Ye YUAN, Kai-ge QU, Li-ji WU, Jia-wei MA, Xiang-min ZHANG, 2019. Correlation power attack on a message authentication code based on SM3. *Frontiers of Information Technology & Electronic Engineering,* 20(7):930-945. https://doi.org/10.1631/FITEE.1800312

Correlation power attack on a message authentication code based on SM3

Key words: HMAC-SM3; Side channel analysis; Correlation power attack; Bit-wise chosen-plaintext

Corresponding author: Kai-ge QU
E-mail: kaigequ@gmail.com

Motivation

1. As a Chinese Hash algorithm, the SM3 algorithm is gradually winning domestic market value in China.

2. The side channel security of HMAC based on SM3 (HMAC-SM3) is still to be evaluated, especially in hardware implementation, where only intermediate values stored in registers have apparent Hamming distance leakage.

3. The algorithm structure of SM3 determines the difficulty in HMAC-SM3 side channel analysis.

Main idea

1. In this study, we deal with one-round-per-cycle hardware implementation. The eight intermediate values mentioned are classified into two groups and specific attack strategies are designed for each group.

2. A tricky bit-wise chosen-plaintext attack strategy is proposed for the second group beyond the word-wise chosen-plaintext strategy proposed in Guo et al. (2015).

3.Bit-wise here refers to choosing each bit of one plaintext word as zero or random.

Guo LM, Wang LH, Liu D, et al., 2015. A chosen-plaintext differential power analysis attack on HMAC-SM3. 11th Int Conf on Computational Intelligence and Security, p.350-353. https://doi.org/10.1109/CIS.2015.91

Method

1. By putting the easy and tricky parts together, we achieve one procedure for attacking the whole key of HMAC-SM3 hardware implementation.

2. We evaluate the proposed method on a field programmable gate array (FPGA) board.

Method

3. Chosen-plaintext modes

Table 2 Chosen-plaintext modes and corresponding to-be-attacked intermediate values

No.	Plaintext mode	To-be-attacked intermediate value
1	$W_0,\ W_1,\ \ldots,\ W_{15}$ all random	$\theta_0 = (A_0 \oplus B_0 \oplus C_0) + D_0 + (((A_0 \lll 12) + E_0 + T) \lll 7 \oplus (A_0 \lll 12))$ $\varphi_0 = (E_0 \oplus F_0 \oplus G_0) + H_0 + ((A_0 \lll 12) + E_0 + T) \lll 7$
2	$W_0 = W_4 = 0$, others random	$\theta_1 = (\theta_0 \oplus A_0 \oplus (B_0 \lll 9)) + C_0 + (((\theta_0 \lll 12) + P_0(\varphi_0) + (T \lll 1)) \lll 7 \oplus (\theta_0 \lll 12))$ $\varphi_1 = (P_0(\varphi_0) \oplus E_0 \oplus (F_0 \lll 19)) + G_0 + ((\theta_0 \lll 12) + P_0(\varphi_0) + (T \lll 1)) \lll 7$
3	$W_0 = W_4 = 0$, $W_1 = W_5 = 0$, others random	$\theta_2 = (\theta_1 \oplus \theta_0 \oplus (A_0 \lll 9)) + (B_0 \lll 9) + (((\theta_1 \lll 12) + P_0(\varphi_1) + (T \lll 2)) \lll 7 \oplus (\theta_1 \lll 12))$ $\varphi_2 = (P_0(\varphi_1) \oplus P_0(\varphi_0) \oplus (E_0 \lll 19)) + (F_0 \lll 19) + ((\theta_1 \lll 12) + P_0(\varphi_1) + (T \lll 2)) \lll 7$
4	$W_0 = W_4 = 0$, $W_1 = W_5 = 0$, $W_2 = W_6 = 0$, others random	$\theta_3 = (\theta_2 \oplus \theta_1 \oplus (\theta_0 \lll 9)) + (A_0 \lll 9) + (((\theta_2 \lll 12) + P_0(\varphi_2) + (T \lll 3)) \lll 7 \oplus (\theta_2 \lll 12))$ $\varphi_3 = (P_0(\varphi_2) \oplus P_0(\varphi_1) \oplus (P_0(\varphi_0) \lll 19)) + (E_0 \lll 19) + ((\theta_2 \lll 12) + P_0(\varphi_2) + (T \lll 3)) \lll 7$

Method

4. Details of each word-wise chosen-plaintext CPA attack

Table 3 Details of each word-wise chosen-plaintext CPA attack

CPA No.	Chosen-plaintext mode	Time range for attack	Intermediate value(s)	Expression for power models
CPA 1	Mode 1	Round 0	θ_0, A_0	$\mathrm{HD}(A_0, A_1) = \mathrm{HW}(A_0 \oplus (\theta_0 + W_0'))$
CPA 2	Mode 1	Round 0	φ_0, E_0	$\mathrm{HD}(E_0, E_1) = \mathrm{HW}(E_0 \oplus P_0(\varphi_0 + W_0))$
CPA 3	Mode 2	Round 1	θ_1	$\mathrm{HD}(A_1, A_2) = \mathrm{HW}(\theta_0 \oplus (\theta_1 + W_1'))$
CPA 4	Mode 2	Round 1	φ_1	$\mathrm{HD}(E_1, E_2) = \mathrm{HW}(P_0(\varphi_0) \oplus P_0(\varphi_1 + W_1))$
CPA 5	Mode 3	Round 2	θ_2	$\mathrm{HD}(A_2, A_3) = \mathrm{HW}(\theta_1 \oplus (\theta_2 + W_2'))$
CPA 6	Mode 3	Round 2	φ_2	$\mathrm{HD}(E_2, E_3) = \mathrm{HW}(P_0(\varphi_1) \oplus P_0(\varphi_2 + W_2))$
CPA 7	Mode 4	Round 3	θ_3	$\mathrm{HD}(A_3, A_4) = \mathrm{HW}(\theta_2 \oplus (\theta_3 + W_3'))$
CPA 8	Mode 4	Round 3	φ_3	$\mathrm{HD}(E_3, E_4) = \mathrm{HW}(P_0(\varphi_2) \oplus P_0(\varphi_3 + W_3))$

Major results

1. Results of partial-CPA 1 toward θ_0

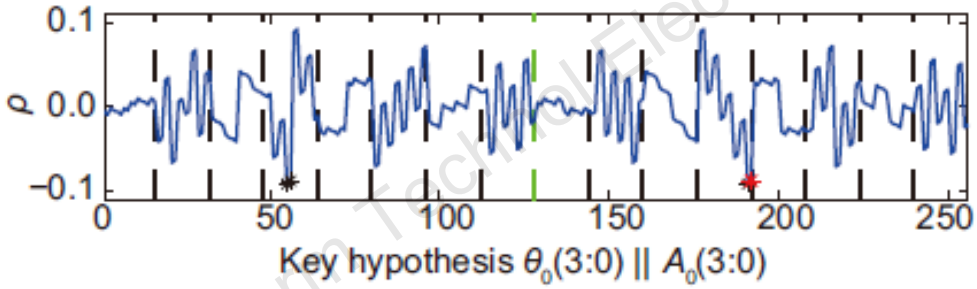

Fig. 4 Results of partial-CPA 1 toward θ_0 (References to color refer to the online version of this figure)

Major results

2. Results of partial-CPA 2 and 3 toward θ_0

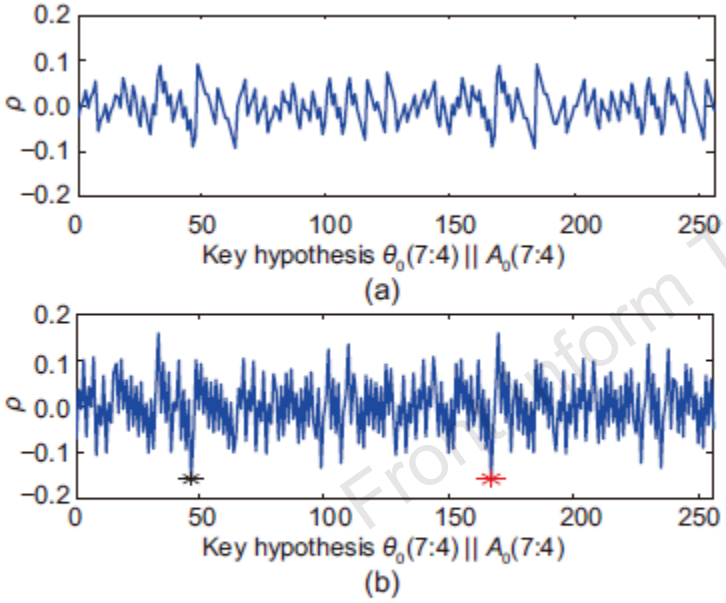

Fig. 5 Results of partial-CPA 2 toward θ_0: (a) candidate 1; (b) candidate 2

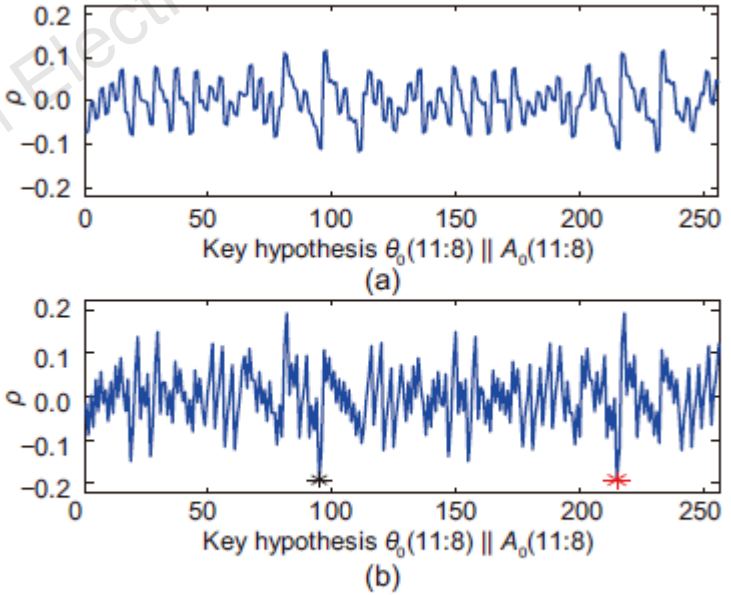

Fig. 6 Results of partial-CPA 3 toward θ_0: (a) candidate 1; (b) candidate 2

Major results

3. Results of partial-CPA 2 and 3 toward θ_1

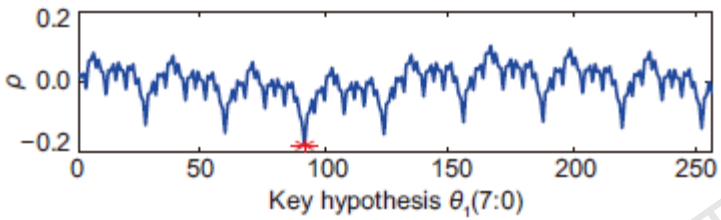

Fig. 8 Results of partial-CPA 1 toward θ_1

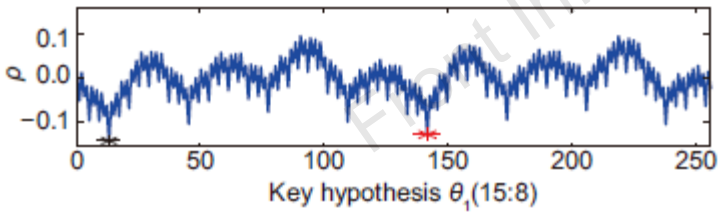

Fig. 9 Results of partial-CPA 2 toward θ_1

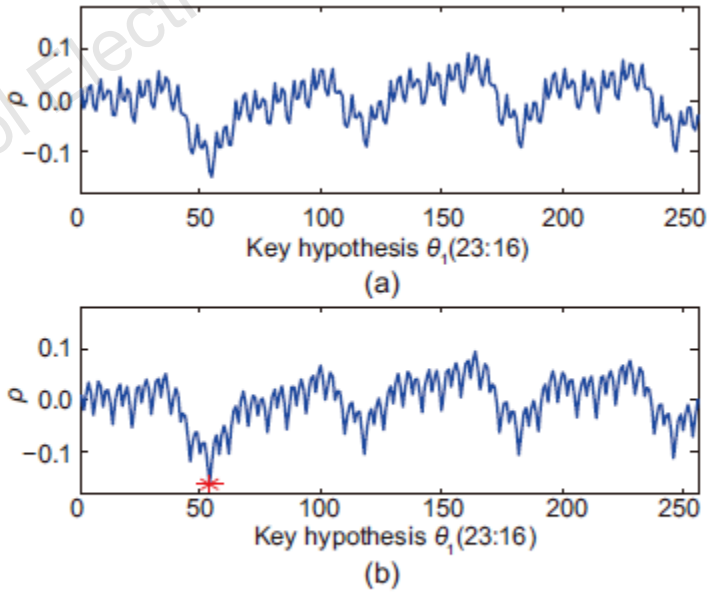

Fig. 10 Results of partial-CPA 3 toward θ_1: (a) candidate 1; (b) candidate 2

Major results

4. Results of partial-CPA 4 toward θ_1

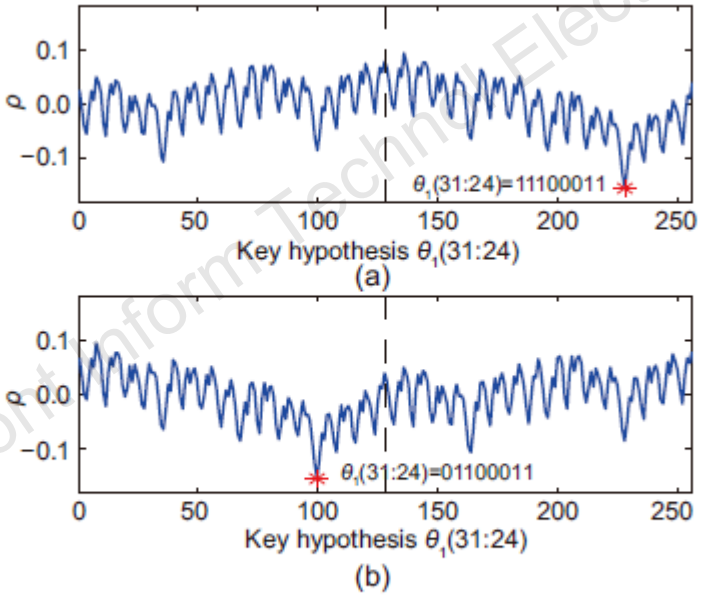

Fig. 11 Results of partial-CPA 4 toward θ_1 assuming $\theta_0(31) = 0$ (a) and $\theta_0(31) = 1$ (b)

Major results

5. Results of partial-CPA 1 toward φ_0

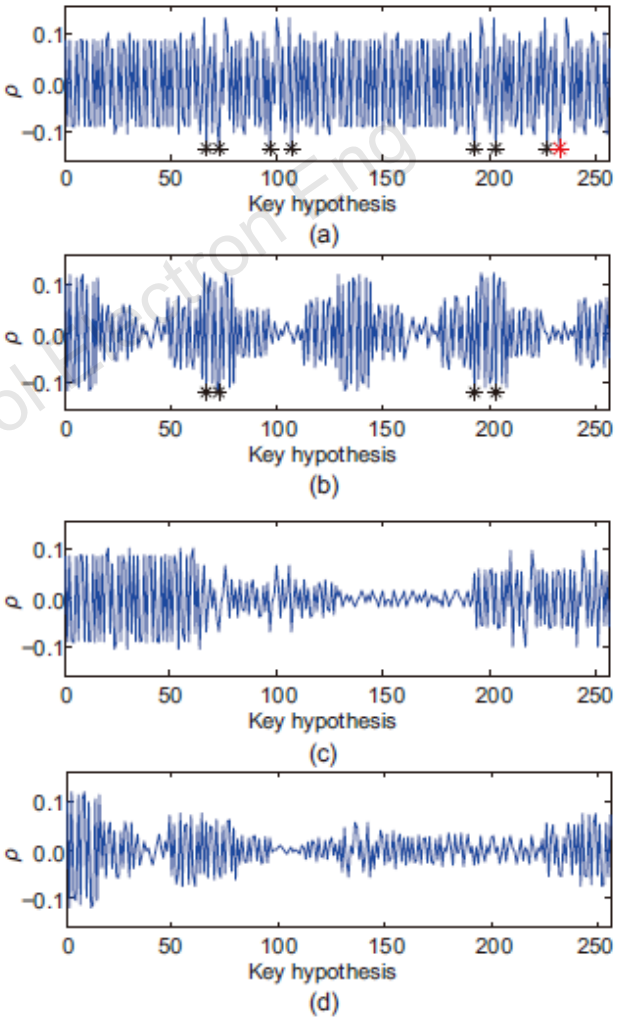

Fig. 14 Results of partial-CPA 1 toward φ_0: (a) case A; (b) case B; (c) case C; (d) case D

Major results

6. Results of partial-CPA 2 toward φ_0

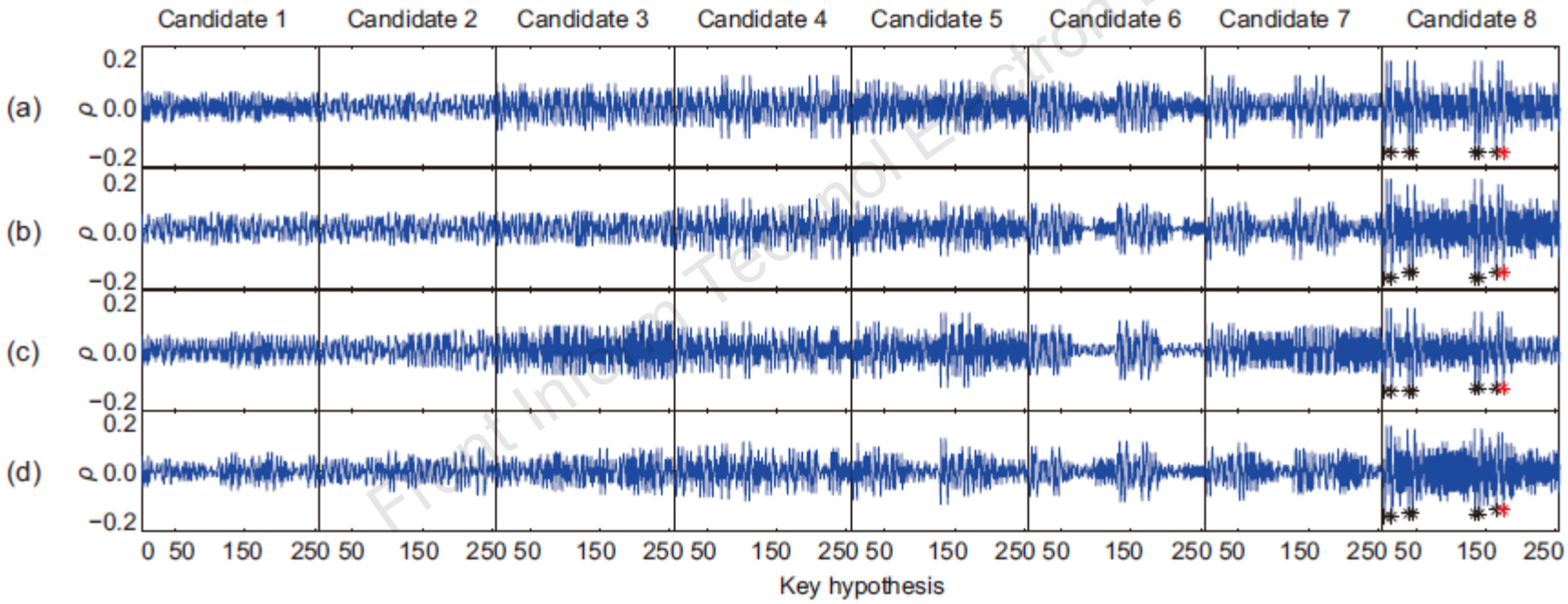

Fig. 16 Results of partial-CPA 2 toward φ_0: (a) case A; (b) case B; (c) case C; (d) case D

Each row represents one case of the power model of partial-CPA 2, while each column corresponds to one candidate for $\varphi_0(1:0)||\varphi_0(16:15)||\varphi_0(24:23)$ from the results of partial-CPA 1. In each sub-figure, the horizontal axis represents the value of the key hypothesis denoted by $\varphi_0(3:2)||\varphi_0(18:17)||\varphi_0(26:25)||E_0(3:2)$, and the vertical axis is the correlation coefficient ρ

Major results

7. Results of partial-CPA 3 toward φ_0

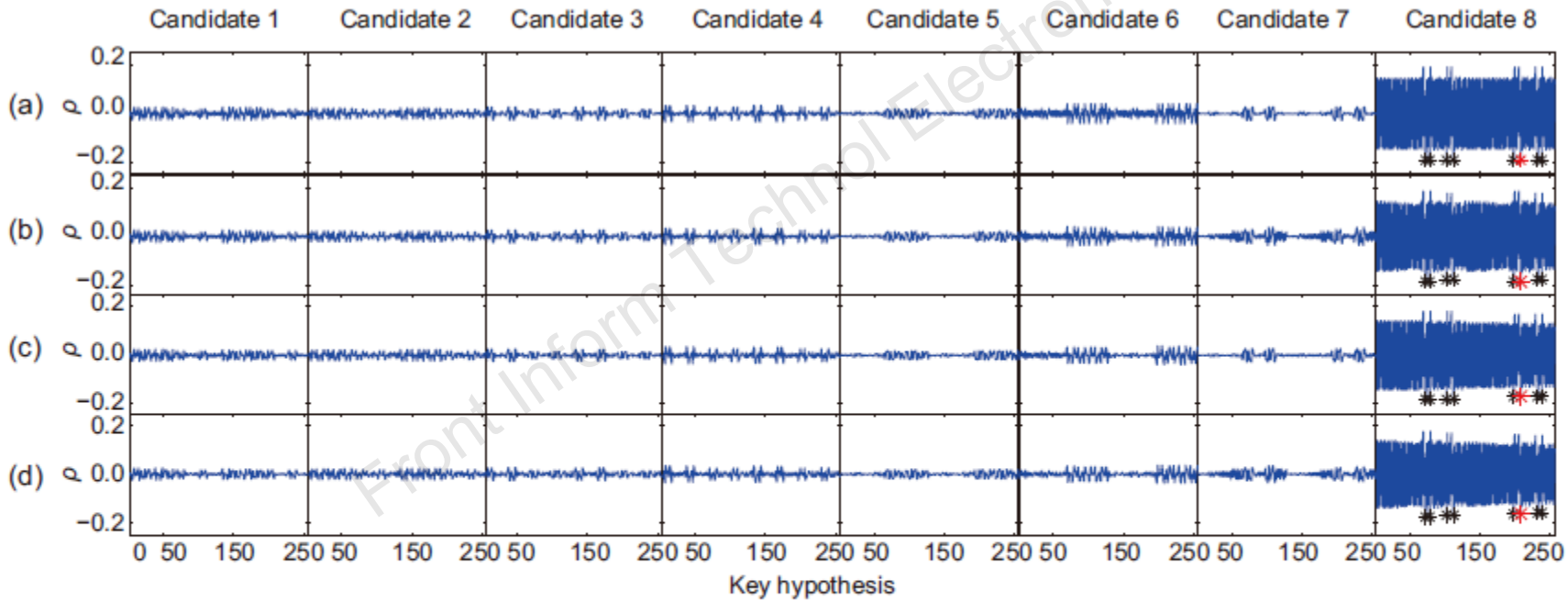

Fig. 19 Results of partial-CPA 3 toward φ_0: (a) case A; (b) case B; (c) case C; (d) case D

Each row represents one case of the power model of partial-CPA 3, while each column corresponds to one candidate for $\varphi_0(3:2)||\varphi_0(18:17)||\varphi_0(26:25)$ from the results of partial-CPA 2. In each sub-figure, the horizontal axis represents the value of the key hypothesis denoted by $\varphi_0(5:4)||\varphi_0(20:19)||\varphi_0(28:27)||E_0(5:4)$, and the vertical axis is the correlation coefficient ρ

Major results

8. Results of partial-CPA 4 toward φ_0

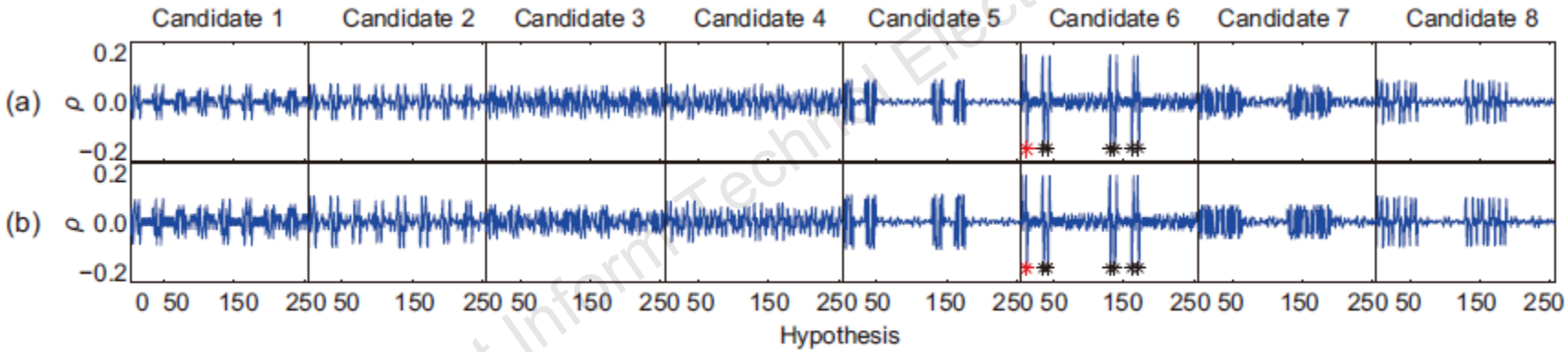

Fig. 20 Results of partial-CPA 4 toward φ_0: (a) case A; (b) case B

Major results

9. Results of partial-CPA 5 and 6 toward φ_0

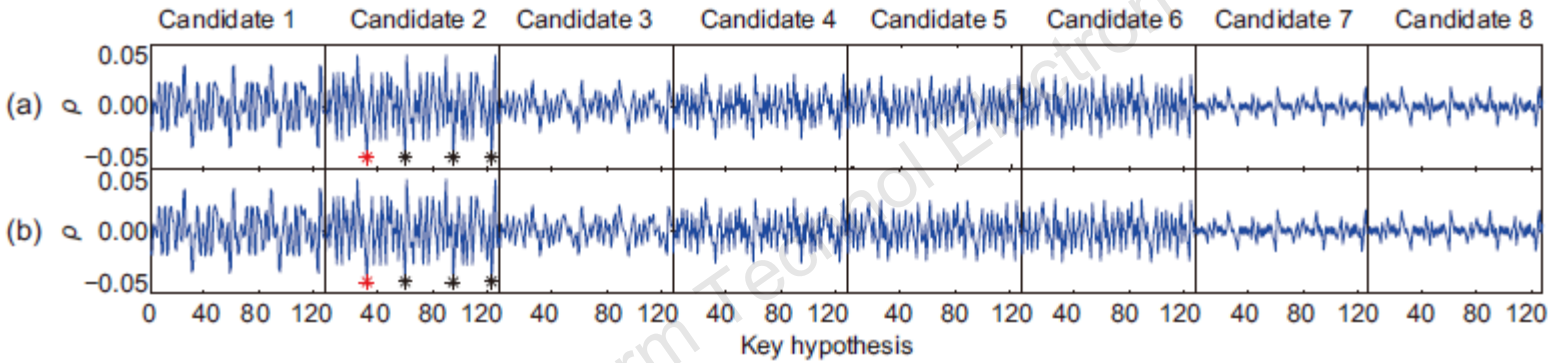

Fig. 22 Results of partial-CPA 5 toward φ_0: (a) case A; (b) case B

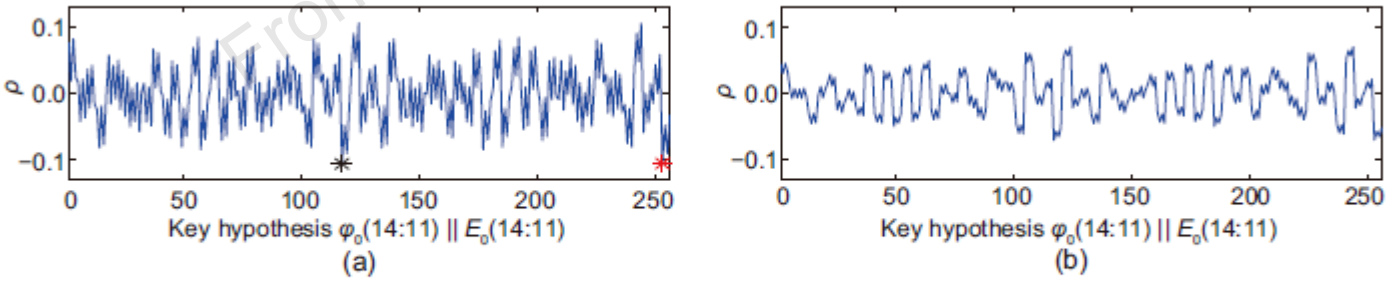

Fig. 24 Results of partial-CPA 6 toward φ_0: (a) candidate 1 ($\varphi_0(10:8) = 011$); (b) candidate 2 ($\varphi_0(10:8) = 111$)

Conclusions

1. The improved word-wise chosen-plaintext attack procedure theory was first given in this paper.

2. According to the different inherent properties of the two groups of secret values in the SM3 algorithm, the methods of divide-and-conquer for them are totally different. One is straightforward, and involves segmenting the long key into parallel shorter subkeys. The other is more trickier, requiring the bit-wise chosen-plaintext CPA attack procedure, which is the main focus of this paper.

3. For the recovery of the whole key, 39 partial-CPA attacks for the two groups were needed, and they should follow the strict sequence in the same group.