Report from Dagstuhl Seminar 22141

Symmetric Cryptography

Nils Gregor Leander[*1], Bart Mennink[*2], María Naya-Plasencia[*3], Yu Sasaki[*4], and Eran Lambooij[†5]

1 **Ruhr-Universität Bochum, DE.** gregor.leander@rub.de
2 **Radboud University Nijmegen, NL.** b.mennink@cs.ru.nl
3 **INRIA – Paris, FR.** maria.naya_plasencia@inria.fr
4 **NTT – Tokyo, JP.** yu.sasaki.sk@hco.ntt.co.jp
5 **University of Haifa, IL.** eranlambooij@gmail.com

Abstract

This report documents the program and the outcomes of Dagstuhl Seminar 20041 "Symmetric Cryptography". The seminar was held on April 3-8, 2022 in Schloss Dagstuhl – Leibniz Center for Informatics. This was the eigth seminar in the series "Symmetric Cryptography". Previous editions were held in 2007, 2009, 2012, 2014, 2016, 2018, and 2022. Participants of the seminar presented their ongoing work and new results on topics of (quantum) cryptanalysis and provable security of symmetric cryptographic primitives. In this report, a brief summary of the seminar is given followed by the abstracts of given talks.

Seminar April 3–8, 2022 – http://www.dagstuhl.de/22141
2012 ACM Subject Classification Security and privacy → Cryptanalysis and other attacks; Security and privacy → Symmetric cryptography and hash functions
Keywords and phrases block ciphers, cryptography, hash functions, stream cipers, symmetric cryptography
Digital Object Identifier 10.4230/DagRep.12.4.1

1 Executive Summary

Nils Gregor Leander (Ruhr-Universität Bochum, DE)
Bart Mennink (Radboud University Nijmegen, NL)
Maria Naya-Plasencia (INRIA – Paris, FR)
and Yu Sasaki (NTT – Tokyo, JP)

IT Security plays an increasingly crucial role in everyday life and business. Virtually all modern security solutions are based on cryptographic primitives. Symmetric cryptography deals with the case where both the sender and the receiver of a message use the same key. Due to their good performance, symmetric cryptosystems are highly relevant not only for academia, but also for industrial activities.

We identified the following areas as some of the most important topics on symmetric cryptography at the moment.

Lessons Learnt from NIST Lightweight Cryptography Project. The US National Institute of Standards and Technology (NIST) acknowledged in 2013 the real-world importance of lightweight cryptography, and announced an initiative for standardization. It is expected that the new lightweight standard will not only be used in the US, but rather worldwide.

[*] Editor / Organizer
[†] Editorial Assistant / Collector

New Design Strategies. This area deals with the development of symmetric cryptographic primitives and modes that must operate for specific applications, such as STARKs, SNARKs, fully homomorphic encryption, and multi-party computation. These novel applications lead to a paradigm shift in design criteria that we are just starting to understand, both in terms of possible optimizations as well as security impacts.

Quantum-Safe Symmetric Cryptography. For symmetric cryptography, it is short-sighted to expect that cryptanalysis will not improve with the help of quantum computers in the future. It is of importance to understand both the possibility to quantize existing classical attacks, as well as the possibility to perform new types of cryptanalytic attacks using a quantum computer.

Understanding Security Implications from Ideal and Keyless Primitives. Permutation-based cryptography has gained astounding popularity in the last decade, and security proofs are performed in an ideal permutation model. Partly as a consequence of this, the concrete security analysis of the involved primitives has become more difficult. One challenge is to understand (i) to what extent distinguishers impact the security of cryptographic schemes and (ii) what non-random properties of permutations seem likely to be translated into an attack on the full scheme.

Seminar Program

The seminar program consisted of a few short presentations and in-depth group meetings. Presentations were about the above topics and other relevant areas of symmetric cryptography, including state-of-the-art cryptanalytic techniques and new designs. Below one can find the list of abstracts for talks given during the seminar.

The research groups were on various topics in symmetric cryptography, all related to one of the above points in one way or another. On the last day of the seminar, the leaders of each group gave brief summaries of achievements. Some teams continued working on the topic after the seminar and started new research collaborations. Here are the summaries of the five groups:

- Group 1 worked and discussed on various problems of provable security, roughly corresponding to one project per person. For three of the projects, the groups had preliminary discussions, and the next step will be to perform the remaining research and investigate the details offline. For two problems, namely improved unforgeability of certain MAC constructions and generic analysis of PRF's and MAC's on 2 public permutations, they advanced quite well and the details will be written down soon after the seminar.
- Group 2 worked on several topics that they plan to continue after the seminar. One was to find good algorithms for detecting the optimal trees of some Boolean functions in the context of improved key-recovery attacks, and figuring out if we actually need trees, or if we could find or use better partitions that do not correspond to a tree and yet improve the complexity. They also worked on building two attacks on the HALFLOOP construction. They solved the problem of finding structures in linear layers and of decomposing them, and they applied this to Streebog. They also continued developing a new cryptanalysis family; differential meet-in-the-middle attacks. They figured out how to correctly combine it with bicliques, and started working on an application on the construction of SKINNY, which should be comparable if not better than the best known attacks.

- Group 3 worked on several topics related to cryptanalysis, that they plan to continue after the seminar. The studied Tweakable Twine, a tweakable variant of Twine proposed in 2019. They looked at impossible differential distinguishers, but unfortunately they were not able to cover more rounds than in previous work. They also looked at the differential propagation of the cipher. They were able to find a distinguisher that would be established with a probability of 2^{-61}, and they rediscovered a 24-round zero correlation attack in Twine. They have also pointed out several observations on TinyJAMBU, including a method to break the P_b permutation (for 384 rounds) if one can observe collisions during the processing phase. They looked at a paper from 2016 on KATAN that searches for extended boomerang distinguishers. They are implementing the attacks to observe the impact of the middle-round dependencies experimentally. Finally, they looked at (free-start) collisions on Romulus-H and tried to find differential characteristics that are suitable to be used in two SKINNY invocations. One idea would be to use the dependencies to have a collision of a higher probability.
- Group 4 has worked on integral distinguishers on big finite fields. After looking at different topics, this group focused in the following problem: can we find integral distinguishers from the knowledge of some properties of the univariate representation of a function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$? In other words, they wanted to find some coefficients $(\lambda_0, \ldots, \lambda_{2^n-1})$ in $\mathbb{F}_{2^n}$ such that $\forall x, \sum_{i=0}^{2^n-1} \lambda_i F(\alpha^i X) = 0$. In the particular case where all $\lambda_i \in \mathbb{F}_{2^n}$, this corresponds to finding sets of inputs such that the corresponding outputs sum to zero. They proved that $\sum_{i=0}^{2^n-1} \lambda_i F(\alpha^i X)$ does not contain any term of degree ℓ if and only if $A_\ell = 0$ or $P(\alpha^\ell) = 0$ where $F(X) = \sum_{i=0}^{2^n-1} A_i X^i = 0$. Therefore, they aimed at finding polynomials P which vanish on all α^ℓ when i varies in a given set, and which have the smallest possible number of terms. Indeed, the number of terms of P is the data complexity of the distinguisher. When the only information we have on F is that $A_i = 0$ for all i of weight $\geq d$, then the polynomial P with binary coefficients and with the smallest weight corresponds to the usual distinguisher obtained with higher-order differentials, i.e., $rot(P) = 2^d$. However, if we have more information on A_i, then we can obtain distinguishers with lower data complexity than expected.
- Group 5 looked at a few different topics, quite unrelated to each other. One of them was how to sample binary words of fixed weight (say 200) and length (say 40000) efficiently and in "cryptographic constant time". A possible approach is to use format-preserving encryption, but this turns out to be quite slow compared to alternatives. They eventually slightly revisited an existing method that oversamples w' indices uniformly and independently such that at least w of them are unique with high probability, by proposing a possibly novel and simple constant-time algorithm to extract such a subset of w indices uniformly: write a list (v_i, i) of the w' samples; sort with respect to v_i, mark any duplicate by setting i to infinity; sort with respect to i and keep the w first entries. Another topic was the study of the exact differential probability of 1/4 round of Salsa, or rather computing exactly the probability of any 1/4 round differential. A "promising" approach would be to use finite automata to parameterize the space of solutions to part of a round, and then iteratively propagate this through the successive steps thereof. They have not implemented this, but one could in principle at least partially rely on some existing tools for the first part. Whether the parameterization would be sufficiently compact to also allow an efficient propagation is not clear yet.

2 Table of Contents

3 Overview of Talks

3.1 New Directions in Cryptanalysis

Orr Dunkelman (University of Haifa, IL)

Joint work of Orr Dunkelman, Itai Dinur, Nathan Keller, Eyal Ronen, Adi Shamir

A central problem in cryptanalysis is to find all the significant deviations from randomness in a given n-bit cryptographic primitive. When n is small (e.g., an 8-bit S-box), this is easy to do, but for large n, the only practical way to find such statistical properties was to exploit the internal structure of the primitive and to speed up the search with a variety of heuristic rules of thumb. However, such bottom-up techniques can miss many properties, especially in cryptosystems which are designed to have hidden trapdoors.

In this paper we consider the top-down version of the problem in which the cryptographic primitive is given as a structureless black box, and reduce the complexity of the best known techniques for finding all its significant differential and linear properties by a large factor of $2^{n/2}$. Our main new tool is the idea of using *surrogate differentiation*. In the context of finding differential properties, it enables us to simultaneously find information about all the differentials of the form $f(x) \oplus f(x \oplus \alpha)$ in all possible directions α by differentiating f in a single arbitrarily chosen direction γ (which is unrelated to the α's). In the context of finding linear properties, surrogate differentiation can be combined in a highly effective way with the Fast Fourier Transform. For 64-bit cryptographic primitives, this technique makes it possible to automatically find in about 2^{64} time all their differentials with probability $p \geq 2^{-32}$ and all their linear approximations with bias $|p| \geq 2^{-16}$; previous algorithms for these problems required at least 2^{96} time. Similar techniques can be used to significantly improve the best known time complexities of finding related key differentials, second-order differentials, and boomerangsa In addition, we show how to run variants of these algorithms which require no memory, and how to detect such statistical properties even in trapdoored cryptosystems whose designers specifically try to evade our techniques.

3.2 Review of the NIST Modes of Operation: Status Update and Standardization of a New Mode?

Nicky Mouha (NIST – Gaithersburg, US)

The Crypto Publication Review Board was established by NIST to identify cryptography standards and other publications to be reviewed. Currently, the NIST-recommended modes of operation (NIST SP 800-38 Series) are undergoing review.

At this time of writing, the Crypto Publication Review Project website (`https://csrc.nist.gov/Projects/crypto-publication-review-project`) lists the following modes of operation as subject to review: SP 800-38A (ECB, CBC, CFB, OFB, CTR), SP 800-38A Addendum (three ciphertext stealing variants for CBC), SP 800-38D (GCM and GMAC), and SP 800-38E (XTS).

In this presentation, we gave a technical overview of the NIST-recommended modes of operation, giving insights into the functionality of the algorithms, and an overview of the public comments received.

Less than two weeks before the presentation, NIST had made an announcement related to the review of these modes of operation. This gave an opportunity to provide a status update, and to collect feedback for NIST from the attendees of this talk at the Dagstuhl Symmetric Cryptography Seminar.

3.3 Simplified MITM Modeling for Permutations: New (Quantum) Attacks

André Schrottenloher (CWI – Amsterdam, NL)

Joint work of André Schrottenloher, Marc Stevens
Main reference André Schrottenloher, Marc Stevens: "Simplified MITM Modeling for Permutations: New (Quantum) Attacks", IACR Cryptol. ePrint Arch., p. 189, 2022.
URL https://eprint.iacr.org/2022/189

Meet-in-the-middle (MITM) is a general paradigm where internal states are computed along two independent paths ("forwards" and "backwards") that are then matched. Over time, MITM attacks improved using more refined techniques and exploiting additional freedoms and structure, which makes it more involved to find and optimize such attacks. This has led to the use of detailed attack models for generic solvers to automatically search for improved attacks, notably a MILP model developed by Bao et al. at EUROCRYPT 2021.

In this paper, we study a simpler MILP modeling combining a greatly reduced attack representation as input to the generic solver, together with a theoretical analysis that, for any solution, proves the existence and complexity of a detailed attack. This modeling allows to find both classical and quantum attacks on a broad class of cryptographic permutations. First, Present-like constructions, with the permutations of the Spongent hash functions: we improve the MITM step in distinguishers by up to 3 rounds. Second, AES-like designs: despite being much simpler than Bao et al.'s, our model allows to recover the best previous results. The only limitation is that we do not use degrees of freedom from the key schedule. Third, we show that the model can be extended to target more permutations, like Feistel networks. In this context we give new Guess-and-determine attacks on reduced Simpira v2 and Sparkle. Finally, using our model, we find several new quantum preimage and pseudo-preimage attacks (e.g. Haraka v2, Simpira v2 ...) targeting the same number of rounds as the classical attacks.

3.4 Triplex: an Efficient and One-Pass Leakage-Resistant Mode of Operation

Yaobin Shen (University of Louvain, BE)

Joint work of Thomas Peters, Yaobin Shen, François-Xavier Standaert

This talk introduces and analyzes Triplex, a leakage-resistant mode of operation based on Tweakable Block Ciphers (TBCs) with $2n$-bit tweaks. Triplex enjoys beyond-birthday ciphertext integrity in the presence of encryption and decryption leakage in a liberal model where all intermediate computations are leaked in full and only two TBC calls operating a long-term secret are protected with implementation-level countermeasures. It provides beyond-birthday confidentiality guarantees without leakage, and standard confidentiality guarantees with leakage for a single-pass mode embedding a re-keying process for the bulk of its computations (i.e., birthday confidentiality with encryption leakage under a bounded leakage assumption). Triplex improves leakage-resistant modes of operation relying on TBCs with n-bit tweaks when instantiated with large-tweak TBCs like Deoxys-TBC (a CAESAR competition laureate) or Skinny (used by the Romulus finalist of the NIST lightweight crypto competition). Its security guarantees are maintained in the multi-user setting.

4 Working groups

4.1 Exact Differential Analysis of One Round of Salsa20

Orr Dunkelman (University of Haifa, IL), Antonio Florez-Gutierrez (INRIA – Paris, FR), Pierre Karpman (Université Grenoble Alpes – Saint Martin d'Hères, FR), Eram Lambooij (University of Haifa, IL), and Nicky Mouha (NIST – Gaithersburg, US)

In Salsa20, one round consists of four parallel quarterround functions on independent inputs. These quarterround functions transform a 128–bit by adding two 32–bit inputs (modulo 2^{32}), rotating the output over a fixed amount of bits and XORing it with a third 32–bit input. This operation is performed four times within a quarterround.

It seems to be an open problem to compute the exact differential probability for one quarterround of Salsa20. It has been shown that theoretical estimates of the probability may not correspond to estimates obtained by experimental verification [1, 2].

The goal of this research group was to explore some methods to calculate the exact differential probability for one quarterround of Salsa20, and confirm these with experiments on a small-scale variant of Salsa20. Because the four quarterround functions are independent of each other, a method to determine the exact differential probability for one quarterround, would also lead to a result for one round of Salsa20.

We explored the problem from both a theoretical and experimental point of view, and arrived at various new insights that will be helpful to find an elegant and efficient solution to this problem.

References

1 Nicky Mouha and Bart Preneel. *Towards Finding Optimal Differential Characteristics for ARX: Application to Salsa20*. Cryptology ePrint Archive, Report 2013/328, 2013.
2 Nicky Mouha. *On Proving Security against Differential Cryptanalysis*. CFAIL 2019, A Conference for Failed Approaches and Insightful Losses in Cryptology, 2019.

4.2 A simple quasi-linear constant-time algorithm for sampling fixed-sized supports

Pierre Karpman (Université Grenoble Alpes – Saint Martin d'Hères, FR), Orr Dunkelman (University of Haifa, IL), Antonio Florez–Gutierrez (INRIA – Paris, FR), Eram Lambooij (University of Haifa, IL), and Nicky Mouha (NIST – Gaithersburg, US)

In this short note, we present a simple algorithm for uniformly sampling a subset of [[0, N – 1]] of size w, for some integers N and w. The cost of our algorithm is quasi- linear in w, assuming a constant cost for arithmetic and random sampling of integers less than N. It is also amenable to "cryptographic constant-time" implementations, that is whose running time and memory accesses neither depend on the random coins used in the sampling. Such an algorithm and implementation find applications in certain code-based cryptosystems.

4.3 Research group on the cryptanalysis of recent primitives

Virginie Lallemand (LORIA – Nancy, FR), Xavier Bonnetain (LORIA & INRIA Nancy, FR), Maria Eichlseder (TU Graz, AT), Daniël Kuijsters (Radboud University Nijmegen, NL), Clara Pernot (INRIA – Paris, FR), Shahram Rasoolzadeh (Radboud University Nijmegen, NL), Yu Sasaki (NTT – Tokyo, JP), and André Schrottenloher (CWI – Amsterdam, NL)

We worked and discussed several topics related to cryptanalysis, that we plan to continue after the seminar:

Tweakable Twine: We studied this cipher which is a tweakable version of Twine proposed in 2019. We looked at impossible differentials distinguishers but unfortunately were not able to cover more rounds than in the previous work. We also looked at the differential properties of the cipher, and were able to find a $2^{-60.21}$ distinguisher on 17 rounds. We (re-)discovered a 24-round zero-correlation on Twine.

Tiny-Jambu: We have several observations, including a method to break the P_k permutation (for 384 rounds) if we can observe collisions during the AD processing phase.

Katan: We looked at a paper from 2016 that searches extended boomerang distinguishers. We are implementing the attack to observe the impact of the middle-round dependencies experimentally.

Romulus-H: (Skinny-Hirose) We looked at free-start and (real) collisions and tried to find differential characteristics that are suitable to be used in two Skinny invocations in Hirose's mode. One idea would be to use the dependencies in the states to have a collision of higher probability.

4.4 Provable Security Research Group

Bart Mennink (Radboud University Nijmegen, NL), Ritam Bhaumik (INRIA – Paris, FR), Aldo Gunsing (Radboud University Nijmegen, NL), Ashwin Jha (CISPA – Saarbrücken, DE), and Yaobin Shen (University of Louvain, BE)

The aim of the provable security group within Dagstuhl was to analyze generic security of modes, either by proving security under certain assumptions or by mounting generic attacks. The provable security group, consisting of Ritam Bhaumik, Aldo Gunsing, Ashwin Jha, Bart Mennink, and Yaobin Shen, worked on various topics in provable security. We discussed five topics in total, one corresponding to each group member. For three problems, we postponed the continuation until after Dagstuhl: it was required that each group member would read certain relevant papers offline, and only then we could continue solving the problem. For two problems we advanced quite well. The first problem was the unforgeability of a strengthened version of the Wegman-Carter-Shoup authenticator. Although this strengthened version only achieves birthday bound PRF-security, we observed that its provable unforgeability is better, and we drafted the proof ideas. The second problem was about a generic description and analysis of PRFs based on two public permutations, and a generic description and analysis of MAC functions based on two public permutations. We described the generic classification and filtered out the "sets" of functions that achieve high security.

4.5 Workgroup 1

Maria Naya-Plasencia (INRIA – Paris, FR), Christof Beierle (Ruhr-Universität Bochum, DE), Christina Boura (University of Versailles, FR), Patrick Derbez (University of Rennes, FR), Patrick Felke (FH Emden, DE), Nils Gregor Leander (Ruhr-Universität Bochum, DE), and Sondre Rønjom (University of Bergen, NO)

We worked on several topics, that we plan to continue after the seminar.

1. Find good algorithms for detecting the optimal trees of some boolean functions in the context of improved key-recovery attacks. Do we need trees? Could we find/use better cases with partitions that do not correspond to a tree?
2. A new type of attack: Differential MitM. We continue to develop its theoretical complexities, adding this to apply the byclique extension and work on building an application on the block cipher Skinny.
3. We built two attacks on the construction HAL + LOOP.
4. We solved how to find structures in linear layers, how to decompose them, and how to apply it to Streeborg.

4.6 Univariate Integral Distinguishers

Yann Rotella (University of Versailles, FR), Subhadeep Banik (University of Lugano, CH), Clémence Bouvier (INRIA – Paris, FR), Anne Canteaut (INRIA – Paris, FR), Margot Funk (University of Versailles, FR), Daniël Kuijsters (Radboud University Nijmegen, NL), Patrick Neumann (Ruhr–Universität Bochum, DE), Léo Perrin (INRIA – Paris, FR), Christian Rechberger (TU Graz, AT), Markus Schofnegger (TU Graz, AT), and Tyge Tiessen (Technical University of Denmark – Lyngby, DK)

Recent surge in development of advanced cryptographic protocols (such as multi-party computation, zero-knowledge proofs) created interest in specialized symmetric-key cryptographic primitives including block ciphers, stream ciphers, hash functions. The new setting favors *algebraic* constructions based on relatively large finite fields, since it leads to lesser costs in the protocols. This contrasts with classic symmetric-key cryptography, where operations are typically bit-oriented and are optimized for performance on common CPUs.

The new paradigm demands for exploring new cryptanalysis methods. In this work, we focused on adapting the *integral* attacks, which before were typically developed in the *binary multivariate* setting.

Integral attacks on classic symmetric primitives are well understood and state-of-the-art includes many tools both for finding and exploiting integral distinguishers. On the other hand, integral attacks on the algebraic constructions are not yet well studied and do not seem to fully exploit the algebraic properties. Initial work in this direction was made in recent works [1, 2, 3, 5]. In this working group, we aimed to advance this direction by exploring and systemizing methods of *searching for* and *exploiting* integral distinguishers in the *univariate* setting. More precisely, we studied which linear combinations of the outputs of a function are constant, given a set of missing monomials in the function's univariate representation.

The working group achieved several interesting results.

1. We briefly studied methods of bounding the degree in large fields and attempted to generalize standard methods based on tracking maximum variable degrees or division property [4]. We reached to conclusion that, in large characteristic, naive approaches seem to often provide the exact degree and thus no significant improvements can be done.
2. We developed a method of studying univariate integral distinguishers based on *function operators*, which act predictably on the univariate coefficients. We considered several operators, such as operators reducing the coefficients to their field trace or trace-based filtering of coefficients, operators summing over a multiplicative subgroup.
3. We discovered a simple operator resembling a composition of polynomials, which includes most previously mentioned operators as special cases. It also has interesting mathemathical properties such as commutativity of operators.
4. We studied a few concrete examples, such as: a single monomial missing, a single cyclotomic class missing, a (multivariate) algebraic degree is bounded – and proved optimal distinguishers for these cases.

References

1 Tim Beyne, Anne Canteaut, Itai Dinur, Maria Eichlseder, Gregor Leander, Gaëtan Leurent, María Naya-Plasencia, Léo Perrin, Yu Sasaki, Yosuke Todo, Friedrich Wiemer. *Out of Oddity – New Cryptanalytic Techniques Against Symmetric Primitives Optimized for Integrity Proof Systems*. CRYPTO, 2020.

2 Maria Eichlseder, Lorenzo Grassi, Reinhard Lüftenegger, Morten Øygarden, Christian Rechberger, Markus Schofnegger, Qingju Wang. *An Algebraic Attack on Ciphers with Low-Degree Round Functions: Application to Full MiMC*. ASIACRYPT, 2020.

3 Carlos Cid, Lorenzo Grassi, Aldo Gunsing, Reinhard Lüftenegger, Christian Rechberger, Markus Schofnegger. *Influence of the Linear Layer on the Algebraic Degree in SP-Networks*. TosC, 2022.

4 Yosuke Todo. *Structural Evaluation by Generalized Integral Property*. EUROCRYPT, 2015.

5 Clémence Bouvier, Anne Canteaut, Léo Perrin. *On the Algebraic Degree of Iterated Power Functions*. EPRINT, 2022.

Participants

- Subhadeep Banik
University of Lugano, CH
- Christof Beierle
Ruhr-Universität Bochum, DE
- Ritam Bhaumik
INRIA – Paris, FR
- Xavier Bonnetain
LORIA & INRIA Nancy, FR
- Christina Boura
University of Versailles, FR
- Clémence Bouvier
INRIA – Paris, FR
- Anne Canteaut
INRIA – Paris, FR
- Patrick Derbez
University of Rennes, FR
- Orr Dunkelman
University of Haifa, IL
- Maria Eichlseder
TU Graz, AT
- Patrick Felke
FH Emden, DE
- Antonio Florez-Gutierrez
INRIA – Paris, FR
- Margot Funk
University of Versailles, FR
- Aldo Gunsing
Radboud University
Nijmegen, NL
- Ashwin Jha
CISPA – Saarbrücken, DE
- Pierre Karpman
Université Grenoble Alpes –
Saint Martin d'Hères, FR
- Daniël Kuijsters
Radboud University
Nijmegen, NL
- Virginie Lallemand
LORIA – Nancy, FR
- Eran Lambooij
University of Haifa, IL
- Nils Gregor Leander
Ruhr-Universität Bochum, DE
- Bart Mennink
Radboud University
Nijmegen, NL
- Nicky Mouha
NIST – Gaithersburg, US
- Maria Naya-Plasencia
INRIA – Paris, FR
- Patrick Neumann
Ruhr-Universität Bochum, DE
- Clara Pernot
INRIA – Paris, FR
- Léo Perrin
INRIA – Paris, FR
- Shahram Rasoolzadeh
Radboud University
Nijmegen, NL
- Christian Rechberger
TU Graz, AT
- Yann Rotella
University of Versailles, FR
- Sondre Rønjom
University of Bergen, NO
- Yu Sasaki
NTT – Tokyo, JP
- Markus Schofnegger
TU Graz, AT
- André Schrottenloher
CWI – Amsterdam, NL
- Yaobin Shen
University of Louvain, BE
- Tyge Tiessen
Technical University of Denmark
– Lyngby, DK
- Aleksei Udovenko
University of Luxembourg, LU