SaTC: CORE: Small: Meta Coding and Applications in Cryptography

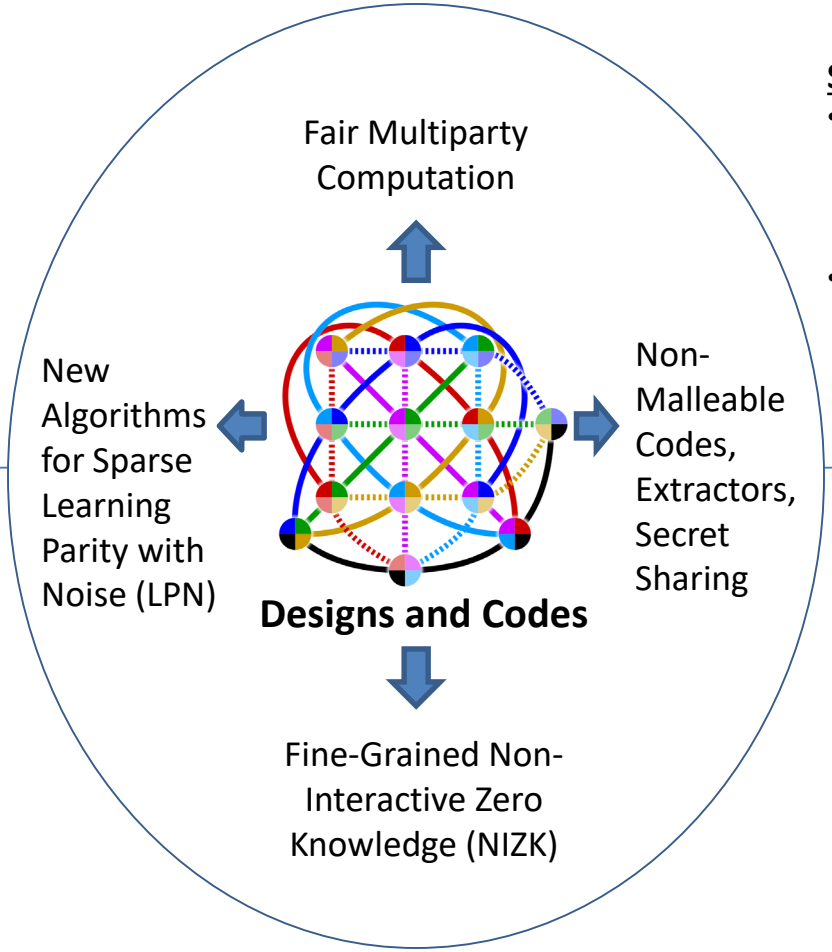
UNIVERSITY OF MARYLAND

Challenge:

- Identify and unify techniques from coding theory and combinatorial designs
- Find applications of those techniques in cryptography

Solution:

- Applied the designs of Nisan and Wigderson to (1 non-uniform cryptographic reductions and (2) learning problems.
- Asymptotic improvement in the exponent for algorithms for sparse LPN in certain regimes.
- First results on Fair MPC without honest majority and with non-threshold access structures.
- First construction of fine-grained NIZK.
- First construction of non-malleable codes, extractors, secret sharing for bounded polynomial tampering without cryptographic assumptions (only worst case assumptions).



Scientific Impact:

- Introduced new research problems such as Fair MPC without honest majority and non-threshold access structures.
- Introduced new combinatorial techniques to the cryptographic setting.

Broader Impact and Broader Participation:

- New insight into hardness of post-quantum assumptions such as Learning Parity with Noise (LPN)
- Graduate student training and professional development, including one female PhD student

Project Info
Award Number: CNS #1933033
Institution: University of Maryland
PI: Dana Dachman-Soled (danadach@umd.edu)