The 23rd Annual International Conference on Information Security and Cryptology

ICISC 2020

December 2 (Wed) ~ December 4 (Fri), 2020 | Virtual Conference

Hosted by
Korea Institute of Information Security and Cryptology (KIISC)
National Security Research Institute (NSR)

Korea Institute of Information Security & Cryptology

(Quantum) Cryptanalysis of Misty schemes

Aline Gouget[1], Jacques Patarin[2] and Ambre Toulemonde[1,2]

[1] *Thales DIS, Meudon, France*

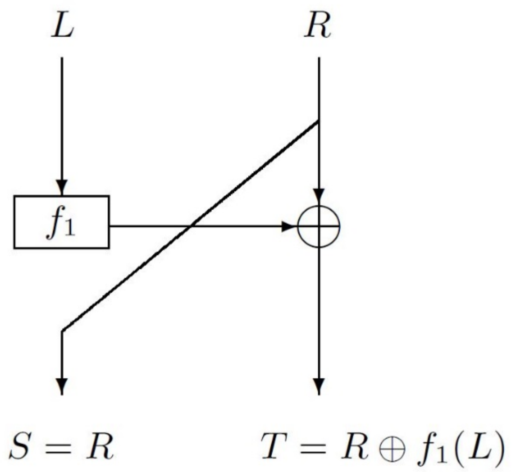
[2] *Université de Versailles Saint-Quentin-en-Yvelines, Versailles, France*

Outlines

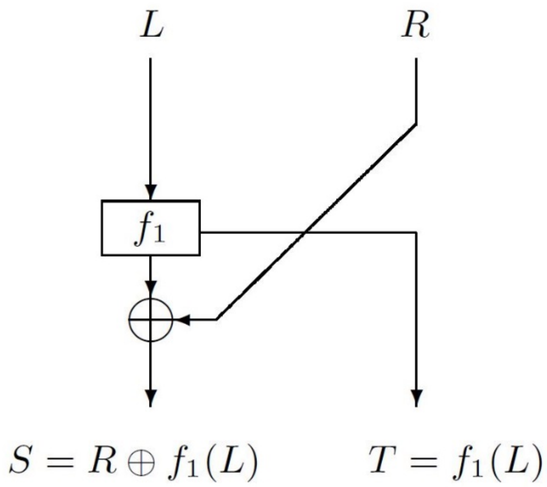
- Misty schemes
- Quantum cryptanalysis
- Quantum distinguishing attack against 4-round Misty L
- Quantum distinguishing attack against 3-round Misty RKF
- Quantum key recovery attack against d-round Misty RKF
- Overview of our results

Misty schemes

- Variant of well-known Feistel schemes
- Used to build pseudo-random permutation $\{0,1\}^{2n} \rightarrow \{0,1\}^{2n}$
- Misty L and Misty R schemes with $f_i: \{0,1\}^n \rightarrow \{0,1\}^n$ secret permutations



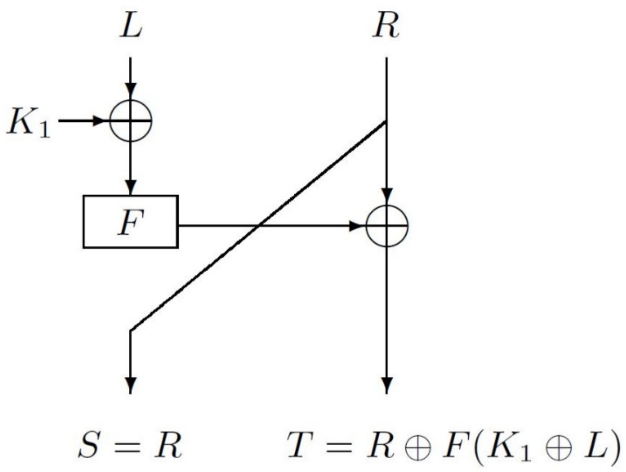
Misty L



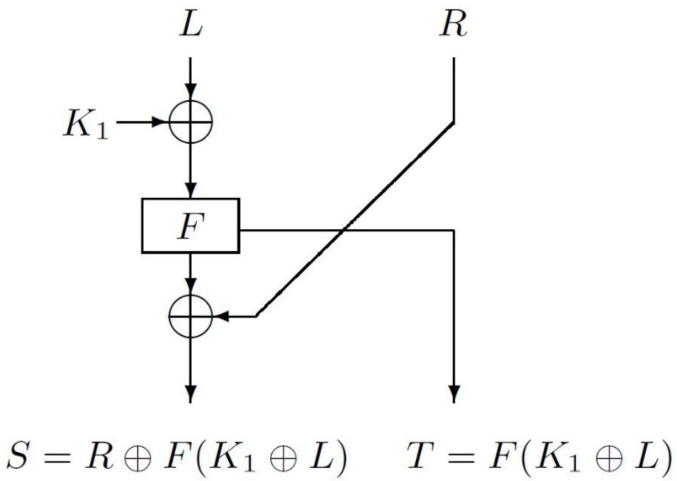
Misty R

Misty schemes

- Variant of well-known Feistel schemes
- Used to build pseudo-random permutation $\{0,1\}^{2n} \rightarrow \{0,1\}^{2n}$
- Misty L and Misty R schemes with $f_i: \{0,1\}^n \rightarrow \{0,1\}^n$ secret permutations
- Misty LKF and Misty RKF schemes with $F: \{0,1\}^n \rightarrow \{0,1\}^n$ public and K_i secret



Misty LKF



Misty RKF

Quantum cryptanalysis

- Attack using quantum computing superposition principle

- Grover's algorithm [Gro96]

  Problem: given a function $f: \{0,1\}^n \rightarrow \{0,1\}^n$ and suppose that there exist a unique $x_0 \in \{0,1\}^n$ such that $f(x_0) = 1$, find x_0.

  ➢ Grover's algorithm requires $O(2^{n/2})$ quantum queries to find x_0.

- Simon's algorithm [Sim97]

  Problem: given a function $f: \{0,1\}^n \rightarrow \{0,1\}^n$ that is observed to be invariant under some n-bit period a, find a.

  ➢ Simon's algorithm requires $O(n)$ quantum queries to find a.

Quantum distinguishing attack against 4-round Misty L

1 round $\begin{cases} S = R \\ T = R \oplus f_1(L) = X^1 \end{cases}$ 3 rounds $\begin{cases} S = X^2 \\ T = X^2 \oplus f_3(X^1) = X^3 \end{cases}$

2 rounds $\begin{cases} S = X^1 \\ T = X^1 \oplus f_2(R) = X^2 \end{cases}$ 4 rounds $\begin{cases} S = X^3 \\ T = X^3 \oplus f_4(X^2) = X^4 \end{cases}$

- $[L_1, R_1], [L_2, R_2], [L_1, R_2]$ and $[L_2, R_1]$ such that $L_1 \neq L_2$ and $R_1 \neq R_2$
- $[S_1, T_1]$, $[S_2, T_2]$, $[S_3, T_3]$ and $[S_4, T_4]$ after applying 4-round Misty L

$$S_1 \oplus S_2 \oplus S_3 \oplus S_4 = X_1^3 \oplus X_2^3 \oplus X_3^3 \oplus X_4^3$$
$$= f_3(R_1 \oplus f_1\,(L_1)) \oplus f_3(R_2 \oplus f_1\,(L_2)) \oplus f_3(R_2 \oplus f_1\,(L_1)) \oplus f_3(R_1 \oplus f_1\,(L_2))$$

- Set $R_1 = x$, we define
$$g(x) = f_3\big(x \oplus f_1(L_1)\big) \oplus f_3\big(R_2 \oplus f_1(L_2)\big) \oplus f_3\big(R_2 \oplus f_1(L_1)\big) \oplus f_3\big(x \oplus f_1(L_2)\big)$$
- g is periodic of period $s = f_1(L_1) \oplus f_1(L_2)$

We can recover s in polynomial time with Simon's algorithm

Quantum distinguishing attack against 3-round Misty RKF

1 round $\begin{cases} S = R \oplus F(K_1 \oplus L) = B^1 \\ T = F(K_1 \oplus L) \end{cases}$

2 rounds $\begin{cases} S = F(K_1 \oplus L) \oplus F(K_2 \oplus B^1) = B^2 \\ T = F(K_2 \oplus B^1) \end{cases}$

3 rounds $\begin{cases} S = F(K_2 \oplus B^1) \oplus F(K_3 \oplus B^2) = B^3 \\ T = F(K_3 \oplus B^2) \end{cases}$

- $[L_1, R]$ and $[L_2, R]$ such that $L_1 \neq L_2$
- $[S_1, T_1]$ and $[S_2, T_2]$ after applying 3-round Misty RKF

$$S_1 \oplus T_1 \oplus S_2 \oplus T_2 = F\big(K_2 \oplus R \oplus F(K_1 \oplus L_1)\big) \oplus F\big(K_2 \oplus R \oplus F(K_1 \oplus L_2)\big)$$

- Set $R = x$, we define

$$g(x) = F\big(K_2 \oplus x \oplus F(K_1 \oplus L_1)\big) \oplus F\big(K_2 \oplus x \oplus F(K_1 \oplus L_2)\big)$$

- g is periodic of period $s = F(K_1 \oplus L_1) \oplus F(K_1 \oplus L_2)$

We can recover s in polynomial time with Simon’s algorithm

Key recovery attack against d-round Misty RKF

- Combine quantum distinguishing attack against 3-round Misty RKF scheme with the Grover search [LM17,DW18,HS18]
- Recover the keys $\boldsymbol{K_1, \dots, K_d}$

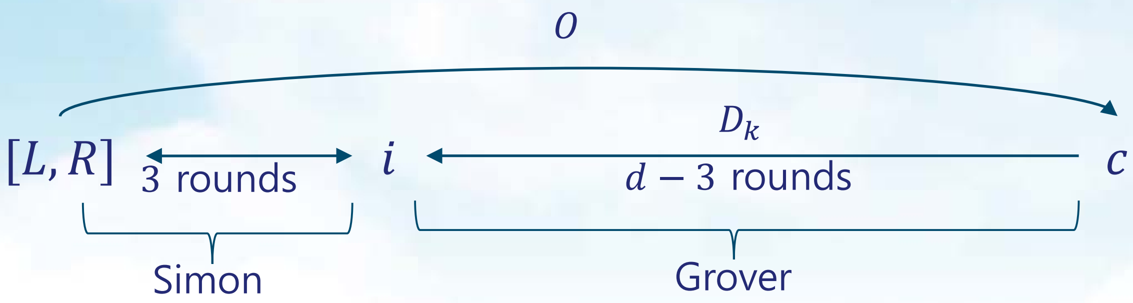
Proposition 1 [HS18] : Let $\Psi: \{0,1\}^m \times \{0,1\}^n \rightarrow \{0,1\}^n$ be a function such that $\Psi(k,\cdot): \{0,1\}^n \rightarrow \{0,1\}^n$ is a random function for any fixed $k \in \{0,1\}^m$.

Let $\Phi: \{0,1\}^m \times \{0,1\}^n \rightarrow \{0,1\}^n$ be a function such that $\Phi(k,\cdot): \{0,1\}^n \rightarrow \{0,1\}^n$ is a random function for any fixed $k \in \{0,1\}^m \backslash \{k_0\}$ and $\Phi(k_0, x) = \Psi(k_0, x \oplus k_1)$.

Then, given a quantum oracle access to $\Phi(\cdot,\cdot)$ and $\Psi(\cdot,\cdot)$, we can recover (k_0, k_1) with a constant probability and $O\left(2^{m/2}\right)$ queries.

- $k_0 = (K_4, \dots, K_d)$ and $k_1 = s$

Key recovery attack against d-round Misty RKF



- Define $W(k, L, R) \coloneqq \mathit{the\ sum\ of\ the\ left\ and\ right\ halves\ of\ } D_k \circ O([L, R])$
- Choose two different n-bit strings α, β: $\Psi(k, x) \coloneqq W(k, \alpha, x)$ and $\Phi(k, x) \coloneqq W(k, \beta, x)$

$$\begin{aligned}\Psi(k_0, x \oplus k_1) &= W(k_0, \alpha, x \oplus k_1) \\ &= F\big(K_2 \oplus x \oplus F(K_1 \oplus \alpha) \oplus F(K_1 \oplus \beta) \oplus F(K_1 \oplus \alpha)\big) \\ &= W(k_0, \beta, x) = \Phi(k_0, x)\end{aligned}$$

By applying Proposition 1, we can recover $K_4, \dots, K_d$ in $O(2^{(d-4)n/2})$

Overview of (quantum) cryptanalysis on Misty schemes

	Classical CPA	Quantum CPA
Misty L and Misty LKF with 4 rounds	$2^{n/2}$ [NPT09,NPT10] (distinguishing attack)	**Our contribution:** n (distinguishing attack)
Misty R and Misty RKF with 3 rounds	$2^{n/2}$ [NPT09,NPT10] (distinguishing attack) **Our contribution**: $2^{n/2}$ (security proof)	n [LYWHL19] (distinguishing attack)
Misty RKF with d rounds d odd, $d > 3$ d even, $d > 4$	$2^{(d-3)n/2}$ $2^{(d-4)n/2}$ (distinguishing attack)	**Our contribution:** $2^{(d-3)n/2}$ $2^{(d-3)n/2}$ (key recovery attack)

References

[DW18] Dong, X., Wang, X.: Quantum key-recovery attack on Feistel structures. Sci. ChinaInf. Sci. 61(10), 102501:1-102501:7 (2018)

[Gro96] Grover, L.K.: A Fast Quantum Mechanical Algorithm for Database Search. In: Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing.p. 212-219. STOC '96 (1996)

[HS18] Hosoyamada, A., Sasaki, Y.: Quantum Demiric-Selçuk Meet-in-the-Middle Attacks: Applications to 6-Round Generic Feistel Constructions. In: Security and Cryptography for Networks - SCN 2018, Proceedings. Lecture Notes in Computer Science, vol. 11035, pp. 386-403. Springer (2018)

[LM17] Leander, G., May, A.: Grover Meets Simon - Quantumly Attacking the FX-construction. In: ASIACRYPT. pp. 161-178. Springer (2017).

[LYWHL19] Luo, Y.Y., Yan, H.L., Wang, L., Hu, H.G., Lai, X.J.: Study on block cipher structures against simon's quantum algorithm. Journal of Cryptologic Research 6, 2019

[NPT09] Nachef, V., Patarin, J., Treger, J.: Generic Attacks on Misty Schemes -5 rounds is not enough-. IACR Cryptology ePrint Archive 2009, 405 (2009)

[NPT10] Nachef, V., Patarin, J., Treger, J.: Generic Attacks on Misty Schemes. In: Progress in Cryptology - LATINCRYPT 2010, Proceedings. Lecture Notes in Computer Science, vol. 6212, pp. 222-240. Springer (2010)

[Sim97] Simon, D.R.: On the Power of Quantum Computation. SIAM J. Comput. 26(5),1474-1483 (1997)