INFORMATION, COMMUNICATION & COMPUTING

Fields of Expertise TU Graz

Source: istockphoto.com

Kay Uwe Römer,
Information, Communication & Computing
Source: Lunghammer – TU Graz

Together with Research & Technology House we are currently working on improving the means for internal and external communication of the FoE ICC. There is a new FoE web page in TU4U which is intended as a means of sharing information among FoE members[1]. However, we need your support, dear FoE members, to fill this page with interesting content and keep it up-to-date. In particular, we want to list science events on this page which are organized by FoE members and which may be interesting to other FoE members. We would also like to add brief success stories about research carried out in the FoE, joint research programs in the FoE, and other news stories that are relevant to FoE members. Please contact us at <FoE_ICC@tugraz.at> if you have information that you would like to share with other FoE members on that page. While this TU4U page is meant for sharing internal information among the FoE members, there is an additional FoE page which is meant to address the broad public and which we plan to revise next[2]. This page contains a long list of research topics covered by the FoE. However, external persons interested in collaboration with TU Graz on particular topics cannot currently easily find out who is the right person to contact for each topic. Also, we are looking for a good way to visualize this information for our currently 140 FoE members. If you have any ideas about how to achieve this, or more generally about how to improve the web presence of the FoE, please contact us.

In this issue of TU Graz research, Maria Eichlseder gives us some insights into her research work. Enjoy reading.

[1] https://tu4u.tugraz.at/bedienstete/forschung/fields-of-expertise-der-tu-graz-foe/information-communication-computing

[2] https://www.tugraz.at/forschung/fields-of-expertise/information-communication-computing/uebrblick-information-communication-computing

Maria Eichlseder

Secure and Efficient Symmetric Cryptography

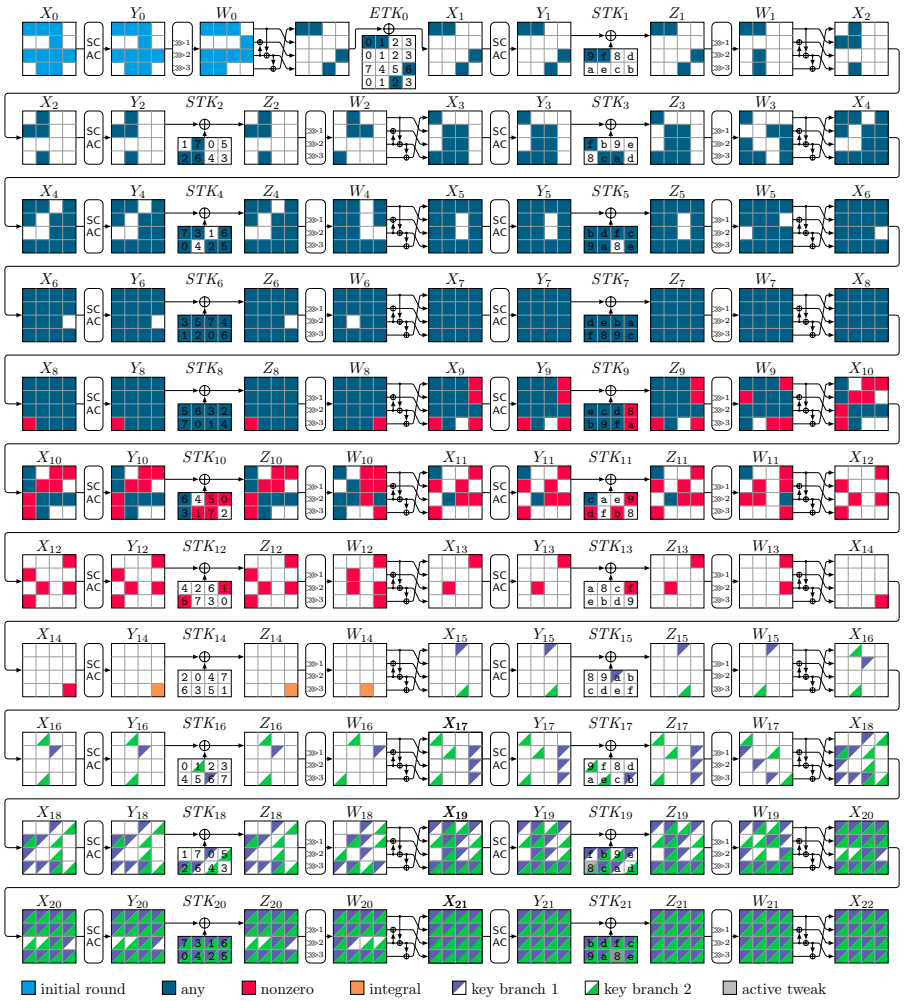
Cryptographic algorithms are the key to secure communication over insecure channels, such as wireless communication or the internet. In our research, we work on new, efficient cryptographic algorithms that remain secure using constrained resources. Additionally, we develop tools for cryptanalysis to improve our understanding of cryptanalytic security.

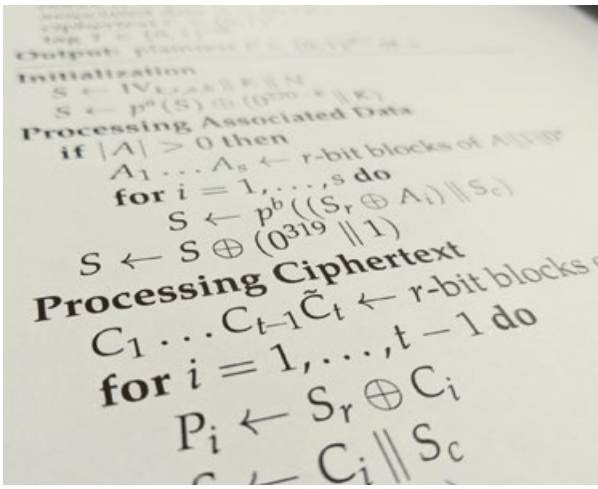
Cryptographers have developed algorithms for various tasks, including the distribution of secret keys, digital signatures, or joint computation on private data. The central algorithms of most secure communication protocols are authenticated encryption algorithms. These symmetric algorithms can encrypt a plaintext message into a ciphertext so that a third party can neither infer any information about the content of the plaintext message nor manipulate the ciphertext undetected. Only the owners of the shared secret key – i.e., the sender and the rightful recipient – can encrypt & authenticate or decrypt & verify.

CRYPTOGRAPHIC SECURITY

This key, a short sequence of securely randomly generated bytes, is the only part of the mechanism they need to keep secret; the entire algorithm is otherwise public. The key must be long enough such that randomly guessing it in a brute-force attack is utterly infeasible. Additionally, the algorithm must not have any other weaknesses that would allow for more efficient attacks than the claimed security level.

There are two ways to study the security of cryptographic algorithms: proofs and cryptanalysis. A security reduction proof is a mathematical proof of a statement like “Cryptographic protocol X is secure if its ingredients, the mathematical schemes A, B, and C, are secure”, at a specific security level. Such proofs are indispensable for arguing the security of complex cryptographic systems by reducing the problem to simpler subproblems. However, this approach reaches its limit when we study the security of cryptographic primitives which are in a sense atomic and have no such simple subproblems. They create security from scratch instead of deriving it from other secure building blocks. Their security level can only be quantified by cryptanalysis, that is, by trying to find the strongest possible attacks on the primitive and verifying that these do not threaten the security level.



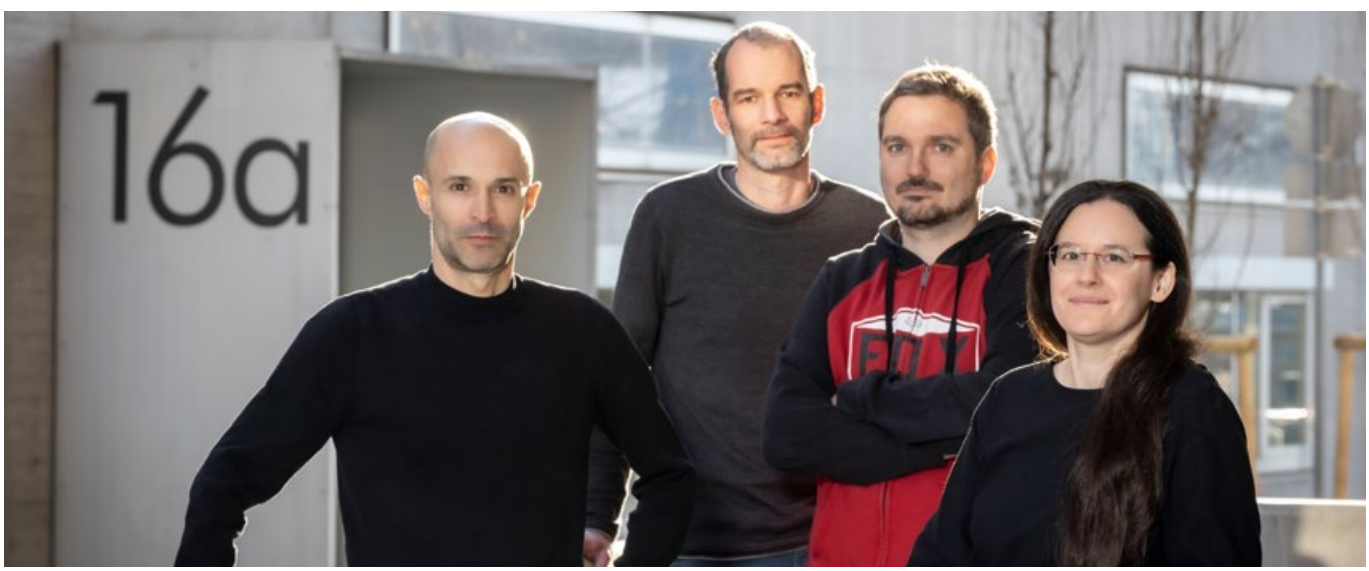


Source: Maria Eichlseder

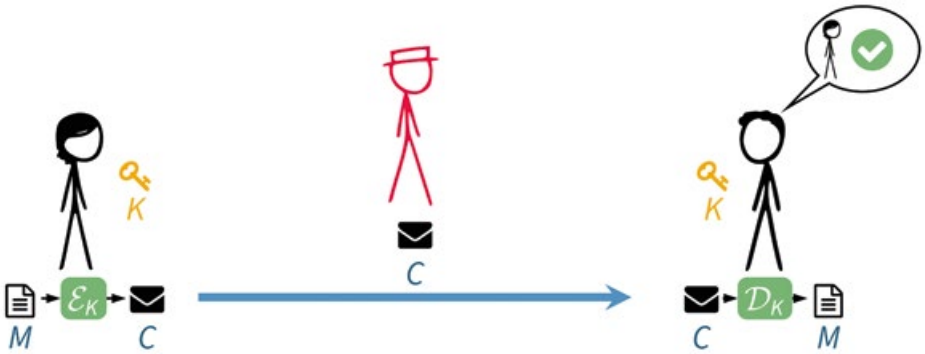
CRYPTOGRAPHIC COMPETITIONS

Building trust in a new primitive with cryptanalysis is hard work – as well as slow work. It requires years of intense scrutiny by experts. This is why widely-used cryptographic systems, such as the TLS protocol that protects internet traffic, rely on a few standardized cryptographic algorithms. The US National Institute of Standards and Technology (NIST) is the most influential standards organization in this context.

When new challenges necessitate the definition of new standards for some constraints not addressed by the available standards, the most transparent available selection process is a cryptographic competition. The two most recent examples are NIST's competitions for post-quantum cryptography (i.e., algorithms that are expected to remain secure even in the case that a cryptographically relevant quantum computer becomes a reality) and lightweight cryptography (i.e., algorithms that can run even in very constrained environments with limited computational resources). The standardization body first publishes a call for submissions defining the requirements for the future standard. Teams of cryptographers worldwide then design and submit candidate algorithms, which >



Source: Lunghammer – TU Graz



Source: Maria Eichlseder

are evaluated in terms of functionality, security, and performance over the next years. To focus the attention of cryptanalysts and implementers on the more promising candidates, the competition is organized in several rounds, in each of which a substantial fraction of candidates is eliminated from the competition by the standardization body, based on the publicly obtained feedback. Finally, the winner is formally standardized and will typically be implemented widely in industry applications and open-source projects.

TU Graz researchers have been participating very actively in past cryptographic competitions – and very successfully. Last year, to our great joy, the Ascon family of cryptographic algorithms was selected as the winner in NIST's lightweight cryptography competition. The authenticated encryption algorithm was designed at TU Graz by the Ascon team and combines a very lightweight implementation footprint with high robustness. We are currently working with NIST to finalize its standardization, while continuing our research to ensure the Ascon family covers all practical needs for lightweight cryptography.

AUTOMATING CRYPTANALYSIS

One of the crucial deciding factors in competitions is cryptanalysis. However, thoroughly analyzing the large number of candidates is a daunting task, even for the international public cryptanalysis research community. Cryptanalytic attacks are mostly discussed theoretically: cryptanalysts propose theoretical attack procedures and estimate their expected complexity and success probability. The most promising attacks need to be identified from an astronomically large search space of possible attack procedures and parameters, even when restricting our focus only to a specific type of cryptanalysis. There are countless variations and potential optimizations of attacks. While manual analysis is still the best way to discover new attack methodologies, it quickly reaches its limitations when systematically exploring known search spaces. For this reason, tools and solvers for automatically finding weaknesses or optimized attack procedures have become a highly attractive area of research. In our research, we develop models that allow us to find optimal attacks (with respect to certain methodologies), providing us with a much clearer understanding of the security level of cryptographic primitives. By advancing cryptographic design as well as cryptanalysis, we aim to make secure, efficient cryptography available on as many platforms as possible.

Maria Eichlseder

is an assistant professor at the Institute of Applied Information Processing and Communications (IAIK). Her research interests include the design and cryptanalysis of symmetric cryptographic algorithms and their underlying primitives. She graduated sub auspiciis in 2018 and visited Ruhr-Universität Bochum and Radboud University Nijmegen as a guest researcher.

Source: Lunghammer – TU Graz

Source: Hanacek – NIST