

Die Abschätzung der (Qu)BER aus der Visibilität

Methode der Entscheidungsschwelle

Methode der Wahrscheinlichkeiten

Dipl.- Ing. Björnstjerne Zindler, M.Sc.

www.Zenithpoint.de

Erstellt: 21. Dezember 2020 – Letzte Revision: 22. Dezember 2020

Inhaltsverzeichnis

1	Die Berechnung der BER aus der Visibilität I	3
2	Die Berechnung der BER aus der Visibilität II	5

Literatur

- [Dip11] Dipl.-Ing. Björnstjerne Zindler. Aufbau von faserbasierten Interferometern für die Quantenkryptografie. Masterarbeit, 2010/11.
- [Nic02] Nicolas Gisin, Grégoire Ribordy. Quantum cryptography. *Reviews of modern physics*, Volume 74:145– 190, 2002.
-

1 Die Berechnung der BER aus der Visibilität durch die *Methode der Entscheidungsschwelle*.

Die Berechnung der BER aus der Visibilität durch die *Methode der Entscheidungsschwelle*. Basierend auf [Dip11] sind bekannt die Berechnungsgrundlagen der Phasenlage φ und die theoretisch messbare optische Leistung am Detektor $P(\psi_m)$ für den mittleren Peak der Time- Bin- Konfiguration unter Nutzung einer cw- Laserquelle.

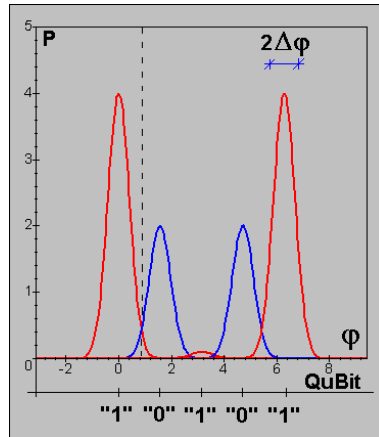
$$P(\psi_m) = 4 \cdot \cos^2 \frac{\varphi}{2} \Rightarrow P(\psi_m) = 4 \cdot \cos^2 \left[\frac{\pi}{\lambda} \cdot n \cdot \Delta L \right]$$

\Rightarrow

$$\Delta\varphi = \frac{2\pi}{\lambda} \cdot n \cdot \left(1 + \frac{dn}{dT} \cdot \Delta T \right) \cdot \Delta L \cdot (1 + \alpha \cdot \Delta T)$$

Letzterer Ausdruck beschreibt das Phasenrauschen infolge Temperaturabweichung vom Sollwert. Weitere Gründe sind möglich, werden jedoch hier nicht weiter betrachtet.

Bei der Phasenkodierung nach dem BB84- Protokoll wird für jedes zu übertragende QuBit eine streng definierte Phase eingestellt ($0\pi, \pi/2, \pi, 3\pi/2$). Am Detektor des Empfängers sind jedoch gaussverteilt um diese Phasen kleinere Abweichungen messbar. Diese Linienverbreiterung soll ausschließlich auf das oben definierte Phasenrauschen begründet werden.



Gewähltes Modell zur Berechnung

Die Entscheidungsschwelle φ_E bestimmt den Fehler 1. Art.

- Wird ein QuBit 1 gesendet und liegt dann dieses oberhalb der Entscheidungsschwelle des Detektors am Detektor an, wird jener das QuBit als 0 interpretieren.
- Wird ein QuBit 1 gesendet und liegt dann dieses unterhalb der Entscheidungsschwelle des Detektors am Detektor an, wird jener das QuBit als 1 interpretieren.

Die Lage der Entscheidungsschwelle φ_E ist maßgeblich für die Ermittlung der BER. Um diese zu berechnen, werden die QuBits definiert.

$$\text{QuBit}_1 = \frac{4}{\Delta\varphi \cdot \sqrt{2\pi}} \cdot e^{-\frac{\varphi^2}{2 \cdot \Delta\varphi^2}} \Leftrightarrow \text{QuBit}_0 = \frac{2}{\Delta\varphi \cdot \sqrt{2\pi}} \cdot e^{-\frac{(\varphi - \frac{\pi}{2})^2}{2 \cdot \Delta\varphi^2}}$$

Die Entscheidungsschwelle ist jener Punkt, wo beide QuBits gleiche Werte besitzen.

$$\text{QuBit}_1 = \text{QuBit}_0$$

\Rightarrow

$$\varphi_E = \frac{\pi}{4} + \frac{\ln 4}{\pi} \cdot \Delta\varphi^2$$

Damit sind die Fehlerintegrale definierbar, die mathematische Beschreibung des Fehlers 1. Art.

$$\text{TRUE} = \int_{-\infty}^{\varphi_E} \text{QuBit}_1 \Leftrightarrow \text{FALSE} = \int_{\varphi_E}^{+\infty} \text{QuBit}_1$$

Mit dem QuBit 0 ist eine äquivalente Berechnung ebenfalls möglich.

$$\frac{1}{2} \cdot \text{TRUE} = 1 + \operatorname{erf} \frac{\varphi_E}{\sqrt{2} \cdot \Delta\varphi} \Leftrightarrow \frac{1}{2} \cdot \text{FALSE} = 1 - \operatorname{erf} \frac{\varphi_E}{\sqrt{2} \cdot \Delta\varphi}$$

Beide Fehlerintegrale unterscheiden sich nur durch das unterschiedliche Vorzeichen. Die BER wird definiert aus den Fehlerintegralen TRUE und FALSE.

$$\text{BER} = \frac{\text{FALSE}}{\text{TRUE}}$$

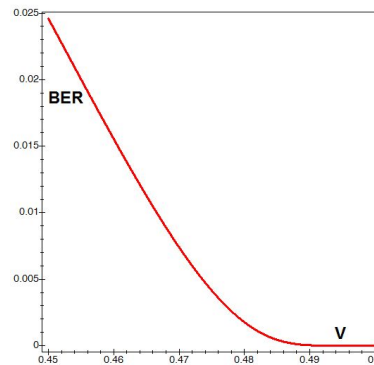
⇒

$$\text{BER} = \frac{1 - \operatorname{erf} \frac{\varphi_E}{\sqrt{2} \cdot \Delta\varphi}}{1 + \operatorname{erf} \frac{\varphi_E}{\sqrt{2} \cdot \Delta\varphi}}$$

Wird in die Berechnungsgrundlage der BER die Entscheidungsschwelle φ_E eingesetzt, ist das Bitfehlerverhältnis nur noch abhängig von $\Delta\varphi$. Aus [Dip11] ist diese Abhängigkeit auflösbar mittels der Visibilität V.

$$\Delta\varphi = \arccos \left(\pm \sqrt{\frac{V}{1-V}} \right)$$

⇒



BER	V	BER	V	BER	V
0,025	0,450	0,007	0,470	0,000.03	0,490
0,016	0,460	0,002	0,480	0,000.00	0,499

Ausgewählte Werte für BER in Abhängigkeit von der Visibilität.

Mit dem von links kommenden Grenzwert gilt:

$$\lim_{V \rightarrow 0,5^{(-)}} \text{BER} = 0$$

2 Die Berechnung der BER aus der Visibilität durch die Methode der Wahrscheinlichkeiten.

Aus [Nic02] ist die Berechnung des Bitfehler- Verhältnisses (zur Unterscheidung zu *Methode der Entscheidungsschwelle* hier QuBER genannt) auf Basis der Wahrscheinlichkeiten bekannt.

$$\text{QuBER} = \frac{R_{OPT}}{R_{SIFT}} + \frac{R_{DET}}{R_{SIFT}} + \frac{R_{ACC}}{R_{SIFT}}$$

⇒

$$\text{QuBER} = \rho_{OPT} + \frac{\rho_{DARK} \cdot n}{2 \cdot t_{link} \cdot \eta \cdot q \cdot \mu} + \frac{\rho_{ACC}}{2 \cdot q \cdot \mu}$$

Über die Bedeutung der die QuBER bestimmenden Größen ist [Nic02] zu konsultieren. Dort ist auch die Zusammenfassung dieser zur Visibilität V beschrieben und wird hier nicht weiter erläutert. So gilt für QuBER.

$$\text{QuBER} = \frac{1 - V}{2}$$

Für V ist eine Temperaturabhängigkeit definierbar.

$$\text{QuBER} = \frac{1 - V \cdot \left(1 - \frac{d}{dT} V \cdot |\Delta T|\right)}{2}$$

Dabei ist ΔT die Temperaturdifferenz von der Solltemperatur und dV/dT die Temperaturabhängigkeit der Visibilität. Um die nun vorliegende Differentialgleichung lösen zu können, werden die Variablen getrennt und anschließend mit einem unbestimmten Integral beaufschlagt.

$$\int dT = |\Delta T| \cdot \int \frac{V}{V - 1 + 2 \cdot \text{QuBER}} dV$$

⇒

$$\frac{T + C}{|\Delta T|} = V + (1 - 2 \cdot \text{QuBER}) \cdot \ln(V - 1 + 2 \cdot \text{QuBER})$$

Die Lösung der Integrale verlangt die Integrationskonstante C und erzeugt eine (im ersten Blick) transzendente Gleichung, die jedoch durch ein Substitut auflösbar ist.

$$1 - 2 \cdot \text{QuBER} = V$$

⇒

$$\frac{T + C}{|\Delta T|} = V + V \cdot \ln(V - 1 + 2 \cdot \text{QuBER})$$

Der linke Term ist eine modifizierte *Heaviside-Funktion*¹, diese wird durch eine *Signum-Funktion*² ersetzt, um weiter die Berechnung der QuBER zu ermöglichen.

$$\pm K = \pm V \cdot \ln(V - 1 + 2 \cdot \text{QuBER})$$

⇒

$$\text{QuBER}_T = \frac{1 - V}{2} \pm \frac{1}{2} \cdot e^{\pm \frac{K}{V} - 1} = \text{QuBER} \pm e^{\pm \frac{K}{V} - 1}$$

Es ist die allgemeine Lösung der Differentialgleichung ermittelt, wobei QuBER_T die nun temperaturabhängige QuBER bezeichnet. Ein Randwertproblem wird aufgestellt, mit dem die partikuläre Lösung ermittelbar ist.

• Randwert 1:

$$V = 0 \quad \Leftrightarrow \quad \text{QuBER}_T = \frac{1}{2}$$

¹Allgemein: $\Theta(x) = \begin{cases} 0 & x < 0 \\ 1 & x \geq 0 \end{cases}$

²Allgemein: $\text{sgn}(x) = \begin{cases} +1 & x > 0 \\ 0 & x = 0 \\ -1 & x < 0 \end{cases}$ Sonderfall: $\text{sgn}(x) = \begin{cases} +1 & x \geq 0 \\ -1 & x < 0 \end{cases} \Rightarrow \text{sgn}(x) = 2 \cdot \Theta(x) - 1$

⇒

$$\text{QuBER} = \frac{1}{2}$$

• Randwert 2:

$$V = \frac{1}{2} \Leftrightarrow \text{QuBER}_T = 0$$

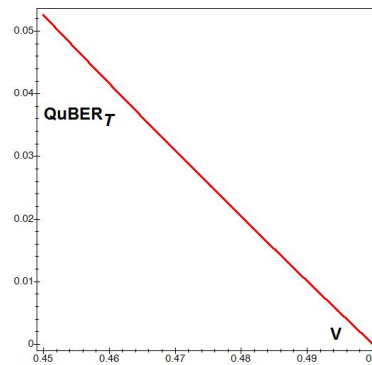
⇒

$$K = -\frac{1}{2}$$

Damit ist die partikuläre Lösung für QuBER_T ermittelt.

$$\text{QuBER}_T = \frac{1}{2} \cdot \left(1 - e^{\frac{2V-1}{2V}}\right)$$

⇒



QuBER_T	V	QuBER_T	V	QuBER_T	V
0,053	0,450	0,031	0,470	0,010	0,490
0,042	0,460	0,020	0,480	0,000	0,500

Ausgewählte Werte für QuBER_T in Abhängigkeit von der Visibilität.

Für Visibilitäten $0.5 \geq V > 0.2$ kann genähert werden.

$$\text{QuBER}_T = (V - 1)^2 - 0,25$$

L^AT_EX 2_ε