Comment prouver la sécurité d'un protocole cryptographique? Une approche académique

Pascal Lafourcade

Chaire industrielle,
Confiance numérique

16 Octobre 2014

Objectifs de la Chaire de Confiance Numérique

Mise en place d'une activité de recherche traitant des aspects de la Confiance Numérique autour de la fiabilisation et de la sécurisation des systèmes et des services informatiques

- Pérenne
- Visible

Activité de recherche:

- Impulsée par almerys et la Caisse d'Epargne d'Auvergne et du Limousin via la Fondation de l'Université d'Auvergne
- Soutenue par le Région Auvergne
- Developpée au LIMOS

FONDATION UNIVERSITÉ D'AUVERGNE

UdA

LIMOS

almerys innover pour la vie

CAISSE D'EPARGNE D'AUVERGNE ET DU LIMOUSIN

Objectifs de la Chaire de Confiance Numérique

- Recrutement d'un enseignant chercheur spécialiste du domaine qui sera le pivot nécessaire au démarrage et l'installation de cette activité
- Organisation d'une réflexion sur les actions de formation à mener des actions de dissémination et de transfert de technologies (Workshop, Projets ANR FUI,..)
- Mise en place et animation d'un groupe de réflexion et d'un séminaire pour échanger sur cette problématique

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

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

- Chiffrement (compltement) homomorphe : de la théorie à la pratique
- Enjeux et impacts juridiques du chiffrement homomorphe
- Combinaison d'analyses statiques pour l'aide à la détection et à l'exploitabilité de vulnérabilités dans du code binaire
- Keep calm and change your password
- Authentication Using Pulse-Response Biometrics
- Security issues and Directions of Intelligent Transport Systems within limited-resources constraints
- IoT: Internet of (Insecure) Things
- Signature électronique et identité numérique : les ingrédients indispensables pour développer la confiance sur Internet.
- Primitives et constructions cryptographiques pour la confiance numérique.
- Je sais tout sur vous grâce au Wi-Fi!
- Vers un carte d'identité respectueuse de la vie privée.
- Identifiants et guesswork.
- Les nouvelles armes de James Bond.
- Virus dans une carte mythe ou (proche) réalité ?
- La confiance numérique, de l'autre côté du miroir...
- Comment avoir confiance dans les applications numériques ? Les méthodes formelles à la rescousse.
- Comment remettre l'internaute au centre des échanges ?

Séminaire Confiance Numérique

Prochain Séminaire

- 14 Novembre 2014, 14h00 : by Jordy Herrera.

Is bitcoin a suitable research topic?

- Live et replay sur la web TV de l'UDA.
- `pascal.lafourcade@udamail.fr`

Séminaire Confiance Numérique

Prochain Séminaire

- 14 Novembre 2014, 14h00 : by Jordy Herrera.

Is bitcoin a suitable research topic?

- Live et replay sur la web TV de l'UDA.
- `pascal.lafourcade@udamail.fr`

1st Symposium on Digital Trust in Auvergne

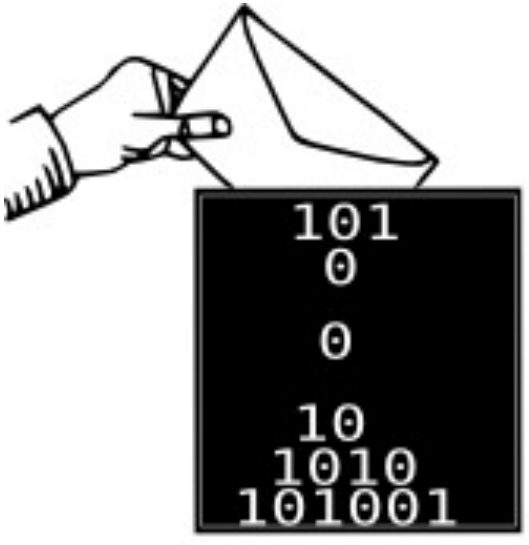
3 et 4 Décembre 2014 à Clermont-Ferrand

`confiance-numerique.clermont-universite.fr/SDTA-2014`

My Research Topics

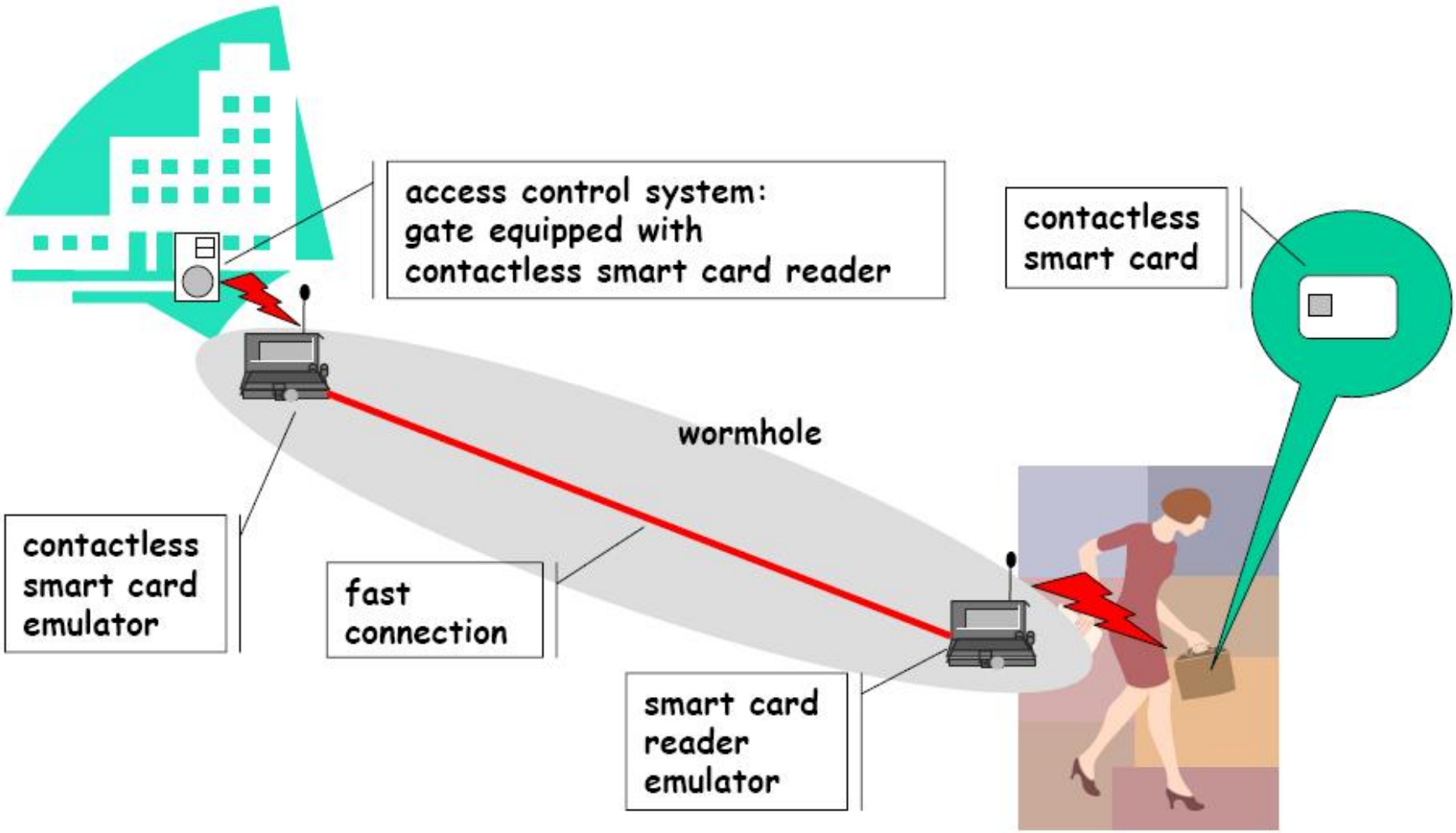
- Automatic analysis of cryptographic primitives.
- Formal analysis: e-exam, e-voting, e-reputation, e-eauction ...
- WSN: Privacy, secure routing, IDS ...

Nowadays Security is Everywhere!

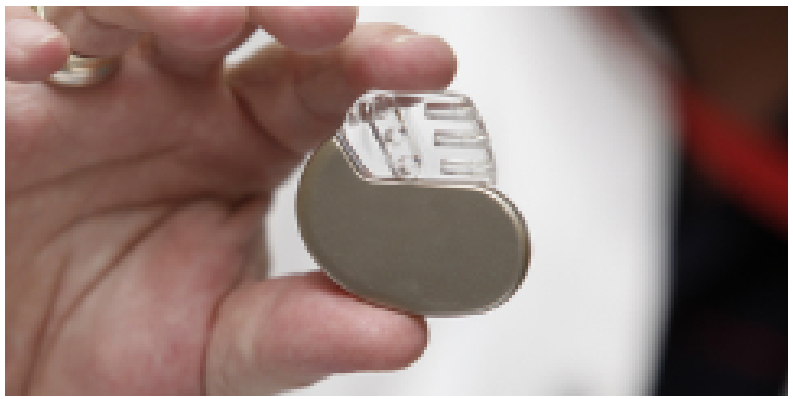


Due to the succes of Computer Science.

Wormhole Attack



Hacking Pacemakers:



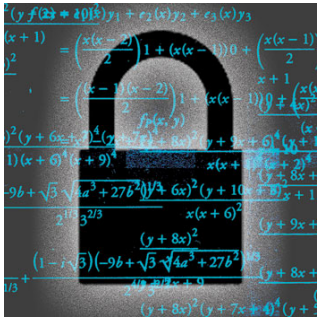
Manufacturers are still not putting security first when designing implantable medical devices (2012)

Paypal Attack

"Model-Based Vulnerability Testing of Payment Protocol Implementations", Ghazi Maatoug, Frédéric Dadeau and Michael Rusinowitch, Hotspot 2014

Formal Verification Approaches

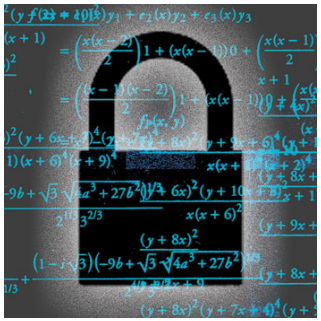
Designer



Attacker

Formal Verification Approaches

Designer

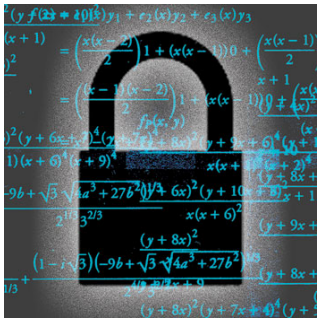


Attacker

Security Team

Formal Verification Approaches

Designer



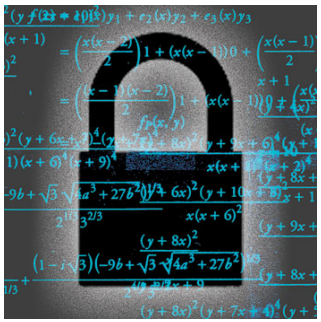
Attacker

Give a proof

Security Team

Formal Verification Approaches

Designer



Attacker

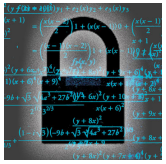
Give a proof

Find a flaw

Security Team

What is cryptography based security?

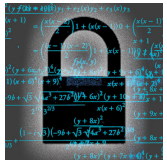
Cryptography:



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

What is cryptography based security?

Cryptography:



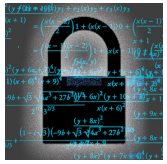
- Primitives: RSA, Elgamal, AES, DES, SHA-3 ...
- Protocols: Distributed Algorithms

Properties:

- Secrecy,
- Authentication,
- Privacy ...

What is cryptography based security?

Cryptography:



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

Properties:

- Secrecy,
- Authentication,
- Privacy ...

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 ...

Intruders:

- Passive
- Active
- CPA, CCA ...

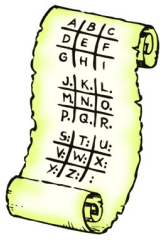
Designing **secure** cryptographic protocols is **difficult**

Security of Cryptographic Protocols

How can we be convinced that a protocols is secure?

Security of Cryptographic Protocols

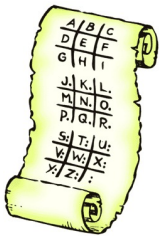
How can we be convinced that a protocols is secure?





Security of Cryptographic Protocols

How can we be convinced that a protocols is secure?

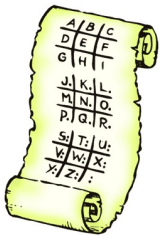




- Prove that there is no attack under some assumptions.

Security of Cryptographic Protocols

How can we be convinced that a protocols is secure?

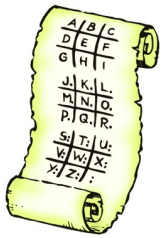




- Prove that there is no attack under some assumptions.
  - proving is a difficult task,
  - pencil-and-paper proofs are error-prone.

Security of Cryptographic Protocols

How can we be convinced that a protocols is secure?



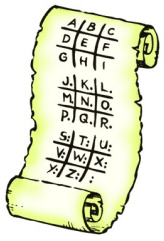


- Prove that there is no attack under some assumptions.
  - proving is a difficult task,
  - pencil-and-paper proofs are error-prone.

How can we be convinced that a proof is correct?

Security of Cryptographic Protocols

How can we be convinced that a protocols is secure?





- Prove that there is no attack under some assumptions.
  - proving is a difficult task,
  - pencil-and-paper proofs are error-prone.

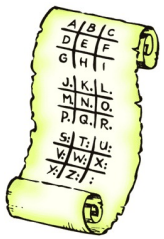
How can we be convinced that a proof is correct?





Security of Cryptographic Protocols

How can we be convinced that a protocols is secure?





- Prove that there is no attack under some assumptions.
  - proving is a difficult task,
  - pencil-and-paper proofs are error-prone.

How can we be convinced that a proof is correct?





Outline:

Outline:

Outline:

Outline:

Outline:

Outline:

Outline

Traditional security properties

- Common security properties are:
  - Confidentiality or Secrecy: No improper disclosure of information
  - Authentification: To be sure to talk with the right person. disclosure of information
  - Integrity: No improper modification of information
  - Availability: No improper impairment of functionality/service

Authentication

"On the Internet, nobody knows you're a dog."

Mechanisms for Authentication

KNOW	HAVE	ARE	DO
			
Passwords ID Questions Secret Images	Token (Smart) Card Phone	Face Iris Hand/Finger	Behavior Location Reputation

Other security properties

- Perfect Forward Secrecy (PFS) is s a property of key-agreement protocols that ensures that a session key derived from a set of long-term keys will not be compromised if one of the long-term keys is compromised in the future.
- Non-repudiation (also called accountability) is where one can establish responsibility for actions.
- Fairness is the fact there is no advantage to play one role in a protocol comparing with the other ones.
- Privacy

  Anonymity: secrecy of principal identities or communication relationships.

  Pseudonymity: anonymity plus link-ability.

  Data protection: personal data is only used in certain ways.

e-services :

- e-voting
- e-auction
- e-examen
- e-reputation
- e-cash
- e-passport
- ...

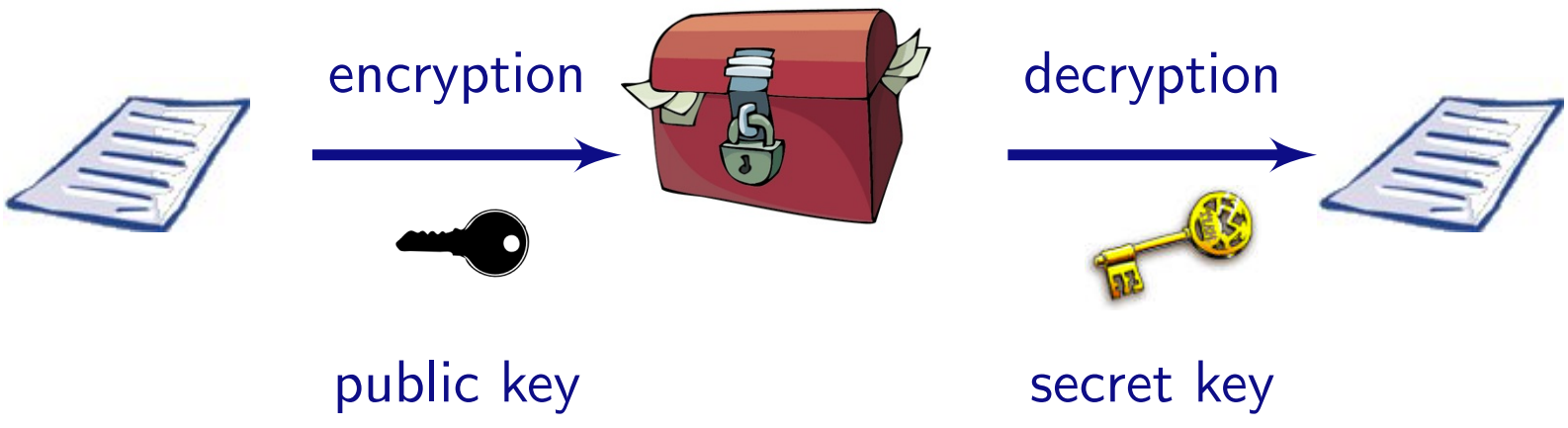
Users except more properties and security with electronic services!

Outline

Symmetric vs Asymmetric Encryption

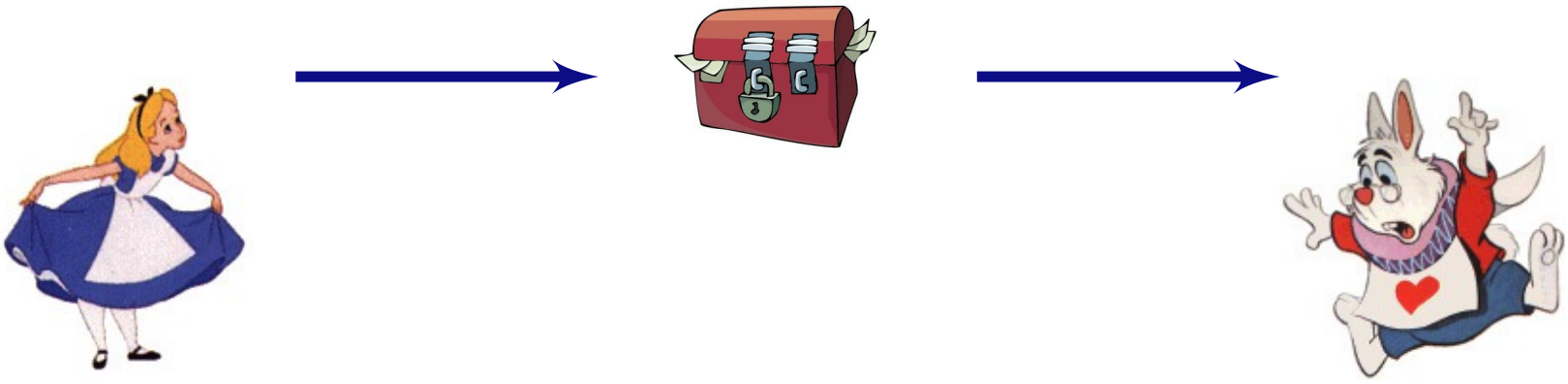
Symmetric Encryption (DES, AES)

Asymmetric Encryption (RSA, Elgamal ...)

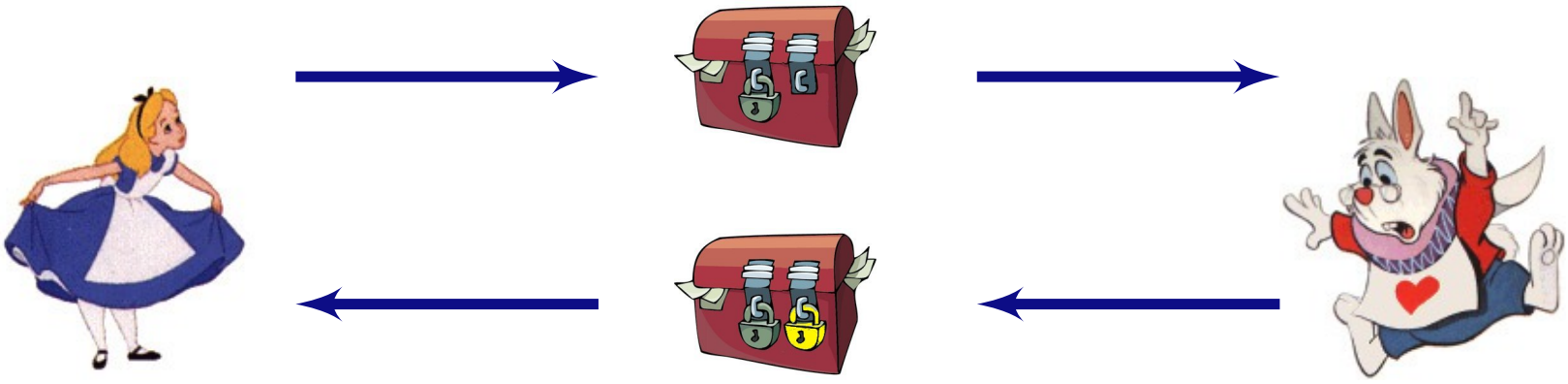


3-pass Shamir

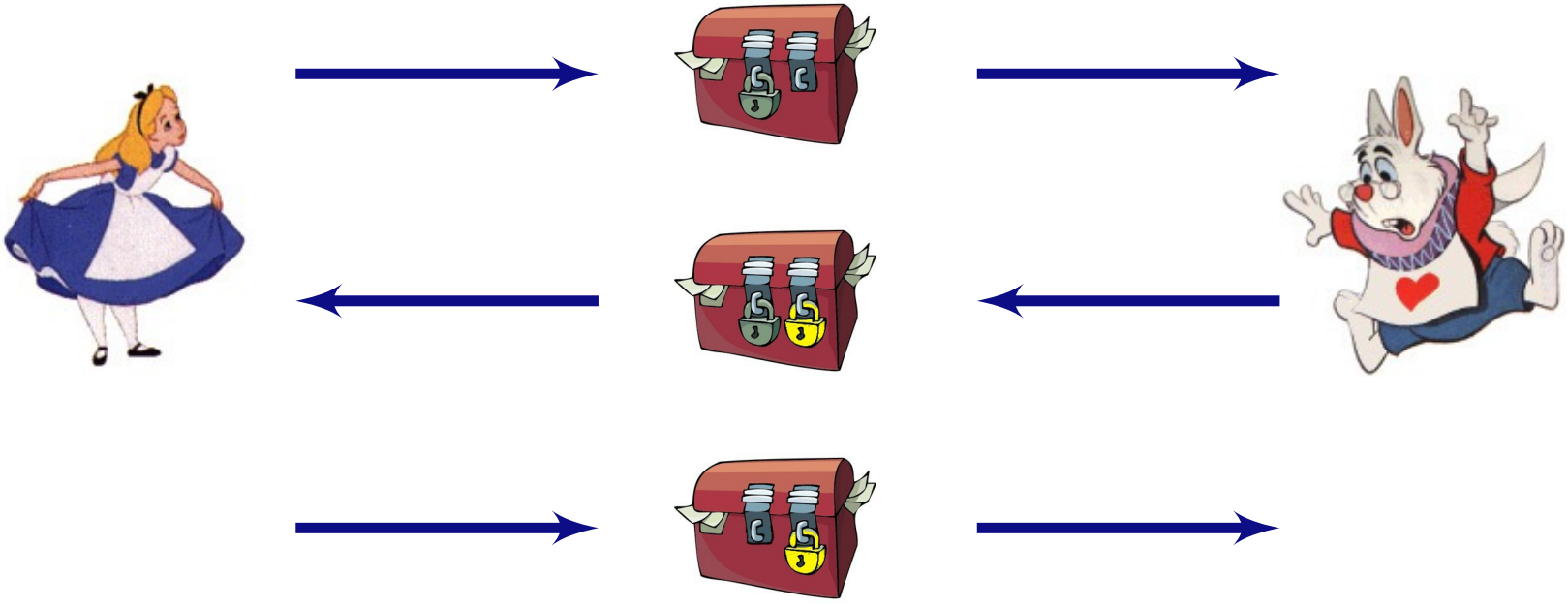
3-pass Shamir



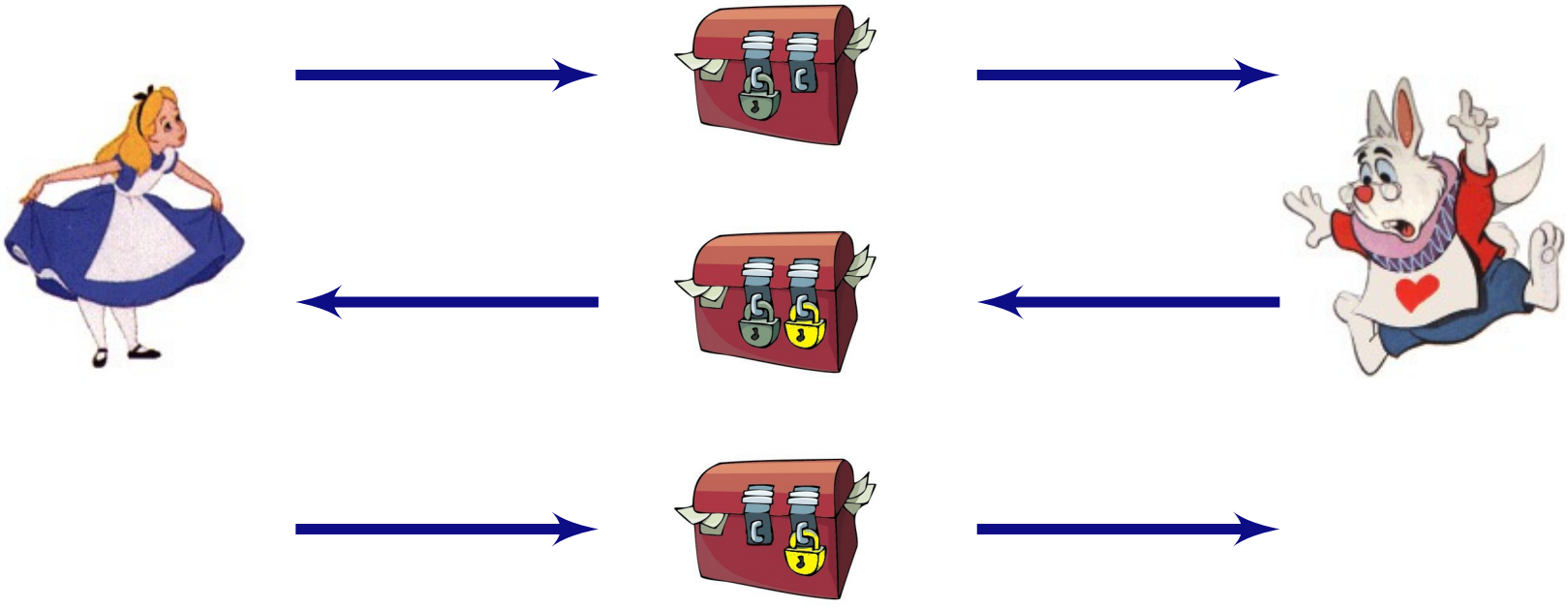
3-pass Shamir



3-pass Shamir



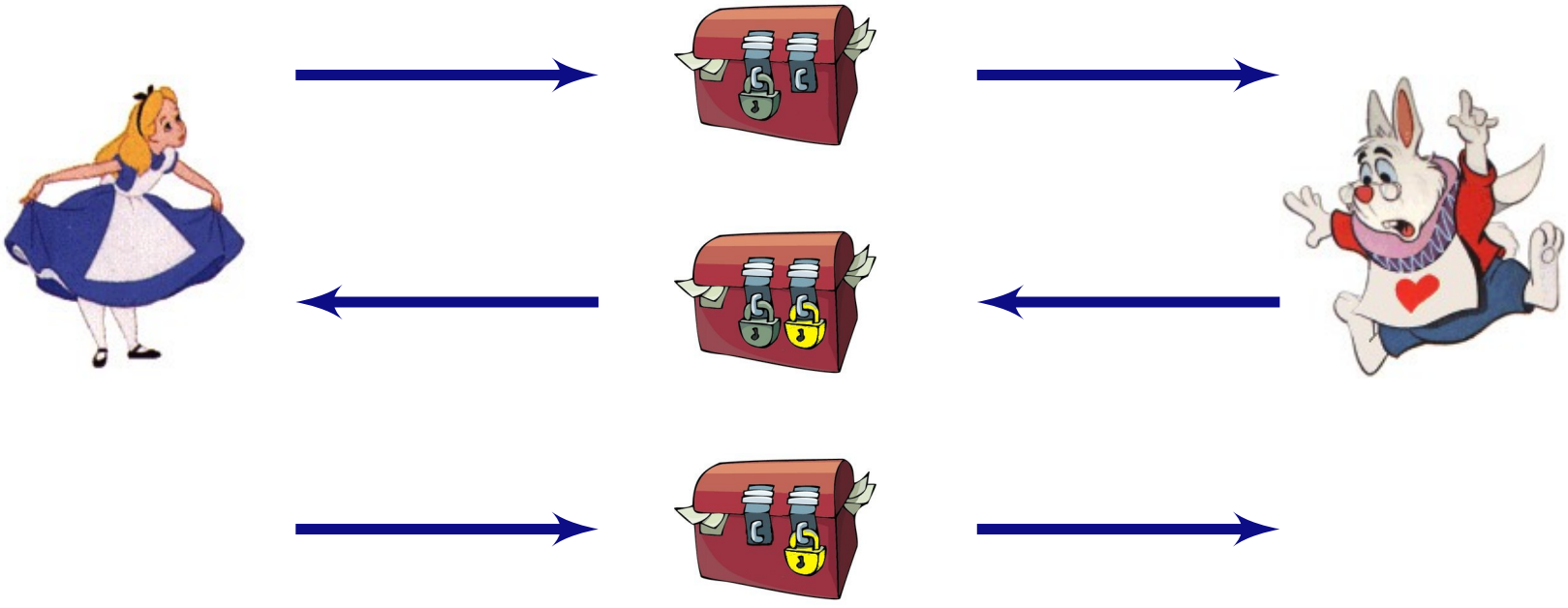
3-pass Shamir



Abstract Representation

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

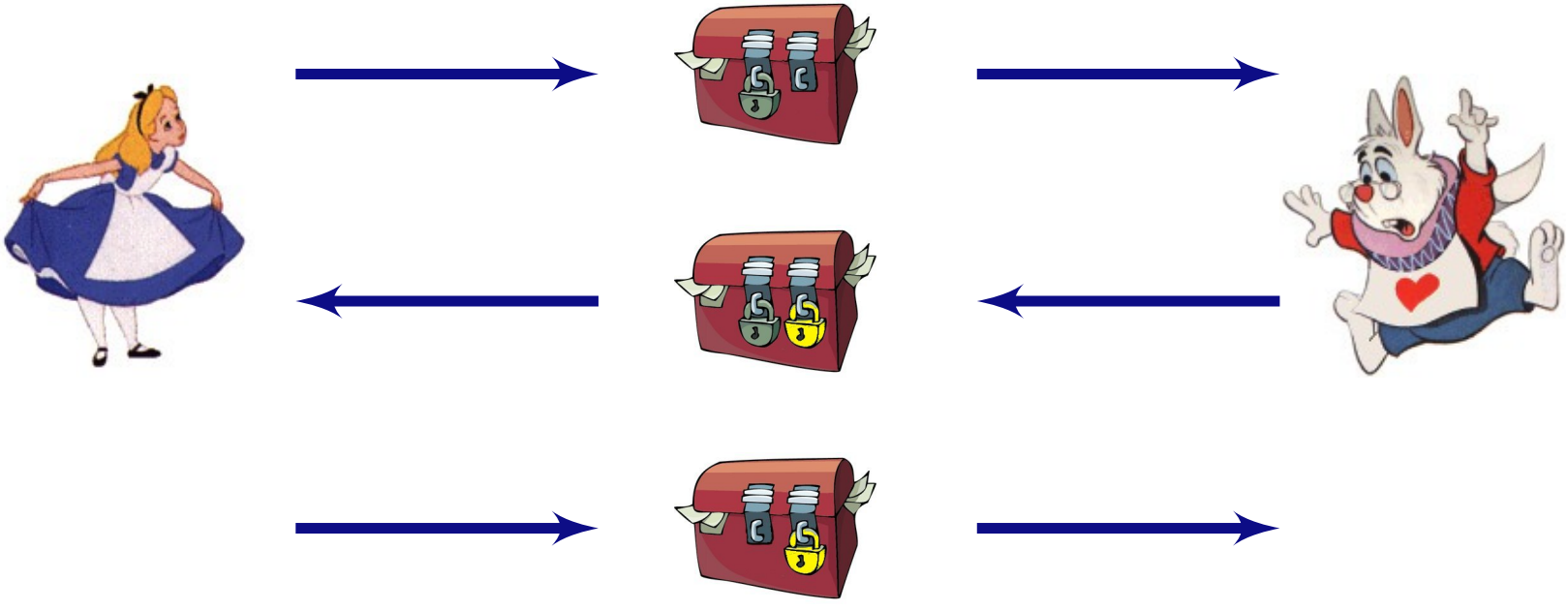
3-pass Shamir



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

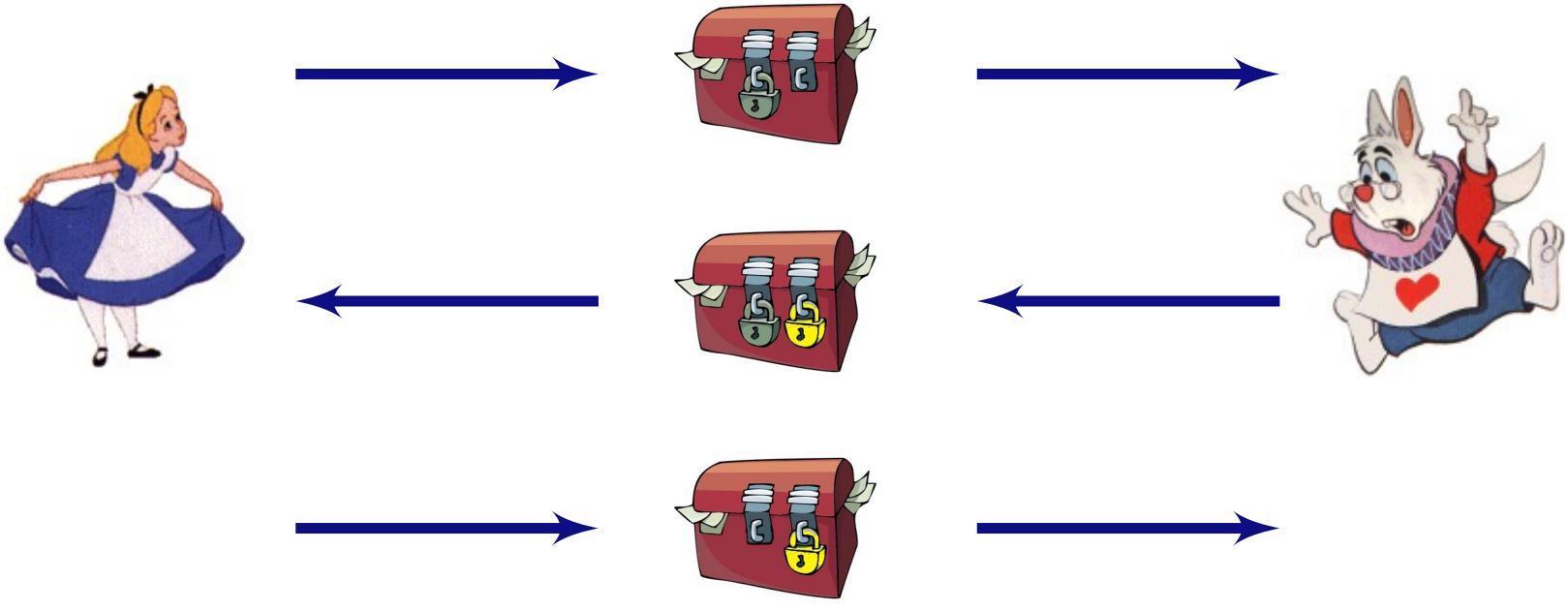


Abstract Representation

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

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

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

Outline

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 :

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

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

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

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

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

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

Computer-Aided Security

Outline

Necessity of Tools

- 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 ...

Questions?

How can we find such attacks automatically?

- Models for Protocols
- Models for Properties
- Theories and Dedicated Techniques
- Tools
  - Automatic
  - Semi-automatic

Why is it difficult to verify such protocols?

- Messages: Size not bounded
- Nonces: Arbitrary number
- Intruder: Unlimited capabilities
- Instances: Unbounded numbers of principals
- Interleaving: Unlimited applications of the protocol.

Complexity

Complexity depends of intruder capabilities. In classical Dolev-Yao intruder model we (pair + encryption) we have the following results:

- Passive Intruder
  Problem is polynomial
- Bounded Number of sessions
  Problem is NP-complete
  Tools can verify 3-4 sessions: useful to finds flaws ! OFMC, Cl-Atse, SATMC, FDR, Athena...
- Unbounded Number of sessions
  Problem is in general undecidable
  Tools are corrects, but uncomplete (can find false attacks, can not terminate) Proverif, TA4SP, Scyther.

Which tool for what ?

	Proverif	Scyther	OFMC	Cl-atse	TA4SP	SAT-MC
Secrecy	X	X	X	X	X	X
Authentication	X	X	X	X	X	X
Equivalence Obs	X					
Bounded nb S		X	X	X	X	X
Unbounded nb S	X	X			X	
Xor	x		X	X		
DH	x		X	X		
Fast	X	X				
User friendly		X				

Success Story of Formal Verification

Tools based on different theories for several properties

1995	Casper/FRD [Lowe]
2001	Proverif [Blanchet]
2003	Proof of certified email protocol with Proverif [AB]
	OFMC [BMV]
	Hermes [BLP]
	Flaw in Kerberos 5.0 with MSR 3.0 [BCJS]
2004	TA4SP [BHKO]
2005	SATMC [AC]
2006	CL-ATSE [Turuani]
2008	Scyther [Cremers]
	Flaw of Single Sign-On for Google Apps with SAT-MC [ACCCT]
	Proof of TLS using Proverif [BFCZ]
2010	TOOKAN [DDS] using SAT-MC for API
2012	Tamarin [BCM]

Outline

Summary

5 points to bring home

- Security is everywhere (IoT)
- Security design is a global process
- Security = Cryptography + Properties + Adversaries
- Users have to be educated
- Computer-Aided Security (Tools)

Thank you for your attention.

pascal.lafourcade@udamail.fr

Questions ?

1st Symposium on Digital Trust in Auvergne

3 et 4 Décembre 2014 à Clermont-Ferrand

confiance-numerique.clermont-universite.fr/SDTA-2014

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