

VERTEIDIGUNG DER MASTERARBEIT

IMPLEMENTIERUNG EINER STEUERUNG FÜR EIN QUANTUM KEY
DISTRIBUTION (QKD) EXPERIMENT INKLUSIVE POSTPROCESSING

Robert Riemann

Institut für Physik – Humboldt-Universität zu Berlin

rriemann@physik.hu-berlin.de

22. März 2013



KRYPTOGRAPHIE



Abbildung: Cäsar-Verfahren mittels Chiffrier-Scheibe um 1460¹



Abbildung: Kryptographie heute mit dem neuen e-Personalausweises²

¹<http://www.chip.de/bildergalerie/>

Die-Geschichte-der-Kryptographie-Galerie_38410733.html, März 2013

²<http://www.reiner-sct.com/presse/fotoarchiv/>, März 2013

ÜBERSICHT

- 1 Einführung**
 - Klassische Kryptographie
 - Unconditional Security
 - Quantum Key Distribution
- 2 Experimenteller Aufbau**
 - Optischer Aufbau
 - Steuerung und Datennahme
- 3 Postprocessing**
 - Error Correction
 - Privacy Amplification
 - Authentifizierung
 - Details der Implementierung und Benchmarks
- 4 Ausblick**



KLASSIFIZIERUNG

Symmetrische Kryptographie

- Schlüssel:
privat
- Verschlüsselung und
Entschlüsselung ist
method. symmetrisch
- mathematisch effizient

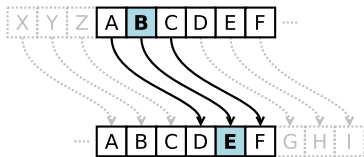


Abbildung: Cäsar-Verfahren (©)

Asymmetrische Kryptographie

- Schlüssel:
privater und öffentl. Teil
- Verschlüsselungsfunktion
nicht trivial umkehrbar,
daher asymmetrisch
- vergleichsweise ineffizient
- Schlüsseltausch öffentlich
- Schlüssel wiederverwendbar
- Sicherheit zweifelhaft

UNCONDITIONAL SECURITY, ONE-TIME PAD

Sicherheitskonzept, welches

- eine beliebige Verkleinerung des Restrisikos erlaubt
- mathematisch vollständig bewiesen ist
- keine weiteren Voraussetzung verlangt

Beispiel One-Time Pad (Symmetrische Verschlüsselung)

Nachricht	1	0	0	1	1
Schlüssel	0	0	1	1	1
Chiffre, XOR	1	0	1	0	0

- Kombination bitweise
- Entschlüsselung wie Verschlüsselung
- Sicherheit bewiesen³

³C. Shannon, Bell System Tech. J. **28**, 656 (1949)

PROBLEMVERLAGERUNG

Problem

- Schlüsseltausch bei klassischer, symmetrischer Kryptographie schwer realisierbar
- Fundamentale Sicherheitsprobleme in asymmetrischer Kryptographie

Lösung: wir verwenden das One-Time Pad

Problem der sicheren Nachrichtenverschlüsselung (Cypher)



Problem des sicheren Schlüsselaustausches



QUANTUM KEY DISTRIBUTION

Fundamentale Idee:

- Codierung und Übertragung der Schlüsselbits in einzelnen Quantenobjekten
- Erster Vorschlag einer Implementierung: BB84⁴

Ausnutzung der Gesetzmäßigkeiten der Quantenmechanik

- Jede Messung verändert das System.⁵
- Quantenobjekte in unbekanntem Zuständen können nicht kopiert werden (**No-Cloning Theorem**⁶).

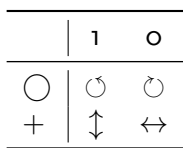
⁴C. H. Bennett und G. Brassard. Proc. of IEEE Int. Conf. on Computers, Systems, and Signal Processing, 175 (1984)

⁵mit der Ausnahme von Systemen im Eigenzustand der Messung

⁶W. K. Wootters und W. H. Zurek, Nature **299**, 802 (1982)



BB84 PROTOKOLL I



■ Sender (Alice) sendet polarisierte Photonen
(4 Zustände möglich)

■ Empfänger (Bob) misst Polarisation
(2 Basen möglich)

- falls Basen übereinstimmen:
Ergebnis zu 100 % korreliert, andernfalls zu 0 %.

Vorteil der Vorgehensweise:

- Abhören durch Dritte (Eve) nicht unbemerkt möglich, da die Messung den Zustand zerstört und Kopieren unmöglich ist



BB84 PROTOKOLL II

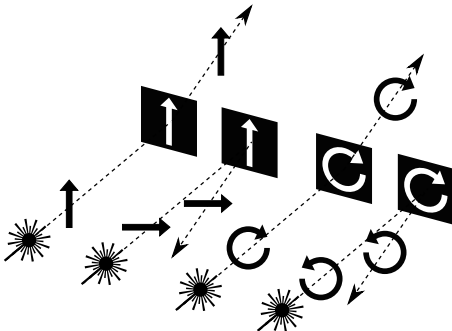


Abbildung: Kompatible Basen

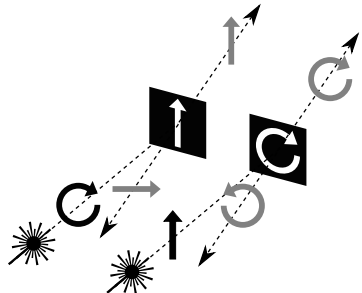


Abbildung: Inkompatible Basen

Unterscheidung der Zustände durch Polarisierende Strahlteiler und $\lambda/4$ -Plättchen.



BEISPIEL-ÜBERTRAGUNG

Alice Basis	Alice Bit	Bob Basis	Bob Bit	Resultat
○	1	○	1	✓
○	1	+	○	✗
○	1	+	1	✓
+	○	+	○	✓
+	○	○	1	✗
○	1	○	○	!

Tabelle: Messergebnisse für einzelne Bits. In der 3. Zeile ist das Ergebnis zufällig richtig. In der Letzten wurde das Bit manipuliert.

Messungen mit inkompatiblen Basen sind nicht deterministisch und müssen verworfen werden (**Sifting**).



OPTISCHER AUFBAU (SCHEMA)

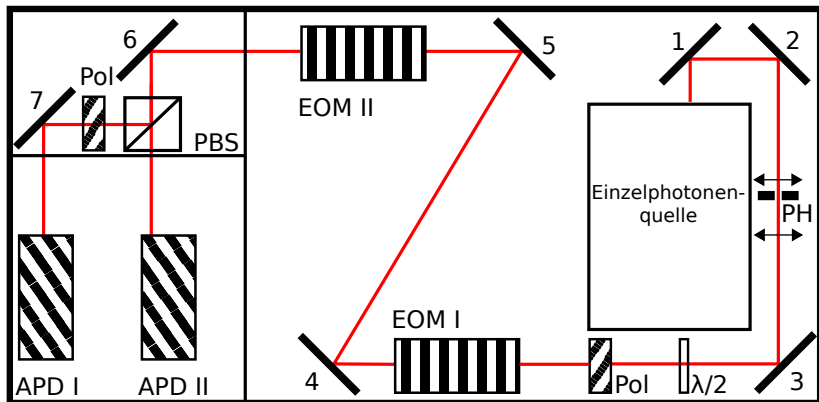


Abbildung: PH Lochblende, Pol Polarisator, EOM Elektro-Optischer Modulator, PBS Polarisierender Strahlteiler, APD Avalanche-Photodiode

OPTISCHER AUFBAU (PHOTO)

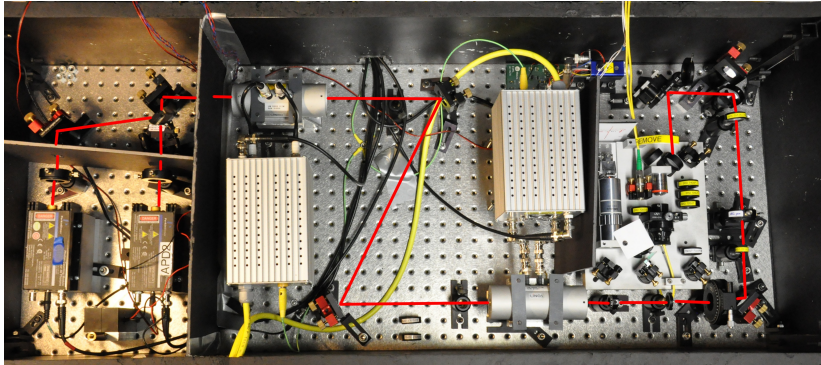


Abbildung: Maße 1,2 m × 0,5 m

ECHTZEITSTEUERUNG DURCH FIELD-PROGRAMMABLE-GATE-ARRAY (FPGA)

Demonstrationsexperiment:

keine räumliche Trennung der Steuerung von Sender & Empfänger

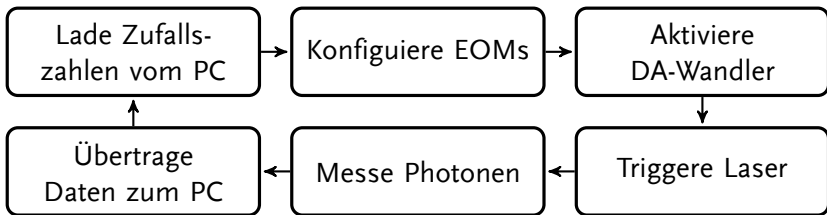
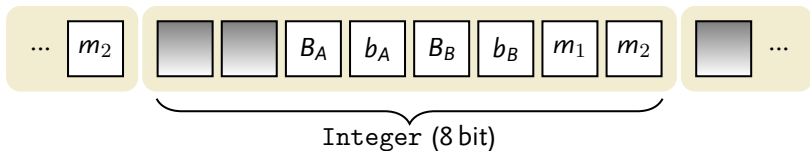


Abbildung: Flussdiagramm der FPGA-Prozesse

BINÄRFORMAT DER MESSDATEN



B_A Basis von Alice

b_A Bit von Alice

B_B Basis von Bob

b_B – *reserviert, ungenutzt* –

m_1 Photon in Detektor I gemessen

m_2 Photon in Detektor II gemessen

NACH DER QUANTENÜBERTRAGUNG

- In idealem Experiment (Detektionseffizient 100 %, kein Angreifer, keine exp. Fehler) **Raw Key** nach Sifting einsatzbereit

Warum Postprocessing

- **Raw Key** nach Sifting nicht identisch, wegen
 - Detektorrauschen, Güte optischer Elemente, Streulicht, ...
 - Abhörversuche durch Eve
 - Fehleranalyse und Fehlerkorrektur notwendig
 - Löschen öffentlicher Information aus dem Schlüssel notwendig
-
- Kommunikation für Postprocessing öffentlich und klassisch



ÜBERSICHT DER TEILSCHRITTE DES POSTPROCESSINGS

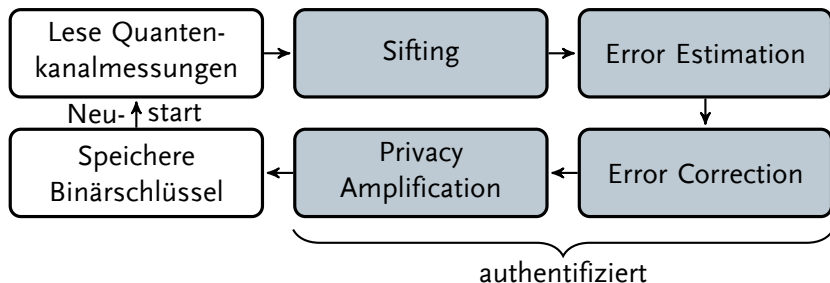


Abbildung: Flussdiagramm zum Postprocessing des Raw Key.

ÜBERSICHT ÜBER ERROR CORRECTION

- Error Estimation durch stichprobenartige Vergleiche
- Error Correction⁷ bestehend aus
 - einem stochastischem Fehler-Test **Parity Check**
 - einem Korrekturverfahren **BINARY**
 - einer Vorschrift **Cascade** zur Wiederholung der Parity Checks um die Fehlerwahrscheinlichkeit zu senken

⁷G. Brassard and L. Salvail. Advances in Cryptology EUROCRYPT '93. 1994.

PARITY

Definition

Die **Parity** einer Bitkette $D = \{D_1, \dots, D_n\}$ ist definiert als die Verknüpfung aller Bits durch XOR:

$$c(D) = \bigoplus_{i=1}^n D_i$$

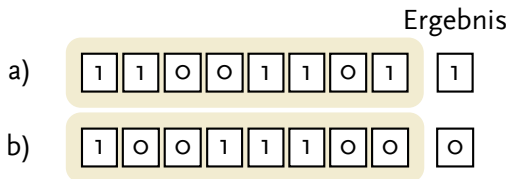


Abbildung: Beispiel für Parity Berechnung



BINARY KORREKTURVERFAHREN

Parity Bit von Alice

Alice

1 1 0 1 1 0 1 0 0 0 1 0 1 1 0 0

Bob

1 1 0 1 1 1 1 0 0 0 1 1 0 1 0 0

1 1 0 1 1 1 1 0

1 1 1 0

1 1

1

1

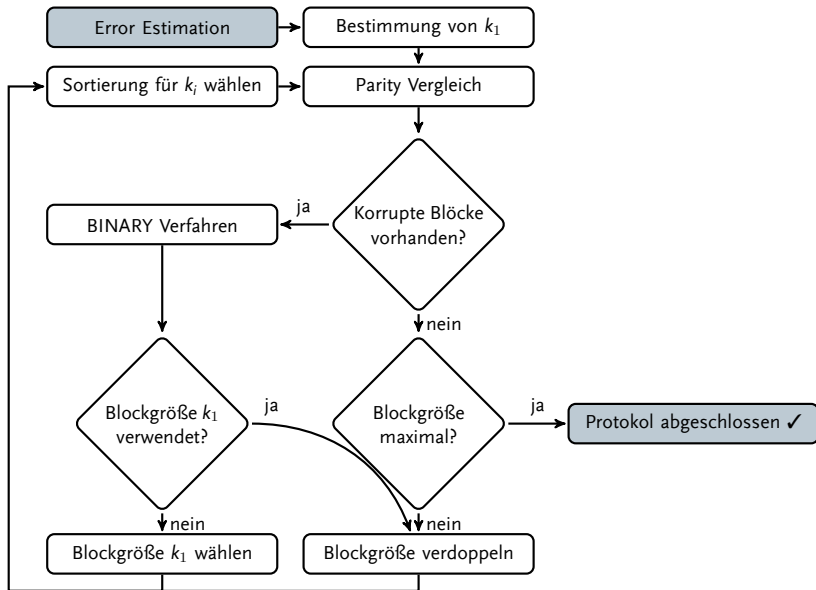
1

1

Abbildung: Ablauf-Schema des Korrekturverfahrens BINARY



CASCADE ALGORITHMUS ZUR FEHLERKORREKTUR



PRIVACY AMPLIFICATION

Nach der Schlüsselkorrektur

Schlüssel nur partiell geheim, da

- Parity-Austausch bei Error Correction Teilinformationen offenlegt
- Eve in reallem Experiment endliche Wahrscheinlichkeit hat unerkannt Schlüsselteile zu messen

Definition

Das Destillieren eines hochsicheren Schlüssels aus einem längeren, weniger sicheren Schlüssel wird **Privacy Amplification** genannt.



VORGEHENSWEISE BEI DER PRIVACY-AMPLIFICATION

- maximale öffentliche Information über den Schlüssel in bit:

$$t = 2 \cdot n \cdot p + n_{\text{parity}}$$

- n : Schlüssellänge in Bit nach Sifting u. Fehlerabschätzung
 - p : experimentell ermittelte Übertragungsfehlerrate pro Bit
 - n_{parity} : Anzahl übertragener Parity-Bits für Fehlerkorrektur
- Kompression via $g : \{0, 1\}^n \rightarrow \{0, 1\}^r$, mit $r = n - t - s$
 - s : Sicherheitsparameter
 - spezielle Wahl der Funktionen-Klasse für g
 - Kompressionsfunktion wird zufällig bestimmt



ALMOST-STRONGLY UNIVERSAL₂ HASH-FUNKTIONEN

Spezielle Klasse(n) von Funktionen \mathbb{H} , die:

- eine Menge \mathbb{M} auf eine Menge Token \mathbb{T} ($|\mathbb{T}| \leq |\mathbb{M}|$) abbildet
- nur wenige Funktionen umfassen und daher effizient sind
- genügend Funktionen umfassen um Vorhersagen fast unmöglich zu machen
- Kriterien der **Unconditional Security** erfüllt:
Sicherheit skaliert mit $\propto 2^{-s}/\ln 2$, mit Sicherheitsparameter s

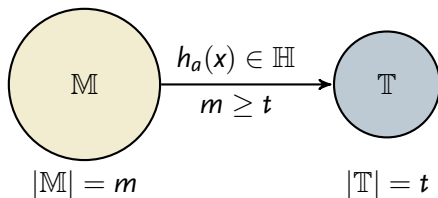


Abbildung: a -te Hash Funktion aus \mathbb{H}

AUTHENTIFIZIERUNG

- Authentifizierung sämtlicher öffentlicher Kommunikation und somit Absicherung gegen **Man in the middle**-Angriffe
- Validierung durch Token, die durch Kompression mittels **Almost-Strongly Universal₂ Hash-Funktionen** erzeugt werden


$$g_a(\text{Postprocessing-Daten}) = \text{Token}, \quad a \text{ Schlüssel}$$

- Auswahl der Kompressions-Funktionen durch vorab geteilten privaten Schlüssel a !
 ⇒ **Quantum Key Growing (QKG)** Verfahren statt **QKD**
- Sicherheit skaliert mit Tokenlänge



IMPLEMENTIERUNG DER SOFTWARE

Postprocessing

- vollst. Implementierung des Postprocessing-Stacks inkl. Authentifizierung
- Klassische Kommunikation mit TCP/IP
- Austauschformat: binäre Dateien
- für: Linux, Mac, Windows (und Embedded Devices)
- verwendet  Bibliothek, <http://qt-project.org>

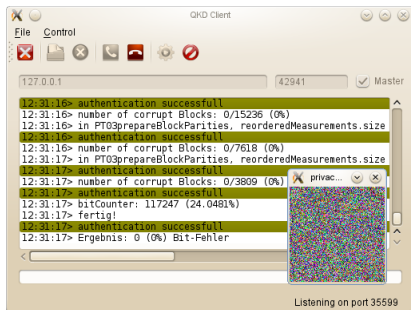
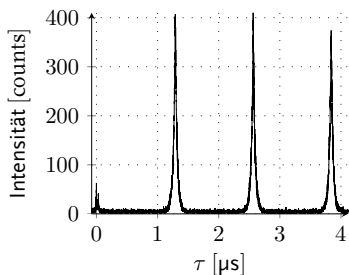
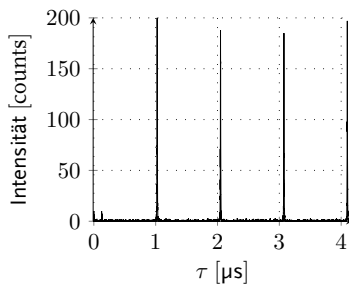


Abbildung: QKD Client nach Postprocessing

MESSERGEBNISSE

Abbildung: $g^{(2)}$ -Fkt. NV FarbzentrenAbbildung: $g^{(2)}$ -Fkt. SiV Farbzentren

	$f_{\text{[Hz]}}$ [kHz]	p_{error} [%]	raw rate [1/ks]	$q_{\text{conversion}}$ [%]	q_{used} [%]	sec. rate [1/ks]
NV	1000	$3,0 \pm 0,1$	4,32	64,0	$1,4 \pm 0,4$	2,77
NV	800	$3,2 \pm 0,1$	3,35	66,0	$1,5 \pm 0,4$	2,21
SiV	1000	$3,3 \pm 0,1$	1,57	65,8	$3,5 \pm 1,0$	1,03

Tabelle: Auswertung der Messungen



VERBESSERUNGEN

Verbesserungen des experimentellen Aufbaus

- strikte Trennung von Sender (Alice) und Empfänger (Bob)
- Miniaturisierung durch eigenes FPGA-Board (Arbeit von Georg)
- Verwendung einer Glasfaser-Verbindung (Time-Bin-Encoding⁸)
- höhere Datenübertragungsrate

Verbesserungen des Postprocessings

- Optimierung der TCP/IP Bandbreitennutzung
- Implementierung von **Adaptive Cascade** zur Effizienzsteigerung

⁸P. D. Townsend et al. Electron. Lett, 29(7):634–635, April 1993.

Vielmals danke ich denjenigen, die mich und meine Arbeit unterstützt haben. Insbesondere:

- Marcel G. (Praktikant; Projekt Messdatensimulation)
- Tim Schröder (Messaufbau)
- Valentin Métillon (Praktikant; Messaufbau, Messung)
- Friedemann G. (Einzelphotonenquelle, Messaufbau, Messung)
- Matthias Leifgen (Betreuung)

KRYPTOGRAPHIE

Definition

Kryptographie ist die Wissenschaft, die sich allgemein mit dem Thema Informationssicherheit, also der Konzeption, Definition und Konstruktion von Informationssystemen befasst, die widerstandsfähig gegen unbefugtes Lesen und Verändern sind.⁹

Die **Quantenkryptographie** vereinigt Elemente der klassischen Kryptographie mit den inherenten quantenmechanischen Eigenschaften.

⁹<http://de.wikipedia.org/wiki/Kryptographie?oldid=113655328>

EINSATZGEBIETE KLASSISCHER KRYPTOGRAPHIE

- Authentifizierung von digitalen Nachrichten (z.B. Finanztransaktionen)
- Abhörsichere Kommunikation (z.B. diplomatische Korrespondenz)
- Internet (Onlinebanking, Chat, Skype, etc.)



PROBLEMATIK KLASSISCHER KRYPTOGRAPHIE

Symmetrische Kryptographie

- privater Schlüssel muss zuvor getauscht werden
- unconditional security beweisbar, z.B. One-Time Pad
- kaum eingesetzt

Asymmetrische Kryptographie

- privater Schlüsseltausch unnötig
- Sicherheit abhängig von fehlendem Existenzbeweis für unumkehrbare Funktionen
- im Praxiseinsatz



IMPLEMENTIERUNG DER SOFTWARE I

Quantenkanalmessungen

- computergestützte Steuerung sämtlicher Hardware
- SmarAct-USB-Interface für Einzelphotonenquelle
- FPGA-PCI-Karte für Laser, EOM, APD
- Programmierung mit LabVIEW

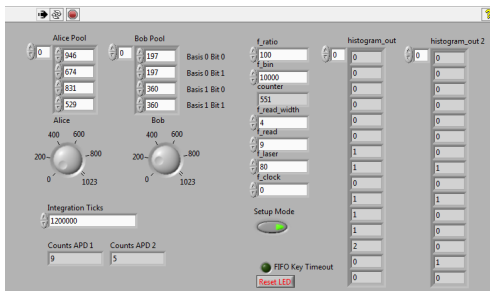


Abbildung: FPGA Software GUI

IMPLEMENTIERUNG DER SOFTWARE II

Daten-Evaluation

- Software zur Messdaten-Verifikation
- Bestimmung der Fehlerrate
- Synthetisierung von Messdaten aus echten Zufallszahlen (Arbeit von Marcel G.)

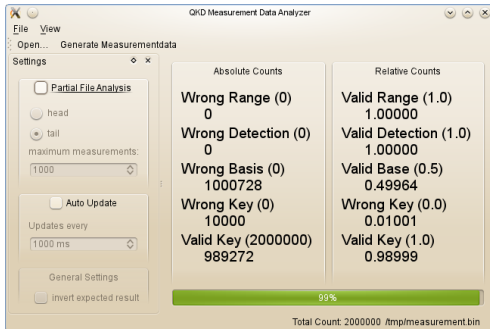


Abbildung: Measurement Analyzer



ABNAHME DER SCHLÜSSELLÄNGE

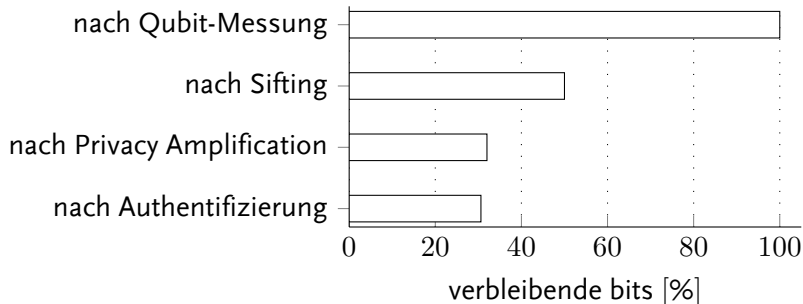
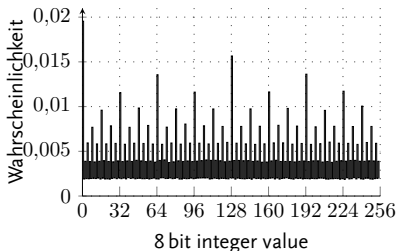
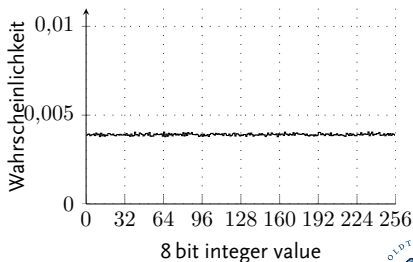


Abbildung: Abnahme der Schlüssellänge nach Messung. Es verbleiben nach der Authentifizierung schließlich 31 %.

SIMULATION ZUR HASH-FUNKTION

Hash-Funktion

$$\mathcal{H} = \{g_c : x \rightarrow [(c \cdot x) \bmod 2^r] \in \{0, 1\}^r \mid x, c \in \{0, 1\}^n, c \text{ ungerade}\}$$

Abbildung: c ist beliebigAbbildung: c ist ungerade