New Russian Hash Function Standard

Dmitry Khovratovich    Alexey Urivskiy

JSC “InfoTeCS”, Russia
New Russian National Hash Function Standard

- based on Stribog (pronounced [`stri:bog]) hash function;
- approved on August 07, 2012;
- put into effect on January 01, 2013;
- replaces the old version that no longer fits performance and security requirements;
Design approach

- well-studied and time-tested constructions;
- no redundancy: each transformation adds to security;
- resistance to all known attacks;
- large security margins;
Basic Construction

- two output lengths — 256 and 512
- fixed IV (different for different output lengths)
- MD-based single pipe hash
- MD-strengthening: additional hashing with
  - the length of the hashed message;
  - the sum modulo $2^{512}$ of all message blocks;

\[ H_{256} \quad 0 \quad 1 \quad t \quad 0 \quad H_{512} \quad 512 \quad \text{padded} \quad M_0 \oplus M_1 \oplus \cdots \oplus M_t \]

\[ H_0 \quad 512 \quad M_0 \quad M_1 \quad \cdots \quad Mt \quad 512 \quad \text{truncated} \quad H \]

\[ H_0 \quad 256 \quad 512 \]
Compression Function

- Miyaguchi-Preneel scheme.
- SP-network both in key schedule and state transformation.
- 13 rounds
  - message/constant addition,
  - S-box layer,
  - transposition,
  - columnwise diffusion,
  - wide trail design strategy.
- Compression function takes the block counter as input.
GOSTbusters are welcome!

And also rebounders, meet-in-the-middlers, integrators, etc.

- Authentic reference description

- Authors’ design principles and rationale