CMU workshop on cryptography

Encrypted Computation

- **New Techniques for Preimage Sampling: Improved NIZKs and More from LWE**
- **Multi-Authority Functional Encryption with Bounded Collusions from Standard Assumptions**
- **Circuit ABE with poly(depth, λ)-sized Ciphertexts and Keys from Lattices**
- **Efficient Laconic Cryptography from Learning With Errors**
- **Attribute-Based Signatures for Circuits with Optimal Parameter Size from Standard Assumptions**

Foundations

- Counting Unpredictable Bits: A Simple PRG from One-way Functions
- A New Approach for LPN-based Pseudorandom Functions: Low-Depth and Key-Homomorphic
- Low-Complexity Weak Pseudorandom Functions in AC0[MOD2]
- Constructing a Pseudorandom Generator Requires an Almost Linear Number of Calls
- Structural Lower Bounds on Black-Box Constructions of Pseudorandom Functions
- On One-way Functions and the Worst-case Hardness of Time-Bounded Kolmogorov Complexity
- Kolmogorov Comes to Cryptomania: On Interactive Kolmogorov Complexity and Key-Agreement
- One-Way Functions and Zero Knowledge (this note provides a simpler proof)
- Instance Compression, Revisited

Proof System

- Public-Coin, Complexity-Preserving, Succinct Arguments of Knowledge for NP from Collision-Resistance
- Fiat-Shamir Transformation of Multi-Round Interactive Proofs
- Universally Composable Sigma-protocols in the Global Random-Oracle Model
- Fully Succinct Batch Arguments for NP from Indistinguishability Obfuscation
- SNARGs and PPAD Hardness from the Decisional Diffie-Hellman Assumption
- On Valiant's Conjecture: Impossibility of Incrementally Verifiable Computation from Random Oracles

FO Transform

- Failing gracefully: Decryption failures and the Fujisaki-Okamoto transform

Secure Messaging

- Forward-Secure Encryption with Fast Forwarding
- On the Worst-Case Inefficiency of CGKA

NIST Candidates (Concrete Construction)

- Kyber (KEM, MLWE), ★★
  https://eprint.iacr.org/2017/634.pdf
  https://pq-crystals.org/kyber/resources.shtml
- Saber (KEM, MLWR), ★★
  https://eprint.iacr.org/2018/230.pdf
  https://www.esat.kuleuven.be/cosic/pqcrypto/saber/resources.html

- NTRU (KEM, NTRU assumption), ★★★
  https://ntru.org/f/ntrukem-20170828.pdf
  https://ntru.org/resources.shtml
- NTRU-Prime (KEM, NTRU assumption, 2nd round) ★★★
  https://ntruprime.cr.yp.to/ntruprime-20170816.pdf

- Dilithium (Signature, Fiat-Shamir, MLWE), ★★★
  https://tches.iacr.org/index.php/TCHES/article/view/839/791

- Falcon (Signature, Hash&Sign, NTRU assumption) ★★★★
  https://falcon-sign.info/falcon.pdf
  https://falcon-sign.info/

Verifiable Delay Functions

- **Verifiable delay functions**
  https://eprint.iacr.org/2018/601.pdf

- **Simple Verifiable Delay Functions**
  https://eprint.iacr.org/2018/627.pdf

- **Efficient verifiable delay functions**
  https://eprint.iacr.org/2018/623.pdf

- **Continuous verifiable delay functions**
  https://eprint.iacr.org/2019/619.pdf

- **Verifiable Delay Functions from Supersingular Isogenies and Pairings**
  https://eprint.iacr.org/2019/166.pdf

- **On the security of time-lock puzzles and timed commitments**
  https://eprint.iacr.org/2020/730.pdf

- **Homomorphic time-lock puzzles and applications**
  https://eprint.iacr.org/2019/635.pdf

- **TARDIS: a foundation of time-lock puzzles in UC**
  https://eprint.iacr.org/2020/537.pdf

- **Non-malleable time-lock puzzles and applications**
  https://eprint.iacr.org/2020/779.pdf

- **Leveraging linear decryption: Rate-1 fully-homomorphic encryption and time-lock puzzles**
  https://eprint.iacr.org/2019/720.pdf

Others

- **On the Worst-Case Inefficiency of CGKA**
  https://eprint.iacr.org/2022/1237.pdf
  https://iacr.org/submit/files/slides/2022/tcc/tcc2022/86/slides.pdf

- **Adaptive Multiparty NIKE**
  https://eprint.iacr.org/2022/1324.pdf
  https://iacr.org/submit/files/slides/2022/tcc/tcc2022/51/slides.pdf

- **Towards Tight Adaptive Security of Non-Interactive Key Exchange**
  https://www.youtube.com/watch?v=WK3TAuxHajQ
  https://eprint.iacr.org/2021/1219.pdf

- **Grafting Key Trees: Efficient Key Management for Overlapping Groups**
  https://www.youtube.com/watch?v=kjeDELfPJFg
  https://eprint.iacr.org/2021/1158

- **Continuous Group Key Agreement with Active Security**
  https://www.youtube.com/watch?v=cxrm9iBDCHA
  https://eprint.iacr.org/2020/752.pdf

- **Security analysis of SPAKE2+**
  https://www.youtube.com/watch?v=IAUhBRr8Rgc
  https://eprint.iacr.org/2020/313.pdf

- **Authenticated Key Exchange and Signatures with Tight Security in the Standard Model**
  https://www.youtube.com/watch?v=H_2hiCO_Dow
  https://iacr.org/submit/files/slides/2021/crypto/crypto2021/398/slides.pdf
  https://eprint.iacr.org/2021/863.pdf

- **KHAPE: Asymmetric PAKE from Key-Hiding Key Exchange**
  https://www.youtube.com/watch?v=qAVEaNnFlNU&feature=youtu.be
  https://iacr.org/submit/files/slides/2021/crypto/crypto2021/102/slides.pdf

https://eprint.iacr.org/2021/873.pdf

- **Universally Composable Relaxed Password Authenticated Key Exchange**
  https://www.youtube.com/watch?v=aYuUN5XXzLk
  https://link.springer.com/chapter/10.1007/978-3-030-56784-2_10