Über Informationstheoretische Sicherheit: Aktuelle Probleme und Lösungen

Stefan Rass

Institut für Angewandte Informatik, Forschungsgruppe Systemsicherheit
Universität Klagenfurt
Universitätsstrasse 65-67, 9020 Klagenfurt, Österreich
stefan.rass@uni-klu.ac.at

Abstract: In dieser Arbeit stellen wir Lösungsvorschläge für zwei ausgewählte Probleme der praktischen Quantenkryptographie vor. Im Kontext von quantenkryptographischem Schlüsselaustausch (QKD) präsentieren wir eine Verbesserung des klassischen Ansatzes zur Fehlerkorrektur für QKD. Darüber hinaus entwickeln wir eine entscheidungstheoretische Bewertung der Ende-zu-Ende-Sicherheit in Quantennetzwerken, und stellen einen Konnex zur Informationstheorie nach Shannon her. Die hier vorgestellten Konzepte ermöglichen auch ein Design von Quantennetzwerken mit maximaler Sicherheit. Wir zeigen, dass dieses Problem im Allgemeinen NP-hart ist.

1 Einführung

Das Konzept der informationstheoretischen Sicherheit wurde von C.E. Shannon eingeführt [Sha49], um auf statistischem Weg die Stärke einer Verschlüsselung quantitativ bewerten zu können. Die Grundidee hierbei liegt in der Forderung, dass aus dem Chiffrat weder den Klartext, noch Wahrscheinlichkeiten für bestimmte Klartexte ableitbar sein sollen, die nicht schon vorher bekannt waren. In Form bedingter Wahrscheinlichkeiten formuliert bedeutet dies, dass für einen beliebigen Klartext M_i und das abgefangene Chiffrat C die Bedingung $P(M_i|C) = P(M_i)$ notwendig ist für eine perfekt sichere Verschlüsselung. Anders ausgedrückt, ein möglicher Klartext M_i ist stets gleich wahrscheinlich, egal ob das Chiffrat C bekannt ist oder nicht.

Shannon bewies, dass die Vernam-Chiffre (besser bekannt als One-Time-Pad) diese Eigenschaft besitzt. Eine praktikable Umsetzung des Verfahrens gelingt durch das im Jahre 1984 von C. Bennett und G. Brassard [BB84], nach Vorarbeiten von S. Wiesner [Wie83], vorgeschlagene Protokoll BB84, heute bekannt als *quantenkryptographischer Schlüsselaustausch* (quantum key distribution oder kurz QKD). Anders als Übertragungsverfahren, welche auf elektromagnetischen oder Laser-Impulsen beruhen, wird die Information beim BB84-Protokoll in die Polarisationsebene einzelner Lichtteilchen codiert. Da diese aufgrund ihrer physikalischen Eigenschaften nicht störungsfrei kopierbar sind (*no-cloning theorem* [WZ82]), führen Abhörversuche im Allgemeinen zu einer erkennbaren Erhöhung der Fehlerrate und damit zum Abbruch der Kommunikation. Ein formaler Beweis der Si-

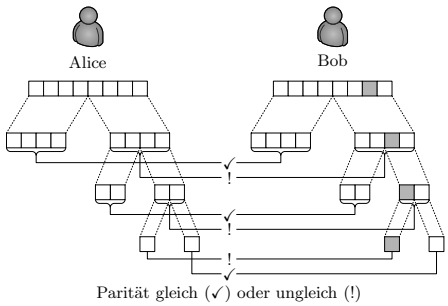

Abbildung 1: Finden von Bitfehlern durch Paritäts-Vergleiche und binäre Suche

cherheit des BB84 Protokolls wird in [SP00] gegeben. Alternative Verfahren (beispielsweise das auf verschränkten Photonen beruhende Protokoll von A. Ekert [Eke91]) existieren, werden hier aber nicht weiter behandelt. Es sei an dieser Stelle jedoch festgehalten, dass Sicherheitsbeweise für QKD im Allgemeinen nur für direkte Verbindungen, jedoch nicht für Kanäle mit Zwischenknoten (Repeatern) geführt werden.

Obgleich die theoretischen Aspekte der Quantenkryptographie in den letzten Jahrzehnten gut erforscht wurden, und sowohl experimentelle [PPM08, ECP$^+$05] als auch kommerzielle Umsetzungen (http://www.idquantique.com/, http://www.magiqtech.com/) existieren, bringt der praktikable Einsatz der Technologie eine Reihe von technischen Schwierigkeiten mit sich. Wir behandeln in dieser Arbeit zwei ausgewählte Probleme: *Fehlerkorrektur* und *Ende-zu-Ende-Sicherheit* in Quantennetzwerken.

2 Adaptive Fehlerkorrektur

Betrachten wir exemplarisch einen Schlüsselaustausch auf Basis des BB84 Protokolls, so findet der Informationsaustausch auf zwei logisch (nicht notwendigerweise physikalisch) getrennten Kanälen statt: der (abhörsichere) Austausch einer Folge polarisierter Photonen geschieht auf dem Quantenkanal (Lichtwellenleiter oder freier Raum). Auf dem klassischen Kanal (herkömmliche und nicht notwendig sichere Netzwerkverbindung) wird aus dem gemessenen Photonenstrom interaktiv zwischen den Teilnehmern ein gemeinsamer geheimer Schlüssel abgeleitet. Naturgemäß treten bei der Übertragung und Detektion der Photonen Fehler auf. Der so entstandene Rohschlüssel muss daher vor der weiteren Verwendung korrigiert werden. Das hierfür traditionell eingesetzte Verfahren wurde in [BBB$^+$92] erstmalig vorgeschlagen und in [BS93] weiterentwickelt. Es beruht auf dem (öffentlichen) Vergleich von Block-Paritäten in Kombination mit einer Binär-Suche um einen Einzelbitfehler innerhalb von n bit in $\mathcal{O}(\log n)$ Schritten zu korrigieren.

Der Vorgang ist in vereinfachter Form in Abbildung 1 dargestellt und arbeitet optimal, falls pro Block höchstens 1 Fehler auftritt. Dies versucht man durch (wiederholte) Permutationen der Bits und hinreichend kleine Blockgrößen zu erreichen. Das gesamte Verfahren ist bekannt unter dem Namen *Cascade-Fehlerkorrektur*. Eine praktische Umsetzung wirft

wenigstens zwei Fragen auf:

1) Welches ist die optimale Blockgröße?
2) Wie kann gesichert werden, dass pro Block höchstens 1 Fehler auftritt?

Ein Beitrag dieser Arbeit ist ein stochastisches Modell für die optimale Wahl der Blockgröße, sowie ein Verfahren um diese Größe dynamisch in Abhängigkeit von variablen Umweltbedingungen anzupassen.

2.1 Fehler-Verteilungsmodell

Wir betrachten die Fehleranzahl als Poisson-verteilte Zufallsvariable und modellieren den Prozess des Auftretens von Fehlern in langen Bitstrings als Poisson-Prozess: es bezeichne λ die (vorerst konstante) Fehlerrate pro Zeiteinheit, und es mögen für die Fehleranzahl $N(t)$ zum Zeitpunkt t folgende Bedingungen gelten: (i) $N(0) = 0$ (keine Fehler zu Beginn), (ii) in zwei disjunkten Intervallen ist die Fehleranzahl stochastisch unabhängig, und (iii) $N(t + \Delta t) - N(t) \sim \text{Po}(\lambda \Delta t)$, d.h. die Anzahl der Fehler in einem Intervall der Länge Δt ist Poisson-verteilt mit einem zu Δt proportionalen Intensitäts-Parameter. Unter diesem Modell können wir, für eine Übertragungsrate von f qubit pro Sekunde und einer Blockgröße von $\approx f/\lambda$, im Mittel einen Fehler pro Block erwarten. Dies bestätigt die von den Erfindern des Cascade-Verfahrens [BBB$^+$92] vorgeschlagene Heuristik auf mathematischem Weg.

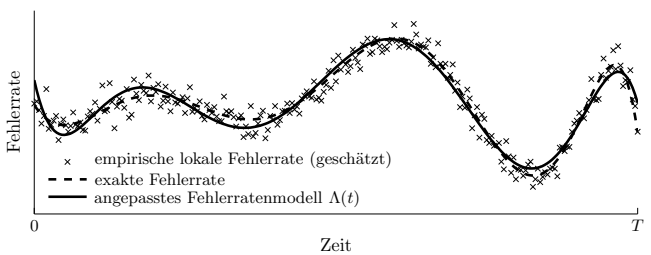

Abbildung 2: Lokale Fehlerraten und angepasstes Fehlerratenmodell

Eine erste Verallgemeinerung des Ansatzes kann durch zeitabhängige Fehlerraten $\Lambda(t)$ erreicht werden. Nehmen wir an, dass die Fehlerrate, wie in Abbildung 2 dargestellt, (periodischen) Schwankungen unterliegt (durchgezogene Linie) und, dass empirische Daten über die aufgetretenen Fehler vorliegen (beispielsweise aus früheren Ausführungen des Protokolls). Dann können wir den konstanten Parameter λ durch eine zeitabhängige Funktion $\Lambda(t)$ ersetzen, was zu einem inhomogenen Poisson-Prozess führt. Wählen wir $\Lambda(t) \in \text{span}(f_1, \ldots, f_n)$, d.h. wir setzen $\Lambda = \sum_{i=1}^{n} \mu_i f_i = \mu^T f$ mit Basisfunktionen $f_1, \ldots, f_n : \mathbb{R} \to \mathbb{R}$ an (zumeist Polynome), so können die Werte $\mu_1, \ldots, \mu_n$ durch Least-Squares-Schätzung ermittelt werden. Unter der Annahme normalverteilter Residuen ist die Schätzung optimal (Gauss-Markov-Theorem). Der Aufwand zur Schätzung von $\Lambda(t)$

(d.h. die Berechnung von μ) liegt in $\mathcal{O}(n^3)$, aufgrund der Bestimmung der Pseudoinversen der Design-Matrix $A = (f_j(x_i))_{i,j}$ (wobei x_i hier die empirische lokale Fehlerrate zum Zeitpunkt t_i bezeichnet) für die Lösung der entstehenden Normalgleichungen. Die effiziente Aktualisierung von $\Lambda(t)$ auf Basis weiterer (neuer) Daten kann mit der Formel von Sherman und Morrison [SM50] und dem Aufwand $\mathcal{O}(n^2)$ erfolgen.

Zu einer weiteren Verallgemeinerung gelangt man bei Ersetzung der deterministischen Funktion $\Lambda(t)$ durch eine Zufallsvariable Λ mit bekannter Verteilung. Experimentelle Untersuchungen [LKS+09] haben die Normalverteilung, sowie die Gamma-Verteilung als probate Kandidaten ausgewiesen. Wählt man die Gamma-Verteilung mit den Parametern $a, b > 0$ als Modell, so erhalten wir eine Poisson-Verteilung mit Gamma-verteiltem Intensitätsparameter. Der Satz über die totale Wahrscheinlichkeit liefert dann unmittelbar die Verteilungsdichte der Fehleranzahl X pro Zeiteinheit als

$$\mathsf{P}[X = k] = \frac{b^a \Gamma(k+a)}{k!(b+1)^{k+a}\Gamma(a)},$$

mit dem Erwartungswert $\mathsf{E}(X) = a/b$. Die zugehörige Verteilungsfunktion besitzt eine "geschlossene" Darstellung durch die hypergeometrischen Funktion, als

$$\mathsf{P}[X > m] = \frac{b^a (a)_{m+1}}{(m+1)!(b+1)^{a+m+1}} \cdot {}_2F_1\left(\begin{matrix}1, m+a+1 \\ m+2\end{matrix} \;\middle|\; \tfrac{1}{b+1}\right).$$

Angewendet auf die im Cascade-Verfahren verwendeten Paritäts-Vergleiche liefern diese Formeln direkt die Wahrscheinlichkeit für das tatsächliche Aufdecken von Fehlern. Bitfehler werden genau dann erkannt, wenn ihre Anzahl ungerade ist. Damit folgt aus den obigen Formeln:

$$\mathsf{P}[\text{Fehler werden entdeckt}] = \mathsf{P}[X \text{ ist ungerade}] = \frac{1}{2}\left[1 - \left(\frac{b}{b+1}\right)^a\right].$$

Die Beweise der obigen Formeln finden sich in [Ras09]. Als Anwendung des Modells ergibt sich unmittelbar eine Möglichkeit, die Interaktion aus dem Fehlerkorrekturverfahren zu eliminieren. Unter der Annahme der Richtigkeit des Fehlerratenmodells kann die Wahrscheinlichkeit für mehr als m Fehler hinreichend klein gemacht werden, und ist es möglich klassische fehler-korrigierende Codes sinnvoll einzusetzen. Die zugehörige mathematische Analyse wurde in [RS10] ausgeführt.

2.2 Experimentelle Auswertung

Abbildung 3 stellt die empirischen Fehlerraten bei fester Blockgröße (herkömmliche Cascade-Fehlerkorrektur) und dynamischer Blockgröße (inhomogener Poisson-Prozess) einander gegenüber. Die simulierten Fehlerraten wurden durch ein bewusst falsch gewähltes Fehlermodell approximiert; siehe Abbildung 2 (in einer realen Anwendung wäre der reale Fehlerprozess im Hintergrund ebenso unbekannt). Eine deutliche Konzentration der Wahrscheinlichkeitsmasse auf der linken Seite zeigt den Gewinn bei Einsatz dynamischer Blockgrößen gegenüber statischen Blockgrößen und steigert die Effizienz der Fehlerkorrektur erheblich.

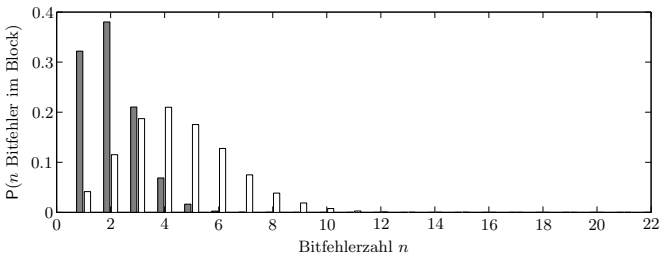

Abbildung 3: Wahrscheinlichkeiten für Bitfehler in einem Block bei statischer Blockgröße (weiß) und dynamischer Blockgröße (grau)

3 Ende-zu-Ende Sicherheit in Quanten-Netzwerken

Aufgrund physikalischer Eigenschaften der zur Übertragung eingesetzten Photonen ist die Reichweite von QKD beschränkt (aktuell auf etwa 144km [SMWF$^+$07]). Dies erfordert den Einsatz von Zwischenknoten für die Übertragung (vgl. Abbildung 4). Die (sichere) Umschlüsselung in als vertrauenswürdig angenommenen Zwischenknoten ist bekannt als *trusted-node model* bzw. *trusted relay*, und bildet die Grundlage realer Quantennetzwerke, wie beispielsweise in [ABB$^+$07] spezifiziert. Die Sichtbarkeit des Klartextes in jedem Zwischenknoten erlaubt dem Angreifer, seine Bemühungen auf den Knoten zu konzentrieren, sodass ein Angriff auf den quantenkryptographischen Schlüsselaustausch, egal ob theoretisch ausgeschlossen oder nicht, de facto nicht mehr erforderlich ist. Formale Beweise für Ende-zu-Ende Sicherheit auf Basis von QKD existieren bislang kaum. Jüngere Forschungsergebnisse [WD08, AKGSPR02] haben belegt, dass (unabhängig von QKD) letztlich die Netzwerktopologie über die Möglichkeit und insbesondere Unmöglichkeit von perfekt sicherer Kommunikation entscheidet. Es wurde in [WD08, AKGSPR02] bewiesen, dass Mehrwegeübertragung eine *notwendige* Maßnahme für nicht abhörbare Kommunikation ist. Grob gesprochen stellen wir damit an die Netzwerktopologie die Forderung, dass zwischen beliebigen Knoten stets wenigstens zwei oder mehr knoten-disjunkte Pfade existieren müssen, um Angriffe erfolgreich abwehren zu können. Wir präsentieren hier einige Erweiterungen dieser Ergebnisse, welche analoge Aussagen über beliebige Netzwerke zulassen.

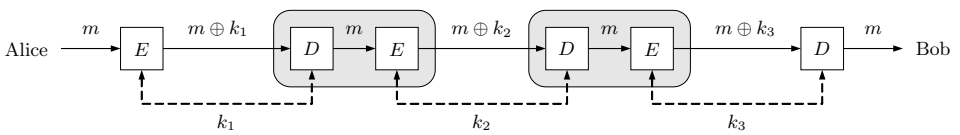

Abbildung 4: Übertragung mit trusted relay

3.1 Das Konzept der Verwundbarkeit

Wir setzen die Netzwerktopologie als bekannt voraus und bezeichnen das zugehörige Graph-Modell mit $G = (V, E)$. Darüber hinaus seien in dem Netzwerk vielfältige weitere Sicherheitsmechanismen im Einsatz, wie Firewalls, Intrusion-Detection-Systeme und ähnliche. Einige Protokolle (z.B. SSL) beinhalten eine Phase, in welcher Protokollparameter vereinbart werden. Wir nehmen an, dass im Laufe dieser Phase die Endstellen auch die Übertragungswege (potentiell mehrere) festlegen und bezeichnen die Menge der möglichen Konfigurationen (einschließlich der Übertragungswege) als PS_1. Der Angreifer verfügt über unbeschränkte Rechenleistung (wir treffen also keine in der klassischen Kryptographie üblichen komplexitätstheoretischen Einschränkungen), kann aber nur eine bestimmte Menge von Komponenten (bzw. ganze Teilsysteme) angreifen. Diese Menge bezeichnen wir mit PS_2. Sie entspricht einer Angreifer-Struktur im Kontext von allgemeinem Secret-Sharing.

Für jede mögliche Konfiguration $s_1 \in PS_1$ und jedes Angriffsszenario $s_2 \in PS_2$ bewerten wir den Erfolg der Übertragung. Zu diesem Zweck wählen wir eine (beliebige) Taxonomie $\mathcal{I}$ zur Bewertung von Sicherheit (beispielsweise CVSS [HF09, MS07] oder das in [IOB09] vorgeschlagene Verfahren) und weisen jeder Kombination (s_i, s_j) eine numerische Bewertung $u(s_i, s_j)$ zu, welche den Grad des Erfolges der Kommunikation ausdrückt. Findet diese Bewertung in Form von Wahrscheinlichkeiten statt (wenn z.B. Intrusion-Detection Systeme, Firewalls oder Virenscanner mit bekannter empirischer Erkennungsrate eingesetzt werden), so kann $\mathcal{I} = [0, 1]$ gesetzt werden. In dem Fall bezeichnet $u(s_i, s_j)$ die Wahrscheinlichkeit, dass die Übertragungsstrategie s_i dem Angriff nach der Strategie s_j erfolgreich standgehalten hat. Im Folgenden verwenden wir $\mathcal{I} = \{0, 1\}$, wobei $u(s_i, s_j) = 1$ eine erfolgreiche Übertragung bezeichnet, und $u(s_i, s_j) = 0$ einen erfolgreichen Angriff modelliert. Diese Wahl ist geeignet für Anwendungen, in denen keine sinnvolle fein-granulare Erfolgs-Bewertung vorgenommen werden kann oder soll.

Um zu einer quantitativen Bewertung der Verwundbarkeit eines Netzwerkes zu gelangen, fassen wir die Matrix $A \in \mathcal{I}^{|PS_1| \times |PS_2|}$ mit den Einträgen $a_{ij} = u(s_i, s_j) \in \mathcal{I}$ als Nullsummenspiel auf, mit der Intuition, unseren erwarteten Erfolg (gemessen in der Skala $\mathcal{I}$) bei frei wähl- und wechselbaren Konfigurationen zu maximieren. Das Nullsummenspiel bringt zwei praktische Vorteile: es ist ein gültiges Worst-Case-Modell [Ras09, Lem.5.3.9] und erspart es eine weiterführende Modellierung des Angreifers, insbesondere seiner genauen Absichten. Bezeichnen wir das durch A induzierte Nullsummenspiel mit $\Gamma(A)$, und schreiben wir weiter $v(\Gamma(A))$ für den Sattelpunktwert des Spiels [Sch04], so bezeichnen wir die Größe $\rho(A) := \max \mathcal{I} - v(\Gamma(A))$ als *Verwundbarkeit* des Systems. Die Bestimmung von ρ erfordert die Berechnung der Matrix A und die Lösung eines linearen Optimierungsproblems zur Bestimmung von $v(\Gamma(A))$. Beide Vorgänge erlauben eine weitgehende Automatisierung und sind effizient durchführbar.

3.2 Anwendungen in der Informationstheorie und der Kryptographie

Die Verwundbarkeit ρ eines Systems besitzt eine Reihe bemerkenswerter Eigenschaften: so wird beispielsweise im Sinne der Common Criteria das Risiko eines Systems als das Produkt von potentiellem Schaden und der zugehörigen Auftrittswahrscheinlichkeit verstanden. Die Verwundbarkeit ρ spiegelt diese Definition fast unmittelbar wieder, wobei ρ die Differenz zwischen dem Best-case und dem tatsächlichen Ereignis ausdrückt. Im entscheidungstheoretischen Sinne [Rob01] ist das Risiko definiert als erwarteter Verlust. Da wir durch $v(\Gamma(A))$ den mittleren Nutzen definieren, entspricht ρ also einer Risikoabschätzung. Dies lässt sich auch formal beweisen, in Form von

Satz 3.1 ([Ras09, Thm.5.3.16]) *Für das (entscheidungstheoretische) Risiko r bei einer Kommunikation, gemessen im Sinne der Taxonomie $\mathcal{I}$, gilt $0 \leq r \leq \rho(A)$, wobei das aus dem durch A induzierten Nullsummenspiel abgeleitete Nash-Gleichgewicht als Verhaltensstrategie für Alice und Bob vorausgesetzt wird. Der Angreifer kann hierbei seine Verhaltensstrategie beliebig wählen.*

Als unmittelbare Konsequenz dieses Satzes ergibt sich eine Möglichkeit die bei einer Übertragung austretende Information zu quantifizieren. Der folgende Satz zeigt den Bezug der Ergebnisse zur Informationstheorie nach Shannon und hat unmittelbare Anwendungen in der Quantenkryptographie, da er Aussagen über die Qualität der Ende-zu-Ende-Verschlüsselung in einem Quantennetzwerk gestattet. Dies geht über die bisherigen Ergebnisse über Quanten-Punkt-zu-Punkt-Verbindungen hinaus.

Satz 3.2 ([Ras09, Cor.5.3.20]) *Es sei Alice eine Nachrichtenquelle mit Entropie $H(M)$, und die Zufallsvariable C das übertragene Chiffrat. Dann gilt für die Transinformation $I(C;M)$ die Abschätzung $I(C;M) \leq \rho(A) \cdot H(M)$.*

Interpretiert man $I(C;M)$ als die Reduktion der Unsicherheit über den Klartext M bei Abfangen des Chiffrats C, so stellt Satz 3.2 eine direkte Verbindung zwischen der Verwundbarkeit und der informationstheoretischen Sicherheit her.

Die Verwundbarkeit $\rho(A)$ ist kompatibel mit den in [WD08] vorgestellten Sicherheitskonzepten: wir nennen eine Übertragung *δ-zuverlässig*, wenn die Wahrscheinlichkeit eines Ausfalls $\leq \delta$ ist. Analog nennen wir eine Übertragung *ε-privat*, wenn die zu zwei verschiedenen zufälligen Klartexten gehörenden Chiffrate Wahrscheinlichkeitsverteilungen mit dem L_1-Abstand $\leq \varepsilon$ besitzen. Es kann gezeigt werden, dass für die Taxonomie $\mathcal{I} = \{0,1\}$ und bekannter Verwundbarkeit ρ ein Protokoll existiert, welches ρ-zuverlässig und 2ρ-privat ist (Satz 5.3.21 in [Ras09]).

Die Verwundbarkeit liefert auch direkt Aussagen darüber, ob eine perfekt abhörsichere Kommunikation in einem Netzwerk überhaupt möglich ist. Es gilt

Satz 3.3 ([Ras09, Thm.5.3.34]) *Für $\mathcal{I} = \{0,1\}$ und die Verwundbarkeit $\rho(A)$ gilt: Falls $\rho(A) < 1$, so existiert für jedes $\varepsilon > 0$ ein Protokoll welches ε-privat ist. Ist $\rho(A) = 1$, so ist die Erfolgswahrscheinlichkeit für einen Angriff gleich 1.*

3.3 Sicherheit als Optimierungsproblem

Die Verwundbarkeit kann als Zielfunktion für ein optimales Netzwerkdesign eingesetzt werden. Betrachten wir der Einfachheit halber ein Netzwerk $G = (V, E)$ welches wir durch zusätzliche Verbindungen $\widetilde{E} \subset E'$ erweitern möchten, wobei E' hierbei die Menge der sinnvollen Kanten-Erweiterungen von G bezeichnet. Wir möchten die Verwundbarkeit für jedes kommunizierende Paar von Teilnehmern minimieren. Das erweiterte Netzwerk bezeichnen wir mit $G(V, E \cup \widetilde{E})$. Die Zielfunktion für das Optimierungsproblem ist $R(U, (V, E \cup \widetilde{E})) := \max_{s,t \in U, s \neq t} \rho(A(s,t))$, wobei U die Menge von potentiellen Kommunikationspartnern bezeichnet und $A(s,t)$ die für den Sender s und Empfänger t spezifische (Spiel-)Matrix A (vgl. Abschnitt 3.1) ist. Das sich ergebende (nicht-lineare) Optimierungsproblem lautet

$$\left.\begin{array}{rc} & \min_{\widetilde{E} \subseteq E'} R(U, (V, E \cup \widetilde{E})) \\ \text{unter der Nebenbedingung} & c(\widetilde{E}) \leq M, \end{array}\right\} \tag{1}$$

wobei $c : \mathcal{P}(E') \to \mathbb{R}^d, M \in \mathbb{R}^d, d \geq 1$ die Kosten für Erweiterungen misst ($\mathcal{P}(E')$ ist die Potenzmenge von E'). Der Fall $d > 1$ modelliert die Unterscheidung verschiedener Kostentypen (Aufbau, Wartung, Personal, etc.). Durch eine Reduktion des 0-1-Integer-Programming Problems auf die Optimierungsaufgabe (1) erhalten wir

Satz 3.4 ([Ras09, Thm.6.3.4]) *Das Optimierungsproblem* (1) *ist NP-hart.*

4 Resümee

Quantenkryptographie gilt als Schlüsseltechnologie der kommenden Jahrzehnte. Ihr Einsatz erfordert die Neu-Konzeption einer Reihe bestehender Verfahren, jedoch konzentriert sich ein signifikanter Teil der Forschung auf die Umsetzung von Hardware und die Sicherheit von Punkt-zu-Punkt Verbindungen. In dieser Abhandlung wurden Lösungsvorschläge für zwei praktische Probleme beim Einsatz von QKD vorgestellt: mangelnde Effizienz und fehlende Ende-zu-Ende Sicherheit. Eine Steigerung der Effizienz kann kann durch adaptive Fehlerkorrekturverfahren erreicht werden. Der hier vorgestellte dynamische Ansatz kann mit lernfähigen statistischen Modellen (Bayes'schen Netzwerken) kombiniert werden, um selbst-kalibrierende Systeme zur Fehlerkorrektur zu erhalten. Dies reduziert den Wartungsaufwand bei den Endgeräten und verringert damit das Risiko eines Angriffs.

Die hier vorgestellte Sicherheitsbewertung für Ende-zu-Ende-Sicherheit in Quantennetzwerken ist ein allgemeines Konzept, dessen Anwendung *nicht* auf Quantenkryptographie oder reine Abhörsicherheit beschränkt ist. Die Verwundbarkeit kann in gleicher Weise auch für Denial-of-Service Angriffe definiert und berechnet werden, und liefert dann analoge Aussagen zu den hier Angegebenen (Details sind in [Ras09] zu finden). Das Konzept der Verwundbarkeit ist eng verwandt mit der topologischen Verwundbarkeitsanalyse [JNO05], jedoch in seiner Anwendung, insbesondere beim Design von Netzwerken, erheblich einfacher als andere Vorschläge (siehe beispielsweise [ARDL09]). Ein besonderer

Vorteil liegt in der natürlichen Kompatibilität mit der Begriffswelt des jeweiligen Einsatzszenarios, welche durch die Wahl der Taxonomie $\mathcal{I}$ frei festgelegt wird. Hiermit eröffnet sich auch für Nicht-Experten ein einfacher Zugang zu einer Technologie, welche mathematisch bewiesene Sicherheit für geheime Kommunikation bietet. Quantenkryptographie bleibt somit nicht länger ein Objekt der Überlegungen hochqualifizierter Physiker und Kryptographen, sondern kann von Entscheidungsträgern mit beliebigem fachlichen Hintergrund sinnvoll und erfolgreich eingesetzt werden.

Danksagung: Der Autor dankt Prof. Horster für wertvolle Diskussionen und Anregungen, welche wesentlich zur Entwicklung der vorgestellten Konzepte beigetragen haben.

Literatur

[ABB+07] R. Alléaume, J. Bouda, C. Branciard, T. Debuisschert, M. Dianati, N. Gisin, M. Godfrey, P. Grangier, T. Länger, A. Leverrier, N. Lütkenhaus, P. Painchault, M. Peev, A. Poppe, T. Pornin, J. Rarity, R. Renner, G. Ribordy, M. Riguidel, L. Salvail, A. Shields, H. Weinfurter und A. Zeilinger. SECOQC White Paper on Quantum Key Distribution and Cryptography, 2007.

[AKGSPR02] M.V.N. Ashwin Kumar, P. R. Goundan, K. Srinathan und C. Pandu Rangan. On perfectly secure communication over arbitrary networks. In *PODC '02: Proc. of the 21st annual symposium on Principles of distributed computing*, Seiten 193–202, New York, NY, USA, 2002. ACM.

[ARDL09] R. Alleaume, F. Roueff, E. Diamanti und N. Lütkenhaus. Topological optimization of quantum key distribution networks. *New J. of Physics*, 11:075002, 2009.

[BB84] C. Bennett und G. Brassard. Public key distribution and coin tossing. In *IEEE Int. Conf. on Computers, Systems, and Signal Processing*, Seiten 175–179, Los Alamitos, 1984. IEEE Press.

[BBB+92] C.H. Bennett, F. Bessette, G. Brassard, L. Salvail und J. Smolin. Experimental quantum cryptography. *J. of Cryptology*, 5:3–28, 1992.

[BS93] G. Brassard und L. Salvail. Secret-key reconciliation by public discussion. In *EUROCRYPT*, Seiten 410–423, 1993.

[ECP+05] C. Elliott, A. Colvin, D. Pearson, O. Pikalo, J. Schlafer und H. Yeh. Current status of the DARPA Quantum Network. arXiv:quant-ph/0503058v2, 2005.

[Eke91] A. Ekert. Quantum Cryptography Based on Bell's Theorem. *Phys. Rev. Lett. 67, No.6*, Seiten 661–663, 1991.

[HF09] S.H. Houmb und V.N.L. Franqueira. Estimating ToE Risk Level using CVSS. In *Proc. of the Int. Conf. on Availability, Reliability and Security*, Seiten 718–725. IEEE Computer Society, 2009.

[IOB09] F. Innerhofer-Oberperfler und R. Breu. An empirically derived loss taxonomy based on publicly known security incidents. In *Proc. of the Int. Conf. on Availability, Reliability and Security*, Seiten 66–73. IEEE Computer Society, 2009.

[JNO05] S. Jajodia, S. Noel und B. O'Berry. *Massive Computing*, Kapitel Topological Analysis of Network Attack Vulnerability, Seiten 247–266. Springer US, 2005.

[LKS+09] K. Lessiak, C. Kollmitzer, S. Schauer, J. Pilz und S. Rass. Statistical Analysis of QKD Networks in Real-life Environments. In *Proc. of the 3rd Int. Conf. on Quantum, Nano and Micro Technologies*, Seiten 109–114. IEEE Computer Society, February 2009.

[MS07] P. Mell und K. Scarfone. A Complete Guide to the Common Vulnerability Scoring System. `http://www.first.org/cvss/cvss-guide.pdf`, June 2007. Version 2.0 (last access: Feb. 12th, 2010).

[PPM08] A. Poppe, M. Peev und O. Maurhart. Outline of the SECOQC Quantum-Key-Distribution Network in Vienna. *Int. J. of Quantum Information*, 6(2):209–218, 2008.

[Ras09] S. Rass. *On Information-Theoretic Security: Contemporary Problems and Solutions*. Dissertation, Klagenfurt University, Institute of Applied Informatics, June 2009.

[Rob01] C.P. Robert. *The Bayesian choice*. Springer-Verlag, New York, 2001.

[RS10] Stefan Rass und Peter Schartner. Non-Interactive Information Reconciliation for Quantum Key Distribution. In *Proc. of the 24th IEEE Int. Conf. on Advanced Information Networking and Applications*, Seiten 1054–1060. IEEE Computer Society Press, 2010.

[Sch04] W. Schlee. *Einführung in die Spieltheorie*. Vieweg, 2004.

[Sha49] C.E. Shannon. Communication Theory of Secrecy Systems. *Bell System Technical J.*, 28:656–715, 1949.

[SM50] J. Sherman und W.J. Morrison. Adjustment of an inverse matrix corresponding to a change in one element of a given matrix. *Ann. Math. Statistics*, 21:124–127, 1950.

[SMWF+07] T. Schmitt-Manderbach, H. Weier, M. Fürst, R. Ursin, F. Tiefenbacher, T. Scheidl, J. Perdigues, Z. Sodnik, C. Kurtsiefer, J. Rarity, A. Zeilinger und H. Weinfurter. Experimental Demonstration of Free-Space Decoy-State Quantum Key Distribution over 144 km. *Physical Review Letters*, 98(1):010504, 2007.

[SP00] P.W. Shor und J. Preskill. Simple Proof of Security of the BB84 Quantum Key Distribution Protocol. *Phys. Rev. Lett.*, 85:441–444, 2000.

[WD08] Y. Wang und Y. Desmedt. Perfectly Secure Message Transmission Revisited. *IEEE Trans. on Information Theory*, 54(6):2582–2595, 2008.

[Wie83] S. Wiesner. Conjugate coding. *Sigact News*, 15(1):78–88, 1983. original manuscript written circa 1970.

[WZ82] W. K. Wootters und W. H. Zurek. A single quantum cannot be cloned. *Nature*, 299(802):802–803, 1982.

Stefan Rass wurde am 7. August 1980 in Klagenfurt geboren. Er studierte Informatik und Technische Mathematik (mit dem Schwerpunkt Statistik) und schloss beide Studien mit dem Grad Diplom-Ingenieur ab. Er promovierte im Fach Technische Mathematik im Jahr 2009. Zwischen 2006 und 2008 war er Mitglied der Forschungsgruppe für Verkehrsinformatik, und seit Mai 2008 ist er Assistent in der Forschungsgruppe Systemsicherheit an der Uni Klagenfurt unter der Leitung von Prof. Dr. Patrick Horster. Er war zwischen 2005 und 2008 Mitarbeiter im EU-Projekt SECOQC. Seine Forschungsinteressen umfassen Statistische Ansätze im Bereich der Kryptographie, Informationstheorie, Komplexitätstheorie und theoretische Informatik.