6.857 Homework	**Problem Set 1**	# 1-3 The SHA-3 Competition
Anonymous		March 12, 2009

We felt that out of KECCAK, LUX, AURORA, and TIB3, AURORA was the best one because of breath and depth of the security analysis provided. The AURORA submission provided proofs of resistance against several attacks as well as proofs of pseudo-randomness and indifferentiability from a random oracle.

Security Properties of KECCAK

Background on sponge function: The KECCAK[r,c,d] sponge function, with parameters capacity c, bitrate r, and diversifier d, is obtained by applying the sponge construction to KECCAK-f[r+c] and by applying a specific padding ot the input (page 3) [**?**].

Shortcut attack: In the KECCAK specifications, shortcut attack is defined as an attack on the sponge function yielding higher expected success probability than the same attack on a random oracle, for a given workload. (page 4)

Workload: The workload of an attack on a sponge function is expressed in terms of the number of calls to the underlying function. The workload of an attack on a random oracle is the sum of the workload of all queries sent to the random oracle by the attacker. For KECCAK[r,c,d], the workload of a single query with input length l and requesting n output bits is given by $\lfloor \frac{8\lfloor \frac{l}{8} \rfloor + 24}{r} \rfloor + \lceil \frac{n}{r} \rceil$ calls. (page 4)

Flat sponge claim: Given the capacity c (and possibly a limitation on the input and/or output sizes), the success probability of any attack should be smaller than or equal to the maximum of that for a random oracle and $1 - e^{(2^{2y-(c+1)})}$, with $N = 2^y$ the number of calls to the round function (or its inverse). For each supported parameter values of the sponge function, the authors make such a flat sponge claim. (page 12) [**?**]

Claim regarding shortcut attack: The expected success probability of any shortcut attack against KECCAK[r,c,d] (the sponge function) with a workload equivalent to N calls to KECCAK-f[r+c] (the underlying function) or its inverse shall be smaller than or equal to $1 - e^{(-N(N+2)2^{-(c+1)})}$. (page 4)

Claim regarding representation: The authors also acknowledge weaknesses of KECCAK sponge functions due to the fact that these functions can be described compactly and can be efficiently executed, e.g., the so called random oracle implementation impossibility. (page 4)

Security Properties of LUX

The security properties of LUX are discussed section 4, "Resistance to Attacks", of the supporting documentation for LUX [**?**]. No rigourous proofs are provided.

The authors provide arguments about the resistance of LUX to attacks that require collitions, specifically the multicollision attack, herding attack, and second preimage attack (pages 10-13). However, the attacks discussed were designed against Merkle-Demgrad constructions, and LUX is not such a construction. The arguments provided draw an analogy between LUX and Merkle-Demgrad, but by the author's own admission these results are preliminary.

The authors claim to have analyzed LUX's resistance to two types of differential trials attacks: a truncated differential attack and an extension to this attack with structures (page 13). The authors do not provide any details on their analysis other than a very brief description of how LUX's internal transformations relate to the probabilities in a differential trial attack.

The authors provide a brief argument as to why LUX is resistant to a specific type of preimage attack called a Meet-in-the-middle attack (page 13). They argue that for LUX-224 and LUX-256 this attack would require 2^{384} effort and that for LUX-384 and LUX-512 would require 2^{768} effort. In both cases they state that this is higher than for brute-force.

Security Properties of Aurora

The security properties of AURORA are discussed in section 4, "Security of AURORA" (page 67-92), in the file "AURORA-updated" [**?**].

Proofs of mode of operation security

- **Indifferentiability from a random oracle** The sMD transform with the finalization function is chosen to preserves CR and indifferentiability (PRO) of the underlying compression function. (page 55) The underlying compression function has no differential paths with high probability that are exploitable in collision-finding attacks or distinguishing attacks. (page 59)
- **Pseudo-randomness** HMAC-AURORA-224/256 is proved to be a good PRF. (page 67). HMACAURORA-384/512 is proved to be a good PRF when keyed via the IV. (page 68) HMAC-AURORA-224M/256M is deduced to be a good PRF. (page 68)
- **Collision resistance** AURORA is proved to have a good resistance to existing collision attacks because of its secure message scheduling. (page 85-87)
- **Preimage-resistance** AURORA is proved to be preimage-resistance. Three preimage attacks are analyzed, including Meet-in-the-middle approach, Correcting impossible messages, and SAT-solver approach. (page 88-89)
- **Second Preimage-resistance** AURORA is proved to be second preimage-resistance. Two second preimage attacks are analyzed, including "Using collision differentials", and "Using multi-near-collision differentials", as well as the "Generic long-message second preimage attacks". (page 89-90)
- **Multi-collision-resistance** Multi-collision attack is unlikely to be applicable to AURORA-224M/256M. However, finding K collision for AURORA-224/256/384/512 is not much harder than finding ordinary collisions. (page 90)
- **Slide attack-resistance** The slide attacks are deduced not to be applicable to AURORA. (page 90)

Provable resistance to differential cryptanalysis

- Differential attacks can be improved through Diffusion Switching Mechanism (DSM). (page 61-63)
- The AURORA structure is based on an 8-bit S-box, matrices and a byte diffusion BD design, and all components are byte-oriented. Thus, it is natural for evaluating the immunity against differential cryptanalysis by counting the minimum number of active S-boxes of AURORA structure using a block cipher evaluation method. (page 82-83)

Provable resistance to linear cryptanalysis: Linear attacks can be improved through Diffusion Switching Mechanism (DSM). (page 61-63)

Provable resistance to length-extension attacks: AURORA is proved to be resistant to length-extension attacks. (page 90)

Security Properties of TIB3

The security properties of TIB3 are discussed in section 5, "Security", of the supporting documentation [**?**].

Collision resistance in the black-box model

The TIB3 hash function uses block ciphers. Given a collision resistant hash function, the authors show that TIB3's integrated scheme, i.e. it's mode of operation with it's compression function, are collision resistant (pages 19-22). Specifically, the advantage of any adversary at breaking collision resistance using at most q queries is less than or equal to $\frac{q(q-1)}{2^n}$. The advantage refers to the maximum of the probability that an adversary, among all adversaries that can make at most q queries to an oracle that chooses E at random, will find two different inputs with the same hash value.

Resistance to preimage attacks in the black-box model

TIB3 is shown to have preimage resistance using an arugment similar to that used for showing collsion resistance (page 23). The advantage of any adversary using at most q queries to find preimages is bounded by $\frac{q}{2^{n-1}}$.

Resistance to differential attacks

The authors show that TIB3 is resistant to differential attacks (pages 25-27).

Resistance to algebraic attacks

The authors provide an explanation of why TIB3 is resistant to algebraic attacks that create a system of non-linear states to represent the internal states of the hash and solve or that use interpolation (page 28).