Thresholding Symmetric-Key Primitives Based on General-Purpose Actively Secure MPC

Xiao Wang (Northwestern University)

MPTS 2023: NIST Workshop on Multi-party Threshold Schemes 2023 Sep 26th 2023

Team

Hongrui Cui (Shanghai Jiao Tong University)
Chun Guo (Shandong University)
David Heath (UIUC)
Jonathan Katz (UMD)
Vlad Kolesnikov (Gatech)
Samuel Ranellucci (Coinbase)
Mike Rosulek (Oregon State University)
Lance Roy (Aarhus University)
Xiao Wang (Northwestern University)
Chenkai Weng (Northwestern University)
Kang Yang (State Key Laboratory of Cryptology)
Yu Yu (Shanghai Jiao Tong University)

Our Goal

Subcategory: Type	(Sub)subcategory #: Family of primitives	Some [Primitives] and/or {Threshold Modes}
C1.4: Symmetric	C1.4.1: AES (en/de)cipher	[encipher, decipher]
	C1.4.2: KDM/KC (for 2KE)	[Hash, CMAC, HMAC, KMAC]

- With support of all I/O interfaces
  - {NSS, SSI, SSO, SSIO}
  -
- With support of all primitives
  - AES, SHA[23], [CHK]MAC, etc
- With possibility to support C2.4

  – C2.4, for symmetric-key primitives (e.g., TF enciphering/deciphering), and hashing-related primitives for key derivation and key confirmation;

Our Solution

Based on generic multi-party computation protocols for Boolean circuits!

Pros:

- Only need to handle one protocol and one implementation
- Usable in other applications

Cons: May not be as efficient as customized protocols

- But the gap is small: most symmetric-key primitives have little structure for improvement

Our Philosophy

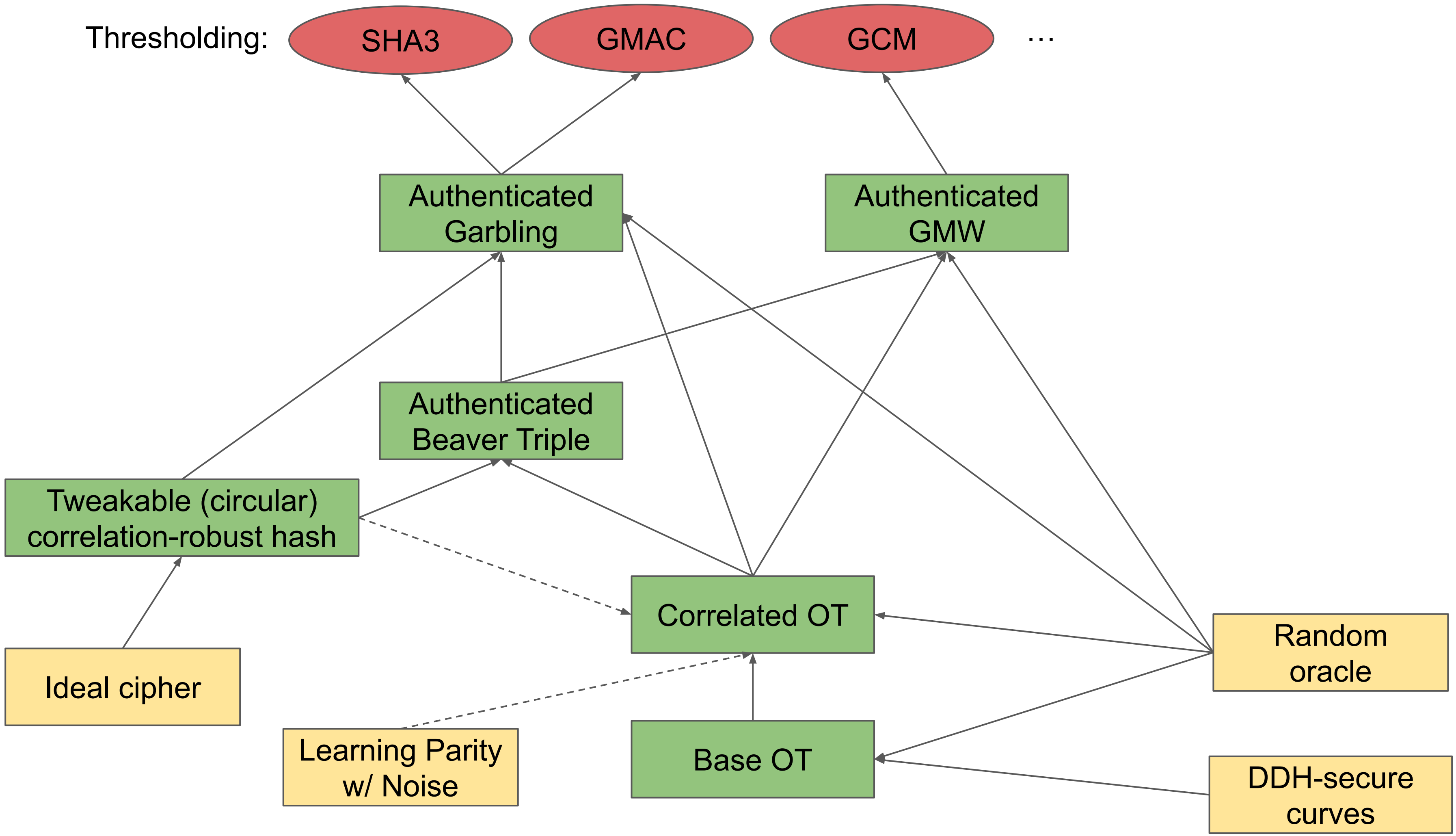
As fast as possible with high security confidence.

High security confidence:

- Active security in the universal composability model
- Tolerate a static corruption of *n-1* parties out of *n* parties.
- Concrete security
- Conservative assumptions

Two solutions

- A solution using only NIST-standardized primitives
  - E.g, AES as ideal cipher, SHA3 as random oracle, and NIST-approved curves.
- A (more efficient) solution using primitives close to what NIST already standardized


Thresholding:
SHA3
GMAC
GCM
...
Authenticated Garbling
Authenticated GMW
Authenticated Beaver Triple
Tweakable (circular) correlation-robust hash
Correlated OT
Random oracle
Ideal cipher
Learning Parity w/ Noise
Base OT
DDH-secure curves

Tweakable (circular) correlation-robust hash

- Use of Fixed-key AES by Bellare et al. [SP:BHKR13], and then by Zahur et al. [EC:ZahRosEva16] for garbling
    - Then, a lot of unprincipled used
- Modular proof by Guo et al. [SP:GKWY20]
    - Still suffer from birthday bound
- Near optimal concrete security by Guo et al. [C:GKWWY20]

Correlated OT

- [C:IKNP03] is the most widely used correlated OT with passive security
  - [C:KelOrsSch15] is the most widely used COT with active security

- Silent OT [C:BCGIKS19, CCS:BCGIKRS19, CCS:SGRR19, CCS:YWLZW20, …]
  - All based on some variations of Learning Partiy w/ Noise
  - Very small communication, moderate computation

- SoftSpokenOT [C:Roy22]
  - No LPN assumption, more rigours analysis of consistency check
  - Smaller communication in trade of more AES-like computation

Authenticated Beaver Triples

Pairwise IT-MAC on “normal” Boolean Beaver Triples

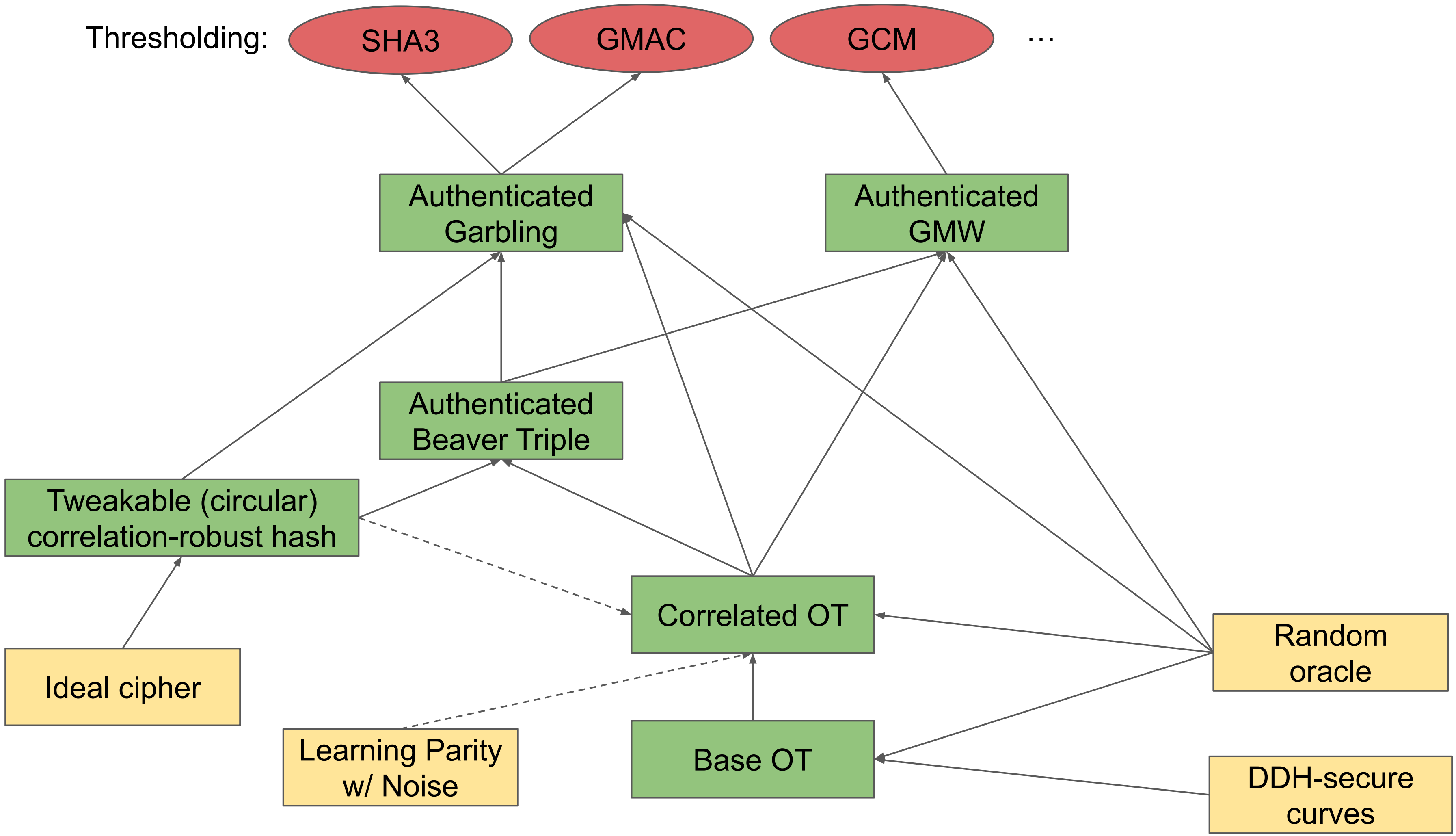
- [C:NNOB12] – Concept and first construction
- [AC:FKOS15], [JC:BLNNOOSS21] – Improved efficiency, two layers of bucketing
- [CCS:WanRanKat17], [CCS:YanWanZha20] — Improved efficiency, one layers of bucketing, w/ a row of GC-like table

Authenticated Garbling

- [CCS:WanRanKat17] – Original Protocol
  - Concurrent to the multi-party extension of WRK: [AC:HazSchSor17]

- [C:KRRW, CCS:YanWanZha20] — Improved online and offline
  - Online can be as small as a half-gate + O(1)
  - Offline works with “leaky” COTs

- [C:DLIO22, EC:CWYY23]
  - Rely on single-sided secure authenticated triples and cheap COT/VOLEs
  - Nearly optimal in communication in trade of high computation


Thresholding:
SHA3
GMAC
GCM
…
Authenticated Garbling
Authenticated GMW
Authenticated Beaver Triple
Tweakable (circular) correlation-robust hash
Correlated OT
Random oracle
Ideal cipher
Learning Parity w/ Noise
Base OT
DDH-secure curves

Planned Submission

Protocols

- Authenticated garbling
- Authenticated GMW “TinyOT”

Gadgets:

- Tweakable robust hash
- Correlated OT
- Garbling scheme
- Authenticated triples