Distributed Privacy Preserving

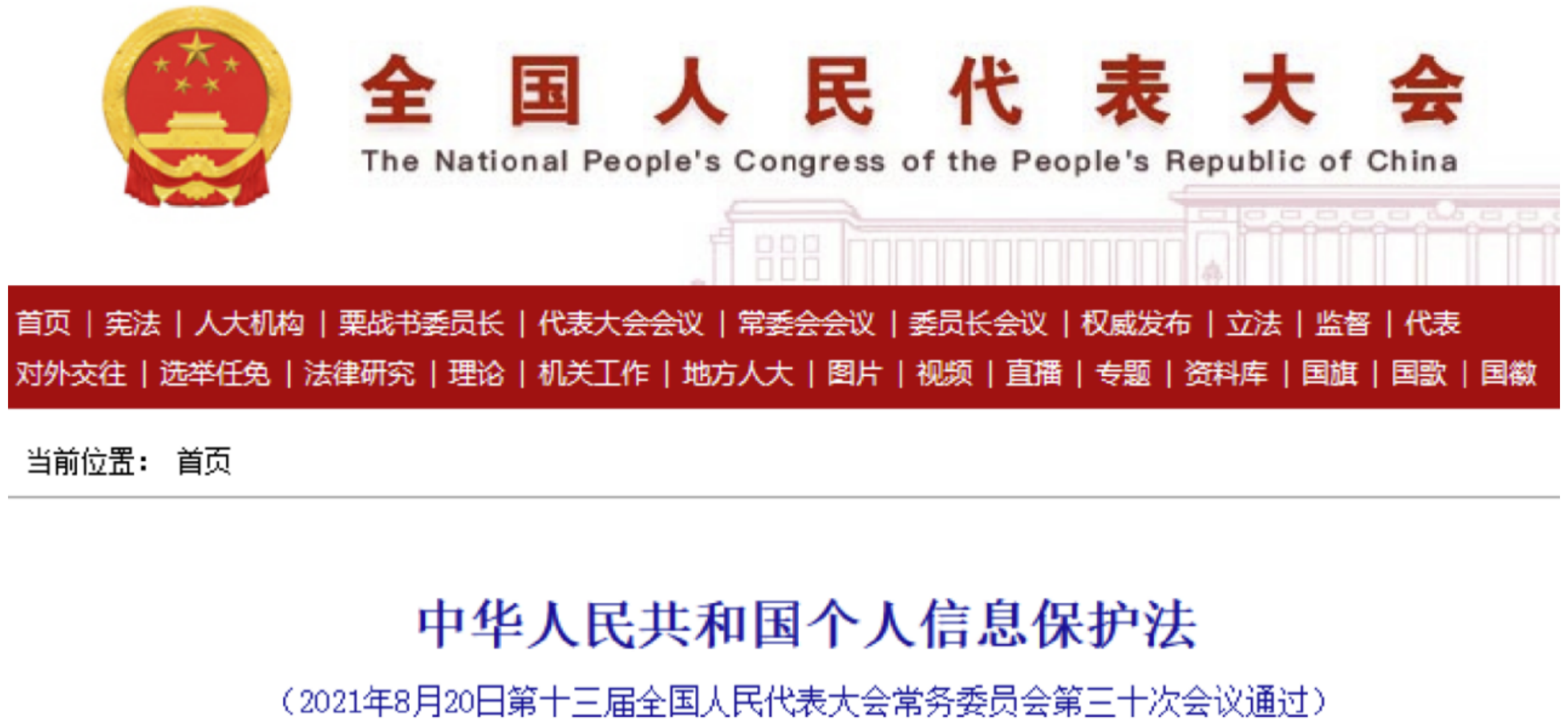
Computer Security from Machine Learning

Hongyang Li
Politecnico di Milano
Presentation of A Research Introduction

POLITECNICO
MILANO 1863

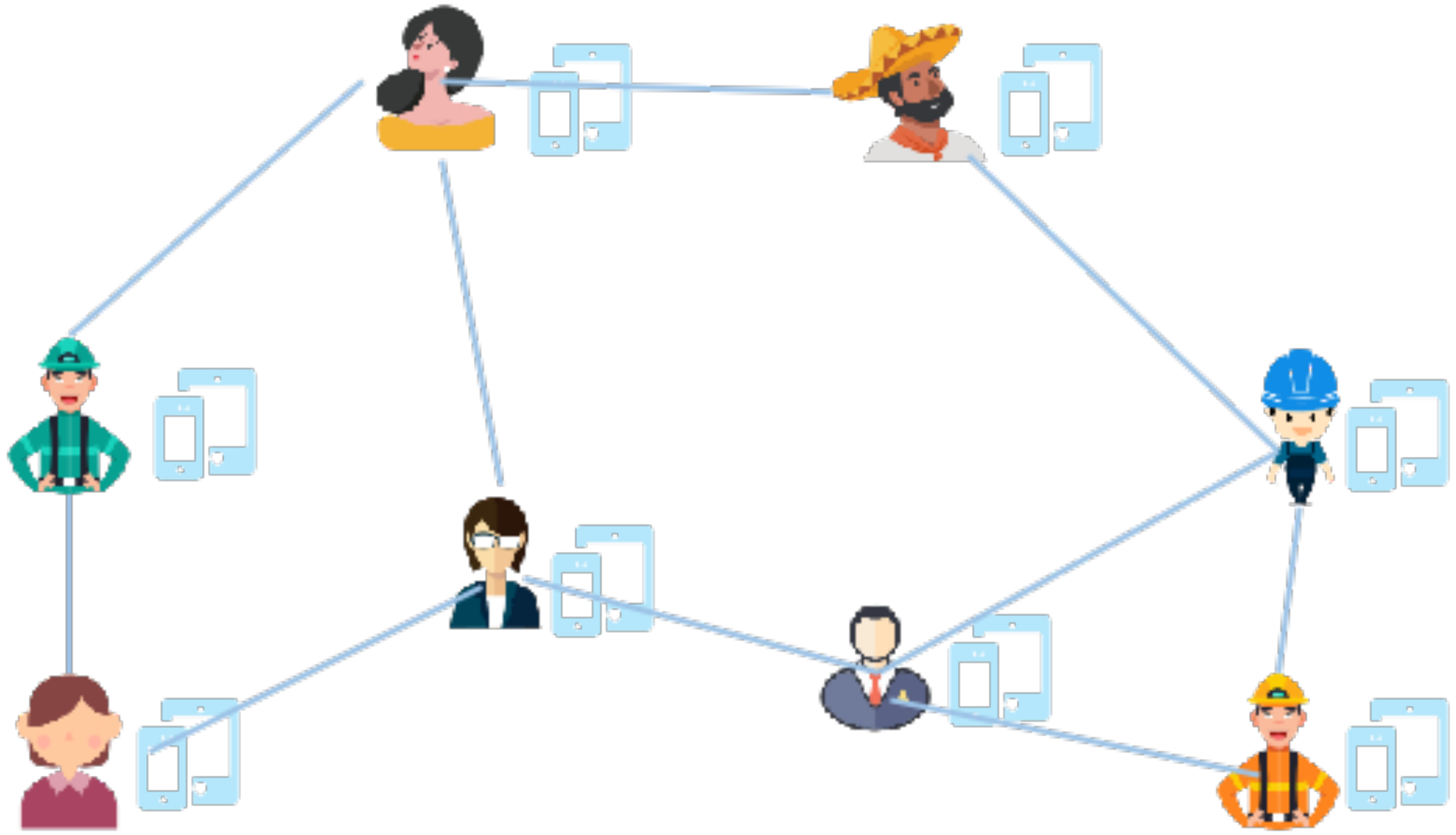
Jan.18 2023

Privacy Regulations



Why distributed?

Centralized system v.s. Distributed system



☹ Totally dependent on the authority
☹ Vulnerable to malicious attack

☺ No dependency on any single party
☺ More flexible system
☺ Robust to malicious attack

POLITECNICO
MILANO 1863

Privacy-preserving distributed processing

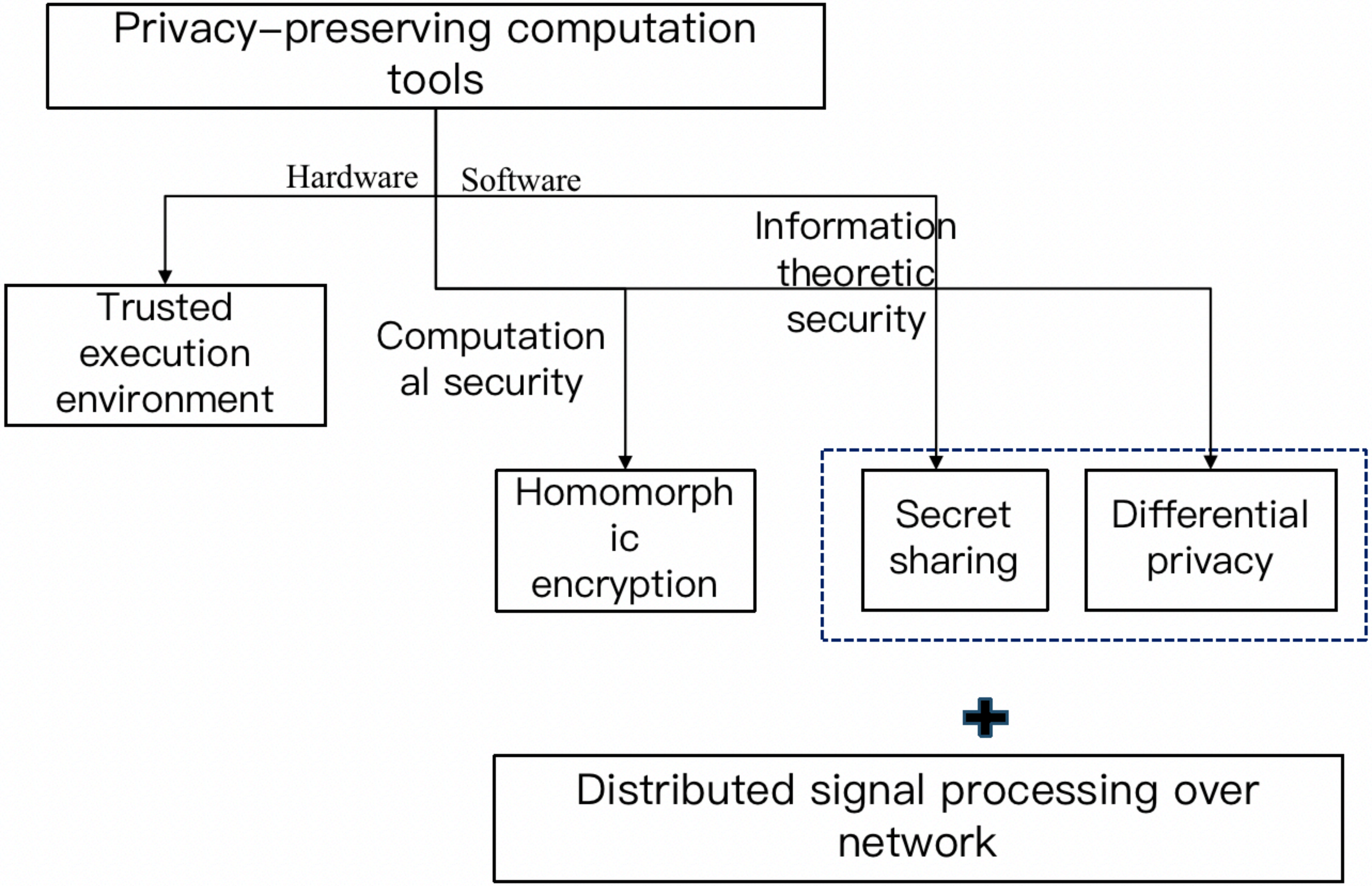
Health care

Contact tracing

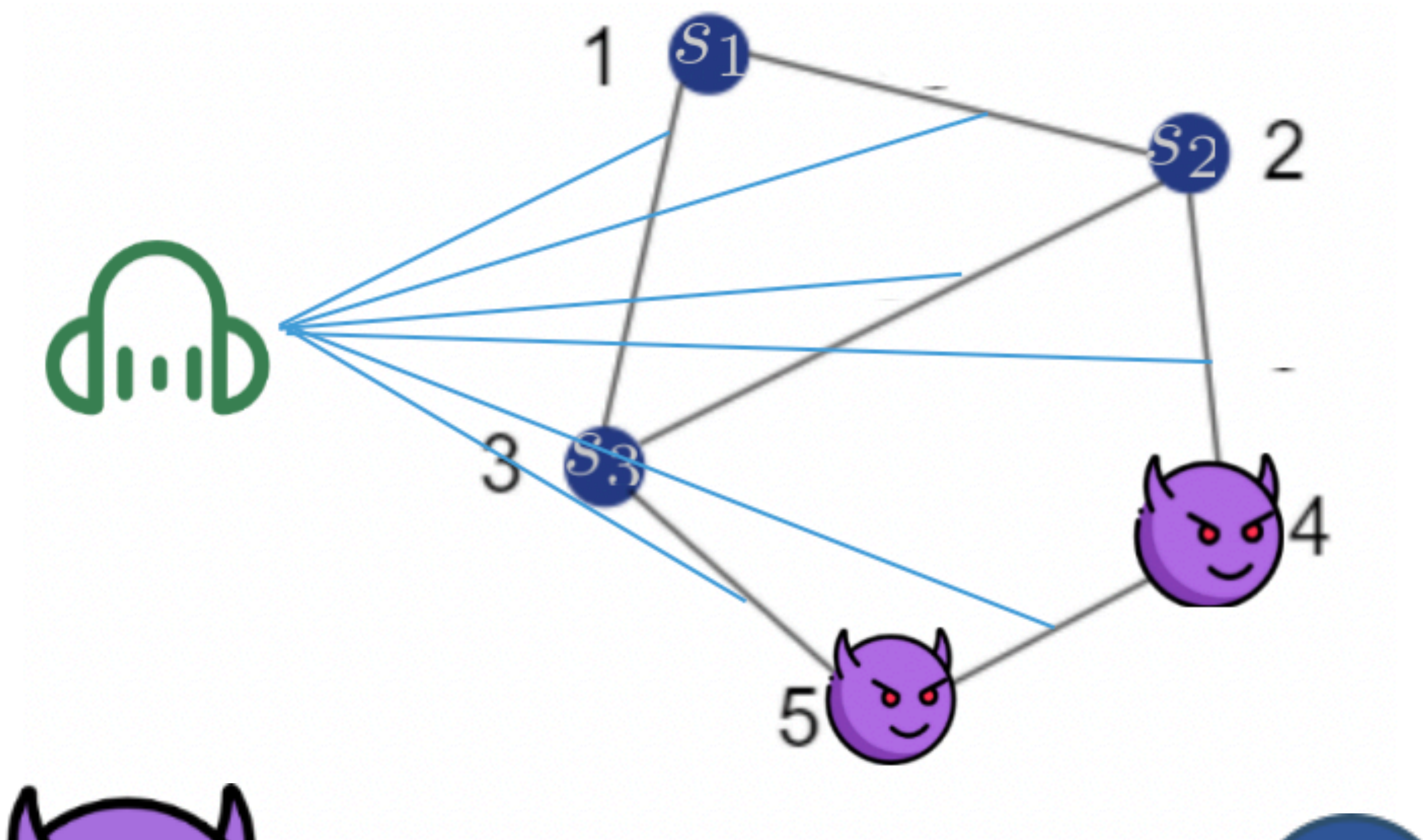
IOT& wireless sensor networks

https://www.kaspersky.com/about/policy-blog/industrial-cybersecurity/security-of-internet-of-things-iot

Overview of exisiting approaches



Adversary Model



Eavesdropping adversary

- eavesdrops all channels between nodes
- assume secure channel encryption
  (expensive for iterative algorithm)

 Corrupted nodes  Honest nodes

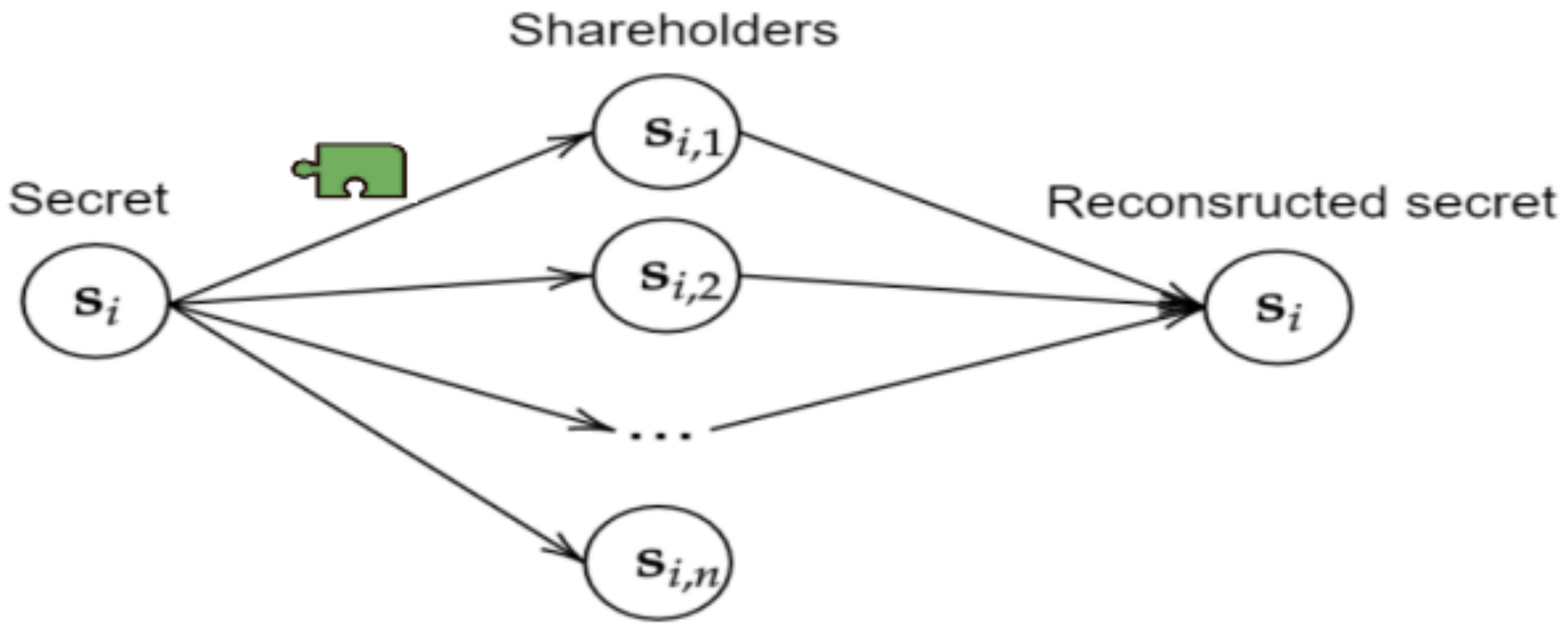
Passive (or semi–honest, honest–but–courious) adversary

- a number of corrupted nodes follow the protocol but share information together to infer the private data of honest nodes

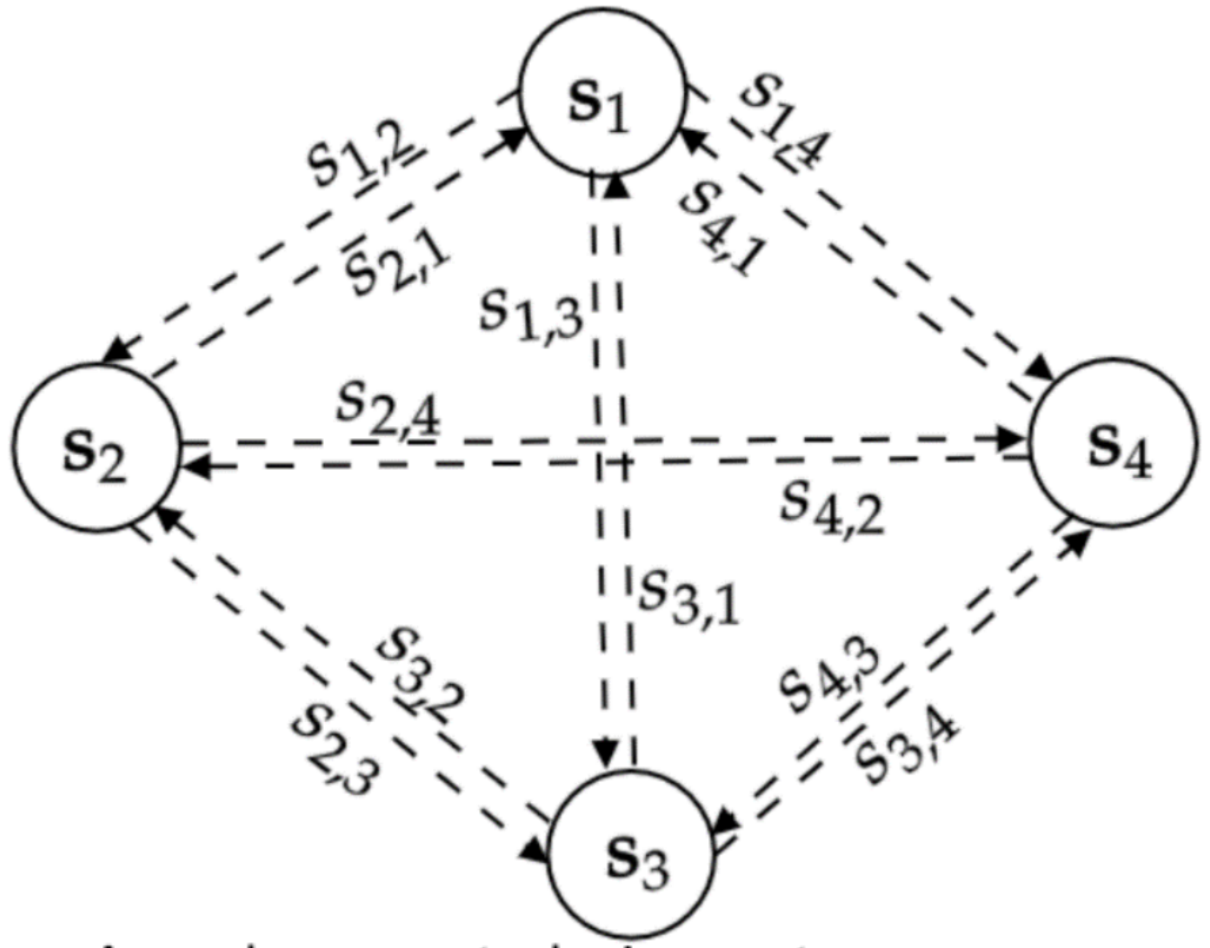
POLITECNICO
MILANO 1863

Overview of exisiting approaches : **Secret sharing based approaches**

Main idea of secret sharing [Cramer, 2015]



Secret sharing + distributed signal processing [Tjell 2019][Tjell 2020]



Appply secret shairng at every iteration

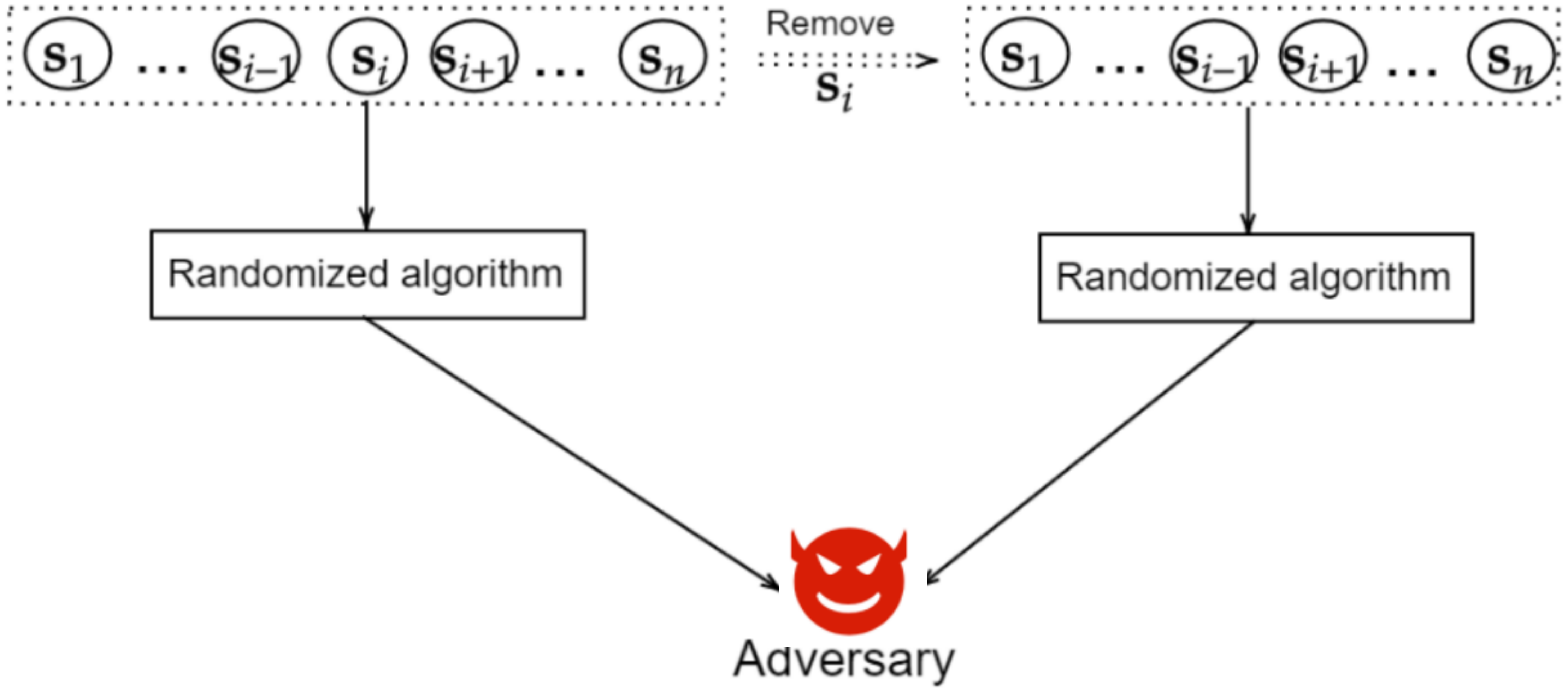
- ☺ Output correctness
  - ☺ no privacy–accuracy trade–off
- ☹ Individual privacy
  - ☹ Secure channel encrytion at all iterations (eavesdropping adversary)
  - ☹ Require at least one honest neighboring node (passive adversary)
- ☹ Communication expensive
- ☹ Often require fully–connected graphs (except specific applications like average or summation

Jan.18 2023

POLITECNICO
MILANO 1863

Overview of exisiting approaches : Differential privacy based approaches

Main idea of differential privacy [Dwork, 2006]



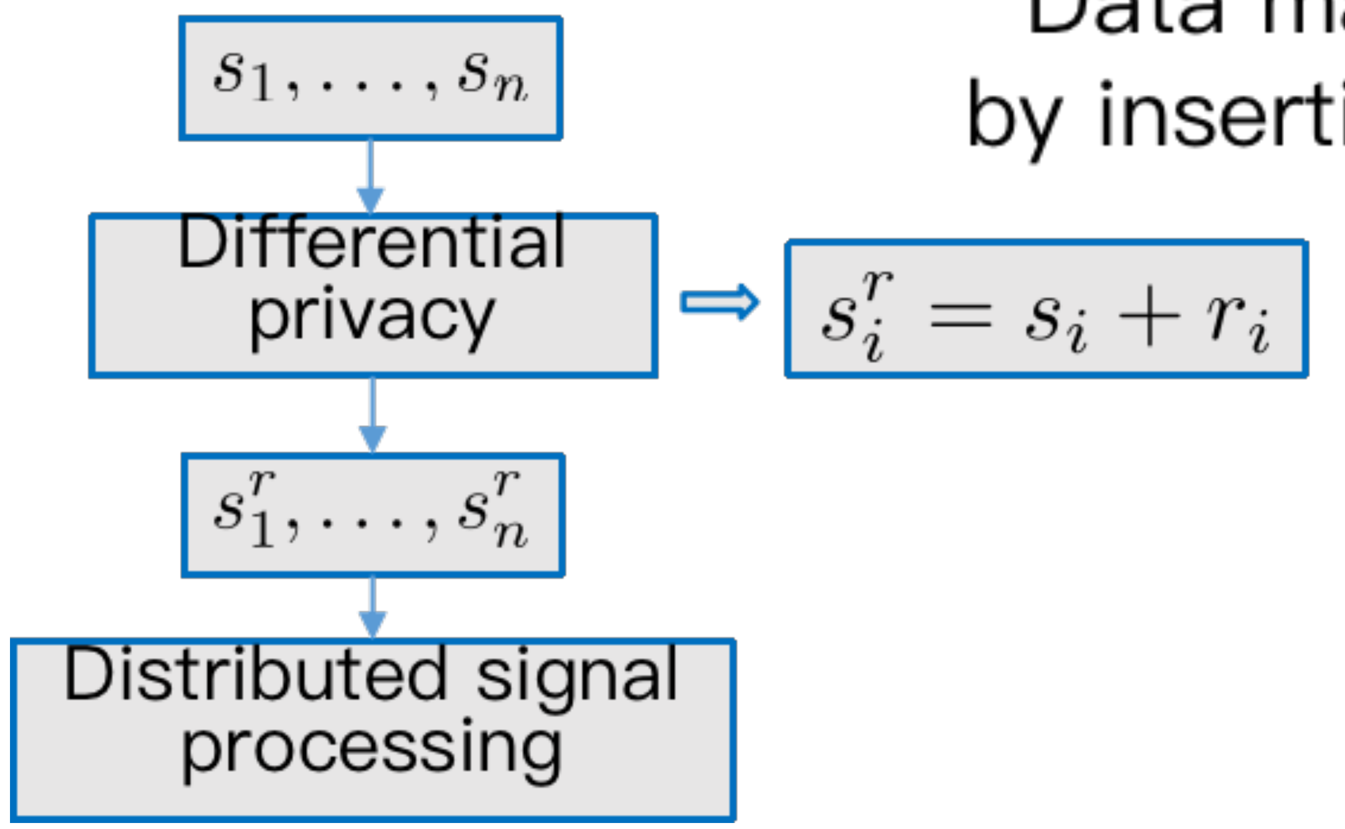
Posterior

$$\forall s_i \in \Omega_i : \quad \frac{P(\hat{F}(\boldsymbol{s}) \in \mathcal{Y}_s)}{P(\hat{F}(\boldsymbol{s}^{-i}) \in \mathcal{Y}_s)} \leq e^{\epsilon}$$

Prior

Differential privacy + distributed signal processing [Huang, 2015] [Nozari, 2018]

Data masking
by inserting noise



- ☺ Simple and general
- ☺ Individual privacy
  - ☺ No secure channel encrytion (eavesdropping adversary)
  - ☺ Secure against $n-1$ corrupted nodes (passive adversary)
- ☹ Output correctness
  - ☹ (traded by individual privacy)

Limitations of existing algorithms for general problems

1. Differential privacy algorithms:
   - privacy–accuracy trade–off

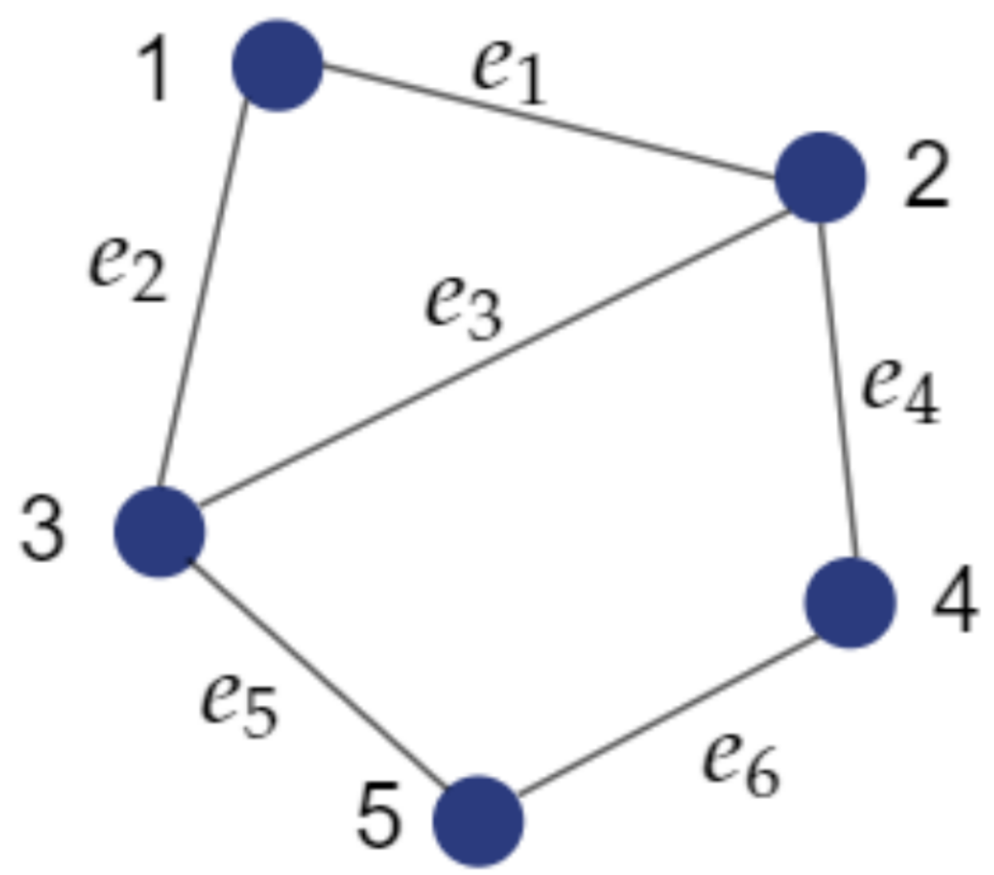
2. Secret sharing approaches:
   - communcationally expensive
   - fully–connected graph assumption

Explore the nature of distributed tools for privacy-preservation

Publication: Q. Li, R. Heusdens, and M. G. Christensen, "*Privacy–Preserving Distributed Optimization via Subspace Perturbation: A General Framework*," in IEEE Trans. Signal Process., vol. 68, pp. 5983 – 5996, 2020.

Contributions:
- A novel privacy–preserving approach derived on distributed optimization: subspace perturbation (DOSP)
- Address the limitations of existing approaches

Distributed optimization over a network



☺ Communication lightweight and do not require fully-connected graphs

☺ General applicable to various optimizers: dual ascent and ADMM [Boyd, 2011]

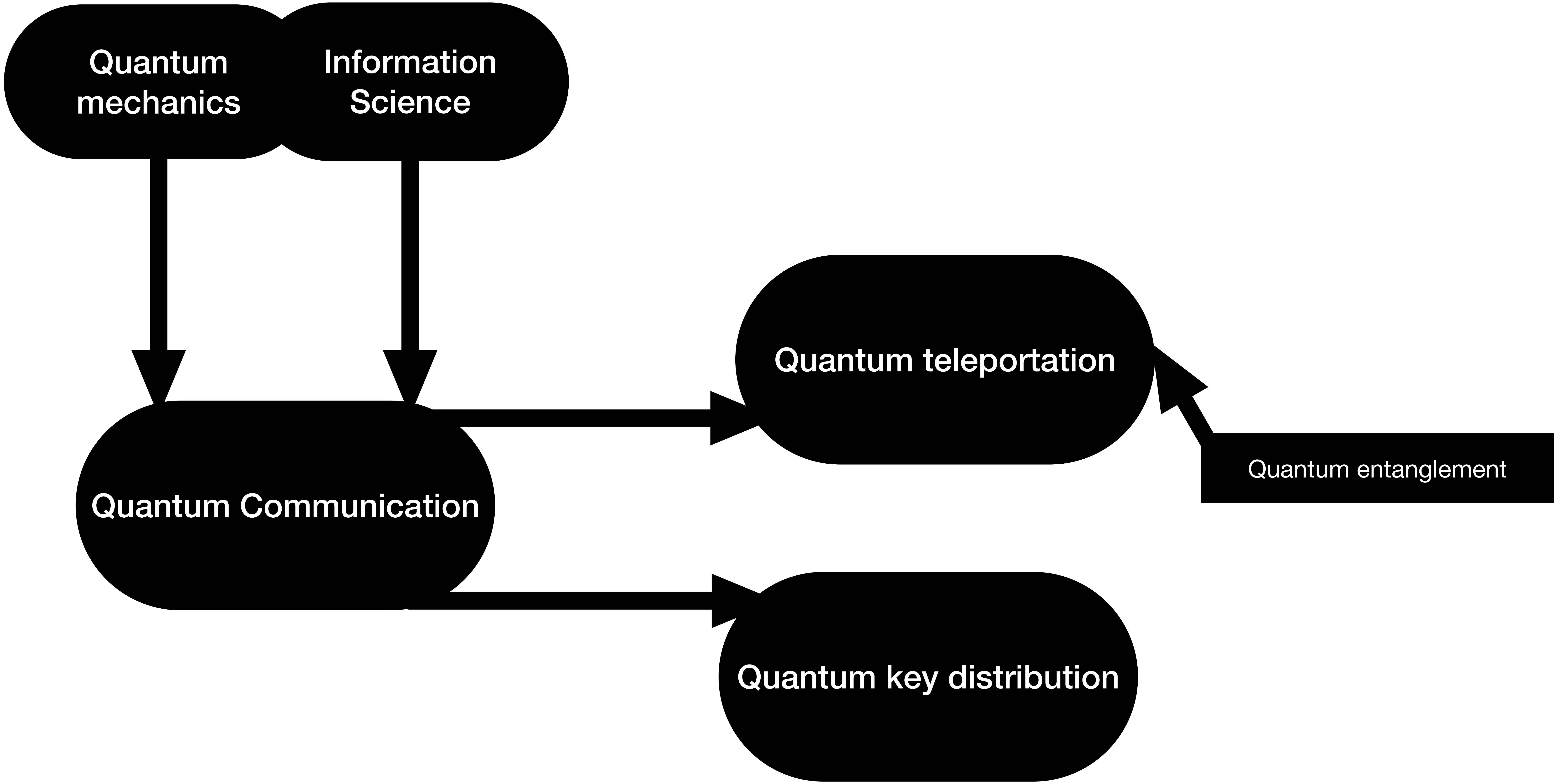
☺ Output correctness: no privacy-accuracy trade-off

☺ Individual privacy

- ☺ Eavesdropping adversary: only one time channel encryption for transmitting
- ☹ Passive adversary: at least one honest neighboring node

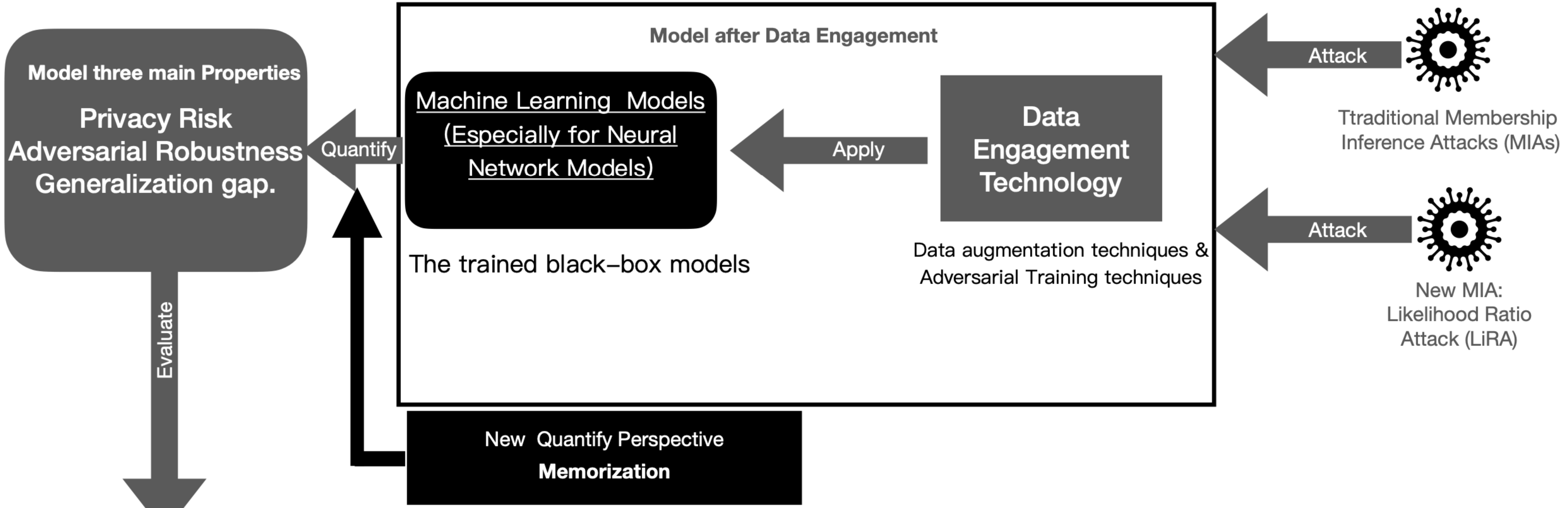
Other Methods for Security and Privacy Preserving

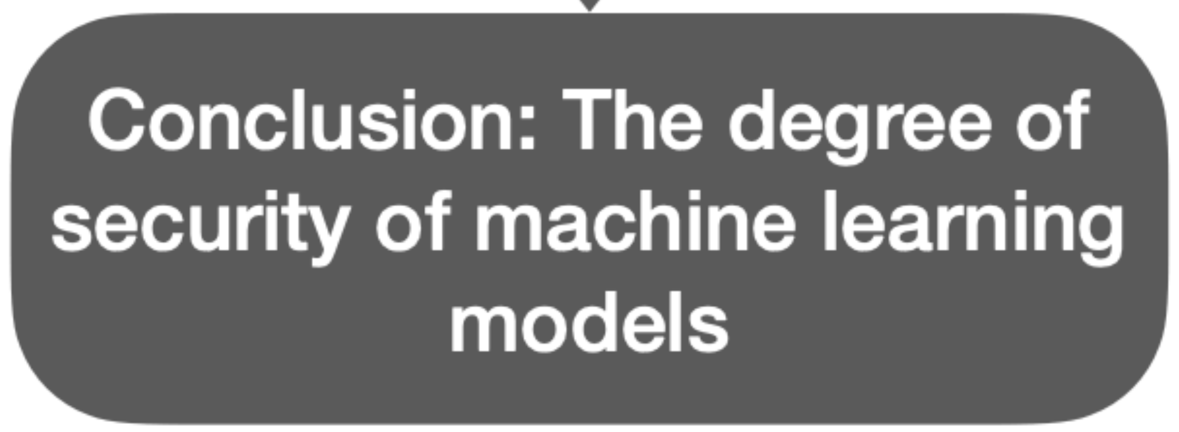
1. Quantum information encryption



POLITECNICO MILANO 1863

2. Machine learning privacy protection or transfer learning, federated learning





Problem: Black-box models may reveal sensitive information, may pose security concerns.

Reference:

1. Krizhevsky Alex, Hinton Geoffrey, et al. Learning multiple layers of features from tiny images. 2009. 4
2. Nicholas Carlini, Steve Chien, Milad Nasr, Shuang Song, Andreas Terzis, and Florian Trame`r. Membership inference attacks from first principles. In IEEE Symposium on Security and Privacy (S
3. Nicholas Carlini, Chang Liu, U´lfar Erlingsson, Jernej Kos, and Dawn Song. The secret sharer: Evaluating and testing unintended memorization in neural networks. In USENIX Security Symposiu
Nicholas Carlini Trame`r, Eric Wallace, Matthew Jagielski, Ariel Herbert-Voss, Katherine Lee, Adam Roberts, TomB. Brown, Dawn Song, U´lfar Erlingsson, Alina Oprea, and Colin Raffel. Extracting
In USENIX Security Symposium (USENIX), pages 2633–2650, 2021. 1
5. Christopher A. Choquette-Choo, Florian Trame`r, Nicholas Carlini, and Nicolas Papernot. Label-only membership in-ference attacks. In Int. Conf. Mach. Learn. (ICML), pages 1964–1974. PMLI
6 .https://arxiv.org/pdf/2208.08270.pdf

Thanks to Dr. Qiongxiu Li (Tsinghua University) help!

POLITECNICO
MILANO 1863

Jan.18 2023