Collusion-Tolerable Privacy-Preserving Sum and Product Calculation without Secure Channel

- previous work:
  - require secure pair-wise channels: both HE & SMC, request keys via secure channel.
  - high complexity: SMC & fully HE
- this paper
  - reduce the complexity to linear time
  - insecure channels
  - tolerate k passive adversaries

Related Work

- Castelluccia et al., HE scheme:
  - provable secure & efficient
  - modular addition, good for nodes in WSN
- Sheikt et al., k-secure sum protocol
  - segments data
  - significantly reduced the prob. of data leakage
- He et al., SMART, similar to above
  - segments data into n slices, distributes $n-1$ slices via secure channel
  - only sum
  - $O(n)$ complexity communication overhead
- Shi et al., similar to our solution
  - periodically upload encrypted data
  - brute-force search or Pollard's λ method, so **restricted**
- Our scheme
  - no trusted aggregator
  - insecure channels
  - segments k data, constant communication overhead
  - based on DDH assumption
  - novel efficient protocols

System Model & Achieving & Security Analysis

- One Aggregator Model & Participants Only Model
- CDH, DDH & CDH-Security
- Lemma 4.1 & 2: segments $O(\ln k)$ slices
- (more details in paper)

Complexity

each participant sends m ciphertexts to the aggregator:

- One Aggregator Model

Aggregator	Computation	Communication
Product	O(mn)	O(mn|p|)
Sum	O(m)	O(m|p|)
Per Participant	Computation	Communication
Setup(Product)	O(1)	O(|p|)
Encrypt(Product)	O(m)	O(m|p|)
Setup(Sum)	O(1)	O(|p|)
Encrypt(Sum)	O(1)	O(|p|)

- Participants Only Model

Per Participant	Computation	Communication
Setup(Prod)	O(1)	O(|p|)
Encrypt(Prod)	O(m)	O(mn|p|)
Product(Prod)	O(mn)	O(mn|p|)
Setup(Sum)	O(1)	O(|p|)
Encrypt(Sum)	O(1)	O(m|p|)
Sum(Sum)	O(m)	O(m|p|)

- Compared with Naehrig et al.'s work, One of main contributions: high speed while security level is still acceptable