Chapter XVII
System-on-Chip Design of the Whirlpool Hash Function

Paris Kitsos
Hellenic Open University (HOU), Patras, Greece

ABSTRACT

In this chapter, a system-on-chip design of the newest powerful standard in the hash families, named Whirlpool, is presented. With more details an architecture and two very large-scale integration (VLSI) implementations are presented. The first implementation is suitable for high speed applications while the second one is suitable for applications with constrained silicon area resources. The architecture permits a wide variety of implementation tradeoffs. Different implementations have been introduced and each specific application can choose the appropriate speed-area, trade-off implementation. The implementations are examined and compared in the security level and in the performance by using hardware terms. Whirlpool with RIPEMD, SHA-1, and SHA-2 hash functions are adopted by the International Organization for Standardization (ISO/IEC, 2003) 10118-3 standard. The Whirlpool implementations allow fast execution and effective substitution of any previous hash families' implementations in any cryptography application.

INTRODUCTION

Nowadays many financial and other electronic transactions are grown exponentially and they play an important role in our life. All these transactions have integrated data authentication processes. In addition many applications like the public key infrastructure (PKI) (Adams & Farrell, 1999; National Institute of Standards and Technology [NIST, 2005=http://csrc.nist.gov/publications/nistpubs/800-77/sp800-77pdf]) and many mobile communications include authentication services. All the aforementioned applications have integrated an authentication module including a hash function embedded in the system's implementation.

A hash function is a function that maps an input of arbitrary length into a fixed number of output bits, the hash value.

One of the most widely used hash function is RIPEMD (Dobbertin, Bosselaers, & Preneel, 1996). These are two different RIPEMD versions the RIPEMD-128 and the RIPEMD-160, with similar design philosophy but different word length of the produced message digest (128- and 160-bit,

respectively). In August 2002, NIST announced the updated Federal Information Processing Standard (FIPS 180-2), which has introduced another three new hash functions referred to as SHA-2 (256, 384, 512). In addition, the new European schemes for signatures, integrity, and encryption (NESSIE) (2004), was responsible to introduce a hash function with high security level. In February 2003, it was announced that the hash function included in the NESSIE portfolio is Whirlpool (Barreto & Rijmen, 2003). Finally, the most known hash function is the secure hash algorithm-1 (SHA-1) (NIST, 1995=http://itl.nist.gov/fipspub/fip180-1.htm). However, some security problems have been raised as it has already (see Wang, Yin, & Yu, 2005) shown. This collision of SHA-1 can be found with complexity less than 2^{69} hash operations. This is the first attack on the full 80-step SHA-1 with complexity less than the 2^{80} theoretical bound. A collision in SHA-1 would cast doubt over the future viability of any system that relies on SHA-1. The result will cause a significant confusion and it will create reengineering of many systems, and incompatibility between new systems and old. In addition, the National Security Agency (NSA) did not disclose the SHA-2 design criteria and also its design philosophy is similar to the design of SHA-1 function. So, the attack against SHA-1 probably will have affected to the SHA-2 function. Also, this issue stands for RIPEMD hash families. On the other hand, the internal structure of Whirlpool is different from the structure of all the aforementioned hash functions. So, Whirlpool function does not suffer for that kind of problems and makes it a very good choice for electronics applications.

All the afore-mentioned hash functions are adopted by the International Organization for Standardization (ISO, 2003) 10118-3 standard.

In this chapter, an architecture and two VLSI implementations of the new hash function, Whirlpool, are proposed. The first implementation is suitable for high speed applications while the second one is suitable for applications with constrained silicon area resources.

The architecture and the implementations presented here were the first in scientific literature (Kitsos & Koufopavlou, 2004). Until then, two hardware architectures have been also presented. The first one (McLoone & McCanny, 2002) is a high speed hardware architecture and the second one (Pramstaller, Rechberger, & Rijmen, 2006) is a compact field-programmable gate array (FPGA) architecture and implementation of Whirlpool. Both architectures are efficient for specific applications; analytical comparisons with the proposed implementations will be given in the rest of this chapter. In addition, comparisons with other hash families' implementations (Ahmad & Shoba Das, 2005; Deepakumara, Heys, & Venkatesam, 2001; Dominikus, 2002; Grembowski et al., 2002; McLoone, McIvor, & Savage, 2005; Sklavos & Koufopavlou, 2003, 2005; Yiakoumis, Papadonikolakis, Michail, Kakarountas, & Goutis, 2005); are provided. From the comparison results it is proven that the proposed implementation performs better and composes an effective substitution of any previous hash families' such as MD5, RIPEMD-160, SHA-1, SHA-2, and so forth, in all the cases.

The organization of the chapter is the following: In the second section, fundamental for hash functions families, is presented. So, the (ISO/IEC) 10118-3 standard first is briefly described and secondly the Whirlpool hash function specifications are defined. In the third section, the proposed architecture and VLSI implementations are presented. Implementation results and discussion (comparison with other works) are reported in the fourth section. Finally, the fifth section concludes this chapter.

FUNDAMENTALS FOR HASH FUNCTIONS

In this section a brief description of the ISO/IEC 10118-3 standard is presented. This standard specifies dedicated hash functions. The hash functions are based on the iterative use of a round-function. Seven distinct round functions are specified, giving rise to distinct dedicated hash-functions. Six of them are briefly described and at last, Whirlpool is described in details.