Security of Quantum Key Distribution

Renato Renner

Department of Applied Mathematics and Theoretical Physics
University of Cambridge
r.renner@damtp.cam.ac.uk

Abstract: Der sicheren Übertragung und Aufbewahrung vertraulicher Daten kommt in unserer von Information dominierten Gesellschaft immer grössere Bedeutung zu. Die heute gebräuchlichen Verfahren zur Datenverschlüsselung bieten allerdings nur berschränkte, so-genannt *berechenmässige*, Sicherheit. Das bedeutet, dass diese prinzipiell von einem Angreifer, der über genügend Rechenleistung (zum Beispiel einen, heute noch hypothetischen, Quantencomputer) verfügt, gebrochen werden können.

Quantenkryptographie bietet eine mögliche Alternative zu diesen klassischen Verfahren. So ermöglicht beispielsweise ein *Quantum Key Distribution (QKD)* Protokoll, einen geheimen Schlüssel sicher zwischen zwei entfernten Parteien auszutauschen. Die Sicherheit beruht dabei alleinig auf physikalischen Gesetzen — es müssen also, im Gegensatz zu berechenmässig sicherer Kryptographie, keine Annahmen über die Rechenleistung eines Angreifers gemacht werden.

Ein weiterer Vorteil der Quantenkryptographie ist, dass deren Sicherheit rigoros bewiesen werden kann (während berechenmässige Sicherheit üblicherweise auf unbewiesenen Vermutungen über die Schwierigkeit gewisser mathematischer Probleme wie Faktorisieren beruht). Jedoch sind solche Sicherheitsbeweise bisher nur beschränkt auf praktische Implementierungen anwendbar.

Das Ziel dieser Arbeit ist es, allgemein verwendbare informationstheoretische Techniken zur Analyse von Quantensystemen zur Verfügung zu stellen. Angewandt auf QKD ermöglichen diese Techniken starke und konzeptuell einfache Sicherheitsbeweise, welche problemlos an fast beliebige (praxisnahe) Modelle und Protokollvariationen angepasst werden können.

1 Einführung

Quantenmechanik ist ein Gebiet der Physik, das sich dem Studium der Naturgesetze widmet, welche das Verhalten von kleinsten Teilchen wie Elektronen oder Photonen bestimmen. Dieses unterscheidet sich grundsätzlich von dem der uns vertrauten makroskopischen Objekte. So ist es beispielsweise prinzipiell unmöglich, physikalische Parameter eines Photons zu messen ohne diese zu beeinflussen.

Solche quantenmechanischen Phänomene sind offensichtlich interessant für Anwendungen im Bereich der Informationsverarbeitung und besonders der Kryptographie. So stellten Bennett und Brassard 1984, basierend auf Ideen von Wiesner [Wie83], ein so-genanntes *Quantum Key Distribution (QKD)* Protokoll vor, das heute unter dem Namen *BB84* bekannt ist [BB84]. Dieses ermöglicht zwei entfernten Parteien mittels Austausches einzel-

ner Photonen über einen unsicheren Kanal einen geheimen Schlüssel zu vereinbaren.

Überraschenderweise verging mehr als ein Jahrzehnt, bis die Sicherheit des BB84-Protokolls gegenüber allgemeinen Attacken bewiesen werden konnte [May96]. Der erste Sicherheitsbeweis war aber lediglich bezüglich einer stark vereinfachten Modellierung der zur Implementierung des Protokolls verwendeten physikalischen Ressourcen gültig. So musste beispielsweise garantiert werden, dass die Photonenquellen Pulse bestehend aus exakt einem einzelnen Photon aussenden, was in der Praxis nur schwer zu realisieren ist. Um solche Probleme zu lösen, wurden in den letzten paar Jahren eine Vielzahl alternativer Beweise vorgeschlagen (die meisten basierend auf Ideen aus [SP00]). Deren Gültigkeit ist aber nach wie vor auf spezifische Modellierungen der verwendeten Quantensysteme und einzelne ausgewählte Protokolle beschränkt.

Die Schwierigkeit, die Sicherheit von quantenkryptographischen Protokollen zu beweisen, liegt hauptsächlich daran, dass die bekannten Techniken der Informationstheorie nicht direkt auf kryptographische Szenarien anwendbar sind. Das Ziel der hier zusammengefassten Arbeit [Ren05] ist es daher, solche Techniken zur Verfügung zu stellen.

2 QKD: Schlüsselvereinbarung über Quantenkanäle

Um einen Einblick in die Funktionsweise der Quantenkryptographie zu erhalten, schauen wir uns im Folgenden das Problem der Schlüsselvereinbarung (QKD) und insbesondere (in Abschnitt 3) das oben erwähnte BB84-Protokoll etwas genauer an.

Wir betrachten ein Szenario bestehend aus zwei Parteien, genannt *Alice* und *Bob*. Diese seien über einen (unsicheren) Quantenkanal verbunden, welcher beispielsweise den Austausch von Photonen erlaubt. Zusätzlich nehmen wir an, dass Alice und Bob einen authentischen[1] klassischen Kommunikationskanal (z.B. eine Telefonverbindung) zur Verfügung haben.

Das Ziel eines QKD-Protokolls ist, Alice und Bob mit einem (beliebig langen) gemeinsamen geheimen Schlüssel zu versorgen. Dieser kann dann beispielsweise als *One-Time-Pad* zur Verschlüsselung von geheimen Meldungen verwendet werden. Dabei wird jedes einzelne Bit der Meldung M_i in ein Chiffratbit C_i transformiert, indem ein Schlüsselbit S_i hinzuaddiert wird, d.h., $C_i \equiv M_i + S_i \mod 2$. Wie der Name *One-Time-Pad* schon sagt, darf dabei jedes Schlüsselbit nur *einmal* verwendet werden. (Der Schlüssel muss also mindestens gleich lang sein wie die zu chiffrierende Meldung.) Damit ist garantiert, dass das Chiffrat aus der Sicht eines möglichen Gegners, der den Schlüssel nicht kennt, völlig unabhägig von der Meldung ist. Der One-Time-Pad bietet also *perfekt sichere* Verschlüsselung, vorausgesetzt dass der Schlüssel geheim ist.

Bevor wir mit der Beschreibung des BB84-Protokolls beginnen, sei noch ein Wort zu den an ein QKD-Protokoll gestellten Anforderungen gesagt. Da nichts über die Sicherheit des Quantenkanals zwischen Alice und Bob angenommen wird, kann dieser prinzi-

[1] *Authentizität* bedeutet, dass Bob verifizieren kann, ob eine von ihm empfangene Meldung tatsächlich von Alice stammt und umgekehrt.

piell vollständig von einem Gegner kontrolliert werden. Insbesondere könnte ein Gegner die Quantenkommunikation vollständig blockieren, was die Erzeugung eines Schlüssels natürlich verunmöglicht. Ein QKD-Protokoll sollte daher in der Lage sein, ernsthafte Attacken eines Gegners zu erkennen und die Berechnung des Schlüssels notfalls abzubrechen. Genauer bezeichnen wir ein QKD-Protokoll als *sicher*, wenn folgende Forderungen efüllt sind: (i) Falls das Protokoll nicht abbricht, muss der erzeugte Schlüssel geheim sein. (ii) Solange sich der Gegner passiv verhält, darf das Protokoll nicht abbrechen.[2]

3 Beispiel eines QKD-Protokolls: BB84

Wie alle QKD-Protokolle basiert auch das BB84-Protokoll auf der Idee, klassische Information als physikalischen Zustand eines Quantensystems zu repräsentieren. Am einfachsten lässt sich die Funktionsweise des Protokolls veranschaulichen, indem man sich unter diesen Datenträgern einzelne Photonen vorstellt, wobei die Information als deren Polarisierungsrichtung codiert wird. Genauer verwendet das BB84-Protokoll zwei verschiedene so-genannte *Codierungsbasen*. In der *rektilinearen Basis* werden die Bitwerte 0 und 1 durch horizontal bzw. vertikal polarisierte Photonen repräsentiert, während dies bei der *diagonalen Basis* die beiden diagonalen Polarisierungsrichtungen sind.

Polarisierte Photonen können in der Praxis relativ einfach erzeugt werden, was natürlich wichtig für Implementierungen ist.[3] Weiter kann bei bekannter Codierungsbasis das in ein Photon codierte Bit mit einem Polarisationsfilter und einem Photodetektor ausgelesen oder *gemessen* werden. Dazu nutzt man die Tatsache, dass beispielsweise ein horizontal ausgerichteter Polarisationsfilter horizontal polarisierte Photonen passieren lässt, während vertikal ausgerichtete absorbiert werden.

Das BB84-Protokoll besteht im Wesentlichen aus zwei Teilen, wobei der Quantenkanal nur im ersteren verwendet wird. Das Ziel des ersten Protokollteils ist es, einen *Rohschlüssel* zu erzeugen. Dazu werden folgende Schritte ausgeführt.

- Alice wählt ein zufälliges Bit X und eine zufällige Basis B (rektilinear oder diagonal). Sie präpariert ein Photon mit einer Codierung von X bezüglich der Basis B und sendet dieses über den Quantenkanal an Bob.
- Bob wählt zufällig eine Basis B' (rektilinear oder diagonal). Er misst das empfangene Photon bezüglich der Basis B', wodurch er ein Bit X' erhält.
- Alice teilt Bob die von ihr gewählte Basis B mit (wobei sie den authentischen klassischen Kommunikationskanal verwendet).
- Bob teilt Alice mit, ob die von ihm zur Messung verwendete Basis B' mit Alices Basis B übereinstimmt. Falls ja, behalten beide ihr Bit (X bzw. X'), andernfalls beginnen sie von vorne.

[2] Genauer gesagt fordert man, dass diese beiden Forderungen höchstens mit einer sehr kleinen Wahrscheinlichkeit (exponentiell in einem Sicherheitsparameter) verletzt sind.

[3] Die Schwierigkeit liegt allerdings darin, Pulse zu generieren, welche garantiert nur ein einzelnes Photon enthalten.

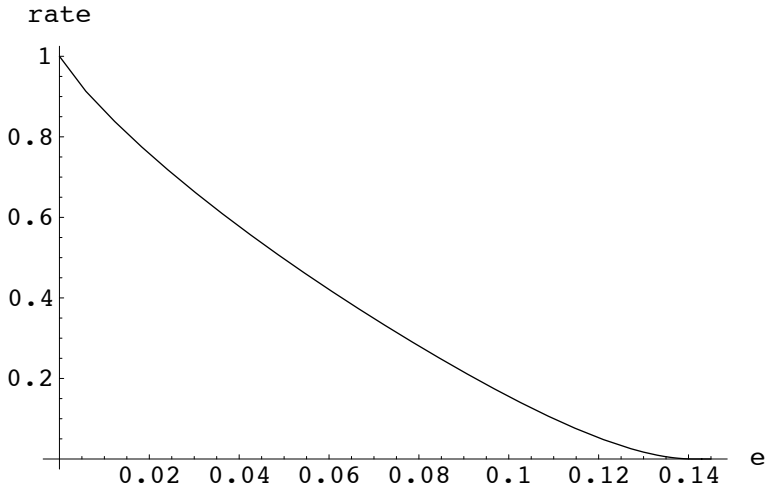

Abbildung 1: Schlüsselrate des *Six-State*-Protokolls [Bru98, BPG99], einer Erweiterung des BB84-Protokolls, in Abhängigkeit von der Bitflip-Wahrscheinlichkeit e des Quantenkanals.

Diese Sequenz von Schritten kann wiederholt werden, um beliebig lange Rohschlüssel zu generieren.

Selbstverständlich sind bei einem fehlerfreien Quantenkanal die erhaltenen Rohschlüsselbits von Alice und Bob (X und X') identisch. Bei realistischen, fehlerbehafteten Kanälen ist dies jedoch nicht mehr der Fall. Ausserdem könnte ein möglicher Gegner durch Interaktion mit den übertragenen Photonen Informationen über den Rohschlüssel erhalten haben. Zweck des zweiten Protokollteils, der übrigens rein klassisch ist, ist es daher, das von Alice und Bob erzeugte Paar von fehlerbehafteten und nur teilweise geheimen Rohschlüsseln X und X' in ein Paar von identischen und geheimen Schlüsseln zu transformieren. Dazu werden folgende Subprotokolle aufgerufen.

- *Parameter-Estimation:* Alice und Bob vergleichen die Bitwerte ihrer Rohschlüssel an ein paar zufällig ausgewählten Positionen, um die Fehlerrate e abzuschätzen. Falls e zu hoch ist, wird das Protokoll abgebrochen.
- *Error-Correction:* Alice sendet Fehlerkorrektur-Information (über den klassischen Kanal) an Bob. Dies erlaubt Bob, aus seinem Rohschlüssel X' den korrekten Rohschlüssel X von Alice zu errechnen.
- *Privacy-Amplification:* Alice und Bob wenden eine Hashfunktion an, welche den eventuell nur teilweise geheimen Rohschlüssel X in einen kürzeren, dafür vollständig sicheren Schlüssel transformiert.

Die Sicherheit von QKD-Protokollen beruht darauf, dass ein Gegner, welcher versucht, Informationen über die über den Quantenkanal gesendeten Photonen zu erhalten, diese notwendigerweise stört. Dies führt zu Fehlern in den Rohschlüsseln, welche im oben be-

schriebenen Parameter-Estimation-Schritt erkannt werden. Genauer kann für jede gegebene Fehlerrate e eine Grenze I_e an die maximal von einem Gegner erhaltene Information errechnet werden. Je grösser I_e ist, desto kleiner ist die Unsicherheit des Gegners über den Rohschlüssel und damit die Länge des perfekten Schlüssels, der im Privacy-Amplification-Schritt berechnet werden kann. Dieser Zusammenhang zwischen der Fehlerrate e und der erreichbaren Schlüsselrate, d.h., der Anzahl (perfekten) Schlüsselbits, die pro Bit des Rohschlüssels erzeugt werden können, ist in Abb. 1 dargestellt.

Da der Gegner die über den Quantenkanal gesendete Information theoretisch beliebig manipulieren kann, ist die Berechnung der maximal erhaltenen Information I_e als Funktion der Fehlerrate e ein nichttriviales mathematisches Problem. Das Ziel der folgenden Abschnitte ist es, informationstheoretische Techniken vorzustellen, die zur Lösung dieses Problems verwendet werden können.

4 Neue Entropie-Masse: Smooth Min- and Max-Entropien

Der Begriff der *Entropie* als ein Mass für Unsicherheit spielt eine zentrale Rolle im Gebiet der Informationstheorie. Entropie kann auf verschiedenste Arten gemessen werden. Das wohl am breitesten bekannte Entropiemass ist die so-genannte *Shannon-Entropie* oder dessen Verallgemeinerung auf Quantensysteme, genannt *von Neumann-Entropie*. Die Bedeutung dieser Entropiemasse folgt aus der Tatsache, dass sie eine *funktionale Bedeutung* haben, d.h., zur Charakterisierung von konkreten informationsverarbeitenden Prozessen verwendet werden können. Ein typisches Beispiel ist Datenkompression: Die Shannon-Entropie $H(X)$ einer klassischen Zufallsvariablen X entspricht der Anzahl Bits, welche asymptotisch zur Speicherung vieler unabhängigen Realisierungen von X benötigt werden.

Die Anwendbarkeit der Shannon- bzw. der von Neumann-Entropie beschränkt sich jedoch auf asymptotische Analysen. So gibt die Shannon-Entropie einer Zufallsvariablen X beispielsweise keinen Aufschluss darüber, wie viele Bits zur Speicherung einer *einzelnen* Realisierung von X benötigt werden. In der Tat können nur Szenarien analysiert werden, in denen ein bestimmter Zufallsprozess sehr oft unabhängig wiederholt wird. Diese Voraussetzung ist aber gerade in kryptographischen Anwendungen, wo ein Gegner eine beliebige Strategie verfolgen kann, allgemein nicht erfüllt.

In der vorliegenden Arbeit führen wir neue Entropiemasse ein, genannt *smooth Min-Entropie* und *smooth Max-Entropie*, welche wir im Folgenden mit $H_{\min}^{\varepsilon}$ bzw. $H_{\max}^{\varepsilon}$ bezeichnen.[4] Diese Entropiemasse sind der oben beschriebenen Einschränkung nicht unterworfen, d.h., sie können auch zur Charakterisierung von Prozessen verwendet werden, die durch eine *einzelne* Realisierung eines Zufallsexperiments definiert sind [RW05]. So entspricht etwa die smooth Min-Entropie $H_{\min}^{\varepsilon}(X)$ einer Zufallsvariablen X der Anzahl gleichmässig verteilter Bits, welche aus einer einzelnen Realisierung von X durch Anwendung einer Hash-Funktion extrahiert werden können. Weiter misst $H_{\max}^{\varepsilon}(X)$ die Anzahl

[4] Genauer handelt es sich um Klassen von Entropiemassen, parametrisiert durch eine reelle Zahl $\varepsilon \geq 0$.

Bits, welche zur Speicherung einer einzelnen Realisierung von X benötigt werden.[5]

Smooth Min- und Max-Entropien können nicht nur für klassische Zufallsvariablen, sondern auch für Quantenzustände definiert werden. Im Zusammenhang mit QKD sind insbesondere Hybridsysteme bestehend aus klassischen und quantenmechanischen Teilsystemen interessant. Sei X zum Beispiel ein klassischer String und E ein Quantensystem, dessen Zustand von X abhängt. Dann entspricht $H_{\min}^{\varepsilon}(X|E)$ der Anzahl gleichmässig verteilter Bits, welche aus X (durch Anwenden einer Hashfunktion) extrahiert werden können und unabhängig vom Zustand des Quantensystems E sind. Interpretiert man X als einen Rohschlüssel und E als ein von einem Gegner kontrolliertes System, so misst $H_{\min}^{\varepsilon}(X|E)$ folglich die Anzahl perfekter Schlüsselbits, welche durch den oben beschriebenen Privacy-Amplification-Schritt generiert werden können.

Da die smooth Entropien zur Analyse derselben Prozesse verwendet werden können, welche asymptotisch auch durch die Shannon-Entropie charakterisiert sind, muss es offensichtlich einen engen Zusammenhang zwischen diesen beiden Entropiemassen geben. Tatsächlich kann die Shannon-Entropie von Zufallsvariablen (und analog die von Neumann-Entropie von Quantenzuständen) als asymptotischer Spezialfall sowohl der smooth Min-Entropie als auch der smooth Max-Entropie gesehen werden. Sei zum Beispiel X^n eine Sequenz von n unabhängigen und identisch verteilten Zufallsvariablen. Dann gilt

$$\lim_{n\to\infty} \frac{1}{n} H(X^n) = \lim_{\varepsilon\to 0} \lim_{n\to\infty} \frac{1}{n} H_{\max}^{\varepsilon}(X^n) = \lim_{\varepsilon\to 0} \lim_{n\to\infty} \frac{1}{n} H_{\min}^{\varepsilon}(X^n) \,. \qquad (1)$$

Die Shannon- als auch die von Neumann-Entropie efüllen eine Reihe von Regeln, welche die Manipulation dieser Grössen erleichtern. So besagt beispielsweise die *Kettenregel*, dass die Entropie $H(XY)$ zweier Zufallsvariablen X und Y als Summe der Entropie $H(Y)$ von Y und der Entropie $H(X|Y)$ von X bedingt auf Y geschrieben werden kann. Man kann zeigen, dass analoge Eigenschaften auch für die smooth Entropien gelten. Eine Auswahl solcher Regeln ist in Tab. 1 zusammengefasst.

Wegen (1) können die Eigenschaften der Shannon- bzw. der von Neumann-Entropie als Spezialfall der entsprechenden Eigenschaften der smooth Entropien gesehen werden. Interessanterweise werden die Beweise einiger dieser Eigenschaften mit der Verallgemeinerung zu smooth Entropien einfacher. So folgt etwa die *starke Subadditivität* [6] für $H_{\max}^{\varepsilon}$ und $H_{\min}^{\varepsilon}$ beinahe trivial aus der Definition (während bisher bekannte Beweise direkt für die von Neumann-Entropie mathematisch relativ anspruchsvoll sind).

5 Struktur symmetrischer Quantenzustände

In dem oben beschriebenen QKD-Protokoll sendet Alice eine Vielzahl von Photonen über einen Quantenkanal zu Bob. Die Reihenfolge, in der diese Photonen gesendet werden, ist dabei aber unwichtig (solange sichergestellt ist, dass Bob weiss, welches Photon zu wel-

[5] Der Parameter ε entspricht dabei der maximalen Fehlerwahrscheinlichkeit.

[6] Für eine detaillierte Beschreibungen dieses Problems verweisen wir auf die Standardliteratur über Quanten-Informationstheorie, z.B. [NC00].

	Shannon / vN Entropie	Smooth Min-/Max-Entropie
Kettenregel	$H(X\|Y) = H(XY) - H(Y)$	$H_{\max}^{\varepsilon+\varepsilon'}(XY) - H_{\max}^{\varepsilon'}(Y) \leq H_{\max}^{\varepsilon}(X\|Y) \lessapprox H_{\max}^{\varepsilon_1}(XY) - H_{\min}^{\varepsilon_2}(Y)$ $H_{\min}^{\varepsilon_1}(XY) - H_{\max}^{\varepsilon_2}(Y) \lessapprox H_{\min}^{\varepsilon}(X\|Y) \leq H_{\min}^{\varepsilon+\varepsilon'}(XY) - H_{\min}^{\varepsilon'}(Y)$
Superadditivität	$H(XY) \leq H(X) + H(Y)$	$H_{\max}^{\varepsilon+\varepsilon'}(XY) \leq H_{\max}^{\varepsilon}(X) + H_{\max}^{\varepsilon'}(Y)$ $H_{\min}^{\varepsilon}(XY) \leq H_{\min}^{\varepsilon+\varepsilon'}(X) + H_{\max}^{\varepsilon'}(Y)$
Starke Subadd.	$H(X\|YZ) \leq H(X\|Y)$	$H_{\max}^{\varepsilon}(X\|YZ) \leq H_{\max}^{\varepsilon}(X\|Y)$ $H_{\min}^{\varepsilon}(X\|YZ) \leq H_{\min}^{\varepsilon}(X\|Y)$

Tabelle 1: Ausgewählte Eigenschaften der smooth Min- und Max-Entropien $H_{\max}^{\varepsilon}$ und $H_{\min}^{\varepsilon}$ im Vergleich zu denen der Shannon- bzw. der von Neumann-Entropie H. Die Approximation $\approx$ bedeutet jeweils, dass die (Un)gleichung bis auf eine additive Konstante $\log(1/\varepsilon)$ efüllt ist. ε, ε', ε_1 und ε_2 sind beliebige positive Parameter. Die Eigenschaften gelten sowohl für klassische Zufallsvariablen als auch für Quantenzustände.

chem codierten Bit gehört). Alice und Bob könnten also beispielsweise die Bits des Rohschlüssels gemäss einer gemeinsam vereinbarten Permutation umordnen, ohne dass sich an der Funktionalität des Protokolls etwas ändern würde. Eine solche Permutationssymmetrie ist typisch für informationsverarbeitende Prozesse. Wie wir sehen werden, erleichtert diese Symmetrie die Analyse solcher Prozesse erheblich.

Der Mathematiker de Finetti hat sich intensiv mit dem Studium symmetrischer klassischer probabilistischer Systeme beschäftigt. Ein nach ihm benannter Satz besagt, dass jede Wahrscheinlichkeitsverteilung, welche genug Symmetrien aufweist, als Konvexkombination von Produktverteilungen dargestellt werden kann [dF37, MC93]. Dieser Satz wurde später in verschiedene Richtungen verallgemeinert [Stø69, HM76, DF80, FLV88, RW89, Pet90, CFS02, FSS04, KR05]. Die Ergebnisse suggerieren, dass mehrteilige permutationssymmetrische Systeme sich „fast“ so verhalten als ob alle Teilsysteme identisch und unabhängig voneinander wären. In der Tat geben wir im Folgenden einen Darstellungssatz für endlich-dimensionale Quantensysteme, welcher diese Aussage mathematisch präzis macht.

Ein n-teiliger Quantenzustand ρ_n heisst *symmetrisch*, falls er invariant ist unter Permutationen der n Teilsysteme. Weiter nennen wir ρ_n einen *Produktzustand*, falls er als n-faches Tensorprodukt eines Zustandes σ geschrieben werden kann, d.h. $\rho_n = \sigma^{\otimes n}$. Allgemeiner sagen wir, dass ρ_n ein *r-fast Produktzustand* ist (für $0 \leq r \leq n$), wenn ρ_n auf $n - r$ Teilsystemen von der Form $\sigma^{\otimes n-r}$ ist. Im Folgenden bezeichnen wir solche n-teilige r-fast Produktzustände mit $[\sigma^{\otimes n-r}]_n$.

Sei nun ρ_n ein symmetrischer Quantenzustand auf n endlich-dimensionalen Teilsystemen und fixiere k und r so dass $k + r \leq n$. Unser Darstellungssatz besagt dann, dass der Zustand ρ_{n-k} der ersten $n-k$ Teilsysteme von ρ_n approximiert wird (bezüglich der L_1-Norm $\|\cdot\|_1$) durch eine Konvexkombination von r-fast Produktzuständen, d.h.,

$$\left\|\rho_{n-k} - \sum_{\sigma} p(\sigma)[\sigma^{\otimes n-k-r}]_{n-k}\right\|_1 \leq e^{-\Omega(\frac{rk}{n})} , \tag{2}$$

wobei $p(\sigma)$ Gewichte sind so dass $\sum_\sigma p(\sigma) = 1$. Beachte, dass für ein beliebig kleines $\mu > 0$ mit der Wahl $r := \mu n$ und $k := \mu n$ die rechte Seite von (2) immer noch exponentiell in n abnimmt. Grob gesprochen kann man also einen beliebigen symmetrischen Quantenzustand als Konvexkombination von „Fast-Produktzuständen“ betrachten.

Die meisten physikalisch relevanten Eigenschaften von r-fast Produktzuständen eines n-teiligen Systems, für $r \ll n$, sind nahezu identisch zu denen von perfekten Produktzuständen. Dies gilt insbesondere für entropische Grössen, wie z.B. die im obigen Abschnitt beschriebenen smooth Entropien $H^\varepsilon_{\max}$ and $H^\varepsilon_{\min}$. Da analog zu (1) die Entropien $H^\varepsilon_{\max}(\sigma^{\otimes n})$ und $H^\varepsilon_{\min}(\sigma^{\otimes n})$ eines Produktzustands $\sigma^{\otimes n}$ durch die von Neumann-Entropie $H(\sigma^{\otimes n}) = n \cdot H(\sigma)$ approximiert werden, können auch die smooth Entropien von symmetrischen Zuständen einfach bestimmt werden.

6 Generischer Sicherheitsbeweis für QKD

Wegen der Schwierigkeit, die Sicherheit von QKD-Protokollen gegenüber allgemeinen Gegnern zu beweisen, wurden oft gewisse vereinfachende Annahmen über die Struktur der möglichen Attacken getroffen. So stellte sich heraus, dass die Sicherheitsanalyse stark vereinfacht wird, wenn man sich auf so-genannte *kollektive Attacken* beschränkt, bei denen ein Gegner jedes über den Quantenkanal gesendete Photon gleich und unabhängig von den anderen Photonen behandelt [BM97b, BM97a, BBB$^+$02]. Tatsächlich sind in diesem Spezialfall die aus der Informationstheorie bekannten Techniken (z.B. die von Neumann-Entropie als Mass für die Unsicherheit eines Gegners) direkt anwendbar. So können einfach explizite Formeln für die Schlüsselraten von Protokollen hergeleitet werden [DW05].

Da die Einschränkung auf kollektive Attacken jedoch physikalisch nicht gerechtfertigt werden kann, drängt sich sofort die Frage auf, ob aus einem Statement über die Sicherheit eines Protokolls gegenüber kollektiven Attacken auch Aussagen über die Sicherheit gegenüber beliebigen Attacken abgeleitet werden können. Diese Frage lässt sich mit den in den obigen Abschnitten vorgestellten Techniken positiv beantworten.

Genauer lässt sich folgendes Statement zeigen: Sei $\mathcal{P}$ ein beliebiges QKD-Protokoll, das sicher gegenüber kollektiven Attacken ist. Das Protokoll $\mathcal{P}$ kann nun *symmetrisiert* werden, indem Alice und Bob nach dem Erstellen der Rohschlüssel diese gemäss einer gemeinsam gewählten zufälligen Permutation umordnen. Das so symmetrisierte Protokoll $\bar{\mathcal{P}}$ ist dann sicher gegenüber jeder beliebigen physikalisch erlaubten Attacke. Mit anderen Worten lässt sich die Sicherheit eines Protokolls $\mathcal{P}$ (oder genauer einer symmetrisierten Version $\bar{\mathcal{P}}$) zeigen, indem man lediglich die Sicherheit von $\mathcal{P}$ gegenüber kollektiven Atta-

cken beweist (was, wie oben erläutert, relativ einfach ist).

Diese generische Beweismethode ist auf beliebige QKD-Protokolle anwendbar. Im Fall von bekannten Protokollen wie BB84 liefert sie ausserdem bessere Grenzen an die Schlüsselrate (und damit den maximal tolerierten Geräuschpegel des Quantenkanals). Zudem ergibt sich, verglichen mit bisherigen Beweisen, ein stärkeres Statement über die Sicherheit des generierten Schlüssels. So ist beispielsweise garantiert, dass der Schlüssel in einer beliebigen Anwendung (z.B. zur Datenverschlüsselung als One-Time-Pad) verwendet werden kann (was überraschenderweise aus früheren Sicherheitsbeweisen nicht direkt gefolgert werden kann [KRBM05]).

Literatur

[BB84] C. H. Bennett und G. Brassard. Quantum Cryptography: Public-Key Distribution and Coin Tossing. In *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, Seiten 175–179, 1984.

[BBB+02] E. Biham, M. Boyer, G. Brassard, J. van de Graaf und T. Mor. Security of Quantum Key Distribution Against All Collective Attacks. *Algorithmica*, 34:372–388, 2002.

[BM97a] E. Biham und T. Mor. Bounds on Information and the Security of Quantum Cryptography,. *Phys. Rev. Lett.*, 79:4034–4037, 1997.

[BM97b] E. Biham und T. Mor. Security of Quantum Cryptography Against Collective Attacks. *Phys. Rev. Lett.*, 78(11):2256–2259, 1997.

[BPG99] H. Bechmann-Pasquinucci und N. Gisin. Incoherent and Coherent Eavesdropping in the Six-State Protocol of Quantum Cryptography. *Phys. Rev. A,*, 59:4238, 1999.

[Bru98] D. Bruss. Optimal Eavesdropping in Quantum Cryptography with Six States. *Phys. Rev. Lett.*, 81:3018, 1998.

[CFS02] C. M. Caves, C. A. Fuchs und R. Schack. Unknown Quantum States: The Quantum de Finetti Representation. *Journal of Mathematical Physics*, Seite 4537, 2002.

[dF37] B. de Finetti. La prévision: ses lois logiques, ses sources subjectives. *Ann. Inst. H. Poincaré*, 7:1–68, 1937.

[DF80] P. Diaconis und D. Freedman. Finite Exchangeable Sequences. *The Annals of Probability*, 8(4):745–764, 1980.

[DW05] I. Devetak und A. Winter. Distillation of Secret Key and Entanglement from Quantum States. *Proc. R. Soc. Lond. A*, 461:207–235, 2005.

[FLV88] M. Fannes, J. T. Lewis und A. Verbeure. Symmetric States of Composite Systems. *Lett. Math. Phys.*, 15:255–260, 1988.

[FSS04] C. A. Fuchs, R. Schack und P. F. Scudo. A de Finetti Representation Theorem for Quantum Process Tomography. *Phys. Rev. A*, 69:062305, 2004.

[HM76] R. L. Hudson und G. R. Moody. Locally Normal Symmetric States and an Analogue of de Finetti's Theorem. *Z. Wahrschein. verw. Geb.*, 33:343–351, 1976.

[KR05] R. König und R. Renner. A de Finetti Representation for Finite Symmetric Quantum States. *Journal of Mathematical Physics*, 46:122108, 2005.

[KRBM05] R. König, R. Renner, A. Bariska und U. Maurer. Locking of Accessible Information and Implications for the Security of Quantum Cryptography. `http://arxiv.org/abs/quant-ph/0512021`, 2005.

[May96] D. Mayers. Quantum Key Distribution and String Oblivious Transfer in Noisy Channels. In *Advances in Cryptology — CRYPTO '96*, Jgg. 1109 of *Lecture Notes in Computer Science*, Seiten 343–357. Springer, 1996.

[MC93] P. Monari und D. Cocchi, Hrsg. *Introduction to Bruno de Finetti's "Probabiliá e Induzione"*. Cooperativa Libraria Universitaria Editrice, Bologna, 1993.

[NC00] M. A. Nielsen und I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

[Pet90] D. Petz. A de Finetti-type Theorem with m-Dependent States. *Prob. Th. Rel. Fields.*, 85(1), 1990.

[Ren05] R. Renner. *Security of Quantum Key Distribution*. Dissertation, Swiss Federal Institute of Technology (ETH) Zurich, 2005. Also available at `http://arxiv.org/abs/quant-ph/0512258`.

[RW89] G. A. Raggio und R. F. Werner. Quantum Statistical Mechanics of General Mean Field Systems. *Helv. Phys. Acta*, 62:980–1003, 1989.

[RW05] R. Renner und S. Wolf. Simple and Tight Bounds for Information Reconciliation and Privacy Amplification. In *Advances in Cryptology — ASIACRYPT 2005*, Jgg. 3788 of *Lecture Notes in Computer Science*, Seiten 199–216. Springer-Verlag, 2005.

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

[Stø69] E. Størmer. Symmetric States of Infinite Tensor Products of C^*-algebras. *J. Funct. Anal.*, 3:48–68, 1969.

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

Renato Renner wurde am 11. Dezember 1974 in Luzern geboren. Nach Abschluss des Realgymnasiums an der Kantonsschule Alpenquai Luzern begann er im Jahr 1994 sein Studium in Physik an der Ecole Polytechnique Fédérale in Lausanne. 1996 rückte er in die Schweizer Armee zu einem einjährigen Militärdienst (Offiziersschule der Übermittlungstruppen) ein. Sein Fachstudium setzte er an der Eidgenössischen Technischen Hochschule (ETH) Zürich fort, wo er im Jahr 2000 mit dem Diplom in Theoretischer Physik abschloss. 2005 promovierte er mit der hier zusammengefassten Arbeit, die in der Forschungsgruppe von Prof. Ueli Maurer am Institut für Theoretische Informatik an der ETH Zürich entstand. Seit 2005 forscht er am Department of Applied Mathematics and Theoretical Physics der Universität Cambridge, UK. Seine wissenschaftlichen Interessen umfassen Fragen im Bereich der Quanten-Informationstheorie und Kryptographie.