Quantum Linear Key-recovery Attacks Using the QFT

André Schrottenloher

Univ Rennes, Inria, CNRS, IRISA

Motivation

A block cipher $E_K : \mathbb{F}_2^n \to \mathbb{F}_2^n$

key-recovery attack on E_K: given access to the black-box E_K, find K in

- $< 2^{|K|}$ evaluations of E_K (classical) (**faster than brute force**)
- $< 2^{|K|/2}$ evaluations of E_K (quantum) (**faster than Grover search**)

Motivation (ctd.)

- **Linear cryptanalysis** is a powerful cryptanalysis technique
- **Advanced linear (key-recovery) attacks** use the FFT

Previous work on quantum linear attacks:

- **[KLLN16]**: using Grover's algorithm
- **[H22]**: using the QFT to speedup some distinguishers

This work: using the QFT in linear **key-recovery attacks**.

Kaplan, Leurent, Leverrier, Naya-Plasencia, "Quantum differential and linear cryptanalysis", ToSC 2016

Hosoyamada, "Quantum speed-up for multidimensional (zero correlation) linear and integral distinguishers", ePrint 2022

Quantum toolbox

- The state of a quantum system is a **superposition**

$$\sum_{x \in \mathbb{F}_2^{\mathbf{n}}} \alpha_x |x\rangle \text{ with } \sum_x |\alpha_x|^2 = 1$$

- The amplitudes α_x are **not** immediately exploitable
- Computing a Walsh-Hadamard transform on the amplitudes is easy: if $f : \{0,1\}^{\mathsf{n}} \to \{-1,1\}$ is a function:

$$\frac{1}{2^{\mathsf{n}/2}} \sum_x f(x) |x\rangle \overset{H}{\longmapsto} \frac{1}{2^{\mathsf{n}}} \sum_y \underbrace{\left(\sum_x (-1)^{x \cdot y} f(x) \right)}_{:= \widehat{f}(y)} |y\rangle$$

Quantum search

Given a **setup** algorithm that produces: $\sum_x \alpha_x |x\rangle |\text{flag}(x)\rangle$, we find x_g such that $\text{flag}(x_g) = 1$ in $\mathcal{O}\left(\frac{1}{|\alpha_{x_g}|}\right)$ calls.

Outline

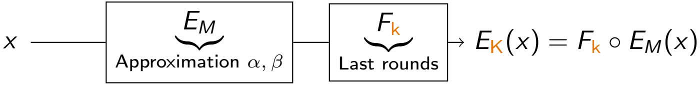
1. Linear Cryptanalysis
2. Correlation State
3. Applications

Linear Cryptanalysis

Linear cryptanalysis

- Exploits a **linear approximation** of E: choice of $(\alpha, \beta) \in \mathbb{F}_2^n$ such that $\alpha \cdot x + \beta \cdot E(x)$ is biased
- The quality of an approximation (α, β) is related to its **ELP**
- If ELP is large enough, we have a **linear distinguisher** which can be used in a **last-rounds** key-recovery attack

(Matsui's) last-rounds attack



Using the whole codebook, time about $\mathcal{O}\left(2^n \times 2^{|k|}\right)$:

1. For each guess z of the subkey k, compute the **experimental correlation**:

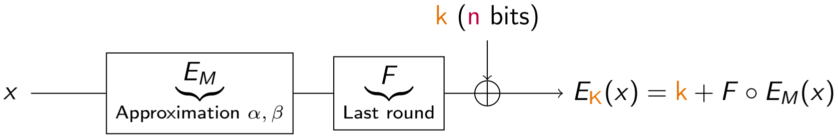
$$\widehat{\mathrm{cor}}(z) := \frac{1}{2^n} \sum_x (-1)^{\alpha \cdot x + \beta \cdot F_z^{-1}(E_K(x))} \quad .$$

2. The good subkey k has (one of) the highest $|\widehat{\mathrm{cor}}(z)|$

Statistics

- Right subkey: $|\widehat{\mathrm{cor}}(k)|$ is around $\sqrt{\mathrm{ELP}}$
- Wrong subkey: $|\widehat{\mathrm{cor}}(z)|$ is around $2^{-n/2}$

Improvement with the FFT



$$\widehat{\mathrm{cor}}(z) = \frac{1}{2^n} \sum_x (-1)^{\alpha \cdot x + \beta \cdot F^{-1}(z + E_K(x))} = \frac{1}{2^n} \sum_x (-1)^{\alpha \cdot E_K^{-1}(x) + \beta \cdot F^{-1}(z+x)}$$

Introduce two functions f, g:

$$\begin{cases} f, g \ : \mathbb{F}_2^n \to \{-1, 1\} \\ f(x) := (-1)^{\alpha \cdot E_K^{-1}(x)} \\ g(x) := (-1)^{\beta \cdot F^{-1}(x)} \end{cases}$$

$$\widehat{\mathrm{cor}}(z) = \frac{1}{2^n} \sum_x f(x) g(z+x) := \frac{1}{2^n} (f \star g)(z)$$

Linear cryptanalysis: the FFT (ctd.)

The experimental correlations = **discrete convolution** of f and g.

In our case: $(f \star g) = \frac{1}{2^n} \widehat{\widehat{f} \cdot \widehat{g}}$.

1. Compute $\widehat{f}$ using a FWHT $\rightarrow \mathcal{O}(n2^n)$
2. Compute $\widehat{g}$ using a FWHT $\rightarrow \mathcal{O}(n2^n)$
3. Do a pointwise product $\rightarrow \mathcal{O}(2^n)$
4. Compute the FWHT again $\rightarrow \mathcal{O}(n2^n)$
5. Find the candidate key(s) of highest correlation

Improved time: $\mathcal{O}(n2^n)$ instead of $\mathcal{O}\left(2^n \times 2^{|k|}\right) = \mathcal{O}(2^n \times 2^n)$.

Correlation State

Definition

$$|\mathsf{Cor}\rangle := \sum_{z} \widehat{\mathrm{cor}}(z)\,|z\rangle$$

1. Now: how do we compute this?
2. Next: how do we use it?

Computing $|\mathrm{Cor}\rangle$

Recall the two functions f, g:

$$\begin{cases} f(x) := (-1)^{\alpha \cdot E_{K}^{-1}(x)} \\ g(x) := (-1)^{\beta \cdot F^{-1}(x)} \end{cases}$$

and

$$\widehat{\mathrm{cor}}(z) = \frac{1}{2^{n}} (f \star g)(z) = \frac{1}{2^{2n}} \widehat{\widehat{f} \cdot \widehat{g}}$$

We need:

$$\frac{1}{2^{2n}} \sum_{z} \widehat{\widehat{f} \cdot \widehat{g}}(z) \, |z\rangle = H \left(\frac{1}{2^{3n/2}} \underbrace{\sum_{y} \widehat{f}(y) \widehat{g}(y) \, |y\rangle}_{\text{So let's compute this}} \right)$$

Computing $|\mathrm{Cor}\rangle$ (ctd.)

1. Compute f in the amplitude (a phase flip)

$$\sum_x f(x) |x\rangle$$

2. Apply H

$$\sum_y \widehat{f}(y) |y\rangle$$

3. Compute $\widehat{g}$ **digitally**

$$\sum_y \widehat{f}(y) |y\rangle |\widehat{g}(y)\rangle$$

4. Transfer $\widehat{g}(y)$ into the amplitude

$\Longrightarrow$ involves quantum **state preparation** / rejection sampling, & a small amplification layer

$$\sum_y \widehat{f}(y)\widehat{g}(y) |y\rangle$$

Computing $|\mathrm{Cor}\rangle$ (ctd.)

There is a quantum algorithm that (on empty input $|0\rangle$) returns $|\mathrm{Cor}\rangle$.

The time complexity is dominated by:

- (a few) queries to E_{K} (to compute f)
- (a few) computations of $\widehat{g}$

Applications

Using the correlation state

Classical case

- We compute all $\widehat{\text{cor}}(z)$
- We find the biggest one(s)

Quantum case

- We can compute $|\text{Cor}\rangle = \sum_z \widehat{\text{cor}}(z)\,|z\rangle$
- We **do not** have access to the values

$|\text{Cor}\rangle$ is a superposition of subkey guesses where **the good guess has a higher amplitude**

Idea: use $|\text{Cor}\rangle$ as a **shortcut** in an exhaustive key search.

Using the correlation state (ctd)

Let $\mathsf{K} = (\mathsf{k}, \mathsf{k}')$ be the full cipher key.

Grover search:

- Create superposition over z, z': $\frac{1}{2^{(|\mathsf{k}|+|\mathsf{k}'|)/2}} \sum_{z,z'} |z, z'\rangle$
- Flag k, k': $\frac{1}{2^{(|\mathsf{k}|+|\mathsf{k}'|)/2}} \sum_{z,z'} |z, z', \mathrm{flag}\rangle$
- Initial amplitude $\frac{1}{2^{(|\mathsf{k}|+|\mathsf{k}'|)/2}} \implies$ **amplify** with $\simeq 2^{(|\mathsf{k}|+|\mathsf{k}'|)/2}$ iterates

"Shortcut":

- **Compute** $|\mathrm{Cor}\rangle$: $\sum_z \widehat{\mathrm{cor}}(z) \, |z\rangle$
- **Complete** with z': $\frac{1}{2^{|\mathsf{k}'|/2}} \sum_{z,z'} \widehat{\mathrm{cor}}(z) \, |z, z'\rangle$
- **Flag** k, k': $\frac{1}{2^{|\mathsf{k}'|/2}} \sum_{z,z'} \widehat{\mathrm{cor}}(z) \, |z, z', \mathrm{flag}\rangle$
- **Amplify** this:

$$\simeq \frac{1}{\widehat{\mathrm{cor}}(\mathsf{k})} \times 2^{|\mathsf{k}'|/2} \simeq \frac{1}{\sqrt{\mathrm{ELP}}} \times 2^{|\mathsf{k}'|/2} < 2^{(|\mathsf{k}|+|\mathsf{k}'|)/2}$$

Quantum - classical comparison

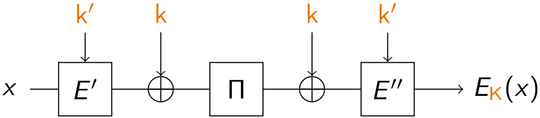
Classical cryptanalysis only needs to distinguish.

$\Longrightarrow$ **extremely small** ELP values are used

- The speedup here depends directly on $\sqrt{\mathrm{ELP}}$, so it's small
- Furthermore, building $|\mathrm{Cor}\rangle$ requires either qRAM or superposition queries

What is the largest speedup?

Consider $|k| = n, |k'| = 2n$, Π an unkeyed permutation.



There is a key-recovery attack on E_K using:

- 2^n classical queries (full codebook)
- $\mathcal{O}(n2^n)$ bits of qRAM
- $\mathcal{O}\left(\sqrt{n}(n + \text{ qRAM query})2^n\right)$ quantum operations

$\Longrightarrow$ super-Grover speedup w.r.t. the best classical attack $2^{2.5n}$

$\Longrightarrow$ **remains** (contrary to Simon-based attack) if we only have half the codebook

Conclusion

- Using the QFT to accelerate a **statistical** attack
- Still few (working) applications so far

Open question:

- Most issues would be solved if we had an efficient algorithm to find the largest correlation in $|\mathrm{Cor}\rangle$
- However, if $|\mathrm{Cor}\rangle$ is produced as a black-box, this seems very difficult

Report: ePrint 2023/184

Thank you!