Some Observations on SHAMATA

Ewan Fleischmann and Michael Gorski

Bauhaus-University Weimar, Germany
{Ewan.Fleischman, Michael.Gorski}@uni-weimar.de

Abstract. In this note we discuss some observation of the SHA-3 candidate SHAMATA [1]. We observe that its internal block cipher is very weak, which could possibly lead to an attack on the hash function.

Keywords: hash function, SHA-3, SHAMATA.

1 Introduction

The design of secure and practical hash functions is of great interest since most hash functions have been broken. Due to the SHA-3 [4] competition many new proposals for hash function primitives have been submitted to become the SHA-3 algorithm. SHAMATA [1] is one of them, which is analyzed in this note.

2 Some Observations of the internal Block Cipher in SHAMATA

In this section we analyze the internal block cipher of SHAMATA-256. This block cipher, say SHAMATA-BC, is a function of the following form:

$$\text{SHAMATA-BC} : \{0,1\}^{512} \times \{0,1\}^{128} \rightarrow \{0,1\}^{512},$$

where a 512 bit message block is encrypted using a 128 bit key so for any one fixed key $k \in \{0,1\}^{128}$ the function SHAMATA-BC$(\cdot, k)$ is a permutation.

Note, that we use the notations as in [1, p. 4 et sqq.]. Now, for $B[i], B^*[i] \in \{0,1\}^{128}$, $i = 1,2,3,4$, let a plaintext be of the form $X = B[0]|B[1]|B[2]|B[3]$ and its corresponding ciphertext be $C = B^*[0]|B^*[1]|B^*[2]|B^*[3]$. Let MC be a MixColumns operation. Let D be the key entered the encryption, $P = MC(D)$, $Q = MC(D^T)$, where D^T is the transpose of the data D and let $P' = P(1)||Q(0)$ and $Q' = Q(1)||P(0)$. The encryption of X can be described as:

$$\begin{aligned}
B[2] &= B[2] \oplus P \oplus \mathit{blockno},\\
B[3] &= B[3] \oplus Q \oplus \mathit{blockno},\\
K[3] &= K[3] \oplus P',\\
K[5] &= K[5] \oplus Q,\\
K[7] &= K[7] \oplus P,\\
K[11] &= K[11] \oplus Q',\\
B^*[0] &= B[2],\\
B^*[1] &= B[3],\\
B^*[2] &= ARF^r(B[2]) \oplus B[0] \oplus K[9] \oplus K[0],\\
B^*[3] &= ARF^r(B[3]) \oplus B[1] \oplus K[10] \oplus K[1].
\end{aligned}$$

2.1 Distinguishing Attack

Regarding the fact that the register K is empty at the beginning, we can be rewrite the algorithm as:

$$\begin{aligned}
B^*[0] &= B[2],\\
B^*[1] &= B[3],
\end{aligned}$$

$$B^*[2] = ARF^r(B[2] \oplus P \oplus \mathit{blockno}) \oplus B[0], \tag{1}$$

$$B^*[3] = ARF^r(B[3] \oplus Q \oplus \mathit{blockno}) \oplus B[1], \tag{2}$$

where ARF^r is the AES round function without key addition, i.e. $MC(SR(SB(\cdot)))$.

At this stage it is obvious that half if the plaintext, i.e. $B[2]$ and $B[3]$, is not influenced by the the cipher key. Thus, a trivial distinguishing attack can be mounted on the internal block cipher SHAMATA-BC to distinguish it with a overwhelming probability from a random oracle. Even if the round key is updated by the data and the cipher key, as stated by the authors, it will not strength the cipher against this trivial attack.

2.2 Extracting the Key

We can even extract the key using only one plain-/ciphertext pair as follows. It is even possible to recover the cipher key by regarding only the *modified* half of the cipher $B^*[2]||B^*[3]$. We can rewrite (1) and (2) as:

$$\begin{aligned}
SB^{-1}(SR^{-1}(MC^{-1}(B^*[2] \oplus B[0]))) \oplus B[2] \oplus \mathit{blockno} &= P,\\
SB^{-1}(SR^{-1}(MC^{-1}(\Delta B^*[3] \oplus \Delta B[1]))) \oplus B[3] \oplus \mathit{blockno} &= Q.
\end{aligned}$$

Thus, the cipher key can easily be recovered from only one plaintext ciphertext pair by using the computation above.

3 Conclusion

In this note we have shown some observations on the internal block cipher of SHAMATA-256. We found that the internal block cipher is very weak, which does not directly imply the weakness of the hash function. Nevertheless, a prominent example is SHA-1 [5]. The internal block cipher SHACAL-1 has been attacked successfully [3, 2] as well as the hash function SHA-1 [6].

References

[1] Adem Atalay, Orhun Kara, Ferhat Karakoc, and Cevat Manap. SHAMATA HASH FUNCTION ALGORITHM SPECIFICATIONS. Submission to NIST, 2008.

[2] Eli Biham, Orr Dunkelman, and Nathan Keller. A Simple Related-Key Attack on the Full SHACAL-1. In Masayuki Abe, editor, *CT-RSA*, volume 4377 of *Lecture Notes in Computer Science*, pages 20–30. Springer, 2007.

[3] Orr Dunkelman, Nathan Keller, and Jongsung Kim. Related-Key Rectangle Attack on the Full SHACAL-1. In Eli Biham and Amr M. Youssef, editors, *Selected Areas in Cryptography*, volume 4356 of *Lecture Notes in Computer Science*, pages 28–44. Springer, 2006.

[4] National Institute of Standards and Technology. Cryptographic Hash Project. See http://csrc.nist.gov/groups/ST/hash/index.html.

[5] National Institute of Standards and Technology. FIPS 180-1: Secure Hash Standard. April 1995. See http://csrc.nist.gov.

[6] Xiaoyun Wang, Yiqun Lisa Yin, and Hongbo Yu. Finding Collisions in the Full SHA-1. In Victor Shoup, editor, *CRYPTO*, volume 3621 of *Lecture Notes in Computer Science*, pages 17–36. Springer, 2005.