Julian Harttung 21.05.2013

Quantenkryptografie

Proseminar Kryptografische Grundlagen der Datensicherheit
Dozent: Stefan Köpsell
Lehrstuhl für Datenschutz und Datensicherheit

Einführung

Die heutzutage eingesetzten Verschlüsselungsverfahren gelten im Allgemeinen als sicher. Mit dem Aufkommen einer neuen Art von Rechnern, den Quantencomputern, werden jedoch die asymmetrischen Verschlüsselungsverfahren in ihrer Existenz bedroht. Ein solcher Computer ermöglicht es bei vielen Kryptosystemen, z.B. dem RSA-Verfahren, den privaten Schlüssel in polynomieller Zeit aus dem öffentlichen Schlüssel zu berechnen, wodurch das Verfahren unbrauchbar wird.

Aufgrund physikalischer Hürden existieren diese Rechner jedoch heutzutage nur in der Theorie und können noch nicht praktisch eingesetzt werden. Dennoch wird bereits an neuen Verschlüsselungsmöglichkeiten geforscht, die den Quantencomputern standhalten und sich selbst die Quantenphysik zu Nutze machen. Diese werden zum Bereich der Quantenkryptografie gezählt und sollen den Hauptaspekt meines Vortrags bilden.

Gliederung des Vortrags

1. Was versteht man unter Quantenkryptografie?
2. Motivation
    - 2.1. Quantencomputer als Gefahr für heutige Verfahren
    - 2.2. Shor-Algorithmus
3. Vision der Quantenkryptografie: Unbrechbarkeit
    - 3.1. No-Cloning-Theorem
4. Quantenschlüsselaustauch
    - 4.1. 1-Photonen-4-Zustände-Protokoll (BB84-Protokoll)
    - 4.2. 2-Photonen-2-Zustände-Protokoll
    - 4.3. Typisches Nutzungsszenario
    - 4.4. Angriffsszenario
5. Ausblick – Zukunft der Quantenkryptografie
6. Quellen- und Literaturverzeichnis

Zusammenfassung

1. Was versteht man unter Quantenkryptografie?

Als Quantenkryptografie wird im Allgemeinen die Verwendung quantenmechanischer Effekte als Teil kryptografischer Verfahren bezeichnet. Hier werden zur Informationsübertragung Photonen eingesetzt, die ein Qbit (das quantenmechanische Äquivalent zum herkömmlichen Bit) repräsentieren. Diese besitzen einige ungewöhnliche Eigenschaften, die ich in meinem Vortrag erläutern werde.

2. Motivation

Wie bereits in der Einführung erwähnt, stellt der Quantencomputer eine Gefahr für viele populäre Verschlüsselungsverfahren dar. Betroffen sind vor allem die asymmetrischen Verfahren, die darauf basieren, dass die Faktorisierung sehr großer Zahlen mit klassischen Mitteln extrem schwer ist. Unter Einsatz eines Quantencomputers ist für die Faktorisierung z.B. der Shor-Algorithmus nutzbar.

In meinem Vortrag möchte ich kurz auf diesen Algorithmus und seine Arbeitsweise eingehen.

3. Vision der Quantenkryptografie: Unbrechbarkeit

Die Quantenkryptografie zeichnet sich dadurch aus, dass sie im Gegensatz zu allen herkömmlichen Verschlüsselungsmethoden auf physikalischen Grundprinzipien basiert, statt auf mathematischen Algorithmen.

Die Grundlage jedes quantenkryptografischen Verschlüsselungsverfahrens ist das sogenannte No-Cloning-Theorem. Dies besagt, dass es unmöglich ist, eine exakte Kopie eines Qbits auf ein anderes zu erstellen, ohne dabei das ursprüngliche Qbit irreversibel zu verändern. Die Sicherheit quantenkryptografischer Verschlüsselung liegt also nicht darin, einen Angriff auf den Kommunikationskanal auszuschließen, sondern darin, dass sich ein Angreifer in jedem Fall bemerkbar macht, da zum Abhören des Kanals Kopien der übertragenen Qbits angelegt werden müssen. Bei klassischer Kommunikation ist diese Sicherheit nicht gegeben, da ein übertragenes Bit einfach abgefangen, kopiert und weitergeschickt werden kann, ohne dass es Sender oder Empfänger bemerken.

In meiner Präsentation werde ich das No-Cloning-Theorem kurz erläutern. Im Abschnitt über den Quantenschlüsselaustausch wird sichtbar werden, wie sich dieses Theorem auf die Informationsübertragung und -abhörung auswirkt.

4. Quantenschlüsselaustausch

Der Quantenschlüsselaustausch ist das wohl bekannteste Verfahren der Quantenkryptografie und wird heutzutage bereits experimentell eingesetzt. Hier wird ein gemeinsames Geheimnis – der Schlüssel – zwischen zwei Parteien vereinbart, welcher im Nachhinein für konventionelle symmetrische Verschlüsselungsverfahren (z.B. AES) verwendet wird.

In meinem Vortrag werde ich hier das 1-Photonen-4-Zustände-Protokoll (auch BB84-Protokoll genannt) genauer erläutern. Zudem werde ich auf das 2-Photonen-2-Zustände-Prokotoll eingehen, bei dem miteinander verschränkte Photonen zur Kommunikation verwendet werden. Für das BB84-Protokoll werde ich zudem ein typisches Nutzungsszenario schrittweise erläutern, sowie ein Angriffsszenario auf den Quantenkanal.

5. Ausblick – Zukunft der Quantenkryptografie

Obwohl bereits seit Jahrzehnten an quantenkryptografischen Verfahren geforscht wird (das BB84-Protokoll wurde bereits 1984 vorgestellt) und es bereits einige funktionierende Anwendungen gab (z.B. ein quantenkryptografisch verschlüsseltes Telefongespräch im Jahr 2008) ist diese Technik noch nicht alltagstauglich, da es noch viele technische Hürden zu überwinden gibt. Die Distanz der Datenübertragung ist begrenzt, und Signalverstärker existieren noch nicht. Zudem ist die Übertragung deutlich langsamer als das Internet. Forscher geben sich jedoch optimistisch, diese Probleme beseitigen zu können. Von manchen Forschern wird jedoch die Sicherheit der Grundprinzipien der Quantenkryptografie in Frage gestellt.

An dieser Stelle werde ich kurz auf einige Zeitungsartikel der vergangenen Jahre eingehen, um den Zuhörern einen Eindruck der Entwicklung zu geben.

6. Quellen- und Literaturverzeichnis

[1] Gilbert Brands: „Einführung in die Quanteninformatik – Quantenkryptografie, Teleportation und Quantencomputing“,
1. Auflage, eXamen.press, Springer Verlag Berlin Heidelberg, 2011

[2] Seite „Shor-Algorithmus“. In: Wikipedia, Die freie Enzyklopädie.
Bearbeitungsstand: 11. Mai 2013, 08:36 UTC.

URL: *http://de.wikipedia.org/w/index.php?title=Shor-Algorithmus&oldid=118394778*
(Abgerufen: 21. Mai 2013, 15:47 UTC)

[3] Seite „Quantenkryptographie“. In: Wikipedia, Die freie Enzyklopädie.
Bearbeitungsstand: 12. Mai 2013, 12:50 UTC.

URL: *http://de.wikipedia.org/w/index.php?title=Quantenkryptographie&oldid=118432029*
(Abgerufen: 21. Mai 2013, 15:53 UTC)

[4] Seite „Quantenschlüsselaustausch“. In: Wikipedia, Die freie Enzyklopädie.
Bearbeitungsstand: 12. April 2013, 18:30 UTC.

URL: *http://de.wikipedia.org/w/index.php?title=Quantenschl%C3%BCsselaustausch&oldid=117436990*
(Abgerufen: 21. Mai 2013, 15:54 UTC)

[5] Artikel „Quantenkryptografie: Physiker demonstrieren unknackbares Netzwerk“, SPIEGEL ONLINE, 8. Oktober 2008 - 15:36 UTC.

URL: *http://www.spiegel.de/netzwelt/tech/quantenkryptografie-physiker-demonstrieren-unknackbares-netzwerk-a-582951.html*
(Abgerufen: 21. Mai 2013, 16:00 UTC)

[6] Philipp Hummel: „Wie sicher ist Quantenkryptographie wirklich?“, ZEIT ONLINE, 17. August 2012 - 13:40 UTC.

URL: *http://www.zeit.de/digital/internet/2012-08/quantenkryptographie*
(Abgerufen: 21. Mai 2013, 16:06 UTC)

[7] Pressemitteilung „World Premiere: Bank Transfer via Quantum Cryptography Based on Entangled Photons “, Wien, 21. April 2004 - 09:30 UTC.

URL: *http://www.secoqc.net/downloads/pressrelease/Banktransfer_english.pdf*
(Abgerufen: 21. Mai 2013, 16:11 UTC)

[8] Datenblatt „Q-Box Workbench – Quantum Key Distribution System“, hergestellt von MagiQ.

URL: *http://www.magiqtech.com/MagiQ/Products_files/QBox%20Datasheet-2011.pdf*
(Abgerufen: 21. Mai 2013, 16:17 UTC)