6.857 Problem Set #1
Tom Brown
Nick Semenkovich Last printed
Capen Low

Problem 1-3. The SHA-3 Competition

Our recommended choice of the following four proposals for SHA-3 is, by far, SHABAL. SHABAL's proposal is well-written (if long) and offers strong formal mathematical proofs for its securities. Each form of resistance is given its own well-ordered section and dealt with accordingly. The other papers generally seem to declare that the resistances are dealt with and do not afford the same kind of attention to these aspects.

CHEETAH:

CHEETAH Security Property Analysis:
Section 3 (p. 11-15) provides a summary of security features.
- Herding Attack p. 11
- Preimage Resistance p. 14
  * The authors state that since the internals of CHEETAH are based on Rijndael, that CHEETAH is as resistant to preimage attacks as Rijndael is."
- 2nd Preimage Resistance p. 11-12
  * This is mentioned hastily, and summarized as "So far there is no evidence how to carry out the Kelsey-Schneier attack to the construction with the block counter."
- Multicollision Attacks p. 12
  * Summarized as dependent upon 2nd preimage resistance and therefore secure given the block counter."
- Length Extension Attacks p.12:
  * The authors assert this is prevented by permuting an internal value, though there is some discussion (in the form of an OFFICIAL COMMENT) that disputes this claim. As of 2/6/209, the authors claim it could be resolved, but have not published code to resolve the issue."
- Differential Cryptanalysis p. 12-15
- HMAC-PRF Security p. 15
  * Again, the authors rely on the underlying Rijndael function.
- Randomized Hashing Attack p. 15

Overall Comment: This is not a strong presentation. The researchers offer little proof of any of their assertions, mostly stating that "since Rijndael is secure, CHEETAH is secure." The researchers also seem to have performed much less work implementing the cypher than others. There is only an outdated codebase available (that does not fix the length extension problems from the official comment), and there is no analysis of hardware/FPGA implementations.

SHABAL:

SHABAL Security Property Analysis:

- Indifferentiability from a Random Oracle p. 51
- Pseudo-randomness p. 15*

*The proof is mentioned only briefly, but it is assumed to be a part of the p.51 proof of Indifferentiability

- Collision resistance p. 65
- Pre-image Resistance p. 74
- 2nd Pre-image Resistance p. 85
- Resistance to Differential Cryptanalysis p. 123
- Resistance to Length Extension Attacks p. 129
- Resistance to Multi-Collision Attacks p. 129

Overall Comment: This is the strongest presentation of the four that we examined. The proposal is well written and each security is explained with detailed mathematical proofs. Additionally, possible means of attacking SHABAL are described and dealt with.

SHAMATA: (note that this was withdrawn on 2/17/09)

SHAMATA Security Property Analysis:

- Collision Resistance p. 11-13

* The researchers devote a lot of time to describing collision resistance proofs.

- Preimage Resistance p. 13
- 2nd Pre-image Resistance p. 13
- Resistance to Differential Cryptanalysis p. 14
- Herding Attack p. 14
- Resistance to Length Extension Attacks p. 15
- Resistance to Slide Attacks p. 15

Overall Comment: This looked like a strong presentation, but was trashed in a publication: "Some Observations on SHAMATA" by Fleischmann and Gorski (see http://www.uni-weimar.de/cms/fileadmin/medien/medsicherheit/Research/SHA3/Observations_for_SHAMATA.pdf). The paper seems to prove that the internal block cypher of SHAMATA is incredibly weak.

Blender:

Blender Security Property Analysis:

6.857 Problem Set #1
Tom Brown
Nick Semenkovich Last printed
Capen Low

- Pseudo-randomness p. 21
- Collision resistance p. 20
    * Authors simply state that hash functions are all vulnerable to the Birthday Attack and there is no way around it. They offer no additional proof of security.

A telling quote: "A Birthday Attack will succeed against all hash algorithms, including this one; the only defense is to increase the size of the message digest."

- Pre-image Resistance p. 19
- 2nd Pre-image Resistance p. 19
    * Authors insist that this is simply difficult because it's hard to choose two messages that give the same checksum. This seems hand-wavy.
- Resistance to Differential Cryptanalysis p. 20
- Resistance to Length Extension Attacks p. 20
- Resistance to Multi-Collision Attacks p. 20
    * The proof is questionable for the same reasons as Collision Resistance above.

Overall Comment: Blender offers little to no formalization in their proofs, excepting claiming "This sort of attack would never work unless the attackers are able to discover part [x] of the original message!" This seems a poor basis for believing in one's security.