Quantum Speed-Up for Multidimensional (Zero Correlation) Linear Distinguishers

NTT Social Informatics Laboratories

Akinori Hosoyamada

Background on Classical Cryptanalysis

Linear Distinguisher (1-dimensional) [Matsui 1993]

NTT

- $P: \{0,1\}^n \to \{0,1\}^n$: permutation (random permutation or block cipher E_K)
- α, β : n-bit strings (input & output masks)
- The **linear correlation** is defined by

$$\mathrm{Cor}(P; \alpha, \beta) \coloneqq \Pr_x[\alpha \cdot x = \beta \cdot P(x)] - \Pr_x[\alpha \cdot x \neq \beta \cdot P(x)]$$

- P : random permutation ⇒ $|\mathrm{Cor}(P; \alpha, \beta)|$ is very small
- If $|\mathrm{Cor}(E_K; \alpha, \beta)|$ is large, then E_K is distinguished by checking whether the proportion of x satisfying $\alpha \cdot x = \beta \cdot E_K(x)$ is likely to be much larger/smaller than 1/2.
  - Data/time complexity: $\mathrm{Cor}(E_K; \alpha, \beta)^{-2}$

Multidimensional Linear Distinguisher

[Hermelin & Nyberg 2008]

- $V \subset (\{0,1\}^n)^2$: an ($\mathbb{F}_2$-)vector space with a basis $(\alpha_1, \beta_1), \dots, (\alpha_d, \beta_d)$
- $\mathrm{Lin}^P(x) \coloneqq (\ \alpha_1 \cdot x \oplus \beta_1 \cdot P(x),\ \dots\ ,\ \alpha_d \cdot x \oplus \beta_d \cdot P(x)\ ) \in \{0,1\}^d$
  - "multidimensional linear approximation" of P (w.r.t. V and the basis)
- $p^P(z) := \Pr_x[\mathrm{Lin}^P(x) = z]$ (→ close to the uniform distribution if P is random)

Multidimensional Linear Distinguisher
[Hermelin & Nyberg 2008]

- $V \subset (\{0,1\}^n)^2$: an ($\mathbb{F}_2$-)vector space with a basis $(\alpha_1, \beta_1), \ldots, (\alpha_d, \beta_d)$
- $\mathrm{Lin}^P(x) := (\ \alpha_1 \cdot x \oplus \beta_1 \cdot P(x), \ \ldots \ , \ \alpha_d \cdot x \oplus \beta_d \cdot P(x) \ ) \in \{0,1\}^d$
  - "multidimensional linear approximation" of P (w.r.t. V and the basis)
- $p^P(z) := \Pr_x[\mathrm{Lin}^P(x) = z]$ (→ close to the uniform distribution if P is random)

Fact $\displaystyle\sum_{(\alpha,\beta)\in V-\{0\}} \mathrm{Cor}(P;\alpha,\beta)^2 = \mathrm{Cap}(p^P)$

"capacity", related to χ^2 test statistic

Multidimensional Linear Distinguisher
[Hermelin & Nyberg 2008]

- $V \subset (\{0,1\}^n)^2$: an ($\mathbb{F}_2$-)vector space with a basis $(\alpha_1, \beta_1), \ldots, (\alpha_d, \beta_d)$
- $\mathrm{Lin}^P(x) \;:=\; (\;\alpha_1 \cdot x \oplus \beta_1 \cdot P(x),\; \ldots\;,\; \alpha_d \cdot x \oplus \beta_d \cdot P(x)\;) \in \{0,1\}^d$
  - "multidimensional linear approximation" of P (w.r.t. V and the basis)
- $p^P(z) := \Pr_x[\mathrm{Lin}^P(x) = z]$ (→ close to the uniform distribution if P is random)

Fact $\displaystyle\sum_{(\alpha,\beta)\in V-\{0\}} \mathrm{Cor}(P;\alpha,\beta)^2 = \mathrm{Cap}(p^P)$

"capacity", related to χ^2 test statistic

If $\sum_{(\alpha,\beta)\in V-\{0\}} \mathrm{Cor}(E_K;\alpha,\beta)^2$ is large, then E_K can be distinguished by computing the χ^2 test statistic and checking if it is large or not

Complexity: $\sqrt{2^d}/\mathrm{Cap}(p^{E_K})$

Multidimensional Zero Correlation Linear Distinguisher
[Bogdanov & Rijmen 2014, Bogdanov et al. 2012]

- If $\mathrm{Cor}(E_K; \alpha, \beta)$ is exactly zero for some E_K and all (α, β) in a ($\mathbb{F}_2$-)vector space V, then the corresponding $\mathrm{Cap}(p^{E_K})$ is exactly zero
- If P is a random permutation, the corresponding capacity $\mathrm{Cap}(p^P)$ is non-zero with high probability

- Thus E_K is distinguished by computing a suitable test statistic
  - Complexity is $\approx 2^n/\sqrt{2^{\dim(V)}}$ for general cases
  - Faster for some special cases → a link to integral distinguisher

Link to Integral Distinguishers
[Bogdanov et al. 2012, Sun et al. 2015]

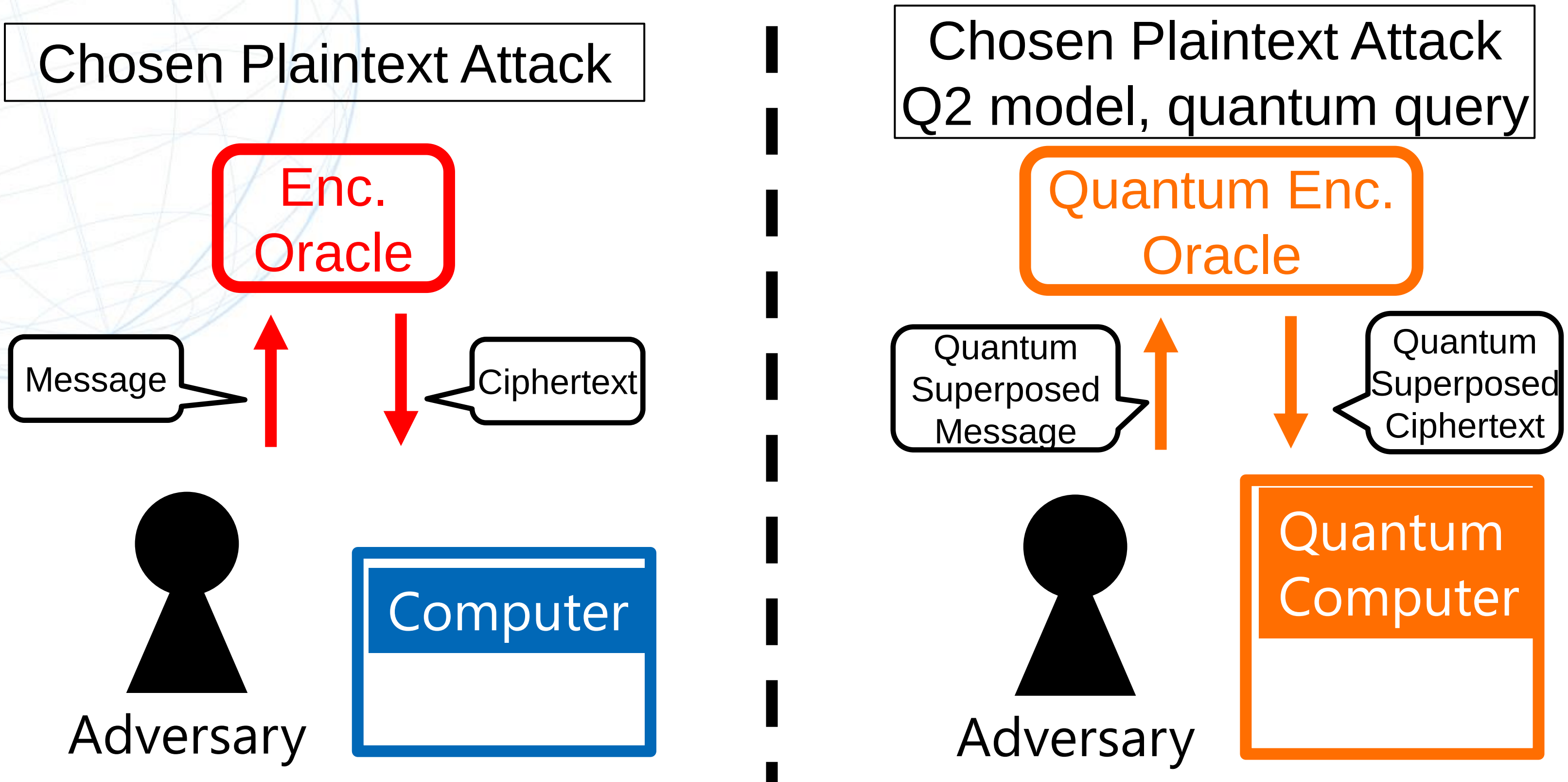
- V : the set (vector space) of input output masks
- We say that input-output masks are **linearly independent** if V is decomposed as $V = V_1 \times V_2$

Multidimensional zero correlation linear distinguisher w/ linearly independent masks
⇕ equivalent
Integral distinguisher based on balanced functions

- Complexity of integral distinguisher: $2^{n-\dim(V_1)}$
  - Faster than zero correlation linear distinguisher ($2^n/\sqrt{2^{\dim(V)}}$) sometimes

Background on Quantum Cryptanalysis & Motivation of Research

Attack Models



Simon's Period Finding Algorithm [Simon 1997]

NTT

Problem

Suppose a function $f\colon\{0,1\}^n \to S$ and a secret value $s \in \{0,1\}^n$ satisfy

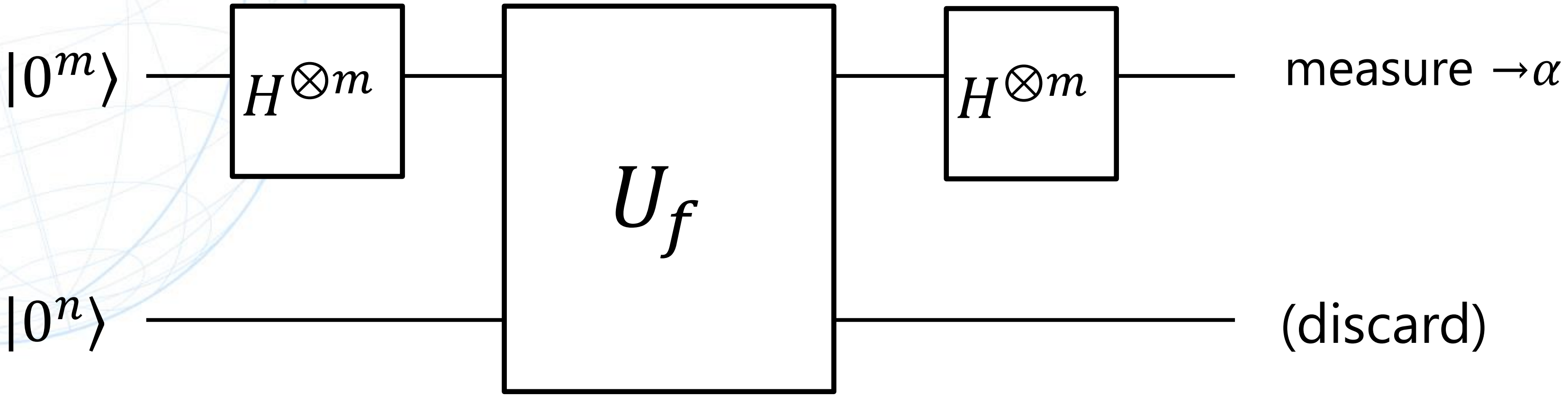
$$\forall x \in \{0,1\}^n \;\; f(x \oplus s) = f(x).$$

Given the (quantum) oracle of f, find s.

Classical Algorithms: Exponential Time

Simon's algorithm: Polynomial Time

Simon's subroutine



1. Run the subroutine multiple times to get multiple α
2. Do some linear algebra

Quantum Amplitude Amplification (QAA)
[Brassard et al. 2002]

- What is given :

  Access to Boolean function $F\colon \{0,1\}^n \to \{0,1\}$, n-bit unitary U

  p := (prob. of getting x s.t. $F(x) = 1$ when measuring $U|0^n\rangle$)

- Goal :

  a unitary that outputs x s.t. $F(x) = 1$ with high probability

- What QAA does :

  Achieve the goal with $p^{-1/2}$ queries to U, U^*, and F

Kaplan et al.'s Quantum Distinguisher

NTT

- Kaplan et al. showed a quadratic speed-up for **1-dimensional** linear distinguisher [Kaplan et al. 2016]

Idea of the attack

- Define $F: \{0,1\}^n \rightarrow \{0,1\}$ by $F(x) = 1$ iff $\alpha \cdot x = \beta \cdot E_K(x)$
  - Classical linear distinguisher ⇔ approximately counting x s.t. $F(x) = 1$
- Apply quantum counting algorithm [Brassard et al. 2002]
  - Quantum counting algorithm provides a quadratic speed-up for counting x s.t. $F(x) = 1$ for a Boolean function F

Motivation of Research

- We want a quantum speed-up for multidimensional linear distinguishers
  - If a high-dimensional approximation is available, it makes sense to utilize it
  - The best classical linear distinguishers are often multidimensional
  - We also want a quantum speed-up for (multidimensional) zero correlation / integral distinguishers if possible
- Issue: It seems hard to extend Kaplan et al.'s technique to multidimensional cases
  - The core of their technique is to count $|F^{-1}(1)|$ for some Boolean function F
  - Multidimensional linear distinguishers are essentially χ^2-test, and it's unclear whether there is a Boolean function corresponding to the χ^2-test
  - A new technique is needed

How to Extract Linear Correlations into Quantum Amplitudes

Idea: Focusing on Fourier Transforms

NTT

Fact 1 Linear correlations are related to the Fourier transform

$$\mathrm{Cor}(P;\alpha,\beta) \propto \underline{\mathcal{F}(P_{\mathrm{emb}})}(\alpha,\beta)$$

Fourier transform of a function derived from P

Fact 2 The source of some exponential quantum speed-up is quantum Fourier transform (QFT) : Shor's, Simon's, etc.

(Hadamard = QFT on $(\mathbb{Z}/2\mathbb{Z})^n$)

Idea: Focusing on Fourier Transforms

Fact 1 Linear correlations are related to the Fourier transform

$$\mathrm{Cor}(P;\alpha,\beta) \propto \underline{\mathcal{F}(P_{\mathrm{emb}})}(\alpha,\beta)$$

Fourier transform of a function derived from P

Fact 2 The source of some exponential quantum speed-up is quantum Fourier transform (QFT) : Shor's, Simon's, etc.

(Hadamard = QFT on $(\mathbb{Z}/2\mathbb{Z})^n$)

Any technique to connect
linear correlations & quantum computation
via Fourier transform?

Idea: Focusing on Fourier Transforms

NTT

Fact 1 Linear correlations are related to the Fourier transform

$$\mathrm{Cor}(P;\alpha,\beta) \propto \underline{\mathcal{F}(P_{\mathrm{emb}})}(\alpha,\beta)$$

Fourier transform of a function derived from P

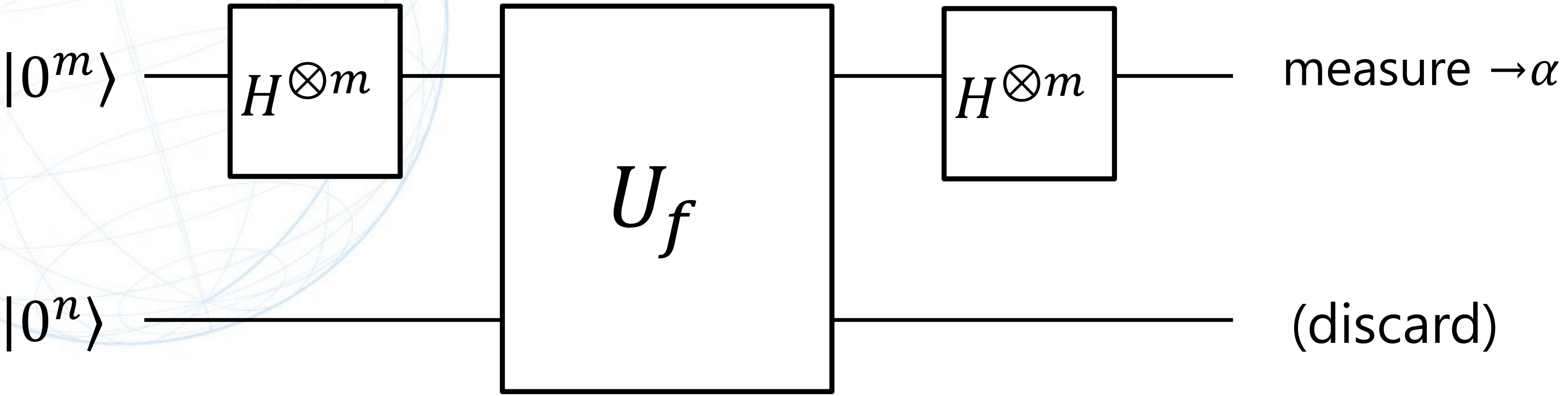
Fact 2 The source of some exponential quantum speed-up is quantum Fourier transform (QFT) : Shor's, Simon's, etc.

(Hadamard = QFT on $(\mathbb{Z}/2\mathbb{Z})^n$)

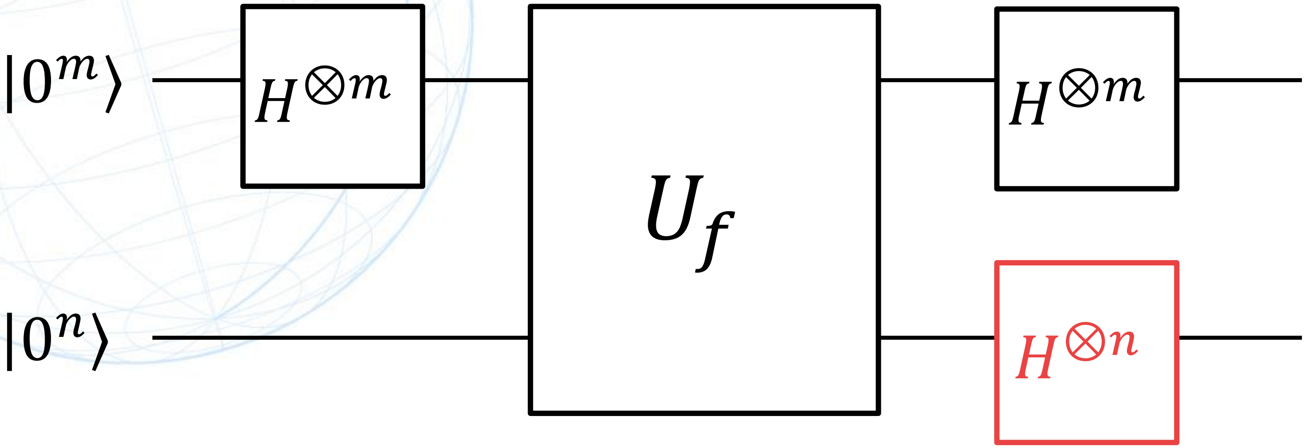
Any technique to connect linear correlations & quantum computation via Fourier transform?

➡ **Simon's subroutine**

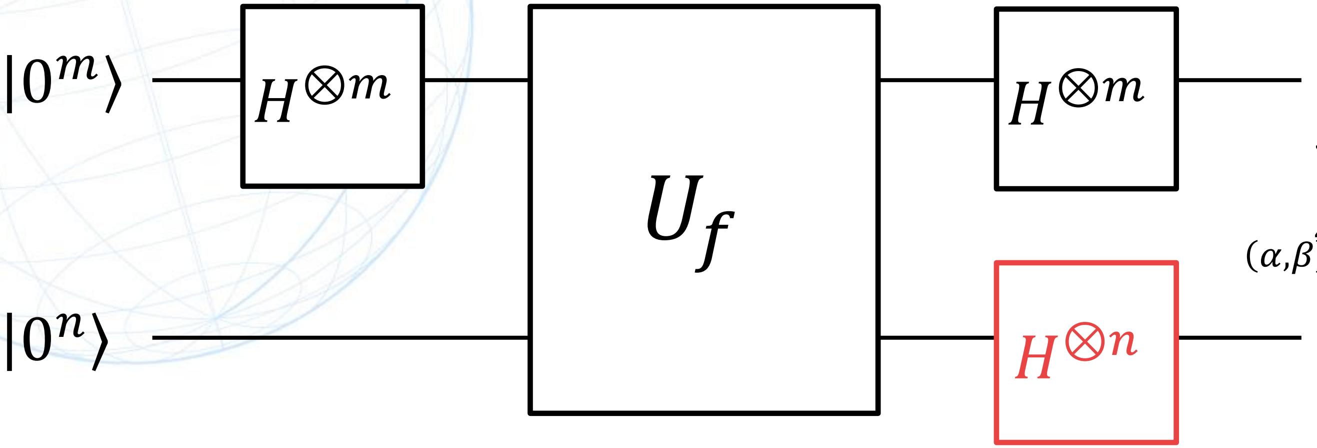
Simon's Subroutine



Simon's Subroutine, Slightly Modified

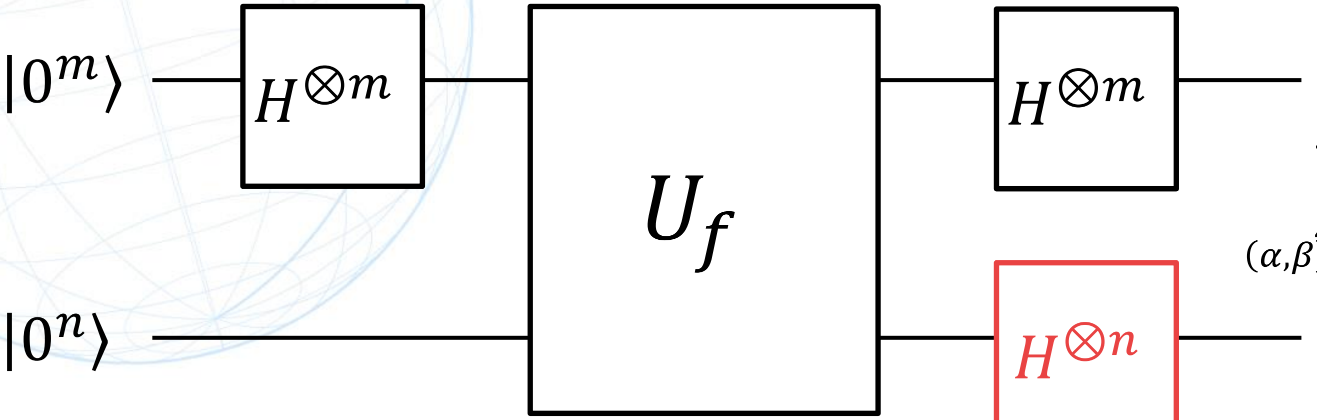


Simon's Subroutine, Slightly Modified



$$\sum_{(\alpha,\beta)\in V-\{0\}} \frac{\mathrm{Cor}(f;\alpha,\beta)^2}{\sqrt{2^n}} |\alpha,\beta\rangle$$

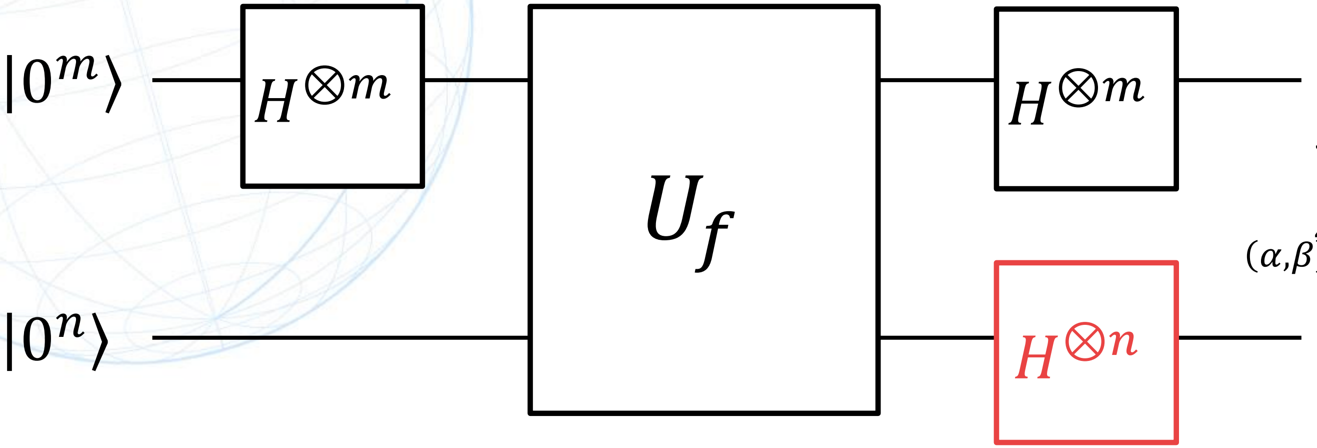
Simon's Subroutine, Slightly Modified



$$\sum_{(\alpha,\beta)\in V-\{0\}} \frac{\mathrm{Cor}(f;\alpha,\beta)^2}{\sqrt{2^n}} |\alpha,\beta\rangle$$

Correlation appears in the amplitudes!

Simon's Subroutine, Slightly Modified



$$\sum_{(\alpha,\beta)\in V-\{0\}} \frac{\mathrm{Cor}(f;\alpha,\beta)^2}{\sqrt{2^n}} |\alpha,\beta\rangle$$

Correlation appears in the amplitudes!

Denote this by CEA^f

(CEA: **C**orrelation **E**xtraction **A**lgorithm)

Quantum Speed-up for Various Distinguishers by CEA and QAA

Application of CEA to Multidim. Linear Distinguishers

- V : Vector space of input-output masks (for multidim. Linear approximation)
  - Assume the capacity of E_K w.r.t. V is large
- F : Boolean function s.t. $F(\alpha,\beta) = 1$ iff $(\alpha,\beta) \in V \setminus \{0\}$

$$\Pr[\,(\alpha,\beta) \leftarrow \text{measure } \mathrm{CEA}^P|0^n\rangle : F(\alpha,\beta) = 1] = \frac{\text{capacity}}{2^n}$$

- If QAA is applied on CEA and F with $\sqrt{2^n/\text{capacity}}$ iterations, $(\alpha,\beta) \in V \setminus \{0\}$ s.t. $F(\alpha,\beta) = 1$ is obtained
  - with high prob. if the given oracle is E_K
  - with low prob. if the given oracle is a random permutation
- E_K is distinguished in time $\approx \sqrt{2^n/\text{capacity}}$

Application of CEA to Multidim. Linear Distinguishers

- If the input-output masks are linearly independent or linearly completely dependent, a better speed-up is obtained by applying some linear transformation on the cipher (oracle)

Linear dependency	Complexity
Completely dependent	$\sqrt{2^{\dim(V)}/\text{capacity}}$
Independent ($V = V_1 \times V_2$)	$\sqrt{2^{\dim(V_2)}/\text{capacity}}$

Quadratic speed-up is obtained in some cases

Application of CEA to Integral and Multidim. Zero Correlation Linear Distinguishers

NTT

- Similar speed-up is obtained in the same way as for multidimensional linear distinguishers

Linear dependency	Complexity
Completely dependent	$\sqrt{2^n}$
Independent ($V = V_1 \times V_2$)	$\sqrt{2^{n-\dim(V_1)}}$

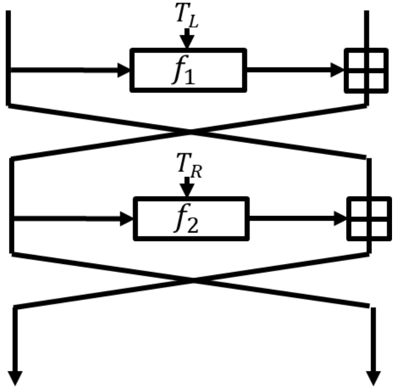
(⇔ integral distinguisher based on balanced functions)

Quadratic speed-up is obtained in some cases

Further Applications

Extension to Generalized Linear Distinguishers

- Linear cryptanalysis assumes basic operations are XORs
- Generalized linear cryptanalysis is used for other operations [Baignères et al. 2007]

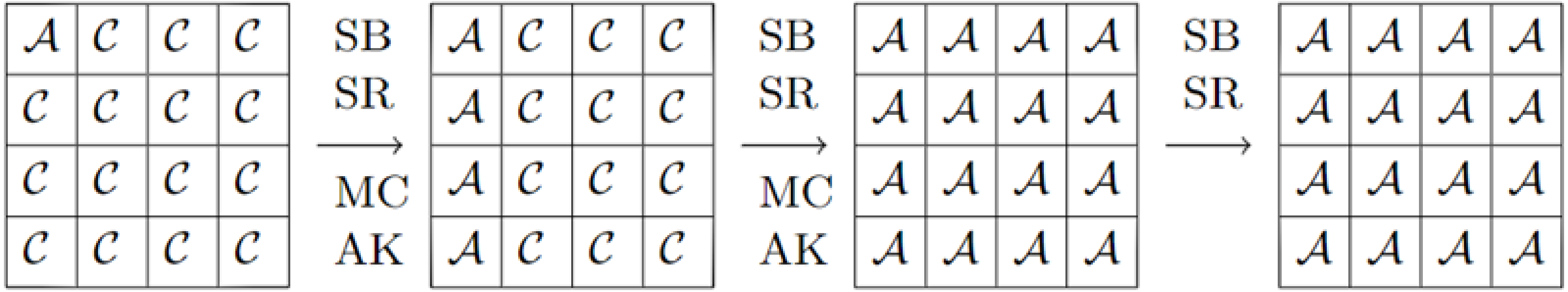


2 rounds of FF3-1 (NIST standard FPE)
[SP800-38G]

- Our technique also generalizes to modular additions by replacing the Hadamard operators in CEA with general quantum Fourier transforms

Possibility of More-than-Quadratic Speed-Up

- Some integral properties yield **multiple** multidimensional zero correlation linear approximations, when CEA leads to a more-than-quadratic speed-up in some cases



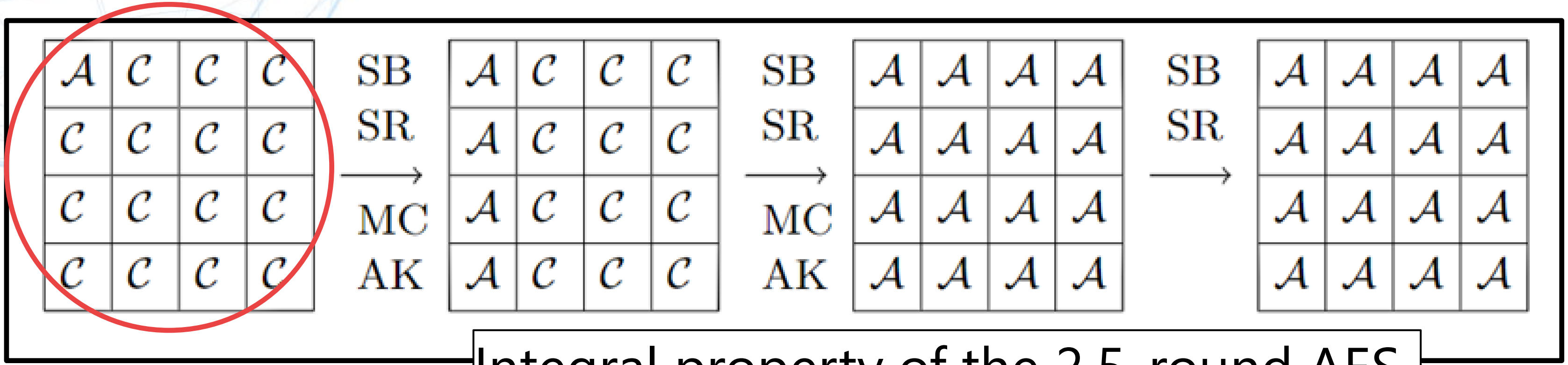
Integral property of the 2.5-round AES

[Daemen & Rijmen 1999]

Possibility of More-than-Quadratic Speed-Up

NTT

- Some integral properties yield **multiple** multidimensional zero correlation linear approximations, when CEA leads to a more-than-quadratic speed-up in some cases



16 choices

Integral property of the 2.5-round AES

[Daemen & Rijmen 1999]

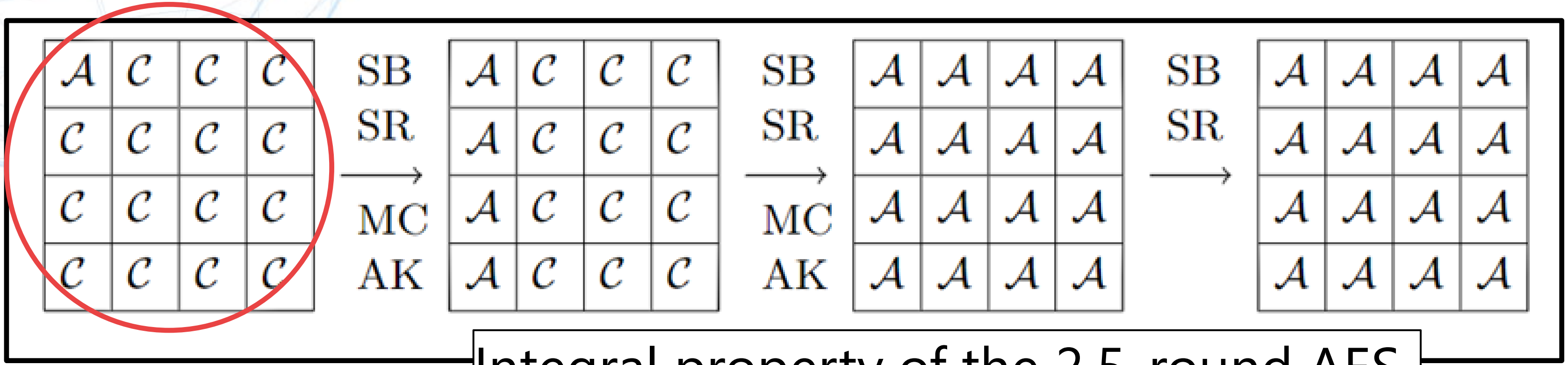
Activating the i-th input cell ⇔ The i-th byte of input mask α is zero

16 multidimenstional approximations exist

Possibility of More-than-Quadratic Speed-Up

NTT

- Some integral properties yield **multiple** multidimensional zero correlation linear approximations, when CEA leads to a more-than-quadratic speed-up in some cases



16 choices

Integral property of the 2.5-round AES

[Daemen & Rijmen 1999]

If a 4-bit cell cipher has the integral property as above, the cipher can be distinguished by **just a single query**

Discussions

Limitations of Our Techniques / Future Works

NTT

- Unclear how to combine our technique with FFT-based key-recovery
  - Classical attacks usually extend distingiushers to key-recovery attacks, often with advanced techniques based on FFT [Collard et al. 2007]
  - Recently Schrottenloher quantumized FFT-based key recovery [Schrottenloher 2023], but the attack is mainly 1-dimensional and the technique is completely different, so it’s unclear how/whether it can be combined with ours
- Inapplicable to integral distinguishers based on zero-sum properties
  - Usually, zero-sum properties lead to breaking more rounds than balanced properties
- Investigating other more-than-quadratic speed-ups?

Summary

Summary

- (At most quadratic) quantum speed-up is obtained for multidimensional (zero correlation) linear distinguishers
- The speed-up is achieved by using a modified version of the subroutine of Simon's algorithm
- The technique can be adapted to generalized linear distinguishers
- If multiple multidimensional linear approximations are available, a more-than-quadratic speed-up is possible in some specific cases
- Further research is needed on how to combine the technique with (FFT-based) key recovery

Thank you!