FX Construction and Quantum Attacks
or
How not to extend your key-length

Gregor Leander (joint work with Alex May)

ESC 2017

Horst Görtz Institute
for IT-Security

Outline

Introduction

- Quantum attacks on symmetric schemes understudied.
- Basic conclusion is: double the key-length.
- Two most popular generic ways of doing so:
  - Multiple-encryption
  - FX-construction
- Both not as good as you might think.
  - Multiple encryption: Kaplan 2014
  - FX construction: This talk

Quantum Attacks on Symmetric Crypto

Basically two attacks known:

Simon's Algorithm

Used to e.g. break Even-Mansour

Grover's Algorithm

Used to speed-up brute force

Grover's Algorithm

Grover's Algorithm

Given $f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2$ such that $\exists! x_0$

$$f(x) = \begin{cases} 1 & \text{if } x = x_0 \\ 0 & \text{else} \end{cases}$$

than one can recover x_0 in time $\mathcal{O}(2^{n/2})$

- Very general search algorithm.
- Later generalized: amplitute amplification.

Grover's Algorithm to break block ciphers

Generic block cipher

$$\text{Enc}(m) = E_k(m)$$

$$m \longrightarrow \boxed{E_k} \longrightarrow c$$

Conversion into Grover's problem (given a message/cipher-text pair):

$$f(x) = \begin{cases} 1 & \text{if } E_x(m) = c \\ 0 & \text{else} \end{cases}$$

The Attack

Apply Grover's Algorithm to f. Recover k in time $\mathcal{O}(2^{n/2})$.

Simon's Algorithm

Simon's Algorithm

Given $F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$ such that $\exists s$

$$F(x) = F(x + s) \quad \forall x$$

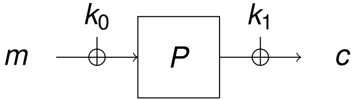
than one can recover s in linear time.

- Originally: $F(x) = F(y) \Leftrightarrow y = x + s$
- Used by Kuwakado and Morii to break Even-Mansour
- Extended to many modes in [KLLNP]

Simon's Algorithm to break EM

The Even-Mansour scheme:

$$\text{Enc}(m) = E(m + k_0) + k_1$$



Conversion into Simon's problem:

$$F(x) = \text{Enc}(x) + P(x)$$

Then

$$F(x) = F(x + k_0)$$

The Attack (with quantum queries)

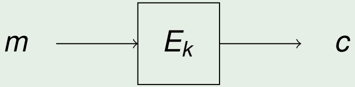
Apply Simon's algorithm to F. Recover k_0 in linear time.

Outline

Combine?

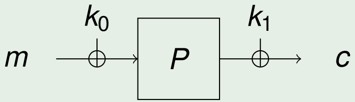
We can break:

Generic Ciphers



Time: $\mathcal{O}(2^{n/2})$

Even-Mansour

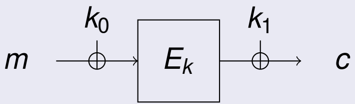


Time: $\mathcal{O}(n)$

What about combining this?

The FX-Construction

FX-Construction



Question

How to attack the FX construction in a quantum setting?

Attacking the FX construction

Question

How to attack the FX construction in a quantum setting?

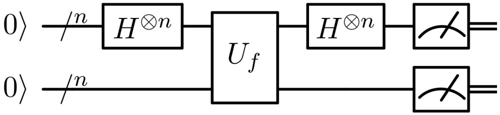
This is actually a question about:

Combining Simon and Grover

How to combing Simon's and Grover's algorithm?

Let's have a closer look.

Inside Simon's Algorithm



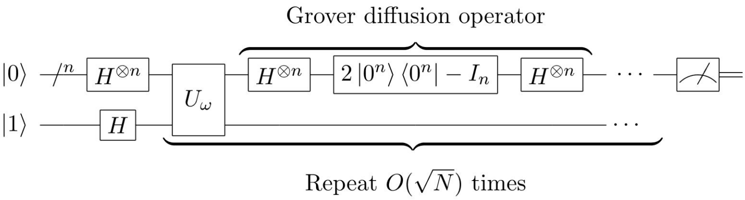
Key-features:

- Requires to implement Enc$(x) + P(x)$ as unitary embedding.
- Running once and measuring results in x s.t.

$$\langle k_0, x \rangle = 0$$

- Running $n + \epsilon$ times results in k_0 by solving linear equations

Inside Grover's Algorithm (Amplitude Amplification)



Key-features:

- Requires a quantum algorithm $\mathcal{A}$ with initial success probability p.
- Requires phase-flipping for good states
- Running $p^{-1/2}$ times results in a good state with high prob.

Combining: Avoid Measurements

Approach: Use Simon's algo for $\mathcal{A}$

Problem

Measuring not allowed in $\mathcal{A}$ for Grover. Simon's algo requires measuring.

Combining: Avoid Measurements

Approach: Use Simon's algo for $\mathcal{A}$

Problem

Measuring not allowed in $\mathcal{A}$ for Grover. Simon's algo requires measuring.

Sketch of the solution:

- Run $n + \epsilon$ Simons in parallel
- Linear algebra to compute candidate for k_0
- Check against message/cipher-text pairs
- If that fits: flip the phase

Combining: Avoid Measurements

Approach: Use Simon's algo for $\mathcal{A}$

Problem

Measuring not allowed in $\mathcal{A}$ for Grover. Simon's algo requires measuring.

Sketch of the solution:

- Run $n + \epsilon$ Simons in parallel
- Linear algebra to compute candidate for k_0
- Check against message/cipher-text pairs
- If that fits: flip the phase

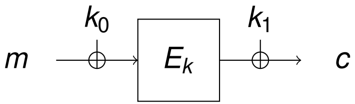
Result

The FX construction can be broken in time $\mathcal{O}(2^{n/2})$. Quantum computer gets n times bigger.

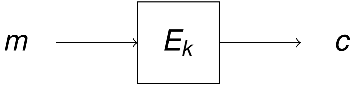
Outline

Conclusion

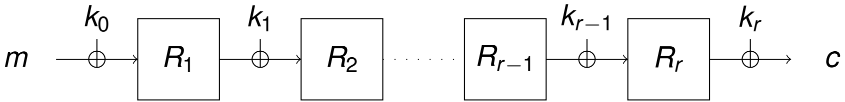
In a quantum world



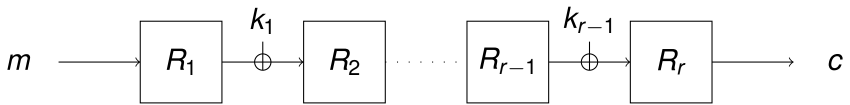
is as secure (linear overhead) as



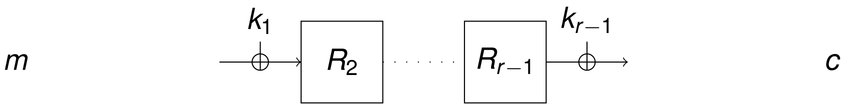
Key-Alternating Ciphers



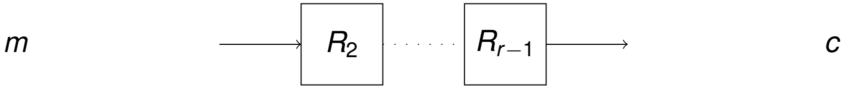
Key-Alternating Ciphers



Key-Alternating Ciphers



Key-Alternating Ciphers



Key-Alternating Ciphers

m c

Polynomial attack on key-alternating ciphers

Key-Alternating Ciphers

m c

Polynomial attack on key-alternating ciphers does not work like that

Future Work

Possible future topics:

- Correct attacks on key-alternating ciphers
- Other applications of Simon/Grover combination

Thank you.