The 23rd Annual International Conference on Information Security and Cryptology

Korea Institute of Information Security & Cryptology

ICISC 2020

December 2 (Wed) ~ December 4 (Fri), 2020 | Virtual Conference

Hosted by
Korea Institute of Information Security and Cryptology (KIISC)
National Security Research Institute (NSR)

Federated Learning in Side Channel Analysis

Huanyu Wang, Elena Dubrova

huanyu@kth.se

KTH Royal Institute of Technology

Overview

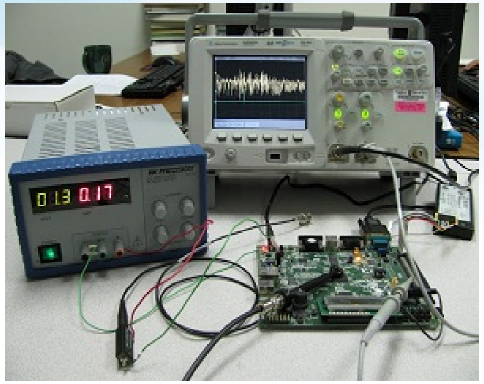
- The newly proposed Federated Learning [1-3] is an attractive framework for distributed learning.
- Use federated learning framework to achieve a more efficient deep-learning side-channel attack.
- Compare federated learning to other aggregation methods in deep-learning side-channel attacks' contexts.

Overview

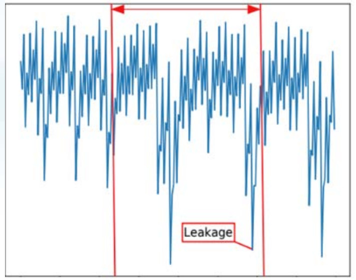
- Introduction and Background
- Aggregation Approach
- Experimental setup
- Result
- Conclusion and Future Work

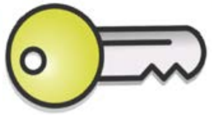
Introduction and Background

Side-channel attack (SCA):



source: hackaday.com

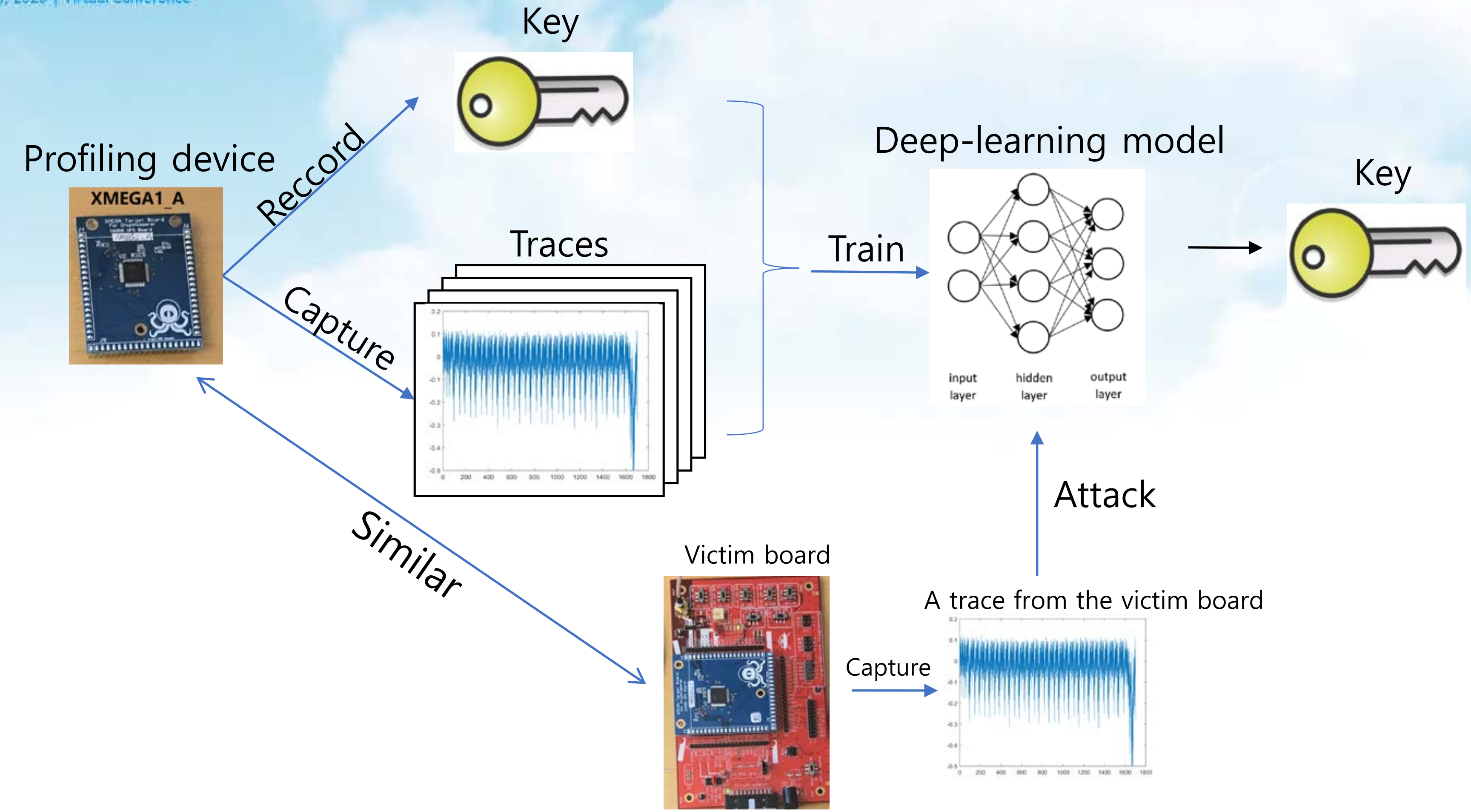




- Side-channel signals are related to the data processed
  - e.g. different amount of power is consumed

- Deep Learning (DL) makes SCA more powerful

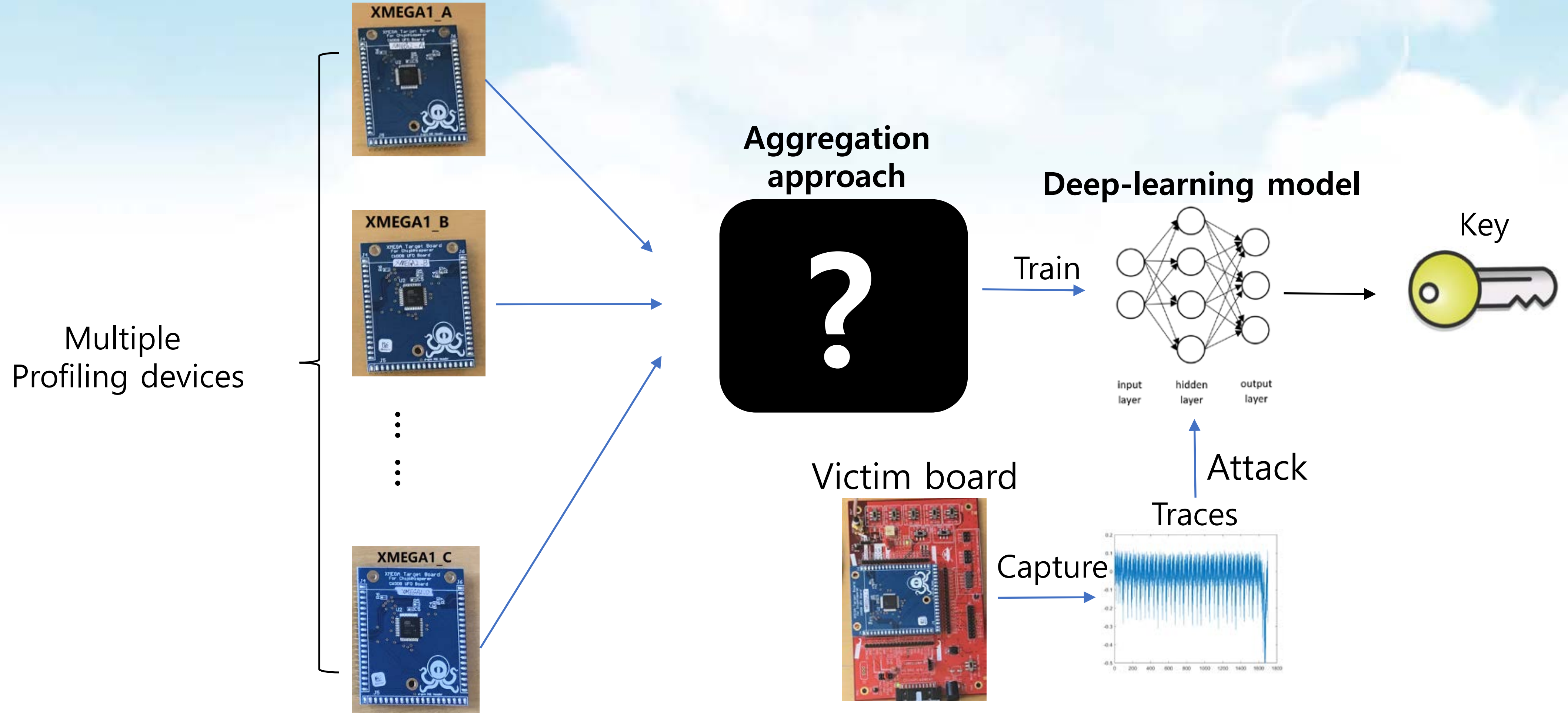
Introduction and Background



- The attacker doesn't have full control to the victim device..
- The board diversity can significantly reduce the attack accuracy (96%-13%)[4].
  - How to mitigate the effect caused by the board diversity?

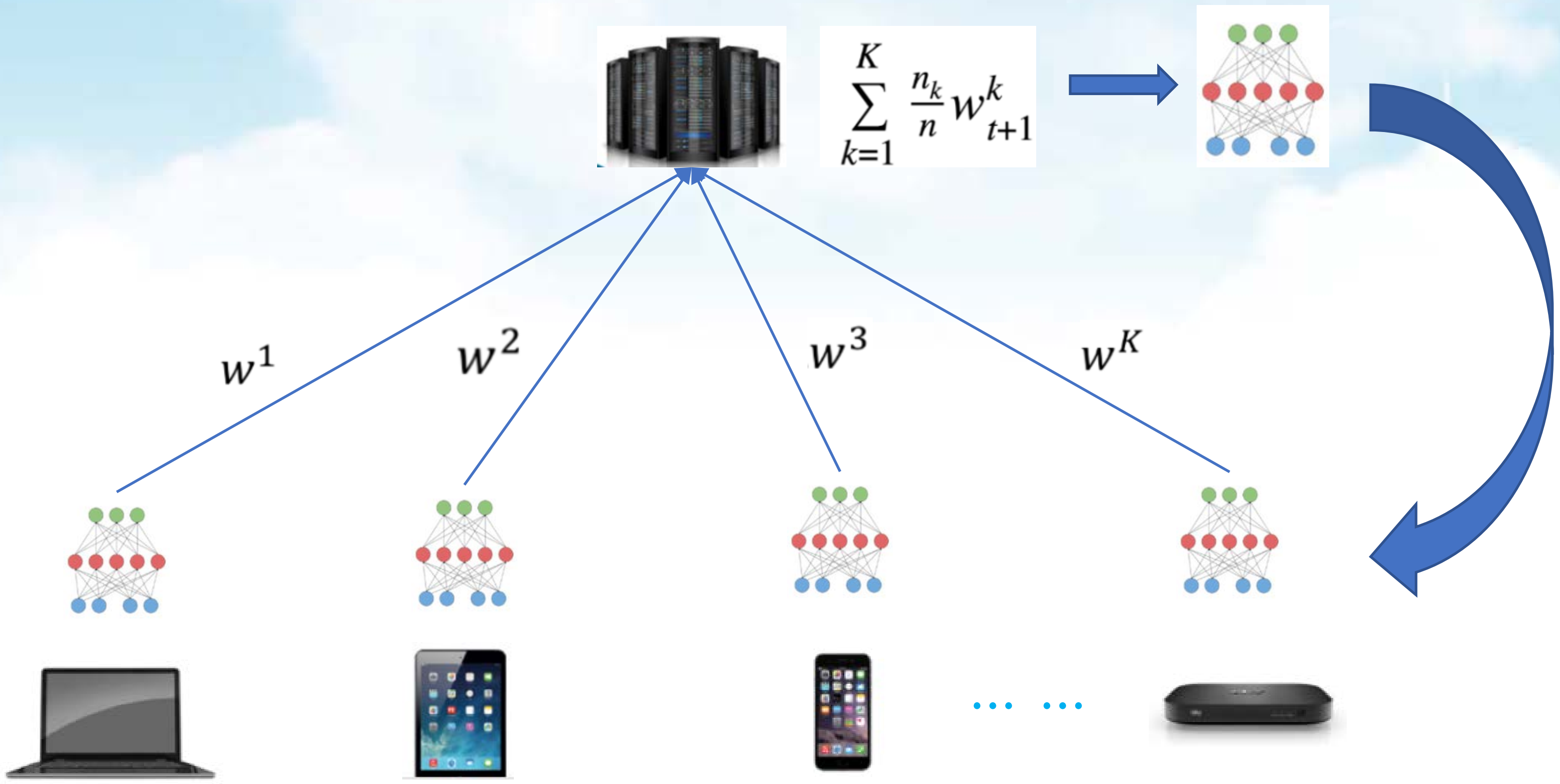
Introduction and Background

To solve this problem:



Introduction and Background

1. Federated learning [1-3]



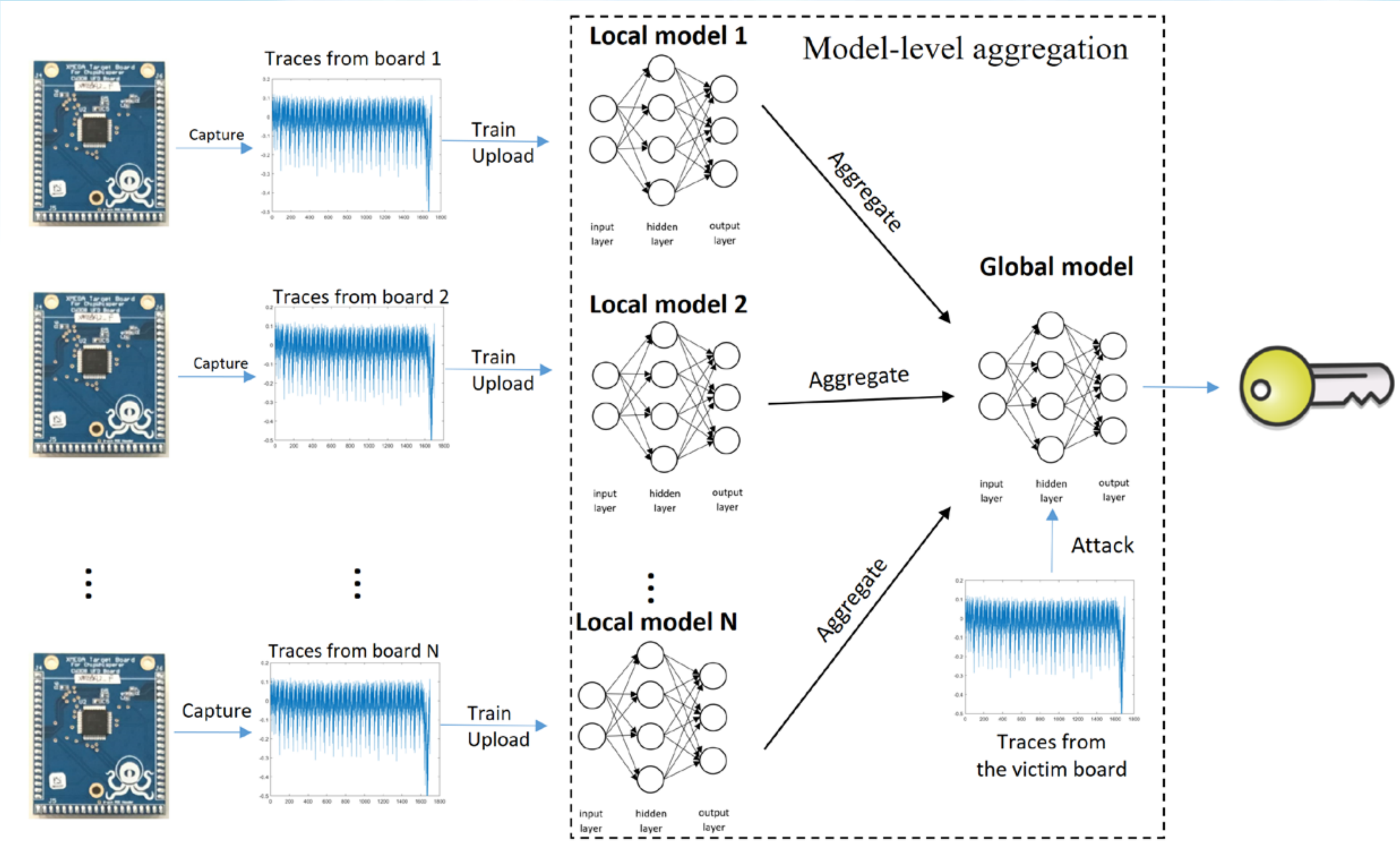
https://proandroiddev.com/federated-learning-e79e054c33ef

Overview

- Introduction and Background
- Aggregation Approach
- Experimental setup
- Result
- Conclusion and Future Work

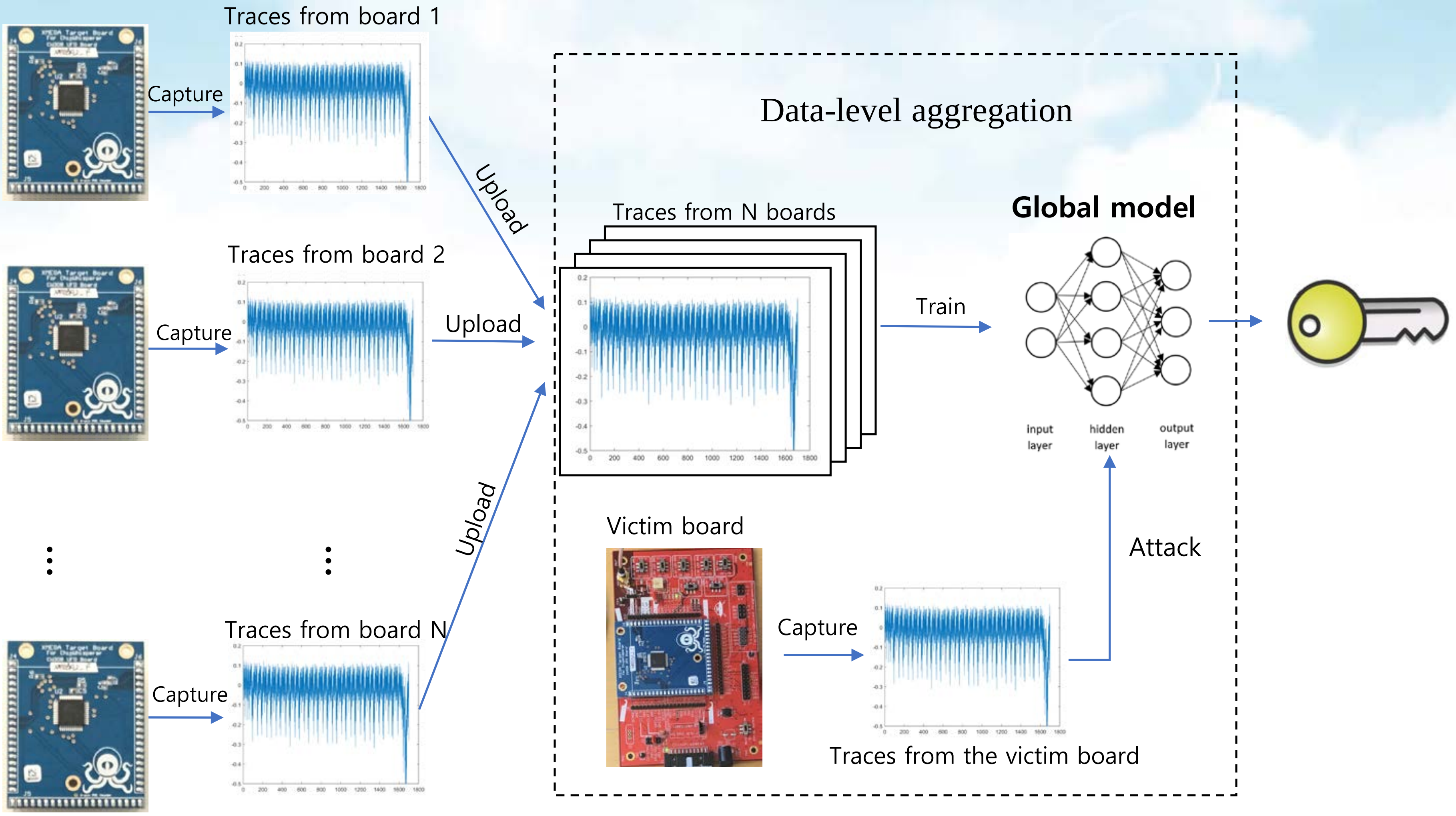
Aggregation Approach

1. Model-level aggregation (Federated learning)



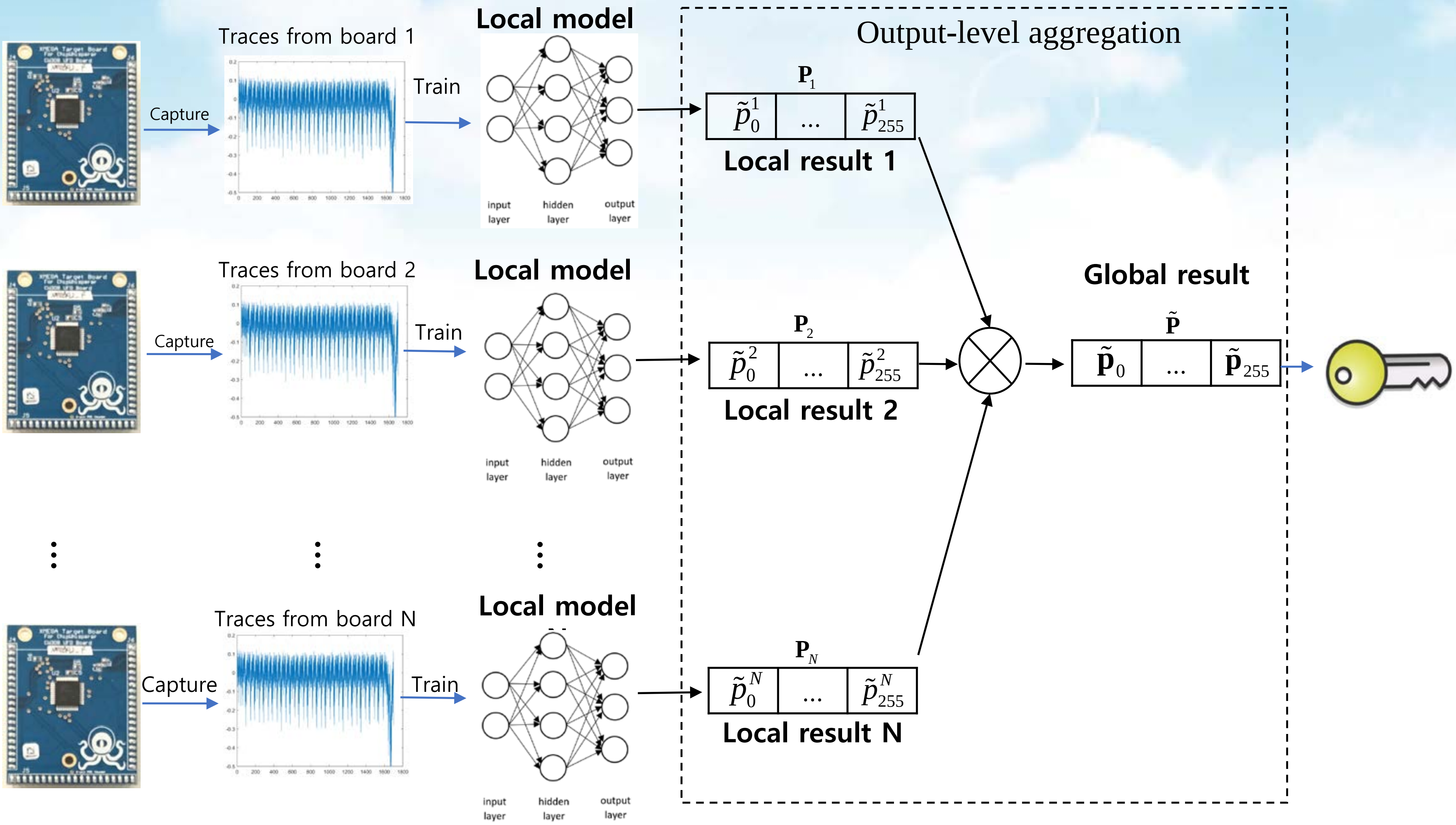
Aggregation Approach

2. Data-level aggregation (Multi-source training [5-7])



Aggregation Approach

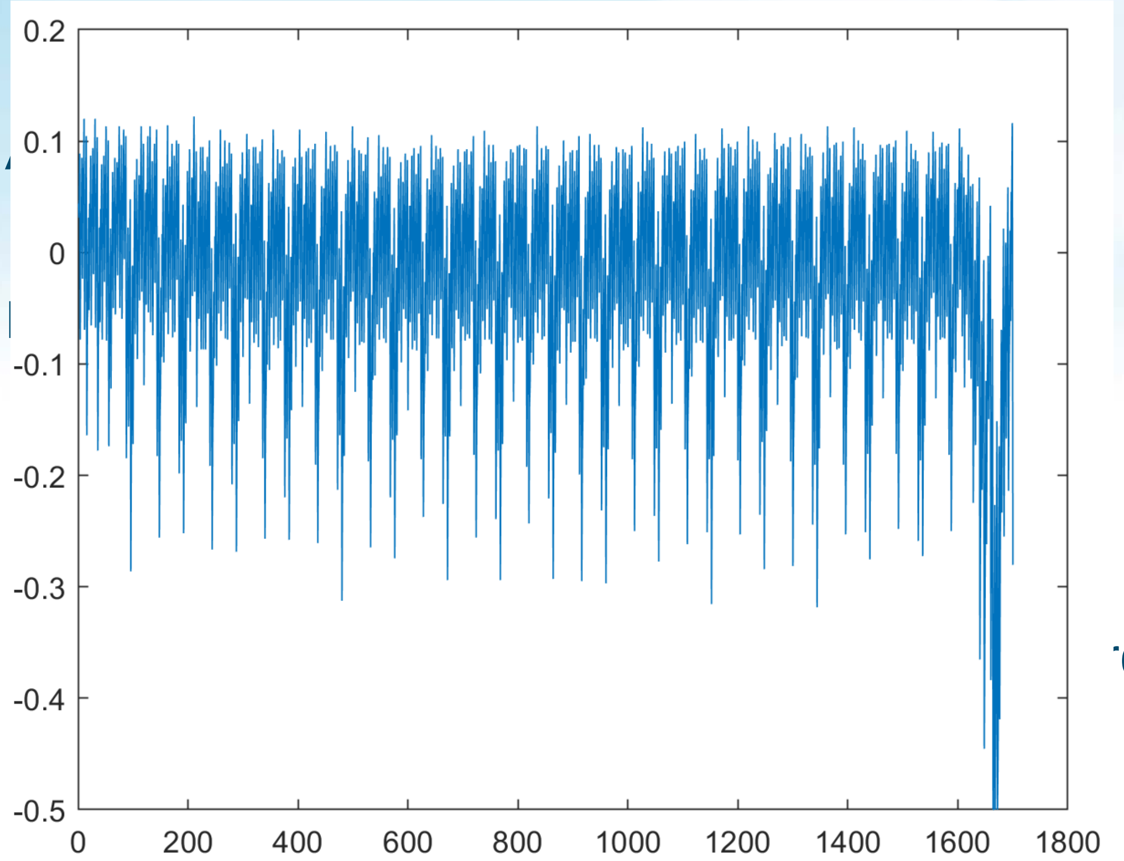
3. Output-level aggregation (Tandem DL-SCA [8])

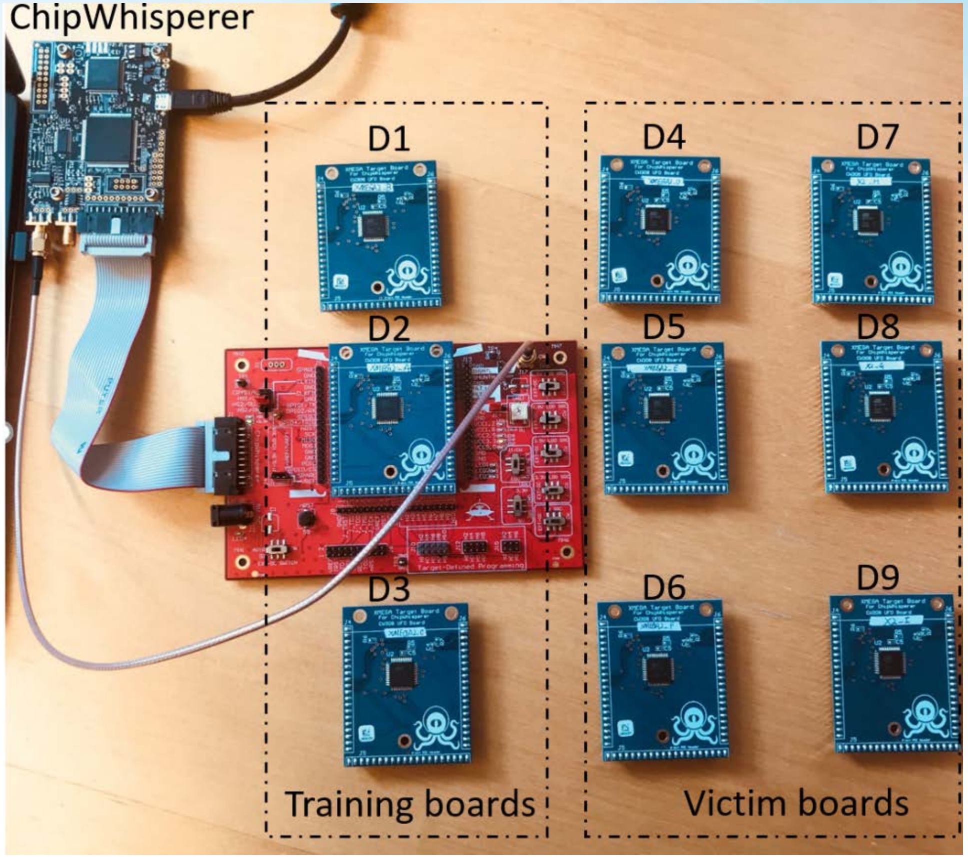


Overview

- Introduction and Background
- Aggregation Approach
- Experimental setup
- Result
- Conclusion and Future Work

Experimental Setup

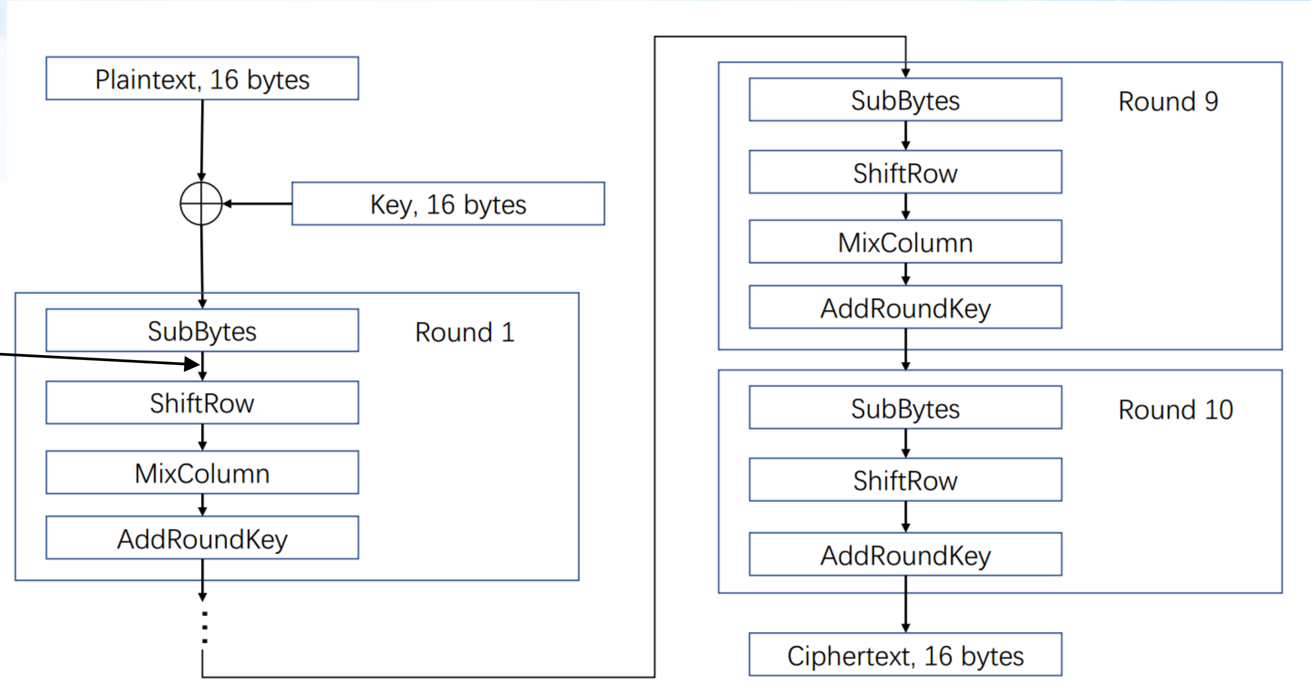




Experimental Setup

Advanced Encryption Standard (AES) [9]

- Attack point



Experimental Setup

Local model structure

- Multi-Layer Perceptron (MLP)
- Input size: 96 (defined by the subkey)
- Output size: 256 (defined by the identity model)

Layer Type	Output Shape	Parameter #
Input (Dense)	(None, 200)	19400
Dense 1	(None, 200)	40200
Dense 2	(None, 200)	40200
Dense 3	(None, 200)	40200
Dense 4	(None, 200)	40200
Output (Dense)	(None, 256)	51456
Total Parameters: 231,656		

Table 1. Local model's architecture summary.

Overview

- Introduction and Background
- Aggregation Approach
- Experimental setup
- Result
- Conclusion and Future Work

Experimental Result

1. Output-level aggregation

Three local models:

- Local model 1 is trained on D1 (91.3% tested on D1)
- Local model 2 is trained on D2 (92.7% tested on D2)
- Local model 3 is trained on D3 (90.2% tested on D3)

Table.1 Probability of recovering the key from a single trace by using local models

Device	Local model 1	Local model 2	Local model 3
D4	29.1%	42.6%	40.8%
D5	48.4%	63.8%	21.8%
D6	38.3%	33.6%	39.7%
D7	6.8%	10.4%	57.9%
D8	27.3%	36.1%	50.0%
D9	33.9%	51.8%	35.4%
Average	34.9%	41.3%	40.9%

Table.2 The probability of recovering the key from a single trace by using the output-level aggregation

Device	D4	D5	D6	D7	D8	D9	Average
Single-trace key recovery rate	64.5%	76.0%	66.0%	18.4%	68.3%	58.8%	58.7%

Experimental Result

2. Model-level aggregation (Federated Learning)

- Train federated model on D1, 2 and 3.
- Test on D4~9
- We choose model generated at the 17th round.

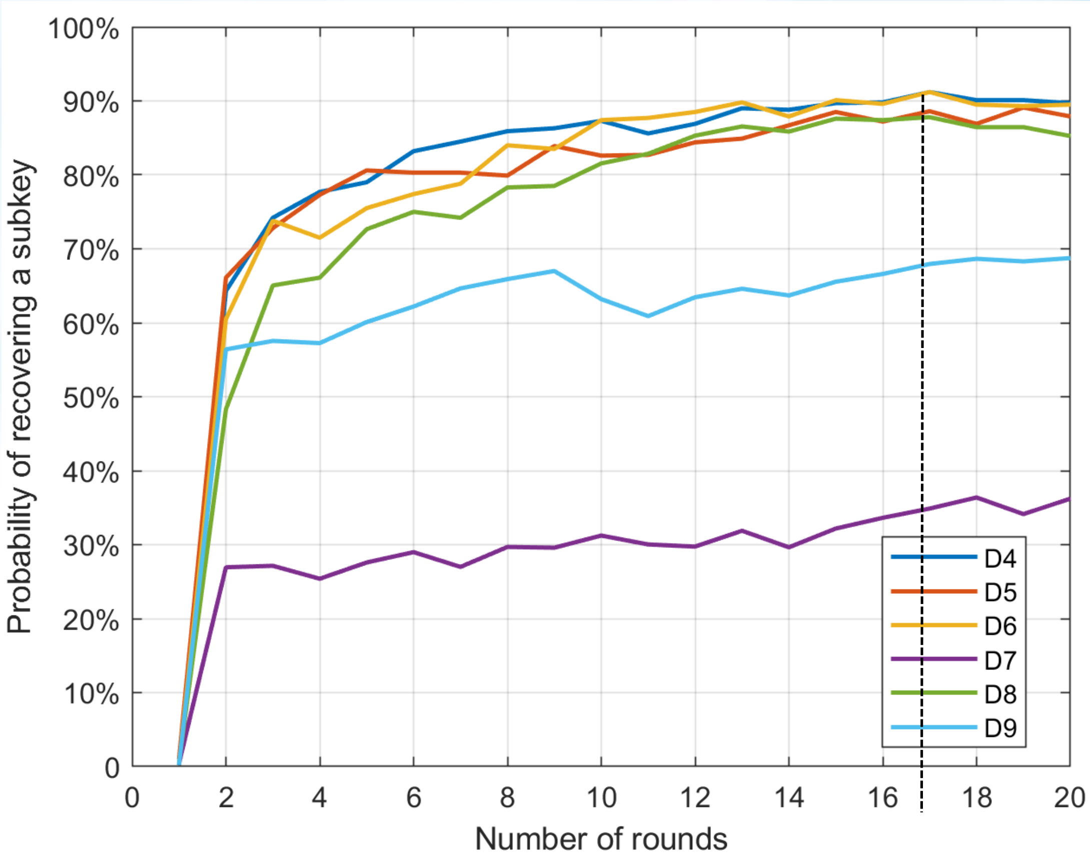


Table.3 The probability of recovering the key from a single trace by using the model-level aggregation

Device	D4	D5	D6	D7	D8	D9	Average
Single-trace key recovery rate	89.8%	91.2%	91.4%	35.5%	88.5%	69.6%	77.7%

Experimental Result

3. Data-level aggregation

Table.4 The probability of recovering the key from a single trace by using the data-level aggregation

Device	D4	D5	D6	D7	D8	D9	Average
Single-trace key recovery rate	74.6%	83.0%	73.6%	37.5%	62.3%	81.5%	68.8%

Summary

Table.5 The probability of recovering the key from a single trace with different aggregation approaches

Device	Aggregation method		
	Model-level approach	Output-level approach	Data-level approach
D_4	89.8%	64.5%	74.6%
D_5	91.2%	76.0%	83.0%
D_6	91.4%	66.0%	73.6%
D_7	35.5%	18.4%	37.5%
D_8	88.5%	68.3%	62.3%
D_9	69.6%	58.8%	81.5%
average	77.7%	58.7%	68.8%

Overview

- Introduction and Background
- Aggregation Approach
- Experimental setup
- Result
- Conclusion and Future Work

Conclusion & future work

Conclusion:

- We use federated learning framework to make DLSCA more efficient.
- Model-level aggregation (federated learning) is capable of outperforming data and output –level aggregation approaches.

Future Work:

- Countermeasures

Reference

[1] Konečný J, McMahan H B, Yu F X, et al. Federated learning: Strategies for improving communication efficiency[J]. arXiv preprint arXiv:1610.05492, 2016.
[2] Konečný J, McMahan H B, Ramage D, et al. Federated optimization: Distributed machine learning for on-device intelligence[J]. arXiv preprint arXiv:1610.02527, 2016.
[3] McMahan B, Moore E, Ramage D, et al. Communication-efficient learning of deep networks from decentralized data[C]//Artificial Intelligence and Statistics. PMLR, 2017: 1273-1282.
[4] Wang, Huanyu, et al. "How diversity affects deep-learning side-channel attacks." 2019 IEEE Nordic Circuits and Systems Conference (NORCAS): NORCHIP and International Symposium of System-on-Chip (SoC). IEEE, 2019.
[5] Das, Debayan, et al. "X-DeepSCA: Cross-device deep learning side channel attack." Proceedings of the 56th Annual Design Automation Conference 2019. 2019.
[6] Wang, H., Forsmark, S., Brisfors, M., Dubrova, E.: Multi-source training deep learning side-channel attacks. IEEE 50th International Symposium on MultipleValued Logic (2020)
[7] Golder, Anupam, et al. "Practical approaches toward deep-learning-based cross-device power side-channel attack." IEEE Transactions on Very Large Scale Integration (VLSI) Systems 27.12 (2019): 2720-2733.
[8] Wang, Huanyu, and Elena Dubrova. "Tandem Deep Learning Side-Channel Attack Against FPGA Implementation of AES." IACR Cryptol. ePrint Arch. 2020 (2020): 373.
[9] Daemen, J., Rijmen, V.: The Design of Rijndael. Springer-Verlag New York, Inc., Secaucus, NJ, USA (2002)

Thank you!