

Security of the TCG Privacy-CA Solution

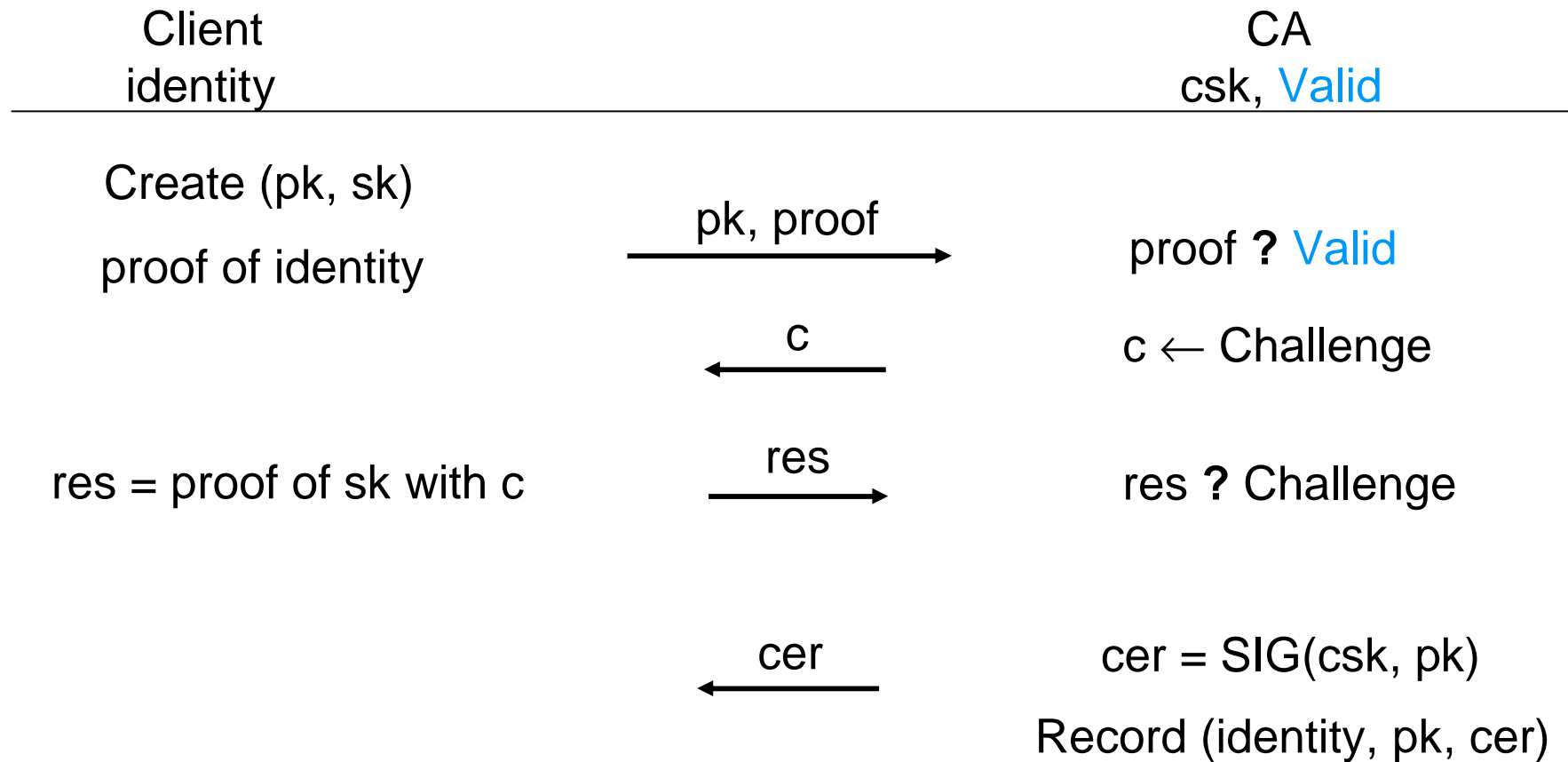
Liqun Chen and Bogdan Warinschi

The paper will be presented at TrustCom 2010

Outline

- What is the TCG privacy-CA solution (PCAS)?
 - A certification service supporting anonymity
 - Designed by Trusted Platform Module (TPM) WG – TCG TPM V1.2, ISO/IEC 11889
 - An elder brother of DAA
- A rigorous security analysis of the TCG PCAS protocol
 - Security model
 - Security proof
- What has the proof told us?
 - TCG PCAS is secure only under a weak model
- Propose an enhanced protocol secure under a stronger model
- Conclusions

A Conventional Certification Service



A "Conventional" Certification Service Supporting Anonymity

Client
esk/epk \rightarrow identity

CA
csk, Valid

Create (pk, sk)

$\xrightarrow{\text{epk, pk}}$

epk \in ? Valid

\xleftarrow{c}

$c \leftarrow$ Challenge

res = proof of (sk, esk, c)

$\xrightarrow{\text{res}}$

res ? (Challenge, eps, pk)

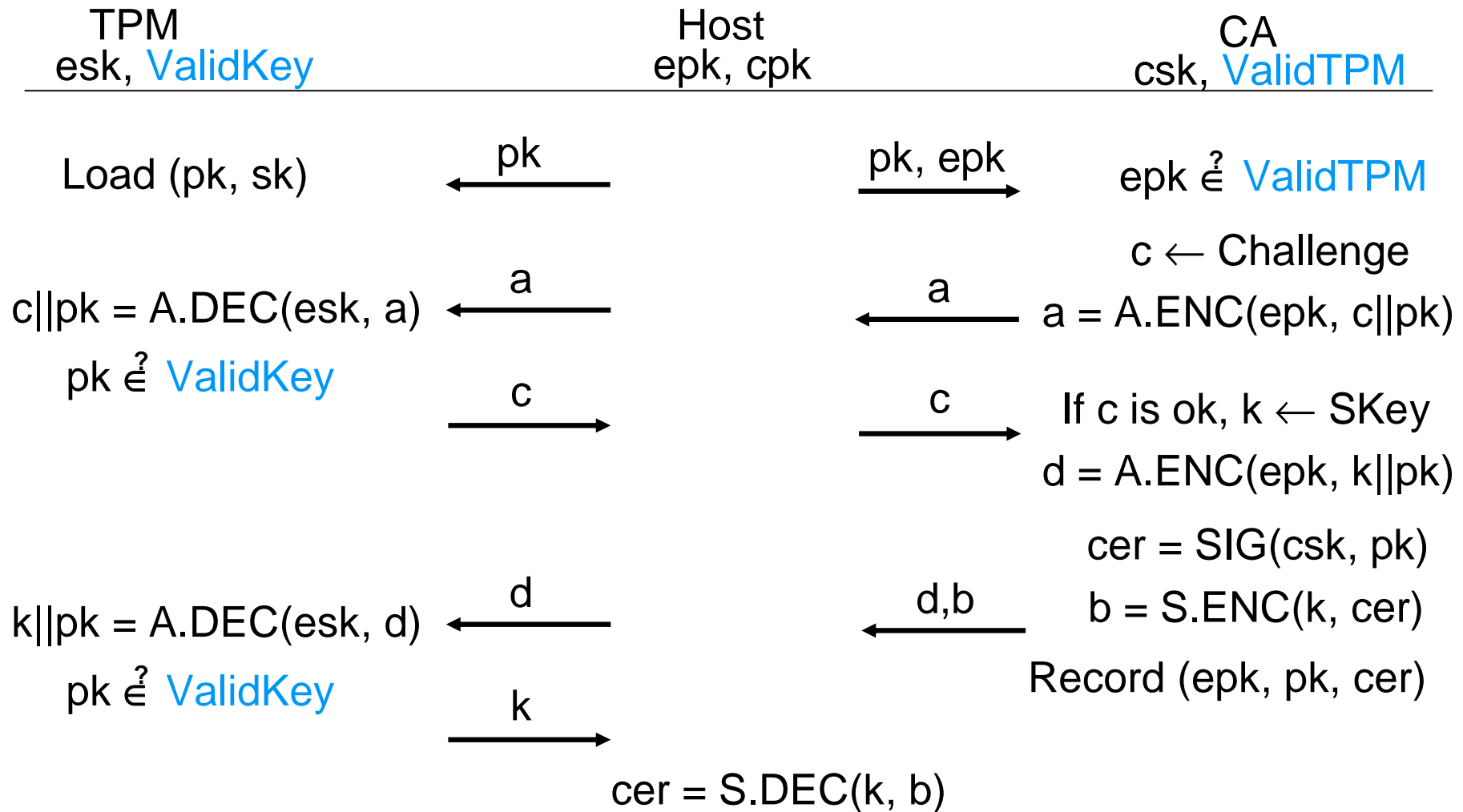
$\xleftarrow{\text{cer}}$

cer = SIG(csk, pk)

Record (epk, pk, cer)

Since there is no link between epk and future uses of (pk, cer), this service preserves the client anonymity to third parties.

The TCG Privacy-CA Protocol



Security Properties

- Authentication
- Anonymity
- Unlinkability
- Deniability

Security Model for Authentication

- An experiment
- Adversary controls communications between TPMs and CAs
- Three oracles
 - TPM oracle (epk, esk)
 - CA oracle (cpk, csk)
 - CA corruption
- Two global variables
 - ValidKey: (epk, pk); $\text{ValidKey}(\text{epk}_i, \text{pk}) = 1$ means TPM_i knows both esk_i and sk
 - ValidTPM: (cpk, epk); $\text{ValidTPM}(\text{cpk}_j, \text{epk}_i) = 1$ means CA_j approves of TPM_i
- One registration list
 - RegList: (epk, cpk, pk, cer)

Two Oracles

TPM (epk, esk)

1. receive pk
if $\text{ValidKey}(\text{epk}, \text{pk}) = 0$
then abort
2. receive a
if $\text{A.DEC}(\text{esk}, a) \neq c \parallel \text{pk}$
then abort
send c
3. receive d
if $\text{A.DEC}(\text{esk}, d) \neq k \parallel \text{pk}$
then abort
send k

CA(cpk, csk)

1. receive (epk, pk)
if $\text{ValidTPM}(\text{cpk}, \text{epk}) = 0$ then abort
select $c \leftarrow \{0, 1\}^n$
 $a \leftarrow \text{A.Enc}(\text{epk}, c \parallel \text{pk})$
send a
2. receive c'
if $c \neq c'$ then abort
 $\text{cer} \leftarrow \text{SIG}(\text{csk}, \text{pk}); k \leftarrow \text{A.KG}(\eta);$
 $b \leftarrow \text{S.ENC}(k, \text{cer}); d \leftarrow \text{A.ENC}(\text{epk}, k \parallel \text{pk})$
append (epk, cpk, pk, cer) to RegList
send b, d

Experiment: adversary against protocol

$\text{Exp}_{\text{PCAS}, \mathbf{A}}(\eta)$

for each CA c_j do $(\text{cpk}_j, \text{csk}_j) \leftarrow \text{KG}(\eta)$

for each TPM t_i do $(\text{epk}_i, \text{esk}_i) \leftarrow \mathbf{A}.\text{KG}(\eta)$

$\text{ValidTPM}, \text{ValidKey} \leftarrow \mathbf{A}(\text{cpk}, \text{epk})$

$\text{RegList} \leftarrow \text{empty}$

$(\text{epk}_{i^*}, \text{cpk}_{j^*}, \text{pk}^*, \text{cer}^*) \leftarrow \mathbf{A}^{\text{TPM}, \text{CA}, \text{CorrCA}}$

if $\text{VER}(\text{cpk}_{j^*}, (\text{pk}^*, \text{cer}^*)) = 0$ or csk_{j^*} is corrupt return 0

if $(i^*, \text{cpk}_{j^*}, \text{pk}^*, \text{cer}^*) \neq \text{RegList}$ return 1 ----- a certificate has been forged

if $(\text{epk}_{i^*}, \text{cpk}_{j^*}, \text{pk}^*, \text{cer}^*) \in \text{RegList}$ and

$\text{ValidKey}(\text{epk}_{i^*}, \text{pk}^*) = 0$ return 1 ---- a cer has been given to a wrong pk

return 0

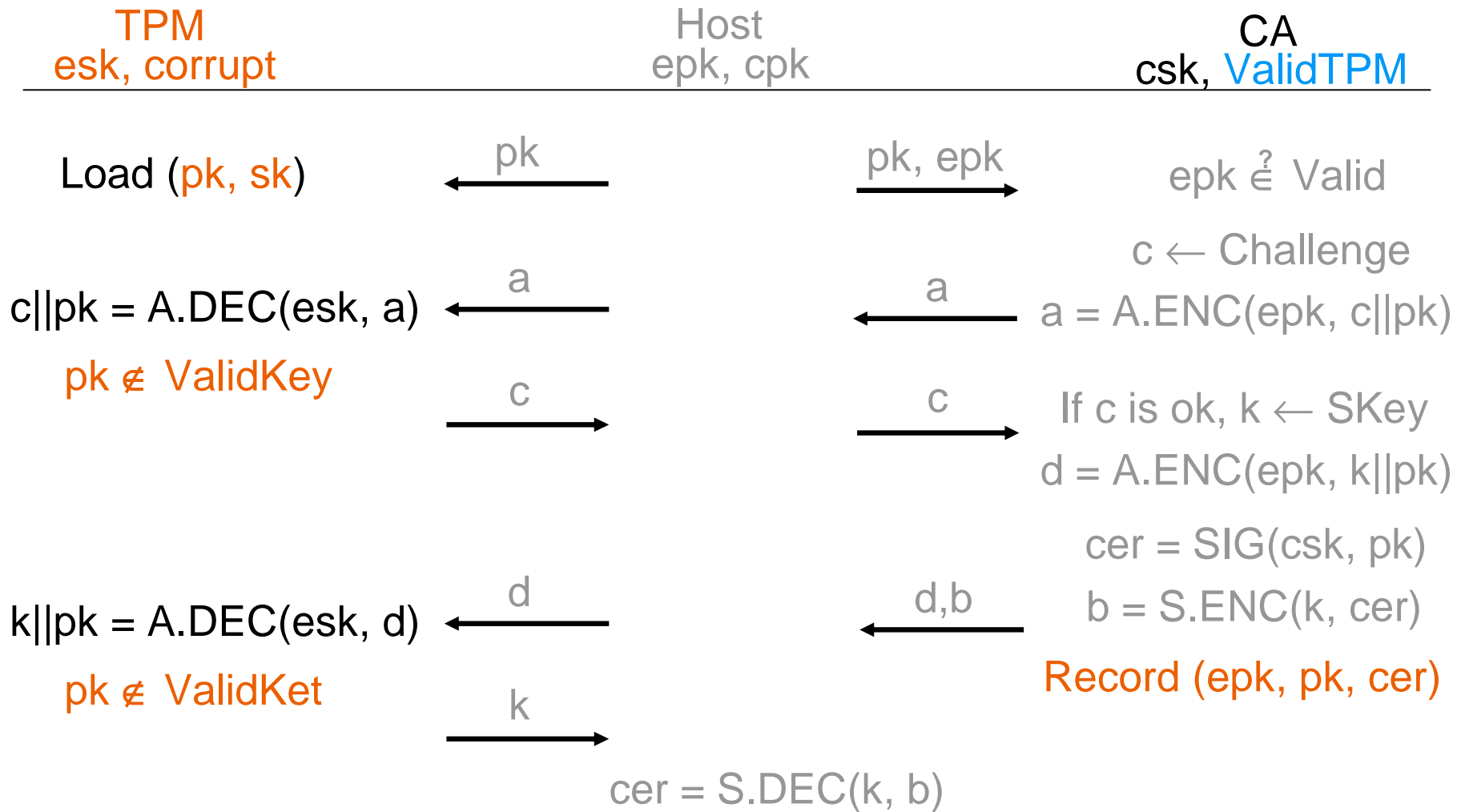
$\text{Adv}_{\text{PCAS}, \mathbf{A}}(\eta) = \Pr[\text{Exp}_{\text{PCAS}, \mathbf{A}}(\eta) = 1]$ is negligible

$\text{TPM}_i^n, \text{CA}_j^m$
The number is
bounded by $p(\eta)$

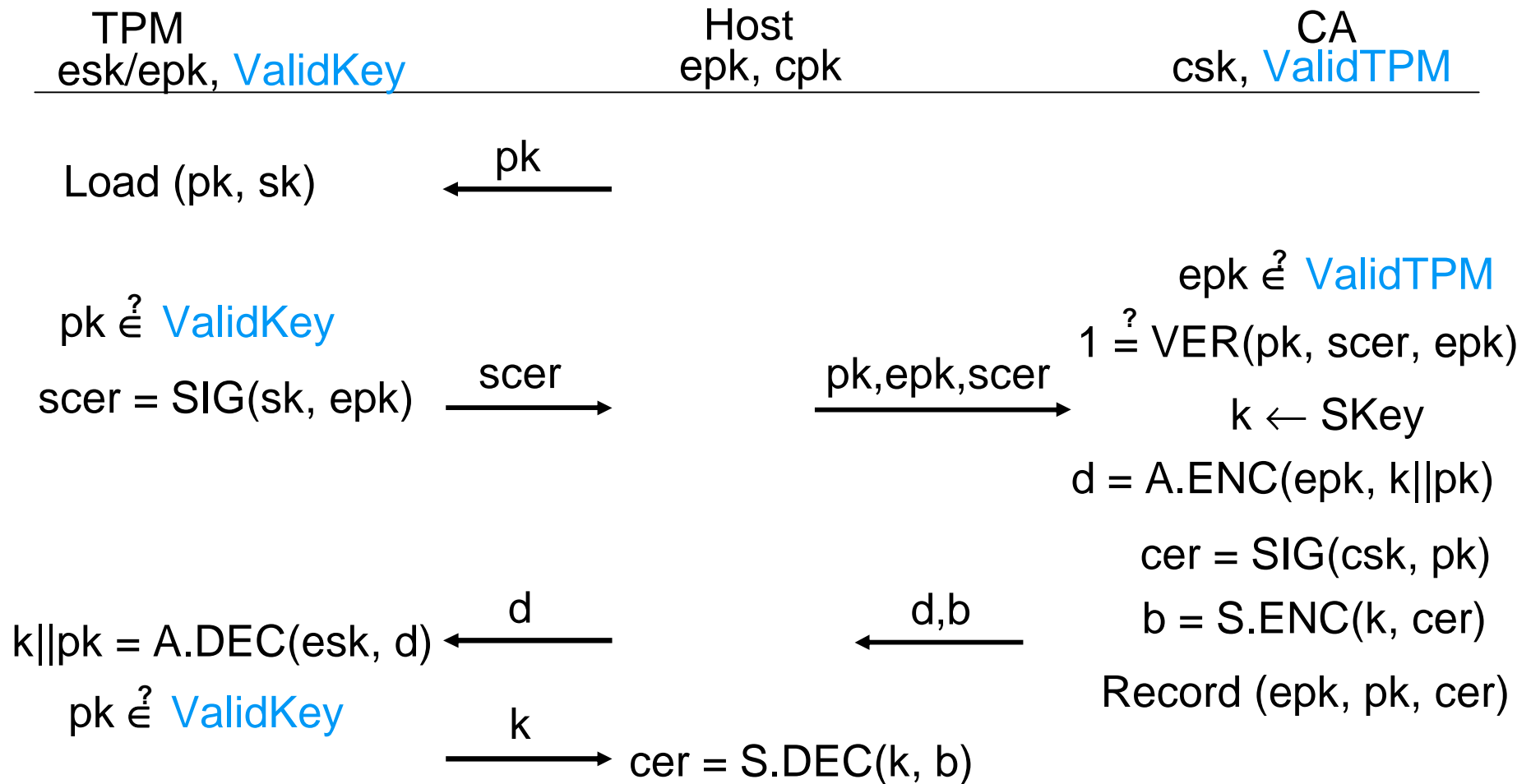
Proof Result

- Not surprisingly
- If the signature scheme SIG is EU-CMA secure, and the asymmetric encryption scheme A.ENC is IND-CCA secure, then the PCAS protocol is secure under the model
- Security of the symmetric encryption scheme S.ENC is not required for the security proof
- The model is appropriate for our purpose but weak, since there is no TPM corruption oracle

Attack to The TCG PCAS



The Enhanced Privacy-CA Protocol



Conclusions

- Studied security notion and model of the authentication property for the TCG privacy-CA protocol
- Made a rigorous security analysis of the TCG privacy-CA protocol
- The protocol has been proved secure under a weak model (without corrupting TPMs), assuming standard security notions for the underlying asymmetric encryption and signature schemes
- Proposed a strengthened protocol that meets a stronger notion of security where the adversary is allowed to adaptively corrupt TPMs
- Is the enhanced scheme strong enough from a cryptographer's point of view?
- Is the enhanced scheme practical from the TCG perspective?

Q&A?