An observation on `Grøstl`

Paulo S. L. M. Barreto

November 21, 2008

Abstract

An alternative view of the `Grøstl` SHA-3 submission is presented. It does *not* lead to an effective attack nor reveals a weakness in the design, but illustrates the importance of the double-width pipe in this construction.

1 Alternative view of `Grøstl`

The `Grøstl` specification [3, section 2.3] describes it as being based "on a few individual permutations rather than a large family of permutations indexed by a key," to avoid the necessity of a key schedule as in hash functions based on block ciphers. It would thus consist of a Merkle-Damgård designs that iterates a dedicated compression function f rather than a more conventional scheme like Davies-Meyer.

It turns out, however, that function f *can* be viewed as a Davies-Meyer compression function on top of an Even-Mansour 1-round block cipher [2]. This is shown in Figure 1.

This interpretation by itself does not lead to effective attacks. However, Daemen showed [1] how to mount against an Even-Mansour cipher a space-time tradeoff in the form of a differential attack that recovers an ℓ-bit key in $O(2^{\ell/2})$ steps using $O(2^{\ell/2})$ storage units. Thus the alternative view shows that the wide-pipe is essential to keep the effort to compute preimages at $O(2^n)$ steps for hash size $n = \ell/2$. Notice that the `Grøstl` specification [3, section 4.1 and 6.5] already recognizes that preimages can be obtained in $O(2^n)$ time, so this observation does *not* invalidate their security analysis.

Figure 1: Alternative view of the `Grøstl` function f.
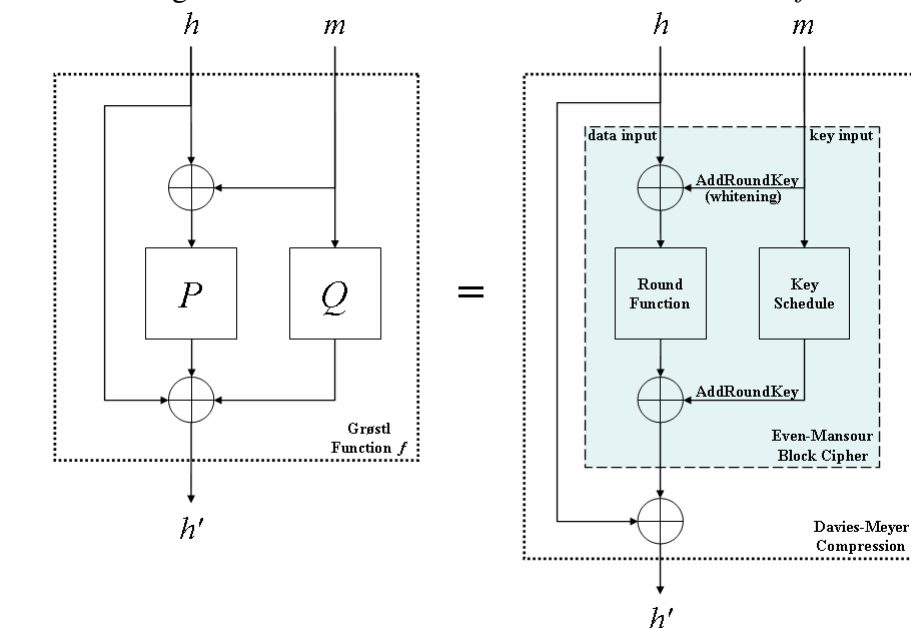
2   Acknowledgements

References

[1] J. Daemen, "Limitations of the Even-Mansour Construction", Advances in Cryptology – Asiacrypt'91, LNCS 739, pp. 495–498, 1991.

[2] S. Even and Y. Mansour, "A construction of a cipher from a single pseudo-random permutation", Advances in Cryptology – Asiacrypt'91, LNCS 739, pp. 210–224, 1991.

[3] P. Gauravaram, L. R. Knudsen, K. Matusiewicz, F. Mendel, C. Rechberger, M. Schläffer, and S. S. Thomsen, "`Grøstl` – a SHA-3 candidate," NIST submission, 2008.