Update on Tiger*

Florian Mendel[1], Bart Preneel[2], Vincent Rijmen[1],
Hirotaka Yoshida[3], and Dai Watanabe[3]

[1] Graz University of Technology
Institute for Applied Information Processing and Communications
Inffeldgasse 16a, A–8010 Graz, Austria
{Florian.Mendel, Vincent.Rijmen}@iaik.tugraz.at
[2] Katholieke Universiteit Leuven, Dept. ESAT/SCD-COSIC,
Kasteelpark Arenberg 10, B–3001 Heverlee, Belgium
Bart.Preneel@esat.kuleuven.be
[3] Systems Development Laboratory, Hitachi, Ltd.,
1099 Ohzenji, Asao-ku, Kawasaki-shi, Kanagawa-ken, 215-0013 Japan
{hirotaka.yoshida.qv, dai.watanabe.td}@hitachi.com

Abstract. Tiger is a cryptographic hash function with a 192-bit hash value which was proposed by Anderson and Biham in 1996. At FSE 2006, Kelsey and Lucks presented a collision attack on Tiger reduced to 16 (out of 24) rounds with complexity of about 2^{44}. Furthermore, they showed that a pseudo-near-collision can be found for a variant of Tiger with 20 rounds with complexity of about 2^{48}.

In this article, we show how their attack method can be extended to construct a collision in the Tiger hash function reduced to 19 rounds. We present two different attack strategies for constructing collisions in Tiger-19 with complexity of about 2^{62} and 2^{69}. Furthermore, we present a pseudo-near-collision for a variant of Tiger with 22 rounds with complexity of about 2^{44}.

Keywords: cryptanalysis, hash functions, differential attack, collision, near-collision, pseudo-collision, pseudo-near-collision.

1 Introduction

Recent results in cryptanalysis of hash function show weaknesses in many commonly used hash functions, such as SHA-1 and MD5 [4,5]. Therefore, the cryptanalysis of alternative hash functions, such as Tiger, is of great interest.

In [2], Kelsey and Lucks presented a collision attack on Tiger-16, a round reduced variant of Tiger (only 16 out of 24 rounds), with complexity of about 2^{44}. In the attack they used a kind of message modification technique developed

* This work was supported in part by the Austrian Science Fund (FWF), project P18138. This work was supported in part by a consignment research from the National Institute on Information and Communications Technology (NiCT), Japan. This work was supported in part by the Concerted Research Action (GOA) Ambiorics 2005/11 of the Flemish Government.

R. Barua and T. Lange (Eds.): INDOCRYPT 2006, LNCS 4329, pp. 63–79, 2006.

for Tiger to force a differential pattern in the chaining variables after round 7, which can then be canceled by the differences in the expanded message words in the following rounds. This led to a collision in the Tiger hash function after 16 rounds. Furthermore, they showed that a pseudo-near-collision can be found in a variant of Tiger with 20 rounds in about 2^{48} applications of the compression function.

In this article, we extend the attack to construct a collision in Tiger-19. We present two different collision attacks on Tiger-19 with complexity of 2^{62} and 2^{69}. Furthermore, we present a pseudo-near-collision attack for a variant of Tiger with 22 rounds with complexity of about 2^{44} and a pseudo-collision attack for Tiger-23/128, a version of Tiger reduced to 23 rounds with truncated output, with complexity 2^{44}. A summary of our results is given in Table 1.

Table 1. Overview of attacks on the Tiger hash function

number of rounds	type	complexity	
Tiger-16	collision	2^{44}	in [2]
Tiger-19	collision	2^{62} and 2^{69}	in this article
Tiger-19	pseudo-collision	2^{44}	in this article
Tiger-21	pseudo-collision	2^{66}	in this article
Tiger-23/128	pseudo-collision	2^{44}	in this article
Tiger-20 [1]	pseudo-near-collision	2^{48}	in [2]
Tiger-21	pseudo-near-collision	2^{44}	in this article
Tiger-22	pseudo-near-collision	2^{44}	in this article

The remainder of this article is structured as follows. A description of the Tiger hash function is given in Section 2. The attack of Kelsey and Lucks on Tiger-16 is described in Section 3. In Section 4, we describe a method to construct collisions in Tiger-19. Another method for construction collisions in Tiger-19 is described in Section 5. Furthermore, we present a pseudo-near-collision for Tiger-22 in Section 6 and a pseudo-collision for Tiger-23/128 in Section 7. Finally, we present conclusions in Section 8.

2 Description of the Hash Function Tiger

Tiger is a cryptographic hash function that was designed by Ross Anderson and Eli Biham in 1996 [1]. It is an iterative hash function that processes 512-bit input message blocks and produces a 192-bit hash value. In the following, we briefly describe the hash function. It basically consists of two parts: the key-schedule and the state update transformation. A detailed description of the hash function is given in [1]. For the remainder of this article we use the same notation as is used in [2]. The notation is given in Table 2.

[1] Kelsey and Lucks show a pseudo-near-collision for the last 20 rounds of Tiger.