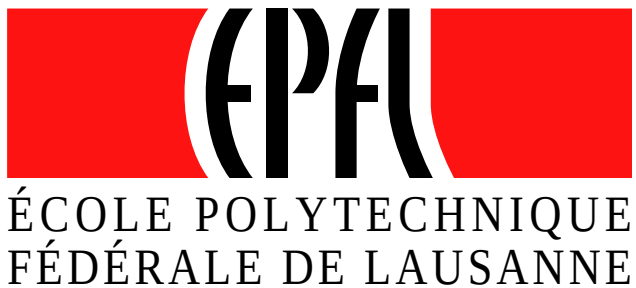
La cryptographie

Quelles perspectives?

Serge Vaudenay



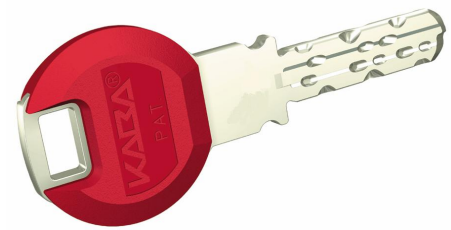
http://lasecwww.epfl.ch/

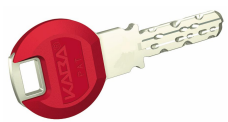
1. Eléments de cryptographie
2. Cryptographie dans la vraie vie
3. Des pistes pour l'avenir?

La communication confidentielle

[illustration de Zep]

Chiffrement symétrique



- clef secrète (session): 

Principe de Kerckhoffs

Principes de Kerckhoffs

1. Le système doit être matériellement, sinon mathématiquement, indéchiffrable;
2. **Il faut qu'il n'exige pas le secret, et qu'il puisse sans inconvénient tomber entre les mains de l'ennemi;**
3. La clef doit pouvoir en être communiquée et retenue sans le secours de notes écrites, et être changée ou modifiée au gré des correspondants;
4. Il faut qu'il soit applicable à la correspondance télégraphique;
5. Il faut qu'il soit portatif et que son maniement ou son fonctionnement n'exige pas le concours de plusieurs personnes;
6. Enfin, il est nécessaire, vu les circonstances qui en commandent l'application, que le système soit d'un usage facile, ne demandant ni tension d'esprit, ni la connaissance d'une longue série de règles à observer.

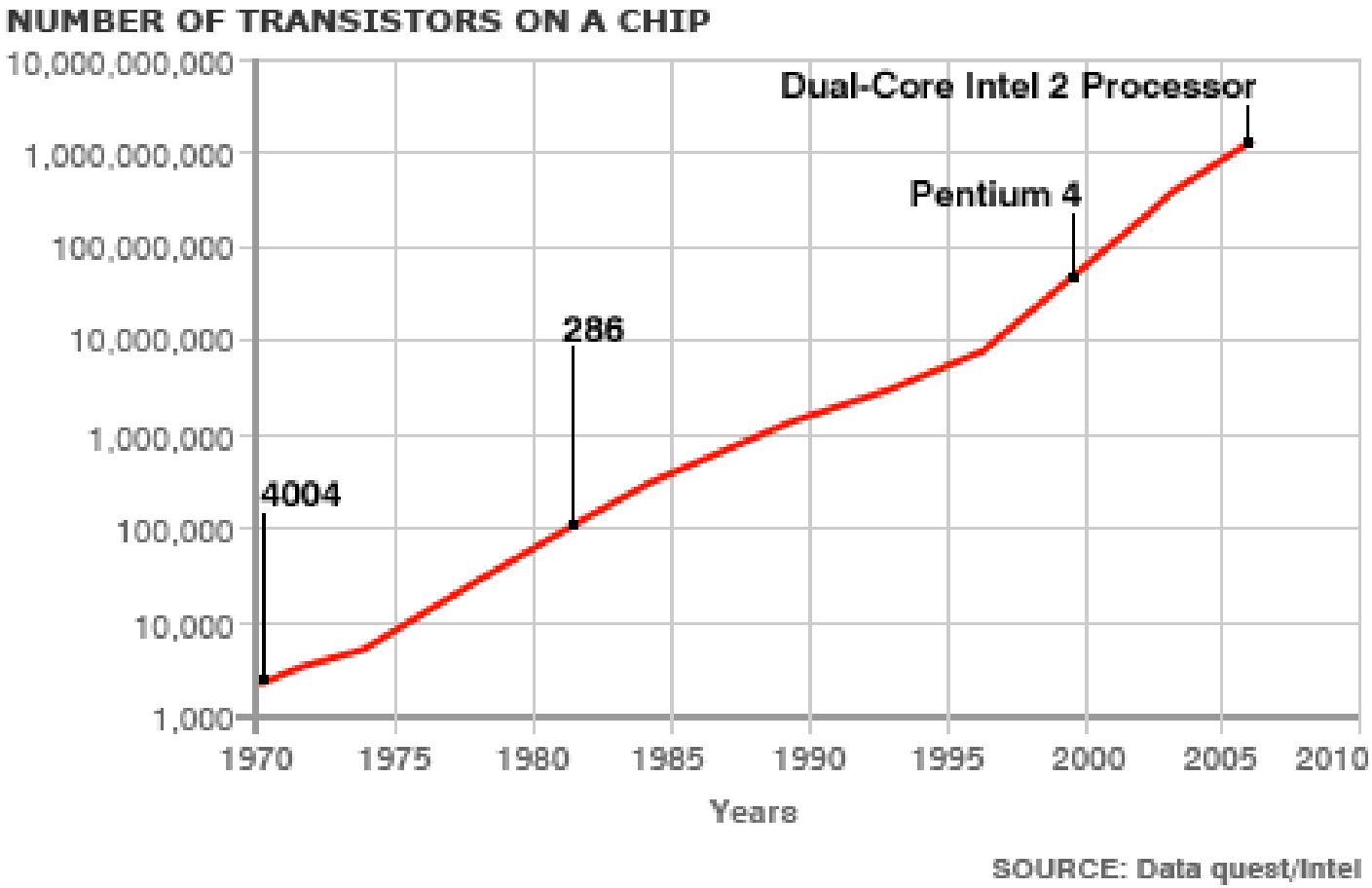
Sécurité par la longueur des clefs

- pour un système bien fait, la meilleure attaque possible est la recherche exhaustive de la clef
- à une date t_0, pour un système destiné à offir une sécurité jusqu'à une date $t_0 + \Delta$, la clef doit avoir une taille de

$$\text{marge} + \log_2 \left(\int_{t_0}^{t_0+\Delta} f_t \, dt \right)$$

  où f_t est le nombre de clefs par seconde pouvant être testées avec la technologie disponible à la date t
- si f_t a une croissance exponentielle, la taille nécessaire de la clef est une fonction **linéaire** de Δ

Loi de Moore

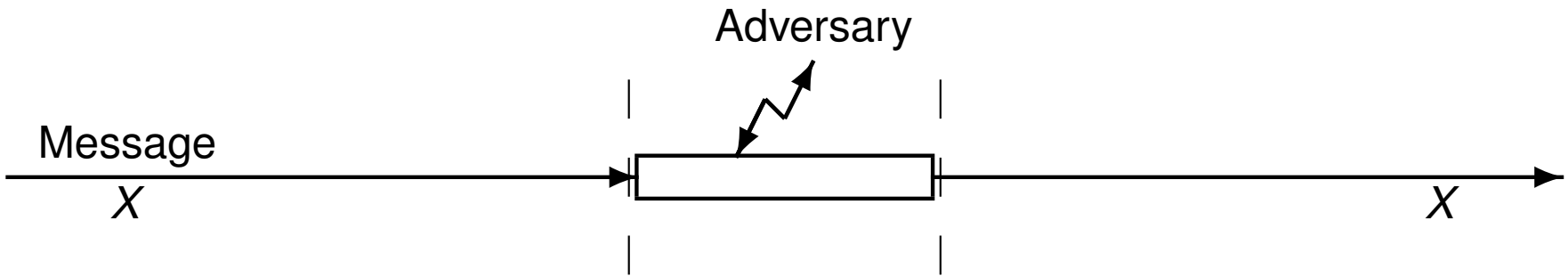


$$f_t \approx 10^9 \times 10^{\frac{5}{30\ \text{ans}}(t-2005)} \times \text{cste}$$

Petit calcul (blasphématoire)

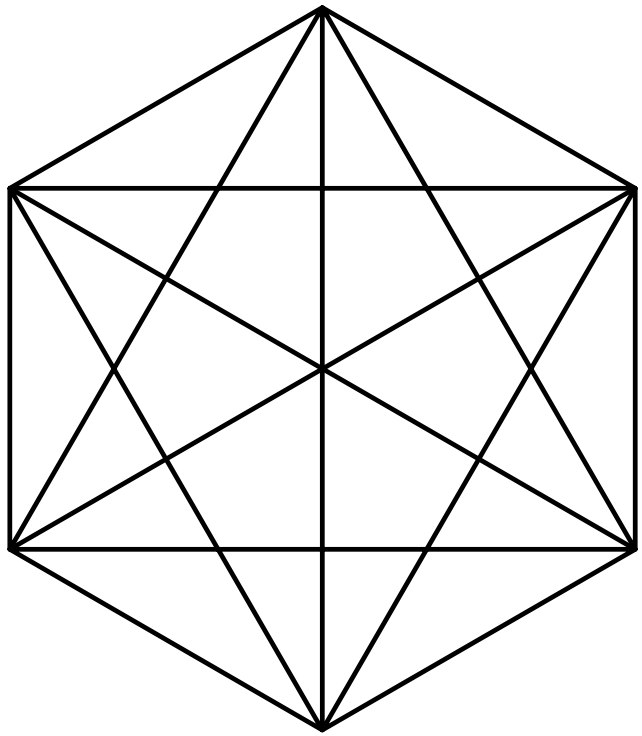
- Dieu cherche à casser des clefs de 128 bits
- en 2007, un PC standard permet de tester 1 000 000 clefs par seconde
- pour y parvenir en 15 milliards d'années, il faut 720 000 milliards de PCs version 2007
- si la loi de Moore maintient le cap, dans 162 ans, un seul PC y parviendra en une seconde
- mieux vaut donc créer le Big Bang et prendre **15 milliards + 162 années de vacances** pour résoudre le problème en une seconde!
- est-ce la fin du monde dans 158 ans?

Vers un canal de communication sécurisé

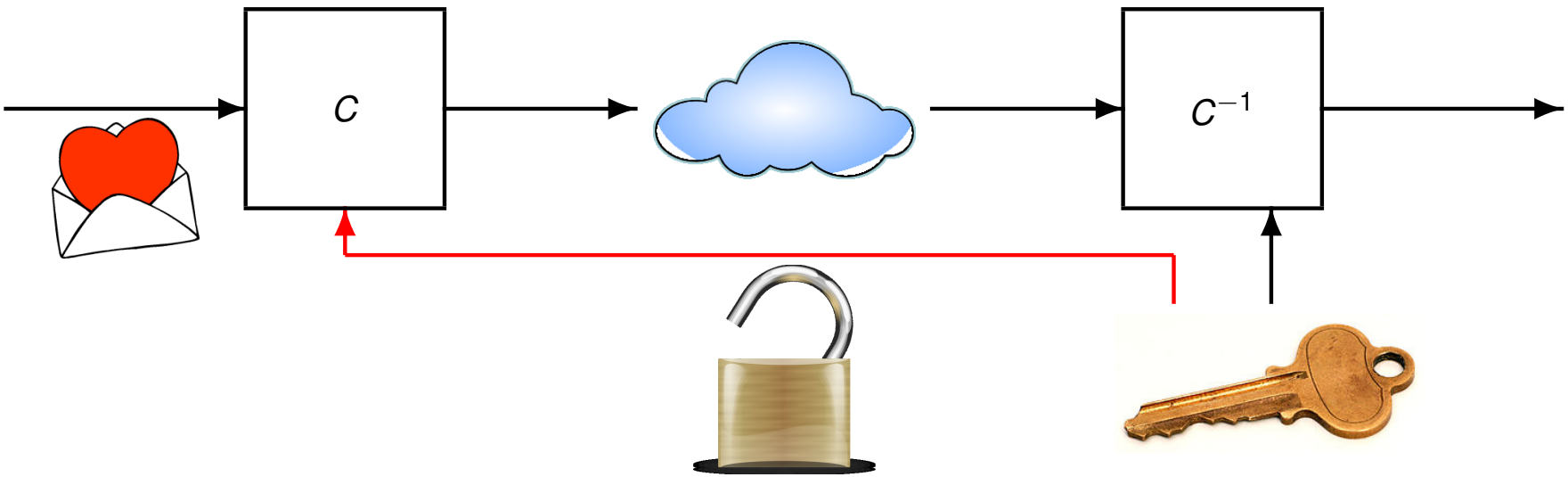


- **confidentialité**: seul le destinataire légitime reçoit le message
- **intégrité**: le message n'est pas modifié durant la transmission
- **authenticité**: le message provient bien de l'expéditeur supposé
- **fraîcheur**: le message est nouveau
- **disponibilité**: le message sera inévitablement délivré
- ...

Limitation de la cryptographie symétrique

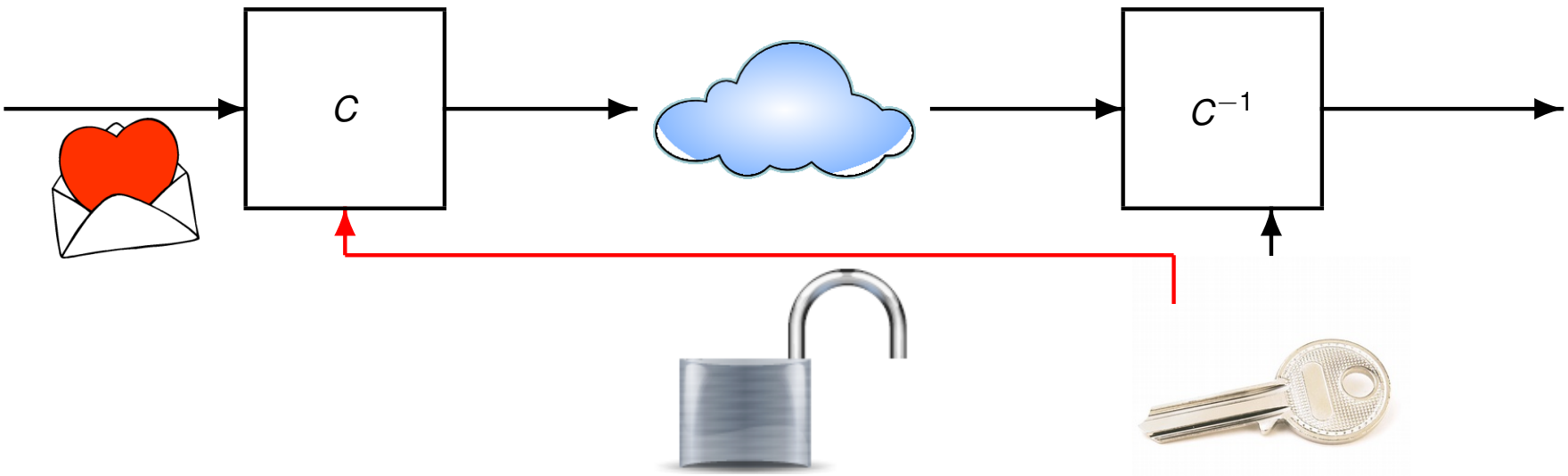


Chiffrement asymétrique



- clef publique (liée à l'identité): 
- clef secrète (privée): 

Attaque de l'intermédiaire

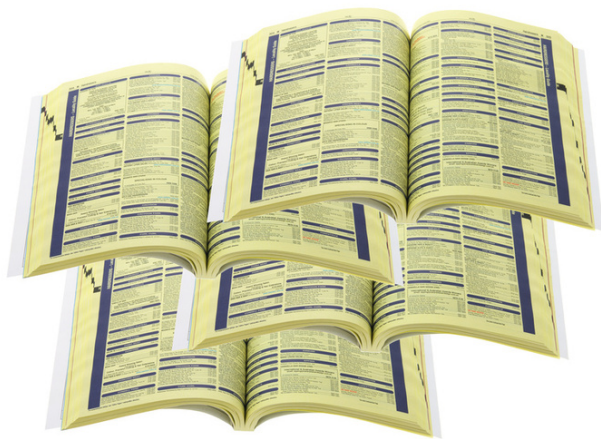


Dumbo se fait passer pour Nadia en transmettant une autre clef publique

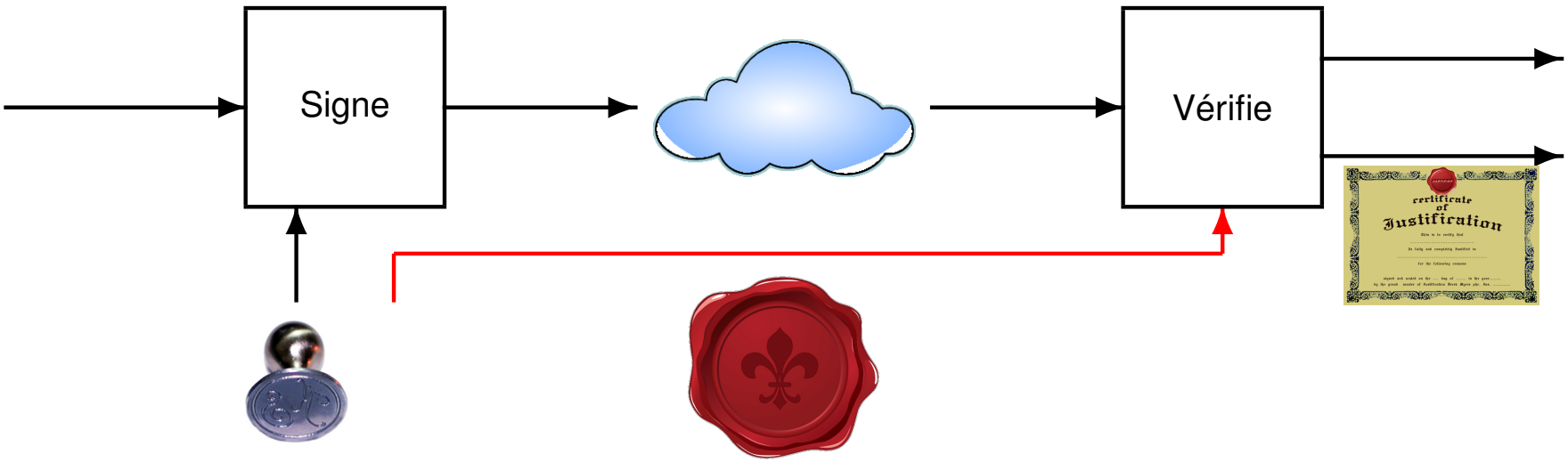
Lier une clef publique à une identité

il faut lier  à l'identité

il faut un répertoire fiable

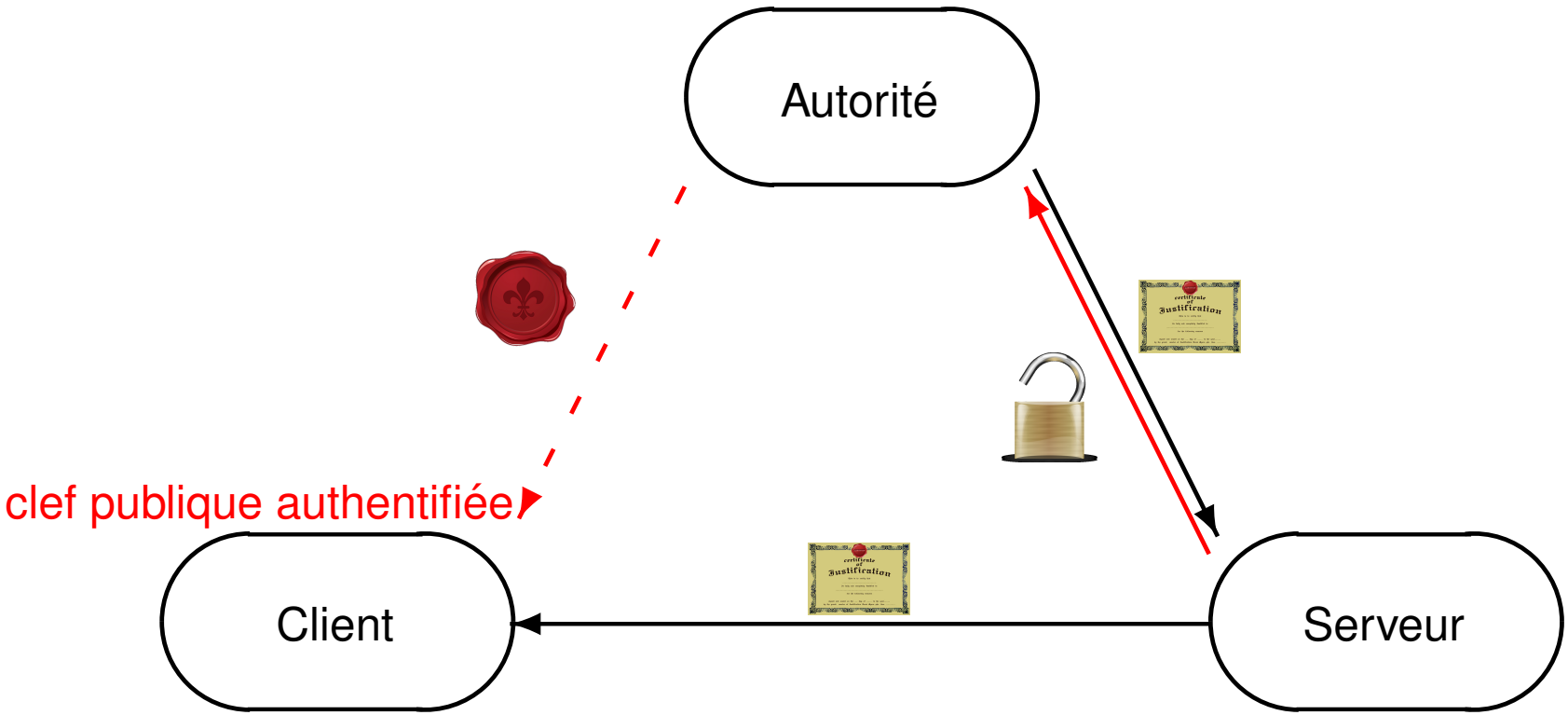


Signature numérique



- clef publique (autorité):
- clef secrète:
- certificat:

Infrastructure à clef publique



Deux familles d'algorithmes à clef publique

Famille RSA

- quasi-partout
- pb de la factorisation

Famille Diffie-Hellman

- accepte les courbes elliptiques
- pb du logarithme discret

La factorisation

RSA200

= 27997833911221327870829467638722601621070446786955428537560009929326128400107609345671052955360856061822351910951365788637105954482006576775098580557613579098734950144178863178946295187237869221823983

= 35324619344027701212726049781984643686711974001976250236493034687761212536794232000585479565280883491521353814093047401854675678728181521353814093047401854675

factorisé en 2005

Logarithme discret

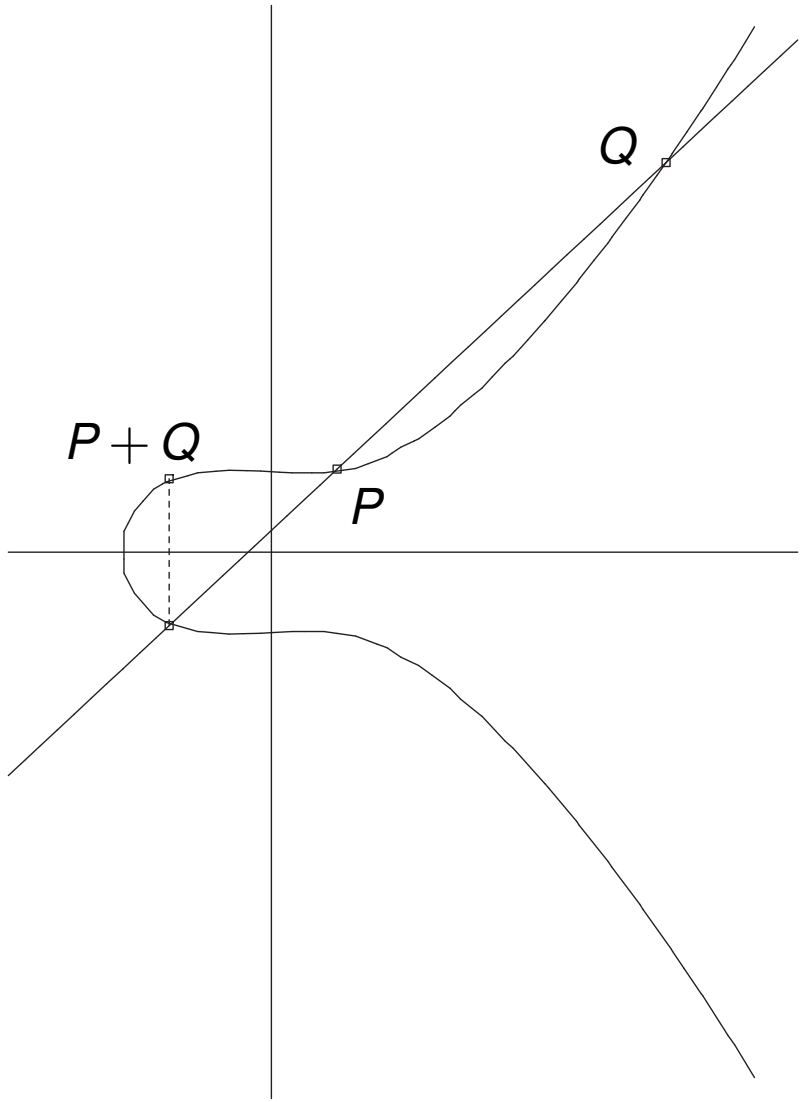
dans une structure de groupe

- paramètre standard: G
- clef publique: Q

trouver un entier d tel que

$$Q = dG$$

Courbe elliptique



Menace quantique

Théorème

Avec un ordinateur quantique, ces problèmes se résolvent très simplement!

Les causes de chute de sécurité

- la loi de Moore (chute gracieuse)
- des avancées algorithmiques (chute brutale)
  exemple: progrès dans la factorisation, collisions de MD5
- cas particuliers
  exemple: RSA avec clef courte, courbe elliptique de trace 1
- l'ordinateur quantique
- découverte de mauvaises implémentations (chute brutale)
  exemple: mauvais générateur pseudo-aléatoire (Debian, PS3), GPG
- effets de bord (chute brutale)
  mesure de courant, mesure de champs

Le Zoo symétrique

- **faune**: ARMADILLO BEAR BLOWFISH DRAGON FOX FROG LION MOSQUITO RABBIT SERPENT SHACAL SHARK TWOFISH
- **flore**: CAMELLIA LILY SEED
- **gastronomiques**: COCONUT GRANDCRU KFC MILENAGE PEANUT WALNUT
- **panthéon**: ANUBIS MARS KHAFRE KHUFU LUCIFER MICKEY SHANNON TURING
- **éléments**: CRYPTON ICE ICEBERG RAINBOW SNOW
- **les originaux**: ABC ACHTERBAHN AKELARRE CAST DEAL DECIM EDON FEAL FUBUKI GOST HELIX HIEROCRYPT IDEA KASUMI KATAN KHAZAD KTANTAN LEX LEVIATHAN LOKI MACGUFFIN MADRYGA MAGENTA MIR MISTY NIMBUS NOEKEON NUSH PHELIX PRESENT PY QUAD REDOC RIJNDAEL SAFER SALSA SCREAM SFINKS SKIPJACK SMS4 SQUARE SOBER SOSEMANUK XTEA 3-WAY YAMB
- **les pas inspirés**: A5 AES BMGL C2 CJCSG CMEA CS-CIPHER DES DFC E0 E2 FCSR HPC MMB Q RC2 RC4 RC5 RC6 SC TSC WG

...en pratique

BLOWFISH

MILENAGE

IDEA

KASUMI

SAFER

A5 AES

DES E0 RC4

Le Zoo asymétrique

- **patronymiques**:
  Ajtai-Dwork Chor-Rivest Cramer-Shoup ElGamal
  Goldreich-Goldwasser-Halevi Diffie-Hellman McEliece
  Merkle-Hellman Niederreiter Okamoto-Uchiyama Paillier Rabin
  RSA Williams
- **originaux**:
  ACE C* CEILIDH DRAGON EPOC HFE HIME(R) NTRU PSEC
  SFLASH TCHO XTR
- **composés**:
  ECDH HECC LUCELG Rabin-SAEP RSA-OAEP

...en pratique

Diffie-Hellman

RSA

ECDH

RSA-OAEP

Algorithmes populaires

genre	nom	inventeur	développement
chiffrement symétrique	DES	IBM	1977
	RC4	Rivest	1987
	A5/1	GSM	1987
	AES	Daemen-Rijmen	2001
fonction de hachage	MD5	Rivest	1991
	SHA-1	NIST	1993
code d'authentification	HMAC	Bellare-Canetti-Krawczyk	1997
échange de clefs	DH	Diffie-Hellman	1976
chiffrement asymétrique	RSA	Rivest-Shamir-Adleman	1978
	ElGamal	ElGamal	1984
signature numérique	RSA	Rivest-Shamir-Adleman	1978
	DSA	NIST	1994
	ECDSA	Vanstone	1998

Manque de crypto-diversité

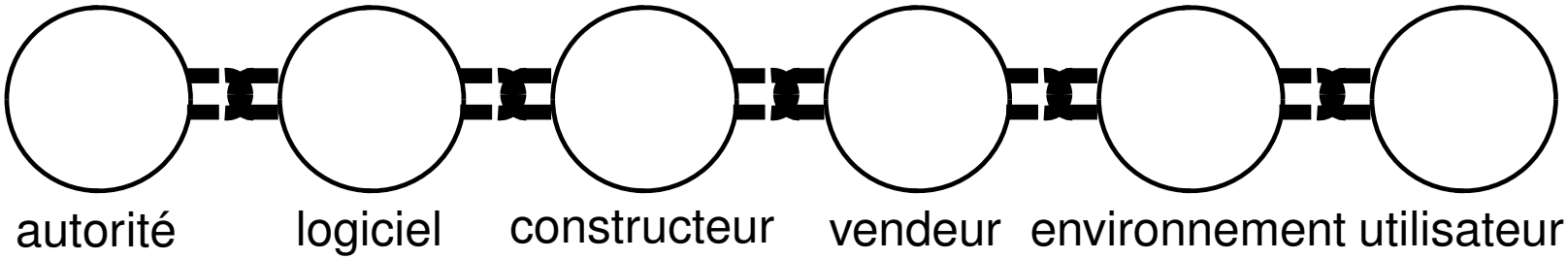
Standards de communication sans fils

- GSM
  pas de contrôle d'intégrité
  pas d'authentification du réseau
  pas d'*awareness* au niveau du chiffrement
  anonymat faible
  algorithmes cryptographiques faibles
- 3G
  pas d'authentification du réseau
- DECT
  algorithmes cryptographiques faibles
- WiFi
  WEP mort (attaque totale passive)
  WPA semble robuste
- Bluetooth
  pas de contrôle d'intégrité
  peu ergonomique, risque de mauvaise utilisation

Manque de maturité

[illustration de Chappatte]

La chaîne de confiance des PKI

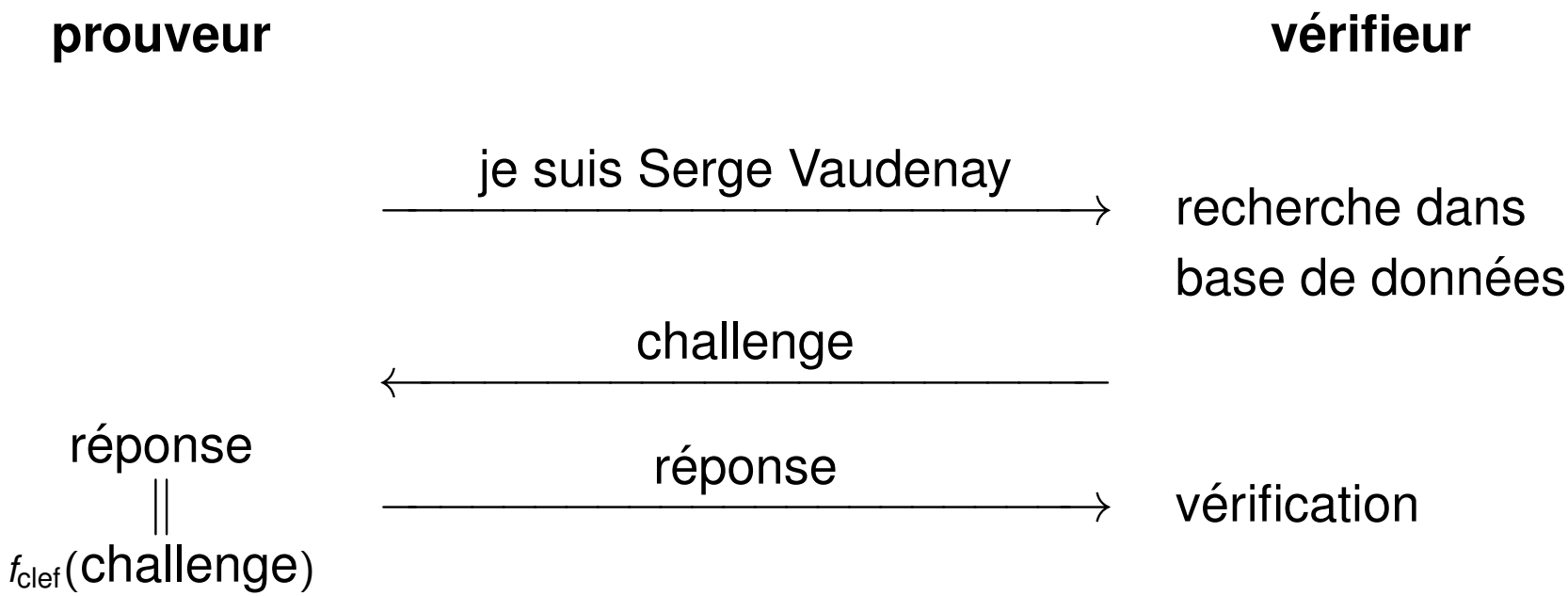


- les CAs doivent n'émettre que des certificats corrects
- les logiciels doivent inclure les bonnes clefs des CAs
- le matériel n'exécute que ce qu'il est supposé exécuter
- le vendeur ne doit pas introduire d'autre élément
- l'environnement doit rester sain
- l'utilisateur doit s'inquiéter des certificats invalides

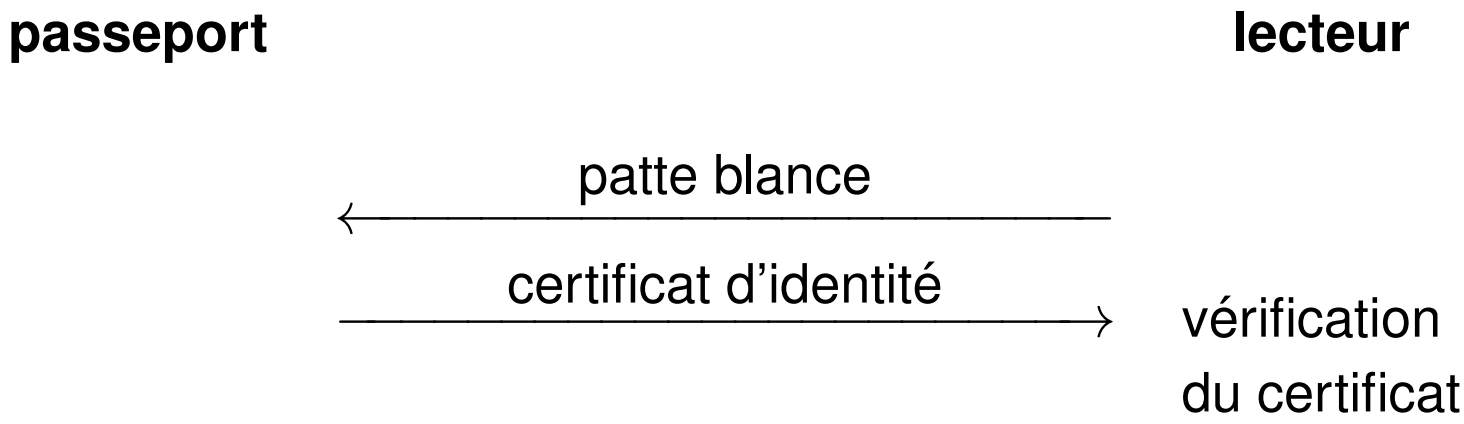
Aie confiance en moi

[illustration de Disney]

Comment se prouver soi-même



Preuve de l'identité



On a inventé la roue!

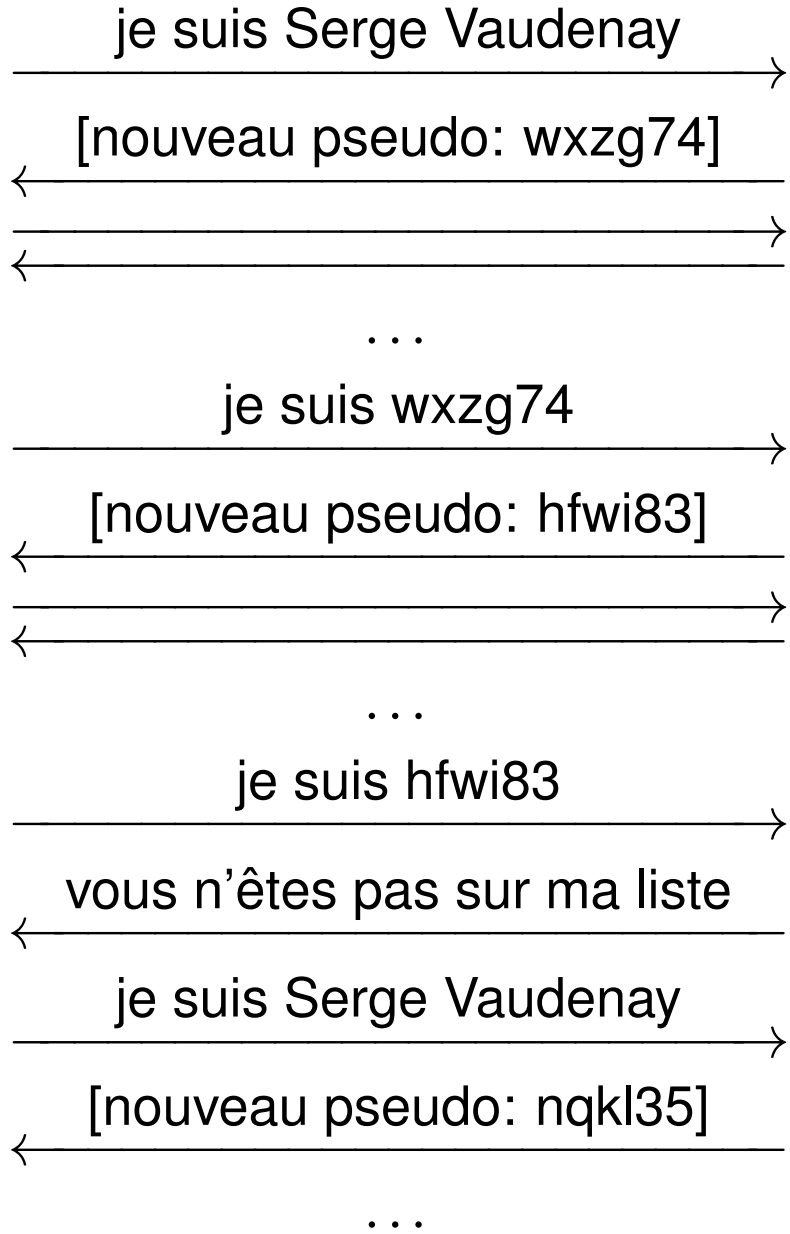
[illustration]

Protection de la sphère privée

Protection de la sphère privée

[illustration de Chappatte]

Un dialogue possible entre un téléphone et une antenne



La crypto dans la vraie vie

- très peu de diversité
- des standards faibles
- un best-of des années 80
- pas (ou peu) de protection de la sphère privée

Crypto-diversité

- **symétrique**:
  favoriser le développement d'(autres) algorithmes
  favoriser l'interchangeabilité des algorithmes
- **asymétrique**:
  recherche d'algorithmes "post-quantiques"
  quête du sacré Graal

Les nouvelles nouvelles technologies

[illustration de Chappatte]

Technologie dans les nuages

[illustration de Chappatte]

Sécurité dans les nuages

- calcul:
  chiffrement homomorphique
- bases de données:
  attribute-based encryption
- stockage:
  searchable encryption

La sphère privée, enfin?

Améliorer la composabilité

$$\text{sûr} + \text{sûr} \stackrel{?}{=} \text{sûr}$$

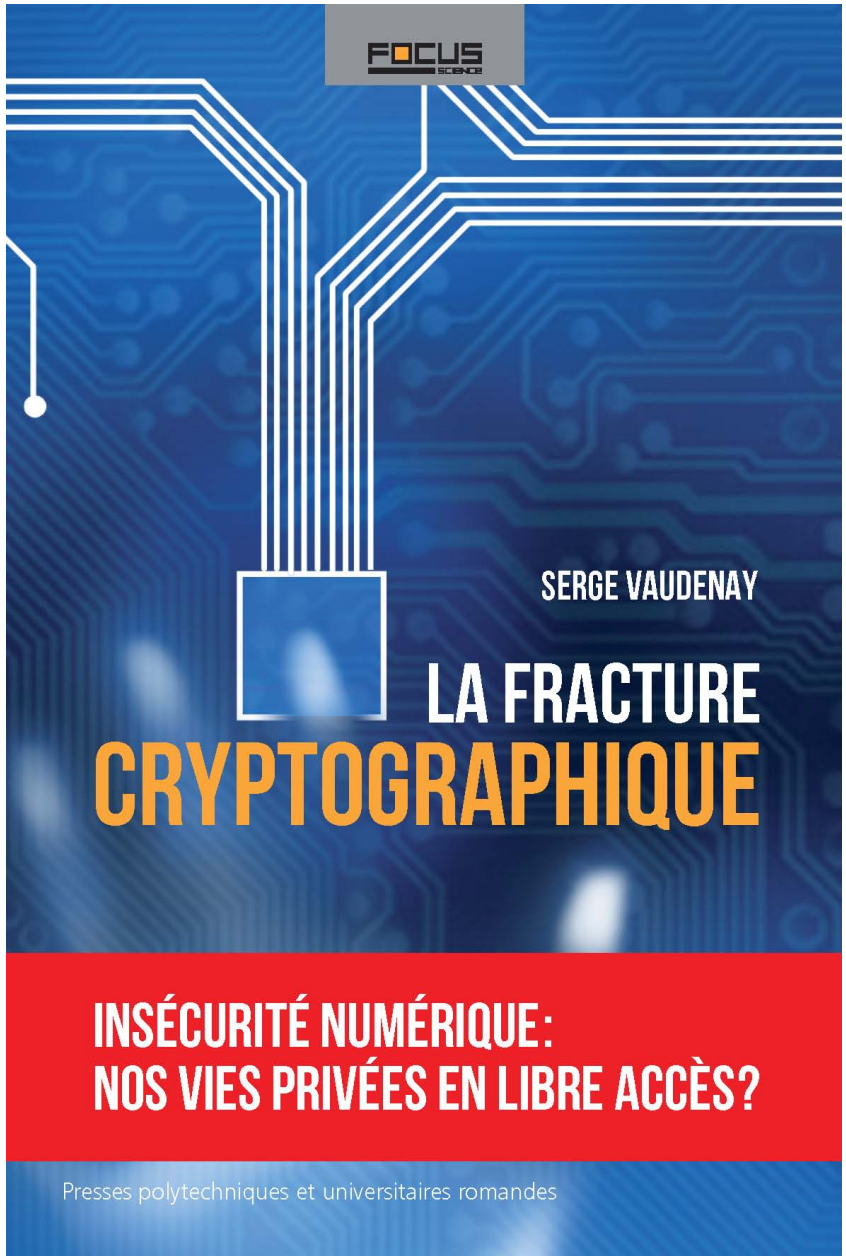
Confiance dans les preuves de sécurité

[illustration de Chappatte]

Mise en développement

- intégrer les algorithmes cryptographiques au faîte de l'état de l'art
- assumer les effets de bord
- assumer les chutes de sécurité (résilience)

Pub


FOCUS
SERGE VAUDENAY
LA FRACTURE
CRYPTOGRAPHIQUE
INSÉCURITÉ NUMÉRIQUE:
NOS VIES PRIVÉES EN LIBRE ACCÈS?
Presses polytechniques et universitaires romandes

Conclusion