Security Analysis of ORANGE-Zest

Bishwajit Chakraborty and Mridul Nandi
Indian Statistical Institute, Kolkata

6th Nov 2019
ORANGE-Zest Mode of AEAD

1. Rate is 1 (256-bit message with 256-bit permutation).
2. Additional state size is 128-bit.
**Figure:** The Feedback Processing ($FB^+$). Black dot means $\alpha^m$ multiplication where $m = 0/1/2$ for intermediate block, complete last block, partial last block respectively. Gray dot means $\alpha$ multiplication.
Forgery Attack (Dobraunig, Mendel, Mennink)

\[ N \rightarrow P \rightarrow Y_1 \]
\[ K \rightarrow \alpha \cdot K \]
\[ C_1^0 \]
\[ Y_0^0 \]
\[ x_1^0 \]
\[ M_1^1 \]

\[ N' \rightarrow P \rightarrow Y_1' \]
\[ K \rightarrow \alpha \cdot K \]
\[ C_1' \]
\[ Y_0'^0 \]
\[ x_1'^0 \]
\[ M_1'^1 \]

\[ N' \rightarrow P \rightarrow Y_1 \]
\[ K \rightarrow \alpha \cdot K \]
\[ C_1'' \]
\[ Y_0''^0 \]
\[ x_1''^0 \]
\[ M_1''^1 \]

\[ C_1''^0 = x_1''^0 \oplus y_0''^0 \]

Figure: (a) 1\textsuperscript{st} query, (b) 2\textsuperscript{nd} query, (c) Forgery.


- the extra state input while processing the first message block to be nonce dependent.

- When $|A| = 0$, To make $S_1 \neq K$ we pad $A$ so that $|\text{pad}(A)| = n$.

- The **modified** ORANGE-Zest is well secured within NIST requirements.
Modified ORANGE-Zest

Figure: Modified ORANGE-Zest encryption ($|A| = 0, |M| = 2n$)
ORANGISH Hash Function

Figure: ORANGE-Zest AD Module

Figure: ORANGISH Hash Function
1. Similar to Transform-then-Permute (though it does not fall under this paradigm).

2. Need multi-chain analysis (note that tag generation is same as CBC type MAC over ciphertext.)

3. Refer workshop paper for details.
Conclusion

- The **modified** ORANGE-Zest satisfies NIST requirements.

- Among all Sponge type submissions: Only ORANGE-Zest has Rate 1. (absorbs 256-bit massage/associated data per 256-bit permutation call.)

- High rate from using a small extra state.

- The hash function ORANGISH can be implemented by suitably using ORANGE-Zest associated data processing module.

- ORANGISH is a JH-hash type construction which is well analyzed.
Thank You!