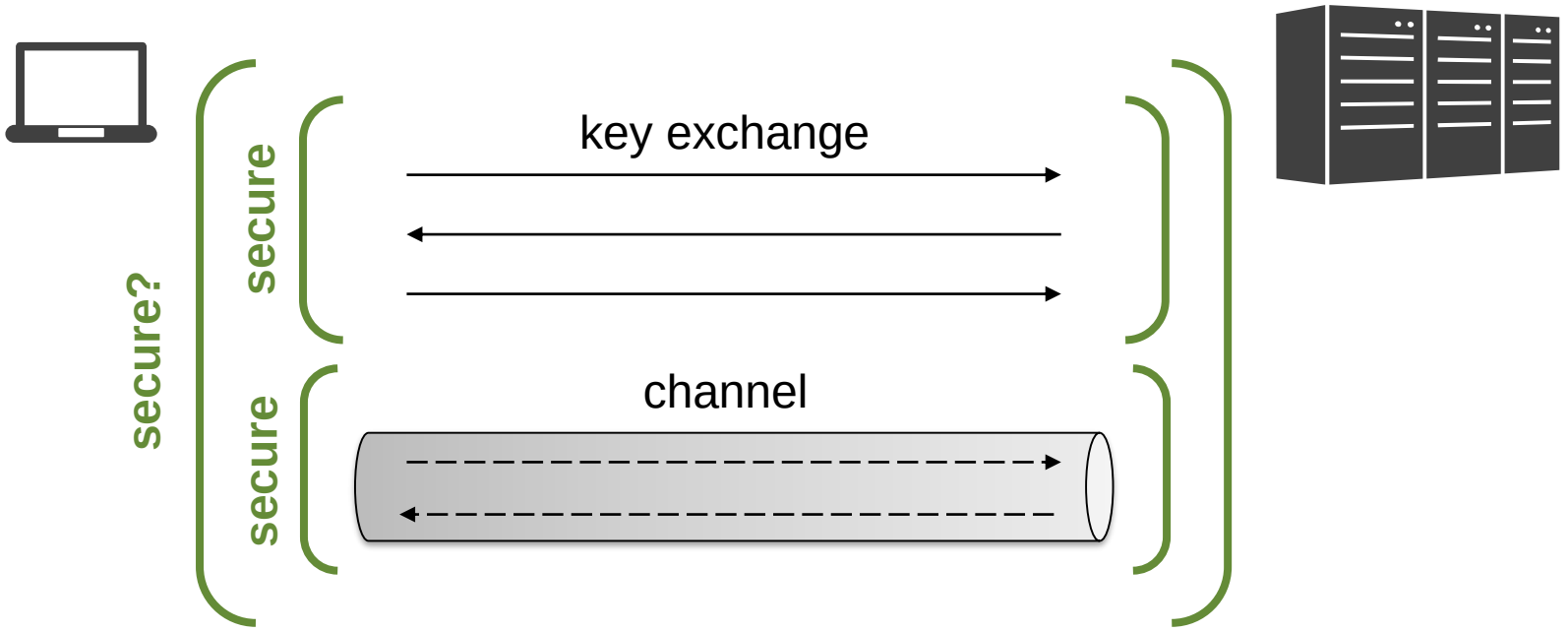
Part VI
Composition

8th BIU Winter School on Key Exchange, 2018

Marc Fischlin

Secure Composition



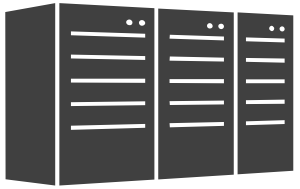
Note: We want provable security of composition!

Compositional Security of Bellare-Rogaway Key Exchange

Canetti, Krawczyk: Analysis of Key-Exchange Protocols and Their Use for Building Secure Channels, Eurocrypt 2001

Composition with *any* SymKey-Protocol

Brzuska, Fischlin, Warinschi, Williams: Composability of Bellare-Rogaway key exchange protocols, CCS 2011



key exchange

key K

Enc(K,m)

Enc(K,m‘)

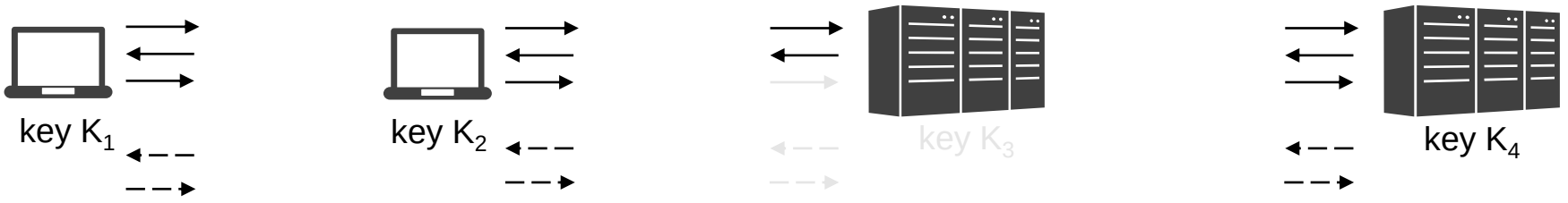
key K

Attack on composed protocol:
adversary tries to find out m and/or m‘

no REVEAL queries on composed protocol

but multiple instances

Prerequisites for Composition Result (I)

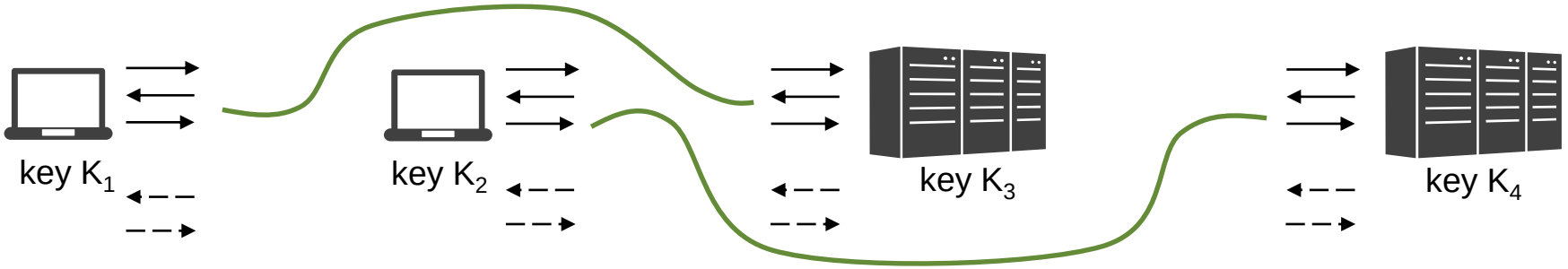


This channel session may have already started…

…when corrupt on this party comes

1. Key-exchange protocol needs to be forward secret

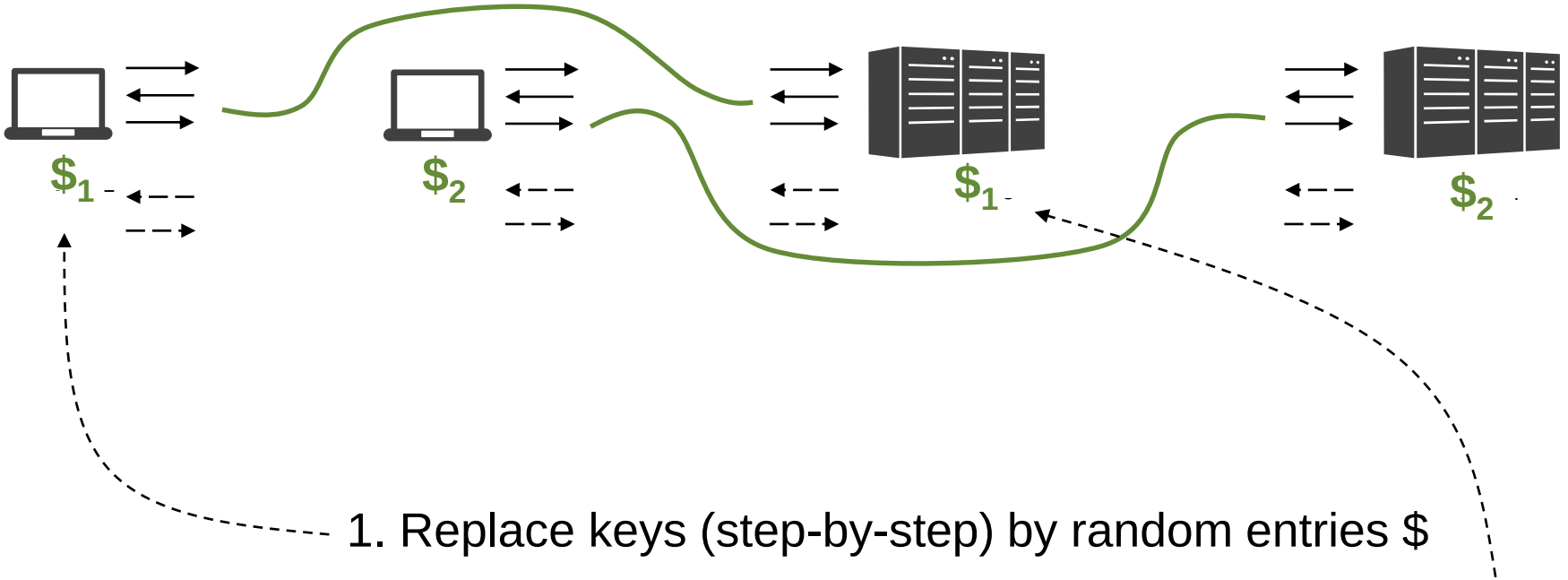
Prerequisites for Composition Result (II)



1. Key-Exchange-Protocol needs to be forward secret

2. We need to know session partners via transcripts (public session matching)

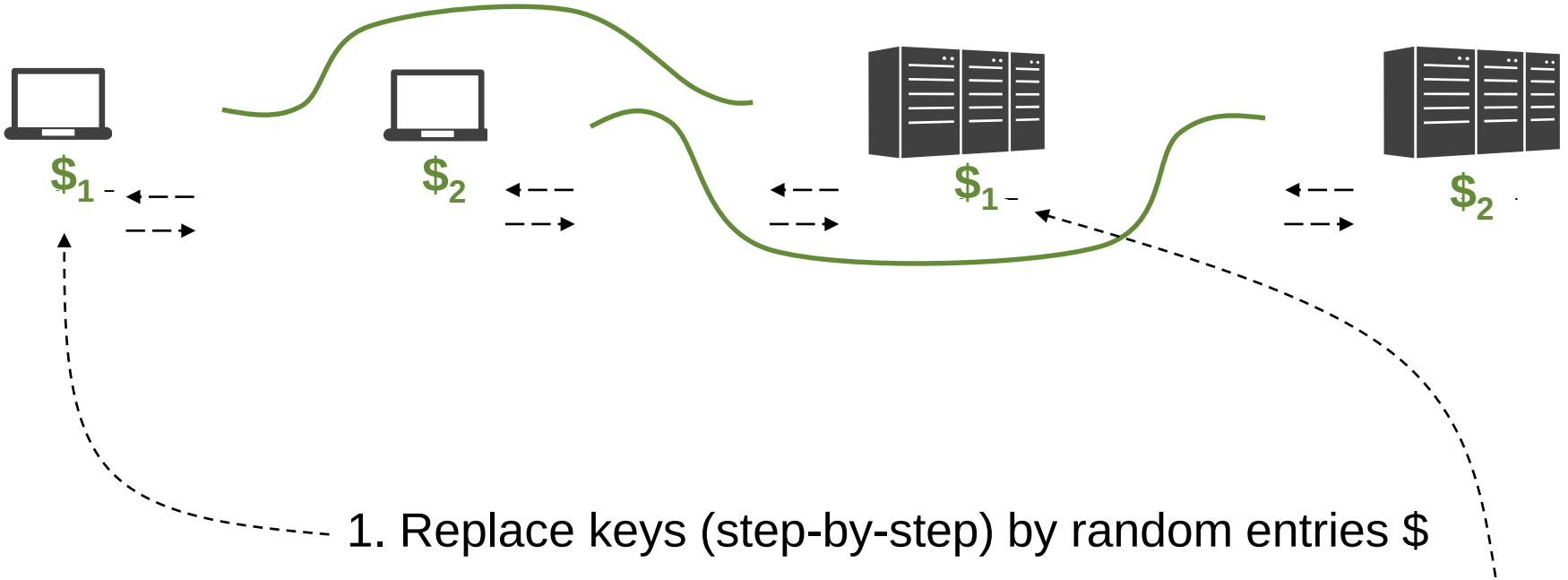
Proof Idea (I)



1. Replace keys (step-by-step) by random entries $

2. Each time replace partner key by same random string $

Proof Idea (II)



1. Replace keys (step-by-step) by random entries $

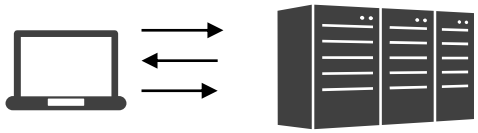
2. Each time replace partner key by same random string $

3. Key exchange protocol has become irrelevant

4. Adversary attacks (multi-instances of) symmetric protocol

Simulation-based Security

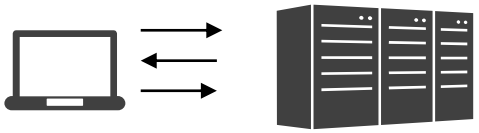
So far: Game-based Security



real key in TEST session ≈ random key in TEST session

Simulation-based Security

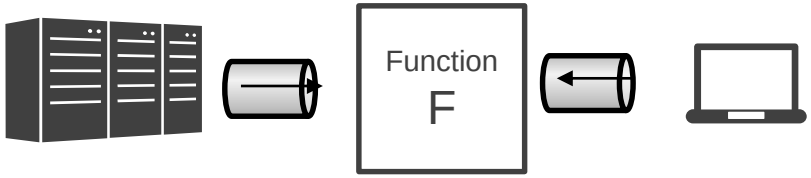
„Real World“

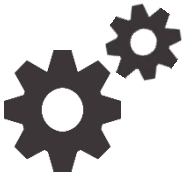


real-world adversary

Whatever an adversary can learn when attacking real protocol,

„Ideal World“



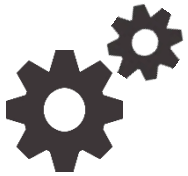


ideal-world adversary

can be learned by a simulator in ideal world where F performs task securely.

$\forall$ Adversary A : $\exists$ Simulator S: REAL $\approx$ IDEAL

Rule of Thumb

Protocol complexity() ≥ Protocol complexity()

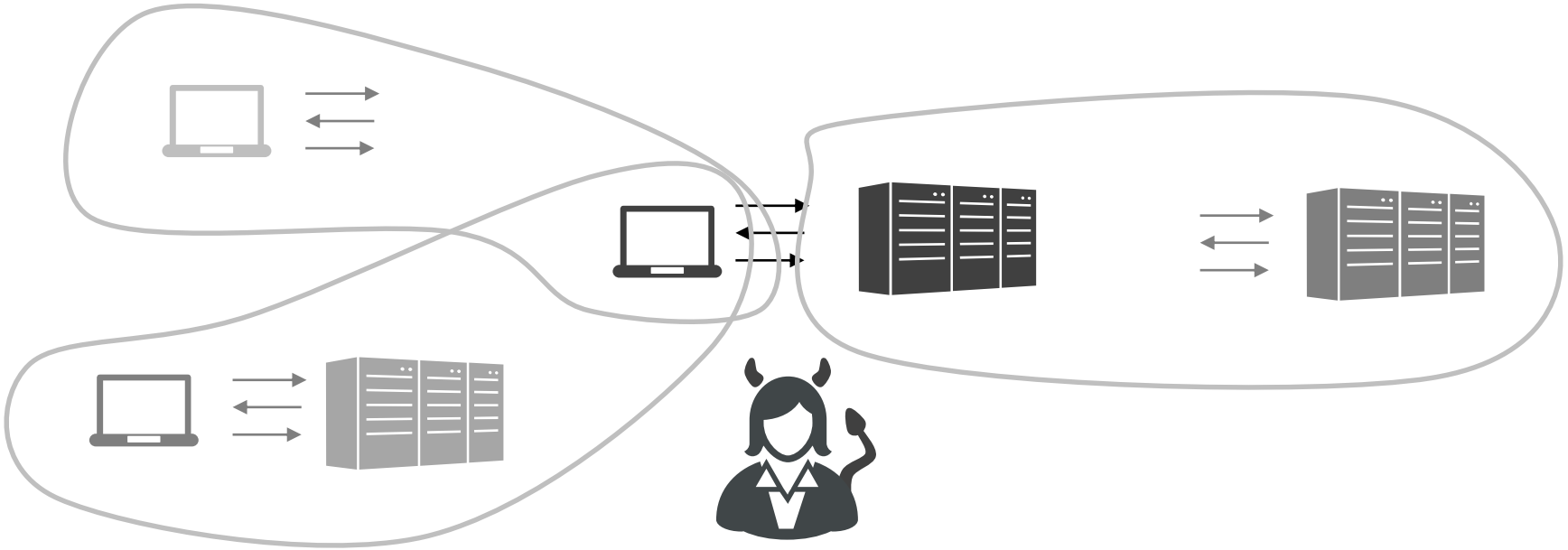
Security guarantees() ≥ Security guarantees()

sometimes identical:
semantically secure encryption = IND-CPA

sometimes different:
ZK proofs > WI proofs

Universal Composition (UC)

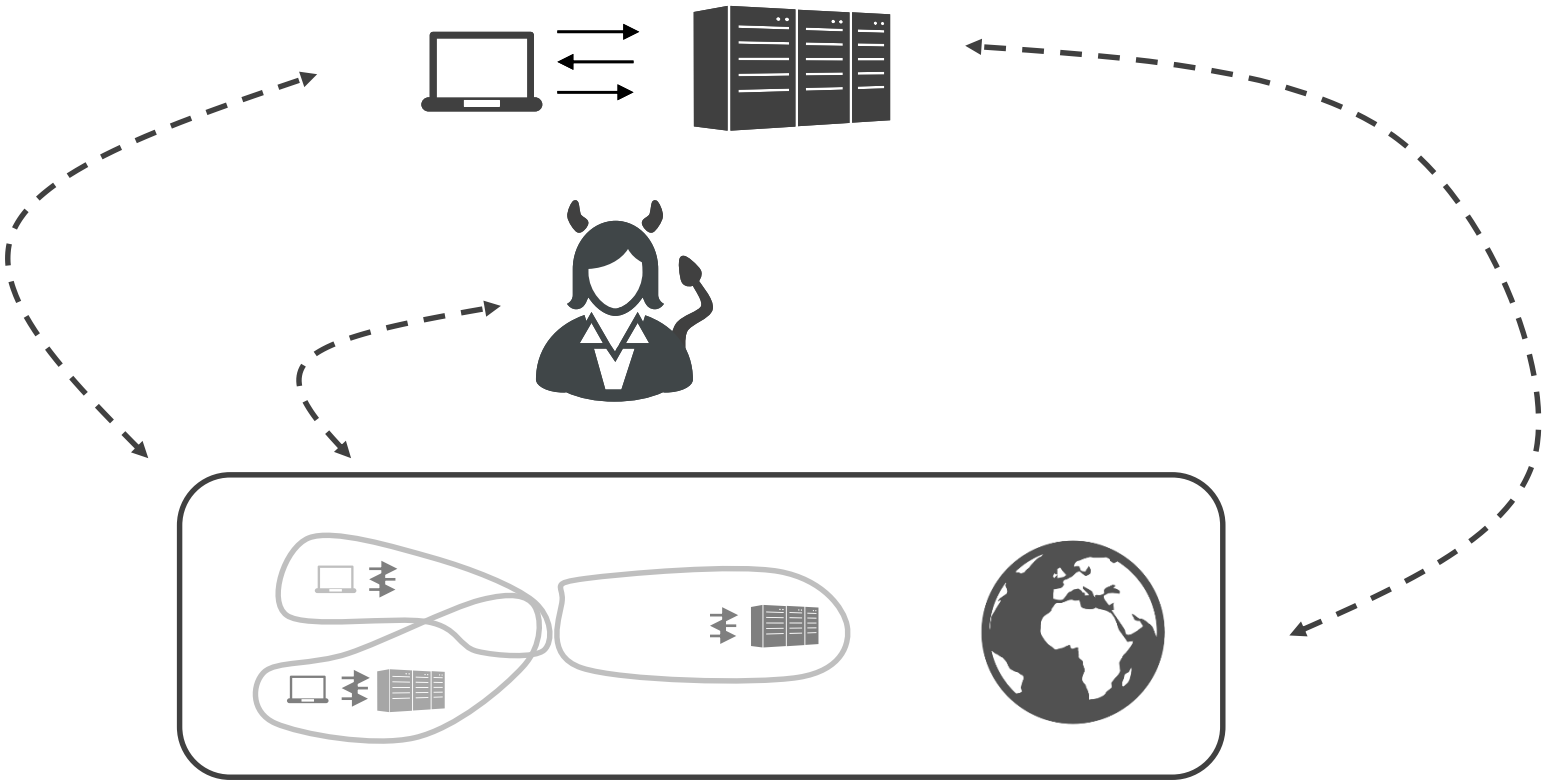
General Composition Problem



Other Protocol executions may interfere with execution in question
(input/output behavior, timing of messages,…)

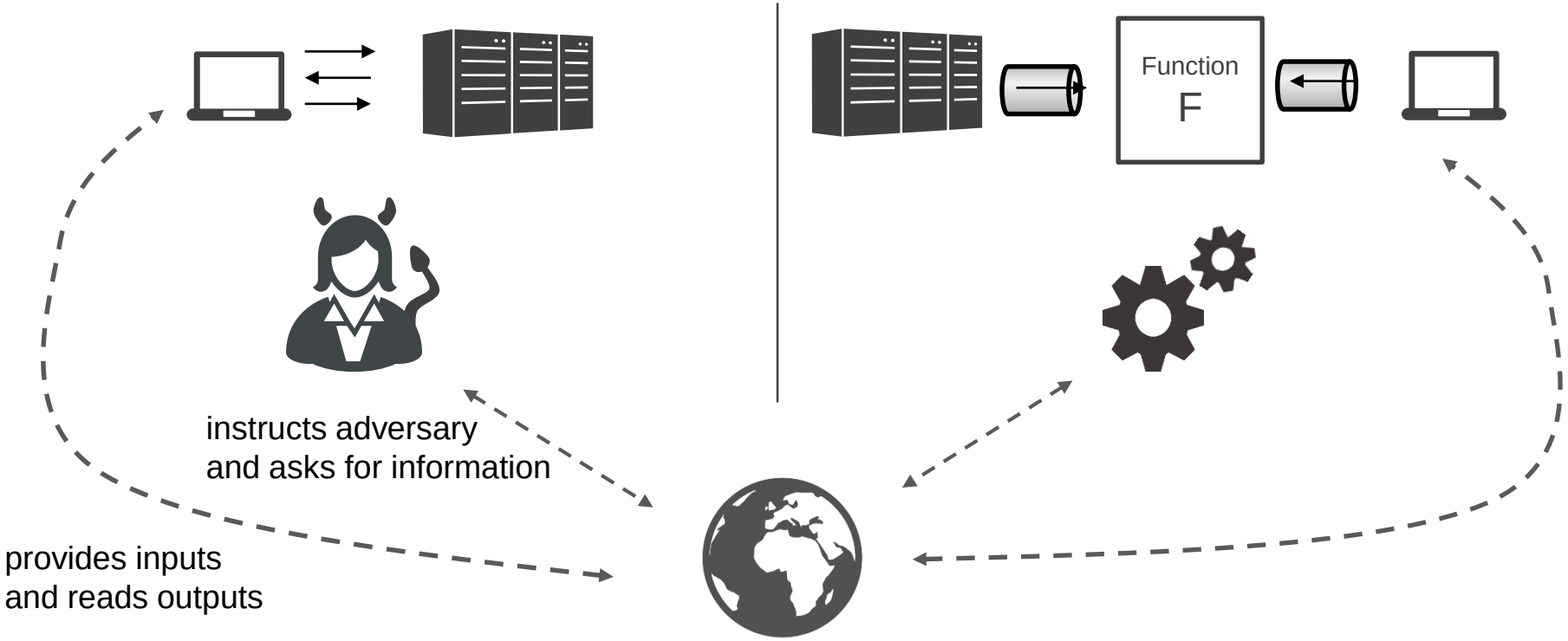
Towards General Composition

Move other executions
into abstract environment



Universally Composable Security

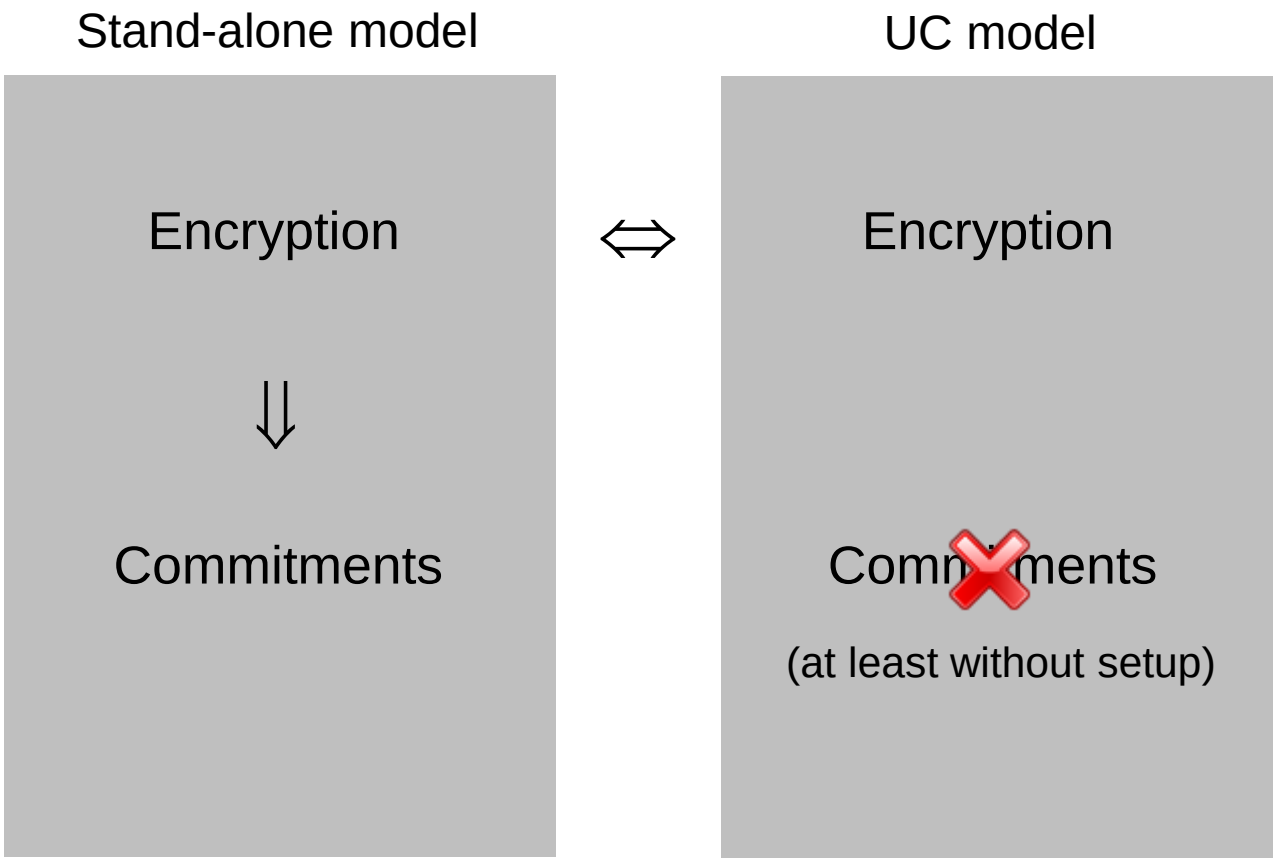
Canetti: Universally Composable Security: A New Paradigm for Cryptographic Protocols, FOCS 2001



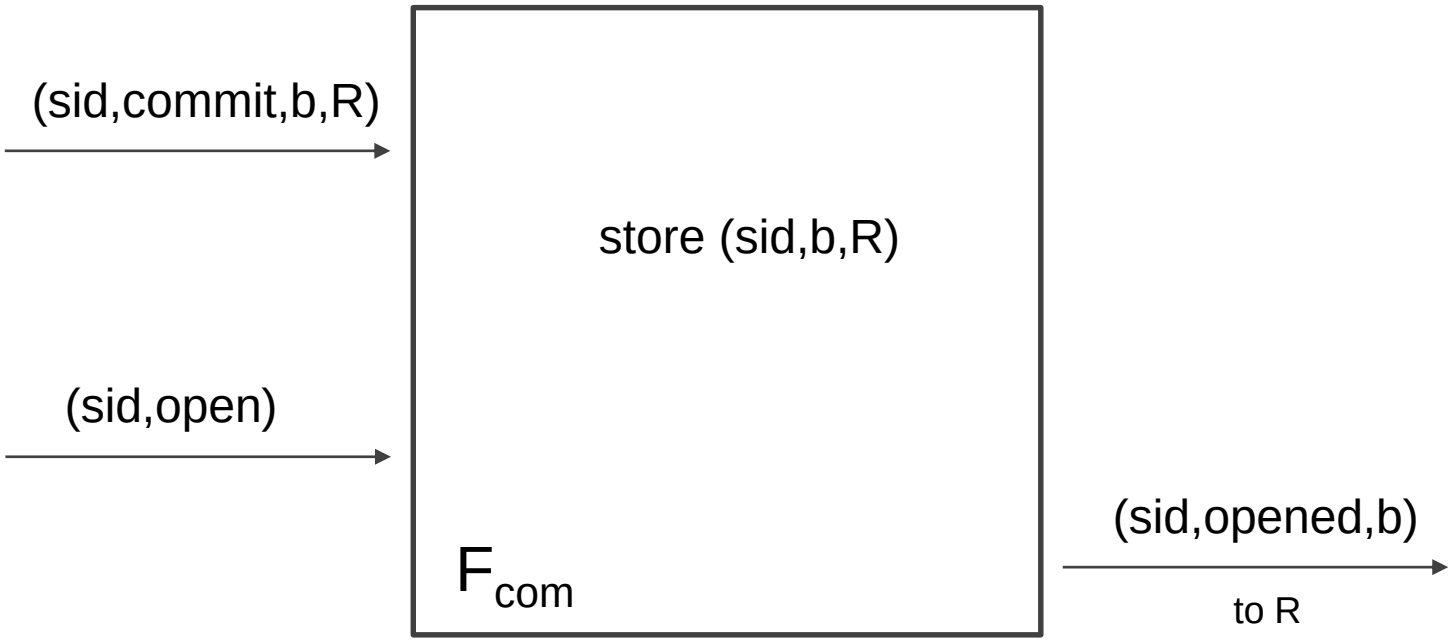
∀ Adversary A: ∃ Simulator S: ∀ **Environments Z**: REAL ≈ IDEAL

UC is special

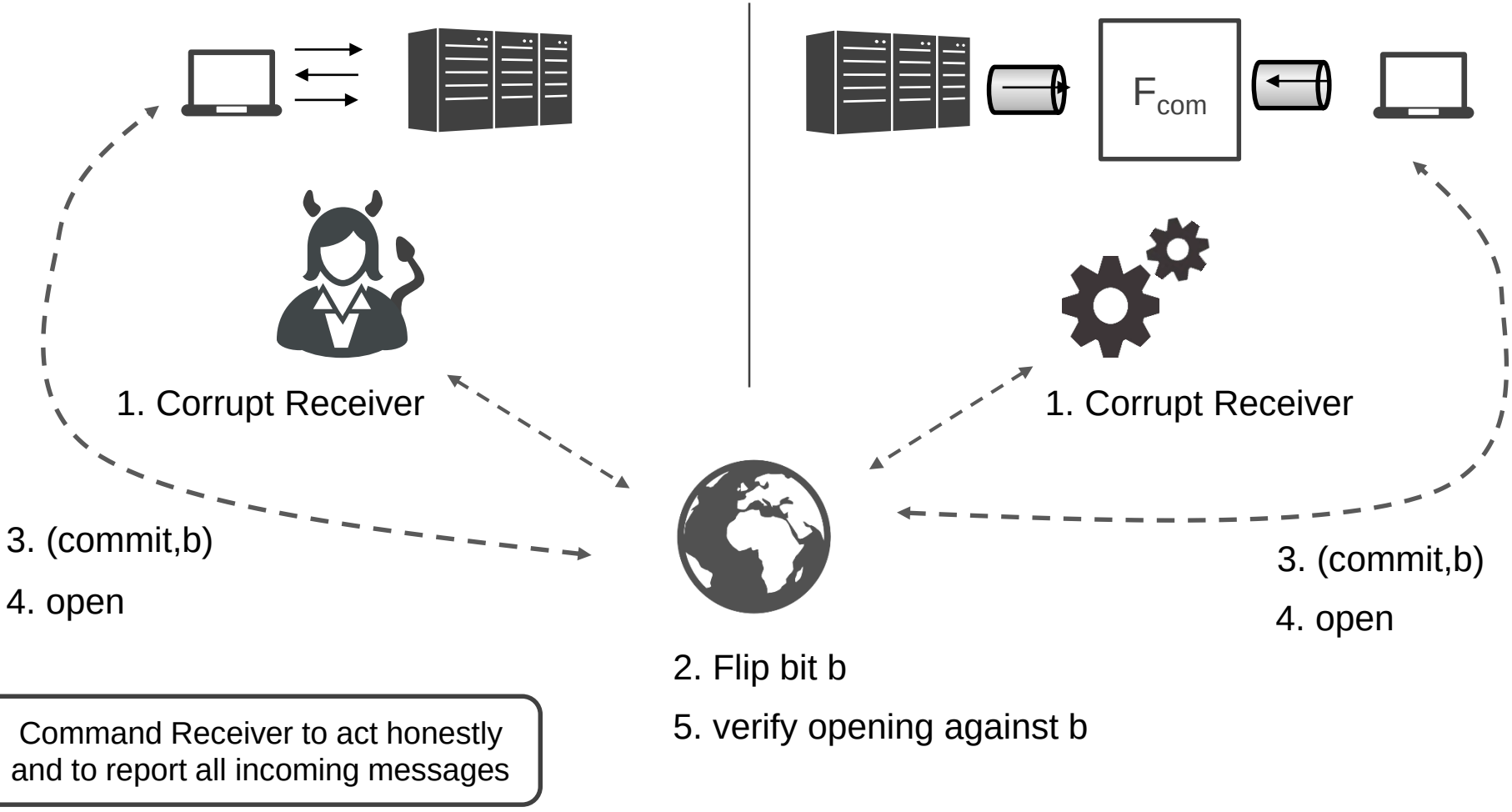
Canetti, Fischlin: Universally Composable Commitment Schemes, Crypto 2001



Ideal Commitment (simplified)



Impossibility of UC Commitments (I)



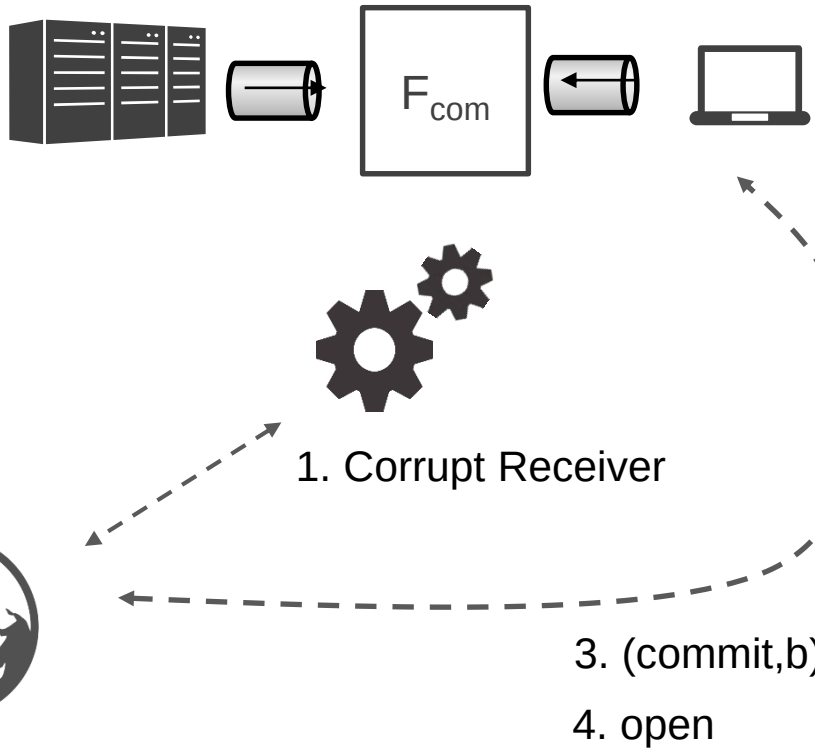
Command Receiver to act honestly and to report all incoming messages

Impossibility of UC Commitments (II)

in 3. simulator S would have to report commitment communication before learning b

Communication with Receiver is binding

Simulator is wrong with probability 1/2

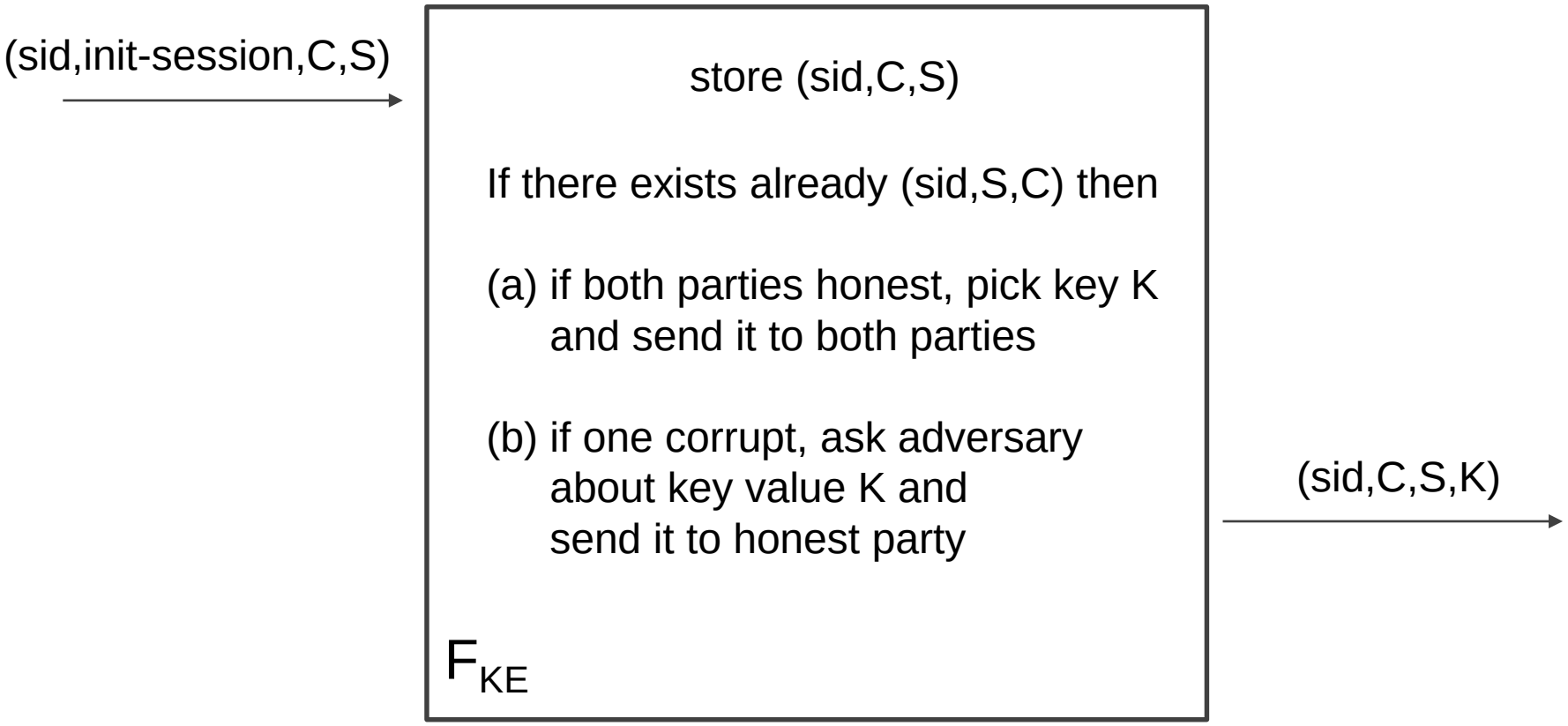


Command Receiver to act honestly and to report all incoming messages

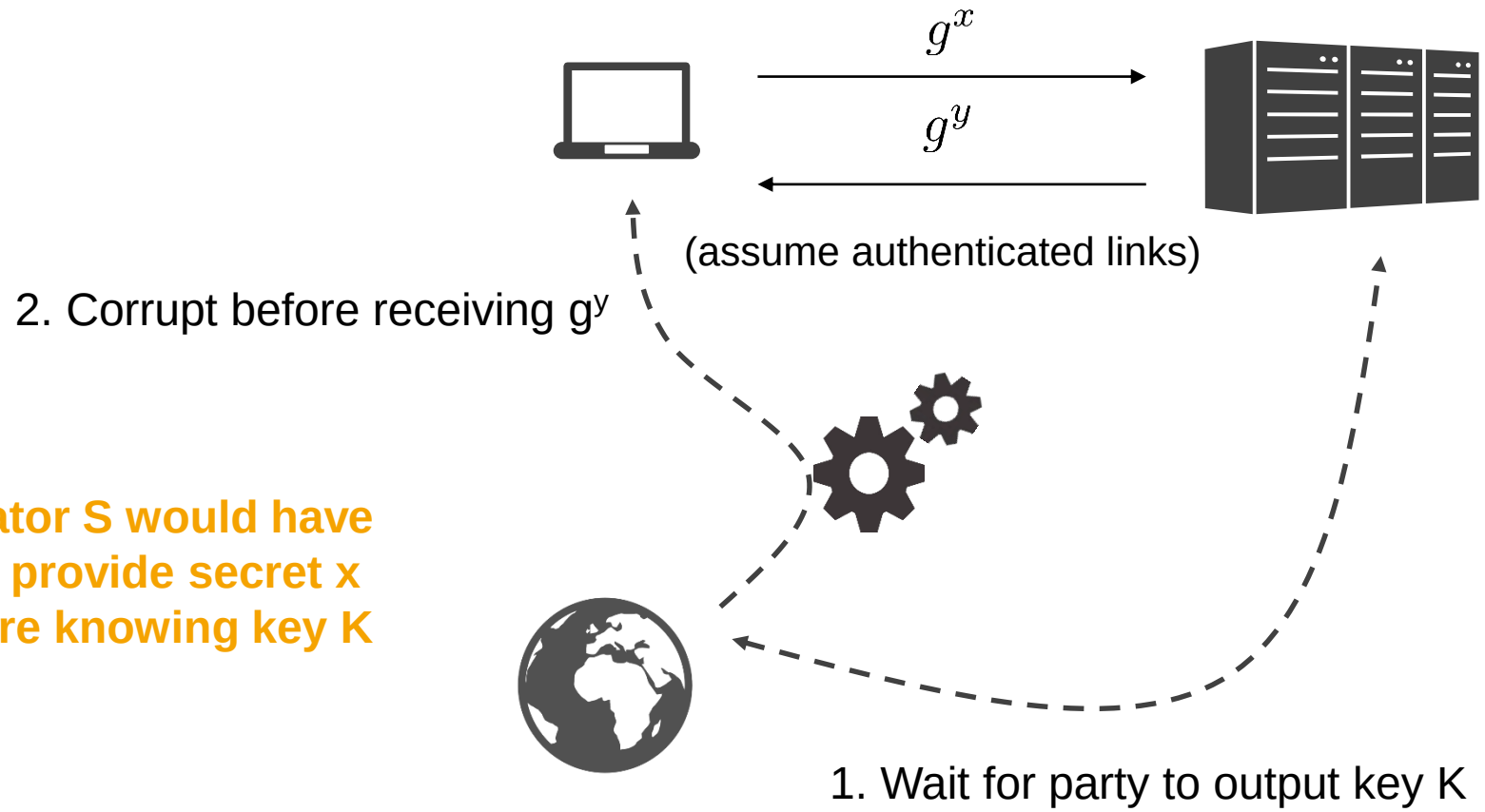
Universally Composable Key Exchange

Ideal Key Exchange (simplified)

Canetti, Krawczyk: Universally Composable Notions of Key Exchange and Secure Channels, Eurocrypt 2002

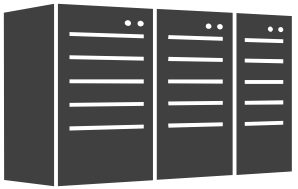


The Commitment Problem, again



ACKnowledgements to Rescue

g^x



$g^y,\ \mathrm{Sig}(\mathrm{sk}_S, g^x, g^y, C), \mathrm{cert}_S$

compute DH key

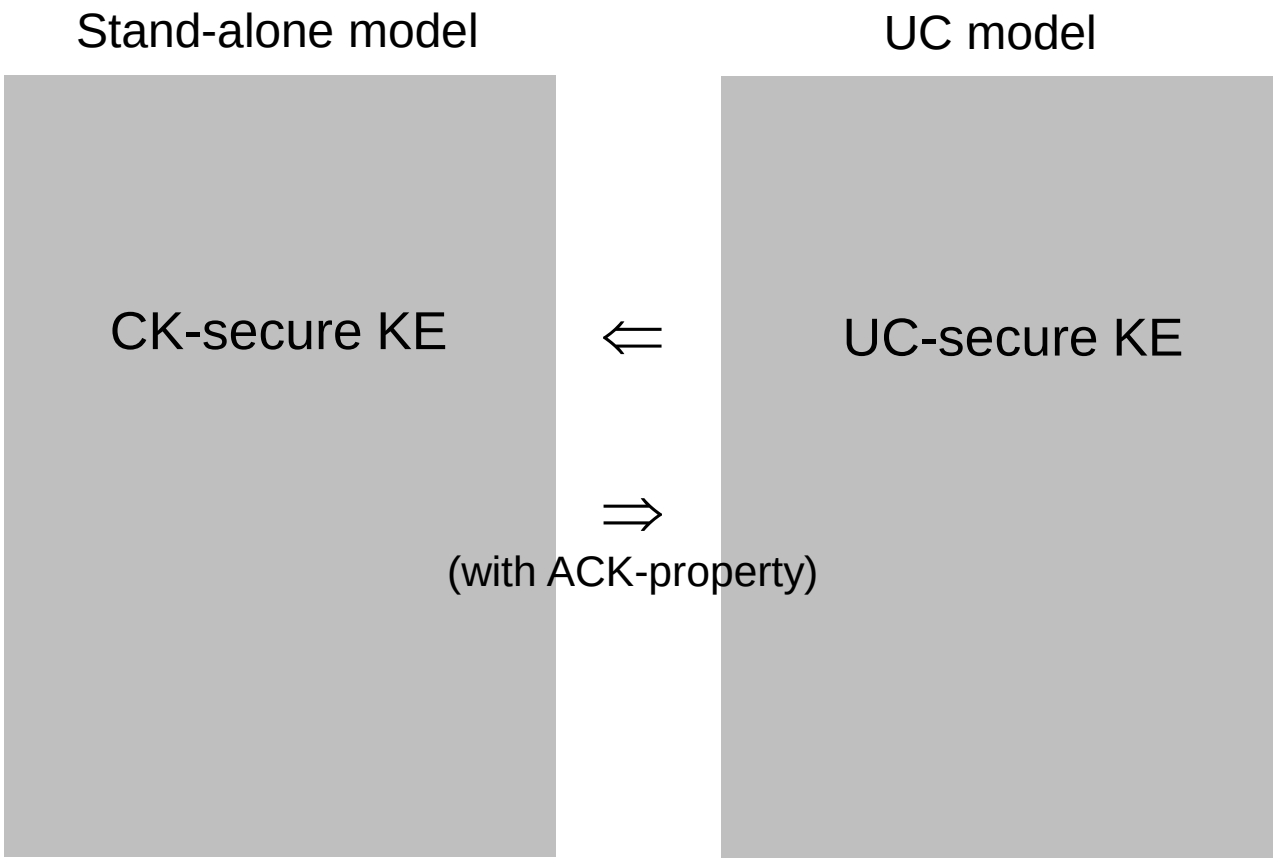
erase x

$\mathrm{Sig}(\mathrm{sk}_C, g^y, g^x, S), \mathrm{cert}_C$

ACK-property:
If corruption happens,
then simulator can provide
consistent(-ly looking) state
(given key K)

ISO/IEC 9798-3 / SIG-DH is
UC-secure key exchange protocol

Equivalence of CK and UC



The End