

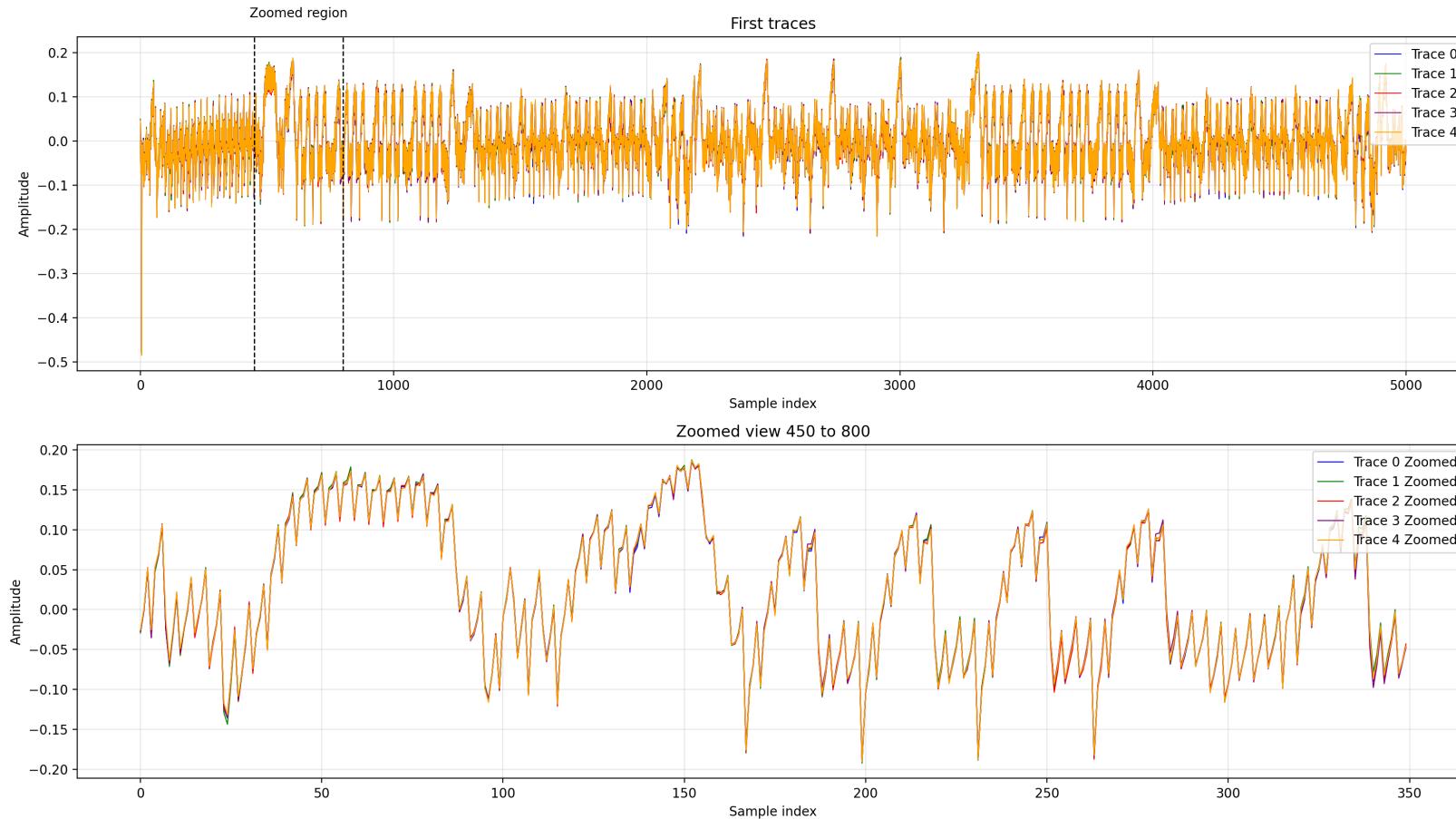
Projet Sécurité – DPA et CPA

Vers la découverte des attaques cyber-physique

Benjamin GROLLEAU – Lundi 5 janvier 2025

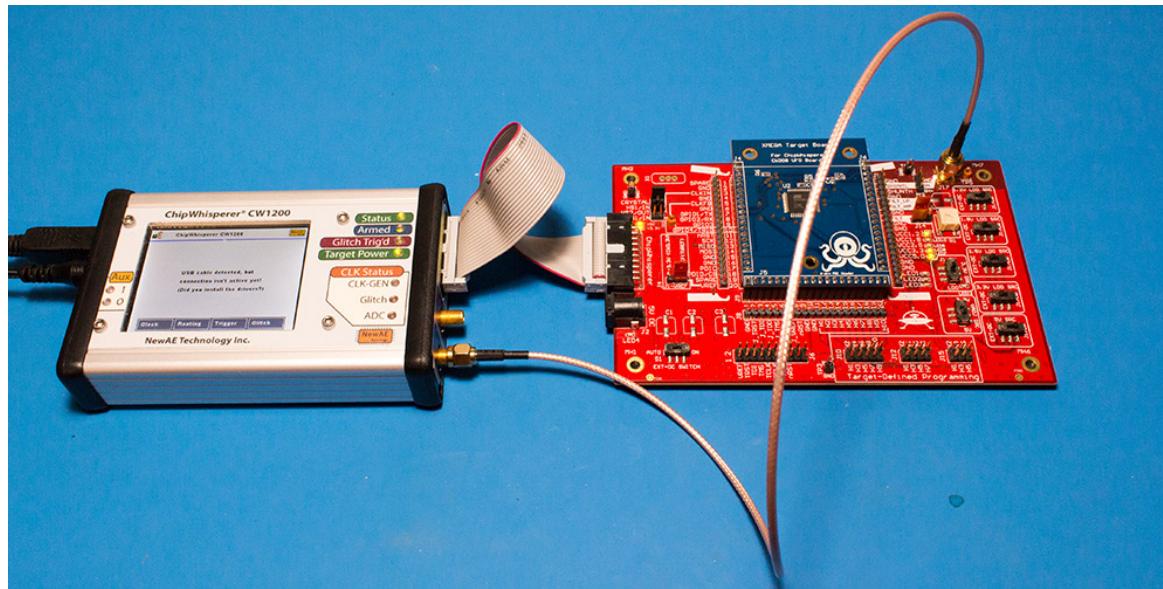
- DPA — Differential Power Analysis
- CPA — Correlation Power Analysis
- Comparaison
- Cas d'usages

Données d'entrées



Données d'entrées

ChipWhisperer CW1200



DPA

Differential Power Analysis

Valeurs intermédiaire ciblée

DPA – Méthodologie de l'attaque

$$v = \text{SBox}(\text{plaintext}[i] \oplus \text{key}[i]) \quad (2)$$

$$\text{leak} = v \& 0x01 \quad (3)$$

```
src > aes > contents.py > [s] sbox
1   sbox = [
2     # 0   1   2   3   4   5   6   7   8   9   a   b   c   d   e   f
3     0x63, 0x7c, 0x77, 0x7b, 0xf2, 0x6b, 0x6f, 0xc5, 0x30, 0x01, 0x67, 0x2b, 0xfe, 0xd7, 0xab, 0x76, # 0
4     0xca, 0x82, 0xc9, 0x7d, 0xfa, 0x59, 0x47, 0xf0, 0xad, 0xd4, 0xa2, 0xaf, 0x9c, 0xa4, 0x72, 0xc0, # 1
5     0xb7, 0xfd, 0x93, 0x26, 0x36, 0x3f, 0xf7, 0xcc, 0x34, 0xa5, 0xe5, 0xf1, 0x71, 0xd8, 0x31, 0x15, # 2
6     0x04, 0xc7, 0x23, 0xc3, 0x18, 0x96, 0x05, 0x9a, 0x07, 0x12, 0x80, 0xe2, 0xeb, 0x27, 0xb2, 0x75, # 3
7     0x09, 0x83, 0x2c, 0x1a, 0x1b, 0x6e, 0x5a, 0xa0, 0x52, 0x3b, 0xd6, 0xb3, 0x29, 0xe3, 0x2f, 0x84, # 4
8     0x53, 0xd1, 0x00, 0xed, 0x20, 0xfc, 0xb1, 0x5b, 0x6a, 0xcb, 0xbe, 0x39, 0xa4, 0x4c, 0x58, 0xcf, # 5
9      0xd0, 0xef, 0xaa, 0xfb, 0x43, 0x4d, 0x33, 0x85, 0x45, 0xf9, 0x02, 0x7f, 0x50, 0x3c, 0x9f, 0xa8, # 6
10    0x51, 0xa3, 0x40, 0x8f, 0x92, 0x9d, 0x38, 0xf5, 0xbc, 0xb6, 0xda, 0x21, 0x10, 0xff, 0xf3, 0xd2, # 7
11    0xcd, 0x0c, 0x13, 0xec, 0x5f, 0x97, 0x44, 0x17, 0xc4, 0xa7, 0x7e, 0x3d, 0x64, 0x5d, 0x19, 0x73, # 8
12    0x60, 0x81, 0x4f, 0xdc, 0x22, 0x2a, 0x90, 0x88, 0x46, 0xee, 0xb8, 0x14, 0xde, 0x5e, 0x0b, 0xdb, # 9
13    0xe0, 0x32, 0x3a, 0x0a, 0x49, 0x06, 0x24, 0x5c, 0xc2, 0xd3, 0xac, 0x62, 0x91, 0x95, 0xe4, 0x79, # a
14    0xe7, 0xc8, 0x37, 0x6d, 0x8d, 0xd5, 0x4e, 0xa9, 0x6c, 0x56, 0xf4, 0xea, 0x65, 0x7a, 0xae, 0x08, # b
15    0xba, 0x78, 0x25, 0x2e, 0x1c, 0xa6, 0xb4, 0xc6, 0xe8, 0xdd, 0x74, 0x1f, 0x4b, 0xbd, 0x8b, 0x8a, # c
16    0x70, 0x3e, 0xb5, 0x66, 0x48, 0x03, 0xf6, 0x0e, 0x61, 0x35, 0x57, 0xb9, 0x86, 0xc1, 0x1d, 0x9e, # d
17    0xe1, 0xf8, 0x98, 0x11, 0x69, 0xd9, 0x8e, 0x94, 0x9b, 0x1e, 0x87, 0xe9, 0xce, 0x55, 0x28, 0xdf, # e
18    0x8c, 0xa1, 0x89, 0x0d, 0xbf, 0xe6, 0x42, 0x68, 0x41, 0x99, 0x2d, 0x0f, 0xb0, 0x54, 0xbb, 0x16 # f
19 ]
```

Construction des hypothèses de fuite

DPA — Méthodologie de l'attaque

- $guess \in \{0x00; 0x01; \dots; 0xff\}$
- v_k représente la valeur de v pour le plaintext d'indice k
- $mask[k] \in \{0; 1\}$ en fonction du LSB de v_k

$$v_k = \text{SBox}(\text{plaintext}[k][0] \oplus guess) \quad (4)$$

$$mask[k] = v_k \& 0x01 \quad (5)$$

Séparation en deux groupes de traces

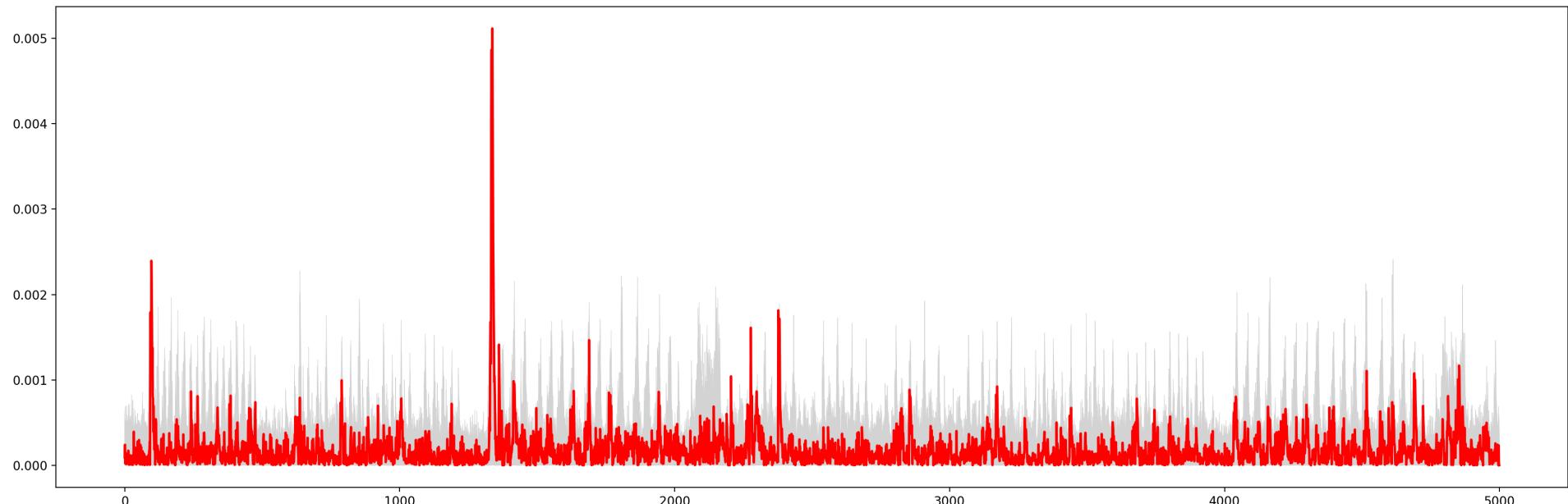
DPA – Méthodologie de l'attaque

- Sel1 => traces pour lesquelles $mask[k] = 1$
- Sel2 => traces pour lesquelles $mask[k] = 0$
- Deux listes d'environ 300 traces pour un ensemble initiales de 600 entrées sur des textes purement aléatoire.

Calcul du vecteur de différence

DPA — Méthodologie de l'attaque

$$\text{diff}(t) = |\text{mean}(\text{sel1}[t]) - \text{mean}(\text{sel0}[t])| \quad (6)$$

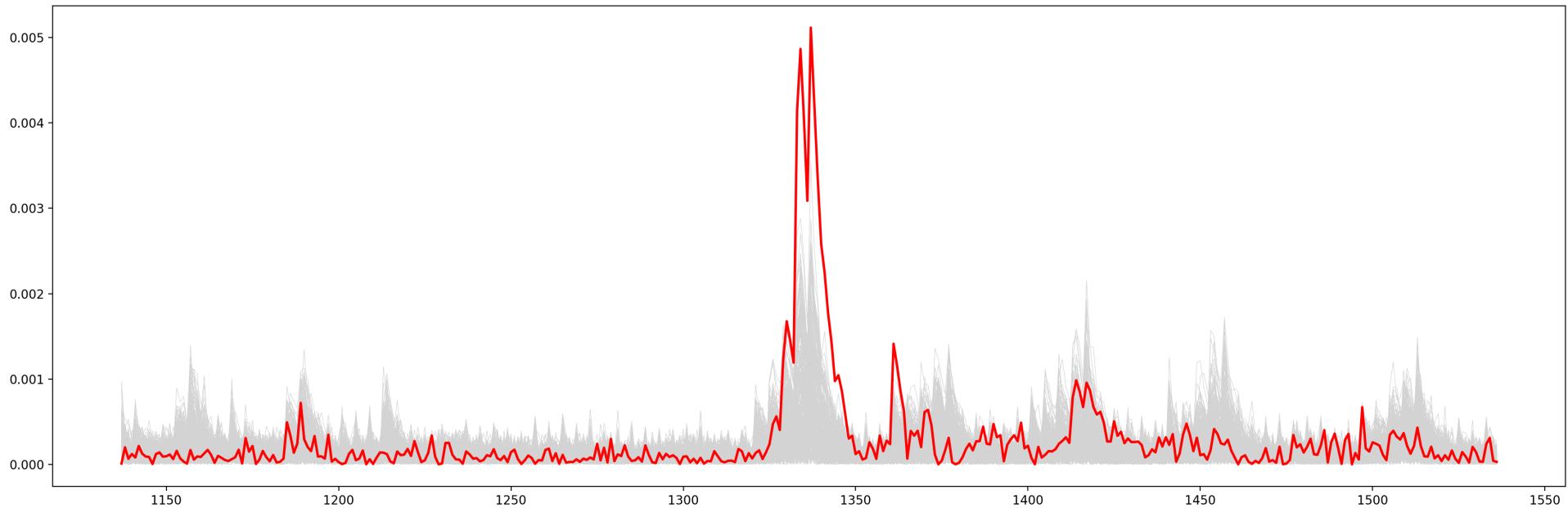


Vecteurs de différences pour les 256 hypothèses de clé (byte 0). La courbe rouge correspond à la bonne hypothèse.

Calcul du vecteur de différence

DPA — Méthodologie de l'attaque

$$\text{diff}(t) = |\text{mean}(\text{sel1}[t]) - \text{mean}(\text{sel0}[t])| \quad (6)$$

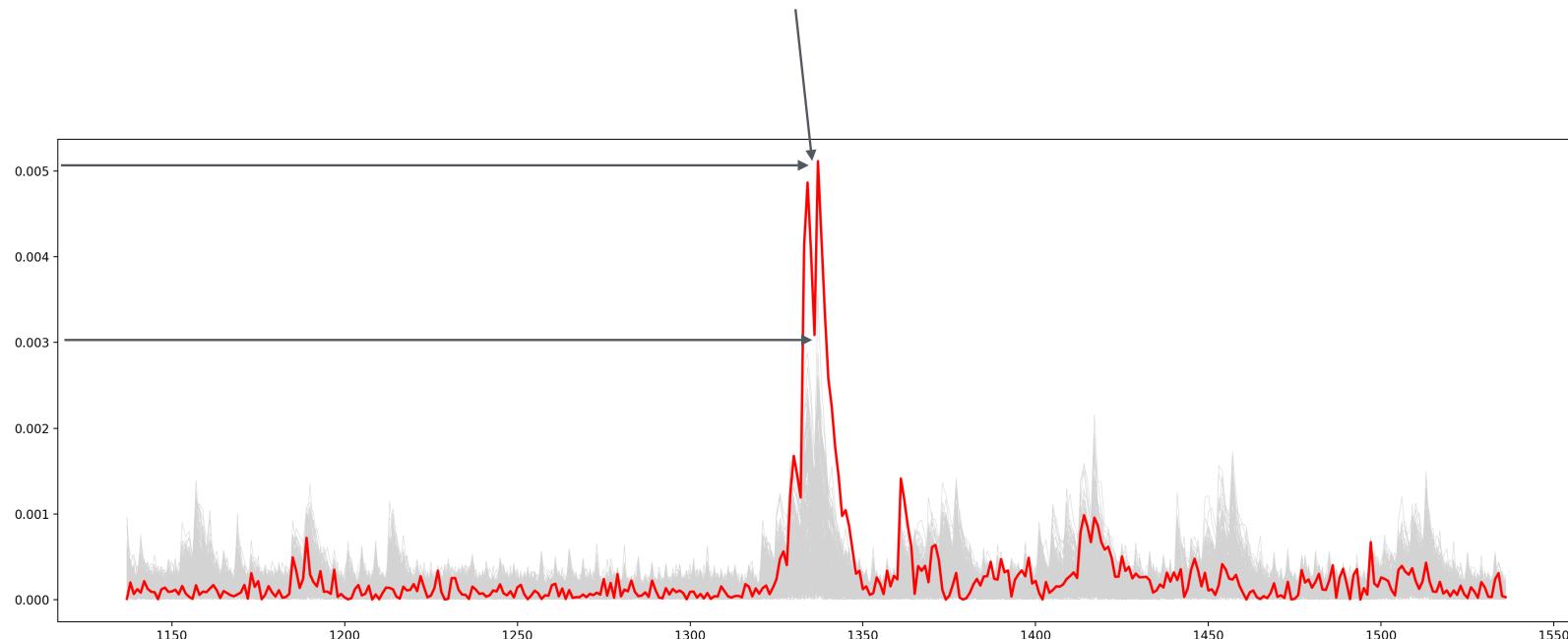


Zoom sur la zone de fuite illustrant le pic caractéristique de la bonne clé.

Définition du score DPA

DPA — Méthodologie de l'attaque

$$\text{score}(guess) = \max_t(\text{diff}(t)). \quad (7)$$

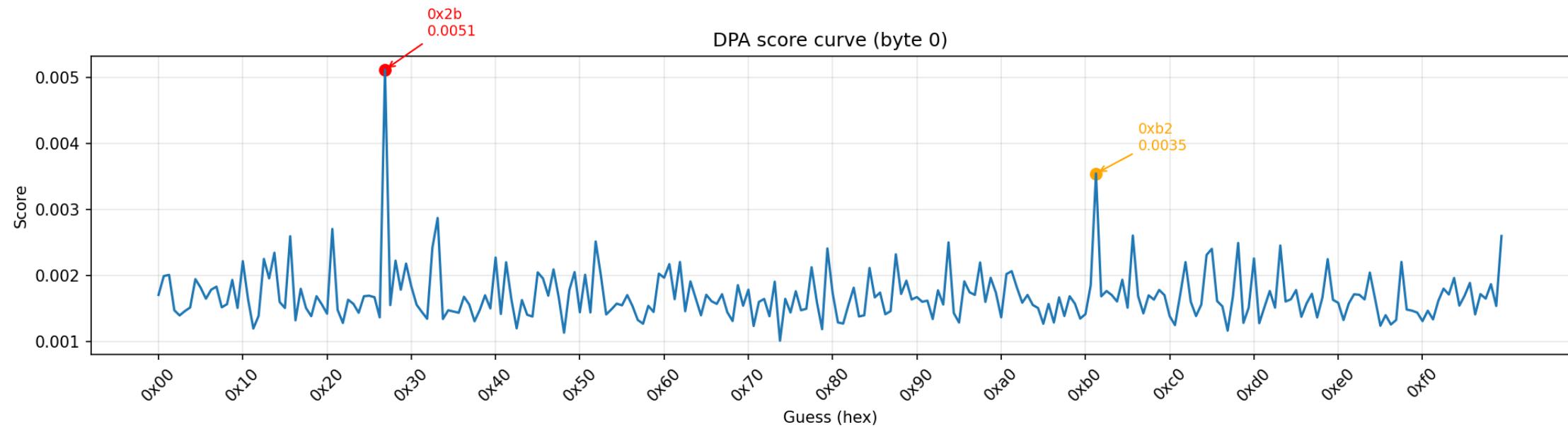


Zoom sur la zone de fuite illustrant le pic caractéristique de la bonne clé.

Sélection de la clé

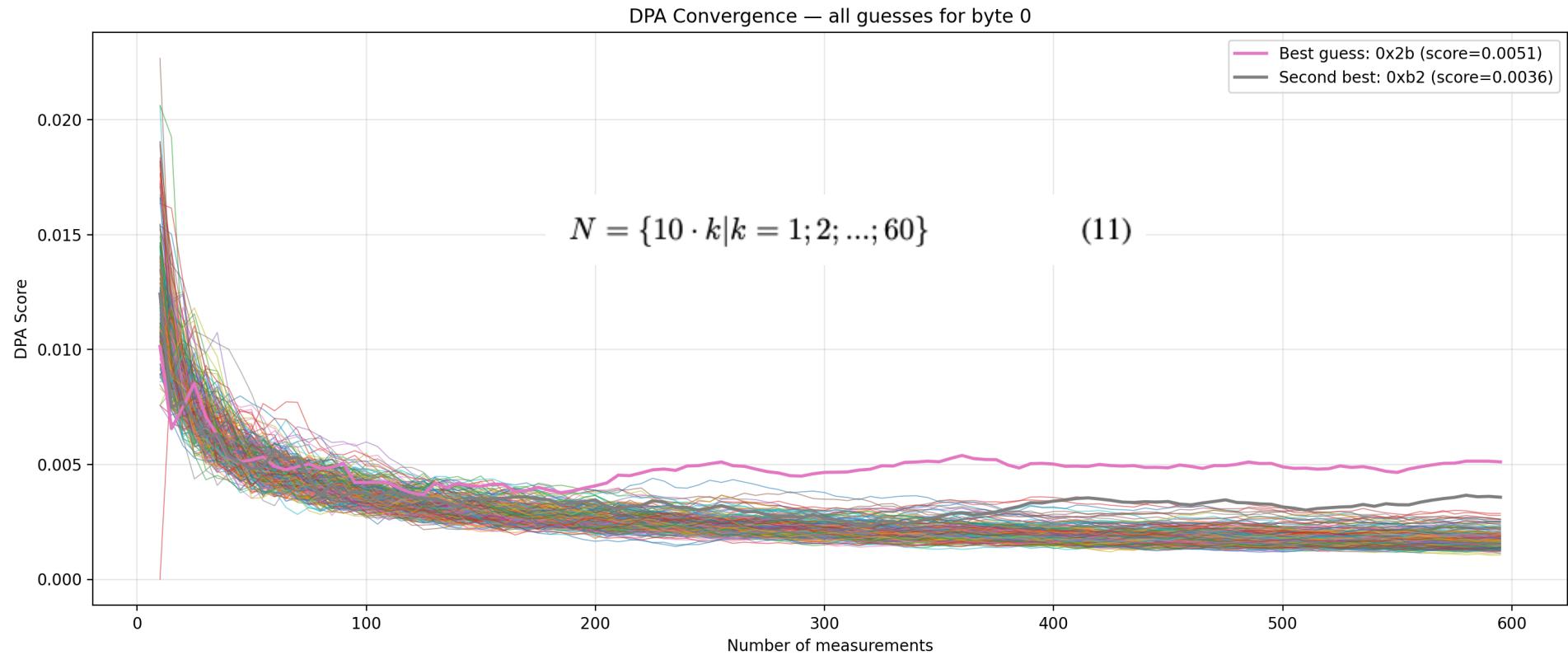
DPA — Méthodologie de l'attaque

$$\text{key}[0] = \arg \max_{\text{guess} \in [0x00; 0xff]} \text{score}(\text{guess}) \quad (8)$$



Vitesse de convergence

DPA — Méthodologie de l'attaque



Taux de confiance

DPA — Méthodologie de l'attaque

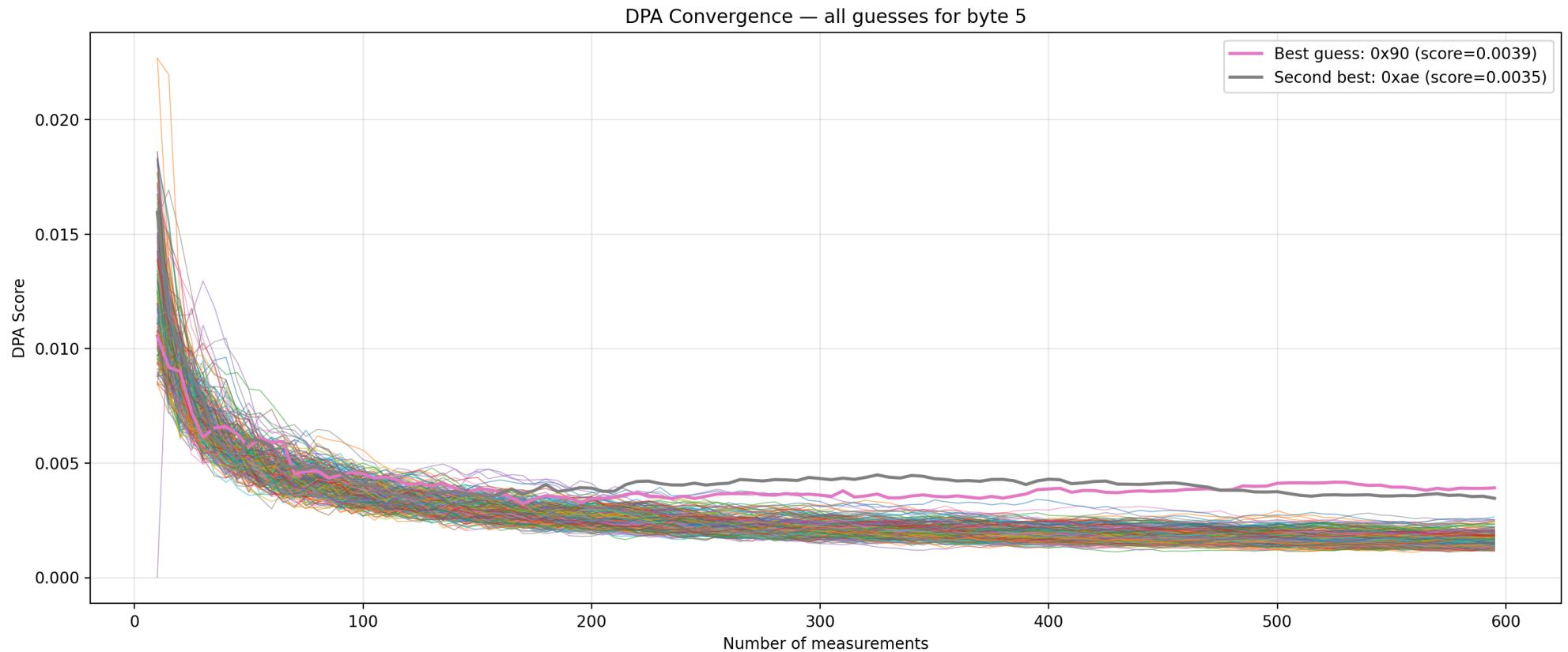
$$\text{contrast} = \frac{\text{best_score} - \text{second_score}}{\max(\text{second_score}, 10^{-15})} \quad (9)$$

$$\text{confidence} = \min(\max(\text{contrast}, 0), 1) \quad (10)$$

== DPA BYTE SUMMARY ==					
Byte	Guess	Correct	Status	Confidence	Second Best
0	0x2b	0x2b	OK	44.29%	
1	0x7e	0x7e	OK	60.68%	
2	0x15	0x15	OK	50.77%	
3	0x16	0x16	OK	61.69%	
4	0x28	0x28	OK	77.38%	
5	0x90	0xae	NOK	15.23%	0xae (0.00342 vs 0.00395)
6	0xd2	0xd2	OK	35.74%	
7	0xa6	0xa6	OK	49.49%	
8	0xab	0xab	OK	54.54%	
9	0xf7	0xf7	OK	30.03%	
10	0x15	0x15	OK	29.08%	
11	0x88	0x88	OK	34.25%	
12	0x09	0x09	OK	24.69%	
13	0xcf	0xcf	OK	30.99%	
14	0x4f	0x4f	OK	52.42%	
15	0x3c	0x3c	OK	43.56%	

Probabilité d'erreur

DPA — Méthodologie de l'attaque



CPA

Correlation Power Analysis

Valeurs intermédiaire ciblée

CPA – Méthodologie de l'attaque

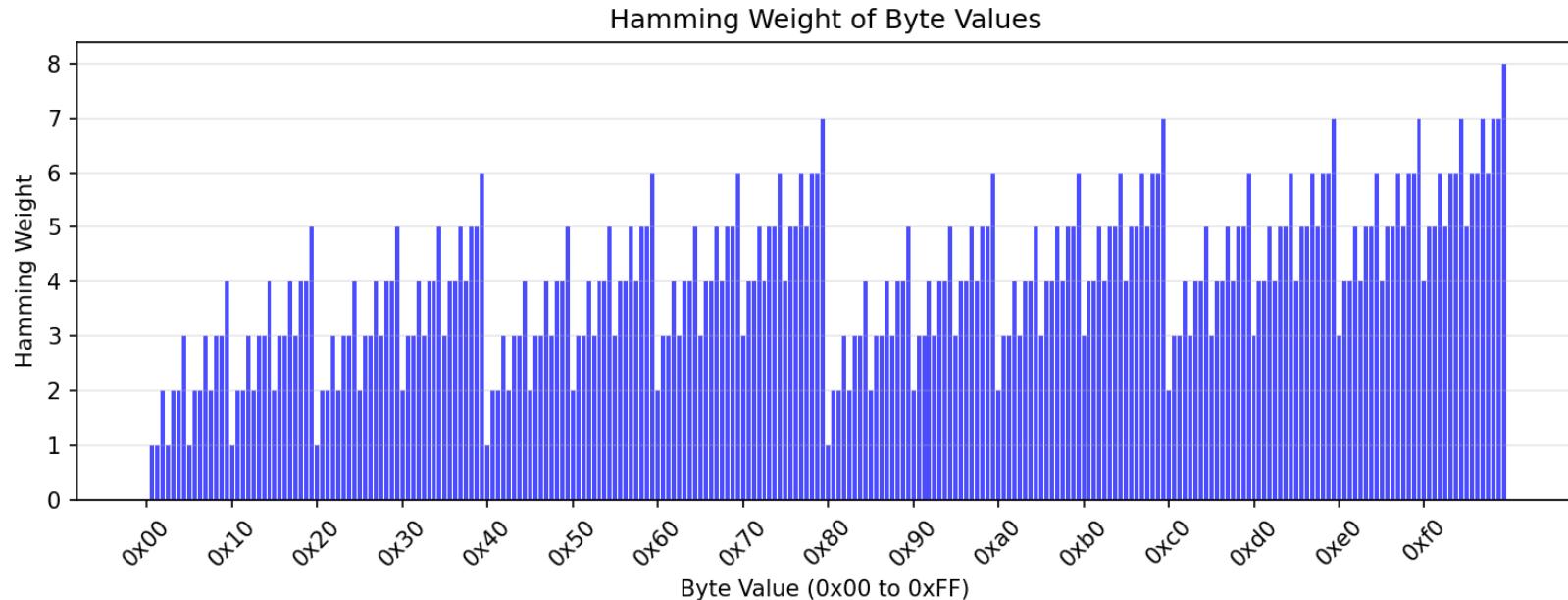
$$v = \text{SBox}(\text{plaintext}[i] \oplus \text{key}[i]) \quad (2)$$

```
src > aes > contents.py > [s] sbox
1   sbox = [
2     #  0   1   2   3   4   5   6   7   8   9   a   b   c   d   e   f
3     0x63, 0x7c, 0x77, 0x7b, 0xf2, 0x6b, 0x6f, 0xc5, 0x30, 0x01, 0x67, 0x2b, 0xfe, 0xd7, 0xab, 0x76, # 0
4     0xca, 0x82, 0xc9, 0x7d, 0xfa, 0x59, 0x47, 0xf0, 0xad, 0xd4, 0xa2, 0xaf, 0x9c, 0xa4, 0x72, 0xc0, # 1
5     0xb7, 0xfd, 0x93, 0x26, 0x36, 0x3f, 0xf7, 0xcc, 0x34, 0xa5, 0xe5, 0xf1, 0x71, 0xd8, 0x31, 0x15, # 2
6     0x04, 0xc7, 0x23, 0xc3, 0x18, 0x96, 0x05, 0x9a, 0x07, 0x12, 0x80, 0xe2, 0xeb, 0x27, 0xb2, 0x75, # 3
7     0x09, 0x83, 0x2c, 0x1a, 0x1b, 0x6e, 0x5a, 0xa0, 0x52, 0x3b, 0xd6, 0xb3, 0x29, 0xe3, 0x2f, 0x84, # 4
8     0x53, 0xd1, 0x00, 0xed, 0x20, 0xfc, 0xb1, 0x5b, 0x6a, 0xcb, 0xbe, 0x39, 0xa4, 0x4c, 0x58, 0xcf, # 5
9      0xd0, 0xef, 0xaa, 0xfb, 0x43, 0x4d, 0x33, 0x85, 0x45, 0xf9, 0x02, 0x7f, 0x50, 0x3c, 0x9f, 0xa8, # 6
10    0x51, 0xa3, 0x40, 0x8f, 0x92, 0x9d, 0x38, 0xf5, 0xbc, 0xb6, 0xda, 0x21, 0x10, 0xff, 0xf3, 0xd2, # 7
11    0xcd, 0x0c, 0x13, 0xec, 0x5f, 0x97, 0x44, 0x17, 0xc4, 0xa7, 0x7e, 0x3d, 0x64, 0x5d, 0x19, 0x73, # 8
12    0x60, 0x81, 0x4f, 0xdc, 0x22, 0x2a, 0x90, 0x88, 0x46, 0xee, 0xb8, 0x14, 0xde, 0x5e, 0x0b, 0xdb, # 9
13    0xe0, 0x32, 0x3a, 0x0a, 0x49, 0x06, 0x24, 0x5c, 0xc2, 0xd3, 0xac, 0x62, 0x91, 0x95, 0xe4, 0x79, # a
14    0xe7, 0xc8, 0x37, 0x6d, 0x8d, 0xd5, 0x4e, 0xa9, 0x6c, 0x56, 0xf4, 0xea, 0x65, 0x7a, 0xae, 0x08, # b
15    0xba, 0x78, 0x25, 0x2e, 0x1c, 0xa6, 0xb4, 0xc6, 0xe8, 0xdd, 0x74, 0x1f, 0x4b, 0xbd, 0x8b, 0x8a, # c
16    0x70, 0x3e, 0xb5, 0x66, 0x48, 0x03, 0xf6, 0x0e, 0x61, 0x35, 0x57, 0xb9, 0x86, 0xc1, 0x1d, 0x9e, # d
17    0xe1, 0xf8, 0x98, 0x11, 0x69, 0xd9, 0x8e, 0x94, 0x9b, 0x1e, 0x87, 0xe9, 0xce, 0x55, 0x28, 0xdf, # e
18    0x8c, 0xa1, 0x89, 0x0d, 0xbf, 0xe6, 0x42, 0x68, 0x41, 0x99, 0x2d, 0x0f, 0xb0, 0x54, 0xbb, 0x16 # f
19 ]
```

Définition du poids de hamming

CPA – Méthodologie de l'attaque

$$\text{HW}(x) = \sum_{i=0}^7 ((x \gg i) \& 1) \quad (4)$$

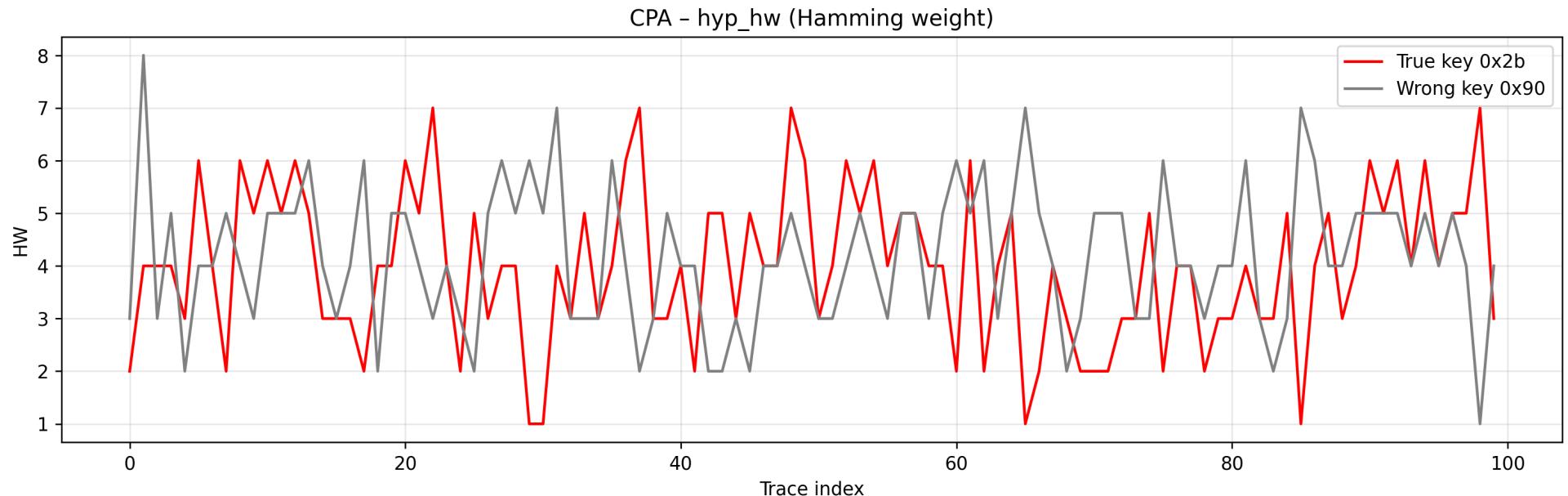


Construction des hypothèses de fuite

CPA — Méthodologie de l'attaque

$$v_k(g) = \text{SBox}(\text{plaintext}[k][0] \oplus g) \quad (5)$$

$$\text{hyp}_g[k] = \text{HW}(v_k(g)) \quad (6)$$

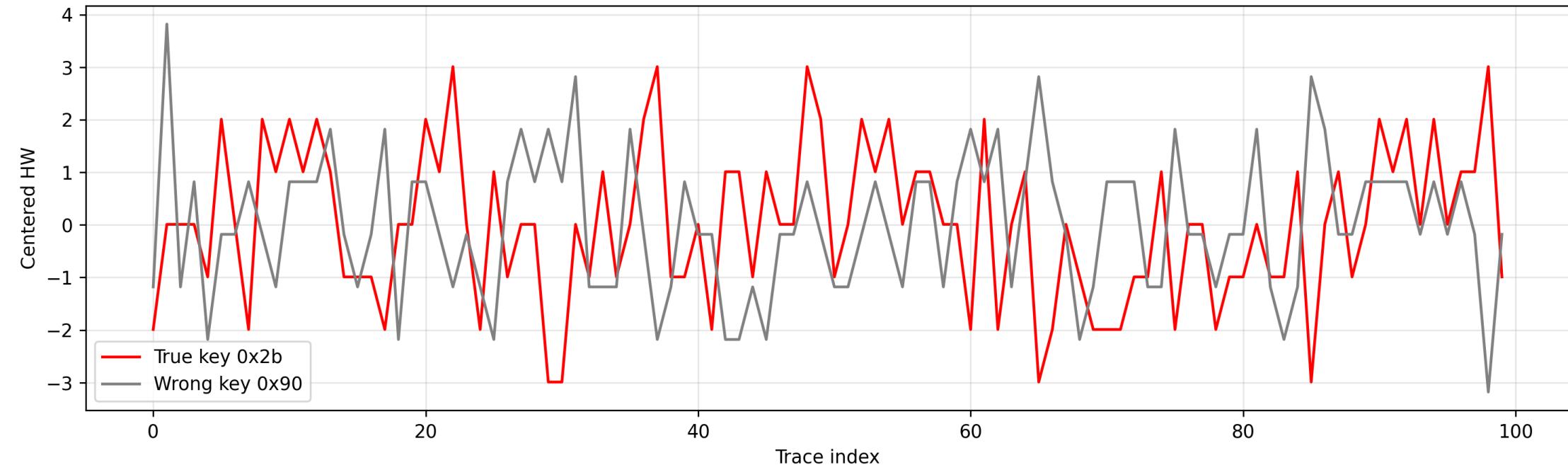


Centrage des données

CPA — Méthodologie de l'attaque

$$\text{hyp}_{g,c}[k] = \text{hyp}_g[k] - \text{mean}(\text{hyp}_g) \quad (7)$$

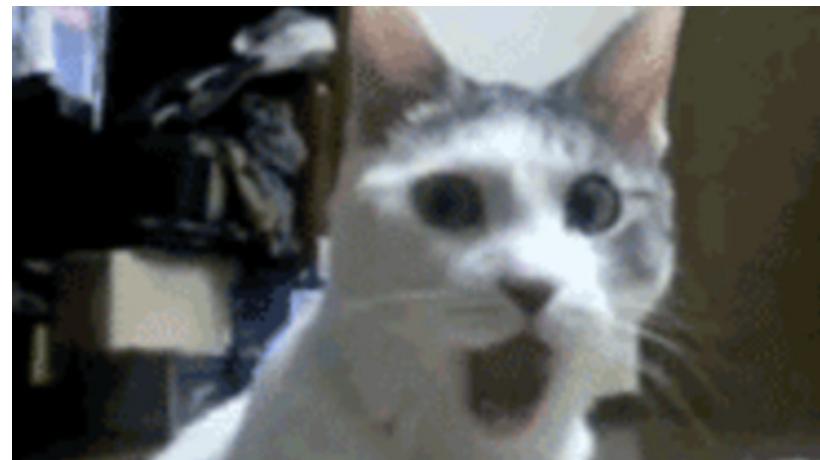
CPA - hyp_c (centered leakage model)



Calcul du vecteur de corrélation de PEARSON

CPA – Méthodologie de l'attaque

$$\rho(g, t) = \frac{\sum_k \text{hyp}_{g,c}[k] \cdot \text{traces}_c[k][t]}{\sqrt{\sum_k \text{hyp}_{g,c}[k]^2} \sqrt{\sum_k \text{traces}_c[k][t]^2}} \quad (9)$$



Calcul du vecteur de corrélation de PEARSON

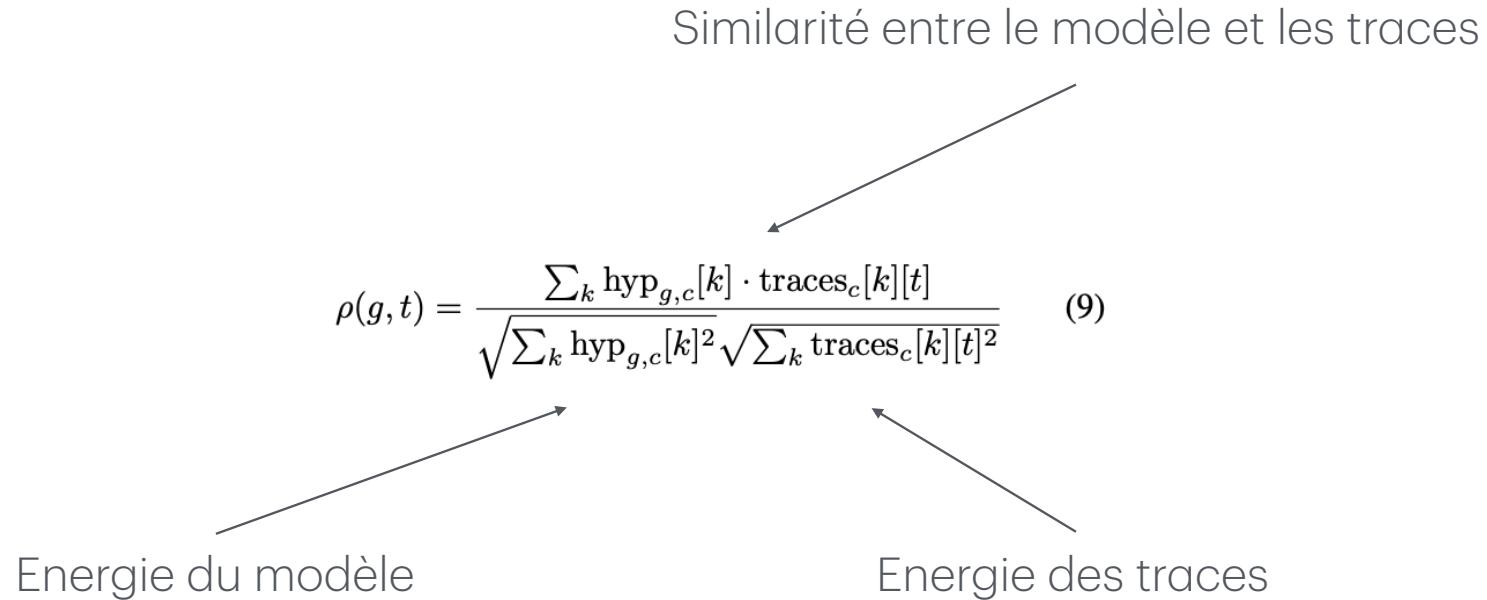
CPA – Méthodologie de l'attaque

Similarité entre le modèle et les traces

$$\rho(g, t) = \frac{\sum_k \text{hyp}_{g,c}[k] \cdot \text{traces}_c[k][t]}{\sqrt{\sum_k \text{hyp}_{g,c}[k]^2} \sqrt{\sum_k \text{traces}_c[k][t]^2}} \quad (9)$$

Energie du modèle

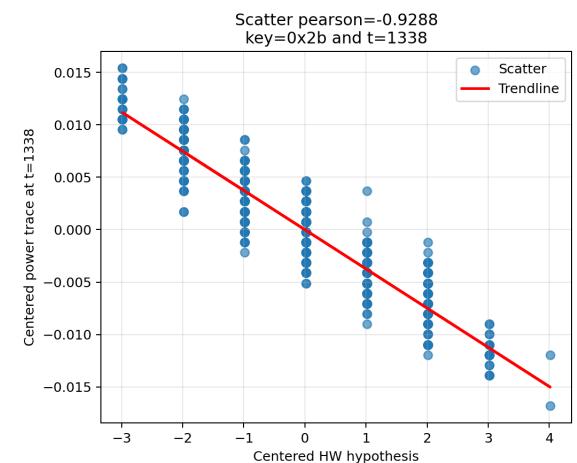
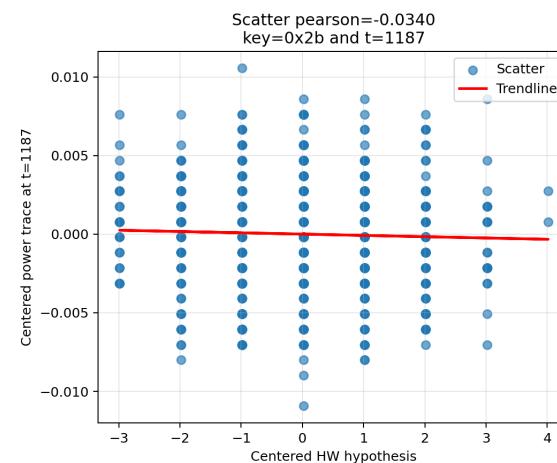
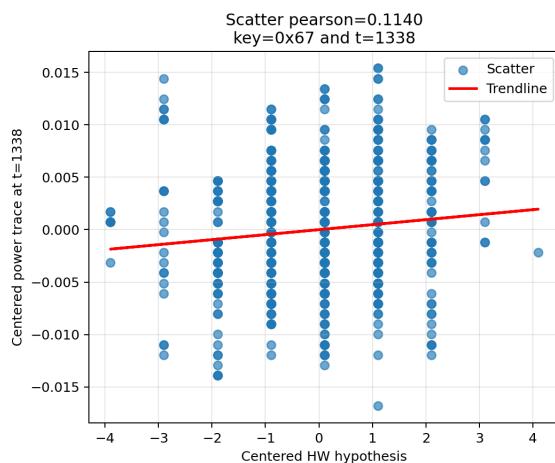
Energie des traces



Calcul du vecteur de corrélation de PEARSON

CPA – Méthodologie de l'attaque

$$\rho(g, t) = \frac{\sum_k \text{hyp}_{g,c}[k] \cdot \text{traces}_c[k][t]}{\sqrt{\sum_k \text{hyp}_{g,c}[k]^2} \sqrt{\sum_k \text{traces}_c[k][t]^2}} \quad (9)$$



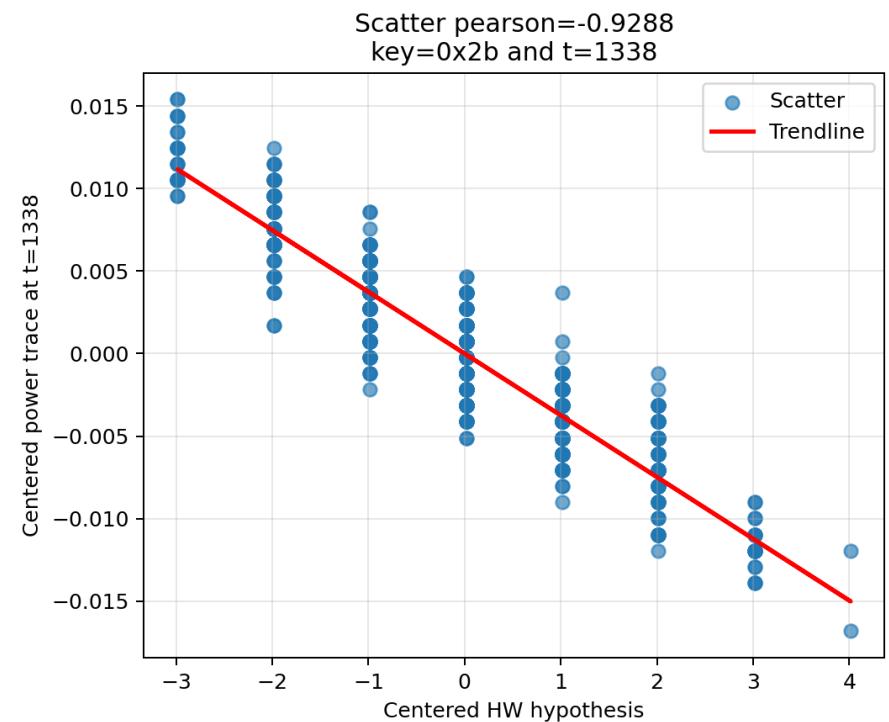
Calcul du vecteur de corrélation de PEARSON

CPA – Méthodologie de l'attaque

$$x_k = \text{hyp}_{g,c}[k]$$

$$y_k = \text{traces}_c[k][t]$$

$$\rho(g, t) = \frac{\sum_k \text{hyp}_{g,c}[k] \cdot \text{traces}_c[k][t]}{\sqrt{\sum_k \text{hyp}_{g,c}[k]^2} \sqrt{\sum_k \text{traces}_c[k][t]^2}} \quad (9)$$



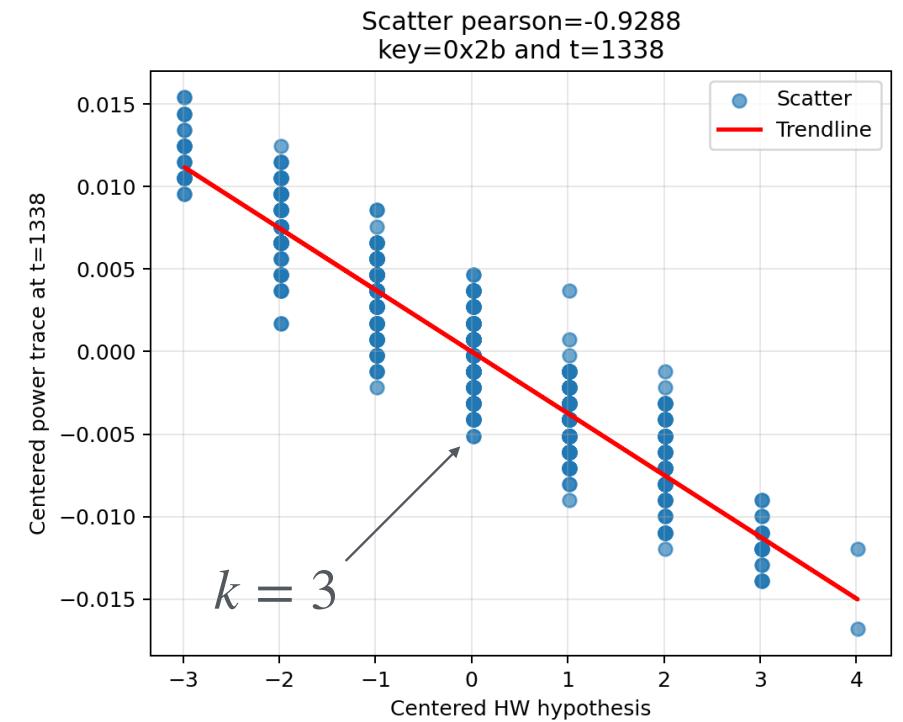
Calcul du vecteur de corrélation de PEARSON

CPA – Méthodologie de l'attaque

$$x_k = \text{hyp}_{g,c}[k]$$
$$y_k = \text{traces}_c[k][t]$$

e.g. $k = 3$

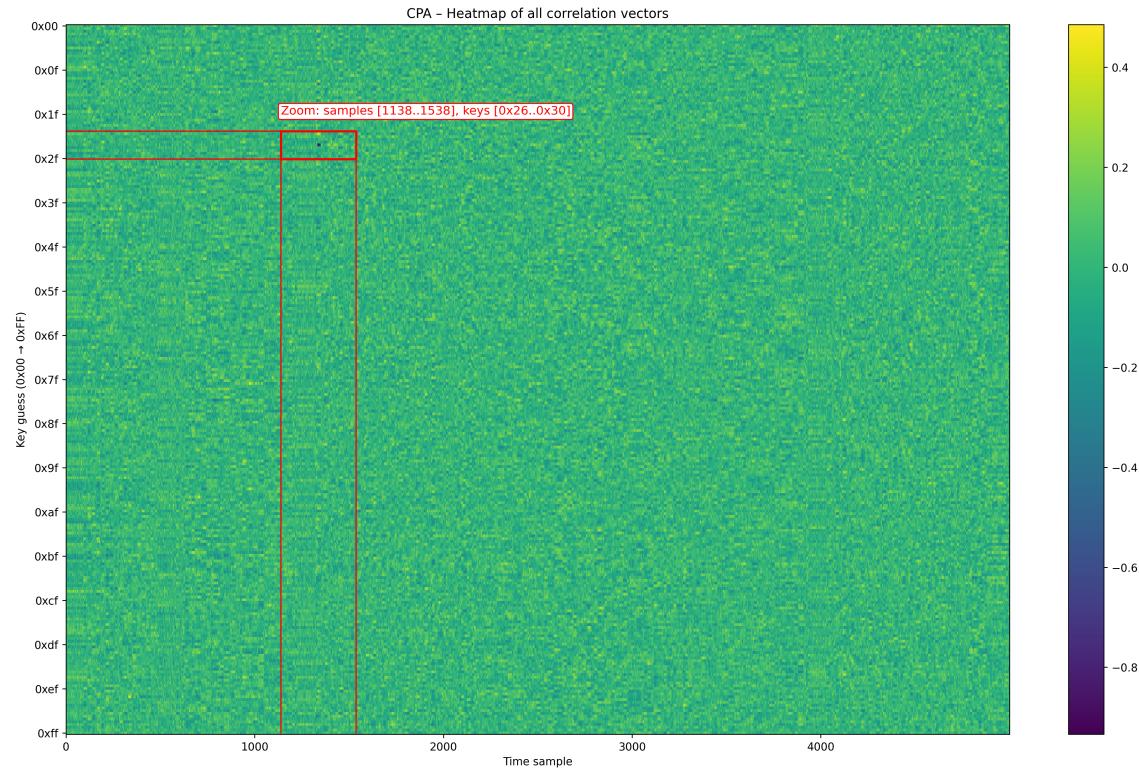
$$x_k = 0$$
$$y_k = -0.005$$



Calcul du vecteur de corrélation de PEARSON

CPA – Méthodologie de l'attaque

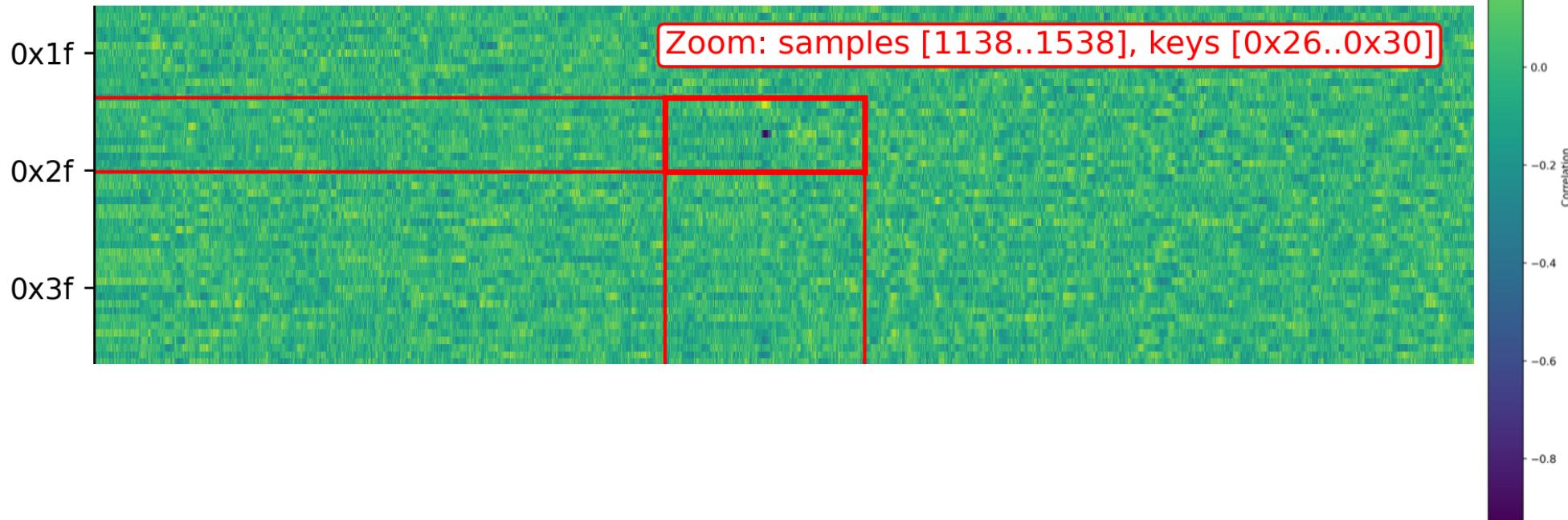
$$\rho(g, t) = \frac{\sum_k \text{hyp}_{g,c}[k] \cdot \text{traces}_c[k][t]}{\sqrt{\sum_k \text{hyp}_{g,c}[k]^2} \sqrt{\sum_k \text{traces}_c[k][t]^2}} \quad (9)$$



Calcul du vecteur de corrélation de PEARSON

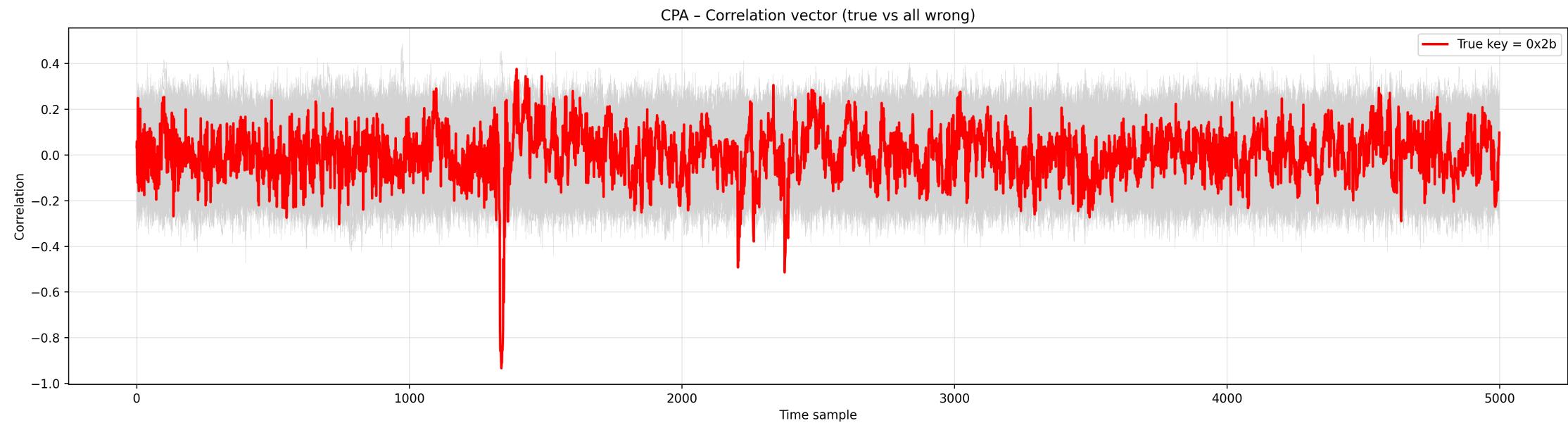
CPA – Méthodologie de l'attaque

$$\rho(g, t) = \frac{\sum_k \text{hyp}_{g,c}[k] \cdot \text{traces}_c[k][t]}{\sqrt{\sum_k \text{hyp}_{g,c}[k]^2} \sqrt{\sum_k \text{traces}_c[k][t]^2}} \quad (9)$$



Analyse du vecteur de corrélation

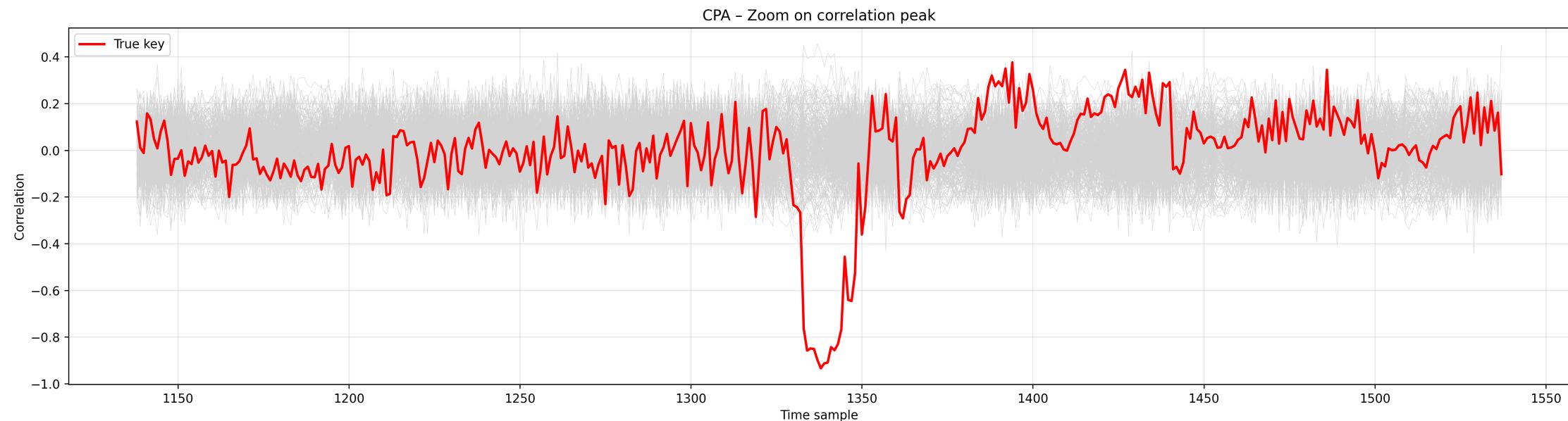
CPA – Méthodologie de l'attaque



Graphe précédent en 2D

Analyse du vecteur de corrélation

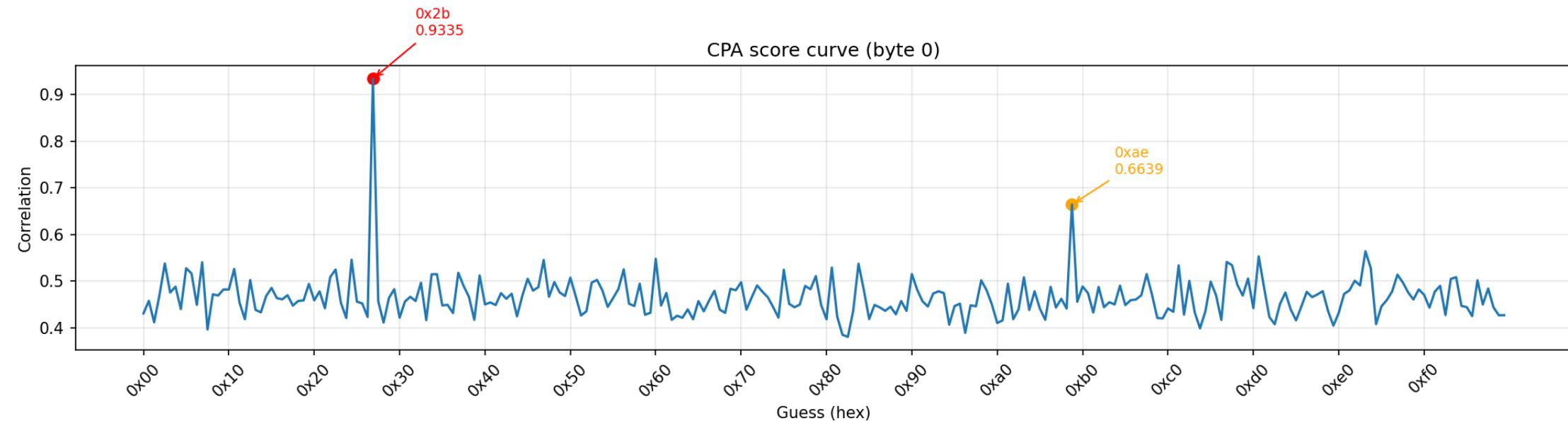
CPA — Méthodologie de l'attaque



Définition du score et sélection du byte

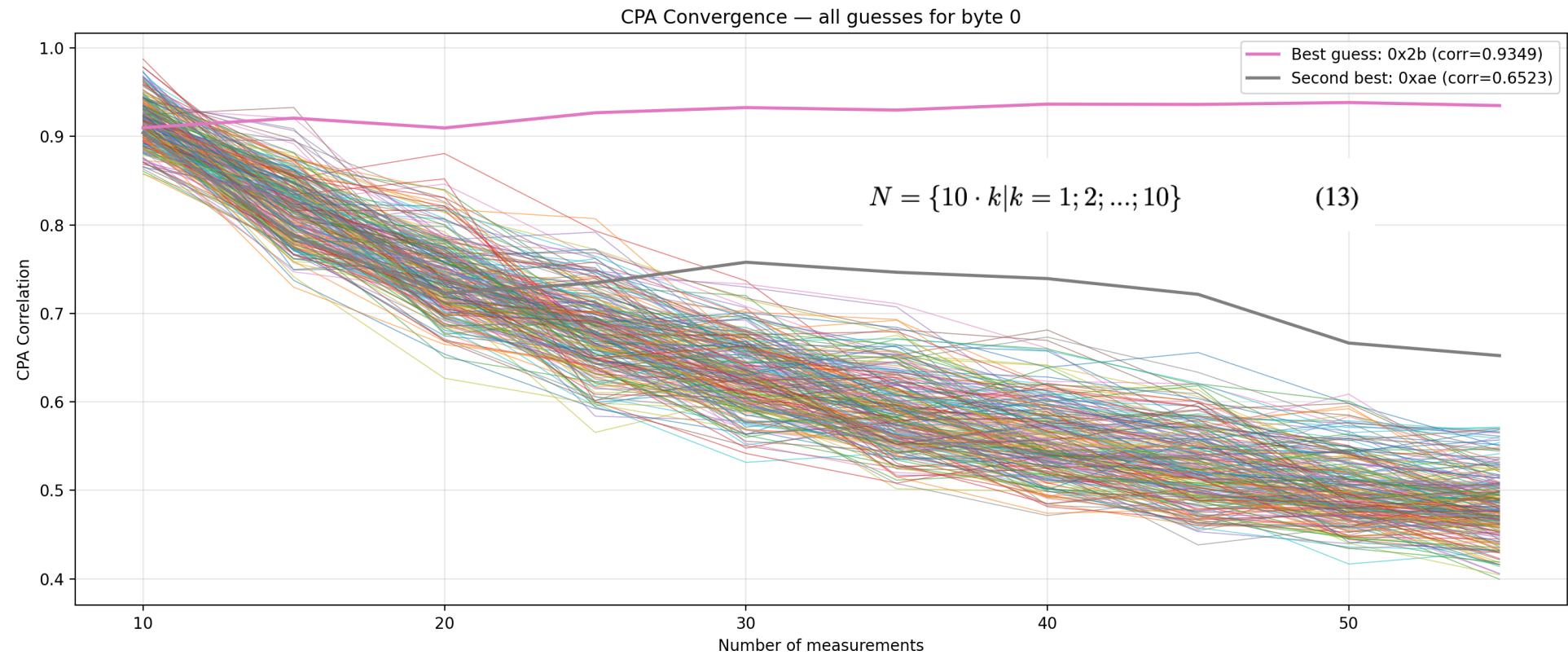
CPA — Méthodologie de l'attaque

$$\text{score}(g) = \max_t |\rho(g, t)| \quad (10)$$



Vitesse de convergence

CPA — Méthodologie de l'attaque



Résultat

CPA — Méthodologie de l'attaque

== CPA BYTE SUMMARY ==					
Byte	Guess	Correct	Status	Confidence	Second Best
0	0x2b	0x2b	OK	92.40%	
1	0x7e	0x7e	OK	100.00%	
2	0x15	0x15	OK	88.12%	
3	0x16	0x16	OK	85.76%	
4	0x28	0x28	OK	88.86%	
5	0xae	0xae	OK	84.90%	
6	0xd2	0xd2	OK	86.72%	
7	0xa6	0xa6	OK	72.50%	
8	0xab	0xab	OK	67.33%	
9	0xf7	0xf7	OK	63.53%	
10	0x15	0x15	OK	89.13%	
11	0x88	0x88	OK	80.76%	
12	0x09	0x09	OK	95.56%	
13	0xcf	0xcf	OK	98.42%	
14	0x4f	0x4f	OK	94.11%	
15	0x3c	0x3c	OK	80.67%	

Comparaison

Comparaison

	DPA (Differential Power Analysis)	CPA (Correlation Power Analysis)
Modèle de fuite	Binaire (dernier bit)	Analogique (poids de Hamming)
Méthode statistique	Différence de moyenne	Corrélation de Pearson
Besoins de traces	> 300	> 25
Résistance aux aléas	Moyenne	Très bonne
Vitesse de calcul	Très rapide	Plus longue (beaucoup de calcul à faire)
Taux de confiance moyen	43% (600 traces)	85% (100 traces)

Cas d'usages

Cas d'usages

- Evaluation de Secure Element pour la certification EAL5+
- Attaques sur les cartes ARM Cortex-M (STM32)
- Attaques sur les ESP32
- Implémentation AES sur FPGA

Merci de votre écoute