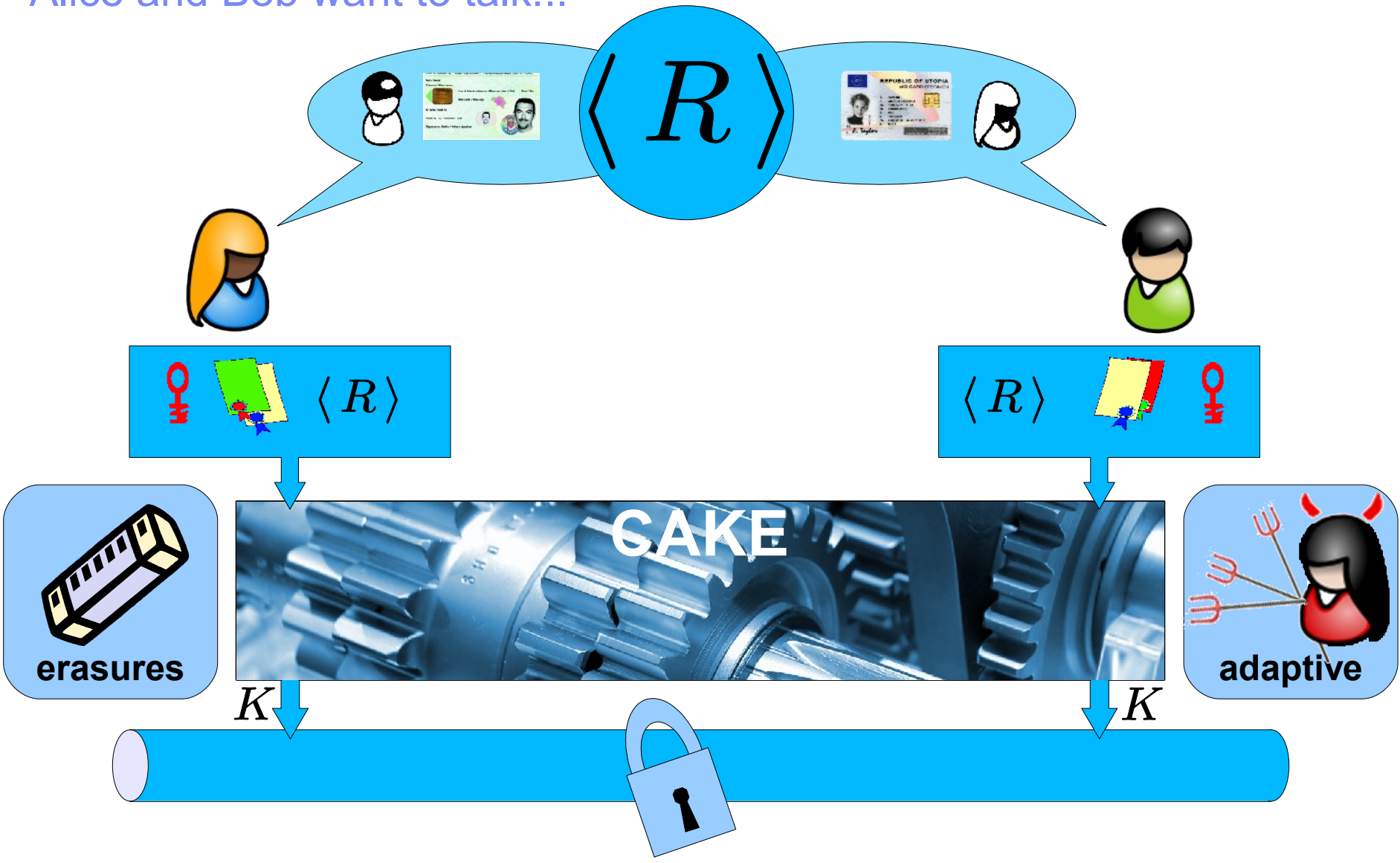


Credential-Authenticated Identification and Key Exchange

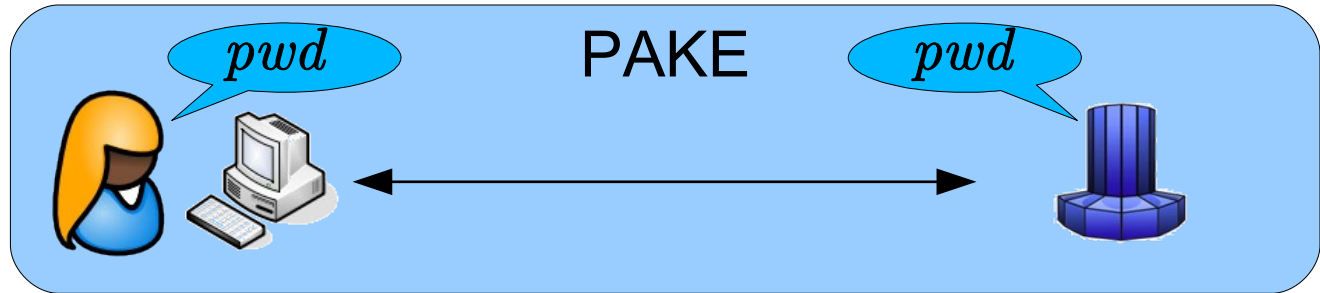


Alice and Bob want to talk...



What to do with a CAKE?

$$s = t$$



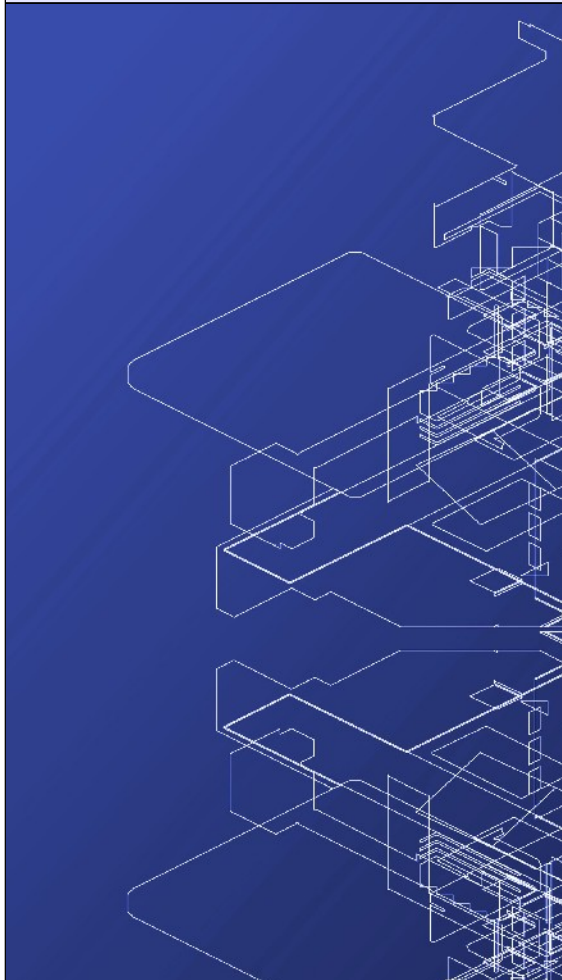
$$g^s = t$$



$$(x, s) \in E \wedge (y, t) \in F$$



Problem



Tools



Solution



Problem

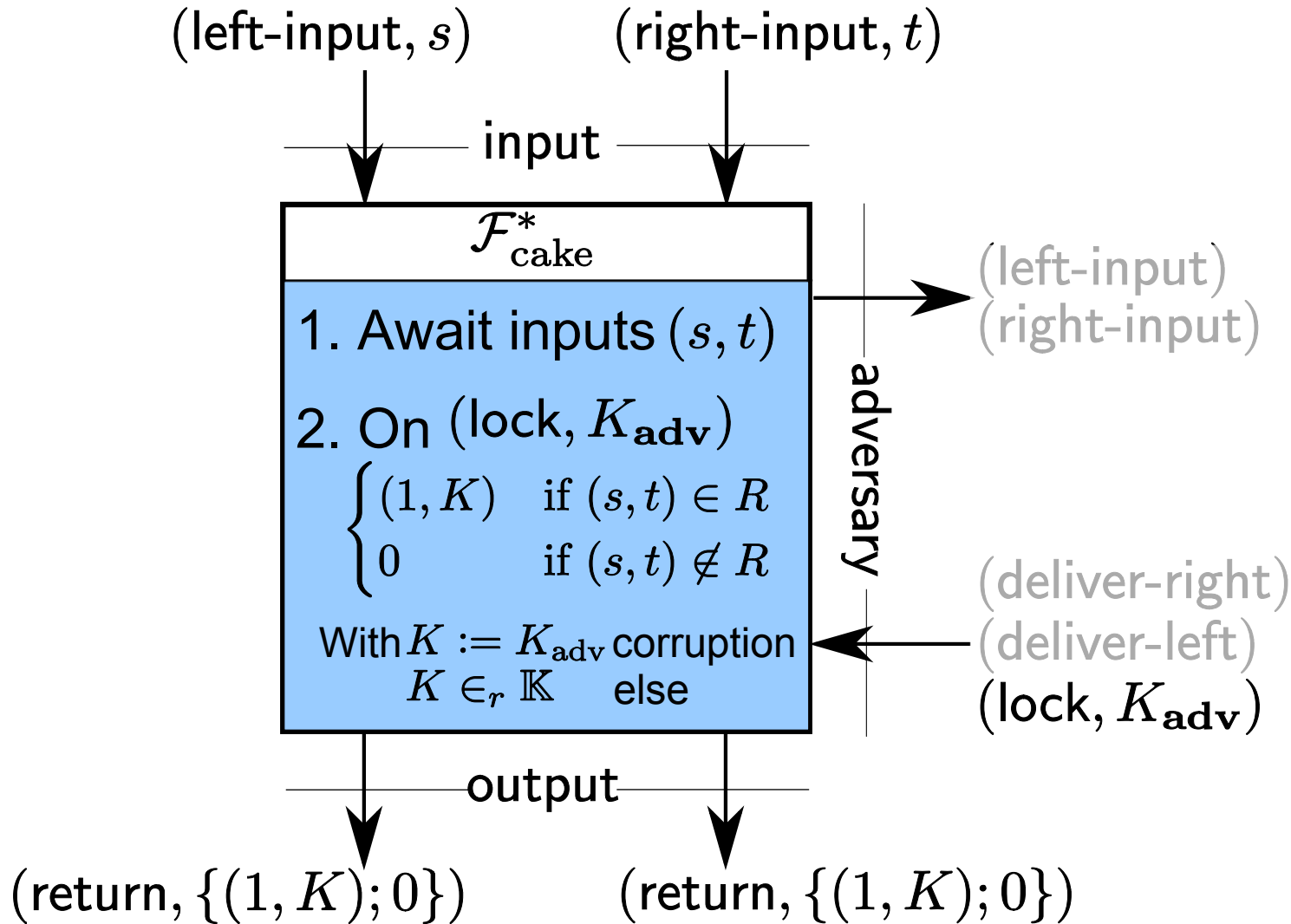
What's the CAKE ideal functionality?

What's key ideal world building block?

What challenges to solve for CAKE?

What's the Strong CAKE ideal functionality?

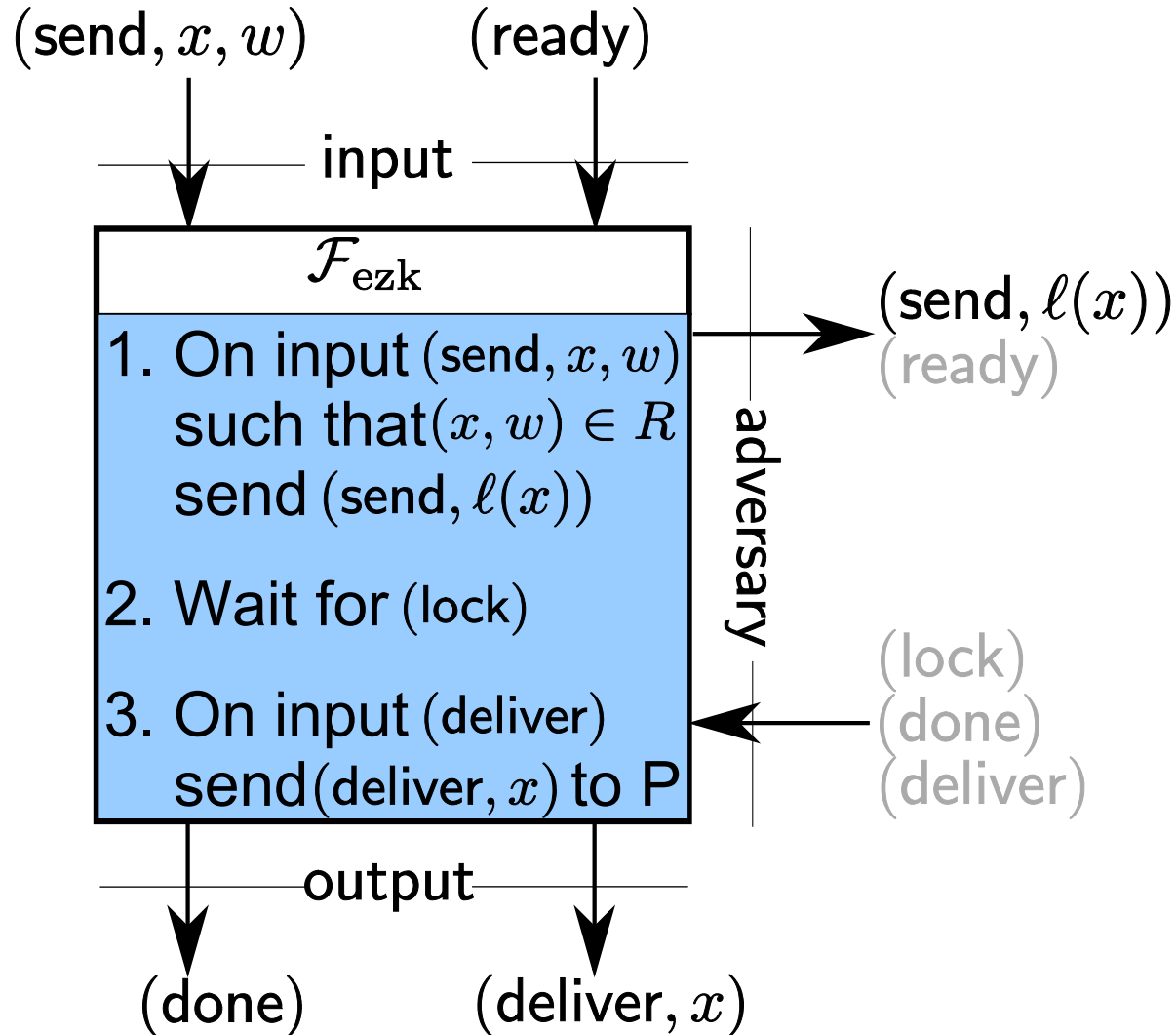
$sid := parent/ ext : P_{pid} : Q_{pid} : \langle R \rangle$



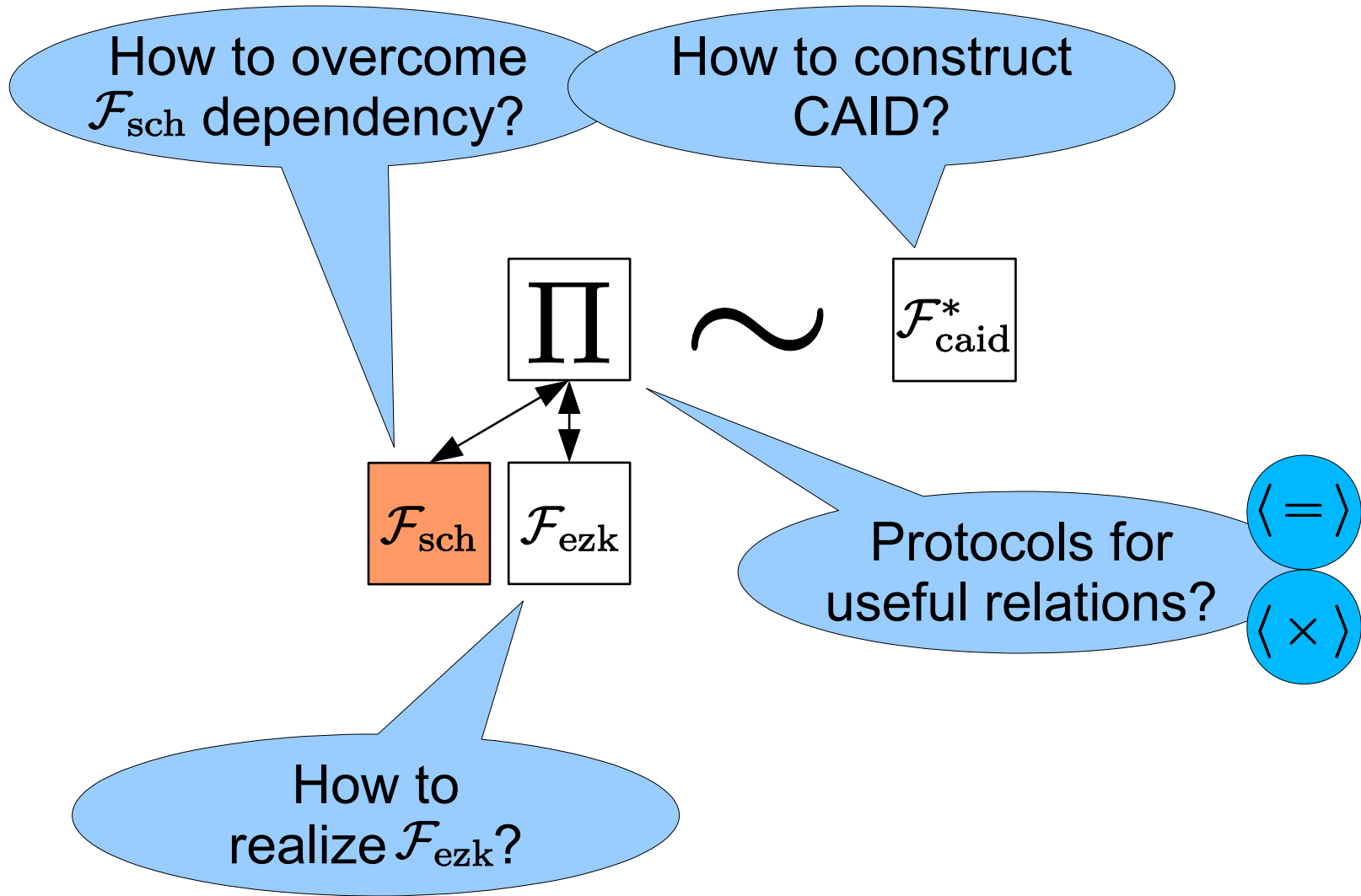
What is the enhanced zero knowledge ideal functionality?

[Can2005]

$sid := parent/ ext : P_{pid} : Q_{pid} :$



How to realize CAID protocols?



Tools

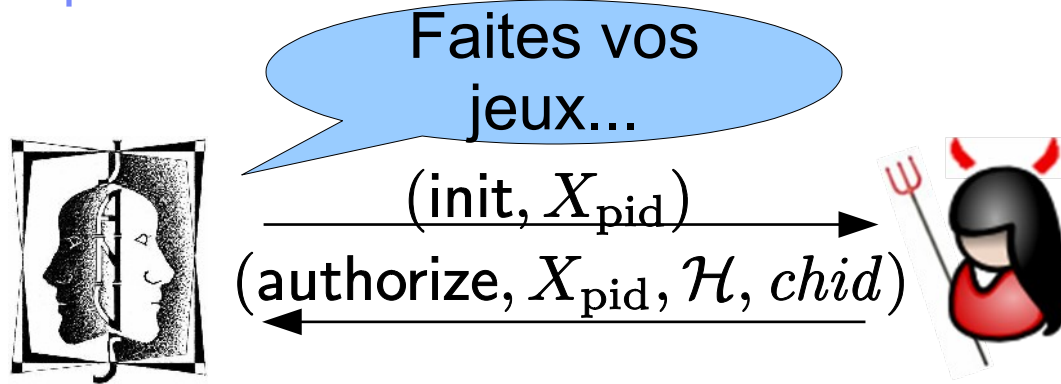
How to bootstrap an authenticated channel?

How to realize UC EZK?

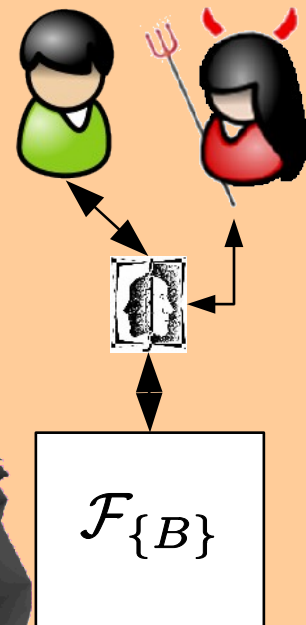
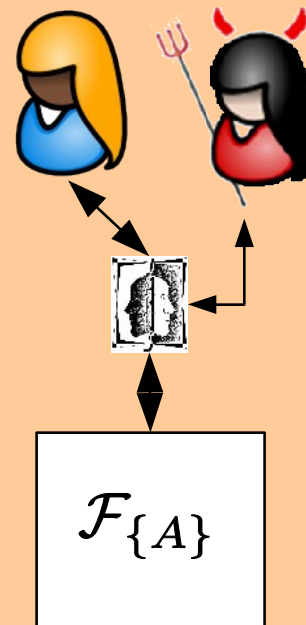
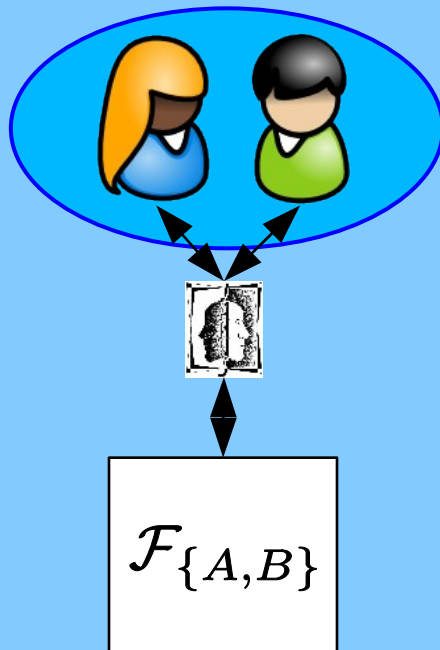
How to prove equality?

How to bootstrap an authenticated channel?

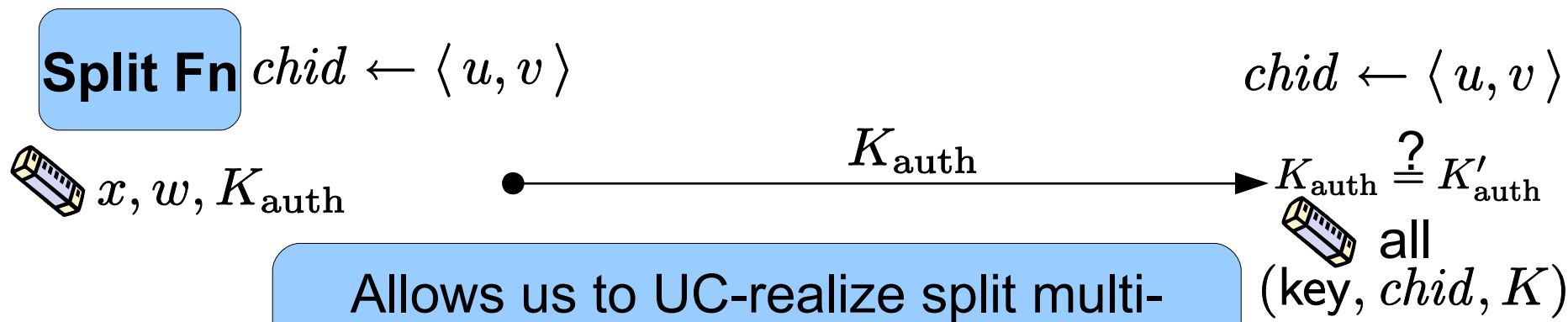
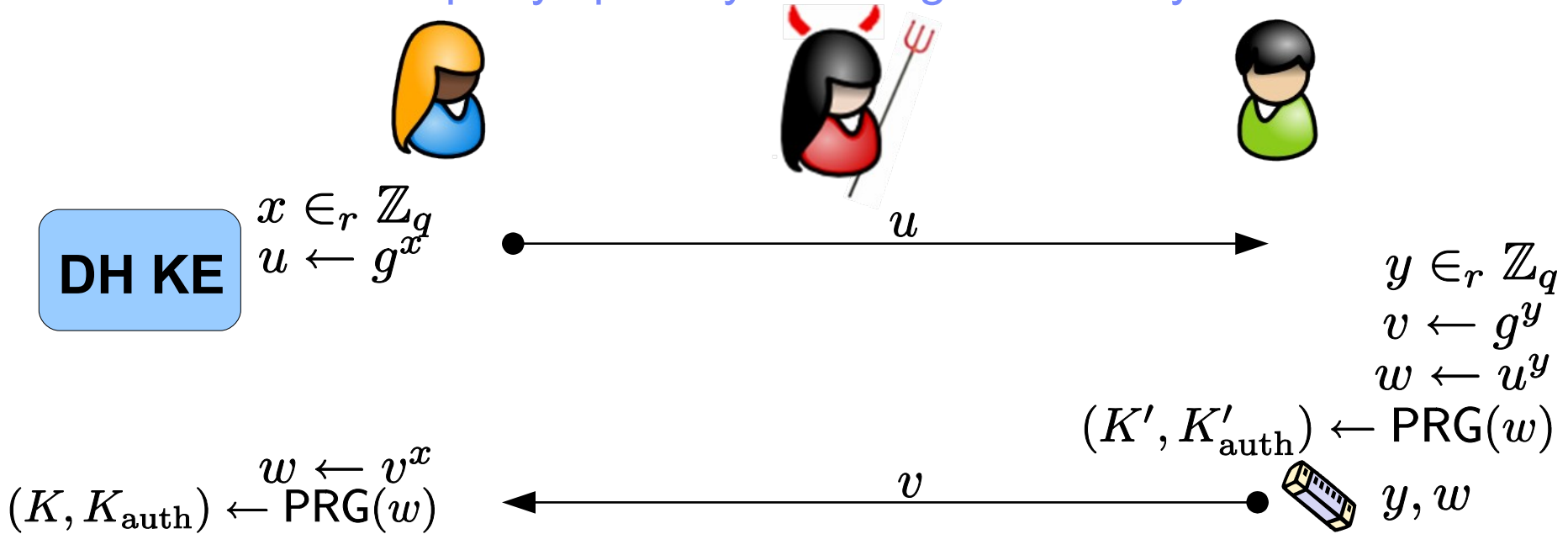
[BCLPR2005]



EITHER: $\mathcal{H}' = \mathcal{H} \wedge chid' = chid$ **OR:** $\mathcal{H}' \cap \mathcal{H} = \emptyset \wedge chid' \neq chid$



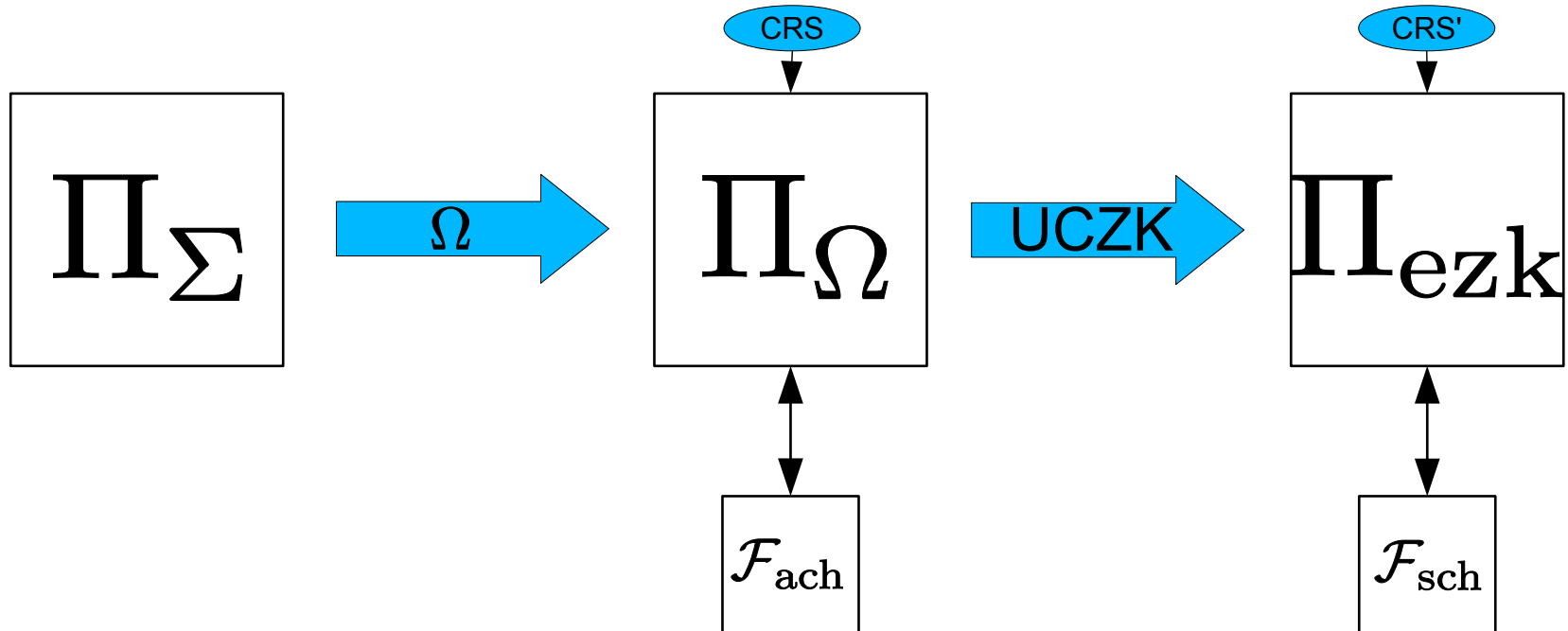
How to realize two-party split key exchange efficiently?



Allows us to UC-realize split multi-session secure channels under DDH.

How to realize enhanced zero-knowledge?

[GaMaYa2003, JarLys2000]



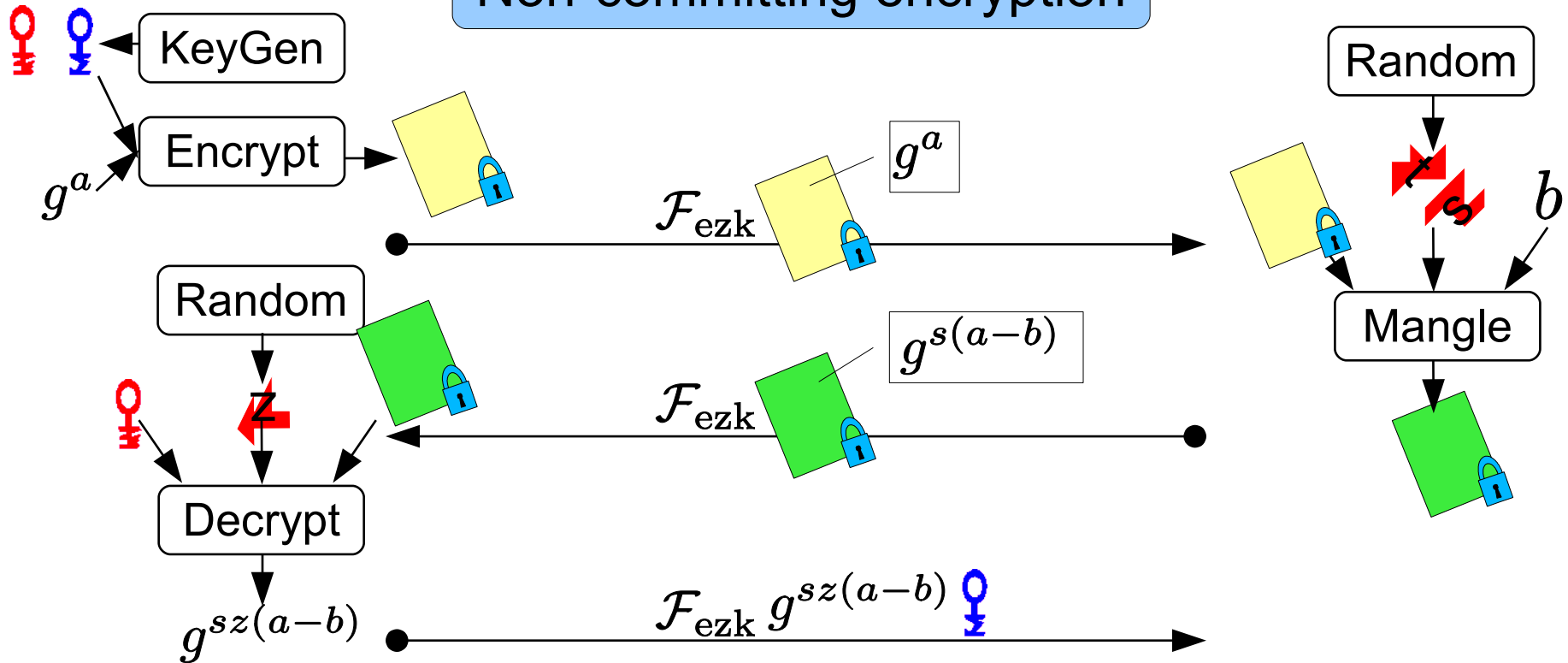
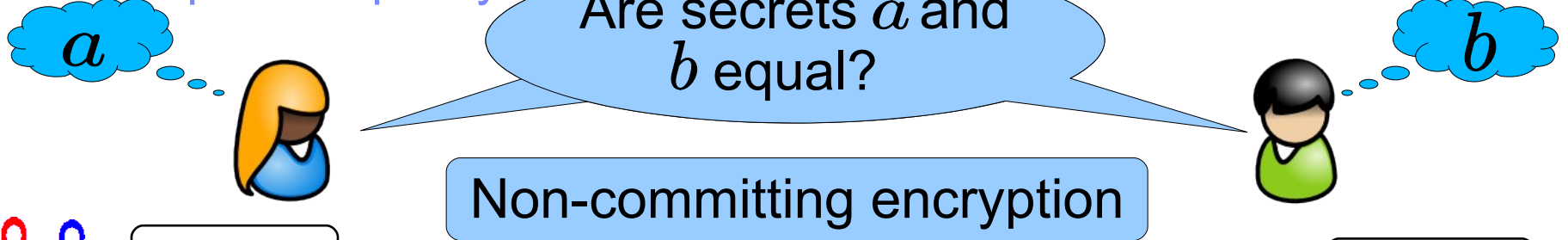
Strong
RSA

[GaMaYa2003]
Paillier encrypt
and commit (w, r)
Proof of
representation

[JarLys2000]
Committed proof
[MacYan2003]
SSTC trapdoor
commitment

How to prove equality?

[CraSho1998, JarLys2000]



UC-realize \mathcal{F}_{caid}^* for $\langle = \rangle$ under DDH assumption in the $(\mathcal{F}_{ezk}, \mathcal{F}_{sch})$ hybrid model.

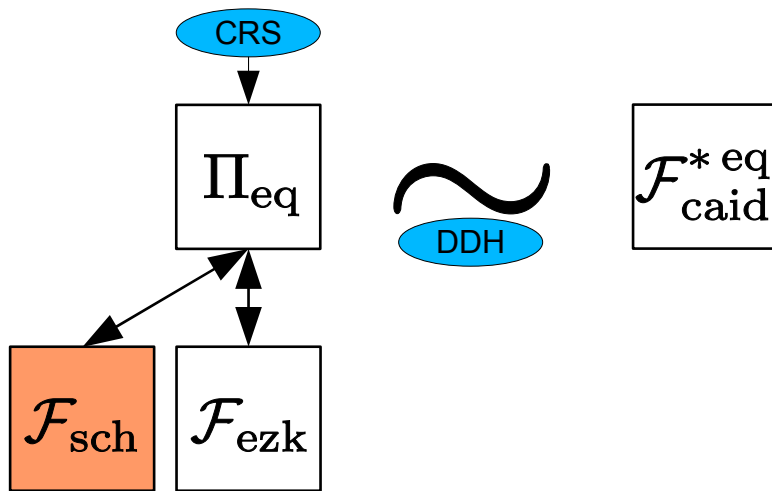
Solution

How to put it all together?

How to prove the protocols UC secure?

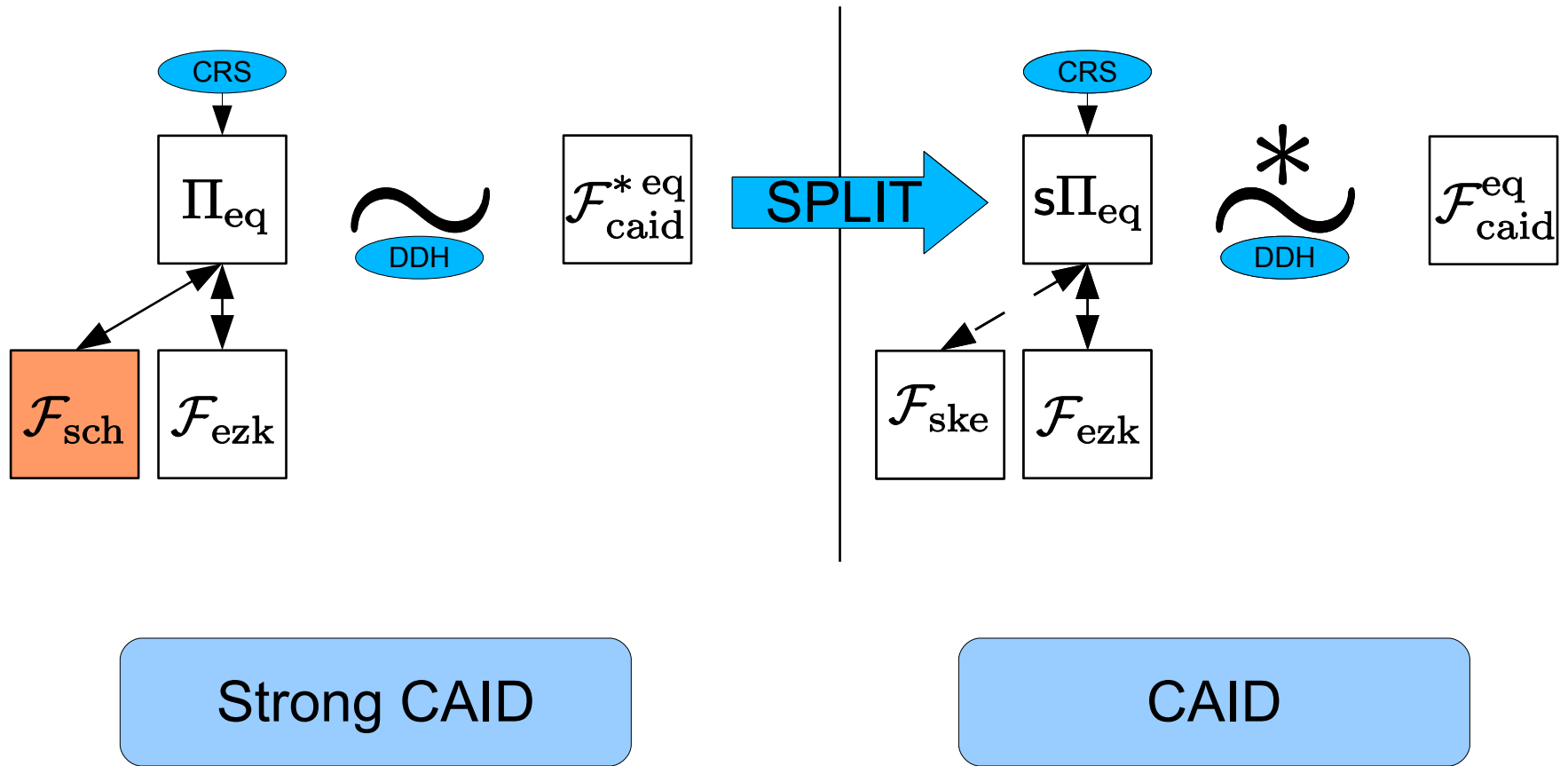


How to put it together and prove it UC secure?



Strong CAID

How to put it together and prove it UC secure?



Summary

[\[http://eprint.iacr.org/2010/055\]](http://eprint.iacr.org/2010/055)**Corruption Model**

Adaptive corruptions with erasures

System Parameters \mathbb{G} of prime order q , generator g .
Joint access to CRS (for Ω & UCZK realization)**General Protocols****CAID*** for $\langle \times \rangle$: UC-secure under CDH.
CAID* for $\langle = \rangle$: UC-secure under DDH.
Split transformation to CAID.
Split multi-session KE: UC-secure under DDH**Derived Protocols****PAKE** secure against adaptive corruptions, UC-secure under DDH, w/o ROM.
PAKE* secure against adaptive corruptions and server compromise, UC-secure under DDH.

Credential-Authenticated Identification and Key Exchange

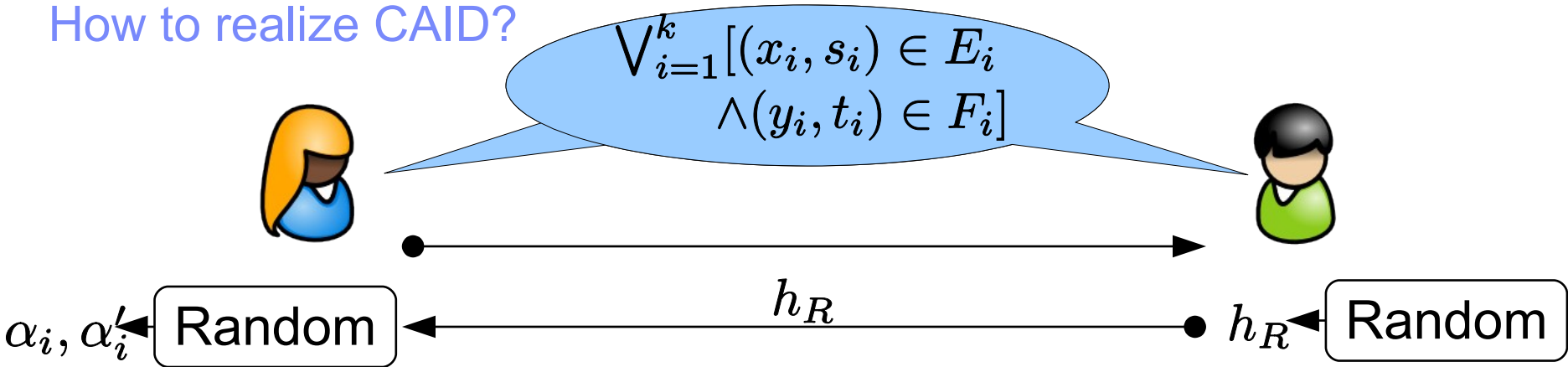
Speaker: Thomas Gross (thomasgross@acm.org, thomasgross.net)

Extended Version on IACR ePrint: <http://eprint.iacr.org/2010/055>



BACKUP

How to realize CAID?



If $(x_i, s_i) \in E_i$
 then $e_i \leftarrow g^{\alpha_i}$
 else $e_i \leftarrow h_R / g^{\alpha'_i}$

$\alpha'_i \mathcal{F}_{\text{ezk}}\{s_i \in S_i^*, \alpha'_i \in \mathbb{Z}_q\} :$
(e_i)

$$[(x_i, s_i) \in E_i \vee g^{\alpha'_i} = h_R / e_i]$$

$(f_i) \leftarrow \mathcal{F}_{\text{ezk}}(f_i)$
(v_i)

If $(x_i, s_i) \in E_i$
 then $u_i \leftarrow f_i^{\alpha_i}$
 else $u_i \leftarrow_{\mathbb{R}} \mathbb{G}$

CAID:
$$\bigvee_{i=1}^k (u_i = v_i)$$

local data

How to prove the protocols UC secure?

