Disk Encryption

Cuauhtemoc Mancillas-López

Laboratoire Hubert Curien, UMR CNRS 5516, Saint-Etienne, France

Abstract. Security of data stored in bulk storage devices like hard disks, flash memories, CDs and DVDs have gained a lot of importance in the current days. The importance of this topic is reflected in recent standardizing activities and a variety of cryptographic schemes proposed in the last decade as a solution to this problem. In this work we address various issues related to the problem of encryption of stored data. Our main focus is on block oriented storage medias like hard disks and flash memories. In the following paragraphs we summarize the different problems that we addressed along with our contributions.

There have been a consensus among researchers that a class of cryptographic algorithms called tweakable enciphering schemes (TES) can be used in the application of encrypting hard disks. In the last decade there have been many different proposals of TES each using different philosophies of construction. As a first contribution we provide the first experimental performance data for (almost) all existing TES. The reported performance data is based on optimized implementations of the schemes on several families of reconfigurable hardware.

We also propose some new schemes suitable for the problem. Among others, we propose a new TES called STES (Small TES) which is designed using a different philosophy compared to the other existing TES. The design goal of STES is to make it suitable for encrypting storage provided in devices which are constrained in terms of power consumption and area. STES uses cryptographic primitives which when implemented would have a very low hardware and power footprint in a novel way. We formally prove that STES provides adequate security for the application and also provide performance data in two classes of FPGAs which are suitable for low-power implementations. The performance of STES both in terms of throughput per area and power consumption is very encouraging.

TES are length preserving schemes, in the sense that the length of the cipher text produced by a TES is same as that of the plain text. This property of length preservation has been considered very important for an encryption scheme to be suitable for encrypting hard disks. We contest this well established notion, and argue why it may be possible to use encryption schemes which are not length preserving. We argue about this taking in consideration the structure of modern day hard disk. Finally we propose a new scheme called BRW-Counter mode (BCTR) which is not length preserving but provides the same security of that of a TES. We also present an optimal hardware architecture for BCTR and show that BCTR would outperform all other TES in terms of throughput.

Finally, we address the problem of securing backups by use of a new cryptographic scheme. We propose a cryptographic primitive which we call as the double cipher text mode (DCM) and discuss the general syntax and security definition of a DCM. We provide two efficient constructions of DCM which we name as DCMG and DCM-BRW. We argue why DCM would be suitable for the application of secure backup.