6.857 Homework **Problem Set 1** # 1-3 - The SHA-3 Competition
Group 8
Manal Dia, Curtis Liu, Eric Marion, Victoria Popic March 12, 2009

BLAKE BLAKE is a proposed hash function that uses the HAIFA iteration mode and whose compression function is built on the ChaCha function. It claims indifferentiability from a random oracle (p.38)[1], collision resistance (pp. 39-40), second preimage resistance (pp. 40-41), resistance to linear approximations (p.31), resistance to length extension attacks (p.39), resistance to backward and differential attacks (p.42), and resistance to slide attacks (p.43). However, these proofs are not very rigorous. For indifferentiability from a random oracle, second preimage resistance, and resistance to differential attacks, the proof is simply citing similarity to other functions such as ChaCha and Salsa20, and claiming these other functions have the desired properties. There is no formal proof of collision resistance, only indications that specific attacks would not apply to the BLAKE hash function. The proofs for resistance to length extension, backward, and slide attacks seem to be more rigorous.

Twister Twister has some provable security claims but mostly hand waving arguments for operation security: it is "heavily based" on the Merkle-Damgard design principle, and uses a compression function that is "similar to the Advanced Encryption Standard"(p.13)[2]. Authors do not mention indifferentiability from a random oracle. They claim resistance to pseudo-collision (p.33) with no formal proof. They claim collision resistance (p.30) by proving collision resistance for the core of the compression function, and preimage-resistance (p.33) with no formal proof. However, cryptanalysis done by Mendel et al.[3] show that the collision resistance proof used is not applicable, and present practical pseudo-collision, and theoretical collision and 2nd preimage attacks that invalidate Gorski et al.'s assumption about the compression function. Authors claim resistance to differential cryptanalysis (p.30) by providing strong "countermeasures" but no formal proof. They present a formal proof for resistance to length-extension attacks (p.27).

Additional Properties:

- Multi-Collision Attacks:(p.27) proof by reference to literature.
- Herding Attacks:(p.28) no formal proof but arguments for resistance.
- Long 2nd pre-image Attacks:(p.28) no formal proof but arguments for resistance.
- Slide Attacks:(p.29) no formal proof but arguments for resistance.

Blue Midnight Wish The authors show (via a proof) that BMW hash function can be expressed as a generalized PGV6 scheme and later show (via a proof) that it can be seen as a generalized

[1] Jean-Philippe Aumasson, Luca Henzen, Willi Meier, Raphael C.-W. Phan - SHA-3 proposal BLAKE Submission to NIST, 2008

[2] Ewan Fleischmann, Christian Forler, Michael Gorski - The Twister Hash Function Family. Submission to NIST, 2008

[3] Florian Mendel, Christian Rechberger, Martin Schlffer - Cryptanalysis of Twister. Available online, 2008

scheme of any of the 12 PGV secure schemes (PGV1,$\cdots$, PGV12) (pp.31-32) [4]. They state that the PGV6 design is second-preimage resistant and collision resistant and therefore, claim that BMW is also second-preimage resistant and collision resistant(p.39). Moreover, authors claim without proof that it is infeasible to find collisions, preimages or second preimages based on some properties of BMW (40).

Authors claim to have incorporated the suggestions from Literature to guarantee resistance against a generic multicollision attack and a length extension attack (p.19). They claim to take an effective precaution against differential attacks (attacker will have to use twice the number of variables in the differential paths) (p.19).

The authors claim that BMW is resistant against attacks for finding preimages and pseudo-collisions and illustrate the claim with a representation of a sequence of simplified versions of BMW (pp.34-35). Authors measure the deviation from ideal random Boolean function of the block cipher using NANT tests and find that an operation used in BMW is distinguishable from a random permutation (p.37). They conclude that BMWs underlying block cipher is a weak block cipher but present reasons to believe that the overall hash function is not weak: wide block size, most words not distinguishable from random 32-bit (64-bit) variables, complex feedback information function, complex and generalized folding function instead of a simple XOR function.

The compression function of BMW uses bitwise operations of XORing, rotating, and shifting. Authors claim that known attacks exploiting this design will not work on BMW since the known algorithms are for equations with two variables and will have exponential complexity when applied to systems of equations with three or more variables as is BMW (no proof of this is presented) (p.41).

Authors also claim that BMW is resistant to attacks of SHA-2 due to a huge change in the internal structure from SHA-2 to BMW. They summarize the strengths of BMW in its use of bijections, non-linear transformations, good propagation characteristics, and use of 16 operands in most operations (p.52).

Luffa Luffa is a hash function based on a variant of a sponge function whose security is based on the randomness of the underlying permutation (p.3)[5]. The design uses eight Sboxes which guarantees “almost” random generation (p.5). The author omits proofs for collisions, second preimage, and preimage attacks:

“Bertoni et al. proved that the best attack And to nd a collision of outputs, a second preimage, and a preimage all belong to the inner collision. We believe that it is also the case for Luffa and we have not found any serious attack to nd an inner collision even though Luffa has no security proof so far. Therefore we think Luffa has the suffcient collision resistance, second preimage resistance, and preimage resistance.” (p.21)

However, the supporting document discusses various modern techniques and shows that all of them are infeasable. Authors prove resistance against differential attack (p.10), but do not mention resistance against linear attacks or length-extension attacks, though they discuss non-linearity (p.5).

[4] Danilo Gligoroski, Vlastimil Klima, Svein Johan Knapskog, Mohamed El-Hadedy, Jorn Amundsen, Stig Frode Mjolsnes - Cryptographic Hash Function BLUE MIDNIGHT WISH. Submission to NIST, 2008

[5] Christophe De Canniere, Hisayoshi Sato, Dai Watanabe - Hash Function Luffa: Specification Submission to NIST, 2008

Additional Properties:

- Long message attack: proof (p.16)
- Meet-in-the-middle attack: proof (p.17)
- Multicollision attack: proof (p.19)

Discussion We summarize our findings in Table **??** below.

	BLAKE	Twister	BMW	Luffa
Indifferentiability from a random oracle	Argument by similarity(p.38)	No mention	Not indifferentiable(p.34)	Approximate Indifferentiability using Sboxes(p.5)
Collision Resistance	Argument by similarity(pp.39-40)	Proof for compression func(p.30)	Proof by reference(p.39)	Non rigorous Argument(p.21)
Preimage-resistance	Argument by similarity(pp.40-41)	Non rigorous argument(p.33)	Proof by reference(p.39)	Non rigorous Argument(p.21)
Resistance to differential cryptanalysis	Argument by similarity(p.42)	Strong "countermeasures", no formal proof (p.30)	Rigorous Argument(p.19)	Proof(p.10)
Resistance to length-extension attacks	Proof (p.39)	Proof(p.27)	Argument by similarity(p.19)	No mention
Additional Properties	Backward(p.42) and slide attacks(p.43): Proof.	Multi-Collision Attacks: proof by ref(p.27). Herding Attacks(p.28),Long 2nd pre-image Attacks(p.28), Slide Attacks(p.29): no proof but arguments.	Multicollision attack: argument by similarity (p.19)	Long message attack (p.16) Meet-in-the-middle attack (p.17) Multicollision attack (p.19)

Table 1: *Summary of Security Features for BLAKE, Twister, Blue Midnight Wish and Luffa. Page numbers refer to corresponding documentation cited above.*

We decided to mainly focus on two criteria:

1. Proof of resistance to differential attacks, which is one of the main reasons for the SHA-3 competition.
2. Indifferentiability from a random oracle, wich will ensure that the overall hash function is secure. Twister for example proves that the compression function is well founded, but its cryptanalysis shows that the hash function is vulnerable to practical (in time and memory) attacks.

Starting from the belief that a good candidate should provide a design that addresses security concerns raised by recent attacks on existing hash functions (e.g. MD5), we think that BLAKE and Luffa are the strongest contenders among the 4 given choices, with a slight preference for BLAKE for its more comprehensive security features (e.g. length-extension attacks).