Building blocks for Threshold FHE

Andreea Alexandru
aalexandru@dualitytech.com

A. Al Badawi, N. Genise, D. Micciancio, Y. Polyakov,
S. Ramanathapuram Vancheeswaran, V. Vaikuntanathan

MPTS 2023: NIST Workshop on Multi-Party Threshold Schemes 28 Sep 2023
Quick overview of Fully Homomorphic Encryption (FHE)

- **Correctness**: \( \text{Dec}(\text{Enc}(x)) = (\approx) x \); \( \text{Dec}(\text{Eval}(f, \text{Enc}(x))) = (\approx) f(x) \)

- **Complex algorithms**: (functional) bootstrapping

- **Compactness + efficiency**: key/modulus switching, RNS representation, relinearization

- **Lattice-based schemes**: [Gen09, Bra12, FV12, GHS13, BGV14, DM15, CGGI16, CKKS17]

- **Typical single-server use case**
  - Trusted client generates the keys, encrypts and decrypts
  - Server might or might not operate with secrets
Quick overview of Threshold FHE (ThFHE)

- Multiple types of multi-party FHE
  - Multi-key FHE, Threshold FHE, Hybrid

- Goal: multiple parties emulate both the client and the server

- [BD10, AJL+12, LATV12, BGG+18, CCS19, SPT+21, MBH23, CCK23]

- Typical threshold FHE use case: each party has some local secret input
  - Parties **jointly** generate the secret and public keys
  - Each party evaluates the function (can be both **non-interactive** and **interactive**)
  - Parties **jointly** decrypt the result
FHE -> Threshold FHE

1. Key generation
2. Encryption
3. Evaluation
4. Decryption

1. Threshold key generation
2. Encryption
3. (Threshold) Evaluation
4. Threshold decryption

Static vs Adaptive Corruptions
Game- vs Simulation-based Definition

Trusted vs Untrusted Setup
Synchronous vs Asynchronous Communication

Honest vs Dishonest Majority
Pre-Q vs PQ resilience

Passive vs Active Security

Andreea Alexandru      aalexandru@dualitytech.com
Background: Security notions for PKE

- IND-CPA: encryption oracle access
- IND-CCA1: a priori decryption oracle access or “lunchtime attack”
- IND-CCA2: decryption oracle access
Security notions for TPKE

- The adversary has access to partial decryptions
- IND-TCPA, IND-TCCA [FPS01]: encryption + partial decryption oracle access, + decryption oracle access
- Smudging/Noise flooding/Sanitization [DS16, MW16]
- Threshold PKE: threshold key gen + threshold decryption
  - **Not trivial** to thresholdize existing lattice-based PKE schemes [BGGK17, BGG+18, CS19, KLO+19, DLN+21, CCMS21, CHI+21, BTT22, ASY22, GKS23]
  - Issues: secret sharing of key, growth of parameters, complex algorithms, transforms, etc.
Is TPKE a building block for ThFHE?

Yes... and no.
Evaluation brings new challenges!
Background: “Passive” security notions for FHE

- IND-CPA': encryption + evaluation oracle access (careful in the modular approach)

- IND-CPA\textsuperscript{D} [LM21, LMSS22]: oracle access to “encrypt-evaluate-decrypt”

- Circuit privacy [Gen09, OPCPC14, BdPMW16, KS23]: all ciphertexts have the same distribution

- funcCPA [AV21, AGHV22]: oracle access for “decrypt-evaluate-encrypt”
Standardizing passive ThFHE

- Security of threshold PKE does not automatically imply security of threshold FHE
- IND-TCPA’ [BS23, KS23]: encryption + evaluation + partial decryption oracle access
- Real/Ideal functionality [DPSZ12]

Gadgets & building blocks

- Passive security definitions for ThFHE: IND-TCPA’, passive MPC, (thresholdized?) funcCPA
- Noise flooding/sanitization/smudging
- Cryptographic closeness: statistical distance [AJL+12], bit-security distance [MW18, LMSS22], Rényi divergence [BLRL+18, BS23, CSS+23]
More protocol-gadgets for passive ThFHE

- Key generation
  - Secret sharing schemes

- Interactive masked decryption
  - => Interactive bootstrapping/scheme switching [CLO+13, SPT+21, MBH23, GGP+23]
  - Useful to make evaluation more efficient and to translate to other cryptographic schemes
What about active security?

Slower, but on its way?
Background: Active security notions for (Th)FHE

- **IND-CCA1**: a priori decryption oracle access
  - Practical FHE schemes require encryptions (of functions) of the secret key -> incompatible with the decryption oracle; other constructions in [CRRV17]

- **IND-CCA2**: decryption oracle access
  - No HE can satisfy this

- **Targeted malleability** [PR08, BSW11]: allow decryptions of some function families

- **IND-CVA** [LMNV10, CGG16, CCCM22, CCCM23]: oracle access for plaintext validity

- **Malicious security** [VKH23]: correctness, completeness, soundness

- **IND-TCPA + threshold verifiability + decryption simulatability** [BGG+18, ABGS22]

- **Real/ideal functionality with active security** [DDE+23, Sma23]
Standardizing active ThFHE

- Threshold additively/somewhat HE, FHE with active security [DKL+13, KPR18, RST+22, ABGS22, CMS+23, DDE+23]

Gadgets & building blocks

- Active security definition for ThFHE
- Honest majority to help with verifiable computation
- Non interactive zero-knowledge proofs (PQ) / Homomorphic signatures
References


References


References


References


References


Thank you!

Andreea Alexandru
aalexandru@dualitytech.com