SCIENCE CHINA
Information Sciences

• **Supplementary File** •

Correlation Leakage Analysis on Masking Schemes

Jiawei Zhang[1], Yongchuan Niu[1*] & An Wang[2*]

[1] *Data Communication Science and Technology Research Institute, Beijing,* 100191*, China;*
[2] *School of Computer Science, Beijing Institute of Technology, Beijing,* 100081*, China*

Appendix A Proof of Proposition 1

Proof. Since $Z_1 = z \oplus M$, $Z_2 = M$ and M is uniformly distributed over $\mathbb{F}_2^n$, we have $\mathrm{E}[\mathrm{HW}(M)] = \mathrm{E}[\mathrm{HW}(z \oplus M)] = \frac{n}{2}$. Moreover, since B_1 and B_2 are independent and satisfy $\mathrm{E}[B_1] = \mathrm{E}[B_2] = 0$, we get

$$\mathrm{E}[L(Z_1)] = \mathrm{E}[\delta_1 + \mathrm{HW}(z \oplus M) + B_1] = \mathrm{E}[\mathrm{HW}(z \oplus M)] + \delta_1 = \frac{n}{2} + \delta_1 \tag{A1}$$

and

$$\mathrm{E}[L(Z_2)] = \mathrm{E}[\delta_2 + \mathrm{HW}(M) + B_2] = \mathrm{E}[\mathrm{HW}(M)] + \delta_2 = \frac{n}{2} + \delta_2. \tag{A2}$$

From Proposition 10 in [1], we have

$$\mathrm{E}[L(Z_1) \times L(Z_2)|Z = z] = -\frac{1}{2}\mathrm{HW}(z) + \frac{n^2+n}{4} + \frac{n}{2}(\delta_1 + \delta_2) + \delta_1\delta_2. \tag{A3}$$

The Lemma 20 in [1] gives that $\mathrm{E}[\mathrm{HW}(M)^2] = \mathrm{E}[\mathrm{HW}(z \oplus M)^2] = \frac{n^2+n}{4}$, and hence $\mathrm{E}[L(Z_1)^2] = \frac{n^2+n}{4} + n\delta_1 + \delta_1^2 + \sigma^2$ and $\mathrm{E}[L(Z_2)^2] = \frac{n^2+n}{4} + n\delta_2 + \delta_2^2 + \sigma^2$. As a result, we can get

$$\mathrm{Var}[L(Z_1)] = \mathrm{E}[L(Z_1)^2] - \mathrm{E}[L(Z_1)]^2 = \frac{n}{4} + \sigma^2 \tag{A4}$$

and

$$\mathrm{Var}[L(Z_2)] = \mathrm{E}[L(Z_2)^2] - \mathrm{E}[L(Z_2)]^2 = \frac{n}{4} + \sigma^2. \tag{A5}$$

By using (A1)-(A5), we can simplify (A6) to obtain Proposition 1.

$$\rho(L(Z_1), L(Z_2)|Z = z) = \frac{\mathrm{E}[L(Z_1) \times L(Z_2)|Z = z] - \mathrm{E}[L(Z_1)] \times \mathrm{E}[L(Z_2)]}{\sqrt{\mathrm{Var}[L(Z_1)]\mathrm{Var}[L(Z_2)]}} \tag{A6}$$

References

1 Prouff E, Rivain M, Bevan R. Statistical analysis of second order differential power analysis. IEEE Transactions on computers, 2009, 58(6): 799-811.

* Corresponding author (email: niuyongchuan@hotmail.com, wanganl@bit.edu.cn)