

Slicing Up a Perfect Hardware Masking



Zhimin Chen and Patrick Schaumont
Electrical and Computer Engineering Department
Virginia Tech



Side Channel Attack (SCA) presents a concern to crypto devices.

An SCA is any attack based on side-channel information gained from the physical implementation of a cryptosystem, such as power consumption, electromagnetic radiation, timing, and others. The basis of SCA is the relationship between the detectable side-channel information and the internal secret key. The setup of SCA is not complicated nor inexpensive.

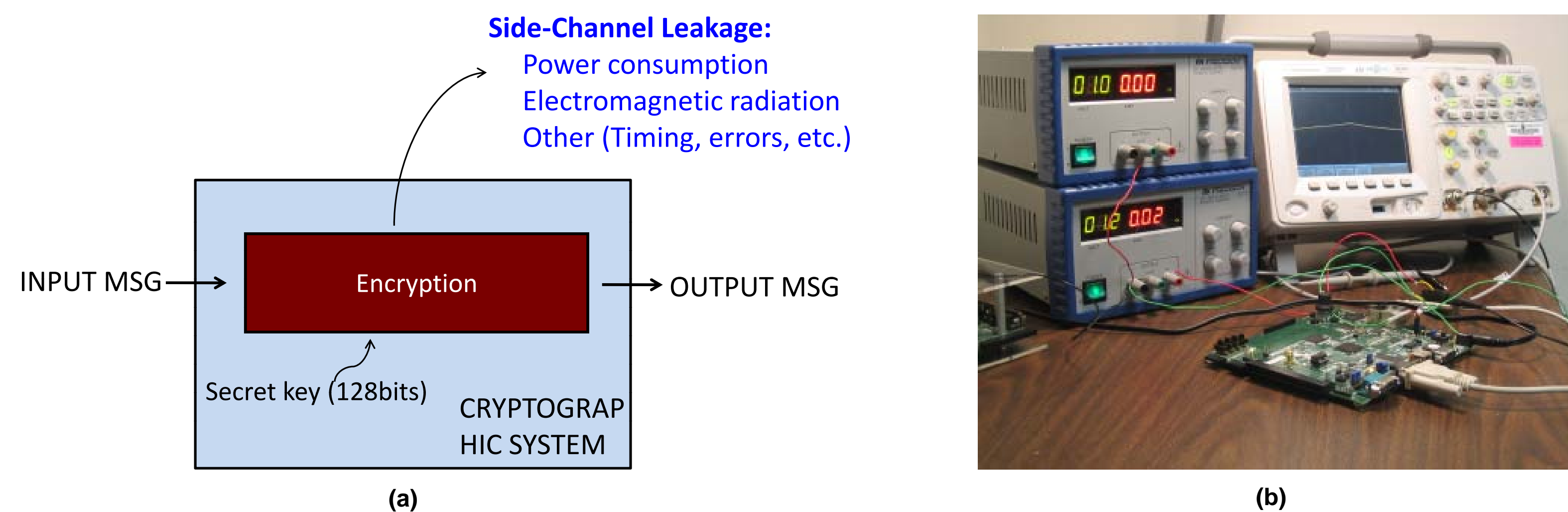


Figure 1. (a) Concept of Side-Channel Attack
(b) A setup of Side-Channel Attack.

Masking provides protects but still leaks information.

Masking is a popular countermeasure technique that makes use of random numbers, called masks, to randomize the internal circuit nodes and therefore eliminates correlation between those nodes and the actual processed data.

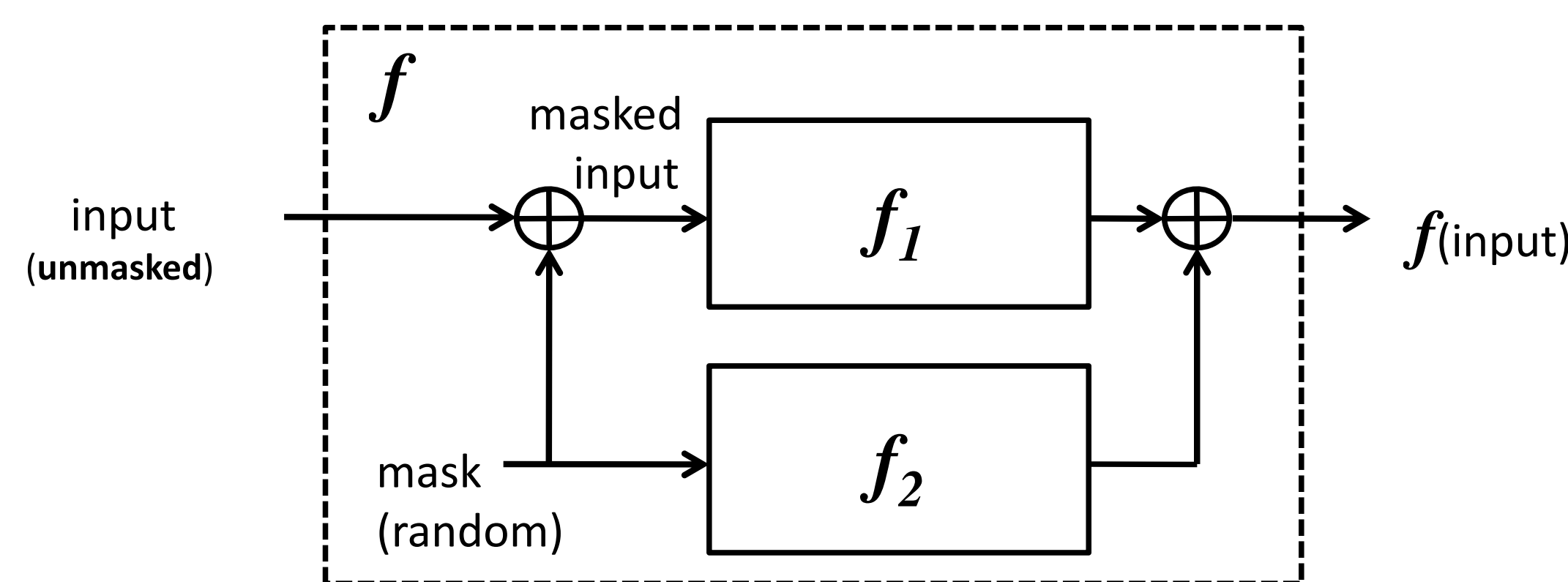


Figure 2. Concept of masking.

The mask should be treated as a secret. In other words, it should be an uniformly distributed and unbiased random variable. Mask variables have side-channel leakage, and our research shows that this can be used to mount an SCA.

Partial selection of the power samples introduces bias to the mask and eventually leads to a successful attack.

Side-channel leakage changes as mask changes. This enables a better-than-random guess of the mask. Once the conditional probability of the mask is biased, the cryptosystem is not secure anymore.

Experiments on a masked AES SBox in combination with a key addition (key=0x23) has been done. We found partial selection of the power samples introduces bias to the mask. Subsequently, successful attack was mounted.

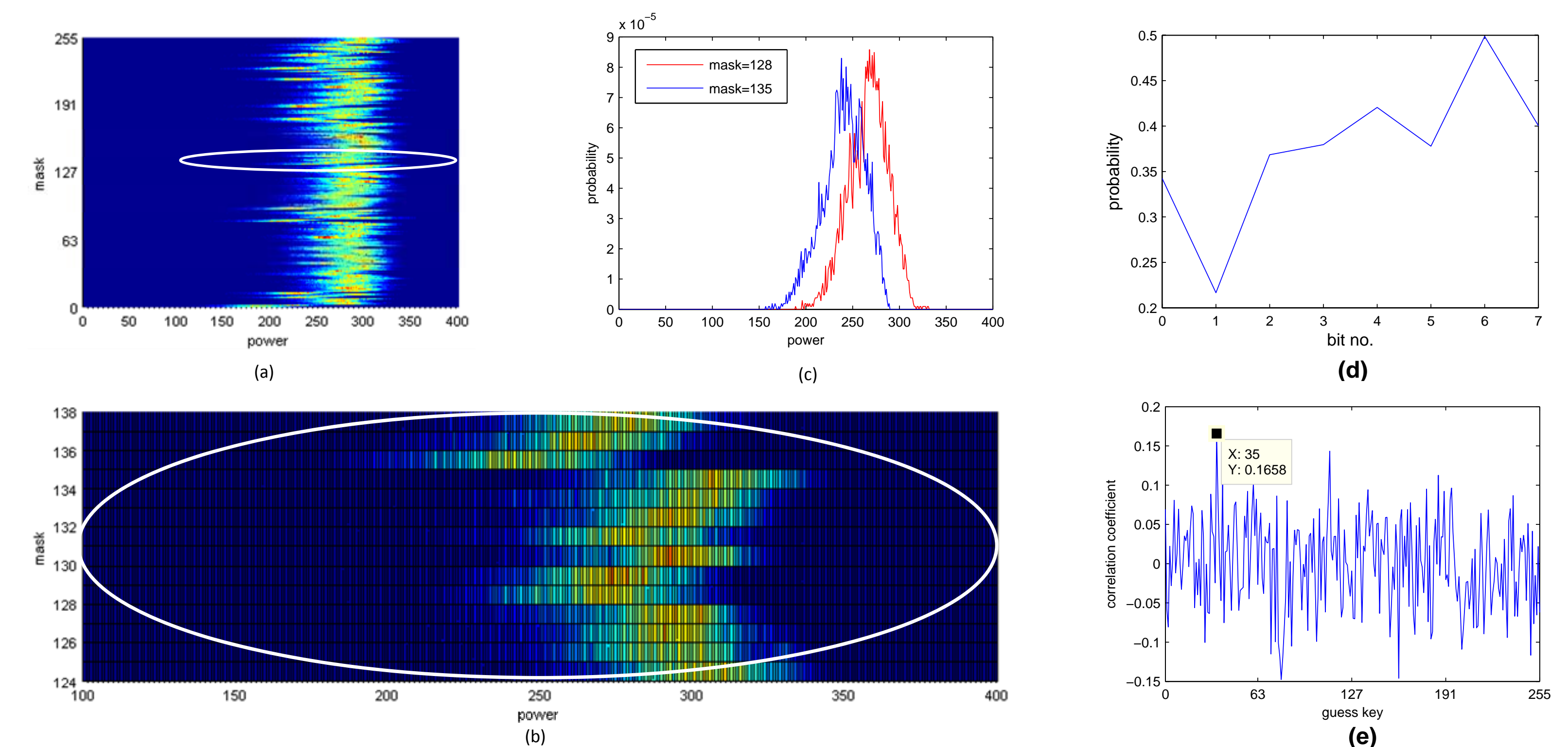


Figure 3. Experimental results:

(a) Joint probability of *power* and *mask*; (b) Detailed view of the elliptical area of (a); (c) Joint probability of *power* and *mask* when $m = 128$ and $m = 135$ illustrates dependence of the power on the mask; (d) Conditional probability of each mask bit after partial selection; (e) Attack result based on partial selection.

Conclusion

Hardware masking remains susceptible to direct DPA because of the relationship between the mask and side-channel leakage.

Acknowledgments

This work was supported in part by NSF Grant No. 0644070. We would also like to express our gratitude to Kris Tiri.