Cryptanalysis of StreamHash

Dmitry Khovratovich and Ivica Nikolić

University of Luxembourg

1 Description of StreamHash

StreamHash-256[1] internally has 8 32-bit words $A[i], i = 0, 7$, which are updated with each message word m as follows:

```
for i=0 to 7
    $A[i] = A[i] \oplus sbox32[A[i] \oplus m \oplus i)\&0xff];$
```

2 Cryptanalysis on StreamHash

Note that in the update phase there is no diffusion among the state words, i.e. each word is updated separately. Therefore one can consider that the state words are simply concatenated and thus use Joux's approach[2] for this type of constructions. Let F be the function for the first four state words A_0, A_1, A_2, and A_3, and G be the function for the last four words A_4, A_5, A_6, and A_7. Then one collision for F can be obtained with $2^{128/2} = 2^{64}$ effort. If we obtain 64 consecutive collisions (thus 2^{64} multicollisions), among them there will be one collision for G also. Therefore the attack complexity is $128 \cdot 2^{64} = 2^{73}$.

Similarly, for preimage attack, using Joux's approach, one can find preimages for StreamHash with $128 \cdot 2^{128} = 2^{135}$ computations.

In general, for StreamHash-n, the collisions can be found with $\frac{n}{2}2^{n/4}$ effort, and preimages with $\frac{n}{2}2^{n/2}$ effort.

References

1. Michal Trojnara: StreamHash Algorithm. `http://csrc.nist.gov/groups/ST/hash/sha-3/Round1/documents/StreamHash.zip`
2. Antoine Joux: Multicollisions in Iterated Hash Functions. Application to Cascaded Constructions. In Matthew K. Franklin, editor, *Advances in Cryptology - CRYPTO 2004*, volume 3152 of *Lecture Notes in Computer Science*, pages 306-316. Springer, 2004.