



Institute of
mathematics
& its applications

19th IMA International Conference on Cryptography and Coding

Abstract Book

Table of Contents

1- An Upper-Bound on the Decoding Failure Probability of the LRPC Decoder- Étienne Burle and Ayoub Otmani	2
2- Coset leaders of the first order Reed-Muller codes in the classes of Niho functions and Threshold functions- Serge Christian Feukoua Jonzo	3
3- Revisiting Nearest-Neighbor-Based Information Set Decoding- Andre Esser	4
4-Feistel Ciphers Based on A Single Primitive- Kento Tsuji and Tetsu Iwata	5
5- Rectangle Attacks on Reduced Versions of the FBC Block Cipher - Wenchang Zhou and Jiqiang Lu	6
6-zk-SNARKs from Codes with Rank Metrics - Xuan-Thanh Do, Dang-Truong Mac and Quoc-Huy Vu	7
7-Zero-Knowledge Systems from MPC-in-the-Head and Oblivious Transfer - Cyprien Delpech de Saint Guilhem, Ehsan Ebrahimi and Barry van Leeuwen	8
8-ZK-for-Z2K MPC-in-the-Head Zero-Knowledge Proofs for Z2k - Lennart Braun, Cyprien Delpech de Saint Guilhem, Robin Jadoul, Emmanuela Orsini, Nigel P. Smart and Titouan Tanguy	9
9- Efficient Secure Two Party ECDSA - Sermin Kocaman and Younes Talibi Alaou	10
10-Selective Delegation of Attributes in Mercurial Signature Credentials - Colin Putman and Keith M. Martin	11
11-Middle-Products of Skew Polynomials and Learning with Errors - Andrew Mendelsohn and Cong Ling	12
12- Identity-Based Threshold Signatures from Isogenies- Shahla Atapoor	13
13-Dynamic Security Aspects of Onion Routing- Alessandro Melloni, Martijn Stam and Øyvind Ytrehus	14
14- Practical and Efficient FHE- Nigel Smart	15

An Upper-Bound on the Decoding Failure Probability of the LRPC Decoder

Étienne Burle and Ayoub Otmani

LITIS, University of Rouen Normandie, France
{Etienne.Burle,Ayoub.Otmani}@univ-rouen.fr

Abstract. Low Rank Parity Check (LRPC) codes form a class of rank-metric error-correcting codes that was purposely introduced to design public-key encryption schemes. An LRPC code is defined from a parity check matrix whose entries belong to a relatively low dimensional vector subspace of a large finite field. This particular algebraic feature can then be exploited to correct with high probability rank errors when the parameters are appropriately chosen. In this paper, we present theoretical upper-bounds on the probability that the LRPC decoding algorithm fails.

Keywords: Rank metric · Decoding problem · LRPC code · Homogeneous matrix

Coset leaders of the first order Reed-Muller codes in the classes of Niho functions and Threshold functions *

Claude Carlet[†], Serge Feukoua[‡] and Ana Sălăgean[§]

Abstract

The notion of coset leader has applications in coding theory and cryptography. It has been studied in several papers. In this paper, we extend a recent study, made on the coset leaders of the first order Reed-Muller codes, to two classes of Boolean functions which have played an important role in diverse domains of Boolean functions, and whose study was missing in this context. We characterize the coset leaders that belong to the classes of Niho functions and threshold functions (this second class being a generalization of the class of majority functions).

KEYWORDS: Boolean functions, coset leader, Walsh transform.

Revisiting Nearest-Neighbor-Based Information Set Decoding

Andre Esser

Technology Innovation Institute, UAE
andre.esser@tii.ae

Abstract. The syndrome decoding problem lies at the heart of code-based cryptographic constructions. Information Set Decoding (ISD) algorithms are commonly used to assess the security of these systems. The most efficient ISD algorithms rely heavily on nearest neighbor search techniques. However, the runtime result of the fastest known ISD algorithm by Both-May (PQCrypto '18) was recently challenged by Carrier et al. (Asiacrypt '22), which introduce themselves a new technique called RLPN decoding which yields improvements over ISD for codes with small rates $\frac{k}{n} \leq 0.3$.

In this work we first revisit the Both-May algorithm, by giving a clean exposition and a corrected analysis. In this context we confirm the result by Carrier et al. that the initial analysis is flawed and conclude with the same runtime exponent. Our work aims at fully substantiating the corrected runtime exponent by a detailed analysis. Furthermore, we show that the Both-May algorithm significantly improves on memory complexity over previous algorithms. Our main contribution is therefore to give the correct perspective on the significance of the Both-May algorithm and to clarify any remaining doubts on the corrected baseline.

Further, we outline a potential strategy for enhancing the Both-May algorithm by merging two of its subroutines, by introducing a fixed weight nearest neighbor variant. Although we do not obtain immediate improvements, the nearest neighbor variant has already found novel applications in recent research. This initiated study of algorithms to solve the fixed-weight variant could potentially lead to future improvements through our construction.

Keywords: representation technique - syndrome decoding - nearest neighbor search - code-based cryptography

Feistel Ciphers Based on A Single Primitive

Kento Tsuji and Tetsu Iwata

Nagoya University, Nagoya, Japan
tsuji.kento.y1@s.mail.nagoya-u.ac.jp,
tetsu.iwata@nagoya-u.jp

Abstract. We consider Feistel ciphers instantiated with tweakable block ciphers (TBCs) and ideal ciphers (ICs). The indistinguishability security of the TBC-based Feistel cipher is known, and the indifferntiability security of the IC-based Feistel cipher is also known, where independently keyed TBCs and independent ICs are assumed. In this paper, we analyze the security of a single-keyed TBC-based Feistel cipher and a single IC-based Feistel cipher. We characterize the security depending on the number of rounds. More precisely, we cover the case of contracting Feistel ciphers that have $d \geq 2$ lines, and the results on Feistel ciphers are obtained as a special case by setting $d = 2$. Our indistinguishability security analysis shows that it is provably secure with $d + 1$ rounds. Our indifferntiability result shows that, regardless of the number of rounds, it cannot be secure. Our attacks are a type of a slide attack, and we consider a structure that uses a round constant, which is a well-known counter measure against slide attacks. We show an indifferntiability attack for the case $d = 2$ and 3 rounds.

Keywords: Feistel cipher · Tweakable block cipher · Ideal cipher · Provable security

Rectangle Attacks on Reduced Versions of the FBC Block Cipher

Wenchang Zhou^{1,2,3} and Jiqiang Lu^{1,2,3(B)}

¹ School of Cyber Science and Technology, Beihang University, Beijing 100083, China

² State Key Laboratory of Cryptology, P. O. Box 5159, Beijing 100878, China

³ Hangzhou Innovation Institute, Beihang University, Hangzhou 310051, China
{wenchangzhou, lvjiqiang}@buaa.edu.cn

Abstract. The FBC block cipher is an award-winning algorithm of the recent Cryptographic Algorithm Design Competition in China, which has three versions: FBC128-128 with a 128-bit block size and a 128-bit key size, FBC128-256 with a 128-bit block size and a 256-bit key size, and FBC256 with a 256-bit block size and a 256-bit key size. The best previously published cryptanalysis results on FBC are an impossible differential attack on 13-round FBC128-128 and a boomerang attack on 13-round FBC128-256. In this paper, we exploit a 12-round rectangle distinguisher with probability 2^{-234} of FBC128 and a 16-round rectangle distinguisher with probability 2^{-448} of FBC256, and observe that preliminary satisfying ciphertext quartets can be efficiently filtered out by sorting plaintext pairs according to some nibble positions at the ciphertext side during key-recovery phase, and finally we mount rectangle attacks on 14-round FBC128-128, 15-round FBC128-256 and 19-round FBC256 to recover their respective user key. Our attacks break more rounds than any previously published attacks on FBC.

Keywords:

Cryptology – Block cipher – FBC – Rectangle attack.

zk-SNARKs from Codes with Rank Metrics

Xuan-Thanh Do¹, Dang-Truong Mac , and Quoc-Huy Vu²

¹ Institute of Cryptography Science and Technology, Vietnam

² Léonard de Vinci Pôle Universitaire, Research Center, Paris-La Défense, France

Abstract. Succinct non-interactive zero-knowledge arguments of knowledge (zk-SNARKs) are a type of non-interactive proof system enabling efficient privacy-preserving proofs of membership for NP languages. A great deal of works has studied candidate constructions that are secure against quantum attackers, which are based on either lattice assumptions, or post-quantum collision-resistant hash functions. In this paper, we propose a code-based zk-SNARK scheme, whose security is based on the rank support learning (RSL) problem, a variant of the random linear code decoding problem in the rank metric. Our construction follows the general framework of Gennaro *et al.* (CCS'18), which is based on square span programs (SSPs). Due to the fundamental differences between the hardness assumptions, our proof of security cannot apply the techniques from the lattice-based constructions, and indeed, it distinguishes itself by the use of techniques from coding theory. We also provide the scheme with a set of concrete parameters.

Keywords: Code-based Cryptography, Rank support learning problem, Square span programs, zk-SNARKs

Zero-Knowledge Systems from MPC-in-the-Head and Oblivious Transfer

Cyprien Delpech de Saint Guilhem¹[0000–0002–0147–2566],
Ehsan Ebrahimi²[0000–0001–6917–7734],
and Barry van Leeuwen¹[0000–0002–3792–4042]

¹ COSIC, KU Leuven, Leuven, Belgium,
cyprien.delpechdesaintguilhem@kuleuven.be
barry.vanleeuwen@kuleuven.be

² Department of Computer Science, University of Luxembourg, Luxembourg
eebrahimi.pqc@gmail.com

Abstract. Zero-knowledge proof or argument systems for generic NP statements (such as circuit satisfiability) have typically been instantiated with cryptographic commitment schemes; this implies that the security of the proof system (e.g., computational or statistical) depends on that of the chosen commitment scheme. The MPC-in-the-Head paradigm (Ishai et al., JoC 2009) uses the same approach to construct zero-knowledge systems from the simulated execution of secure multiparty computation protocols.

This paper presents a novel method to construct zero-knowledge protocols which takes advantage of the unique properties of MPC-in-the-Head and replaces commitments with an oblivious transfer protocol. The security of the new construction is proven in the Universal Composability framework of security and suitable choices of oblivious transfer protocols are discussed together with their implications on the security properties and computational efficiency of the zero-knowledge system.

Keywords: Zero-Knowledge · Oblivious Transfer · MPC-in-the-Head

ZK-for-Z₂K: MPC-in-the-Head Zero-Knowledge Proofs for Z₂^k

Lennart Braun¹, Cyprien Delpech de Saint Guilhem², Robin Jadoul², Emmanuela Orsini³, Nigel P. Smart^{2,4}, and Titouan Tanguy⁴

¹ Department of Computer Science, Aarhus University, Aarhus, Denmark,

² COSIC, KU Leuven, Leuven, Belgium,

³ Department of Computing Sciences, Bocconi University, Milan, Italy,

⁴ Zama. Inc, Paris, France.

braun@cs.au.dk, cyprien.delpechdesaintguilhem@kuleuven.be,
robin.jadoul@esat.kuleuven.be, emmanuela.orsini@unibocconi.it,
nigel.smart@kuleuven.be, titouan.tanguy@zama.ai

Abstract. In this work, we extend the MPC-in-the-Head framework, used in recent efficient zero-knowledge protocols, to work over the ring Z_2^k , which is the primary operating domain for modern CPUs. The proposed schemes are compatible with any threshold linear secret sharing scheme and draw inspiration from MPC protocols adapted for ring operations. Additionally, we explore various batching methodologies, leveraging Shamir’s secret sharing schemes and Galois ring extensions, and show the applicability of our approach in RAM program verification. Finally, we analyse different options for instantiating the resulting ZK scheme over rings and compare their communication costs.

Efficient Secure Two Party ECDSA

Sermin Kocaman^{1*} and Younes Talibi Alaou^{2**}

¹ Department of Cryptology, Institute of Applied Mathematics, METU, Ankara, Turkey

² Fabric Cryptography

sermin.cakin@gmail.com, talibialaouiyounes@gmail.com

Abstract. Distributing the Elliptic Curve Digital Signature Algorithm (ECDSA) has received increased attention in past years due to the wide range of applications that can benefit from this, particularly after the popularity that the blockchain technology has gained. Many schemes have been proposed in the literature to improve the efficiency of multi-party ECDSA. Most of these schemes either require heavy homomorphic encryption computation or multiple executions of a functionality that transforms Multiplicative shares to Additive shares (MtA). Xue et al. (CCS 2021) proposed a 2-party ECDSA protocol secure against malicious adversaries and only requires one execution of MtA, with an online phase that consists of only one party sending one field element to the other party with a computational overhead dominated by the verification step of the signature scheme. We propose a novel protocol, based on the assumption that the Computational Diffie-Hellman problem is hard, that offers the same online phase performance as the protocol of Xue et al., but improves the offline phase by reducing the computational cost by one elliptic curve multiplication and the communication cost by two field elements. To the best of our knowledge, our protocol offers the most efficient offline phase for a two-party ECDSA protocol with such an efficient online phase.

Keywords: ECDSA · Two-party Protocols · Threshold Signature

Selective Delegation of Attributes in Mercurial Signature Credentials

Colin Putman¹ and Keith M. Martin¹[0000–0001–7877–9075]

Royal Holloway, University of London, Egham, Surrey, TW200EX, UK
{Colin.Putman.2017,Keith.Martin}@rhul.ac.uk

Abstract. Anonymous credential schemes enable service providers to verify information that a credential holder willingly discloses, without needing any further personal data to corroborate that information, and without allowing the user to be tracked from one interaction to the next. Mercurial signatures are a novel class of anonymous credentials which show good promise as a simple and efficient construction without heavy reliance on zero-knowledge proofs. However, they still require significant development in order to achieve the functionality that most existing anonymous credential schemes provide. Encoding multiple attributes of the credential holder in such a way that they can be disclosed selectively with each use of the credential is often seen as a vital feature of anonymous credentials, and is one that mercurial signatures have not yet implemented. In this paper, we show a simple way to encode attributes in a mercurial signature credential and to regulate which attributes a credential holder can issue when delegating their credential to another user. We also extend the security model associated with mercurial signatures to account for the inclusion of attributes, and prove the security of our extension with respect to the original mercurial signature construction.

Keywords: Privacy · Anonymous credentials · Delegatable credentials · Mercurial signatures · Selective disclosure.

Middle-Products of Skew Polynomials and Learning with Errors

Cong Ling and Andrew Mendelsohn

Department of EEE, Imperial College London, London, SW7 2AZ, United Kingdom.

andrew.mendelsohn18@imperial.ac.uk

c.ling@imperial.ac.uk

Abstract. We extend the middle product to skew polynomials, which we use to define a skew middle-product Learning with Errors (LWE) variant. We also define a skew polynomial LWE problem, which we connect to Cyclic LWE (CLWE), a variant of LWE in cyclic division algebras. We then reduce a family of skew polynomial LWE problems to skew middle-product LWE, for a family which includes the structures found in CLWE. Finally, we give an encryption scheme and demonstrate its IND-CPA security, assuming the hardness of skew middle-product LWE.

Keywords: middle product · LWE · cyclic division algebras · skew polynomials

Identity-Based Threshold Signatures from Isogenies

Shahla Atapoor
COSIC, KU Leuven, Leuven, Belgium.

Abstract. The identity-based signature, initially introduced by Shamir plays a fundamental role in the domain of identity-based cryptography. It offers the capability to generate a signature on a message, allowing any user to verify the authenticity of the signature using the signer’s identifier information (e.g., an email address), instead of relying on a public key stored in a digital certificate. Another significant concept in practical applications is the threshold signature, which serves as a valuable tool for distributing the signing authority. The notion of an identity-based threshold signature scheme pertains to the distribution of a secret key associated with a specific identity among multiple entities, rather than depending on a master secret key generated by a public key generator. This approach enables a qualified group of participants to jointly engage in the signing process. In this paper, we present two identity-based threshold signature schemes based on isogenies, each of which addresses a different aspect of security. The first scheme prioritizes efficiency but offers security with abort, while the second scheme focuses on robustness. Both schemes ensure active security in the quantum random oracle model. To build these identity-based threshold signatures, we begin by modifying the identity-based signature scheme proposed by Shaw and Dutta [27], to accommodate the CSI-SharK signature scheme. Subsequently, we leverage the resulting identity-based signature and build two threshold schemes within the CSIDH (Commutative Super singular Isogeny Diffie-Hellman) framework. Our proposed identity based threshold signatures are designed based on CSI-SharK and can be easily adapted with minimal adjustments to function with CSI-FiSh.

Keywords: Identity-based signature · Identity-based threshold signature · Isogeny based cryptography · CSI-SharK · CSI-FiSh · CSIDH

Dynamic Security Aspects of Onion Routing

Alessandro Melloni 1, Martijn Stam 1, and Øyvind Ytrehus 1

Simula UiB, Bergen, Norway.
{alessandro,martijn,oyvindy}@simula.no

Abstract.

An *anonymous communication network (ACN)* is designed to protect the identities of two parties communicating through it, even if an adversary controls or observes parts of the network. Among the ACNs, Tor represents a practical trade-off between offering a reasonable level of anonymity and, simultaneously, an acceptable transmission delay. Due to its practical impact, there is abundant literature on the performance of Tor concerning both communication and security aspects. Recently, a static framework was suggested for evaluating and comparing, in a quantifiable way, the effect of different scenarios (attacks, defence mechanisms, and other protocol changes). Although a static model is useful, many scenarios involve parameters and stochastic variables that change or evolve over time, or that may be influenced by active and malicious adversaries. In this paper, we propose a *dynamic* framework for evaluating such scenarios. We identify several scenarios where this framework is applicable, and illustrate our framework by considering the *guard node* mechanism in Tor. We evaluate and compare variations on the guard node concept suggested in the literature with respect to relevant performance metrics and, using the framework, support our evaluation with a theoretical analysis.

Keywords: Anonymity · Onion Routing · Tor · Traffic Analysis

Practical and Efficient FHE-based MPC

Nigel P. Smart

¹ COSIC, KU Leuven, Leuven, Belgium.

² Zama Inc., Paris, France.
nigel.smart@kuleuven.be/nigel@zama.ai.

Abstract. We present a *reactive MPC* protocol built from FHE which is *robust* in the presence of active adversaries. In addition the protocol enables reduced bandwidth via means of transciphering, and also enables more expressive/efficient programs via means of a Declassify operation. All sub-components of the protocol can be efficiently realised using existing technology. We prove our protocol secure in the UC framework