Making a Best Paper **Bester**: Improved Attacks on Full MISTY1

Achiya Bar-On

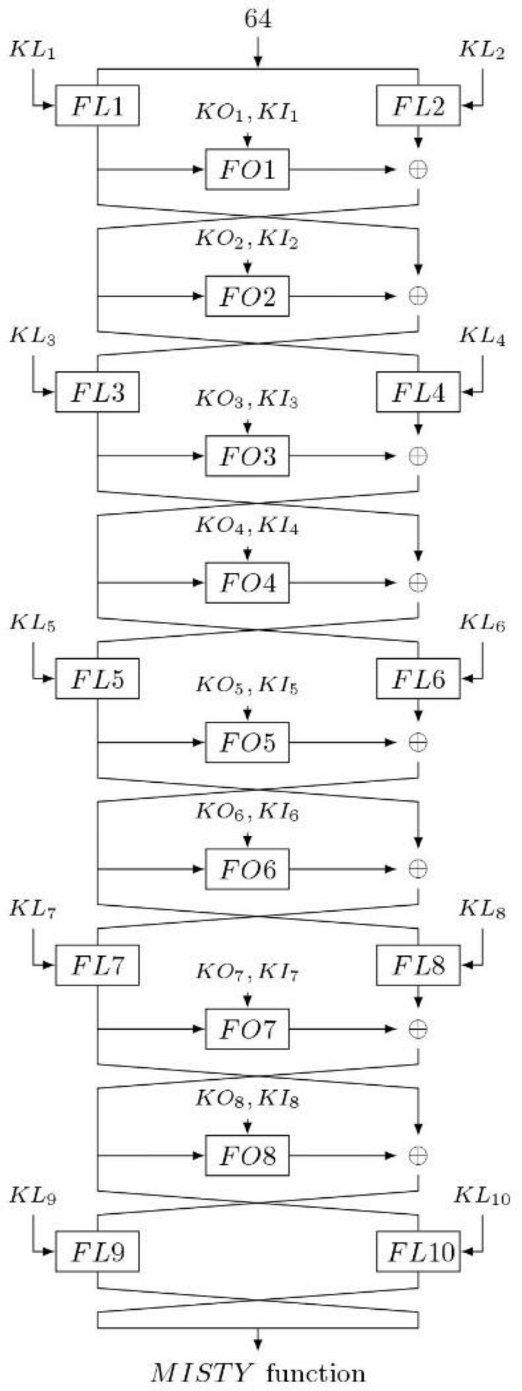
Bar Ilan University

MISTY1 is a Major Block Cipher:

- Designed by Matsui in 1997.
- Resisted all cryptanalytic attacks for 18 years.
- Selected by the Japanese government to be one of the CRYPTREC e-government ciphers (2002).
- Widely deployed in Japan.
- European NESSIE-recommended cipher (2003).
- ISO standard (2005).
- Successor - KASUMI (widely used in 3G cellular).

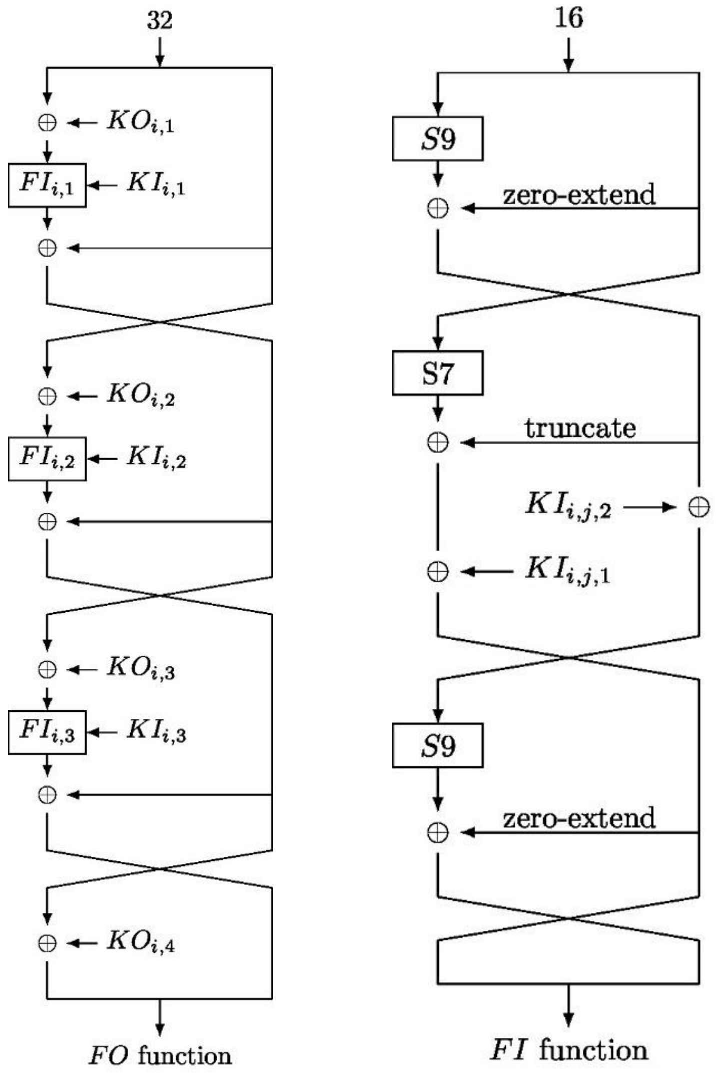
Overall Structure of Misty1:

- 64-bit block size.
- 128-bit master key.
- 8-round Feistel structure.

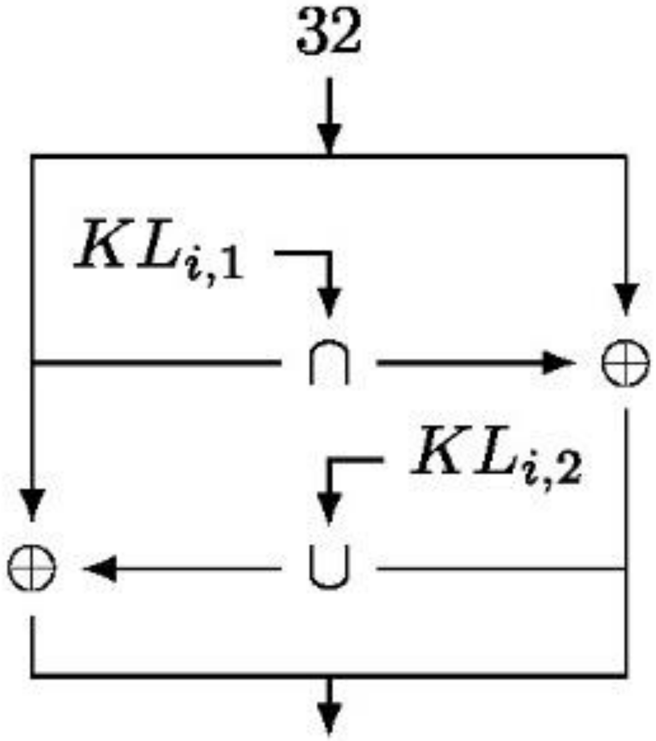


Internal Structure of The Round Function F0:

- 3-round Feistel structure with round function FI.
- Complex function:
  - Involves 112 key bits and 9 S-boxes.

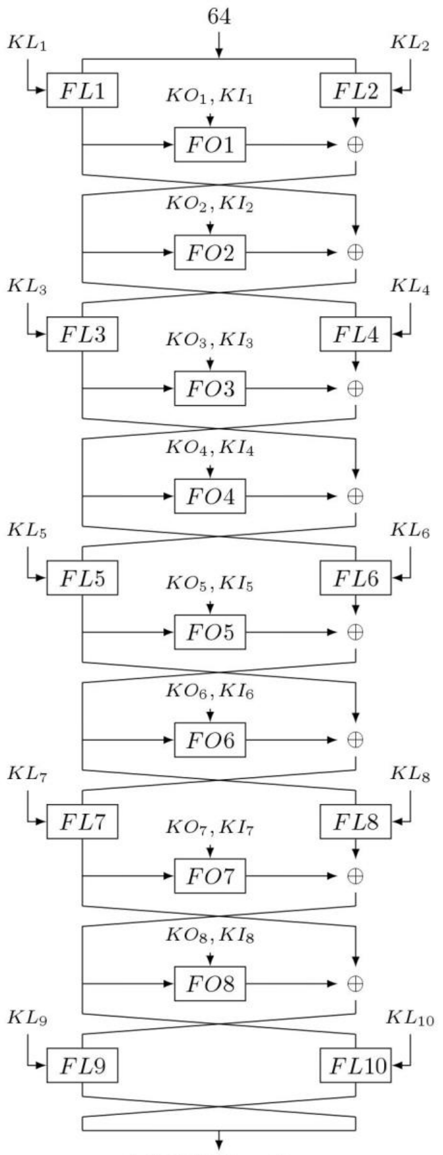


An Additional mixing layer (FL's)



FL function

∩
bitwise AND
∪
bitwise OR



$MISTY$ function

The Security of MISTY1:

- So far all the previously known cryptanalytic attacks had failed to break the full version of MISTY1

The Security of MISTY1:

- So far all the previously known cryptanalytic attacks had failed to break the full version of MISTY1

- Tomorrow morning you will hear a fantastic new result obtained by a young Japanese researcher, Yosuke Todo

The Security of MISTY1:

- So far all the previously known cryptanalytic attacks had failed to break the full version of MISTY1

- Tomorrow morning you will hear a fantastic new result obtained by a young Japanese researcher, Yosuke Todo

- By using a very clever new technique called the Division Property, Todo was able to reduce the time complexity of the attack on full MISTY1 from $\mathbf{2^{128}}$ to $\mathbf{2^{107.3}}$

In recognition of this breakthrough:

- Todo's result was justifiably selected by the Crypto 2015 program committee to receive both awards:
  - **Best Paper Award**
  - **Best Young Researcher Award**

New Improvements of Todo’s Attack:

- After studying Todo’s paper, a young Israeli student, Achiya Bar-On (who had just started his PhD research under the supervision of Nathan Keller) found a way to extend it and to improve Todo’s attack on full MISTY1

New Improvements of Todo’s Attack:

- After studying Todo’s paper, a young Israeli student, Achiya Bar-On (who had just started his PhD research under the supervision of Nathan Keller) found a way to extend it and to improve Todo’s attack on full MISTY1

- His new techniques reduce the time complexity of the attack from $\mathbf{2^{107.3}}$ to $\mathbf{2^{69.5}}$, while keeping the data complexity essentially unchanged

New Improvements of Todo's Attack:

- After studying Todo's paper, a young Israeli student, Achiya Bar-On (who had just started his PhD research under the supervision of Nathan Keller) found a way to extend it and to improve Todo's attack on full MISTY1

- His new techniques reduce the time complexity of the attack from $\mathbf{2^{107.3}}$ to $\mathbf{2^{69.5}}$, while keeping the data complexity essentially unchanged

- In fact, after spending just $\mathbf{2^{64}}$ time, the new attack can already find 49 of the 128 key bits

Implications of the New Attack:

- MISTY1 currently provides at most $\mathbf{2^{70}}$ security instead of the expected $\mathbf{2^{128}}$ security

Implications of the New Attack:

- MISTY1 currently provides at most $\mathbf{2^{70}}$ security instead of the expected $\mathbf{2^{128}}$ security

- While this is still considered an impractical complexity, it may be prudent to reevaluate the status of the various standards that support MISTY1