Une brève histoire de la carte à puce

Pascal Lafourcade

LIMOS

UNIVERSITÉ Clermont Auvergne

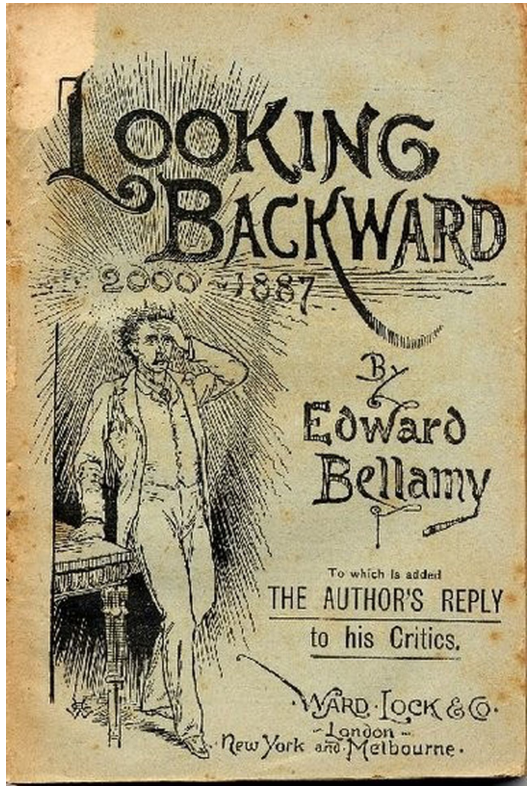
Mars 2023

Plan

- Histoire
- Technologie
- Attaques
  - Yes Card
  - Side channels (Canaux cachés)
  - Injection de fautes
- Application IOT : Distance Bounding
- Conclusion

1887 “Looking Backward”, de Edward Bellamy

Nouvelle utopique



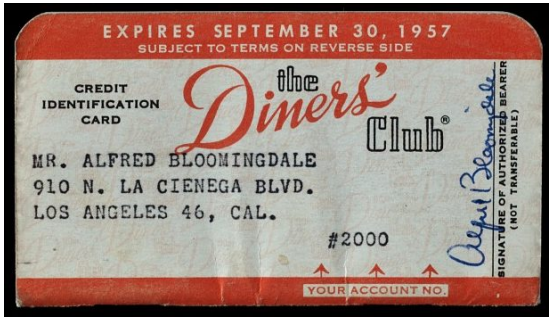
Introduction du terme “credit card” (11 occurrences)

1914 Western Union

Identification sur une plaque de métal, payement différé

1920 : Cartes de crédits pour des chaînes d'Hotels et de stations.

1950 Diner Club (USA)



- Plastic cards, payement différé avec intérêts

1951 American Express

1958 Carte Gold

1967 Carte Bleue (CB)

6 banques francaises

Numéro de CB : Algorithme de Luhn 10

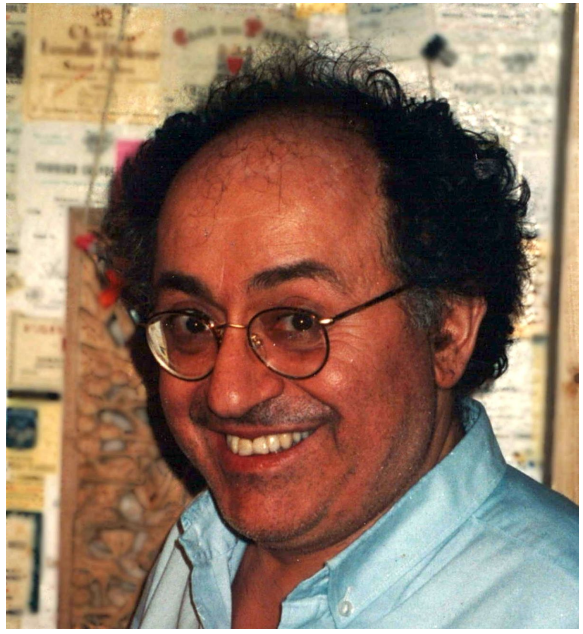
Numéro à 16 chiffres

$c_{15}c_{14}c_{13}c_{12} - c_{11}c_{10}c_9c_8 - c_7c_6c_5c_4 - c_3c_2c_1c_0$

Multiplier les chiffres d'indice impair par 2 (soustraire 9 si le nombre obtenu est supérieur à 9)

La somme de tous ces chiffres additionnés aux chiffres d'indice pair doit être un multiple de 10.

1974 Carte à puce, Roland Moreno



25 mars 1974, Brevet 74.10191 (INNOVATRON)
Carte vitale, SIM, identité, TV, téléphone (1983 “Carte pyjama”)
1992 toutes les cartes bancaires françaises offrent des cartes à puces.

1977 Michel Ugon

- 1977, carte à microprocesseur (Motorola chip by BULL CP8, bi-puces)
- 1979, CII-Honeywell Bull et Motorola : une mémoire 2716 EPROM et un microprocesseur 8 bits Mostek 3870.
- 1981, le brevet SPOM (Self Programmable One Chip Microprocessor)

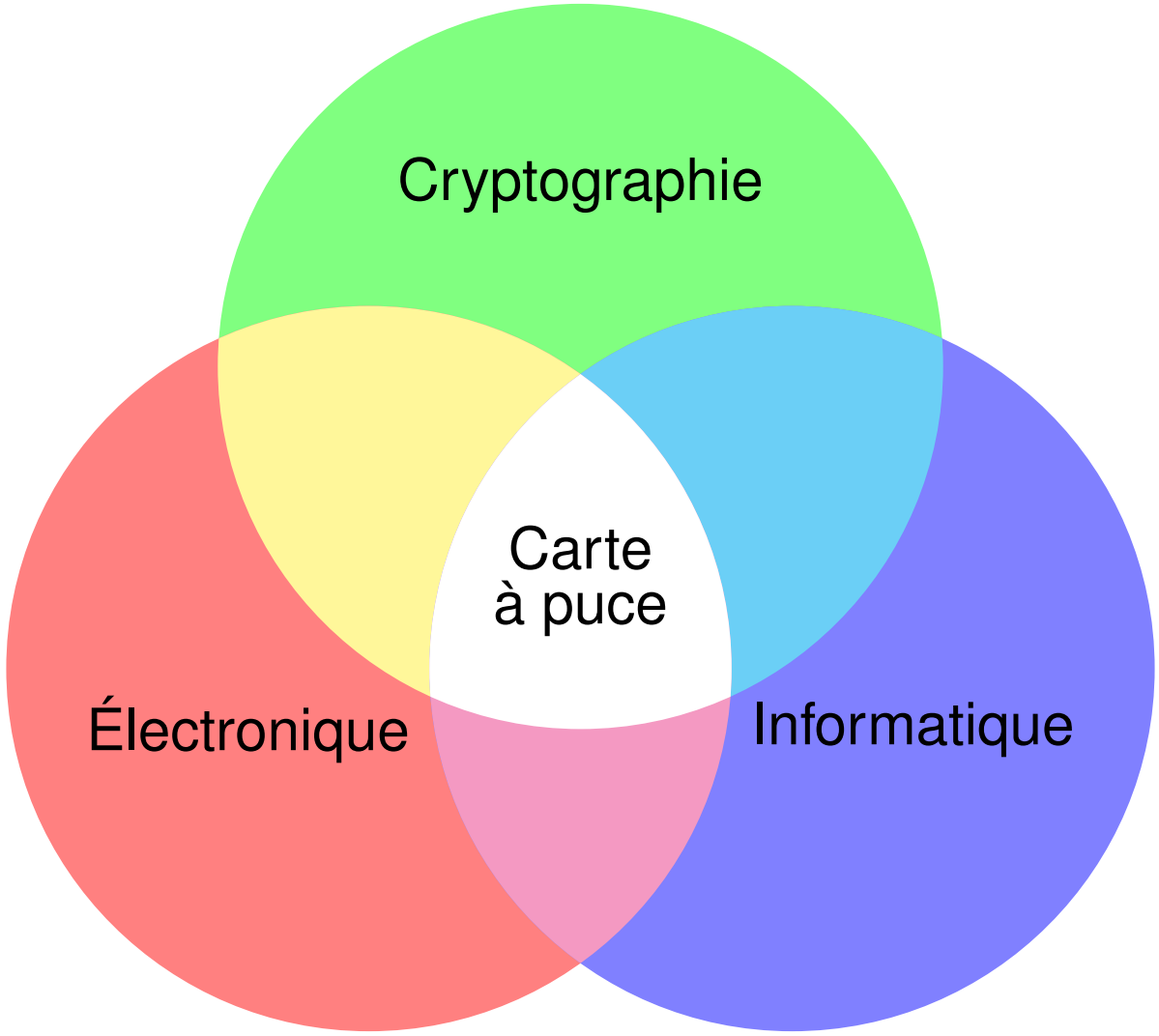
Historique

- 1974, Brevet de R.Moreno
- 1977, Brevet de M.Ugon
- 1987, Première norme ISO 7816
- 1988, Spécification de la carte SIM
- 1994, EMV
- 1995, Attaque DPA Paul Kocher
- 1997, Brevet Java Card, US 6,308,317
- 1989, First version of the GSM
- 2000, Windows for Smart Card
- 2002, dotnet smart card, Hiveminded
- 2013 NFC deployment
- 2016 eSE(apple pay, Samsung Pay)

Plan

- Histoire
- Technologie
- Attaques
  - Yes Card
  - Side channels (Canaux cachés)
  - Injection de fautes
- Application IOT : Distance Bounding
- Conclusion

Au carrefour des technologies



Exemples


carte d'assurance maladie
vitale
EMSE LE 04/09/2006


Union européenne
République française
PASSEPORT

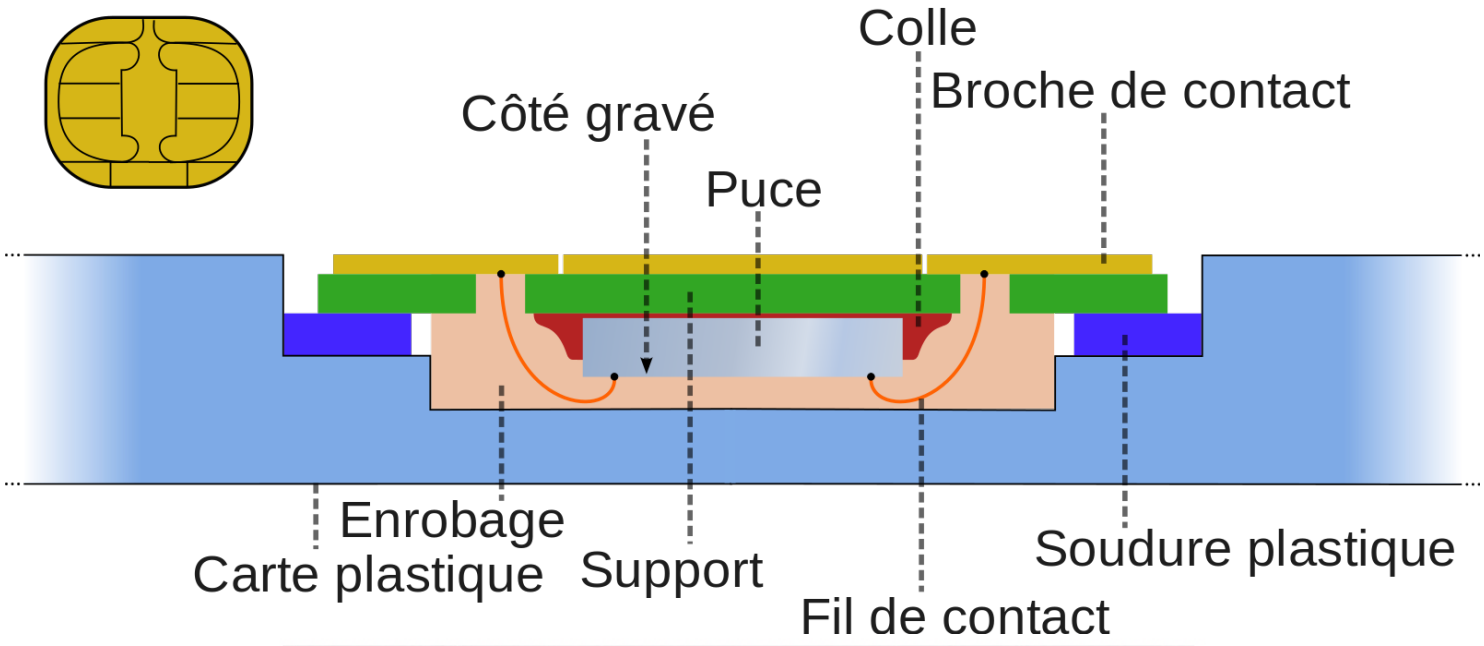

RÉPUBLIQUE FRANÇAISE
CARTE NATIONALE D'IDENTITÉ / IDENTITY CARD
MARTIN
Maëlys-Gaëlle, Marie
1,68 m
12 02 2020
RÉSIDENCE DU PLEIN AIR BÂT 4
33000 BORDEAUX
FRANCE
RÉPUBLIQUE FRANÇAISE
IDFRAX4RTBPFW46<<<<<<<<<<<<<<
9007138F3002119FRA<<<<<<<<<<<6
MARTIN<<MAELYS<GAELLE<MARIE<<<

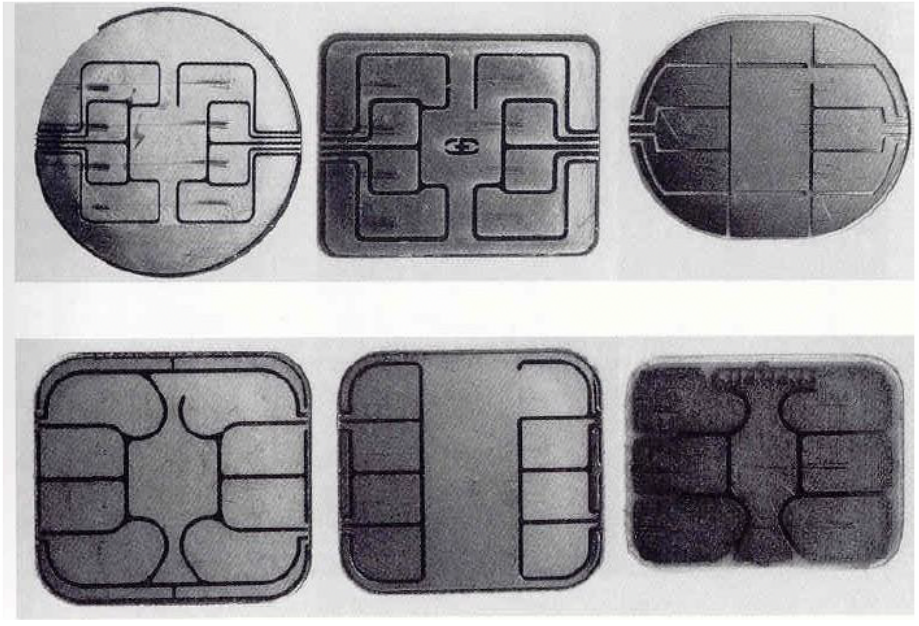

ABSA
VISA
MasterCard


nomi
mobile


VISA
Maestro
DEBIT CARD
VISA

Carte à puce


Colle
Broche de contact
Côté gravé
Puce
Enrobage
Carte plastique
Support
Fil de contact
Soudure plastique



3 Marchés principaux

Télécommunication (70 % des revenus)

Augmenter la pénétration des SIM

Services financiers (20% des revenus)

EMV migration

ID / Securité (10% des revenus)

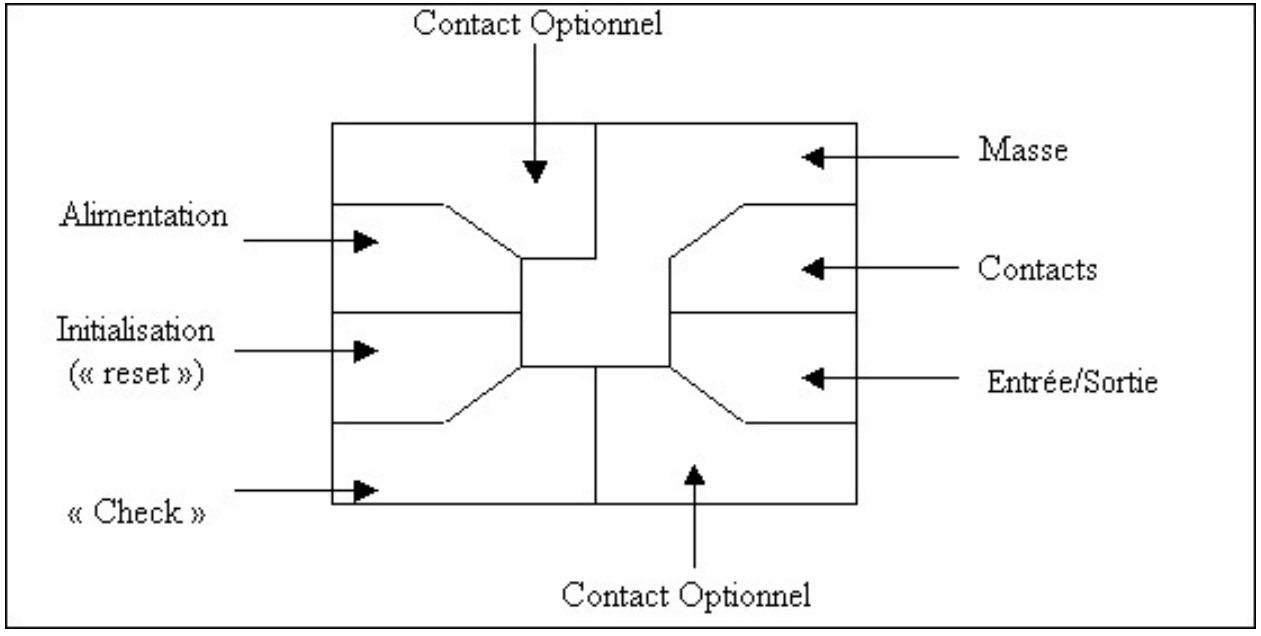
Émergence des nouveaux marchés

Les acteurs principaux

- Fabricants de Smart Card : gemalto a Thales company, inside secure, Giesecke+Devrient
- Vendeurs de circuits intégrés : Infineon technologies, NXP, Atmel, ST, HITACHI, SAMSUNG
- Consortium industriel : simalliance, JAVA CARD Forum, Wi Fi ALLIANCE
- Vendeurs d'appareils : SAMSUNG, Apple
- Développeurs d'applications : Thales-DIS (Gemalto), Idemia (Oberthur Technologies + Sagem-Morpho)
- Autorités de normes et de certifications : ANSSI, ETSI, ISO ...
- Utilisateurs : télécommunications, banques, gouvernements
- Autres : Centre d'Évaluation de Sécurité

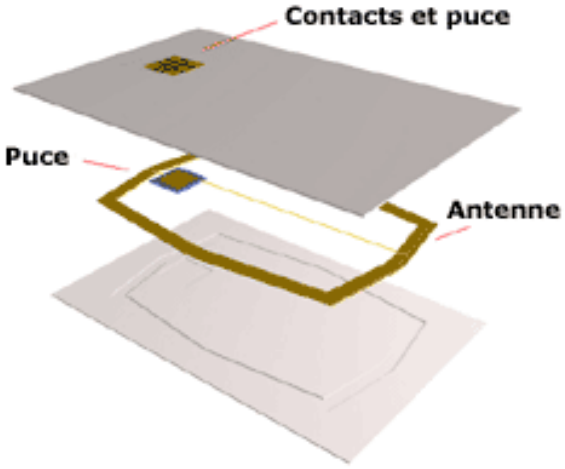
Norme ISO 7816

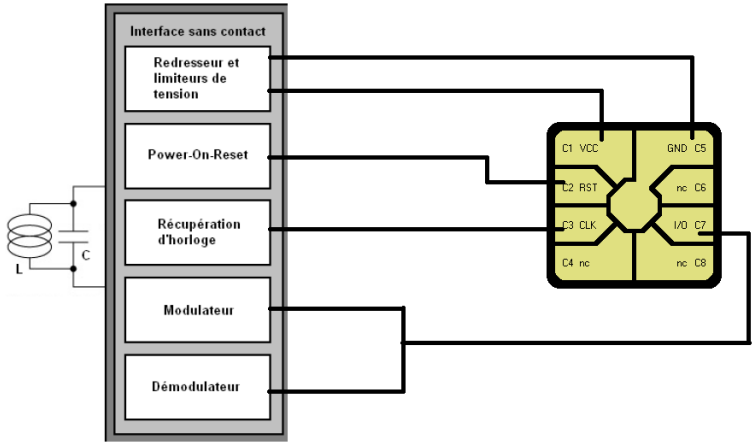
Taille : $85mm \times 54mm \times 0.76mm$



Communication half-duplex, asynchrone, sans horloge.
Format des données APDU (Application Programming Data Units)

Sans contact





La genèse NFC

- 1994, Mifare 1K
- 2001, Standards ISO 14443 (13,56 Mhz) : Type A (Mifare) et Type B
- Mifare (NXP), ISO14443A, ISO14443B, Felica (Sony)

3 modes fonctionnels :

- Reader/Writer
- Card Emulation
- Peer to Peer

En 2011, Mifare représente 70 % du marché du transport

Trusted Platform Module - TPM 2006

Trusted Computing Group, TPM 2.0 en 2014

Atmel, Broadcom, Infineon, Intel, Nuvoton (anciennement Winbond), Sinosun et STMicroelectronics

Trusted execution environment ARM sous la marque TrustZone.

Plan

- Histoire
- Technologie
- Attaques
  - Yes Card
  - Side channels (Canaux cachés)
  - Injection de fautes
- Application IOT : Distance Bounding
- Conclusion

Yes Card

1997, Serge Humpich casse la clé privée RSA de 320 bits.

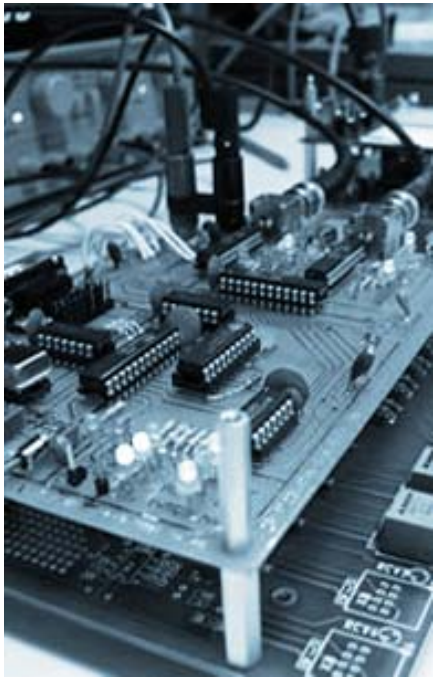
Création de cartes acceptées par tous terminaux
$\Rightarrow$ 10 mois de prison

Exemple du Digicode

- Digicode avec 10 nombres possibles (0..9)
- Un code composé de 4 nombres
- A chaque erreur d'un chiffre une lumière rouge s'allume sinon une lumière verte s'allume.

Combien d'essais sont nécessaires pour ouvrir la porte protégée avec ce digicode ?

Differents types de Canaux Cachés



But obtenir des informations sur un secret ou une clé par l'observation :

- Temps
- Énergie
- Cache
- Émission électromagnetique ...

Timing Attacks on Implementations of Diffie–Hellman, RSA, DSS, and Other System... Paul Kocher - CRYPTO - 1996

Code Pin à l'épreuve du temps

Pour un 8 bytes code PIN, il y a $(2^8)^8 = 256^8$ possibilités par attaque par Brute Force.

Programme

```
for ( i = 0 ; i <= 7; i++)
      if ( pinCarte[i] != pinPresente[i] )
         return false;
return true ;
```

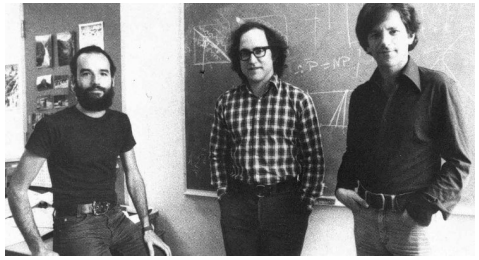
Combien faut-il d'essais pour trouver le code PIN vérifé par ce programme ?

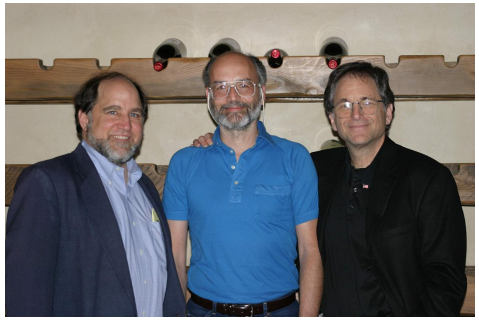
Code correct

Program

```
boolean test = true ;
for ( i = 0 ; i <= 7; i++)
    test = test && ( pinCarte[i] == pinPresente[i])
return test ;
```

Rivest Shamir Adelmann (RSA 1978)





Soit $n = pq$, p et q deux nombres premiers.

Clé Publique : (e, n)

Clé Secrète : d où $d = e^{-1} \mod \phi(n)$
et $pgcd(e, \phi(n)) = 1$

Chiffrement : $c = m^e \mod n$

Déchiffrement: $m = c^d \mod n$

Correction

$c^d = m^{de} = m.m^{k\phi(n)} \mod n$

Rappel : Théorème d'Euler $\forall x \in (Z/nZ)^*, x^{\phi(n)} = 1 \mod n$

Calcul naïf

```
def expo(n,p,x):
    res = 1
    for i in range(n) :
        res = res * x % p
    return res
```

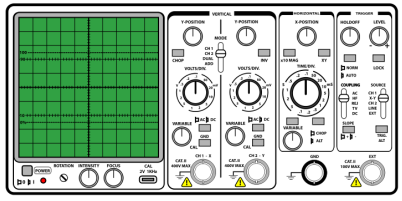
Exponentielle rapide

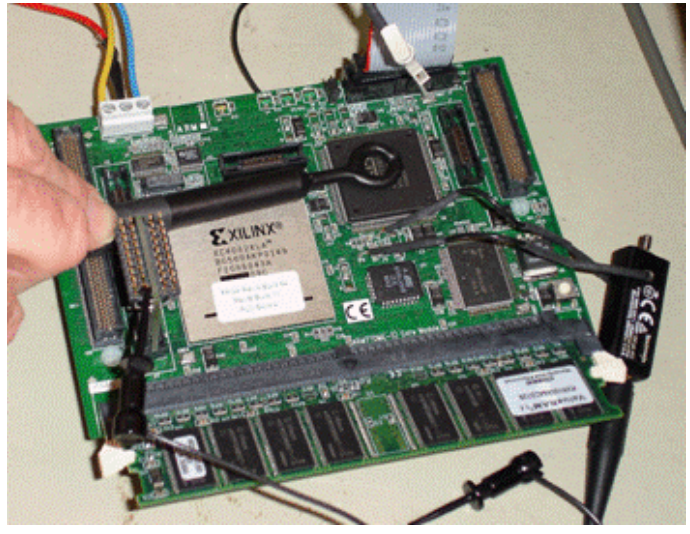
L'algorithme d'**exponentielle rapide** calcule plus vite $x^n \bmod p$

$$\text{expo}(x, n, p) =$$

$$\begin{cases} 1, & \text{si } n = 0 \\ \text{expo}(x^2 \bmod p,\ n/2, p), & \text{si } n \text{ est pair} \\ x \times \text{expo}(x^2 \bmod p,\ (n-1)/2, p) \bmod p, & \text{si n est impair} \end{cases}$$

Messurer la consommation électrique



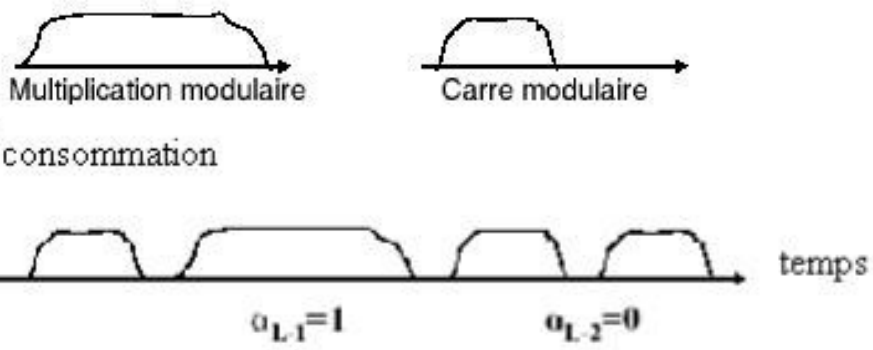


Attaque par consommation électrique sur le déchiffrement de RSA

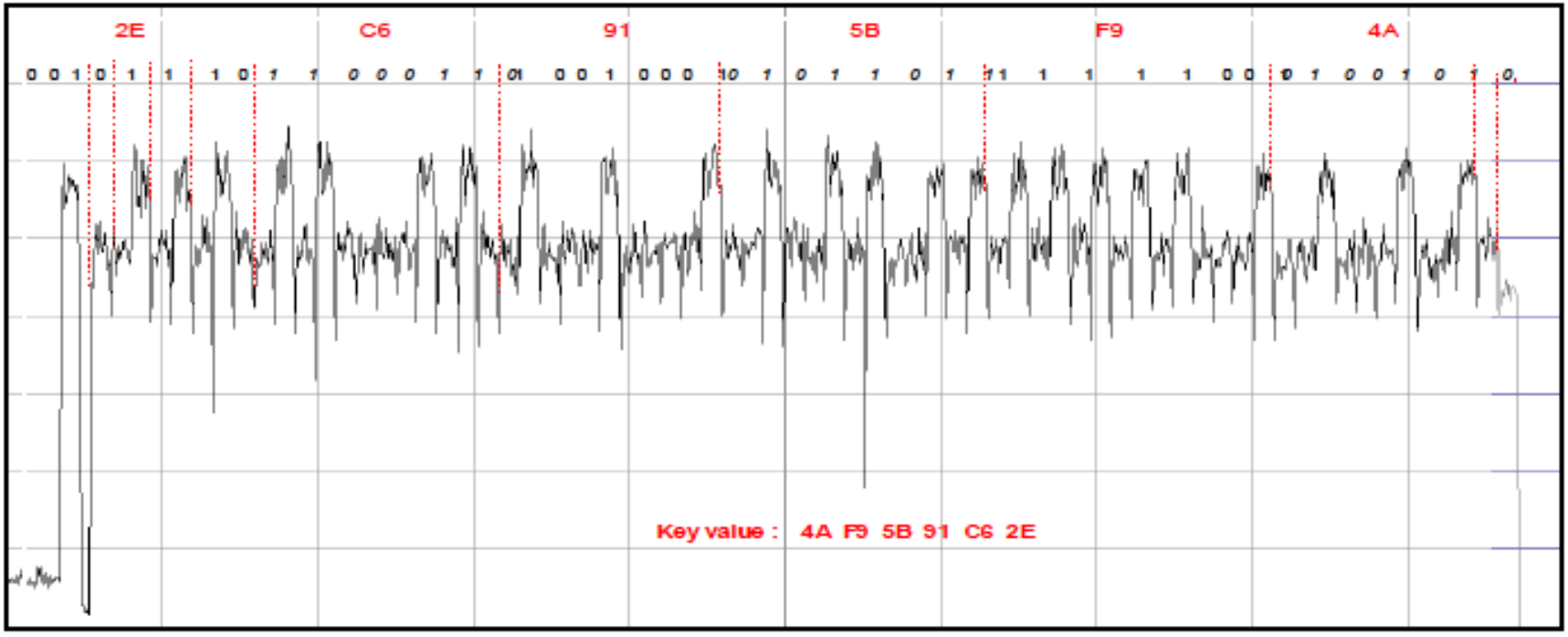
Pour déchiffrer, il faut calculer $y^d \bmod n$, où y est le chiffré, n est public et d est la clé secrète.

Programme d'exponentielle rapide

```
s = 1 ;
for ( i = L-1 ; i >= 0; i --) {
      s = s*s mod n ;
      if ( d [ i ] == 1)
            s = s*y mod n ;
}
return s
```

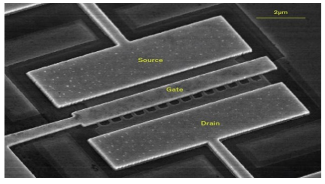


In reality



PIN injection test

Glitch, sur la variable `status`




```
procedure VERIFY PIN(candidate PIN V)
status = COMPARISON(U,V)
if status = TRUE then
    Perform transaction
else
    Halt
end if
return
```

Attaques

Température : Apple Coldgate!

- Préparation : d'aucune à une décapsulation
- Contremesures : Température du capteur

Clock glitches

- Préparation : Aucune
- Contremesures : Utiliser une horologe interne

Voltage glitches

- Préparation : d'aucune à ôter les protections
- Contremesures : Régulateur de voltage

Rappel : Théorème des restes Chinois

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$$

Soient $n_1, \ldots, n_k$ des entiers deux à deux premiers entre eux, c'est-à-dire que $PGCD(n_i, n_j) = 1$ lorsque $i \neq j$. Alors pour tous entiers $a_1, \ldots, a_k$, il existe un entier x, unique modulo $n = \prod_{i=1}^{k} n_i$, tel que :

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ &\ldots \\ x &\equiv a_k \pmod{n_k} \end{aligned}$$

$$x = \sum_{i=1}^{i=n} a_i \times e_i$$

Où, $e_i = \frac{n}{n_i} \times ((\frac{n}{n_i})^{-1} \mod n_i)$

Utilisé pour RSA et dans l'algorithme de Silver-Pohlig-Hellman pour le calcul du logarithme discret.

Calculs rapides : 99, 98, 97

Remarques :

- $99 \times 98 \times 97 = 941094$
- 99, 98, 97 sont premiers entre eux.

Calculer

$x = a_1 \mod 99$

$x = a_2 \mod 98 \Rightarrow (a_1, a_2, a_3)$

$x = a_3 \mod 97$

et

$y = b_1 \mod 99$

$y = b_2 \mod 98 \Rightarrow (b_1, b_2, b_3)$

$y = b_3 \mod 97$

Puis calculer $(c_1, c_2, c_3) = (a_1 \times b_1, a_2 \times b_2, a_3 \times b_3)$

$x \times y = c_1 \mod 99$

$x \times y = c_2 \mod 98$

$x \times y = c_3 \mod 97$

Signature RSA-CRT

Rappel Signature RSA :
$\sigma = m^d \mod n$ où $sk = d$, $pk = (e, n)$, $n = pq$

Signature RSA-CRT

- Cacluler, $s_1 = m^d \mod p$ et $s_2 = m^d \mod q$
- Pré-calculer $a = q \times (q^{-1} \mod p)$ et $b = p \times (p^{-1} \mod q)$
- $m^d \mod n = a \times s_1 + b \times s_2$

Grâce au théorème des restes Chinois :

$$\begin{aligned} m^d \bmod n &= a \times s_1 + b \times s_2 \\ &= q \times (q^{-1} \bmod p) \times m^d \bmod p + \\ &\quad p \times (p^{-1} \bmod q) \times m^d \bmod q \\ &= m^d \bmod (p \times q) \\ &= m^d \bmod n \end{aligned}$$

Attaque de Bellcore, D.Boneh 1997

$$\sigma = m^d \bmod n = a \times s_1 + b \times s_2$$

$a = q \times (q^{-1} \bmod p)$ et $b = p \times (p^{-1} \bmod q)$

Injection de la faute sur s_1

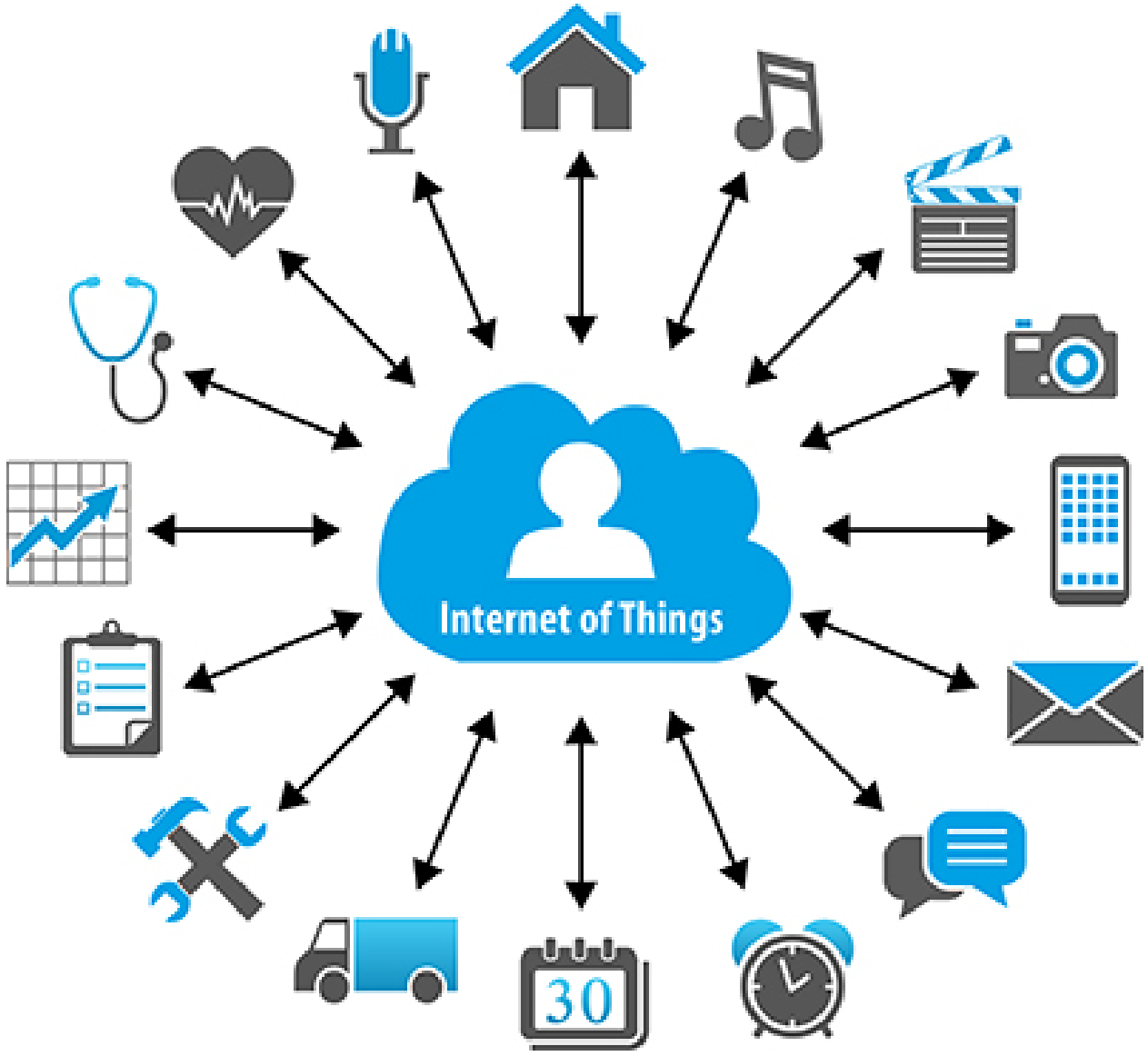
$$\sigma^* = a \times s_1^* + b \times s_2$$

Première observation : $\sigma \bmod q = b \times s_2 = \sigma^* \bmod q$
ainsi $\sigma - \sigma^* = 0 \bmod q$, donc q divise $\sigma - \sigma^*$.
Seconde observation : $\sigma \bmod p = a \times s_1 \neq \sigma^* \bmod p = a \times s_1^*$
donc $\sigma - \sigma^* \neq 0 \bmod p$
donc p ne divise pas $\sigma - \sigma^*$.
Ainsi : $pgcd(\sigma - \sigma^*, n = p \times q) = q$

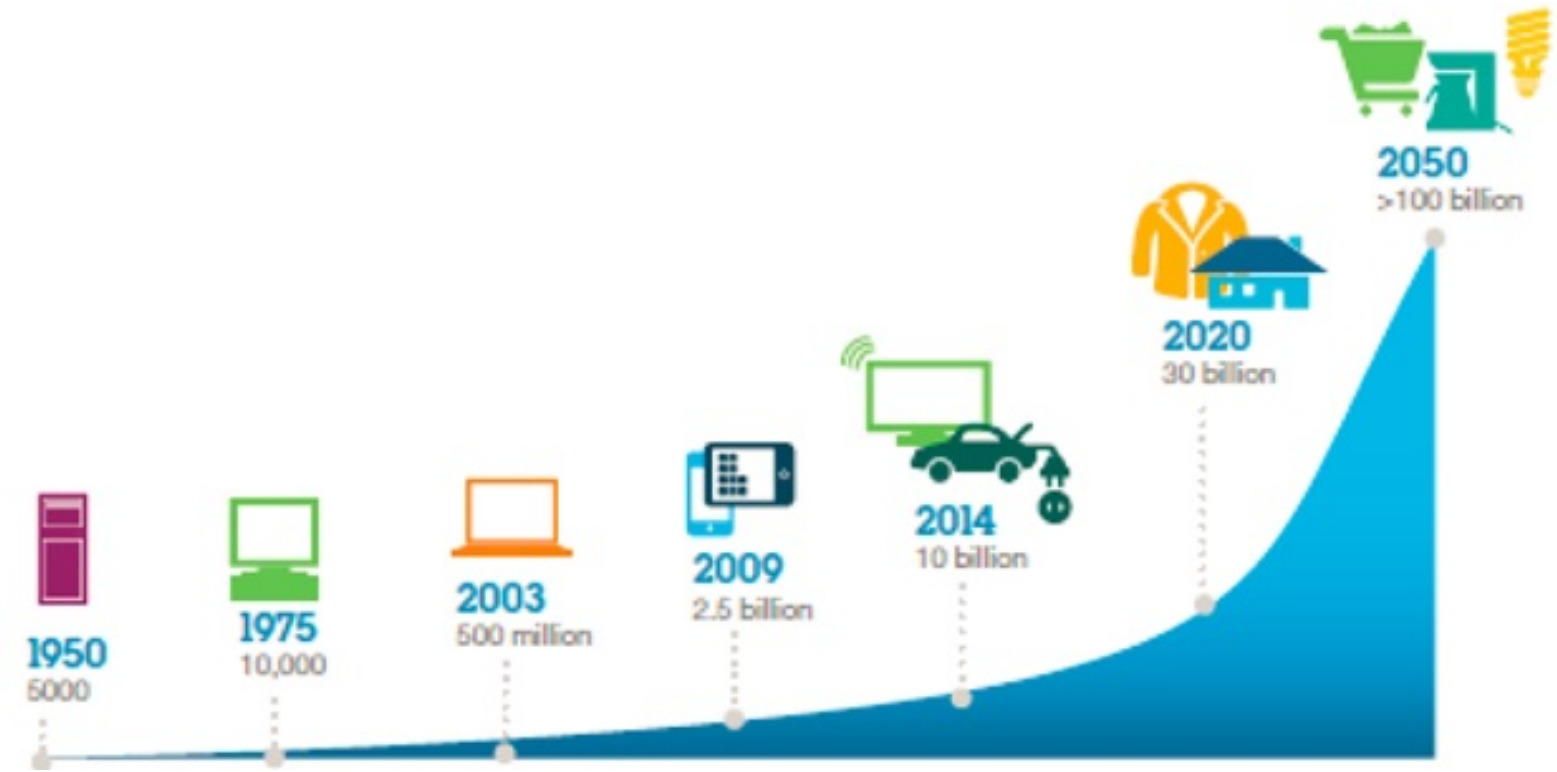
Plan

- Histoire
- Technologie
- Attaques
  - Yes Card
  - Side channels (Canaux cachés)
  - Injection de fautes
- Application IOT : Distance Bounding
- Conclusion

IoT



IoT


1950
5000
1975
10,000
2003
500 million
2009
2.5 billion
2014
10 billion
2020
30 billion
2050
>100 billion

Raison de ce succès

Usage

- Monitoring
- Hyperconnectivité
- Disponibilité
- Open data

Raison de ce succès

Usage

- Monitoring
- Hyperconnectivité
- Disponibilité
- Open data

Technologie

- Communications sans fils: Wifi, 3G, 4G, Bluethooth ...
- Batteries
- CPU
- Capteurs
- Prix

Raison de ce succès

Usage

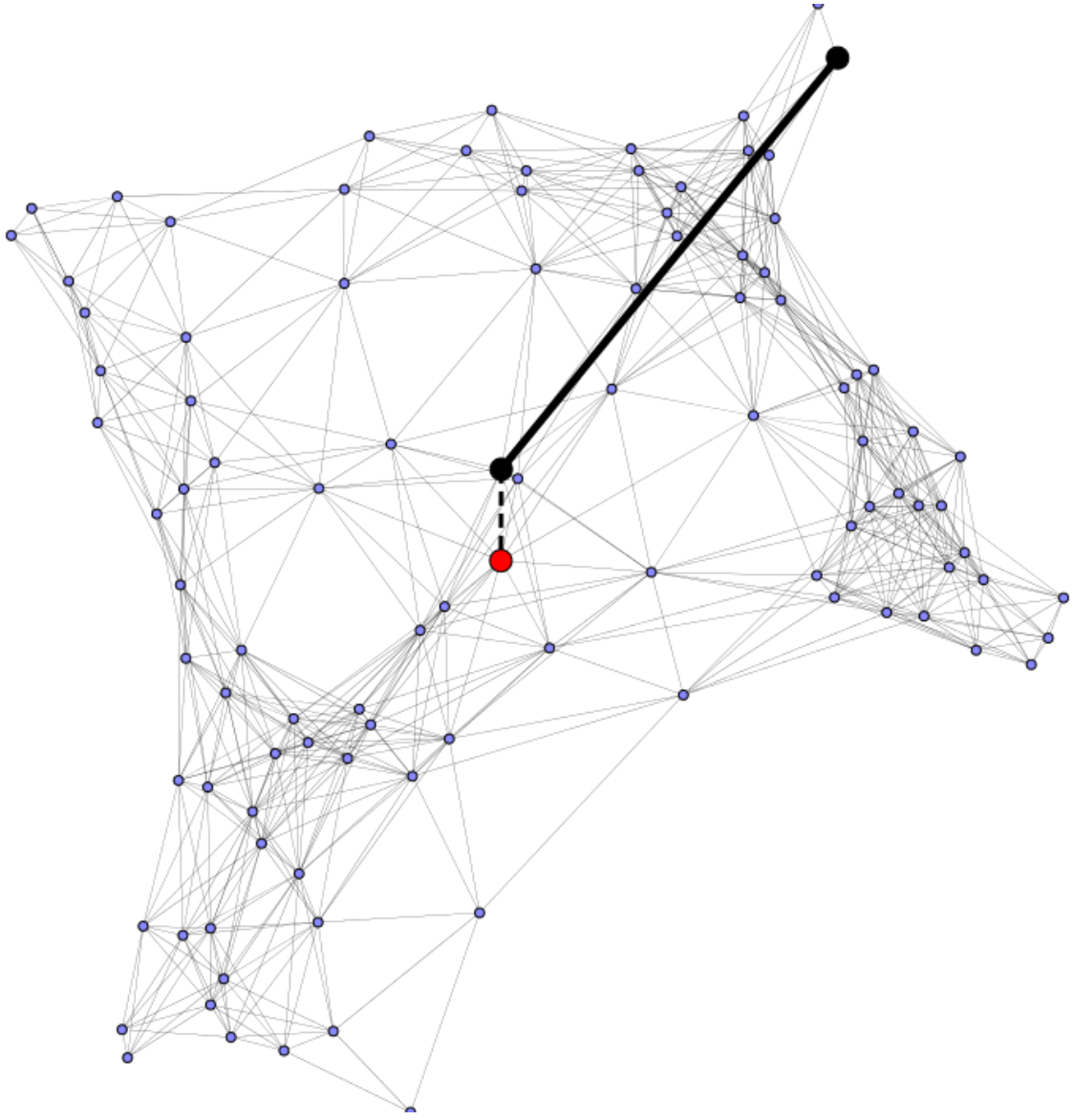
- Monitoring
- Hyperconnectivité
- Disponibilité Sécurité?
- Open data

Technologie

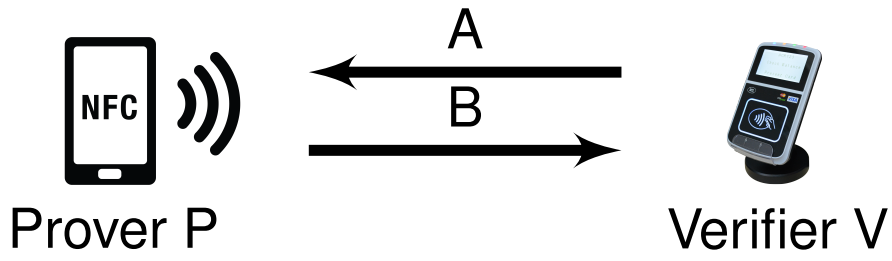
- Communications sans fils: Wifi, 3G, 4G, Bluethooth ...
- Batteries
- CPU
- Capteurs
- Prix

Ces objets sont partout

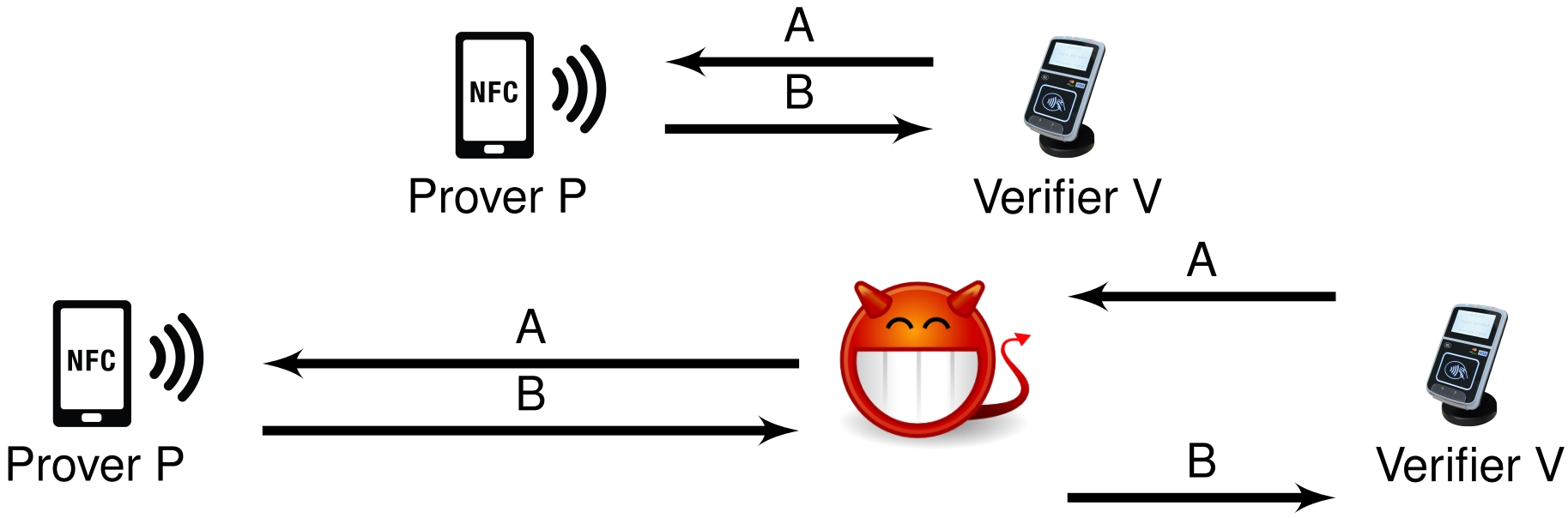
“Wormhole Attack”



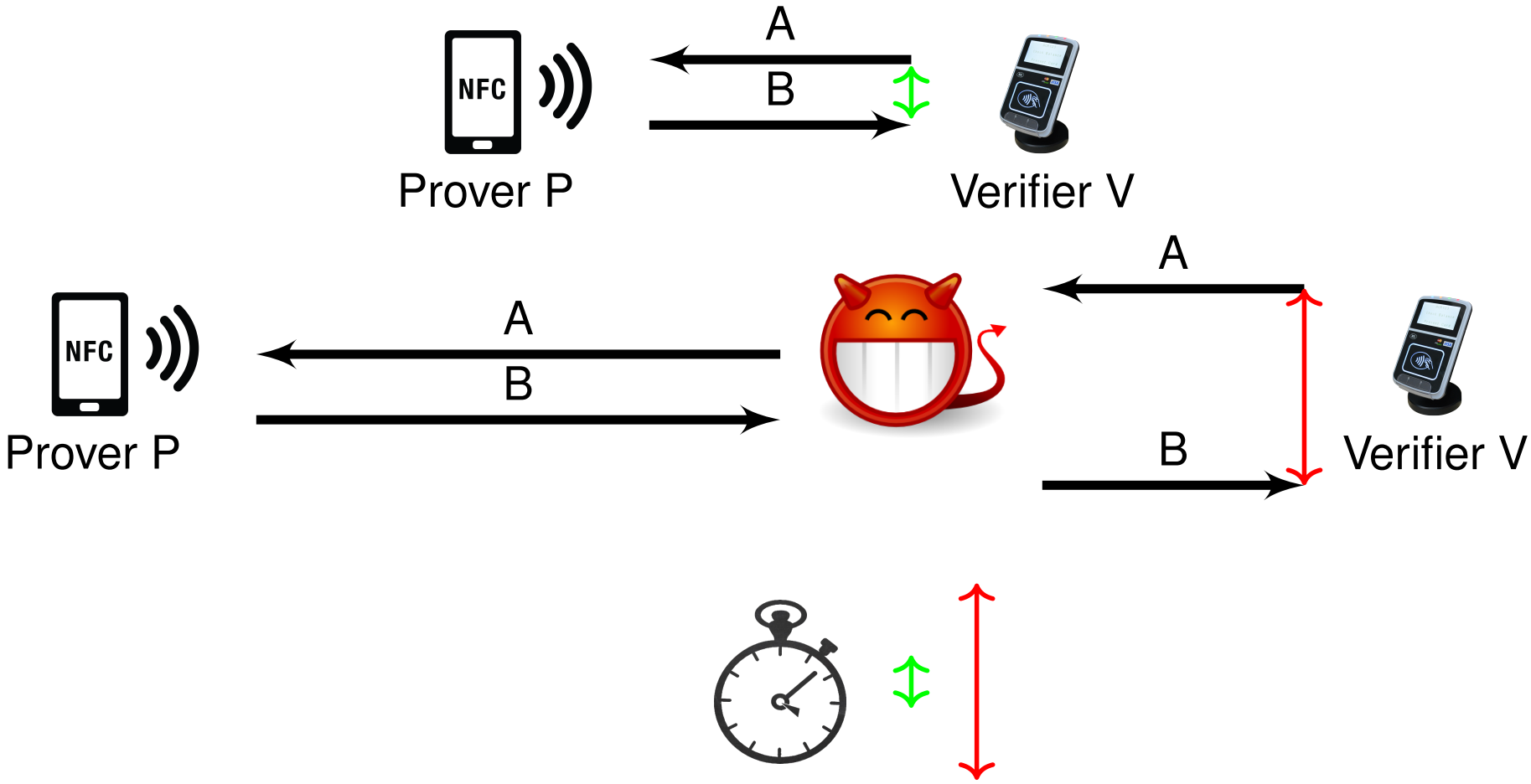
Distance Bounding Idée



Distance Bounding Idée

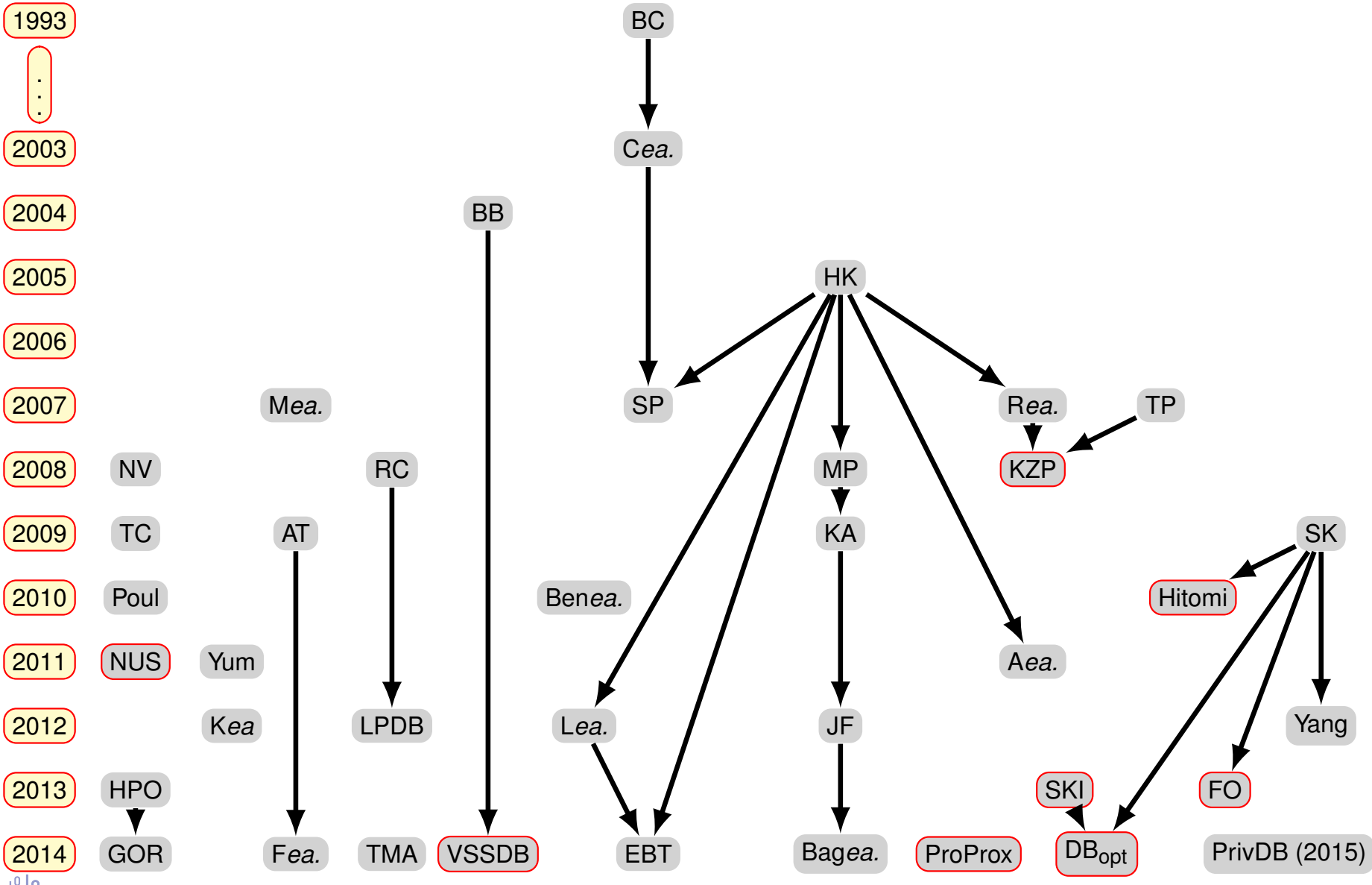


Distance Bounding Idée



Solution against MF: Distance Bounding (Brands and Chaum, 1991)

42 protocoles de 1993 à 2015.



Plan

- Histoire
- Technologie
- Attaques
  - Yes Card
  - Side channels (Canaux cachés)
  - Injection de fautes
- Application IOT : Distance Bounding
- Conclusion

Conclusion

- Les mathématiques sont aussi dans les cartes à puce
- Les attaquants sont puissants et créatifs
- Le diable se cache dans les détails

Thank you for your attention!

Questions?

pascal.lafourcade@uca.fr