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 backpopagation 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 adversial 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) --> (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}* --> $\{0, 1\}^k$. Consider the following probabilistic experiment, parametrized by a PPT adversary **M**, a bit *b* and a security parameter *k*.
>
> **DDH-Exp**$^b_{G, M}$(k):
>
> - (1) (G', g, q, H) <-- G(k)
> - (2) a <-- Z_q; A <-- g^a
> - (3) b <-- Z_q; B <-- g^b
> - (4) if b = 1, s <-- H(g^{ab}), else <-- $\{0, 1\}^k$
> - (5) M(G', g, q, H, A, B, s) --> b'
> - (6) Output 1 if b = b', 0 o/w

Key points:

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

TODO: Read later from the beginning

A generic framework for privacy preserving deep learning

Theo Ryffel, Andrew Trask, Morten Dahl, Robby Wagner, Jason Mancuso, Daniel Rueckert, Jonathan Passerat-Palmbach 1811.04017v2.pdf

Notes:

- Secure Multiparty Computation (SMPC) is becoming increasingly popular. Machine learning, SMPC --> Federated learning
- Securely trained models are still vulnerable to reverse-engineering attacks that can extract sensitive information --> Differentially Private (DP) methods address this and can efficiently protect the data

Advances and Open Problems in Federated Learning

Peter Kairouz, Brendan Mcmahan, Brendan Avent, Aurélien Bellet, Mehdi Bennis, et al..

Notes:

- McMahan et al. were the first to coin the "Federated Learning" term in *Communication-Efficient Learning of Deep Networks from Decentralized Data*:

> We term our approach *Federated Learning*, since the learning task is solved by a loose federation of participating device

-

Further Reading:

- Jakub Konečnỳ, 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.
- McMahan papers
- Martin Abadi, Andy Chu, Ian Goodfellow, H. Brendan McMahan, Ilya Mironov, Kunal Talwar, and Li Zhang. Deep learning with differential privacy.
- Ivan Damgård, Valerio Pastro, Nigel Smart, and Sarah Zakarias. Multiparty computation from somewhat homomorphic encryption