Specifying authentication protocols for pervasive and social computation

Dusko Pavlovic

Kestrel Institute
and
Oxford University

Granada, January 2008

Outline

Deriving distance bounding authentication protocols

Deriving social authentication protocols

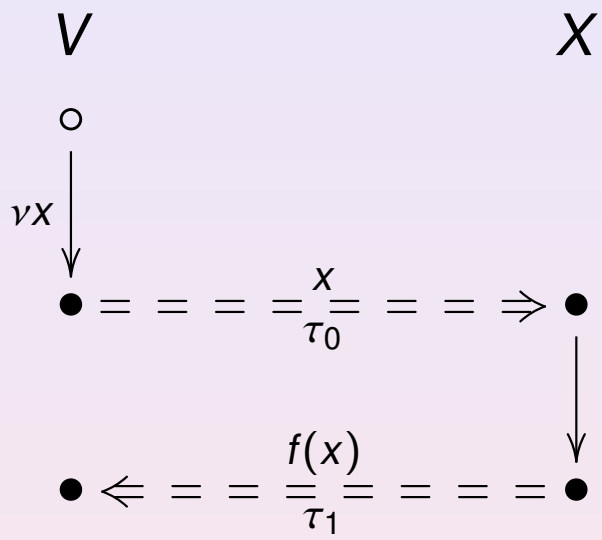
Outline

Deriving distance bounding authentication protocols

- Timed challenge-response
- Binding timed response and crypto response
- Binding timed response and crypto challenge
- Mixing timed channels

Deriving social authentication protocols

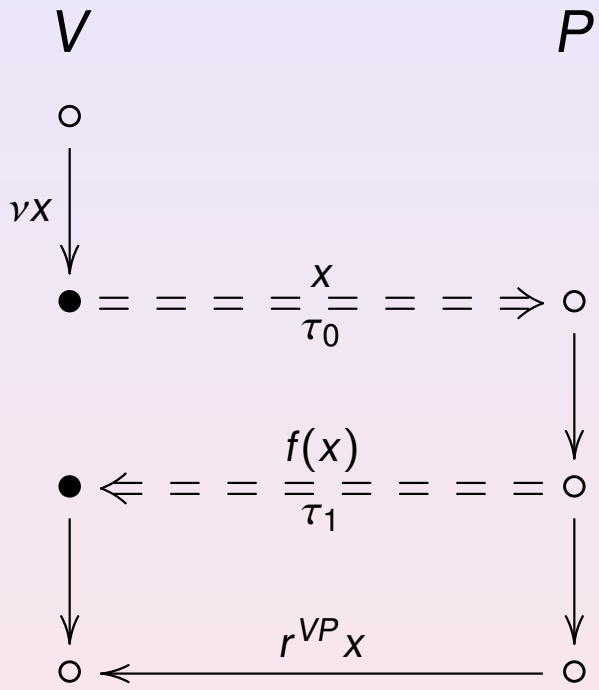
Timed challenge-response



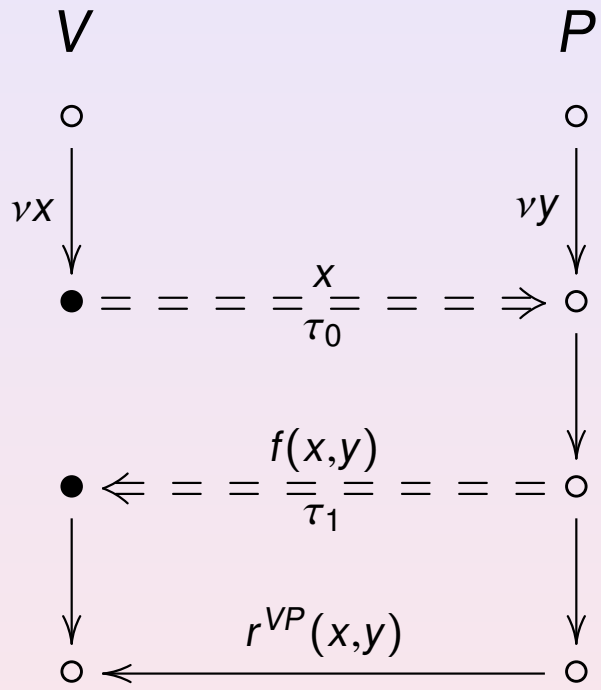
supports the axiom

$$V:\ (\nu x)_V\Big(\tau_0\langle x\rangle_V < \tau_1((x))_V \Longrightarrow \exists X.\, d(V,X) \le \tau_1 - \tau_0\Big)$$

Combining timed response and cryptographic response

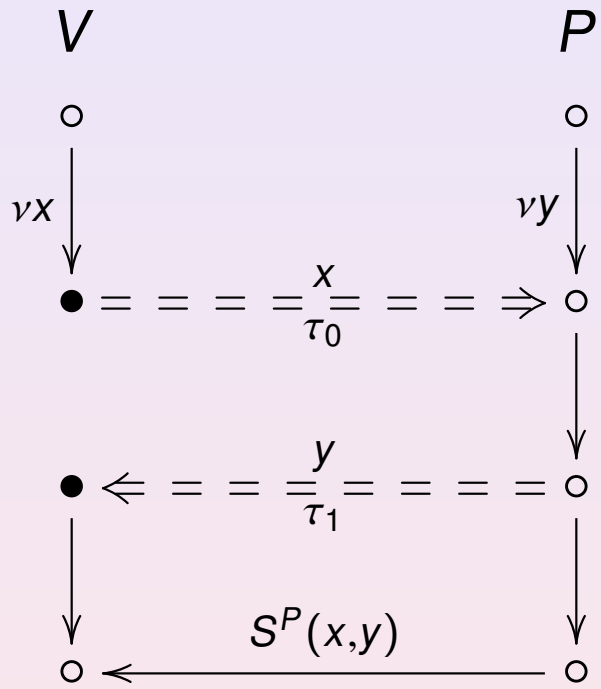


Binding timed response to cryptographic response



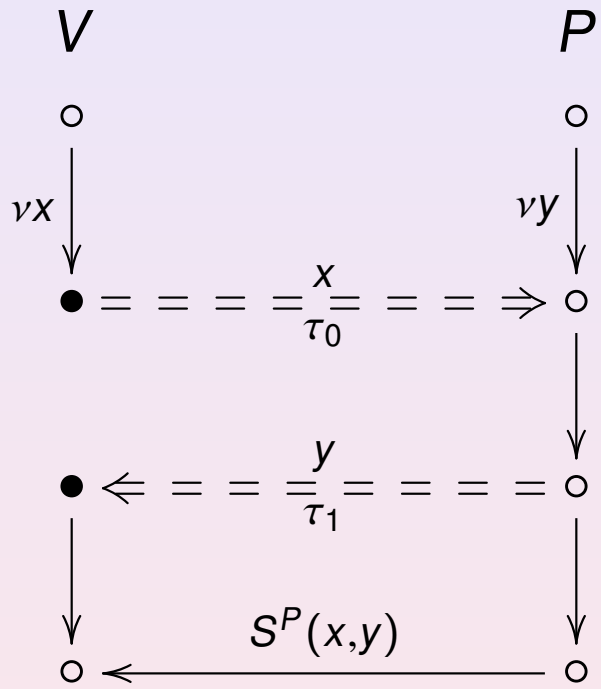
Binding timed response to cryptographic response

Brands-Chaum 1



Binding timed response to cryptographic response

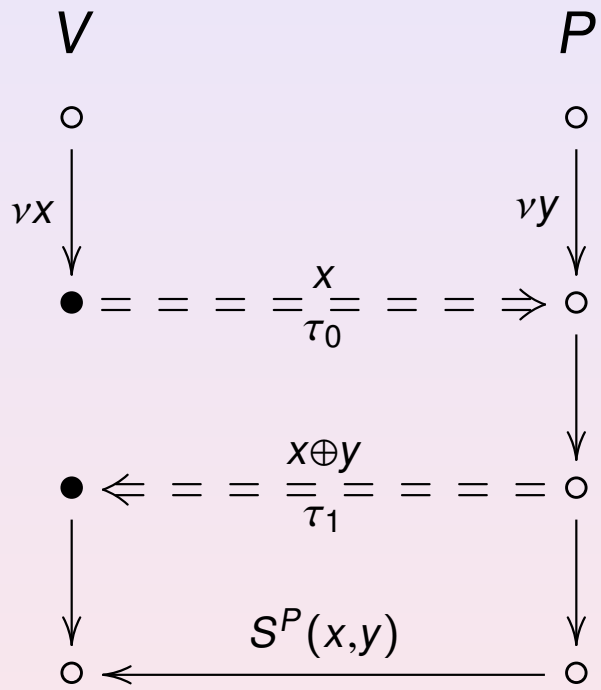
Brands-Chaum 1



- V : P honest $\Longrightarrow$ $d(V,P) < \tau_1 - \tau_0$
- V : $\forall X.P$ responds to $X \Longrightarrow d(V,X)+d(X,P) < \tau_1 - \tau_0$

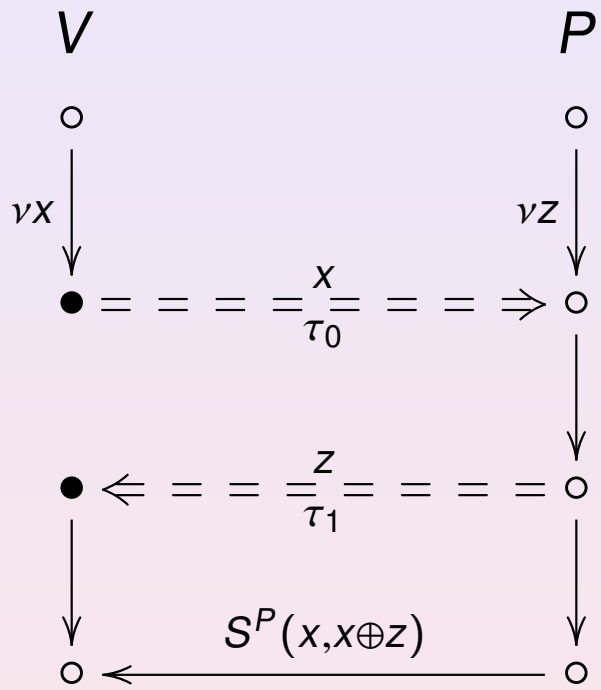
Binding timed response to cryptographic response

Discharge the honesty assumption?



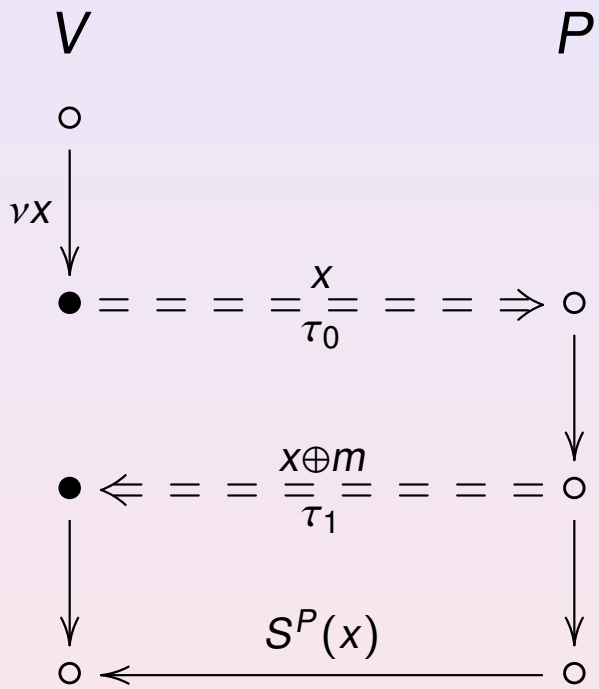
Binding timed response to cryptographic response

P can still cheat



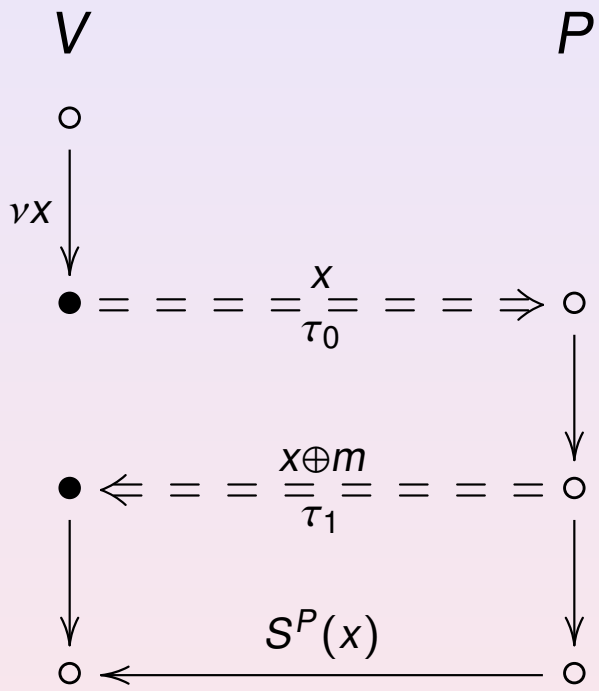
Binding timed response to cryptographic response

Brands-Chaum 2



Binding timed response to cryptographic response

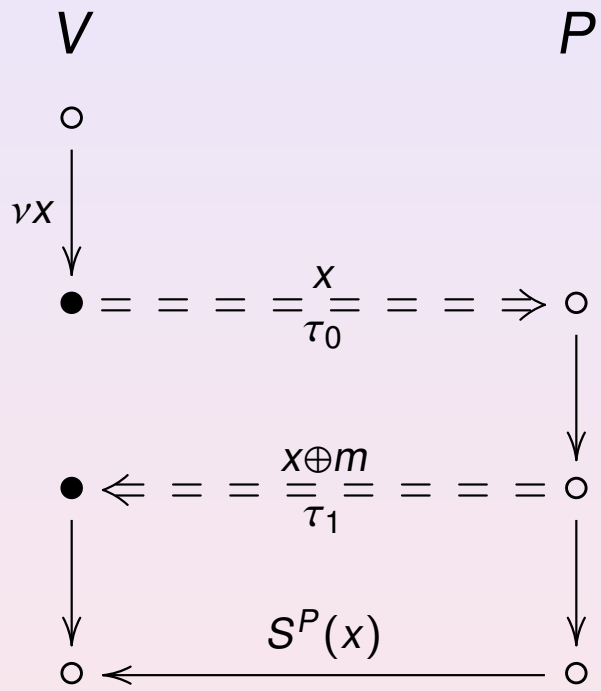
Brands-Chaum 2



- Peggy cannot cheat

Binding timed response to cryptographic response

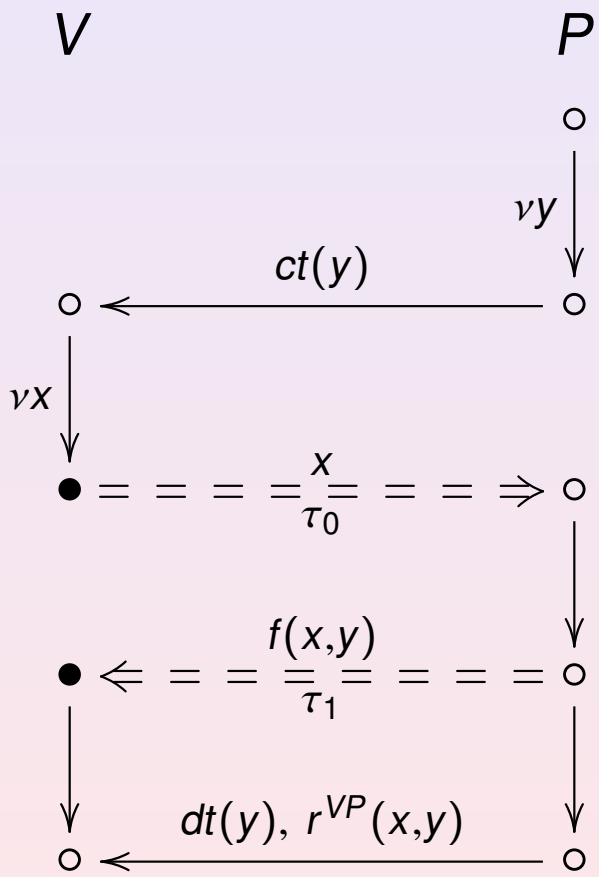
Brands-Chaum 2



- Peggy cannot cheat
- Ivan can impersonate her, and relay $S^P(x)$

Binding timed response to cryptographic response

— with commitment



Digression: Symbolic commitment

Definition

A *commitment schema* consists of three publicly known functions over the space of messages $\mathcal{T}$,

- *commitment* $ct : \mathcal{T} \longrightarrow \mathcal{T}$,
- *decommitment* $dt : \mathcal{T} \longrightarrow \mathcal{T}$, and
- *open commitment* $ot : \mathcal{T} \times \mathcal{T} \longrightarrow \mathcal{T}$,

such that

- ct is a one-way collision-free function,
- $ot\,(ct(x), dt(x)) = x$.

Digression: Symbolic commitment

Definition

A *commitment schema* consists of three publicly known functions over the space of messages $\mathcal{T}$,

- *commitment* $ct : \mathcal{T} \longrightarrow \mathcal{T}$,
- *decommitment* $dt : \mathcal{T} \longrightarrow \mathcal{T}$, and
- *open commitment* $ot : \mathcal{T} \times \mathcal{T} \longrightarrow \mathcal{T}$,

such that

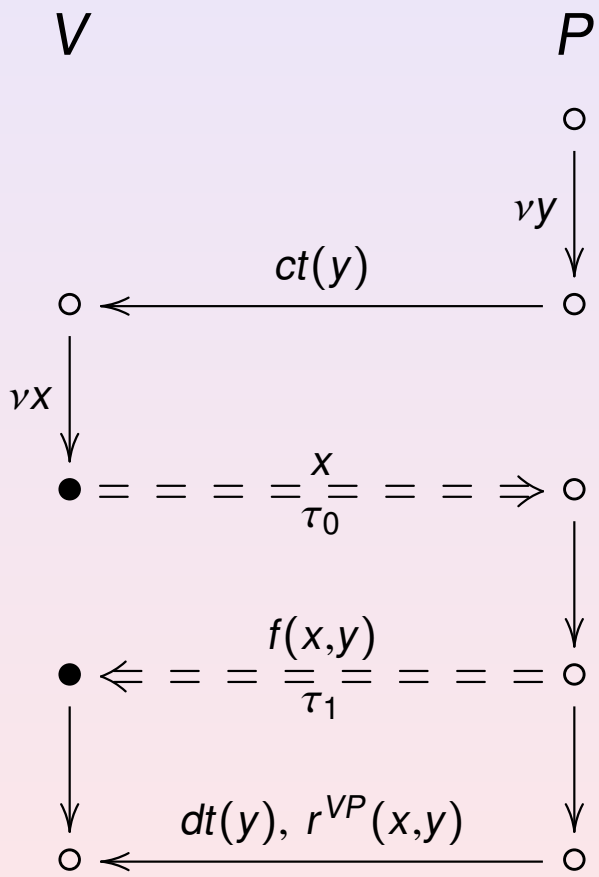
- ct is a one-way collision-free function,
- $ot\,(ct(x), dt(x)) = x$.

E.g.,

$$ct(x) = H(x) \qquad ct(x) = H_0(x) \qquad ct(x) = E(x_0, x_1)$$
$$dt(x) = x \qquad dt(x) = H_1(x)::x \qquad dt(x) = x_0$$
$$ot(y,z) = z \qquad ot(y,z) = z_1 \qquad ot(y,z) = D(z,y)$$

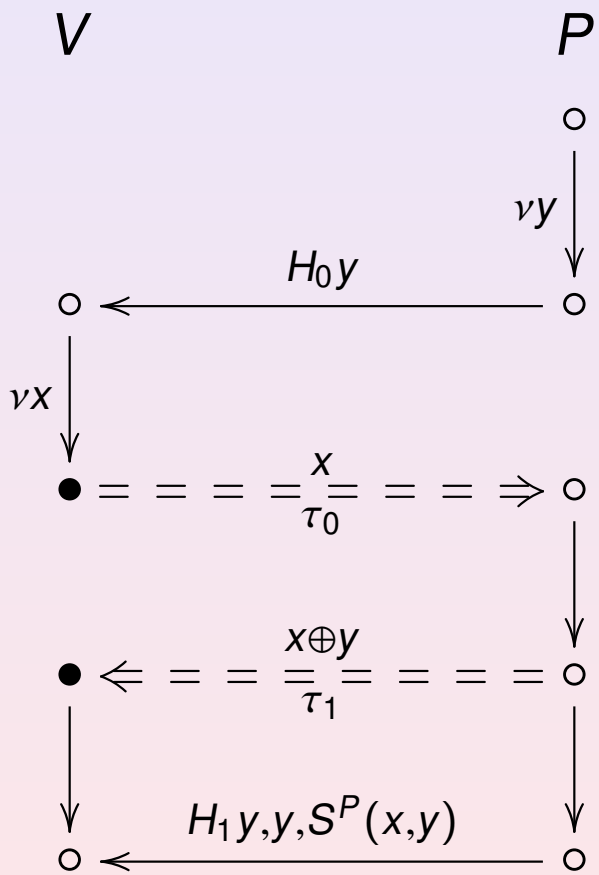
Binding timed response to cryptographic response

— with commitment



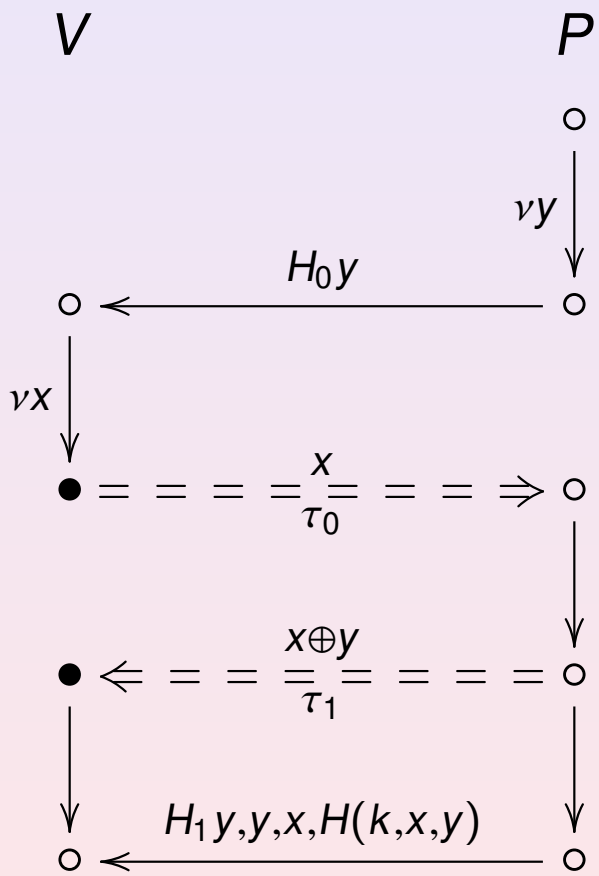
Binding timed response to cryptographic response

Brands-Chaum 3



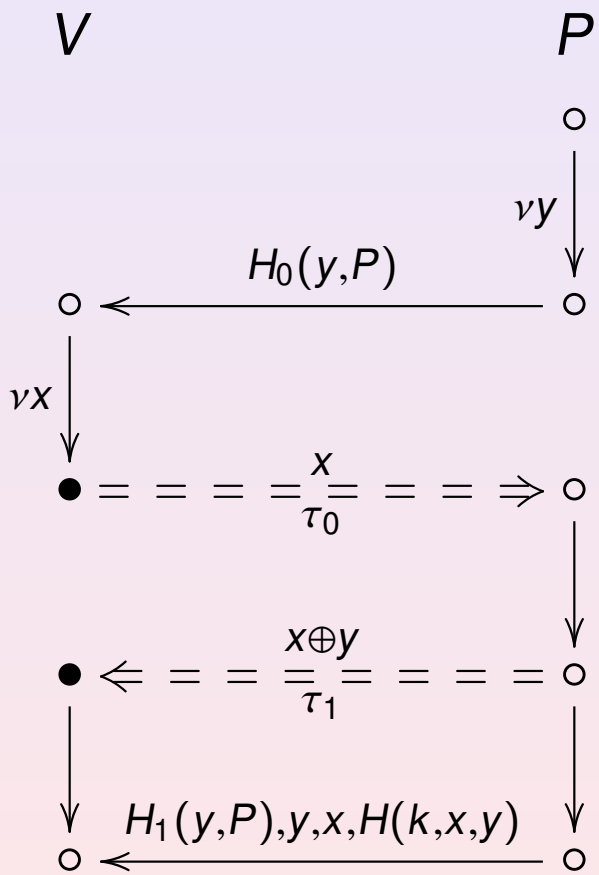
Binding timed response to cryptographic response

Čapkun-Hubaux



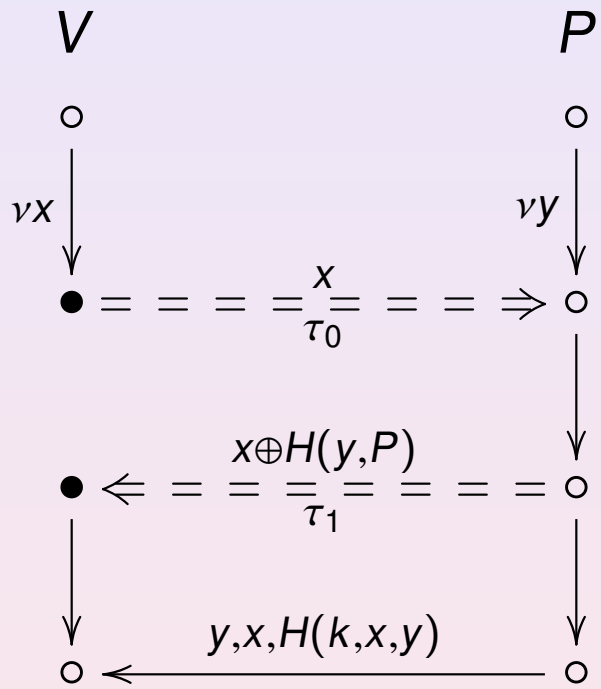
Binding timed response to cryptographic response

Meadows-Syverson



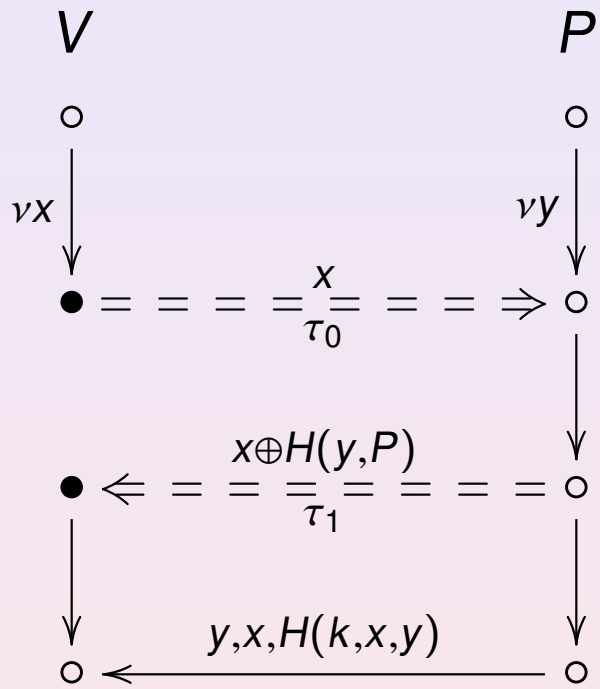
Binding timed response to cryptographic response

Meadows-P-Syverson



Binding timed response to cryptographic response

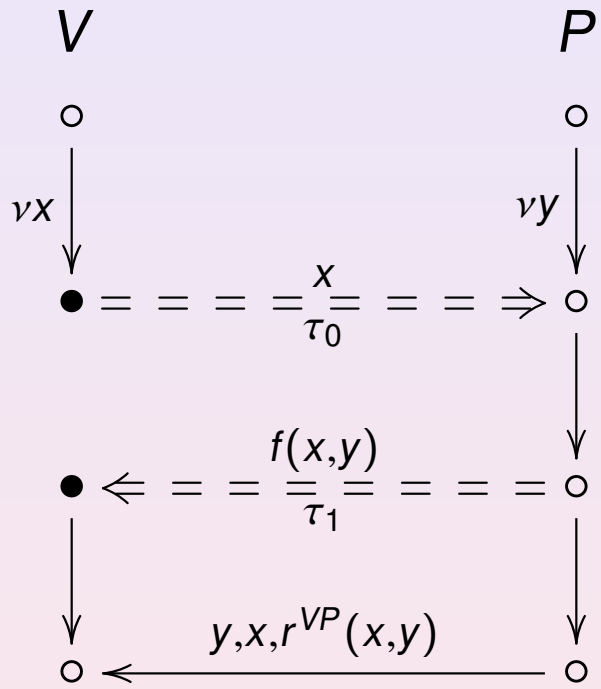
Meadows-P-Syverson



- $V:\ d(V,\widetilde{P}) < \tau_1 - \tau_0$
- $V:\ \forall X.P$ responds to $X \Longrightarrow d(V,X)+d(X,P) < \tau_1 - \tau_0$

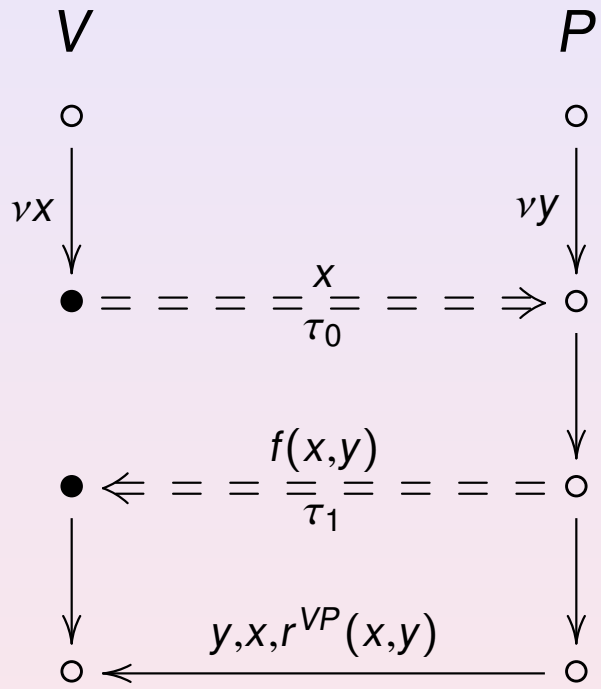
Binding timed response to cryptographic response

. . . and in general



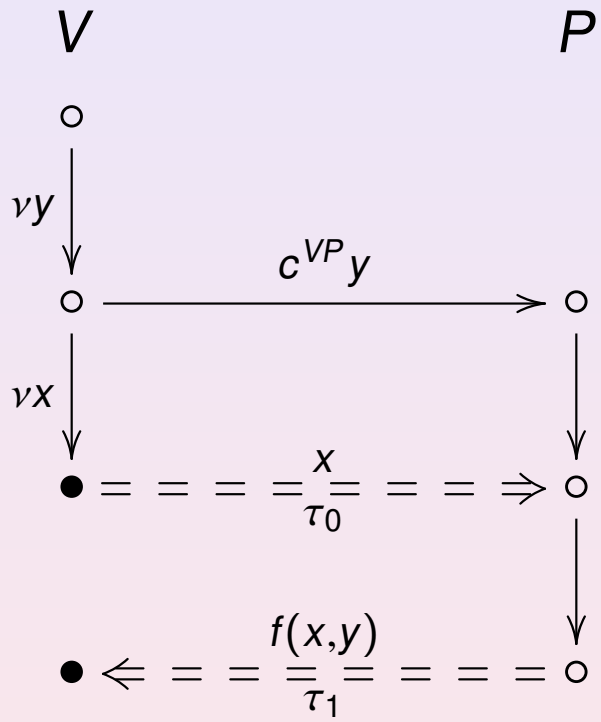
Binding timed response to cryptographic response

. . . and in general

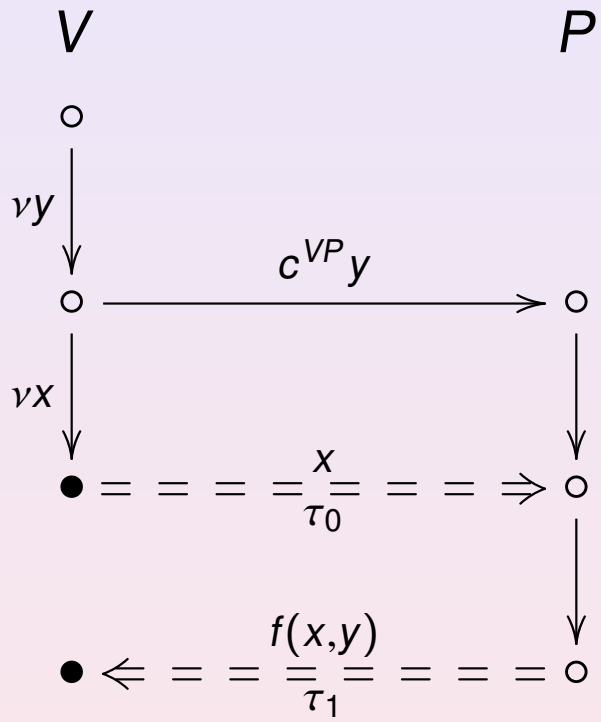


- $f(x, y)$ one-way function in y
- only P could generate $r^{VP}(x, y)$.

Binding timed response and cryptographic **challenge**

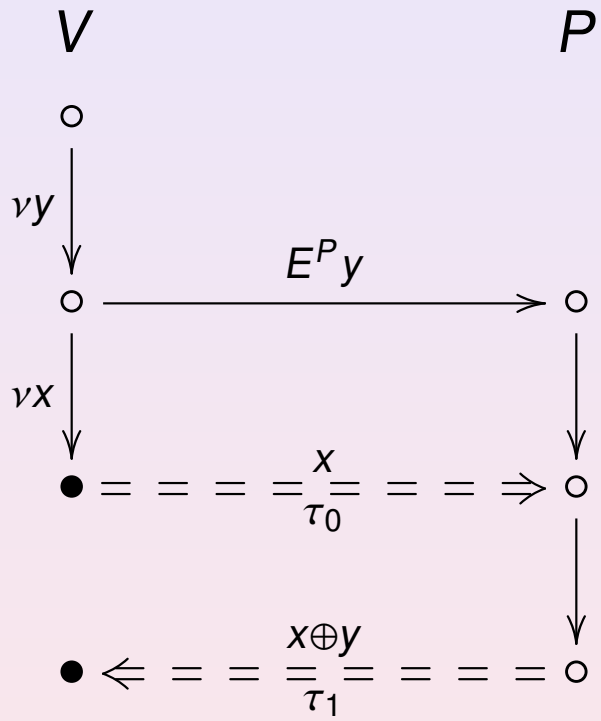


Binding timed response and cryptographic **challenge**



(more convenient when P is a smart card)

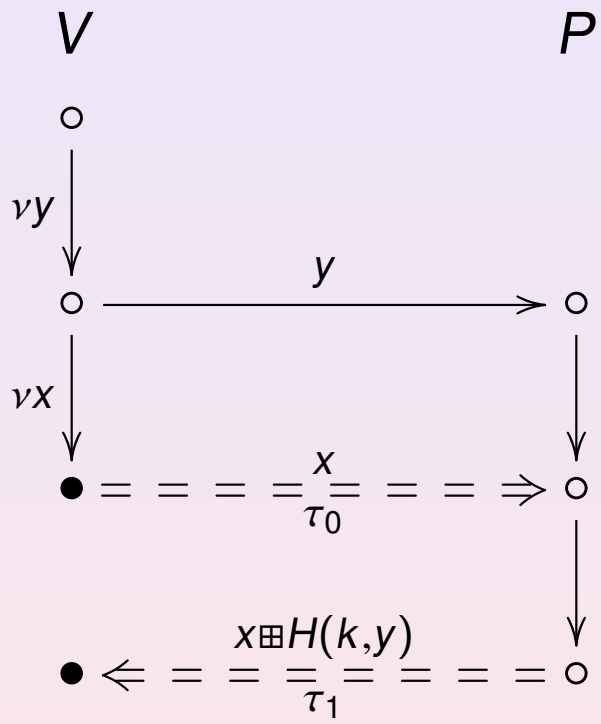
Binding timed response and cryptographic challenge



(if P has a public key)

Binding timed response to cryptographic challenge

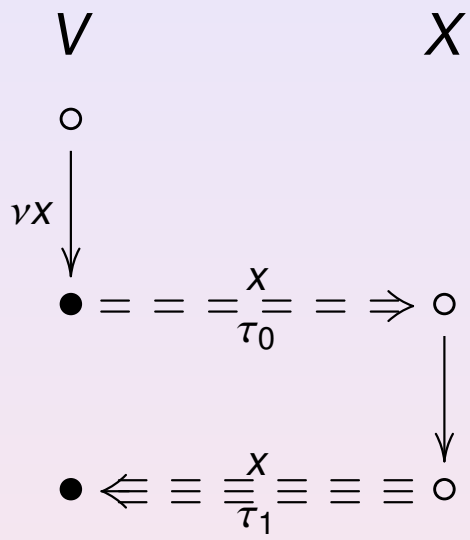
Hancke-Kuhn



$$x \boxplus z \;=\; [z_i^{(x_i)}] \quad \text{where } z = z^{(0)}::z^{(1)}$$

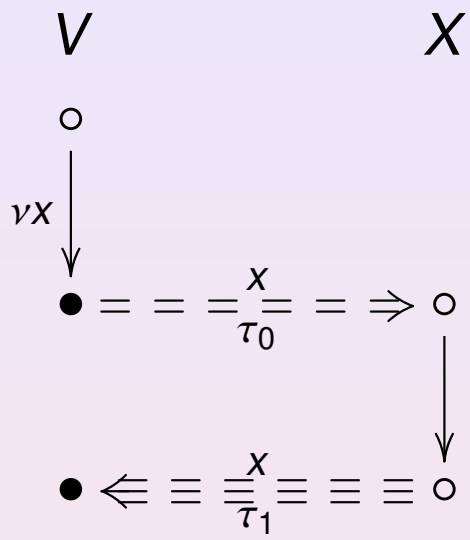
Mixing different kinds of timed channels

ECHO: Sastry-Sankar-Wagner



Mixing different kinds of timed channels

ECHO: Sastry-Sankar-Wagner

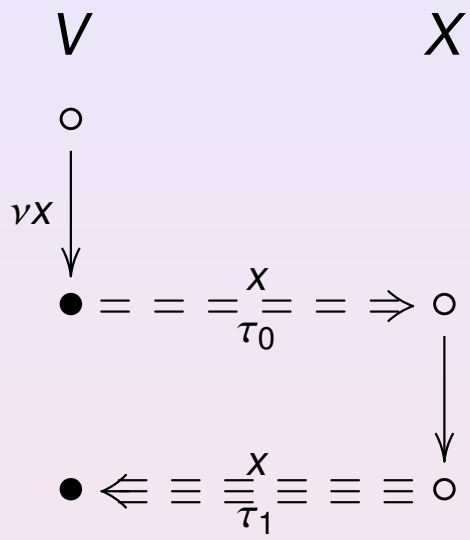


$$V:\ (\nu x)_V\Big(\tau_0\langle\langle x\rangle\rangle_V < \tau_1((x))_V \Longrightarrow \exists X.\ d(V,X) \le (\tau_1-\tau_0)\frac{c+s}{cs}\Big)$$

- where c is the speed of light and s the speed of sound

Mixing different kinds of timed channels

ECHO: Sastry-Sankar-Wagner

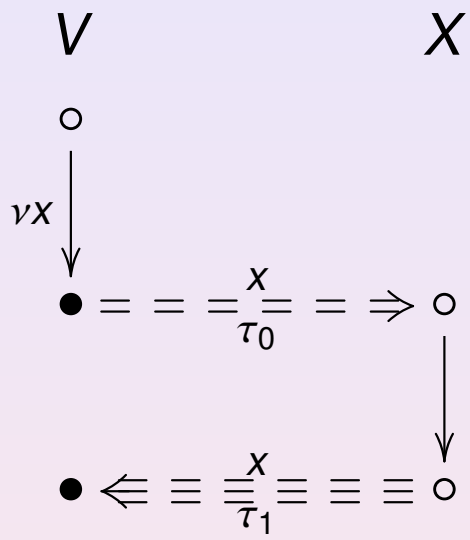


$$V:\ (\nu x)_V\Big(\tau_0\langle\langle x\rangle\rangle_V < \tau_1((x))_V \Longrightarrow \exists X.\, d(V,X) \le (\tau_1-\tau_0)\frac{c+s}{cs}\Big)$$

- where c is the speed of light and s the speed of sound
- the reasoning boils down to (crt)), because $s \ll c \implies \frac{c+s}{cs} \approx 1$

Mixing different kinds of timed channels

ECHO: Sastry-Sankar-Wagner



$$V:\ (\nu x)_V\Big(\tau_0\langle\langle x\rangle\rangle_V < \tau_1((x))_V \Longrightarrow \exists X.\, d(V,X) \le (\tau_1-\tau_0)\frac{c+s}{cs}\Big)$$

- where c is the speed of light and s the speed of sound
- the reasoning boils down to (crt)), because $s \ll c \implies \frac{c+s}{cs} \approx 1$
- **pro:** measuring longer response times requires less precision
- **con:** s less robust, due to the influences of the environment

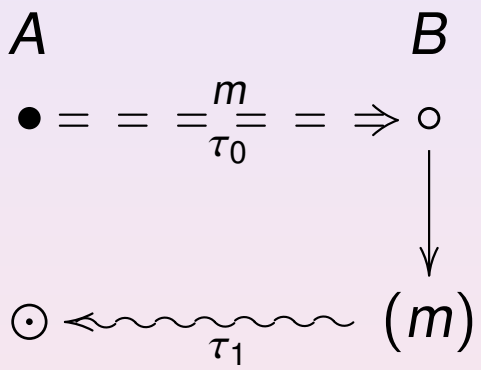
Outline

Deriving distance bounding authentication protocols

Deriving social authentication protocols

- Social channel basics
- Socially authenticated key distribution
- Socially authenticated key exchange

Preliminary example: a timed social protocol



Social actions

- $<\!\!\cdot\vartheta\cdot\!\!>_{B\to A}$ — B displays ϑ for A to see
  - where ϑ may be a term t, or an action β

Social actions

- $\langle\!\langle \vartheta \rangle\!\rangle_{B \to A}$ — B displays ϑ for A to see
  - where ϑ may be a term t, or an action β

such that

- $\langle\!\langle \beta \rangle\!\rangle_{B \to A} \implies A : \beta_B$
  - "If A observes an action β, then A knows that this action has occurred."
- $\langle\!\langle \beta \rangle\!\rangle_{B \to A} < \langle\!\langle \gamma \rangle\!\rangle_{C \to A} \implies A : \beta_B < \gamma_C$
  - "If A observes an action β_B before γ_C, then she knows that β_B really occurs before γ_C."
- $\langle\!\langle \beta(t) \rangle\!\rangle_{B \to A} \implies \sigma t \in \Gamma_A$
  - "If A observes an action with a term t, then the digest σt of that term becomes an element of A's environment."
- $\forall T \in \Theta \forall t \in T \exists u \in T.\ u \neq t \ \wedge \ \sigma u = \sigma t$
  - "For every sufficiently large set of terms T and every $t \in T$ it is feasible to find a different term $u \in T$ with the same digest."

Social actions

Graphic notation

- $\odot_A \beta(t)_B$ is represented by $\beta_B \overset{\sigma t}{\rightsquigarrow} \odot_A$
- $\langle\!\langle \sigma t \rangle\!\rangle_{B \to A}$ is represented by $\circ_B \overset{\sigma t}{\rightsquigarrow} \odot_A$

Social actions

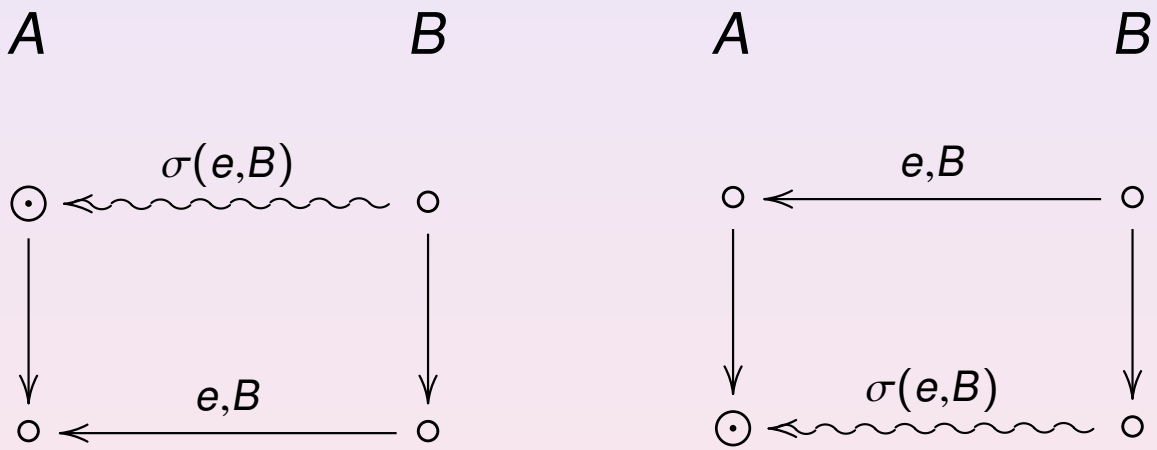
Graphic notation

- $\odot_A \beta(t)_B$ is represented by $\beta_B \overset{\sigma t}{\rightsquigarrow} \odot_A$
- $\langle\!\langle \sigma t \rangle\!\rangle_{B \to A}$ is represented by $\circ_B \overset{\sigma t}{\rightsquigarrow} \odot_A$

(σ annotations are redundant; a useful reminder.)

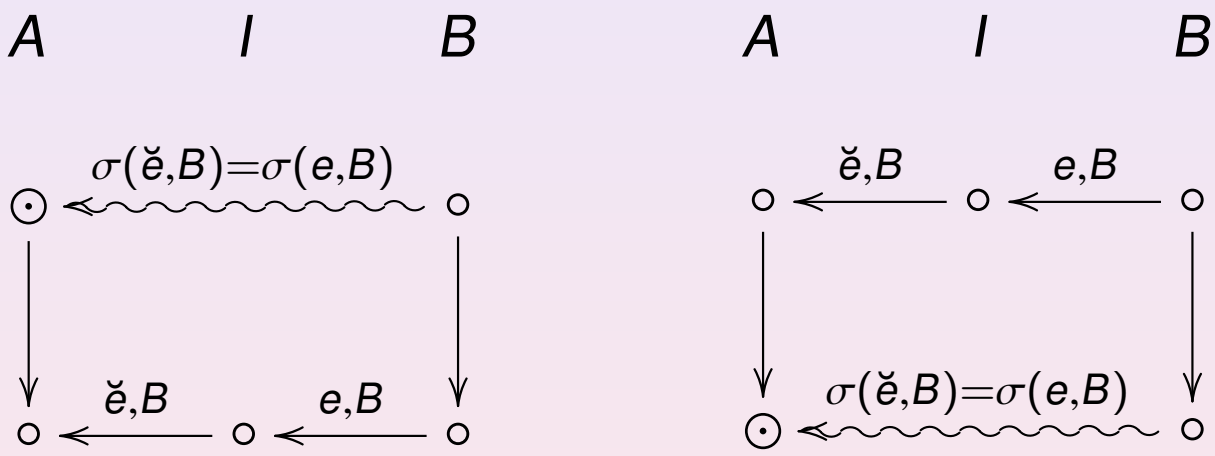
Socially authenticated key distribution

Bob announces his public key e from $B(d, e)$

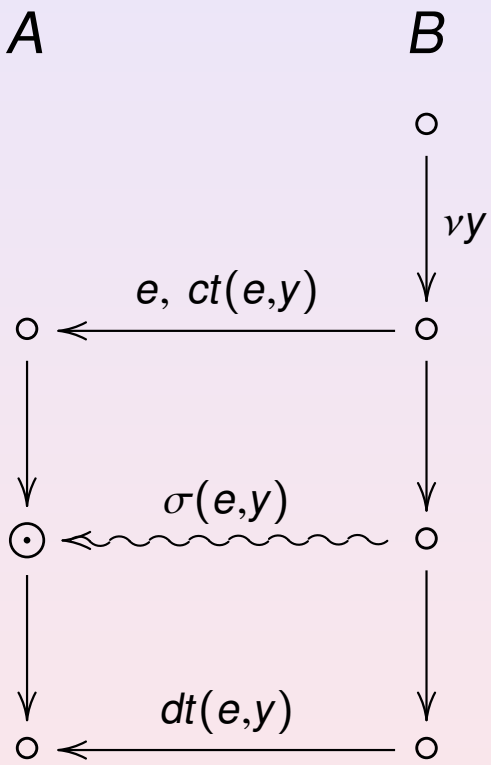


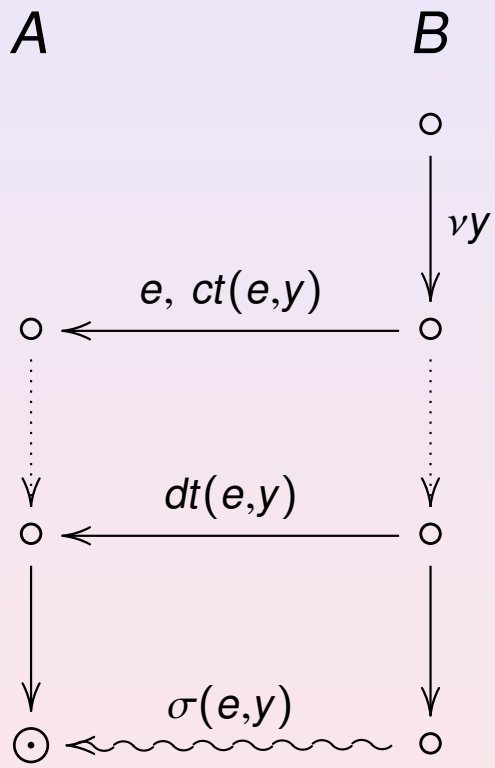
Socially authenticated key distribution

Ivan replaces it with $\check{e}$ from $I(\check{d}, \check{e})$



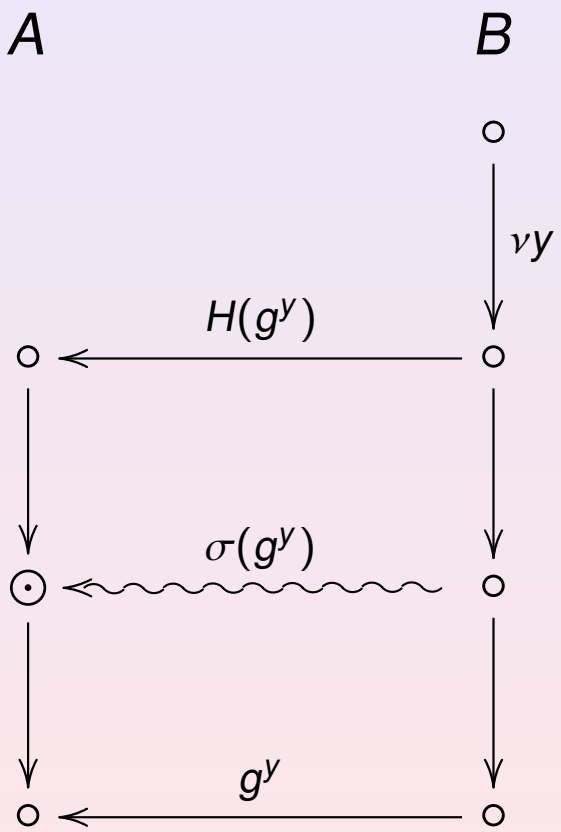
Social commitment



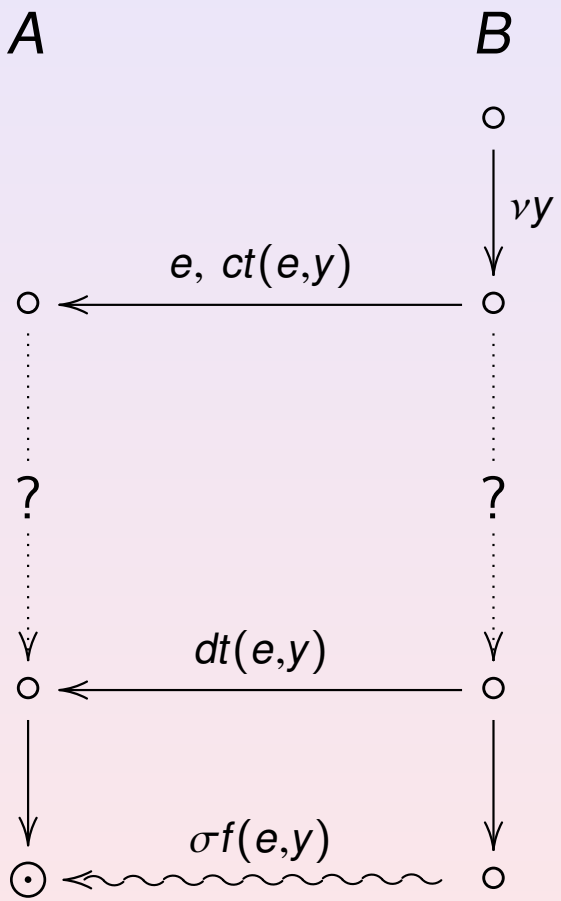


Authentication before decommitment

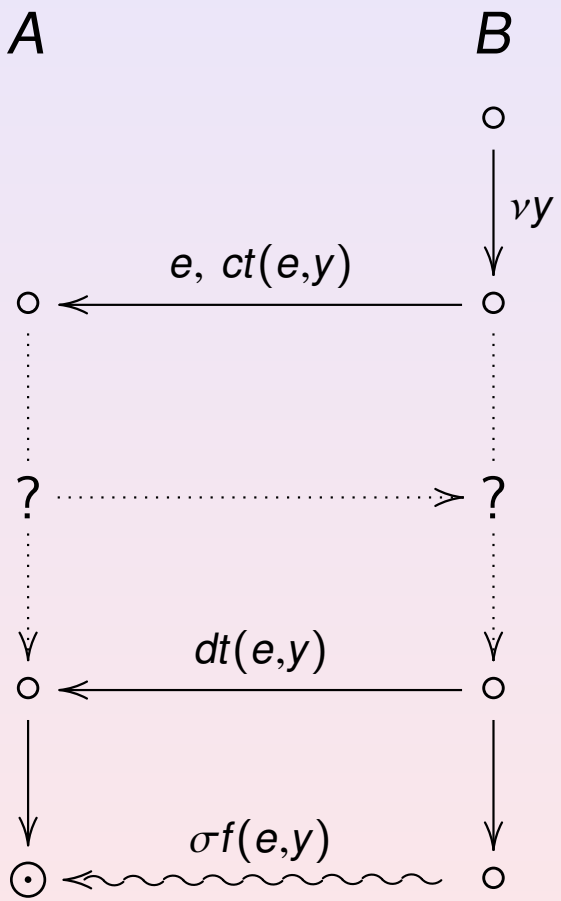
Hoepman



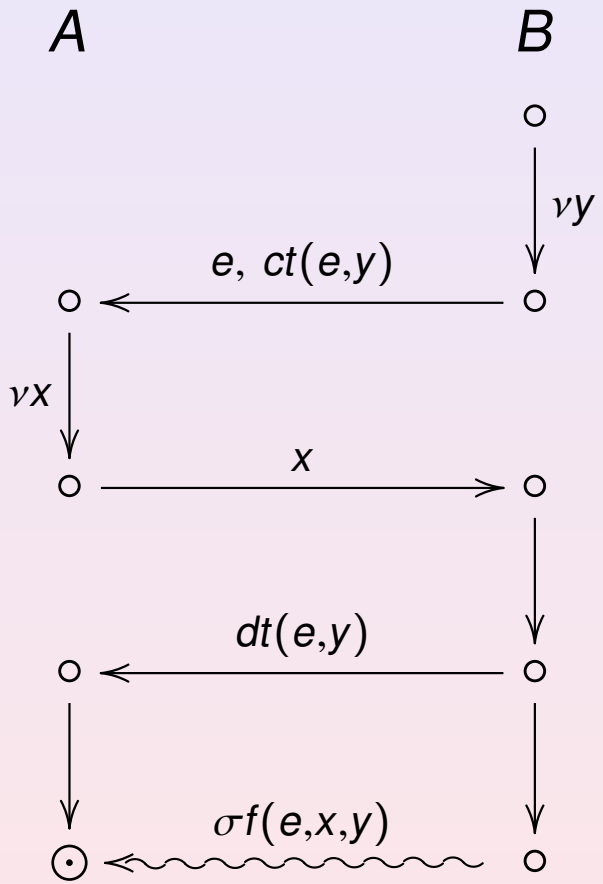
Authentication after decommitment



Authentication after decommitment

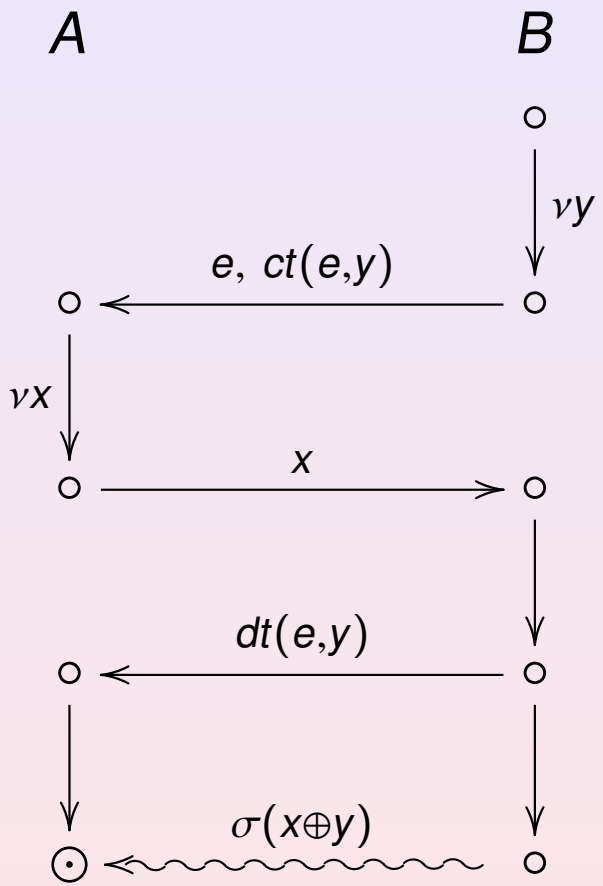


Authentication after decommitment

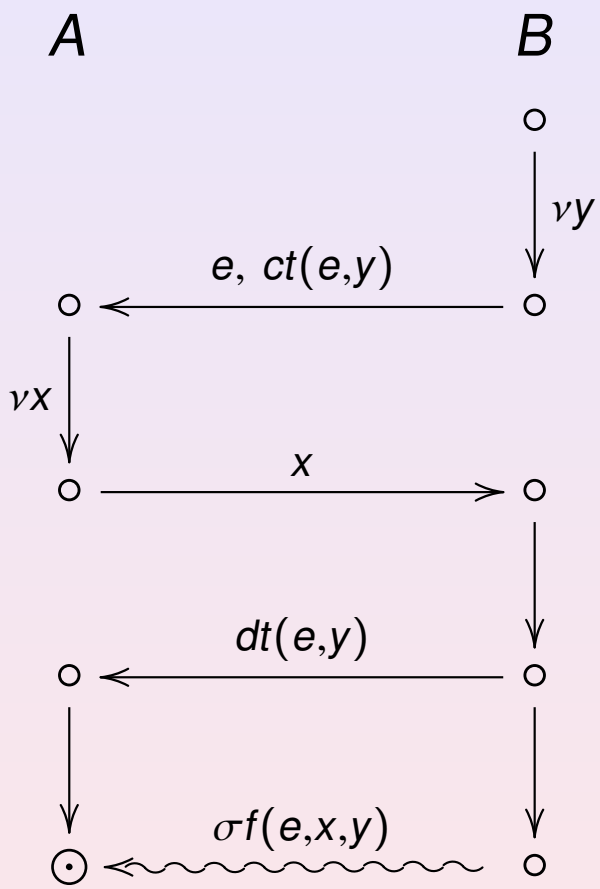


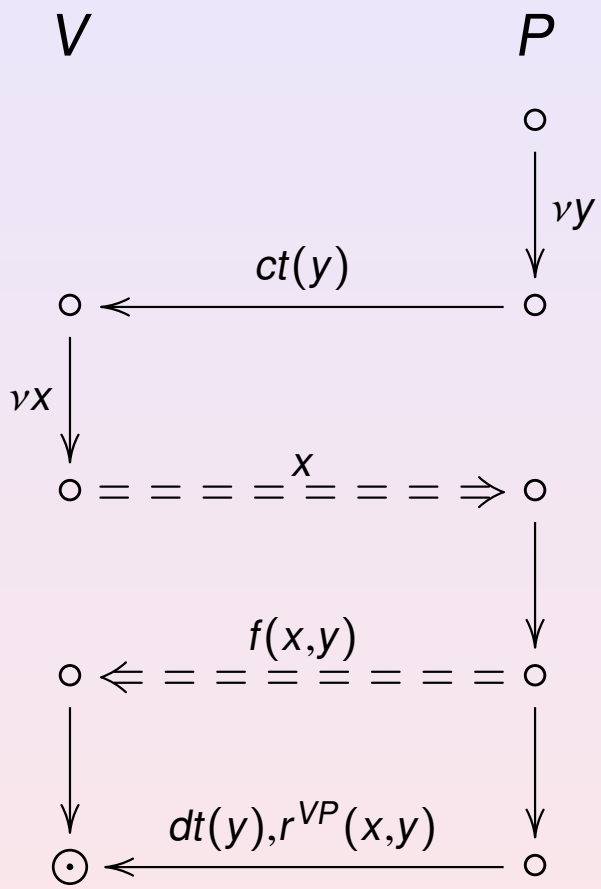
Authentication after decommitment

SAS: Vaudenay

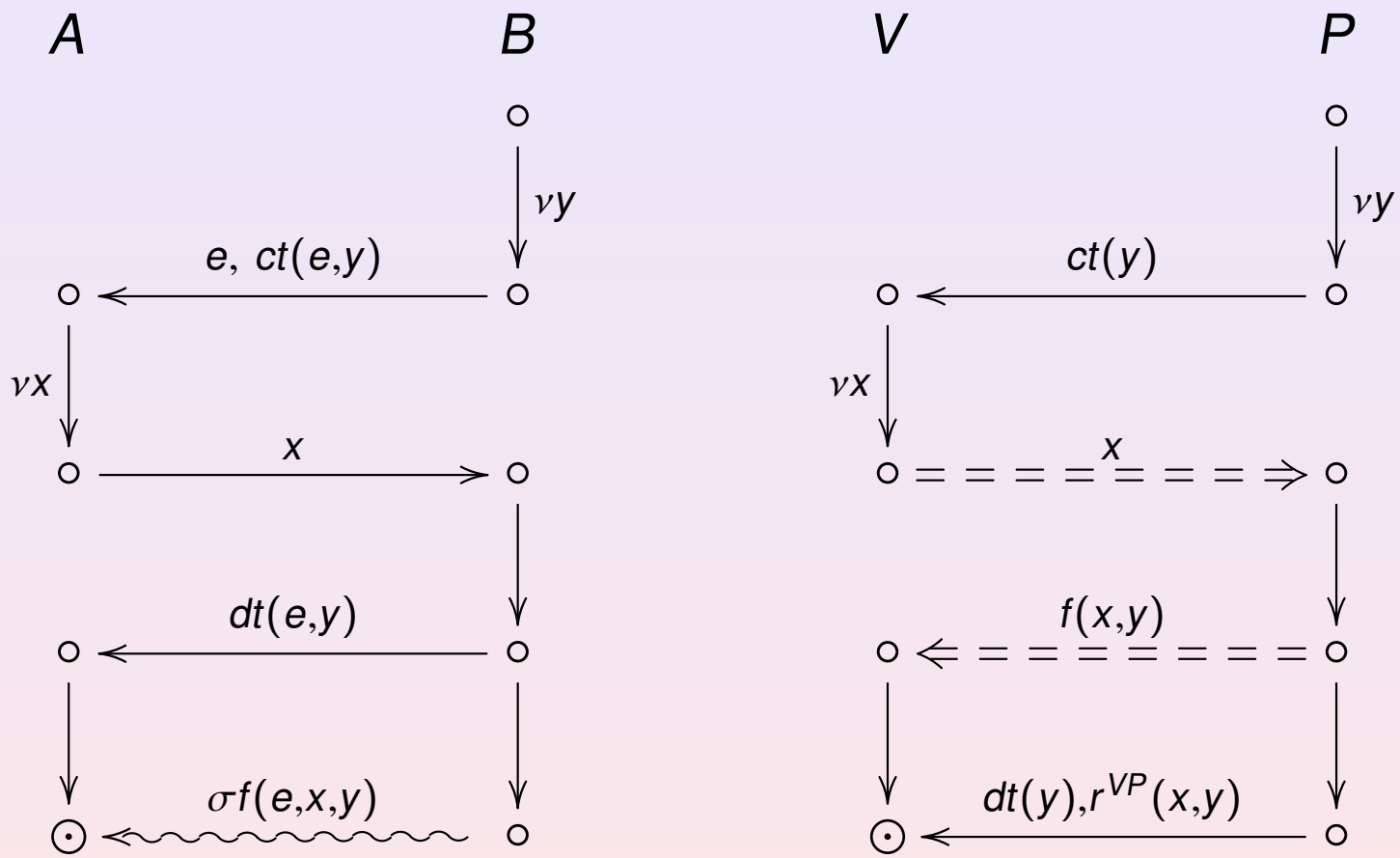


Structural similarity — conceptual difference





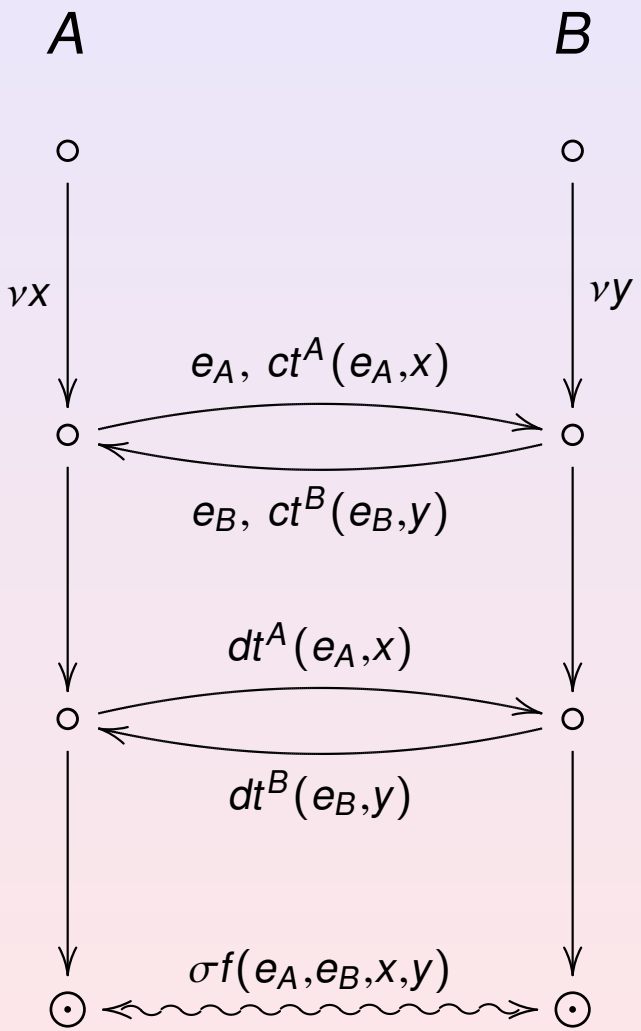
Structural similarity — conceptual difference



Social authentication is not challenge-response:

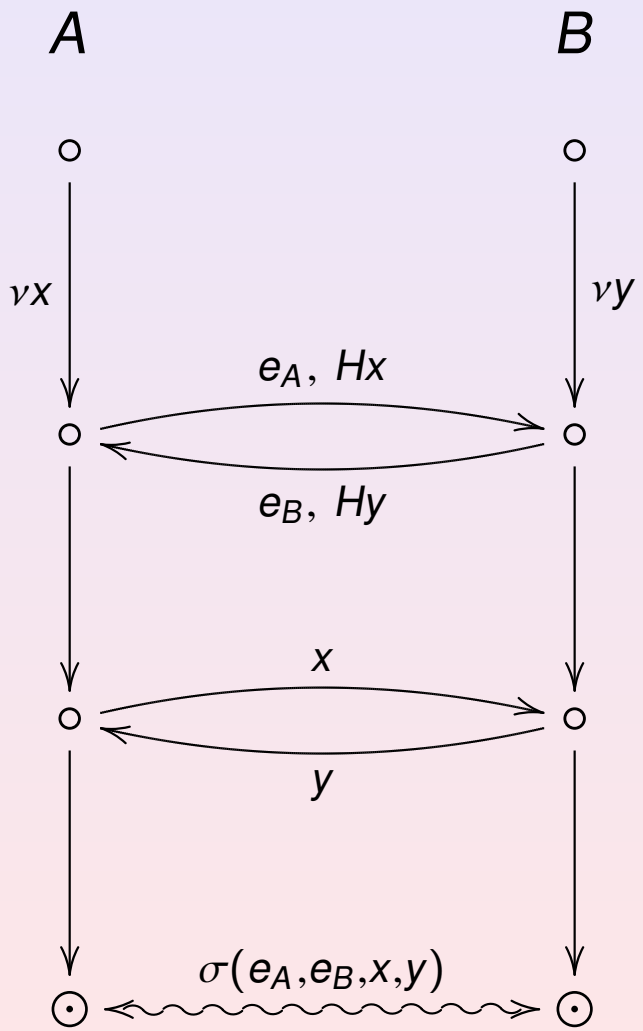
x on the left is not a challenge, but a binder, analogous to y.

Mutual authentication



Mutual authentication

HCBK: Nguyen-Roscoe



Mutual authentication

HCBK: Nguyen-Roscoe

$$\Big((\nu x)_A \ \langle e_A, Hx \rangle_A \ (u_1, u_2)_A \ \otimes$$

$$(\nu y)_B \ \langle e_B, Hy \rangle_B \ (v_1, v_2)_B \Big) \ ;$$

$$\Big(\langle x \rangle_A \ (u_3)_A \ (u_1, u_2 / e_B, Hu_3)_A \ \prec \sigma(e_A, e_B, x, u_3) \succ_A \ \otimes$$

$$\langle y \rangle_B \ (v_3)_B \ (v_1, v_2) / e_A, Hv_3)_B \ \prec \sigma(e_A, e_B, v_3, y) \succ_B \Big)$$