



Improved Linear Cryptanalysis on Quantum Computers

Verteidigung Masterarbeit

Hannes Hattenbach
Freie Universität Berlin

22. Februar 2024

Inhaltsübersicht

Einordnung

- Vorkenntnisse

 - Lineare Kryptoanalyse

 - Quantum Computing

- Bestehende Ansätze

- Problematik

Analytische Untersuchung des Malviya-Algorithmus

- Ausgabewahrscheinlichkeit

- Triviale Approximation

- Erfolgswahrscheinlichkeit

Erweiterter Algorithmus

- Amplitudenverstärkung

- + Malviya-Algorithmus

Das Orakel

Fazit

Outline

Einordnung

Vorkenntnisse

Lineare Kryptoanalyse

Quantum Computing

Bestehende Ansätze

Problematik

Analytische Untersuchung des Malviya-Algorithmus

Ausgabewahrscheinlichkeit

Triviale Approximation

Erfolgswahrscheinlichkeit

Erweiterter Algorithmus

Amplitudenverstärkung

+ Malviya-Algorithmus

Das Orakel

Fazit

Bitweise Schlüssel-Extraktion aus Chiffre-Text-Paaren durch Mehrheitsentscheidung¹

Sei $f : \mathbb{F}_2^{n_m} \times \mathbb{F}_2^{n_k} \rightarrow \mathbb{F}_2^{n_c}$ eine (Boolsche) Verschlüsselungsfunktion mit $f(m, k) = c$

Finde $\alpha, \beta, \gamma \in \mathbb{F}_2^{n_{(m,c,k)}}$; ($b \in \mathbb{F}_2$), sodass

$$(m \bullet \alpha) \oplus (k \bullet \gamma) \oplus (f(m, k) \bullet \beta) \approx b$$

2^{3n} Möglichkeiten \rightarrow generell schwer

¹vgl. [Mat93, Algorithmus 1]

Daten

- ▶ **Qubit** $|\psi\rangle_1 \in \mathbb{C}^2 = \alpha_0 |0\rangle + \alpha_1 |1\rangle$ mit $|\alpha_0|^2 + |\alpha_1|^2 = 1$
 - ▶ Basiszustände $|0\rangle = (1, 0)^t$ und $|1\rangle = (0, 1)^t$
- ▶ **Quanten-Register** aus n Qubits $|\psi\rangle_n \in \mathbb{C}^{2^n} = \sum_{i=0}^{2^n-1} \alpha_i |i\rangle$ mit $\sum_{i=0}^{2^n-1} |\alpha_i|^2 = 1$

Operationen

- ▶ **Unitäre Matrix** $U : \mathbb{C}^{2^n} \rightarrow \mathbb{C}^{2^n}$ mit $UU^\dagger = I$
- ▶ Entweder: Zusammengesetzt (\otimes und \cdot) aus lokalen **Gates**
- ▶ Oder: Black-Box **Orakel** $O|\psi_t\rangle \mapsto |\psi_{t+1}\rangle$

Ausgabe

- ▶ **Messung** hier: $|\psi\rangle = \sum_{i=0}^{2^n-1} \alpha_i |i\rangle \xrightarrow{\text{Messung}} |i\rangle$ mit Wahrscheinlichkeit $|\alpha_i|^2$; beobachte i .

Daten

- ▶ **Qubit** $|\psi\rangle_1 \in \mathbb{C}^2 = \alpha_0 |0\rangle + \alpha_1 |1\rangle$ mit $|\alpha_0|^2 + |\alpha_1|^2 = 1$
 - ▶ Basiszustände $|0\rangle = (1, 0)^t$ und $|1\rangle = (0, 1)^t$
- ▶ **Quanten-Register** aus n Qubits $|\psi\rangle_n \in \mathbb{C}^{2^n} = \sum_{i=0}^{2^n-1} \alpha_i |i\rangle$ mit $\sum_{i=0}^{2^n-1} |\alpha_i|^2 = 1$

Operationen

- ▶ **Unitäre Matrix** $U : \mathbb{C}^{2^n} \rightarrow \mathbb{C}^{2^n}$ mit $UU^\dagger = I$
- ▶ Entweder: Zusammengesetzt (\otimes und \cdot) aus lokalen **Gates**
- ▶ Oder: Black-Box **Orakel** $O|\psi_t\rangle \mapsto |\psi_{t+1}\rangle$
- ▶ 2^n klassische Operation gleichzeitig

Ausgabe

- ▶ **Messung** hier: $|\psi\rangle = \sum_{i=0}^{2^n-1} \alpha_i |i\rangle \xrightarrow{\text{Messung}} |i\rangle$ mit Wahrscheinlichkeit $|\alpha_i|^2$; beobachte i .

Daten

- **Qubit** $|\psi\rangle_1 \in \mathbb{C}^2 = \alpha_0 |0\rangle + \alpha_1 |1\rangle$ mit $|\alpha_0|^2 + |\alpha_1|^2 = 1$
 - Basiszustände $|0\rangle = (1, 0)^t$ und $|1\rangle = (0, 1)^t$
- **Quanten-Register** aus n Qubits $|\psi\rangle_n \in \mathbb{C}^{2^n} = \sum_{i=0}^{2^n-1} \alpha_i |i\rangle$ mit $\sum_{i=0}^{2^n-1} |\alpha_i|^2 = 1$

Operationen

- ▶ **Unitäre Matrix** $U : \mathbb{C}^{2^n} \rightarrow \mathbb{C}^{2^n}$ mit $UU^\dagger = I$
- ▶ Entweder: Zusammengesetzt (\otimes und \cdot) aus lokalen **Gates**
- ▶ Oder: Black-Box **Orakel** $O|\psi_t\rangle \mapsto |\psi_{t+1}\rangle$
- ▶ 2^n klassische Operation gleichzeitig

Ausgabe

- **Messung** hier: $|\psi\rangle = \sum_{i=0}^{2^n-1} \alpha_i |i\rangle \xrightarrow{\text{Messung}} |i\rangle$ mit Wahrscheinlichkeit $|\alpha_i|^2$; beobachte i .
- Ziel: α_j des gesuchten $|j\rangle$ maximieren

Outline

Einordnung

Vorkenntnisse

Lineare Kryptoanalyse

Quantum Computing

Bestehende Ansätze

Problematik

Analytische Untersuchung des Malviya-Algorithmus

Ausgabewahrscheinlichkeit

Triviale Approximation

Erfolgswahrscheinlichkeit

Erweiterter Algorithmus

Amplitudenverstärkung

+ Malviya-Algorithmus

Das Orakel

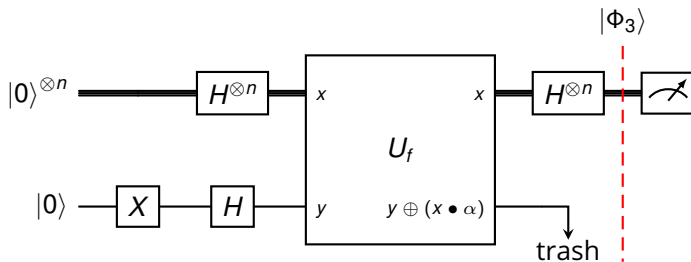
Fazit

Bernstein-Vazirani-Algorithmus

Erinnerung: Finde $\alpha, \beta, \gamma \in \mathbb{F}_2^{n(m,c,k)}$, sodass $(m \bullet \alpha) \oplus (k \bullet \gamma) \approx (f(m, k) \bullet \beta)$

Unter Voraussetzung: $f(x) = x \bullet \alpha$ (f ist eine lineare Funktion)

Ziel: Finde α

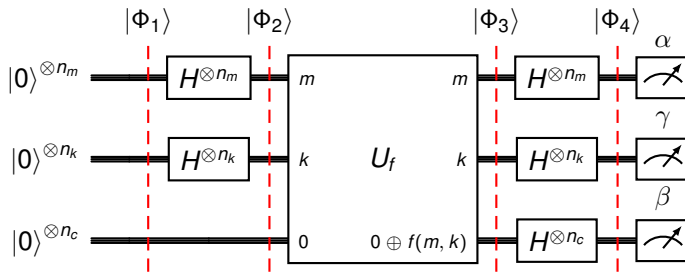


Bernstein-Vazirani-Algorithmus (Cont.)

$$|\Phi_3\rangle = \frac{1}{2^n} \sum_{\alpha, i \in \mathbb{F}_2^n} (-1)^{f(i) \oplus (i \bullet \alpha)} |\alpha\rangle = \frac{1}{2^n} \sum_{\alpha \in \mathbb{F}_2^n} \chi_f(\alpha) |\alpha\rangle$$

Da $f(i) := i \bullet \alpha$, an $\alpha = i$:

$$|\Phi_3\rangle = \frac{1}{2^n} \sum_{x \in \mathbb{F}_2^n} 1 |\alpha\rangle = |\alpha\rangle .$$



Output der modifizierten Variante

$$|\Phi_4\rangle = \frac{1}{\sqrt{2^{3n}}} * \sum_{m,k \in \mathbb{F}_2^n} \sum_{\alpha\beta\gamma \in \mathbb{F}_2^n} (-1)^{(\alpha \bullet m) \oplus (\gamma \bullet k) \oplus (\beta \bullet f(m,k))} |\alpha\gamma\beta\rangle$$

„Güte“ einer Approximation $\alpha\gamma\beta$ ist nun in der Amplitude ihres Zustandes eingebettet
 \Rightarrow je besser eine Approximation, desto wahrscheinlicher wird sie gemessen.

Outline

Einordnung

Vorkenntnisse

Lineare Kryptoanalyse

Quantum Computing

Bestehende Ansätze

Problematik

Analytische Untersuchung des Malviya-Algorithmus

Ausgabewahrscheinlichkeit

Triviale Approximation

Erfolgswahrscheinlichkeit

Erweiterter Algorithmus

Amplitudenverstärkung

+ Malviya-Algorithmus

Das Orakel

Fazit

Probleme an [MT20]

- ▶ Unvollendete analytische Erfolgsabschätzung
- ▶ Empirische Erfolgsuntersuchung nicht aussagekräftig
 - ▶ Scheinbar sehr schlechte Erfolgswahrscheinlichkeit
 - ▶ Triviale Approximation ($\alpha = \beta = \gamma = 0$) immer perfekt und damit sehr wahrscheinlich?

| Iteration size | Trivial | Highly | Least |
|----------------|---------------|-----------------|-----------------|
| 1024 | 60.8 (5.94%) | 150.4 (14.69%) | 436.4 (42.62%) |
| ... | | | |
| 7168 | 447.4 (6.24%) | 1024 (14.29%) | 3003 (41.89%) |
| 8192 | 520.8 (6.36%) | 1163.6 (14.20%) | 3446.8 (42.08%) |
| Average % | 6.25% | 14.17% | 42.09% |

Tabelle: Ausschnitt Ergebnisse Simulation
[MT20]

Probleme an [MT20]

- ▶ Unvollendete analytische Erfolgsabschätzung
- ▶ Empirische Erfolgsuntersuchung nicht aussagekräftig
 - ▶ Scheinbar sehr schlechte Erfolgswahrscheinlichkeit
 - ▶ Triviale Approximation ($\alpha = \beta = \gamma = 0$) immer perfekt und damit sehr wahrscheinlich?

| Iteration size | Trivial | Highly | Least |
|----------------|---------------|-----------------|-----------------|
| 1024 | 60.8 (5.94%) | 150.4 (14.69%) | 436.4 (42.62%) |
| ... | | | |
| 7168 | 447.4 (6.24%) | 1024 (14.29%) | 3003 (41.89%) |
| 8192 | 520.8 (6.36%) | 1163.6 (14.20%) | 3446.8 (42.08%) |
| Average % | 6.25% | 14.17% | 42.09% |
| * % | 1.67% | 1.53% | 37.14% |

Tabelle: Ausschnitt Ergebnisse Simulation

* *Ergebnisse auf IBM Q Systemen, 53.47% unmöglich [MT20]*

Outline

Einordnung

- Vorkenntnisse

 - Lineare Kryptoanalyse

 - Quantum Computing

- Bestehende Ansätze

- Problematik

Analytische Untersuchung des Malviya-Algorithmus

- Ausgabewahrscheinlichkeit

- Triviale Approximation

- Erfolgswahrscheinlichkeit

Erweiterter Algorithmus

- Amplitudenverstärkung

- + Malviya-Algorithmus

Das Orakel

Fazit

- Untersuchung der Amplituden nach jeden Schritt
- Ergebnis:

$$p_{\alpha,\gamma,\beta} = \frac{|c(\bar{t}_{\alpha||\gamma,\beta}(f))|^2}{2^{n_c}},$$

wobei

$$c(\bar{t}_{\alpha||\gamma,\beta}(f)) := \frac{\#\{m \in \mathbb{F}_2^{n_m}, k \in \mathbb{F}_2^{n_k} \mid (m \bullet \alpha) \oplus (k \bullet \gamma) = (f(m, k) \bullet \beta)\}}{2^{n_m+n_k-1}} - 1.$$

- Untersuchung der Amplituden nach jeden Schritt
- Ergebnis:

$$p_{\alpha,\gamma,\beta} = \frac{|c(\bar{t}_{\alpha||\gamma,\beta}(f))|^2}{2^{n_c}},$$

wobei

$$c(\bar{t}_{\alpha||\gamma,\beta}(f)) := \frac{\#\{m \in \mathbb{F}_2^{n_m}, k \in \mathbb{F}_2^{n_k} \mid (m \bullet \alpha) \oplus (k \bullet \gamma) = (f(m, k) \bullet \beta)\}}{2^{n_m+n_k-1}} - 1.$$

Erinnerung: Ziel Lineare Kryptoanalyse: Finde α, β, γ , sodass

$$(m \bullet \alpha) \oplus (k \bullet \gamma) \approx (f(m, k) \bullet \beta).$$

Outline

Einordnung

- Vorkenntnisse

 - Lineare Kryptoanalyse

 - Quantum Computing

- Bestehende Ansätze

- Problematik

Analytische Untersuchung des Malviya-Algorithmus

- Ausgabewahrscheinlichkeit

- Triviale Approximation**

- Erfolgswahrscheinlichkeit

Erweiterter Algorithmus

- Amplitudenverstärkung

- + Malviya-Algorithmus

Das Orakel

Fazit

- ▶ Tatsächlich: $p_{\alpha,\beta,\gamma} \sim (\text{„Güte“}_{\alpha,\beta,\gamma})^2$
- ▶ Genaue Formel
 - ▶ Bestätigung Tabelle 1 (Malviya Simulation)
- ▶ Triviale Approximation, $\alpha, \beta, \gamma = 0$, damit

$$p_{0,0,0} = \frac{1}{2^{n_c}}$$

- ▶ *perfekt* = immer ($2^{n_m+n_k}$ mal) richtig

- ▶ Tatsächlich: $p_{\alpha,\beta,\gamma} \sim (\text{„Güte“}_{\alpha,\beta,\gamma})^2$
- ▶ Genaue Formel
 - ▶ Bestätigung Tabelle 1 (Malviya Simulation)
- ▶ Triviale Approximation, $\alpha, \beta, \gamma = 0$, damit

$$p_{0,0,0} = \frac{1}{2^{n_c}}$$

- ▶ *perfekt* = immer ($2^{n_m+n_k}$ mal) richtig
- ▶ Problematik
 - ▶ Triviale Approximation ($\alpha = \beta = \gamma = 0$) immer perfekt und damit sehr wahrscheinlich?

- ▶ Tatsächlich: $p_{\alpha,\beta,\gamma} \sim (\text{„Güte“}_{\alpha,\beta,\gamma})^2$
- ▶ Genaue Formel
 - ▶ Bestätigung Tabelle 1 (Malviya Simulation)
- ▶ Triviale Approximation, $\alpha, \beta, \gamma = 0$, damit

$$p_{0,0,0} = \frac{1}{2^{n_c}}$$

- ▶ *perfekt* = immer ($2^{n_m+n_k}$ mal) richtig
- ▶ Problematik
 - ▶ Triviale Approximation (~~$\alpha = \beta = \gamma = 0$~~) immer ~~perfekt und damit sehr wahrscheinlich?~~
 - ▶ Nein.
 - ▶ $p_{\alpha,\beta,\gamma} \Rightarrow 0$ mit einem Orakel-Aufruf

Outline

Einordnung

- Vorkenntnisse

 - Lineare Kryptoanalyse

 - Quantum Computing

- Bestehende Ansätze

- Problematik

Analytische Untersuchung des Malviya-Algorithmus

- Ausgabewahrscheinlichkeit

- Triviale Approximation

- Erfolgswahrscheinlichkeit

Erweiterter Algorithmus

- Amplitudenverstärkung

- + Malviya-Algorithmus

Das Orakel

Fazit

- ▶ Messen² einer Approximation, welche eine gewisse Mindestgüte τ hat
 - ▶ $\tau \leq |c(\tilde{t}_{\alpha||\gamma,\beta}(f))|$
- ▶ Erfolg hängt stark von *Linearer Approximierbarkeit* von f ab
- ▶ Keine eindeutige Definition in Literatur
 - ▶ Definition und Betrachtung einiger Maße in meiner Arbeit
 - ▶ Für beliebige f schwer (exponentiell) zu Berechnen
 - ▶ \Rightarrow Betrachtung spezieller f
 - ▶ (Teil-)Linear, affin
 - ▶ Bent
 - ▶ Pseudorandom

²des assoziierten Zustandes

Outline

Einordnung

- Vorkenntnisse

 - Lineare Kryptoanalyse

 - Quantum Computing

- Bestehende Ansätze

- Problematik

Analytische Untersuchung des Malviya-Algorithmus

- Ausgabewahrscheinlichkeit

- Triviale Approximation

- Erfolgswahrscheinlichkeit

Erweiterter Algorithmus

- Amplitudenverstärkung

 - + Malviya-Algorithmus

Das Orakel

Fazit

Verallgemeinerung des Grover Algorithmus

Boosting ausgewählter Zustände

Boosting = Amplituden und damit Mess-Wkt. bestimmter Zustände erhöhen

M = Anzahl dieser *guten* Zustände

Durch mehrfaches Anwenden eines speziellen Operators

- ▶ Amplitude der *guten* Zustände erhöht sich pro Anwendung um etwa einen konstanten Faktor
- ▶ Lineares Amplitudenwachstum \Rightarrow Mess-Wkt. der *guten* Zustände steigt quadratisch an
 - ▶ Etwa $\sqrt{\frac{N}{M}}$ bzw. $\sqrt{\frac{2^n}{M}}$ Anwendungen

Der Amplitudenverstärkungs-Operator

$$(U_s U_f)$$

- ▶ U_f dreht³ die Phasen der *guten* Zustände
- ▶ U_s *Diffusion-Operator* spiegelt am Durchschnitt der Amplituden unabhängig von den *guten* Zuständen

³um 180° , invertiert Amplituden

Outline

Einordnung

- Vorkenntnisse

 - Lineare Kryptoanalyse

 - Quantum Computing

- Bestehende Ansätze

- Problematik

Analytische Untersuchung des Malviya-Algorithmus

- Ausgabewahrscheinlichkeit

- Triviale Approximation

- Erfolgswahrscheinlichkeit

Erweiterter Algorithmus

- Amplitudenverstärkung

- + Malviya-Algorithmus

Das Orakel

Fazit

Malviya mit Amplitudenverstärkung

Idee: Amplitudenverstärkung, um die Wahrscheinlichkeit für eine gute Approximation zu erhöhen

Aufgabe: U_f so konstruieren, dass die Phase der *guten* Zustände invertiert wird

Problem: Was sind die *guten* Zustände?

- ▶ Mindestamplitude nach Malviya-Algorithmus
- ▶ Amplitude ist nicht direkt messbar/verwendbar [SUR⁺20]

Malviya mit Amplitudenverstärkung

Idee: Amplitudenverstärkung, um die Wahrscheinlichkeit für eine gute Approximation zu erhöhen

Aufgabe: U_f so konstruieren, dass die Phase der *guten* Zustände invertiert wird

Problem: Was sind die *guten* Zustände?

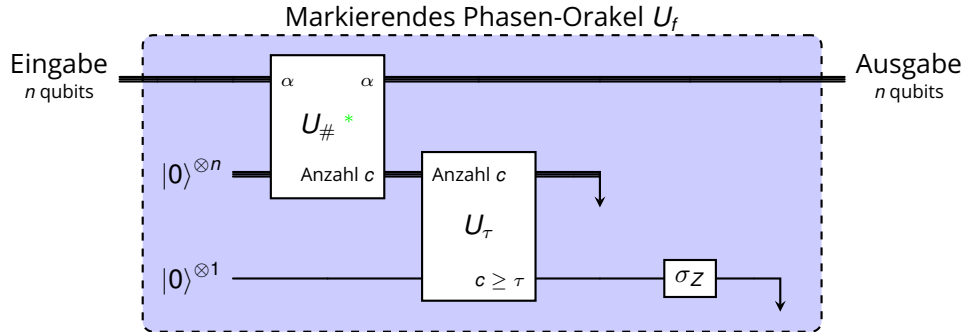
- ▶ Mindestamplitude nach Malviya-Algorithmus
- ▶ Amplitude ist nicht direkt messbar/verwendbar [SUR⁺20]

Lösung: Amplitude abschätzen (und in zusätzliches Register schreiben)



FU Berlin, Quantum Linear Cryptanalysis, 24. Februar 2024

Das Orakel

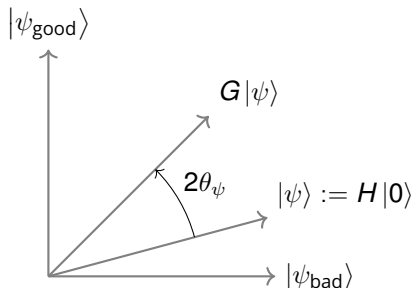


- Hier vereinfacht⁴: gesucht α , sodass $(x \bullet \alpha) \approx f(x)$
- Ziel: $U_{\#}^*$ zu bauen

⁴D.h. nicht multivariat oder vektoriell, ähnlich zu Bernstein Vazirani statt Malviya

Ansatz 1: via QPE

- Möglich, via QPE⁵ über Grover-Operator die Amplitude der guten Zustände zu bestimmen
- Quantum Counting von $|f_{\alpha}^{-1}(1)|$, wobei $f_{\alpha}(x) = (\alpha \bullet x) \oplus f(x)$

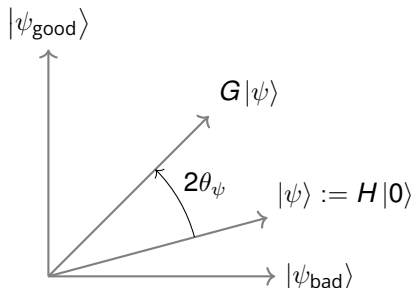


- Laufzeit $O(2^t)$

⁵Quantum Phase Estimation, Subroutine zum bestimmen der Phasenveränderung durch ein Orakel

Ansatz 1: via QPE

- Möglich, via QPE⁵ über Grover-Operator die Amplitude der guten Zustände zu bestimmen
- Quantum Counting von $|f_\alpha^{-1}(1)|$, wobei $f_\alpha(x) = (\alpha \bullet x) \oplus f(x)$



- Laufzeit $O(2^t)$ bzw. $O(2^n/\varepsilon)$ um \tilde{c} mit $|c - \tilde{c}| \leq \varepsilon$ zu erhalten

⁵Quantum Phase Estimation, Subroutine zum bestimmen der Phasenveränderung durch ein Orakel

- ▶ Quantum Approximate Counting [BHMT02]
- ▶ Finde \tilde{c} mit $|c - \tilde{c}| \leq \varepsilon$
- ▶ Laufzeit $O(\sqrt{2^n}/\varepsilon)$
- ▶ Benötigt wiederholtes Messen zwischendurch \Rightarrow nicht einfach als Orakel nutzbar

Ansatz 3: Walsh Transform

- ▶ Kein Count, sondern direkt Walsh transform

$$\frac{\hat{\chi}_f(\alpha) + 2^n}{2} = (\text{Corr}(\bar{t}_{\alpha,1}(f)) + 1) \cdot \frac{2^n}{2} = c$$

- ▶ Einfache Verwendung Hadamard-Gate nicht möglich
- ▶ Fast Walsh Hadamard Transform (FWHT) ebenfalls nicht
- ▶ Mapping klassischer Walsh Transform als Quantum Circuit möglich
- ▶ Laufzeit $O(2^n)$

Ansatz 4: Verwendung Hoeffding-Schranke

Algorithm 1: Walsh transform approximation

Input : function $f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2$, $\alpha \in \mathbb{F}_2^n$, $s \in \mathbb{N}$
sample $x = (x_1, \dots, x_s) \sim (\mathbb{F}_2^n)^s$ uniformly;

for $i \in \{1, \dots, s\}$ **do**
 $X_i \leftarrow (-1)^{(\alpha \bullet x_i) \oplus f(x_i)}$;

end

$\aleph \leftarrow \frac{1}{s} \sum_{i=1}^s X_i$;

Output: $\aleph \cdot 2^n$ with $\aleph \approx \frac{\hat{\chi}_f(\alpha)}{2^n}$

Ansatz 4: Verwendung Hoeffding-Schranke

Theorem (Hoeffding)

Seien $X_1, \dots, X_s \in [0, 1]$ iid. Zufallsvariablen mit Durchschnitt $\aleph := \frac{1}{s} \sum_{i=1}^s X_i$, dann gilt für jeden Fehler $\varepsilon > 0$:

$$\Pr [|\aleph - \mathbb{E}[\aleph]| < \varepsilon] > 1 - 2e^{-2\varepsilon^2 s}. \quad (1)$$

- ▶ Wähle X_i so, dass $\mathbb{E}[\aleph] \approx \frac{\hat{x}_f(\alpha)}{2^n}$
 - ▶ Leichte Transformation des Hoeffding-Theorems notwendig
- ▶ Laufzeit

$$O\left(\frac{-2^{2n} \ln(1-p)}{\varepsilon^2}\right)$$

- $$O\left(\sqrt{\frac{1}{\mathcal{L}_{p_\tau}}} \cdot O_\# \right)$$

- $$\mathcal{L}_{\mathbf{p}_\tau} := \frac{1}{2^{n_y}} \sum_{\substack{m_x, m_y \in \mathbb{F}_2^n \\ m_y \neq 0}} \mathbf{p}_\tau(|c(\bar{t}_{m_x, m_y}(f))|) \text{ mit } \mathbf{p}_\tau(x) := \begin{cases} x^2 & \text{falls } x \geq \tau \\ 0 & \text{sonst} \end{cases}$$

$$O\left(\frac{2^{n_k+n_m}}{\varepsilon}\right) \text{ oder } \tilde{O}\left(\frac{2^{2n_k+2n_m}}{\varepsilon^2}\right)$$

- 30

- ▶ Erfolgreiche analytische Untersuchung Erfolgswahrscheinlichkeit Malviya-Algorithmus

- ▶ Erfolgreiche analytische Untersuchung Erfolgswahrscheinlichkeit Malviya-Algorithmus
- ▶ Praktische Einschätzung der Ergebnisse anhand einiger Funktionsklassen
 - ▶ Effiziente Berechnung für beliebige Funktionen nicht möglich
 - ▶ Abschätzung für pseudozufällige Funktionen leider fehlgeschlagen

- ▶ Erfolgreiche analytische Untersuchung Erfolgswahrscheinlichkeit Malviya-Algorithmus
- ▶ Praktische Einschätzung der Ergebnisse anhand einiger Funktionsklassen
 - ▶ Effiziente Berechnung für beliebige Funktionen nicht möglich
 - ▶ Abschätzung für pseudozufällige Funktionen leider fehlgeschlagen
- ▶ Erstellung neuer Algorithmen

- ▶ Erfolgreiche analytische Untersuchung Erfolgswahrscheinlichkeit Malviya-Algorithmus
- ▶ Praktische Einschätzung der Ergebnisse anhand einiger Funktionsklassen
 - ▶ Effiziente Berechnung für beliebige Funktionen nicht möglich
 - ▶ Abschätzung für pseudozufällige Funktionen leider fehlgeschlagen
- ▶ Erstellung neuer Algorithmen
 - ▶ Amplitude-Amplifikation + Malviya / Grover

- ▶ Erfolgreiche analytische Untersuchung Erfolgswahrscheinlichkeit Malviya-Algorithmus
- ▶ Praktische Einschätzung der Ergebnisse anhand einiger Funktionsklassen
 - ▶ Effiziente Berechnung für beliebige Funktionen nicht möglich
 - ▶ Abschätzung für pseudozufällige Funktionen leider fehlgeschlagen
- ▶ Erstellung neuer Algorithmen
 - ▶ Amplitude-Amplifikation + Malviya / Grover
 - ▶ Counting Orakel / Probabilistisches Orakel

- ▶ Erfolgreiche analytische Untersuchung Erfolgswahrscheinlichkeit Malviya-Algorithmus
- ▶ Praktische Einschätzung der Ergebnisse anhand einiger Funktionsklassen
 - ▶ Effiziente Berechnung für beliebige Funktionen nicht möglich *
 - ▶ Abschätzung für pseudozufällige Funktionen leider fehlgeschlagen
- ▶ Erstellung neuer Algorithmen
 - ▶ Amplitude-Amplifikation + Malviya / Grover
 - ▶ Counting Orakel / Probabilistisches Orakel
- ▶ Laufzeit dieser hängt von Erfolgswahrscheinlichkeit des Malviya-Algorithmus ab *





Ergebnisse

- ▶ Erfolgreiche analytische Untersuchung Erfolgswahrscheinlichkeit Malviya-Algorithmus
- ▶ Praktische Einschätzung der Ergebnisse anhand einiger Funktionsklassen
 - ▶ Effiziente Berechnung für beliebige Funktionen nicht möglich *
 - ▶ Abschätzung für pseudozufällige Funktionen leider fehlgeschlagen
- ▶ Erstellung neuer Algorithmen
 - ▶ Amplitude-Amplifikation + Malviya / Grover
 - ▶ Counting Orakel / Probabilistisches Orakel
- ▶ Laufzeit dieser hängt von Erfolgswahrscheinlichkeit des Malviya-Algorithmus ab *
- ▶ ... und davon, wie der Zufall propagiert

Vielen Dank!

Zeit für Fragen

Referenzen I

-  Gilles Brassard, Peter Hoyer, Michele Mosca, and Alain Tapp, Quantum Amplitude Amplification and Estimation, vol. 305, 2002, Comment: 32 pages, no figures, pp. 53–74.
-  Gilles Brassard, Peter Hoyer, and Alain Tapp, Quantum Counting, arXiv:quant-ph/9805082 **1443** (1998), 820–831, Comment: 12 pages, LaTeX2e.
-  Matthias Homeister, Quantum Computing verstehen: Grundlagen - Anwendungen - Perspektiven, 6., erweiterte und überarbeitete auflage ed., Computational intelligence, Springer Vieweg, Wiesbaden [Heidelberg], 2022.
-  Hongwei Li and Li Yang, A quantum algorithm to approximate the linear structures of Boolean functions, Mathematical Structures in Computer Science **28** (2018), no. 1, 1–13, The abstract does not fit the core and result section of the paper
Ä quantum algorithm to determine approximations of linear structures of Boolean functions
is presented and analysed.”
vs

Referenzen II

Ä polynomial-time quantum approximate algorithm for deciding whether a function $f \in B^n$ has non-zero linear structures has been presented.”.



Mitsuru Matsui, Linear Cryptanalysis Method for DES Cipher, Advances in Cryptology — EUROCRYPT '93, vol. 765, Springer Berlin Heidelberg, Berlin, Heidelberg, July 1993, pp. 386–397.



A. K. Malviya and N. Tiwari, Linear approximation of a vectorial Boolean function using quantum computing, EPL (Europhysics Letters) **132** (2020), no. 4, 40001.



Michael A. Nielsen and Isaac L. Chuang, Quantum computation and quantum information, 10th anniversary ed ed., Cambridge University Press, Cambridge ; New York, 2010.



Yohichi Suzuki, Shumpei Uno, Rudy Raymond, Tomoki Tanaka, Tamiya Onodera, and Naoki Yamamoto, Amplitude estimation without phase estimation, Quantum Information Processing **19** (2020), no. 2, 75.

Definition (Lineare Struktur)

$a \in \mathbb{F}_2^n$ wird *lineare Struktur* einer Booleschen Funktion $f : \mathbb{F}_2^n \mapsto \mathbb{F}_2$ genannt, wenn

$$\forall x \in \mathbb{F}_2^n : f(x \oplus a) = f(x) \oplus c_{a,f}$$

wobei $c_{a,f} \in \mathbb{F}_2 := f(a) \oplus f(0)$ als konstant angesehen werden kann, da a und f fix sind.

Idee: Keine 'gute' lineare Struktur \rightarrow keine 'gute' lineare Approximation \rightarrow lineare Kryptoanalyse nicht möglich

[LY18] präsentierten den einzigen uns bekannten Quantenalgorithmus über lineare Strukturen

- ▶ relativ kompliziert
- ▶ Bernstein-Vazirani als Subroutine
- ▶ Meta-Parameter p , beeinflusst Erfolg und (proportional) Laufzeit

Ausgabe: keine Struktur **schlechter** als $1 - \frac{1}{p}$
→ Keine *obere* Schranke für lineare Approximierbarkeit

```
 $H \leftarrow \emptyset;$   
repeat  $p(n)$  times  
   $w_1, \dots, w_{n+1} \in \{w \in \mathbb{F}_2^n \mid \chi_f(w) \neq 0\} \leftarrow$  run Bernstein-Vazirani algorithm;  
   $H \leftarrow H \cup \{w_1, \dots, w_{n+1}\};$   
   $A^c \leftarrow \{x \in \mathbb{F}_2^n \mid \forall i : (x \bullet H[i]) = c\};$   
  if  $A^0 = \{0\}$  and  $A^1 = \emptyset$  then  
    return no;  
  end  
end  
return yes:  $A^0, A^1;$ 
```

Ausgabe: keine Struktur schlechter als $1 - \frac{1}{p}$
→ Keine obere Schranke für lineare Approximierbarkeit

$$|\Phi_1\rangle = H^{\otimes n} |0\rangle^{\otimes n} \otimes H X |0\rangle = \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} |i\rangle \otimes \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) = |+\rangle^{\otimes n} \otimes |-\rangle.$$

Apply Oracle $U_f : |x\rangle |y\rangle \mapsto |x\rangle |s \cdot y\rangle$

$$|\Phi_2\rangle = U_f |\Phi_1\rangle = \sum_{i=0}^{2^n-1} |i\rangle \otimes \frac{|0 \oplus (s \cdot i)\rangle - |1 \oplus (s \cdot i)\rangle}{\sqrt{2}} = \left(\sum_{i=0}^{2^n-1} (-1)^{s \cdot i} |i\rangle \right) \otimes |-\rangle.$$

Ignore last qubit and apply another Hadamard on first register:

$$|\Phi_3\rangle = (H^{\otimes n} \otimes I) |\Phi_2\rangle = \sum_{j=0}^{2^n-1} \left(\frac{1}{2^n} \sum_{i=0}^{2^n-1} (-1)^{s \cdot i} (-1)^{j \cdot i} \right) |j\rangle.$$

For $j = s$ therefor:

$$|\Phi_3\rangle = \frac{1}{2^n} \sum_{i=0}^{2^n-1} 1 |s\rangle = |s\rangle.$$

sei $f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2$ eine (Boolsche) Funktion

finde $\alpha \in \mathbb{F}_2^n$; ($b \in \mathbb{F}_2$) s.t.

$$(x \bullet \alpha) \oplus f(x) \approx b$$

2^n Möglichkeiten \rightarrow generell schwer

Definition

Die Walsh-Transformation ist gegeben durch:

$$\hat{\chi}_f : \mathbb{F}_2^n \rightarrow \mathbb{Z}, \alpha \mapsto \sum_{x \in \mathbb{F}_2^n} (-1)^{(\alpha \bullet x) \oplus f(x)}$$