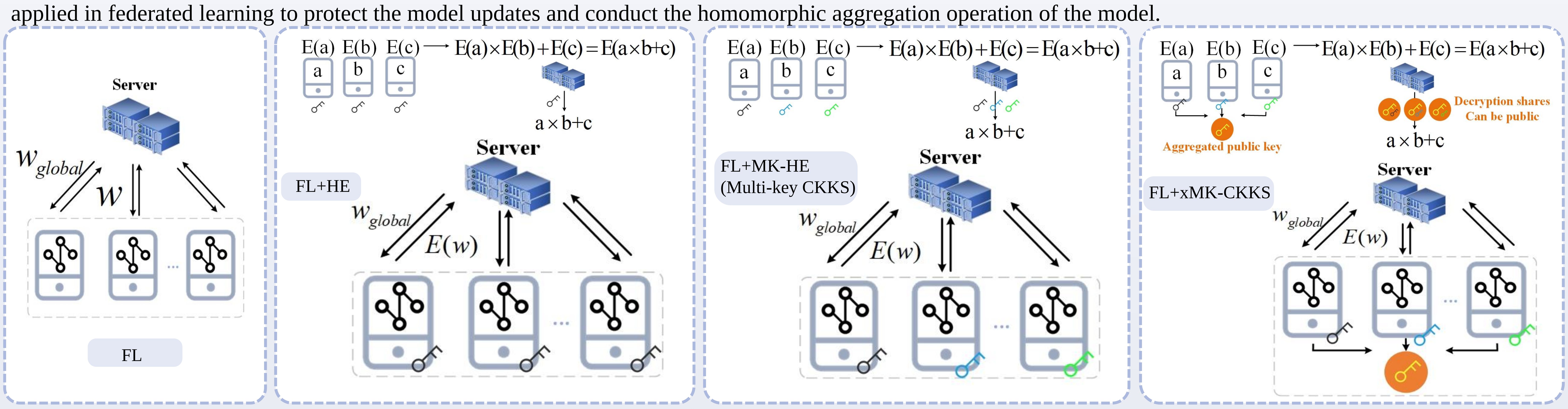
Privacy-preserving Federated Learning based on Multi-key Homomorphic Encryption

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.



1) We improve xMK-CKKS by setting an aggregated public key which is the sum of individual public key. Decryption requires information of secret keys and aggregated cipheretexts from all participants, thus has no threat to individual ciphertexts

2) Our privacy-preserving multi-key federated learning guarantees confidentiality of model updates in the honest-but-curious setting. It is robust also against collusion attacks between k<N-1 participants and the server.

3) We evaluate the scheme on Jetson Nano IoT devices and against the state-of-the-art. Results show significant reduction in computational load and reasonable energy consumption is achieved while maintaining accuracy.

Framework

xMK-CKKS

Key generation: u_i selects secret key s_i and computes public key $b_i = -s_i \cdot a + e_i (\mathrm{mod}\, q)$

Aggregated public key: $\tilde{b} = \sum_{i=1}^{N} b_i = \sum_{i=1}^{N} (-s_i \cdot a) + \sum_{i=1}^{N} e_i (\mathrm{mod}\, q)$

Encryption: $ct_i = (c_0^{d_i}, c_1^{d_i}) = (v^{d_i} \cdot \tilde{b} + m_i + e_0^{d_i}, v^{d_i} \cdot a + e_1^{d_i})(\mathrm{mod}\, q)$

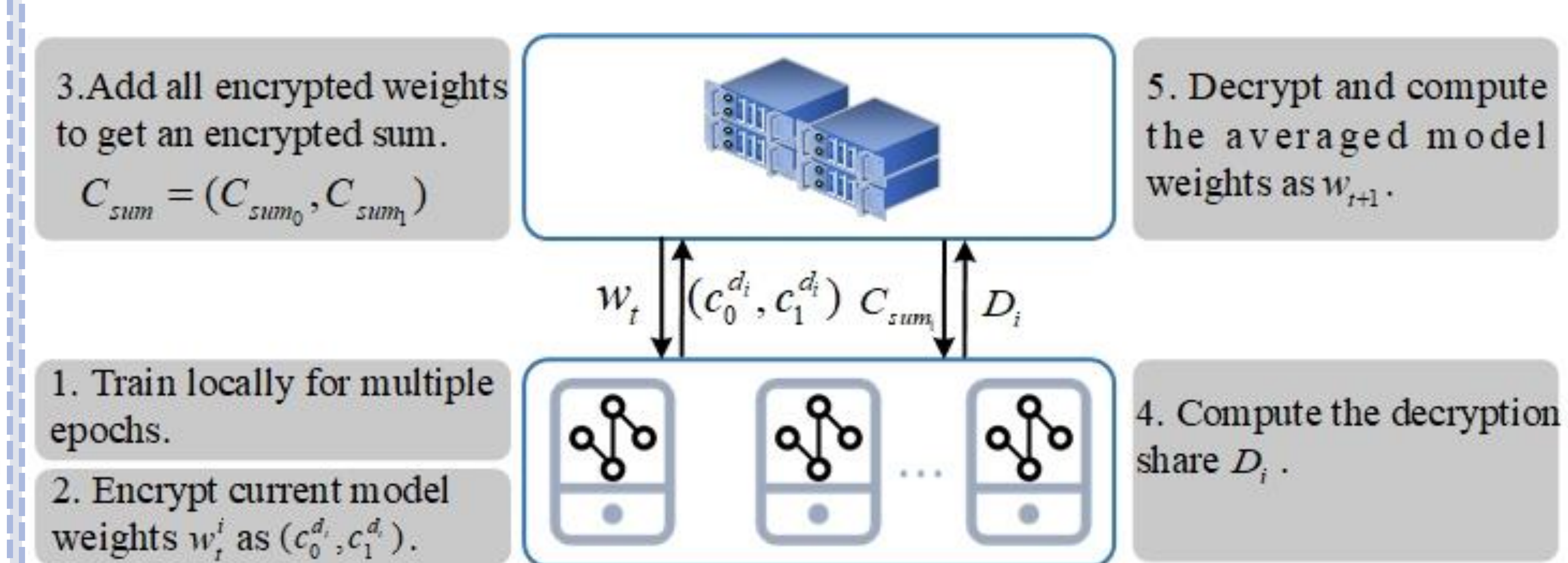
Cipher sum: $C_{sum} = \sum_{i=1}^{N} ct_i \triangleq (C_{sum_0}, C_{sum_1}) = \left(\sum_{i=1}^{N} c_0^{d_i}, \sum_{i=1}^{N} c_1^{d_i}\right)$

Decryption of cipher sum:

u_i computes decryption share: $D_i = s_i \cdot C_{sum_1} + e_i^* (\mathrm{mod}\, q) = s_i \cdot \sum_{i=1}^{N} (v^{d_i} \cdot a + e_1^{d_i}) + e_i^* (\mathrm{mod}\, q)$

Server computes: $C_{sum_0} + \sum_{i=1}^{N} D_i = \sum_{i=1}^{N} (v^{d_i} \cdot \tilde{b} + m_i + e_0^{d_i}) + \sum_{i=1}^{N} s_i \cdot \sum_{i=1}^{N} (v^{d_i} \cdot a + e_1^{d_i}) + \sum_{i=1}^{N} e_i^* = \sum_{i=1}^{N} m_i$

Privacy-preserving federated learning scheme based on xMK-CKKS



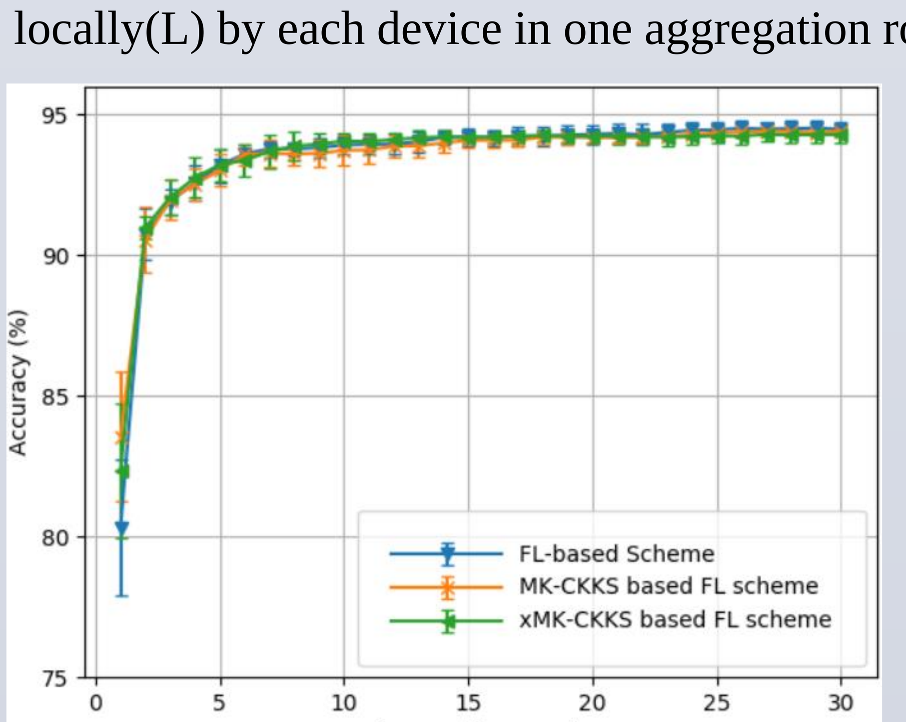
Training process in one aggregation round. Repeats until model converges.

Evaluation

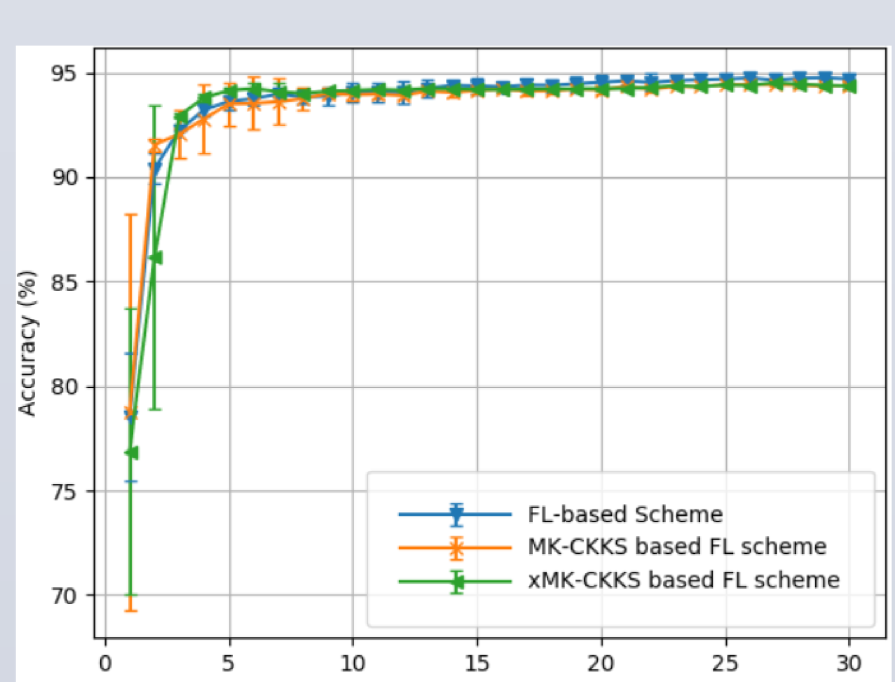
Setting: Scenario: Elderly-fall detection Dataset: UP-Fall detection dataset CNN baseline: TensorFlow and Keras.

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

a. Classification accuracy comparison with different number of training epochs executed locally(L) by each device in one aggregation round

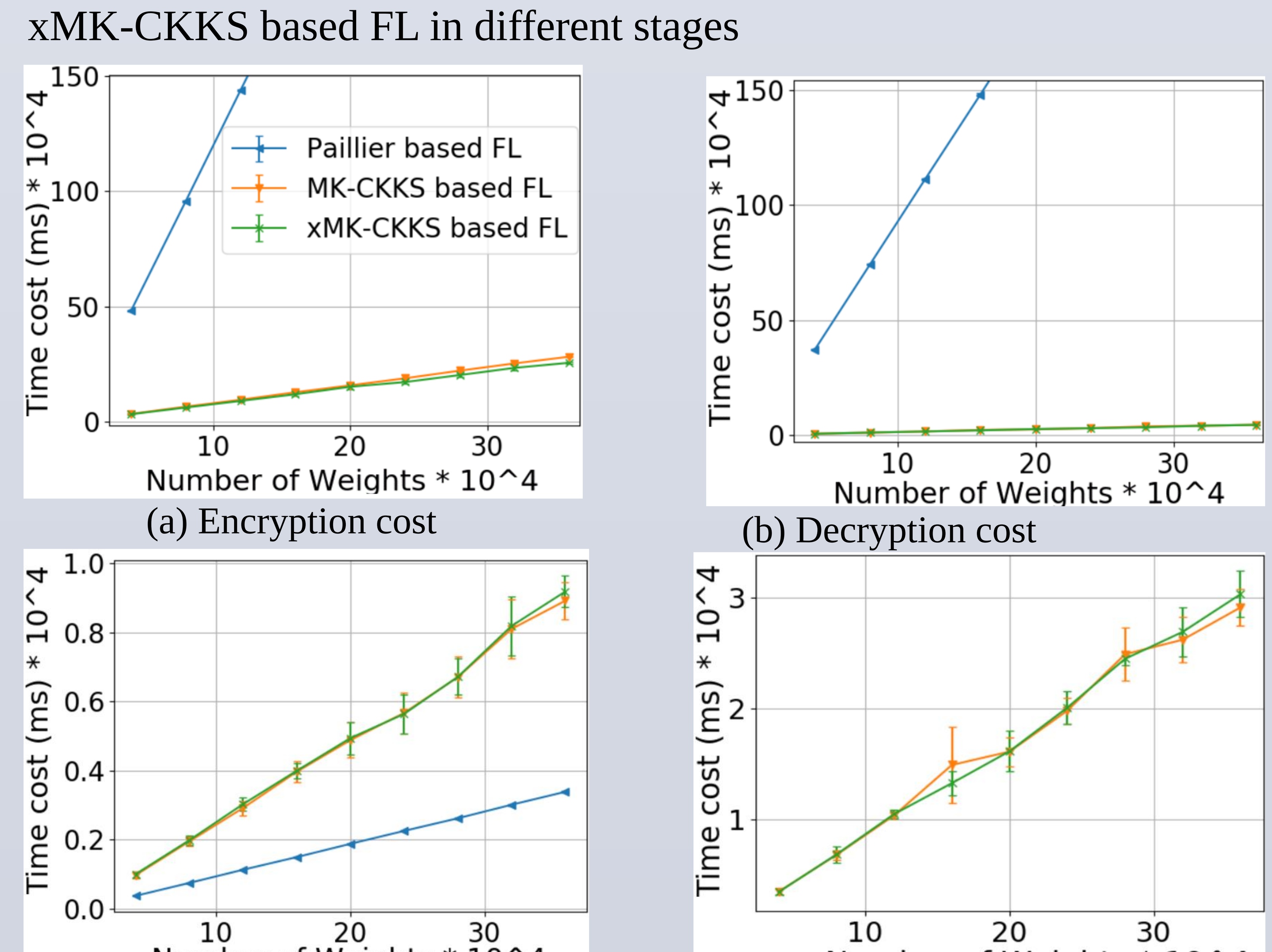


L = 20



L = 40

c. Computational cost for Paillier based FL, MK-CKKS based FL, and xMK-CKKS based FL in different stages



(a) Encryption cost (b) Decryption cost

(c) Ciphers sum cost (d) Decryption share cost

b. Energy consumption of different FL schemes executed on distributed Jetson Nano IoT Devices(max 10 W)

Scenario	xMK-CKKS based FL	MK-CKKS based FL	Paillier based FL	FL w/o encryption	No activity (idle)
Energy (W)	2.4	2.4	2.1	2.3	1.8

Conclusion

a. xMK-CKKS achieves higher security and simpler operations than MK-CKKS, which is more suitable for federated learning scenarios.

b. 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.

c. Evaluation results show significant reduction in computational load and reasonable energy consumption while maintaining the accuracy.

Contact to us: jing.ma@aalto.fi