online Payment



$$B \xleftrightarrow[\text{withdraw}]{} U \xleftrightarrow[\text{pay}]{} M$$

Mobile Online Payment

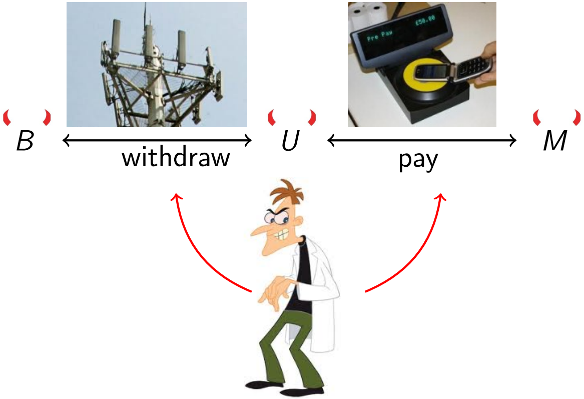


$B \longleftrightarrow U \longleftrightarrow M$

withdraw

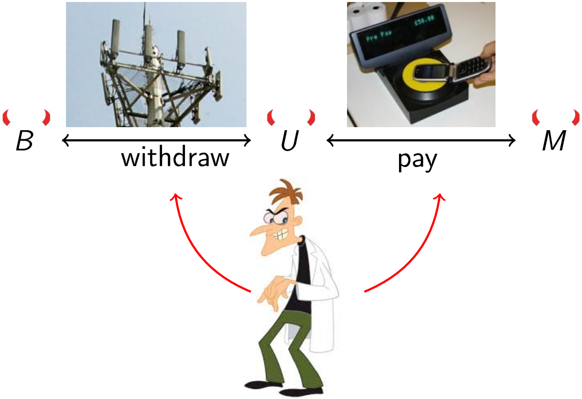
pay

Mobile Online Payment



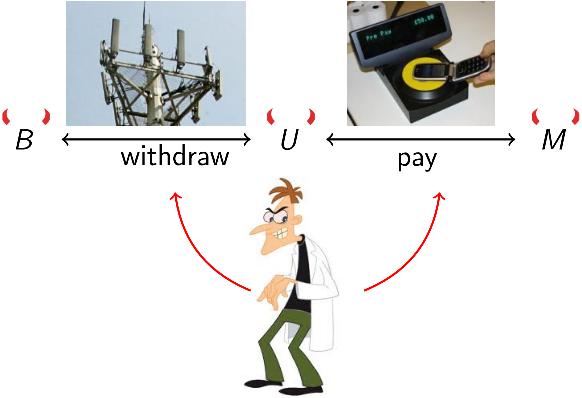
B withdraw U pay M

Mobile Online Payment



- Many potential threats.

Mobile Online Payment



- Many potential threats.
- Hidden players: Network operator N, Mobile Service Provider S.

Properties

Transaction security:

- Bank security (withdraw $\geq$ claim).
- Merchant security (claim $\geq$ pay).
- User security (pay $\geq$ withdraw).

Privacy:

- Bank should learn who you are, but not where (same with N).
- Merchant should learn where you are, but not who (same with S).

Weak Blind Signatures

- Blind signatures allow users to request signatures from someone without disclosing the message to be signed.
- A blind signature scheme consist of five algorithms:
  Key generation (Gen),
  Request (Req),
  Issue (Issue),
  Unblind (UnBlind), and
  Verify (Ver).
- Completeness:
  $(sk, vk) \leftarrow \mathsf{Gen}$
  $(\rho, s) \leftarrow \mathsf{Req}(vk, m)$
  $\tilde{\sigma} \leftarrow \mathsf{Issue}(sk, \rho)$
  $\sigma \leftarrow \mathsf{UnBlind}(s, \tilde{\sigma})$
  $\Rightarrow \mathsf{Ver}(vk, \sigma, m) = true$

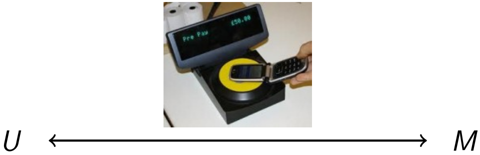
Weak Blind Signatures

- Weak Unforgeability:
  No efficient adversary (given a honestly generated vk) can sign more messages than he has received issue tokens $\tilde{\sigma}$.
- Weak Blindness:
  A bit technical, but essentially no efficient adversary (given honestly generated keys (sk, vk) can distinguish $\rho \leftarrow \mathsf{Req}(vk, m)$ from $\rho' \leftarrow \mathsf{Req}(vk, m')$ for any m, m'.

Weak Blind Signatures

- Weak Unforgeability:
  No efficient adversary (given a honestly generated vk) can sign more messages than he has received issue tokens $\tilde{\sigma}$.
- Weak Blindness:
  A bit technical, but essentially no efficient adversary (given honestly generated keys (sk, vk) can distinguish $\rho \leftarrow \mathsf{Req}(vk, m)$ from $\rho' \leftarrow \mathsf{Req}(vk, m')$ for any m, m'.
  (Even after seeing the corresponding signatures.)

Near Field Channel



- Attacker can delay/stop messages and eavesdrop, but not modify (unless U or M are corrupted).
- User identity does not leak.
- User location leaks if M is corrupt or adversary is eavsdropping.

Anonymous Online Channel

$$B \longleftrightarrow U$$

- A bit technical functionality (previous work).
- Adversary has full control of the network in corrupted locations.
- U's identity leaks only if service provider S is corrupted.
- However N can trace U through corrupted locations by denial of service attack.

Protocol

B U M

Protocol

$$\begin{tikzcd}
 & Tr, M, B \arrow[d] & Tr \arrow[d] \\
B & U & M
\end{tikzcd}$$

Protocol

$$\begin{tikzcd}
 & Tr, M, B \arrow[d] & Tr \arrow[d] \\
B & U \arrow[r, "Tr"] & M
\end{tikzcd}$$

Protocol

$$\begin{tikzcd}
 & Tr, M, B \arrow[d] & Tr \arrow[d] & \\
B & U \arrow[r, "Tr"] & M & \\
 & & & \color{red}{c}
\end{tikzcd}$$

Protocol

$$\begin{tikzcd}
 & Tr, M, B \arrow[d] & & Tr \arrow[d] & \\
B & U \arrow[rr, shift left=2, "Tr"] & & M \arrow[ll, shift left=2, "{c, \sigma_M(c, Tr)}"] & c
\end{tikzcd}$$

Protocol

$$\begin{tikzcd}
 & Tr, M, B \arrow[d] & & Tr \arrow[d] & \\
B & U \arrow[rr, shift left, "Tr"] & & M \arrow[ll, shift left, "{c, \sigma_M(c, Tr)}"'] & \textcolor{red}{c} \\
 & \textcolor{red}{k} & & & \\
 & \textcolor{red}{(\rho, s)} & & &
\end{tikzcd}$$

- $(\rho, s) \leftarrow \mathsf{Req}(vk, (M, c))$.

Protocol

$$\begin{tikzcd}
 & Tr, M, B \arrow[d] & Tr \arrow[d] & \\
B & U \arrow[l, "\{\rho, U, k, \sigma_U\}_{pk_B}"'] \arrow[r, shift left, "Tr"] & M \arrow[l, shift left, "{c, \sigma_M(c, Tr)}"'] & c \\
 & \begin{array}{c} k \\ (\rho, s) \end{array} & &
\end{tikzcd}$$

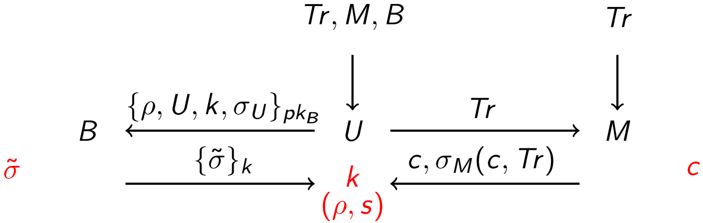
- $(\rho, s) \leftarrow \mathsf{Req}(vk, (M, c))$.
- $\tilde{\sigma} \leftarrow \mathsf{Issue}(sk, \rho)$.

Protocol

$$\begin{tikzcd}
 & & Tr, M, B \arrow[d] & Tr \arrow[d] & \\
 & B & U \arrow[l, "\{\rho, U, k, \sigma_U\}_{pk_B}"'] \arrow[r, "Tr"] & M \arrow[l, shift left=2, "{c, \sigma_M(c, Tr)}"'] & \\
\tilde{\sigma} & & \begin{array}{c} k \\ (\rho, s) \end{array} & & c
\end{tikzcd}$$

- $(\rho, s) \leftarrow \mathrm{Req}(vk, (M, c))$.
- $\tilde{\sigma} \leftarrow \mathrm{Issue}(sk, \rho)$.

Protocol



Tr, M, B

Tr

$\{\rho, U, k, \sigma_U\}_{pk_B}$

B

U

Tr

M

$\tilde{\sigma}$

$\{\tilde{\sigma}\}_k$

k

(ρ, s)

$c, \sigma_M(c, Tr)$

c

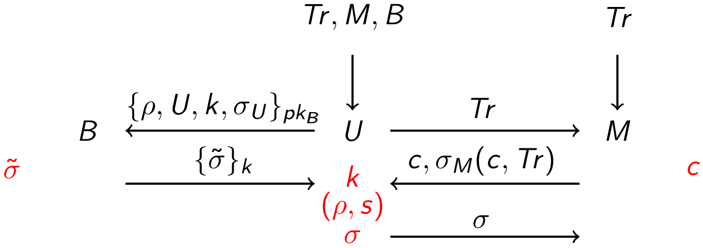
- $(\rho, s) \leftarrow \mathsf{Req}(vk, (M, c))$.
- $\tilde{\sigma} \leftarrow \mathsf{Issue}(sk, \rho)$.

Protocol

$$\begin{tikzcd}
 & & Tr, M, B \arrow[d] & Tr \arrow[d] & \\
 & B & U \arrow[l, "\{\rho, U, k, \sigma_U\}_{pk_B}"'] \arrow[r, "Tr"] & M & \\
\tilde{\sigma} & {} \arrow[r, "\{\tilde{\sigma}\}_k"] & \begin{array}{c} k \\ (\rho, s) \\ \sigma \end{array} & {} \arrow[l, "{c, \sigma_M(c, Tr)}"'] & c
\end{tikzcd}$$

- $(\rho, s) \leftarrow \mathsf{Req}(vk, (M, c))$.
- $\tilde{\sigma} \leftarrow \mathsf{Issue}(sk, \rho)$.
- $\sigma \leftarrow \mathsf{UnBlind}(s, \tilde{\sigma})$.

Protocol



- $(\rho, s) \leftarrow \mathrm{Req}(vk, (M, c))$.
- $\tilde{\sigma} \leftarrow \mathrm{Issue}(sk, \rho)$.
- $\sigma \leftarrow \mathrm{UnBlind}(s, \tilde{\sigma})$.

Thank You.