**Privacy-preserving Federated Learning based on Multi-key Homomorphic Encryption**

**Jing Ma, Si-Ahmed Naas, Stephan Sigg, Xixiang Lyu**

**Aalto University, Xidian University**

---

### Introduction

**Motivation:** Federated learning (FL) has the problem of privacy leakage as the model updates contain private information. Homomorphic encryption (HE) can be applied in federated learning to protect the model updates and conduct the homomorphic aggregation operation of the model.

---

### Framework

**xMK-CKKS**
- Key generation: $u_i$ selects secret key $s_i$ and computes public key $b_i = -s_i \cdot a + e_i (mod\ q)$
- Aggregated public key: $b = \sum b_i = \sum (-s_i \cdot a) + \sum e_i (mod\ q)$
- Encryption: $c_t = (c_{t_1}, c_{t_2}) = (v^k \cdot b + m + e_{t_1} \cdot v^d \cdot a + e_{t_2}) (mod\ q)$

**Privacy-preserving federated learning scheme based on xMK-CKKS**
- 1. Train locally for multiple epochs.
- 2. Encrypt current model weights $w_i$ as $(c_{w_1}, c_{w_2})$.
- 3. Add all encrypted weights to get an encrypted sum $C_{sum} = (C_{sum_1}, C_{sum_2})$.
- 4. Decrypt and compute the averaged model weights as $w_{avg}$.
- Server computes $c_{sum_1} = \sum_{i=1}^{n} s_i \cdot c_{w_1}$ and $c_{avg_1} = \sum_{i=1}^{n} s_i \cdot c_{w_2}$.

---

### Evaluation

**Setting:** Scenario: Elderly-fall detection  
**Dataset:** UP-Fall detection dataset
**Model:** Classification of five types of falls. Training optimizer: Adam optimizer at a learning rate of 0.01 with 20 and 40 local epochs in one aggregation round

---

### Conclusion

- **xMK-CKKS** achieves higher security and simpler operations than MK-CKKS, which is more suitable for federated learning scenarios.
- The privacy-preserving federated learning scheme based on xMK-CKKS guarantees confidentiality of model. This scheme is robust against attacks from the participants and also against collusion attacks between $k + N - 1$ participants and the server.
- Evaluation results show significant reduction in computational load and reasonable energy consumption while maintaining the accuracy.

---

Contact to us: jing.ma@aalto.fi