Efficient Quantum Algorithms Related to Autocorrelation Spectrum

Debajyoti Bera[1] Subhamoy Maitra[2] **Tharrmashastha SAPV**[1]

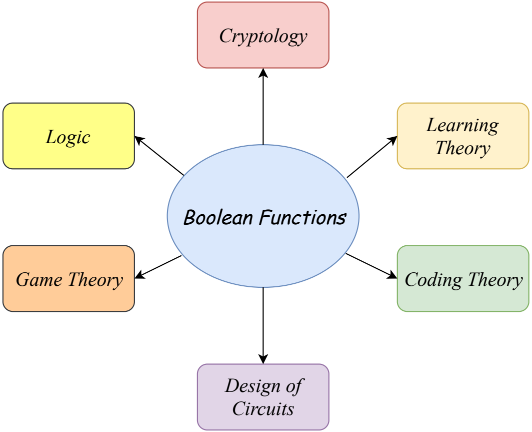
[1]IIIT-D

[2]ISI Calcutta

18 December 2019

The second author would like to acknowledge the support from the project "Cryptography & Cryptanalysis: How far can we bridge the gap between Classical and Quantum paradigm", awarded under DAE-SRC, BRNS, India.

Boolean Functions



Walsh and Autocorrelation Spectrum

Walsh function of a function $f : \{0,1\}^n \longrightarrow \{0,1\}$ is defined as the following function from $\{0,1\}^n$ to $\mathbb{R}[-1,1]$

$$\text{for } y \in \{0,1\}^n, \quad \hat{f}(y) = \frac{1}{2^n} \sum_{x \in \{0,1\}^n} (-1)^{f(x)} (-1)^{x \cdot y}$$

where $x \cdot y$ stands for the $0-1$ valued expression $\oplus_{i=1 \ldots n} x_i y_i$:

Autocorrelation function of the function f is defined as the following transformation from $\{0,1\}^n$ to $\mathbb{R}[-1,1]$.

$$\text{for } a \in \{0,1\}^n, \quad \breve{f}(a) = \frac{1}{2^n} \sum_{x \in \{0,1\}^n} (-1)^{f(x)} (-1)^{f(x \oplus a)}$$

Walsh and Autocorrelation Spectrum

Walsh function of a function $f : \{0,1\}^n \longrightarrow \{0,1\}$ is defined as the following function from $\{0,1\}^n$ to $\mathbb{R}[-1,1]$

$$\text{for } y \in \{0,1\}^n, \quad \hat{f}(y) = \frac{1}{2^n} \sum_{x \in \{0,1\}^n} (-1)^{f(x)} (-1)^{x \cdot y}$$

where $x \cdot y$ stands for the $0-1$ valued expression $\oplus_{i=1\ldots n} x_i y_i$:

Autocorrelation function of the function f is defined as the following transformation from $\{0,1\}^n$ to $\mathbb{R}[-1,1]$.

$$\text{for } a \in \{0,1\}^n, \quad \breve{f}(a) = \frac{1}{2^n} \sum_{x \in \{0,1\}^n} (-1)^{f(x)} (-1)^{f(x \oplus a)}$$

Walsh and Autocorrelation Spectrum

- Shannon in his paper[1] related Walsh spectra and Autocorrelation spectra to **confusion** and **diffusion** of cryptosystems respectively.
- Boolean functions with low absolute Walsh sprectral values resist linear cryptanalysis.
- Boolean function with low absolute autocorrelation values resist differential cryptanalysis.

[1] Shannon, C. E. (1948). A mathematical theory of communication. Bell system technical journal, 27(3), 379-423.

Walsh and Autocorrelation Spectrum

- Shannon in his paper[1] related Walsh spectra and Autocorrelation spectra to **confusion** and **diffusion** of cryptosystems respectively.
- Boolean functions with low absolute Walsh spectral values resist linear cryptanalysis.
- Boolean function with low absolute autocorrelation values resist differential cryptanalysis.

[1] Shannon, C. E. (1948). A mathematical theory of communication. Bell system technical journal, 27(3), 379-423.

Walsh and Autocorrelation Spectrum

- Shannon in his paper[1] related Walsh spectra and Autocorrelation spectra to **confusion** and **diffusion** of cryptosystems respectively.
- Boolean functions with low absolute Walsh spectral values resist linear cryptanalysis.
- Boolean function with low absolute autocorrelation values resist differential cryptanalysis.

[1] Shannon, C. E. (1948). A mathematical theory of communication. Bell system technical journal, 27(3), 379-423.

Quantum in a Page

- Qubits are the quantum version of classical bits. E.g., $|0\rangle, |1\rangle$.
- A quantum state is a configuration of the qubits. It is denoted by a ket $|\cdot\rangle$.
- A fundamental principle in quantum computing is superposition.

$$|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle.$$

- The squares of the amplitudes add up to one. Normalization is very important in a quantum state.
- Oracles are quantum black-boxes and are denoted by U_f. They act as

$$U_f|x\rangle|a\rangle \longrightarrow |x\rangle|a \oplus f(x)\rangle.$$

Quantum in a Page

- Qubits are the quantum version of classical bits. E.g., $|0\rangle, |1\rangle$.
- A quantum state is a configuration of the qubits. It is denoted by a ket $|\cdot\rangle$.
- A fundamental principle in quantum computing is superposition.

$$|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle.$$

- The squares of the amplitudes add up to one. Normalization is very important in a quantum state.
- Oracles are quantum black-boxes and are denoted by U_f. They act as

$$U_f |x\rangle |a\rangle \longrightarrow |x\rangle |a \oplus f(x)\rangle.$$

Quantum in a Page

- Qubits are the quantum version of classical bits. E.g., $|0\rangle, |1\rangle$.
- A quantum state is a configuration of the qubits. It is denoted by a ket $|\cdot\rangle$.
- A fundamental principle in quantum computing is superposition.

$$|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle.$$

- The squares of the amplitudes add up to one. Normalization is very important in a quantum state.
- Oracles are quantum black-boxes and are denoted by U_f. They act as

$$U_f |x\rangle |a\rangle \longrightarrow |x\rangle |a \oplus f(x)\rangle.$$

Quantum in a Page

- Qubits are the quantum version of classical bits. E.g., $|0\rangle, |1\rangle$.
- A quantum state is a configuration of the qubits. It is denoted by a ket $|\cdot\rangle$.
- A fundamental principle in quantum computing is superposition.

$$|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle.$$

- The squares of the amplitudes add up to one. Normalization is very important in a quantum state.
- Oracles are quantum black-boxes and are denoted by U_f. They act as

$$U_f|x\rangle|a\rangle \longrightarrow |x\rangle|a \oplus f(x)\rangle.$$

Quantum in a Page

- Qubits are the quantum version of classical bits. E.g., $|0\rangle, |1\rangle$.
- A quantum state is a configuration of the qubits. It is denoted by a ket $|\cdot\rangle$.
- A fundamental principle in quantum computing is superposition.

$$|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle.$$

- The squares of the amplitudes add up to one. Normalization is very important in a quantum state.
- Oracles are quantum black-boxes and are denoted by U_f. They act as

$$U_f |x\rangle |a\rangle \longrightarrow |x\rangle |a \oplus f(x)\rangle.$$

Quantum Algorithm for Walsh Spectrum

- Due to Parseval's identity which is
$$\sum_{x \in \{0,1\}^n} \left(\hat{f}(x)\right)^2 = 1,$$
it was easy to design a quantum algorithm for the Walsh sepctrum.
- It was indeed readily available as Deutsch-Jozsa algorithm.

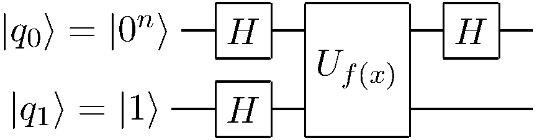
Quantum Algorithm for Walsh Spectrum

- Due to Parseval's identity which is

$$\sum_{x \in \{0,1\}^n} \left(\hat{f}(x)\right)^2 = 1,$$

  it was easy to design a quantum algorithm for the Walsh sepctrum.
- It was indeed readily available as Deutsch-Jozsa algorithm.

Quantum Algorithm for Walsh Spectrum

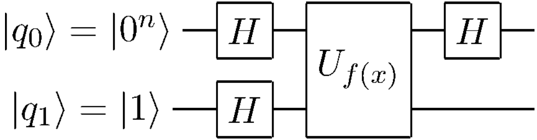


- The state of the system post the gate operations is given by

$$|\psi\rangle = \frac{1}{2^n} \sum_{y \in \{0,1\}^n} \left[\sum_{x \in \{0,1\}^n} (-1)^{f(x) \oplus x \cdot y} \right] |y\rangle |-\rangle = \sum_{y \in \{0,1\}^n} \hat{f}(y) |y\rangle |-\rangle$$

- So, on sampling a constant number of times and with linear number of gates, we can obtain points with high Walsh coefficient value.

Quantum Algorithm for Walsh Spectrum

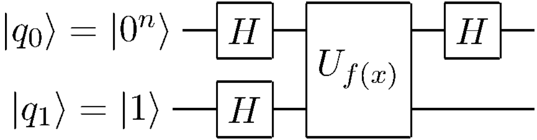


- The state of the system post the gate operations is given by

$$|\psi\rangle = \frac{1}{2^n} \sum_{y \in \{0,1\}^n} \left[\sum_{x \in \{0,1\}^n} (-1)^{f(x) \oplus x \cdot y} \right] |y\rangle \, |-\rangle = \sum_{y \in \{0,1\}^n} \hat{f}(y) \, |y\rangle \, |-\rangle$$

- So, on sampling a constant number of times and with linear number of gates, we can obtain points with high Walsh coefficient value.

Quantum Algorithm for Walsh Spectrum



- The state of the system post the gate operations is given by

$$|\psi\rangle = \frac{1}{2^n} \sum_{y \in \{0,1\}^n} \left[\sum_{x \in \{0,1\}^n} (-1)^{f(x) \oplus x \cdot y} \right] |y\rangle \, |-\rangle = \sum_{y \in \{0,1\}^n} \hat{f}(y) \, |y\rangle \, |-\rangle$$

- So, on sampling a constant number of times and with linear number of gates, we can obtain points with high Walsh coefficient value.

Problem with Autcorrelation Spectrum

- However, there was no study on quantum algorithms for Autocorrelation spectrum.
- This was due to the fact that

$$\sum_a \breve{f}(a)^2 \in [1, 2^n].$$

- Unlike Deutsch-Jozsa algorithm, it appears that obtaining a quantum algorithm as an immediate corollary would be difficult.

Problem with Autcorrelation Spectrum

- However, there was no study on quantum algorithms for Autocorrelation spectrum.
- This was due to the fact that

$$\sum_a \breve{f}(a)^2 \in [1, 2^n].$$

- Unlike Deutsch-Jozsa algorithm, it appears that obtaining a quantum algorithm as an immediate corollary would be difficult.

Problem with Autcorrelation Spectrum

- However, there was no study on quantum algorithms for Autocorrelation spectrum.
- This was due to the fact that
$$\sum_a \breve{f}(a)^2 \in [1, 2^n].$$
- Unlike Deutsch-Jozsa algorithm, it appears that obtaining a quantum algorithm as an immediate corollary would be difficult.

Preliminaries: Sum of Squares

The sum-of-squares indicator for the characteristic of f is defined as

$$\sigma_f = \sum_{a \in \mathbb{F}_2^n} \breve{f}(a)^2$$

- In particular, $\sigma_f = 1$ if f is a Bent function and $\sigma_f = 2^n$ if f is a linear function.
- A small σ_f indicates that a function satisfies the *global avalanche criteria* (GAC).

Preliminaries: Sum of Squares

The sum-of-squares indicator for the characteristic of f is defined as

$$\sigma_f = \sum_{a \in \mathbb{F}_2^n} \breve{f}(a)^2$$

- In particular, $\sigma_f = 1$ if f is a Bent function and $\sigma_f = 2^n$ if f is a linear function.
- A small σ_f indicates that a function satisfies the *global avalanche criteria* (GAC).

Preliminaries: Sum of Squares

The sum-of-squares indicator for the characteristic of f is defined as

$$\sigma_f = \sum_{a \in \mathbb{F}_2^n} \breve{f}(a)^2$$

- In particular, $\sigma_f = 1$ if f is a Bent function and $\sigma_f = 2^n$ if f is a linear function.
- A small σ_f indicates that a function satisfies the *global avalanche criteria* (GAC).

Preliminaries: Derivative of a Boolean Function

- Given a point $a \in \{0,1\}^n$, the (first-order) derivative of an n-bit function f *at* a is defined as

$$\Delta f_a(x) = f(x \oplus a) \oplus f(x)$$

- For a list of points $\mathcal{A} = (a_1, a_2, \ldots, a_k)$ (where $k \leq n$) the k-th derivative of f at $(a_1, a_2, \ldots, a_k)$ is recursively defined as

$$\Delta f_{\mathcal{A}}^{(k)}(x) = \Delta f_{a_k}(\Delta f_{a_1,a_2,\ldots,a_{k-1}}^{(k-1)}(x)),$$

where $\Delta f_{a_1,a_2,\ldots,a_{k-1}}^{(k-1)}(x)$ is the $(k-1)$-th derivative of f at points $(a_1, a_2, \ldots, a_{k-1})$.

Preliminaries: Derivative of a Boolean Function

- Given a point $a \in \{0,1\}^n$, the (first-order) derivative of an n-bit function f *at* a is defined as

$$\Delta f_a(x) = f(x \oplus a) \oplus f(x)$$

- For a list of points $\mathcal{A} = (a_1, a_2, \ldots, a_k)$ (where $k \leq n$) the k-th derivative of f at $(a_1, a_2, \ldots, a_k)$ is recursively defined as

$$\Delta f_{\mathcal{A}}^{(k)}(x) = \Delta f_{a_k}(\Delta f_{a_1,a_2,\ldots,a_{k-1}}^{(k-1)}(x)),$$

where $\Delta f_{a_1,a_2,\ldots,a_{k-1}}^{(k-1)}(x)$ is the $(k-1)$-th derivative of f at points $(a_1, a_2, \ldots, a_{k-1})$.

Preliminaries: Derivative of a Boolean Function

The i-th derivative of f at $\mathcal{A} = (a_1, a_2, \dots a_i)$ can be shown[2] to be

$$\Delta f_{\mathcal{A}}^{(i)}(x) = \bigoplus_{S \subseteq A} f(x \oplus S)$$

where $X_s = \bigoplus_{a \in S} a$, $f(x \oplus S) = f(x \oplus X_s)$ and $S \subseteq A$ indicates all possible sub-lists of $\mathcal{A}$ (including duplicates, if any, in $\mathcal{A}$).

[2] The proof is present in Xuejia Lai. Higher Order Derivatives and Differential Cryptanalysis. Springer US, 1994.

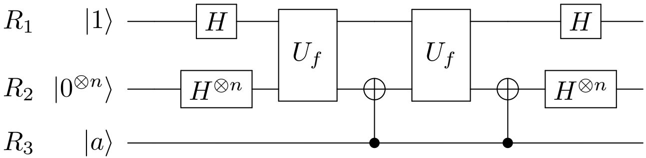
Preliminaries: Derivative of a Boolean Function

- Higher-order derivatives form the basis of many cryptographic attacks, especially those that generalize the differential attack technique against block ciphers such as Integral attack, AIDA, cube attack, zero-sum distinguisher, etc.
- If the non-trivial i^{th} derivatives of the function are constant for small i, then we can use that fact to mount attacks on the cryptosystem.

Preliminaries: Derivative of a Boolean Function

- Higher-order derivatives form the basis of many cryptographic attacks, especially those that generalize the differential attack technique against block ciphers such as Integral attack, AIDA, cube attack, zero-sum distinguisher, etc.
- If the non-trivial i^{th} derivatives of the function are constant for small i, then we can use that fact to mount attacks on the cryptosystem.

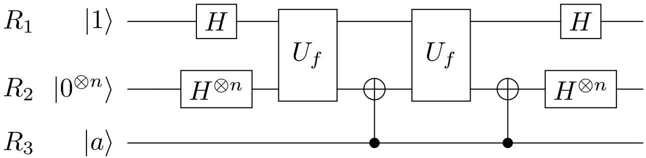
Quantum Algorithm for Walsh-Hadamard 1^{st} Derivative Sampling



The final state of this circuit is given as

$$|\psi\rangle = |1\rangle \sum_y \left[\frac{1}{2^n}\sum_x (-1)^{(x\cdot y)}(-1)^{f(x)\oplus f(x\oplus a)}\right]|y\rangle\,|a\rangle$$
$$= |1\rangle \sum_y \widehat{\Delta f_a}(y)\,|y\rangle\,|a\rangle$$

Quantum Algorithm for Walsh-Hadamard 1^{st} Derivative Sampling



The final state of this circuit is given as

$$
\begin{aligned}
|\psi\rangle &= |1\rangle \sum_{y} \left[\frac{1}{2^n} \sum_{x} (-1)^{(x\cdot y)} (-1)^{f(x)\oplus f(x\oplus a)}\right] |y\rangle\, |a\rangle \\
&= |1\rangle \sum_{y} \widehat{\Delta f_a}(y)\, |y\rangle\, |a\rangle
\end{aligned}
$$

Autocorrelation Sampling

Lemma

$\breve{f}(a) = \widehat{\Delta f_a^{(1)}}(0^n)$

Proof.

LHS is equal to $\frac{1}{2^n}\sum_x (-1)^{f(x)}(-1)^{f(x\oplus a)} = \frac{1}{2^n}\sum_x \Delta f_a^{(1)}(x)$. Now observe that $\widehat{\Delta f_a^{(1)}}(0^n) = \frac{1}{2^n}\sum_x \Delta f_a^{(1)}(x)$ and this proves the lemma. □ □

Quantum Algorithm for Autocorrelation Sampling

1: Start with three registers initialized as $|1\rangle$, $|0^n\rangle$, and $|0^n\rangle$.

2: Apply H^n to R_3 to generate the state $\frac{1}{\sqrt{2^n}} \sum_{b \in \mathbb{F}_2^n} |1\rangle |0^n\rangle |b\rangle$.

3: Apply $HoDJ_n^1$ on the registers R_1, R_2 and R_3 to generate the state

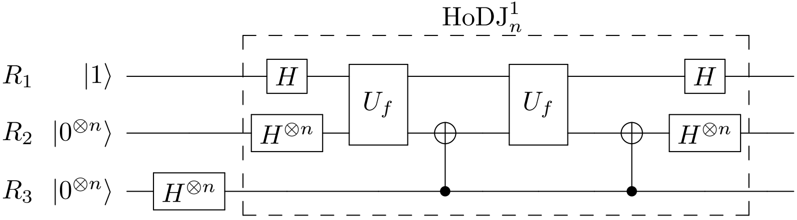
$$|\Phi\rangle = \frac{1}{\sqrt{2^n}} |1\rangle \sum_{b \in \mathbb{F}_2^n} \sum_{y \in \mathbb{F}_2^n} \widehat{\Delta f_b^{(1)}}(y) |y\rangle |b\rangle.$$

4: Apply fixed-point amplitude amplification[3] on $|\Phi\rangle$ to amplify the probability of observing R_2 in the state $|0\rangle$ to $1 - \delta$ for any given constant δ

5: Measure R_3 in the standard basis and return the observed outcome

[3] Theodore J. Yoder, Guang Hao Low, and Isaac L. Chuang. Fixed-point quantum search with an optimal number of queries. Phys. Rev. Lett., 113:210501, Nov 2014.

Quantum Algorithm for Autocorrelation Sampling



The final state of the circuit is given as

$$|\psi\rangle = |1\rangle \otimes |0^n\rangle \otimes \left(\frac{1}{\sqrt{2^n}} \sum_b \breve{f}(b) |b\rangle\right) + \sum_y |1\rangle |y\rangle \otimes \left(\frac{1}{\sqrt{2^n}} \sum_b \widehat{\Delta f_b}(y) |b\rangle\right)$$

Quantum Algorithm for Autocorrelation Sampling

Theorem

The observed outcome returned by the above algorithm is a random sample from the distribution $\{\breve{f}(a)^2/\sigma_f\}_{a\in\mathbb{F}_2^n}$ *with probability at least* $1-\delta$. *The algorithm makes* $O(\frac{2^{n/2}}{\sqrt{\sigma_f}}\log\frac{2}{\delta})$ *queries to* U_f *and uses* $O(n\frac{2^{n/2}}{\sqrt{\sigma_f}}\log\frac{2}{\delta})$ *gates altogether.*

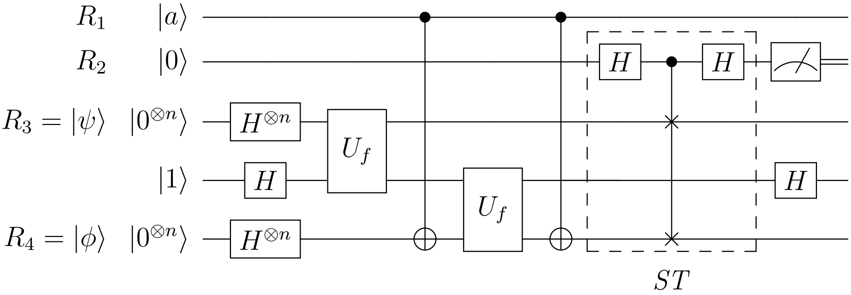
Classical Autocorrelation Estimation at a point a

- Observe that $\breve{f}(a) = \frac{1}{2^n}\sum_x (-1)^{f(x)}(-1)^{f(x \oplus a)} = \mathbb{E}_x[X_x]$ where the ± 1-valued random variable $X_x = (-1)^{f(x) \oplus f(x \oplus a)}$ is defined for x chosen uniformly at random from $\{0,1\}^n$.
- The number of samples needed if we were to classically estimate $\breve{f}(a)$ with accuracy ϵ and error δ is $O(\frac{1}{\epsilon^2} \log \frac{1}{\delta})$.

Classical Autocorrelation Estimation at a point a

- Observe that $\breve{f}(a) = \frac{1}{2^n}\sum_x (-1)^{f(x)}(-1)^{f(x\oplus a)} = \mathbb{E}_x[X_x]$ where the ±1-valued random variable $X_x = (-1)^{f(x)\oplus f(x\oplus a)}$ is defined for x chosen uniformly at random from $\{0,1\}^n$.
- The number of samples needed if we were to classically estimate $\breve{f}(a)$ with accuracy ϵ and error δ is $O(\frac{1}{\epsilon^2}\log\frac{1}{\delta})$.

Quantum Autocorrelation Estimation at a point a



Quantum Autocorrelation Estimation at a point a I

Require: Parameters: ϵ (confidence), δ (error)

1: Start with four registers of which R_1 is initialized to $|a\rangle$, R_2 to $|0\rangle$, and R_3, R_4 to $|0^n\rangle$.

2: Apply these transformations.

$$|a\rangle |0\rangle |0^n\rangle |0^n\rangle$$

$$\xrightarrow{H^n \otimes H^n} |a\rangle |0\rangle \left(\frac{1}{\sqrt{2^n}} \sum_x |x\rangle \right) \left(\frac{1}{\sqrt{2^n}} \sum_y |y\rangle \right)$$

$$\xrightarrow{CNOT} |a\rangle |0\rangle \left(\frac{1}{\sqrt{2^n}} \sum_x |x\rangle \right) \left(\frac{1}{\sqrt{2^n}} \sum_y |y \oplus a\rangle \right)$$

$$\xrightarrow{U_f \otimes U_f} |a\rangle |0\rangle \left(\frac{1}{\sqrt{2^n}} \sum_x (-1)^{f(x)} |x\rangle \right) \left(\frac{1}{\sqrt{2^n}} \sum_y (-1)^{f(y \oplus a)} |y \oplus a\rangle \right)$$

▷ Uses reusable $|-\rangle$

$$\xrightarrow{CNOT} |a\rangle |0\rangle \left(\frac{1}{\sqrt{2^n}} \sum_x (-1)^{f(x)} |x\rangle \right) \left(\frac{1}{\sqrt{2^n}} \sum_y (-1)^{f(y \oplus a)} |y\rangle \right)$$

Quantum Autocorrelation Estimation at a point a II

$= |a\rangle |0\rangle |\psi\rangle |\phi_a\rangle$

- Normalized state $\frac{1}{\sqrt{2^n}} \sum_x (-1)^{f(x)} |x\rangle$ denoted ψ
- Normalized state $\frac{1}{\sqrt{2^n}} \sum_y (-1)^{f(y \oplus a)} |y\rangle$ denoted ϕ_a

3: Apply ST on R_2, R_3 and R_4 to obtain

$$|a\rangle \Big[|0\rangle \otimes \frac{1}{2}\big(|\psi\rangle |\phi_a\rangle + |\phi_a\rangle |\psi\rangle \big) + |1\rangle \otimes \frac{1}{2}\big(|\psi\rangle |\phi_a\rangle - |\phi_a\rangle |\psi\rangle \big) \Big]$$

4: $\ell \leftarrow$ estimate the probability of observing R_2 in the state $|0\rangle$ with accuracy $\pm\frac{\epsilon}{2}$ and error δ

5: Return $2\ell - 1$ as the estimate of $|\breve{f}(a)|^2$

Quantum Autocorrelation Estimation at a point a

Theorem

The QAE algorithm makes $\Theta\left(\frac{\pi}{\epsilon}\log\frac{1}{\delta}\right)$ *calls to* U_f *and returns an estimate* α *such that*

$$\Pr\left[\alpha - \epsilon \leq \breve{f}(a)^2 \leq \alpha + \epsilon\right] \geq 1 - \delta$$

Estimation of Sum-of-Squares Indicator

- The sum of squares indicator is given as

$$\sigma_f = \sum_{a \in \mathbb{F}_2^n} \breve{f}(a)^2$$

.

- Note that $1 \leq \sigma_f \leq 2^n$.
- Objective is to obtain an estimate of σ_f with ϵ accuracy and δ probability of error.

Estimation of Sum-of-Squares Indicator

- The sum of squares indicator is given as

$$\sigma_f = \sum_{a \in \mathbb{F}_2^n} \breve{f}(a)^2$$

.

- Note that $1 \leq \sigma_f \leq 2^n$.
- Objective is to obtain an estimate of σ_f with ϵ accuracy and δ probability of error.

Estimation of Sum-of-Squares Indicator

- The sum of squares indicator is given as

$$\sigma_f = \sum_{a \in \mathbb{F}_2^n} \breve{f}(a)^2$$

.

- Note that $1 \leq \sigma_f \leq 2^n$.
- Objective is to obtain an estimate of σ_f with ϵ accuracy and δ probability of error.

Classical Estimation of Sum-of-Squares Indicator

Let a, b, c be three random variables chosen uniformly at random from $\mathbb{F}_2^n$ such that $b \neq c$ and let $X_{a,b,c}$ be the ± 1-valued random variable $(-1)^{f(a\oplus b)}(-1)^{f(a\oplus c)}$. Then,

$$\begin{aligned}\sigma_f &= \sum_{a\in\mathbb{F}_2^n} \breve{f}(a)^2 = \sum_{a\in\mathbb{F}_2^n}\left[\frac{1}{2^n}\sum_{b\in\mathbb{F}_2^n}(-1)^{f(b)\oplus f(b\oplus a)}\right]^2 \\ &= \frac{1}{2^{2n}}\sum_{a\in\mathbb{F}_2^n}\left[2^n + \sum_{\substack{b\neq c\\ b,c\in\mathbb{F}_2^n}}(-1)^{f(a\oplus b)\oplus f(a\oplus c)}\right] \\ &= 1 + \frac{1}{2^{2n}}\sum_{\substack{a\in\mathbb{F}_2^n\\ b\neq c}}(-1)^{f(a\oplus b)\oplus f(a\oplus c)} \\ &= 1 + (2^n - 1)\mathbb{E}_{a,b,c}[X_{a,b,c}]\end{aligned}$$

Classical Estimation of Sum-of-Squares Indicator

Let a, b, c be three random variables chosen uniformly at random from $\mathbb{F}_2^n$ such that $b \neq c$ and let $X_{a,b,c}$ be the ± 1-valued random variable $(-1)^{f(a\oplus b)}(-1)^{f(a\oplus c)}$. Then,

$$\begin{aligned}
\sigma_f &= \sum_{a\in\mathbb{F}_2^n} \breve{f}(a)^2 = \sum_{a\in\mathbb{F}_2^n} \left[\frac{1}{2^n}\sum_{b\in\mathbb{F}_2^n}(-1)^{f(b)\oplus f(b\oplus a)}\right]^2 \\
&= \frac{1}{2^{2n}}\sum_{a\in\mathbb{F}_2^n}\left[2^n + \sum_{\substack{b\neq c\\ b,c\in\mathbb{F}_2^n}}(-1)^{f(a\oplus b)\oplus f(a\oplus c)}\right] \\
&= 1 + \frac{1}{2^{2n}}\sum_{\substack{a\in\mathbb{F}_2^n\\ b\neq c}}(-1)^{f(a\oplus b)\oplus f(a\oplus c)} \\
&= 1 + (2^n - 1)\mathbb{E}_{a,b,c}[X_{a,b,c}]
\end{aligned}$$

Classical Estimation of Sum-of-Squares Indicator

- We estimate $\mathbb{E}[X_{a,b,c}]$ using multiple independent samples of a, b, c.
- Note that $\mathbb{E}[X_{a,b,c}] = \frac{\sigma_f - 1}{2^n - 1} \approx \frac{\sigma_f}{2^n}$.
- We can estimate $\mathbb{E}[X_{a,b,c}]$ with ϵ' accuracy and δ error in $O(\frac{1}{\epsilon'^2} \log \frac{1}{\delta})$ calls to $f()$.
- To estimate σ_f with accuracy ϵ, we set $\epsilon' = \frac{\epsilon}{2^n - 1} \approx \frac{\epsilon}{2^n}$.
- Hence, the number of calls to $f()$ would be $O(\frac{2^{2n}}{\epsilon^2} \log \frac{1}{\delta})$.

Classical Estimation of Sum-of-Squares Indicator

- We estimate $\mathbb{E}[X_{a,b,c}]$ using multiple independent samples of a, b, c.
- Note that $\mathbb{E}[X_{a,b,c}] = \frac{\sigma_f - 1}{2^n - 1} \approx \frac{\sigma_f}{2^n}$.
- We can estimate $\mathbb{E}[X_{a,b,c}]$ with ϵ' accuracy and δ error in $O(\frac{1}{\epsilon'^2} \log \frac{1}{\delta})$ calls to $f()$.
- To estimate σ_f with accuracy ϵ, we set $\epsilon' = \frac{\epsilon}{2^n - 1} \approx \frac{\epsilon}{2^n}$.
- Hence, the number of calls to $f()$ would be $O(\frac{2^{2n}}{\epsilon^2} \log \frac{1}{\delta})$.

Classical Estimation of Sum-of-Squares Indicator

- We estimate $\mathbb{E}[X_{a,b,c}]$ using multiple independent samples of a, b, c.
- Note that $\mathbb{E}[X_{a,b,c}] = \frac{\sigma_f - 1}{2^n - 1} \approx \frac{\sigma_f}{2^n}$.
- We can estimate $\mathbb{E}[X_{a,b,c}]$ with ϵ' accuracy and δ error in $O(\frac{1}{\epsilon'^2} \log \frac{1}{\delta})$ calls to $f()$.
- To estimate σ_f with accuracy ϵ, we set $\epsilon' = \frac{\epsilon}{2^n - 1} \approx \frac{\epsilon}{2^n}$.
- Hence, the number of calls to $f()$ would be $O(\frac{2^{2n}}{\epsilon^2} \log \frac{1}{\delta})$.

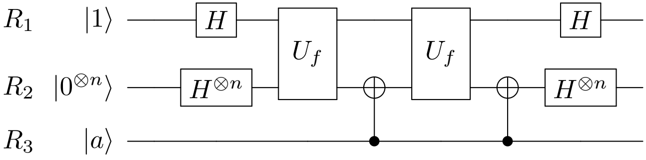
Classical Estimation of Sum-of-Squares Indicator

- We estimate $\mathbb{E}[X_{a,b,c}]$ using multiple independent samples of a, b, c.
- Note that $\mathbb{E}[X_{a,b,c}] = \frac{\sigma_f - 1}{2^n - 1} \approx \frac{\sigma_f}{2^n}$.
- We can estimate $\mathbb{E}[X_{a,b,c}]$ with ϵ' accuracy and δ error in $O(\frac{1}{\epsilon'^2} \log \frac{1}{\delta})$ calls to $f()$.
- To estimate σ_f with accuracy ϵ, we set $\epsilon' = \frac{\epsilon}{2^n - 1} \approx \frac{\epsilon}{2^n}$.
- Hence, the number of calls to $f()$ would be $O(\frac{2^{2n}}{\epsilon^2} \log \frac{1}{\delta})$.

Classical Estimation of Sum-of-Squares Indicator

- We estimate $\mathbb{E}[X_{a,b,c}]$ using multiple independent samples of a, b, c.
- Note that $\mathbb{E}[X_{a,b,c}] = \frac{\sigma_f - 1}{2^n - 1} \approx \frac{\sigma_f}{2^n}$.
- We can estimate $\mathbb{E}[X_{a,b,c}]$ with ϵ' accuracy and δ error in $O(\frac{1}{\epsilon'^2} \log \frac{1}{\delta})$ calls to $f()$.
- To estimate σ_f with accuracy ϵ, we set $\epsilon' = \frac{\epsilon}{2^n - 1} \approx \frac{\epsilon}{2^n}$.
- Hence, the number of calls to $f()$ would be $O(\frac{2^{2n}}{\epsilon^2} \log \frac{1}{\delta})$.

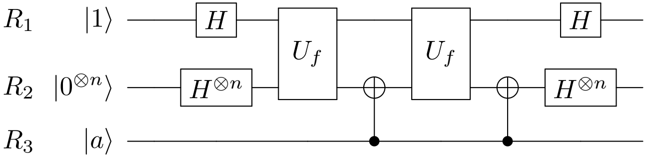
Quantum Estimation of Sum-of-Squares Indicator



- Remember that the final state of this circuit is
$$|\psi\rangle = |1\rangle \otimes |0^n\rangle \otimes \left(\frac{1}{\sqrt{2^n}} \sum_b \check{f}(b)\,|b\rangle\right) + \sum_y |1\rangle\,|y\rangle \otimes \left(\frac{1}{\sqrt{2^n}} \sum_b \widehat{\Delta f_b}(y)\,|b\rangle\right).$$

- Since the probability of observing the output $|0^{\otimes n}\rangle$ in R_2 is $\sigma_f/2^n$, we ca estimate σ_f with an accuracy ϵ and error δ in $\Theta\left(\frac{2^n}{\epsilon}\log\frac{1}{\delta}\right)$ calls to U_f.

Quantum Estimation of Sum-of-Squares Indicator



- Remember that the final state of this circuit is
$$|\psi\rangle = |1\rangle \otimes |0^n\rangle \otimes \left(\frac{1}{\sqrt{2^n}} \sum_b \check{f}(b) |b\rangle \right) + \sum_y |1\rangle |y\rangle \otimes \left(\frac{1}{\sqrt{2^n}} \sum_b \widehat{\Delta f_b}(y) |b\rangle \right).$$

- Since the probability of observing the output $|0^{\otimes n}\rangle$ in R_2 is $\sigma_f / 2^n$, we ca estimate σ_f with an accuracy ϵ and error δ in $\Theta\left(\frac{2^n}{\epsilon} \log \frac{1}{\delta}\right)$ calls to U_f.

Conclusion

- Autocorrelation is an important tool in constructing Boolean functions with good cryptographic properties and in performing differential attacks.
- We presented an extension of Deutsch-Jozsa algorithm that can be used to sample the Walsh spectrum of any higher order derivatives.
- We presented an algorithm to sample according to the distribution of normalized autocorrelation spectral values.
- We presented techniques to estimate the autocorrelation coefficient value at a point a and to estimate the Sum-of-Squares indicator of any given Boolean function.

Thank you for your attention! Any questions?

Hope you slept comfortably!