



IST-2002-507932

ECRYPT

European Network of Excellence in Cryptology

Network of Excellence

Information Society Technologies

D.PROVI.3

First Summary Report on Unconditionally Secure Protocols

Due date of deliverable: 31. January 2005

Actual submission date: 21. February 2005

Start date of project: 1. February 2004

Duration: 4 years

Lead contractor: University of Aarhus (BRICS)

Revision 1.0

Project co-funded by the European Commission within the 6th Framework Programme		
Dissemination Level		
PU	Public	X
PP	Restricted to other programme participants (including the Commission services)	
RE	Restricted to a group specified by the consortium (including the Commission services)	
CO	Confidential, only for members of the consortium (including the Commission services)	

First Summary Report on Unconditionally Secure Protocols

Editors

Jesper Buus Nielsen (BRICS)

Contributors

Christian Cachin (IBM), Ivan Damgård (BRICS),
Kirill Morozov (BRICS), Louis Salvail (BRICS)

21. February 2005

Revision 1.0

The work described in this report has in part been supported by the Commission of the European Communities through the IST program under contract IST-2002-507932. The information in this document is provided as is, and no warranty is given or implied that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability.

Contents

1	Introduction	1
2	Noisy-channel cryptography	3
2.1	Introduction	3
2.2	Goals	3
2.2.1	Brief interlude on secure function evaluation (SFE) and secure computation (SC)	4
2.2.2	Goals of noisy-channel cryptography	4
2.3	State of the art in noisy-channel cryptography	5
2.4	The exact relationship between unfair noisy channels and oblivious transfer .	5
2.5	More realistic models of noisy channels	7
3	Bounded-storage cryptography	9
3.1	Introduction	9
3.2	State of the art in bounded-storage cryptography	10
3.3	The bounded-quantum-storage model	11
3.4	Oblivious transfer in the bounded-quantum-storage model	12
4	Quantum cryptography	13
4.1	Introduction	13
4.2	The problems with quantum adversaries	13
4.3	Zero-knowledge against a quantum adversary without protocol setup	14
4.4	New physical-complexity aware models	15

Chapter 1

Introduction

This document describes the state of the art and some of the main open problems in the area of unconditionally secure cryptographic protocols.

The most essential part of a cryptographic protocol is not its being secure. Imagine a cryptographic protocol which *is* secure, but where we do not *know* that it is secure. Such a protocol would do little in providing security. When all comes to all, cryptographic security is done for the sake of people, and the essential part of security is for people what it has always been, namely *to feel secure*. To feel secure employing a given cryptographic protocol we need to *know* that it is secure. I.e., we need a *proof* that it is secure.

Today the proof of security of essentially all practically employed cryptographic protocols relies on computational assumptions. To prove that currently employed ways to communicate securely over the Internet are secure we e.g. need to assume that it is possible to compute an encryption, which, even though it contains the message to be sent, cannot be decoded by anyone but the legitimate receiver. This is equivalent to assuming that there exist so-called one-way functions: Functions which are easy to compute on a given input, but which are infeasible to invert. In fact, the security proofs of all currently employed cryptographic protocols need to assume some component being a one-way function. Unfortunately, at our current point in history, we really have no idea whether one-way functions even exist, and though most researchers in computational complexity would be surprised if one-way functions do not exist [Gas02], it is perfectly conceivable that all currently cryptographic protocols in use today are insecure.

This discomfoting fact invites us to try to find other means on which to base security. Maybe even means which allow us to *prove* that the resulting protocols are secure. This is the realm of *unconditionally secure* cryptographic protocols.

Three popular approaches to unconditional security are *noisy-channel cryptography*, *bounded-storage cryptography* and *quantum cryptography*. It is actually a too brave statement, that these approaches do not make unproved assumptions. Instead they make fewer assumptions or alternative assumptions, which are of another nature than the assumption that one-way functions exists, and they are better justifiable by our current technological and scientific level. In noisy-channel cryptography security proofs are based on the assumption that a given physical means of communication is at a sufficiently low level inherently noisy. In bounded-storage cryptography security proofs are based on the assumption that there exists streams of information, generated by computers or other physical phenomena, so intense that no one is able to fully store them. In quantum cryptography security proofs are based on the

assumption that nature behaves consistently with quantum mechanics.

In the following we describe the state of the art and some main open problems in the three abovementioned research areas.

Chapter 2

Noisy-channel cryptography

2.1 Introduction

In noisy-channel cryptography one investigates which cryptographic problems can be solved unconditionally secure in a setting where two parties, Alice and Bob, are connected by a communication channel which is inherently noisy. I.e., with some significant probability the message received by Bob will not be the message sent by Alice. This should be true for any receiver. In particular it should also hold for an eavesdropper Eve that she does not always see the message sent by Alice.

Most communication channels are at a sufficiently low level inherently noisy, which is generally considered a nuisance. Indeed the entire field of coding theory is essentially devoted to implementing noiseless channels on top of a noisy channels. From the viewpoint of cryptography an inherently noisy channel can however be a very useful tool. As Shannon showed us, the unconditional security obtainable by a system is proportional to the uncertainty of the adversary. If the adversary knows all communication between Alice and Bob, the uncertainty of the adversary cannot grow, and the obtainable unconditional security will be proportional to the initial secret key shared by Alice and Bob. An inherently noisy channel on the other hand guarantees exactly uncertainty for the adversary; it cannot be sure that the bits it sees are the bits sent (received) by Alice (Bob). This opens the prospects of obtaining unconditional security in a system with a small or no initial key shared between Alice and Bob. Any protocol for the noisy channel model must of course deal with the fact that Alice and Bob do not have certainty either.

2.2 Goals

The primary goals of noisy-channel cryptography is to give believable models of noisy channels and to investigate what cryptographic problems can be solved unconditionally secure in a given model. As in most parts of cryptographic protocol theory, the problems considered are typically secure function evaluation (SFE) and secure computation (SC).

2.2.1 Brief interlude on secure function evaluation (SFE) and secure computation (SC)

In a SFE Alice and Bob hold inputs a respectively b and agree on a function $(A, B) = f(a, b)$. The goal of the SFE protocol is that Alice should learn A and Bob should learn B ; this in such a way that Alice learns no information about b or B and Bob learns no information about a or A (extra to what they can learn through their respective outputs, A and B , of course). Additionally an adversary attacking the protocol should learn nothing at all about the inputs and outputs of Alice and Bob.

Many problems in cryptography can be expressed as a SFE problem. For example, solving the SFE problem for the function $(b, a) = f(a, b)$ corresponds to implementing a secure channel. The SFE problem for the function $(\epsilon, a_b) = f((a_0, a_1), b)$ is called oblivious transfer (OT); Here Alice has as input two bits a_0 and a_1 and Bob has as input a bit b . The goal of the protocol is that Bob learns the bit a_b without learning anything about the other input bit of Alice. At the same time Alice should learn nothing about the input b of Bob (Alice's output is the empty string ϵ). The OT problem might seem artificial, but is interesting from a theoretical point of view as it is known to be complete for SFE [Kil88]; in other words, a secure protocol for the OT problem can be used as a sub-protocol to efficiently solve *any* SFE problem.

The SC problem is the generalisation of the SFE problem, where Alice and Bob can give inputs in several rounds. In round i Alice and Bob give new inputs a_i respectively b_i and learn new outputs A_i respectively B_i computed as a function, $(A_i, B_i) = f_i((a_1, \dots, a_i), (b_1, \dots, b_i))$, of all previous inputs. As an example the SC problem where Alice inputs a in the first round and Bob as response receives a fixed string `Alice input a value`, and where Bob is given a as output in the first round where Alice inputs the string `give the value to Bob`, is equivalent to secure commitment, which is an essential primitive in cryptography. Most problems in cryptographic protocol theory can be expressed as a SC problem. Solving the SC problem might seem harder than solving the SFE problem. It was however proved in [CGT95] that OT is also complete for SC — any secure protocol for the OT problem can be used as a sub-protocol to efficiently solve *any* SC problem.

2.2.2 Goals of noisy-channel cryptography

Primarily three security goals have been studied in noisy-channel cryptography. The first is the problem of implementing a secure channel from Alice to Bob based on an open noisy channel (where the adversary can read the communication between Alice and Bob over the noisy channel). The second is the problem of implementing oblivious transfer based on a closed noisy channel from Alice to Bob (where the adversary can *not* read the communication of the noisy channel between Alice and Bob). The third is the problem of implementing bit commitment from Alice to Bob.

The motivation for the first problem should be obvious, as secure communication is one of the most essential special cases of two-party computation. The motivation for the second study is that, as mentioned above, OT is known to be complete for secure computation. So, showing that OT can be solved unconditionally secure given a noisy channel, one has shown that *any* cryptographic protocol problem can be solved unconditionally secure given a noisy channel. The motivation for typically basing the second study on a closed noisy channel, as opposed to an open noisy channel, is that the problem of 'closing' a noisy channel is

dealt with (and is best dealt with) by the study of implementing secure channels from open noisy channels.¹ The motivation for the third study is that even though commitment is not complete for secure computation, it is a fundamental primitive in cryptography.

2.3 State of the art in noisy-channel cryptography

Maurer and Wolf [MW03] give a comprehensive study of when it is possible to implement a secret channel characterised by the mutual information of Alice, Bob and the adversary about each other. Their framework in particular characterises when it is possible to implement a secure channel based on an open noisy channel. The work by Maurer and Wolf in principle characterises completely when it is possible to implement a secure channel from an open noisy channel, and we are not aware of any essential open problems. The problem of implementing OT based on a closed noisy channel was first studied by Crépeau and Kilian [CK88]. Notable later work includes [DKS99, DFMS04]. The work in [DKS99] is the first to explicitly consider implementing commitment based on a noisy channel. Below we describe some open problems in implementing OT based on a closed noisy channel.

2.4 The exact relationship between unfair noisy channels and oblivious transfer

The problem of implementing OT based on a closed noisy channel was first studied by Crépeau and Kilian [CK88]. They showed that OT can be implemented based on a binary symmetric channel (BSC). A BSC is a channel for transmitting single bits, and for every bit transmitted, the channel decides with some fixed probability ν to flip the bit before it is given to the receiver. It was proved in [CK88] that if Alice and Bob have any BSC with $0 < \nu < \frac{1}{2}$ then they can implement OT between them unconditionally secure. This is the best one can hope for: If $\nu = 0$, then the channel is noiseless, and if $\nu = \frac{1}{2}$, then the channel is useless, as it cannot carry information.

Unfortunately, results based on BSCs do not give realistic security guarantees. The reason for this is that one must expect that a cheating Bob (Alice) will try to influence the channel and have this work to his (her) advantage, for instance by lowering the noise rate ν in order to learn more than expected about what the other party sent (received). Note that one can always hide the fact that the channel was made less noisy by pretending to have sent(received) a more noisy signal than the one actually sent(received). Moreover, even in the absence of cheating parties, it is hardly realistic to assume that the noise rate is known exactly.

To remedy this shortcoming of the BSC model, Damgård, Kilian and Salvail [DKS99] introduced the Unfair Noisy Channel (UNC) model to be a more realistic cryptographic model of a noisy channel.

A (γ, δ) -UNC is basically a BSC, where, however, the noise rate ν is only known to be in a certain interval $[\gamma, \delta]$, and where if the sender or receiver is cheating can set the noise rate to any desired value in the interval without the other party noticing. So, a UNC models

¹If an open noisy channel does not allow to implement a secure channel it cannot be complete of two-party multiparty computation, as a secure channel is a special case of SFE. If on the other hand an open noisy channel does allow to implement a secure channel, then Alice and Bob can 'close' the noisy channel by exchanging uniformly random pads over the implemented secure channel and use the pads to one-time pad encrypt the bits sent over the noisy channel, giving them a closed version of the original open noisy channel.

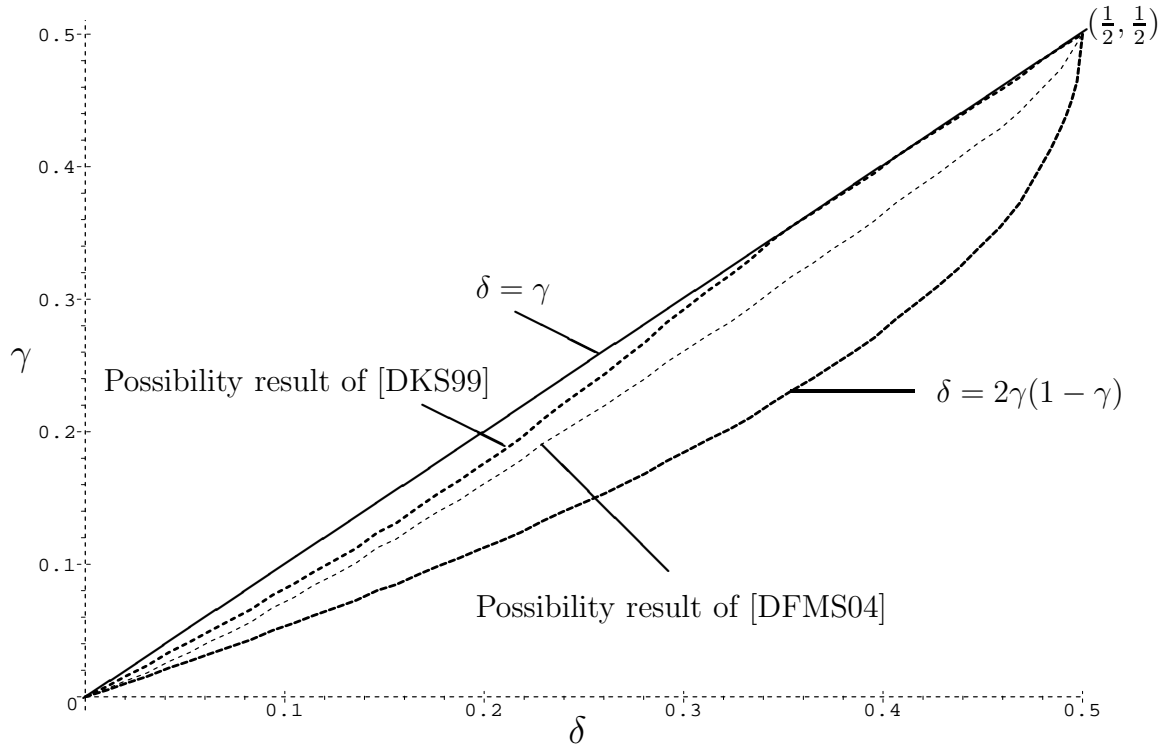


Figure 2.1: Depiction of known possibility and impossibility results for OT based on a (δ, γ) -UNC

active cheating directed against the way a physical channel works in order to manipulate the error rate. If the channel is a radio link, for instance, the cheating party could invest in more sophisticated equipment without telling the other party and thereby lowering the noise rate from his point of view. However, it may still be realistic to assume that he cannot remove *all* noise from the channel, so such a case can be captured in the UNC model.

In [DKS99], it was proved that bit commitment can be implemented with unconditional security based on a (γ, δ) -UNC if and only if the interval $[\gamma, \delta]$ is not too wide, more precisely, if and only if $\gamma \leq \delta < 2\gamma(1 - \gamma)$ (the condition $\gamma \leq \delta$ comes from the fact that the model does not make sense for $\gamma > \delta$). This means that commitment can be based on a (γ, δ) -UNC iff (δ, γ) , in Fig. 2.1, is positioned under the straight line $\gamma = \delta$ and above the bottom curve $\delta = 2\gamma(1 - \gamma)$.

Since OT is complete for two-party computation, and thus in particular implies commitment, the negative part of the abovementioned result also applies to OT, i.e., one cannot base OT on a (γ, δ) -UNC if $\delta \geq 2\gamma(1 - \gamma)$. This means that for the set of values of (γ, δ) positioned under the bottom curve in Fig. 2.1, OT cannot be based on a (γ, δ) -UNC. On the positive side, it was shown that if γ and δ satisfy a rather complex condition (stronger than $\delta < 2\gamma(1 - \gamma)$), then OT (with *passive* security) can be based on a (γ, δ) -UNC. The results of [DKS99] imply that for the set of values of (γ, δ) positioned between the straight line $\delta = \gamma$ and the top curve in Fig. 2.1, OT can be based on a (γ, δ) -UNC.

Later [DFMS04] gave new protocols simultaneously improving the positive result for OT and obtaining active security. The protocol from [DFMS04] gives a secure OT protocol based on any (γ, δ) -UNC with (δ, γ) positioned over the middle curve in Fig. 2.1, significantly extending the area where OT can be based on a (γ, δ) -UNC. Furthermore, it was proved

in [DFMS04] that this extension would not be possible using the techniques from [DKS99], but required the new techniques introduced in [DFMS04].

Evidently from Fig. 2.1 there is still a significant area left where it is not known whether OT can be based on a (γ, δ) -UNC (the area between the bottom curve and the middle curve, which we call the *OT gap* below). This of course opens the problem of investigating the relation between a (γ, δ) -UNC and OT in this area. Making the problem even more intriguing, it was proved in [DKS99] that narrowing the gap considerably cannot be done with simple extensions of the work in [DKS99], but would again require the invention of new techniques.

Open Problem No. 1: Investigate the OT gap of unfair noisy channels.

2.5 More realistic models of noisy channels

The motivation for introducing the UNC model was that the BSC model was not a realistic model of noisy channels found in nature. It is evident that the UNC is only a starting point.

Open Problem No. 2: Investigate more relaxed models of noisy channels than UNC and evaluate the cryptographic capabilities of these models.

Chapter 3

Bounded-storage cryptography

3.1 Introduction

In bounded-storage cryptography one investigates which cryptographic problems can be solved unconditionally secure under the assumption that we know some bound B on the number of bits that the adversary is able to store.

Recall again that Shannon taught us that the unconditional security obtainable by a system is proportional to the uncertainty of the adversary, and that this implies that if the adversary knows all communication between Alice and Bob, the uncertainty of the adversary cannot grow, and the obtainable unconditional security will be proportional to the initial secret key shared by Alice and Bob. The prospect of obtaining unconditional security in the bounded-storage model with no (or a small) initial key then comes from the fact that it is exactly possible to establish a situation where the adversary does not know all communication between Alice and Bob. If, e.g., Alice is able to send to Bob more random bits than the adversary is able to store, then due to the incompressibility of uniformly random strings, after the communication took place, the adversary no longer knows all information about the communication which took place. Of course any protocol for the bounded-storage model must deal with the fact that neither can Alice or Bob store all communication.¹

Notice that, exactly as for cryptography based on time complexity, bounded-storage cryptography is based on a scarcity assumption. Now we only assume a bound on available storage instead of a bound on the available bit operations. As opposed to cryptography based on time complexity, bounded-storage cryptography does however not make assumptions extra to the scarcity assumption. The protocols are secure if only the storage-scarcity assumption holds — cryptography based on time complexity has to *assume* that the bit-operation-scarcity assumption is actually useful, e.g., by assuming that there exist functions which can be computed

¹To see how the bounded-storage model allows Alice and Bob to get an advantage over the adversary, assume that Alice, Bob and the adversary each can store at most B bits, and assume that Alice can send to Bob a uniformly random string R of length $2B - 1$. During the sending if the random string both Alice and Bob store B of the bits, each choosing the indices of the bits to store uniformly at random. After the string is sent Alice and Bob announce the bit positions that they stored. They are guaranteed that there is at least one common index i such that both stored the bit R_i . They pick a uniformly random such index i and take the stored value R_i from that position to be their output. The index i is clearly uniformly random among all $2B - 1$ indices and independent of the information about R stored by the adversary. So, since the adversary stored at most B bits, the expected information that the adversary has about R_i is very close to half a bit (namely $\frac{B}{2B-1}$ bits of information). This means that the parties Alice and Bob created themselves an advantage in information over the adversary.

comfortably within the available bit operations but cannot be inverted using the available bit operations.

3.2 State of the art in bounded-storage cryptography

Cryptographic protocols in the bounded-storage model have first been designed for encryption, where one expands a short pre-shared secret key to a longer one. The oblivious transfer (OT) problem has been considered later, in a setting with no pre-established secrets, and the reason for focusing on oblivious transfer is explained in Section 2.1. We review both cases here.

Probably the most important task in cryptography is information transmission secure against eavesdropping. In the bounded-storage model, one assumes the existence of a public high-capacity source of randomness to which all parties have access. Because of the storage bound, no party can record all data generated by the source. The model and a first implementation were proposed by Maurer [Mau92]; this and most subsequent encryption protocols are based on a shared secret key that is used by the legitimate parties to randomly select bits from the random source about which the adversary has only partial information. Intuitively, this works because the bound on the adversary’s storage prevents it from knowing all bits with certainty, and because the random selection ensures that it has only partial information “on average” about the selected bits.

With some further processing, the legitimate parties then convert these partially secret bits into a key which the adversary cannot distinguish from a truly random string (in an information-theoretic sense). This key can safely be used for cryptographic purposes, for example in a one-time pad for encryption.

A progression of works [Mau92, CM97, ADR02, DM04, Lu04, Vad04] has developed increasingly secure and efficient protocols in this model. In particular, the works of Aumann, Ding, and Rabin [ADR02] made the observation explicit that protocols in this model enjoy a property called *everlasting security*; this means that the security is preserved even if the key is revealed to the adversary and the adversary’s storage becomes unbounded *after* the protocol has been used.

Recently, Lu [Lu04] showed that the problem statement can be cast nicely in the framework of so-called *extractors* of randomness. Extractors are algorithms for extracting almost-uniform, “almost perfectly random” bits from “non-perfect” sources of non-uniform and correlated bits [NZ96]. These powerful tools have been the subject of intense study, and have found many applications to a wide variety of topics in the theory of computation [NTS99]. Lu showed that any extractor of a particular class yields secure private-key cryptosystems in the bounded-storage model. The restrictions of the bounded-storage model require a non-standard property from extractors in the sense that they can be computed “on-line” (or “locally”), as the input string is read (because the public randomness is not recorded anywhere!). He gave a construction of such an extractor via an intermediate step of a locally computable error-correcting code.

Vadhan [Vad04] suggested a general “sample-then-extract approach” for constructing locally computable extractors. A so-called *randomness-efficient sampler* is first used to select the bits from the source (i.e., their locations); essentially any extractor can then be applied to the selected bits. Exploiting existing powerful constructions of suitable samplers and extractors, this work yields cryptosystems in the bounded-storage model whose parameters improved all previously known constructions, in fact, they are nearly optimal. The extractors

needed to implement the approach are still far from practical realization at the high data and processing rates that would be necessary to implement the system. Dziembowski and Maurer [DM04] presented a system with much simpler implementation (the only computations involved are XORs of bit strings), which does not achieve the near-optimal parameters, however.

Open Problem No. 3: Construct an encryption scheme in the bounded-storage model with near-optimal parameters *and* protocols that are practical.

Cachin, Crépeau, and Marcil [CCM98] initiated the study of secure function evaluation (SFE) in the bounded-storage model by formulating a protocol for oblivious transfer between two parties (cf., Section 2.2.1). The problem is different because there are only two parties, each mistrusting the other, who cannot exploit an initial shared key. This construction was later improved by Ding [Din01]. Ding et al. [DHRS04] presented a constant-round protocol that took up ideas from the extractor-based approach to encryption in the bounded-storage model.

Open Problem No. 4: Determine the optimal parameters (storage requirement, error probabilities) of oblivious transfer protocols in the bounded-storage model and find a scheme that matches it.

In particular, all oblivious transfer schemes suffer from the limitation that the parties must store $O(\sqrt{N})$ bits when the source outputs N bits. This is necessary to guarantee a sufficiently large overlap in the bits that both parties stored. The same limitation exists for key-agreement protocols [Mau92, CM97], that is, protocols that establish a shared secret key *without* using an initial, shorter secret key.

Open Problem No. 5: Prove or disprove that both parties must use $\Omega(\sqrt{N})$ storage space in oblivious transfer or key agreement protocols in the bounded-storage model.

3.3 The bounded-quantum-storage model

A variation of the bounded-storage model is the *bounded-quantum-storage model* (see Section 4 for “pure” quantum cryptography). In the bounded-quantum-storage model one assumes that the number of *quantum bits* that the adversary can store is considerably less than the number of quantum bits that Alice and Bob can communicate. Besides this, the model makes no assumptions. In particular, the adversary is allowed to be a quantum machine and has access to storing an unbounded number of classical bits.

A problem with the classical bounded-storage model is that it requires that advances in standard transmitting and receiving technology proceed in such a manner that it is possible to transmit and/or receive considerably larger amounts of data than any physical system which can reasonable by deployed by an adversary can store for just a reasonable amount of time. It is not clear that we have any guarantee this will be the case in the near future. This problem is considerably smaller for the bounded-quantum-storage model.

Whereas sending quantum information can be accomplished by sending a light beam, for example, current techniques for storing quantum information seem to still be distant

from providing large long-term storage. For the foreseeable future it thus seems more than reasonable to assume that Alice and Bob can exchange far more quantum bits than the adversary can store.

Under all circumstances the bounded-quantum-storage model makes strictly weaker assumptions than the classical storage model, as it allows the adversary access to an unbounded classical storage. The bounded-quantum-storage model therefore seems to be a very exciting weakening of the classical bounded-storage model.

3.4 Oblivious transfer in the bounded-quantum-storage model

As discussed in Section 2.2.1 the OT problem is complete for secure computing. The very first question to ask when considering a new model is therefore *can it do OT?* This is a non-trivial question for any restriction of the plain quantum model, as it is known that in the plain quantum model, where there is no bound on the quantum memory of the adversary, commitment, and thus OT, is impossible [LC97, May97].

Open Problem No. 6: Find an oblivious transfer protocol in the bounded-quantum-storage model.

To see that this is indeed an open problem we clarify the relationship of the bounded-quantum-storage model with the so-called *bounded-coherent-measurement model*. In [Sal98] Salvail showed how to do commitment under the assumption that the sender is not able to perform generalised measurements involving more than n qubits coherently. It would seem that an adversary which cannot store n qubits cannot perform a generalised measurement on n qubits either, so that the commitment scheme in [Sal98] should also be secure in the bounded-quantum-storage model. This line of argument does not apply as the bounded-quantum-storage allows the adversary to make an arbitrary generalised measurement and store the classical outcome of the measurement. The adversary is only restricted in the number of qubits it can store between seeing the initial random qubits exchanged by Alice and Bob and attacking the rest of the protocol.

What furthermore makes the bounded-quantum-storage model interesting is the nature of the secure protocol that the model seems to allow. For example, it seems that the model allows non-interactive OT. All previously unconditionally secure OT schemes, like the BBCS scheme were interactive.

Open Problem No. 7: Find a non-interactive oblivious transfer protocol in the bounded-quantum-storage model or give evidence that it is impossible.

Chapter 4

Quantum cryptography

4.1 Introduction

Quantum cryptography was born from the search for problems that have unconditionally secure solutions *only* based on the fundamental laws of quantum mechanics, but not in the classical world. This led the ground to early work such as the oblivious transfer (OT) protocol suggested by Wiesner [Wie83] and the key distribution and coin-flip protocols suggested by Bennett and Brassard [BB94].

However, with the emergence of Shor's [Sho94] efficient quantum algorithm for factoring integers and computing discrete logarithms it became evident that the power of quantum mechanics also had implications for classical cryptography based on computational assumptions. From the day of the first construction in a laboratory of just one quantum computer with registers large enough to factor contemporary RSA moduli, the RSA cryptosystem will be rendered more or less useless, and very few people and institutions would feel comfortable using the system, even for increased key-lengths. We have no guarantee that this day is far into the future. One often hears recommendations for key-sizes of public-key cryptosystems needed to obtain security for 30 years and even 50 years. Anyone wanting a real security of this magnitude should probably take the construction of the quantum computer into consideration.

This asks an important question, of which cryptographic protocols remain secure, and if too few, whether we can construct new ones remaining secure, after the construction of the first quantum computer. This is in many cases not a question about unconditional security, and falls within the field of unconditional security as discussed in this document only in the sense that the researchers and techniques in the fields largely overlap.

4.2 The problems with quantum adversaries

So what extra problems occur by having to prove security against a quantum adversary? In classical cryptography a protocol is typically proved secure by postulating some more or less accepted computational assumption, like the existence of one-way functions, and then proving that if this assumption holds, then the protocol in question is secure. In order to assess the security of a protocol after the construction of the first quantum computer, two issues are therefore important. First, the computational assumption(s) on which the protocol is based must remain true even if the adversary has a quantum computer. As mentioned above, this

rules out many assumptions such as hardness of factoring or extracting discrete logs, but a few candidates still remain, for instance some problems related to lattices or error correcting codes. In general, it is widely believed that quantum one-way functions exist, i.e., functions that are easy to compute classically, but hard to invert, even on a quantum computer.

A second and more difficult question is whether the proof of security remains valid against a quantum adversary. A major problem in this context comes from the way quantum information behaves in contrast to classical information, e.g., the possibility of super-positions and the no-clone theorem (the impossibility of copying quantum states). This renders many classical proof techniques useless in the quantum model, and more fundamentally, even leaves classical *definitions* of security useless.

As an example of the latter, the computational binding of a commitment scheme is classically defined by the sender not being able to construct a commitment which can be opened to two different messages. Such a definition does not make sense in the quantum model, e.g., for perfect hiding commitment schemes. In the quantum model, the sender, having a quantum machine, can set up a quantum message, which is an equal super-position of all classical messages that the commitment scheme can commit to. Furthermore, the sender can set up a quantum randomiser, which is an equal super-position of all possible random strings used by the commitment scheme. If the commitment scheme is perfect hiding, then when the sender runs the commitment algorithm on this quantum message and quantum randomiser and measures the output (to get a classical commitment to send to the receiver) the quantum message committed to by this classical commitment will still be in an equal super-position of all possible messages and will not be determined until the sender chooses to measure the message. Furthermore, when the sender measures the message to have the state super-position collapse and decide on the message committed to, then the randomiser will collapse to a value allowing to open the commitment to the chosen value.

Open Problem No. 8: Find equivalent security definitions in the quantum model for all notions of classical cryptography, such as computationally hard problems, cryptographic primitives, and cryptographic protocols. Investigate which ones of the classically hard problems can be solved using a quantum computer and which problems and protocols remain secure.

4.3 Zero-knowledge against a quantum adversary without protocol setup

As an example of how the specificities of quantum mechanics can render classical proof techniques useless, one can consider the concept of zero-knowledge (ZK), which since its introduction by Goldwasser, Micali and Rackoff [GMR89] has become a fundamental tool in cryptography. Informally, in a ZK proof of a statement, the verifier learns nothing beyond the validity of the statement. In particular, everything the verifier can do as a result of the interaction with the prover during the ZK proof, the verifier could also do without interacting with the prover. This is argued by the existence of an efficient *simulator* which produces a simulated transcript of the execution, indistinguishable from a real transcript. ZK protocols exist for any NP language if one-way functions exist [BC86, BCC88, GMW91].

A major problem with the security proof of almost all known zero-knowledge protocols comes from the fact that the simulator *rewinds* the verifier in order to generate a simulated

transcript of the protocol execution. However, if prover and verifier are allowed to run quantum computers, rewinding is not generally applicable, as it was originally pointed out by Van de Graaf [vdG97]. Intuitively, the reason is that when a quantum computer must produce a classical output, such as a message to be sent, a (partial) measurement on its state must be done. This causes an irreversible collapse of the state, so that it is not generally possible to reconstruct the original state. Moreover, copying the verifier’s state before the measurement is forbidden by the no-cloning theorem. Therefore, protocols that are proven ZK in the classical sense using rewinding of the verifier may not be secure with respect to a quantum verifier.

It is well known that rewinding can cause problems already in a classical setting. In particular, it has been realized that rewinding the verifier limits the composability of ZK protocols. As a result, techniques have been proposed that avoid rewinding the verifier, for instance the non-black-box ZK technique from [Bar01], or – in the common reference string model – techniques providing concurrent ZK [DNS98, RK99, Dam00], non-interactive ZK [BFM88] or universally-composable (UC) ZK [CF01, DN03]. One might hope that some of these ideas would translate easily to the quantum setting.

However, the non-black box technique from [Bar01] is based on the simulator using the verifier’s program and current state to predict its reaction to a given message. Doing so for a quantum verifier will collapse its state when a measurement is done to determine its next message, so it is not clear that this technique will generalise to a quantum setting. The known constructions of UCZK protocols and non-interactive ZK are all based on computational assumptions that are either false in a quantum setting or for which we have no good candidate for concrete instantiations: the most general sufficient assumption is the existence of one-way trapdoor permutations (i.e. as far as we know) but all known candidates are easy to invert on a quantum computer. Regardless of this type of problem, great care has to be taken with the security proof: despite the fact that the simulator in the UC model must not use rewinding, it is *not* true that a security proof in the UC model automatically implies security against quantum adversaries (c.f [DFS04]). Finally, the technique for concurrent ZK from [Dam00] avoids rewinding the verifier but instead rewinds the prover to prove soundness, leading to similar problems.

In [DFS04] Damgård, Fehr and Salvail proved that it is indeed possible to construct a ZK protocol secure against quantum adversaries. This protocol is for the so-called common reference string (CRS) model, where prior to the protocol being run a trusted party generates a uniformly random string and gives to both parties. It is known that strong security notions for classical commitment protocols, like UC security, cannot be realized without some kind of setup assumption like a CRS.

Open Problem No. 9: Determine whether or not a CRS is needed for zero-knowledge in the quantum model.

4.4 New physical-complexity aware models

As discussed in Chapter 3 it is known that unconditionally secure commitment and unconditionally secure OT is impossible in the plain quantum model, where we put no restrictions on the adversary extra to being consistent with quantum mechanics. I.e. for any such scheme there exists some quantum process breaking the scheme. However, as discussed in Section 3.3, in the bounded-coherent-measurement model and the bounded-quantum-storage

model, unconditionally commitment *is* possible. I.e. if we put some restriction on the physical complexity of the adversary, like only being able to do coherent measurements on n qubits, then the model can allow more.

Open Problem No. 10: Formulate other physical restrictions of the plain quantum model justified by practical limitations and investigate their strengths.

Bibliography

- [ADR02] Yonatan Aumann, Yan Zong Ding, and Michael O. Rabin. Everlasting security in the bounded storage model. *IEEE Transactions on Information Theory*, 48(6), June 2002.
- [Bar01] B. Barak. How to go beyond the black-box simulation barrier. In *42nd Annual Symposium on Foundations of Computer Science*, pages 106–115, Las Vegas, Nevada, 14–17 October 2001. IEEE.
- [BB94] C.H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin-tossing. In *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, pages 175–179, 1994.
- [BC86] G. Brassard and C. Crépeau. Zero-knowledge simulation for boolean circuits. In A. M. Odlyzko, editor, *Advances in Cryptology - Crypto '86*, pages 223–233, Berlin, 1986. Springer-Verlag. Lecture Notes in Computer Science Volume 263.
- [BCC88] G. Brassard, D. Chaum, and C. Crépeau. Minimum disclosure proofs of knowledge. *Journal of Computer and System Sciences*, 37(2):156–189, 1988.
- [BFM88] M. Blum, P. Feldman, and S. Micali. Non-interactive zero-knowledge and its applications (extended abstract). In *Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing*, pages 103–112, Chicago, Illinois, 2–4 May 1988.
- [CCM98] Christian Cachin, Claude Crépeau, and Julien Marcil. Oblivious transfer with a memory-bounded receiver. In *Proc. 39th IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 493–502, 1998.
- [CF01] R. Canetti and M. Fischlin. Universally composable commitments. In J. Kilian, editor, *Advances in Cryptology - Crypto 2001*, pages 19–40, Berlin, 2001. Springer-Verlag. Lecture Notes in Computer Science Volume 2139.
- [CGT95] C. Crépeau, J. van de Graaf, and A. Tapp. Committed oblivious transfer and private multi-party computation. In Don Coppersmith, editor, *Advances in Cryptology - Crypto '95*, pages 110–123, Berlin, 1995. Springer-Verlag. Lecture Notes in Computer Science Volume 963.
- [CK88] C. Crépeau and J. Kilian. Achieving oblivious transfer using weakened security assumptions. In *29th Annual Symposium on Foundations of Computer Science*, pages 42–52, White Plains, New York, USA, 24–26 October 1988. IEEE.

- [CM97] Christian Cachin and Ueli Maurer. Unconditional security against memory-bounded adversaries. In Burt Kaliski, editor, *Advances in Cryptology: CRYPTO '97*, volume 1294 of *Lecture Notes in Computer Science*, pages 292–306. Springer, 1997.
- [Dam00] I. Damgård. Efficient concurrent zero-knowledge in the auxiliary string model. In Bart Preneel, editor, *Advances in Cryptology - EuroCrypt 2000*, pages 418–430, Berlin, 2000. Springer-Verlag. Lecture Notes in Computer Science Volume 1807.
- [DFMS04] I. Damgård, S. Fehr, K. Morozov, and L. Salvail. Unfair noisy channels and oblivious transfer. In *The First Theory of Cryptography Conference, TCC 2004*, volume 2951 of *Lecture Notes in Computer Science*, pages 355–373, Cambridge, MA, USA, February 2004. Springer-Verlag.
- [DFS04] I. Damgård, S. Fehr, and L. Salvail. Zero-knowledge proofs and string commitments withstanding quantum attacks. Research Series RS-04-9, BRICS, Department of Computer Science, University of Aarhus, May 2004.
- [DHRS04] Yan Zong Ding, Danny Harnik, Alon Rosen, and Ronen Shaltiel. Constant-round oblivious transfer in the bounded storage model. In Moni Naor, editor, *Proc. 1st Theory of Cryptography Conference (TCC 2004)*, volume 2951 of *Lecture Notes in Computer Science*, pages 446–472. Springer, 2004.
- [Din01] Yan Zong Ding. Oblivious transfer in the bounded storage model. In Joe Kilian, editor, *Advances in Cryptology: CRYPTO 2001*, volume 2139 of *Lecture Notes in Computer Science*. Springer, 2001.
- [DKS99] I. Damgård, J. Kilian, and L. Salvail. On the (im)possibility of basing bit commitment and oblivious transfer on weakened security assumptions. In Jacques Stern, editor, *Advances in Cryptology - EuroCrypt '99*, pages 56–73, Berlin, 1999. Springer-Verlag. Lecture Notes in Computer Science Volume 1592.
- [DM04] Stefan Dziembowski and Ueli Maurer. Optimal randomizer efficiency in the bounded-storage model. *Journal of Cryptology*, 17(1):5–26, 2004.
- [DN03] I. Damgård and J.B. Nielsen. Universally composable efficient multiparty computation from threshold homomorphic encryption. In D. Boneh, editor, *Advances in Cryptology - Crypto 2003*, pages 272–287, Berlin, 2003. Springer-Verlag. Lecture Notes in Computer Science.
- [DNS98] C. Dwork, M. Naor, and A. Sahai. Concurrent zero-knowledge. In *Proceedings of the Thirtieth Annual ACM Symposium on the Theory of Computing*, pages 409–418, Dallas, TX, USA, 24–26 May 1998.
- [Gas02] M.R. Gasarch. Guest column: The $P=?NP$ poll. *SIGACT NEWS*, 33(2):34–47, June 2002.
- [GMR89] S. Goldwasser, S. Micali, and C. Rackoff. The knowledge complexity of interactive proof-systems. *SIAM Journal on Computing*, 18(1):186–208, 1989.

- [GMW91] O. Goldreich, S. Micali, and A. Wigderson. Proofs that yield nothing but their validity, or all languages in np have zero-knowledge proof systems. *Journal of the ACM*, 38(3):691–729, 1991.
- [Kil88] J. Kilian. Founding cryptography on oblivious transfer. In *Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing*, pages 20–31, Chicago, Illinois, 2–4 May 1988.
- [LC97] H.-K. Lo and H.F. Chau. Is quantum bit commitment really possible? *Physical Review Letters*, 78:3410–3413, 1997.
- [Lu04] Chi-Jen Lu. Encryption against storage-bounded adversaries from on-line strong extractors. *Journal of Cryptology*, 17(1):27–42, 2004.
- [Mau92] Ueli M. Maurer. Conditionally-perfect secrecy and a provably-secure randomized cipher. *Journal of Cryptology*, 5:53–66, 1992.
- [May97] D. Mayers. Unconditionally secure quantum bit commitment is impossible. *Physical Review Letters*, 78:3414–3417, 1997.
- [MW03] U. Maurer and S. Wolf. Secret key agreement over a non-authenticated channel — part i: Definitions and bounds. *IEEE Transactions on Information Theory*, 49(4):822–831, April 2003.
- [NTS99] Noam Nisan and Amnon Ta-Shma. Extracting randomness: A survey and new constructions. *Journal of Computer and System Sciences*, 58(1):148–173, 1999.
- [NZ96] Noam Nisan and David Zuckerman. Randomness is linear in space. *Journal of Computer and System Sciences*, 52(1):43–52, February 1996.
- [RK99] R. Richardson and J. Kilian. On the concurrent composition of zero-knowledge proofs. In Jacques Stern, editor, *Advances in Cryptology - EuroCrypt '99*, Berlin, 1999. Springer-Verlag. Lecture Notes in Computer Science Volume 1592.
- [Sal98] L. Salvail. Quantum bit commitment from a physical assumption. In Hugo Krawczyk, editor, *Advances in Cryptology - Crypto '98*, pages 338–353, Berlin, 1998. Springer-Verlag. Lecture Notes in Computer Science Volume 1462.
- [Sho94] P. Shor. Algorithms for quantum computation: Discrete logarithms and factoring. In *35th Annual Symposium on Foundations of Computer Science*, pages 124–134, Santa Fe, New Mexico, 20–22 November 1994. IEEE.
- [Vad04] Salil P. Vadhan. Constructing locally computable extractors and cryptosystems in the bounded-storage model. *Journal of Cryptology*, 17(1):43–77, 2004.
- [vdG97] J. van de Graaf. *Towards a Formal Definition of Security for Quantum Protocols*. PhD thesis, Computer Science and Operational Research Department, Université de Montréal, 1997.
- [Wie83] S. Wiesner. Conjugate coding. *Sigact News*, 15(1):78–88, 1983. Early manuscript circa 1969.