ABSTRACTS

1) Can volcanoes help us against quantum computers?

The theory of elliptic curves is an essential topic in number theory and, consequently, cryptography. Everyone of us comes across elliptic curves on a daily basis every time we connect to the internet. At the core, the safety of these connections relies on hard problems in number theory, including the discrete logarithm problem on an elliptic curve. However, with the introduction of quantum computing, these problems do not seem to be hard enough for secure communication. The solution brings the isogeny based cryptography, which is based on particular maps between elliptic curves. These maps, called isogenies, form structures of a particular shape, called volcanos. This presentation will be your guide to isogeny volcanoes and my work on them as well as their importance in the age of quantum computers.

2) Identification and Assessment of Active Cyber Threats

One of the proactive approaches utilized to protect critical assets and govern cyber threats is the sharing of data describing threats. Given the potentially large volume of data about threats, security teams need to select and efficiently process only information relevant from the perspective of protected assets. Existing standards and methods from threat, vulnerability, and asset management can solve separate issues belonging to this research area, but their restricted mutual interoperability hinders accurate identification of cyber threats and their properties. Besides, current mature methods for threat assessment are too slow for near real-time prioritization of threats. In this talk, the contextualization of globally shared data about cyber threats with local knowledge about assets and consequent threat assessment using attack graphs will be introduced. Proposed approaches should improve the combination of data from various sources beyond simple joins of data and enable the prioritization of the most severe threats.

3) Minerva: The curse of ECDSA nonces

This talk presents the Minerva group of side-channel vulnerabilities in implementations of the ECDSA signature algorithm in a widely used Atmel AT90SC FIPS 140-2 certified smartcard chip and five cryptographic libraries. Vulnerable implementations leak the bit-length of the scalar used in scalar multiplication via timing. Using the leaked bit-length, we mount a lattice attack on a 256-bit curve, after observing enough signing operations. We propose two new methods to recover the full private key requiring just 500 signatures for simulated leakage data, 1200 for real cryptographic library data, and 2100 for smartcard data.
We use the set of vulnerabilities reported in this paper, together with the recently published TPM-FAIL vulnerability as real-world leakage datasets to systematically compare our newly proposed methods and all previously published applicable lattice-based key recovery methods. The resulting exhaustive comparison highlights the methods' sensitivity to its proper parametrization and demonstrates that our methods are more efficient in most cases. For the TPM-FAIL dataset, we reduced the number of required signatures from approximately 40 000 to mere 900.

4) Secure Nonce Caching in Schnorr-Based Multi-Signatures

The Schnorr signature is a type of digital signature, which is suitable for the construction of efficient multi-signature protocols. Multi-signature protocols allow secret information used for signing to be divided among multiple parties, all of which need to participate in the signing protocol in order to create a valid signature. This property is used to better secure the secret information against compromise, which is especially valued in the context of cryptocurrencies, as the compromise leads to an immediate monetary loss. However, even with the use of Schnorr signatures, several subtle issues need to be addressed in order to obtain a secure multi-signature protocol, as? seemingly insignificant change can introduce vulnerability. In this talk, we focus on an optimization used in Schnorr multi-signatures to speed up signing by precomputation, which makes the protocol vulnerable to an attack via a solution for the ROS problem, and discuss possible countermeasures against such an attack.

5) Clustering of the motion capture data

Recently, a rapid rise in the amount of motion capture data has occurred, which has led to the necessity of new processing approaches of such data. To classify specifically selected short motion segments, neural networks can be used. However, they are not applicable in scenarios where the data is captured as a long sequence without semantic partitioning knowledge. A new approach has recently been proposed, based on the transformation of the motion capture data into motion words, which can afterwards be processed by mature text processing algorithms. One of the crucial parts of this transformation is a clustering of segments, which make up one action (e.g., sitting down or walking a few steps). The purpose of our work is to analyze and evaluate the quality of various clustering approaches. Considering the evaluation, we focus on both statistical measures and two real-world application scenarios, namely, the action classification and searching for similar actions to a selected query action.