Stellingen

behorende bij het proefschrift *"Cryptography from Quantum Uncertainty in the Presence of Quantum Side Information"* van Niek J. Bouman

1. In spite of the fact that the quantum key distribution (QKD) protocol invented by Bennett and Brassard in 1984 (a.k.a. *BB84*) [1] is theoretically well understood by now, successful attacks on commercially-available physical implementations of BB84 demonstrate a harmful discrepancy between the theoretical QKD model and the real world.
(Chapters 1 and 3 of this thesis)

2. The non-locality property of quantum mechanics enables *device-independent* QKD, which guarantees security *even* if Alice's and Bob's quantum devices behave in an unanticipated or arbitrarily malicious manner. *(Chapter 1 of this thesis)*

3. The interaction between quantum cryptography and physics is bidirectional.

4. Let $\mathcal{H} = (\mathbb{C}^2)^{\otimes n}$ be the state space of an n-qubit quantum system, for some positive integer n. Let $m \geq 2$ be a positive integer and let $\mathcal{B}_1, \ldots, \mathcal{B}_m \subseteq \mathcal{H}$ be pairwise distinct orthonormal bases for $\mathcal{H}$. Let δ be the positive real number defined by

$$\delta := -\frac{1}{n} \log_2 \max_{\substack{j,k \in \mathbb{N}: \\ 1 \leq j < k \leq m}} \max_{\substack{|\phi\rangle \in \mathcal{B}_j \\ |\psi\rangle \in \mathcal{B}_k}} |\langle \phi | \psi \rangle|^2.$$

   Let ρ be any density matrix acting on $\mathcal{H}$, let J be a random variable over $[m]$ (with arbitrary distribution P_J), and let X be the random variable that represents the outcome when measuring ρ in basis $\mathcal{B}_J$.

   Then, for any $\epsilon \in \mathbb{R}$ such that $1/n < \epsilon < \delta/4$, there exists a random variable J' with joint distribution $P_{JJ'X}$ such that (1) J and J' are independent and (2) there exists an event Ω with $\Pr[\Omega] \geq 1 - 2 \cdot 2^{-\epsilon n}$ such that

$$H_{\min}(X|J = j, J' = j', \Omega) \geq \Big(\frac{\delta}{2} - 2\epsilon\Big)n - 1$$

   for all $j, j' \in [m]$ with $j \neq j'$ and $P_{JJ'|\Omega}(j, j') > 0$. *(Theorem 5.3 of this thesis)*

5. *Bitcoin* is an Internet-based currency system that does not involve participation of any traditional financial institution, such as a bank, or any other trusted third party for that matter. In fact, users *jointly* verify and approve transactions by a process called *mining*. Introduced by Satoshi Nakamoto in 2008, and further developed by a team of open-source software enthusiasts, Bitcoin has been adopted by users on the Internet. Currently, it has a volume of over 140 million USD.

   The mining protocol works as follows. Any user can earn the right to participate in the mining process by demonstrably spending a certain minimum amount of computational resources. Currently, this is implemented by requiring miners[1] to compute partial hash collisions by

[1] users that contribute to the mining process.

brute-force search. The security of the mining protocol is based on the assumption that honest miners control the majority of the total computational power of all miners.

Interestingly, Bitcoin's mining protocol provides a game-theoretic handle by which *dishonest* miners controlling a *minority* of the total computational power can effectively *expel* honest miners from the system. In the long run, this puts the validity of the very trust assumption upon which the security of Bitcoin is based into serious question.

6. The *Erdős–Rényi random graph* $G(n, p)$, where $n \in \mathbb{N}$ and $p \in [0, 1] \subset \mathbb{R}$, is a graph (V, E), where the set of vertices V has cardinality n and the set of edges E is a random variable as follows: for each $\{v, w\} \subset V$ with $v \neq w$, it holds that $\Pr[\{v, w\} \in E] = p$, independently of everything else.

   Suppose that $\widetilde{p} : \mathbb{N} \to [0, 1]$ is a function such that the limit $\ell := \lim_{n\to\infty} n \cdot \widetilde{p}(n)$ exists. If $\ell > 1$, then, except with probability negligible in n, the random graph $G(n, \widetilde{p}(n))$ has a unique connected component consisting of $\Omega(n)$ vertices, and moreover, any other component has $O(\log n)$ vertices. [2]

   This result, and more generally, the theory of random graphs as such, provides one way of illustrating the phenomenon that random objects may very well exhibit fascinating structural properties. In particular, this demonstrates that the presence of structure does not necessarily imply intended design. The latter observation has been nearly invisible in the public debate in recent years about *"Intelligent Design."*

7. Cryptography in Maurer's *bounded storage model* [3] requires a massive data set, about which observers experience sufficient uncertainty, as well as *oblivious* access to this data. It is tempting to consider the Web as a basis for a practical realization of cryptography in Maurer's model. However, the Web is not suited for this purpose because it fails to provide oblivious access to its content, due to the challenge-response nature of the *Hypertext Transfer Protocol* (HTTP).

   Multicast, on the other hand, which is a method to broadcast a stream of packets over the Internet to a group of receivers, enables oblivious access to packets within the stream, and, in principle, makes cryptography in the bounded storage model possible via the Internet.

8. Wetenschappers en wetenschapsfinancieringsorganisaties dienen de handen ineen te slaan om de stroom van belastinggeld, die via de universiteitsbibliotheek bij wetenschappelijke uitgevers terecht komt, in te dammen. Het omarmen van het "Open Access" model is hiervoor geen afdoende maatregel.

Referenties:

[1] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proc. IEEE Int. Conf. on Comp., Syst., and Sig. Proc.*, pages 175–179, 1984.

[2] P. Erdős and A Rényi. On the evolution of random graphs. In *Publ. of the Math. Inst. of the Hungar. Acad. of Sc.*, pages 17–61, 1960.

[3] U. M. Maurer. A provably-secure strongly-randomized cipher. In *Eurocrypt*, LNCS, pages 361–373. Springer, 1990.