



Federated Learning and Supercomputing: New Opportunities for International Cooperation

2026 Russian Supercomputing Days



MINISTÉRIO DA
**CIÊNCIA, TECNOLOGIA
E INOVAÇÃO**

Prof. Vladimir Voevodin in Shanghai, 2023



-  Climate and disaster resilience — Joint forecasting and early-warning models.
-  Cross-border health research — Collaborative models with patient records held locally.
-  Multilingual AI — Models for regional languages.
-  Smart grids and energy — Demand forecasting, renewables, and fault detection.
-  Scientific foundation models — Joint research in materials, chemistry, agriculture, and biodiversity.

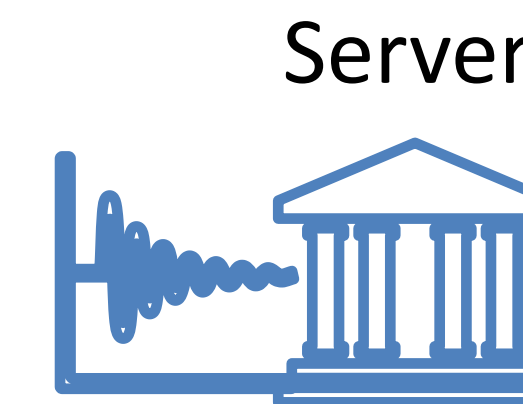


Building the Collaboration

-  Privacy and security research — Secure aggregation, encryption, and training.
-  Interoperable HPC network — Supercomputers for federated experiments.
-  Benchmarks, training, and mobility — Shared evaluations, exchanges, and summer schools.
-  Governance and standards — Common documentation, provenance, and audit trails.
-  Joint funding and infrastructure — Multinational calls and shared pilot projects.

Federated Learning

- Federated Learning is more than Distributed Learning and mightn't be parallel
- Big Data: Privacy, Bandwidth, Latency, Cost, Feasibility, ...
- Cross-devise Federated Learning
- Cross-silo Federated Learning
- Receives a model and gives data aggregated
- Federate Analytics is local analyses of raw data

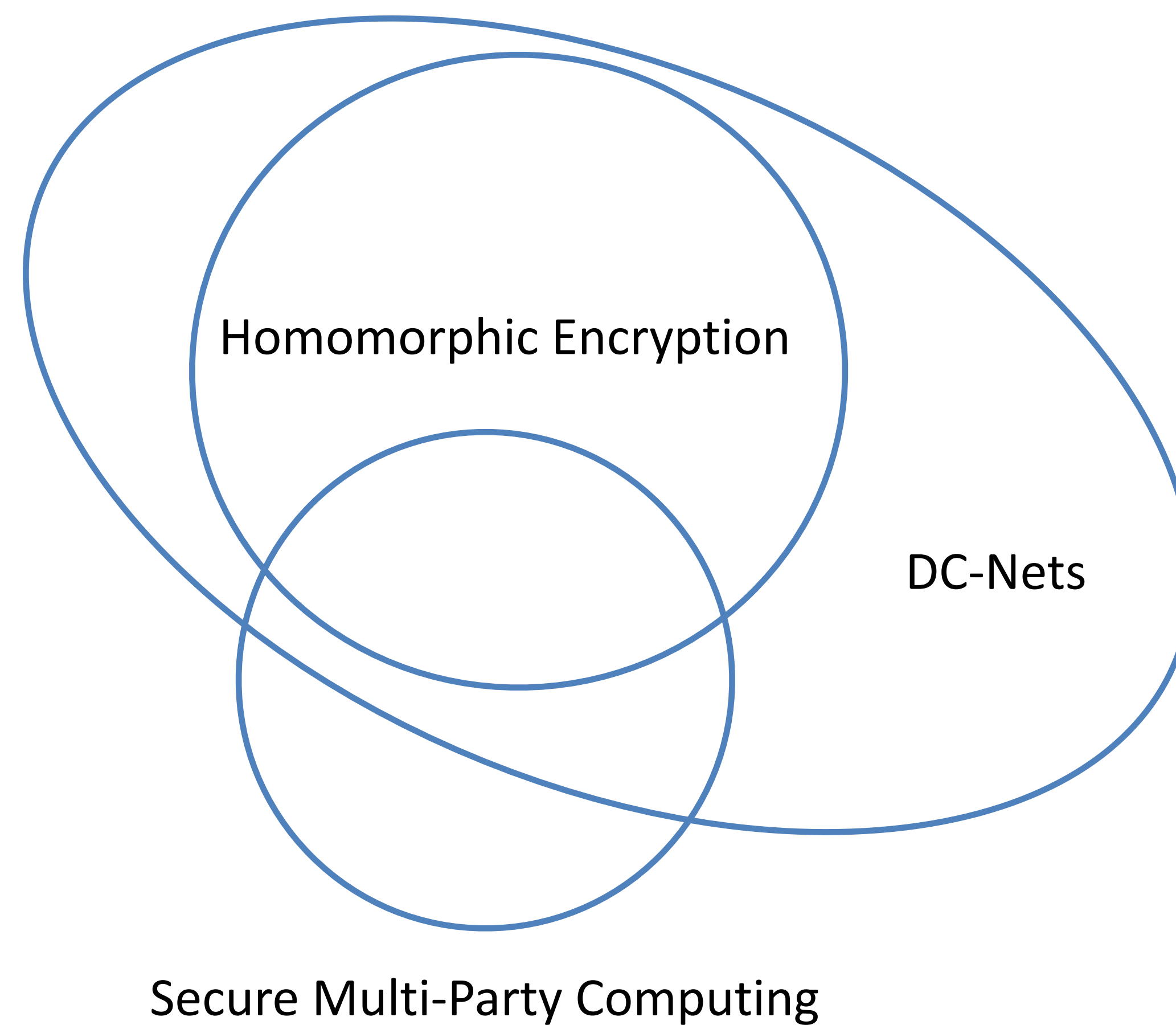




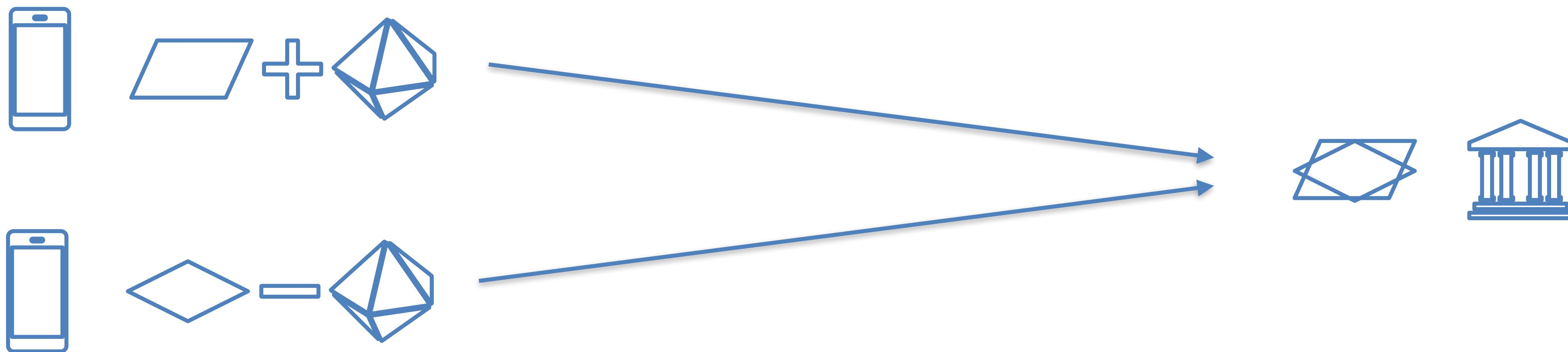
Attack

- Deceptive client
- Recovering data from the gradients
- De-anonymization

■ Aggregation



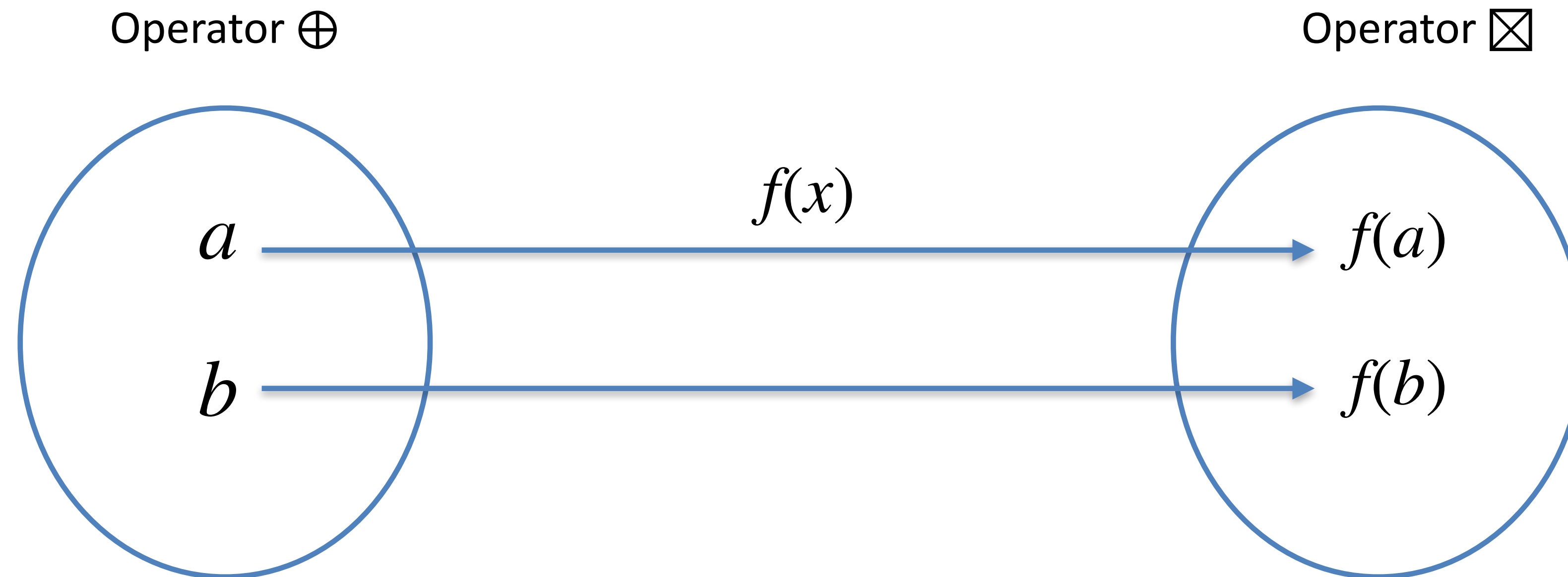
DC-Nets (Dining cryptographers problem)



$$\mathfrak{M}_{i,j} \stackrel{\text{def.}}{=} \text{Enc}(m_{i,j}) = m_{i,j} + \sum_{o \in \mathcal{M} - \{i\}} \text{H}(k_{i,o} \parallel j) - \text{H}(k_{o,i} \parallel j).$$

DC-Nets (Dining cryptographers problem)

PROPERTIES	SDC-Net	AHEP	ADC-Net
Resistance to collusion of $O(\tilde{i})$ users	✓	✗	✓
Set of trusted users	✓	✗	✓
Messages to the counting agent	✓	✗	✓
Minimum number of messages	✓	✓	✓
Scalable	✗	✓	✓
Permanent keys	✓	✓	✓
Based on trapdoors	✓	✓	✓
Keys stored per user	$2(\tilde{i} - 1)$	1	1
Total number of keys	$O(\tilde{i}^2)$	2	$O(\tilde{i})$
Polynomial time	✓	✓	✓
Resistance to disruption by a single user	✗	✗	✓
Verification as cryptographic commitment	✗	✗	✓



$$f(b \oplus b) = f(a) \boxtimes f(b)$$

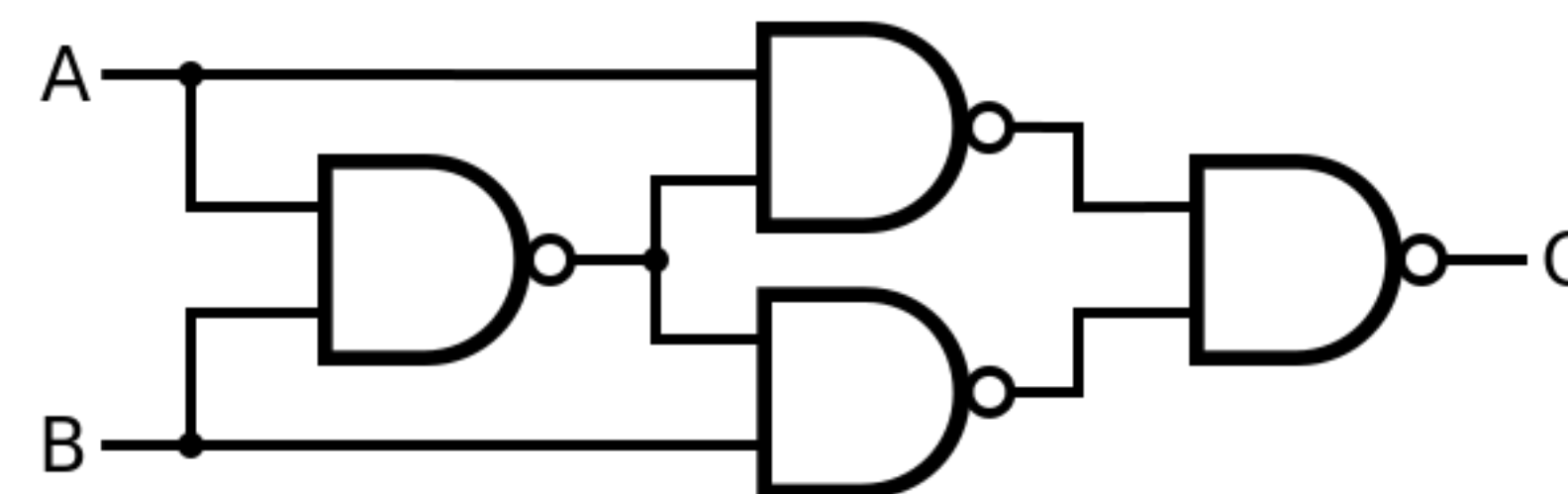
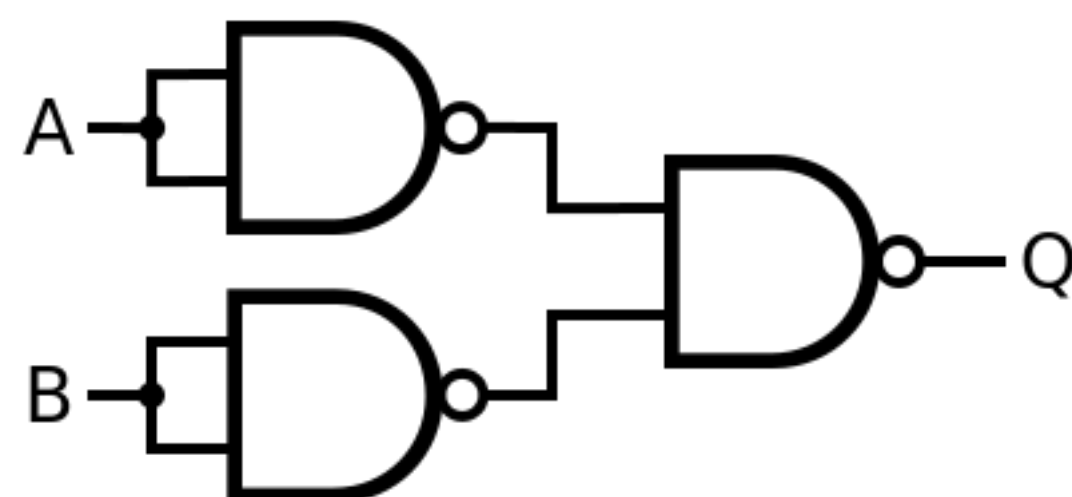
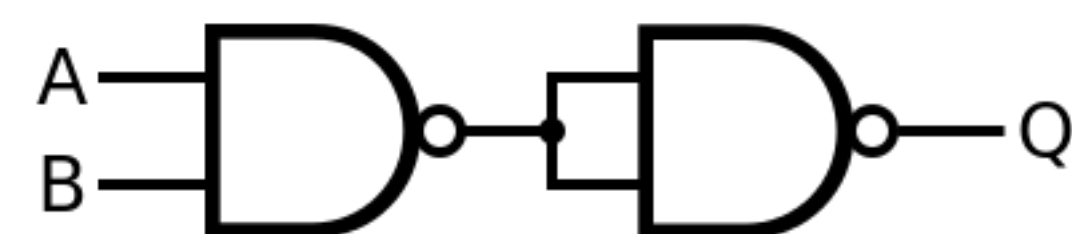


Homomorphism

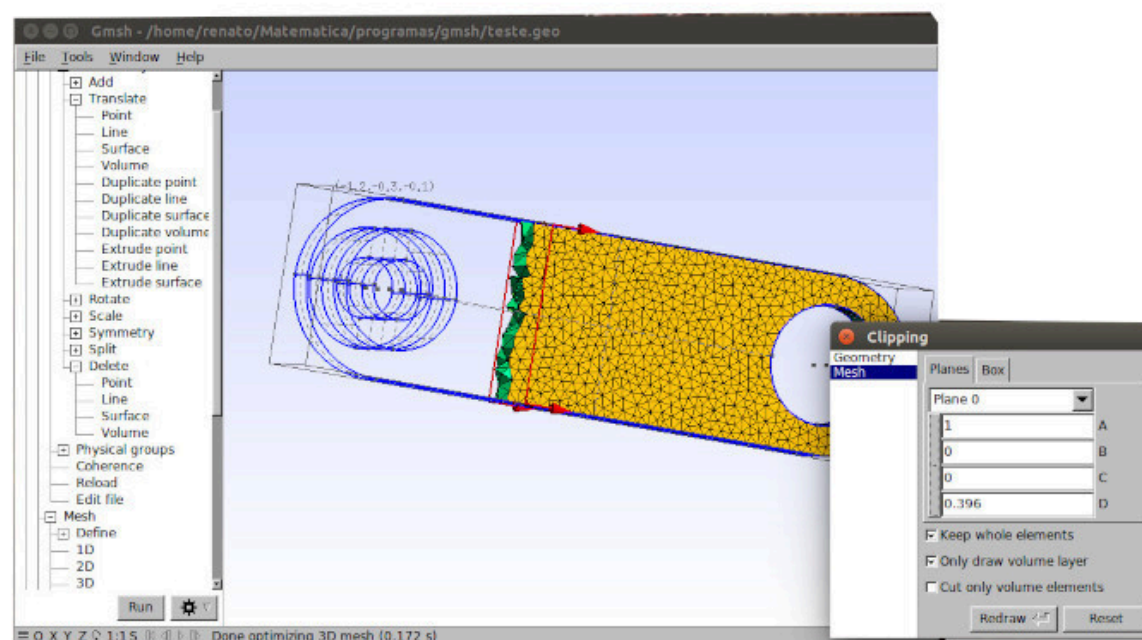
$$m_1^e \times m_2^e = (m_1 \times m_2)^e$$

$$r^{m_1} \times r^{m_2} = r^{m_1+m_2}$$

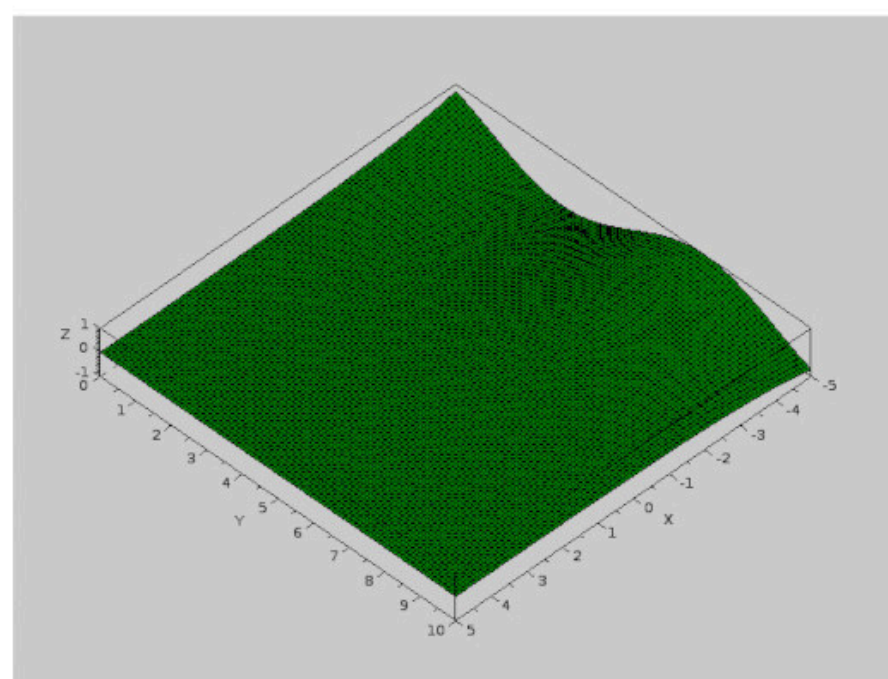
$$\text{NAND}(a, b) = a \times b + 1 \mod 2$$



Homomorphic Encryption in a Client-Server Scenario



Physical problem



Solution

Public Key



Encrypt



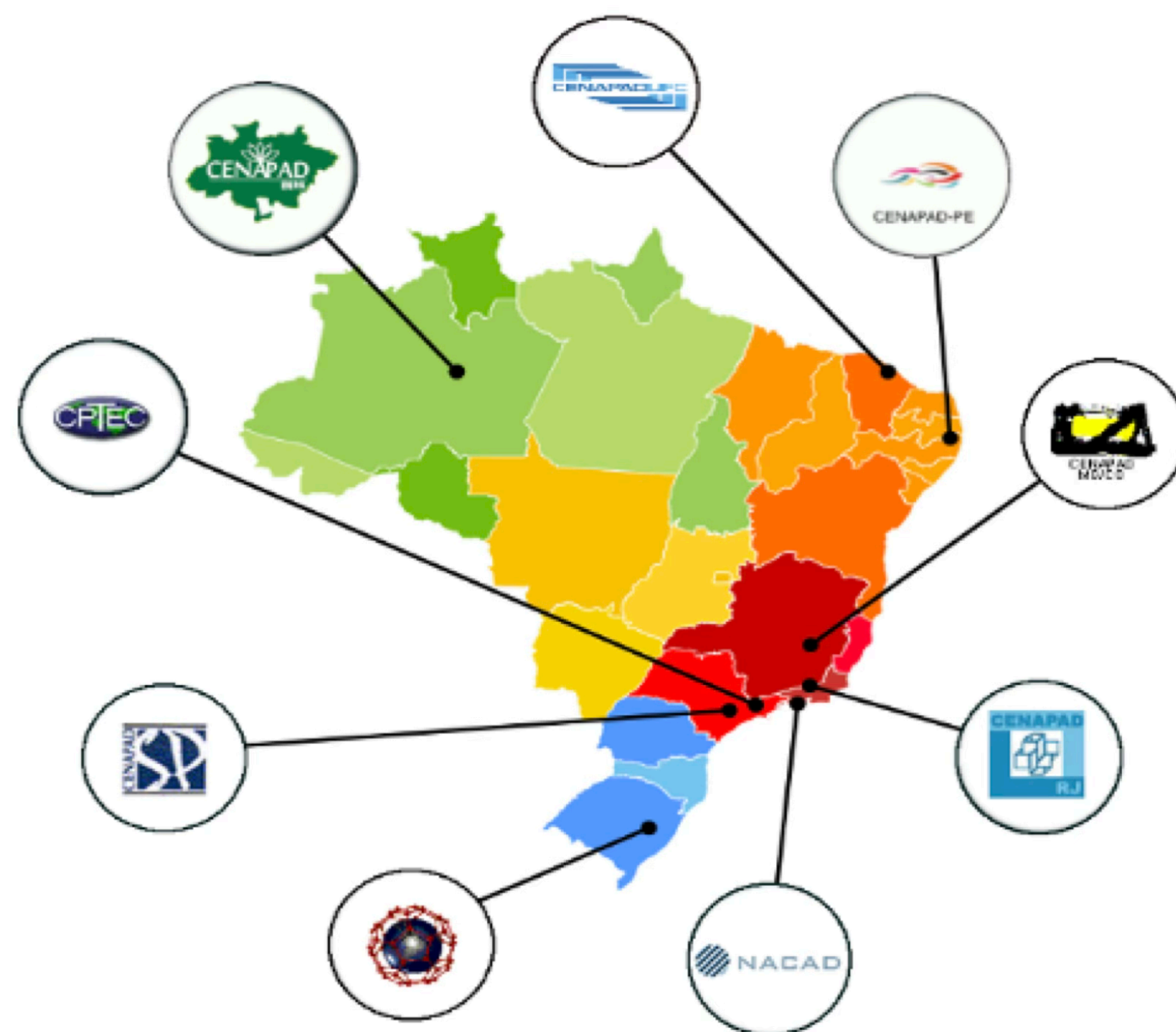
Private Key

Decrypt



Server

SINAPAD Brazil's shared national capacity



- **12 nodes** in the renewed network.
- **5 designations completed:** LNCC, UFRN, UNICAMP, UFG, and UFRGS.
- **7 designations underway:** UFRJ, UFMG, UFAM, UFPI, UFES, INPA, and INPE.
- Presence across **all five Brazilian regions**.
- A combination of national, regional and thematic capabilities.

9

historical centers

The 2025 governance framework adds CENAPAD-IA centers and opens SINAPAD to new qualified members.

Current governance

MCTI coordinates • LNCC runs the Executive Secretariat • RNP sits on the Governing Council



20

PFLOP/s installed +

4 PB

parallel storage

3

accelerator families

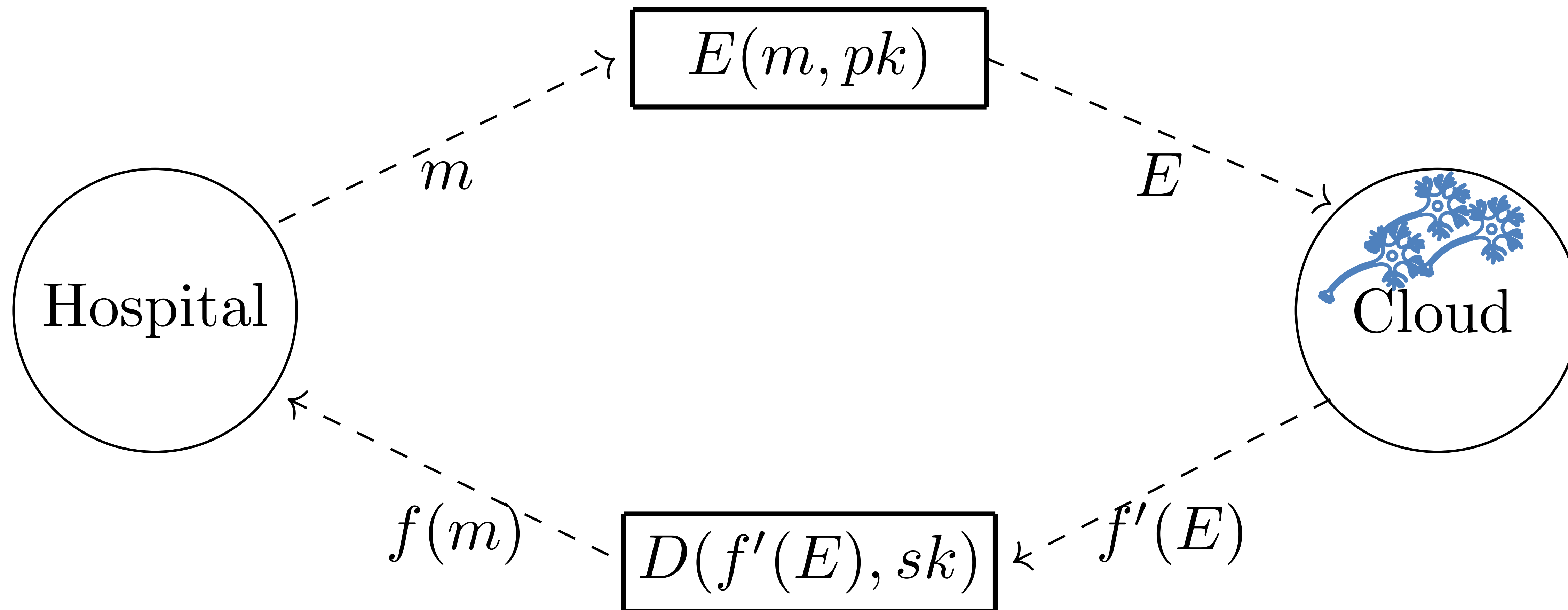
NVIDIA H100 • NVIDIA GH200 • AMD MI300A

The hybrid architecture supports simulation, data-intensive science and AI on one national platform.

Top 1 Academic HPC in Top500 in LA (2024, 89), ..., (2026, 141)

Top 1 Green500 in LA

LNCC has 15/17 United Nations Sustainable Development Goals in Scopus



- Bootstrapping decrypts and encrypts to control the error.
- Relinearization evaluates the multiplication with the private key.

- $\mathcal{R}_q = \mathbb{Z}_q[X]/(X^N + 1)$

- $\text{Enc}(\mu, p) = C = (c_0, c_1) = (\mu, 0) + p = (b + \mu, a) \in \mathcal{R}_q^2$

- $\text{Dec}(C, s) = c_0 + c_1 \cdot s = \mu + e$

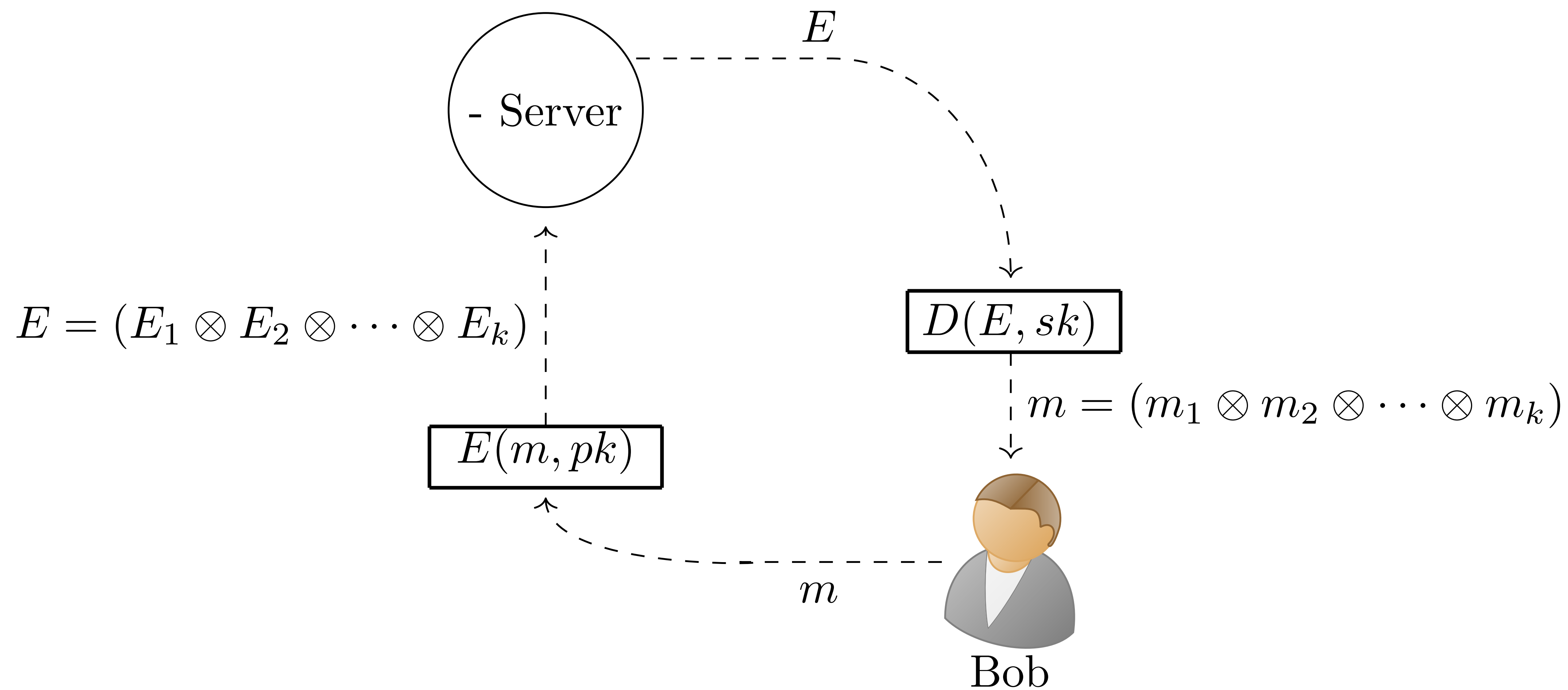
- $C_1 + C_2$

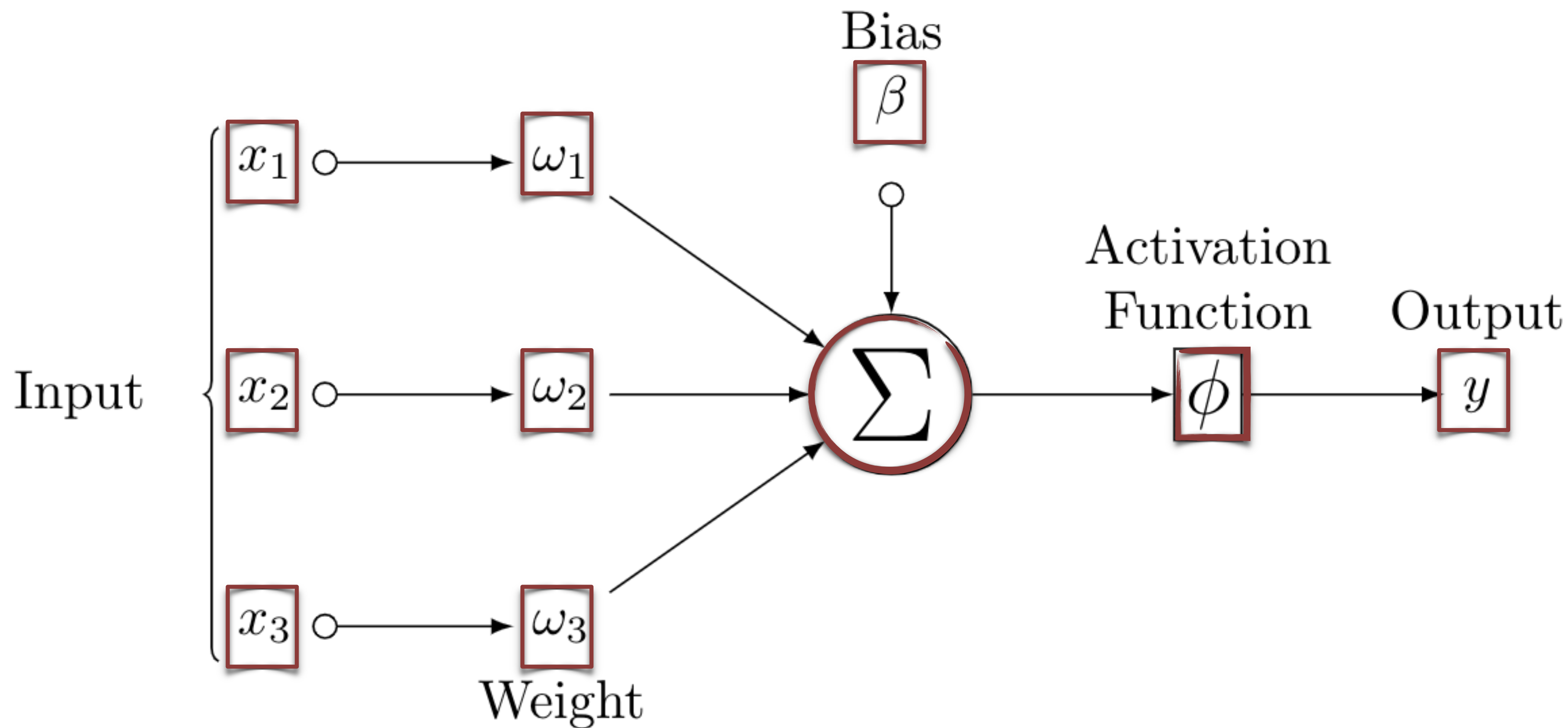
- $C_1 \times C_2$

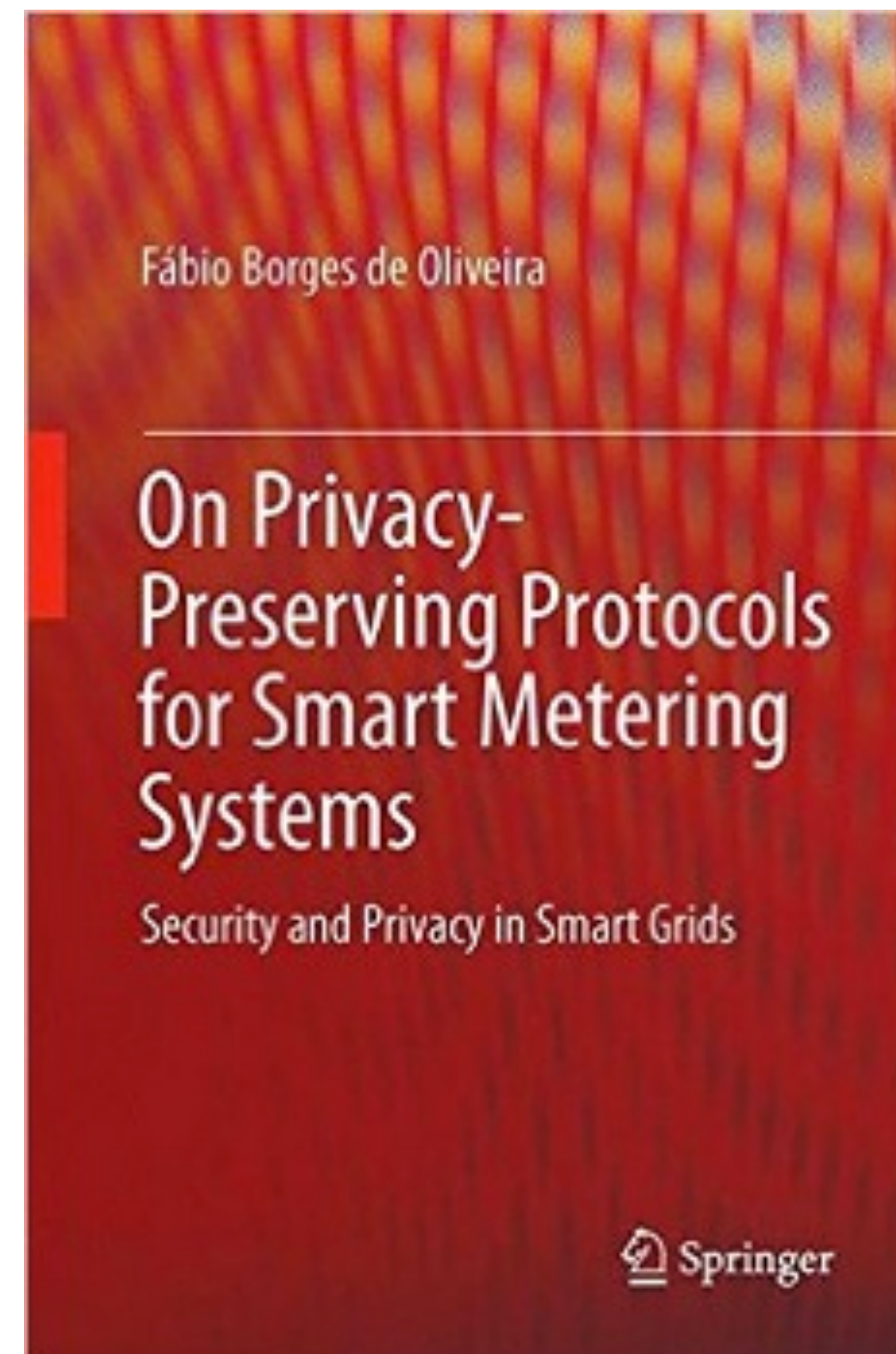
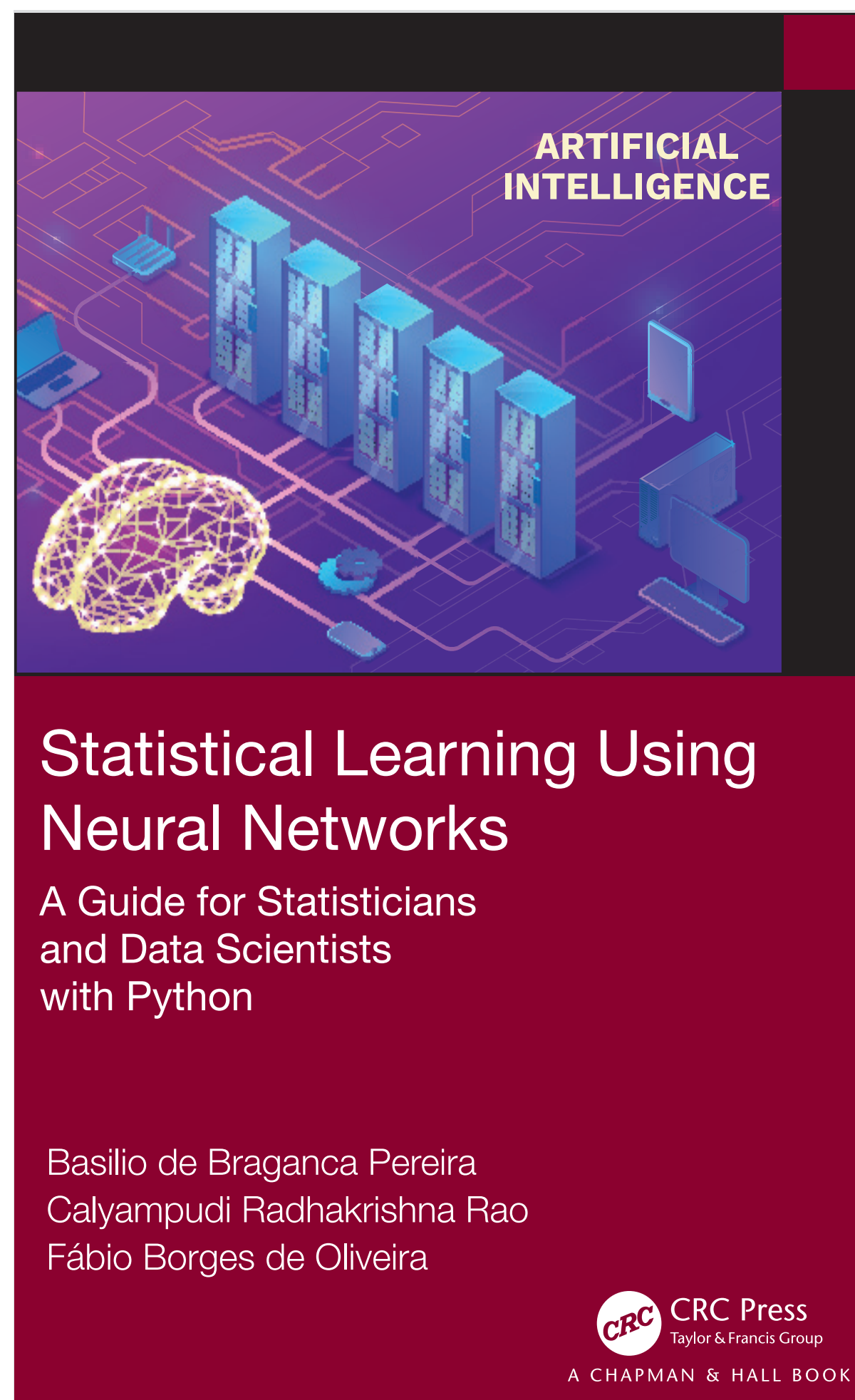
$$\text{Enc} : \mathbb{Z}_n \times \mathbb{Z}_n^* \rightarrow \mathbb{Z}_{n^2}$$

$$\text{Enc}(m_{i,j}, r_{i,j}) \mapsto g^{m_{i,j}} \cdot r_{i,j}^n \mod n^2$$

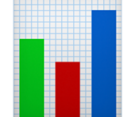
$$\text{Dec} \left(\prod_{i=1}^{\tilde{t}} \text{Enc}(m_{i,j}) \mod n^2 \right) = \sum_{i=1}^{\tilde{t}} m_{i,j} \mod n$$







Opportunities for International Cooperation

-  Connect HPC centers — Run federated experiments across nations.
 -  Advance AI for science — Train models using scientific data.
 -  Develop large-scale and multimodal models — Combine local expertise.
 -  Scale federated training — Scheduling, communication, and performance.
 -  Protect data and model updates — Develop secure aggregation.
 -  Create shared benchmarks — Evaluate accuracy, scalability, and security.
 -  Build lasting research teams — Launch joint pilots, researcher exchanges, and training activities.
- From a community of HPC centers to a distributed ecosystem for scientific AI.

Prof. Vladimir Voevodin in Nizhny Novgorod, 2024





спасибо 谢谢
GRACIAS 谢谢
THANK YOU
ありがとうございました MERCI
DANKE धन्यवाद
شُكراً OBRIGADO