Cryptographie: de la théorie à la pratique

Pascal Junod // HEIG-VD

heig-vd
Haute Ecole d'Ingénierie et de Gestion
du Canton de Vaud

Plan

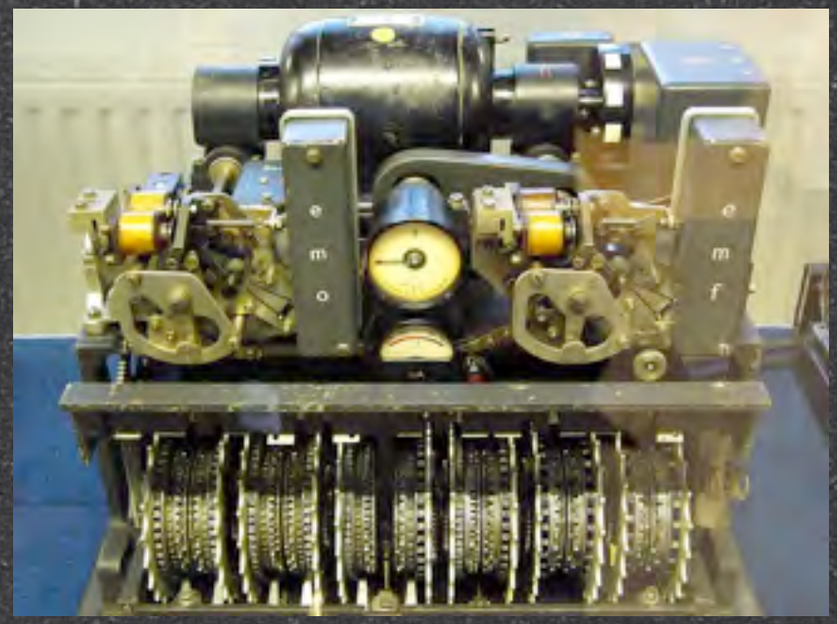
- Crypto Académique
- Crypto Pratique
- Perspectives

Crypto Académique

Pascal Junod -- Cryptographie: de la théorie à la pratique
CLUSIS, 8 mars 2011, Genève, Suisse

Cryptologie

- Historiquement, l'affaire des gouvernements (diplomatie, armée, services secrets, ...



- Situation change dès la publication du DES dans les années 1970
  - Industrie bancaire
  - Internet

Cryptologie

- Aujourd'hui
  - Des milliers de personnes «cherchent» dans le domaine de la cryptologie
    - Monde académique
    - Industrie
    - (Gouvernements)
- Des milliards de personnes utilisent de la cryptographie tous les jours

Cryptologie

- Aujourd'hui
  - Des dizaines de nouveaux algorithmes/protocoles publiés chaque année
  - Des centaines de publications scientifiques par année
  - Du logiciel open-source disponible partout


Cryptology ePrint Archive: Search Results

2011/112 (PDF)
An efficient certificateless two-party authenticated key agreement scheme from pairings
He Debiao

2011/111 (PDF)
Generalizations of Bent Functions. A Survey
Natalia Tokareva

2011/110 (PDF)
Fully Homomorphic Encryption over the Binary Polynomials
Gu Chunsheng

2011/109 (PDF)
Secure Blind Decryption
Matthew Green

2011/108 (PDF)
Practical Secure and Efficient Multiparty Linear Programming Based on Problem Transformation
Jannik Dreier and Florian Kerschbaum

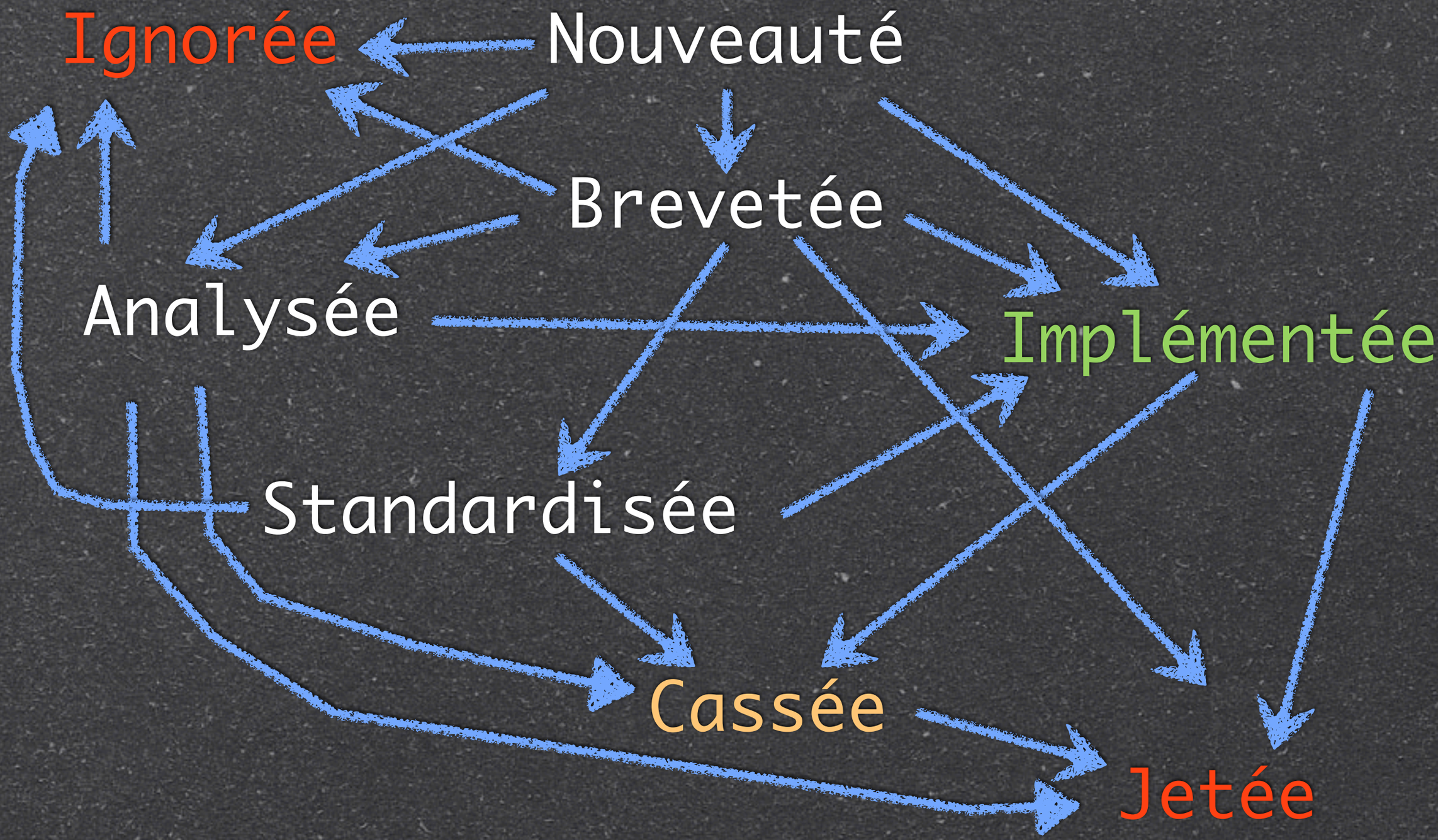
2011/107 (PDF)
Threshold Encryption into Multiple Ciphertexts
Martin Stanek

2011/106 (PS PS.GZ PDF)
Common Randomness and Secret Key Capacities of Two-way Channels
Hadi Ahmadi and Reihaneh Safavi-Naini

2011/105 (PDF)
Explicit Formulas for Real Hyperelliptic Curves of Genus 2 in Affine Representation
S. Erickson and M. J. Jacobson, Jr. and A. Stein

2011/104 (PDF)
Unconditionally Secure Signature Schemes Revisited
Colleen M. Swanson and Douglas R. Stinson

Cryptologie

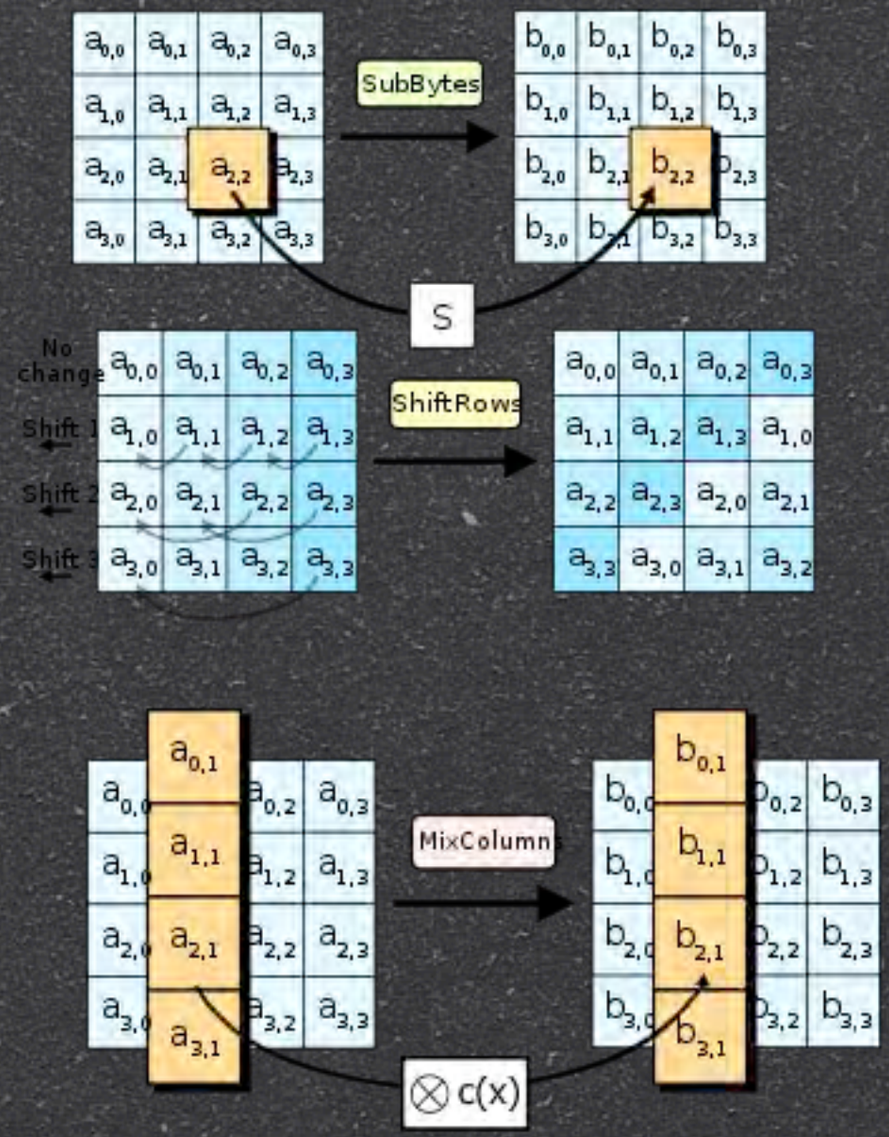


Exemples: DES

- Data Encryption Standard
  - Algorithme de chiffrement symétrique
  - Standardisé par le NBS dans les années 70
  - Très analysé et très implémenté
  - Cassé (clef trop courte)
  - Retiré petit à petit au profit de Triple-DES / AES

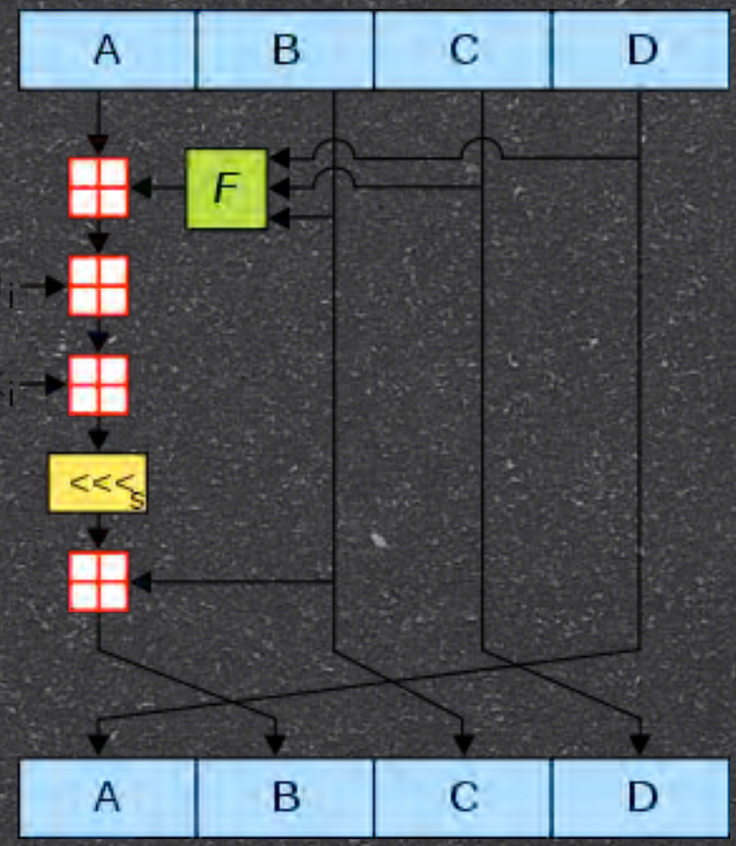
Exemples: AES

- Advanced Encryption Standard
  - Algorithme de chiffrement symétrique
  - «Développé» par le NIST de 1997 à 2000
  - Standardisé en 2001
  - Très analysé
  - De plus en plus implémenté

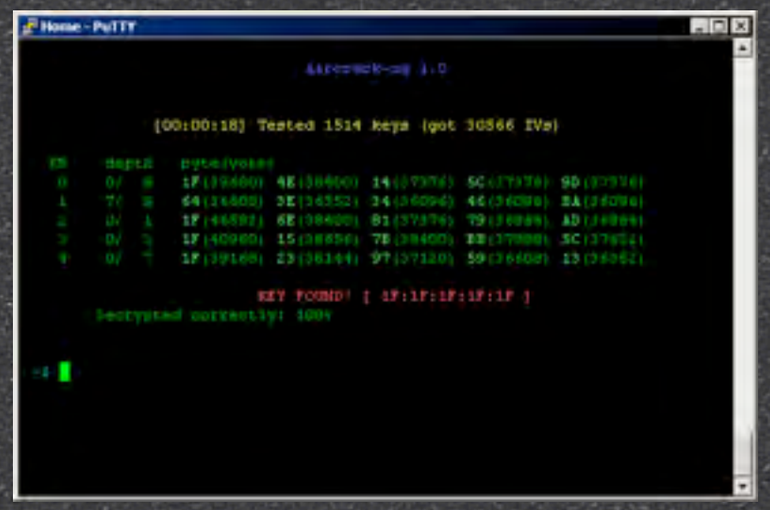


Exemples: MD5

- Fonction de hachage conçue par Ron Rivest (MIT)
- Relativement peu analysée
- Cassée dès 1995, puis en 2004
  - Collisions
  - Pas encore de secondes préimages
- Encore très présente



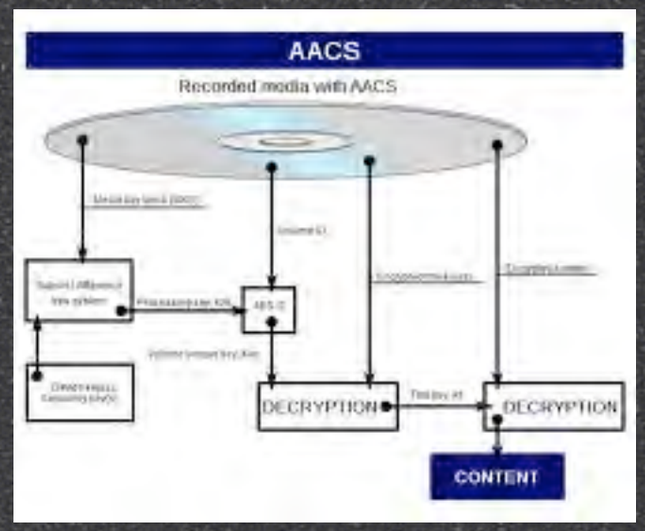
Exemples: WEP



- Wired Equivalent Privacy
- Standardisé en 1997
- Cassé dès 2001
- Encore énormément utilisé

Exemples: AACS

- Advanced Access Content System
- Sécurise les Blu-Ray / (HD-DVD)
- Standardisé en 2005
- Utilise de la cryptographie de pointe
- Néanmoins, en pratique...



Crypto Académique

- Principal fournisseur de solutions «algorithmiques»
- Très peu impliquée dans l’implémentation des solutions qu’elle propose
- Très active dans le domaine de la cryptanalyse
- Souvent relativement éloignée des besoins de l’industrie

Crypto Académique

- Un «breakthrough» dans le domaine de la crypto académique n'a souvent aucune influence en pratique...
- ... mais pas toujours !
- Exemple: les attaques récentes contre WEP vs. celles contre MD5, SHA-1 ou AES.

En Résumé...

- La sécurité d'un algorithme décroît inévitablement avec le temps.
- La cryptographie ne résout souvent pas tous les problèmes de sécurité.
- Un algorithme pas cassé est sûrement un algorithme que personne n'a étudié.
- Une attaque de type «académique» n'a pas forcément d'impact en pratique... mais pas toujours !

Crypto Pratique

Pascal Junod -- Cryptographie: de la théorie à la pratique
CLUSIS, 8 mars 2011, Genève, Suisse

De la Théorie à la Pratique

- Théorie
  - Algorithmes
  - Spécifications
  - Papier scientifique
- Pratique
  - Implémentation
  - Software / hardware
  - Sécurisation d’un système

Adversaires «Black-Box»

- C’est la définition privilégiée des cryptologues

Les scientifiques qui n’utilisent leur ordinateur que pour faire du mail et écrire des papiers en LaTeX ;-)

Adversaires «Black-Box»

- Je modélise mon algorithme/protocole/système comme un ensemble d'oracles
- Interaction avec ces oracles:
  - Chiffré
  - Texte clair connu
  - Texte clair/chiffré choisi (adaptatif ou non)

Adversaires «Black-Box»

- Je prouve (mathématiquement) que mon algorithme/protocole/système est sûr si les primitives cryptographiques utilisées sont sûres.
- Exemples:
  - RSA-OAEP
  - RSA-PSS

Adversaires «Grey-Box»

- Adversaires pas vraiment prévus par les cryptologues (théoriciens)
- Ils interagissent avec les primitives cryptographiques, mais ils obtiennent en plus un tout petit peu d'information sur le calcul:
  - Timings
  - Fuites physiques
  - Fautes

Adversaires «White-Box»

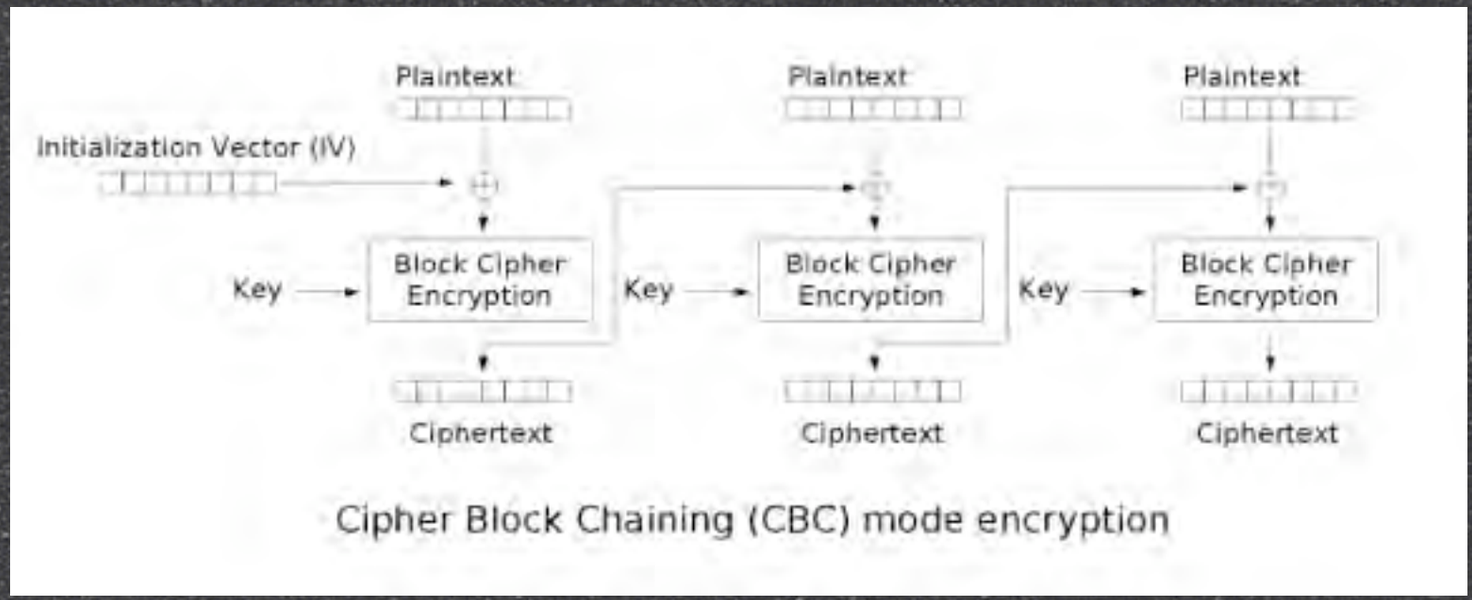
Ceux qui travaillent dans la jungle ...

- Le cauchemar de nombreux cryptologues
- Peuvent faire TOUT ce qu'ils souhaitent
- «Reverse-engineering» du SW/HW
- Lire/écrire toutes les mémoires, y-compris celles contenant des secrets
- Perturber tous les calculs

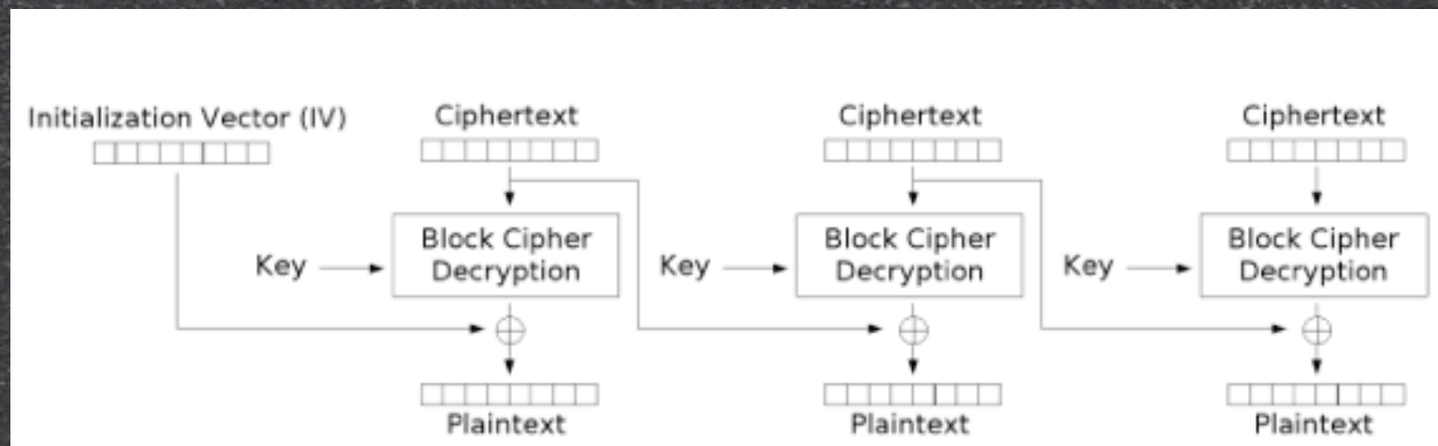
Attaques par «Side-Channel»

- Timing
- Fuites physiques
- Fautes

Attaques par «Timing»



Cipher Block Chaining (CBC) mode encryption



Cipher Block Chaining (CBC) mode decryption

Attaques par «Timing»

- Le chiffrement en mode CBC exige que les données aient une longueur qui soit multiple de la taille de bloc de l'algorithme de chiffrement utilisé.
  - AES-CBC: multiple de 16 octets
  - TDES-CBC: multiple de 8 octets

Attaques par «Timing»

- «Padding» standard avec des blocs de 8 octets:
  - 3 octets manquants: pad avec 03 03 03
  - 7 octets manquants: pad avec 07 07 07 07 07 07 07
  - Pas d'octet manquant: pad avec 08 08 08 08 08 08 08 08

Attaques par «Timing»

- Problème si la routine qui vérifie le «padding» ne travaille pas en temps constant:

Password Interception in a SSL/TLS Channel

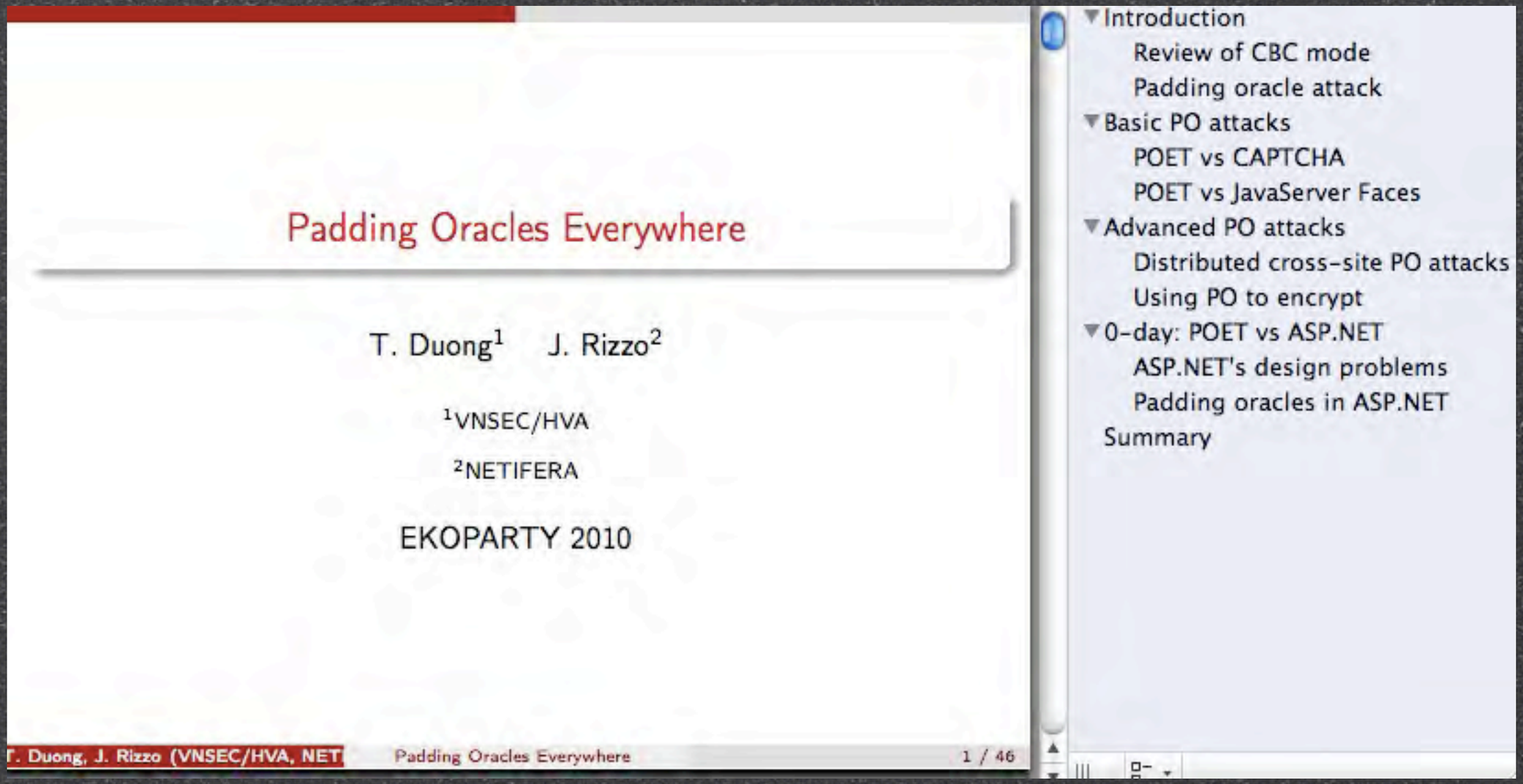
Brice Canvel[1], Alain Hiltgen[2], Serge Vaudenay[1], and Martin Vuagnoux[3]

[1] Swiss Federal Institute of Technology (EPFL) - LASEC
http://lasecwww.epfl.ch
[2] UBS AG
email:alain.hiltgen@ubs.com
[3] EPFL - SSC, and Ilion
http://www.ilionsecurity.ch

Abstract. Simple password authentication is often used e.g. from an email software application to a remote IMAP server. This is frequently done in a protected peer-to-peer tunnel, e.g. by SSL/TLS.
At Eurocrypt'02, Vaudenay presented vulnerabilities in padding schemes used for block ciphers in CBC mode. He used a side channel, namely error information in the padding verification. This attack was not possible against SSL/TLS due to both unavailability of the side channel (errors are encrypted) and premature abortion of the session in case of errors. In this paper we extend the attack and optimize it. We show it is actually applicable against latest and most popular implementations of SSL/TLS (at the time this paper was written) for password interception.
We demonstrate that a password for an IMAP account can be intercepted when the attacker is not too far from the server in less than an hour in a typical setting.
We conclude that these versions of the SSL/TLS implementations are not secure when used with block ciphers in CBC mode and propose ways to strengthen them. We also propose to update the standard protocol.

Attaques par «Timing»

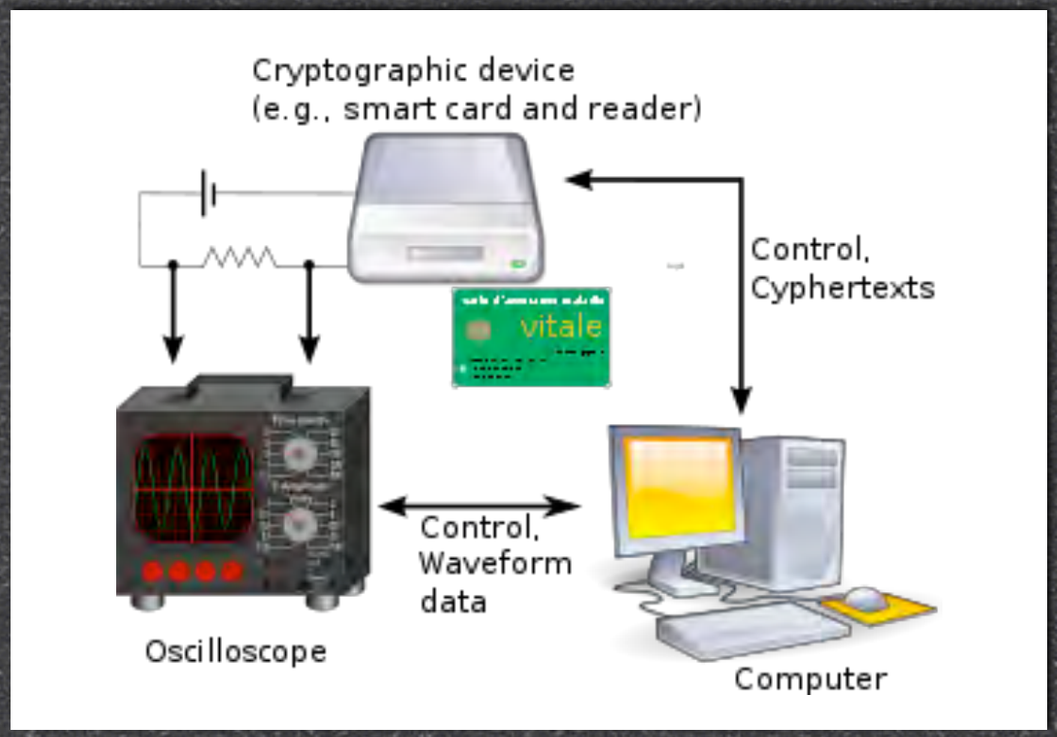
- Autre exemple d'exploitation de problèmes de «padding» :

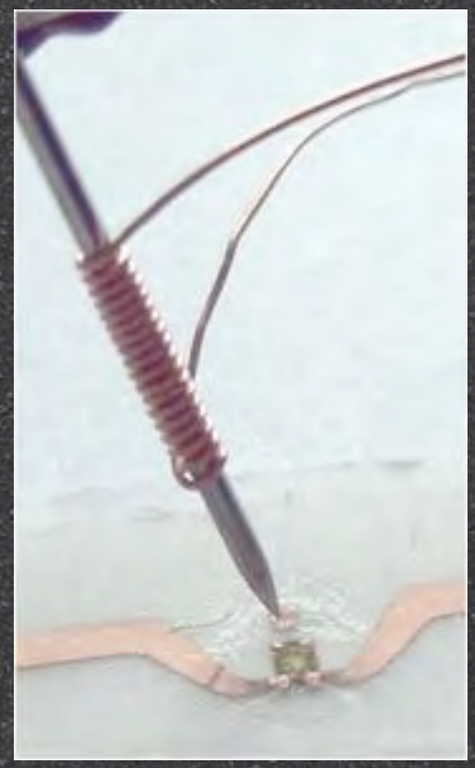


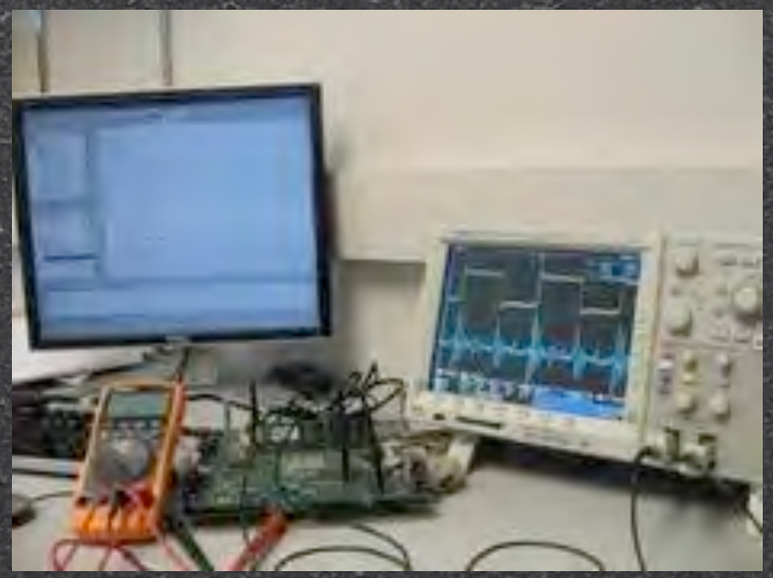
Attaques exploitant les Fuites Physiques

- N’importe quel calcul va inévitablement consommer de l’énergie.
- Si cette consommation d’énergie est corrélée à des valeurs secrètes, alors les secrets sont exposés...

Attaques exploitant les Fuites Physiques





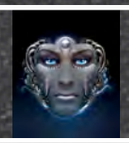


Attaques exploitant des Fautes

OpenSSL et Consoeurs

- De nombreuses librairies cryptographiques open-source et généralistes existent (liste non-exhaustive):
  - OpenSSL
  - libgcrypt
  - Mozilla NSS
  - libtomcrypt
  - NaCl
  - Botan
  - Crypto++
  - cryptlib

OpenSSL et Consoeurs

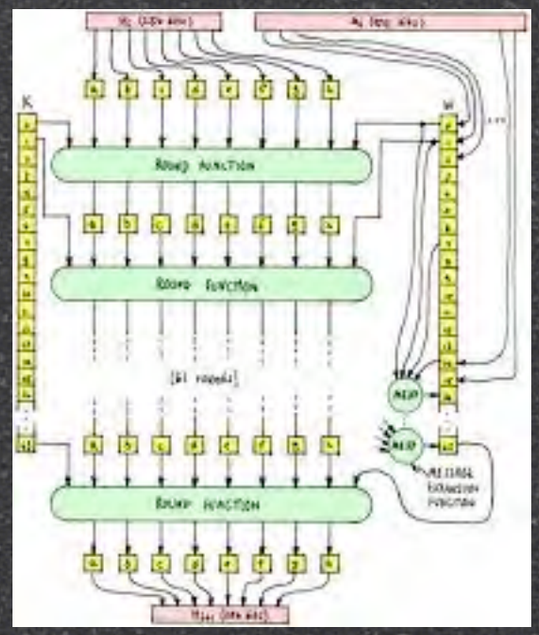
					
OpenSSL	✔	~	~	✖	✖
libgcrypt	✔	✖	✖	✖	✖
libtomcrypt	✖	✖	✖	✖	✖
NSS	✔	✖	~	✖	~
NaCl	✔	✔	✔	✖	✖
Botan	✔	✔	~	✖	~
Crypto++	✔	~	~	✖	✖
cryptlib	✔	✖	~	~	~

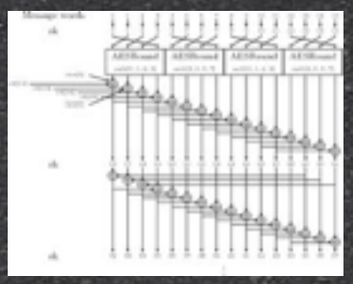
Perspectives

SHA-3

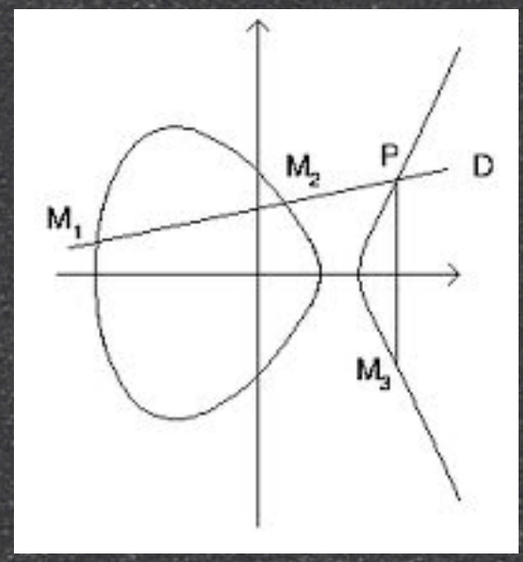
- Suite aux attaques contre les fonctions de hachage, le NIST a initié une nouvelle compétition.
- Actuellement, cinq candidats (sur 64) ont survécu, dont un Suisse !
- Le gagnant sera connu probablement fin 2012.
- Effort de développement/analyse énorme !

National Institute of Standards and Technology





Courbes Elliptiques



- Technologie alternative à RSA
- Chiffrement asymétrique/ signature
- Besoins moindre en temps de calcul/mémoire/bande passante
- Se déploie de plus en plus

certicom
securing innovation

Cryptographie basée sur des Couplages

- Technologie découverte en 2000
- Permet de définir des dizaines de nouvelles applications
  - Signatures très courtes
  - Chiffrement par identité
- Encore très peu implémenté
- Pas très analysé

Algorithm 8: Millers algorithm using double-and-add

Data: elliptic curve E/K, points $P, Q \in E(K) \setminus \{\mathcal{O}\}$, positive integer $n = \sum_{i=0}^{\lfloor \log n \rfloor} b_i 2^i$
Result: value $t \in \mathbb{Z}_n$

$t \leftarrow 1$
$V \leftarrow P$
$i \leftarrow \lfloor \log n \rfloor - 2$
while $i >= 1$ **do**
  $t \leftarrow t^2 \cdot g_{V,V}(Q)$
  $V \leftarrow 2V$
  If $b_i = 1$ **then**
    $t \leftarrow t \cdot g_{V,P}(Q)$
    $V \leftarrow V + P$
  $i \leftarrow i - 1$
return t

Voltage security

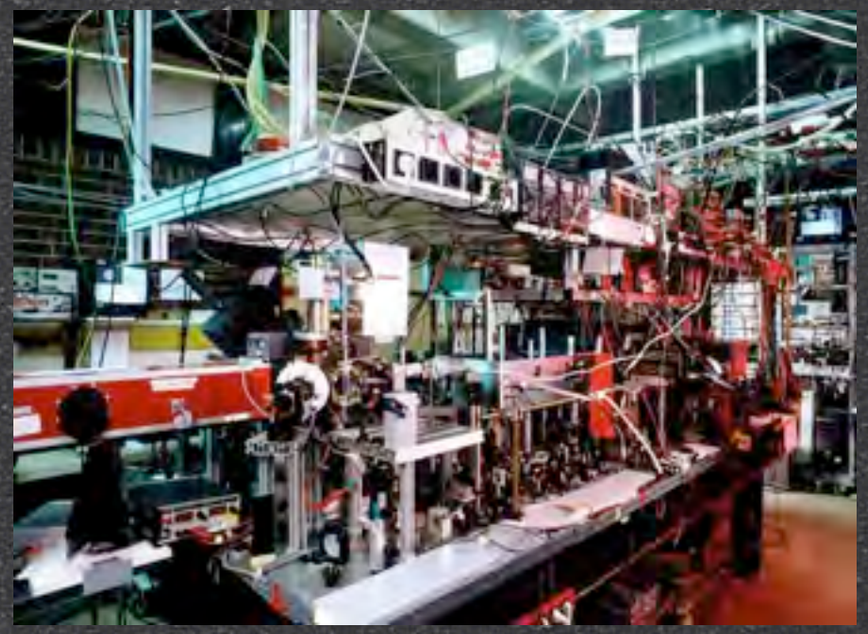
Cryptographie Résistante au Fuites

- Nouvelle ligne de recherche initiée dès 2006

- Algorithmes dont les fuites d'information sont quantifiées
- Ne sera pas pratique avant de nombreuses années...

Cryptographie Post-Quantique

- Si l'on est capable de construire un ordinateur quantique, la plupart des algorithmes utilisés aujourd'hui seront morts



- On essaye tout de même de penser à l'au-delà...

Cryptographie «White-Box»

- Développement d'algorithmes résistant à un adversaire «white-box»
- Mot-clef: obfuscation

Cryptographie Homomorphique

- But: être capable de faire des calculs sur des textes chiffrés sans les déchiffrer
- Applications: bases de données stockant des données sensibles
- En pratique: il y a encore du travail !

MERCI !

Information de Contact

- Site Web http://crypto.junod.info
- Twitter @cryptopathe
- E-mail pascal@junod.info