Privacy–friendly Aggregation for the Smart-grid

Klaus Kursawe, George Danezis, and Markulf Kohlweiss

Ting-Wen(Benson) Chen

Content

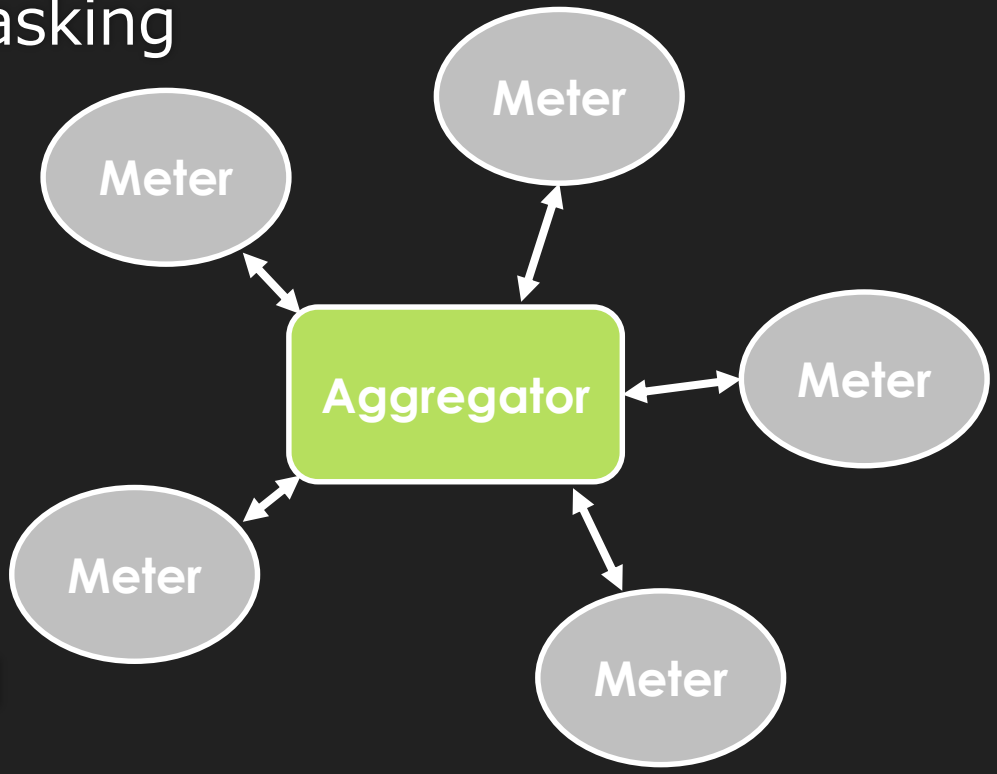
- Introduction
- Basic Protocol Types
  - Aggregation / Comparison
- Concrete Protocols
  - Interactive / DH Key-Exchange based
  - DH and Bilinear-map based / Low-overhead
- Comparison
- Conclusion

Introduction

- Why Aggregation?
  - **Privacy Concern** (personal data leakage)
  - Security Concern (fraud)
  - Safety Concern (leakage of gas)
  - Forecasting
  - …
- The meter here can also from the system of water or gas …

Introduction

- Consumption($c_{i,j}$) Masking
  - i: round, j: meter
- Masking values should cancel out after aggregation
- Should be encrypted



Basic Protocol Types

- Aggregation Protocol
  - Blinded value: $x_{i,j} + c_{i,j}$
  - Result = $\Sigma(c_{i,j})$; $\Sigma(x_{i,j}) = 0$
- Comparison Protocol
  - Blinded value: $g_i^{x_j + c_{i,j}}$
  - Result = $g_i^{\sum c_{i,j}}$, $g_i \in$ Diffie–Hellman group $\mathbb{G}$
  - Compare the result and its guess $g_i^{c_a}$
- Masking value: $x_{i,j}$

Concrete Protocols

- Interactive Protocol
  - Each user j have private key (X_j) and public key (Pub_j)
  - Choose p leaders from n users: $l_1, \dots, l_p$
  - Everyone generates p shares: $s_{i,1}, \dots, s_{i,p}$
  - After receiving the shares(encrypted), leaders can compute their own share such that the sum of these shares is zero and replace the original one
  - The main share s_j for user j is the sum of all his shares
  - Aggregation or Comparison Protocol

Concrete Protocols

- Diffie-Hellman Key-Exchange Based Protocol
  - Each meter j has its own secret key X_j
  - In each round i, it will have a generator of $\mathbb{G}$ $g_i = \mathrm{H}(i)$, and also each meter j has its public key $Pub_{i,j} = g_i^{X_j}$
  - $g_i^{x_j} = \prod_{k \neq j} Pub_{i,k}^{(-1)^{k<j} \cdot X_j}$
  - $\sum_j x_j = 0$
  - Only Comparison Protocol

Concrete Protocols

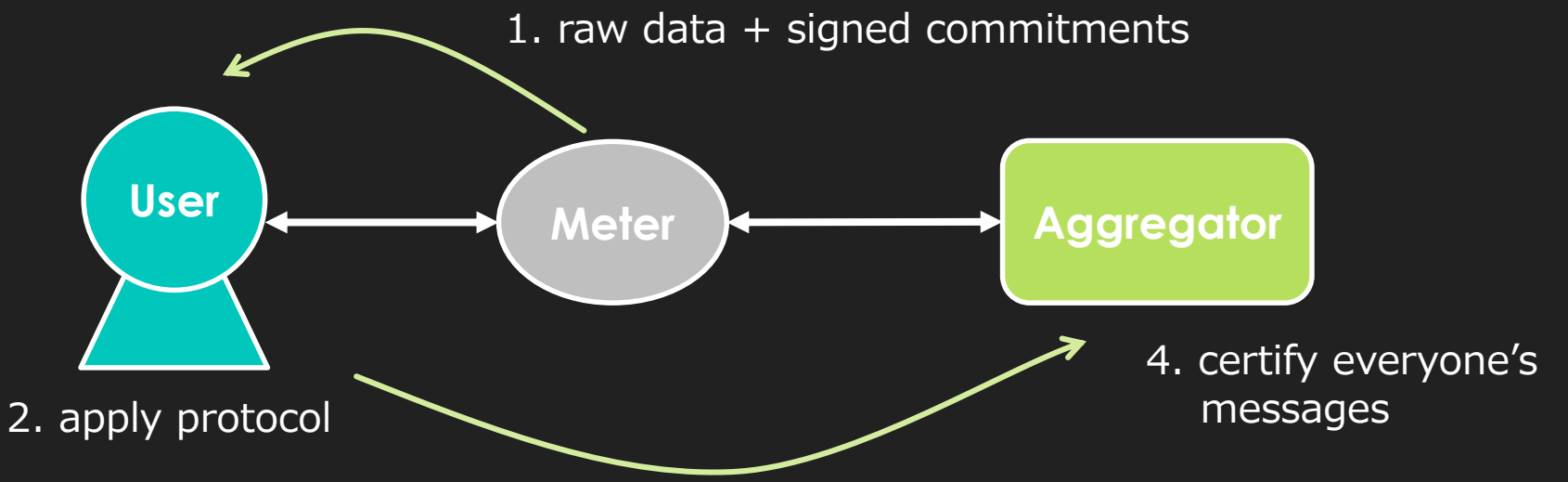
- Diffie-Hellman and Bilinear-map Based Protocol
  - Similar to the previous one but only need one public key (Pub_j) for each mdeter: $Pub_j = \hat{g}_0{}^{X_j}$
  - Bi-linear function $e(\mathbb{G}_1, \mathbb{G}_2) \rightarrow \mathbb{G}_T$
  - $g_i{}^{x_j} = (\prod_{k \neq j} e(Pub_k, \hat{g}_i)^{(-1)^{k<j}})^{X_j}$
  - $\hat{g}_0$: generator of $\mathbb{G}_1$; $\hat{g}_i = H(i),\ H(\{0,1\}^*) \rightarrow \mathbb{G}_2$
  - Also only Comparison Protocol

Concrete Protocols

- Low-overhead Protocol
  - Each pair of meter has their shared key $K_{j,k} = H\left(Pub_k{}^{X_j}\right)$,where $Pub_k = g^{X_k}$, $H(\{0,1\}^*) \rightarrow \mathbb{G}$, g: generator of $\mathbb{G}$
  - $x_{i,j} = \sum_{k \neq j} (-1)^{k<j} H(K_{j,k} \,||\, i)$
  - Aggregation or Comparison Protocol

Comparison

- Cryptographic Verifiability
  - Transmit data with commitments and certifications



Comparison

- Computation & Communication Overheads

	Initialization	Communication	Computation
Interactive (agg)	$O(N^2) \cdot PK$	$O(N \cdot p) \cdot \mathbb{Z}_q$	$O(p) \cdot \mathsf{Enc}$
Interactive (comp)	$O(N^2) \cdot PK$ $+O(N \cdot p) \cdot \mathbb{Z}_q$	$O(N) \cdot \mathbb{G}$	$O(1) \cdot E$
DH	$O(N^2) \cdot \mathbb{G}$	$O(N^2) \cdot \mathbb{G}$	$O(N) \cdot M + O(1) \cdot E$
Pairing	$O(N^2) \cdot \mathbb{G}$	$O(N) \cdot \mathbb{G}$	$O(N) \cdot P + O(1) \cdot E$
Low-overhead (agg)	$O(N^2) \cdot \mathbb{G}$	$O(N) \cdot \mathbb{Z}_{2^{32}}$	$O(N) \cdot H$
GC [4]	$O(N^2) \cdot PK$	$O(N^2) \cdot \mathbb{Z}_{n^2}$	$O(N) \cdot \mathsf{Enc} + O(1) \cdot \mathsf{Dec}$

Table 1. Performance comparison: PK.. size of public keys, $|\mathbb{Z}_x|$, $\mathbb{G}$.. size of algebraic group, Enc, Dec, E, M, H.. cost of encryption, decryption, exponentiation, multiplication, or hash function evaluation respectively.

Comparison

- Availability
  - Critical parts → inside meter
- Privacy
  - Passive attackers
  - Active attackers
- Forward Secrecy
  - Interactive and DH based protocol

Conclusion

Questions?

anyone

Thank you!