Part I
Bellare-Rogaway Model
(Passive Adversaries)

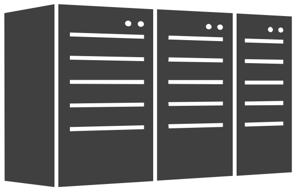
8th BIU Winter School on Key Exchange, 2018

Marc Fischlin

Diffie-Hellman Key Exchange (1976)

pick x

g^x →



pick y

← g^y

$g^{xy} = (g^y)^x$
$K = \mathrm{KDF}(g^{xy})$

$g^{xy} = (g^x)^y$
$K = \mathrm{KDF}(g^{xy})$

passive adversary,
only observing

KDF=Key Derivation Function

Security Models

Game-based	Simulation-based
Bellare-Rogaway `93, `95	Bellare-Canetti-Krawczyk`98
…	Shoup `99
	Canetti-Krawczyk `02
	…
Bellare-Pointcheval-Rogaway `00	Boyko-MacKenzie-Patel `00

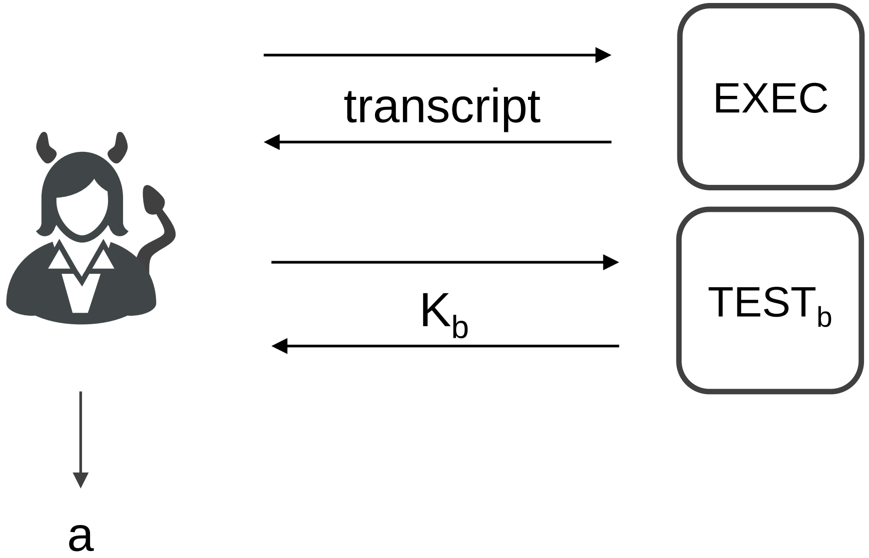
password-based

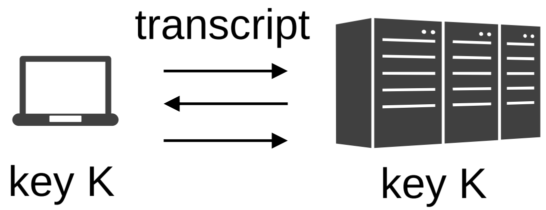
„The“ Bellare-Rogaway (BR) Model

Bellare-Rogaway (BR93)	Two-party scenario	Crypto `93
Bellare-Rogaway (BR95)	Three-party scenario	STOC `95
Bellare-Pointcheval-Rogaway (BPR00)	Password-based scenario	Eurocrypt 2000

+many derivates

Key Indistinguishability / Secrecy (I)





secret random bit b:
return K_0=K (if b=0) or K_1=$ (if b=1)

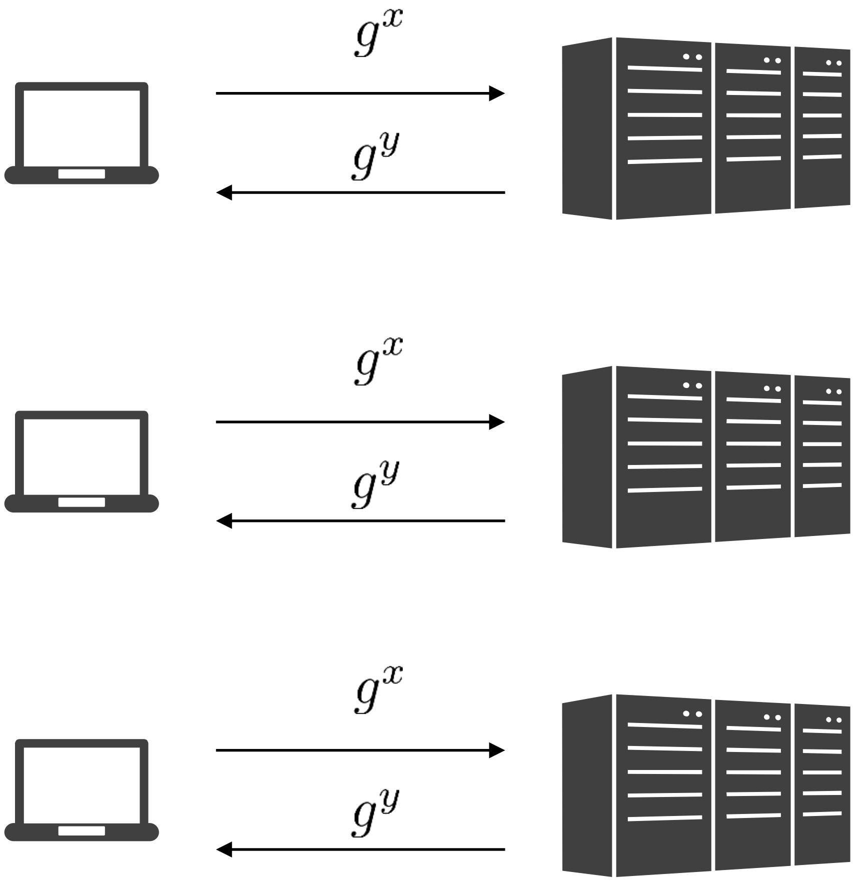
$=independent random key

Adversary wins if
a=b

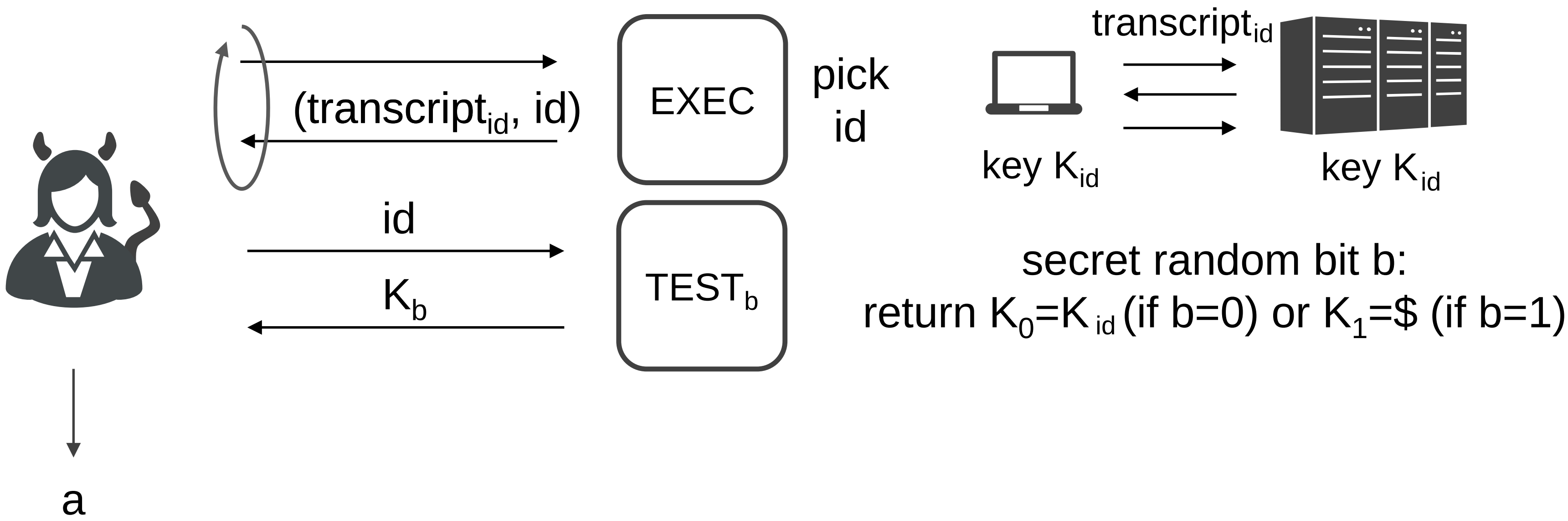
KE is secure against passive adversaries if
for any efficient adversary: Pr[A wins] ≤ ½ +neg

Problem: No Dependencies in Model

assume parties always use the same secrets



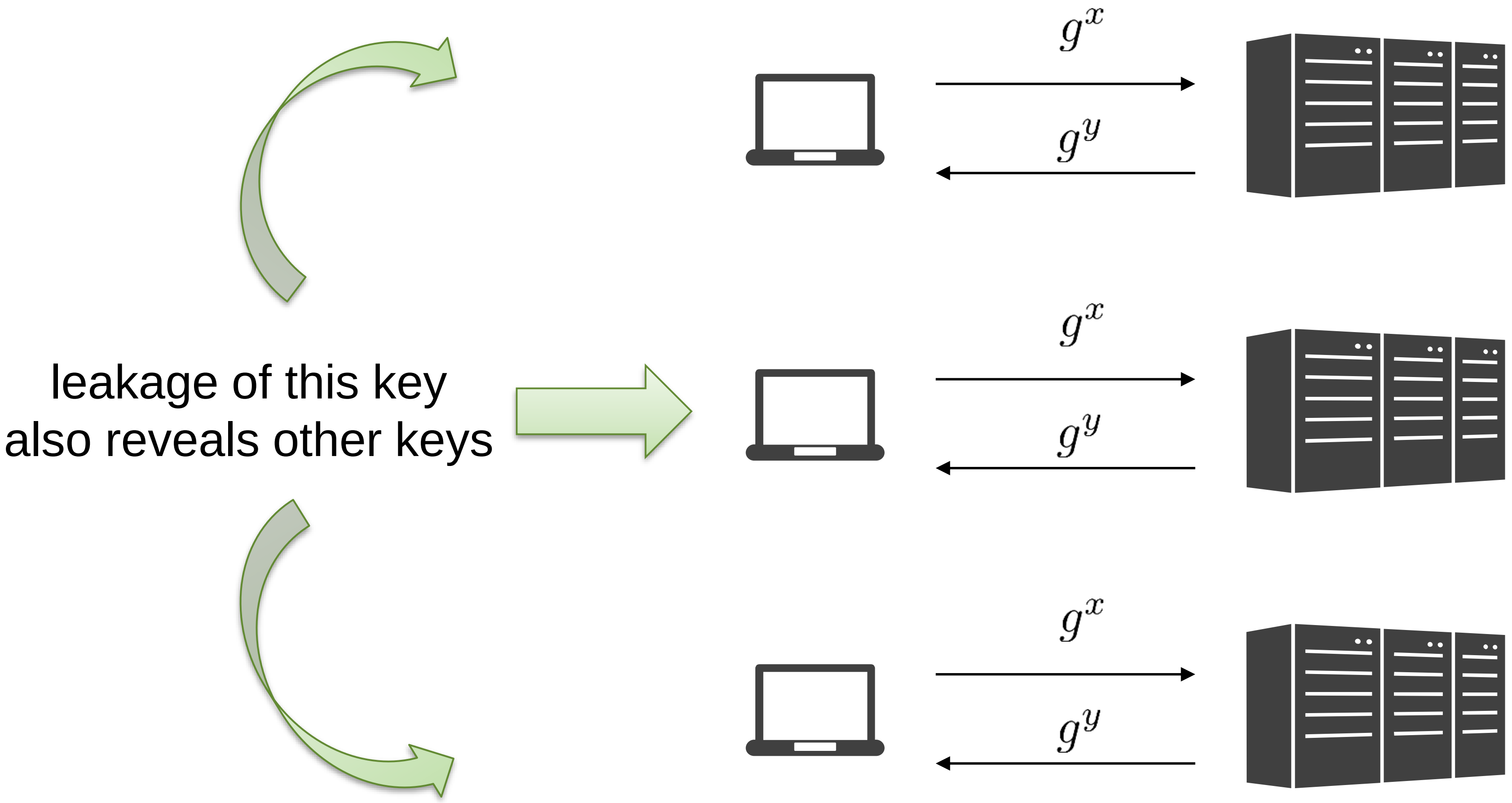
Key Indistinguishability / Key Secrecy



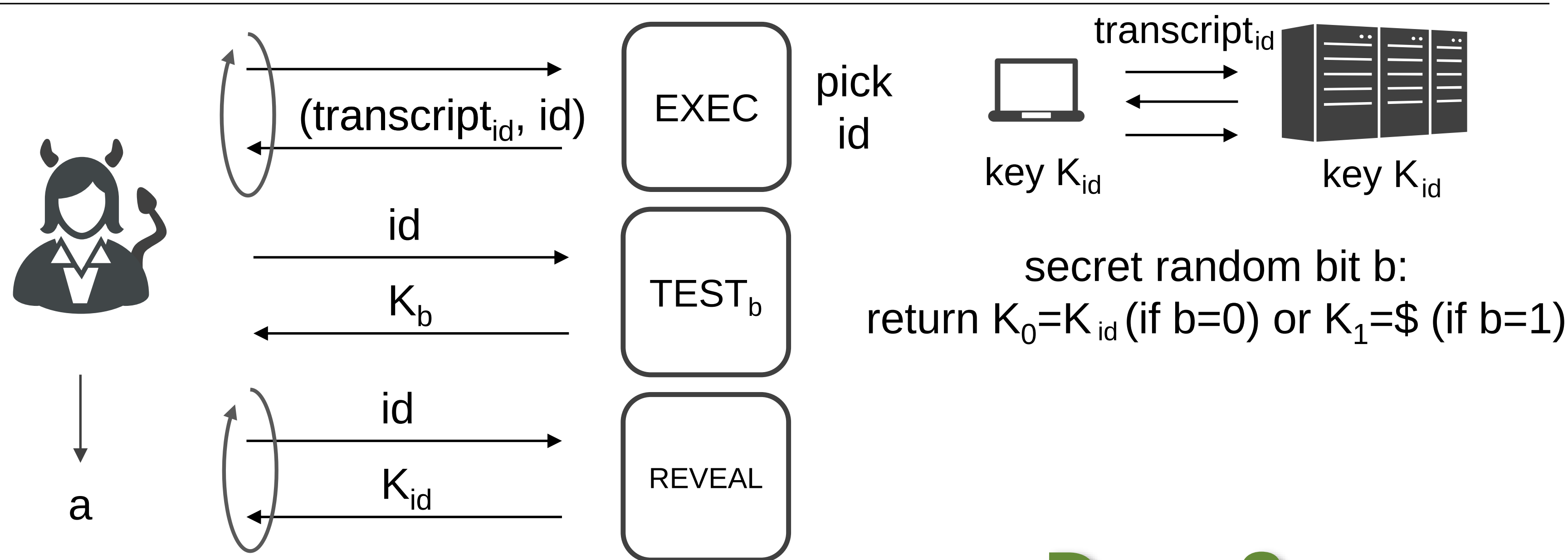
Adversary wins if
a=b

KE is secure against passive adversaries if
for any efficient adversary: Pr[A wins] $\leq$ ½ +neg

The Problem, revisited



Adding Reveals

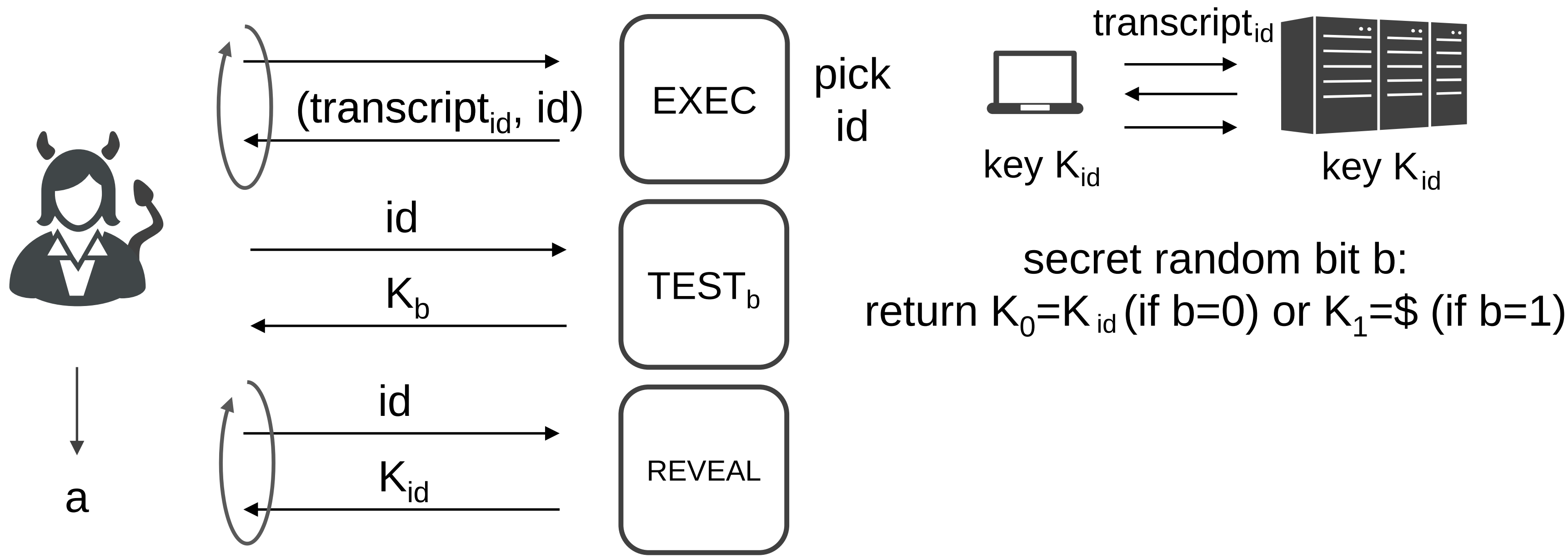


Done?

Adversary wins if a=b

KE is secure against passive adversaries if for any efficient adversary: $\Pr[A \text{ wins}] \leq ½ + neg$

BR-Security (passive adversaries)



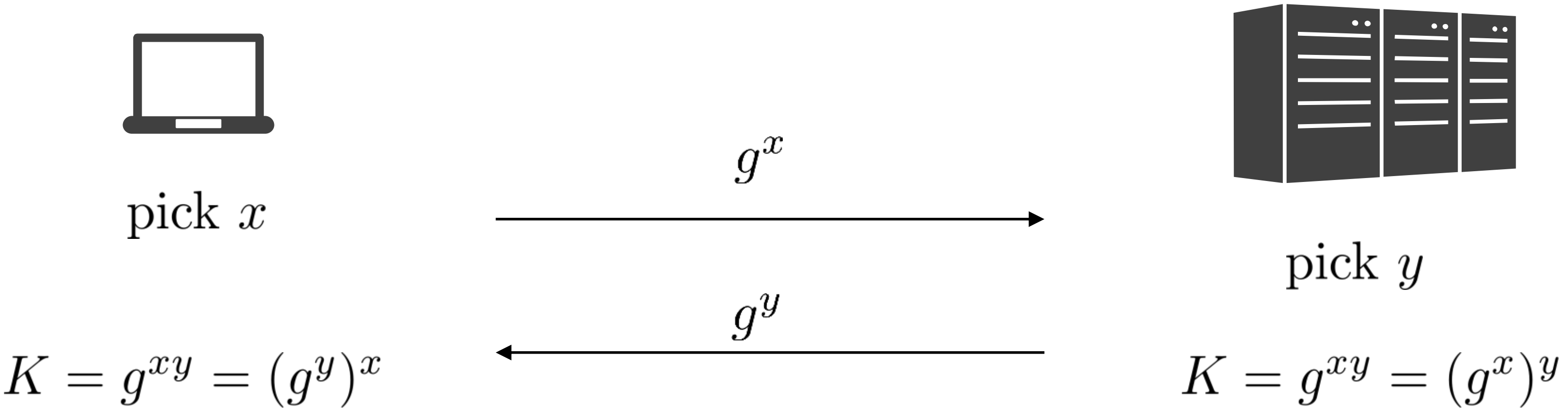
„Freshness“ condition

Adversary wins if

a=b **and has not asked TEST and REVEAL about same id**

KE is BR-secure against passive adversaries if for any efficient adversary: Pr[A wins] ≤ ½ +neg

Example: Plain DH is passively BR-secure



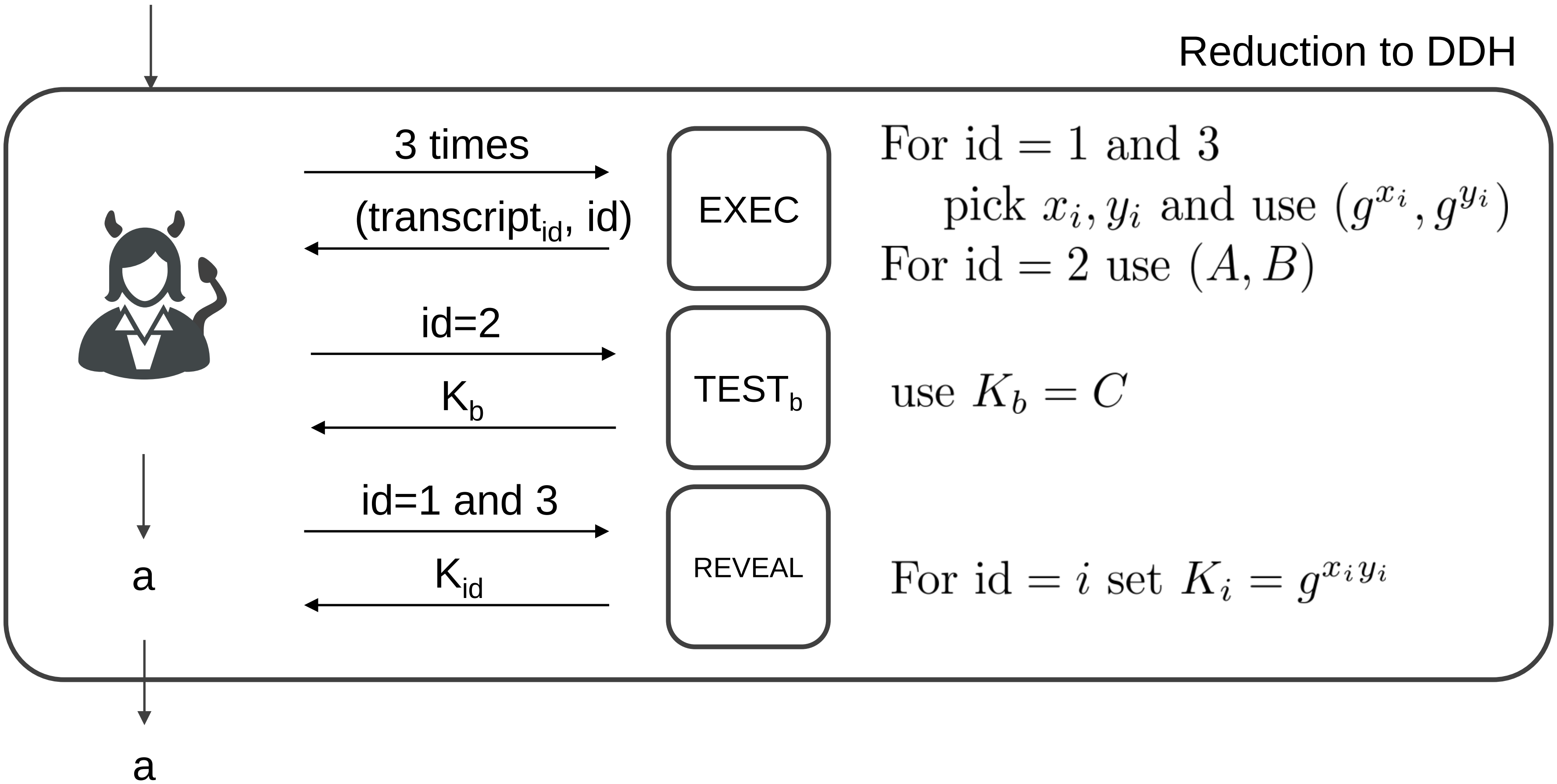
…under the Decisonal Diffie-Hellman (DDH) assumption:

$$(g^a, g^b, g^{ab}) \approx (g^a, g^b, g^c)$$

Reduction (Idea)

suppose we know that A picks id=2 to TEST

$$(A, B, C) = (g^a, g^b, g^{ab}) \text{ or } (g^a, g^b, g^c)$$



Teaser for the Break

We have defined:

KE is BR-secure against passive adversaries if for any efficient adversary: $\Pr[A \text{ wins}] \leq ½ + neg$

Could we also define this equivalently as:

KE is BR-secure against passive adversaries if for any efficient adversary: $\mathbf{| \Pr[A \text{ wins}] - ½ | \leq neg}$

?