Secure Communication using Authenticated Channels

Sylvain Pasini

PhD Public Defense

October 2nd, 2009

ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

LABORATOIRE DE SECURITE
ET DE CRYPTOGRAPHIE

Outline of the presentation

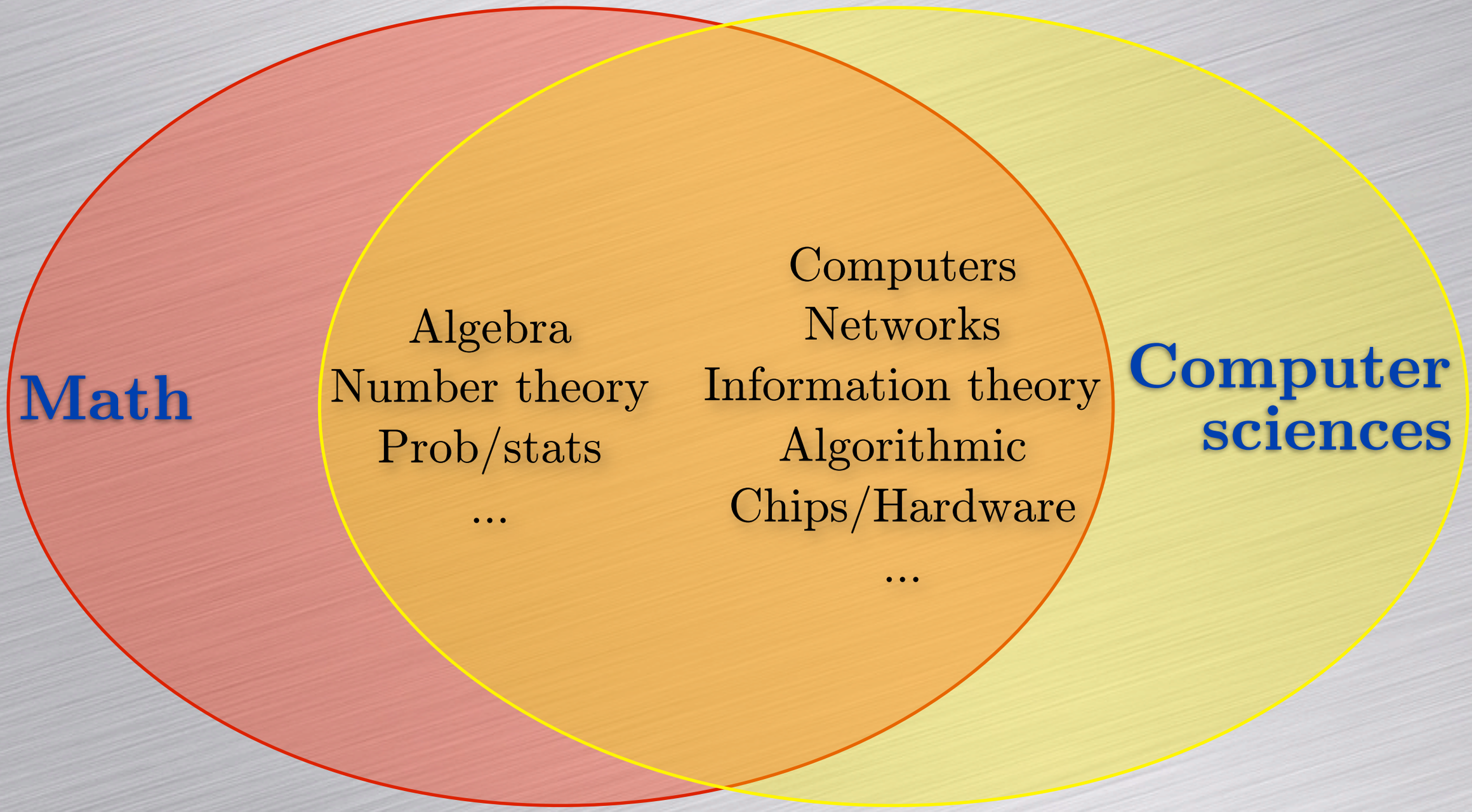
- Cryptography...
- Motivation
  - How to setup a secure communication?
  - How to authenticate a message?
- SAS-based cryptography
- Privacy protection (ePassports)
- Practical attacks against keyboards

Cryptography

Kryptos: “hidden secret”

Grapho: “I write”

Cryptography uses ...



Cryptography may ensures ...

- Confidentiality
- Authenticity
- Integrity

- and also privacy protection, anti-clonage, anti-piracy, ...

Cryptography is everywhere

- Data encryption
  - From Jules Cesar to the Internet...

- Data authentification
  - Software updates, website's public key, ...

- Rights management
  - Video, music, ...

Cryptography is everywhere (2)

- Access control
  - Building, car, garage, ...

- Wireless networks
  - Wifi, Bluetooth, ...

- Mobile phones
  - Encryption, authentication, ...

Cryptography is everywhere (3)

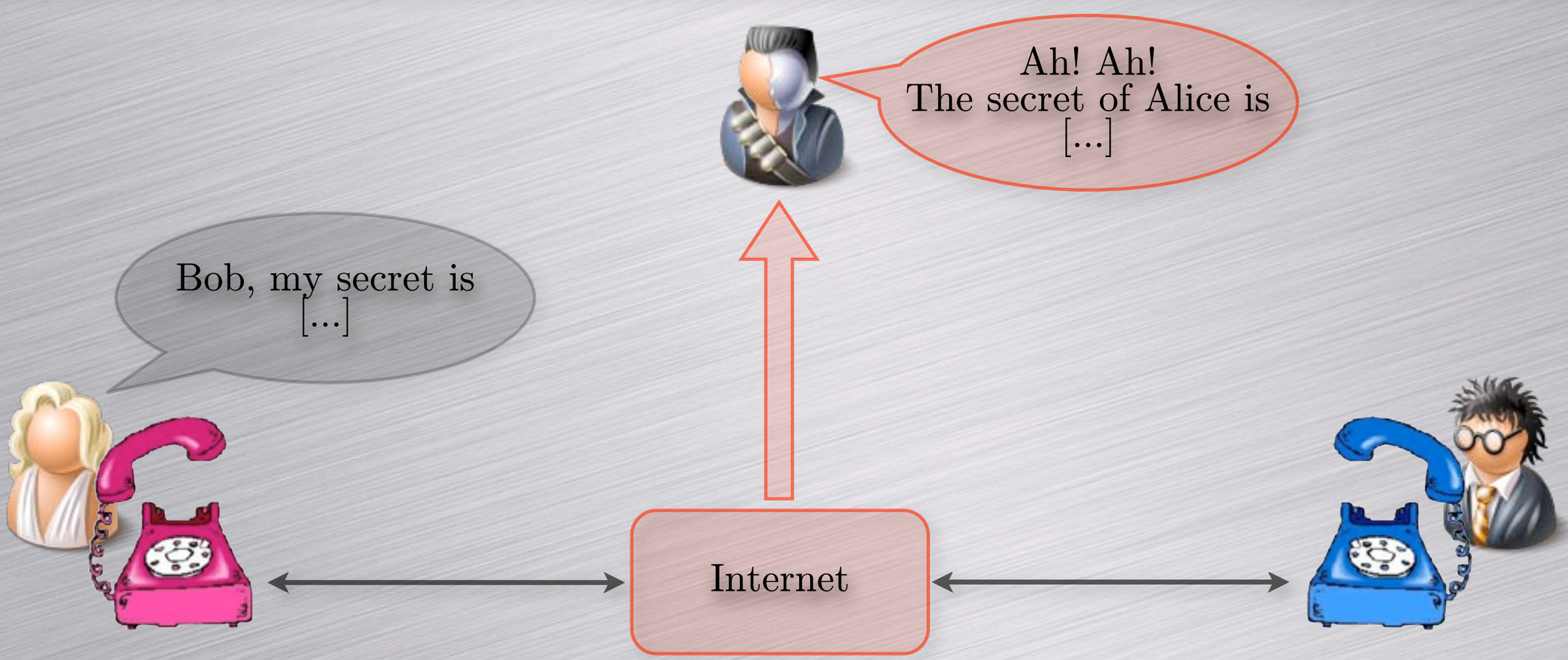
- Pay TV
  - Conditional access, ...

- e-Passeports
  - Data access control, privacy, ...

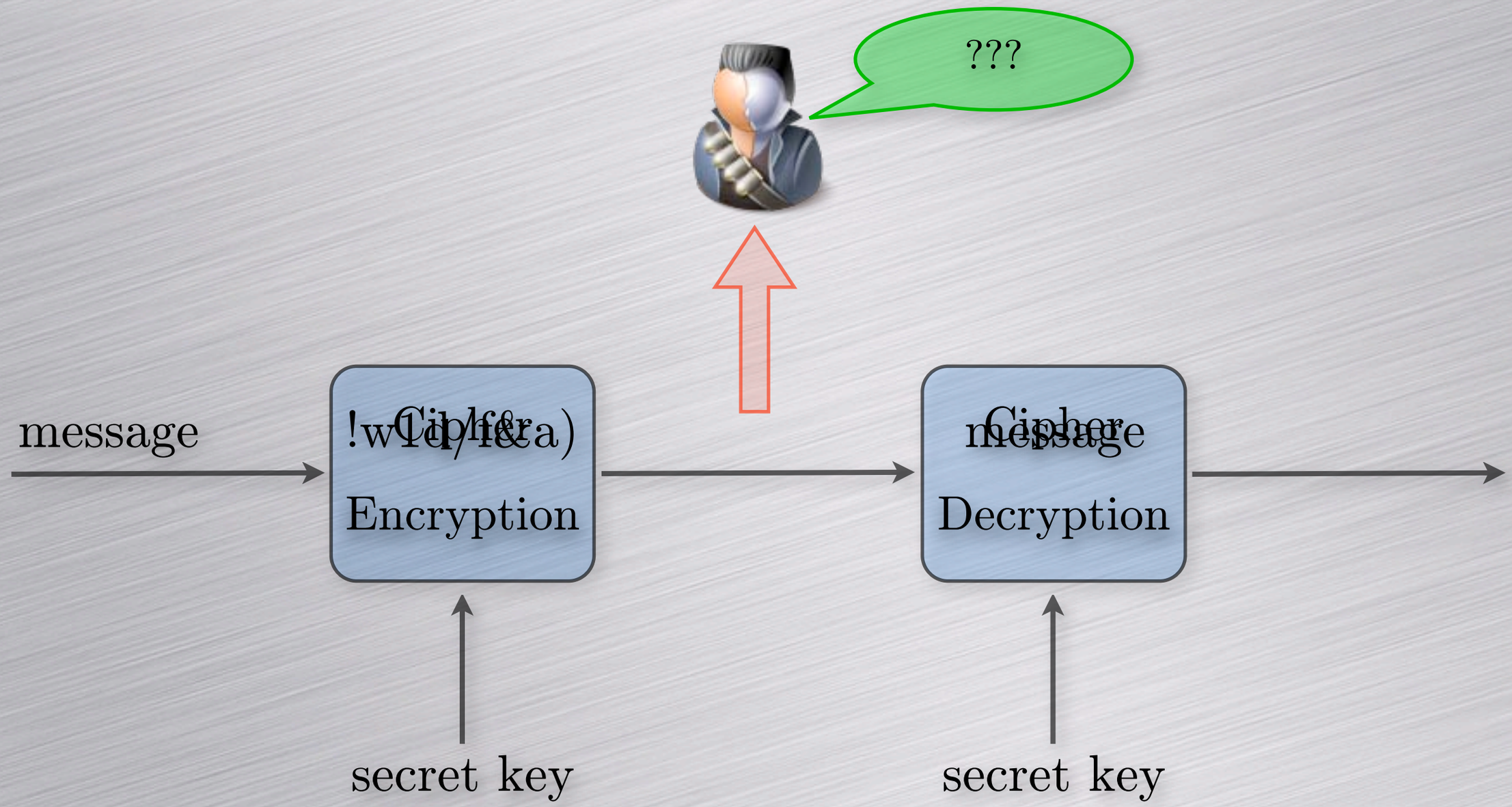
- And many others...

How to establish a secure communication?

Scenario: phone over IP

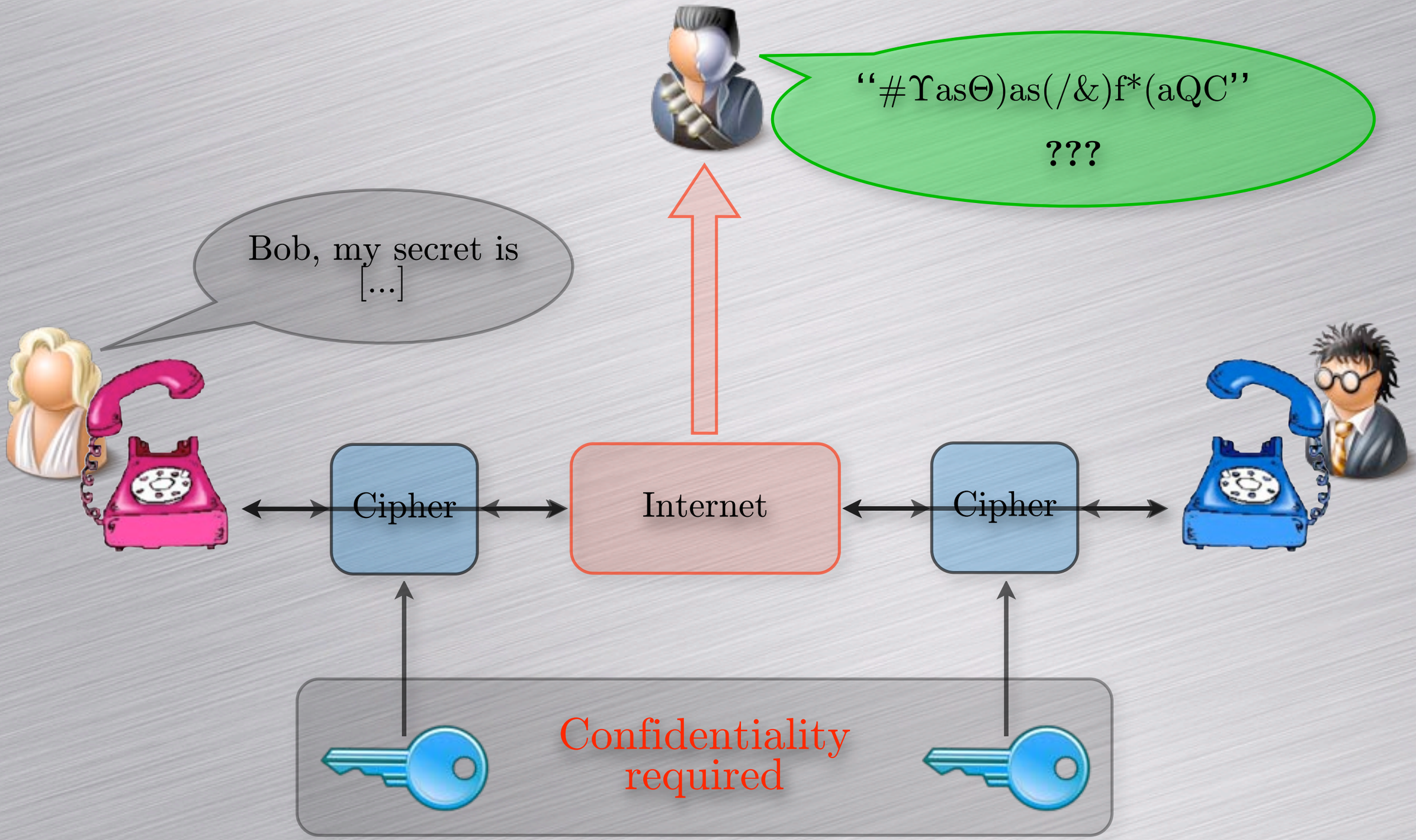


Symmetric cryptography



Examples: DES, AES, IDEA, FOX, RC4, A5/1, ...

Scenario: secure phone over IP



Secret key exchange in reality

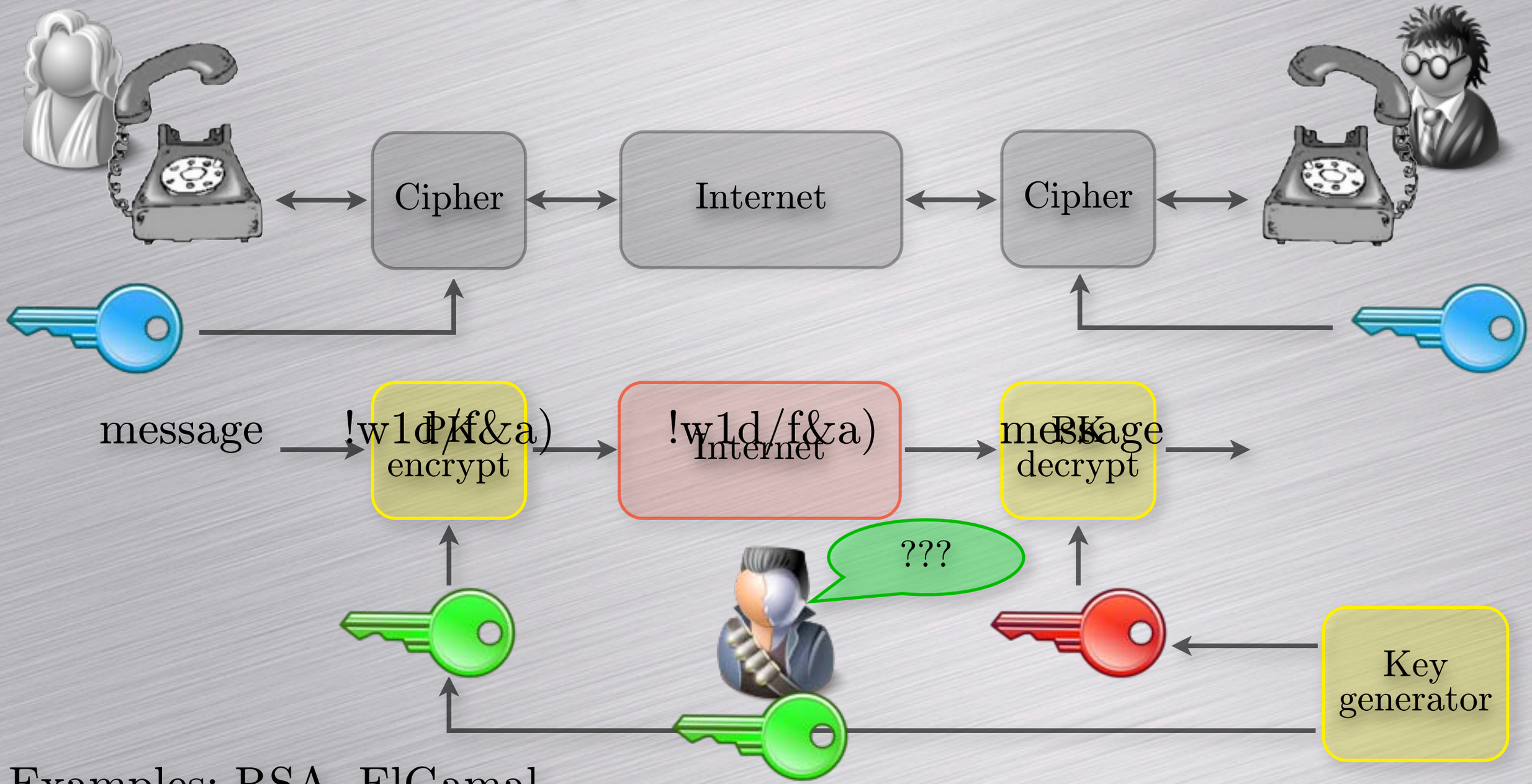
	Encounter	Telephone	Voice mail	E-mail
Confidentiality	☺			
Authenticity	☺	☺	☺	
Low cost		☺	☺	☺
Availability			☺	☺
Speed rate				☺

Confidential channel: expensive and bad availablility.

Can we avoid confidentiality and only use authentication?

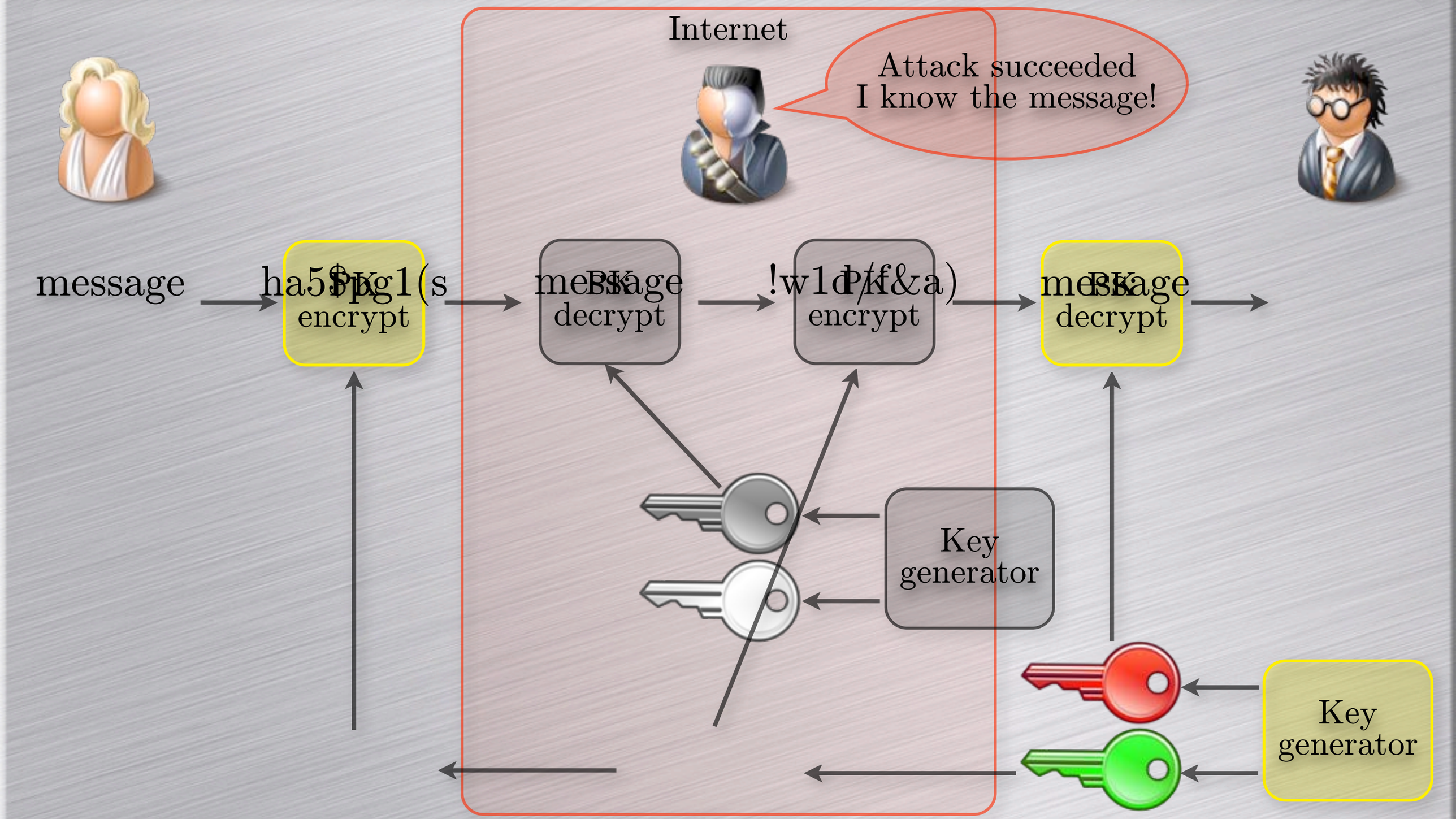
Public-key cryptography

Semi-authenticated key transfer:



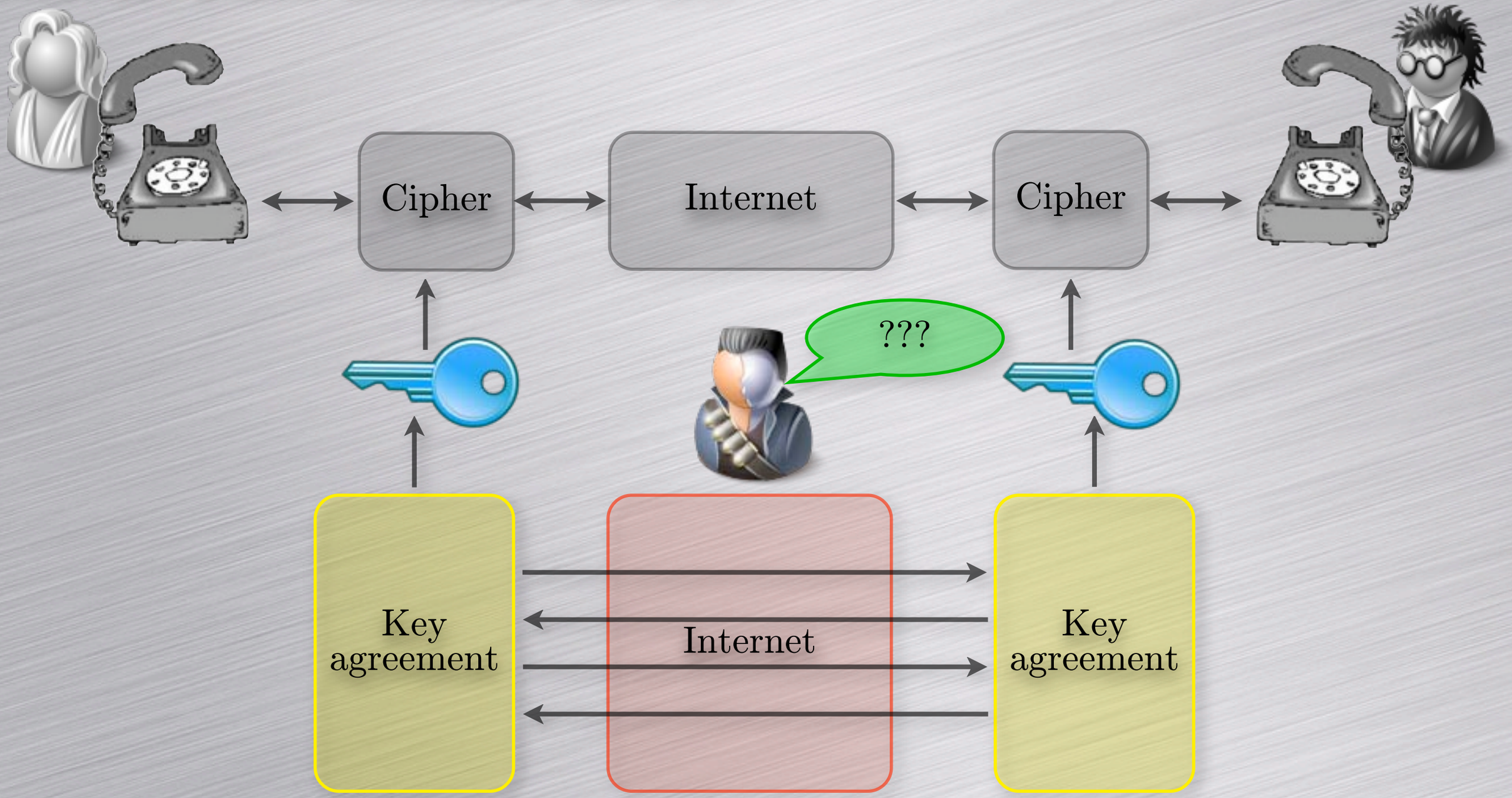
Examples: RSA, ElGamal, ...

Man-in-the-middle attack



Key Agreement

Merkle-Diffie-Hellman model:



In a nutshell

- Goal:
  - Alice and Bob want to communicate securely
- Hypothesis:
  - no prior exchanged data (no PSK, no PKI)
- A secure channel can be setup
- A secret

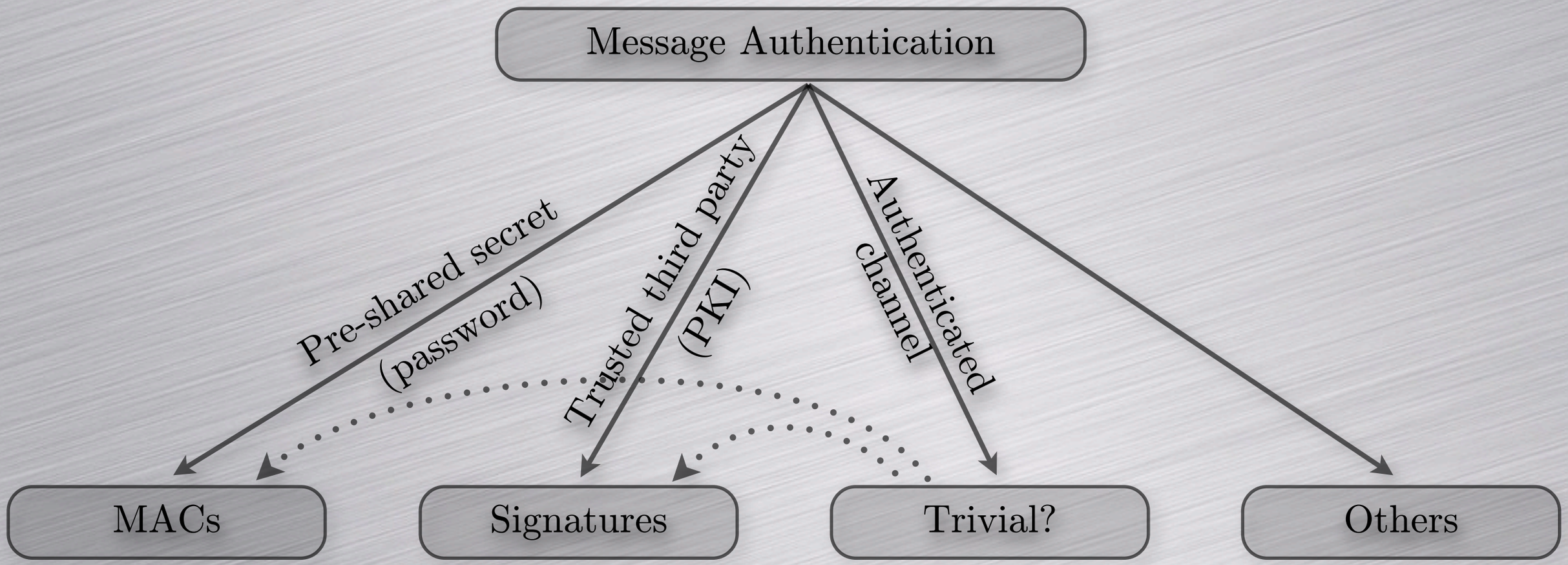
Claim

As long as parties are able to **authenticate** data,
they are able to setup a secure communication.

ed key agreement

How to authenticate messages?

Authentication Overview



Authenticated Channel

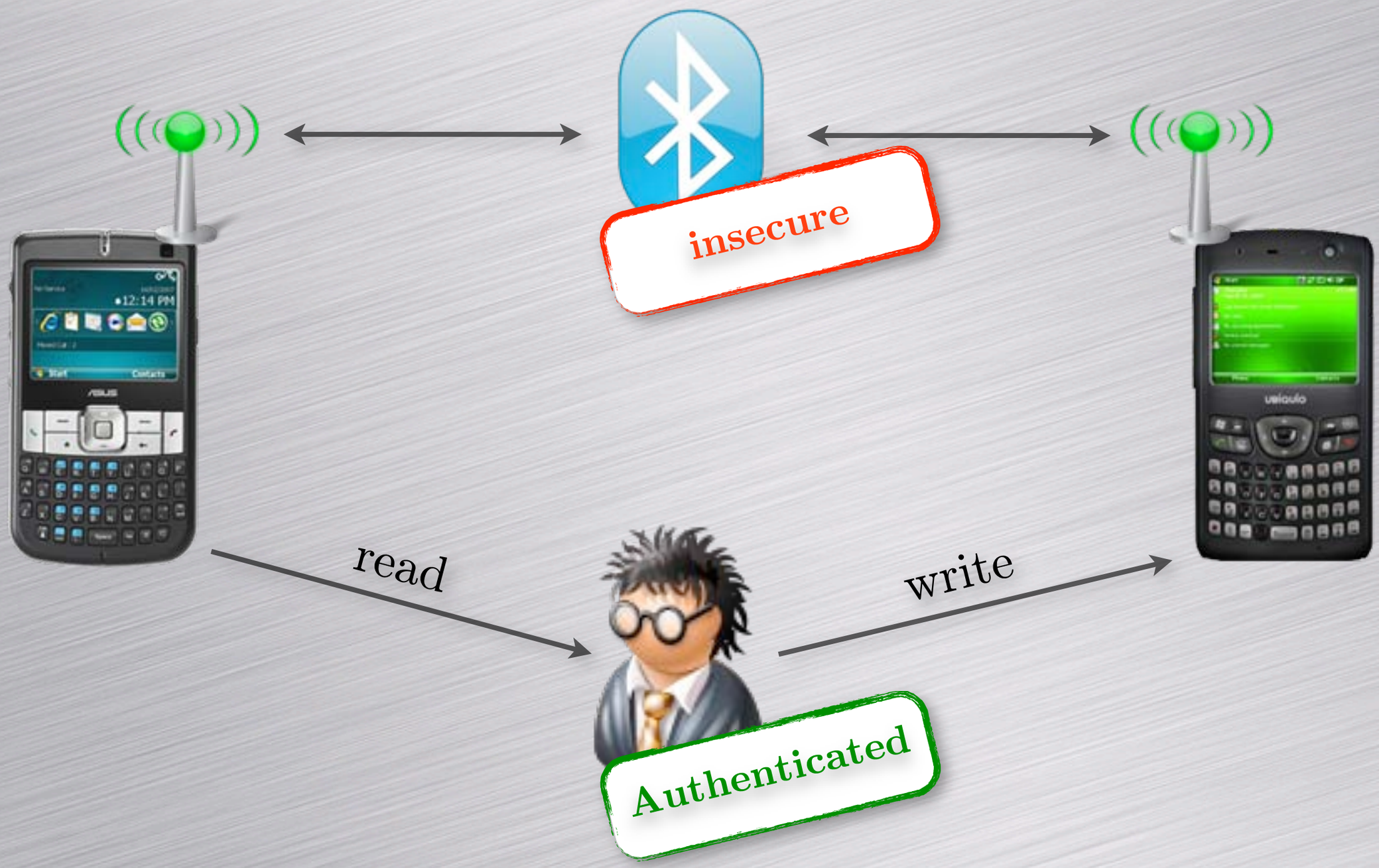
Internet

insecure

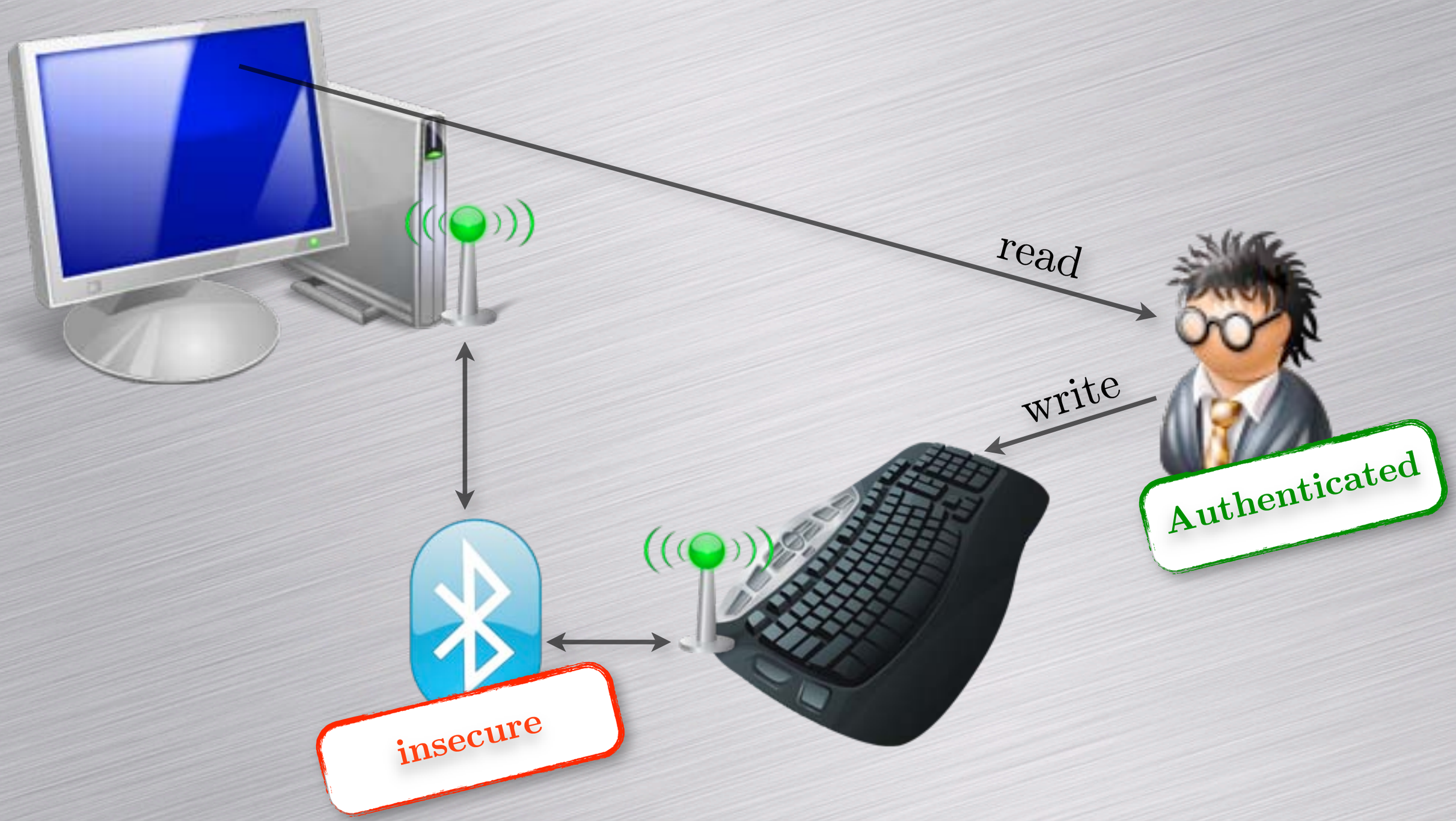
Telephone network

Authenticated

Authenticated Channel (2)

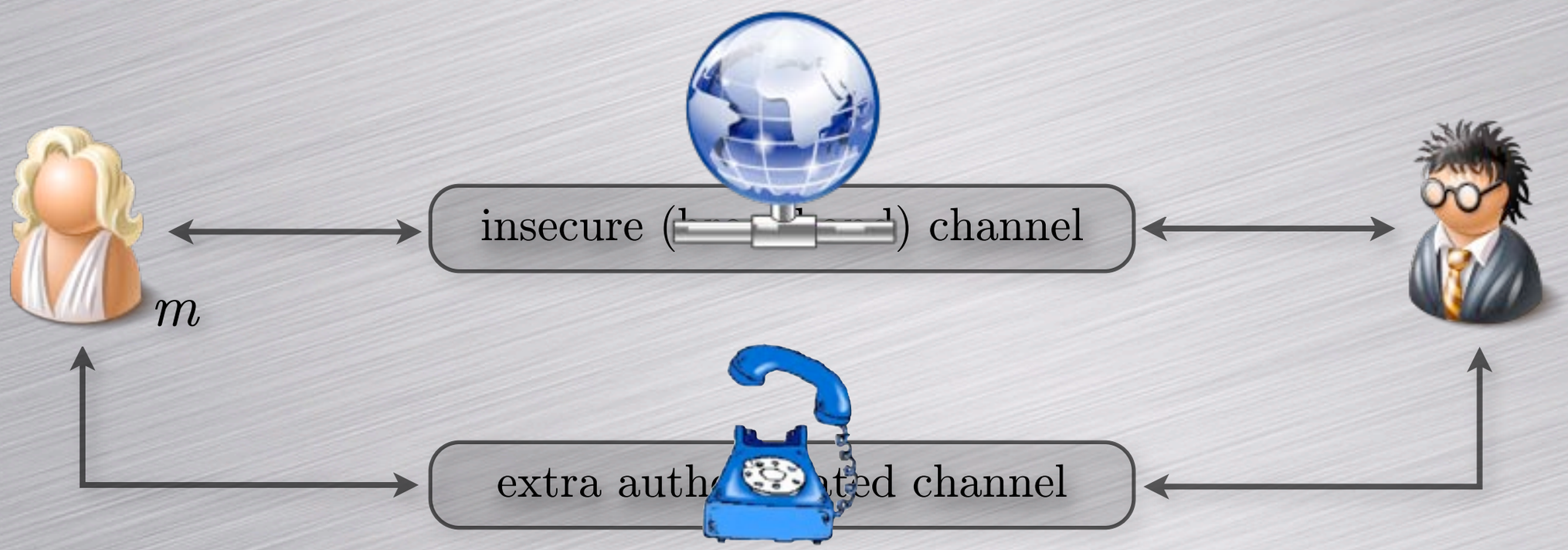


Authenticated Channel (3)



Trivial solution

Goal: authenticate the message m.



User-friendly...

Example of an RSA 1024-bit key:

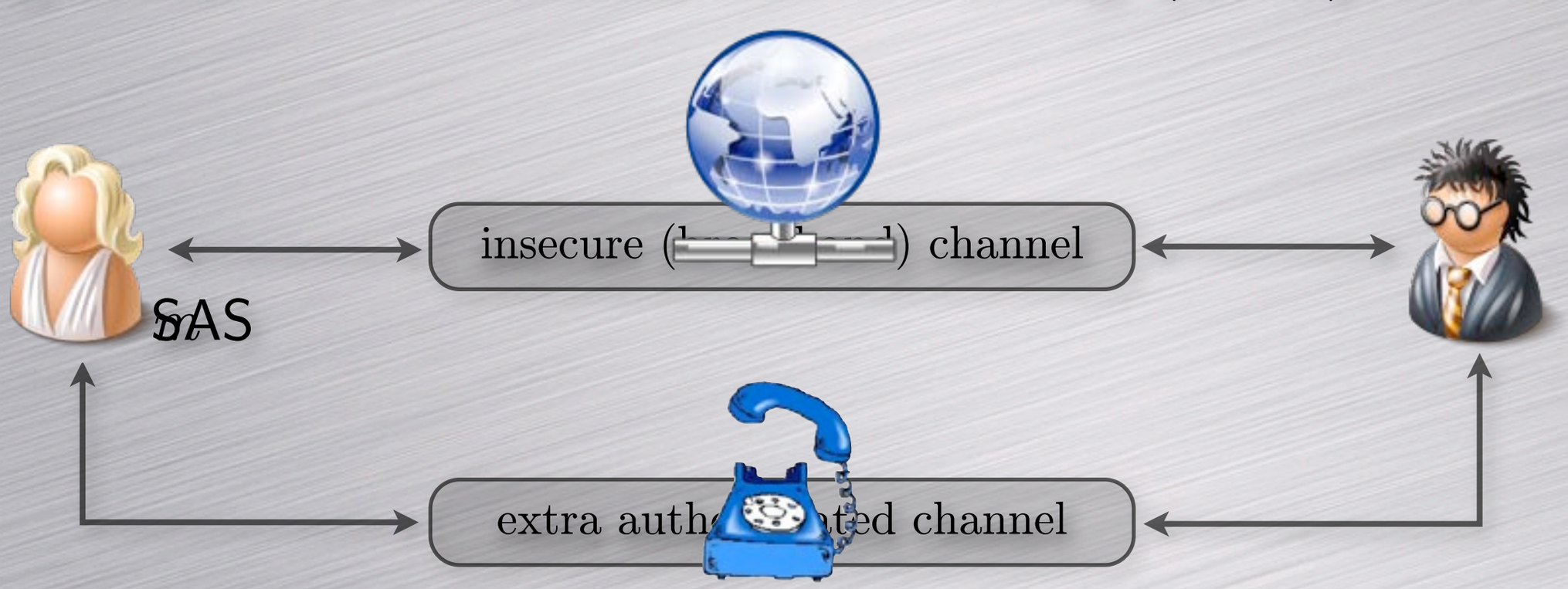
```
ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEApZTXilQgosFxe
vR9ewub/qE1/BoHXCkpzWwopTHkiY2e8pMxMXOc/
DzKV0qgsdC3X9pQODRy+awoANAgttPX
h6JM4ZlYgaEN6azJSyrK0SlOLDn
+YmjjhaKEn1ufLbroQ6Cpg0lj3lXvHEN52P32IfhY08ivC
0pBmO4Y eyErBiE=
```

By telephone... good luck!

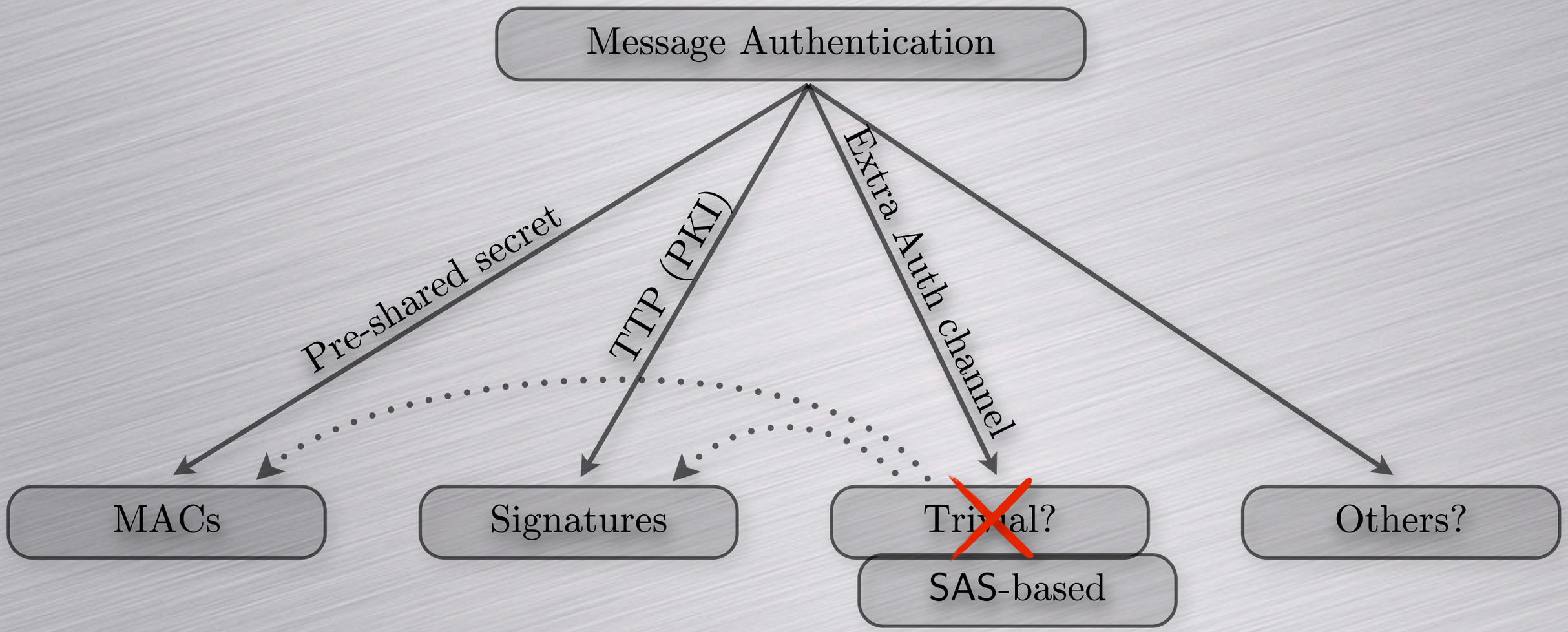
In practice...

Goal: authenticate the message m.

Using a Short Authenticated String (SAS):

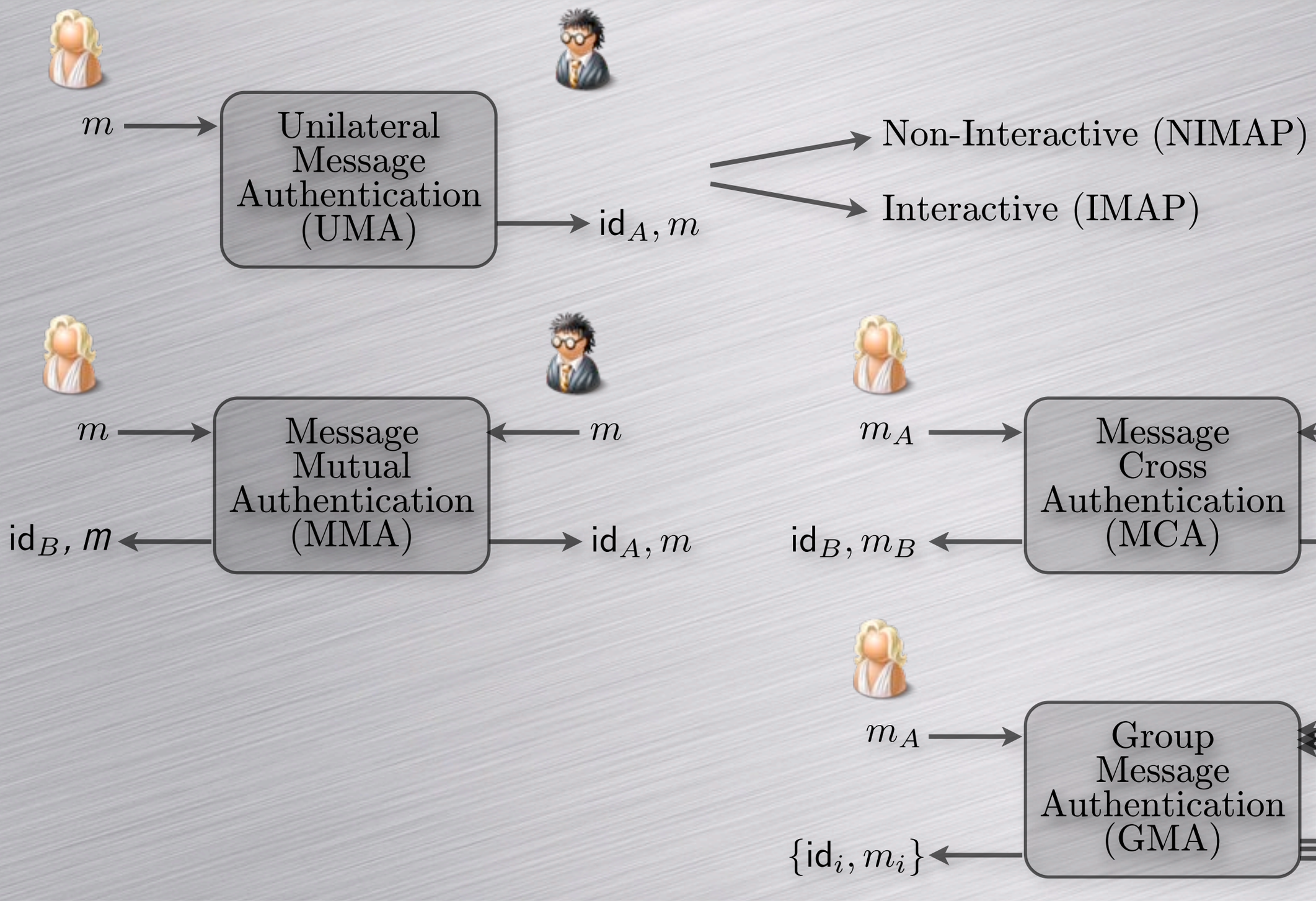


Authentication Overview



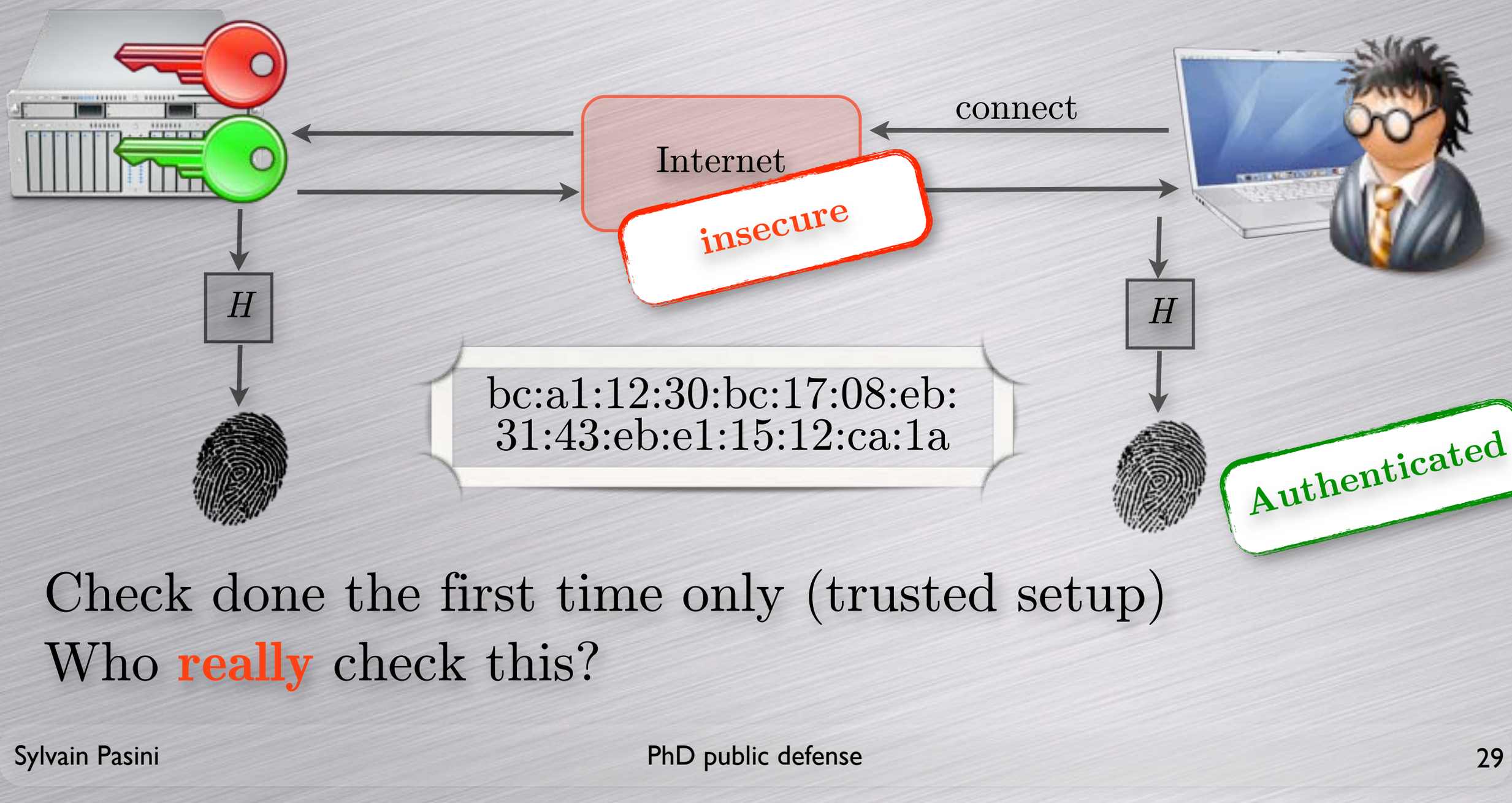
SAS-based Cryptography

Message Authentication



Example: Secure Shell (SSH)

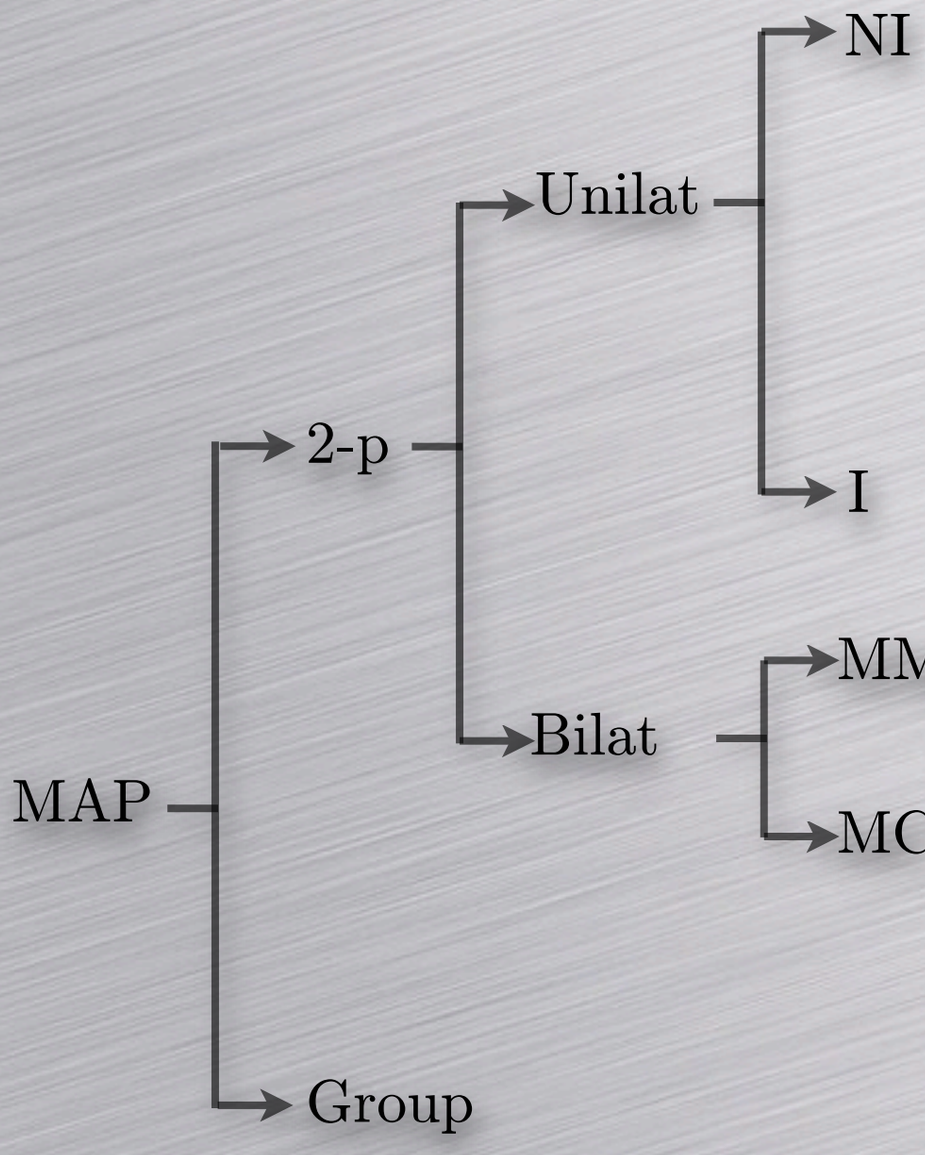
Goal: authenticate the server's public key.



Check done the first time only (trusted setup)

Who **really** check this?

Overview of Proposed Protocols



	Auth channel	Optimal	Sec proof
CRHF-based [BSSW02]	weak		y
MANA I [GMN04]	strong		y
PV-NIMAP[PV06a]	weak	y	y
eTCR-based [RWSN07]	weak	y	y
HCR-based [MS07]	weak	?	y
Vau-SAS-IMAP [Vau05]	weak	y	y
ICR-based [MS08]	weak	?	y
MANA III [GMN04]	strong		y
PV-SAS-MMA [PV06b]	weak	y	y
Vau-SAS-MCA [Vau05]	weak		
PV-SAS-MCA [PV06b]	weak	y	y
PV-SAS-AKA [PV06b]			
MANA IV [LN06]	weak	y	y
Group-MANA IV [VAN06]	weak		y
LP-SAS-GMA [LP08]	weak	y	y
LP-SAS-GKA [LP08]			

Bilateral Protocol [PV-SAS-MCA]

[PV-SAS-AKA]

pick x_A
$m_A = g^{x_A}$

~~Input: m_A~~

~~Input: m_B~~

pick x_B
$m_B = g^{x_B}$

pick $R_A \in \{0,1\}^\ell$

pick $R_B \in \{0,1\}^k$

$(c, d) = \mathsf{commit}(m_A, R_A)$

$m_A, c \rightarrow$

$\leftarrow m_B, R_B$

$d \rightarrow$

$\widehat{R}_A = \mathsf{open}(\widehat{m}_A, \widehat{c}, \widehat{d})$

$\mathsf{SAS} = \widehat{R}_B \oplus h(\widehat{m}_B, R_A)$

$\mathsf{SAS} \rightarrow$

check $\mathsf{SAS} \stackrel{?}{=} R_B \oplus h(m_B, \widehat{R}_A)$

$\leftarrow \mathsf{SAS}$

check SAS are the same

$\mathsf{sk}_A = \widehat{m}_B^{x_A}$

$\mathsf{sk}_B = \widehat{m}_A^{x_B}$

- Interactivity allows to avoid offline attacks.
- As a consequence, SAS are shorter (5 digits).

User Task...

Public key

ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEApZTXilQgosFxe
vR9ewub/qE1/BoHXCkpzWwopTHkiY2e8pMxMXOc/
DzKV0qgsdC3X9pQODRy+awoANAgttPX
h6JM4ZlYgaEN6azJSyrK0SlOLDn
+YmjjhaKEn1ufLbroQ6Cpg0lj3lXvHEN52P32IfhY08ivC
0pBmO4Y eyErBiE=

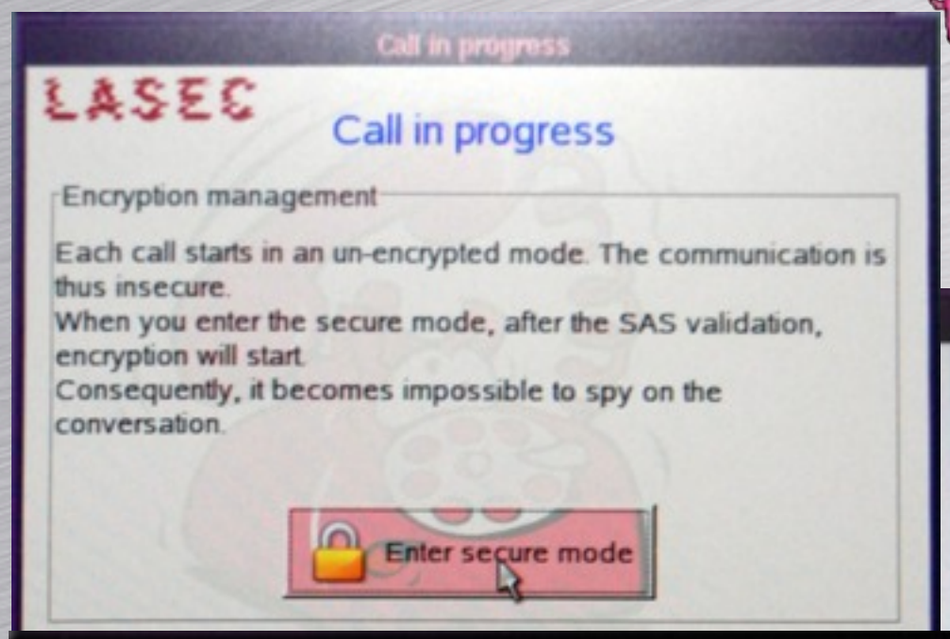
In SSH

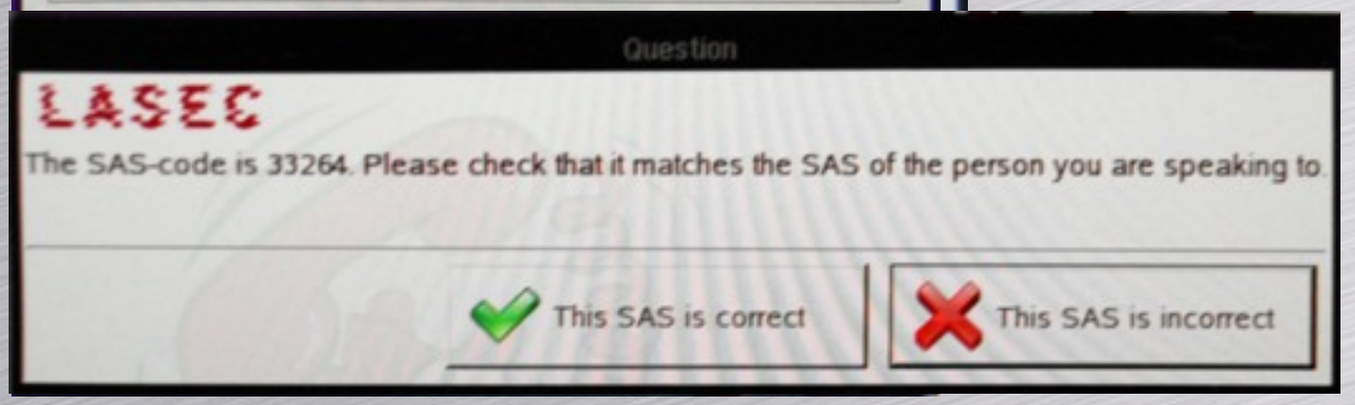
bc:a1:12:30:bc:17:08:eb:
31:43:eb:e1:15:12:ca:1a

SAS-based

45781

SAS-based phone over IP

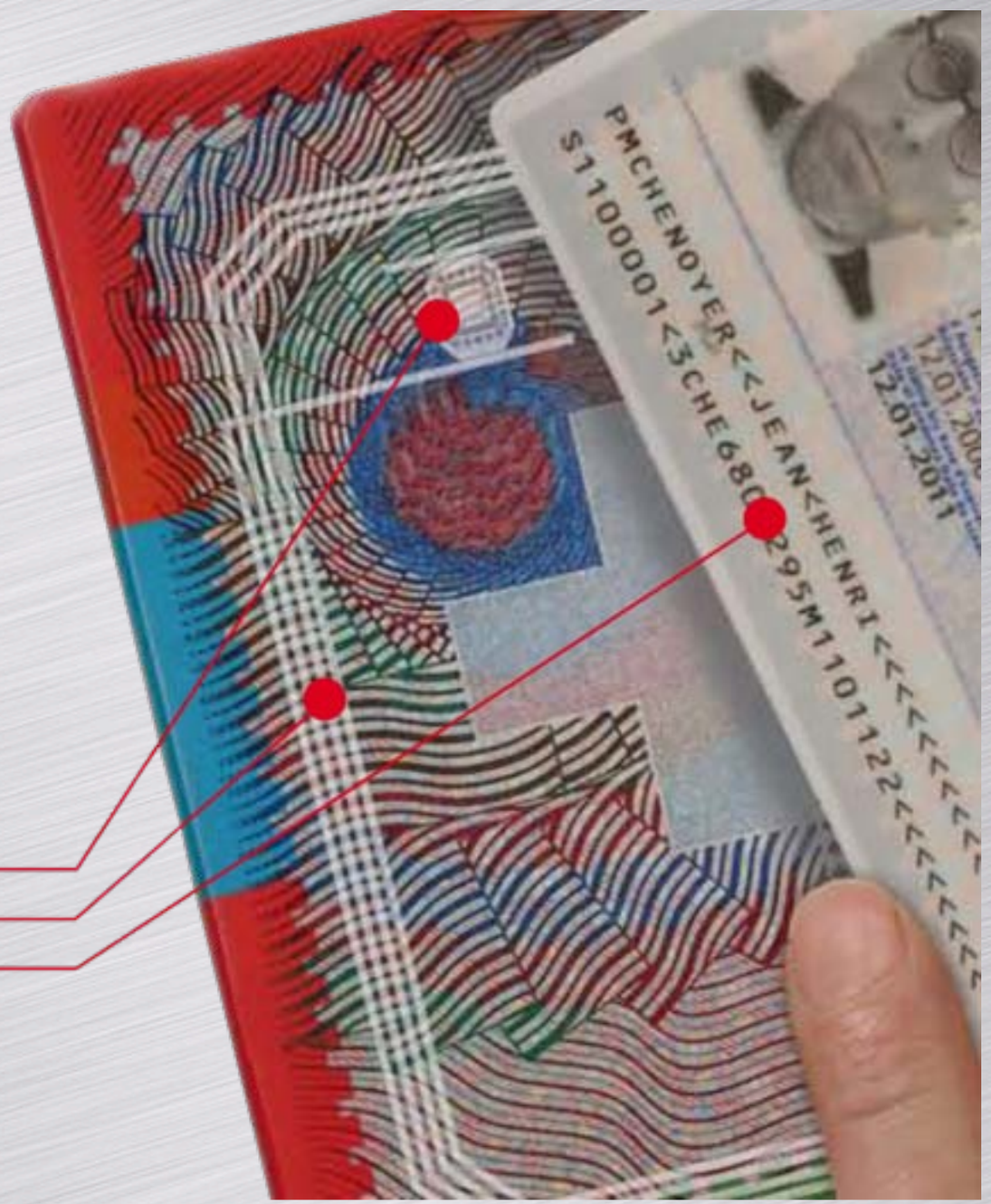




Efficient Deniable Authentication for Signatures

Application to Electronic Passport

An Electronic Passport



Reading an E-passport

- Usually Basic Access Control (BAC) is used
  - Prove to the e-passport that you have visual access
  - Use an encryption key *sk=f(MRZ)*

MRZ
(Machine Readable Zone)

Radio channel

Visual channel

Reader

cost 50$

Data Accessible from the Chip

- Basic information (name, birthdate, MRZ, ...)
- Facial picture (JPEG)
- Optional :
  - Fingerprint(s)
  - Eye(s)
  - Signature
  - Personal details
  - ...
- Security Object Document (SOD)

Issue / Proposed solution

data
SOD

Passport creation

data
~~SOD~~

data, ~~SOD~~

~~data~~ is valid

Privacy issue

non-tranferable interactive proof "I know a valid SOD"

Example (RSA-based signature)

Reader

RSA : p, q, N, e, d
$K_p = (N, e)$
$K_s = d$

K_p $\longrightarrow$ K_p $\longrightarrow$

$\sigma_p = \mathsf{H}_{\mathsf{seed}}(m)$
$\sigma_s = \sigma_p^d \bmod N$

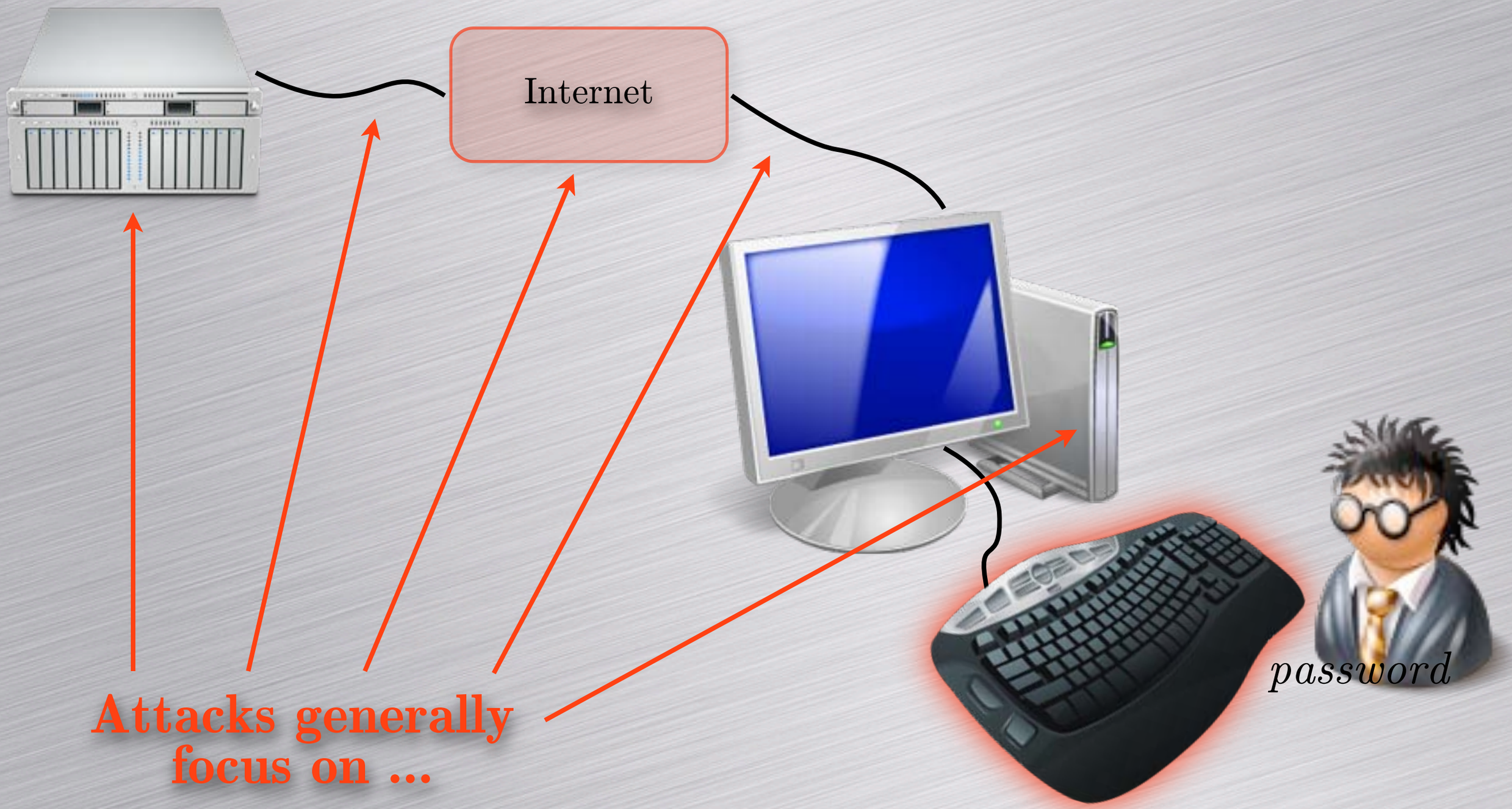
m, σ_p, σ_s $\longrightarrow$ m $\longrightarrow$

$Y = y^e \bmod N$ — commit(crs, r)
$r = \mathsf{open}(\mathsf{crs}, c, d)$ — $\mathsf{V}(\sigma_p, m) \stackrel{?}{=} 1$
$z = y\sigma_s^r \bmod N$ — check $z^e \stackrel{?}{=} Y\sigma_p^r \bmod N$

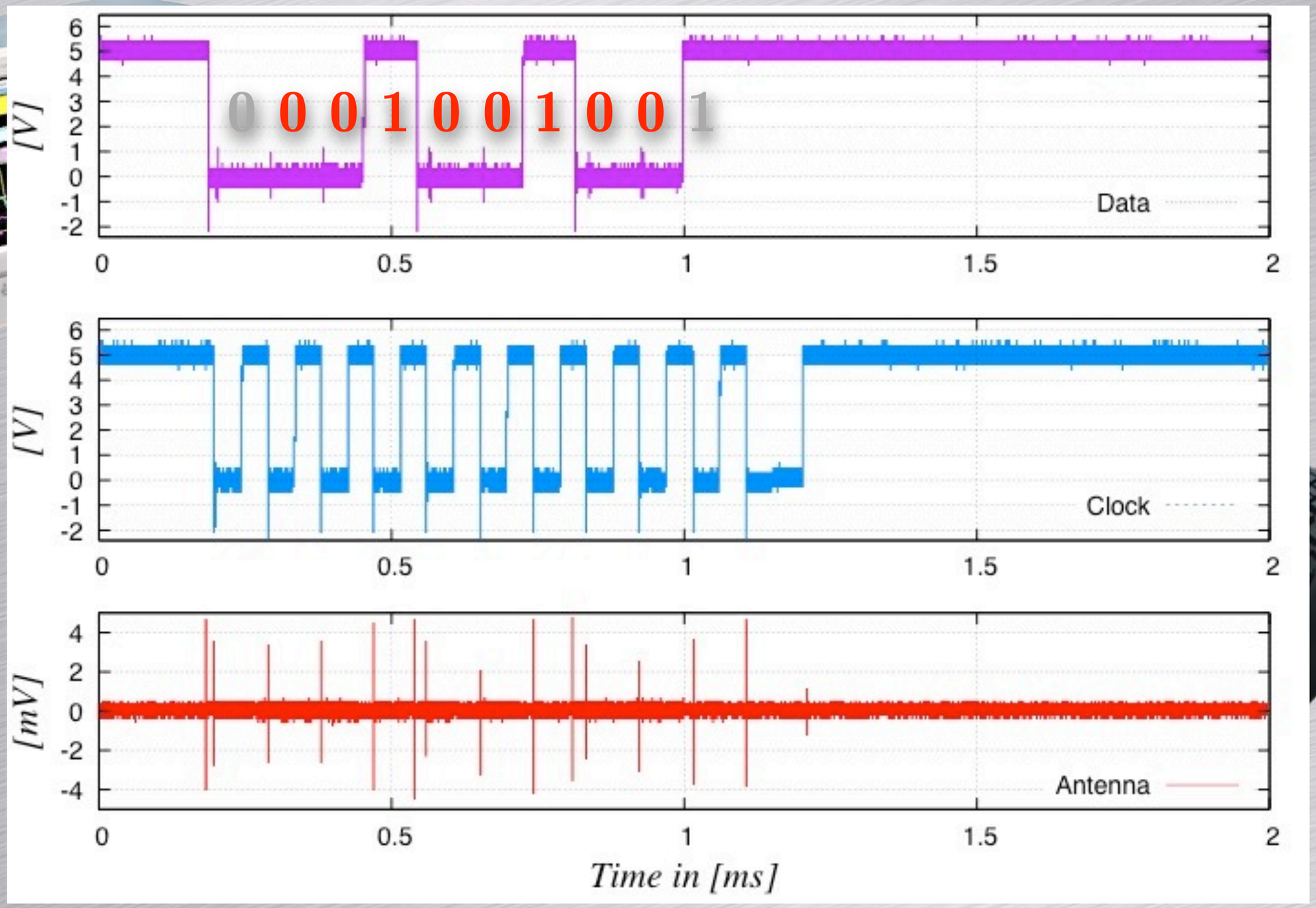
Passport proves to Reader:
I know the signature

Practical Attacks against Keyboards

The Transit of a Password

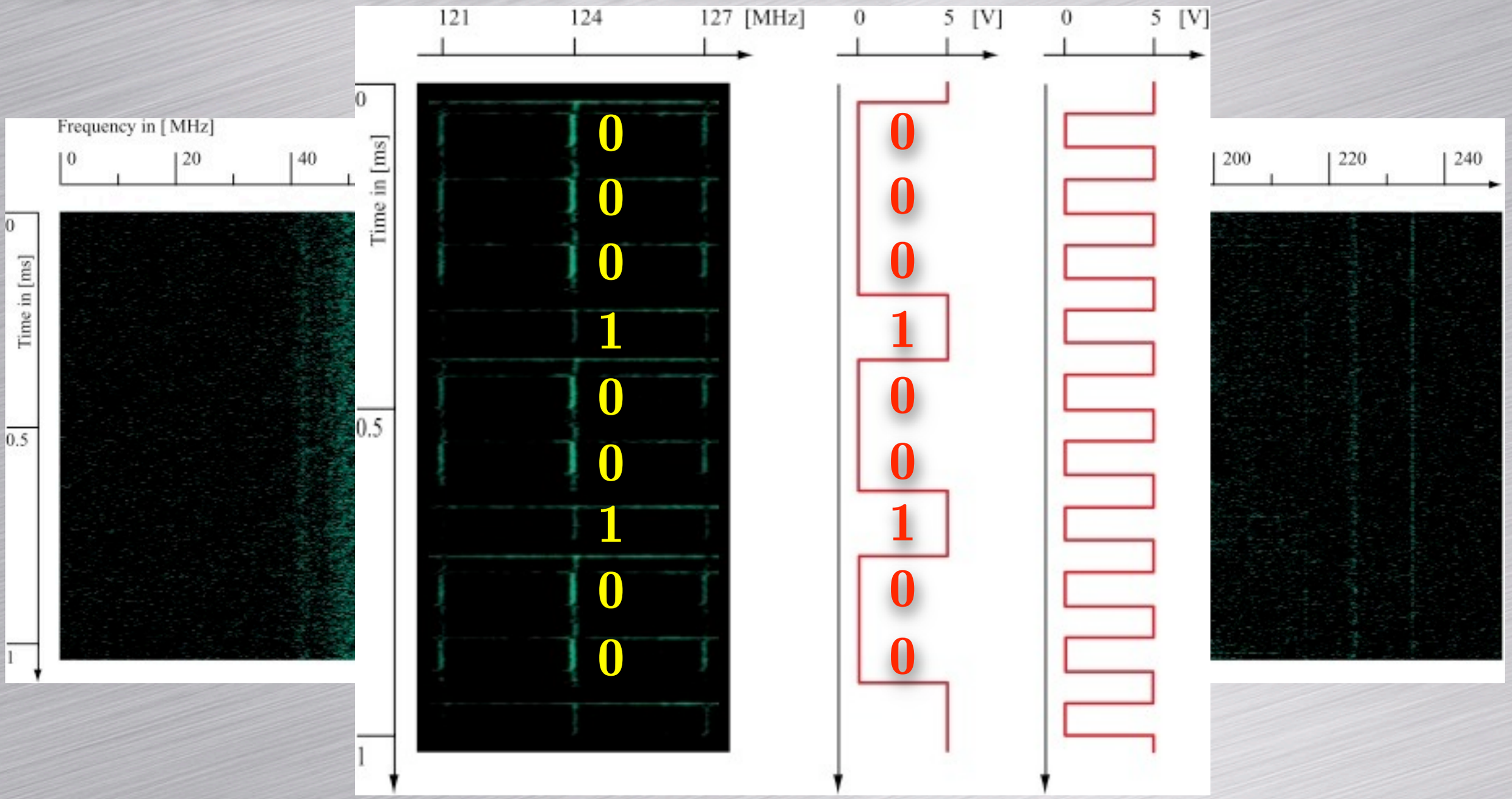


Experimental Setup



Full Spectrum

Short Time Fourier Transform



Conclusion

Contributions

- SAS-based cryptography:
  - dedicated network and adversarial model
  - generic security analysis (notion of optimality)
  - optimal NIMAP, MMA, MCA, and GMA protocols
  - optimal AKA and GKA protocols
- Offline Non-Transferable Authentication Protocol
  - solve privacy issue in a three-party setting (e-passport)
- (Hash-and-sign-based signatures)
  - pre-processing strengthening actual implementations
- Practical attacks against Keyboards

Thanks to ...

- My thesis supervisor, Serge
- Our secretary, Martine
- My colleagues (from the LASEC)
- My family and my friends
- My new colleagues (from Nagra)
- All missed ones?

More details written in my thesis...

C'est l'heure

de l'apéro !!!

Thank you for your attention!