Schlußbericht

Zuwendungsempfänger	Förderkennzeichen
E.I.S.S. Fakultät für Informatik Universität Karlsruhe Am Fasanengarten 5 76128 Karlsruhe	13N8014
Vorhabenbezeichnung Quantenkryptographie	
Laufzeit des Vorhabens 01.02.2001-31.01.2004	
Berichtzeitraum 01.02.2001-31.07.2004	

1. Aufgabenstellung

Die an das Vorhaben gestellten Aufgaben beschränkten sich anfangs auf die Fragestellung des sicheren Schlüsselaustauschs mit Quantenkryptographie. Im Antrag des Verbundprojekts wurde der Schwerpunkt auf den Schlüsselaustausch gelegt, da die bewiesene Unmöglichkeit der wichtigen kryptographischen Primitive *Bit Commitment* viele Forscher entmutigt hat nach weiteren Anwendungen zu suchen. Im Verlauf des Projektes wurde aber nachgewiesen, daß die Möglichkeiten der Quantenkryptographie über die ursprünglich gesetzten Ziele hinausgehen und die Aufgabenstellungen wurden nach dem ersten Zwischenbericht den neuen Erkenntnissen angepaßt und erweitert.
Die im Projekt zu bearbeitenden Aufgaben umfassen:

Die theoretische Untersuchung der Sicherheit quantenkryptographischer Protokolle unter Berücksichtigung des konkreten physikalischen Aufbaus. Die algorithmische Nachbearbeitung eines an der LMU in München entwickelten Quantenzufallszahlen-generators. Die Entwicklung formaler Sicherheitsmodelle für Quantenprotokolle, die insbesondere die unbedenkliche Einsetzbarkeit (universelle Komponierbarkeit) garantieren sollen sowie neuartiger quantenkryptographischer Anwendungen, die über einfache Anwendungen des Schlüsselaustauschs hinausgehen.

2. Vorraussetzungen, unter denen das Vorhaben durchgeführt wurde

Das Projekt wurde in der Zeit von 01.02.01 bis 31.12.02 von Jörn Müller-Quade geleitet und durchgeführt. Ab dem 01.01.03 war es möglich Chris Charnes für einen Monat an dem Projekt zu beteiligen. Weiterhin wurde die Projektarbeit von Jörn Müller-Quade und Dominique Unruh in Zusammenarbeit mit den Projekten PROSECCO (EU) und CrySTALS (DFG) durchgeführt. In dem Projekt Quantenkryptographie war nach dem 01.09.03 außer wissenschaftlichen Hilfskräften niemand mehr angestellt.

3. Planung und Ablauf des Vorhabens

Die Ursprüngliche Planung des Projektes bezog sich auf die reine Untersuchung von Schlüsselaustauschprotokollen und wurde im Verlauf des Vorhabens geändert und erweitert. Der Plan gliedert das Projekt in die folgenden Teilaufgaben.

III.1 Evaluierung der Sicherheit von quantenkryptographischen Primitiven.
Ziel: Eine Sicherheitsanalyse der Primitive erlaubt es, die erreichbare Sicherheit abzuschätzen. Hier soll auch auf technologische Imperfektionen der Implementierung geachtet werden.

III.2 Entwurf bzw. Anpassung von Protokollen zur Authentifikation, zum Schlüsselaustausch und zur verschlüsselten Kommunikation unter Einbeziehen von quantenkryptographischen Primitiven.

III.3 Evaluierung der von den Projektpartnern entwickelten Zufallszahlengeneratoren und Einbindung bzw. Anpassung an kryptographische Systeme.
Ziel: Realisierung eines Zufallszahlengenerators mit Qualitätsnachweis. Die Analyse der Daten, Verbesserungsvorschläge für den Generator und eine Nachbearbeitung der Daten im Rechner sollten hier realisiert werden um eine Vorhersagbarkeit der Daten auszuschließen.

III.4 Realisierung von Prototypen zur Authentifikation, zum Schlüsselaustausch und zur verschlüsselten Kommunikation unter Einbeziehen von quanten-kryptographischen Primitiven.

4. Wissenschaftlicher und Technischer Stand vor Projektbeginn

Vor Beginn des Projektes gab es einen Quantenzufallszahlengenerator der Universität Genf, der heute von der Firma idQuantique angeboten wird. Die Rate dieses Generators ist im kilobit Bereich, da die für die Zufallszahlen verwendeten Meßergebnisse eine Abhängigkeit hätten wenn häufiger gemessen würde. Das im Projekt zu entwickelnde Nachbearbeitungsverfahren sollte solche Gedächtnis-Effekte bereinigen können um eine höhere Rate zu ermöglichen.

Vor Projektbeginn war bekannt, daß die Quanten-Kryptographie gegenüber der klassischen Kryptographie den entscheidenden Vorteil hat, daß sie beweisbar sichere Schlüsselgenerierung mit informationstheoretischer Sicherheit ermöglicht [BB84,M98]. Auch für andere kryptographische Anwendungen erlaubt die Quantenkryptographie Lösungen, die von den klassischen Annahmen unabhängig sind [S98].

Der technische Stand der klassischen Kryptographie vor dem Start des Projektes wurde auch durch Arbeiten des Antragstellers bestimmt. Besonders zu erwähnen sind die Entwicklung und Realisierung des ersten kryptographischen Protokolls, das Smartcards eingesetzt hat [B91,BBKS94,BKSW94] und die erfolgreiche Kryptoanalyse von verschiedenen Systemen [B99,BLM94,SGGB00,W98].
Ein Zusammenhang von Quanten-Computing und Quanten-Kryptographie liegt in der Sicherheitsanalyse. Die Sicherheit einiger Quantenprotokolle hängt an technologischen Annahmen [S98], etwa der Begrenztheit von Quantenspeichern oder der Instabilität von Quantenzuständen. Die Sicherheitsanalyse solcher Protokolle hängt direkt mit der Analyse von quantenfehlerkorrigierenden Codes zusammen [BG98,GBP97,PBGM96]. Obwohl hochverschränkte

Zustände sehr instabil sind [JB00], könnten sie durch Fehlerkorrektur stabilisiert werden. Eine Sicherheitsanalyse muss die Möglichkeit der Fehlerkorrektur berücksichtigen, wenn technologische Annahmen gemacht wurden.
Der Angriff von Mayers auf quanten-kryptographische Bit Commitment Protokolle verwendet Quantenzustandstransformationen, die im wesentlichen einen Quantencomputer vorraussetzen. Neben der Stabilisierung und der Transformation von Quantenzuständen wurde auch die mathematische Struktur von kleinen Quantensystemen, wie sie auch in der Quanten-Kryptographie auftreten, schon vor Projektbeginn untersucht [GRB98]. Der Stand der Technik bezüglich Quanten-Authentifikationsverfahren vor Projektbeginn wird in [BKM98] beschrieben, wo ein Quanten-Authentifikationsverfahren vorgestellt und auf Robustheit bezüglich Doppelphotonen analysiert wird.

[BB84] C. Bennett und G. Brassard, „Quantum Cryptography: Public Key Cryptography and Coin Tossing“, in Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India, IEEE New York, 1984.

[B91] Th. Beth, „Keeping Secrets a Personal Matter or: The Exponential Security System TESS“, in: Proceedings of Cryptography and Coding, Cirencester, Oxford University Press, S. 1-9, 1991.

[B99] Th. Beth, „The State of Public-Key Cryptography - Not only after the Invention of Quantum Computers“, E.I.S.S. Report 3/1999, Europäisches Institut für Systemsicherheit, Universität Karlsruhe, 1999.

[BBKS94] Th. Beth, F. Bauspieß, H.-J. Knobloch und St. Stempel, „TESS - A Security System based on Discrete Exponentiation“, in: Computer Communications Journal (Special Issue) 7, S. 466-475, 1994.

[BEM94] Th. Beth, S. Egner und J. Müller-Quade, „Workshop on Quantum Cryptography and Quantum Information Theory“, E.I.S.S. Report 5/1994, Europäisches Institut für Systemsicherheit, Universität Karlsruhe, 1994.

[BG98] Th. Beth und M. Grassl, „The Quantum Hamming and Hexacodes“, Fortschritte der Physik, Special Focus Issue Quantum Computing/Quantum Cryptography Message Coding with the Help of Quantum Mechanics, Vol. 46, Nr. 4/5, 1998, S. 459-491.

[BKM98] Th. Beth, H.-J. Knobloch und J. Müller-Quade, „A Quantum Authentication Scheme“ E.I.S.S. Report 10/1998, Europäisches Institut für Systemsicherheit, Universität Karlsruhe, 1998.

[BKSW94] Th. Beth, H.-J. Knobloch, St. Stempel und P. Wichmann, „Authentifikationssystem SELANE - Modularisierung und Einsatz“, E.I.S.S Report 3/1994, Europäisches Institut für Systemsicherheit, Universität Karlsruhe, 1994.

[BLM94] Th. Beth, D. Lazic und A. Mathias, „Cryptoanalysis of Cryptosystems based on Remote Chaos Replication“, in Proceedings. CRYPTO ´94, Ed.: Y. Desmedt, Springer, LNCS 839, S. 318-331, 1994.

[BLMS99] G. Brassard, N. Lütkenhaus, T. Mor und B. Sanders, „Security Aspects of Practical Quantum Cryptography“, LANL preprint no. quant-ph/9911054.

[BL99] D. Bruß und N. Lütkenhaus, „Quantum Key Distribution: from Principles to Practicalities“, LANL preprint no. quant-ph/9901061.

[CZJW99] S. Chinangga, P. Zarda, T. Jennewein und H. Weinfurter, „Towards practical Quantum Cryptography“, Appl. Phy. B, Nr. 69, 389, 1999.

[GBP97] M. Grassl, Th. Beth und Th. Pellizzari, „Codes for the Quantum Erasure Channel“, Physical Review A, Vol. 56, Nr. 1, S. 33-38, 1997.

[GRB98] M. Grassl, M. Rötteler und Th. Beth, „Computing local invariants of quantum-bit systems“, Physical Review A, Vol. 58, Nr. 3, S. 1833-1839, 1998.

[JB00] D. Janzing und Th. Beth „Fragility of a class of highly entangled states with *n* qubits“, Physical Review A, Vol. 61, Nr. 5, S. 052308 1-10, 2000.

[JSWWZ00] T. Jennewein, Ch. Simon, G. Weihs, H. Weinfurter und A. Zeilinger, „A physical Random Number Generator“ , Rev. Sci. Instr. Nr. 41, 1675, 2000.
[KB95] A. Klappenecker und Th. Beth, „Galois Theory and Wavelet Transforms“, Proc. IEEE, IEEE Press, Whistler, Kanada, S. 132, 1995.
[KLSSSW00] N. Korolkova, G. Leuchs, S. Schmitt, C. Silerhorn, A. Sizmann, M. Stratmann, O. Weiss, „Controlling the quantum properties of optical solitons in fibers“, Nonlinear Optics, 2000.
[LL90] G. Leuchs und R. Lazecki, „Anwenderfreundliches Laserinterferometer in Glasfasertechnik zur Maschinenüberwachung“ VDI-Bericht Nr. 836, S. 169-184, VDI-Verlag, Düsseldorf, 1990.
[L99] H.-K. Lo, „A simple proof of the unconditional security of quantum key distribution“, LANL preprint no. quant-ph/9904091.
[M98] D. Mayers, „Unconditional Security in Quantum Cryptography“, LANL preprint no. quant-ph/9802025.
[PBGM96] Th. Pellizzari, Th. Beth, M. Grassl und J. Müller-Quade, „Stabilization of Quantum States in Quantum Optical Systems“, Physical Review A, Vol. 54, Nr. 4, S. 2698-2702, 1996.
[R99] M. O. Reid, „Quantum Cryptography using continous Variable Einstein-Podolsky-Rosen correlations and quadrature phase amplitude measurements“, LANL preprint no. quant-ph/9909030.
[RB99] M. Rötteler und Th. Beth, „Efficient Realisation of Discrete Cosine Transforms on a Quantum Computer“, in Proceedings X. International Symposium on Theoretical Electrical Engineering (ISTET'99), Magdeburg, S. 85-89, 1999.
[RPB99] M. Rötteler, M. Püschel und Th. Beth, „Fast Signal Transforms for Quantum Computers“, in Proceedings Workshop „Physik und Informatik“, DPG-Frühjahrstagung, Heidelberg, S. 31-43, 1999.
[S98] L. Salvail, „Quantum Bit Commitment from a Physical Assumption“, in Proceedings Crypto 1998, Ed. H. Krawczyk, Springer, LNCS 1462, S. 338-354,1998.
[SGGB00] R. Steinwandt, M. Grassl, W. Geiselmann und Th. Beth, „Weaknesses in the $SL_2(F_{2^n})$ Hashing Scheme“, in Proceedings Crypto 2000, Ed. M. Bellare, Springer, LNCS 1880, S. 288-301, 2000.
[W98] P. Wichmann, „Systematische Analyse von Kryptosystemen“, Dissertation Universität Karlsruhe, 1998.

5. Zusammenarbeit mit anderen Stellen

Die wichtigste Zusammenarbeit während des Projektes war naturgemäß mit der Gruppe von Gerd Leuchs an der Universität Erlangen-Nürnberg und der Gruppe von Harald Weinfurter an der LMU in München. Insbesondere für die Entwicklung des Nachbearbeitungsverfahrens für den an der LMU entwickelten Zufallszahlengenerator war eine Zusammenarbeit unverzichtbar.

Weiterhin bestand im Rahmen des Projektes Kooperation mit Chris Charnes (Deakin University, Burwood, Victoria), Adrian Kent (Cambridge University), Hans Briegel (Universität Innsbruck), Louis Salvail (Aarhus Universitet), Anderson Nascimento und Hideki Imai (beide University of Tokyo).

6. Erzielte Ergebnisse

Im Rahmen des Vorhabens wurden die nachfolgenden Ergebnisse erzielt. Dabei sind Ergebnisse, die nach dem 01.01.03 erarbeitet wurden, sind in Zusammenarbeit mit den Projekten PROSECCO und CrySTALS entstanden.

- Der Beweis der Existenz eines abstreitbaren Quantenschlüsselaustauschs, der auch Sicherheit gegen Erpressung gibt,
- die Entwicklung eines Quantenauthentifikationsverfahrens für ein quanten-kryptographisches Protokoll, das eine andauernde Verkehrsanalyse eines Kommunikationskanals erkennt,
- Quanten-Mehrparteienprotokolle, die nach ihrer Terminierung eine bessere Geheimhaltung bieten als alle klassisch möglichen Verfahren und
- der Vorschlag neuer Verfahren zur algorithmischen Nachbearbeitung einer Quanten-zufallszahlenquelle.
- Die Entwicklung formaler Sicherheitsmodelle für Quantenprotokolle, die insbesondere die unbedenkliche Einsetzbarkeit (universelle Komponierbarkeit) garantieren sollen.
- Ein neues Signaturverfahren: „quantum pseudosignatures“, das beweisbare Vorteile im Vergleich zu jedem klassischen Signaturverfahren hat.
- Ein klassisch unmögliches Verfahren „anonymous quantum key exchange“, welches einen Schlüsselaustausch mit unbekanntem Empfänger erlaubt.
- Eine informationstheoretische Betrachtung von *Quantum Secret Sharing.*
- Kryptoanalyse eines Banktransfer Protokolls.
- Der formale Sicherheitsbeweis eines Verfahrens zur geheimen Nachrichtenübertragung, das auf einem Schlüsselaustausch, dem One Time Pad und der Nachrichtenauthentifikation beruht.

Nachfolgend wird genauer auf die einzelnen Ergebnisse und ihre Einordnung in den Kontext der Projektaufgaben eingegangen.

Zu Teilaufgabe III.1

Die erste Teilaufgabe widmet sich insbesondere der Evaluierung der Sicherheit quantenkryptographischer Primitive unter Berücksichtigung imperfekter Realisierungen.
Ein Schwerpunkt lag dabei auf der Primitive *Deniable Quantum Key Exchange* (abstreitbarer Schlüsselaustausch). Ein Quantenschlüsselaustauschprotokoll heißt abstreitbar, wenn ein Angreifer nicht einmal genug Informationen über Zwischenergebnisse des Protokolls sammeln kann, um die Herausgabe eines Schlüssels erzwingen zu können.
Es ist leicht zu sehen, daß das Schlüsselaustauschverfahren nach Bennett und Brassard nicht abstreitbar ist, da ein Angreifer Informationen über den Rohschlüssel sammeln und dessen Herausgabe somit erzwingen kann. Aus dem Rohschlüssel und der über den unsicheren Kanal ausgetauschten Information kann der geheime Schlüssel errechnet werden.
Auf dem Verbundprojekttreffen am 22.10.01 in Erlangen wurde ein Beweis vorgestellt, daß das Schlüsselaustauschverfahren aus [DEJMPS96] abstreitbar ist. Im Gegensatz zu dem in [B02] vorgeschlagenen Verfahren lässt sich die Sicherheit des in Erlangen vorgestellten Verfahrens auch für imperfekte Apparate beweisen.
Für die Sicherheit des Quantenschlüsselaustauschprotokolls über die Luftschnittstelle, das von H. Weinfurter und C. Kurtsiefer realisiert und auf den Verbundprojekttreffen vorgestellt wurde, bleiben die Argumente aus dem Papier [BLMS00] gültig. Speziell für den Prototypen bedeutet dies, daß eine Luftschnittstelle, die einen höheren Verlust an Photonen hat als die

Rate an Einzelphotonen der verwendeten Photonenquelle, keinen sicheren Schlüsselaustausch erlaubt ohne weitere Annahmen zu verwenden. Um die theoretisch mögliche Sicherheit des Quantenschlüsselaustauschs auch für die Luftschnittstelle zu erreichen sind also Einzelphotonenquellen, wie sie in München entwickelt werden, unablässig.

Jeder wissenschaftlichen Sicherheitsanalyse liegt ein Modell zugrunde. Im Fall von Quantenprotokollen sind diese Modelle bislang für die meisten kryptographischen Primitive einzeln betrachtet worden ohne darauf zu achten, ob die einzelnen Protokolle zusammen benutzt immer noch sicher sind. Die Arbeit von Ran Canetti [Can01] resultierte in einem formalen Sicherheitsmodell, welches diese Problematik für klassische Protokolle mitberücksichtigt. Aufbauend auf [Can01] wurde am E.I.S.S. ein sehr allgemeines Sicherheitsmodell für Quantenprotokolle aufgestellt, in dem ein „composition theorem“ gilt. Dieses Ergebnis verallgemeinert das ähnlich lautende Hauptergebnis von [Can01] auf Quantenprotokolle. Anschaulich besagt das Theorem, daß eine als sicher bewiesene kryptographische Anwendung sicher bleibt, wenn man die verwendeten, als sicher vorausgesetzten Primitive durch sichere Realisierungen ersetzt. Obwohl sich dieses wie eine Selbstverständlichkeit anhört, ist das Ergebnis nichttrivial, da in der Kryptographie Sicherheitslücken häufig nicht durch unsichere Realisierungen grundlegender Primitive, sondern durch deren falschen Gebrauch entstehen.

Die Ergebnisse sind zusammen mit Dominique Unruh entwickelt worden und in dessen Studienarbeit dokumentiert [Unr02] sowie in dem kürzlich erschienenen detaillierten Sicherheitsmodell [Unr04]. Die Untersuchungen brachten einige Subtilitäten ans Licht, die bisher in einfacheren Modellen nicht bemerkt wurden. Etwa die völlig neue Definition der interaktiven Quanten-Turing-Maschine, die über eine nichtkonstante Anzahl von Kommunikationsbändern verfügen muss, damit die Länge einer Nachricht nicht gemessen werden muss. Trotz der Allgemeinheit des Modells blieb das „scheduling“ klassisch ebenso wie Absender und Empfänger einer Nachricht klassische Information sind.

Das vielleicht wichtigste Ergebnis, das mit diesem Modell gewonnen werden konnte, besagt, daß klassisch informationstheoretisch sichere Mehrparteienprotokolle auch dann noch sicher bleiben, wenn der Angreifer, ebenso wie korrumpierte Parteien, über beliebige Quantentechnologie verfügen. Dies bedeutet, daß es durchaus klassische kryptographische Verfahren gibt, die nicht durch Fortschritte in der Quantentechnologie unsicher werden.

[B02] D. Beaver „On Deniability in Quantum Key Exchange“ Advances in Cryptology EUROCRYPT 2002, LNCS, Springer Verlag, 2002.

[BLMS00] G. Brassard, N. Lütkenhaus, T. Mor, and T. Sander „Security Aspects of Practical Quantum Cryptography“, Advances in Cryptology EUROCRYPT 2000, LNCS, Springer Verlag, 2000.

[Can01] R. Canetti „Universally Composable Security: A New Paradigm for Cryptographic Protocols“, Preprint 2000/67 im ePrint Archiv der IACR, www.iacr.org, 2001.

[DEJMPS96] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera „Quantum Privacy Amplification and the Security of Quantum Cryptography Over Noisy Channels“, Phys, Rev. Lett. 1996.

[Unr02] D. Unruh „Formale Sicherheit in der Quantenkryptologie“ Studienarbeit, E.I.S.S.,

Universität Karlsruhe, 2002.

[Unr04] D. Unruh, „Simulatable security for quantum protocols“, Los Alamos Preprint quant-ph/0409125, 2004.

Zu Teilaufgabe III.2

Teilaufgabe III.2 beschäftigte sich vorrangig mit der Entwicklung neuer quanten-kryptographischer Protokolle. Bei der Sicherheitsanalyse von Protokollen ist es wichtig nicht nur einzelne Primitive zu betrachten sondern vollständige Protokolle. Für Quantenschlüsselaustauschprotokolle bedeutet dies insbesondere die Berücksichtigung von Authentifikation und der nötigen Nachbearbeitung des Rohschlüssels. Das Schlüsselaustauschverfahren von [DEJMPS96], welches am E.I.S.S. als abstreitbar bewiesen werden konnte, bedarf eines zusätzlichen Nachbearbeitungsschrittes, wenn man imperfekte Apparate annimmt. Die bei perfekten Geräten nur nötigen *Privacy Amplification* und *Information Reconciliation* werden von der Verschränkungsreinigung übernommen. Bei imperfekten Apparaten jedoch ist eine weitere klassische *Information Reconciliation* nach der Verschränkungsreinigung und Messung nötig. Daß dieser zusätzliche Schritt die Eigenschaft der Abstreitbarkeit nicht zunichte macht, konnte am E.I.S.S. bewiesen werden. Die Möglichkeit eines abstreitbaren Schlüsselaustauschs unter realistischen Bedingungen zeigt, daß auch Quantenprotokolle, die über den normalen Schlüsselaustausch hinausgehen konkrete Anwendung finden könnten.

Im Berichtszeitraum wurde ein in Karlsruhe entwickeltes Protokoll zur Erkennung einer andauernden Verkehrsanalyse veröffentlicht. Klassisch kann man eine Verkehrsanalyse nicht erkennen und eine solche Analyse höchstens durch zusätzliche sinnlose Nachrichten erschweren.
Die Lösung von Steinwandt, Janzing und Beth benutzt Interferenzexperimente um festzustellen ob der Nachrichtenkanal überwacht wird. Im Gegensatz zu Schlüsselaustauschverfahren wird es sogar bemerkt wenn ein Angreifer auch nur die Existenz eines Photons messen will.
In [SJB01] wird davon ausgegangen, daß das Problem der Authentifikation gelöst sei. Nur unter dieser Annahme ist das Protokoll sicher. Auf dem Verbundprojekttreffen am 22.10.01 in Erlangen wurde ein Angriff auf das obige Protokoll vorgestellt, der beweist, daß klassische Nachrichten-Authentifikationscodes für dieses Protokoll nicht hinreichend sind, denn der Angreifer will ja nur die Existenz beziehungsweise die Länge einer Nachricht messen und diese nicht abändern. Ob die Nachricht authentisch ist sagt nichts darüber aus, ob zwei Kommunikationspartner direkt verbunden sind oder ob die Nachrichten von einem „transparenten“ Angreifer weitergeleitet werden. Ein neuartiges zeitabhängiges Authentifikationsverfahren wurde daraufhin am E.I.S.S. entwickelt und zusammen mit dem Angriff in [MS03] vorgestellt.

In der klassischen Kryptographie werden häufig digitale Signaturen verwendet um Nachrichten oder Parteien zu authentifizieren. In der Quantenkryptographie wurden digitale Signaturen bisher kaum beachtet, da sie die Existenz von „trapdoor permutations“ vorauszusetzen scheinen und damit niemals informationstheoretische Sicherheit bieten können.

In der klassischen Kryptographie sind informationstheoretische Signaturverfahren, als spezielle Mehrparteienberechnungen, schon länger bekannt [CR90,PW92]. Später wurde ein

quantenkryptographisches Signaturverfahren vorgeschlagen [CG01], von dem aber nicht bewiesen wurde, daß es eine höhere Sicherheit bietet als die klassischen Verfahren.

Ein wichtiges Problem blieb unbeachtet. In allen prinzipiell möglichen klassischen informationstheoretisch sicheren Signaturverfahren kann das Protokoll von den Teilnehmern abgebrochen werden, wobei nicht unterschieden werden kann ob der Abbruch auf den Unterzeichner zurückgeht. Dies ist ein für Signaturzwecke sehr schwerwiegender Nachteil. Ein Unterzeichner kann eine Unterschrift verweigern, ohne daß er dessen beschuldigt werden kann.

Ein wichtiges Teilproblem, dessen Lösung schon für sich genommen einen Fortschritt darstellt, ist ein Schlüsselaustauschprotokoll mit unbekanntem Empfänger. Das Protokoll „anonymous key exchange“ erlaubt es einer Partei Alice mit Parteien Bob und Carol Schlüssel auszutauschen so, daß Alice nicht wissen kann, wer welchen Schlüssel mit ihr gemeinsam hat.

Im Rahmen von Teilaufgabe II.2 wurde das erste quantenkryptographische Protokoll entwickelt, welches erlaubt in jeder Situation festzustellen, ob der Unterzeichner die Unterschrift verweigert. Das Protokoll wurde im Journal of Modern Optics veröffentlicht [MQ02] und stellt das derzeit sicherste bekannte Signaturverfahren dar.

Eine kryptographische Primitive, die, im Gegensatz zu den bisher geschilderten Primitive, nicht nur Quanteneffekte nutzt, sondern dem Schutz von Quanteninformation dient ist *Quantum Secret Sharing*. Diese Primitive wurde im Rahmen des Projektes weiterentwickelt [NMI01] und mit informationstheoretischen Methoden analysiert [IMNTW03].

[DEJMPS96]] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera „Quantum Privacy Amplification and the Security of Quantum Cryptography Over Noisy Channels“, Phys, Rev. Lett. 1996.

[SJB01] R. Steinwandt, D. Janzing, Th. Beth „On using quantum protocols to detect traffic analysis“, Quantum Information and Computation, 1(3), 2001.

[MS03] J. Müller-Quade and R. Steinwandt. On the problem of authentication in a quantum protocol to detect traffic analysis. *Quantum Information and Computation*, 3(1): 48-54, 2003

[CR90] D. Chaum und S. Roijakkers „Unconditionally Secure Digital Signatures“, Advances in Cryptology: CRYPTO 90, Band 537 der LNCS, Springer Verlag, 1990.

[PW92] B. Pfitzmann und A. Waidner „Unconditional Byzantine Agreement for any Number of Faulty Processors“ , Proc. of STACS, Band 577 der LNCS, Springer Verlag, 1992.

[MQ02] J. Müller-Quade „Quantum pseudosignatures“, Journal of Modern Optics, Band 49, Nr. 8, 2002.

[GC01] D. Gottesman and I. Chuang „Quantum Digital Signatures“, Preprint quant-ph/0105032 auf dem Los Alamos Preprint Server xxx.lanl.gov, 2001.

[NMI01] A. Nascimento, J. Müller-Quade and H. Imai. Improving quantum secretsharing schemes. *Physical Review A*, 64, Oktober 2001.

[IMNTW03] H. Imai, J. Müller-Quade, A. Nascimento, P. Tuyls and A. Winter. An Information Theoretical Model for Quantum Secret Sharing Schemes. Online available at: http://xxx.lanl.gov/abs/quant-ph/0311136, to appear at *Quantum Information and Computation*, 2003.

Zu Teilaufgabe III.3

Bei vielen kryptographischen Verfahren, wie etwa bei dem Quantenschlüsselaustausch nach Bennett und Brassard, werden Zufallszahlen benötigt und häufig ist die Rate mit der die Zufallszahlen generiert werden können ein limitierender Faktor für die Effizienz eines Verfahrens.
Ein kommerziell verfügbarer Quantenzufallszahlengenerator, der unter N. Gisin an der Universität von Genf entwickelt wurde liefert Zufallszahlen im Kilohertzbereich. Nicht schnell genug wenn damit Schlüssel für Kanäle mit hoher Bandbreite generiert werden sollen.
In der Gruppe von H. Weinfurter wurde ein Quantenzufallszahlengenerator entwickelt, der im Megahetzbereich betrieben werden kann. Die so gewonnenen Zufallszahlen sind aber noch nicht ideal gleichverteilt, was eine Nachbearbeitung nötig macht. Die Nachbearbeitung beschränkt sich dabei nicht nur auf die Beseitigung einer unterschiedlichen Häufigkeit von 0 und 1, da statistische Tests ergeben haben, daß die Zufallsquelle ein Gedächtnis hat. Im Projekt wurde ein effizientes Nachbearbeitungsverfahren speziell für diese Quelle entwickelt werden. Allgemeine Zufallsextraktoren konnten für diese Aufgabe nicht verwendet werden, da diese eine weitere unabhängige Zufallsquelle benötigen, die hier nicht zur Verfügung stand. Das neue Verfahren wurde zusammen mit Mathias Haag und Dominique entwickelt.
Die ersten Erfolge dabei sind in der Diplomarbeit von Mathias Haag [Haa02] zusammengefasst. Die Diplomarbeit entwickelt formale Modelle der in München entwickelten Zufallsquelle. Die Modelle sind eine Verallgemeinerung der in der Literatur beschriebenen Modelle und sind besonders geeignet für Quellen mit kontinuierlichem Ausgabestrom. Für das in der Diplomarbeit vorgestellte Modell ist eine sehr einfache Form der Nachbearbeitung möglich, die Zufallszahlen beweisbar guter Qualität liefert. Aufbauend auf diesen Ergebnissen gelang es zusammen mit Dominique Unruh ein wesentlich allgemeineres Modell aufzustellen. Die einzige Anforderung für eine Nachbearbeitung in dem allgemeineren Modell ist eine Annahme über die Wahrscheinlichkeit des wahrscheinlichsten Wortes (und damit über die min-Entropie) in jeder zusammenhängenden Teilfolge fester Länge. Die zugehörige Größe wurde *gefensterte min-Entropie* genannt. Um die gegebene Quantenzufallsquelle zu modellieren wurden „controlled hidden Markoff“-Modelle verwendet. Für ein solches Modell konnte die gefensterte min-Entropie mathematisch abgeleitet werden. Das resultierende Nachbearbeitungsverfahren konnte damit adaptiv gemacht werden und sich der jeweils gegebenen min Entropie anpassen. Der Hauptvorteil der zusammen mit Dominique Unruh entwickelten Nachbearbeitungsverfahren ist damit ihre Robustheit gegen eine Veränderung der zugrunde liegenden Annahmen. Während die meisten Nachbearbeitungsverfahren ihre Qualität nur garantieren solange die zugrunde liegenden Annahmen gültig sind ändert das im Rahmen von Teilaufgabe III.3 entwickelte Verfahren nur die Rate mit der Zufallszahlen produziert werden. In der kryptographischen Praxis bedeutet dies, daß ein Defekt der Zufallsquelle nicht die Sicherheit sondern nur die Betriebsbereitschaft beeinträchtigt.
Die Ergebnisse wurden in der Diplomarbeit [Unr03] genauer beschrieben.

[Haa02] M. Haag „Extraktion zufälliger Bits aus physikalischen Quellen“, Diplomarbeit, E.I.S.S., Universität Karlsruhe, 2002.

[Unr03] D. Unruh „Zufallsextraktoren für Quellen variierender Qualität“, Diplomarbeit, E.I.S.S., Universität Karlsruhe, 2003.

Zu Teilaufgabe III.4

Teilaufgabe 4 betrachtete die prototypische Realisierbarkeit der im Rahmen des Projektes entwickelten Protokolle.
Für die im Rahmen des Projektes entwickelten Quanten-Mehrparteienberechnungen [MQ01] ist eine solche prototypische Realisierung denkbar, da die verwendeten Quantenoperationen alle bei Quantenschlüsselaustauschverfahren prototypisch umgesetzt wurden. Die Protokolle können, basierend auf einer Arbeit von Mayers [M96], rauschtolerant durchgeführt werden.
Eine prototypische Realisierung des oben vorgestellten abstreitbaren Quantenschlüsselaustauschs gestaltet sich weitaus schwieriger, da Verschränkungsreinigung nötig ist. Verschränkungsreinigung stellt immer noch eine große Herausforderung für Experimentalphysiker dar. Da das abstreitbare Schlüsselaustauschverfahren aber auch mit imperfekten Apparaten funktionieren kann, ist eine zukünftige prototypische Umsetzung denkbar.
Die Frage der prinzipiellen Realisierbarkeit des Protokolls für die Erkennung von Verkehrsanalyse bleibt weiterhin offen. Da der Verlust von Photonen im Kanal ununterscheidbar ist von einer Verkehrsanalyse, stellt sich sogar die Frage, ob das vorgeschlagene Protokoll vielleicht prinzipiell nicht praktisch realisierbar ist.

Die technologischen Anforderungen an eine Realisierung von Quantenpseudosignaturen [MQ02] sind anders als die Anforderungen für einen Schlüsselaustausch. Bei einer Realisierung eines Schlüsselaustauschs ist die überbrückte Entfernung eines der Hauptprobleme. Dahingegen sind Quantenpseudosignaturen auch schon über kürzere Distanzen sinnvoll. Da die resultierende Signatur rein klassisch ist (im Gegensatz zu [CG01]) wird nach der Erstellung der Signatur sowie für eine Verifikation keine Quantentechnik benötigt. Trotzdem bleibt eine Schwierigkeit bei der Realisierung von Quantenpseudosignaturen. Zwei Teilnehmer müssen in der Lage sein einen Schlüsselaustausch über eine dritte beteiligte Partei auszuführen, so daß es dem Empfänger nicht möglich ist zu beurteilen, ob der Schlüssel über die dritte Partei oder direkt von der dritten Partei kommt. Diese Anforderung muss bei Realisierungen berücksichtigt werden. So sollten weder die Fehlerrate noch irgendwelche Antwortzeiten Rückschlüsse auf den wahren Absender liefern.

[MQ01] J. Müller-Quade „Quantum Multiparty Computations“, Poster at the QUICK Workshop, Cargèse, Corsica 2001.

[M96] D. Mayers „Quantum Key Distribution and String Oblivious Transfer on Noisy Channels“, Advances in Cryptology EUROCRYPT 1996, LNCS, Springer Verlag, 1996.

[GC01] D. Gottesman and I. Chuang „Quantum Digital Signatures“, Preprint quant-ph/0105032 auf dem Los Alamos Preprint Server xxx.lanl.gov, 2001.

[MQ02] J. Müller-Quade „Quantum pseudosignatures“, Journal of Modern Optics, Band 49, Nr. 8, 2002.

7. Voraussichtlicher Nutzen

Die auf allen gesellschaftlichen Ebenen erfolgte Abhängigkeit von elektronischer Datenverarbeitung und -übertragung zieht zunehmend die Notwendigkeit abhörsicherer Kommunikation und sicherer Berechnungsvorgänge nach sich. Die Quantenkryptographie kann hier eine über die klassisch erreichbare Sicherheit hinausgehende Sicherheitsgarantie geben. Damit ist eine Vermarktung möglich für Kunden, die sehr großen Wert auf Sicherheit legen (müssen). Als potentielle Kunden kämen Banken und Versicherungen in Frage oder auch Ministerien, die in Berlin nah genug beieinander liegen, um eine sichere quantenkryptographische Verbindung mit heutiger Technik zu erlauben. Auch Strecken wie die, für unsere Regierung wichtige, Verbindung von Bonn und Berlin wären mit quantenkryptographischen Methoden sicherer zu machen. Allerdings benötigt man für Entfernungen dieser Größenordnung heute immer noch vertrauenswürdige Zwischenstationen. Eine Kombination mit klassischen Verfahren könnte aber sicherstellen, daß es nicht genügt eine der Stationen zu korrumpieren und, selbst wenn zu viele Stationen korrumpiert sind die Sicherheit nicht unter die von klassischen Verfahren fällt.

Der im Projekt entwickelte Quanten-Zufallszahlengenerator beruht auf wesentlich elementareren Prinzipien als alle üblichen Verfahren zur Generierung von Pseudo-Zufallszahlen und bietet in kryptographischen Anwendungen zusätzliche Sicherheit, da die Zufallszahlen statistisch ununterscheidbar von echtem Zufall sind und damit keine Schwachstelle darstellen wie es herkömmliche Pseudozufallszahlen manchmal sind. Mit der Einbindung eines solchen Gerätes in ein Chiffriermodul würde ein Produkt verfügbar, das Marktchancen hat, die angesichts der Verbreitung von Public-Key-Verfahren auf nicht vertrauenswürdiger Soft- und Hardware nicht zu vernachlässigen sind.
Einfache und billige Module zur Erzeugung von wissenschaftlich gesicherter Zufälligkeit sind für viele Anwendungen in Forschung und Entwicklung attraktiv, nicht zuletzt weil probabilistisch arbeitende Simulationsverfahren durch statistische Verzerrungen verfälscht werden können.

8. Fortschritte von anderer Stelle

Die Quantenkryptographie ist ein sehr lebhaftes Gebiet und es ist kaum möglich den ganzen Fortschritt, der in der Theorie, wie im Experiment in der Projektlaufzeit stattfand hier darzustellen. In diesem Abschnitt werden deshalb nur solche Arbeiten besprochen, die in direktem Zusammenhang mit Fragestellungen des Antrags oder den im Projekt erzielten Ergebnissen stehen.

Die Ergebnisse im Bereich des abstreitbaren Schlüsselaustauschs waren motiviert von einem Gespräch mit Donald Beaver auf der EUROCRYPT 2001. Im Rahmen dieses Gesprächs wurde das im Projekt entwickelte Verfahren schon in Ansätzen gefunden. Beaver veröffentlichte ein anderes Verfahren in [Bea02], das wahrscheinlich sicher ist, für das aber die Sicherheit nicht bewiesen wurde.
Ein im Antrag stark hervorgehobenes Thema ist die Sicherheit des Schlüsselaustauschs unter realen Bedingungen mit imperfekten Geräten. Der größte Fortschritt auf diesem Gebiet

während der Projektlaufzeit war die Veröffentlichung von [BLMS00]. Dort werden verschiedene praktische Unzulänglichkeiten in die bestehenden Sicherheitsbeweise eingearbeitet, um bessere Abschätzungen für die real erreichbaren Entfernungen und Raten von quantenkryptographischen Geräten zu erhalten.

Die Definition von Sicherheit, nicht nur für quantenkryptographische Protokolle, war ein wichtiges Thema für die Forschungsarbeit in diesem Projekt. Die Wichtigkeit einer guten Definition war vor Projektbeginnn nicht absehbar und ist im Antrag deshalb kaum Berücksichtigt. Die Arbeit wurde motiviert von [Can01], obwohl die meisten Ergebnisse später mit dem Modell von [PW01] erzielt wurden.

In der Arbeit [SJB01] wurde ein neuartiges Verfahren zur Erkennung einer andauernden Verkehrsanalyse vorgestellt. Leider führte eine zu optimistische Einschätzung der Fähigkeiten klassischer Authentifikationsverfahren dazu, daß das Verfahren, wie vorgestellt, nicht sicher ist. Ein neues Authentifikationsverfahren speziell für dieses Quantenprotokoll wurde, wie oben dargestellt, im Rahmen des Projektes gefunden.

Die Veröffentlichung [GC01] beschreibt ein informationstheoretisch sicheres Signaturverfahren auf Basis quantenkryptographischer Techniken. Diese Arbeit berücksichtigte aber nicht die klassisch existierenden Verfahren weshalb das im Projekt entwickelte Signaturverfahren das erste Verfahren ist, das einen beweisbaren Vorteil über alle klassischen Verfahren hat.

[B02] D. Beaver „On Deniability in Quantum Key Exchange“ Advances in Cryptology EUROCRYPT 2002, LNCS, Springer Verlag, 2002.

[BLMS00] G. Brassard, N. Lütkenhaus, T. Mor, and T. Sander „Security Aspects of Practical Quantum Cryptography“, Advances in Cryptology EUROCRYPT 2000, LNCS, Springer Verlag, 2000.

[Can01] R. Canetti „Universally Composable Security: A New Paradigm for Cryptographic Protocols“, Preprint 2000/67 im ePrint Archiv der IACR, www.iacr.org, 2001.

[PW01] B. Pfitzmann und M. Waidner „A Model for Asynchronous Reactive Systems and its Application to Secure Message Transmission“, IEEE Symposium on Security and Privacy, 2001.

[SJB01] R. Steinwandt, D. Janzing, Th. Beth „On using quantum protocols to detect traffic analysis“, Quantum Information and Computation, 1(3), 2001.

[GC01] D. Gottesman and I. Chuang „Quantum Digital Signatures“, Preprint quant-ph/0105032 auf dem Los Alamos Preprint Server xxx.lanl.gov, 2001.

9. Erfolgte Veröffentlichungen

[Unr02] D. Unruh „Formale Sicherheit in der Quantenkryptologie“ Studienarbeit, E.I.S.S., Universität Karlsruhe, 2002.

[Unr04] D. Unruh, „Simulatable security for quantum protocols“, Los Alamos Preprint quant-ph/0409125, 2004.

[MS03] J. Müller-Quade and R. Steinwandt. On the problem of authentication in a quantum protocol to detect traffic analysis. *Quantum Information and Computation*, 3(1): 48-54, 2003

[MQ02] J. Müller-Quade „Quantum pseudosignatures“, *Journal of Modern Optics*, Band 49, Nr. 8, 2002.

[Haa02] M. Haag „Extraktion zufälliger Bits aus physikalischen Quellen“, Diplomarbeit, E.I.S.S., Universität Karlsruhe, 2002.

[Unr03] D. Unruh „Zufallsextraktoren für Quellen variierender Qualität“, Diplomarbeit, E.I.S.S., Universität Karlsruhe, 2003.

[MQ01] J. Müller-Quade „Quantum Multiparty Computations“, Poster at the QUICK Workshop, Cargèse, Corsica 2001.

[NMI01] A. Nascimento, J. Müller-Quade and H. Imai. Improving quantum secret sharing schemes. *Physical Review A*, 64, Oktober 2001.

[IMNTW03] H. Imai, J. Müller-Quade, A. Nascimento, P. Tuyls and A. Winter. An Information Theoretical Model for Quantum Secret Sharing Schemes. Online available at: http://xxx.lanl.gov/abs/quant-ph/0311136, to appear at *Quantum Information and Computation*, 2005.