Is unconditionally secure Quantum Cryptography unbreakable?

Rajagopal Nagarajan
Department of Computer Science
University of Warwick
Coventry CV4 7AL, UK
biju@dcs.warwick.ac.uk

> *If computers that you build are quantum,*
> *Then spies everywhere will all want 'em.*
> *Our codes will all fail,*
> *And they'll read our email,*
> *Till we get crypto that's quantum and daunt'em.*
>
> — Jennifer and Peter Shor

The ability to communicate information secretly has been important for many centuries and is an integral part of life in modern society. However, cryptographic systems in use today rely on unproven mathematical assumptions, such as the difficulty of factoring large integers. This means that if fast procedures for factoring large integers are discovered, the whole privacy and discretion of cryptosystems could vanish instantly. For example, the celebrated algorithm of Shor[12] demonstrates that quantum computers can perform factoring much faster than classical computers. Clearly current security technology is highly vulnerable to unexpected mathematical discoveries, increase in computing power, and to the advent of new technologies. Although the possibility of a quantum–mechanical computer is a threat to cryptosystems in use today, the use of quantum effects can also enable more powerful modes of secure communication. Quantum Cryptography, or more specifically Quantum Key Distribution, uses the laws of physics to provide a provably secure[8] method of distributing keys. Heisenberg's uncertainty principle, as well as the phenomenon of quantum entanglement, can be exploited in a system of secure communication, which, in principle, is unbreakable.

Quantum cryptography is rapidly becoming a practical technology: secure communication based on quantum–mechanical principles has recently been used in a real–world scenario, in order to transfer a sum of money from the Vienna City Hall to an Austrian bank. Quantum cryptographic systems are commercially available; the companies MAGIQ, ID QUANTIQUE and NEC are already marketing devices for this purpose. Notably, plans have been reported to establish a nationwide quantum communication network in Singapore. The DARPA defense agency in the United States is implementing a quantum network,[3] while a European research consortium (SECOQC), in which we are involved, has been formed with similar objectives.

The major selling point of Quantum Cryptography is absolute security. *But can this be guaranteed?* Even when protocols have been mathematically proved to be secure, it is notoriously difficult to achieve robust and reliable implementations of secure systems; security can be compromised by flaws at the implementation level or at the system boundaries. Real world applications of quantum key distribution must take into account real world problems. No system for quantum cryptography is going to be ideal, and therefore checks must be made to ensure that minor flaws in the quantum or classical components, or amongst their interfaces will not lead to major flaws in the security of the overall system.

Quantum communication is perfectly secure only in principle and would benefit from further thorough investigation. Computer scientists have developed an impressive armoury of techniques and tools for formal modelling, analysis and verification of classical security protocols and communication systems which use them.[10] These techniques have been remarkably successful, both in establishing the security of new protocols and in demonstrating flaws in protocols which had previously been believed to be secure. For example, Lowe[7] used the model checker FDR to discover a flaw in the well–known Needham–Schroeder authentication protocol which had been proposed several years previously and suggested a fix for it. While current analyses of quantum protocols use a traditional mathematical approach and require considerable understanding of the underlying physics, we argue that automated verification techniques provide an elegant alternative.We have recently established fundamental and general techniques for formal verification of quantum protocols.[5] We have demonstrated these techniques through the use of PRISM,[6] a probabilistic model-checking tool. Our approach is conceptually simpler than existing proofs, and allows us to disambiguate protocol definitions and assess their properties. It will also facilitate detailed analyses of actual implemented systems.

As a foundation for our work we would like to have a formal language which can be used for modelling communication and cryptographic systems with both classical and quantum elements. This will allow the behaviour of systems to be accurately defined, which is an essential prerequisite for formal verification. System models will then be validated using the low-level modelling and analysis techniques developed, including the PRISM model-checker. In future, we will investigate the formulation of behavioural properties in type-theoretic terms, with the aim of carrying out verification by type-checking. The use of automated theorem-proving systems could also be considered in the long-term. We hope to be able to model the quantum and classical components of cryptographic protocols such as BB84[1] or Ekert's protocol,[2] then specify suitable correctness properties, and automatically translate the model and specifications into the low-level analysis framework.

We already have a design[4] of the high-level modelling language, which we call *Communicating Quantum Processes* (CQP), for combined quantum and classical communication and cryptographic systems. CQP combines the communication primitives of the pi calculus[9] with the quantum data processing and measurement primitives of Selinger's language QPL,[11] as well as classical data processing primitives. As an illustration of our techniques we have been able to demonstrate the modelling of a range of quantum protocols (such as superdense coding, quantum teleportation, and quantum error correction) and verification of their basic correctness properties. Our results provide a foundation for further work on modelling and analysing larger systems such as those used for quantum cryptography, in which basic protocols are used as components. More generally, we would like to be able to perform end-to-end verification of larger systems in which protocols such as teleportation are embedded. Our ultimate aim is to be able to model and verify complete systems such as BB84 or communication networks of realistic complexity.

The objectives of the research which we are now proposing are: to translate CQP into the model-checking tool PRISM; to develop a high-level specification language for correctness properties; to describe BB84 and other related protocols in CQP; to translate the specification of BB84 in CQP to PRISM; and to verify BB84 in PRISM. In the long-term we will consider modelling and verification of authentication; combined verification of classical and quantum components of protocols; and also design and analysis of secure interface components and network infrastructure for practical key distribution.

Our work draws on various disciplines including quantum mechanics, programming language theory, information security and formal verification to develop techniques and tools for next-generation secure communication systems. It will contribute to the grand challenge facing the quantum cryptography community—to develop a practical system of secure communication to exchange keys (and messages) in a network environment at a viable rate. Such a system is required to deliver, if not absolute security, much greater level of security than that offered by existing systems.

One can consider our ideas as application of techniques from mainstream computer science to quantum information and is very much in the spirit of the International Workshop on The Grand Challenge in Non-classical Computation. We hope that our efforts would be appreciated by the broader inter-disciplinary community involved in non-classical computing research; early indications are that quantum physicists are certainly interested.

ACKNOWLEDGEMENTS

The concepts outlined here are being further developed in collaboration with Simon Gay at the University of Glasgow and Nikolaos Papanikolaou at the University of Warwick.

References

[1] C. H. Bennett and G. Brassard. Quantum Cryptography: Public-key Distribution and Coin Tossing. In *Proceedings of the IEEE International Conference on Computer, Systems and Signal Processing, Bangalore, India*, pages 175–179, December 1984.

[2] A. K. Ekert. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.*, 67:661–663, 1991.

[3] C. Elliott. Building the Quantum Network. *New Journal of Physics*, 4:46.1–46.12, 2002.

[4] S. J. Gay and R. Nagarajan. Communicating Quantum Processes. In *POPL '05: Proceedings of the 32nd ACM Symposium on Principles of Programming Languages*, Long Beach, California , January 2005.

[5] S. J. Gay, R. Nagarajan and N. Papanikolaou. Probabilistic Model-Checking of Quantum Protocols. Submitted for publication. Preprint available from www.arxiv.org/abs/quant-ph/0504007.

[6] M. Z. Kwiatkowska, G. Norman, and D. Parker. PRISM: Probabilistic symbolic model checker. In T. Field, P. Harrison, J. Bradley, and U. Harder, editors, *Computer Performance Evaluation (TOOLS '02)*, pages 200–204. Springer-Verlag, 2002. See also `http://www.cs.bham.ac.uk/~dxp/prism/`.

[7] G. Lowe. Breaking and fixing the Needham-Schroeder public-key protocol using FDR. *Software Concepts and Tools*, 17:93–102, 1996.

[8] D. Mayers. Unconditional Security in Quantum Cryptography. *Journal of the ACM*, 48(3):351–406, May 2001.

[9] R. Milner, J. Parrow, and D. Walker. A calculus of mobile processes, I and II. *Information and Computation*, 100(1):1–77, September 1992.

[10] P. Ryan, S. Schneider, M. Goldsmith, G. Lowe, and A. W. R. Roscoe. *Modelling and Analysis of Security Protocols*. Addison-Wesley, 2001.

[11] P. Selinger. Towards a quantum programming language. *Mathematical Structures in Computer Science*, 14(4):527-586, 2004.

[12] P. W. Shor. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. In *FOCS '94: Proceedings of the 35th Annual Symposium on Foundations of Computer Science*. IEEE Computer Society Press, 1994.