An Approach for Symmetric Encryption Against Side Channel Attacks in Provable Security

Wei Li and Dawu Gu

Department of Computer Science and Engineering,
Shanghai Jiao Tong University,
Shanghai 200240, China
{liwei2003,dwgu}@sjtu.edu.cn

Abstract. This paper defines perfect security against side channel attacks for a cryptosystem implementation, and discusses the implication of secure notions for a cryptosystem in provable security. Then we give some security notions for symmetric encryption against side channel attacks, UB-SCA (unbreakability in side channel attacks) and IND-CPA-SCA (indistinguishability of chosen plaintext attacks and side channel attacks). On the basis of these definitions, we propose and prove that IND-CPA + UB-SCA ⇒ IND-CPA-SCA by reduction, and IND-CPA-SCA is stronger than IND-CPA or UB-SCA.

1 Introduction

During the last ten years a new class of attacks against cryptographic devices has become public [1,2]. These attacks exploit easily accessible information like power consumption[3], running time[4], and can be mounted by anyone using low–cost equipment. These *side–channel attacks* amplify and evaluate leaked information with the help of statistical methods, and are often much more powerful than traditional cryptanalysis. Examples show that a very small amount of side–channel information is enough to completely break a cryptosystem [5]. While many previously–known cryptanalytic attacks can be analyzed by studying algorithms, the vulnerabilities of side–channel attacks result from electrical behavior of transistors and circuits of an implementation. Therefore, it extends theoretically the current mathematical models of cryptography to the physical setting which takes into consideration side–channel attacks [6].

Indistinguishability of encryptions (IND), which captures a strong notion of privacy, formalizes that an adversary's inability to learn information about the plaintext given a challenge ciphertext in provable security[7]. Connecting an ability of an adversary with chosen-plaintext attack leads to security notions of symmetric encryption, eg. IND-CPA[8] etc. Likewise, the security of symmetric encryption against side channel attacks does not violate this definition as above[9–11]. However, it's difficult to limit the power of the adversary in implementation. As a result, the security goals and adversary models may be considered from other directions. The best we can hope to do is combining the security of designing with that of implementation.

W. Susilo, J.K. Liu, and Y. Mu. (Eds.): ProvSec 2007, LNCS 4784, pp. 178–187, 2007.

Therefore, in this paper we propose several notions of privacy for symmetric encryption: UB-SCA and IND-CPA-SCA. The former notion describes the security of a symmetric encryption against side channel attacks in implementation, while the latter notion gives us a notion for a secure symmetric encryption both in designing and implementation. We seek an approach that can put these attacks to a common foundation, since designing and implementation for a secure cryptosystem are not independent.

The rest of this paper is organized as follows. Section 2 and 3 focus on defining a cryptosystem implementation in perfect security against side channel attacks. Then we present security notions for a symmetric encryption based on IND-CPA in section 4, and further section 5 generalizes the relations by reductions. Finally we conclude some remarks about a secure cryptosystem.

2 Syntax of a Symmetric Encryption Scheme

Secure notions for symmetric encryption schemes against traditional attack are given in [12]. The definitions for the symmetric encryption include the syntax and formal security measures as follows. Let $\mathcal{SE}$=($\mathcal{P}$, $\mathcal{C}$, $\mathcal{K}$, $\mathcal{E}$, $\mathcal{D}$) denote a symmetric encryption scheme. The key schedule $\mathcal{K}$ takes a security parameter $k \in N$ as its input and returns a key K, denoted as $K \leftarrow \mathcal{K}(k)$. The encryption algorithm $\mathcal{E}$ could be randomized or stateful. It takes the key K and a plaintext P as inputs to return a ciphertext C, denoted as $C \leftarrow \mathcal{E}_K(P)$. The decryption algorithm $\mathcal{D}$ is deterministic and stateless. It takes the key K and a string C as its input to return either the corresponding plaintext P or the symbol $\perp$, denoted as $x \leftarrow \mathcal{D}_K(C)$ where $x \in \{0,1\}^* \bigcup \{\perp\}$. It requires $\mathcal{D}_K(\mathcal{E}_K(P)) = P$ for all $P \in \{0,1\}^*$.

3 Implementation of Security

3.1 Implementation of Perfect Security Against Side Channel Attacks

Side channel information is a kind of information leaked from the physical implementation of a cryptosystem.So an adversary concerns mostly how much side channel information contributes to the recovery of key. We present perfect security against side channel attacks for a cryptosystem implementation as follows.

Definition 1. *Let ($\mathcal{P}$, $\mathcal{C}$, $\mathcal{S}$, $\mathcal{K}$, $\mathcal{E}$, $\mathcal{D}$) be a cryptosystem implementation with side channel information $\mathcal{S}$. Let $H(\cdot)$ denote entropy of the information. If*

$$H(K|S) = H(K)$$

where $K \in \mathcal{K}$ and $S \in \mathcal{S}$, then the cryptosystem implementation is perfect secure against side channel attacks. □