Beweisbare Sicherheit durch Quantenkryptografie

Provable Security in Quantum Cryptography

Renato Renner, University of Cambridge (UK), GI-Dissertationspreis 2005

Zusammenfassung Die Sicherheit heutiger kryptografischer Verfahren beruht meist auf der nicht beweisbaren Annahme, dass einem Gegner nur beschränkte Rechenleistung zur Verfügung steht. Im Gegensatz dazu bietet die Quantenkryptografie, die quantenmechanische Eigenschaften kleinster Teilchen wie zum Beispiel Photonen nutzt, beweisbare Sicherheit. Dieser Artikel erläutert die Funktionsweise dieser neuartigen Technik. ►►► **Summary** The security of established cryptographic schemes mostly relies on the non-provable assumption that a potential adversary only has limited computational power. In contrast, quantum cryptography provides provable security, using properties of small particles such as photons. In this article we explain how this new technique works.

KEYWORDS E.3 [Data Encryption], H.1.1 [Systems and Information Theory] cryptography, secure message transmission, quantum key distribution, provable security, Kryptografie, sichere Kommunikation

1 Einleitung

Die sichere Übertragung vertraulicher Meldungen ist ein Problem, das die Menschheit seit jeher beschäftigt. Im Zeitalter der elektronischen Datenverarbeitung hat sich die Untersuchung dieses und verwandter Probleme sogar zu einem eigenen Wissenschaftsgebiet entwickelt, der *Kryptografie*. Daraus sind verschiedenste Technologien zur sicheren Übertragung von Daten über potenziell unsichere Kanäle (wie z. B. das Internet) hervorgegangen, welche aus der modernen Welt nicht mehr wegzudenken sind.

Die meisten der heute verwendeten kryptografischen Verfahren wie beispielsweise der *Advanced Encryption Standard (AES)* oder das Public-Key-System *RSA* bieten *berechenmäßige* Sicherheit. Das bedeutet, dass ein Gegner, um das Kryptosystem zu brechen, Berechnungen durchführen müsste, welche nicht innerhalb vernünftiger Zeit abgeschlossen werden können.

Jedoch konnte bisher kein mathematisches Argument gefunden werden, das die Sicherheit dieser Verfahren rigoros beweist. Es scheint sogar, dass es für viele der heute verwendeten Kryptosysteme gar keinen solchen Sicherheitsbeweis geben kann. In der Tat könnten etablierte Public-Key-Systeme wie etwa RSA mit dem *Shor-Algorithmus*, der effizient Zahlen in ihre Primzahlen zerlegen kann, gebrochen werden. Allerdings nutzt der Shor-Algorithmus Quanteneffekte, setzt also die Existenz eines sogenannten *Quantencomputers* voraus.

Obwohl Quantencomputer mit heutiger Technik (noch) nicht realisiert werden können, zeigt dieses Beispiel, dass Sicherheit oft lediglich von (vermuteten) technischen Limitierungen potenzieller Gegner abhängt. Dies ist problematisch, da die Entwicklung der Technologie, wie die Geschichte wiederholt gezeigt hat, mittel- bis langfristig kaum vorausgesagt werden kann. Die heute gebräuchlichen kryptografischen Verfahren bieten also keine Langzeit-Sicherheit – eine verschlüsselt versendete Meldung bleibt möglicherweise nur für eine beschränkte Zeitdauer geheim.

Während, wie oben beschrieben, Quantencomputer von einem Gegner verwendet werden könnten, um Kryptosysteme zu brechen, kann man sich Quanteneffekte auch zu Nutze machen, um neuartige und *beweisbar sichere* Kryptosysteme zu entwickeln. Dies ist die der *Quan-*

Die an der ETH Zürich von Herrn Dr. Renner angefertigte Dissertation wurde mit dem GI-Dissertationspreis 2005 ausgezeichnet. Die Gutachter des Promotionsverfahrens waren Prof. Dr. Ueli Maurer (ETH Zürich) und Dr. Charles H. Bennett (IBM Research Yorktown Heights).

tenkryptografie zu Grunde liegende Idee, mit der sich dieser Artikel näher befasst.

2 Perfekt sichere Verschlüsselung

Nehmen wir an, ein Sender *Alice* möchte eine vertrauliche Meldung m an einen Empfänger *Bob* schicken. Alice und Bob seien aber lediglich durch einen unsicheren Kanal verbunden, sodass alle übermittelten Signale von einem Gegner abgehört werden können. Für den Moment gehen wir aber davon aus, dass der Kanal *authentisch* ist, ein Gegner also die übermittelten Signale nicht verändern kann.

Wir werden nun ein Verfahren beschreiben, genannt *One-Time-Pad-Verschlüsselung*, mit dem Alice die Meldung m sicher an Bob schicken kann. Das Verfahren benötigt allerdings einen *gemeinsamen Schlüssel* s, d. h. eine Folge von Zufallsbits welche nur Alice und Bob (nicht aber dem Gegner) bekannt ist. Aus Sicht des Gegners sollen dabei alle möglichen Werte von s gleich wahrscheinlich sein.

Um ihre Meldung zu verschlüsseln, berechnet Alice aus jedem Meldungsbit m_i ein *Chiffratbit* c_i, indem sie das *exclusive or (XOR)* zwischen m_i und einem entsprechenden Schlüsselbit s_i bildet (siehe Bild 1). Jedes Chiffratbit c_i wird dann über den (unsicheren) Kanal an Bob geschickt, der dieses wiederum entschlüsselt, indem er das XOR von c_i und s_i berechnet. Es ist einfach zu sehen, dass dieses Verfahren *korrekt* ist: Der von Bob entschlüsselte Wert wird immer mit dem von Alice verschlüsselten Meldungsbit m_i übereinstimmen. Andererseits ist aus der Sicht eines Gegners, der das Schlüsselbit s_i nicht kennt, das Chiffratbit c_i gleichverteilt und unabhängig vom Wert des Meldungsbits m_i. Der Wert von c_i (den der Gegner durch Abhören der Kommunikation ermitteln könnte) lässt also keine Rückschlüsse auf m_i zu; das Verfahren ist somit *perfekt sicher*.

Wie der Name *One-Time-Pad-Verschlüsselung* schon sagt, ist entscheidend, dass jedes Bit des Schlüssels höchstens einmal genutzt wird. Würde nämlich *dasselbe* Schlüsselbit s_i zur Codierung zweier aufeinanderfolgender Meldungsbits m_i und m_{i+1} verwendet, so wäre, wie man sich einfach überlegen kann, aus den entsprechenden Chiffratbits c_i und c_{i+1} einfach abzulesen, ob m_i und m_{i+1} identisch sind. Das Chiffrat würde also Informationen über die Meldung enthalten.

In der Tat kann man beweisen, dass jede perfekt sichere Verschlüsselung pro Meldungsbit mindestens ein Schlüsselbit „aufbraucht“. Damit also Alice mit Bob sicher kommunizieren kann, müssen diese laufend neue Schlüsselbits vereinbaren, was aber wiederum ohne sicheren Kanal zumindest mit rein klassischen Methoden unmöglich ist. Wie wir aber sehen werden, löst die Quantenkryptografie genau dieses Problem.

3 Detektierbarkeit von Beobachtungen

Das Verhalten kleinster Teilchen wie beispielsweise Elektronen oder Photonen (also Lichtteilchen) unterliegt den Gesetzen der Quantenphysik. Diese sind grundlegend verschieden von denen der klassischen Physik, welche das Verhalten der uns im Alltag vertrauten makroskopischen Objekten beschreibt (dies, obwohl die klassische Physik als Spezialfall der Quantenphysik verstanden werden kann). Für kryptografische Anwendungen besonders interessant ist die Tatsache, dass sich gemäß der Quantenphysik ein Teilchen nicht beobachten lässt, ohne es zu verändern. Jede Beobachtung hinterlässt also Spuren, die wiederum detektiert werden können.

Um diese Eigenschaft genauer zu beschreiben, betrachten wir als Beispiel das Photon. (Dieses ist beliebt in Anwendungen, da es sich über Glasfaserleitungen leicht über große Distanzen transportieren lässt.) Jedes Photon hat eine *Polarisation*, die man sich bildlich als Rotation um die eigene Achse vorstellen kann. Die Richtung dieser Achse kann mit verschiedensten Techniken beobachtet und verändert werden. Schickt man beispielsweise ein Photon durch einen *Polarisationsfilter*, wird es diesen abhängig von der Polarisation mit einer gewissen Wahrscheinlichkeit passieren, andernfalls wird es absorbiert. Passiert das Photon den Filter, wird es immer dieselbe (nur vom Filter abhängige) Polarisation aufweisen. Ein Polarisationsfilter kann also dazu verwendet werden, gewisse Informationen über die Polarisation des Photons zu erhalten, verändert diese aber gleichzeitig.

Die Gesetze der Quantenphysik besagen nun, dass dies für jeden physikalisch möglichen Prozess gilt. Eine Messung kann folglich immer nur partielle Informationen über die Polarisation des Photons liefern. Zudem wird die Polarisation durch den Messprozess zwingend verändert, wobei das Ausmaß dieser Veränderung von der Menge der gewonnenen Information abhängt.

4 Schlüsselvereinbarung über Glasfaser

Im Jahr 1984 haben Charles Bennett und Gilles Brassard [1], basierend auf Ideen von Stephen Wiesner, ein Protokoll zur Schlüsselvereinbarung zwischen zwei entfernten Parteien vorgestellt, welches die oben beschriebenen quantenmechanischen Eigenschaften von Photonen nutzt.

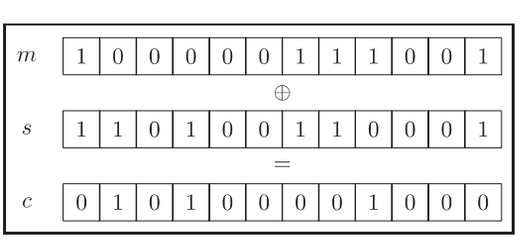

Bild 1 One-Time-Pad-Verschlüsselung: Das Chiffrat c wird durch bitweises XOR aus der Nachricht m und einem Schlüssel s berechnet.

Es setzt voraus, dass die beiden Parteien Photonen austauschen können, also beispielsweise über eine (möglicherweise unsichere) Glasfaserleitung miteinander verbunden sind.

Das Protokoll funktioniert im Wesentlichen wie folgt: In einem ersten Schritt generiert ein Sender (Alice) lokal eine Folge von zufälligen so genannten *Rohschlüssel-Bits* und präpariert gleichzeitig Photonen, deren Polarisation von den Werten dieser Bits abhängt. Diese werden dann zum Empfänger (Bob) geschickt. Bob führt die Photonen einer Messapparatur (beispielsweise basierend auf Polarisationsfiltern) zu, welche ihm Teilinformation über deren Polarisation und damit auch über Alices Rohschlüssel liefert.

In einem zweiten Schritt sendet Alice Fehlerkorrektur-Information (über einen klassischen authentischen Kanal) an Bob, welche diesem erlauben sollte, Alices Rohschlüssel vollständig zu rekonstruieren. Aus dem Rohschlüssel wird dann durch Anwendung einer *Hashfunktion* der endgültige Schlüssel errechnet. Die Hashfunktion stellt sicher, dass der endgültige Schlüssel geheim ist, solange der Gegner nur beschränktes Wissen über den Rohschlüssel hat (das er zum Beispiel durch Abhören der von Alice gesendeten Fehlerkorrektur-Information erlangt haben könnte).

Die Sicherheit dieses Schlüsselvereinbarungs-Protokolls beruht nun auf den oben diskutierten Gesetzen der Quantenphysik, gemäß denen ein Belauschen der übertragenen Photonen unweigerlich deren Polarisation verändert. Dies hat zur Folge, dass die Korrelation zwischen Alices Rohschlüssel und Bobs Messergebnissen abnimmt, was festgestellt werden kann. Wird diese Korrelation zu klein, was darauf hindeutet, dass der Gegner zu viel Information über den Rohschlüssel gesammelt haben könnte, müssen Alice und Bob das Protokoll abbrechen und den Rohschlüssel verwerfen. (Der Gegner kann das Protokoll also immer zum Abbruch bringen, was allgemein unvermeidbar ist, da er zum Beispiel auch den Kommunikationskanal zwischen Alice und Bob durchtrennen könnte.) Umgekehrt garantiert starke Korrelation zwischen Alice und Bobs Daten, dass der am Ende des Protokolls erzeugte Schlüssel geheim ist.

5 Sicherheit in der Praxis

Quantenkryptografische Protokolle zur Schlüsselvereinbarung, wie das oben beschriebene, können (im Gegensatz zu Quantencomputern) mit heute verfügbarer Technik tatsächlich realisiert werden. Jedoch sind die für praktische Implementierungen verwendeten Komponenten nie perfekt. So nimmt beispielsweise mit zunehmender Länge der Glasfaserleitung auch deren Rauschen zu, was wiederum einen negativen Einfluss auf die Qualität der von Bob empfangenen Daten hat.

Eine grundsätzliche Schwierigkeit ergibt sich nun daraus, dass eine durch Rauschen entstandene Störung sich prinzipiell nicht unterscheiden lässt von einer Störung, die durch einen Lauschangriff verursacht wurde. Um Sicherheit garantieren zu können, muss deshalb vorsichtigerweise davon ausgegangen werden, dass die Abnahme der Korrelation zwischen Alice und Bobs Daten vollständig durch einen Lauschangriff verursacht wurde. Mit zunehmendem Rauschpegel vergrößert sich also die Menge an Information, welche ein Gegner potenziell hätte sammeln können, wodurch die Effizienz des Protokolls abnimmt, bis irgendwann Schlüsselvereinbarung völlig unmöglich wird (Bild 2). Quantenkryptografischer Schlüsselaustausch mit heutiger Technologie ist daher auf Distanzen um 100 km beschränkt.

In [2] wird ein allgemeiner Sicherheitsbeweis für quantenkryptografische Protokolle vorgestellt, welcher auf praktische Realisierungen anwendbar ist. Im Unterschied zu früheren Beweisen wird dabei gezeigt, dass Sicherheit auch gegenüber einem *beliebig starken* Gegner gilt, der beispielsweise über einen Quantencomputer verfügt. Bisher wurde jeweils (implizit) die Annahme getroffen, dass ein Gegner ab einem bestimmten Zeitpunkt (bevor der Schlüssel in einer Anwendung verwendet wird) nur noch klassische Daten verarbeiten kann.

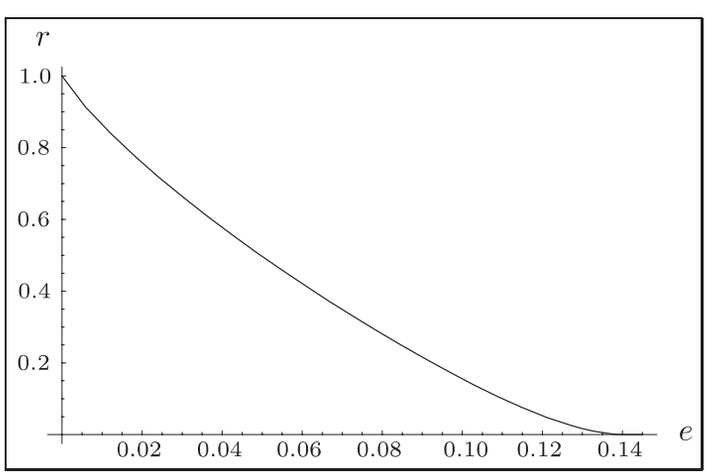

Bild 2 Schlüsselrate r (Anzahl Schlüsselbits, die pro Photon erzeugt werden) eines typischen Protokolls in Abhängigkeit des Rauschpegels e (Bitflip-Wahrscheinlichkeit) des Kanals.

Literatur

[1] Charles H. Bennett and Gilles Brassard, Quantum cryptography: Public-key distribution and coin tossing, in *Proc. of IEEE Int'l Conf. on Computers, Systems and Signal Processing*, pp. 175–179, 1984.

[2] Renato Renner, *Security of Quantum Key Distribution*, ETH Diss. Nr. 16242, 2005; elektronisch verfügbar unter http://arxiv.org/abs/quant-ph/0512258.

Dr. sc. nat. Renato Renner studierte an der École Polytechnique Fédérale in Lausanne und der Eidgenössischen Technischen Hochschule (ETH) Zürich, wo er im Jahr 2000 mit dem Diplom in Theoretischer Physik abschloss. 2005 promovierte er mit einer Arbeit im Bereich der Quantenkryptografie, welche 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 Quantenphysik und der Informationstheorie.

Adresse: Department of Applied Mathematics and Theoretical Physics, Wilberforce Road, CB3 OWA, Cambridge, United Kingdom, Tel.: +44 1223 76 42 69, E-Mail: r.renner@damtp.cam.ac.uk