Cryptanalysis of GlobalPlatform Secure Channel Protocols

Mohamed Sabt and **Jacques Traoré**

SSR 2016

December 5, 2016

3rd International Conference on Research in Security Standardisation

orange™

Outline

- Context
- GlobalPlatform
- Secure Channel Protocols
- Theoretical attacks against SCP02
- SCP03 security results
- Conclusion

Introduction

Context

GlobalPlatform (GP)

A cross-industrial consortium that issues specifications about smart cards.

GP Card Specification

A set of technical documentation relating to the deployment and management of multiple applications on smart cards.

GP Goal

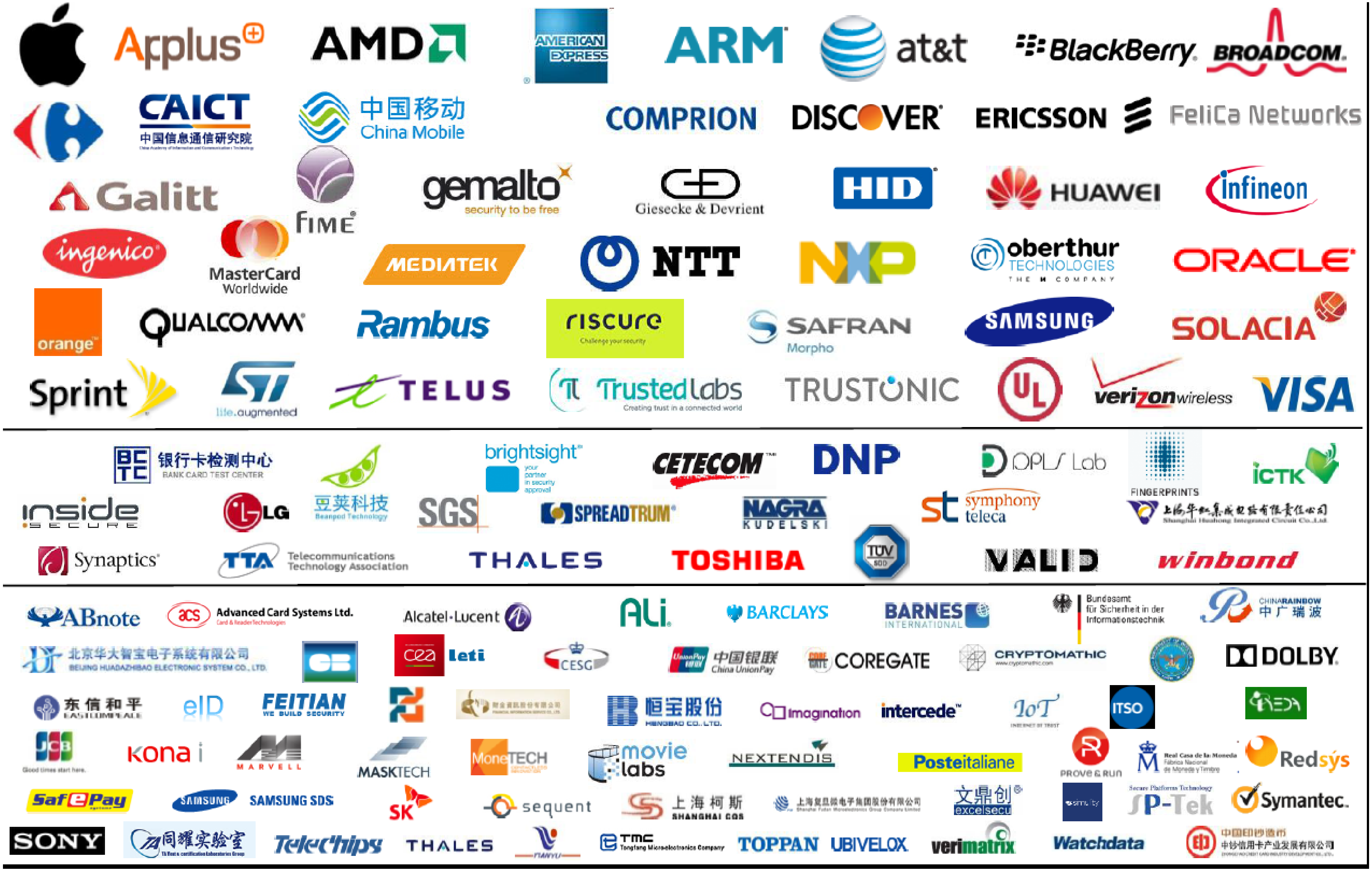
To dynamically and remotely manage the content of smart cards by different and independent parties. This management includes the installation and the removal of applications on smart cards.

17.7 billion secure elements (SEs) are based on GP Card Specifications
That is 41% of all SEs shipped since 2010

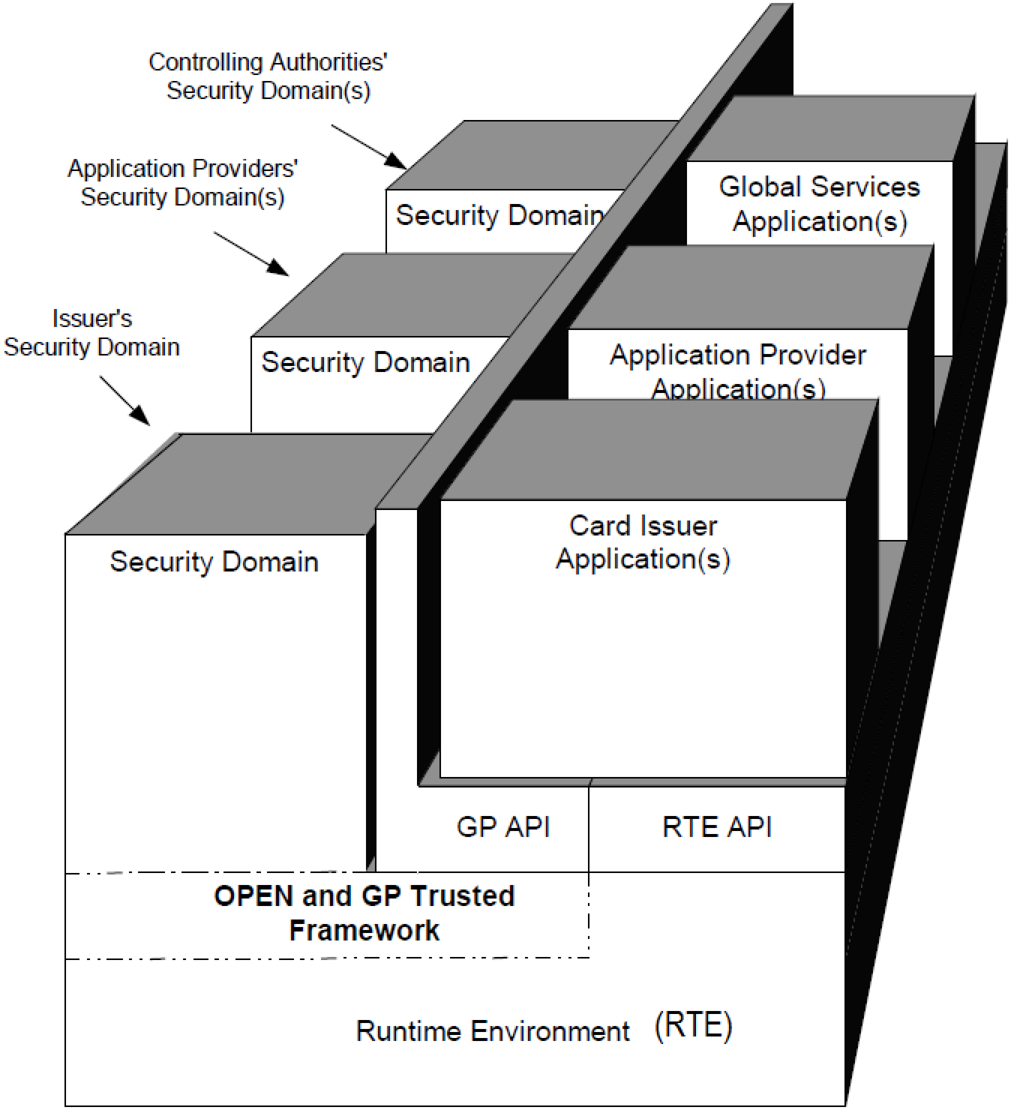
GLOBALPLATFORM®
THE STANDARD FOR MANAGING APPLICATIONS ON SECURE CHIP TECHNOLOGY

orange™

120+ GlobalPlatform members



GP Architecture


Controlling Authorities' Security Domain(s)
Application Providers' Security Domain(s)
Issuer's Security Domain
Security Domain
Security Domain
Security Domain
Global Services Application(s)
Application Provider Application(s)
Card Issuer Application(s)
GP API
RTE API
OPEN and GP Trusted Framework
Runtime Environment (RTE)

Secure Content Management

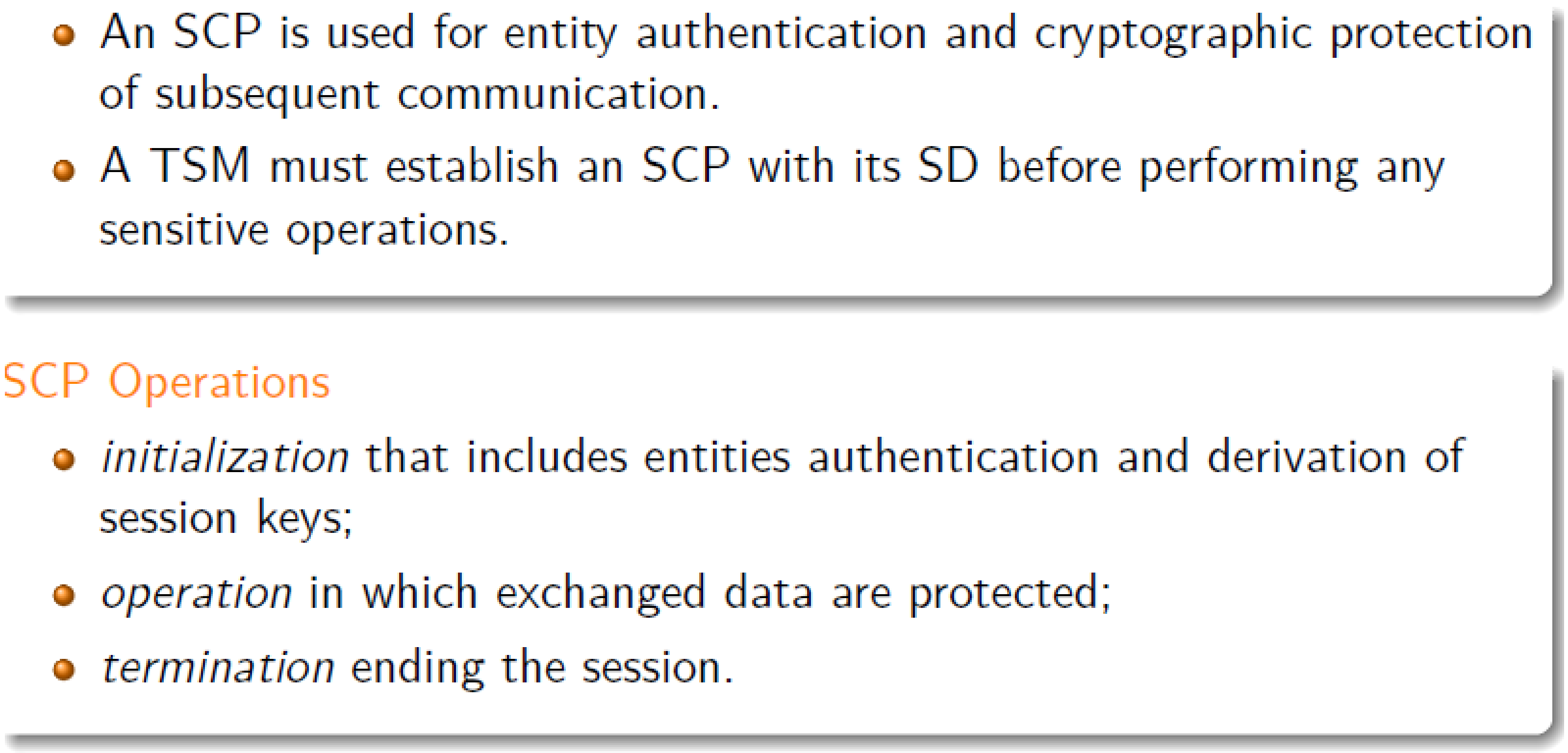
Delegated Management Model

The Card Issuer leases the ability of managing card content to one or several Trusted Service Managers.

Security Domain (SD)

- A security domain is a private portion of smart cards that is created by the Card Issuer.
- Each SD can download, install and maintain several smart card applications.
- Each SD shares some secret cryptographic keys with its owner.

Secure Channel Protocols (SCPs)



- An SCP is used for entity authentication and cryptographic protection of subsequent communication.
- A TSM must establish an SCP with its SD before performing any sensitive operations.

SCP Operations

- *initialization* that includes entities authentication and derivation of session keys;
- *operation* in which exchanged data are protected;
- *termination* ending the session.

Secure Channel Protocols (SCPs)

- An SCP is used for entity authentication and cryptographic protection of subsequent communication.
- A TSM must establish an SCP with its SD before performing any sensitive operations.

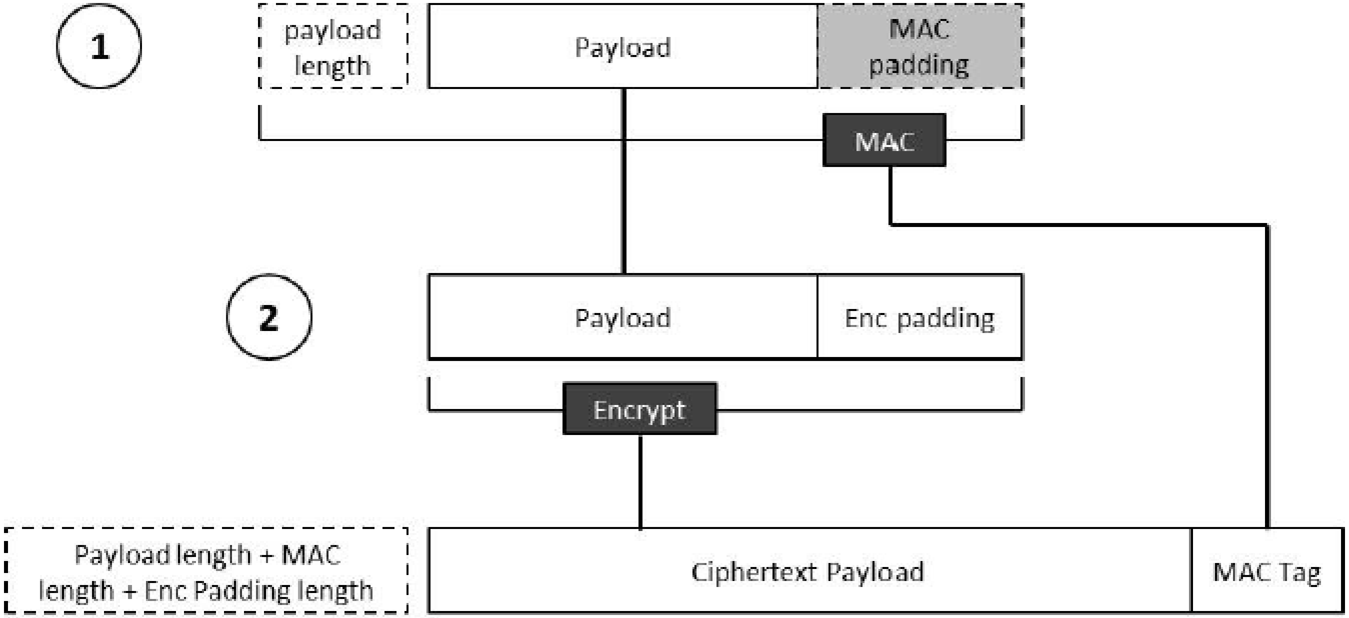
SCP Operations

- *initialization* that includes entities authentication and derivation of session keys;
- *operation* in which exchanged data are protected;
- *termination* ending the session.

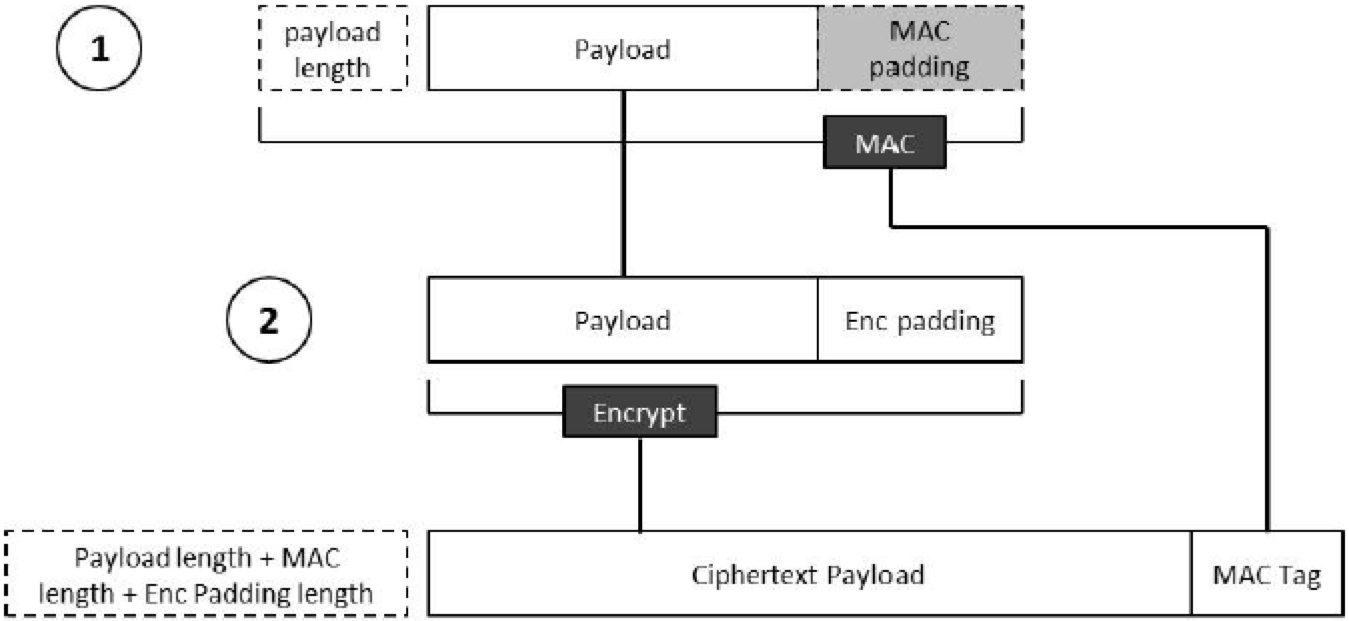
Secure Channel Protocol ‘2’

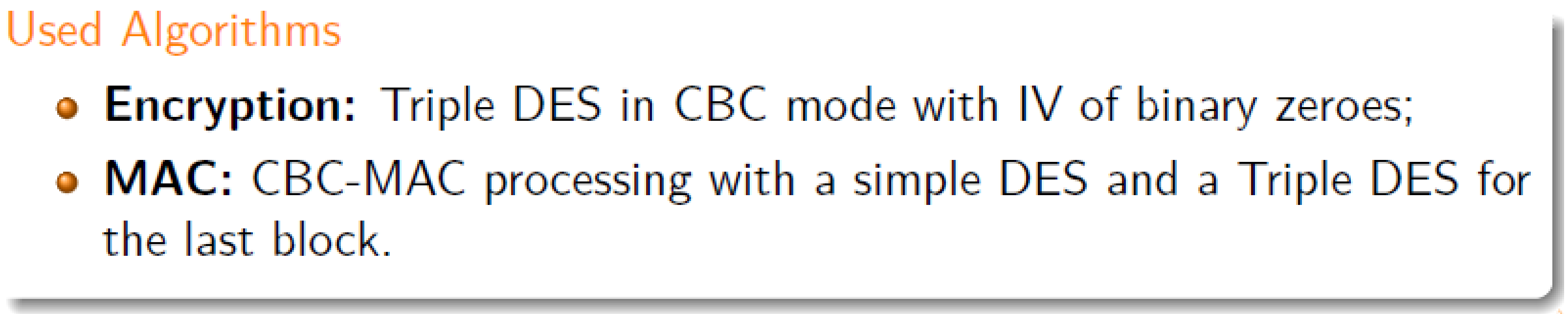
Description

SCP02 relies on the « Encrypt-and-MAC » method



Description





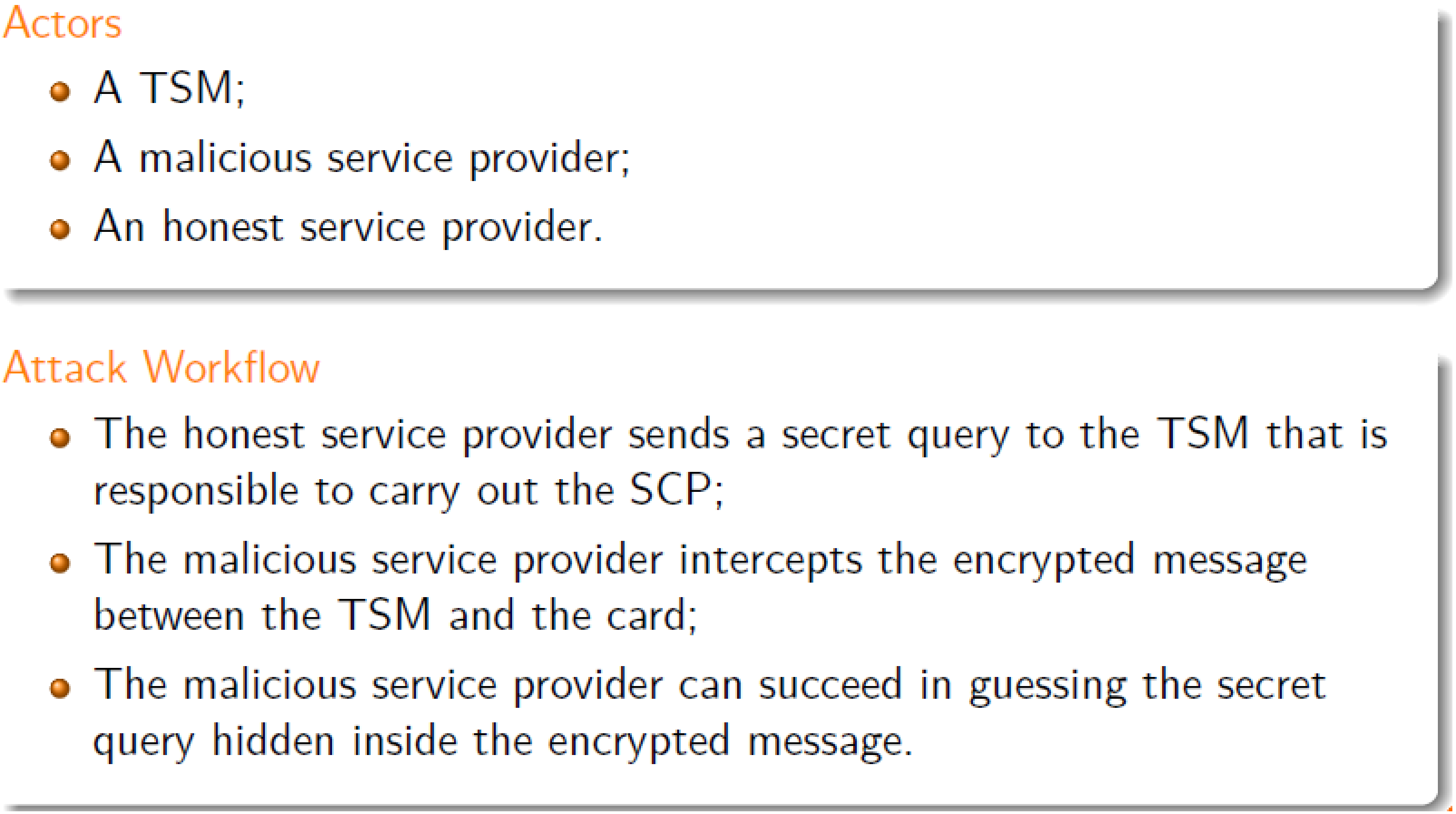
Used Algorithms

- **Encryption:** Triple DES in CBC mode with IV of binary zeroes;
- **MAC:** CBC-MAC processing with a simple DES and a Triple DES for the last block.

Security Flaw

- SCP02 uses CBC-mode with a fixed IV
- The SCP02 encryption scheme is deterministic and clearly not IND-CPA secure
- It is vulnerable to a classical plaintext-recovery attack (for plaintext messages with small entropy, e.g., PIN):
  1. let C = $\mathcal{E}_{k}\_\mathrm{SCP02}(m)$ be the targeted ciphertext
  2. The adversary A randomly chooses a message m' among the set of possible values for m'
  3. Ask the challenger to encrypt m'in order to obtain C' = $\mathcal{E}_{k}\_\mathrm{SCP02}(m$')
  4. If C' = C then A has correctly guessed $m = m'$.

Plaintext Recovery Against GP compliant Smart Cards



Actors

- A TSM;
- A malicious service provider;
- An honest service provider.

Attack Workflow

- The honest service provider sends a secret query to the TSM that is responsible to carry out the SCP;
- The malicious service provider intercepts the encrypted message between the TSM and the card;
- The malicious service provider can succeed in guessing the secret query hidden inside the encrypted message.

Discussion About Feasibility of This Attack

One Common SD

- ☹ Both the malicious and the honest service providers share the same SD;
- ☺ There is no mention in the GP specifications that sharing the same SD is a bad practice;
- ☺ The TSM might install several applications into the same SD for the service providers that are not willing to pay the cost of having their own SD.

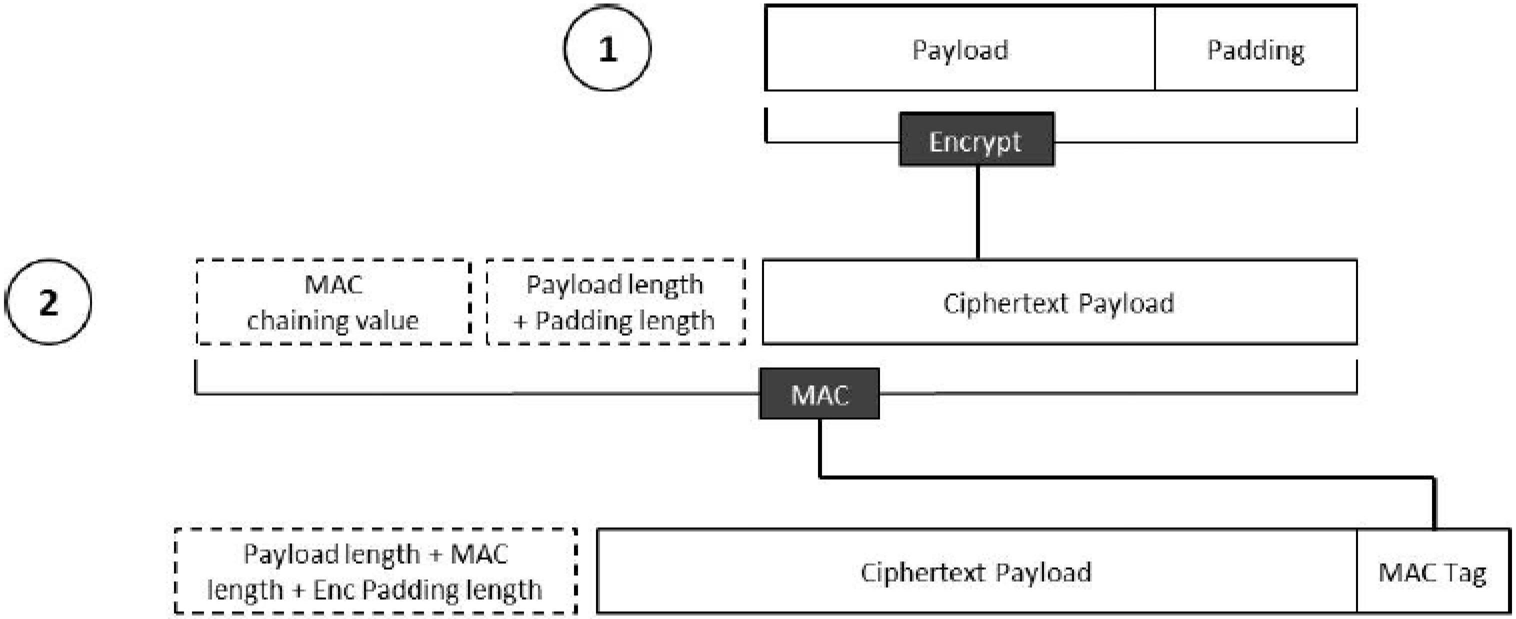
Low-Entropy Data

- ☹ The encrypted data must be of low entropy;
- ☺ These kind of data are not rare in the context of smart cards;
- ☺ GP commands are often structured with ASN.1 BER-TLV.

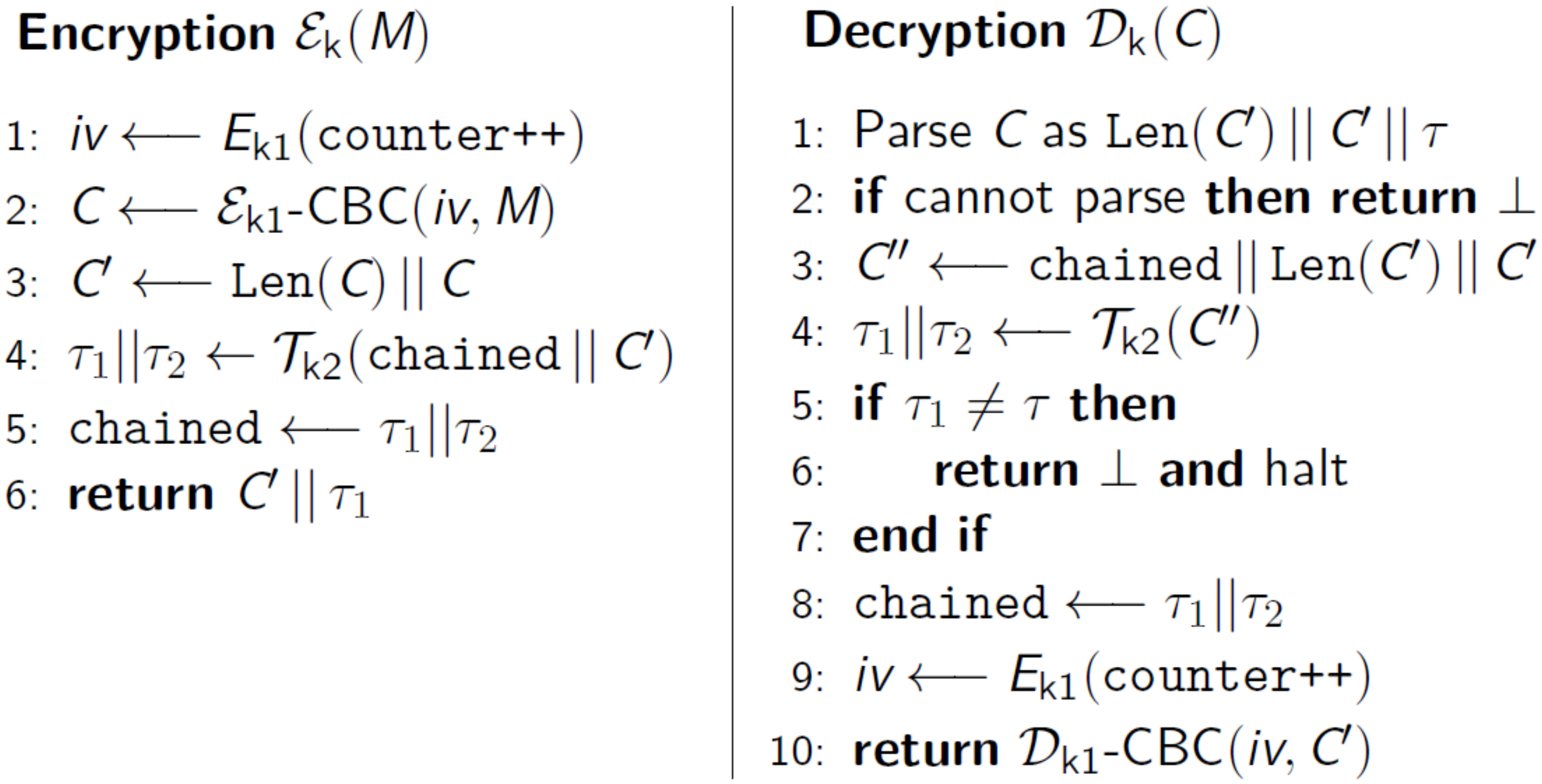
Secure Channel Protocol ‘3’

Description of SCP03

SCP03 relies on the « Encrypt-then-MAC » method



Formal Construction



Encryption $\mathcal{E}_k(M)$

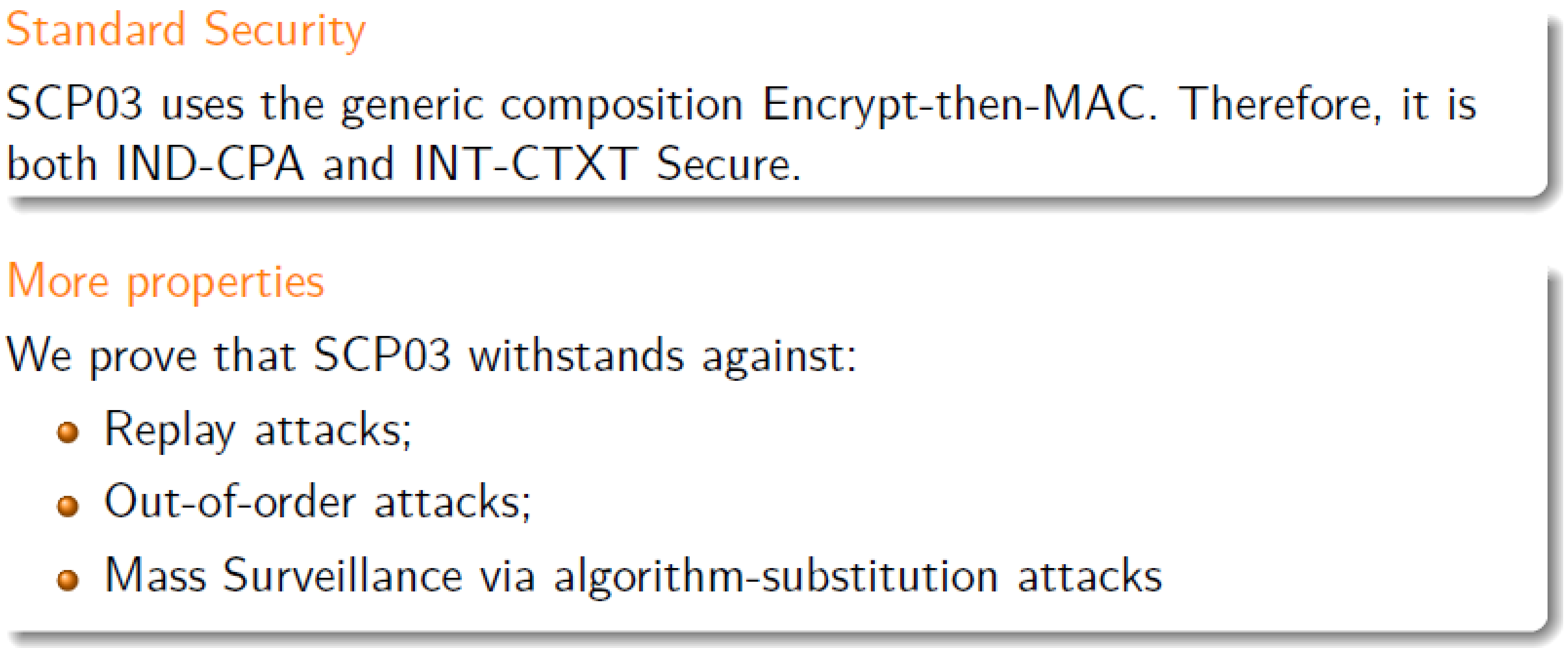
```
$iv \longleftarrow E_{k1}(\texttt{counter++})$
$C \longleftarrow \mathcal{E}_{k1}\text{-CBC}(iv, M)$
$C' \longleftarrow \texttt{Len}(C) \,||\, C$
$\tau_1||\tau_2 \leftarrow \mathcal{T}_{k2}(\texttt{chained} \,||\, C')$
$\texttt{chained} \longleftarrow \tau_1||\tau_2$
return $C' \,||\, \tau_1$
```

Decryption $\mathcal{D}_k(C)$

```
Parse $C$ as $\texttt{Len}(C') \,||\, C' \,||\, \tau$
if cannot parse then return $\perp$
$C'' \longleftarrow \texttt{chained} \,||\, \texttt{Len}(C') \,||\, C'$
$\tau_1||\tau_2 \longleftarrow \mathcal{T}_{k2}(C'')$
if $\tau_1 \neq \tau$ then
    return $\perp$ and halt
end if
$\texttt{chained} \longleftarrow \tau_1||\tau_2$
$iv \longleftarrow E_{k1}(\texttt{counter++})$
return $\mathcal{D}_{k1}\text{-CBC}(iv, C')$
```

An unusual MAC construction is used in the Encrypt-then-MAC method: only part of the MAC is included with the ciphertext

Security Analysis



Standard Security

SCP03 uses the generic composition Encrypt-then-MAC. Therefore, it is both IND-CPA and INT-CTXT Secure.

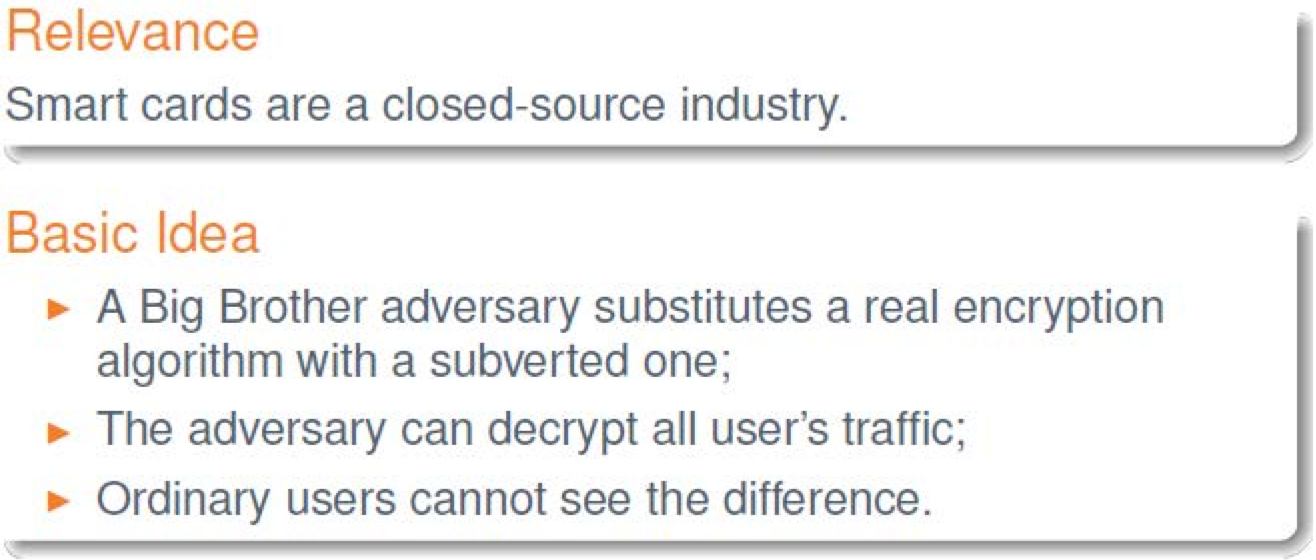
More properties

We prove that SCP03 withstands against:

- Replay attacks;
- Out-of-order attacks;
- Mass Surveillance via algorithm-substitution attacks

Mass Surveillance

Algorithm-Substitution Attacks (ASA)



Relevance

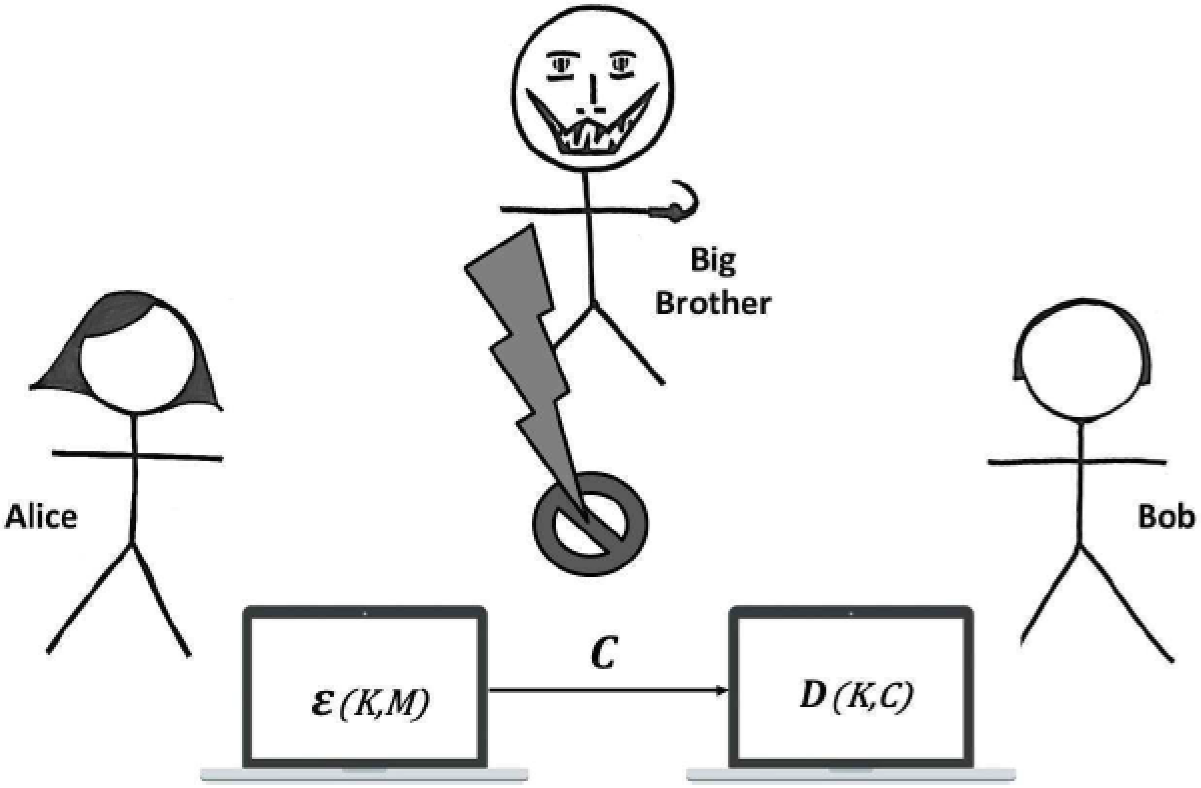
Smart cards are a closed-source industry.

Basic Idea

- A Big Brother adversary substitutes a real encryption algorithm with a subverted one;
- The adversary can decrypt all user’s traffic;
- Ordinary users cannot see the difference.

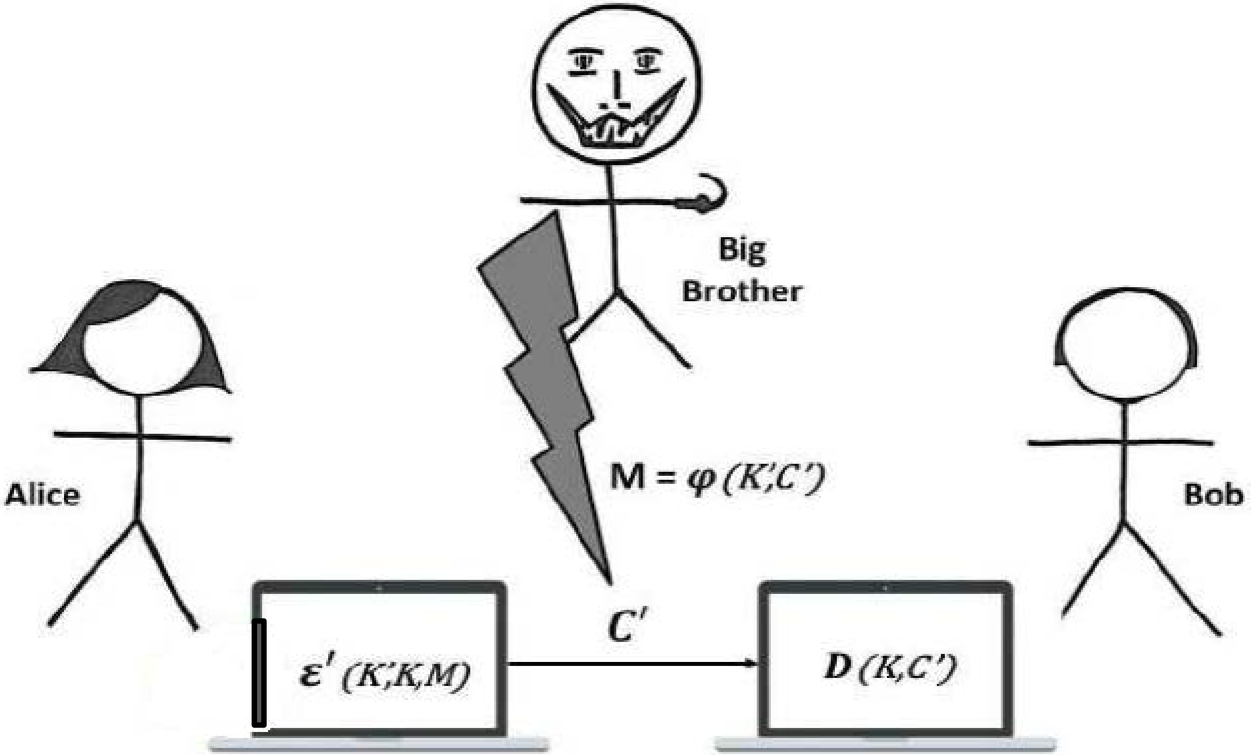
ASA Overview

No Algorithm Substitution

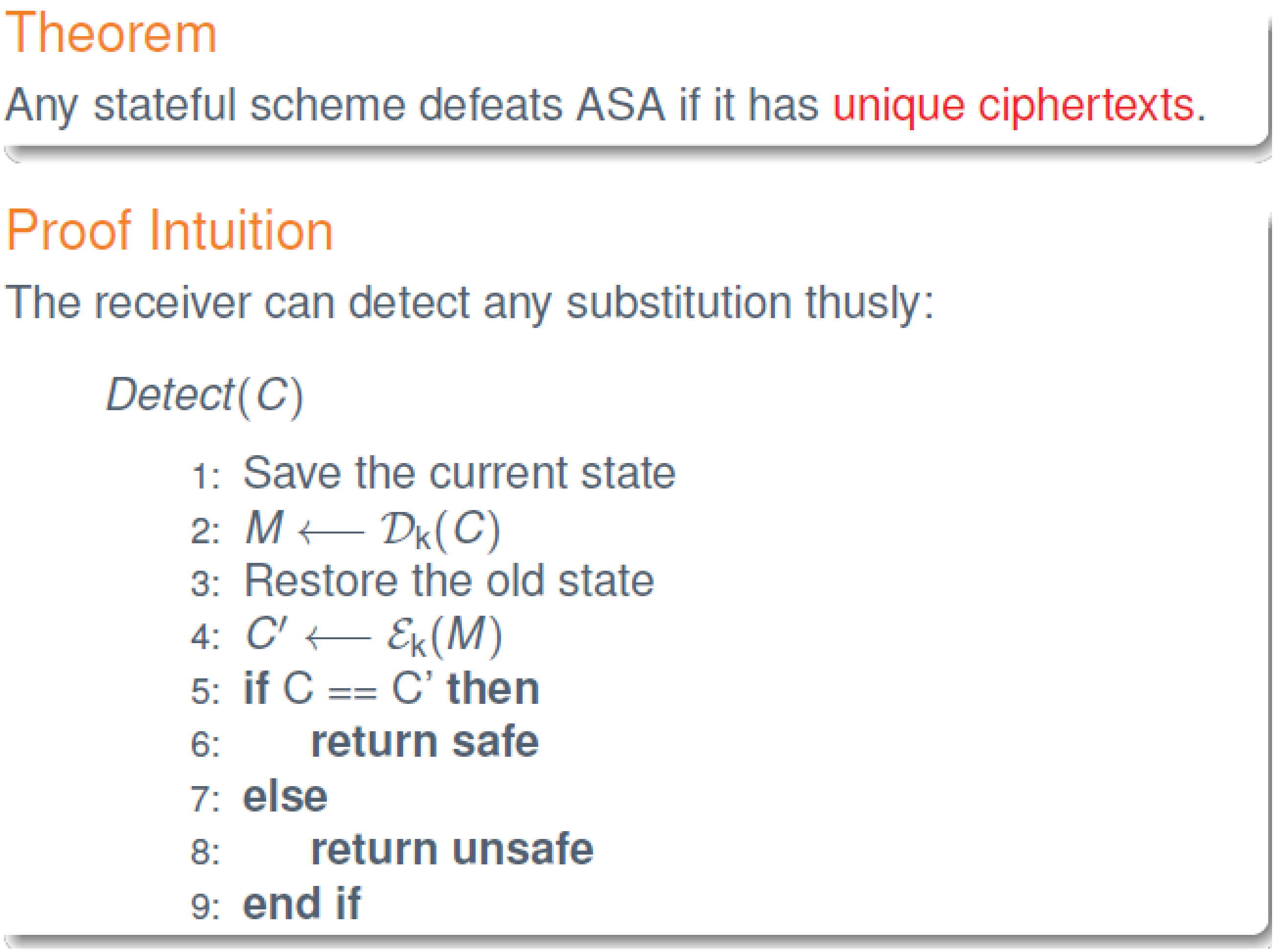


ASA Overview

Algorithm Substitution



Defeating ASA



Theorem

Any stateful scheme defeats ASA if it has unique ciphertexts.

Proof Intuition

The receiver can detect any substitution thusly:

Detect(C)

```
Save the current state
$M \longleftarrow \mathcal{D}_{\mathsf{k}}(C)$
Restore the old state
$C' \longleftarrow \mathcal{E}_{\mathsf{k}}(M)$
if C == C' then
    return safe
else
    return unsafe
end if
```

Conclusion

- GP secure channel protocols are widely used
- we have presented security results – positive and negative- on two Global Platform SCP
- Bad news
  - SCP 02 is vulnerable to a simple plaintext recovery attack
- Good news
  - SCP 03 provides strong security guarantees: resistance to replay, out-of-order delivery and algorithm substitution attacks
  - our proof guarantees that SCP03 cannot undetectably contain hidden backdoors allowing mass surveillance
  - This is, to the best of our knowledge, the first formal security analysis on SCP03
  - creation of the GP ‘Crypto Sub-Task Force’

We advocate the deprecation of SCP02 as soon as possible and the switch over to SCP03

Questions?

orange™