

Homomorphic Inference of Deep Neural Network

USING TFHE [CGGI16]

Samuel Tap - Zama samuel.tap@zama.ai



Agenda

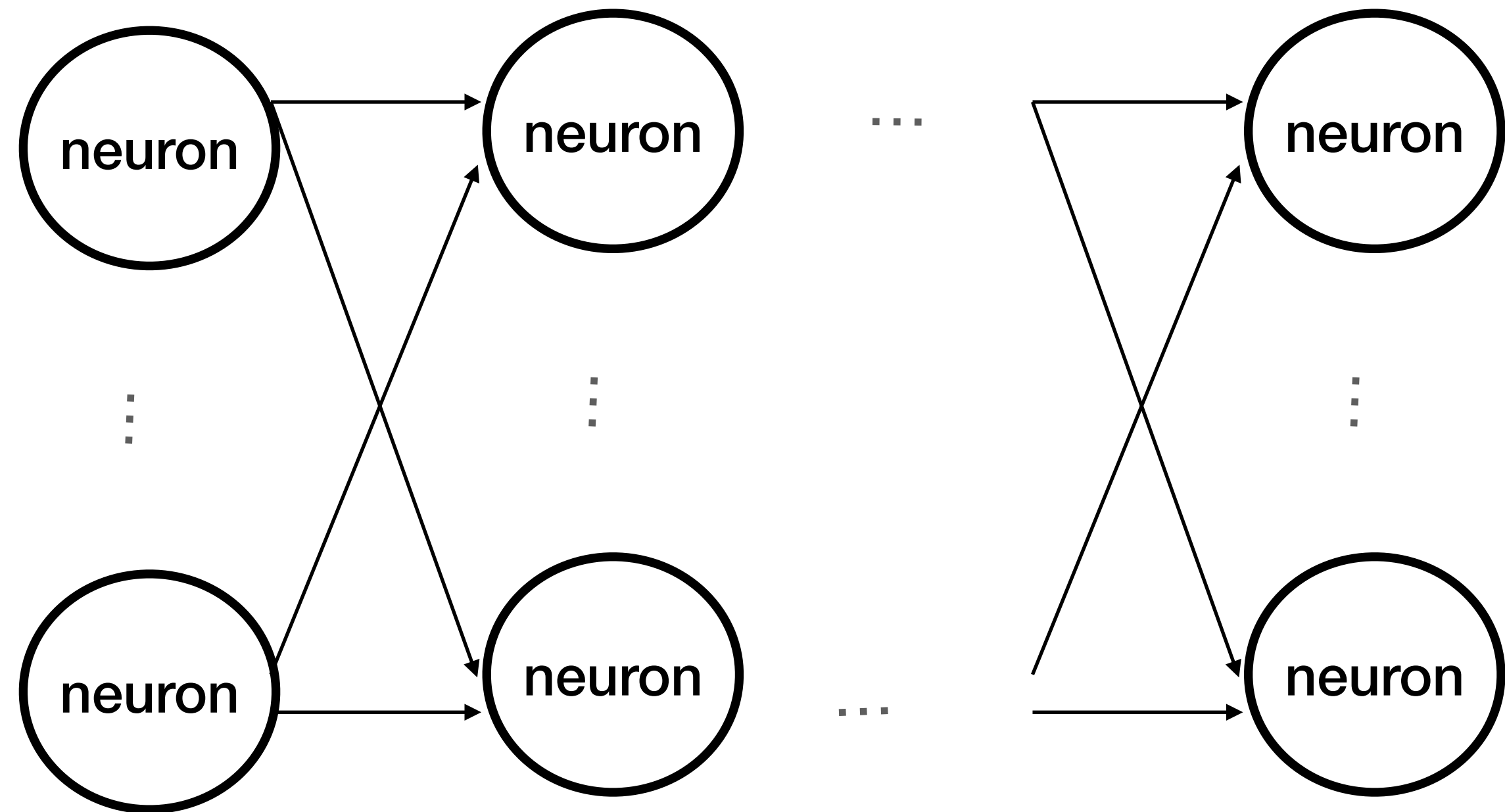
- 1. Problem**
- 2. Toward Homomorphic Neuron**
- 3. Conclusion**

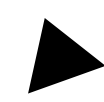
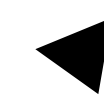
Me

- One year of research at Zama => speed up homomorphic inference
- Co-author of Concrete Library

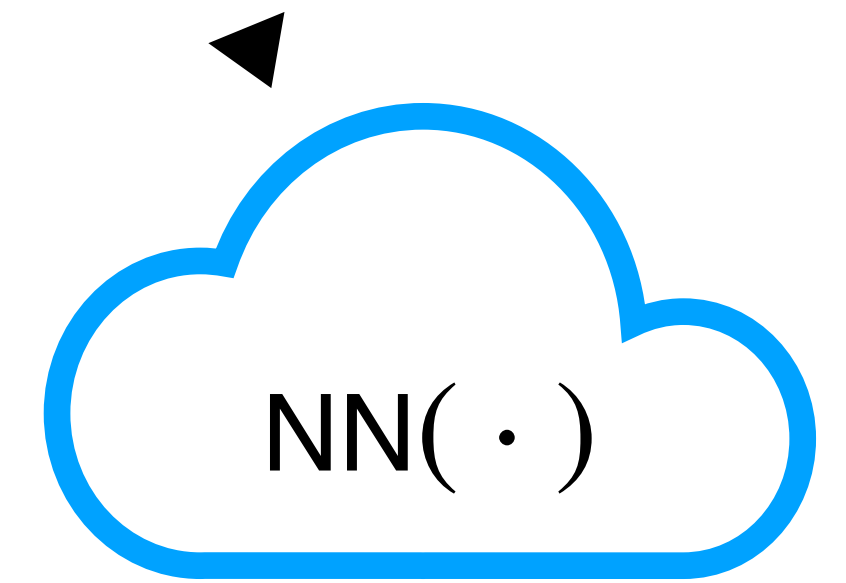
- PhD Director: Teddy Furon (INRIA)
- PhD Supervisor: Pascal Paillier (ZAMA)

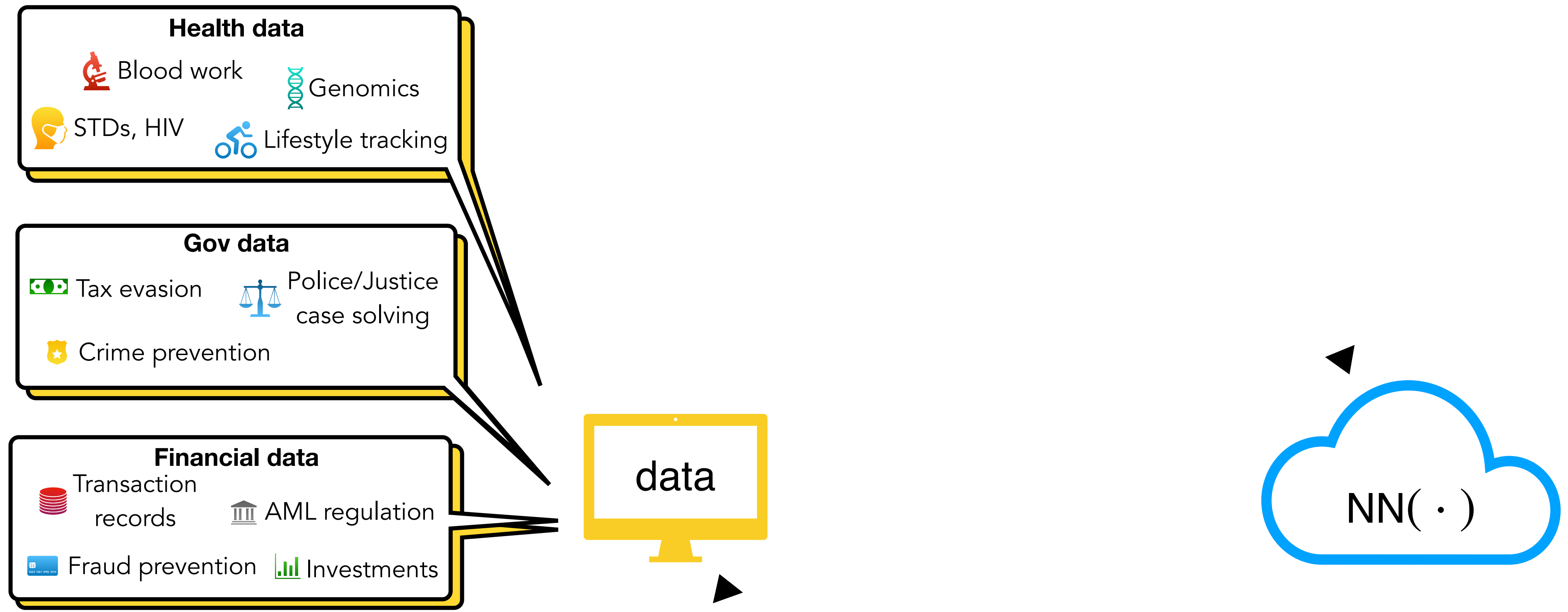
Neural Network

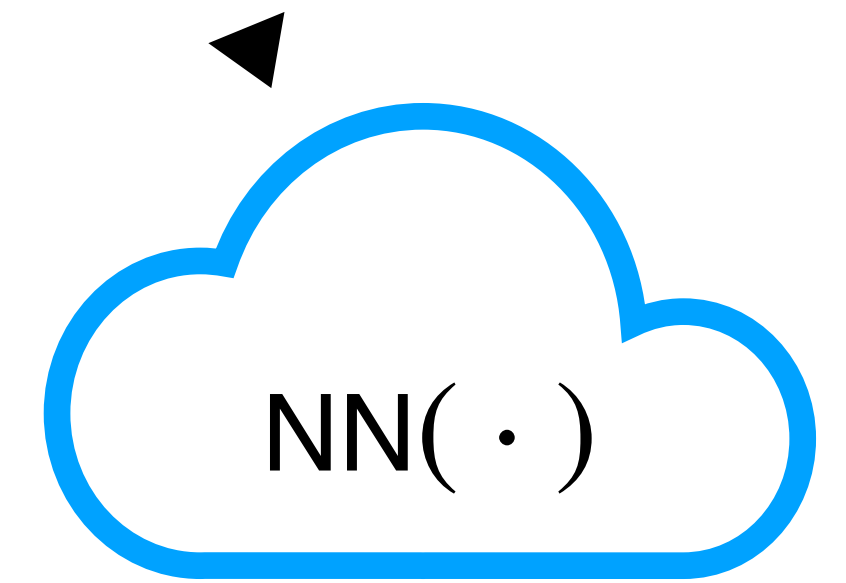


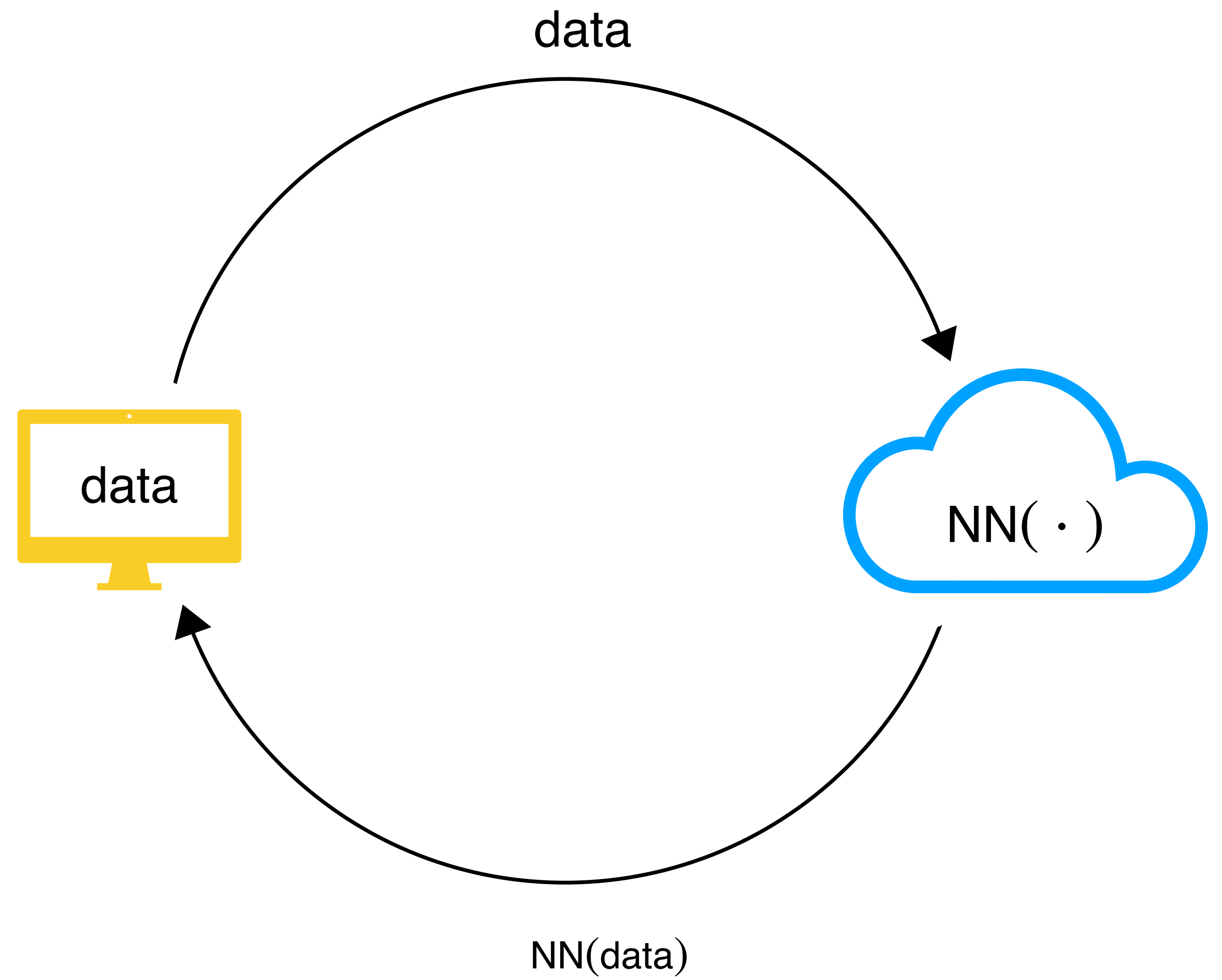






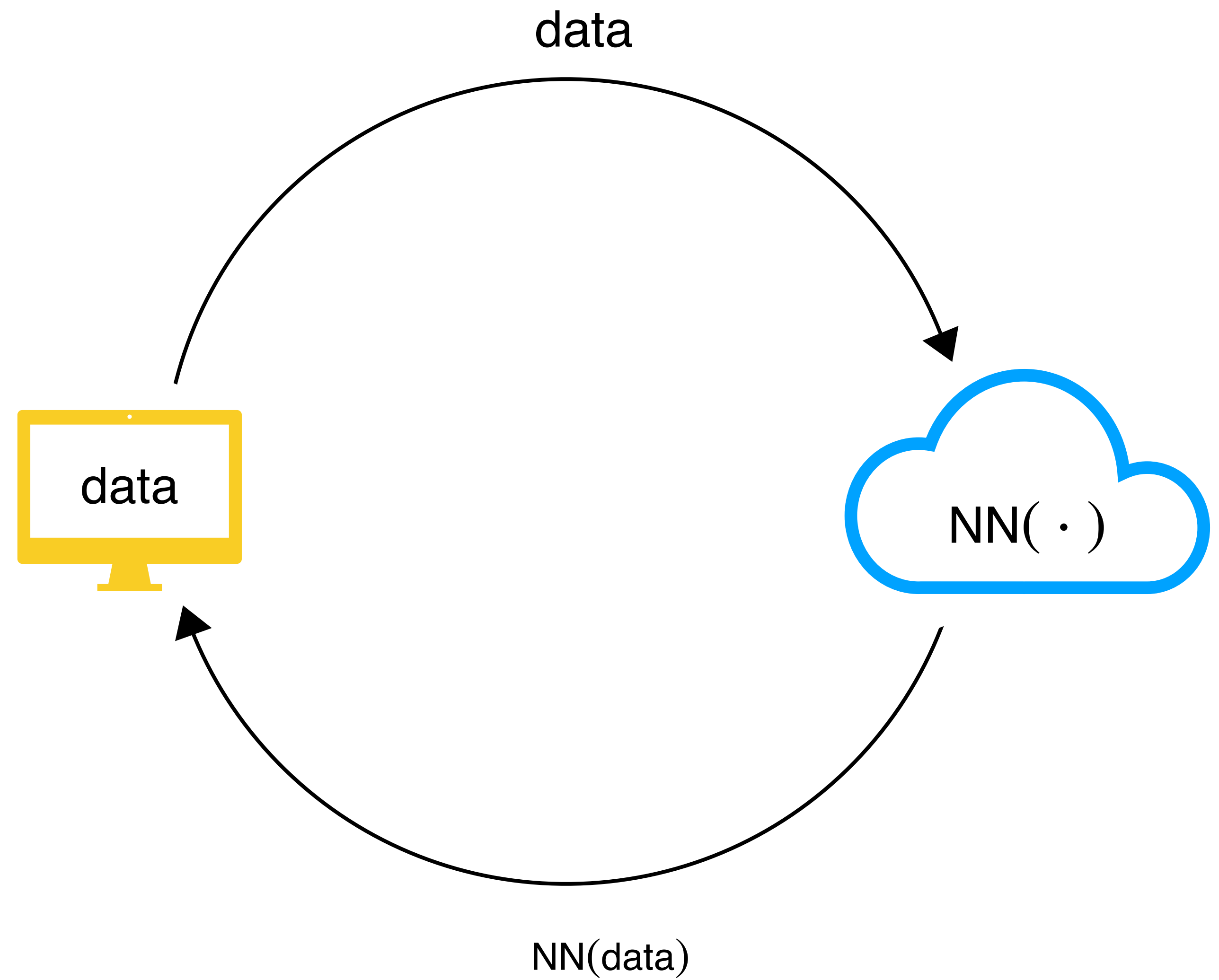






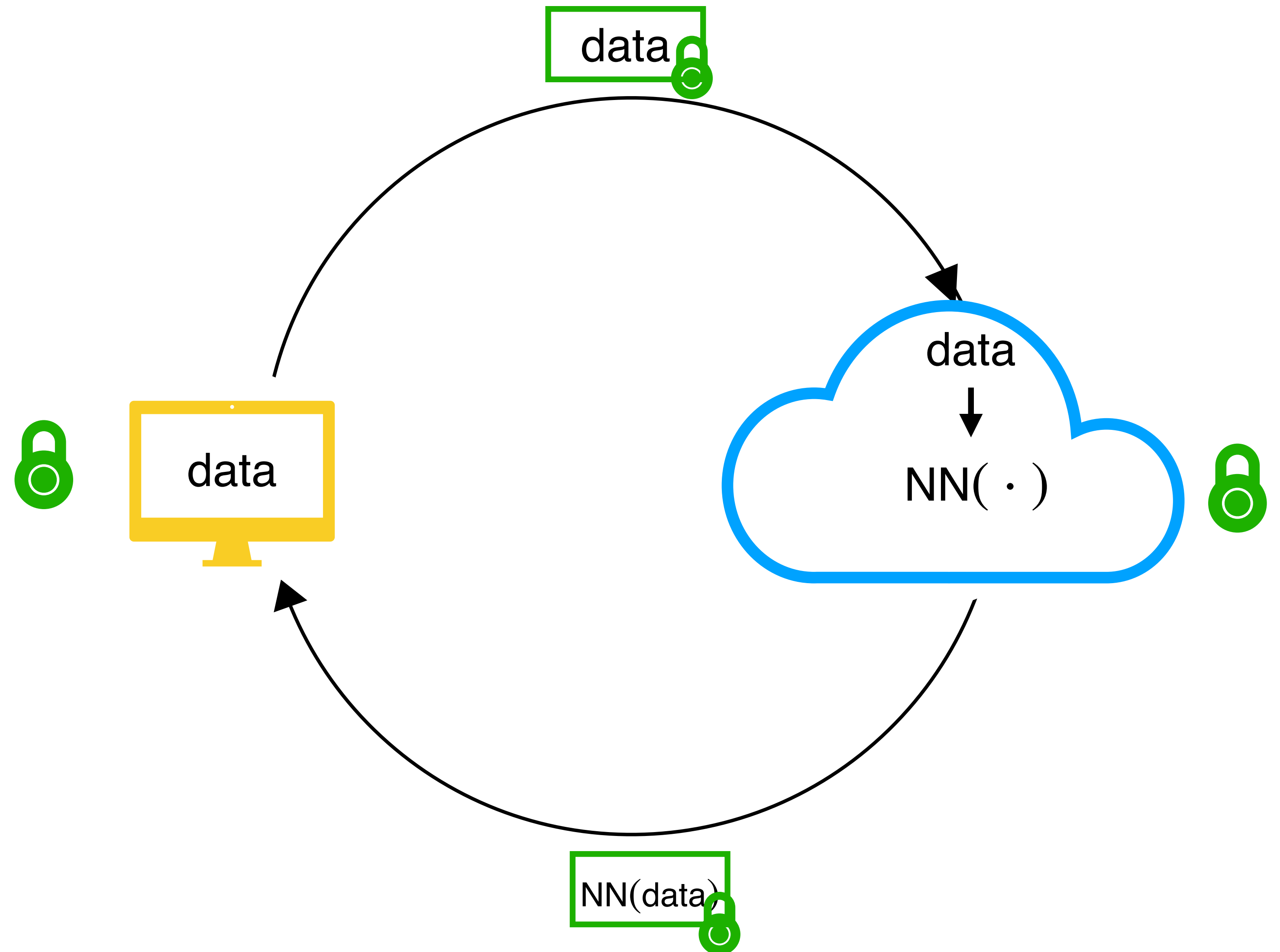
Past

X in transit
X in processing



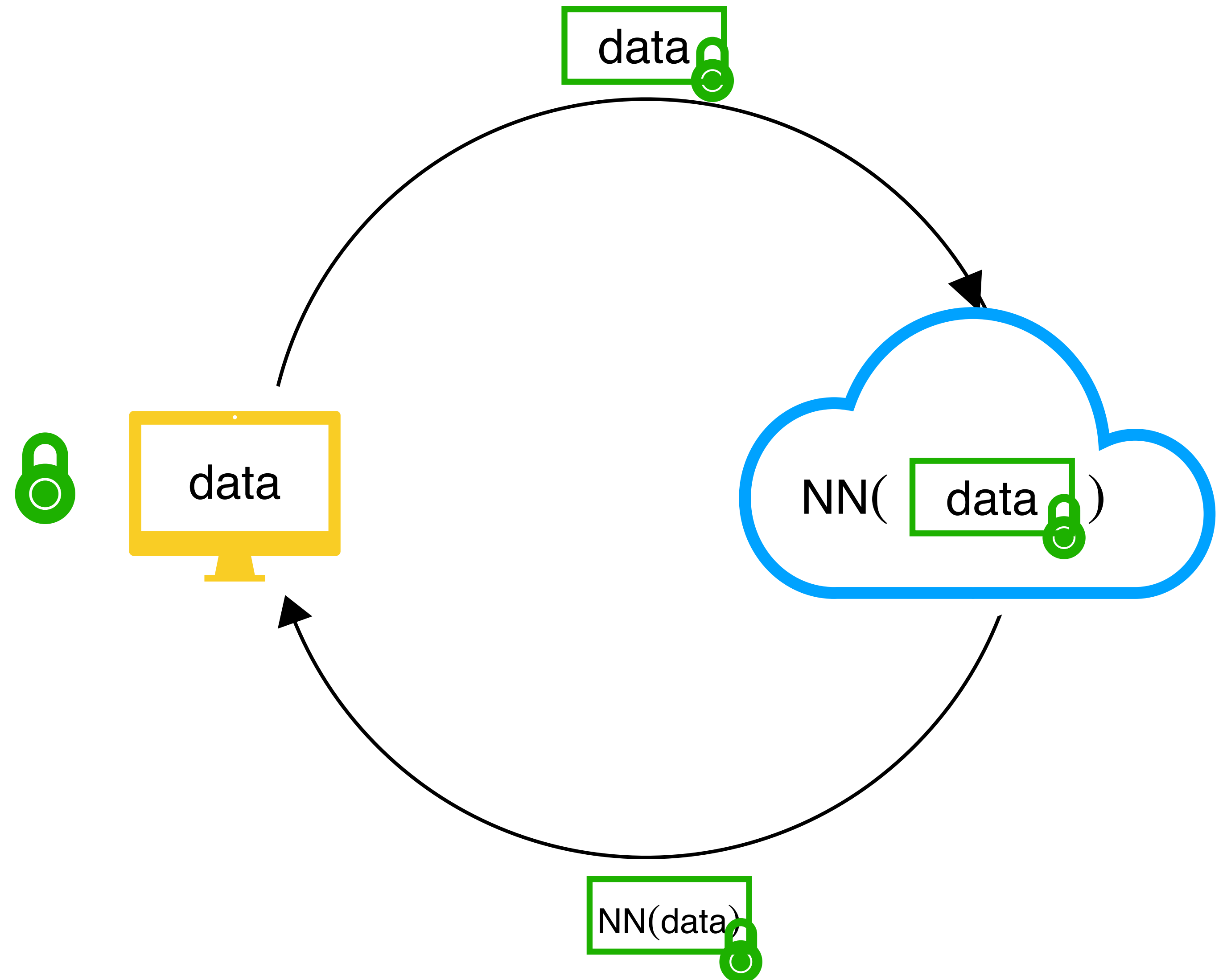
Present

 in transit
 in processing



(One) Future

 in transit
 in processing



Problematic

Homomorphic Inference

Encrypted Neural Network

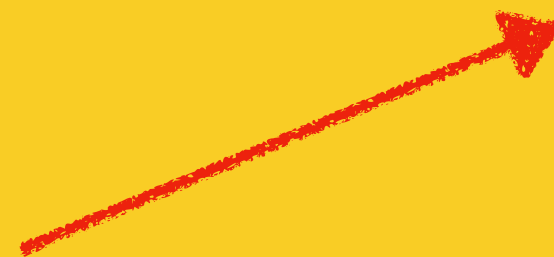
Homomorphic Training

HOW ?

FHE using TFHE

HOW ?

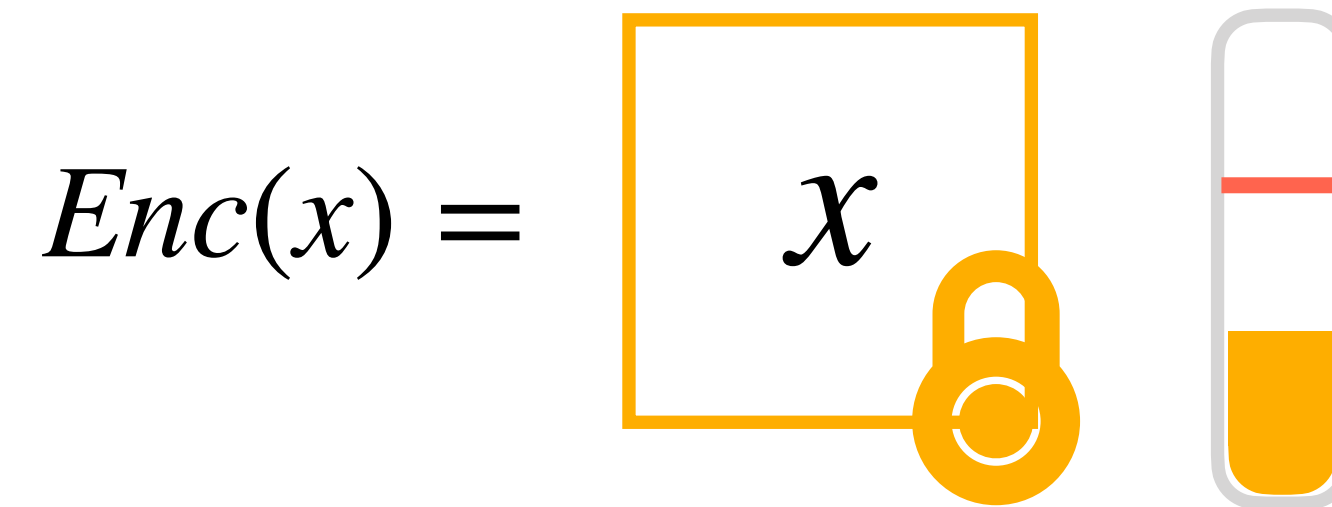
FHE using TFHE



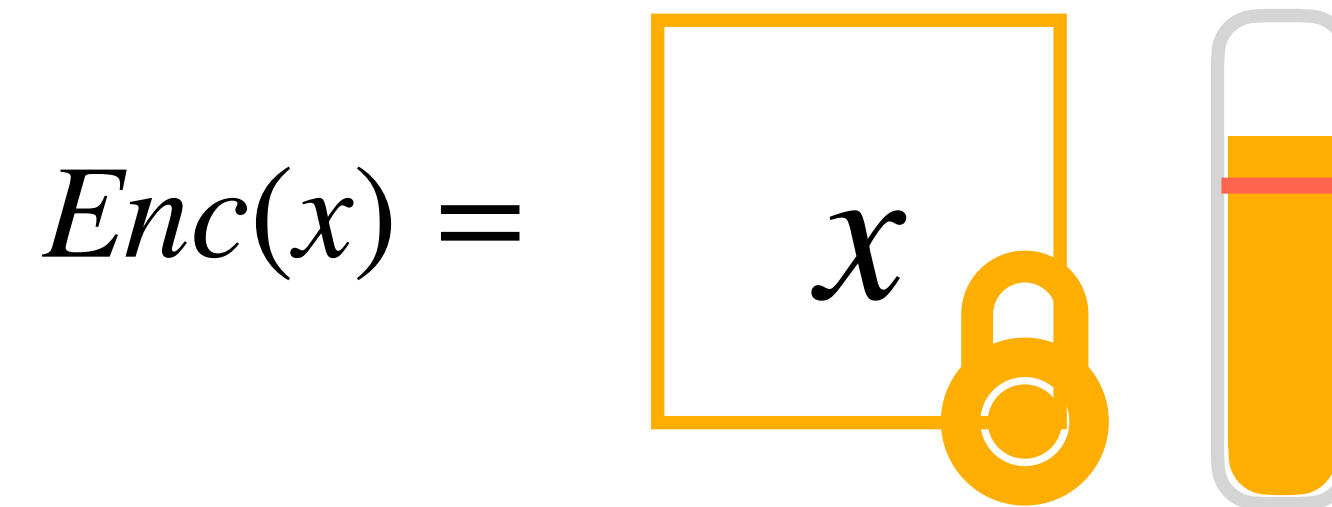
Fully Homomorphic
Encryption

Noise in ciphertexts

Security rely on
LWE / RLWE
hardness
assumption



decryptable



incorrect decryption

Fully Homomorphic Encryption

Fully Homomorphic Encryption

m_1

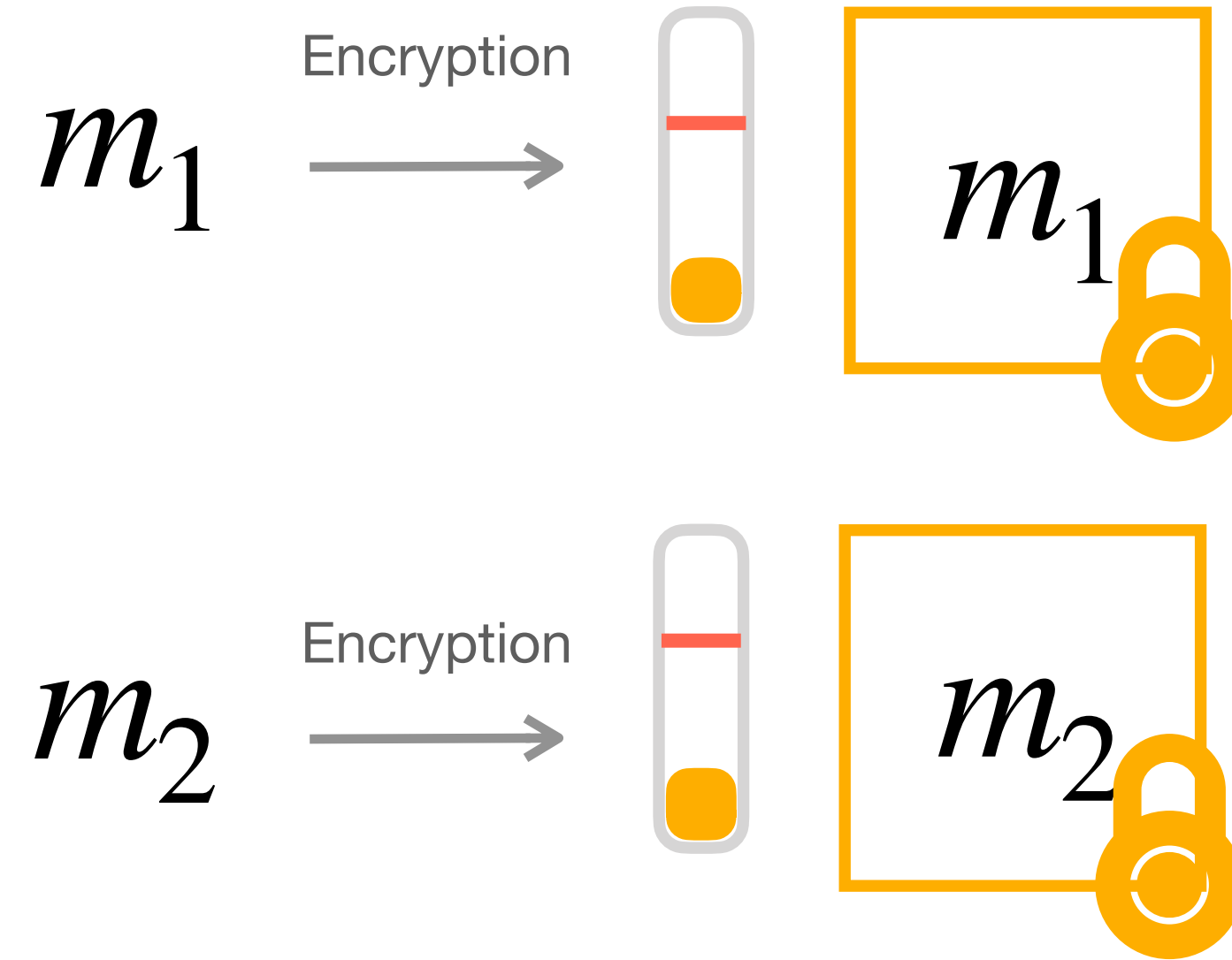
m_2

Fully Homomorphic Encryption

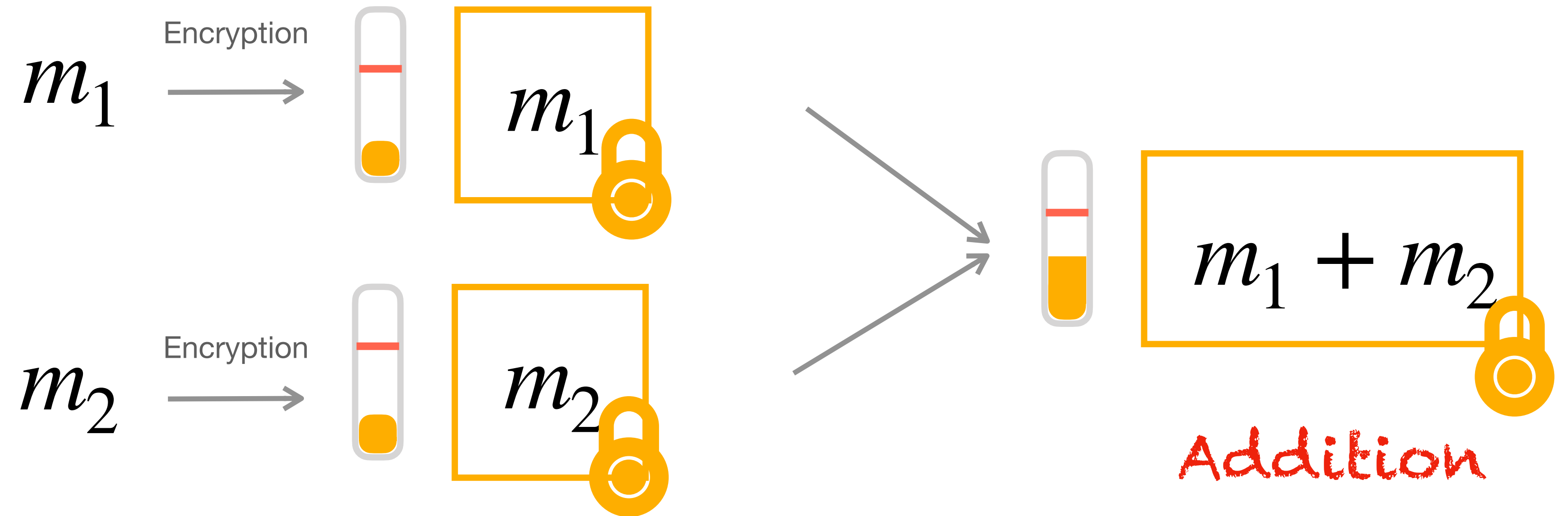
m_1 Encryption
 →

m_2 Encryption
 →

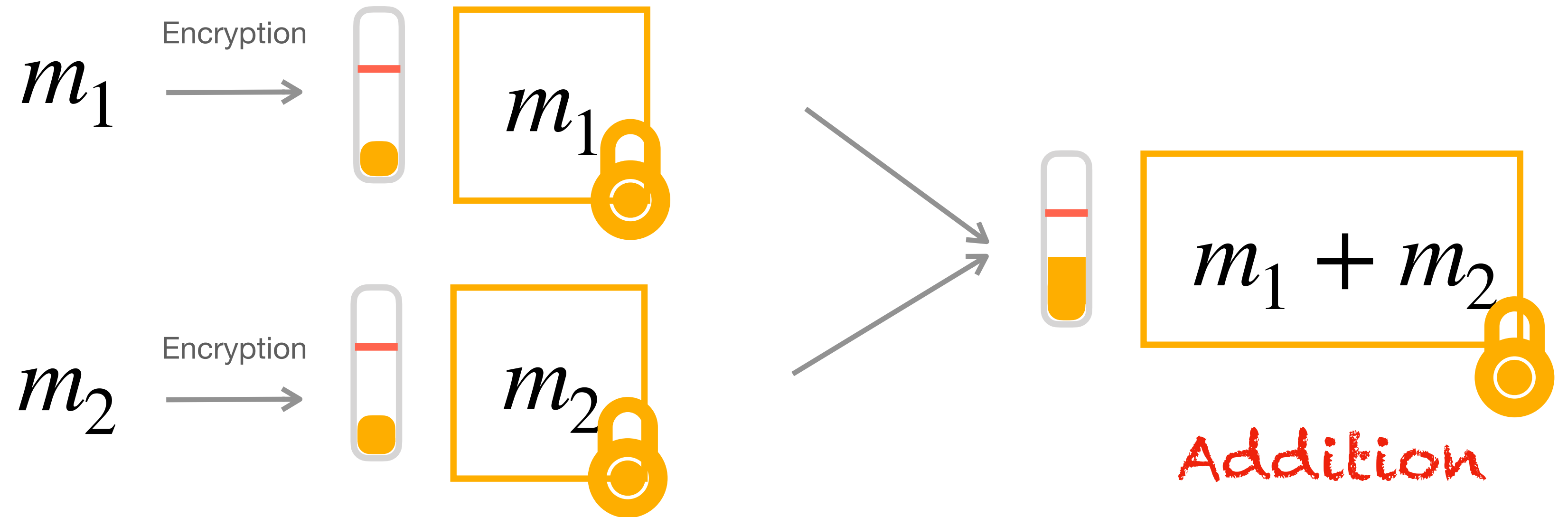
Fully Homomorphic Encryption



Fully Homomorphic Encryption



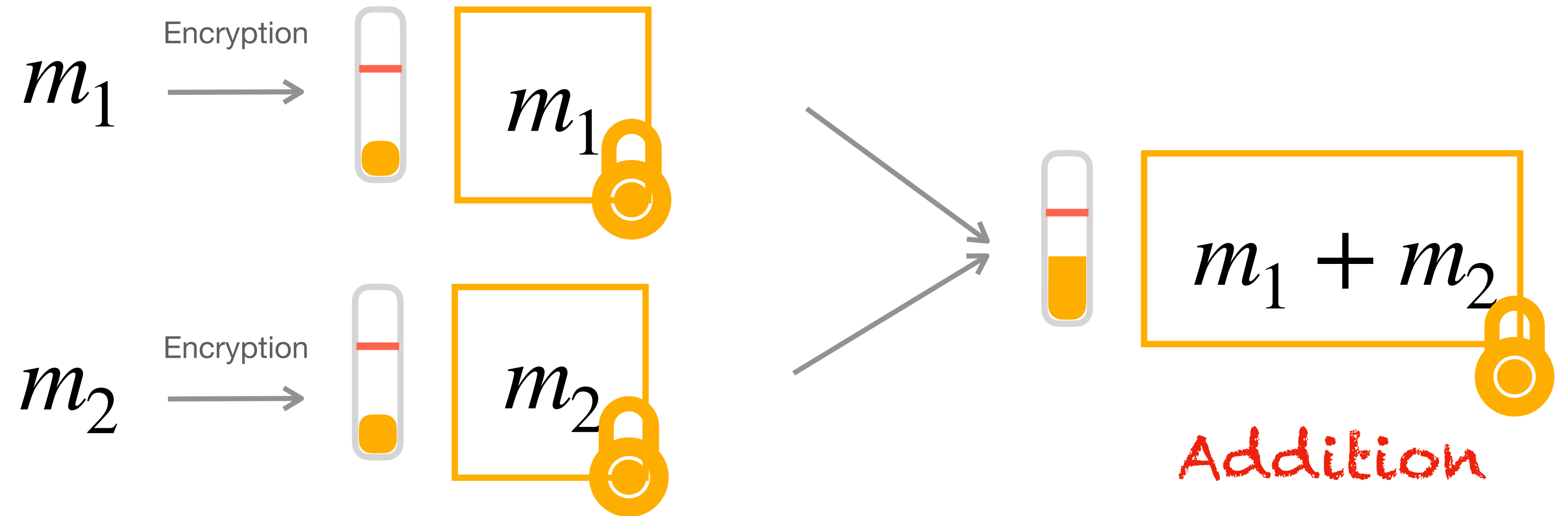
Fully Homomorphic Encryption



m_1

m_2

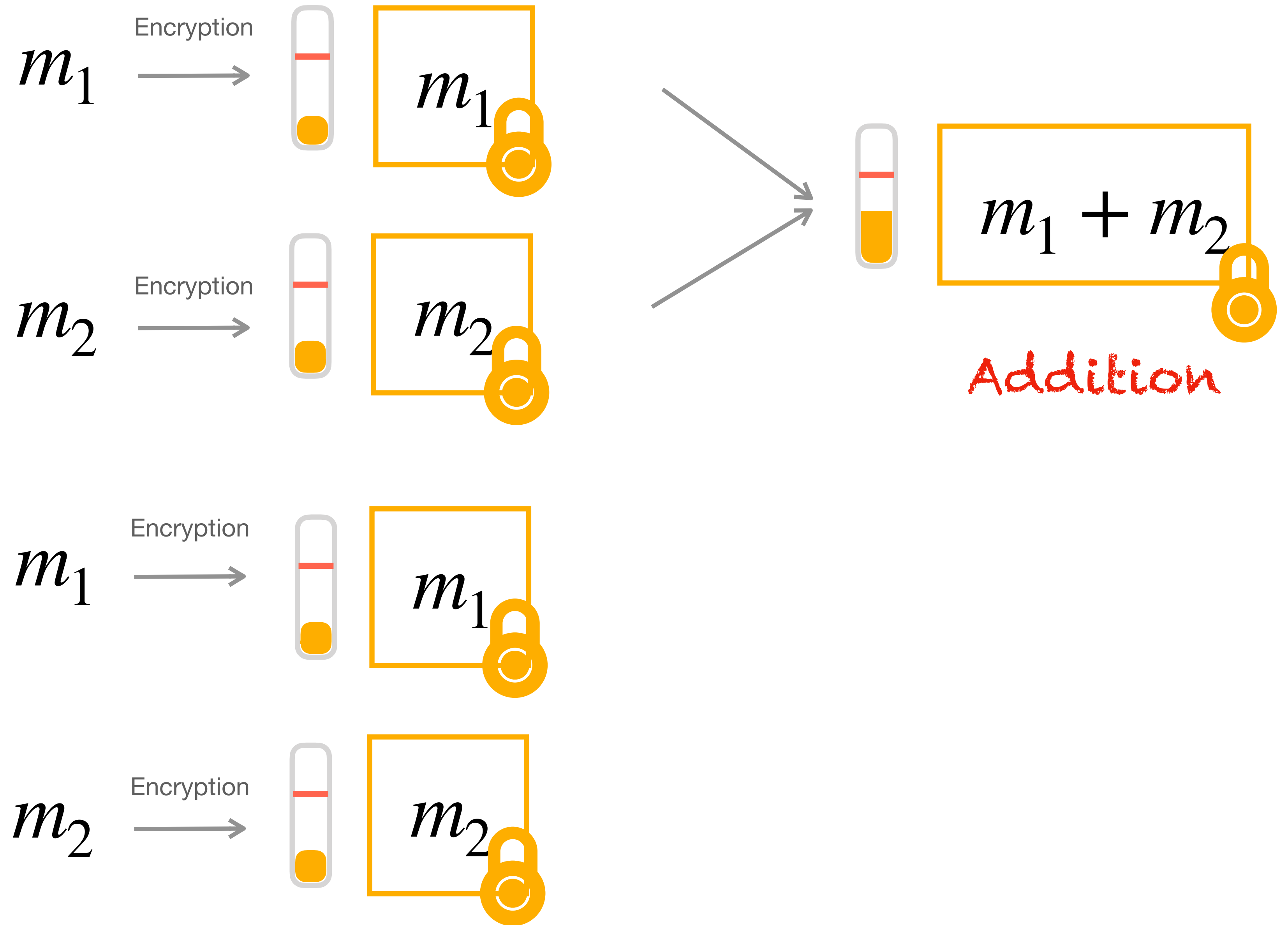
Fully Homomorphic Encryption



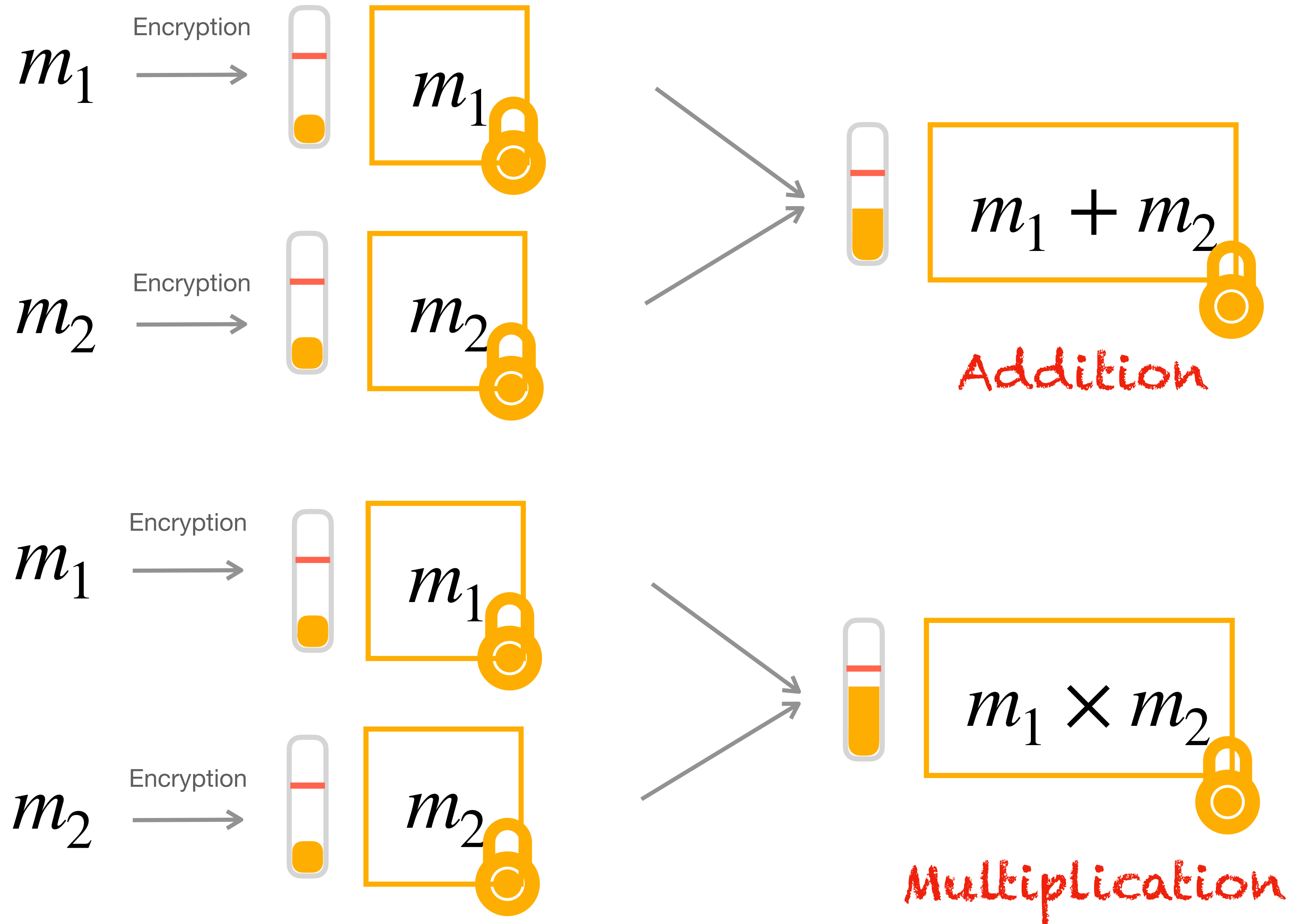
m_1 Encryption →

m_2 Encryption →

Fully Homomorphic Encryption



Fully Homomorphic Encryption



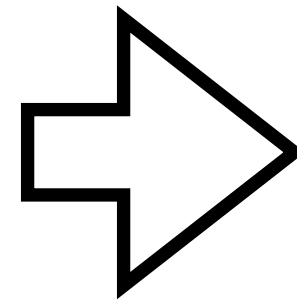
Somewhat HE Approach

Somewhat HE Approach

Choose a circuit
to evaluate

Somewhat HE Approach

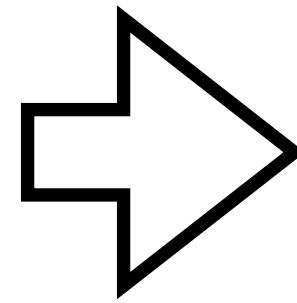
Choose a circuit
to evaluate



Choose cryptographic
parameters large enough

Somewhat HE Approach

Choose a circuit
to evaluate

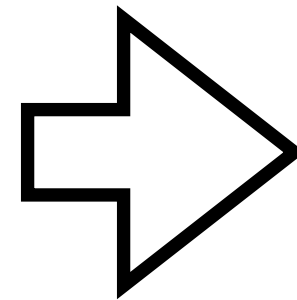


Choose cryptographic
parameters large enough

Bigger parameters

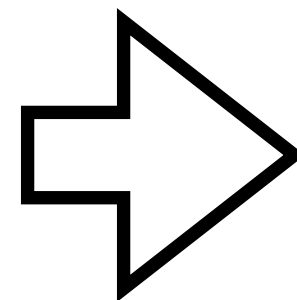
Somewhat HE Approach

Choose a circuit
to evaluate



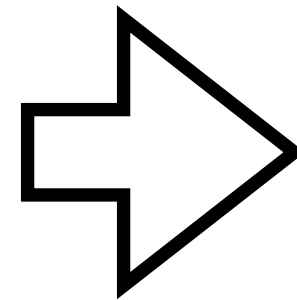
Choose cryptographic
parameters large enough

Bigger parameters



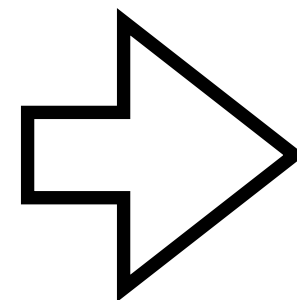
Somewhat HE Approach

Choose a circuit
to evaluate



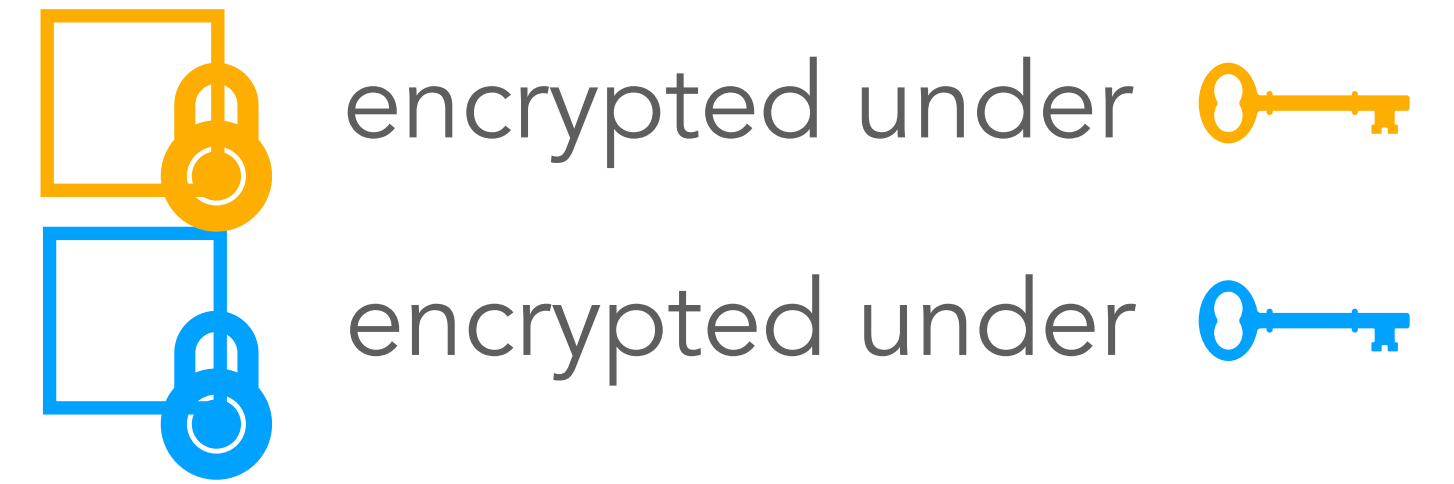
Choose cryptographic
parameters large enough

Bigger parameters

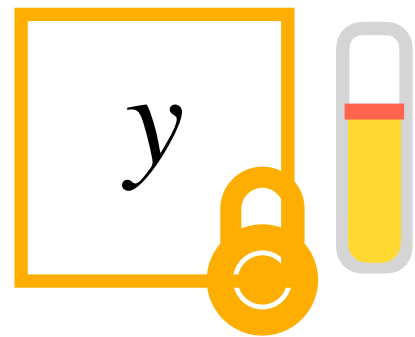
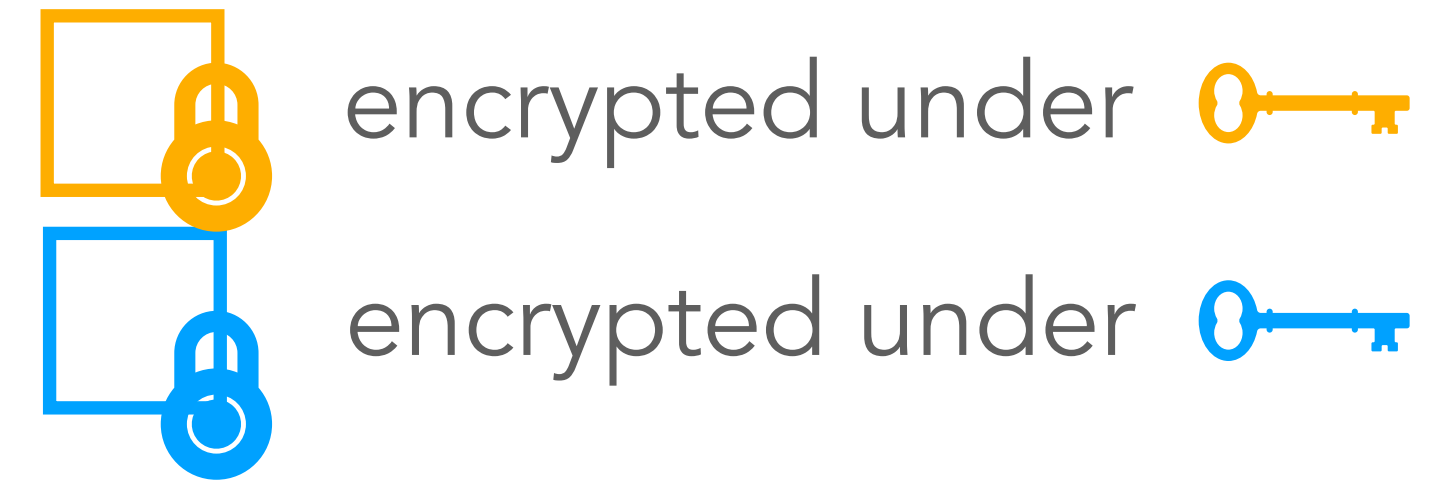


Slower computation

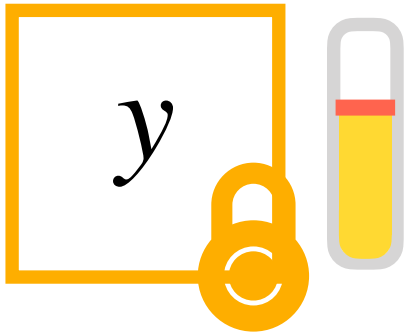
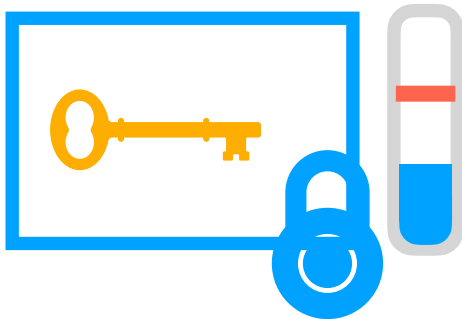
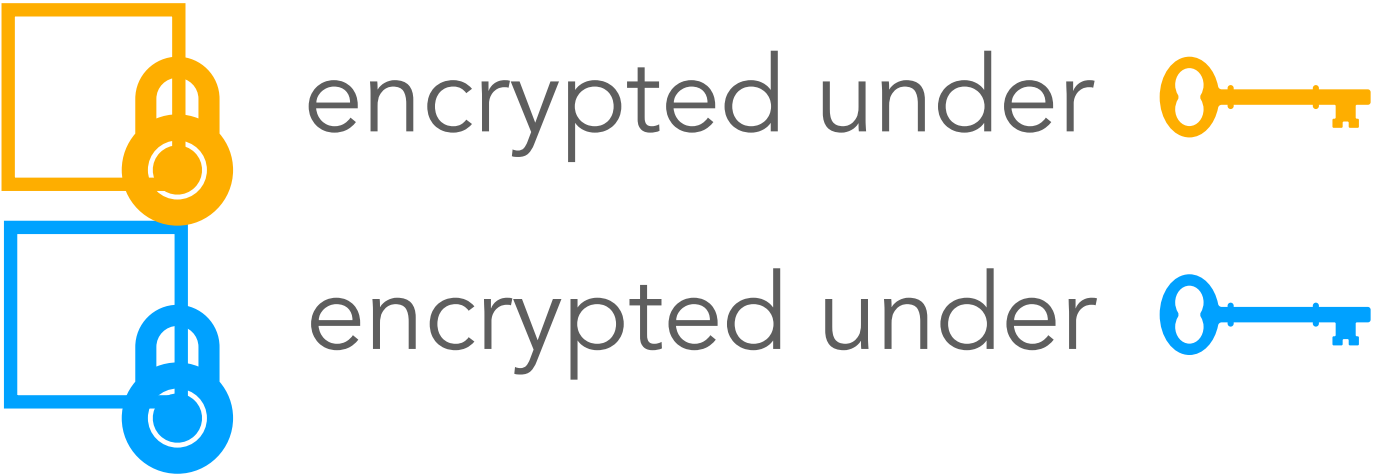
Bootstrapping [Gen09]



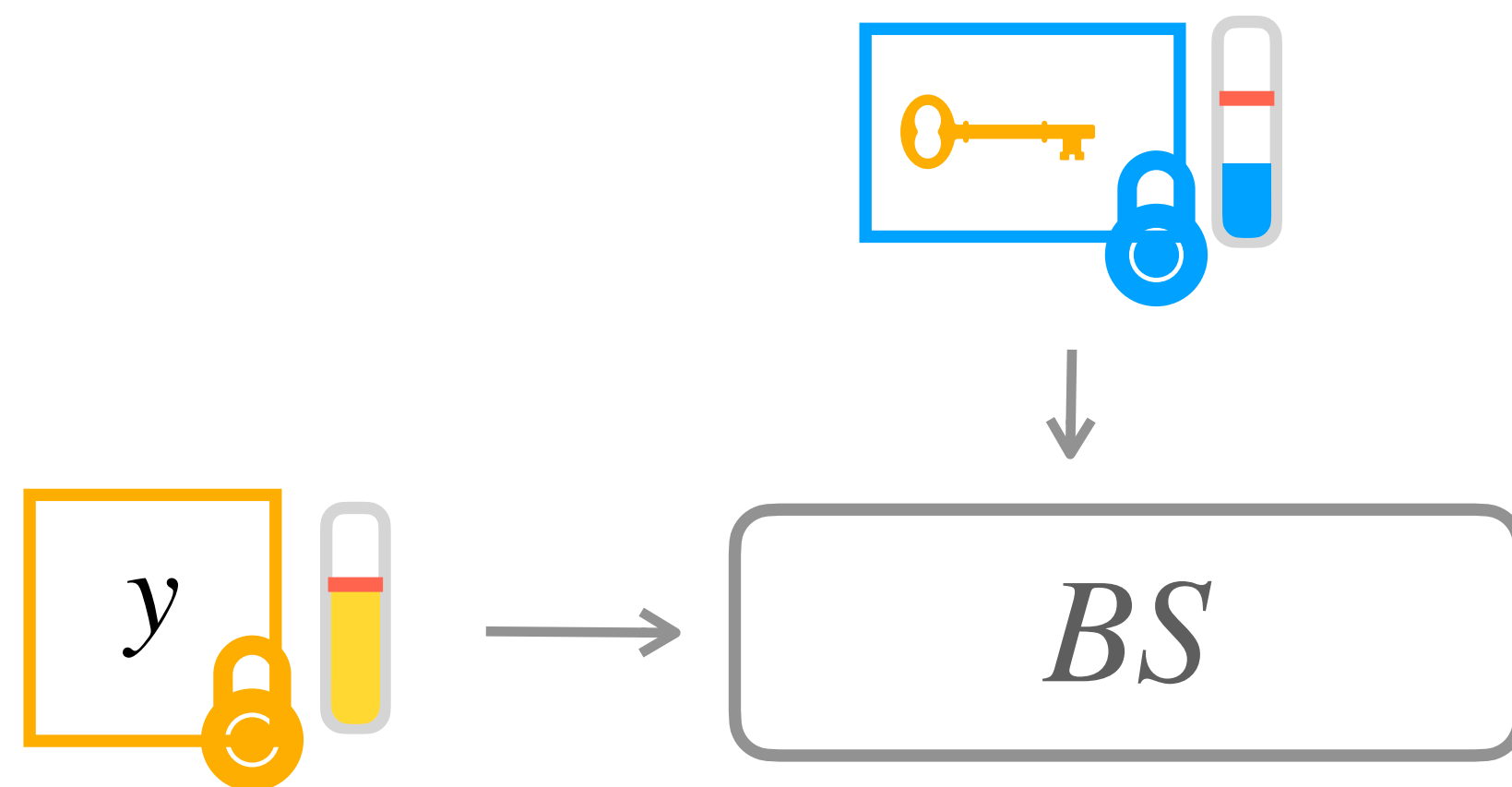
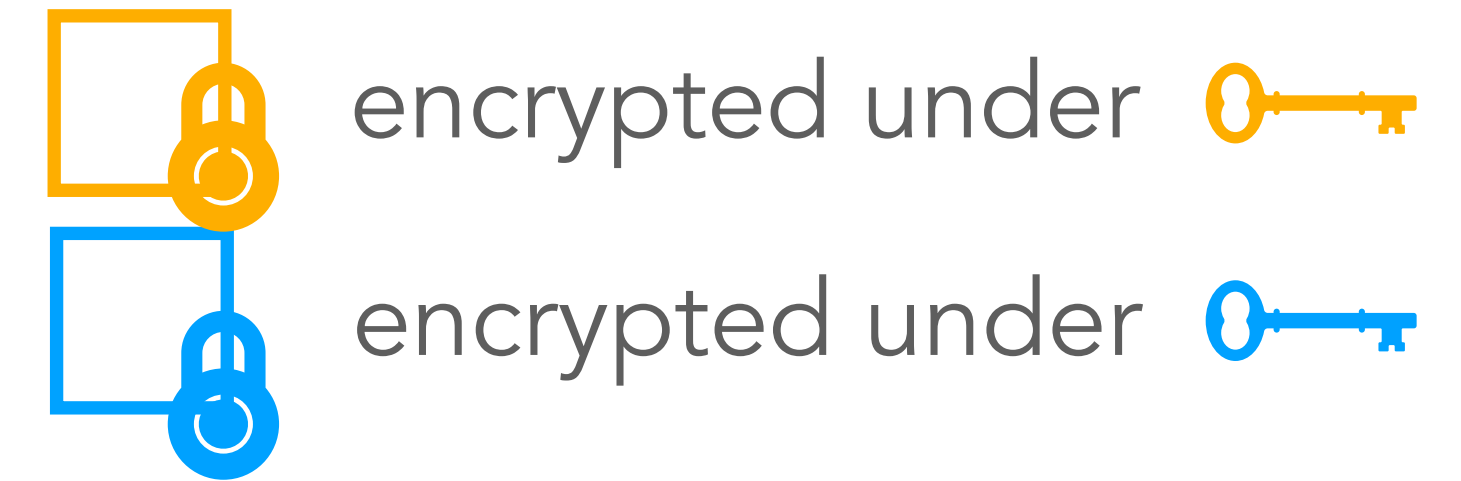
Bootstrapping [Gen09]



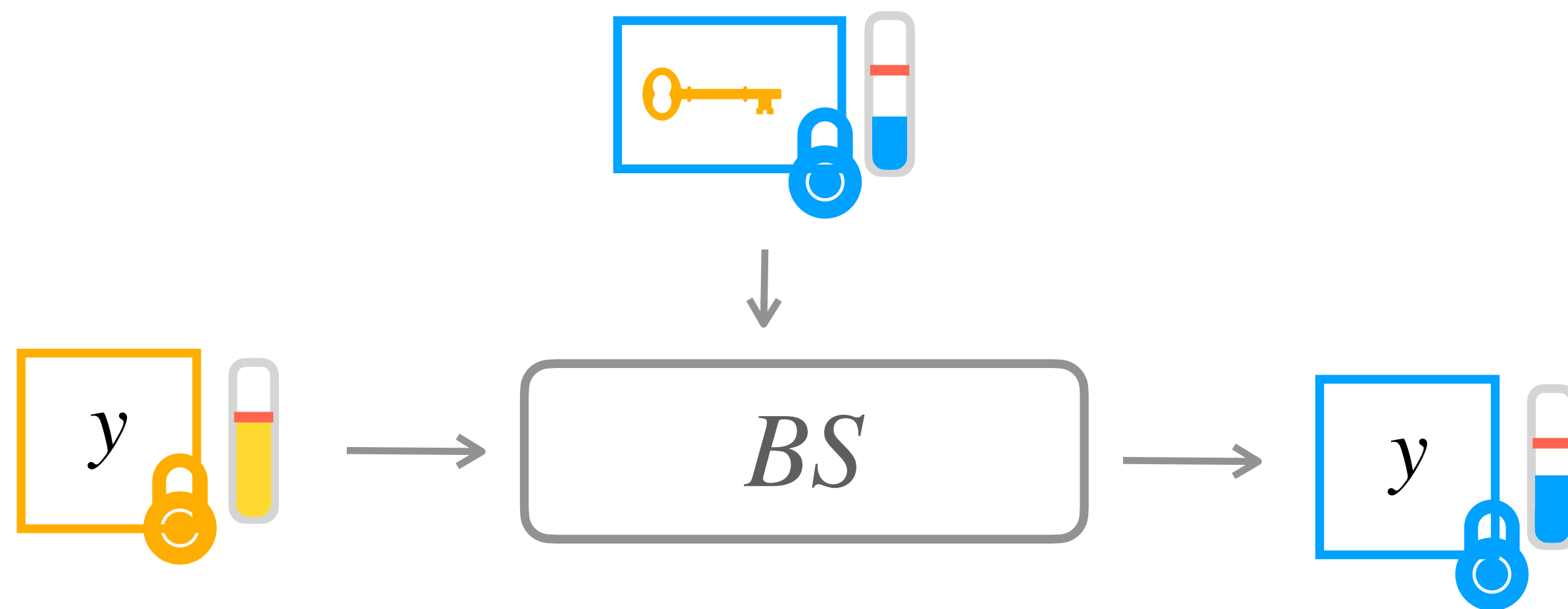
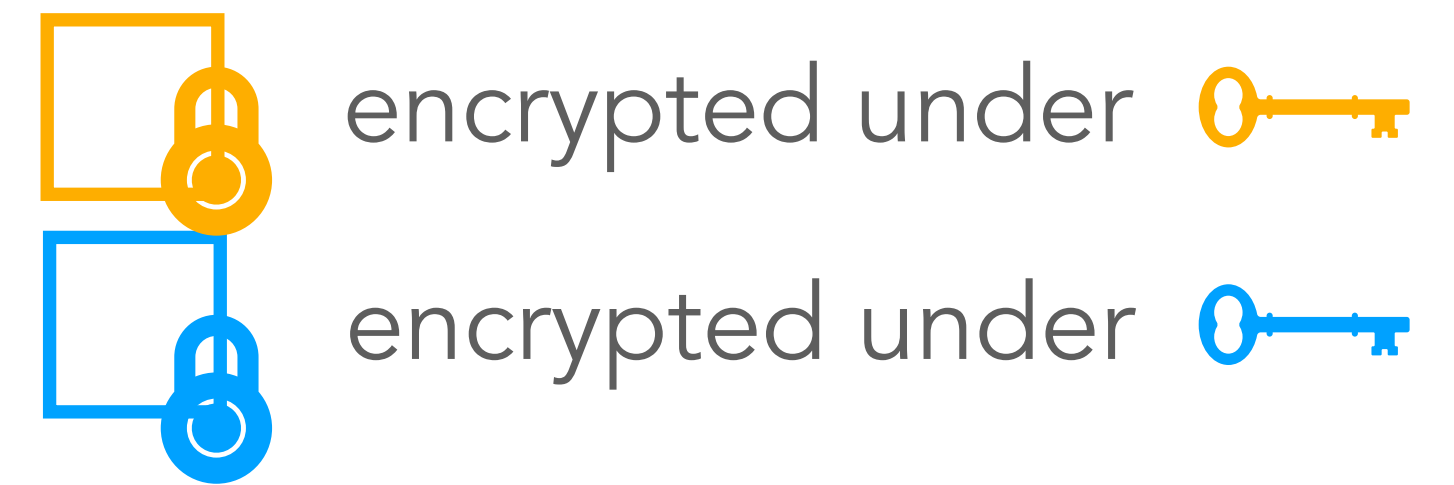
Bootstrapping [Gen09]



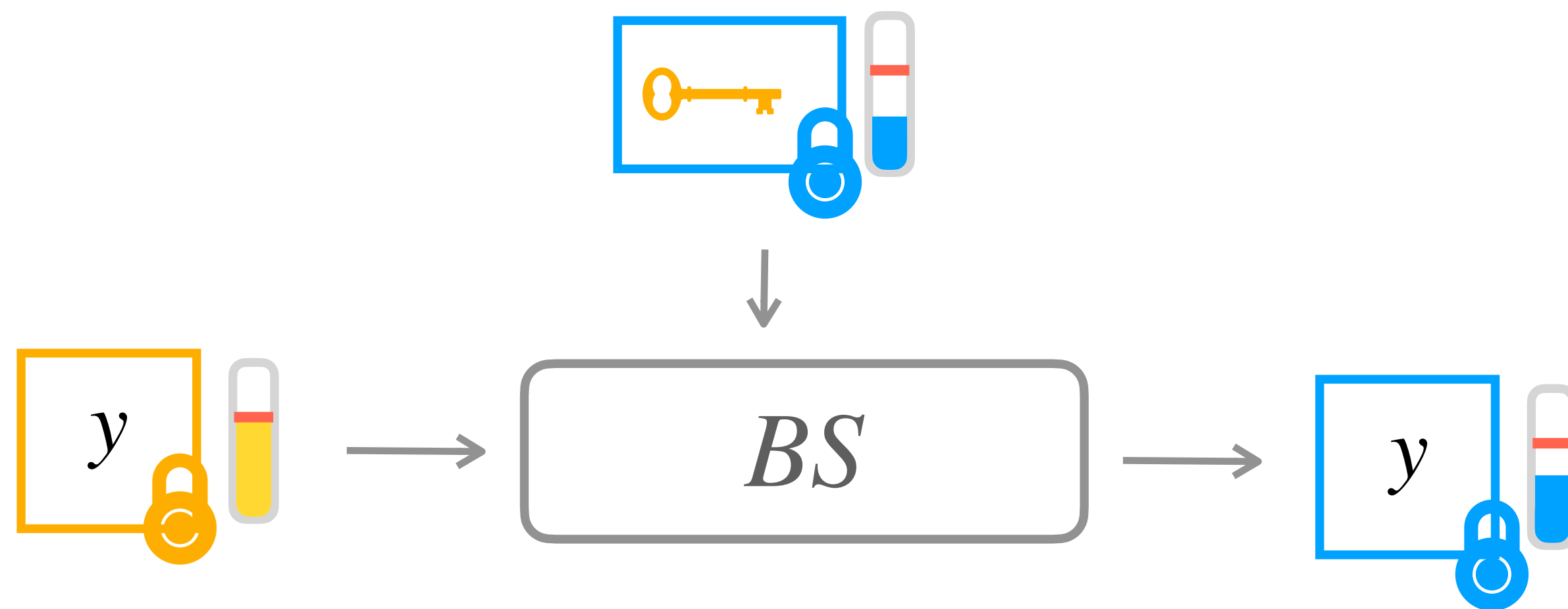
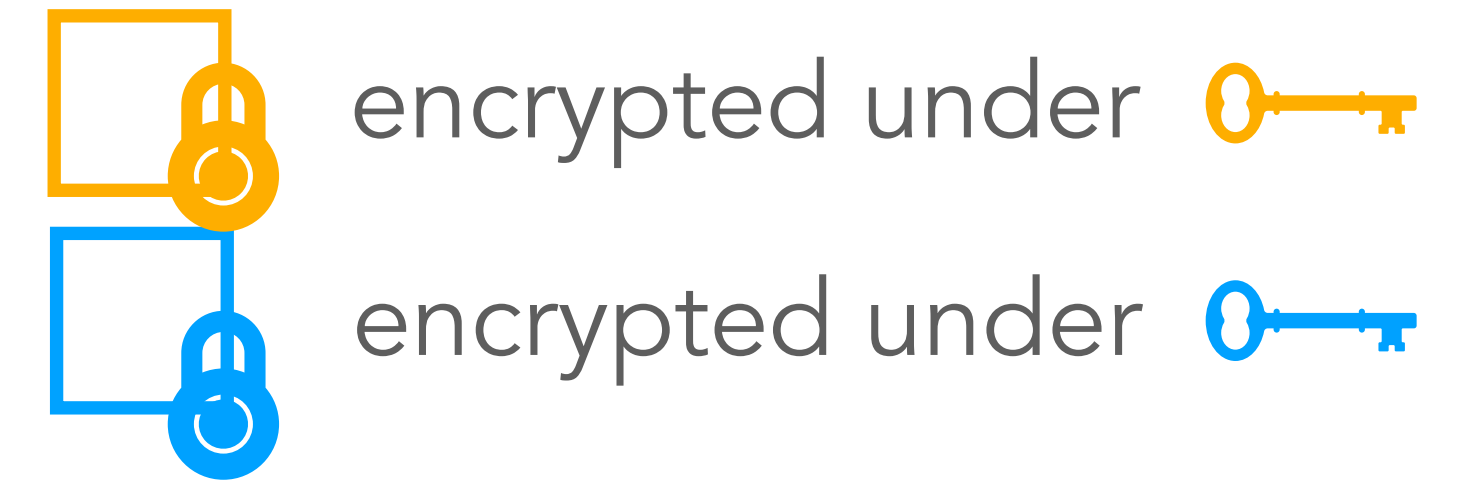
Bootstrapping [Gen09]



Bootstrapping [Gen09]

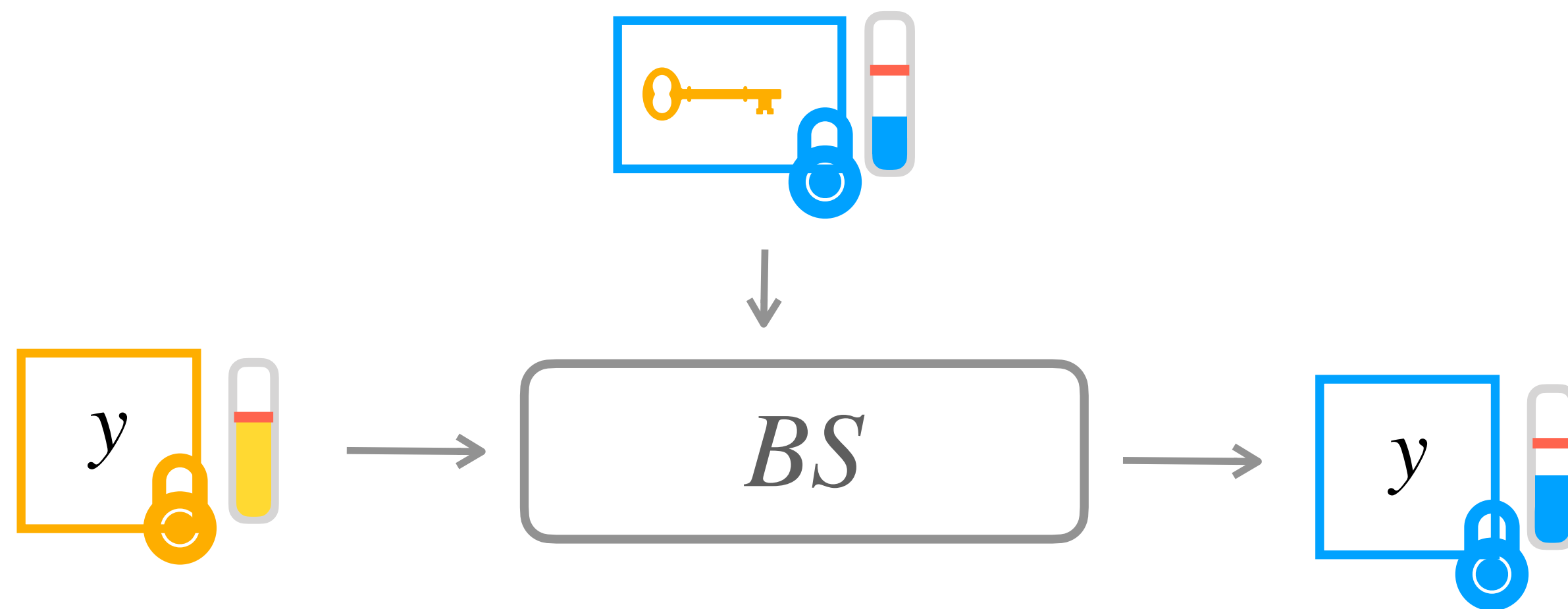
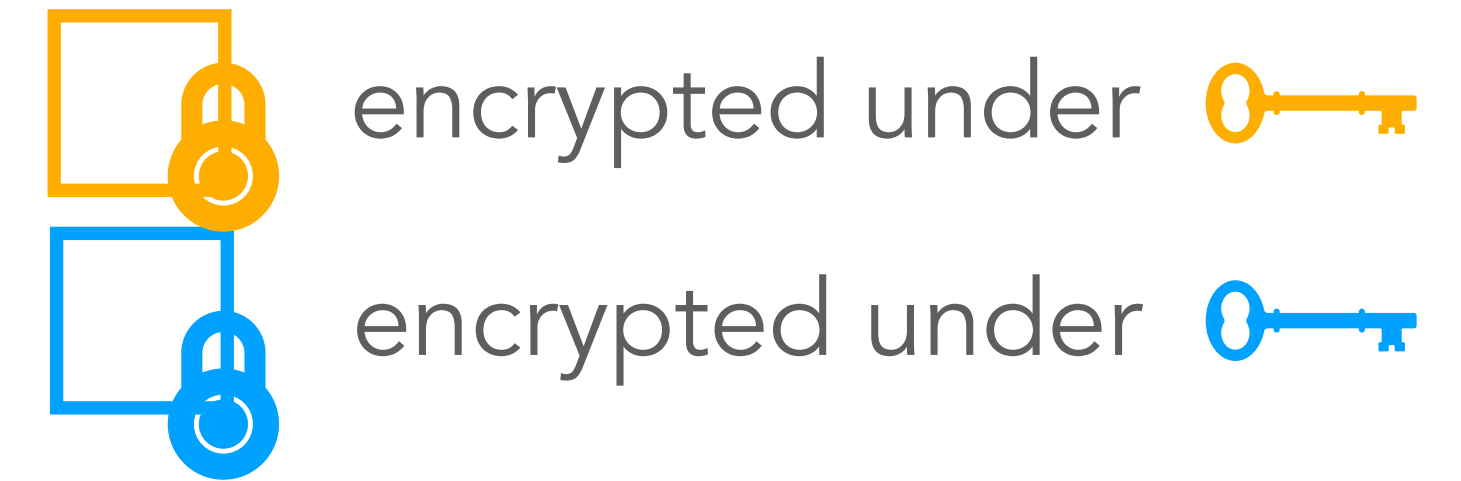


Bootstrapping [Gen09]



\approx Homomorphic decryption

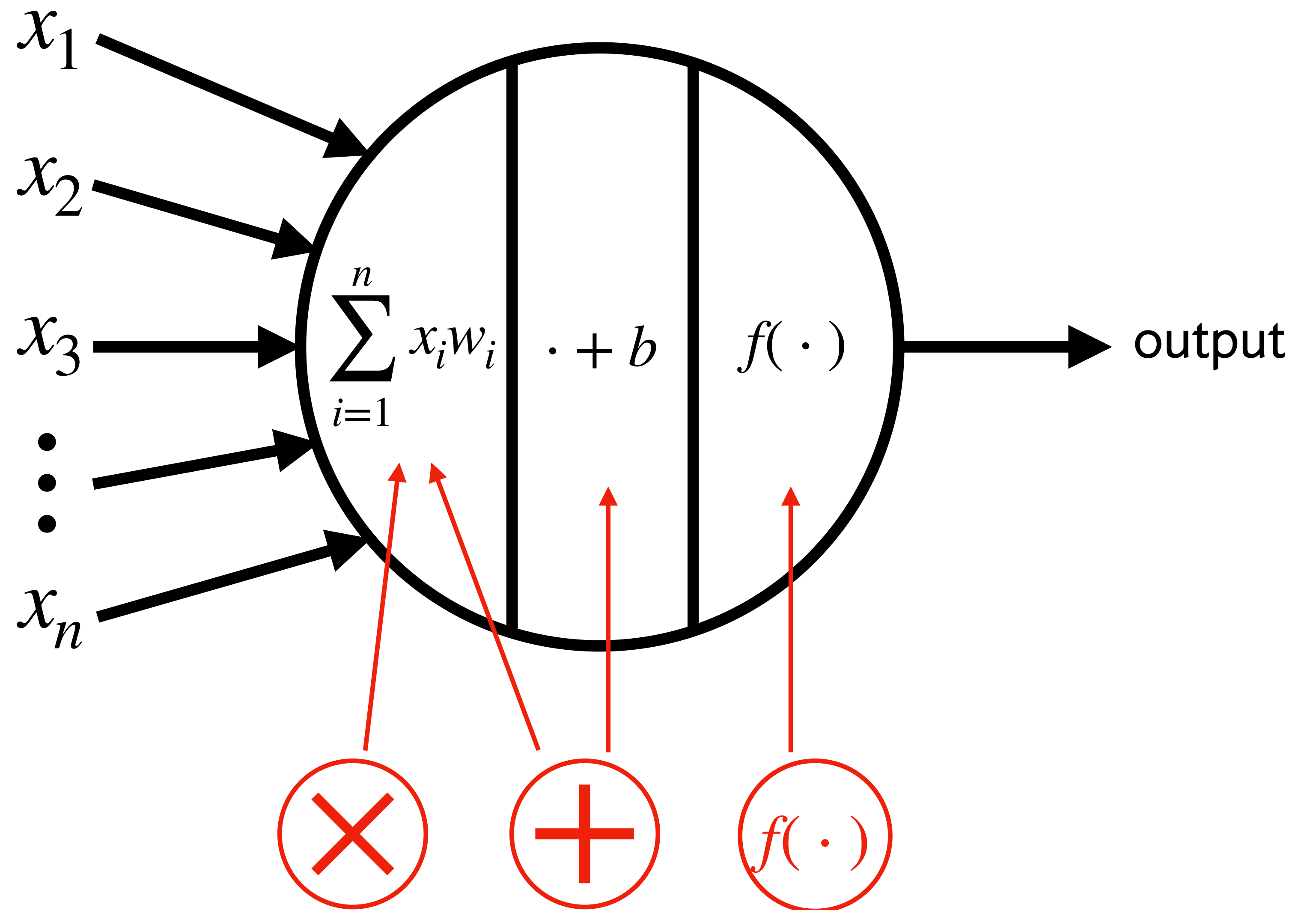
Bootstrapping [Gen09]



\approx Homomorphic decryption

No need to know the circuit beforehand anymore

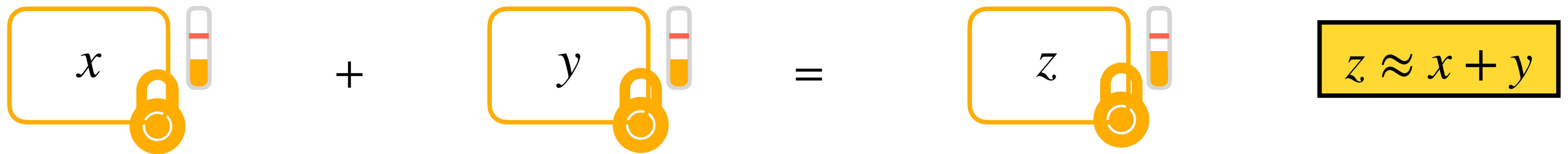
A neuron



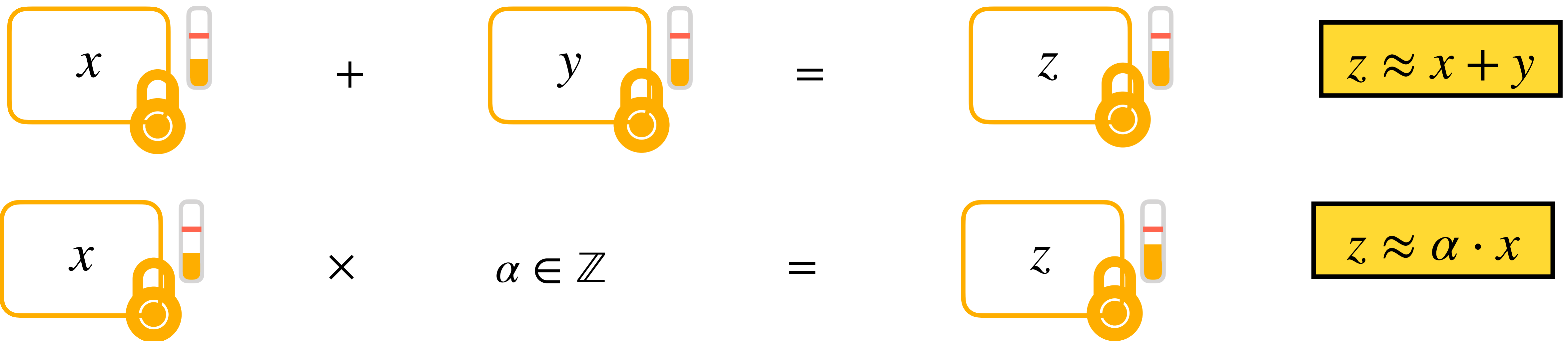
Addition

Homomorphic Addition of LWE Ciphertext

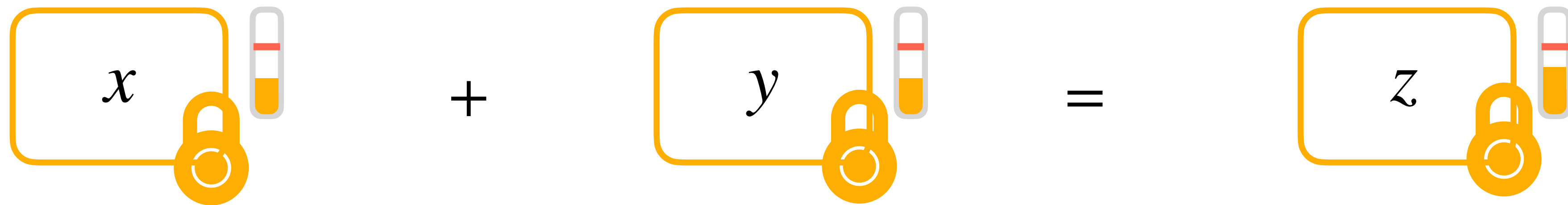
Homomorphic Addition of LWE Ciphertext



Homomorphic Addition of LWE Ciphertext

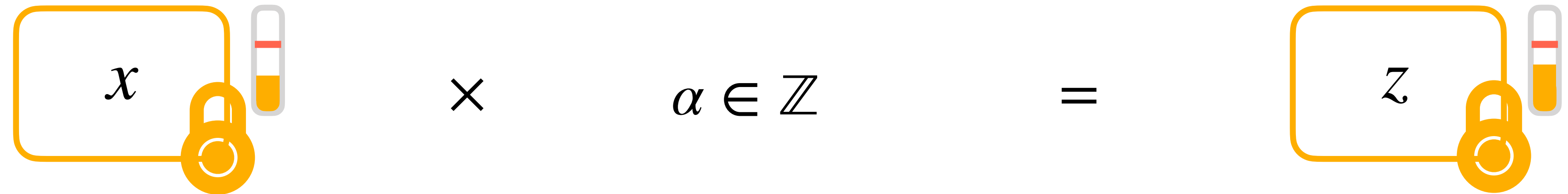


Homomorphic Addition of LWE Ciphertext



$x + y = z$

$z \approx x + y$



$x \times \alpha \in \mathbb{Z} = z$

$z \approx \alpha \cdot x$

$$\sum_{i=1}^n x_i w_i$$

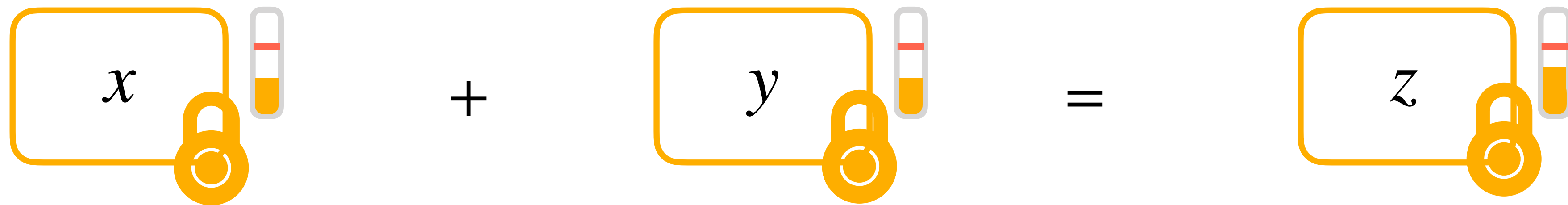
Homomorphic Addition of LWE Ciphertext

$$\begin{array}{c} \boxed{x} \end{array} \begin{array}{c} \text{lock} \\ \text{noise} \end{array} + \begin{array}{c} \boxed{y} \end{array} \begin{array}{c} \text{lock} \\ \text{noise} \end{array} = \begin{array}{c} \boxed{z} \end{array} \begin{array}{c} \text{lock} \\ \text{noise} \end{array} \quad \boxed{z \approx x + y}$$

$$\begin{array}{c} \boxed{x} \end{array} \begin{array}{c} \text{lock} \\ \text{noise} \end{array} \times \alpha \in \mathbb{Z} = \begin{array}{c} \boxed{z} \end{array} \begin{array}{c} \text{lock} \\ \text{noise} \end{array} \quad \boxed{z \approx \alpha \cdot x}$$

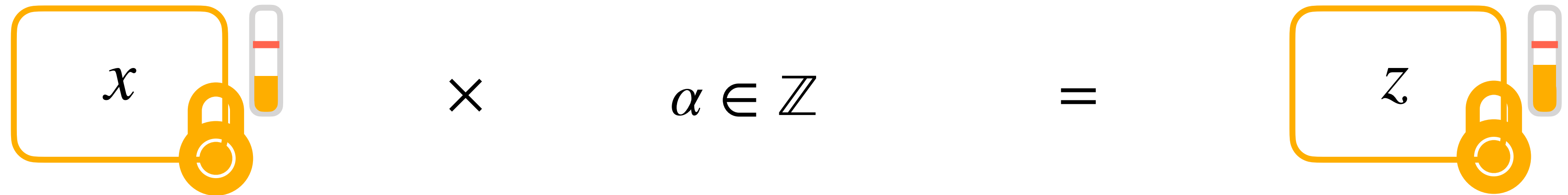
$$\sum_{i=1}^n x_i w_i \quad \longrightarrow \quad \frac{1}{\Delta} \sum_{i=1}^n x_i \lceil w_i \times \Delta \rceil$$

Homomorphic Addition of LWE Ciphertext



$$x + y = z$$

$z \approx x + y$



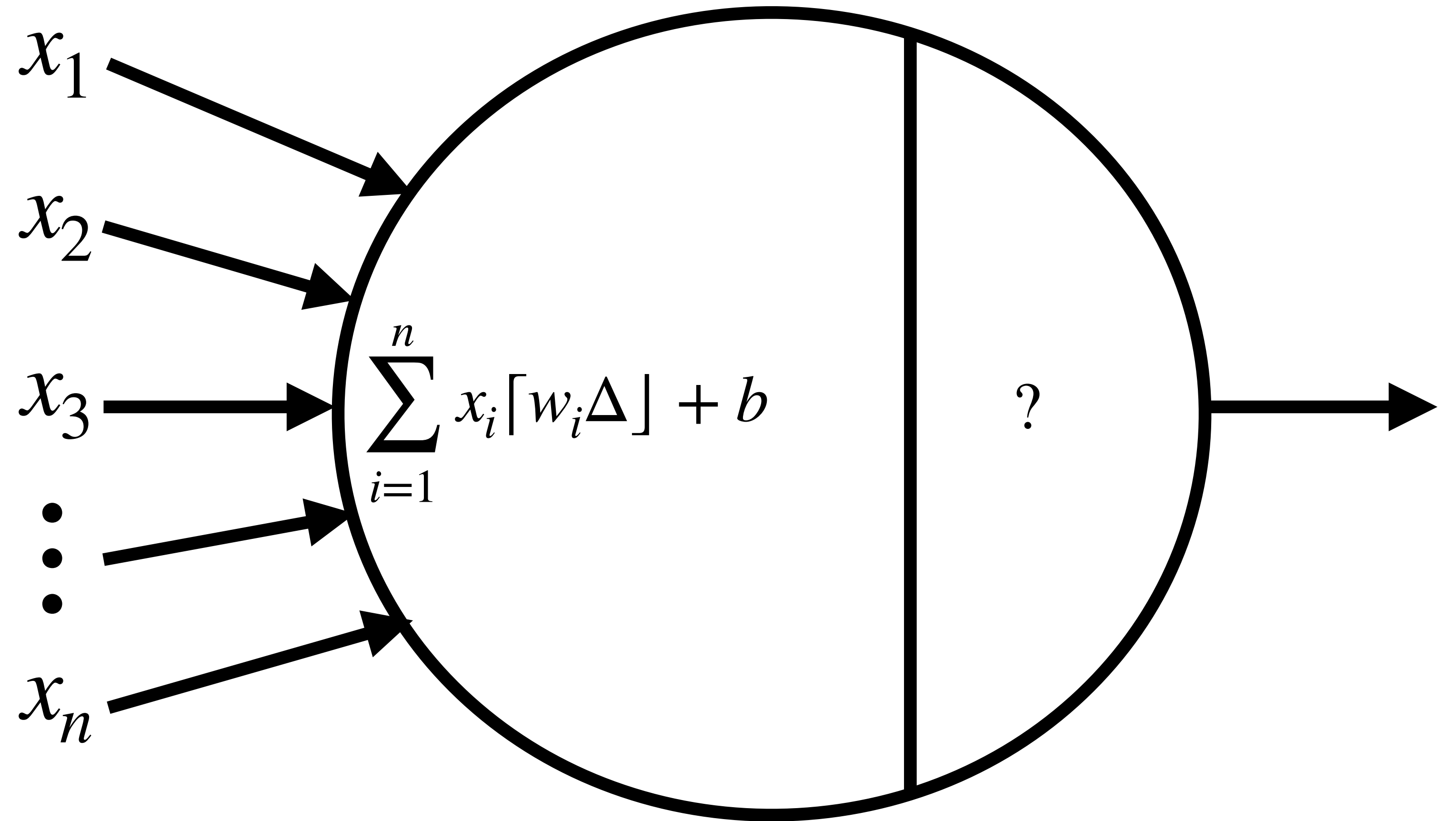
$$x \times \alpha \in \mathbb{Z} = z$$

$z \approx \alpha \cdot x$

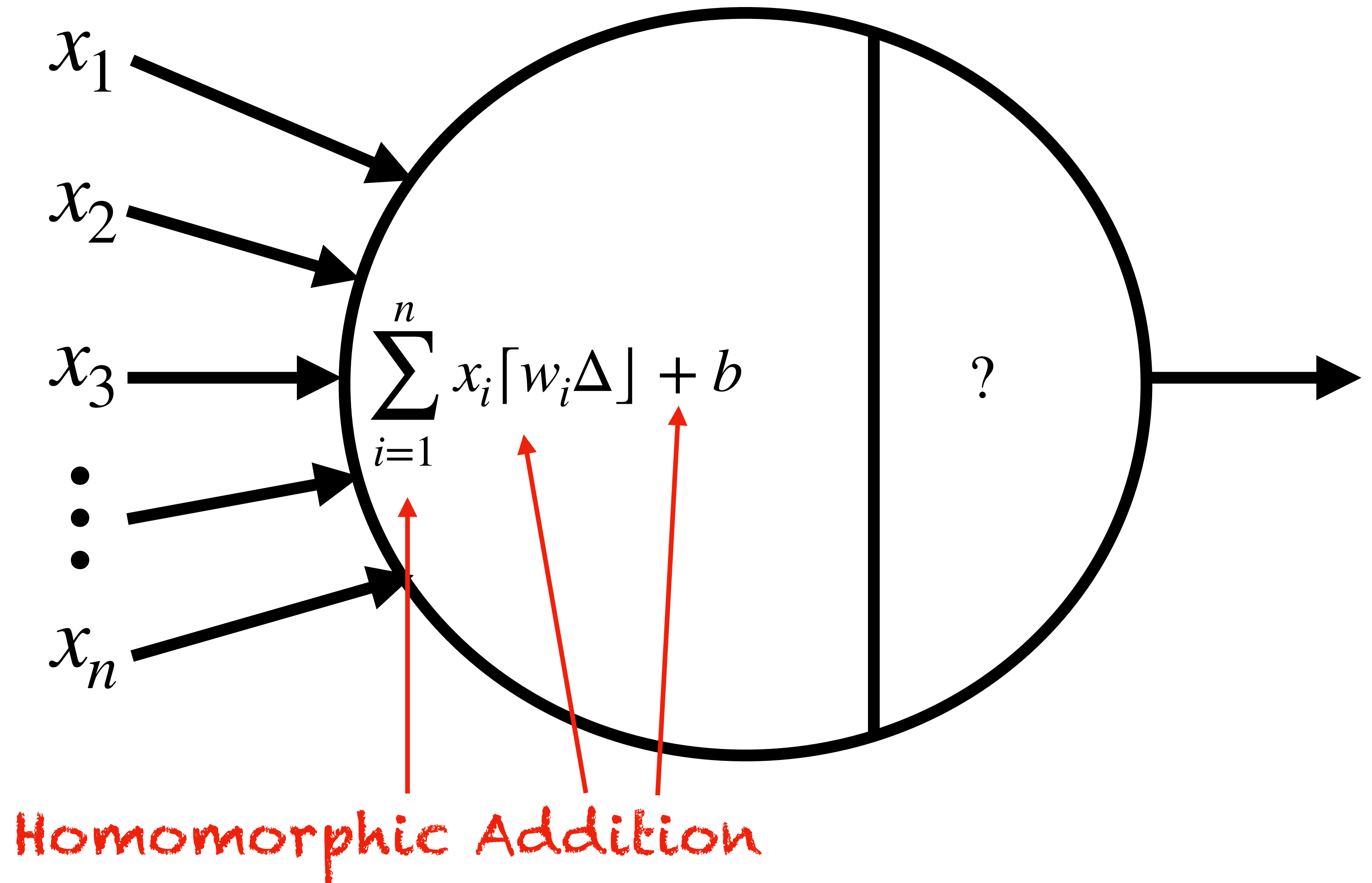
$$\sum_{i=1}^n x_i w_i \quad \rightarrow \quad \frac{1}{\Delta} \sum_{i=1}^n x_i \lceil w_i \times \Delta \rceil$$

\uparrow
 $\in \mathbb{Z}$

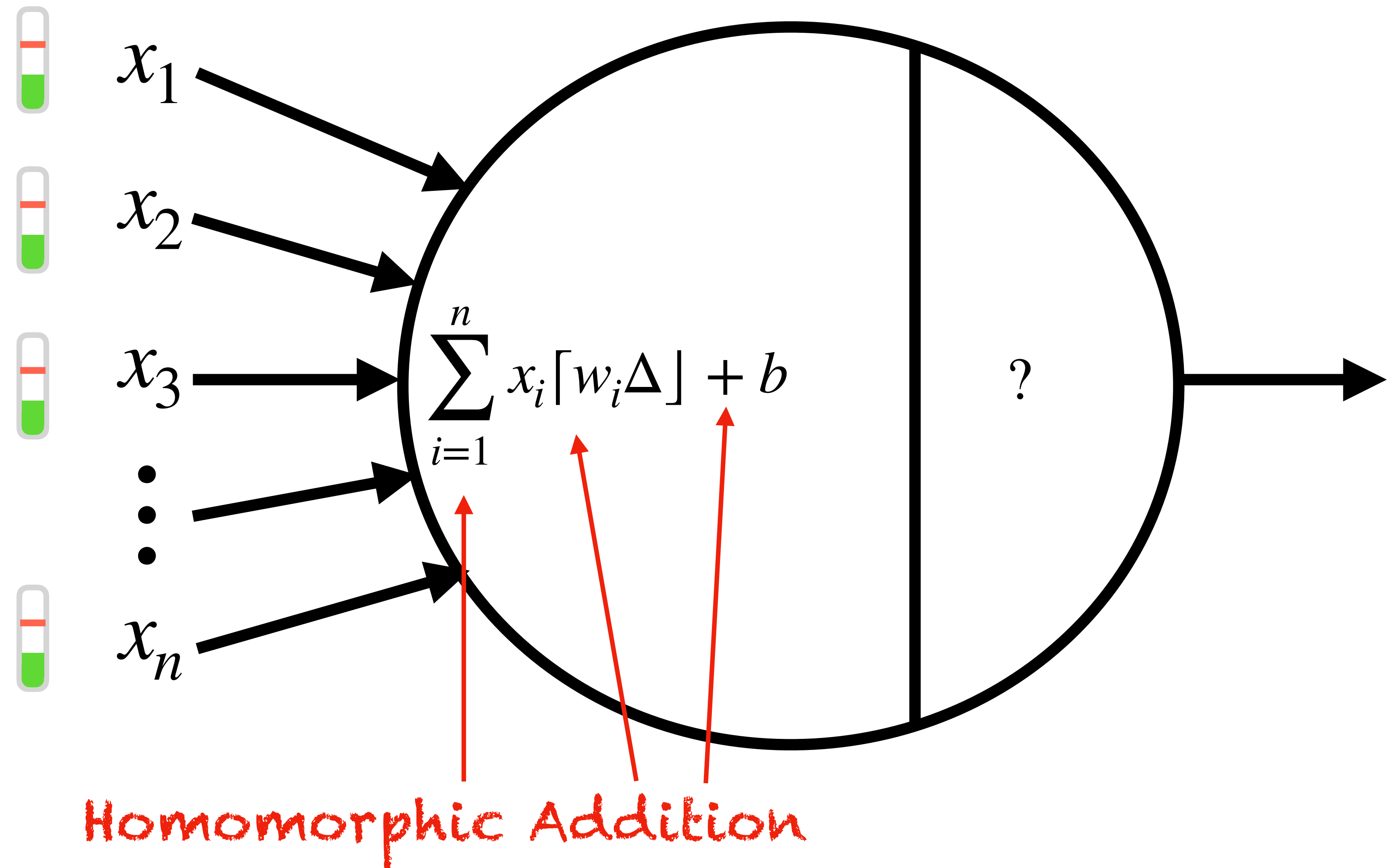
Toward an homomorphic neuron



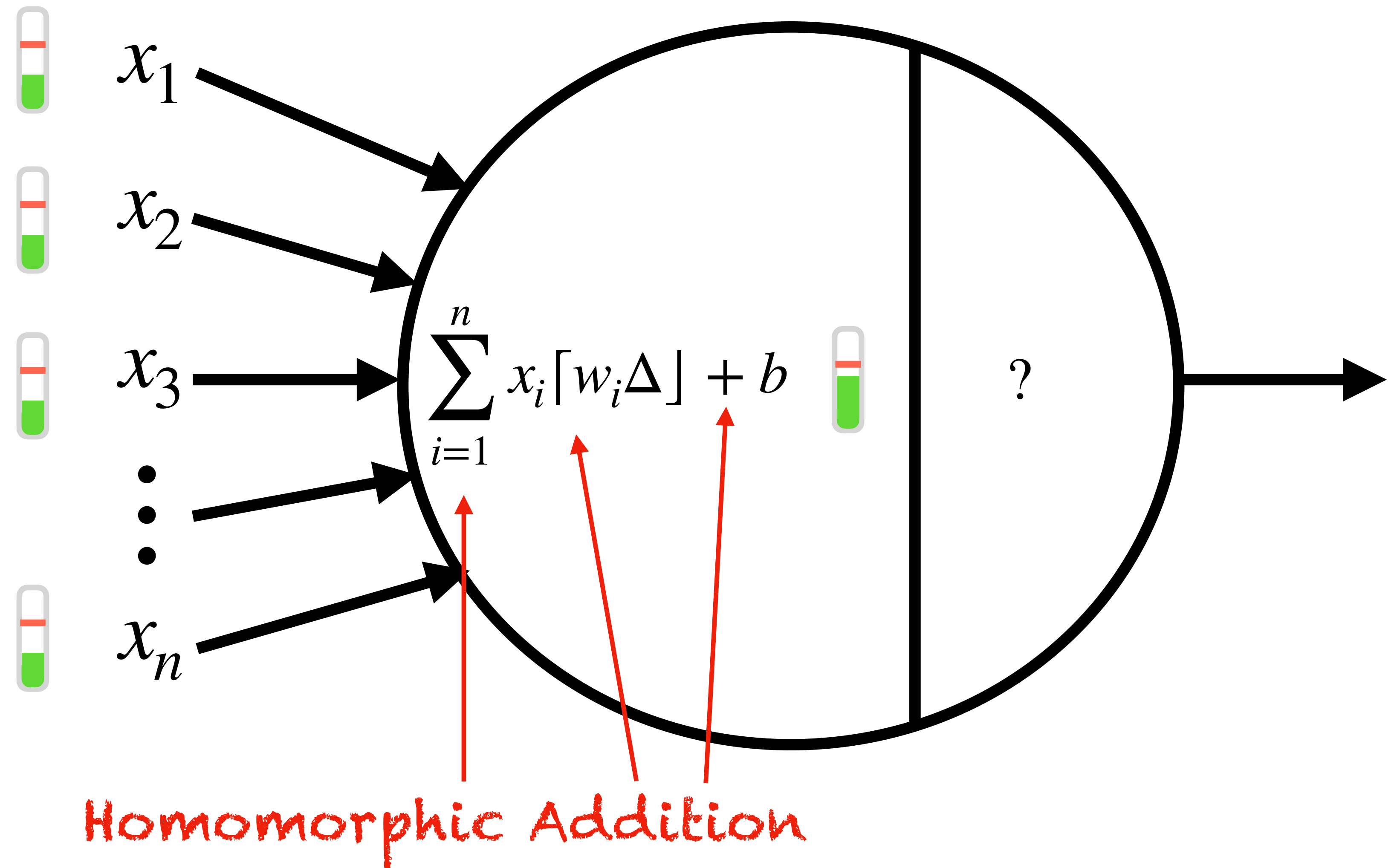
Toward an homomorphic neuron



Toward an homomorphic neuron



Toward an homomorphic neuron



Activation function

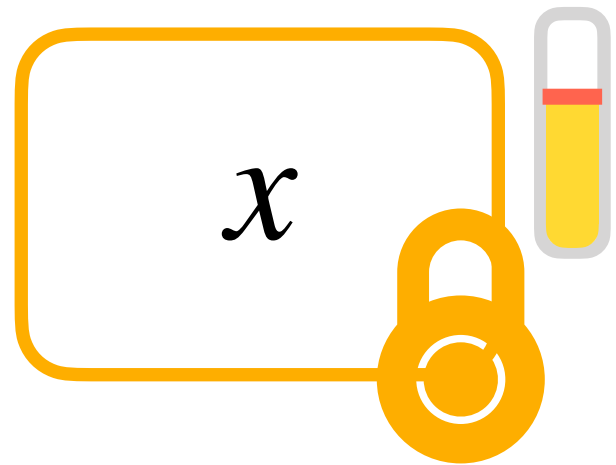
Programmable bootstrapping

Programmable bootstrapping

= Bootstrapping + homomorphic lookup table

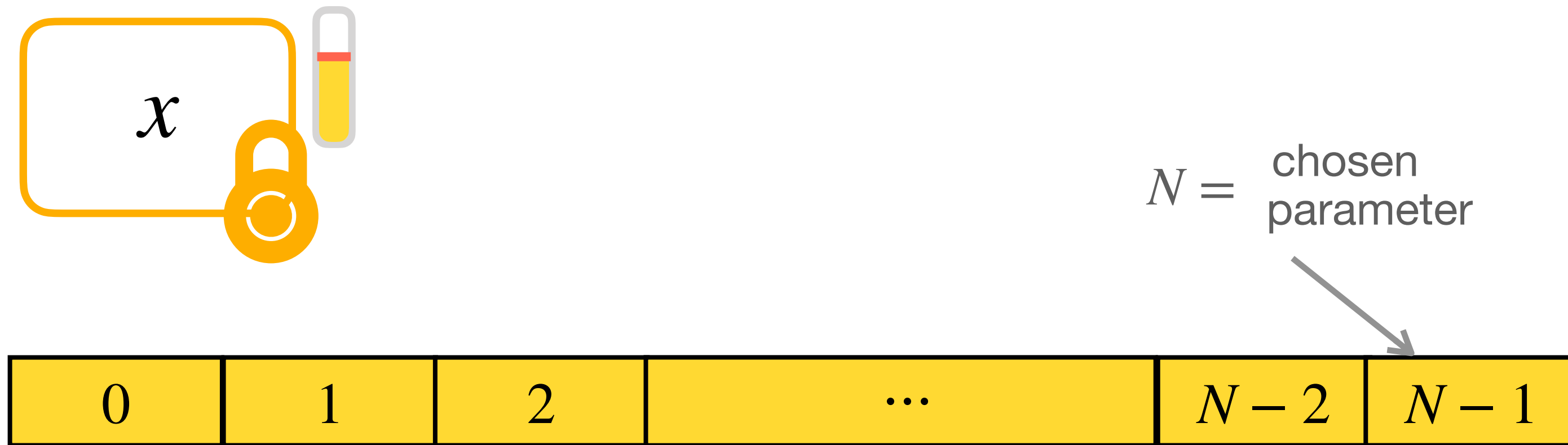
Programmable bootstrapping

= Bootstrapping + homomorphic lookup table



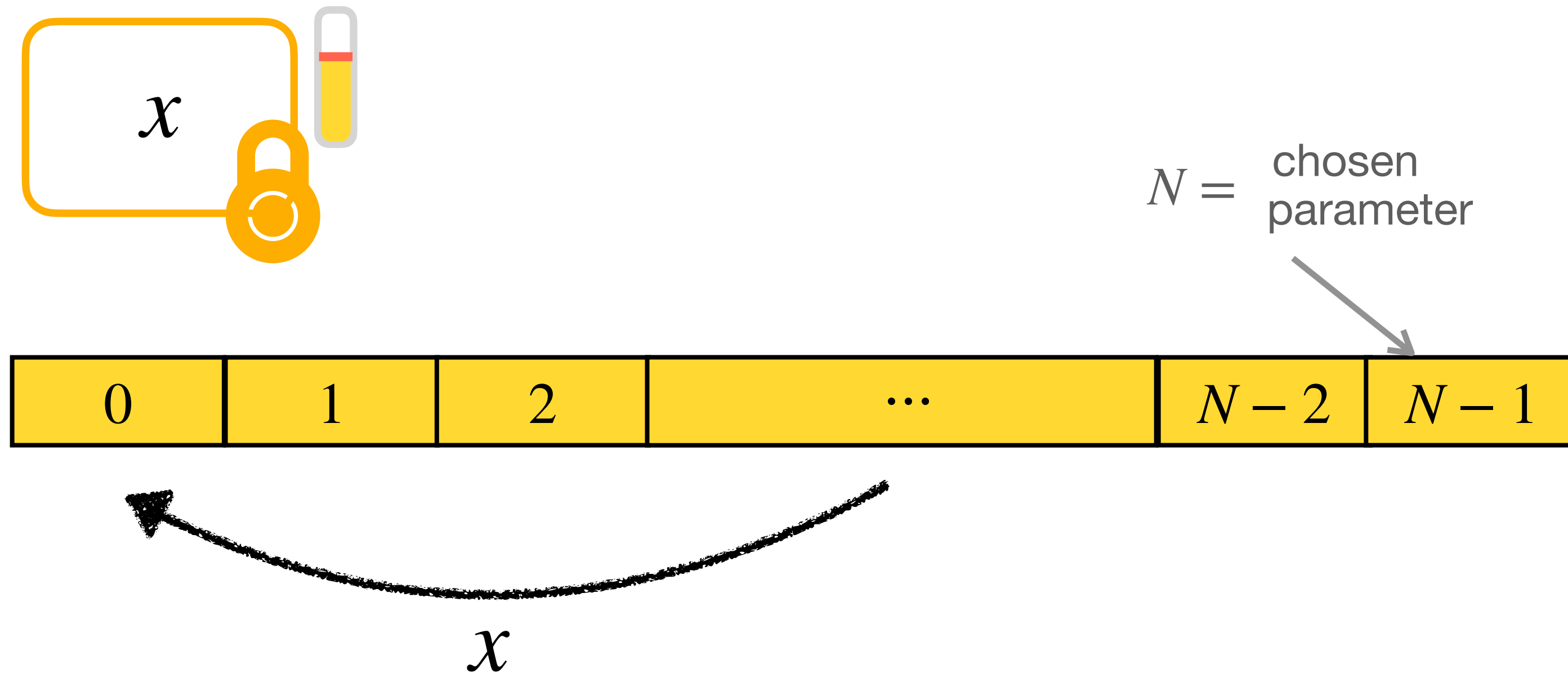
Programmable bootstrapping

= Bootstrapping + homomorphic lookup table



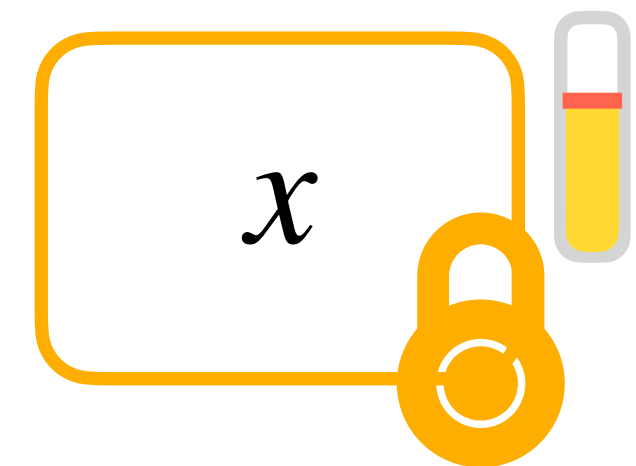
Programmable bootstrapping

= Bootstrapping + homomorphic lookup table

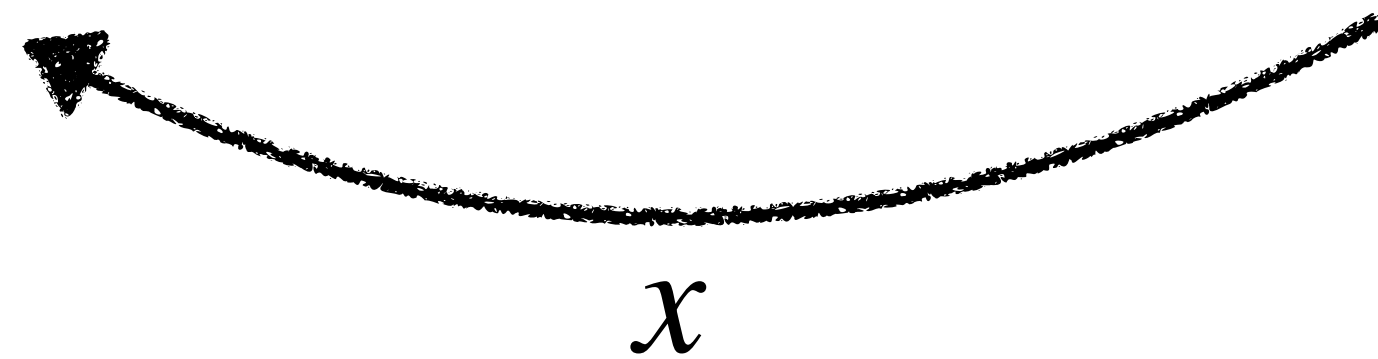


Programmable bootstrapping

= Bootstrapping + homomorphic lookup table



$N =$ chosen parameter

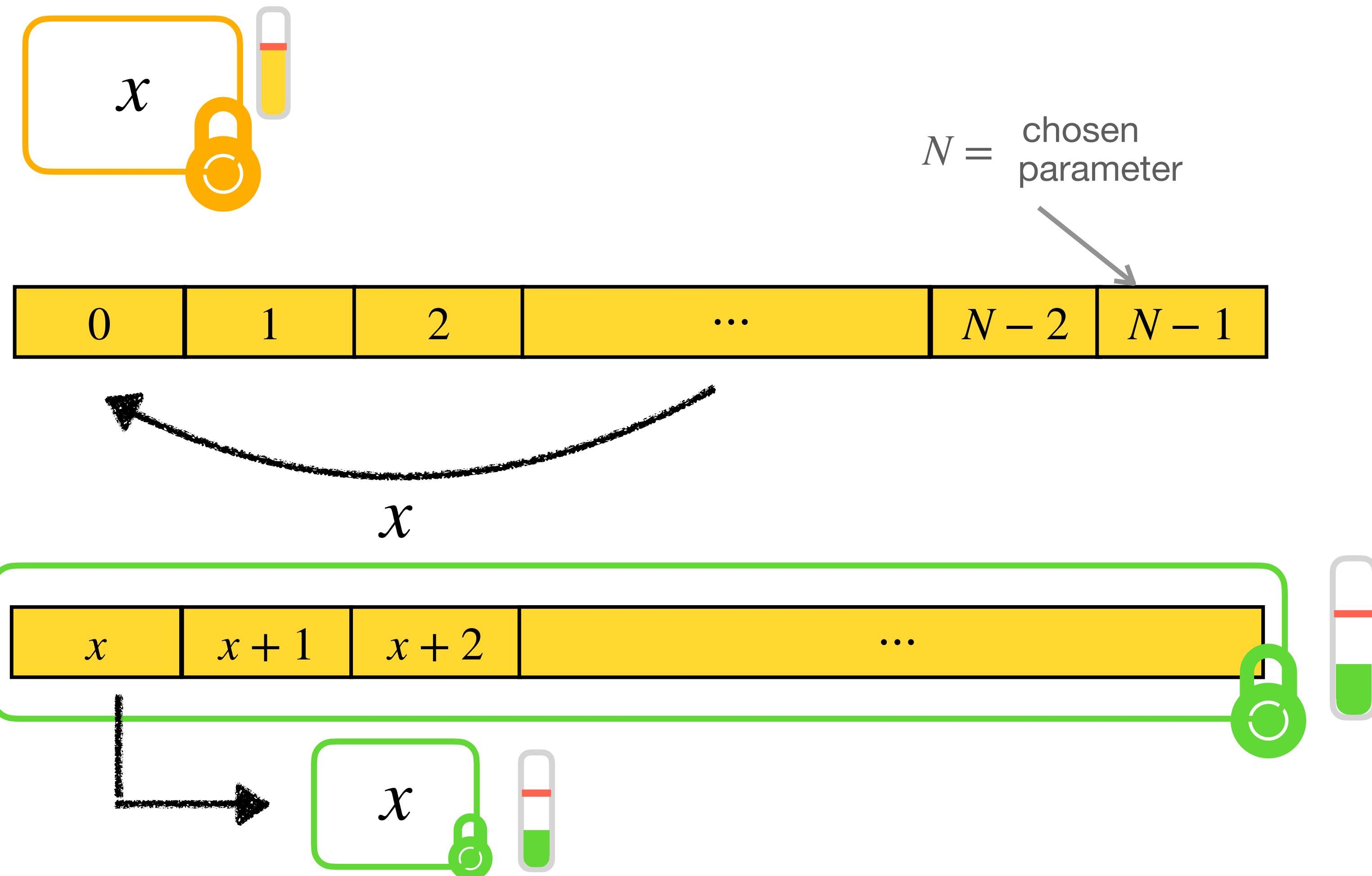


=



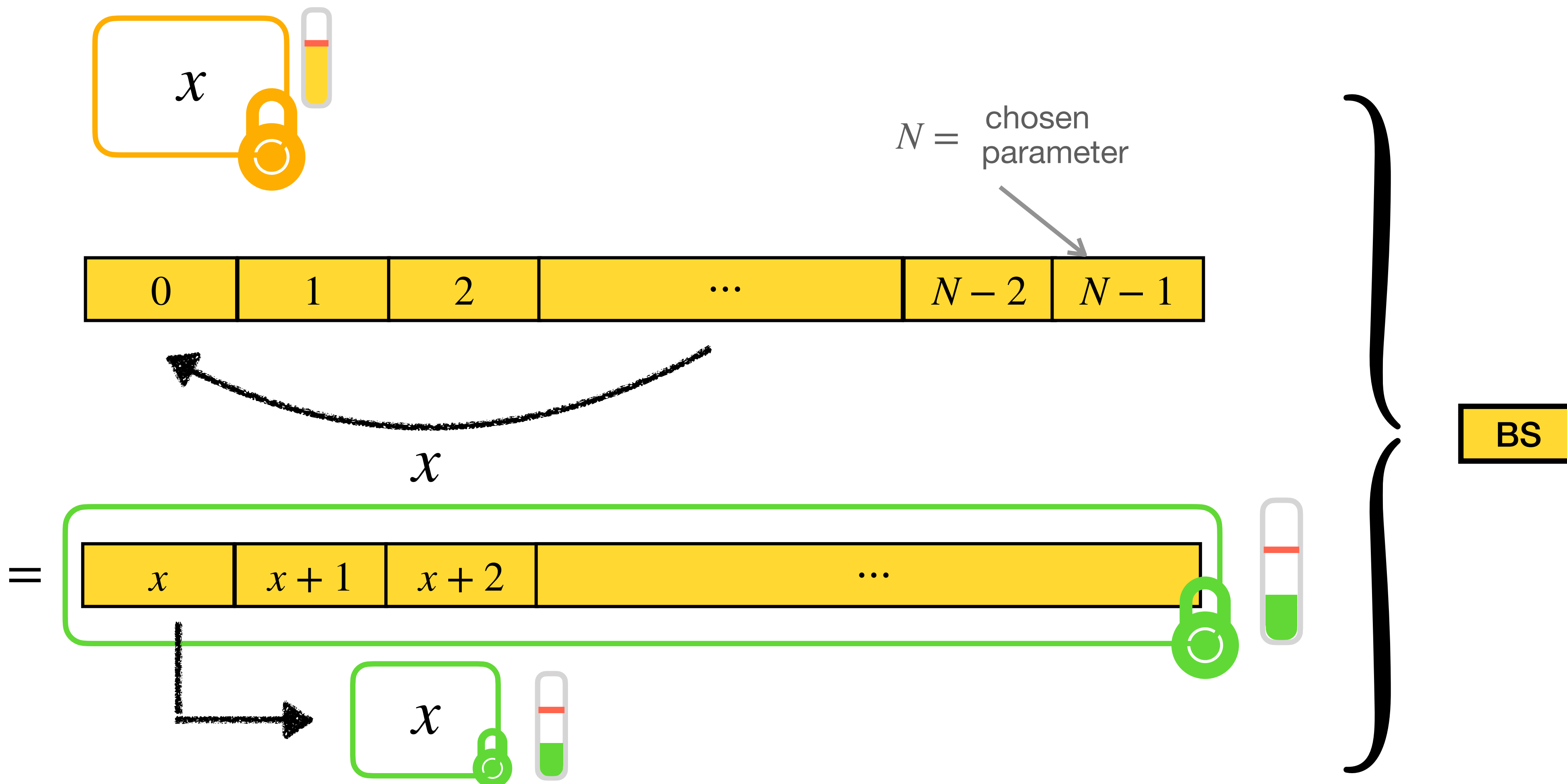
Programmable bootstrapping

= Bootstrapping + homomorphic lookup table



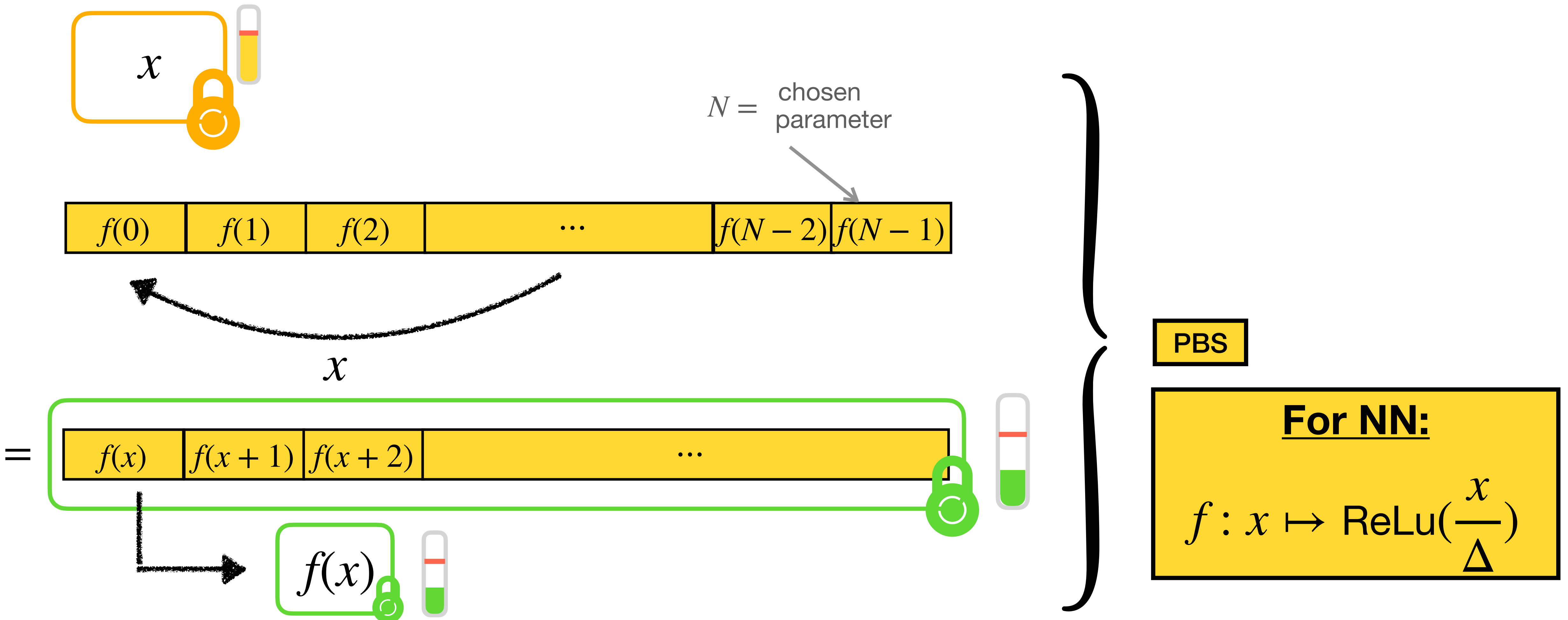
Programmable bootstrapping

= Bootstrapping + homomorphic lookup table

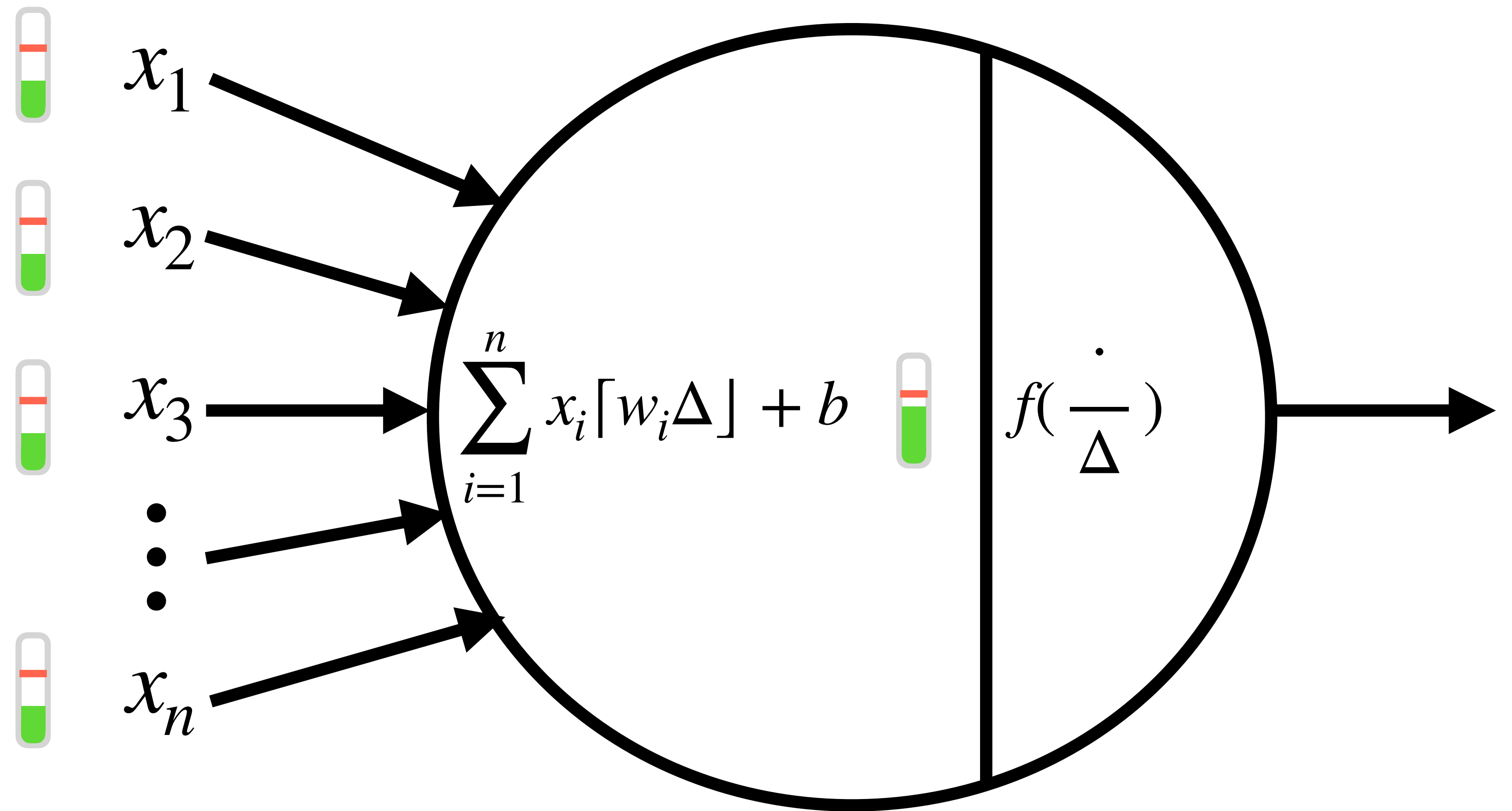


Programmable bootstrapping

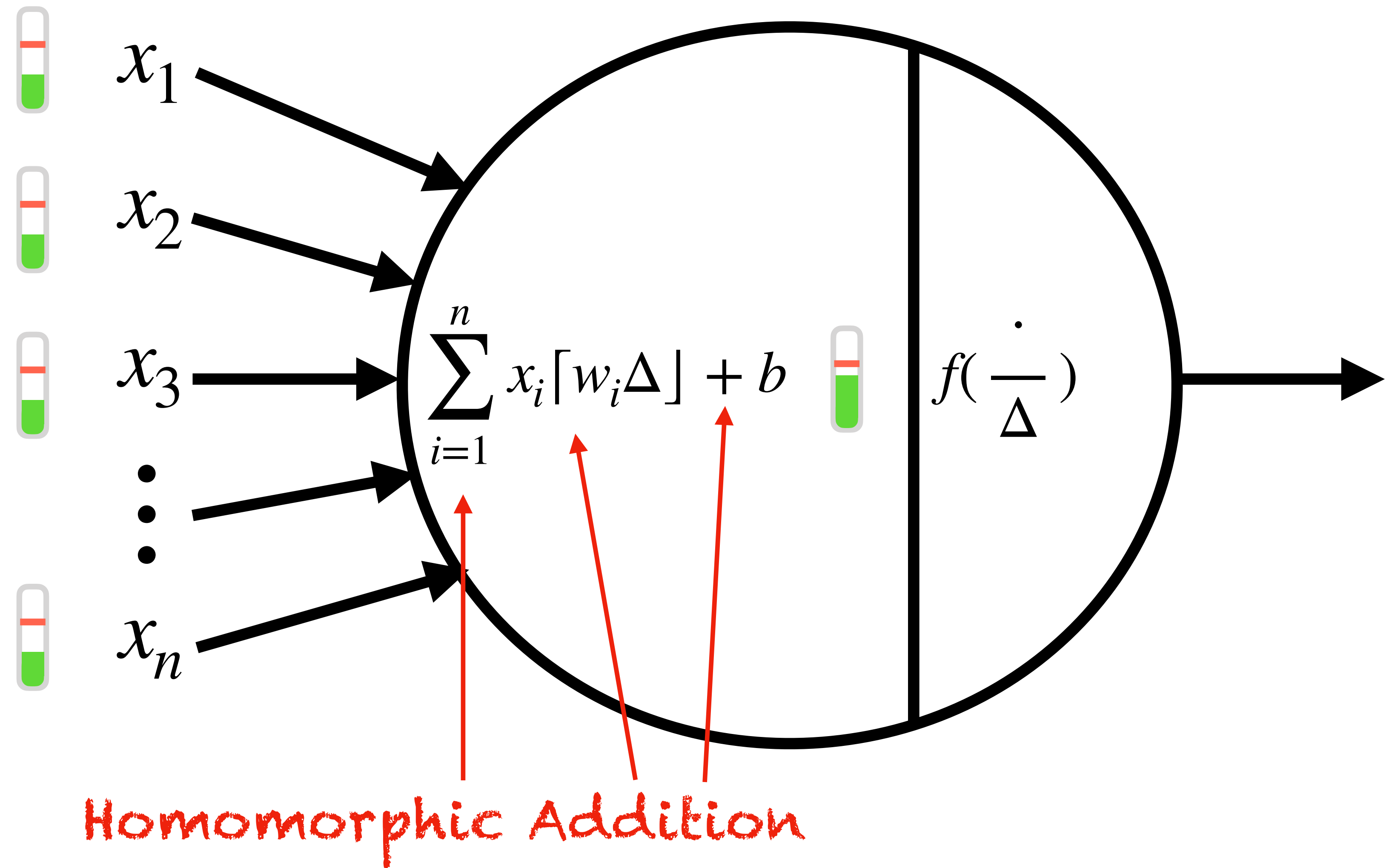
= Bootstrapping + homomorphic lookup table



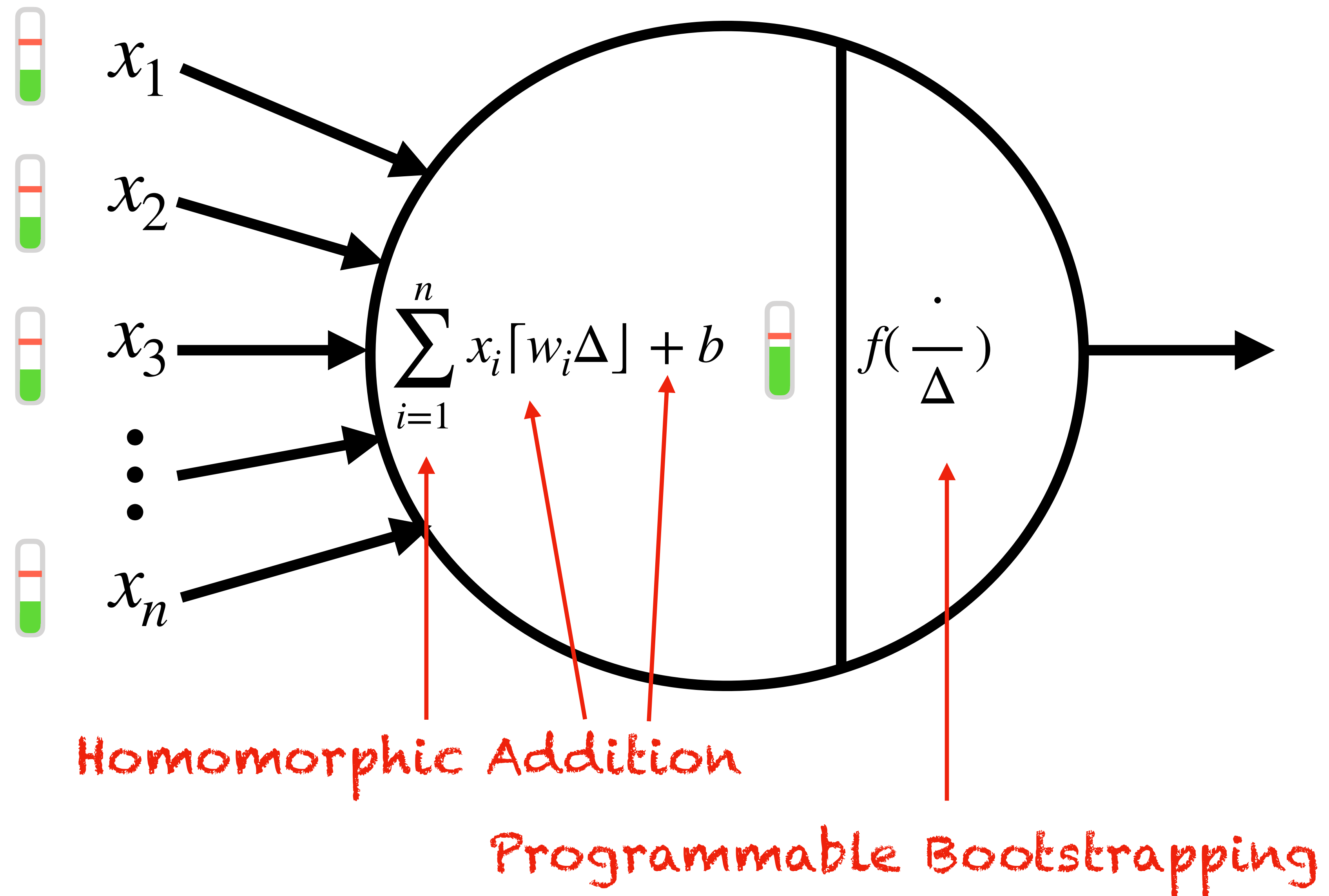
An homomorphic neuron



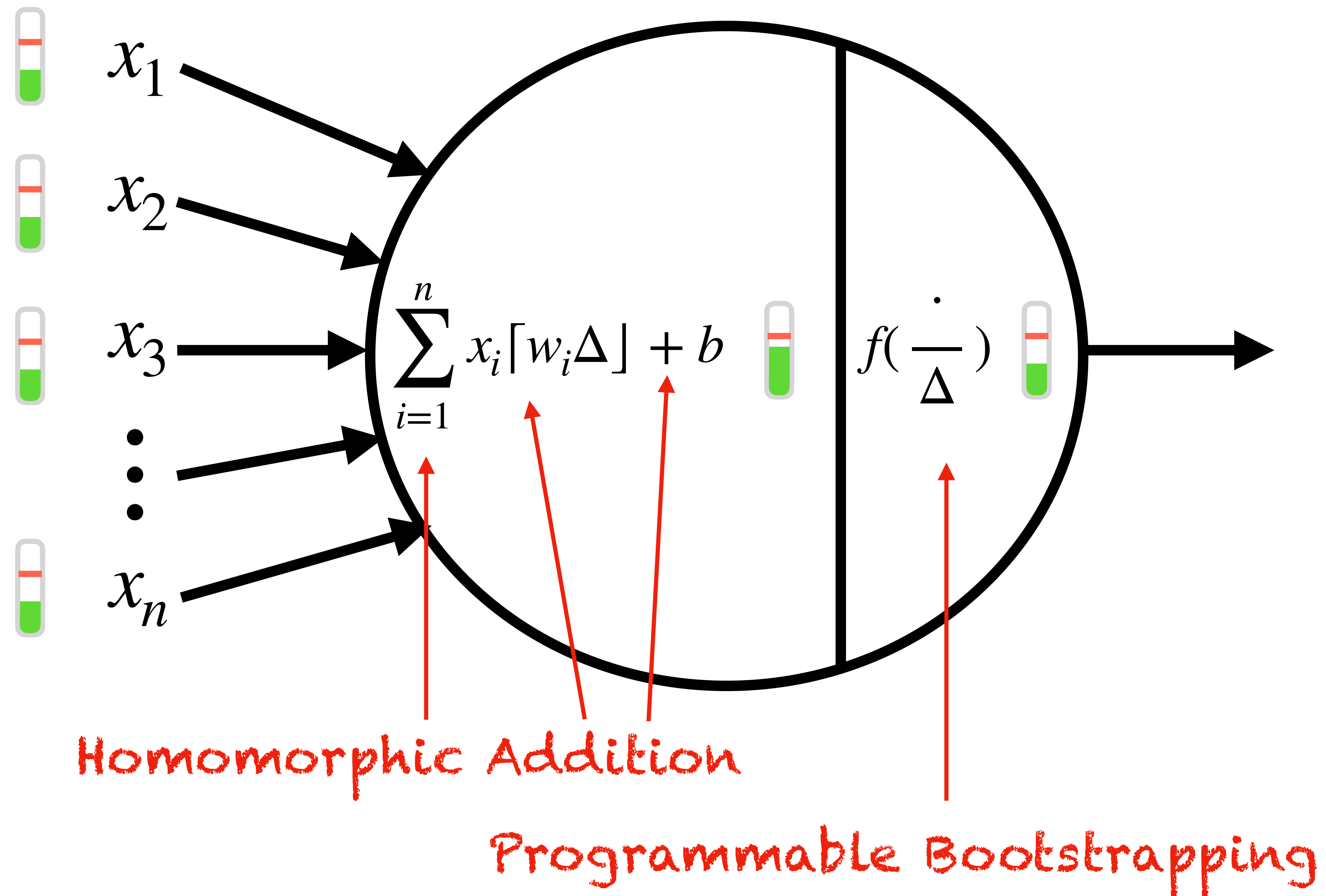
An homomorphic neuron



An homomorphic neuron



An homomorphic neuron



Conclusion

	Accuracy	CPU	AWS	
in the clear				
NN-20	97.5%	0.17ms	0.19ms	
NN-20	97.4%	30.04s	5.10s	80 bits security
homomorphic	97.5%	115.5s	17.96s	128 bits security

	Accuracy	CPU	AWS	
in the clear				
NN-50	95.4%	0.20ms	0.30ms	
NN-50	95.4%	233.5s	37.69s	128 bits security
homomorphic				

~ 100 neurons by layer

Future work

Kolmogorov Superposition
Theorem (KST):

1957

$$f(x_1, x_2, \dots, x_n) = \sum_{i=1}^{2n+1} g_i \left(\sum_{j=1}^n f_{ij}(x_j) \right)$$

univariate

Homomorphic Inference

Encrypted Neural Network

Homomorphic Training

Bibliography

- [Reg05]** O. Regev. On lattices, learning with errors, random linear codes, and cryptography. STOC 2005.
- [SSTX09]** D. Stehlé, R. Steinfeld, K. Tanaka, K. Xagawa. Efficient public key encryption based on ideal lattices. ASIACRYPT 2009.
- [LPR10]** V. Lyubashevsky, C. Peikert, O. Regev. On ideal lattices and learning with errors over rings. EUROCRYPT 2010.
- [Gen09]** C. Gentry. Fully homomorphic encryption using ideal lattices. STOC 2009.
- [RAD78]** R. L. Rivest, L. Adleman, M. L. Dertouzos. On data banks and privacy homomorphisms. Foundations of secure computation 1978.
- [DGHV10]** M. van Dijk, C. Gentry, S. Halevi, V. Vaikuntanathan. Fully homomorphic encryption over the integers. EUROCRYPT 2010.
- [BGV12]** Z. Brakerski, C. Gentry, V. Vaikuntanathan. (leveled) fully homomorphic encryption without bootstrapping. ITCS 2012.
- [Bra12]** Z. Brakerski. Fully homomorphic encryption without modulus switching from classical gapsvp. CRYPTO 2012.
- [FV12]** J. Fan, F. Vercauteren. Somewhat practical fully homomorphic encryption. IACR Cryptology ePrint Archive, 2012.
- [CKKS17]** J. H. Cheon, A. Kim, M. Kim, Y. Song. Homomorphic encryption for arithmetic of approximate numbers. ASIACRYPT 2017.
- [GSW13]** Craig Gentry, Amit Sahai, and Brent Waters. Homomorphic encryption from learning with errors: Conceptually-simpler, asymptotically-faster, attribute-based. CRYPTO 2013.
- [DM15]** L. Ducas, D. Micciancio. FHEW: bootstrapping homomorphic encryption in less than a second. EUROCRYPT 2015.
- [CGGI16]** I. Chillotti, N. Gama, M. Georgieva, M. Izabachène. Faster fully homomorphic encryption: Bootstrapping in less than 0.1 seconds. ASIACRYPT 2016.