On the Correctness of An Approach Against Side-channel attacks

Peng Wang[1] and Dengguo Feng[2] and Wenling Wu[2] and Liting Zhang[2]

[1] State Key Laboratory of Information Security
Graduate University of Chinese Academy of Sciences, Beijing 100049, China
wp@is.ac.cn
[2] State Key Laboratory of Information Security
Institution of Software of Chinese Academy of Sciences, Beijing 100080, China
{feng,wwl,zhangliting}@is.iscas.ac.cn

Abstract. Side-channel attacks are a very powerful cryptanalytic technique. Li and Gu [ProvSec'07] proposed an approach against side-channel attacks, which states that a symmetric encryption scheme is IND-secure in side-channel model, if it is IND-secure in black-box model and there is no adversary who can recover the whole key of the scheme computationally in side-channel model, i.e. WKR-SCA $\wedge$ IND $\rightarrow$ IND-SCA. Our researches show that it is not the case. We analyze notions of security against key recovery attacks and security against distinguishing attacks, and then construct a scheme which is WKR-SCA-secure and IND-secure, but not IND-SCA-secure in the same side-channel environment. Furthermore, even if the scheme is secure again partial key recovery attacks in side-channel model, this approach still does not hold true.

Key words: Provable security, Side-channel attack, Symmetric encryption.

1 Introduction

In traditional cryptanalysis, an adversary has only black-box access to cryptographic algorithms, i.e. the adversary can query the keyed cryptographic algorithm with input of its choice and get the corresponding output, but it can not get any other information of what's going on during the computation of the output. Unfortunately, in physical implementations, this kind of information sometimes can be easily obtained, such as timing information [8], power consumption [7], electromagnetic leakage [4], etc. We call the attacks based on this leaked information side-channel attacks. The researches in the last decade

show that side-channel attacks are a very powerful cryptanalytic technique. The security of some cryptographic algorithms may collapse suddenly given some tiny side-channel information, even though they are very secure in traditional cryptanalysis.

The black-box model illustrates a theoretical world in which we focus on design in the level of algorithm, on the other hand the side-channel model illustrates a practical world in which we have to face the leaked information in implementations. We have millions of experiences on designing secure cryptographic algorithms in black-box model. *But how to guarantee the security of the algorithms in side-channel model?*

Let's first look at some notions of security. The minimal security requirement is the privacy of the secret key. Key recovery attacks are often used to analyze the security of cryptographic primitives such as block cipher both in black-box model [2, 3] and side-channel model [6]. Recently the researches on how to establish a unified framework to evaluate the implementation security also focus on key recovery attacks [10–12]. If no adversary can recover the whole key computationally, we say it is WKR-secure (in black-box mode) or WKR-SCA-secure (in side-channel model)[3]. If no adversary can recover any part of key computationally, we say it is PKR-secure (in black-box mode) or PKR-SCA-secure (in side-channel model).

But as to a concrete cryptographic scheme, we need a corresponding security notion. For example, an encryption scheme requires the privacy of the plaintext, i.e. any adversary can not learn any information of the plaintext (except the length) computationally given a challenge ciphertext. This notion was firstly defined by Goldwasser and Micali as semantic security [5], which is equivalent to indistinguishability of the ciphertexts [5, 1]. If no information about the plaintext (except the length) is revealed computationally by the ciphertext, we say the scheme is IND-secure (in black-box mode) or IND-SCA-secure (in side-channel model).

Li and Gu proposed an approach against side-channel attacks in ProvSec 2007 [9], which states that if a symmetric encryption scheme is both WKR-SCA-secure and IND-secure, then it is IND-SCA-secure. In other words, in order to guarantee the practically security of the scheme, we only need to guarantee the theoretically security of the scheme and there is no adversary who can recover the whole key of the scheme computationally in the practical world.

Unfortunately, it is not the case.

[3] The notion of WKR is the same as the notion of UB in [9], which means "unbreakability of the key".

Our results are based on the following two basic observations:

- The notion of WKR (WKR-SCA) is much weaker than the notion of IND (IND-SCA).
- The security of the scheme in side-channel model is closely related to the leaked information.

Our contributions. We first analyze the relations among PKR, WKR and IND both in black-box model and side-channel model. Please see Figure 1 and Figure 2, which show that WKR is the weakest notion, and PKR and IND are incomparable. We give proofs for all the implications of the notions and construct concrete examples for all the separations of the notions.

We then explore the security of notion combination. Our results show that WKR-SCA $\wedge$ IND does not imply IND-SCA. Given a symmetric encryption scheme which is IND-secure, we can construct a scheme which is both IND-secure and WKR-SCA-secure, but not IND-SCA-secure in the same side-channel environment.

Furthermore, we show that even the scheme is PKR-SCA-secure and IND-secure, this approach still does not hold. Based on a symmetric encryption scheme which is both PKR-secure and IND-secure, we construct a new scheme which is both PKR-SCA-secure and IND-secure, but not IND-SCA-secure in the same side-channel environment.

2 Preliminaries

Notations. We write $s \xleftarrow{\$} S$ to denote choosing a random element s from a set S by uniform distribution. An *adversary* is an (randomized) algorithm with access to one or more oracles which are written as superscripts. We write the adversary $\mathbf{A}$ with oracle $\mathcal{O}$ outputing a bit b as $\mathbf{A}^{\mathcal{O}} \Rightarrow b$. $\mathbf{Adv}^{\mathrm{GGG}}_{SSS}(\mathbf{A})$ denotes the advantage of $\mathbf{A}$ attacking a scheme "SSS" with a goal of "GGG".

$\mathsf{A} \rightarrow \mathsf{B}$ means any scheme meeting notion A also meets notion B and $\mathsf{B} \nrightarrow \mathsf{A}$ means there exists a scheme meeting notion B but do not meets notion A.

Symmetric Encryption Scheme. A *symmetric encryption scheme* $\mathcal{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ consists of three algorithms. The randomized *key generation algorithm* $\mathcal{K}$ generates a key K, denoted as $K \leftarrow \mathcal{K}$. The randomized or stateful *encryption algorithm* $\mathcal{E}$ takes the key K and a plaintext M to return a ciphertext C, denoted as $C \leftarrow \mathcal{E}_K(M)$. The deterministic and sateless *decryption algorithm* $\mathcal{D}$ takes the

key K and a string C to return the corresponding plaintext M or the symbol $\perp$, denoted as $x \leftarrow \mathcal{D}$, where $x \in \{0,1\}^* \cup \{\perp\}$. We require that $\mathcal{D}_K(\mathcal{E}_K(M)) = M$ for any plaintext M.

In this paper, we focus on the security of symmetric encryption scheme under chosen plaintext attacks.

Side-channel Leakage Function. In side-channel attacks, the adversary not only can query the encryption oracle $\mathcal{E}_K$ and get the corresponding ciphertext, but also can get some side-channel information during the computation of the ciphertext. We notice that the side-channel information is relevant to the key K and the queried plaintext M, so we treat it as a function $L(K, M)$ and call it a leakage function. We define a new oracle $\mathcal{E}_K^+(M) = (\mathcal{E}_K(M), L(K, M))$ which returns both the ciphertext and the leaked information. Therefore in side-channel attacks, the adversary has actually oracle access to $\mathcal{E}_K^+(\cdot)$[4].

Security against Key Recovery Attacks. Key recovery attacks aim to recover the whole or partial key of the cryptographic algorithm. We define two kinds of security of symmetric encryption scheme against key recovery attacks both in black-box model and in side-channel model. In whole key recovery attacks, the adversary tries to recovery the full key.

Definition 1 (WKR and WKR-SCA). *Let $\mathcal{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ be a symmetric encryption scheme. Consider following two advantages:*

$$\mathbf{Adv}_{\mathcal{SE}}^{\mathrm{WKR}}(\mathbf{A}) = \Pr[K \leftarrow \mathcal{K}, \mathbf{A}^{\mathcal{E}_K(\cdot)} \Rightarrow K' : K = K'],$$

$$\mathbf{Adv}_{\mathcal{SE}}^{\text{WKR-SCA}}(\mathbf{A}) = \Pr[K \leftarrow \mathcal{K}, \mathbf{A}^{\mathcal{E}_K^+(\cdot)} \Rightarrow K' : K = K'].$$

We say that $\mathcal{SE}$ is secure against whole key recovery attacks in black-box model (in side-channel model), or WKR-*secure* (WKR-SCA-*secure*), *if the advantage* $\mathbf{Adv}_{\mathcal{SE}}^{\mathrm{WKR}}(\mathbf{A})$ ($\mathbf{Adv}_{\mathcal{SE}}^{\mathrm{WKR}}(\mathbf{A})$) *is negligible for any adversary* $\mathbf{A}$ *with feasible resources.*

In partial key recovery attacks, the adversary tries to recover any information of the key. We adopt a simulator-based definition, in which we use a function $f(K)$ to represent the targeted information of the key and define the security

[4] In [9], the adversary has oracle access to $\mathcal{E}_K(\cdot)$ and $S_K^*(\cdot)$ in side-channel model, where the input to $S_K^*(\cdot)$ is the side-channel information and the output of $S_K^*(\cdot)$ is a key $K' \in \{0,1\}^* \cup \{\perp\}$. This formalization conceals where the side-channel information comes from, and brings about confusions in subsequent discussions.

against partial key recovery attacks as whatever an adversary $\mathbf{A}$ with oracle $\mathcal{E}_K$ ($\mathcal{E}_K^+$) can do, a simulator $\mathbf{S}$ without oracle also can do.

Definition 2 (PKR and PKR-SCA). *Let $\mathcal{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ be a symmetric encryption scheme. Consider following two advantages:*

$$\begin{aligned}
&\mathbf{Adv}^{\mathrm{PKR}}_{\mathcal{SE}}(\mathbf{A}, \mathbf{S}) \\
=&\Pr[K \leftarrow \mathcal{K}, \mathbf{A}^{\mathcal{E}_K(\cdot)} \Rightarrow b : f(K) = b] - \Pr[K \leftarrow \mathcal{K}, \mathbf{S} \Rightarrow b : f(K) = b], \\
&\mathbf{Adv}^{\mathrm{PKR\text{-}SCA}}_{\mathcal{SE}}(\mathbf{A}, \mathbf{S}) \\
=&\Pr[K \leftarrow \mathcal{K}, \mathbf{A}^{\mathcal{E}_K^+(\cdot)} \Rightarrow b : f(K) = b] - \Pr[K \leftarrow \mathcal{K}, \mathbf{S} \Rightarrow b : f(K) = b],
\end{aligned}$$

where $f : \{0,1\}^* \to \{0,1\}^*$ is a function. We say that $\mathcal{SE}$ is secure against partial key recovery attacks in black-box model (in side-channel model), or PKR*-secure* (PKR-SCA*-secure*)*, if for any function f and any adversary $\mathbf{A}$ with feasible resources, there exists an algorithm $\mathbf{S}$ (we often call it a simulator) with feasible resources, such that the advantage $\mathbf{Adv}^{\mathrm{PKR}}_{\mathcal{SE}}(\mathbf{A}, \mathbf{S})$ ($\mathbf{Adv}^{\mathrm{PKR\text{-}SCA}}_{\mathcal{SE}}(\mathbf{A}, \mathbf{S})$) is negligible.*

Security against Distinguishing Attacks. We adopt the security definition of Real-Or-Random in [1] for symmetric encryptions, which define the security as indistinguishability of ciphertexts of required plaintexts and ciphertexts of random strings.

Definition 3 (IND and IND-SCA). *Let $\mathcal{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ be a symmetric encryption scheme. Consider following two advantages:*

$$\mathbf{Adv}^{\mathrm{IND}}_{\mathcal{SE}}(\mathbf{A}) = \Pr[K \leftarrow \mathcal{K}, \mathbf{A}^{\mathcal{E}_K(\cdot)} \Rightarrow 1] - \Pr[K \leftarrow \mathcal{K}, \mathbf{A}^{\mathcal{E}_K(\$(\cdot))} \Rightarrow 1],$$

$$\mathbf{Adv}^{\mathrm{IND}}_{\mathcal{SE}}(\mathbf{A}) = \Pr[K \leftarrow \mathcal{K}, \mathbf{A}^{\mathcal{E}_K^+(\cdot)} \Rightarrow 1] - \Pr[K \leftarrow \mathcal{K}, \mathbf{A}^{\mathcal{E}_K^+(\$(\cdot))} \Rightarrow 1],$$

where $\$(\cdot)$ returns a random string with the same length of the input. We say that $\mathcal{SE}$ is secure against distinguishing attacks in black-box model (in side-channel model), or IND*-secure* (IND-SCA*-secure*)*, if the advantage $\mathbf{Adv}^{\mathrm{IND}}_{\mathcal{SE}}(\mathbf{A})$ ($\mathbf{Adv}^{\mathrm{IND\text{-}SCA}}_{\mathcal{SE}}(\mathbf{A})$) is negligible for any adversary $\mathbf{A}$ with feasible resources.*

3 KR vs. IND in Block-box Model

In this section, we elaborate the implications or separations of the notions summarized in Figure 1.

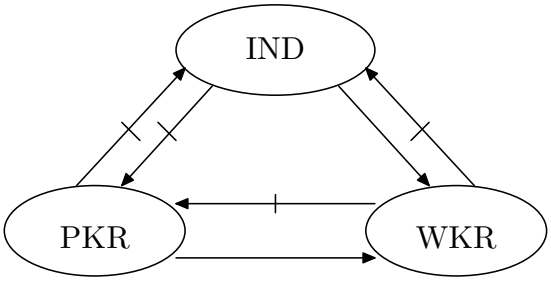

Fig. 1. Relations among PKR, WKR and IND.

Theorem 1 (PKR → WKR). *Let $\mathcal{SE}$ be an encryption scheme. If $\mathcal{SE}$ is* PKR*-secure, then it is* WKR*-secure as well.*

Proof. If $\mathbf{A}$ is an adversary against WKR-security, we construct an adversary $\mathbf{B}$ against PKR-security: run $\mathbf{A}$ and get K', then return K'. We set $f = ID$ where ID is the identical transformation, then for any simulator $\mathbf{S}$, we have $\mathbf{Adv}^{\mathrm{PKR}}_{\mathcal{SE}}(\mathbf{B}, \mathbf{S}) \geq \mathbf{Adv}^{\mathrm{PKR}}_{\mathcal{SE}}(\mathbf{A}) - 1/2^k$, where k is the length of the key. □

Theorem 2 (IND → WKR). *Let $\mathcal{SE}$ be a symmetric encryption scheme. If $\mathcal{SE}$ is* IND*-secure, then it is* WKR*-secure as well.*

Proof. If $\mathbf{A}$ is an adversary against WKR-security, we construct an adversary $\mathbf{B}$ against IND-security: run $\mathbf{A}$ and get K', then query $M \in \{0,1\}^n$ and get C, if $\mathcal{E}_{K'}(M) = C$, then return 1, else return 0. We have that $\mathbf{Adv}^{\mathrm{IND}}_{\mathcal{SE}}(\mathbf{B}) \geq \mathbf{Adv}^{\mathrm{WKR}}_{\mathcal{SE}}(\mathbf{A}) - 1/2^n$. □

Proposition 1 (PKR ↛ IND). *There exists a symmetric encryption scheme which is* PKR*-secure, but not* PKR*-secure.*

Proof. We construct a symmetric encryption scheme $\mathcal{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$, where $\mathcal{E}_K(M) = M$, i.e. the encryption algorithm is an identical transformation and has nothing to do with the key K. Hence no matter how the adversary queries the encryption oracle, no information about K is obtained. More specifically, for any function f and adversary $\mathbf{A}$ against PKR-security, the simulator $\mathbf{S}$ just runs $\mathbf{A}^{ID(\cdot)}$ and returns whatever $\mathbf{A}$ returns, where $ID(\cdot)$ is the identical transformation. Then $\mathbf{Adv}^{\mathrm{PKR}}_{\mathcal{SE}}(\mathbf{A}, \mathbf{S}) = 0$.

Furthermore, the identical transformation reveals all the information about the plaintext. More specifically, the adversary $\mathbf{B}$ just queries $M \in \{0,1\}^n$, if the answer is M then return 1, else return 0. We have $\mathbf{Adv}^{\mathrm{IND}}_{\mathcal{SE}}(\mathbf{B}) = 1 - 1/2^n$. □

Proposition 2 (IND ↛ PKR). *Given a symmetric encryption scheme $\mathcal{SE}$ which is* IND*-secure, we can construct a symmetric encryption scheme $\mathcal{SE}'$ which is also* IND*-secure, but not* PKR*-secure.*

Proof. Suppose $\mathcal{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ is IND-secure. We construct $\mathcal{SE}' = (\mathcal{K}', \mathcal{E}', \mathcal{D}')$ as follows:

	$\mathcal{SE}$	$\mathcal{SE}'$
Key generation	$K \leftarrow \mathcal{K}$	$K_1 \leftarrow \mathcal{K}, K_2 \xleftarrow{\$} \{0,1\}^n$
Encryption	$\mathcal{E}_K(M)$	${\mathcal{E}'}_{K_1K_2}(M) = \mathcal{E}_{K_1}(M)\|\|K_2$
Decryption	$\mathcal{D}_K(C)$	${\mathcal{D}'}_{K_1K_2}(C) = \mathcal{D}_{K_1}(C)$

The new encryption scheme $\mathcal{SE}'$ generates an extra key $K_2 \in \{0,1\}^n$, but reveals it in the ciphertext. If $\mathcal{SE}$ is IND-secure, then $\mathcal{SE}'$ is also IND-secure. More specifically, for any adversary $\mathbf{A}$ attacking $\mathcal{SE}'$, we construct adversary $\mathbf{B}^{\mathcal{O}}$ attacking $\mathcal{SE}$: $K_2 \xleftarrow{\$} \{0,1\}^n$, run $\mathbf{A}$, when $\mathbf{A}$ queries M, answer it with $\mathcal{O}(M)||K_2$, and return whatever $\mathbf{A}$ returns. We have $\mathbf{Adv}^{\mathrm{IND}}_{\mathcal{SE}}(\mathbf{B}) = \mathbf{Adv}^{\mathrm{IND}}_{\mathcal{SE}'}(\mathbf{A})$.

Furthermore, the ciphertext reveals the partial key of the $\mathcal{SE}'$, so it is not PKR-secure. More specifically, given the function $f(K_1K_2) = K_2$ and the adversary $\mathbf{A}$ which returns K_2 after arbitrary one query, any simulator $\mathbf{S}$ has no information about K_2, therefore $\mathbf{Adv}^{\mathrm{PKR}}_{\mathcal{SE}'}(\mathbf{A}, \mathbf{S}) \geq 1 - 1/2^n$. □

Corollary 1 (WKR $\nrightarrow$ IND). *There exists a symmetric encryption scheme $\mathcal{SE}$ which is* WKR*-secure, but not* IND*-secure.*

Proof. We have PKR $\rightarrow$ WKR by Theorem 1. If WKR $\rightarrow$ IND, then PKR $\rightarrow$ IND. That contradicts Proposition 1. □

Corollary 2 (WKR $\nrightarrow$ PKR). *There exists a symmetric encryption scheme $\mathcal{SE}$ which is* WKR*-secure, but not* PKR*-secure.*

Proof. We have IND $\rightarrow$ WKR by Theorem 2. If WKR $\rightarrow$ PKR, then IND $\rightarrow$ PKR. That contradicts Proposition 2. □

4 KR vs. IND in Side-channel Model

Attacks in black-box model can be regarded as special attacks in side-channel model when the leakage function returns nothing. Therefore the separations of the notions still hold in side-channel model. It is easy to verify the implications of the notions also hold in side-channel model. We summarize these results in Figure 2.

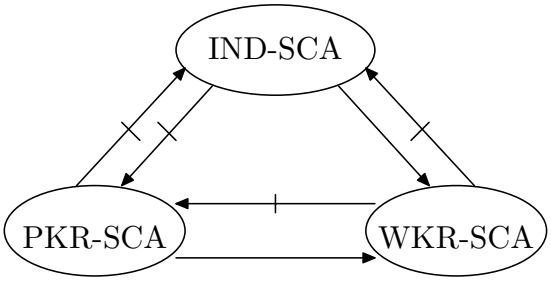

Fig. 2. Relations among PKR-SCA, WKR-SCA and IND-SCA.

5 Failing Combination of notions

From the above section, we know that the notion of WKR-SCA is much weaker than the notion of IND-SCA. Even if we combine the notion of WKR-SCA with that of IND, we can not get the notion of IND-SCA. Therefore we actually overturn the main result in [9].

Proposition 3 (WKR-SCA $\wedge$ IND $\nrightarrow$ IND-SCA). *Given a symmetric encryption scheme $\mathcal{SE}$ which is* IND*-secure, we can construct a symmetric encryption scheme $\mathcal{SE}'$ which is both* IND*-secure and* WKR-SCA*-secure for some leakage function, but not* IND-SCA*-secure for the same leakage function.*

Proof. Suppose $\mathcal{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ which is IND-secure. We construct $\mathcal{SE}' = (\mathcal{K}', \mathcal{E}', \mathcal{D}')$ as follows:

	$\mathcal{SE}$	$\mathcal{SE}'$
Key generation	$K \leftarrow \mathcal{K}$	$K_1 \leftarrow \mathcal{K}, K_2 \xleftarrow{\$} \{0,1\}^n$
Encryption	$\mathcal{E}_K(M)$	$\mathcal{E}'_{K_1K_2}(M) = \mathcal{E}_{K_1}(M)$
Decryption	$\mathcal{D}_K(C)$	$\mathcal{D}'_{K_1K_2}(C) = \mathcal{D}_{K_1}(C)$

The new encryption scheme $\mathcal{SE}'$ generates an extra $K_2 \xleftarrow{\$} \{0,1\}^n$, but does not used in the encryption. The encryption algorithms of $\mathcal{SE}$ and $\mathcal{SE}'$ are the same, so $\mathcal{SE}'$ is also IND-secure.

Now we consider the security of $\mathcal{SE}'$ in side-channel model, given that the leakage function is $L(K_1K_2, M) = K_1$.

The encryption algorithm of $\mathcal{SE}'$ does not use the key K_2, which is also not revealed by the leakage function, so it is WKR-SCA-secure. More specifically, for any adversary $\mathbf{A}$, $\mathbf{Adv}^{\text{WKR-SCA}}_{\mathcal{SE}'}(\mathbf{A}) \leq 1/2^n$.

Furthermore, the key K_1 used in the encryption algorithm is revealed by the leakage function, so $\mathcal{SE}'$ is not IND-SCA-secure. More specifically, the adversary $\mathbf{B}$ makes arbitrary query and gets K_1 through the leakage function, and then

queries $M \in \{0,1\}^n$, gets C. If $C = \mathcal{E}'_{K_1}(M)$, then return 1, else return 0. We have $\mathbf{Adv}^{\text{IND-SCA}}_{\mathcal{SE}}(\mathbf{A}) = 1 - 1/2^n$. □

Moreover, we show that even the scheme is PKR-SCA-secure and IND-secure, the approach in [9] still does not hold.

Proposition 4 (PKR-SCA ∧ IND ↛ IND-SCA). *Given a symmetric encryption scheme $\mathcal{SE}$ which is both* PKR*-secure and* IND*-secure, we can construct a symmetric encryption scheme $\mathcal{SE}'$ which is both* PKR-SCA*-secure and* IND*-secure for some leakage function, but not* IND-SCA*-secure for the same leakage function.*

Proof. Suppose $\mathcal{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ is both PKR-secure and IND-secure.

Now we consider the security of $\mathcal{SE}$ in side-channel model, given that the leakage function is $L(K, M) = M$.

The leakage function does not reveal any information about the key K, so $\mathcal{SE}$ is PKR-SCA-secure.

The leakage function reveals the queried plaintext, so $\mathcal{SE}$ is not IND-SCA-secure. More specifically, the adversary $\mathbf{A}$ just queries $M \in \{0,1\}^n$ and gets (C, M'). If $M = M'$ then return 1, else return 0. We have $\mathbf{Adv}^{\text{IND-SCA}}_{\mathcal{SE}}(\mathbf{A}) = 1 - 1/2^n$. □

6 Conclusion

This paper gives implications or separations among the notions of IND, PKR and WKR both in black-box model and side-channel model, which show that the notion of WKR is much weaker than the notion of IND. Then we construct a concrete scheme to show that the approach against side-channel attacks proposed in [9] is flawed. The security against key recovery attacks does not help much for a practically cryptographic requirement. We note that the results are not limited to the security of symmetric encryption scheme, as to the security of the other cryptographic algorithms, such as block ciphers or authenticated encryption schemes, the corresponding results still hold true.

References

1. M. Bellare, A. Desai, E. Jokipii, and P. Rogaway. A concrete security treatment of symmetric encryption: Analysis of the DES modes of operation. In *Proceedings of the 38th Symposium on Foundations of Computer Science (FOCS)*, pages 394–403. IEEE Computer Society Press, 1997.

2. E. Biham and A. Shamir. Differential cryptanalysis of DES-like cryptosystems (extended abstract). In A. J. Menezes and S. A. Vanstone, editors, *Advances in Cryptology - CRYPTO 1990*, volume 537 of *Lecture Notes in Computer Science*, pages 2–21. Springer-Verlag, 1990.
3. H. Dobbertin, L. Knudsen, and M. Robshaw. The cryptanalysis of the AES - a brief survey. In H. Dobbertin, V. Rijmen, and A. Sowa, editors, *Advanced Encryption Standard - AES: 4th International Conference, AES 2004*, volume 3373 of *Lecture Notes in Computer Science*, pages 1–10. Springer-Verlag, 2005.
4. K. Gandolfi, C. Mourtel, and F. Olivier. Electromagnetic analysis: Concrete results. In Ç. K. Koç, D. Naccache, and C. Paar, editors, *Cryptographic Hardware and Embedded Systems - CHES 2001*, volume 2162 of *Lecture Notes in Computer Science*, pages 251–261. Springer-Verlag, 2001.
5. S. Goldwasser and S. Micali. Probabilistic encryption. *Journal of Computer and System Sciences*, 28:270–299, 1984.
6. L. Goubin and J. Patarin. DES and differential power analysis (the "duplication" method). In Ç. K. Koç and C. Paar, editors, *Cryptographic Hardware and Embedded Systems - CHES 1999*, volume 1717 of *Lecture Notes in Computer Science*, pages 158–172. Springer-Verlag, 1999.
7. P. Kocher, J. Jaffe, and B. Jun. Introduction to differential power analysis and related attacks, 1999. `http://www.cryptography.com/dpa/technical/`.
8. P. C. Kocher. Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems. In N. Koblitz, editor, *Advances in Cryptology - CRYPTO 1996*, volume 1109 of *Lecture Notes in Computer Science*, pages 104–113. Springer-Verlag, 1996.
9. W. Li and D. Gu. An approach for symmetric encryption against side channel attacks in provable security. In W. Susilo, J. K. Liu, and Y. Mu, editors, *Provable Security 2007*, volume 4784 of *Lecture Notes in Computer Science*, pages 178–187. Springer-Verlag, 2007.
10. S. Micali and L. Reyzin. Physically observable cryptography (extended abstract). In M. Naor, editor, *Theory of Cryptography Conference, TCC 2004*, volume 2951 of *Lecture Notes in Computer Science*, pages 278–296. Springer-Verlag, 2004.
11. F.-X. Standaert, T. G. Malkin, and M. Yung. A unified framework for the analysis of side-channel key recovery attacks. Cryptology ePrint Archive, Report 2006/139, 2006. `http://eprint.iacr.org/`.
12. F.-X. Standaert, E. Peeters, C. Archambeau, and J.-J. Quisquater. Towards security limits in side-channel attacks. In L. Goubin and M. Matsui, editors, *Cryptographic Hardware and Embedded Systems - CHES 2006*, volume 4249 of *Lecture Notes in Computer Science*, pages 30–45. Springer-Verlag, 2006.