On the Notions of PRP-RKA, KR and KR-RKA for Block Ciphers

Ermaliza Razali[1], Raphael C.-W. Phan[2], and Marc Joye[3]

[1] Information Security Research (iSECURES) Lab
Swinburne University of Technology, Sarawak campus, Kuching, Malaysia
erazali@swinburne.edu.my
[2] Laboratoire de sécurité et de cryptographie, EPFL
Station 14 - Building INF, 1015 Lausanne, Switzerland
raphael.phan@epfl.ch
[3] Thomson R&D France
Technology Group, Corporate Research, Security Laboratory
1 avenue de Belle Fontaine, 35576 Cesson-Sévigné Cedex, France
marc.joye@thomson.net

Abstract. Security of commonly used block ciphers is typically measured in terms of their resistance to known attacks. While the provable security approach to block ciphers dates back to the first CRYPTO conference (1981), analysis of modern block cipher proposals basically do not benefit fully from this, except for a few cases. This paper considers the security of recently proposed PRP-RKA secure block ciphers and discusses how they relate to existing types of attacks on block ciphers.

Keywords: Provable security, pseudorandom permutation (PRP), key recovery (KR), block cipher, related key attacks (RKA).

1 Introduction

The right approach to analyzing the security of public-key encryption schemes and protocols is by reduction, in a given security model, to an underlying hard problem: the so-called the provable security approach. In the symmetric-key setting, while formal definitions of security do exist (e.g., Luby and Rackoff), security of a modern block cipher is often measured by its resistance to known attacks. Thus, from the perspective of the provable security community, the security of modern block ciphers may seem heuristic.

This paper considers the formal provable security approach to analyzing block ciphers. The advantage is clear. Security of a block cipher can be proved in a generic sense, by specifying bounds on the adversary's resources, without assuming the exact approach taken by the adversary. It encompasses all possible attacks mountable by the adversary given those resources. This compares favorably with the heuristic case where a primitive is designed to resist some list of attacks but may later fall to attacks not considered by the designer. Historically, building on work by Luby and Rackoff, the provable security of block ciphers

W. Susilo, J.K. Liu, and Y. Mu. (Eds.): ProvSec 2007, LNCS 4784, pp. 188–197, 2007.

have been analyzed with respect to the notion of pseudorandomness (PRP). This is advantageous since PRP implies security against key recovery (KR).

Except for a few cases (e.g., [8,1,11,12,9]), we are however not aware of any work that analyzes the security of modern block ciphers in the context of PRP. We also note that the assumption that the underlying block cipher is a PRP was used in the security analysis of CBC-MAC [2]. To the best of our knowledge, the earliest result on provable security analysis of block ciphers is by Hellman *et al.* [5]. In particular, the security was formalized in the ideal cipher model (a.k.a. Shannon model or black-box model) and in terms of an adversary winning a key-recovery game. The formalization of the security of block ciphers against related-key attacks in fact dates back to the work of Winternitz and Hellman [15], also considered in the context of a key-recovery game in the ideal cipher model, but here in the presence of related-key oracles. The first known block cipher with a provable security proof of pseudorandomness (PRP) is DESX [8].

Since the bulk of block cipher analysis is dedicated to key-recovery attacks, it is sensible to formally cast these PRP-RKA ciphers also in the context of resistance to key-recovery attacks either in the presence of related-key oracles (KR-RKA) or not (KR). Interestingly, doing so brings us back to where it started, since the first results [5,15] on provable security of block ciphers were in the context of KR and KR-RKA.

The rest of this paper is organized as follows. In the next section, we introduce some notation and review different security notions for block ciphers. Section 3 is the core of our paper. We describe several key recovery attacks on some PRP-RKA secure ciphers and relate the corresponding success probability with the security bound derived from a generic attacker. Finally, we conclude in Section 4.

2 Definitions

Consider a family of functions $F : \mathbb{K} \times \mathbb{D} \to \mathbb{R}$, where $\mathbb{K} = \{0,1\}^k$ is the set of keys of F, $\mathbb{D} = \{0,1\}^l$ is the domain of F and $\mathbb{R} = \{0,1\}^L$ is the range of F, and where k, l and L are the key, input and output lengths in bits. We use $F_K(\mathbb{D})$ as a shorthand for $F(K,\mathbb{D})$. By $K \xleftarrow{\$} \mathbb{K}$, we denote the operation of selecting a string K at random from $\mathbb{K}$. Similar notations apply for a family of permutations $E : \mathbb{K} \times \mathbb{D} \to \mathbb{D}$, where $\mathbb{K} = \{0,1\}^k$ is the set of keys of E and $\mathbb{D} = \{0,1\}^l$ is the domain and range of E.

2.1 Related Keys

The *related-key-deriving* (RKD) function $\phi \in \Phi$ is a map $\phi : \mathbb{K} \to \mathbb{K}$, where Φ is a subset of functions mapping $\mathbb{K}$ to $\mathbb{K}$. Given F and $K \in \mathbb{K}$, the *related-key oracle* $F_{\mathrm{RK}(K,\cdot)}(\cdot)$ takes two arguments: a function $\phi : \mathbb{K} \to \mathbb{K}$ and an element $P \in \mathbb{D}$, and returns $F_{\phi(K)}(P)$, where $\mathrm{RK}(K,\phi) = \phi(K)$. An attack exploiting access to the oracle $F_{\mathrm{RK}(K,\phi)}(\cdot)$ where $\phi \in \Phi$ is called a Φ-restricted related-key attack (RKA). Similar definitions apply for E.