Specification Update of the Hash Family LUX

Ivica Nikolić, Alex Biryukov, Dmitry Khovratovich

University of Luxembourg

Abstract. The paper provides a simple update of LUX.

The hashing procedure in LUX can be divided into three phases: input message, blank rounds, output hash. The exact definition of the phases can be found in [1]. Further we introduce an improvement for LUX.

Change. We propose to fully discard the output hash phase and to increase the number of rounds in the blank rounds from 16 to 20. Therefore the hashing procedure will consist of only two phases: input message and blank rounds. The hash of a message is the value of the core after the blank rounds phase. For LUX-224 the left-most 7 columns (32×7 bits) should be taken as an output; for LUX-384 the left-most 6 columns (64×6 bits).

Motivation. The *state update function* of LUX does not mix the whole state (in one round). This property was used in the analysis presented in [2]: in the output hash phase, a correlation between consecutive output columns of the core was found. By discarding this phase and outputting the whole core at once, the attacker now has to find weakness in the full 20-round block cipher. The number of rounds in the blank rounds phase is increased from the minimal 16 rounds to 20 rounds in order to keep the mixing that was done by the now discarded phase. This also adds extra protection against short-message analysis given in [3] which shows how to distinguish LUX with 8 blank rounds.

Performance. Note that with this improvement the speed of the function will even slightly increase: we discard the output hash that has 6-8 rounds and introduce additional 4 rounds in the blank rounds phase.

References

1. Ivica Nikolić, Alex Biryukov, Dmitry Khovratovich. Hash Family LUX - Algorithm Specifications and Supporting Documentation. Available `http://ehash.iaik.tugraz.at/uploads/f/f3/LUX.pdf`
2. Shuang Wu, Dengguo Feng, Wenling Wu. Cryptanalysis of the Hash Function LUX-256. Available at `http://ehash.iaik.tugraz.at/uploads/3/36/Analysis_LUX_1.pdf`
3. Peter Schmidt-Nielsen. A Distinguisher for Reduced-round LUX. Available at `http://ehash.iaik.tugraz.at/uploads/3/3b/LUXATTACKNext.pdf`