AES side-channel countermeasure using random tower field constructions

Alexis Bonnecaze
Université de la Méditerranée, IML – ERISCS

Pierre Liardet
Université de Provence, LATP

Alexandre Venelli
Inside Secure

Crypto'Puces
09/05/2011

DRIVING TRUST inside SECURE

Sommaire

1. Attaques physiques
2. Rappels AES et contre-mesures DPA
3. Notre proposition
4. Conclusion

Sommaire

1. Attaques physiques
2. Rappels AES et contre-mesures DPA
3. Notre proposition
4. Conclusion

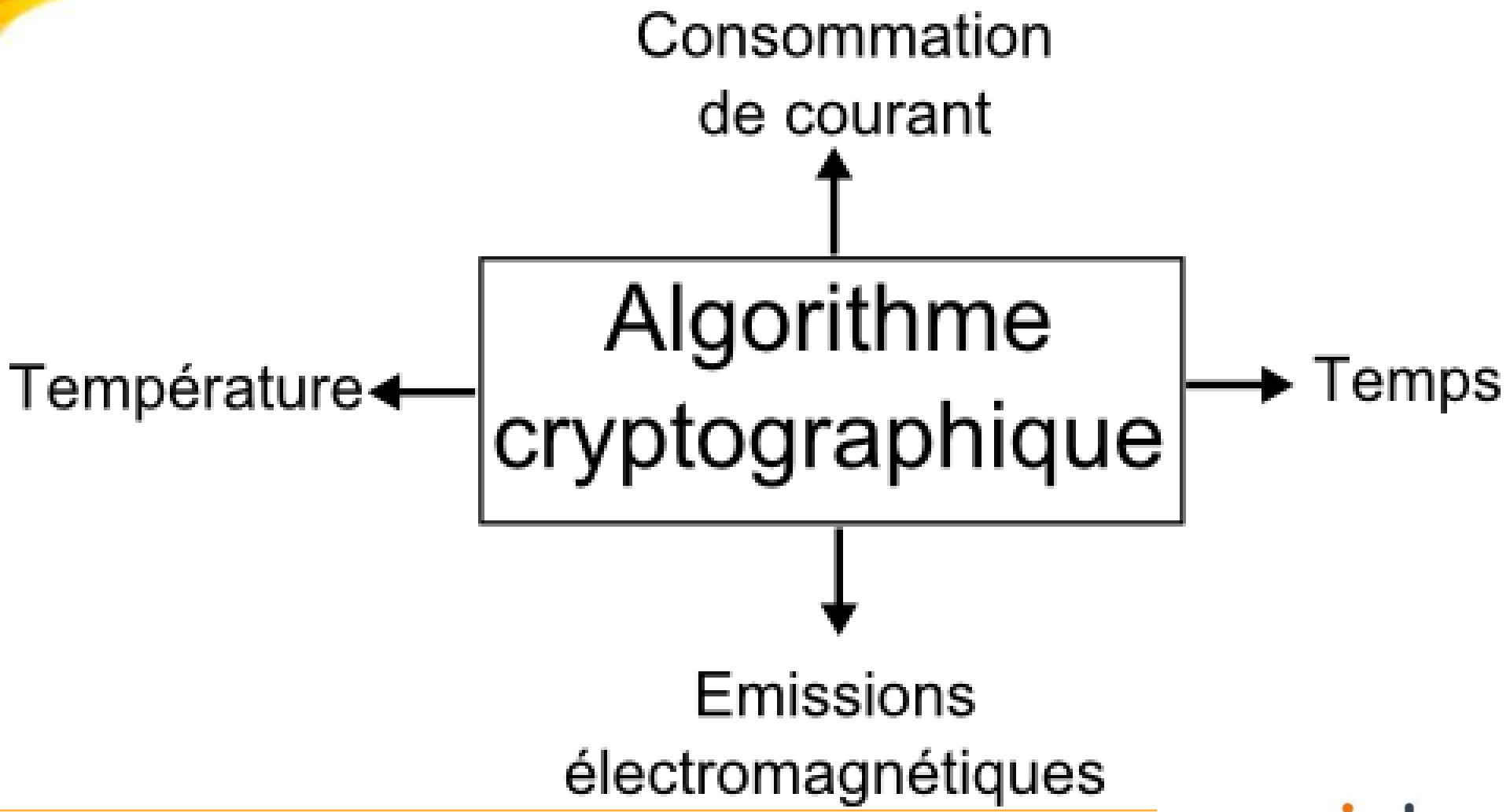
Familles d'attaques physiques

- **Attaques par analyse simple**
  L'attaquant observe un canal caché du composant lors d'un calcul cryptographique et retrouve la clé secrète

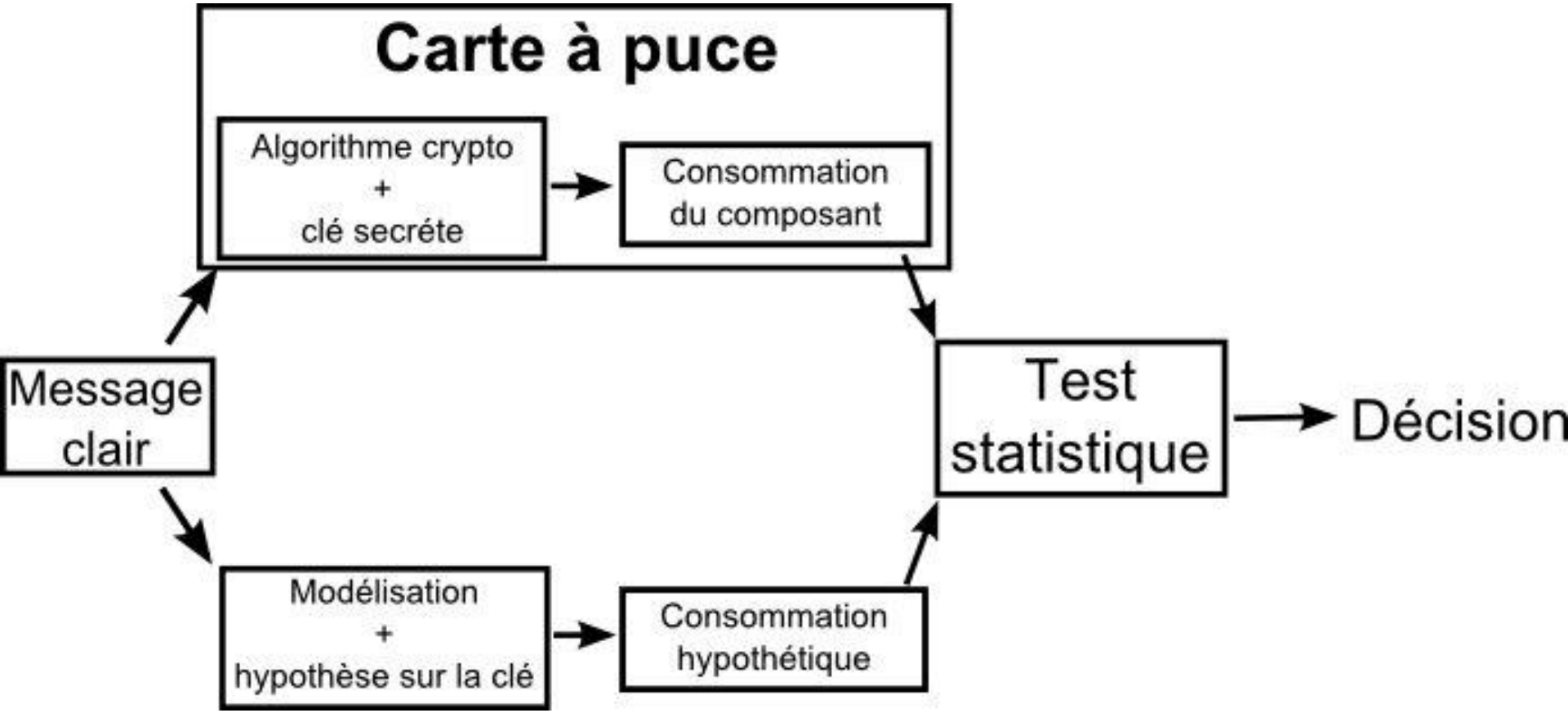
- **Attaques par analyse différentielle**
  L'attaquant observe plusieurs courbes du canal caché et retrouve le secret à l'aide d'outils statistiques

- **Attaques par injection de faute**
  L'attaquant utilise des résultats de calculs corrects, des résultats faux dus à une injection de faute et l'endroit précis où la faute a été effectuée pour retrouver le secret

Types de canaux cachés



Attaque par analyse différentielle de courant (DPA)



Sommaire

1. Attaques physiques
2. Rappels AES et contre-mesures DPA
3. Notre proposition
4. Conclusion

Rappels sur AES

- Algorithme de chiffrement par blocs.
- Trois tailles de clés : 128, 192, 256 bits
- Un tour est constitué des opérations :
  - AddRoundKey
  - SubBytes
  - ShiftRows
  - MixColumns
- On travaille dans $GF(2^8)$
- SubBytes = inverse dans $GF(2^8)$ et transformation affine

- Problème : on veut masquer aléatoirement une valeur v tel que si en entrée d'inverse on a $v + r_1$ on obtienne $v^{-1} + r_2$ en sortie

Types de contre-mesures DPA

- Plusieurs types de contre-mesures :
  - Désynchronisation avec des boucles d'attentes aléatoires
  - Ajout de bruit au niveau hardware
  - Utilisation de logique équilibrée
  - Masquer les données liées au secret au niveau de l'algorithme

Historique de quelques contre-mesures DPA (1)

- 2001 : Transform Masking Method – Akkar et Giraud
  - Masquage booléen → masquage multiplicatif
- 2001 : Random Value Masking Method – Messerges
  - Recalculer des Sboxes masquées dynamiquement
- 2002 : Embedded Multiplicative Masking – Golic et Tymen
  - Calculs dans l'anneau $GF(2^8) \times GF(2^k)$

Historique de quelques contre-mesures DPA (2)

- 2005 : Masked Modular Exponentiation – Blomer et al.
  - Calcul de A^{254} avec des algorithmes *square* et *multiply* spéciaux
- 2005 : Masking using Log Tables – Trichina et al.
  - γ générateur de $GF(2^8)$. Soit $\alpha = \gamma^i$ pour $0 \leq i \leq 255$, on pré-calcule les tables : $\log(\alpha) = i$ et $alog(i) = \alpha$
  - Les opérations sur $GF(2^8)$ sont transformées en accès à ces tables
- 2005 : Random Isomorphisms on AES Field – Rostovtsev et al.
  - 240 représentations possibles de $GF(2^8)$

Historique de quelques contre-mesures DPA (3)

- 2006 : Split-Mask Countermeasure – Gebotys
  - Soit deux tables $SBox'$ et M telles que
  - $SBox'(v + r_1) = SBox(v) + r_v$
  - $M(v + r_1) = r_v + r_2$
- 2006 : Resistant Sbox based on Fourier Transform – Prouff et al.
- 2005 : Boolean Masking in Tower Field – Oswald et al.
  - Combine la méthode de calcul d'AES efficace dans des sous-corps avec une méthode de masquage

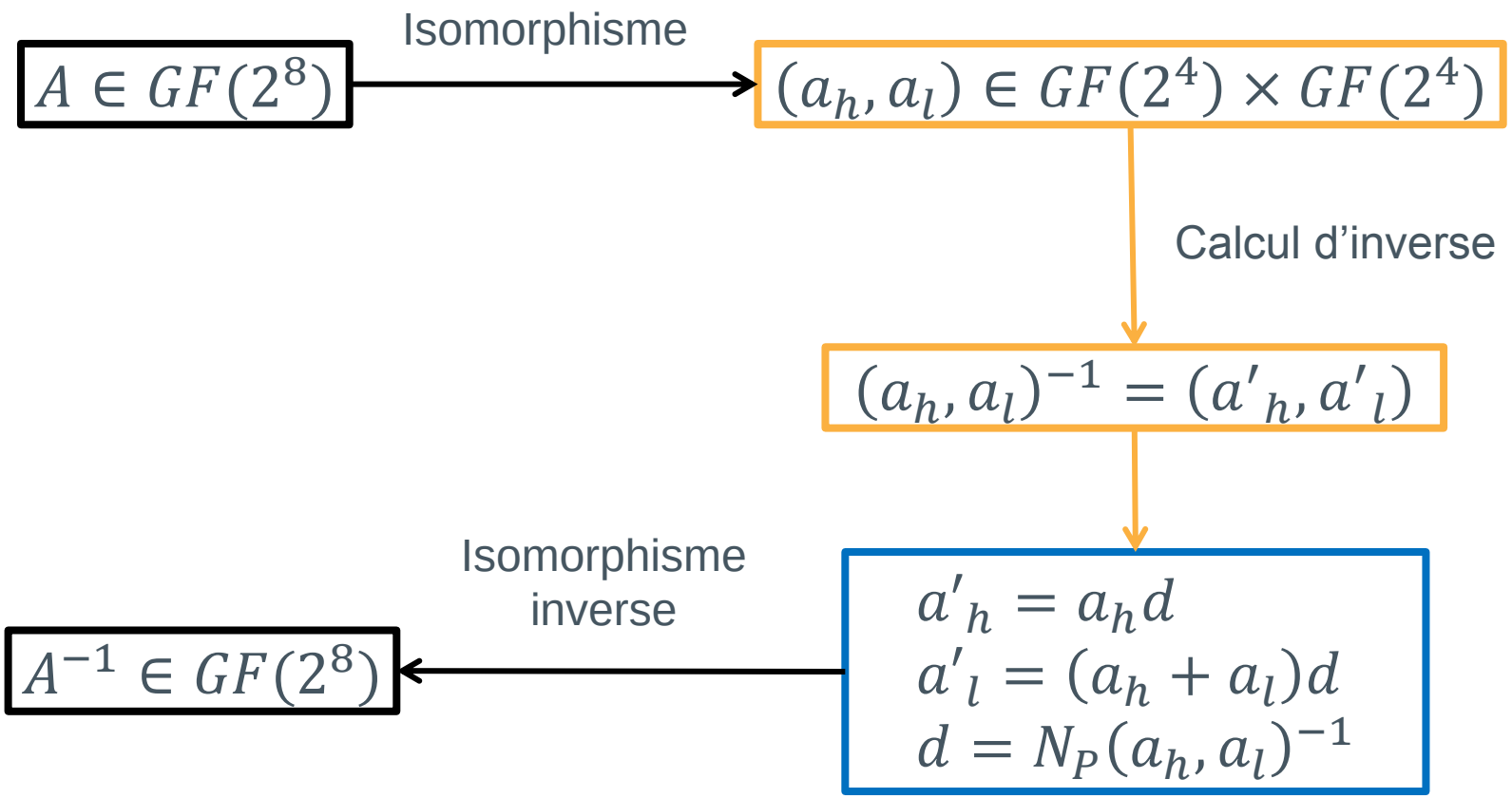
Sommaire

1. Attaques physiques
2. Rappels AES et contre-mesures DPA
3. Notre proposition
4. Conclusion

AES avec une tour d'extensions de corps

- Tour d'extensions : $GF(2) \subset GF(2^2) \subset GF(2^4) \subset GF(2^8)$
- Principe : calculer l'inverse dans un sous-corps de $GF(2^8)$ pour accélérer l'opération
- Implémentation très intéressante en hardware
- Proposé en 2002 par Wolkerstorfer et al.

Inverse dans une tour d'extensions



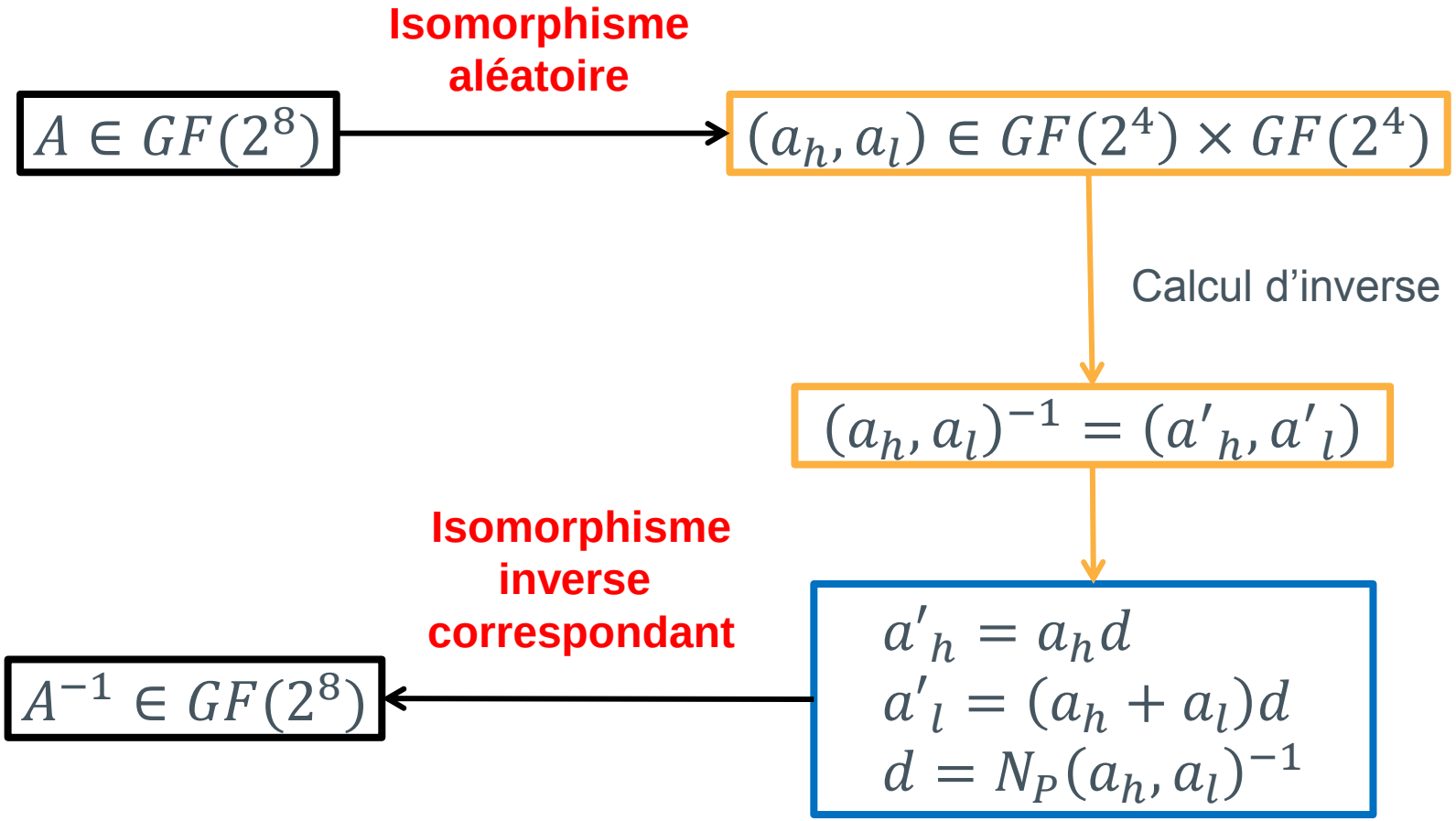
$GF(2^8)$ $GF(2^4) \times GF(2^4)$ $GF(2^4)$

Proposition de contre-mesure DPA pour AES (1)

- 1) Choisir au hasard la représentation du corps pour calculer l'inverse
  - Utilisation de différents polynômes, différents éléments primitifs

- Notations :
  - $R(z) = z^8 + z^4 + z^3 + z + 1$
  - $GF(2^8) \coloneqq GF_2(R)$
  - Q polynôme irréductible de degré 4 sur $GF(2)$
  - P polynôme irréductible de degré 2 sur $GF_2(Q)[z]$
  - On a l'isomorphisme $\mu: GF_2(Q,P) \rightarrow GF_2(R)$

Proposition de contre-mesure DPA pour AES (1)

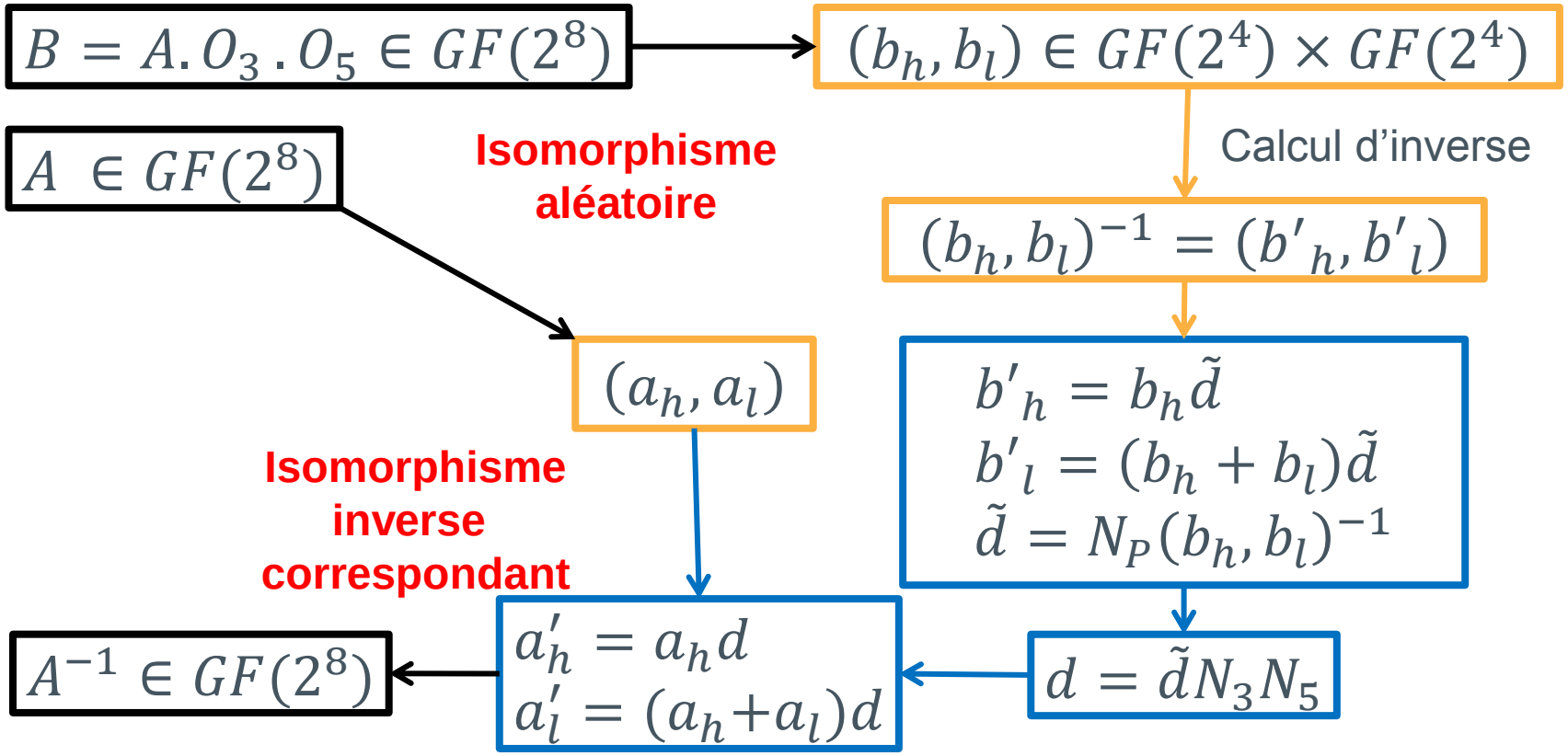


$\boldsymbol{GF(2^8)}$ $\boldsymbol{GF(2^4) \times GF(2^4)}$ $\boldsymbol{GF(2^4)}$

Proposition de contre-mesure DPA pour AES (2)

- 2) Augmenter le nombre de représentations possibles de la norme
  - Relation entre la norme d'un élément dans $GF(2^4)$ et son ordre dans $GF(2^8)$
  - Modification de l'ordre pour un faible surcoût mémoire/complexité

Proposition de contre-mesure DPA pour AES (2)



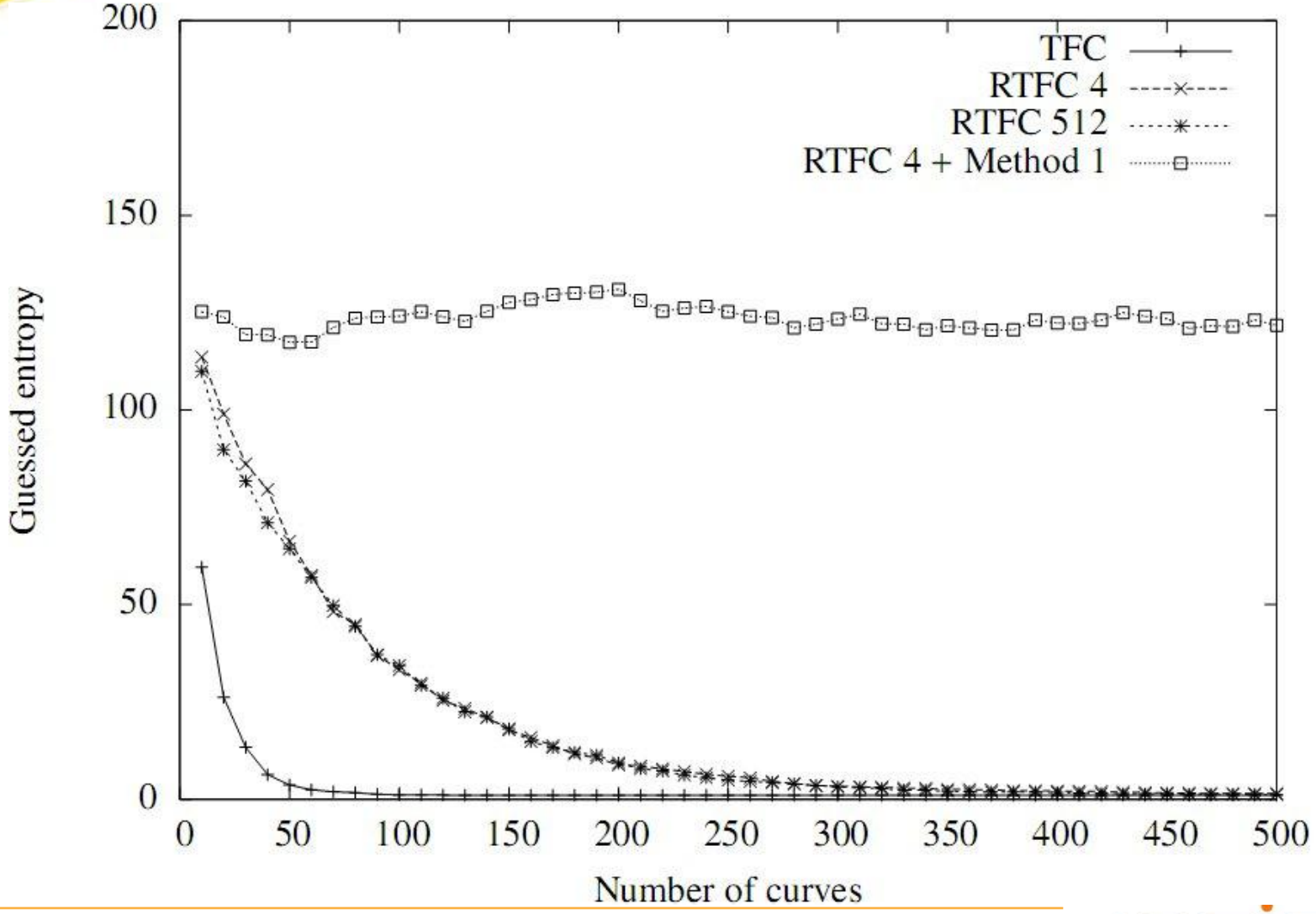
$GF(2^8)$ $GF(2^4) \times GF(2^4)$ $GF(2^4)$

Coût de la contre-mesure

- Mémoire :
  - 4 matrices pour les isomorphismes et 4 matrices inverses = 64 octets
  - Éléments de O_3 et O_5 = 8 octets
  - Éléments de N_3 et N_5 = 32 octets

- Complexité :
  - 2 multiplications dans $GF(2^8)$
  - 4 multiplications dans $GF(2^4)$

Expérimentations



Sommaire

1. Attaques physiques
2. Rappels AES et contre-mesures DPA
3. Notre proposition
4. Conclusion

Conclusion

- Contre-mesure pour un AES adapté au hardware
- Faible surcoût
- Accompagnée d’un masquage booléen, on améliore la résistance aux attaques différentielles de premier ordre

Merci de votre attention