Ref. Ares(2024)1066130 - 13/02/2024

Funded by
the European Union

QSI Project 101072637

HORIZON-MSCA-2021-DN-01

Quantum-Safe Internet (QSI)

Scientific Deliverable 1:

Quantum Protocols Projects State of Play

Deliverable D.1.1 – WP 1

Index:

I. INTRODUCTION

In Work Package 1, we consider a suite of protocols that exploit quantum, post-quantum and hybrid techniques towards the final goal of achieving a quantum-safe Internet, and we study their security and performance by combining our expertise in quantum and modern cryptography, quantum algorithms, computer science, and mathematics.

The doctoral candidates participating in Work Package 1 and the institutions to which they belong are listed below:

Doctoral Candidate 1:	Alessandro Marcomini,	University of Vigo.	(Spain)
Doctoral Candidate 2:	Silvia Ritsch,	University of Eindhoven.	(Netherlands)
Doctoral Candidate 3:	Álvaro Yángüez,	University of Sorbonne.	(France)
Doctoral Candidate 4:	Gina Muuss,	University of Amsterdam.	(Netherlands)
Doctoral Candidate 5:	Massimo Ostuzzi,	University of Bochum.	(Germany)
Doctoral Candidate 12:	Fabrizio Sissini,	University of Denmark.	(Denmark)

Next we provide a brief overview of the main objectives of their projects. For a detailed description of the projects, see section II.

Doctoral Candidate 1 will improve the security proofs of Quantum Key Distribution (QKD) protocols by considering the most relevant device imperfections of the users' apparates, which may result in side-channels compromising the security of the real implementations. He will also design novel QKD protocols with enhanced performance. One further limitation of QKD is its requirement to pre-share secret information between the legitimate users of the system, and various solutions will be investigated to this problem.

Doctoral Candidate 2 will study Key Exchange (KE) protocols that do not have the requirement of pre-sharing secret information between the legitimate users of the system, and investigate if the use of quantum communications could be advantageous in a post-quantum setting. Indeed, developing hybrid techniques that can keep the best functionalities of quantum and post-quantum cryptography, namely, the long-term security provided by QKD and the versatility of implementation and high performance of Post Quantum Cryptography (PQC), is a necessity for many applications to improve the performance and security of existing solutions.

Doctoral Candidate 3 will investigate the possibility of implementing certain functionalities/subroutines within PQC algorithms more efficiently by means of quantum communications protocols. Here, special attention is paid to secure multiparty computation (MPC) algorithms.

Doctoral Candidate 4 takes on the challenge of finding techniques to upgrade existing security proofs of hash-based constructions such as memory-hard functions (MHFs) against classical adversaries to quantum adversaries.

Doctoral Candidate 5 and **Doctoral Candidate 12**, on the other hand, are concerned with the quantum security of the coding and lattice-based PQC cryptosystems and their key encapsulation mechanisms in the National Institute of Standards and Technology (NIST) standardization competition, and will investigate the effectiveness of quantum attacks against them.

II. DETAILED DESCRIPTION OF THE PROJECTS

Project of Doctoral Candidate 1: Alessandro Marcomini, University of Vigo.

“QUANTUM KEY DISTRIBUTION WITH ENHANCED SECURITY AND PERFORMANCE”.

OBJECTIVES

Improve the implementation security and performance of prepare-and-measure QKD setups, particularly those based on quantum interference. Investigate methods to address the authentication problem in QKD.

EXPECTED RESULTS

Security proof techniques that incorporate device imperfections of QKD transmitters. Novel twin-field QKD schemes with improved performance. Efficient solutions to authenticate the first QKD round.

DESCRIPTION

The principal merit of QKD is that, in theory, it allows to securely expand an initial secret key shared between distant users. In practice, however, device imperfections of real QKD implementations could open security loopholes, or so-called side-channels, that might compromise the security of the key. One main goal of this project is to develop methods to efficiently tackle device imperfections in the security proofs of QKD. For this, we will consider QKD setups based on quantum interference, e.g., measurement-device-independent (MDI) and twin-field (TF) QKD, and prove their security in a realistic setting. These setups have the advantage of being immune against any side-channel from the measurement unit, and, thus, only transmitter’s imperfections must be considered. Also, we shall investigate variants of TF-QKD which might improve the performance and/or practicality of current leading approaches, which include the CAL19 and the sending-and-not-sending TF-QKD protocols as prominent examples. Finally, we will study efficient solutions to authenticate the first QKD round, which currently requires that the legitimate users of the system pre-share initial short secret keys (e.g. these keys could be preinstalled in the QKD equipment) in order to authenticate the classical communication channel between them. This might be particularly problematic when the number of users increases.

METHODOLOGY

The Doctoral Candidate will use the reference technique to account for the security loop holes due to side channels; improvements to reference technique will also be considered. Key features responsible for the performance of TF-QKD variants will be determined, and the feasibility of novel schemes combining the best features will be studied.

RISKS

If analytical security proof techniques are loose, numerical methods will be used. If no TF-QKD variant is found to outperform current schemes, we study restricted parameter regimes.

Project of Doctoral Candidate 2: Silvia Ritsch, University of Eindhoven.

“SECURE KEY-EXCHANGE IN A QUANTUM WORLD”.

OBJECTIVES

Modelling and developing secure KE protocols in a setting with quantum adversaries. Understanding the impact of quantum communications in this setting.

EXPECTED RESULTS

Sound models for KE in a quantum world and proven security in these models.

DESCRIPTION

One of the most challenging tasks of modern cryptography is to establish a commonly known secret between two parties, without pre-shared information, using only publicly known information. This is a setting that everyone faces multiple times a day when securely connecting to servers on the Internet. The KE mechanisms used today are all vulnerable to attacks using Shor’s algorithm and consequently will all be broken by quantum computers. This setting is also not solved by standard QKD protocol, which require pre-shared information and therefore are of no use in this scenario. Different applications have different requirements on

KE mechanisms. Most importantly, KE mechanisms are distinguished by which parties are authenticated (authenticated or partially authenticated KE), if no parties are authenticated (anonymous KE), or if parties can even deny having participated in a KE although being authenticated towards the other party (deniable authenticated KE). The first step of the project will be to define appropriate security models for these different flavours of KE for settings in which adversaries and possibly also honest parties have quantum computing capabilities. So far there only exist models that consider quantum adversaries for the most basic flavour of KE; models for the more advanced flavours of KE are still lacking in this setting. In the case of honest parties with quantum computing capabilities, models are limited to the more basic primitives of secret key encryption, message authentication, and digital signatures. After defining sound models, the Doctoral Candidate will do research in protocols that are secure in these models and will analyse advantages and disadvantages of using quantum communications to achieve KE in this setting.

METHODOLOGY

The project takes the approach of exact provable security, where reductionist proofs relate the security of protocols to the complexity of solving a (supposedly hard) mathematical problem, or of breaking a smaller building block, like an encryption scheme. In this approach, the given bounds are given exactly, which allows us to later justify parameter choices using these proofs.

RISKS

It might be impossible to develop KE mechanisms with the discussed special properties, even when considering quantum communications. If the research points in this direction, the project will aim at proving this instead. This would be a major result demonstrating what is achievable.

Project of Doctoral Candidate 3: Álvaro Yángüez, University of Sorbonne.

“QUANTUM-ENHACED SECURE MULTIPARTY COMPUTING”.

OBJECTIVES

Developing efficient quantum-safe functionalities by embedding quantum subroutines in PQC schemes.

Funded by
the European Union

EXPECTED RESULTS

A methodological approach to identifying quantum subroutines within post-quantum schemes for distributed quantum computing and communications tasks, supported by a proof-of-principle photonic demonstration for MPC.

DESCRIPTION

Classical and quantum worlds each offer a distinct feature when it comes to security. Classical solutions offer solid mathematical foundations and easiness of implementation, while quantum ones can enhance the security of cryptographic techniques by making them unbreakable against future technological advancements. A hybrid QS infrastructure should then offer the best of both worlds. To enable the transition to such an infrastructure, it is necessary to put in place a concrete methodology combining theoretical, simulation and experimental techniques. In this project, we propose a step-by-step approach to solve this problem. We first establish the security and efficiency bottlenecks associated with novel post-quantum functionalities, e.g., in multiparty computing, verification and delegation.

Afterwards, we design quantum subroutine protocols for these bottlenecks. Finally, we implement these protocols by constructing purpose built devices. We use as a basis the quantum protocol zoo (https://wiki.veriqloud.fr), an open repository of protocols for quantum networks.

This provides a suitable platform to decompose the protocols under study into building blocks that can be benchmarked as possible subroutines within classical schemes. Our focus and case study will be quantum MPC, which we will analyse and implement in an all photonic client-server setting. We will also consider an extension of this implementation to quantum networks with small processors.

METHODOLOGY

We develop efficient and practical hybrid cryptographic techniques, currently missing in the literature, by identifying a case study. We define and benchmark building blocks for subroutines in classical schemes in view of a realistic photonic implementation.

RISKS

The main challenge is how to benchmark the identified protocols and demonstrate quantum advantage. We expect that the strong interplay between theory and experiment in this project, and the extended experience of our group in verification techniques, and in the demonstration of quantum advantage with practical photonic systems, will mitigate these risks and lead to realistic solutions for a hybrid infrastructure.

Project of Doctoral Candidate 4: Gina Muuss, University of Amsterdam.

“QUANTUM SECURITY OF MEMORY-HARD FUNCTIONS”.

OBJECTIVES

Investigate and establish the quantum security of memory-hard functions.

EXPECTED RESULTS

Framework of post-quantum security definitions and proofs for memory-hard functions, proofs of space, proofs of sequential work and verifiable delay functions.

DESCRIPTION

Memory-hard functions (MHFs) are moderately hard to evaluate when using a large amount of memory, but in case only a small amount of memory is available, they are slow to evaluate. Such functions are useful for the application of password hashing in order to prevent brute-force attacks when password hashes are stolen. MHFs can also be used to build proofs of space, proofs of sequential work or verifiable-delay functions. Partly fuelled by the rise of cryptocurrencies, there has been a lot of (non-quantum) research in this area over the last few years. However, we are not aware of any post-quantum analysis of these primitives. The underlying principle for constructing MHFs are evaluations of hash functions, therefore, security proofs are usually given in the random-oracle model (ROM) where the hash functions are assumed to be perfectly random functions. It is a very natural and timely problem to investigate the post-quantum security of these constructions against quantum attackers. In practice, if fully specified hash functions such as SHA2 or SHA3 are used, a quantum attacker can run these functions in superposition on its quantum computer. Hence, it is imperative to revisit the security proofs in the quantum ROM (QROM).

METHODOLOGY

In this project, the Doctoral Candidate will define quantum security notions of MHFs as well as their derivatives. We then investigate which ROM proofs can be upgraded to the QROM.

RISKS

The current QROM proof techniques might be insufficient to analyse all of the existing constructions. If the development of stronger tools turns out to be infeasible during the project period, the schemes will be modified (at the cost of efficiency) in order to be able to prove QROM security.

Project of Doctoral Candidate 5: Massimo Ostuzzi, University of Bochum.

“FROM CLASSSICAL TO QUANTUM CRYPTOANALYSIS OF POST-QUANTUM CRYPTOGRAPHY”.

OBJECTIVES

Design new quantum attacks for the post-quantum cryptosystems in NIST standardization.

EXPECTED RESULTS

Precise definition of quantum bit-security level, possibly requiring adaptation of current parameter settings.

DESCRIPTION

NIST will soon announce winners of their post-quantum cryptographic standardization process. For encryption, these will be coding- and lattice-based cryptosystems. While the classic hardness of these schemes has been studied thoroughly, their hardness against quantum attacks is way less understood. As an example, classical decoding algorithms have seen tremendous improvements within the last decade with implications to McEliece parameter selection, while the best known quantum attack on McEliece is still a simple Groverversion of a decoding algorithm from 1962. Also in lattices, in the last decade there were plenty of algorithmic improvements on the classical side, including sieving and locality sensitive hashing, while the speedup from quantum algorithms is almost negligible. We will design new quantum attacks directly on PQC, and provide a concrete quantum security bit estimator software for coding- and lattice-based cryptosystems.

METHODOLOGY

We build on typical quantum tools for algorithm design, such as quantum random walks. Whenever possible, we focus on algorithmic tools with small quantum memory consumption.

RISKS

If we fail to find asymptotic improvements for quantum cryptanalytic algorithms, as a fall back, we will concentrate on second order improvements and on improved implementations. Improvements in these areas are also highly relevant to the current post-quantum standardization process.

Project of Doctoral Candidate 12: Fabrizio Sissini, University of Denmark.

"EFFICIENT SECURITY FOR POST-QUANTUM KEY ENCAPSULATION WITH CORRECTNESS ERRORS".

OBJECTIVES

Establish and tighten the PQC security of the Fujisaki-Okamoto (FO) transform with focus on Lattice and Code-based schemes.

EXPECTED RESULTS

Security reductions for correctness error finding in lattice-based and code-based chosen cipher text attack (CCA)-secure key encapsulation mechanisms (KEMs). Attack algorithms for finding failures in lattice-based and code-based public key encryption (PKE). Improved security proof or attack for FO-based PKE DE randomization in the QROM.

DESCRIPTION

PQC-secure KEMs have received a lot of attention due to the ongoing NIST standardization efforts. All-important PQC KEMs with chosen cipher text security use the FO transformation whose security needs to be established in the QROM.

Security proofs have improved steadily over the years, but leave two important loose ends:

1) The way decryption errors have been handled in security proofs involved heuristics and suffered from arguably unnatural security losses.

2) A central technique for QROM security proofs of FO, the one way-to-hiding (O2H) lemma suffers from unexplained security losses despite many improvements. Recent progress for 1) has provided a framework for a heuristic-free and tightened security reduction technique dealing with decryption errors. It requires, however, two additional security properties from the underlying PKE. After familiarizing themselves with different code-based and lattice-based PKE schemes, the Doctoral Candidate will work on the characterization of lattice- and

code-based PKE with respect to the two security properties needed for conclusively tying up loose end 1). In addition, the Doctoral Candidate will study the O2H lemma and its application to PQC security proofs for FO and work on tightening those proofs.

METHODOLOGY

The project will exploit the complexity theory of lattice problems. Crucially, the Doctoral Candidate will develop analytical tools to handle discretized versions of classic random matrix ensembles.

RISKS

It might be the case that the current application of the O2H lemma to FO is tight due to a uniquely quantum attack. To mitigate this risk, the Doctoral Candidate will pivot to researching attack avenues in case the provable security effort stalls.

III. PROGRESS OF EACH DOCTORAL CANDIDATE AND HER/HIS PROJECT

Project of Doctoral Candidate 1: Alessandro Marcomini, University of Vigo.

CONTRACT STARTING DATE: 26/01/2023.

SUPERVISORS: Curty (UVIGO), Tamaki (UT), Zbinden (UNIGE), Shields (TOSHEU), Azuma (NTT), Hülsing (TU/e)

PROGRESS AND RESULTS:

Quantum key distribution (QKD) protocols promise to enable information-theoretically secure encryption schemes by exploiting the laws of quantum mechanics. Nevertheless, an actual security certification for practical implementations of QKD requires to take into account the experimental limitations and imperfections of real devices. A particularly important class of defects is that involving phase correlations across laser pulses for QKD schemes that rely on weak coherent laser pulses (WCPs). These pulses can be modelled as a classical mixture of photon number states under the hypothesis of perfect phase randomization. However, this is not the case for lasers working under high-speed gain-switching conditions, as residual photons in the cavity can induce phase correlations across consecutive pulses, violating the requirement of uniformly random phases.

A security proof robust against such imperfections has been recently proposed in [1]. To be applied, this security proof requires knowledge of a parameter that quantifies how close the conditional distribution of each phase is to a uniform distribution, given knowledge of all the other phases. Thus, the missing step to close this imperfection is to figure out how to experimentally estimate this parameter. In [2] authors showed that, under the assumption that the correlation length is one, one can estimate the dispersion of the phase probability distribution by measuring the visibility of interference between adjacent pulses. However, in practical high-speed setups, non-negligible correlations might exist beyond immediately adjacent pulses.

The goal of my first talk within this project is to extend the approach introduced in [1] and [2] by proposing an experimental method to characterize the parameter in the case of arbitrary length of correlations in realistic setup conditions. In particular, it requires modelling of the phase generation process inside the cavity in the presence of multiple correlating factors as an extension of known studies on first-order correlations [2]. Moreover, I aim to design an implementable experimental routine to enable the measurement of the required parameter for the aforementioned security proof.

Work and results:

I dedicated the first months of the project to the study of laser physics and device characterization. I have been facing drawbacks mainly due to the very technical aspects of my investigation. In detail, higher-order phase correlations in laser pulses happened to be considered a very marginal phenomenon often addressed as “neglectible”, causing it to be never really analyzed properly in the literature. This caused me to spend an unforeseen amount of time searching for reliable and accurate references to set the ground base of my research. Eventually, I found sufficient material to justify the introduction of my own model to tackle the task I was given [1,2,3].

In detail, the crucial part of my work consists of determining experimentally the probability distribution function (PDF):

$$f(\phi_i|\phi_{i-1},\phi_{i-2},\dots,\phi_{\ell_c})$$

That is, the conditional probability of the phase of the i –th pulse, given knowledge of the ℓ_c previous ones. To figure out the analytical form of this function, one needs to understand deeply the fundamental physics that rules the field buildup in the case in which multiple photon populations survive in the laser cavity. I devolved over three months to the investigation of this phenomenon, eventually concluding that the previous PDF takes the form of a wrapped gaussian distribution:

$$f_{wg}(\phi_i;\hat{\phi}_i,\sigma) = \sum_{k=-\infty}^{\infty} f_g(\phi_i + 2k\pi;\hat{\phi}_i,\sigma)$$

being f_g the gaussian distribution. The most probable value $\hat{\phi}_i$ depends on the previous realisations of the phase $\phi_{i-1},\dots,\phi_{i-\ell_c}$ as:

$$\hat{\phi}_i(\phi_{i-1},\dots,\phi_{i-\ell_c}) = arg\left(\phi_{i-1} + \sum_{n=2}^{\ell_c} r_n e^{j\phi_{i-n}}\right)$$

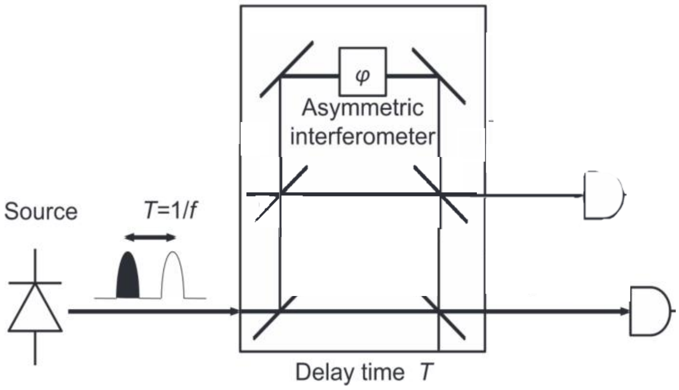
where j denotes the imaginary unit and $\{r_n\}_n$ are experimental parameters to be estimated or bounded, describing the strength of correlations in the cavity.

Importantly, I noticed how the security of the protocol depends on the standard deviation of the phase conditional distribution. Hence, I needed to design an experimental routine that allows for the estimate of this parameter. In particular, I found that for fixed values of $\phi_{i-1},\dots,\phi_{i-\ell_c}$, the random variable $\tilde{\phi}_i(\phi_{i-1},\dots,\phi_{i-\ell_c}) := \phi_i - \hat{\phi}_i(\phi_{i-1},\dots,\phi_{i-\ell_c})$ follows the distribution $f_{wg}\left(\tilde{\phi}_i(\phi_{i-1},\dots,\phi_{i-\ell_c});0,\sigma\right)$ and

$$\langle e^{i\tilde{\phi}_i}\rangle = e^{-\frac{\sigma^2}{2}}$$

Importantly, the expectation value in the equation above is strongly related to the visibility of an interferometric measure. Hence, I proposed the preparation of an interferometer with multiple delay lines so to use previously emitted light to recreate the phenomena occurring inside the cavity. An example of such for the case ℓ_c = 2 is reported in the figure below. By introducing amplitude attenuators in the delay lines of the interferometer, it is possible to sweep over different relative intensities to ultimately find the maximum of the interference visibility. This occurs when the attenuators settings match the values of the $\{r_n\}_n$ parameters of the cavity. In this situation, the only limitation to visibility is due to spontaneous emissions in the cavity that ultimately cause decoherence and phase randomization. Hence, this approach effectively allows to measure the ignorance on the next pulse phase, given access to the previous ones.

The final part of my work consisted in talks with experimentalists to verify the actual feasibility of my proposal. Eventually, it resulted in us preparing a plan for an experiment that might validate the model also on a real implementation. At the time of writing I am polishing the details of a paper for journal submission.



Interferometric scheme to measure the parameters of the wrapped normal distribution of the phase. Figure adapted from [2].

Conclusions and outlook:

In this work I successfully modelled phase correlations in gain-switching lasers beyond the first order. By introducing experimental schemes and optimization targets, I enable the application of the security proof proposed in [1] to real devices, ultimately allowing for security estimation in high-speed implementations of QKD. An experimental validation of the proposal has been planned and is currentlyunder development.

References:

[1] G. Currás-Lorenzo, S. Nahar, N. Lütkenhaus, K. Tamaki, M. Curty, "Security of quantum key distribution with imperfect phase randomisation", Quantum Science Technology 9, 015025 (2023).

[2] Kobayashi T., Tomita A. and Okamoto A., "Evaluation of the phase randomness of a light source in quantum-key-distribution systems with an attenuated laser". *Physical Review A 90, 07 (2014).*

[3] Glauber R.J., Nobel Lecture 2005.

PUBLICATIONS:

- A. Marcomini, G. Currás-Lorenzo, D. Rusca, M. Curty, "Characterising higher-order phase correlations in gain-switched laser sources with application to decoy-state QKD", "Primera Reunión Nacional del Plan Complementario de Comunicacione Cuánticas", Universidad Politécnica de Madrid (Spain), September 19-21, 2023.

- Marcomini, G. Currás-Lorenzo, D. Rusca, M. Curty, “Characterising higher-order phase correlations in gain-switched laser sources with application to decoy-state QKD”, 13th international conference on quantum cryptography (QCRYPT2023), University of Maryland, USA, 14 August–18 August 2023.

Project of Doctoral Candidate 2: Silvia Ritsch, University of Eindhoven.

CONTRACT STARTING DATE: 05/10/2022.

SUPERVISORS: Hülsing (TU/e), Skoric (TU/e), Lange (TU/e), Schaffner (UvA), Broadbent (TTBE), Daum (Genua), Shields (TOSHEU).

PROGRESS AND RESULTS:

Key exchange is a fundamental concept in cryptography that allows two parties to establish a shared secret key over an insecure communication channel. This shared secret key can then be used to encrypt and decrypt messages between the two parties.

Asymmetric encryption algorithms such as RSA can be used to encrypt messages, but they are not suitable for encrypting large amounts of data due to their slow speed and limited message length.

Symmetric encryption algorithms, on the other hand, are much faster and can encrypt large amounts of data. However, symmetric encryption requires that both parties share the same secret key, which is difficult to establish over an insecure communication channel. This is where key exchange algorithms come into play. Key exchange algorithms allow two parties to establish a shared secret key over an insecure communication channel. This shared secret key can then be used for symmetric encryption, which is much faster and more efficient for encrypting large amounts of data.

In summary, key exchange is necessary to establish a shared secret key between two parties over an insecure communication channel. This shared secret key can then be used for symmetric encryption, which is much faster and more efficient for encrypting large amounts of data than asymmetric encryption algorithms such as RSA.

As a result, secure key exchange is a major area of study. Main goals of key exchange protocols are to ensures that the communication remains encrypted (confidentiality), data is transmitted securely without modification (integrity), and no attacker can impersonate a client (authenticity). There are several approaches to address the challenge of authenticated key exchange, with public-key infrastructure (PKI) and password-authenticated key exchange (PAKE) as examples.

Password-Authenticated Key Exchange

One of the major advantages of PAKE is its relative simplicity. All that is required from a user is a password, with no additional structure such as certificates or key management. We need the protocol to offer strong security guarantees even when this password is short, simple (i.e., human-memorable), offering only low entropy. Most models include forward-secrecy, guaranteeing the security of past exchanges even if a password is leaked in the future. This is in part due to the fact that they are resistant to offline dictionary attacks, which would enable an attacker to infer information on the exchange simply by observing the exchange. Active attacks on the protocol can be mitigated in many ways, for example by limiting the amount of wrong password attempts per user. PAKEs are resistant to man-in-the-middle attacks, and also do not require additional hardware.

These properties have made it attractive for developers, and it is currently deployed in applications such as secure backups of the messaging client WhatsApp, end-to-end encrypted messaging (such as in Signal’s X3DH) and authentication methods such as the PACE protocol as it is used in German personal ID’s.

Provident cryptography

Since the keys established by key exchange may be used to protect data that will be considered sensitive for a long time (such as company or even military secrets), it is important that security is guaranteed even against attackers whose attack capabilities might increase over time. Crucially, an attacker may record encrypted communications to attempt decrypting the communication at a later point in time. In consequence, past communication will be at risk when the used cryptography can be broken by novel attacks or attacks that are enabled by advances in computing. Along the same lines, this motivates the design of protocols with vigorous cryptographic security proofs, to minimize the possibility of attacks on the protocol being discovered. Of particular concern are advances in quantum computing that enable attacks on many currently deployed protocols and encryption schemes, such as the widely used Diffie-Hellman Key Exchange or RSA Encryption.

Goals

Interest in authentication methods that do not rely on bulky public-key infrastructure (PKI) has increased in recent years, as evidenced in the Internet Research Task Force (IRTF)'s call for proposals. Partially motivated by this interest, one goal of the project was the design of a PAKE protocol that is proven secure against attackers with quantum computing capabilities. This includes the study of existing protocols, selection of a candidate protocol and developing a rigorous security proof.

Background research

Working on security proofs in a post-quantum setting required some background in quantum-computing, proof techniques for post-quantum cryptography and security models for authenticated key exchange (AKE), among others. To that end, I spent some time during the first months of the project to familiarize myself with these topics, with the support of my supervisors.

Collaboration

Soon, a collaboration was established with researchers in several countries, including Germany, Portugal, Luxembourg and the USA, to jointly work on several ideas for PAKE.

OCAKE

There are several types of PAKE protocols, with encrypted key exchange (EKE) being one of the earliest and most common. It has recently been shown how its quantum-vulnerable DH component can be replaced by a suitable post-quantum secure asymmetric encryption key. This allows the use of key encapsulation mechanism (KEM) algorithms such as the NIST finalists Kyber, FrodoKEM, Classic McEliece among others. During the project, we identified the OCAKE protocol (https://eprint.iacr.org/2023/1368) as a promising candidate for a post-quantum secure protocol. While the original paper already gave a security proof, this proof only considered attackers without quantum capabilities.

A major first goal thus was to adapt the security proof in a way such that security can also be shown against quantum attackers, but we encountered two barriers:

Firstly, the original proof of OCAKE was given in in a theoretical framework called the universal composability (UC) framework, which does not yet have an extension that considers quantum attackers.

Secondly, the OCAKE construction involves another building block, called block cipher. The original security proof uses an idealization of that cipher. Again, there is no quantum-accessible counterpart for this model that allows for the needed proof techniques. The involvement of the ideal cipher model will pose a big challenge since recent results have given indication that establishing proof techniques of such a model poses a number of difficulties.

Standard-Model Proof of OCAKE

To address the first barrier, we decided to first switch from the UC framework to a framework that is more compatible with post-quantum proof techniques. To that end, we decided to switch from the UC model to the (also well-established) PAKE model often referred to as the BPR model after its inventors.

This effort lead to a paper (https://eprint.iacr.org/2023/1368.pdf) which is now available on the preprint server of the International Association for Cryptologic Research (enabling open-access) and is currently in submission. The submission features a detailed proof of security of the OCAKE protocol in the BPR model, paving the way to a proof of security against quantum attackers.

This required the study of security models for PAKE, in particular the BPR model, the Universal Composability framework, proof techniques for the random oracle and ideal cipher, hybrid proof techniques, and KEM security properties.

Outlook: Solving the ideal cipher question

To address the second barrier, that is the issues that the ideal cipher presents in a post-quantum setting, we studied several approaches. Simple masking-based approaches proved insufficient, so further research will be in the direction of symmetric primitives that offer the necessary programmability in a quantum-accessible setting. A secondary area of study is if and how the UC framework can be expanded such that it becomes compatible with our main goal, proving PAKE security against quantum attackers.

PUBLICATIONS:

- N. Alnahawi, K. Hövelmanns, A. Hülsing, S. Ritsch, and A. Wiesmaier. Towards post-quantum secure PAKE – A tight security proof for OCAKE iPR model. Currently submitted to EUROCRYPT. Preprint to be found at https://eprint.iacr.org/2023/1368.

Project of Doctoral Candidate 3: Álvaro Yángüez, University of Sorbonne.

CONTRACT STARTING DATE: 01/10/2023.

SUPERVISORS: Diamanti (SU), Kashefi (SU), Speelman (UvA), Jeffery (CWI), Kaplan (VERIQLOUD), Layat (IDQUANTIQUESA).

PROGRESS AND RESULTS:

The goal of my doctoral project within the Doctoral Network is to devise efficient quantum-resistant functionalities by integrating quantum subroutines into post-quantum cryptography (PQC) schemes. Furthermore, the overarching objective encompasses the exploration of multiparty computing (MPC) functionalities and their implementation within an all-photonic client-server framework. To initiate this endeavor, our preliminary focus has been on analyzing and implementing its foundational primitive: the oblivious transfer (OT) functionality.

In the field of cryptography, a foundational approach commonly employed is the utilization of primitives. These primitives serve as fundamental building blocks, encompassing basic operations and algorithms that underpin more complex cryptographic systems. The primitive of MPC is OT. Thus, by establishing a viable implementation of a post-quantum secure OT protocol, we can subsequently advance towards achieving a post-quantum secure MPC protocol.

It has been demonstrated that by incorporating quantum subroutines, a quantum-resistant OT functionality can be realized [1] [3]. Furthermore, both studies arrive at a consistent conclusion: OT can be constructed based solely on the presumption of quantum-hard one-way functions (OWF). This implies that quantum-enhanced OT necessitates less stringent security assumptions compared to its classical counterpart.

In the initial weeks, I acquainted myself with the research area and, in particular, the OT protocol proposed by Bartusek *et al.* [1]. This focus was informed by the findings of prior research conducted by my colleagues, which determined that Bartusek’s protocol was more feasible for implementation compared tothe protocol presented by Grilo *et al.* [3]. Upon understanding the protocol, my initial objective was to introduce modifications aimed at reducing memory requirements. The first task involved determining the necessary number of distribution photons to ensure a quantum-secure OT interaction. To accomplish this, we utilized the distance inequality provided by Bouman and Fehr [2].

The first result we obtained was to realize that the inequality proposed by Bouman and Fehr [2] was incorrect in the OT case. The inequality we derived, which quantifies the distance between a non-correlated state and a correlated one based on statistical sampling error and privacy amplification, proved to be more accurate than the previously proposed one.

Secondly, we found that the protocol proposed by Bartusek *et al.* [1] is not practically implementable, as it would necessitate on the order of 10^{10} photons for a single OT interaction. Such a requirement would result in an execution time of roughly one week using an average single-photon source.

Therefore, we have developed a new protocol based on the one proposed by Bartusek*et al.* Through simulation-based proof techniques, we have demonstrated that our bit commitment subprotocol satisfies both equivocality and extractability criteria. Further- more, we have introduced new analytical expressions that facilitate precise quantification of the security parameters, a crucial aspect for its experimental implementation. Notably, our proposed protocol necessitates between 10^6 - 10^7photons, translating to a runtime of mere seconds for a single OT interaction.

Given that the ultimate goal is to establish a quantum-secure MPC protocol, the underlying OT protocol must exhibit not only simulation-based quantum security but also practical implement ability. While prior protocols [1] [3] made significant strides by demonstrating that quantum-enhanced OT demands fewer security assumptions than its classical counterpart, thereby confirming their quantum security, the existing literature has yet to introduce a protocol with a viable implementation. Consequently, our proposed OT protocol represents a pivotal advancement towards the development of a quantum-secure MPC protocol.

The proposed OT protocol has to be further studied in order to understand its scalability and security. Moreover, a more general distance inequality [2] for quantifying the security has to be provided for setting a general scenario in which a malicious Bob can split the measurement basis in any way, not only in a honest one.

We have proposed a new quantum-secure OT protocol which has a feasible experimental implementation. The first step will be to review the protocol while another member of the group implements it. Moreover, I would like to generalize the distance inequality given by Bouman and Fehr [2] and to study possible lighter security assumptions like the use of pseudorandom states (PRS). In order to do so, I will visit the CWI in Amsterdam in the following months.

At the same time, we should study how to scale the OT protocol for designing and implementing a quantum-secure MPC protocol.

References:

[1] James Bartusek. One-way functions imply secure computation in a quantum world. In Advances in Cryptology–CRYPTO 2021: 41st Annual International Cryptology Conference, CRYPTO 2021, Virtual Event. Springer International Publishing, 2021.

[2] Niek J. Bouman and Serge Fehr. Sampling in a quantum population, and applications,2012.

[3] Alex B. Grilo, Huijia Lin, Fang Song, and Vinod Vaikuntanathan. Oblivious transfer is in miniqcrypt. In Advances in Cryptology–EUROCRYPT 2021: 40th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, 2021. Springer International Publishing.

PUBLICATIONS:

- Innocenzi, V. Yacoub, Á. Yángüez, P. Lefebvre, A. B. Grilo,E. Diamanti, “Experimental implementation of Simulation secure Quantum Oblivious Transfer”, 1st Colloquium GdR TeQ “Quantum Technologies”, University of Montpellier, France, November 22-24 (2023).

Project of Doctoral Candidate 4: Gina Muuss, University of Amsterdam.

CONTRACT STARTING DATE: 17/05/2023.

SUPERVISORS: Schaffner (UvA), Speelman (UvA), Jeffery (CWI), May (RUB), Huelsing (TU/e), Vredendaal (NXP).

PROGRESS AND RESULTS:

Memory-hard functions are in use today as hash functions and are for example used to help mitigate problems of spam and password pre-image attacks. With advances in the development of quantum devices, it is important to check their security in this new quantum world. The goal of this project is to establish the quantum security of memory-hard functions and similar notions like proofs of space, proofs of sequential work and verifiable delay functions. Concrete results that are expected for this project are proofs about the memory-hardness of existing functions, and more general results on memory-hardness with quantum adversaries. If the project finds current notions or constructions inadequate, these new results will help users of the functions choose more secure alternatives. Results will also contribute to defining the power of a quantum computer in an academic sense.

To achieve this goal of giving meaningful advice to users of memory hard functions and encompassing the capabilities of quantum devices, I investigate the quantum security of these functions and if the current notions turn out to be inadequate, I will propose new notions that capture security in real world scenarios. To achieve this, I will first upgrade security notions so that they capture the power of quantum devices. With these notions, an attempt will be made to upgrade existing proofs of memory hardness to our new notions utilizing the classical proofs. This will involve modifying the requirements for meeting the notions; resulting in a need for reevaluating existing functions. I will try to keep this as compatible with the classical notions as possible to have results that are comparable and useful. So, to be able to start this work, I first need to review the literature that proofs memory-hardness against classical adversaries, to then upgrade the proofs to a quantum setting.

So far, my work consisted of systemizing and gaining an overview of security proofs against classical adversaries. Understanding these proofs is paramount in building upon them to construct either attacks or security proofs utilizing quantum adversaries. In literature, the predominant way of analyzing the memory-hardness of functions is using pebbling games [1, 2, 3]. Pebbling games are a type of mathematical game played on directed-acyclic graphs; in each turn, the player can either place a pebble on a vertex or remove a pebble from a vertex, according to certain rules. There are different variants of this game, some have been proposed to specifically encompass quantum players. These games are used to analyze classical algorithms for functions that correspond to such a directed-acyclic graph. It has been shown that the amount of memory such a function requires to be computed classically and effectively is lower bounded by the pebbling complexity of the underlying graph.

The question I am currently working towards answering is whether pebbling games (or variations) are a good measure to evaluate memory-hardness for quantum adversaries. To do so, I am currently formalizing the proof of the lower bound more suited towards analysis of quantum adversaries and in parallel I am developing a version of the theorem taking the quantum setting into account. In doing so, I also take note of in which places the proofs breaks when considering a quantum adversary. Giving a proof for the quantum version of the theorem involves fixing all the places the classical proof breaks in the quantum case. First strides towards fixing these issues have been made, but the work is unfinished. In the coming months, I hope to further crystallize the problems that still need solving to prove memory-hardness for certain functions. Leading to insights on a lower-bound for the memory needed to execute certain functions on a quantum computer.

References:

[1] Joël Alwen and Vladimir Serbinenko. High Parallel Complexity Graphs and Memory-Hard Functions. Publication info: Preprint. MINOR revision. 2014. URL: https://eprint.iacr.org/2014/238 (visited on 12/08/2023).

[2] Jeremiah Blocki and Blake Holman. “Sustained Space and Cumulative Complexity Trade-Offs for Data-Dependent Memory-Hard Functions”. en. In: Advances in Cryptology – CRYPTO 2022. Ed. by Yevgeniy Dodis and Thomas Shrimpton. Lecture Notes in Computer Science. Cham: Springer Nature Switzerland, 2022, pp. 222–251. ISBN: 978-3-031-15982-4. DOI: 10. 1007/978-3-031-15982-4_8.

[3] Dan Boneh, Henry Corrigan-Gibbs, and Stuart Schechter. Balloon Hashing: A Memory-Hard Function Providing Provable Protection Against Sequen-tial Attacks. Publication info: A major revision of an IACR publication in ASIACRYPT 2016. 2016. URL: https:// eprint. iacr. org/ 2016 / 027(visited on 10/23/2023).

Project of Doctoral Candidate 5: Massimo Ostuzzi, University of Bochum.

CONTRACT STARTING DATE: 05/10/2023.

SUPERVISORS: May (RUB), Walter (RUB), Güneysu (RUB), Schaffner (UvA), Kashefi (SU), Daum (Genua).

PROGRESS AND RESULTS:

I started by studying the material from a course held in Bochum in the past year from my second supervisor, Michael Walter, about Quantum Computing. I had no precise prior knowledge about it as I just knew couple ideas, hence it was really interesting. I've learnt about qubits, quantum logical gates and how to combine them. Then I've studied quantum Fourier transforms, Simon's, Shor's and Grover's algorithms and quantum random walks.

My next task was to try to adapt an algorithm that works perfectly for discrete logarithms to isogenies, fixing the problems I might encounter in the way. I worked on this problem in parallel with another student who is also doing his Ph.D. with Alexander May.

We realized that we could extend our results to a wider range of cryptographic schemes, not just the ones based on isogenies and I started writing a paper on this. We have designed three algorithms and I wrote them down precisely, each of them with its description and proof that shows they work.

We are now finishing the writing of the paper as we want to add a comparison chapter with the already existing algorithms for discrete logarithms. Moreover, together with Michael Walter, and we are now trying to design an algorithm that works even better and faster on quantum computers. We aim to submit the paper to Crypto 2024, which will be held in Santa Barbara next August.

On December, I have joined a reading group about lattice-based cryptography together with some colleagues from my research group and the Cryptography Chair. I have given the first talk, which was about hard problems in lattice theory, SIS and Ring-SIS. After this, I have started getting interested in lattices and I kept reading and studying them.

Project of Doctoral Candidate 12: Fabrizio Sissini, University of Denmark.

STARTING DATE: 08/12/2022

SUPERVISORS: Dragoni (DTU), Majenz (DTU), Hülsing (TU/e), Walter (RUB), Schaffner (UvA), Vredendaal (NXP).

PROGRESS AND RESULTS:

My project is mainly focused on Provable Security both in the Random Oracle Model (ROM) [BR93] and Quantum Random Oracle Model (QROM) [BDF+11]. The aim is to provide rigorous mathematical proofs that demonstrate the security of a system or algorithm under certain conditions. This approach is important in ensuring a strong foundation for security, as it goes beyond empirical evidence and relies on formal mathematical reasoning.

Key points related to provable security include:

1. **Adversarial Model:** Provable security often begins by defining an adversarial model. This model outlines the capabilities and limitations of potential attackers. The proof then demonstrates that, under these conditions, breaking the security of the system requires solving a specific mathematical problem that is assumed to be hard.
2. **Underlying Hard Problem:** The security proof typically relies on the assumption that certain mathematical problems are computationally difficult to solve. For example, the security of many new cryptographic protocols is the Learning with Error (LWE) problem.
3. **Limitations:** Provable security has its limitations. The proofs often make assumptions about the computational capabilities of the attacker and may not account for all possible real-world scenarios, such as side-channel attacks or implementation-specific vulnerabilities. In practice, a system may still be vulnerable to attacks that were not considered in the original proof.
4. **Cryptographic Protocols:** Provable security is commonly applied in the analysis of cryptographic protocols. For instance, protocols for secure communication, digital signatures, and encryption often undergo rigorous mathematical analysis to demonstrate their security properties. As suggested by the name of the project, I am going to study a specific cryptographic construction called Key Encapsulation Mechanism (KEM).
5. **Dynamic Nature:** The field of provable security evolves as new mathematical

techniques are developed and as computational power increases. What might have been considered a secure assumption in the past could become insecure with advancements in technology or new mathematical breakthroughs.

6. **Trade-offs:** While provable security provides a strong foundation for confidence in a system's security, it may come with trade-offs. Some algorithms or protocols that are provably secure might be less efficient than those relying on heuristics or empirical evidence.

In particular, I am interested in protocols based on the plain Learning With Errors (LWE) [Reg05] problem and two related, more algebraic variations: the Ring Learning With Errors (RLWE) [LPR13] and the Module Learning With Errors (MLWE) [LS15]. The entire scientific community is currently closely examining this family of hardness assumptions. This heightened interest stems from the absence of known quantum algorithms capable of solving these problems significantly faster than classical algorithms. For this reason, this problem is supposed to be quantum resistant.

At the beginning of the PhD, I spent most of my time reading and studying several papers about lattice-based cryptography, the Learning With Error problem and probability tools used to analysis both. After this first period I started to tackle the first project of my PhD, that is to provide a security reduction from the Learning With Error problem to a security game called Find Failing Plaintext that are Non Generic (FFP-NG) [HHM22]. The FFP family of security games was first introduced by Kathrin Hövelmanns, Andreas Hülsing and Christian Majenz in [HHM22]. They describe how to handle decryption failures in security reductions. In particular, the FFP-NG game describes a situation in which a public key is given to an adversary and asks it to find a message that triggers a decryption failure more likely with respect to the given key than with respect to an independent key.

The *main goal* is to get these reductions by using CRYSTALS-KYBER [BDK+18] as the underlying cryptographic protocol. KYBER emerged as a finalist in an extensive international standardization process overseen by the National Institute for Standards and Technology (NIST), which spanned several years. KYBER is an IND-CCA2-secure (gold standard security notion) KEM based on the MLWE problem. Before getting to work with this more involved scheme, we started studying the first LWE based schemes due to O. Regev [Reg05]. We have studied for several months the protocol using as error distribution the so-called, Rounded Gaussians. Due to the bad behavior of these probability distributions under linear combinations, achieving the desired reduction proved to be more challenging than we initially thought. We then decided to change the error distribution and use the so-called Discrete Gaussians. These probability distributions are commonly used with lattice-based constructions, and they behave like normal Gaussians under certain assumptions. By using this error distribution we've got the desired reduction and currently I am working on generalizing it. I am writing a paper about this reduction.

The *second main goal* of this PhD is to investigate the Fujisaki-Okamoto (FO) transformation, first introduced in [FO99], in the Quantum Random Oracle Model. This transformation allows to upgrade the security level of a scheme to get an IND-CCA one. The transformation has been widely studied in the ROM and there are several tight bounds over different versions of the FO transformation. In the QROM the same tools suffer for unexplainable losses. I am going to study the FO transformation in the QROM and the One-Way to Hiding Lemma, an important tool for security reductions. At the beginning of 2024 I will go to the Technical University of Eindhoven for my first secondment, visiting professors Kathrin Hövelmanns and Andreas Hülsing. Here, I am going to study the FO transformationboth in the ROM and QROM.

References:

[Reg05] O. Regev. On lattices, learning with errors, random linear codes, and cryptography. J.ACM, 56(6):1–40, 2009. Preliminary version in STOC 2005.

[LPR13] Vadim Lyubashevsky, Chris Peikert, and Oded Regev. On ideal lattices and learningwith errors over rings. pages 1–23, 2010. 1, 2

[LS15] Adeline Langlois and Damien Stehlé. Worst-case to average-case reductions for module lattices. Des. Codes Cryptography, 75(3):565–599, 2015. 2, 5

[BDK+18] Joppe W. Bos, Léo Ducas, Eike Kilts, Tancrède Lepoint, Vadim Lyubashevsky, John M. Schanck, Peter Schwabe, Gregor Seiler, Damien Stehlé. CRYSTALS - Kyber: A CCA-Secure Module-Lattice-Based KEM. EuroS&P 2018: 353-367

[HHM22] Kathrin Hövelmanns, Andreas Hülsing, Christian Majenz. Failing Gracefully: DecryptionFailures and the Fujisaki-Okamoto Transform. ASIACRYPT 2022.

[FO99] Eiichiro Fujisaki and Tatsuaki Okamoto. Secure integration of asymmetric and symmetric encryption schemes. In Michael J. Wiener, editor, Advances in Cryptology – CRYPTO'99, volume 1666 of Lecture Notes in Computer Science, pages 537–554, Santa Barbara, CA, USA, August 15–19, 1999. Springer, Heidelberg, Germany.

[BR93] Mihir Bellare and Phillip Rogaway. Random oracles are practical: A paradigm for designing efficient protocols. In Proc. of ACM Conference on Computers and Communication Security, pages 62–73, 1993.

[BDF+11] Dan Boneh, Özgür Dagdelen, Marc Fischlin, Anja Lehmann, Christian Schffaner, and Mark Zhandry. Random oracles in a quantum world. In Dong Hoon Lee and Xiaoyun Wang, editors, ASIACRYPT 2011, volume 7073 of LNCS, pages 41{69. Springer, Heidelberg, December 2011.