ASK 2024: Invited Talks – Title and Abstract

[Christina Boura: Transistor: a TFHE-friendly Stream Cipher]

Abstract - In this talk we will introduce Transistor, a novel stream cipher specifically designed for efficient homomorphic evaluation within the TFHE scheme, a widely-used FHE framework known for its fast bootstrapping and ability to handle low-precision data. Transistor operates on F_17 which is chosen to optimize TFHE performance. Its components are carefully engineered to both control noise growth and provide strong security guarantees. First, a simple TFHE-friendly implementation technique for LFSRs allows us to use such components to cheaply increase the state size. At the same time, a small Finite State Machine is the only part of the state updated non-linearly, each non-linear operation corresponding in TFHE to a very expensive Programmable Bootstrapping. This update is done using an AES-round-like transformation. But, in contrast to other stream ciphers like SNOW or LEX, our construction comes with information-theoretic security arguments proving that an attacker cannot obtain any information about the secret key from three or fewer consecutive keystream outputs. These information-theoretic arguments also lead to a bound on the minimal keystream length required for recovering the secret key. Our implementation of Transistor significantly outperforms the state of the art, achieving a throughput of over 60 bits/s on a standard CPU, all while avoiding the need for an expensive initialization process.

[Jean Paul Degabriele: What's wrong with Poly1305? - Improving Poly1305 through a Systematic Exploration of Design Aspects of Polynomial Hash Functions]

Abstract - One of the most popular symmetric encryption schemes in use on the Internet is ChaCha20-Poly1305. It is the default choice in tools like OpenSSH and Wireguard, and one of only three supported ciphersuites in TLS 1.3. ChaCha20Poly1305 utilizes a polynomial-based hash function for constructing Message Authentication Codes via the Wegman-Carter MAC construction. This entails evaluating the polynomial hash over the data, and blinding the output with a pseudorandom value obtained by enciphering a nonce with a blockcipher. More specifically, it uses Poly1305, originally designed with specific hardware in mind. Today, nearly 20 years later, we ask the following question: Given today's advancements and applications would we still converge to this same design?

[Patrick Derbez: Alternative Key Schedules for the AES]

Abstract - The AES block cipher is today the most important and analyzed symmetric algorithm. While all versions of the AES are known to be secure in the single-key setting, this is not the case in the related-key scenario. In this talk I will answer the question whether the AES would resist better differential-like related-key attacks if the key schedule was different. For this, I will present how we searched for alternative permutation-based key schedules by extending the work of Khoo et al. at ToSC 2017 and Derbez et al. at SAC 2018. We developed different approaches together with MILP-based tools to find good permutations that could be used as the key schedule for AES-128, AES-192 and AES-256. Our methods permitted to find permutations that outperform the permutation exhibited by

Khoo et al. for AES-128. Moreover, our new approach based on two MILP models that call one another allowed us to handle a larger search space and thus to search for alternative key schedules for the two bigger versions of AES. This method permitted us to find permutations for AES-192 and AES-256 that provide better resistance to related-key differential attacks. Most importantly, we showed that these variants can resist full-round boomerang attacks.

[Hossein Hadipour: Revisiting Differential-Linear Attacks]

Differential-linear cryptanalysis, introduced by Langford and Hellman at CRYPTO 1994, is a powerful method for analyzing symmetric-key primitives, exemplified by its role in achieving the best-known attack on SERPENT, the runner-up in the AES competition. By combining statistical properties of differential and linear attacks, it surpasses the effectiveness of either technique alone. Despite its close relationship with the boomerang attack—introduced by Wagner at FSE 1999—the systematic exploration of the connection between these two methods has remained unexplored.

In this talk, we present our recent findings, published at CRYPTO 2024 (https://ia.cr/2024/255), which establish a formal link between the tools used for differential-linear and boomerang distinguishers. This unification not only sheds light on their shared principles but also facilitates the reuse of advances and tools developed for one technique in the context of the other. Additionally, we share recent results, discuss related developments, and propose future research directions to further enhance cryptanalytic techniques in this domain.

[Ashwin Jha: Evasive Properties: A Gap in the Quantum Oracles Zoo]

Abstract - In this talk, I will characterize a class of information-theoretic problems that appear to evade recent advances in quantum oracle-based proof techniques. In particular, the well-known problem of distinguishing the 4-round Luby-Rackoff construction from a random function falls into this category. Consequently, state-of-the-art proof techniques remain ineffective against this problem and others within the class of evasive properties.

[Eik List: Revisiting Demirci-Selcuk Meet-in-the-Middle Attacks on the AES]

Abstract - As the most widespread block cipher, the AES has been the target of tremendous cryptanalytical efforts. During the past decade, the focus of its analysis had shifted towards the search for novel properties and improving results on fewer rounds than what is known for the best attacks. Thus, Demirci-Selcuk Meet-in-the-Middle (DS-MitM) attacks still represent the best attacks on all AES versions in the single-key setting. In this work, we revisit the DS-MitM attacks by Derbez et al. on the AES-128 and related others and show observations, optimizations, and possible directions for further work.

[Bart Mennink: Efficient Instances of Docked Double Decker With AES, and Application to Authenticated Encryption]

Abstract - A tweakable wide blockcipher is a construction which behaves in the same way as a tweakable blockcipher, with the difference that the actual block size is flexible. Due to this feature, a tweakable wide blockcipher can be directly used as a strong encryption scheme that provides full diffusion when encrypting plaintexts to ciphertexts and vice versa. Furthermore, it can be the basis of authenticated encryption schemes fulfilling the strongest security notions. In this paper, we present three instantiations of the docked double decker tweakable wide blockcipher: ddd-AES, ddd-AES^+, and bbb-ddd-AES. These instances exclusively use similar building blocks as AES-GCM (AES and finite field multiplication), are designed for maximal parallelism, and hence, can make efficient use of existing hardware accelerators. ddd-AES is a birthday bound secure scheme, and ddd-AES^+ is an immediate generalization to allow for variable length tweaks. bbb-ddd-AES achieves security beyond the birthday bound provided that the same tweak is not used too often. Moreover, bbb-ddd-AES builds upon a novel conditionally beyond birthday bound secure pseudorandom function, a tweakable variant of the XOR of permutations, facilitating in the need to include a tweak in the AES evaluations without sacrificing flexibility in docked double decker. We furthermore introduce an authenticated encryption mode aaa specifically tailored to be instantiated with ddd-AES and bbb-ddd-AES, where special attention is given to how the nonce and associated data can be processed. We prove that this mode is secure in the nonce-respecting setting, in the nonce-misuse setting, as well as in the setting where random nonces are used. We finally present a comparison with other tweakable wide blockciphers, give a high-level idea of the efficiency potential of our schemes, and provide benchmarks that confirm this idea.

[Palash Sarkar: Two Decades of Research on Tweakable Enciphering Schemes]

Abstract - In 2003, Halevi and Rogaway introduced the notion of tweakable encihpering scheme (TES) and proposed the first construction of such a scheme. In the ensuing two decades there has been a lot of research on TES leading to new constructions and attacks on proposed constructions. In the coming years, NIST of USA will be standardising a mode of operation called the accordion mode, which is closely related to TES. This effort by NIST is expected to lead to a substantial growth in research on TES and its applications. Standing at this intermediate juncture, the talk will provide an overview of the past two decades of research on TES which hopefully will inform future research on this subject.

[André Schrottenloher: Single-query Quantum Hidden Shift Attacks]

Quantum attacks using superposition queries are known to break many classically secure modes of operation. While these attacks do not necessarily threaten the security of the modes themselves, since they rely on a strong adversary model, they help us to draw limits on their provable security.

Typically these attacks use the structure of the mode (stream cipher, MAC or authenticated encryption scheme) to embed a period-finding problem, which can be solved with a dedicated quantum algorithm. The hidden period can be recovered with a few superposition queries (e.g., $O(n)$ for Simon's algorithm), leading to state or key-recovery attacks. However, this strategy breaks down if the period changes at each query, e.g., if it depends on a nonce.

In this work, we focus on this case and give dedicated state-recovery attacks on the authenticated encryption schemes Rocca, Rocca-S, Tiaoxin-346 and AEGIS-128L. These attacks rely on a procedure to find a Boolean hidden shift with a single superposition query, which overcomes the change of nonce at each query. This approach has the drawback of a lower success probability, meaning multiple independent (and parallelizable) runs are needed.

We stress that these attacks do not break any security claim of the authors, and do not threaten the schemes if the adversary only makes classical queries.

[Yaobin Shen: Security Analyses and Enhanced Variants of Standardized MAC Algorithms]

Abstract - Message Authentication Codes (MACs) are ubiquitous primitives deployed in multiple flavors through standards such as HMAC, CMAC, GMAC, LightMAC, and many others. Its versatility makes it an essential building block in applications necessitating message authentication and integrity checks, in authentication protocols, authenticated encryption schemes, or as a pseudorandom or key derivation function. This talk will introduce the current standardized MAC algorithms and their enhanced variants, explore algorithm design concepts, security analyses and related applications, and look forward to potential future research directions.