Project Proposal
within SPP 1736 – Algorithms for Big Data

Memory-Efficiency for Big Data Cryptography (MemoC)

Marc Fischlin, TU Darmstadt
Alexander May, Ruhr Universität Bochum

Summary

The security of cryptographic protocols is related via reductions to the security of presumably hard problems. Such a reduction transforms any successful adversary against a protocol into one against the underlying problem such that, vice versa, the hardness of the problem implies the hardness of the protocol. In the past, cryptographers used classical number-theoretic problems like the RSA problem or the discrete logarithm problem. But these problems will become insecure once quantum computers become real. It is therefore no surprise that the National Institute of Standards and Technology (NIST) announced a call for quantum-resistant cryptographic primitives in autumn 2016.

Most likely, the majority of reasonable candidates for the NIST competition will be based on hard problems from coding theory and lattices, such as Learning Parity with Noise (LPN) and Learning with Errors (LWE). NIST requests well-defined security levels of 128, 192 and 256 bits classically, and 64, 80, 128 bits quantumly. This means that for instantiating LPN with, say, 128 bit classical security, one has to make sure that any algorithm for LPN will need at least 2^{128} steps on a classical computer.

Since running times of 2^{128} escape current computational power, one nowadays typically studies medium security levels of $50 - 60$ bits in practical experiments, and then extrapolates via asymptotic formulas to the desired security level to make a reasonable security claim. However, besides running time, the memory requirement is a major factor. In fact, for the interesting problems LPN and LWE current algorithms also require to store an exponential number of samples. This huge amount of data and its storage requirement do not allow to run experiments even for medium security levels, and thus prevent a reliable prediction of cryptographically secure key sizes.

The current project studies low-memory algorithms for problems in coding and lattice theory, and how this translates to the case when these problems are deployed in one of the prevailing applications of modern cryptography, namely, key exchange protocols.

Zusammenfassung

Die Sicherheit kryptographischer Protokolle wird mittels Reduktionen auf die Sicherheit vermeintlich schwerer Probleme zurückgeführt. Solche Reduktionen transformieren einen erfolgreichen Angreifer auf ein Protokoll in einen Algorithmus für das zugrundeliegende Problem. Damit impliziert im Umkehrschluss die Schwere des Problems die Sicherheit des Protokolls. In der Vergangenheit nutzten Kryptographen klassische zahlentheoretische Probleme wie das RSA-Problem oder das Diskrete Logarithmus Problem. Diese Probleme sind allerdings leicht auf Quantenrechnern zu lösen. Aufgrund der fortschreitenden Entwicklung von Quantenrechnern hat das National Institute of Standards and Technology (NIST) folgerichtig im Herbst 2016 einen Aufruf zur Einreichung quantenresistenter kryptographischer Primitiven gestartet.

Sehr wahrscheinlich wird die Mehrzahl der praktikablen Kandidaten in diesem NIST-Wettbewerb auf der Schwere von Problemen der Kodierungs- und Gittertheorie basieren, wie z.B. Learning Parity with Noise (LPN) und Learning with Errors (LWE). NIST fordert wohldefinierte Sicherheitslevel von 128, 192 und 256 Bit auf klassischen Rechnern und 64, 80, 128 Bit auf Quantenrechnern. D.h. für eine Instantiierung von LPN mit z.B. 128 Bit klassischer Sicherheit muss sichergestellt werden, dass jeder LPN-Algorithmus mindestens 2^{128} Schritte auf einem klassischen Rechner benötigt.

Da 2^{128} Schritte weit jenseits derzeitiger Berechnungsmöglichkeiten liegen, studiert man heutzutage typischerweise mittlere Sicherheitslevel von $50 - 60$ Bit in praktischen Experimenten und extrapoliert mittels asymptotischer Formeln zum gewünschten Sicherheitslevel, um vernünftige Sicherheitsaussagen zu treffen. Allerdings spielt neben der Laufzeit der Speicherbedarf bei solchen Aussagen eine herausragende Rolle. Für die interessanten Probleme LPN und LWE benötigen die heutzutage besten Algorithmen die Speicherung exponentiell vieler Samples. Diese riesigen Datenmengen und der damit verbundene Speicherbedarf machen derzeit eine Durchführung von Experimenten selbst für mittlere Sicherheitslevel unmöglich und verhindern somit eine verlässliche Vorhersage von kryptographischen Schlüssellängen.

Das folgende Projekt beschäftigt sich mit Algorithmen mit geringem Speicherbedarf für Probleme der Kodierungs- und Gittertheorie und betrachtet den Einsatz dieser quanten-resistenten Probleme in einer der fundamentalsten Anwendungen moderner Kryptographie, dem Schlüsselaustausch-Protokoll.

1 State of the art and preliminary work

Following the guidelines for applications we report on the state of the art as well as the PI's preliminary work. Although, technical speaking, this is *not* a renewal proposal, the proposal here should continue our participation within the priority program SPP 1736 (Algorithms for Big Data). We therefore report about the achievements of our project SecOBig in the first phase of the program and the reason for discontinuing SecOBig in Section 1.3.

1.1 State of the art

Big data processing in cryptography often refers to the efficiency of mounting attacks. Typically, if an adversary gets access to a sufficient amount of data and can provide enough resources, then the sought-after information becomes available. Remarkably, in most cases cryptographers focus on the time requirements of attacks in order to assess the security of solutions. Yet, the memory consumption for both storing large amounts of data and for executing attacks is an important factor, too.[1]

The Impact of Memory Consumption. For analyzing and instantiating cryptographic systems one usually focuses on the aspect of adversarial running time. For instance, for cryptographic reductions one usually does not care about memory requirements, such as for the storage for oracle queries and answers. The same is true for the study of the underlying hard problems. The reason is that, often, the fastest algorithm with running time t also has a memory consumption of roughly t.

In cryptography, however, the space requirement for an attack can be a significant factor. While performing 2^{60} operations today is considered to be feasible, even on a medium-sized computing cluster in a reasonable amount of time, any algorithm with RAM consumption 2^{60} bits will not be implementable in the near future. An Internet investigation shows that nowadays the largest supercomputers[2] have a RAM of at most 1.6 PB $< 2^{54}$ bits. If an algorithm has to use external memory, then its running time usually slows down significantly.

Hence, for estimating the security of cryptographic constructions one should also consider an upper bound on the memory consumption. This in turn defines a need for finding efficient algorithms with small memory consumption.

The Impact on LPN and LWE. In this proposal we combine the question of memory consumption with a recent development in cryptography, due to the potential advances in quantum computing. Nowadays the question pops up which cryptography can still be considered to be suitable to protect data, since classical problems like RSA or discrete logarithms will become insecure once quantum computers reach maturity.

In November 2017, the National Institute of Standards and Technology (NIST) will open a call for candidates of cryptosystems for encryption, signature and key exchange, which are presumably immune to quantum attacks. The candidates will then undergo a period of 3-5 years of cryptanalytic research, before a recommendation is made. Most likely, a majority of these systems will be based on problems from coding and lattice theory, such as Learning Parity with Noise (LPN) and Learning with Errors (LWE). But the currently best algorithms for both problems have a memory consumption which is as large as their running time, making them useless for implemention even on medium

[1] A concrete example where this fact has been brought back to the center of attention is the (officially confirmed) initiative of the US National Security Agency (NSA) to build the so-called Utah Data Center for mass storage of data.

[2] e.g. the IBM 20-Petaflops cluster installed in Sequoia, Lawrence Livermore National Laboratory, California

size security levels. Let us have a closer look at LPN/LWE and their currently best algorithms.

LPN and the BKW algorithm. In LPN [Ale03], one has to find a secret $\mathbf{s} \in \mathbb{F}_2^n$ given access to an oracle that outputs samples of the form $(\mathbf{a}_i, b_i)$, where $\mathbf{a}_i \in_R \mathbb{F}_2^n$ and $b_i = \langle \mathbf{a}_i, \mathbf{s} \rangle + e_i$ for some Bernoulli error e_i. The algorithm of Blum, Kalai and Wasserman (BKW) [BKW00] achieves the best currently known running time $t = 2^{\mathcal{O}(\frac{n}{\log n})}$ for constant error, but suffers from requiring to store t samples in memory. Due to its large sample complexity, there is no chance to speed up BKW quantumly, since LPN-samples are inherently classical.

LWE and Lattice Sieving. LWE [Reg05] is a generalization of LPN to arbitrary fields $\mathbb{F}_q$. Namely, one has to find a secret $\mathbf{s} \in \mathbb{F}_q^n$ given access to an oracle that output samples of the form $(\mathbf{a}_i, b_i)$, where $\mathbf{a}_i \in_R \mathbb{F}_q^n$ and $b_i = \langle \mathbf{a}_i, \mathbf{s} \rangle + e_i$ for some discrete error e_i whose distribution is centered around 0 (e.g. a discrete Gaussian). Depending on the LWE-parameters, the best algorithm for LWE is either a generalization of BKW to $\mathbb{F}_q$ [ACF+15] or lattice sieving [ADRS15]. Both algorithms achieve for cryptographic parameter settings a running time of $2^{\mathcal{O}(n)}$, consuming the same exponential amount of memory. Moreover, for both algorithms no significant speed-up via quantum search methods is known.

Deployment of LPN and LWE in Key Exchange Protocols. Analogously to the problem of determining the necessary resources for mounting attacks, in order to make recommendations for secure choices for the underlying problems, we are interested in the security when these problems are deployed in more complex protocols. We are especially interested in securing communication data and the question how we can prevent attackers to decipher data which is stored now and potentially sifted through later, e.g., once quantum computers are available. The connection to the first part of the proposal is via the estimated hardness of potentially quantum-resistant problems such as LPN and LWE.

Securing communication data between two parties typically consists of composing a so-called key exchange protocol with a secure channel protocol. With the secure key exchange protocol the participants establish a shared cryptographic key, which should be known only to them. Then, this key is used in a secure channel protocol to send the actual data in a confidential and authentic way.

The focus for securing communication against advanced attacks, especially against quantum cryptanalysis, currently lies on the key exchange part. The reason is that it is currently unclear if quantum attacks improve over classical attacks for the channel part. In contrast, most of the practically deployed key exchange protocols (such as the ones used in TLS 1.2 [DR08] and the future TLS 1.3 [Res16]) rely on number-theoretic problems which are highly amenable to quantum attacks. The best known examples are the paramount Diffie-Hellman based protocols which can be broken in polynomial time by quantum attackers.

Concerning efforts to build quantum-resistant key exchange protocol, this area has gained quite some momentum, culminating in proposals to derive such protocols from (Ring-)LWE [Pei14, BCNS15, ADPS16, BCD+16]. For the scheme in [ADPS16], the "New Hope" key exchange protocol, Google recently announced to experiment with the scheme in its Chrome browser [Goo16]. Another recent proposal for a potentially quantum-resistant key exchange protocol is based on ideal lattices [ZZD+15].

Shortcomings of current LPN-/LWE-based Key Exchange Protocols. Unfortunately, most of the quantum-immune key exchange candidates have at least one shortcoming. For example, the analysis of New Hope [ADPS16] relies on the classical random oracle model, although it has been argued in [BDF+11] that quantum access to this idealized primitive should be preferred in such settings. Others, such as [BCNS15, BCD+16] provide security in the ACCE notion of Jager et al. [JKSS12], arguing security when the key exchange protocol is composed with an atomic channel. This at the moment excludes a modular analysis if instead a stream-based channel is used (as possible in TLS) [FGMP15]. Moreover, all the analyses follow the classical choice of investigating primarily the run time and success probability of adversaries, mainly neglecting the memory consumption in the reduction.

Furthermore, most of the aforementioned works start with the unauthenticated key exchange setting, where parties and transmissions are not authenticated. They argue that this can be accomplished later by adding signatures. Here, however, it is unclear if breaking the authentication with a quantum computer afterwards could not lead to a break of current executions (since the secrets may still be in use later). Furthermore, in some cases this requires some changes to the structure, such that for example [BCNS15, BCD+16] are, strictly speaking, not compatible to TLS.

Another shortcoming of the current proposals is that it they may not be easy to integrate into the upcoming TLS 1.3 protocol. While [BCNS15, ADPS16, BCD+16] argue how this can be done for TLS 1.2 and provide impressive implementation and performance details, the next TLS 1.3 version adds significantly enhanced functional properties such as zero round-trip time steps. In the Diffie-Hellman setting this often necessitates to switch to other number-theoretic problems, such as the PRF-ODH assumption [JKSS12]. It is unclear what this would mean for LWE- and LPN-based protocols, and if adopting a new assumption, for the memory consumption for this related problem.

1.2 Preliminary Work of the PIs

Memory-efficient LPN algorithm. We have extensive expertise on the design of algorithms for decoding random binary linear codes [8, BJMM12, 9]. LPN can be seen as a decoding problem in a random binary linear code generated by the LPN sample vectors $\mathbf{a}_i$, where the b_i represent the erroneous codeword.

We already have a preliminary paper that proposes new memory-efficient LPN algorithms [3], both classically and also for the first time quantumly. This work is based on our methods for decoding random binary linear codes, especially the May-Meurer-

Thomae algorithm [8]. The preliminary paper [3] is currently under submission, and is attached as supplementary material to this project proposal.

Asymptotic Complexity Analysis of LWE. We also studied already the asymptotic complexity of existing algorithms for solving LWE concerning the metrics time, memory and number of samples. Our work [6] summarizes the state of the art and identifies the best algorithms for specific choices of the LWE parameters n, q and the error distribution. However, all the algorithms in [6] suffer from their huge memory consumption, making them an inadequate choice for establishing secure LWE parameters in practice.

Key Exchange. We have extensively contributed to fundamental question about key exchange models [BFWW11, FG14], dealing with composability and multi-stage key exchange protocols. We have provided analyses of the (Diffie-Hellman based) TLS protocols [BFS+13, DFGS15], both for versions 1.2 and the (candidates for) 1.3. We have also investigated the special modes and properties of the candidates for TLS version 1.3 [DFGS15, FGSW16].

Cryptographic Reductions. Since our research area is complexity-based cryptography, reductions are our main tool in conducting security proofs of cryptographic protocols and appear in the majority of our works. Concerning reductions themselves we have extensive expertise about notions of reductions [Fis12, BBF13]. All the aforementioned works about key exchange involve reductions in the domain of key exchange.

1.3 Preliminary Work in the first Project SecOBig

In the first phase of the priority program both applicants have conducted a project called *Security-Preserving Operations on Big Data* (*SecOBig*). The focus of this proposal here has changed now. In the following we report briefly on the achievements of *SecOBig* (so far, with the project still running for about 8 months) and the reason for the shift of topic and a fresh application (instead of a renewal application).

Achievements in SecOBig. SecOBig promised to work on efficient operations on secured data, targeted as well as through the deployment of functional encryption and indistinguishable obfuscation, certification of cryptographic primitives, and the invention of new algorithmic techniques for big cryptographic data. At TU Darmstadt, Arno Mittelbach has been working on the project but has meanwhile left academia. At Ruhr-University Bochum, Ilya Ozerov worked on the project, who left academia in February 2016. He was replaced by Elena Kirshanova, who will submit her thesis in November 2016. The following works have been published in the context of the project so far:

Peer-reviewed Publications:

- Marc Fischlin, Amir Herzberg, Hod Bin Noon, Haya Shulman: Obfuscation Combiners. Crypto 2016. This work deals with the certification and obfuscation ques-

tions, as it shows how to build robust solutions in light of malicious obfuscators, and reports about implementation results.

- Elena Kirshanova, Alexander May, Friedrich Wiemer: Parallel Implementation of BDD enumeration for LWE, ACNS 2016 (*Best Student Paper*). Implements a memory-efficient variant of an enumeration technique for LWE.

- Victoria Fehr, Marc Fischlin: Sanitizable Signcryption: Sanitization over Encrypted Data. In submission, see also IACR cryptographic eprint archive 2015. Provides solutions to allow for controlled modifications of authenticated, encrypted data.

- Alexander May, Ilya Ozerov: On Computing Nearest Neighbors with Applications to Decoding of Binary Linear Codes, Eurocrypt 2015. Proposes a new algorithm for finding correlations within two huge lists in time sub-quadratic in the list length.

- Rolf Egert, Marc Fischlin, David Gens, Sven Jacob, Matthias Senker, Jörn Tillmanns: Privately Computing Set-Union and Set-Intersection Cardinality via Bloom Filters. ACISP 2015. This work deals with efficient operations on encrypted data for computing the number of shared elements in large sets. Topic has been inspired by the invited talk of Michael Goodrich about Bloom filters (opening of SPP 1736).

- Gottfried Herold, Elena Kirshanova, and Alexander May. On the Asymptotic Complexity of Solving LWE. IACR Cryptology ePrint Archive 2015, accepted at Journal of Design, Codes and Cryptography. Relates to time, memory and sample complexity of LWE solving algorithms.

- Christina Brzuska, Pooya Farshim, Arno Mittelbach: Random-Oracle Uninstantiability from Indistinguishability Obfuscation. TCC 2015. Relates to the question of obfuscation, and shows that the random oracle methodology for designing practical solutions may not be applicable in general.

- Elena Kirshanova. Proxy Re-encryption from Lattices. PKC 2014. Relates to outsourcing computation in a distributed environment without trusted authorities.

- Christina Brzuska, Arno Mittelbach: Indistinguishability Obfuscation versus Multibit Point Obfuscation with Auxiliary Input. Asiacrypt 2014. Relates to the question of obfuscation and technical details about the realizability.

- Alexander May, Ilya Ozerov. A Generic Algorithm for Small Weight Discrete Logarithms in Composite Groups. Selected Areas in Cryptography 2014. Relates to hardness assumption in general cryptographic groups of large size.

- Christina Brzuska, Pooya Farshim, Arno Mittelbach: Indistinguishability Obfuscation and UCEs: The Case of Computationally Unpredictable Sources, Crypto 2014. Relates to the question of obfuscation and shows that obfuscation can actually be used to show negative result.

Theses:

- Elena Kirshanova. Analysis of Hard Problems on Lattices. Ph.D. Thesis, Ruhr-University Bochum, November 2016.

- Sven Jacob. Realizing Cryptographic Protocols in the MapReduce-Framework. Ongoing Master Thesis, TU Darmstadt, 2016. Provides cryptographically secure protocols in the MapReduce framework, including implementations in Hadoop and Amazon's Elastic MapReduce (EMR) framework.

- Ilya Ozerov. Combinatorial Algorithms for Subset Sum Problems. Ph.D. Thesis, Ruhr-University Bochum, February 2016.

- Arno Mittelbach. Random Oracles in the Standard Model — A Systematic Study of Random Oracle (Un)Instantiability via Universal Computational Extractors and Obfuscation. Ph.D. Thesis, TU Darmstadt, December 2015.

- Kai Schwierczek. Approximation of the Maximum in Big Data, Master-Thesis TU Darmstadt, 2015. Touches the question how to compute the easy statistics (like the maximum or minimum) on encrypted outsourced data efficiently, by sacrificing precision.

- Leif Both. Cryptography with Streaming Algorithms. Master-Thesis Ruhr-University Bochum 2015. Asks which cryptographic primitives can be realized in a streaming model of computation providing only logarithmic space.

- Tobias Weber. Combiners for Robust Pseudorandom Number Generators, Master-Thesis TU Darmstadt, 2015. Deals with certification in the sense that one builds robust pseudorandom generators in the presence of some malicious generators.

Others:

- Dagstuhl seminar about Public-Key Cryptography, organized by Fischlin, May, Rabin, and Pointcheval, September 2016. Big Data has been one of the topics in the seminar.

Shift of Topic. The main focus of the project *SecOBig* was to perform operations on large amounts of cryptographically secured data. In the second phase, with project *MemoC* we turn the focus to the research question what Big Data scenarios actually mean for cryptographic strengths. The reason for this transition is twofold. First, it should allow a smoother collaboration within the priority program. Here, we especially refer to the projects *Scalable Cryptography* of Hofheinz and Kiltz and *Big-Data-DynAmO: Dynamic, Approximate, and Online Methods for Big Data* of Meyer. The former one touches related questions concerning tightness in cryptographic security proofs, and the latter one deals (among others) with limited memory resources. To best of our knowledge, both projects will be continued in the second phase of the priority program.

The other reason is based on recent developments in the cryptographic community. One is that, in the past years, there has been a growing trend to perform general secure operations via so-called garbled circuits. This approach shows impressive performances, but neither one of the applicants here is an expert on this. Also, with NIST's recent call for post-quantum secure primitives and the growing interest by companies like Google, looking into this area in the context of Big data processing seems to be a more fashionable and research-wise a more promising topic.

1.4 Project-related publications

[1] Paul Baecher, Christina Brzuska, and Marc Fischlin. *Notions of black-box reductions, revisited*. In Advances in Cryptology - ASIACRYPT 2013 - 19th International Conference on the Theory and Application of Cryptology and Information Security, Bengaluru, India, December 1-5, 2013, Proceedings, Part I, volume 8269 of Lecture Notes in Computer Science, pages 296-315. Springer, 2013.

[2] Benjamin Dowling, Marc Fischlin, Felix Günther, and Douglas Stebila. *A cryptographic analysis of the TLS 1.3 handshake protocol candidates*. In Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, Denver, CO, USA, October 12-6, 2015, pages 1197-1210. ACM, 2015.

[3] Andre Esser, Robert Kübler, Alexander May. *LPN Decoded*, 2016, **in submission**, attached to this proposal as complementary material.

[4] Marc Fischlin. *Black-box reductions and separations in cryptography*. In Progress in Cryptology - AFRICACRYPT 2012 - 5th International Conference on Cryptology in Africa, Ifrance, Morocco, July 10-12, 2012. Proceedings, volume 7374 of Lecture Notes in Computer Science, pages 413-422. Springer, 2012.

[5] Marc Fischlin, Felix Günther, Benedikt Schmidt, and Bogdan Warinschi. *Key confirmation in key exchange: A formal treatment and implications for TLS 1.3*. In IEEE Symposium on Security and Privacy, SP 2016, San Jose, CA, USA, May 22-26, 2016, pages 452-469. IEEE Computer Society, 2016.

[6] Gottfried Herold, Elena Kirshanova, Alexander May. *On the Asymptotic Complexity of Solving LWE*, IACR Cryptology ePrint Archive, http://eprint.iacr.org/2015/1222, accepted for publication in Journal Design, Codes and Cryptography, 2015.

[7] Elena Kirshanova, Alexander May, Friedrich Wiemer. *Parallel Implementation of BDD enumeration for LWE* , In International Conference on Applied Cryptography and Network Security (ACNS 2016), Lecture Notes in Computer Science, Springer-Verlag, 2016.

[8] Alexander May, Alexander Meurer, Enrico Thomae. *Decoding Random Linear Codes in* $O(2^{0.054n})$, In Advances in Cryptology (Asiacrypt 2011), Lecture Notes in Computer Science, Springer-Verlag, 2011.

[9] Alexander May, Ilya Ozerov. *On Computing Nearest Neighbors with Applications to Decoding of Binary Linear Codes* , In Advances in Cryptology (Eurocrypt 2015), Lecture Notes in Computer Science, Springer-Verlag, 2015.

2 Objectives and work programme

2.1 Anticipated total duration of the project

The total duration time of the project is 36 months (3 years). The project duration spans from the actual project begin (presumably June 2017) to 36 months later. Funding of the DFG is requested for the entire duration of 36 months.

2.2 Objectives

The overall goal of the project is to advance the field of memory-efficient evaluations for the cryptographic problems LWE and LPN, in order to provide sound security estimates even if required data exceeds reasonable memory bounds. These problems are primary candidates in NIST's search for future, quantum-secure primitives. The research should be carried out for the problems itself, but also for the deployment of the problems in the important setting of key exchange. To this end the following sub goals are:

Memory Efficient Combinatorial/Lattice-Based LWE Algorithms. We will develop combinatorial and lattice-based algorithms for LWE, both classically and quantumly, with limited memory consumption. Our goal is to precisely predict cryptographic security levels as a function of the LWE parameters n, q and the size of the error. Therefore, we will implement our algorithms, run them on medium size instances and extrapolate asymptotically to cryptographically relevant security levels.

Practical Cryptanalysis of NIST's Post-Quantum Candidates. Having combinatorial and lattice-based algorithms for tackling LWE-based cryptographic constructions, we will study the security of recent (and upcoming) proposals for the NIST initiative, such as e.g. New Hope [ADPS16] and Frodo [BCD+16].

Analyses of existing LWE/LPN-based Protocols: The idea is to revisit the existing protocols in light of the findings about the memory requirements for LWE and LPN. The goal is to make statements about the security bounds based on these results. This requires to check the memory consumption of the reduction and to verify if solvers for the underlying problems can be directly used in the context of key exchange, e.g., if one can "stream" executions of the key exchange protocol to the solver.

Combining TLS 1.3 with LWE/LPN: The objective here is to make LWE- and LPN-based key exchange protocols resemble the TLS 1.3 structure more closely. We expect that this will require to introduce a "PRF-ODH like" assumption for these problems. The goals here are thus to (a) devise protocols, (b) give a reduction to a suitable LWE- or LPN-based problem, taking the memory requirements into account, and (c) to evaluate the security of the problem in light of the analyses of the original problems in the other part of the project.

2.3 Work programme incl. proposed research methods

The work programme is split into 4 parts. Project parts A+B describe the work programme associated to Alexander May, project parts C+D describe the work programme of Marc Fischlin. The duration of the individual work packages and their dependencies are described in Figure 1.

Work package A.1: Memory Efficient Combinatorial LWE Algorithms. Our starting point is our preliminary work on LPN [3] that we generalize to arbitrary fields $\mathbb{F}_q$. We expect to obtain a hybrid algorithm that for limited memory is close to decoding algorithms for LWE-type problems, and for large memory resembles BKW. Especially, analogous to the LPN case [3], we will divide our algorithm in two steps for dimension-reduction and decoding. The first step makes use of some limited, available amount of memory to reduce the LWE dimension in a BKW-type manner as far as possible, whereas the second decode step solves a resulting LWE-samples in smaller dimension.

This will lead to an algorithm that can be optimally adapted to any given amount of memory. We will implement our algorithm in C, run experiments for medium-size LWE parameters and derive asymptotics that allow for extrapolation to large cryptographic instances.

Work package A.2: Memory Efficient Lattice Reduction. Our starting point is the preliminary work [7], where we implemented a two-step algorithm for LWE. In this algorithm, the first step reduces the lattice basis defined by the LWE-sample matrix. So as opposed to the algorithm in WP A.1, here we do not reduce the dimension but the size of the coefficients. The second step is then a parallel enumeration over all candidates for the LWE secret, which in lattice language is a solution to a closest vector promise problem.

Our work [7] suffers from the fact that we implemented some non-optimal, but memory-efficient, lattice reduction procedure. Recent lattice sieving techniques [ADRS15] are asymptotically much faster, but also require large memory consumption. We will explore possible tradeoffs in lowering the memory consumption of these algorithms by using techniques from streaming algorithms, similar to [3]. This will sacrifice a bit in running time, at the benefit of obtaining implementable and practical algorithms even for large lattice dimensions.

Work package B.1: Memory Efficient Quantum Algorithms for LWE. With the invention of cryptographic systems for the era of quantum computing, it is mandatory to study the best quantum algorithms for LPN and LWE. Many classical algorithms can be significantly speeded up using Quantum Search Techniques, such as e.g. Grover search [Gro96].

We will look at possible extensions and improvements of our algorithms in WP A by enhancing them with quantum techniques. This will settle cryptographic quantum key sizes for LWE, similar to the estimates that have been done in [3] for LPN.

In a quantum world, it seems to be even more comprehensible to focus on small memory consumption, since quantum computing devices currently suffer from scalability. Thus, we will focus on algorithms with a quantum memory that is limited linearly (or even sublinear) in the input size.

Work package B.2: Practical Cryptanalysis of NIST Proposals. In WP A we develop algorithm for tackling LPN and LWE instances in practice. This will enable us to judge the security levels of current NIST post-quantum cryptographic proposals. Interesting candidates that we will analyze with our algorithms are e.g. New Hope [ADPS16] and Frodo [BCD+16].

As the deadline for submitting candidates to NIST is in Nov 2017, we expect to see many more interesting candidates based on the LPN and LWE within the next year. These candidates will by analyzed for security using our algorithms from WP A.

Work package C.1: Memory-efficiency of Existing Reductions. The first task is to explore the memory efficiency of the concrete reductions in [Pei14, BCNS15, ADPS16, BCD+16]. Such a reduction $\mathcal{R}$ from the key exchange protocol takes an adversary $\mathcal{A}_{\mathrm{KE}}$ against the protocol, and turns this into an algorithm $\mathcal{A}_{\mathrm{LWE}} = \mathcal{R}^{\mathcal{A}_{\mathrm{KE}}}$ against the underlying algorithmic problem; in the example here for LWE. Since one usually considers key exchange protocols in the multi-instance setting of Bellare and Rogaway [BR93], the reduction usually needs to simulate the multiple instances of the key exchange protocol, at the expense of a significant storage requirement, e.g., if 2^{20} instances are running concurrently. This has major impact on the assumed hardness of the underlying problem.

We are therefore interested in the exact effect of the reduction's requirements on the suggested parameter choice. This requires us to determine the exact bounds (in particular, in terms of space) and link them to the findings of Work package WP A. We also investigate if we can devise better reductions or bounds, e.g., in the sequential execution model.

Work package C.2: Analysis of Underlying LWE-Problems. In this work package we investigate the hardness of the underlying problem(s) proposed in Work packages D.1 and D.2. This investigation covers several aspects. First, we verify with the results of Work packages WP A how hard the problem itself seems to be. Secondly, we try to relate the new problem (via memory-efficient reductions) to the standard LWE problem, or try to show that the problem is strictly stronger, by giving a black-box separation result.

Work package D.1: Adaptation to TLS 1.2. In this work packages we adopt ideas from the TLS 1.2 concept [DR08] to the suggested LWE-based key exchange protocol designs. The main step is to investigate if one can remove the late signatures in [BCNS15] which make the solution slightly TLS-non-conforming. As discussed in [BCNS15] such a change would most likely imply to switch to a PRF-ODH like assumption, allowing the adversary to mount an active attack against the underlying LWE problem. As pointed out by Peikert [Pei14], the problem seems to be easy under such active attacks, though.

Fortunately, not all is lost: For TLS 1.2 the analysis of Jager et al. [JKSS12] requires only a very limited form of active attacks in which the adversary can make a single chosen queries only. For such active attacks the LWE problem may still be hard. As an alternative, or second step, we consider other design possibilities for the key exchange protocol, thwarting this problem by design.

If possible, solutions should be implemented and compared to existing ones.

Work package D.2: Adaptation to TLS 1.3. This work packages looks into the possibility to adapt the ideas of previous LWE-based proposals to (the current draft of) TLS 1.3 [Res16]. Since TLS 1.3 will be fundamentally different from TLS 1.2 this at foremost requires us to check if the current solutions can be transferred at all.

Next, we address the question if we can augment existing protocols by a 0RTT mode where one derives a fresh key without interaction by consulting previous communication data. As explained above, this presumably requires an even stronger PRF-ODH like assumption, where the adversary can make many active queries. Here the question which should be addressed is if one needs to make some restriction on the number of key exchange sessions in which material is re-used.

If possible, solutions should be implemented and compared to existing ones.

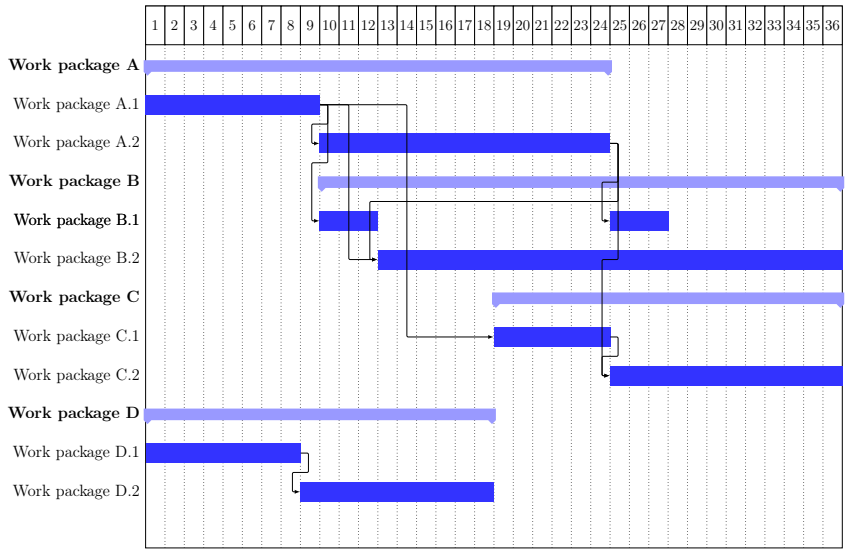

Figure 1: Work package durations and dependencies.

2.4 Data handling

The results of the theoretical work is planned to be published at conferences, workshops, and in journals. This ensures dissemination and availability of the project's results. In addition, we will use the usual electronic archives like IACR's `eprint` service, and the PI's home pages to make full versions available in a lasting way. As for experimental data, like software, we will also make these public, as part of the corresponding publication, and through electronic archives like GitHub.

2.5 Other information

Not applicable.

2.6 Descriptions of proposed investigations involving experiments on humans, human materials or animals

Not applicable.

2.7 Information on scientific and financial involvement of international cooperation partners

Not applicable.

3 Bibliography

[ACF+15] Martin R. Albrecht, Carlos Cid, Jean-Charles Faugère, Robert Fitzpatrick, and Ludovic Perret. On the complexity of the BKW algorithm on LWE. *Des. Codes Cryptography*, 74(2):325–354, 2015.

[ADPS16] Erdem Alkim, Léo Ducas, Thomas Pöppelmann, and Peter Schwabe. Post-quantum key exchange - A new hope. In *25th USENIX Security Symposium, USENIX Security 16*, pages 327–343. USENIX Association, 2016.

[ADRS15] Divesh Aggarwal, Daniel Dadush, Oded Regev, and Noah Stephens-Davidowitz. Solving the shortest vector problem in 2^n time using discrete gaussian sampling: Extended abstract. In Rocco A. Servedio and Ronitt Rubinfeld, editors, *Proceedings of the Forty-Seventh Annual ACM on Symposium on Theory of Computing, STOC 2015*, pages 733–742. ACM, 2015.

[Ale03] Michael Alekhnovich. More on average case vs approximation complexity. In *44th Symposium on Foundations of Computer Science (FOCS 2003)*, pages 298–307. IEEE Computer Society, 2003.

[BBF13] Paul Baecher, Christina Brzuska, and Marc Fischlin. Notions of black-box reductions, revisited. In *Advances in Cryptology - ASIACRYPT 2013*, volume 8269 of *Lecture Notes in Computer Science*, pages 296–315. Springer, 2013.

[BCD+16] Joppe W. Bos, Craig Costello, Léo Ducas, Ilya Mironov, Michael Naehrig, Valeria Nikolaenko, Ananth Raghunathan, and Douglas Stebila. Frodo: Take off the ring! practical, quantum-secure key exchange from LWE. In *CCS*. ACM, 2016.

[BCNS15] Joppe W. Bos, Craig Costello, Michael Naehrig, and Douglas Stebila. Post-quantum key exchange for the TLS protocol from the ring learning with errors problem. In *2015 IEEE Symposium on Security and Privacy*, pages 553–570. IEEE Computer Society, 2015.

[BDF+11] Dan Boneh, Özgür Dagdelen, Marc Fischlin, Anja Lehmann, Christian Schaffner, and Mark Zhandry. Random oracles in a quantum world. In *Advances in Cryptology - ASIACRYPT 2011*, volume 7073 of *Lecture Notes in Computer Science*, pages 41–69. Springer, 2011.

[BFS+13] Christina Brzuska, Marc Fischlin, Nigel P. Smart, Bogdan Warinschi, and Stephen C. Williams. Less is more: relaxed yet composable security notions for key exchange. *Int. J. Inf. Sec.*, 12(4):267–297, 2013.

[BFWW11] Christina Brzuska, Marc Fischlin, Bogdan Warinschi, and Stephen C. Williams. Composability of bellare-rogaway key exchange protocols. In *Proceedings of the 18th ACM Conference on Computer and Communications Security, CCS 2011*, pages 51–62. ACM, 2011.

[BJMM12] Anja Becker, Antoine Joux, Alexander May, and Alexander Meurer. Decoding random binary linear codes in 2 n/20: How 1 + 1 = 0 improves information set decoding. In David Pointcheval and Thomas Johansson, editors, *Advances in Cryptology - EUROCRYPT 2012*, volume 7237 of *Lecture Notes in Computer Science*, pages 520–536. Springer, 2012.

[BKW00] Avrim Blum, Adam Kalai, and Hal Wasserman. Noise-tolerant learning, the parity problem, and the statistical query model. In F. Frances Yao and Eugene M. Luks, editors, *Proceedings of the Thirty-Second Annual ACM Symposium on Theory of Computing*, pages 435–440. ACM, 2000.

[BR93] Mihir Bellare and Phillip Rogaway. Entity authentication and key distribution. In *Advances in Cryptology - CRYPTO '93*, volume 773 of *Lecture Notes in Computer Science*, pages 232–249. Springer, 1993.

[DFGS15] Benjamin Dowling, Marc Fischlin, Felix Günther, and Douglas Stebila. A cryptographic analysis of the TLS 1.3 handshake protocol candidates. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, pages 1197–1210. ACM, 2015.

[DR08] T. Dierks and Eric Rescorla. The transport layer security (tls) protocol, version 1.2. RFC 5246, 2008. `https://tools.ietf.org/html/rfc5246`.

[FG14] Marc Fischlin and Felix Günther. Multi-stage key exchange and the case of google's QUIC protocol. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, pages 1193–1204. ACM, 2014.

[FGMP15] Marc Fischlin, Felix Günther, Giorgia Azzurra Marson, and Kenneth G. Paterson. Data is a stream: Security of stream-based channels. In *Advances*

in Cryptology - CRYPTO 2015, volume 9216 of *Lecture Notes in Computer Science*, pages 545–564. Springer, 2015.

[FGSW16] Marc Fischlin, Felix Günther, Benedikt Schmidt, and Bogdan Warinschi. Key confirmation in key exchange: A formal treatment and implications for TLS 1.3. In *IEEE Symposium on Security and Privacy*, pages 452–469. IEEE Computer Society, 2016.

[Fis12] Marc Fischlin. Black-box reductions and separations in cryptography. In *Progress in Cryptology - AFRICACRYPT 2012*, volume 7374 of *Lecture Notes in Computer Science*, pages 413–422. Springer, 2012.

[Goo16] Google Security Blog. Experimenting with post-quantum cryptography, July 2016.

[Gro96] Lov K. Grover. A fast quantum mechanical algorithm for database search. In Gary L. Miller, editor, *Proceedings of the Twenty-Eighth Annual ACM Symposium on the Theory of Computing*, pages 212–219. ACM, 1996.

[JKSS12] Tibor Jager, Florian Kohlar, Sven Schäge, and Jörg Schwenk. On the security of TLS-DHE in the standard model. In *Advances in Cryptology - CRYPTO 2012*, volume 7417, pages 273–293. Springer, 2012.

[Pei14] Chris Peikert. Lattice cryptography for the internet. In *Post-Quantum Cryptography - 6th International Workshop, PQCrypto 2014*, volume 8772 of *Lecture Notes in Computer Science*, pages 197–219. Springer, 2014.

[Reg05] Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. In Harold N. Gabow and Ronald Fagin, editors, *Proceedings of the 37th Annual ACM Symposium on Theory of Computing*, pages 84–93. ACM, 2005.

[Res16] Eric Rescorla. The transport layer security (tls) protocol version 1.3, draft-ietf-tls-tls13-16. RFC 5246, September 2016. `https://tools.ietf.org/html/draft-ietf-tls-tls13-16`.

[ZZD+15] Jiang Zhang, Zhenfeng Zhang, Jintai Ding, Michael Snook, and Özgür Dagdelen. Authenticated key exchange from ideal lattices. In *Advances in Cryptology - EUROCRYPT 2015*, volume 9057 of *Lecture Notes in Computer Science*, pages 719–751. Springer, 2015.

4 Requested modules/funds

4.1 Basic Module

4.1.1 Funding for Staff

We apply for the following funding for staff, following the DFG's personal rates for 2016 (DFG-Vordruck 60.12). Due to competitive nature of positions in Computer Science and in the area of IT security, we request funding for full doctoral student positions (100%). We apply for funding of two doctoral students for the entire duration of the project. One student will be associated to TU Darmstadt (TUD) and work on packages C and D, the other student will be associated to Ruhr-University Bochum (RUB) and work on packages A and B. Student assistents (one for each project partner) have been calculated with 10h/months for the full duration of the project, with average costs of 11 EUR/h. They should support the implementations in the corresponding work packages.

No	Type	assoc. to	Description	Y1	Y2	Y3
1	Doctoral Student, 100%	TUD	WP C and D	61,800€	61,800€	61,800€
2	Doctoral Student, 100%	RUB	WP A and B	61,800€	61,800€	61,800€
3	Student Assistent, 100%	TUD	Implementations	1,320€	1,320€	1,320€
4	Student Assistent, 100%	RUB	Implementations	1,320€	1,320€	1,320€
	Total Amount			126,240€	126,240€	126,240€

4.1.2 Direct Project Costs

Travel Expenses. We apply for 8,000 Euro travel funding per year, i.e. for a total travel funding of 24,000 Euro. This funding will cover expenses of the project partners for traveling between Darmstadt and Bochum (500 EUR per year per partner), as well as attendances of potential meetings of the SPP (500 EUR per year per partner). In addition, we calculate with 3000 EUR per year and partner for presenting the project results at internationally renowned conferences and workshops (where we assume 1,500 EUR for an intercontinental conference, 1,000 EUR for a European conference, and 500 EUR for a workshop attendance).

5 Project requirements

5.1 Employment status information

Marc Fischlin, Dr.rer. nat
W3-Professor
Year of birth: 1973, Nationality: German

Cryptography and Complexity Theory
Department of Computer Science

Technische Universität Darmstadt
Karolinenplatz 5, 64289 Darmstadt, Germany
Phone office: +49-(0)6151/16-25730
Fax office: +49-(0)6151-16-22487
E-Mail: marc.fischlin@cryptoplexity.de

Privat address: Charlotte-Posenenske-Str.58, 65197 Wiesbaden
Phone private: +49-(0)611/9882730

Alexander May, Dr. rer. nat
W3-Professor
Year of birth: 1974, Nationality German

Faculty of Mathematics, NA 5/73
Ruhr-University Bochum
Universitätsstr. 150, 44801 Bochum

Phone office: 0234/32-23261
Fax office: 0234/32-14430
E-Mail: alex.may@rub.de

Privat address: Im Haarmannsbusch 34, 44797 Bochum
Phone private: 0151-64967032

5.2 First-time proposal data

Not applicable.

5.3 Composition of the project group

TU Darmstadt:

- Prof. Dr. Marc Fischlin, Chair for Cryptography and Complexity Theory. Funded through TU Darmstadt.
- M.Sc.(Math) Jacqueline Brendel. Funded through DFG Doctoral College 2050 Privacy and Trust for Mobile Users.
- M.Sc.(Math) Victoria Fehr. Funded through TU Darmstadt; expected to leave till project start.
- M.Sc.(Math) Tommaso Gagliardoni. Funded through BMBF/Hesse Security Competence Center CRISP; expected to leave till project start.
- M.Sc.(CS), M.Sc.(CS) Felix Günther. Funded through DFG Collaborative Research Center 1119 CROSSING.

- M.Sc.(Math) Christian Janson. Funded through TU Darmstadt.
- M.Sc.(Math) Giorgia Azzurra Marson. Funded through DFG Collaborative Research Center 1119 CROSSING; expected to leave till project start.
- M.Sc.(CS) Sogol Mazaheri. Funded through TU Darmstadt.

Support: 1 secretary.

Ruhr-University Bochum:

- Prof. Dr. Alexander May, Chair for Cryptology & IT security. Founded through RU Bochum.
- Dipl.-Math. Elena Kirshanova. Funded through RU Bochum; expected to leave till project start.
- Dipl.-Math. Robert Kübler. Funded through DFG-SPP 1736 – Big Data.
- MSc (Math) Leif Both. Funded through third party.
- Dipl.-Ing. Matthias Minihold. Funded through ECRYPT-CSA within EU H2020.
- Dip.-Ing. Andre Esser. Founded through DFG-GRK 1817 – Ubiquitous Cryptography

Support: 1 secretary and 1 technical assistant.

5.4 Cooperation with other researchers

Researchers with whom you have agreed to cooperate on this project

We plan to cooperate with Prof. Dennis Hofheinz (KIT, Germany) and Prof. Eike Kiltz (RUB, Germany) on the question of memory-efficient reductions. Prof. Hofheinz and Prof. Kiltz have participated in the first phase of the Priority Program 1736 (Algorithms for Big Data) jointly on a project about tight security reductions and plan to continue their collaboration in the next phase.

We also plan to cooperate with Prof. Ulrich Meyer (Johann Wolfgang Goethe-Universität Frankfurt, Germany) on the question whether external memory techniques can be successfully applied for the LPN/LWE scenario. Prof. Meyer had a project on online methods in the first phase and plans to continue this project in the next phase.

Researchers with whom you have collaborated scientifically within the past three years

Marc Fischlin:

- Prof. Michael Backes (U Saarland, Germany)
- Dr. David Bernhard, Prof. Bogdan Warinschi (U Bristol, UK)
- Dr. Jean Paul Degabriele, Prof. Kenny Paterson (RHUL, UK)
- Prof. Amir Herzberg (Tel-Aviv University)
- Dr. Anja Lehmann (IBM Zurich, Switzerland)
- Prof. Krzysztof Pietrzak (IST, Austria)
- Dr. Benedikt Schmidt (IMDEA, Madrid, Spain)
- Prof. Dominique Schröder (U Nürnberg-Erlangen, Germany)

Alexander May:

- Prof. Johannes Blömer (Paderborn University)
- Prof. Christian Sohler (TU Dortmund)
- Prof. Alon Rosen (Herzliya, Israel)

5.5 Scientific equipment

Not requested.

5.6 Project-relevant interests in commercial enterprises

Not applicable.

6 Additional information

We have not requested funding for this project from any other sources. In the event that we submit such a request, we will inform the Deutsche Forschungsgemeinschaft immediately.

The DFG liaison officer's of TU Darmstadt and Ruhr-University Bochum will be informed of this research funding request.