Vorträge im Rahmen des Besetzungsverfahrens der Laufbahnstelle „Kryptographie“

Montag 15. Mai 2023, 11:00 Uhr
Seminarraum 3W03 ICT Gebäude

Dr. Arnab Roy

Lehrevortrag „Cryptographic Commitments“ (15 Minuten) und anschließend der Forschungsvortrag mit dem Titel:

Novel Cryptography for Zero-Knowledge Proof Systems and Private Computations

Abstract:

Advanced cryptographic ideas, such as multi-party computation (MPC), zero-knowledge proofs (ZKP) and fully homomorphic encryption (FHE) are able to provide secure and private computations on data. Although these ideas date back to 1980s, it has not been until recently that we saw practical uses of MPC, ZKP and HE. In the past several years significant scientific progress has been made in improving their efficiency. The computation protocols built upon these ideas are extremely important and relevant in the modern data driven world. Some prominent applications include privacy-preserving statistical computation and machine learning algorithms, anonymous cryptocurrencies and blockchains, and secure distributed key storage. In this lecture I will give an overview of my research in two areas - novel cryptographic constructions for building efficient ZK proof systems and privacy preserving computations, and new techniques towards practical applications of HE.

In the first part of my talk, I will present novel symmetric cryptographic primitives that are designed over (large) prime fields. I will show why such prime field based primitives are mandated by the higher level protocols. I will demonstrate how these primitives enable building ZK proof systems and MPC protocols that are significantly faster than those relying on symmetric primitives defined over binary extension field or boolean rings, such as AES and SHA-2. I will also discus the distinct features of these novel primitives, their practical applications and impact.

In the second part of my lecture, I will present a new number-theoretic technique that allows practical application of HE encryption on real (valued) data. In the last years, some important

progress has been made towards making HE encryption practical for general applications. While HE schemes are defined over integers or polynomial rings, in practice these schemes must work with real numbers. Numerous existing works propose encoding methods that are tailored for specific ring LWE (Learning with Error) based HE schemes, but their encodings are somewhat adhoc. Here, I will present a new technique based on p-adic number theory that builds a mathematically sound encoding scheme. I will also show the advantages of the new encoding scheme and how it aids the analysis of the underlying HE scheme.
Finally, I will also discuss the future research directions in these two areas.

Montag 15. Mai 2023, 15:00 Uhr
Seminarraum 3W03 ICT Gebäude

Jan Butora PhD

Lehrevortrag „Cryptographic Commitments“ (15 Minuten) und anschließend der Forschungsvortrag mit dem Titel:

JPEG Compression Errors for Image Forensics

Abstract:

JPEG format is arguably the most popular format of digital images due to its ratio between image quality and compression factor. It is probably why JPEG images are more and more used for creating fake images spreading misinformation and disinformation or as a medium for hiding malicious code. In this talk, I will show that JPEG compression creates a particular structure in digital images and we will see that natural images carry a very specific signature-like signal, which could be used for extremely accurate detection of manipulations of JPEG files.

This technique called the Reverse JPEG Compatibility Attack (RJCA) is very reliable in laboratory conditions, however some of its assumptions do not always hold in real-world scenarios. I will outline the basics behind this attack and illustrate its strengths and pitfalls. Next, I will share some of my recent results and demonstrate that by further exploiting the naturally imposed JPEG structure, we can derive various novel methods of image forensics, such as a timing attack on JPEG compatibility. Although there are situations in which the attack will not be applicable, it is important to understand when and why such situations could arrive.

Finally, I will cover my ongoing work on using Convolutional Neural Networks (CNNs) for the RJCA. While CNNs are the most accurate detectors available, we only have empirical guarantees on their performance. Moreover, their training is typically done on images of fixed size, additionally limiting their operational usability. We will address these two issues by restricting ourselves to statistical tests and by modeling the networks' outputs for images of different sizes.

Dienstag 16. Mai 2023, 08:45 Uhr
Seminarraum 3W03 ICT Gebäude

Debayioti Das PhD

Lehrevortrag „Cryptographic Commitments“ (15 Minuten) und anschließend der Forschungsvortrag mit dem Titel:

Making anonymous communication practical and provably secure

Abstract:

Many anonymous communication (AC) protocols have been proposed over the last four decades to protect privacy over the internet. They have been on an eternal quest to be practically applicable in terms of computation and communication overhead, while providing strong anonymity guarantees.

In my talk, I will first present a design of an AC protocol OrgAn that attempts to provide anonymity in an organizational network and support versatile applications including latency-sensitive applications like audio calls. OrgAn provides strong provable anonymity guarantees based on dining cryptographers network (DC-net) design paradigm, and also provide defense against relevant active attacks. This is the first DC-net based protocol that does not require a setup phase before every round to achieve 'key-agreement' and 'slot-agreement' before every round. However, this protocol is not without limitations --- (i) it has to follow a round based communication model, which is difficult to implement in practice; and (ii) it cannot scale for more than few hundred clients (a small to mid-scale organization).

A different design paradigm, mixnets, can easily avoid those problems. Especially, continuous mixnets can easily scale for millions of users and does not require any round based communication model. However, all existing analyses for continuous mixnets rely on experimental evaluations with specific settings and choice of parameters in terms of number of clients, topology, choice of delays etc. Such evaluations cannot provide a comprehensive understanding about how the anonymity guarantees will vary with the variation of those parameters/settings. Our work closes that gap by providing a formal analysis of the anonymity guarantees provided by such designs. I will present the roadblocks we faced, proof-strategy, and interesting corollaries for our proofs. Finally, I will conclude the talk with interesting future research directions in this field.

Dienstag 16. Mai 2023, 15:00 Uhr
Seminarraum 3W03 ICT Gebäude

Katharina Boudgoust PhD

Lehrevortrag „Cryptographic Commitments“ (15 Minuten) und anschließend der Forschungsvortrag mit dem Titel:

New Reductions and Constructions for Module Learning With Errors

Abstract:

The Module Learning With Errors (M-LWE) problem has become a widely used hardness assumption in public-key cryptography, and in particular for post-quantum cryptography. As the US National Institute of Standards and Technology (NIST) announced in 2022 the standardization of the encryption scheme Kyber and the signature scheme Dilithium, two cryptographic schemes whose security relies on M-LWE, it is highly probable that we will see this hardness assumption used in many more cryptographic primitives in the future. It is thus of high importance to continue studying its hardness. Further, now that we gained good knowledge on how to design encryption and signatures based on M-LWE, the next step is to study more advanced cryptographic primitives that allow for additional features. Both aspects are at the center of my research, whose goal is to prove new reductions and constructions for the Module Learning With Errors problem.

During the presentation, I provide a brief introduction to the research area and highlight one of my past scientific projects. I then present my research plan, while sketching the challenges of the questions raised and giving directions that I think are promising for answering these questions.

universität
innsbruck

Institut für Informatik

Mittwoch 17. Mai 2023, 08:45 Uhr
Seminarraum 3W03 ICT Gebäude

Dr. Jeongeun Park

Lehrevortrag „Cryptographic Commitments“ (15 Minuten) und anschließend der Forschungsvortrag mit dem Titel:

Towards real-world applications via homomorphic encryption.

Abstract:

Fully Homomorphic Encryption (FHE) allows a computation over encrypted data.
Therefore, it can be applied to a secure outsourced computation where a server which has strong computational power does a (requested) computation over data of a client, while keeping the server oblivious to the data.
More importantly, FHE is a well known tool to build efficient privacy preserving protocols by allowing them to achieve asymptotically optimal complexity in both communication and computation, as well as non-interactiveness, which is desirable for real-world applications.

In this talk, we study the impact of the current state-of-the art FHE on the real-world.
We introduce privacy preserving building blocks based on FHE such as private information retrieval (PIR), oblivious ram (ORAM) by showing what kinds of benefits FHE can provide.
And we discuss the current limitation and the next step for such building blocks to become deployable applications in the real world, by providing some examples.

universität
innsbruck

Institut für Informatik

Mittwoch 17. Mai 2023, 11:00 Uhr
Seminarraum 3W03 ICT Gebäude

Dr. Aleksej Udovenko

Lehrevortrag „Cryptographic Commitments“ (15 Minuten) und anschließend der Forschungsvortrag mit dem Titel:

From Gray-box to White-box Cryptography

Abstract:

In the field of cryptography, there is a concept called white-box cryptography, which involves an adversary having full access to a software implementation of a symmetric-key primitive, such as the AES block cipher. Despite over 20 years of attempts to create such implementations, it has not been possible to prevent the secret key embedded in the program from being extracted. In fact, most of proposed designs have not even achieved gray-box/side-channel security, where the adversary only has partial physical access to a device executing the cryptographic program. On the other hand, the gray-box setting has been extensively developed, and offers a variety of strong protection techniques.

This contradiction has led to a new research direction of extending gray-box attacks and countermeasures to specifics of the white-box model. In this talk, I will introduce the concept of white-box cryptography and then focus on algebraic attacks and countermeasures against them. Algebraic attacks target the most powerful gray-box protection - linear masking schemes, and thus create the first barrier on the way from gray-box to white-box implementations. I will describe the high-level idea of algebraic attacks and how they apply to linear masking schemes. Then, I will present two protection techniques - a nonlinear masking scheme and dummy shuffling - and discuss some of their shortcomings and related open problems in the topic.

Finally, I will conclude the talk by outlining future research directions for building the path towards white-box cryptography and applications beyond symmetric-key encryption.