6.857 Homework	**Problem Set 1**	# 1-3 - Open Source Security Model
Aleksandar Zlateski		
Ranko Sredojevic		
Sarah Cheng		March 12, 2009

NaSHA

NaSHA was a fairly well-documented submission. Too bad that a collision has already been found. Here are the security properties that they have addressed in their submission:

- **Pseudorandomness.** The paper does not address pseudorandomness directly, though they did show proof of a fairly fast avalanching effect (page 19). Not quite sure if that is related to pseudorandomness, however.
- **First and second preimage resistance.** On page 17, it references a separate document provided in the submission. The proofs are given in the file `Part2B4.pdf`. The proof that its main transfunction is one-way can be found on pages 5-6.
- **Collision resistance.** Same as previous; noted on page 17 of the main document, proof given in `Part2B4.pdf`.
- **Resistance to linear and differential attacks.** Not referenced in the main paper, but `Part2B5.pdf` attempts to provide some justification for this.
- **Resistance to length extension attacks.** Proof of this is given on pages 4-5 of `Part2B4.pdf`.

We should also note that a collision in the $n = 384$ and $n = 512$ versions of the hash function. It was claimed that the best attack would be a birthday attack, whereas a collision was able to be produced within 2^{128} steps.

CubeHash

According to the author, CubeHash is a very simple cryptographic hash function. The submission does not include almost any of the security details, and for the ones that are included the analysis is very poor. But, for the sake of making this PSet more interesting we will cite some of the authors comments on different security issues.

- **Pseudorandomness.** Not mantioned at all.
- **First and second preimage resistance.** Good resistance claimed, and a reference the additional material submitted. However, the additional document is one page long, and does not prove or claim any resistance.
- **Collision resistance.** Same as previous; No proofs or valid arguments.
- **Resistance to linear and differential attacks.** Again, same as above. Citation: "As far as I can tell, 10 rounds are already overkill, providing full protection against linear attacks, differential attacks, etc.". No extra explanation or proof is given.

- **Resistance to length extension attacks.** Again, same as above.

We would like to cite some more claims the author made in the provided document on the analisys of the attacs. "CubeHash has a few constants that could be modified, but as far as I know there is no way that any design of this type could have a hidden vulnerability". Finally, we would like to cite the author's comments on the speed performance of CubeHash algorithm: "High-volume network protection with HMAC is sometimes cited as an exception, but anyone who really cares about speed shouldn't be using HMAC anyway".

SWIFFTX

SWIFFTX was based on an older algorithm the group had been working on called SWIFFT. SWIFTTX contains a couple of features designed to address some of the weaknesses of SWIFFT. Security details have been mentioned as follows:

- **Pseudorandomness.** Did not offer much proof or justification other than to state that SWIFFTX has been designed to solve some of non-randomness of SWIFFT (page 12).
- **First and second preimage resistance.** Referenced some of the old work they've done on SWIFFT and its proofs of preimage resistance (page 10). These old papers have been bundled with their submission.
- **Collision resistance.** Same as previous; proof given in old SWIFFT papers.
- **Resistance to linear and differential attacks.** Stated that SWIFFTX was designed to have a nonlinear "layer" sandwiched between two linear layers. This was an improvement over the highly linear SWIFFT (page 12). That was about the extent of their justification against linear attacks. No word on differential attacks, though.
- **Resistance to length extension attacks.** We did not seem to find a proof for this.

However, they did claim to have established a reasonable bound on the attack time on top of page 11. It basically states that if we can find a collision in SWIFFTX, we would also be able to solve a known hard problem.

Skein

The Skein paper briefly outlined the security properties and their justifications, referencing an in-progress paper for their full proofs (in other words, the full proofs are not yet published). They are briefly described, however, on the following pages:

- **Pseudorandomness.** Proof in unpublished paper; described on page 32.
- **First and second preimage resistance.** Claimed on page 28; authors promise proof in their unpublished paper.
- **Collision resistance.** Claimed on page 28 and explained on pages 30-31; full proof also in unpublished paper.

- **Resistance to linear and differential attacks.** No word on either of these, although in section 9, the authors performed a preliminary cryptanalysis on Skein that resembles differential attacks.
- **Resistance to length extension attacks.** Mentioned on pages 28-29; proof (presumably?) in unpublished paper.

The authors simply state "The claims made about Skein's security are backed by proof" with a reference to the unpublished paper. It's not clear exactly which properties (hopefully all of them) are to be proven in that paper.

Our favorite?

CubeHash, because it says so and CubeHash is god, and we are afraid to invoke its merciless wrath.

As for our favorite amongst the hash functions submitted by mere mortal humans, we will have to pick SWIFFTX. It seems as if the authors have been working and refining the algorithm for a long time and their proofs carefully documented, albeit elsewhere. NaSHA wasn't too bad if collisions hadn't already been found. Skein was also very thorough, but the paper was fairly long and we did not read/understand it as carefully as SWIFFTX. In addition, the fact that all its proofs are "upcoming" (whereas the other groups already had them submitted) places SWIFFTX slightly above Skein.