6.857 Homework	**Problem Set 1**	# 1-3 - SHA-3 Competition
Victor Williamson		
Trevor Rundell		
Oliver Yeh		March 12, 2009

1 Analysis of SHA-3 Hash Functions

1.1 Overview

The four hash functions that we analyzed are as follows...

- FSB
- Lesamnta
- SHAvite-3
- JH

1.2 FSB

Mode of Operation The Merkle-Damgard domain extender is the mode of operation. Its security is proved sufficient by noting that the Merkle-Damagard domain extender, despite weaknesses, is believed to propagate the main security features from the compression function to the hash function (pg. 6). A final compression function is used to obtain birthday bound compatible brute force search protection. Whirlpool is used as the final compression function because it is non-linear and relatively complex enough to be deemed a safe choice. It is insisted that the final compression function itself does not have to be collision resistant or hard to invert for the hash to be (pg. 6). The security of the FSB parallels the security of the Markle-Damgard domain extender which gives complexities $2^{\frac{size}{2}}$ for collision resistance, 2^{size} for preimage resistance and 2^{size-k} for second preimage resistance. (pg. 10)

Collision Resistance The proof is based on difficult computation problems from coding theory (pg. 14), particularly the syndrome primitive where computation syndrome decoding and codeword finding is NP-hard. The proof states that finding a collision for the FSB compression function is at least as difficult as finding a codeword of weight two times the Hamming weight generated by the compression function. (pg. 19)

Preimage-resistance Similarly, the proof states that inverting the FSB compression function is at least as difficult as solving the syndrome decoding problem using the Hamming weight w as input. (pg. 19)

Second preimage resistance aka Weak Collision Resistance The proof states that finding a second preimage for the FSB compression function using Hamming weight w is at least as difficult as finding a codeword of weight $\leq w$ in code whose parity check matrix is a defined submatrix of H, where H is the binary $r \times n$ matrix produced by the syndrome primitive. (pg. 19)

1.3 Lesamnta

Mode of Operation The domain extension scheme consists of Merkle-Damgard iteration of the compression function and an output function to achieve Merkle-Damgard securities as well as security against extension attacks. For the compression function Lesamnta uses one of the twelve PGV modes called Matyas-Meyer-Oseas (MMO) which is one of the more secure of the PGV modes in terms of collision resistance and preimage resistance. The security of MMO is reducible to the security of the underlying block cipher in terms of proof-based and attack-based security. MMO mode prevents an attacker from exploiting poor key scheduling to gain control of the block cipher key (pg. 51).

Indifferentiability from a random oracle This is proven using the assumption that the block ciphers named E and L used for the compression function and ouput function respectively are independent ideal ciphers. It is shown that Lesamnta is indifferentiable from a VIL random oracle in the ideal cipher model and resists attacks for fewer than $2^{n/2}$ (pg. 62).

Collision Resistance This is proven using the assumption that the compression function h and the output function g are ideal ciphers and collision resistant. The proof that MMO mode is collision resistant is referenced to Black et al.'s "Black-box analysis of the block-cipher-based hash-function constructions from PGV" which concludes an adversary must make $2^{n/2}$ queries to find a collision, where n is the block length of the block cipher (pg. 60, 61).

Preimage Resistance This is proven using the assumption that the block cipher E is in place of the ideal cipher. The ideal cipher model is analyzed to show that the pre-advantage of an attacker is minimal and equal to $\frac{1}{2^n - q}$ (pg. 60).

Pseudorandomness The proof holds under the assumption that the block ciphers E and L are independent pseudorandom permutations. It is shown that if E is a secure cipher then Lesamnta is a pseudorandom function by showing that the prf-advantage and prp-advantage of an adversary is within bounds of the advantage obtained with a secure block cipher (pg. 61).

HMAC Lesamnta supports HMAC as specified in FIPS 198 by showing that HMAC security is reducible to the security of the underlying block ciphers E and L as used in the compression function and output function respectively. The proof of pseudorandomness ensures the security of HMAC using Lesamnta requires an adversary to make $2^{n/2}$ queries which is infeasible because Lesamnta only operates with $n \geq 224$. The proof by Bellare in "New proofs for NMAC and HMAC: Security without collision-resistance" is referenced as part of the proof (pg. 62).

Length-extension attacks It is shown that the output function makes length-extension attacks impossible. Furthermore it is stated that already proven indifferentiability from a random oracle implies security against length-extension attacks (pg. 63).

Multicollision Attack If Joux's multicollision attack as outlined in "Multicollisions in iterated hash functions. Application to cascaded construction," is used on Lesamnta to find 2^t collisions it requires complexity $O(t2^{n/2})$, which is infeasible for an attacker (pg. 64).

Kelsey-Schneier Attack for Second-Preimage-Finding If Kelsey-Schneier's "Second preimages on n-bit hash for much less than 2^n" is used to attack, Lesamnta has second-image security resistance approximately $n - k$ bits for messages shorter than 2^k (pg. 64).

Differential and Linear Attacks It is stated that the maximum differential characteristic probability for 12 rounds in Lesamnta-256 is less than 2^{-256} and message block space size 256-bit, both of which are not adequate for Wang et al. differential attacks which require higher differential characteristic probability and a larger block space size. This was shown by abstracting exact differences as patterns of active S-boxes, applying the wide trail strategy, and making experiments with the Viterbi algorithm (pg. 67).

Interpolation Attack The proof expresses Lesamnta-256 using the AES S-box as a polynomial of degree 254 over GF(2^8). After a few rounds, Lesamnta can be expressed as a polynomial with 32 variables, and after 10 rounds the output depends on all 32 variables. From the high degree of the S-box it is expected that the number of coefficients reaches the maximum sometime after the 10th round. Thus it is believed the full 32 rounds of Lesamnta is secure against interpolation (pg. 67).

Square Attack Lesamanta makes this chosen-plaintext attacked outlined by Daemen in "The block cipher SQUARE," infeasible requiring complexity $2^{253.7}$ for Lesamnta-256. This was shown via probability analysis where an attacker constucts 4 sets of 2^{192} texts with the right structure for a characteristic over 19 rounds in order to attack the 20-round version of the block ciphers leading to $2^{253.7}$ complexity (pg. 68).

Known-Key Distinguisher Attack Lesamnta-256 was examined against this distinguishing attack where the attacker knows the key and it was found that a known-key distinguisher could be constructed for Lesamnta-256 reduced to 12 rounds (pg. 69). This attack is described by Knudsen et al. in "Known-Key Distinguishers for Some Blocks Ciphers."

1.4 SHAvite-3

Mode of Operation SHAvite-3 makes use of a mode of operation called Hash Iterative Framework or HAIFA. HAIFA is shown to have many nice security properties including increased resistance to preimage and second preimage attacks, as well as other extension attacks as compared to the standard Merkle-Damgard construction. (pg. 4)

Indifferentiability from a random oracle and pseudorandomness The authors show that when assuming an underlying compression function that acts as a pseudorandom oracle, the mode of operation preserves both the pseudorandom and random oracle properties. The prefix-free encoding property of mode of operation also ensures that attacks based on internal collisions are more difficult than simple brute force attacks. (pg. 24)

Collision resistance To prove collision resistance of the HAIFA mode of operation the authors make use of the Merkle-Damgard prove of collision resistance. As long as the underlying compression function is collision resistant, the mode of operation is shown to be collision resistant as well. (pg. 23)

Preimage resistance The authors offer several arguments for the resistance of their hashing function against known pre-image and second pre-image attacks. Their analysis includes attacks such as Dean's expandable message technique, Kelsey and Schneier's expandable message attack and Herding attacks. In each case they either show the statistical difficulty of such an attack (proving it to be harder than a standard brute force attack) or outline a property of the hashing function which makes the attack impossible or extremely difficult (such as the use of a salt). (pg. 22)

Resistance to differential and linear cryptanalysis SHAvite-3 makes use of an underlying compression function based on the AES block cipher. Using this fact the authors show that the compression function is resistant to many types of attacks including linear cryptanalysis, impossible differential cryptanalysis, differential-linear cryptanalysis, algebraic attacks, side attacks and square attacks. In general, the authors argue that the high number of rounds used in the compression function is sufficient to make differential and linear attacks more difficult than a standard brute force attack. The authors also rely on internal bit counters used as additional inputs for each round to show resistance to side channel attacks. (pg. 22, 23)

Resistance to length extension attacks in keyed mode for a MAC The authors show that SHAvite-3 is secure against length extension attacks when used in a keyed mode for a MAC. One way in which this is shown is by using a randomized salt value as an input to each compression block. HAIFA also uses a bit counter as an additional input to the final compression block. This bit counter represents the number of bits in the uncompressed message, offering additional security against length extension attacks due to the fact that an adversary would need to know this value in addition to the salt value to recompute the final rounds of the hash. (pg. 6)

1.5 JH

Mode of Operation

The JH hashing algorithm uses 64 byte message blocks that pass through a 35.5-round compression function. The author claims that JH is strong against differential attacks, using more than 600 active Sboxes. The hashing algorithm comes in four different flavors JH-224, JH-256, JH-384, and JH-512. This flexible offering of security and size allows the user to choose the JH flavor that best suits his needs. (pg. 4)

Defence against Algebraic attacks JH is secure against algebraic attacks, the author claims. Recovering a message from the message digest would involve at least 36 Sbox layers since one more block is padded to the message. The algebraic degree of the Sbox is 3, coupled with the fact that the number of rounds being involved is large, makes JH secure against Algebraic attacks. (pg. 24)

Collision Resistance The author cites three different approaches that the JH algorithm uses to defend against collisions. First JH uses EDP design that maximizes the difference propagation. Next the algorithm minimizes difference cancelation within a compression function. Lastly, it makes sure that every operation in a compression function is involved in at least one differential path if there is difference propagation within that compression function. (pg. 20)

Preimage Resistance The author claims that since more than one pad is added to the message before computing message digest computation, the complexity of the differential preimage attack is more than the square of that of the collision attack. Therefore the hashing algorithm is secure against pre-image resistance (pg. 22). However, a recently identified attack by Mendel and Thomsen against JH shows that it is possible to construct a preimage attack, though doing so may involve a prohibitive amount of memory.

Second Preimage Resistance

The author explains that since message modification in second-preimage attack is not as efficient as that in collision attack, and at least two message blocks are involved in a differential second-preimage attack, a differential exists with probability much less than 2^{-512}, and JH is secure against the differential second-preimage attack. (pg. 22)

1.6 Summary

We found that in terms of quality and depth of proofs, Lesamnta offered the best security analysis. The authors offered extensive analysis of the security features of all parts of the Lesamnta algorithm, including the modes of operation and the underlying compression function. In addition, they showed that Lesamnta was provably secure against both common and emerging attacks against hash functions. Particularly impressive was that Lesamnta was shown to be provably secure against known key distinguisher attacks, something that we did not even see mentioned in other papers.

Among the other submissions, SHAvite-3 was a close second in terms of security analysis. Though they too offered a good number of proofs against many common attacks, their analysis was not quite as in depth as that of Lesamnta. The other algorithms, FSB and JH, were often very simplistic in their assumptions and limited in the types of attacks that they were able to prove security against.

1.7 References

- SHA-3 competition page: `http://csrc.nist.gov/groups/ST/hash/sha-3/index.html`
- SHA-3 Zoo: `http://ehash.iaik.tugraz.at/wiki/The_SHA-3_Zoo`