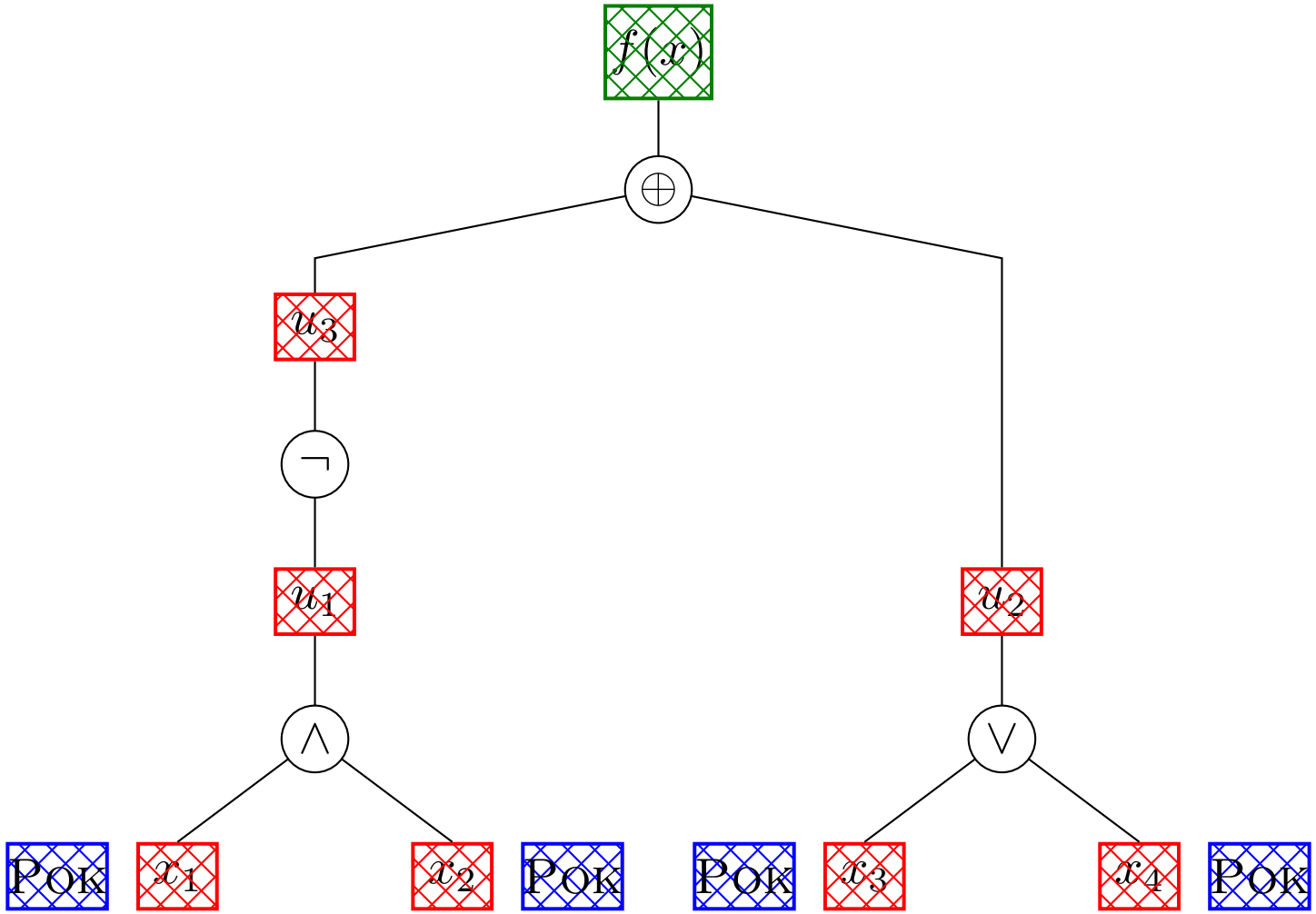
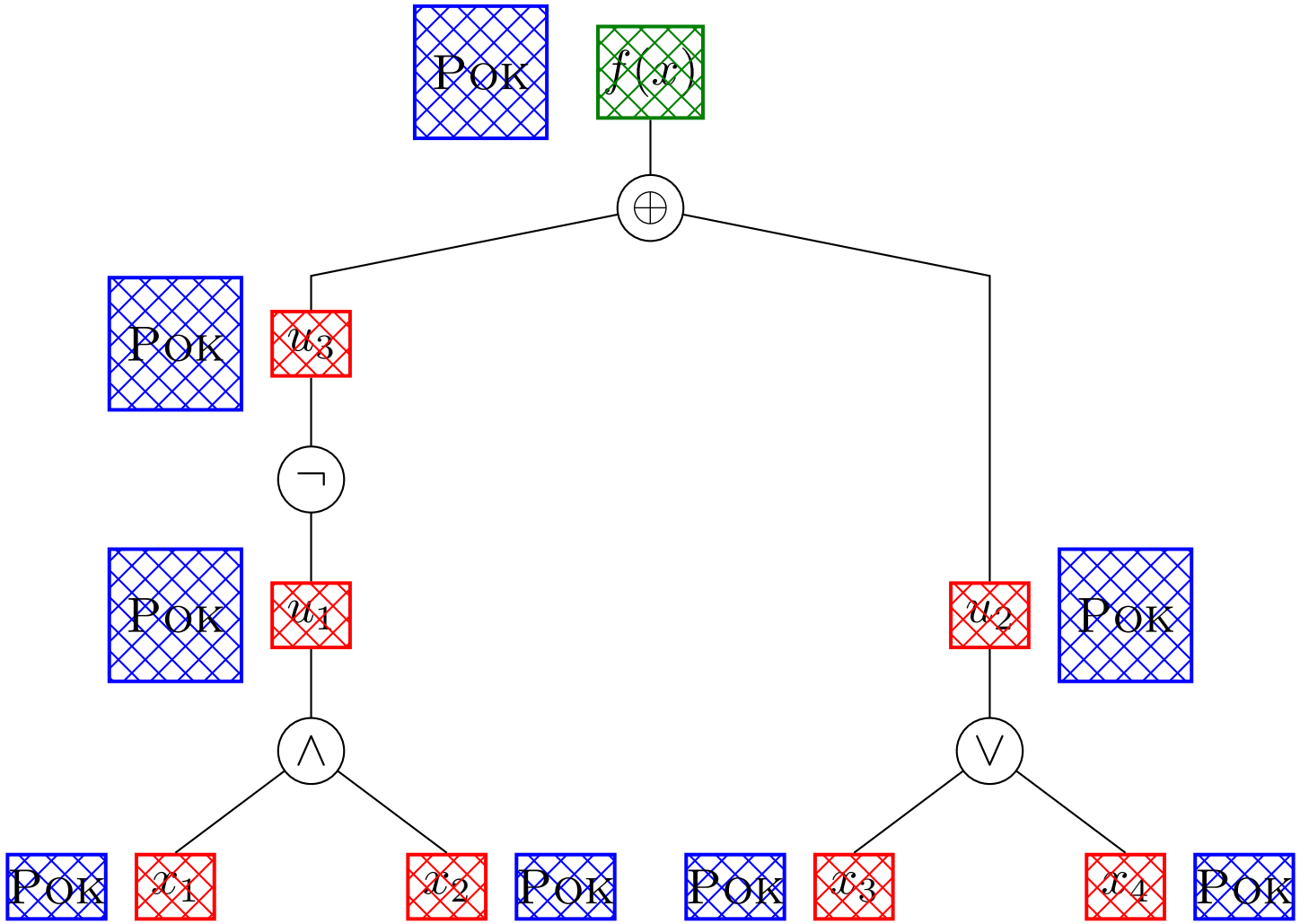
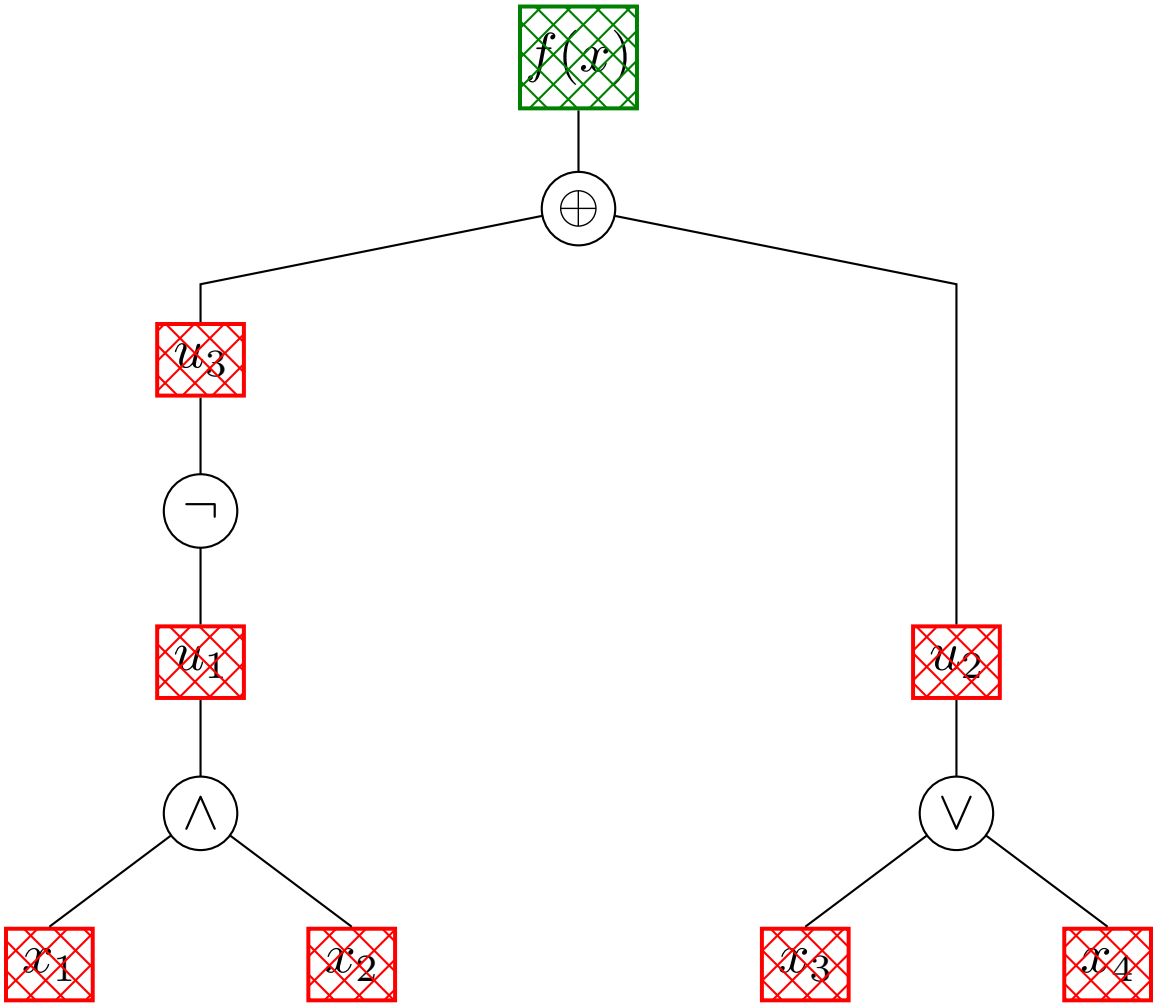
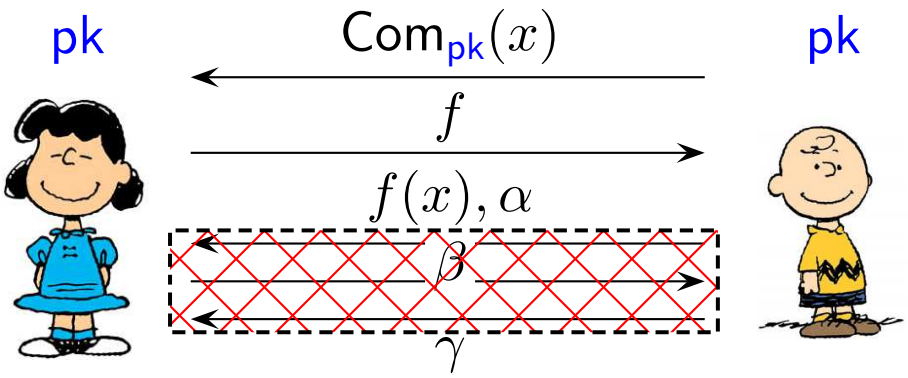
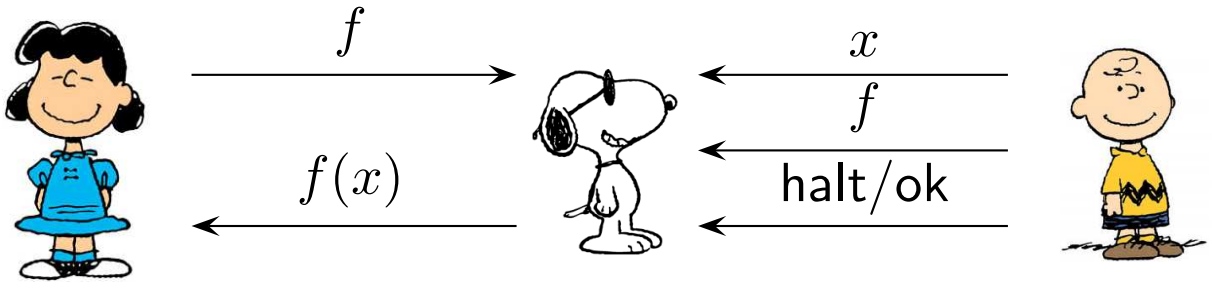

$f(x)$
$\oplus$
u_3
$\neg$
u_1
u_2
$\wedge$
$\vee$
Pok
x_1
x_2
Pok
Pok
x_3
x_4
Pok

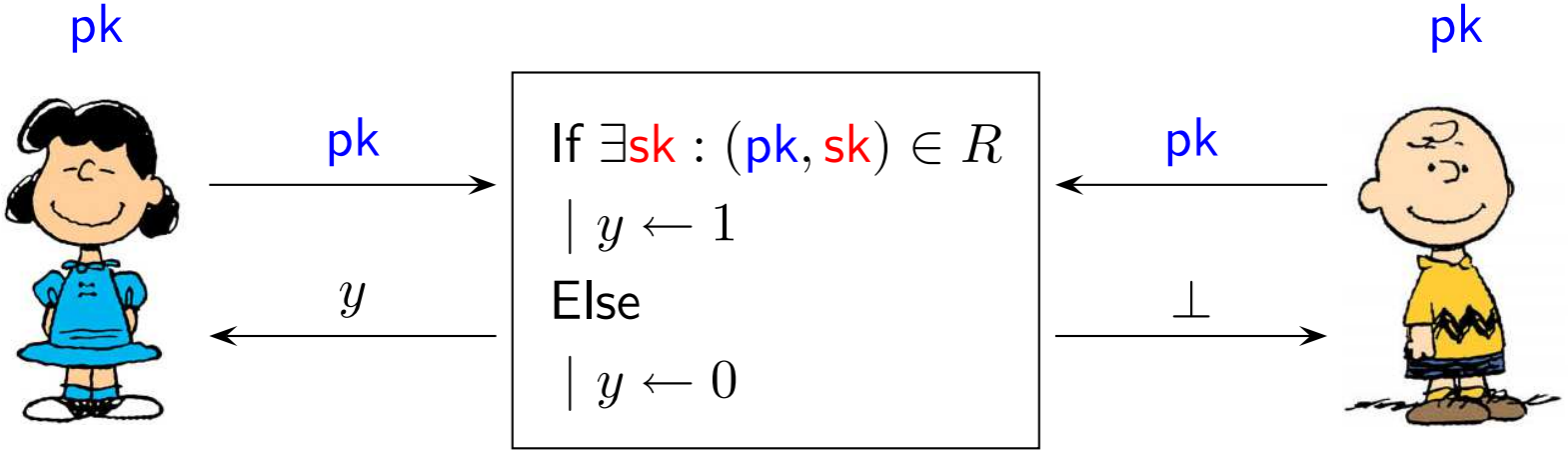

Рок
$f(x)$
$\oplus$
Рок
u_3
$\neg$
Рок
u_1
$\wedge$
Рок
x_1
x_2
Рок
u_2
$\vee$
Рок
Рок
x_3
x_4
Рок


$f(x)$
$\oplus$
w_3
$\neg$
w_1
w_2
$\wedge$
$\vee$
x_1
x_2
x_3
x_4

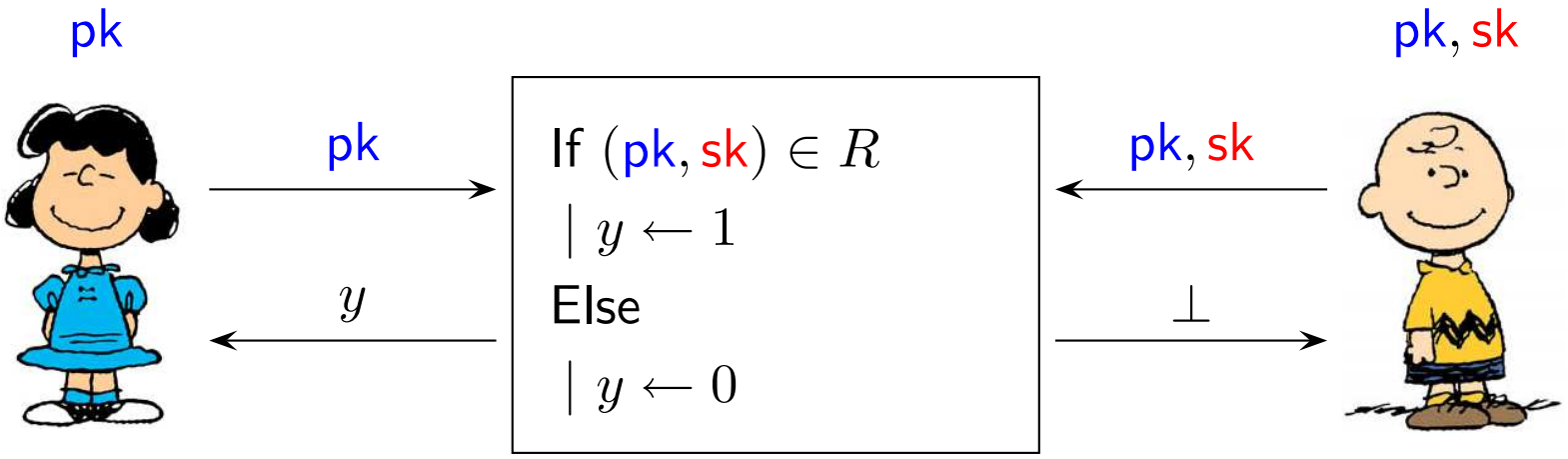

pk
$\mathsf{Com}_{\mathsf{pk}}(x)$
pk
f
$f(x), \alpha$
β
γ

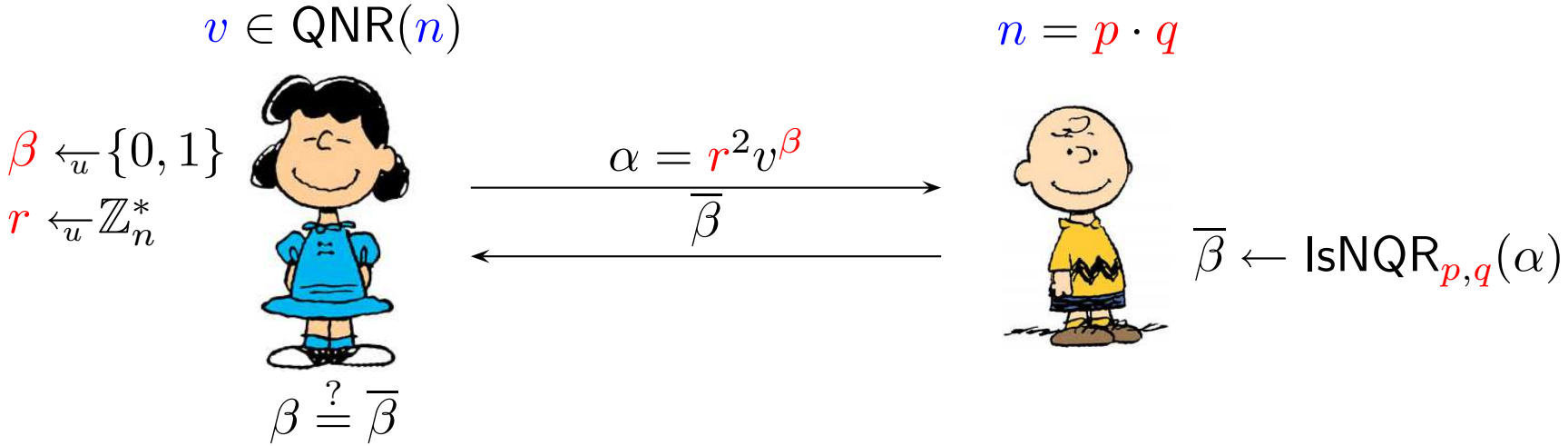

f
x
f
$f(x)$
halt/ok

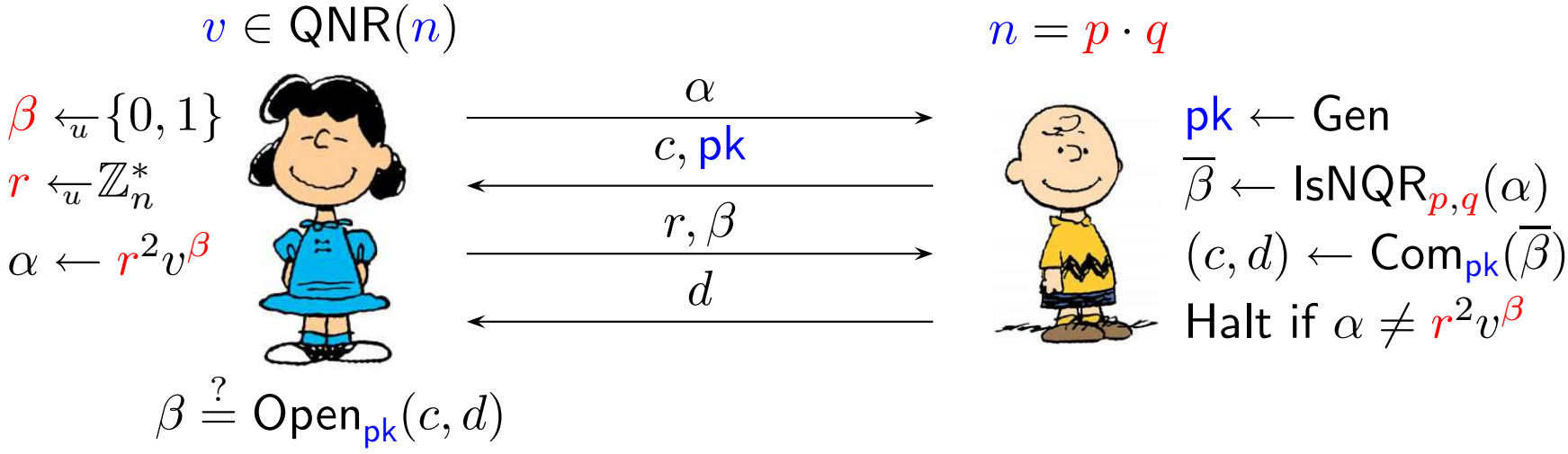
An ideal implementation of a zero-knowledge proof

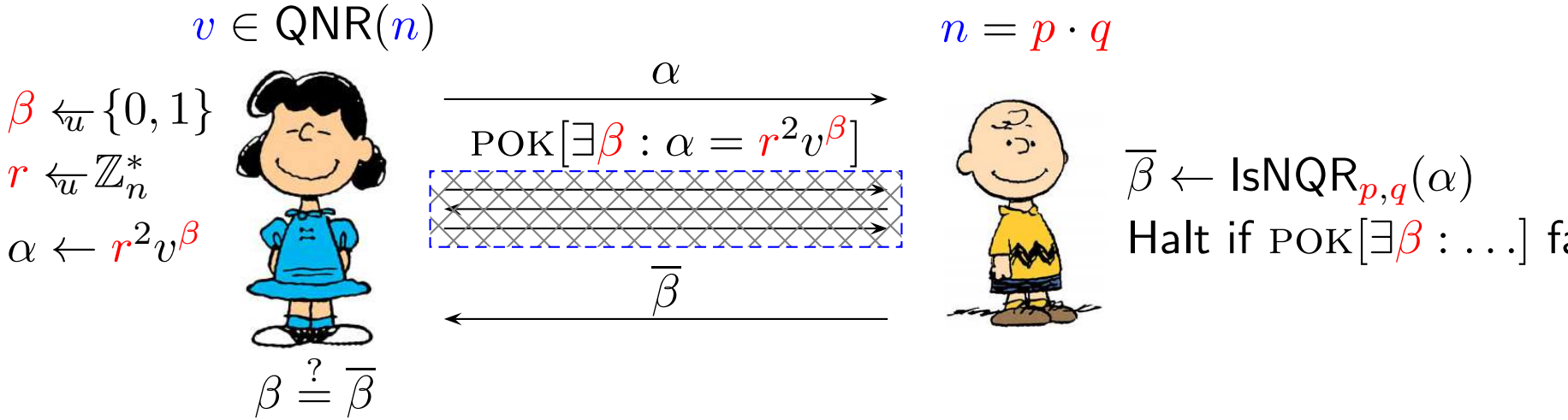


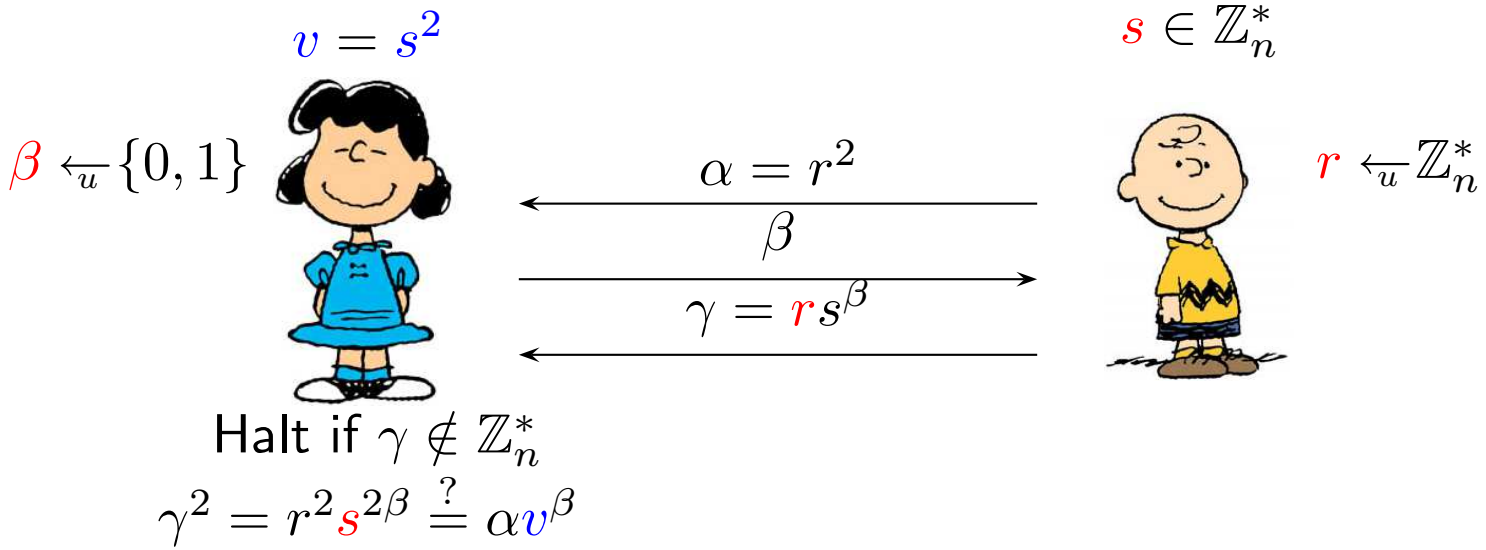
An ideal implementation of a zero-knowledge proof of knowledge

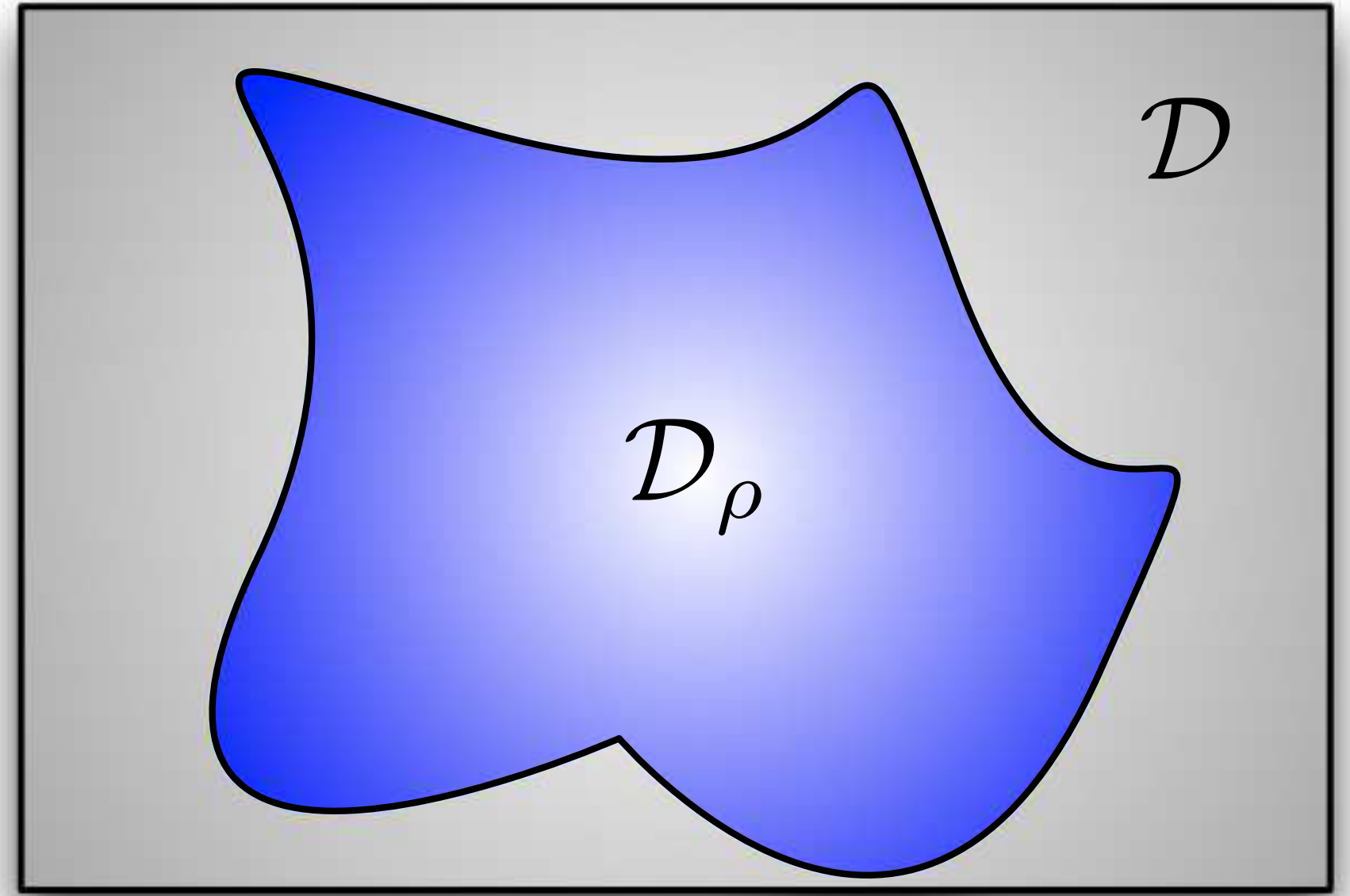


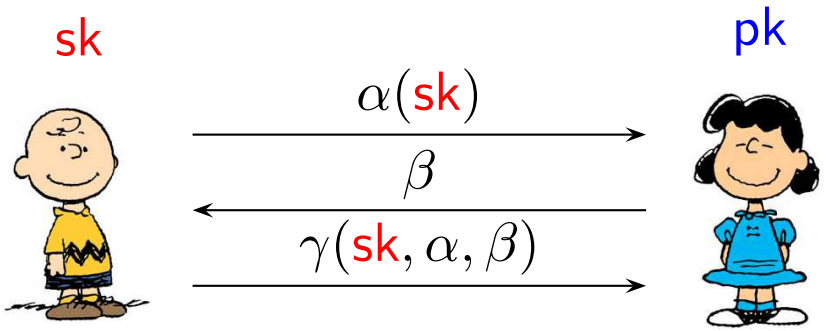

$v \in \mathsf{QNR}(n)$
$n = p \cdot q$
$\beta \xleftarrow{}_u \{0,1\}$
$r \xleftarrow{}_u \mathbb{Z}_n^*$
$\alpha = r^2 v^\beta$
$\overline{\beta}$
$\overline{\beta} \leftarrow \mathsf{IsNQR}_{p,q}(\alpha)$
$\beta \stackrel{?}{=} \overline{\beta}$


$v \in \mathsf{QNR}(n)$
$n = p \cdot q$
$\beta \leftarrow_u \{0,1\}$
$r \leftarrow_u \mathbb{Z}_n^*$
$\alpha \leftarrow r^2 v^\beta$
α
c, pk
r, β
d
$\mathsf{pk} \leftarrow \mathsf{Gen}$
$\overline{\beta} \leftarrow \mathsf{IsNQR}_{p,q}(\alpha)$
$(c, d) \leftarrow \mathsf{Com}_{\mathsf{pk}}(\overline{\beta})$
Halt if $\alpha \neq r^2 v^\beta$
$\beta \stackrel{?}{=} \mathsf{Open}_{\mathsf{pk}}(c, d)$


$v \in \mathsf{QNR}(n)$
$n = p \cdot q$
$\beta \xleftarrow{u} \{0,1\}$
$r \xleftarrow{u} \mathbb{Z}_n^*$
$\alpha \leftarrow r^2 v^\beta$
α
$\mathrm{POK}[\exists \beta : \alpha = r^2 v^\beta]$
$\overline{\beta}$
$\beta \stackrel{?}{=} \overline{\beta}$
$\overline{\beta} \leftarrow \mathsf{IsNQR}_{p,q}(\alpha)$
Halt if $\mathrm{POK}[\exists \beta : \ldots]$ fa


$v = s^2$
$s \in \mathbb{Z}_n^*$
$\beta \leftarrow_u \{0,1\}$
$\alpha = r^2$
β
$\gamma = rs^\beta$
$r \leftarrow_u \mathbb{Z}_n^*$
Halt if $\gamma \notin \mathbb{Z}_n^*$
$\gamma^2 = r^2 s^{2\beta} \stackrel{?}{=} \alpha v^\beta$


$\mathcal{D}$
$\mathcal{D}_\rho$

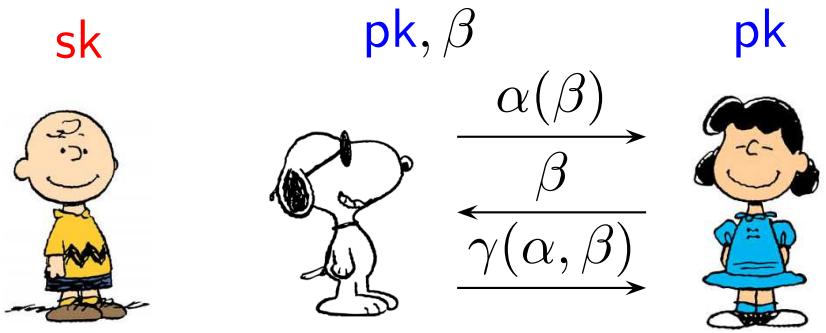


Even if Lucy is *honest*

▷ she might learn something about the secret sk.

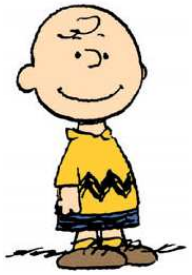
since

▷ messages α and γ depend on the secret sk.



As Lucy is *malicious* the value of β is not known by her before the protocol and Snoopy must guess β to simulate the other messages.

$$\boxed{\mathrm{ZK}_x[(x,w) \in R]}$$



x $\qquad$ x, w

$\beta \leftarrow_u \mathcal{B}$

$(c,d) \leftarrow \mathsf{Com}_{\mathsf{pk}}(\beta)$

pk

c

α

d

γ

$\mathsf{pk} \leftarrow \mathsf{Gen}$

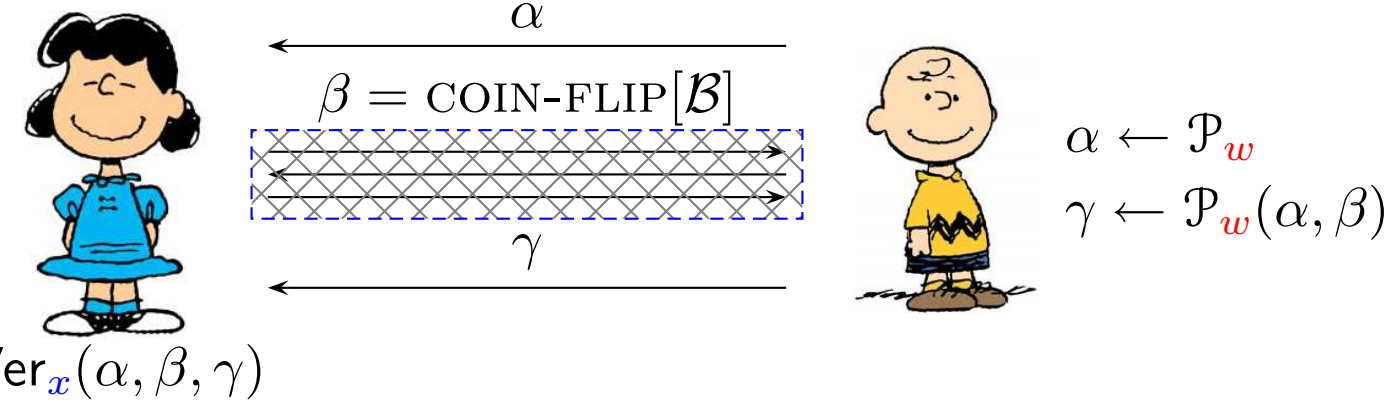
$\alpha \leftarrow \mathcal{P}_w$

$\beta \leftarrow \mathsf{Open}_{\mathsf{pk}}(c,d)$

$\gamma \leftarrow \mathcal{P}_w(\alpha,\beta)$

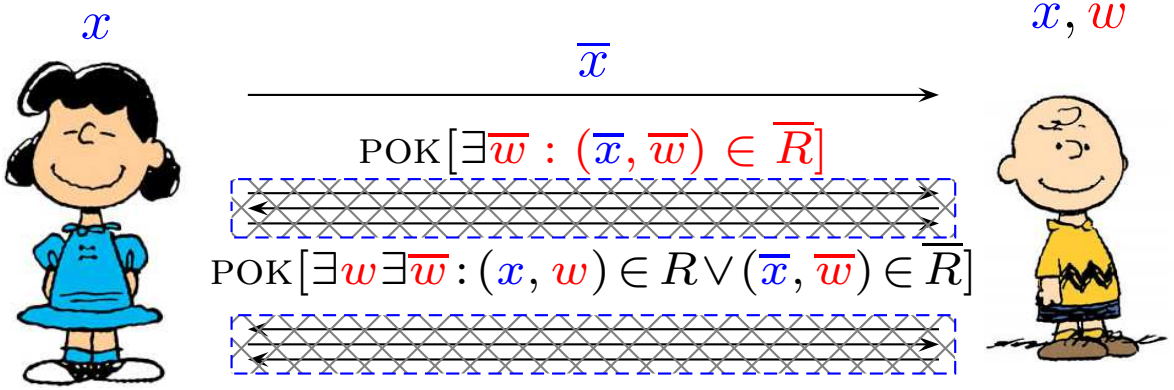
$\mathsf{Ver}_x(\alpha,\beta,\gamma)$

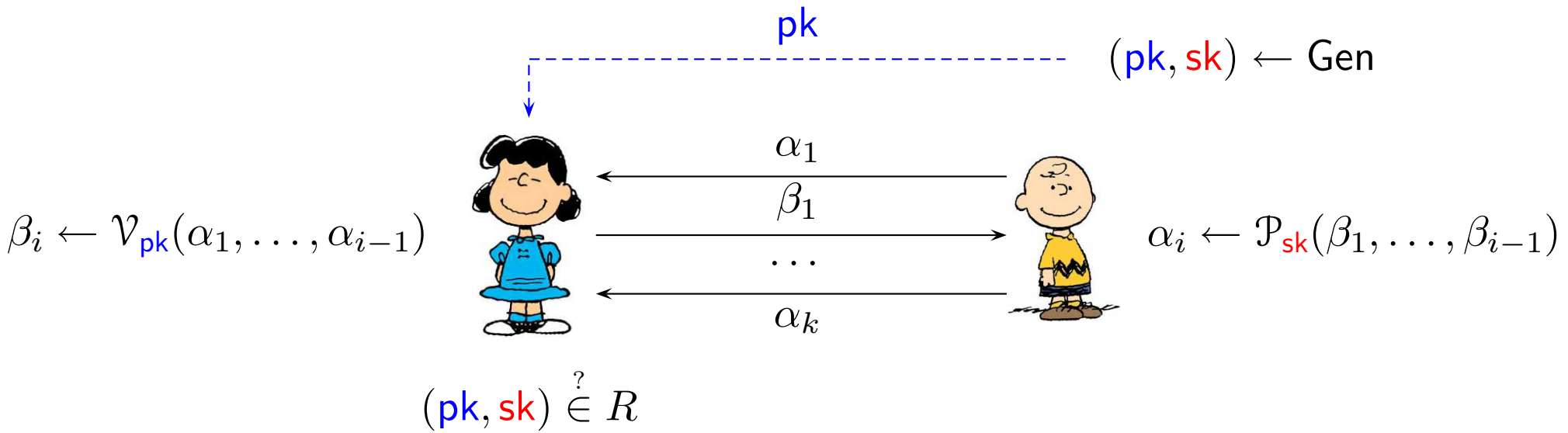
$$\boxed{\text{ZK-POK}_x[(x, w) \in R]}$$



$$\boxed{\text{ZKA-POK}_{x}[(x,w)\in R]}$$

$(\overline{x},\overline{w}) \leftarrow \mathsf{Gen}_{\overline{R}}$




pk
(pk, sk) ← Gen
α_1
β_1
$\ldots$
α_k
$\beta_i \leftarrow \mathcal{V}_{\mathsf{pk}}(\alpha_1, \ldots, \alpha_{i-1})$
$\alpha_i \leftarrow \mathcal{P}_{\mathsf{sk}}(\beta_1, \ldots, \beta_{i-1})$
$(\mathsf{pk}, \mathsf{sk}) \stackrel{?}{\in} R$