Practical Attacks on Reduced-Round Misty1

Computer Science Department
University of Haifa

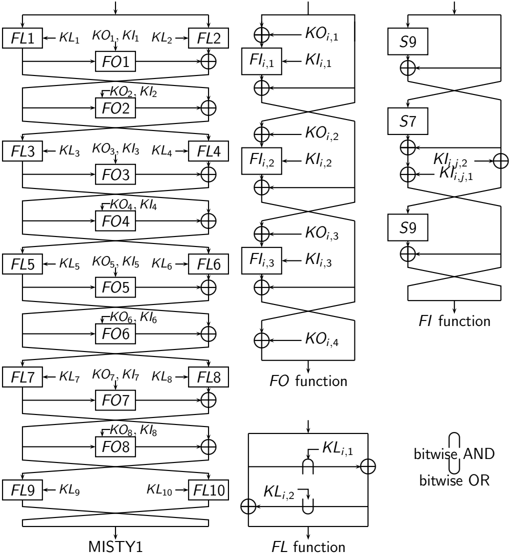
28^{th} May, 2013

Joint work with Nathan Keller

MISTY1

- Introduced by Matsui in 1997.
- 64-bit block, 128-bit key.
- Recursive structure — 8 Feistel rounds, each round function is a 3-round Feistel function.
- Each of these semi-round functions is a 3-round Feistel on its own.
- Uses 7-bit and 9-bit S-boxes for maximal nonlinearity.
- Every two rounds there is an *FL*-layer.
- Cryptrec-approved, NESSIE-portfolio, RFC, ISO.
- Predecessor of KASUMI.

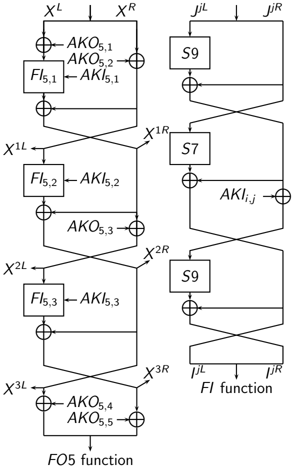
MISTY1


FL1 ← KL1 KO1, KI1 KL2 → FL2
FO1
KO2, KI2
FO2
FL3 ← KL3 KO3, KI3 KL4 → FL4
FO3
KO4, KI4
FO4
FL5 ← KL5 KO5, KI5 KL6 → FL6
FO5
KO6, KI6
FO6
FL7 ← KL7 KO7, KI7 KL8 → FL8
FO7
KO8, KI8
FO8
FL9 ← KL9 KL10 → FL10
MISTY1
KOi,1
FIi,1 ← KIi,1
KOi,2
FIi,2 ← KIi,2
KOi,3
FIi,3 ← KIi,3
KOi,4
FO function
S9
S7
KIi,j,2
KIi,j,1
S9
FI function
KLi,1
KLi,2
FL function
bitwise AND
bitwise OR

MISTY1 — Equivalent *FO* Representation

Each *FO* accepts 112-bit subkey. However, one can reduce these to a 107-bit equivalent subkey:

$$AKO_{i,1} = KO_{i,1}$$
$$AKO_{i,2} = KO_{i,2}$$
$$AKO_{i,3} = KO_{i,2} \oplus KO_{i,3} \oplus KI'_{i,1}$$
$$AKO_{i,4} = KO_{i,2} \oplus KO_{i,4} \oplus KI'_{i,1} \oplus KI'_{i,2}$$
$$AKO_{i,5} = KO_{i,2} \oplus KI'_{i,1} \oplus KI'_{i,2} \oplus KI'_{i,3}$$
$$AKI_{i,j} = [KI_{i,j}]_{\{8,\ldots,0\}}$$



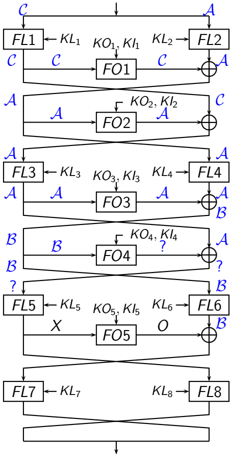
Cryptanalytic Results on MISTY1

Attack	Rounds	*FL* functions	Complexity	
			Data	Time
Impossible Differential [L+08]	6	None	2^{39} CP	2^{85}
Impossible Differential [DK08]	7	None	$2^{50.2}$ KP	$2^{114.1}$
Impossible Differential [JL12]	7	None	$2^{36.5}$ CP	$2^{92.2}$
Integral [KW02]	5	Most	2^{34} CP	2^{48}
Integral [LS09]	5	Most	2^{34} CP	$2^{27.32}$
Integral [LS09]	6	Most	2^{34} CP	$2^{108.1}$
Slicing Attack [K02]	4	All	$2^{22.25}$ CP	2^{45}
Impossible Differential [DK08]	5	All	$2^{38.6}$ CP	2^{46}
Impossible Differential [DK08]	6	All	2^{51} CP	$2^{123.4}$
Integral [LS09]	6	All	2^{32} CP	2^{126}
Impossible Differential [JL12]	6	All	$2^{52.5}$ CP	$2^{112.4}$

Practical Cryptanalytic Results on MISTY1

Attack	Rounds	*FL* functions	Complexity	
			Data	Time
Slicing Attack [K02]	4	All	$2^{22.25}$ CP	2^{45}
Higher-Order Differential [BF00]	5	None	$2^{10.5}$ CP	2^{17}
Integral [KW02]	5	Most	2^{34} CP	2^{48}
Integral [LS09]	5	Most	2^{34} CP	$2^{27.32}$
Impossible Differential [DK08]	5	All	$2^{38.6}$ CP	2^{46}
SQUARE (new)	5	All	$2^{35.6}$ CP	2^{38}
Related-Key Slide (new)	8	None	2^{18} CP	2^{18}
Related-Key Slide (new)	(any)	None	$2^{18+\epsilon}$ CP	2^{18}

A 4-Round SQUARE Property



Main Problem

- Attacking 4-round of MISTY1 using this property is straightforward.
- Attacking the fifth round when no *FL* is present is also quite straightforward ([KW02,LS09]).
- The problem is attacking the last round with the *FL* layer.
- It requires undoing the last *FL* layer **and** *FO*5.

Solution: Division

- Instead of checking the full SQUARE condition on 32 bits, i.e.,
$$\sum_{i=1}^{2^{32}} O_i \oplus FL7^{-1}(C_i^R) \stackrel{?}{=} 0,$$
one can check it on a subset of the bits.
- Following Sakurai-Zheng [SZ99]:
$$\begin{aligned}\Delta O^L_{\{15,14,\ldots,9\}} &= \Delta I^{2L} \oplus \Delta X^{1R}_{\{15,14,\ldots,9\}} \\ &= \Delta I^{2L} \oplus \Delta I^{1L} \oplus \Delta X^{R}_{\{15,14,\ldots,9\}}.\end{aligned}$$
- Really useful when the last *FL* layer is absent ([KW02] $\leftarrow$ [LS09]).

Further Division

- The problem with the Sakurai-Zheng relation is its relying on 16 bits (I^{1L} and I^{2L} rely on AKO_1 and AKO_2, respectively).
- This prevents successful combination with the FL-layer.

Further Division

- The problem with the Sakurai-Zheng relation is its relying on 16 bits (I^{1L} and I^{2L} rely on AKO_1 and AKO_2, respectively).
- This prevents successful combination with the FL-layer.
- Despite the FL-layer being easily divisible into 16 parallel functions [DK08].

Further Division

- The problem with the Sakurai-Zheng relation is its relying on 16 bits (I^{1L} and I^{2L} rely on AKO_1 and AKO_2, respectively).
- This prevents successful combination with the FL-layer.
- Despite the FL-layer being easily divisible into 16 parallel functions [DK08].
- Solution: Further divide Sakurai-Zheng-relation into 7,9,7, and 9 bits.

Further Division

- The problem with the Sakurai-Zheng relation is its relying on 16 bits (I^{1L} and I^{2L} rely on AKO_1 and AKO_2, respectively).
- This prevents successful combination with the *FL*-layer.
- Despite the *FL*-layer being easily divisible into 16 parallel functions [DK08].
- Solution: Further divide Sakurai-Zheng-relation into 7,9,7, and 9 bits.

***FO* can be described as four functions from 32 bits to 7,9,7, and 9, bits**

Attack on 5-Round MISTY1

- To check whether one of the functions is balanced, 71-key bits are needed.
- Luckily, the actucal computation can be done in a Meet-in-the-Middle manner.

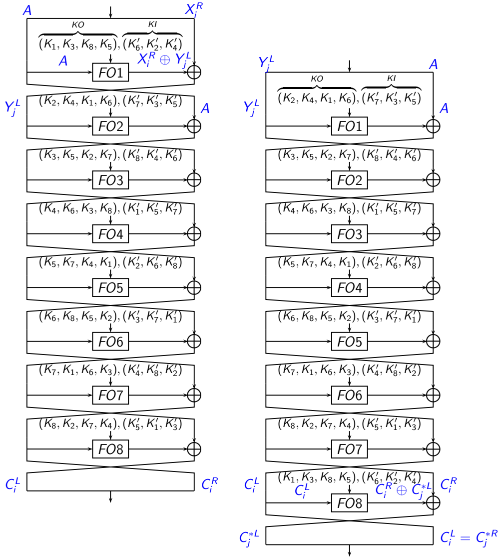
Attack on 5-Round MISTY1

- To check whether one of the functions is balanced, 71-key bits are needed.
- Luckily, the actucal computation can be done in a Meet-in-the-Middle manner.
- A naïve implementation would need 2^{36} trials for each structure.
- This results in time of about $2^{36} \cdot 2^{32} \cdot 12 = 2^{71.6}$ operations.
- A simple partial-sum technique can reduce this figure to just 2^{38} operations.

Attack on 5-Round MISTY1

- To check whether one of the functions is balanced, 71-key bits are needed.
- Luckily, the actucal computation can be done in a Meet-in-the-Middle manner.
- A naïve implementation would need 2^{36} trials for each structure.
- This results in time of about $2^{36} \cdot 2^{32} \cdot 12 = 2^{71.6}$ operations.
- A simple partial-sum technique can reduce this figure to just 2^{38} operations.
- Outcome: 71-key bits are found using $2^{35.6}$ CPs, 2^{38} time and $2^{36.6}$ 64-bit blocks of memory.
- The remaining key bits can be easily found practically for free.

The Related-Key Relation



Some Basic Problems

- By picking 2^{18} CPs, one expects 4 "slid" pairs, and 4 wrong pairs to pass basic filtering.
- One needs to attack 107-bit subkey, so the standard approach yields attacks of 2^{111} operations or so.

Some Basic Problems

- By picking 2^{18} CPs, one expects 4 "slid" pairs, and 4 wrong pairs to pass basic filtering.
- One needs to attack 107-bit subkey, so the standard approach yields attacks of 2^{111} operations or so.
- However, we can (almost certainly) identify the "slid" pairs.
- Same input to first round $\Rightarrow$ same output.
- Sort these pairs according to the suggested output of the first round.

Attack Algorithm

- Assume at least three "slid" pairs exist (probability 76%).
- We obtain four input-output pairs to $FO1$.
- And we apply our divided Sakurai-Zheng relation, retrieving $AKO_{1,1}$ and $AKO_{1,2}$ in MitM.
- For the remaining candidates — apply the full Sakurai-Zheng relation (using the other 9 bits) to retrieve $AKI_{1,1}$ and $AKI_{1,2}$.
- Follow with similar analysis to retrieve $AKI_{1,3}$, and deduce $AKO_{1,4}$ and $AKO_{1,5}$.
- One solution is expected to exist.
- This approach yields 107 bits of the key in 2^{18} time.

Partial Experimental Verification

- We started by verifying we get the right "slid" pairs proportions.
- We run the experiment with MISTY1 code submitted to NESSIE by Mitsubishi.
- 1,000,000 keys, 2^{18} plaintexts (4 expected "slid" pairs).
- We expected that the number of "slid" pairs follows a Poisson distribution with a mean value of 4.

Partial Experimental Verification (cont.)

"Slid" Pairs	0	1	2	3	4	5
Theory ($Poi(4)$)	18,316	73,263	146,525	195,367	195,367	156,293
Experiment	18,324	73,461	146,699	195,390	194,541	156,609

"Slid" Pairs	6	7	8	9	10	11
Theory ($Poi(4)$)	104,196	59,540	29,770	13,231	5,292	1,925
Experiment	104,266	59,338	29,860	13,330	5,348	1,916

"Slid" Pairs	12	13	14	15	16	17
Theory ($Poi(4)$)	641	197	56	15	4	1
Experiment	657	190	54	15	2	0

Partial Experimental Verification of Key Recovery Phase

- We took (by hand) three slid pairs, and put them through the key recovery phase.
- It takes about 0.105 seconds to recover 107 bits of the key, given these pairs.

Partial Experimental Verification of Key Recovery Phase

- We took (by hand) three slid pairs, and put them through the key recovery phase.
- It takes about 0.105 seconds to recover 107 bits of the key, given these pairs.
- We can thus conclude that the attack is practical (it takes about 0.064 seconds to generate the data and identify the pairs).

Conclusions

- New practical attack on 5-round MISTY1.
- New (very practical) related-key attack on 8-round MISTY1 with no *FL* functions.

Conclusions

- New practical attack on 5-round MISTY1.
- New (very practical) related-key attack on 8-round MISTY1 with no *FL* functions.
- First case of a related-key attack on a "reasonable" cipher which is practical.

Conclusions

- New practical attack on 5-round MISTY1.
- New (very practical) related-key attack on 8-round MISTY1 with no *FL* functions.
- First case of a related-key attack on a "reasonable" cipher which is practical.
- TODO: Finalize the verification of the attack.

Questions?

$E\nu\chi\alpha\rho\iota\sigma\tau\omega$!

Thank you for your attention!