

- **Articles:**
 - [Will we adopt AI like we adopted electricity?](#)
 - [A trusted federated system to share granular data among disparate database resources](#)
 - [Practical secure aggregation for privacy-preserving Machine Learning](#)
- **Further Reading:**

Articles:

Will we adopt AI like we adopted electricity?

Hsiao-Ying Lin, IEEE Member

[mco202103.issue.pdf](#)

Notes:

- Geoffrey Hinton -- Turing Award for his contributions to deep learning. His work on the application of the backpropagation algorithm in deep learning was a turning point for AI
- 2012: Hinton + team -> triumph in ImageNet Large Scale Visual Recognition Challenge --> AlexNet
- Remarkable milestones as described by Hsiao-Ying Lin:
 - Object-detection - **YOLO**
 - Generative pretraining GPT-3 - **A. Radford, K. Narasimhan, T. Sali-mans, and I. Sutskever. "Improving language understanding by generative pre-training." Amazonaws. https://s3-us-west-2.amazonaws.com/openai-assets/research-covers/language-unsupervised/language_understanding_paper.pdf (accessed Nov. 10, 2020).**
 - Generative adversarial networks (GANs)
 - Deep reinforcement learning - **V. Mnih et al., "Human-level control through deep reinforcement learning," Nature. vol. 518, pp. 529–533, Feb. 2015. doi: 10.1038/nature14236**
 - **Federated learning (FL)** - A new method that decentralized ML models learning. Potential applications in medicine and health care

A trusted federated system to share granular data among disparate database resources

Joanna F. DeFranco, David F. Ferraiolo, D. Richard Kuhn, Joshua D. Roberts

[mco202103.issue.pdf](#)

Notes:

- n/a

Practical secure aggregation for privacy-preserving Machine Learning

Keith Bonawitz, Vladimir Ivanov, Ben Kreuter, Antonio Marcedone, H. Brendan McMahan, Sarvar Patel, Daniel Ramage, Aaron Segal, Karn Seth

[3133956.3133982.pdf](#)

Notes:

- *Secure Aggregation* == the problem of computing a multiparty sum where no party reveals its update in the clear - even to the aggregator.
- Area of research for secure aggregation: **further discussed in Section 9 of the underlying paper**
- generic secure multi-party computation protocols
- DC-nets
- partially -or fully- homomorphic threshold encryption
- pairwise masking
- Shamir's t -out-of- n Secret Sharing: a user splits a secret s into n shares, such that any t shares can be used to reconstruct s , but any set of at most $t - 1$ shares gives no information about s
- Diffie-Hellman Key Agreement scheme, composed with a hash function.
- Decisional Diffie-Hellman assumption:

Let $G(k) \rightarrow (G', g, q, H)$ be an efficient algorithm which samples a group G' of order q with generator g , as well as a function $H: \{0, 1\}^* \rightarrow \{0, 1\}^k$. Consider the following probabilistic experiment, parametrized by a PPT adversary M , a bit b and a security parameter k .

DDH-Exp $_{G, M}^b(k)$:

- (1) $(G', g, q, H) \leftarrow G(k)$
- (2) $a \leftarrow \mathbb{Z}_q; A \leftarrow g^a$
- (3) $b \leftarrow \mathbb{Z}_q; B \leftarrow g^b$
- (4) if $b = 1$, $s \leftarrow H(g^{ab})$, else $\leftarrow \{0, 1\}^k$
- (5) $M(G', g, q, H, A, B, s) \rightarrow b'$
- (6) Output 1 if $b = b'$, 0 o/w

Key points:

- Simulation-based proof for MPC protocols
- Random oracle model

Further Reading:

- Jakub Konečný, H Brendan McMahan, Felix X Yu, Peter Richtárik, Ananda Theertha Suresh, and Dave Bacon. 2016. Federated learning: Strategies for improving communication efficiency. arXiv preprint arXiv:1610.05492 (2016).
- Collaborative Deep Learning in Fixed Topology Networks, Zhanhong Jiang, Aditya Balu, Chinmay Hegde, Soumik Sarkar, 2017
- Adi Shamir. 1979. How to share a secret. Commun. ACM 22, 11 (1979), 612–613.
- Whitfield Diffie and Martin Hellman. 1976. New directions in cryptography. IEEE transactions on Information Theory 22, 6 (1976), 644–654.

TODO: Continue reading from "or security, in the honest but curious model..." at [3133956.3133982.pdf](#)