

1 Markku's Attack

In July 2010, Markku-Juhani O. Saarinen, a Finnish cryptographer, communicated with Revere about a weakness he had observed in the initialization procedure [1]. As a result of this weakness, two nonces which differ in only a particular single bit produce starting states which differ only in a single bit. Upon further examination, he realized that by using an appropriate pair of chosen ciphertext values, the difference between the internal states at two separate instances would collapse into a constant difference.

Based on this observation, he was able to develop an attack whereby given two starts differing by only the appropriate bit, he could create a series of chosen ciphertext input streams that would allow him to determine a fixed appropriate pair which would cause the constant difference. Then, using another pair of chosen ciphertext input streams with that fixed appropriate pair, he was able to create a series of attacks that allowed solving for the keys of each rotor one at a time. The cost of such an attack was well under the cost of exhausting over the keys for all rotors. This attack was described in code supplied to Revere [2] and in a formal paper [3].

2 Modifications to Hummingbird

Based on Markku's observations and attack, a series of modifications to Hummingbird were considered and evaluated. The final modifications were a result of cryptanalysis by the analysts of Jim Frazer & Son Cryptography, the engineering evaluations by Revere and design by the Revere cryptographers with guidance from JF&SC. The goal was to counter Markku-type attacks, as well as other attacks, and to do so within severe engineering constraints. The end result of these modifications has effectively blocked this type of attack as well as other attacks.

The primary blocking modification is the addition of the rs1 state as a whitener to the output of the final rotor in producing cipher text. This prevents the determination of the appropriate fixed ciphertext pairs that would cause a perpetual steady differential state. With the modification, such a steady differential state could not be achieved via a pair of cipher streams without knowing the stream of rs1 values.

The initialization procedure was also changed, eliminating the particular defect that led Markku to discover his attack.

Two changes were made in the internal states and keys for the rotors. The key space was reduced from 256 bits to 128 bits. This was partly because of engineering constraints as well as to make the actual key space commensurate with the design goal of 128-bit security. Another modification was the introduction of accumulators of rs values. These accumulators are used to dynamically modify the key used in two of the rotors. The effect of this is to double the internal state space from 64 bits to 128 bits. It also blocks the type of constant differential that was used in Markku's attack.

3 References

[1] Email from mjsaarinen to Revere, 7 July 2010.

[2] C code supplied to Revere, 11 July 2010.

[3] Cryptanalysis of Hummingbird-1, Markku-Juhani O. Saarinen, no date on paper.