Note: Full-round distinguisher for Synergy

Orr Dunkelman[1,2] Eran Lambooij[3] Gaëtan Leurent[3]

[1]University of Haifa, Israel
[2]TU Berlin, Germany
[3]Inria, France

July 3, 2025

This short note looks at the proposed cipher Synergy [1]. Synergy is a 16-round, 64-bit Feistel construction with a data-dependent rotation as the round function The master-key is 1024 bits and the roundkeys are computed by applying some PRNGs to a state initialized by the master-key. We can assume the round-keys to be independent as only 512 bits of key material is absorbed into the state.

The round function $f_k : \{0,1\}^{32} \to \{0,1\}^{32}$ can be described by:

$$f_k(x) = k \oplus f(x) \qquad f(x) = \tau_{x[4:0]}(x),$$

where τ_i denotes left rotation by i bits, and $x[4:0]$ extracts bits 0 to 4.

An interesting observation is that if the difference in the 5 least significant bits of the inner round function is 0, the output difference hamming-weight is equal to the input difference hamming weight. In other words, if we have a one bit input difference, the probability of getting a one bit output difference is $\frac{27}{32}$.

This observation leads to the following differntial characteristic, which holds with probability $(27/32) \cdot (1/32) \approx 2^{-5.25}$, where $e_i = 1 \ll i$:

$$(e_i, 0) \xrightarrow{p=27/32} (e_j, e_i) \xrightarrow{p=2^{-5}} (0, e_j) \to (e_j, 0)$$

for $32 > i, j > 4$.

By starting with the input difference $(0, e_i)$, this results in a 16-round characteristic with a probability of approximately $2^{-26.23}$.

We can improve the probability of the characteristic by allowing for any difference in the left hand side in the last round:

$$(e_i, e_j) \to \cdots 12\text{-rounds} \cdots \to (0, e_i) \to (e_i, 0) \to (e_j, e_i) \to (*, e_j)$$

This characteristic will have a probability of $2^{-5} \cdot 2^{-5.25 \cdot 4} \cdot (27/32) \approx 2^{-25.74}$. We can skip the first round by picking the input values of the form: $p_1 = (A, B)$ and $p_2 = (A \oplus e_i, B \oplus f(A) \oplus f(A \oplus e_i))$, with $A, B \in \{0,1\}^{32}$ and $i \geq 5$. This gives us a probability of $2^{-20.74}$ to observe a one bit difference in the right hand side of the output difference.

To verify the above probabilities we did a short experiment by encrypting 2^{32} pairs with input difference $(0, \texttt{0x100})$ and counting the number of pairs where the hamming weight of (part of) the output difference is 1. For the full output difference we got a probability of $2^{-25.96}$, for the right half we get a probability of $2^{-21.29}$ and for the left half we get a probability of $2^{-22.96}$.

References

[1] Lindman A.: Synergy: A Lightweight Block Cipher with Variable Bit Rotation Feistel Network. Eprint 2025/1051.