# Which security for the Factories of the Future


**Pascal Lafourcade**

Chaire de Confiance Numérique



22 January 2015

# Chaire de Confiance Numérique

Research on Digital Trust of information and communication systems

- Supported by almerys and la Caisse d'Epargne d'Auvergne et du Limousin via la Fondation de l'Université d'Auvergne.
- Financially supported by la Région Auvergne

## Seminar

Free and open each month
1st Thuresday IUT Amphi B

`http://confiance-numerique.clermont-universite.fr/`

`http://webtv.u-clermont1.fr/`

# LIMOS Team "Réseaux et Protocoles"

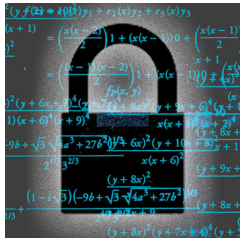
## Topics

Protocol design for Wireless LAN and Wireless Sensor Networks:

- Deterministic and low-power solutions for industrial application monitoring (EDF, AirBus ...)
- Low-power and scalable solutions for environmental applications (ClerVolc, overwater networks)
- Linear sensor networks

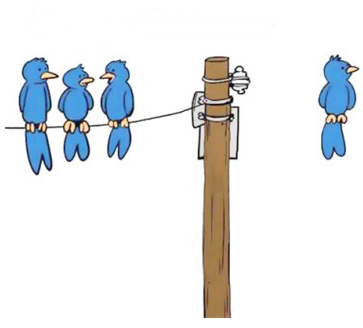
- Specification and evaluation of MAC and Routing protocols
- Simulation and prototyping, simulation toll design, Cross-layering

# My Research Topics



- Verification techniques for **cryptography**
  - Asymmetric Encryptions
  - Encryption Modes
  - Message Authentication Codes

- **Properties** for cryptographic protocols
  - e-vote, e-auction, e-exam, e-reputation ...



- **Intruder** models and algorithms for WSN
  - Neighbourhood Discovery Protocols
  - Secure Routing Algorithms
  - Key Establishments

# Factory Revolutions

## Yesterday

# Factory Revolutions

## Yesterday

Humans $\Rightarrow$ tasks
with machine

# Factory Revolutions

**Yesterday**

**Today**

Humans $\Rightarrow$ tasks
with machine

# Factory Revolutions

## Yesterday

Humans ⇒ tasks with machine

## Today

Humans control machines ⇒ tasks

# Factory Revolutions

## Yesterday

Humans ⇒ tasks with machine

## Today

Humans control machines ⇒ tasks

## Tomorrow

# Factory Revolutions

## Yesterday

Humans ⇒ tasks with machine

## Today

Humans control machines ⇒ tasks

## Tomorrow

Robots control machines ⇒ tasks

# Factories of the Future

- Robots control machines
- Changing the human's roles
- Designing robots is challenging

## Which kind of robots?

- Autonomous robots
- Smart robots
- Adaptative robots
- Collaborative robots

For sure the robots need to communicate!

# Security Challenges in the Factories of the Future

Data exchanged play a VITAL role !

## Properties

- Data Integrity
- Data Confidentiality
- Data Privacy
- Authentication
- Non-repudiation
- Avaibility
- Realtime constraints

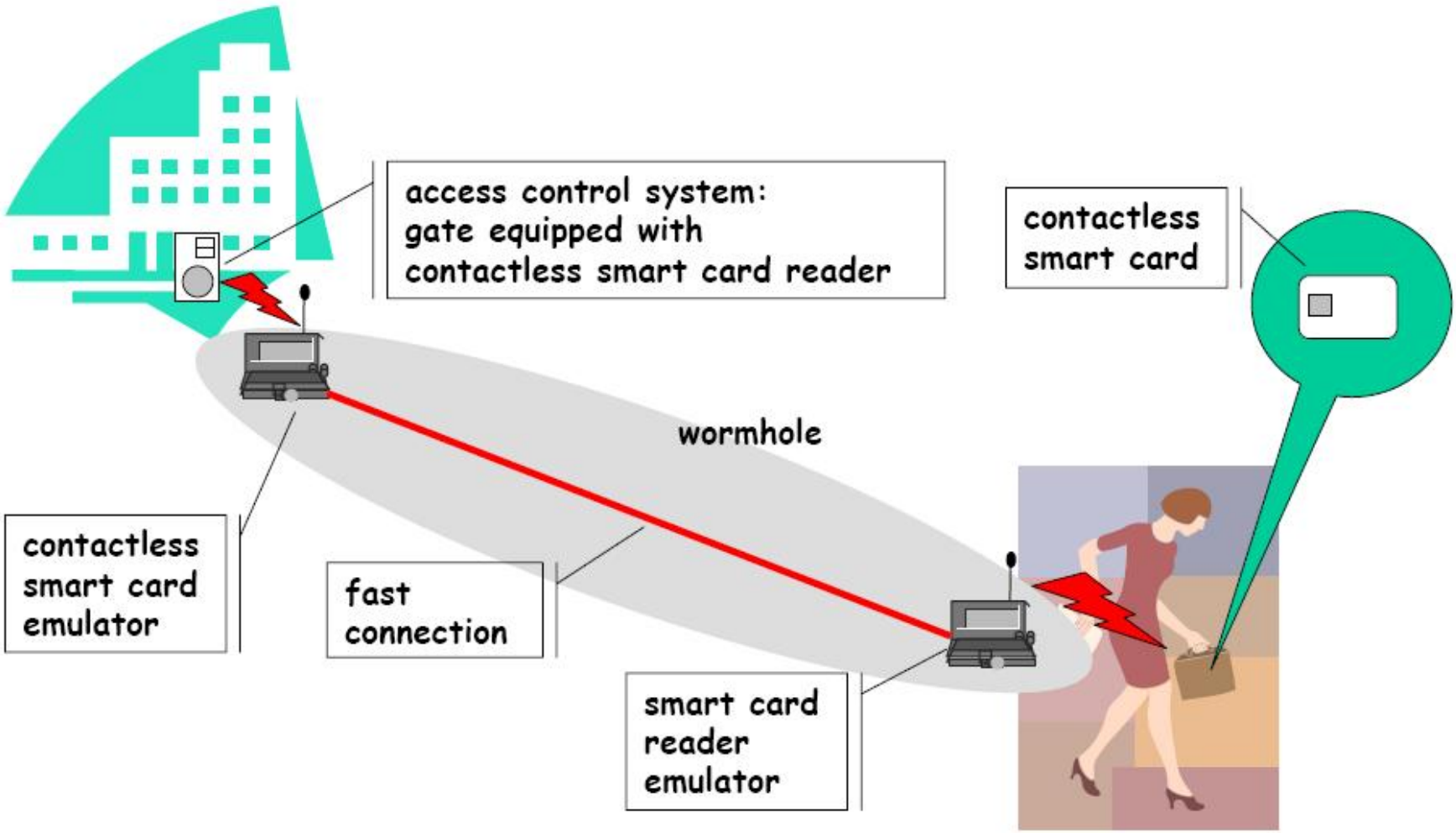

# Several Possible Attackers

- Insider vs Outsider
- Active vs Passive
- Local vs Extended
- Single vs Multiple
- Laptop vs Server



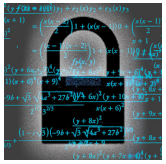



# Wormhole Attack



# What is cryptography based security?

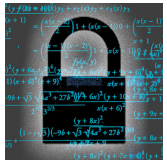
**Cryptography:**



- Primitives: RSA, Elgamal, AES, DES, SHA-3 ...
- Protocols: Distributed Algorithms

# What is cryptography based security?

**Cryptography:**



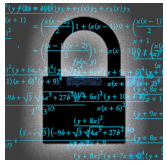
- Primitives: RSA, Elgamal, AES, DES, SHA-3 ...
- Protocols: Distributed Algorithms

**Properties:**


- Secrecy,
- Authentication,
- Privacy
- Non Repudiation ...

# What is cryptography based security?

**Cryptography:**



- Primitives: RSA, Elgamal, AES, DES, SHA-3 ...
- Protocols: Distributed Algorithms

**Properties:**


- Secrecy,
- Authentication,
- Privacy
- Non Repudiation ...

**Intruders:**

- Passive, active
- CPA, CCA ...

# What is cryptography based security?

**Cryptography:**

- Primitives: RSA, Elgamal, AES, DES, SHA-3 ...
- Protocols: Distributed Algorithms

**Properties:**


- Secrecy,
- Authentication,
- Privacy
- Non Repudiation ...

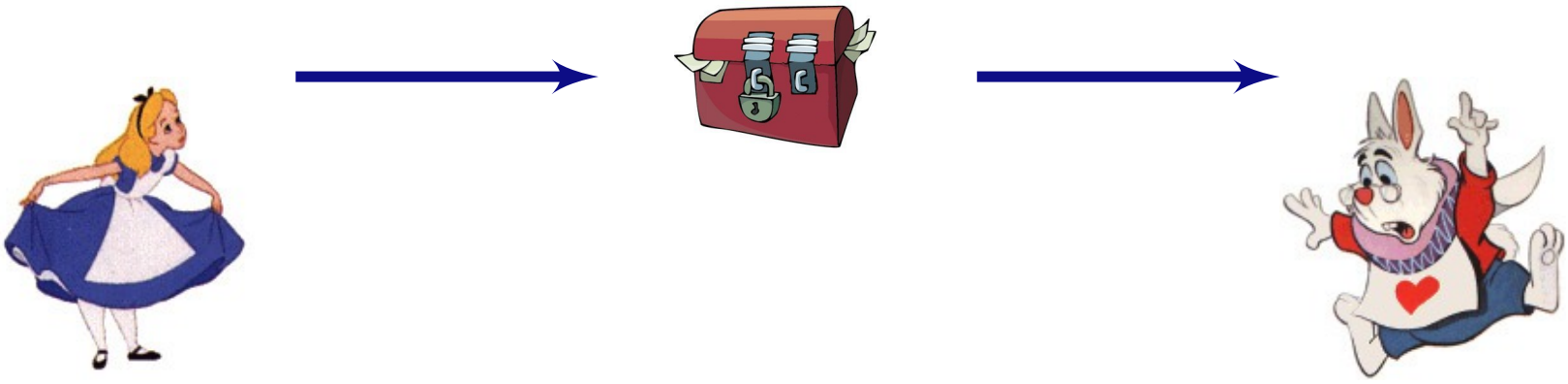
**Intruders:**

- Passive, active
- CPA, CCA ...

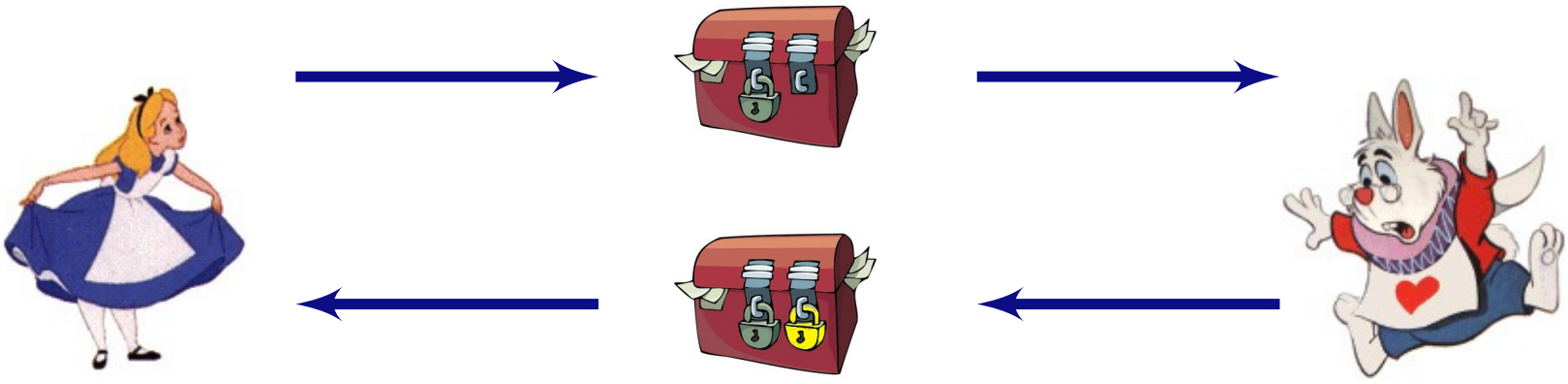
Designing **secure** cryptographic protocols is **difficult**

# 3-pass Shamir

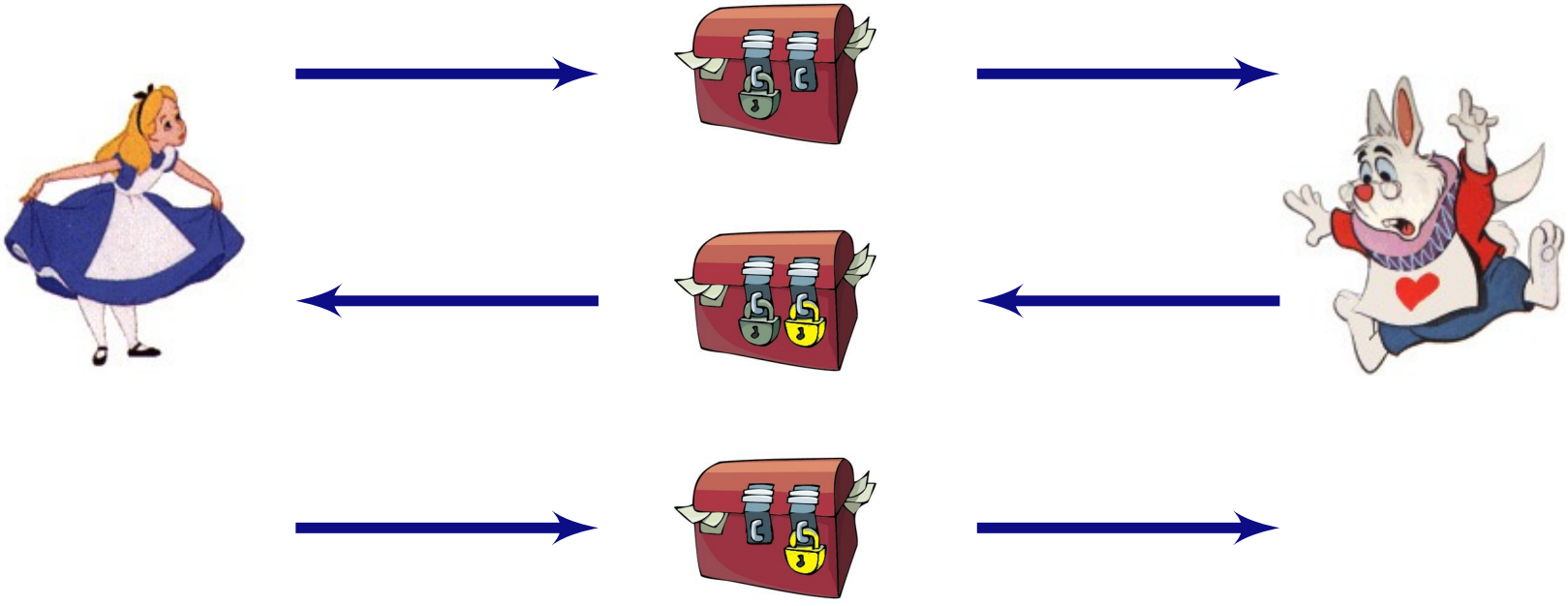
# 3-pass Shamir



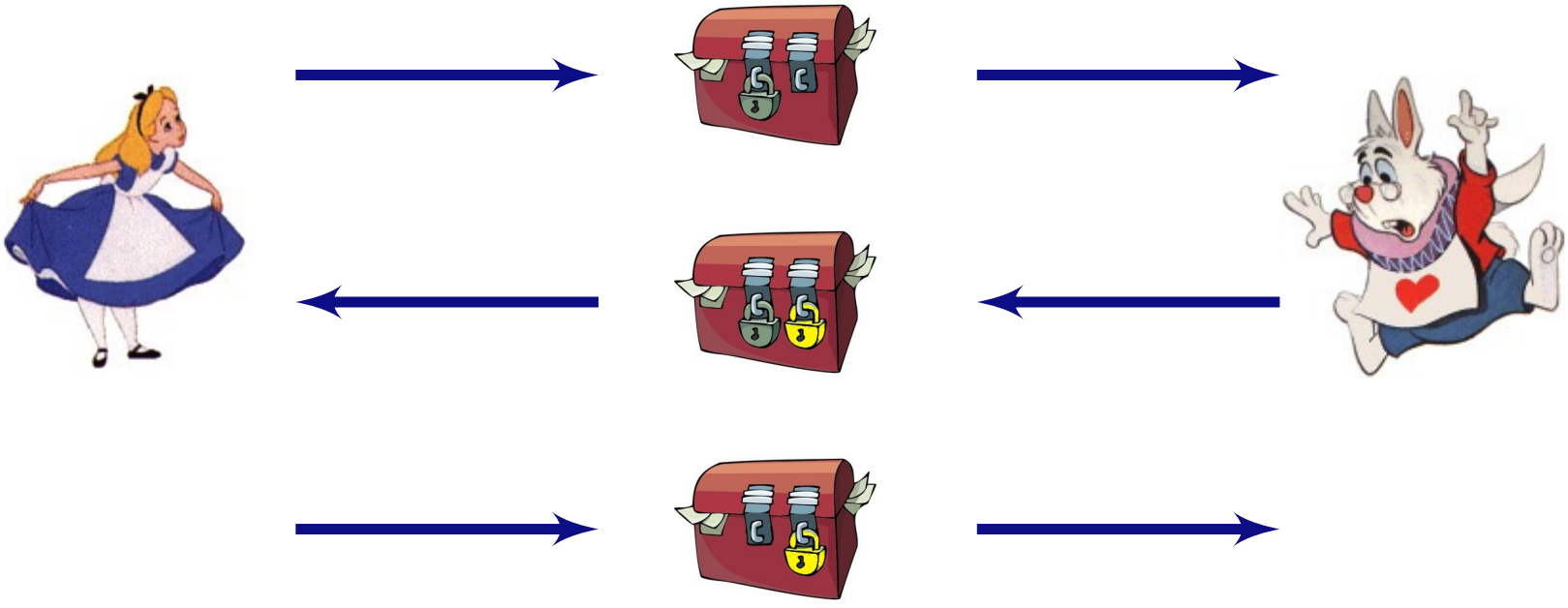
# 3-pass Shamir



# 3-pass Shamir



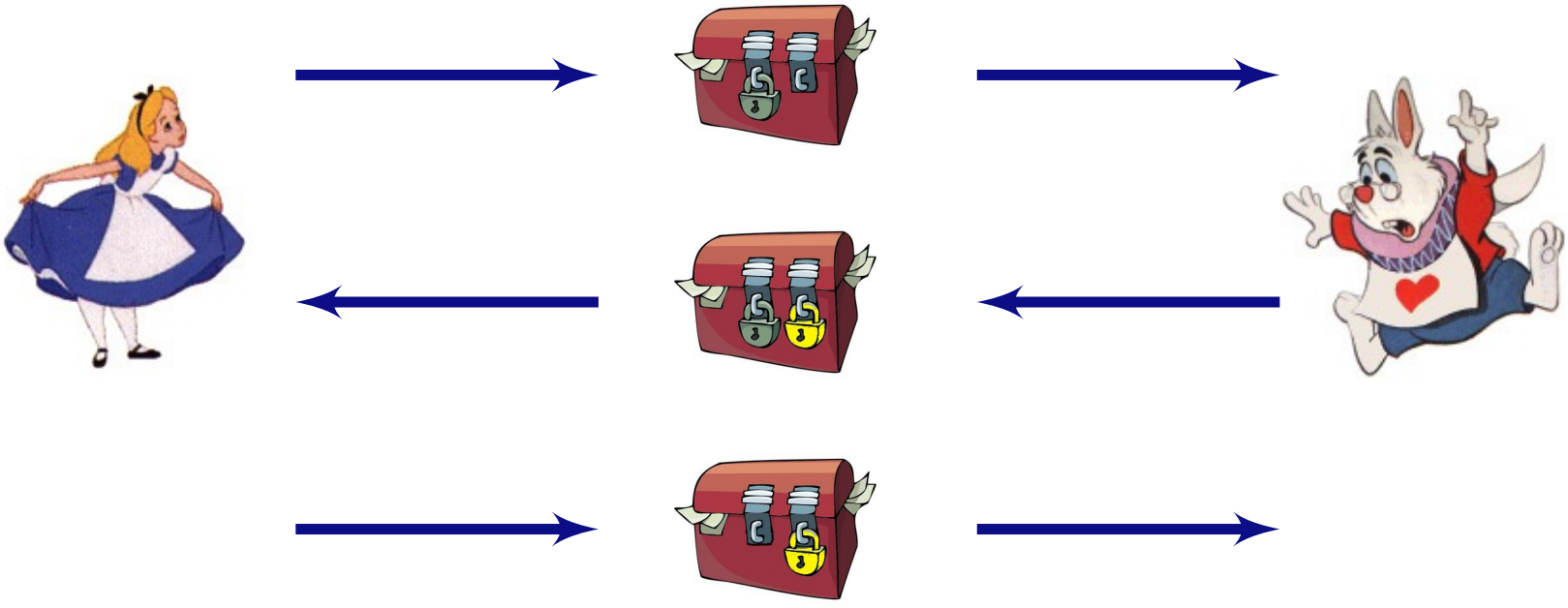
# 3-pass Shamir



## Abstract Representation

$$1 \quad A \quad \rightarrow \quad B \quad : \quad \{m\}_{K_A}$$

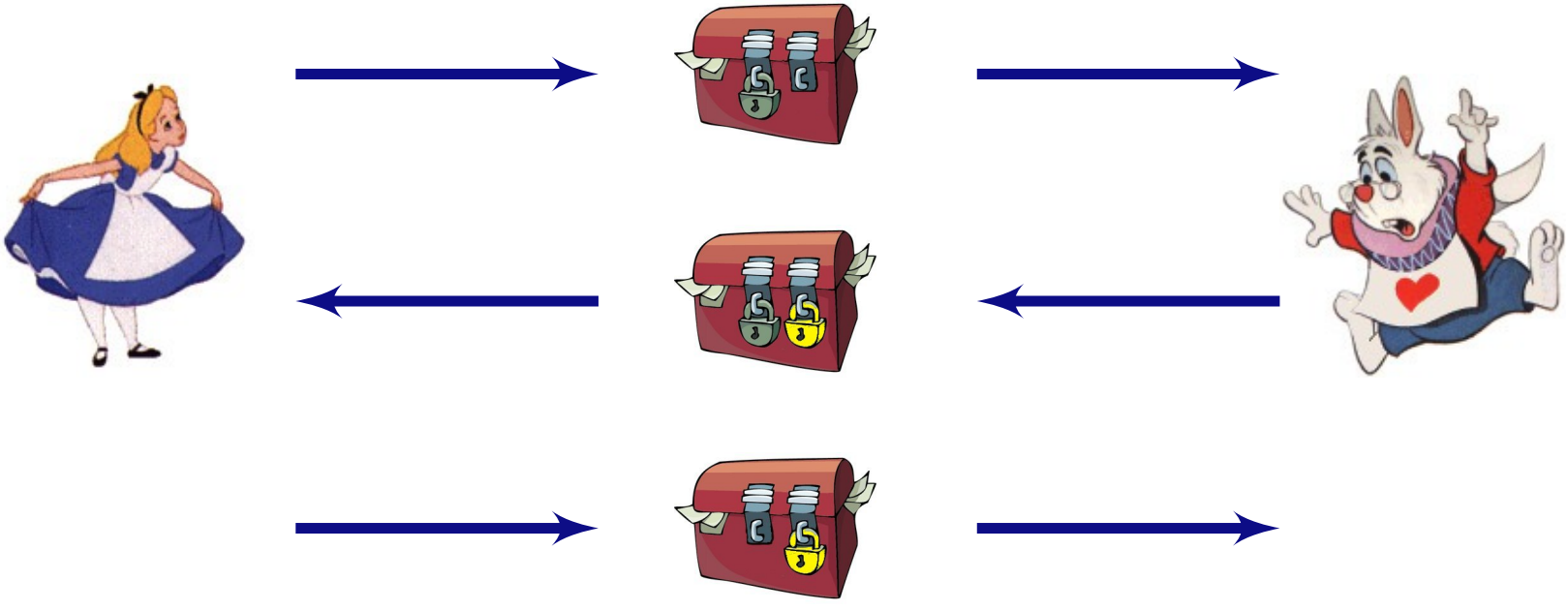
# 3-pass Shamir



## Abstract Representation

$$\begin{array}{llcll} 1 & A & \rightarrow & B & : \{m\}_{K_A} \\ 2 & B & \rightarrow & A & : \{\{m\}_{K_A}\}_{K_B} \end{array}$$

# 3-pass Shamir

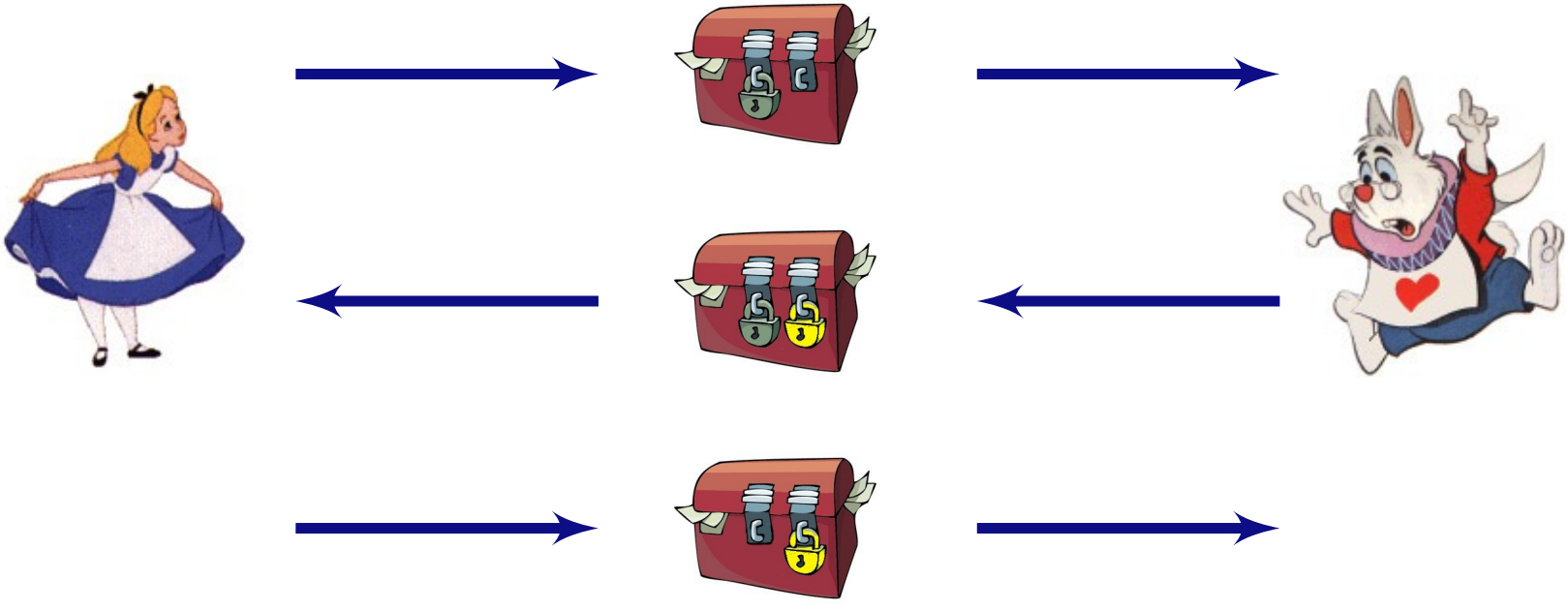


## Abstract Representation

$$\begin{array}{llllll} 1 & A & \rightarrow & B & : & \{m\}_{K_A} \\ 2 & B & \rightarrow & A & : & \{\{m\}_{K_A}\}_{K_B} = \{\{m\}_{K_B}\}_{K_A} \end{array}$$

Commutative Encryption

# 3-pass Shamir



## Abstract Representation

$$
\begin{array}{llllll}
1 & A & \rightarrow & B & : & \{m\}_{K_A} \\
2 & B & \rightarrow & A & : & \{\{m\}_{K_A}\}_{K_B} = \{\{m\}_{K_B}\}_{K_A} \\
3 & A & \rightarrow & B & : & \{m\}_{K_B}
\end{array}
$$

Commutative Encryption

# Logical Attack on Shamir 3-Pass Protocol (I)

## Perfect encryption one-time pad (Vernam Encryption)

$\{m\}_k = m \oplus k$

## XOR Properties (ACUN)

- $(x \oplus y) \oplus z = x \oplus (y \oplus z)$ **A**ssociativity
- $x \oplus y = y \oplus x$ **C**ommutativity
- $x \oplus 0 = x$ **U**nity
- $x \oplus x = 0$ **N**ilpotency

# Logical Attack on Shamir 3-Pass Protocol (I)

## Perfect encryption one-time pad (Vernam Encryption)

$\{m\}_k = m \oplus k$

## XOR Properties (ACUN)

- $(x \oplus y) \oplus z = x \oplus (y \oplus z)$ **A**ssociativity
- $x \oplus y = y \oplus x$ **C**ommutativity
- $x \oplus 0 = x$ **U**nity
- $x \oplus x = 0$ **N**ilpotency

Vernam encryption is a commutative encryption :

$$\{\{m\}_{K_A}\}_{K_I} = (m \oplus K_A) \oplus K_I = (m \oplus K_I) \oplus K_A = \{\{m\}_{K_I}\}_{K_A}$$

# Logical Attack on Shamir 3-Pass Protocol (II)

## Perfect encryption one-time pad (Vernam Encryption)

$\{m\}_k = m \oplus k$

## Shamir 3-Pass Protocol

$$
\begin{array}{llcll}
1 & A & \rightarrow & B: & m \oplus K_A \\
2 & B & \rightarrow & A: & (m \oplus K_A) \oplus K_B \\
3 & A & \rightarrow & B: & m \oplus K_B
\end{array}
$$

Passive attacker :

$m \oplus K_A \qquad m \oplus K_B \oplus K_A \qquad m \oplus K_B$

# Logical Attack on Shamir 3-Pass Protocol (II)

## Perfect encryption one-time pad (Vernam Encryption)

$\{m\}_k = m \oplus k$

## Shamir 3-Pass Protocol

$$
\begin{array}{llll}
1 & A & \rightarrow & B: \quad m \oplus K_A \\
2 & B & \rightarrow & A: \quad (m \oplus K_A) \oplus K_B \\
3 & A & \rightarrow & B: \quad m \oplus K_B
\end{array}
$$

Passive attacker :

$$m \oplus K_A \oplus m \oplus K_B \oplus K_A \oplus m \oplus K_B = m$$

# Second Example

## Needham Schroeder Key Echange 1976

$$A \rightarrow B : \{A, N_A\}_{Pub(B)}$$

$$B \rightarrow A : \{N_A, N_B\}_{Pub(A)}$$

$$A \rightarrow B : \{N_B\}_{Pub(B)}$$

- Use cryptography
- Small programs
- Distributed

# Cryptography is not sufficient !

## Example : Needham Schroeder Key Echange

$$A \rightarrow B : \{A, N_A\}_{Pub(B)}$$

$$B \rightarrow A : \{N_A, N_B\}_{Pub(A)}$$

$$A \rightarrow B : \{N_B\}_{Pub(B)}$$

# Cryptography is not sufficient !

## Example : Needham Schroeder Key Echange

$$A \to B : \{A, N_A\}_{Pub(B)}$$
$$B \to A : \{N_A, N_B\}_{Pub(A)}$$
$$A \to B : \{N_B\}_{Pub(B)}$$

Broken 17 years after, by G. Lowe

$$A \to I : \{A, N_A\}_{Pub(I)} \qquad I \to B : \{A, N_A\}_{Pub(B)}$$
$$A \leftarrow I : \{N_A, N_B\}_{Pub(A)} \qquad I \leftarrow B : \{N_A, N_B\}_{Pub(A)}$$
$$A \to I : \{N_B\}_{Pub(I)} \qquad I \to B : \{N_B\}_{Pub(B)}$$

# Cryptography is not sufficient !

## Example : Needham Schroeder Key Echange

$$A \to B : \{A, N_A\}_{Pub(B)}$$
$$B \to A : \{N_A, N_B\}_{Pub(A)}$$
$$A \to B : \{N_B\}_{Pub(B)}$$

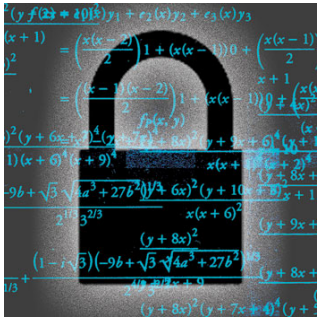
Broken 17 years after, by G. Lowe

$$A \to I : \{A, N_A\}_{Pub(I)} \qquad I \to B : \{A, N_A\}_{Pub(B)}$$
$$A \leftarrow I : \{N_A, N_B\}_{Pub(A)} \qquad I \leftarrow B : \{N_A, N_B\}_{Pub(A)}$$
$$A \to I : \{N_B\}_{Pub(I)} \qquad I \to B : \{N_B\}_{Pub(B)}$$

Computer-Aided Security

# Formal Verification Approaches

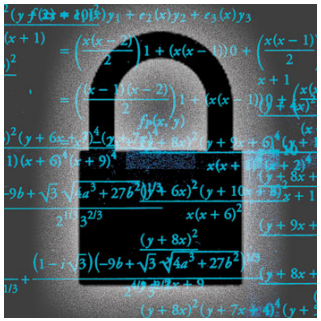
Designer



Attacker

# Formal Verification Approaches

Designer

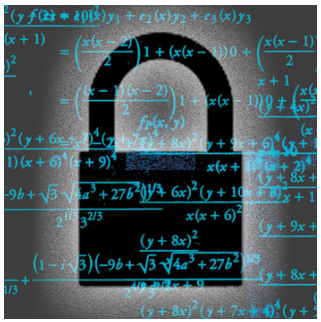


Attacker

Security Team

# Formal Verification Approaches

Designer



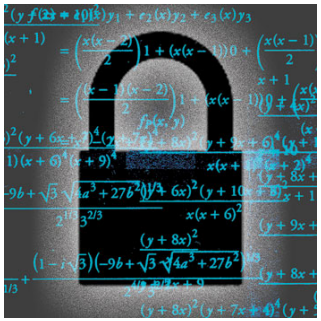
Attacker

Give a proof

Security Team

# Formal Verification Approaches

Designer



Attacker

Give a proof


Find a flaw

Security Team

# Necessity of Tools to Analyze Cryptographic Protocols

- Protocols are small recipes.
- Non trivial to design and understand.
- The number and size of new protocols.
- Out-pacing human ability to rigourously analyze them.

GOAL : A tool is finding flaws or establishing their correctness.

- completely automated,
- robust,
- expressive,
- and easily usable.

Existing Tools: AVISPA, Scyther, Proverif, Hermes, Casper/FDR, Murphi, NRL ...

# Things to bring home

Several **challenges** for the Security
of factories of the future.

- Security should be at the **conception** of the factory
- Designing secure protocols is difficult
- Formal methods are useful for designing secure protocols




*Protocol* + *Properties* + *Intruder* ⇒ *Security*

Thanks for your attention

Questions ?

Do not avoid security issues !