CS621/CSL611
Quantum Computing For Computer Scientists

Quantum Search

Dhiman Saha

Winter 2024

IIT Bhilai

Quantum Search

Applying Simon's Algorithm for Crypanalytic Attacks

Adversarial Models

- Model Q_0

  Classical attacks with classical computers
- Model Q_1

  Q_0 + Access to a quantum computer
- Model Q_2

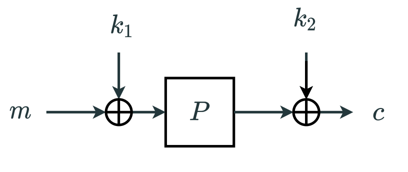
  Q_1 + superposition queries to a quantum cryptographic oracle (QCO)
- Model Q_3

  Q_1 + superposition queries to a QCO with differences in a secret key

Slide Courtesy: Mostafizar Rahman's Internal Talk at de.ci.phe.red LAB

Attack on Even Mansour

- $c = E_{k_1,k_2}(x) = P(m \oplus k_1) \oplus k_2$



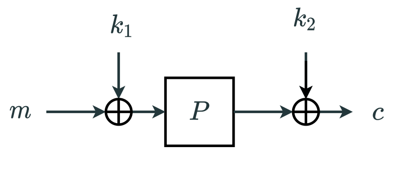
The Attack: Kuwakado and Morii

- $f : \{0,1\}^n \mapsto \{0,1\}^n$
- $x \mapsto E_{k_1,k_2}(x) \oplus P(x)$
- $f(x) = P(x \oplus k_1) \oplus P(x) \oplus k_2$
- $f(x) = f(x \oplus k_1)$
- $s = k_1$

Slide Courtesy: Mostafizar Rahman's Internal Talk at de.ci.phe.red LAB

Attack on Even Mansour

- $c = E_{k_1,k_2}(x) = P(m \oplus k_1) \oplus k_2$



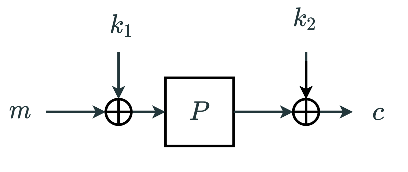
The Attack: Kuwakado and Morii

- $f : \{0,1\}^n \mapsto \{0,1\}^n$
- $x \mapsto E_{k_1,k_2}(x) \oplus P(x)$
- $f(x) = P(x \oplus k_1) \oplus P(x) \oplus k_2$
- $f(x) = f(x \oplus k_1)$
- $s = k_1$

Slide Courtesy: Mostafizar Rahman's Internal Talk at de.ci.phe.red LAB

Attack on Even Mansour

- $c = E_{k_1,k_2}(x) = P(m \oplus k_1) \oplus k_2$



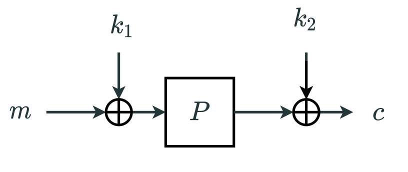
The Attack: Kuwakado and Morii

- $f : \{0,1\}^n \mapsto \{0,1\}^n$
- $x \mapsto E_{k_1,k_2}(x) \oplus P(x)$
- $f(x) = P(x \oplus k_1) \oplus P(x) \oplus k_2$
- $f(x) = f(x \oplus k_1)$
- $s = k_1$

Slide Courtesy: Mostafizar Rahman's Internal Talk at de.ci.phe.red LAB

Attack on Even Mansour

- $c = E_{k_1,k_2}(x) = P(m \oplus k_1) \oplus k_2$



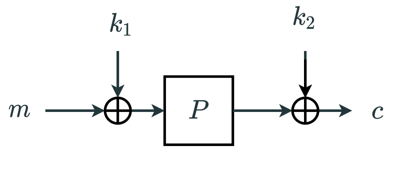
The Attack: Kuwakado and Morii

- $f : \{0,1\}^n \mapsto \{0,1\}^n$
- $x \mapsto E_{k_1,k_2}(x) \oplus P(x)$
- $f(x) = P(x \oplus k_1) \oplus P(x) \oplus k_2$
- $f(x) = f(x \oplus k_1)$
- $s = k_1$

Slide Courtesy: Mostafizar Rahman's Internal Talk at de.ci.phe.red LAB

Attack on Even Mansour

- $c = E_{k_1,k_2}(x) = P(m \oplus k_1) \oplus k_2$

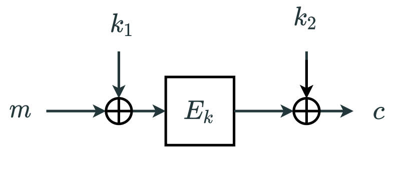


The Attack: Kuwakado and Morii

- $f : \{0,1\}^n \mapsto \{0,1\}^n$
- $x \mapsto E_{k_1,k_2}(x) \oplus P(x)$
- $f(x) = P(x \oplus k_1) \oplus P(x) \oplus k_2$
- $f(x) = f(x \oplus k_1)$
- $s = k_1$

Slide Courtesy: Mostafizar Rahman's Internal Talk at de.ci.phe.red LAB

Attack on FX Construction???



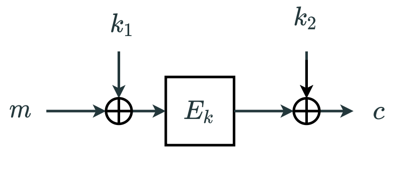
- $c = E_{k,k_1,k_2}(x) = E_k(m \oplus k_1) \oplus k_2$

Possible Attack ??

- $f : \{0,1\}^n \mapsto \{0,1\}^n$
- $x \mapsto E_{k,k_1,k_2}(x) \oplus E_k(x)$
- $f(x) = E_k(x \oplus k_1) \oplus E_k(x) \oplus k_2$
- $f(x) = f(x \oplus k_1)$
- $s = k_1$

Slide Courtesy: Mostafizar Rahman's Internal Talk at de.ci.phe.red LAB

Attack on FX Construction???



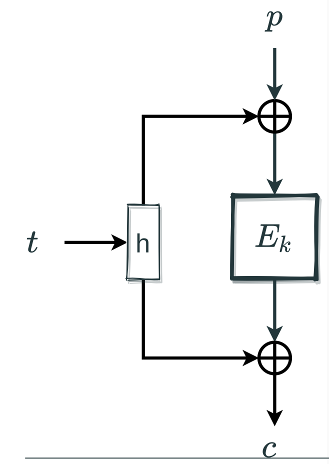
- $c = E_{k,k_1,k_2}(x) = E_k(m \oplus k_1) \oplus k_2$

Possible Attack ??

- $f : \{0,1\}^n \mapsto \{0,1\}^n$
- $x \mapsto E_{k,k_1,k_2}(x) \oplus E_k(x)$
- $f(x) = E_k(x \oplus k_1) \oplus E_k(x) \oplus k_2$
- $f(x) = f(x \oplus k_1)$
- $s = k_1$

Attack on LRW

- $c = E_k(p \oplus h(t)) \oplus h(t)$



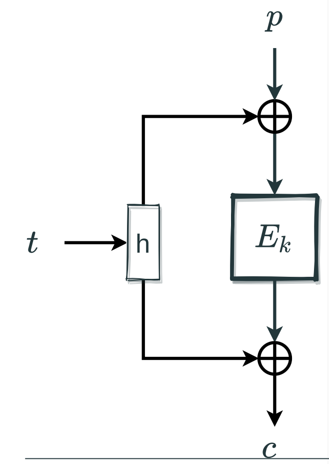
The Attack: Kaplan *et. al.*

- $f : \{0,1\}^n \mapsto \{0,1\}^n$
- $f(x) = E_k(x \oplus h(t_0)) \oplus h(t_0) \oplus E_k(x \oplus h(t_1)) \oplus h(t_1)$
- $s = h(t_0) \oplus h(t_1)$

Slide Courtesy: Mostafizar Rahman's Internal Talk at de.ci.phe.red LAB

Attack on LRW

- $c = E_k(p \oplus h(t)) \oplus h(t)$



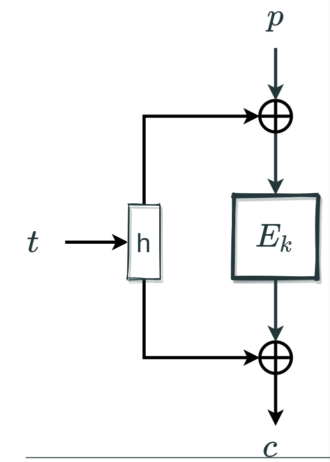
The Attack: Kaplan *et. al*.

- $f : \{0,1\}^n \mapsto \{0,1\}^n$
- $f(x) = E_k(x \oplus h(t_0)) \oplus h(t_0) \oplus E_k(x \oplus h(t_1)) \oplus h(t_1)$
- $s = h(t_0) \oplus h(t_1)$

Slide Courtesy: Mostafizar Rahman's Internal Talk at de.ci.phe.red LAB

Attack on LRW

- $c = E_k(p \oplus h(t)) \oplus h(t)$

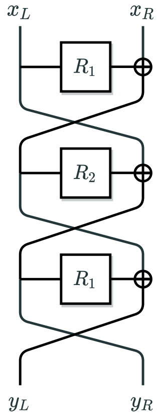


The Attack: Kaplan *et. al.*

- $f : \{0,1\}^n \mapsto \{0,1\}^n$
- $f(x) = E_k(x \oplus h(t_0)) \oplus h(t_0) \oplus E_k(x \oplus h(t_1)) \oplus h(t_1)$
- $s = h(t_0) \oplus h(t_1)$

Slide Courtesy: Mostafizar Rahman's Internal Talk at de.ci.phe.red LAB

Attack on 3-round Feistel

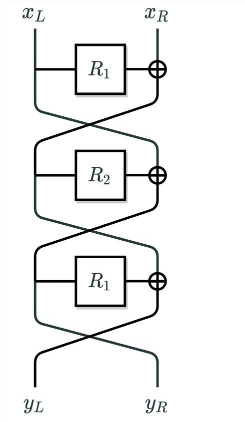


- $y_R = R_2(R_1(x_L) \oplus x_R) \oplus x_L$

The Attack: Kuwakado and Morii

- $f : \{0,1\} \times \{0,1\}^n \mapsto \{0,1\}^n$
- $f(b,x) = R_2(x \oplus R_1(\alpha_b)),\ b \in \{0,1\}$
- $f(b,x) = f(b \oplus 1, x \oplus R_1(\alpha_0) \oplus R_1(\alpha_1))$
- $s = 1 || R_1(\alpha_0) \oplus R_1(\alpha_1)$

Attack on 3-round Feistel

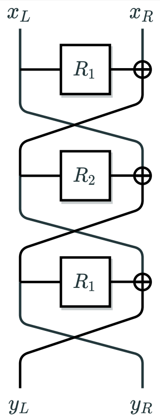


- $y_R = R_2(R_1(x_L) \oplus x_R) \oplus x_L$

The Attack: Kuwakado and Morii

- $f : \{0,1\} \times \{0,1\}^n \mapsto \{0,1\}^n$
- $f(b,x) = R_2(x \oplus R_1(\alpha_b)),\ b \in \{0,1\}$
- $f(b,x) = f(b \oplus 1, x \oplus R_1(\alpha_0) \oplus R_1(\alpha_1))$
- $s = 1||R_1(\alpha_0) \oplus R_1(\alpha_1)$

Attack on 3-round Feistel

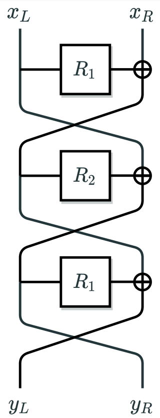


- $y_R = R_2(R_1(x_L) \oplus x_R) \oplus x_L$

The Attack: Kuwakado and Morii

- $f : \{0,1\} \times \{0,1\}^n \mapsto \{0,1\}^n$
- $f(b, x) = R_2(x \oplus R_1(\alpha_b)),\ b \in \{0,1\}$
- $f(b, x) = f(b \oplus 1, x \oplus R_1(\alpha_0) \oplus R_1(\alpha_1))$
- $s = 1 || R_1(\alpha_0) \oplus R_1(\alpha_1)$

Attack on 3-round Feistel



- $y_R = R_2(R_1(x_L) \oplus x_R) \oplus x_L$

The Attack: Kuwakado and Morii

- $f : \{0,1\} \times \{0,1\}^n \mapsto \{0,1\}^n$
- $f(b,x) = R_2(x \oplus R_1(\alpha_b)),\ b \in \{0,1\}$
- $f(b,x) = f(b \oplus 1, x \oplus R_1(\alpha_0) \oplus R_1(\alpha_1))$
- $s = 1||R_1(\alpha_0) \oplus R_1(\alpha_1)$