Compact FPGA Implementations of Selected Round 3 SHA-3 Candidates

Bernhard Jungk

Hochschule RheinMain
Wiesbaden, Germany

Hash functions are a very important building block in many cryptographic protocols. Unfortunately, in the last years research led to attacks against the popular MD5 hash function and many researchers believe, that SHA-1 and the similar SHA-2 family of hash functions will share that fate (cf. [1, 2]). Therefore, the NIST decided to start the SHA-3 competition which is similar to the earlier AES effort (cf. [3]). The present work contributs results of FPGA-based implementations of several SHA-3 candidates. We focus on compact implementations, which are reasonable fast for many applications. In practice this is a suitable approach, because the bottleneck is often a much slower communication link. Furthermore using less area reduces the cost of the implementation.

For each SHA-3 candidate, a compact design can be achieved in several ways. The main challenge is to reduce the parallelism, which leads to a folded design. At first, this seems to be an easy task, but the details of each hash function lead to many problems. We analyzed and implemented three of the candidates, namely Grøstl (cf. [4]), JH (cf. [5]) and Skein (cf. [6]) for Virtex-5 FPGAs. JH is a very flexible candidate, making it easy to use datapath widths down to 8 bit. Grøstl's datapath can be divided into 64 bit parts, leading to a fast, yet compact design. Skein's flexibility in this regard is not that great. Doubtless, it is easy to reduce the datapath to 64 bit or less, but Skein's round function prevents a really efficient pipelined design.

The results vary between the three hash functions. The winner in the category throughput-area ratio is Grøstl-256, achieving over 1 Gbit/s, using only 470 slices. The smallest candidate implementation was achieved for JH-256 with only about 205 slices, at the cost of a large performance gap to Grøstl-256, reaching only 27 MBit/s. Our Skein-256 implementation needs about 555 slices and achieves 237 MBit/s and thus Skein does not excel in either area or speed. On the other hand, it has the second best throughput-area ratio of the three investigated candidates.

References

[1] X. Wang, Y. L. Yin, and H. Yu, "Finding Collisions in the Full SHA-1," in *Proceedings of Crypto*, Lecture Notes in Computer Science, Vol. 3621. Springer, 2005, pp. 17–36.

[2] S. Sanadhya and P. Sarkar, "New collision attacks against up to 24-step SHA-2," in *Progress in Cryptology-INDOCRYPT*, Lecture Notes in Computer Science, Vol. 5365. Springer, 2008.

[3] R. F. Kayser, "Announcing Request for Candidate Algorithm Nominations for a New Cryptographic Hash Algorithm (SHA-3) Family," in *Federal Register*. National Institute of Standards and Technology, November 2007, vol. 72, pp. 62 212–62 220.

[4] P. Gauravaram, L. R. Knudsen, K. Matusiewicz, F. Mendel, C. Rechberger, M. Schläffer, and S. S. Thomsen, "Grøstl – a SHA-3 candidate," Submission to NIST, 2011. [Online].
Available: `http://groestl.info/Groestl.pdf`

[5] H. Wo, "The Hash Function JH," Submission to NIST, 2011. [Online].
Available: `http://www3.ntu.edu.sg/home/wuhj/research/jh/jh_round3.pdf`

[6] N. Ferguson, S. Lucks, B. Schneier, D. Whiting, M. Bellare, T. Kohno, J. Callas, and J. Walker, "The Skein Hash Function Family," Submission to NIST, 2010. [Online].
Available: `http://www.skein-hash.info/sites/default/files/skein1.3.pdf`