life.augmented

Full Homomorphic Encryption and its applications with Neural Networks and smart card

March 2021

Amedeo Veneroso
amedeo.veneroso@st.com

STMicroelectronics

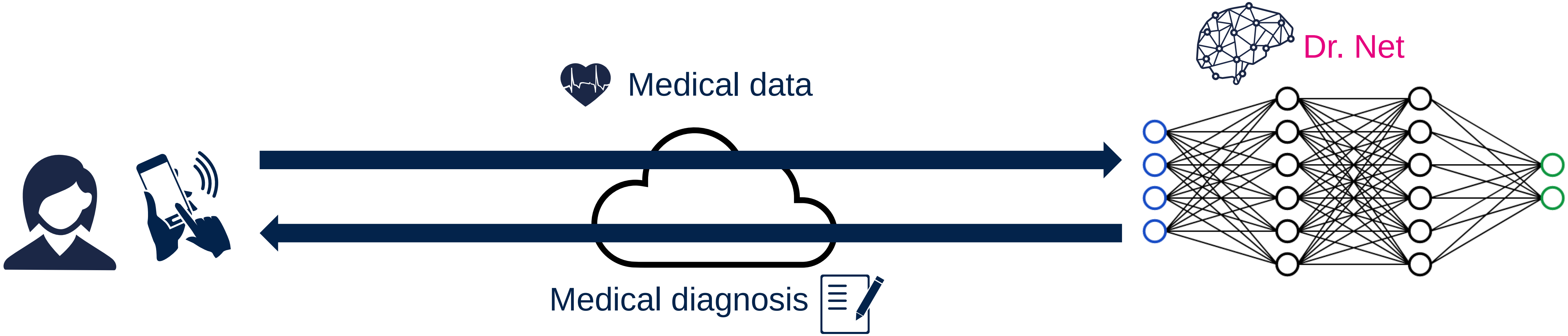
- One of the world’s largest semiconductor companies
- 2020 revenues of **$10.2 B**
- **46,000** employees of which **8,100** in R&D
- Over **80** Sales & marketing offices serving over **100,000** customers across the globe
- **11** Manufacturing sites
- Signatory of the United Nations Global Compact (UNGC), Member of the Responsible Business Alliance (RBA)

life.augmented

As of December 31, 2020

Need some privacy?

Dr. Net is a cool guy, but it doesn't mean that you have to trust him!



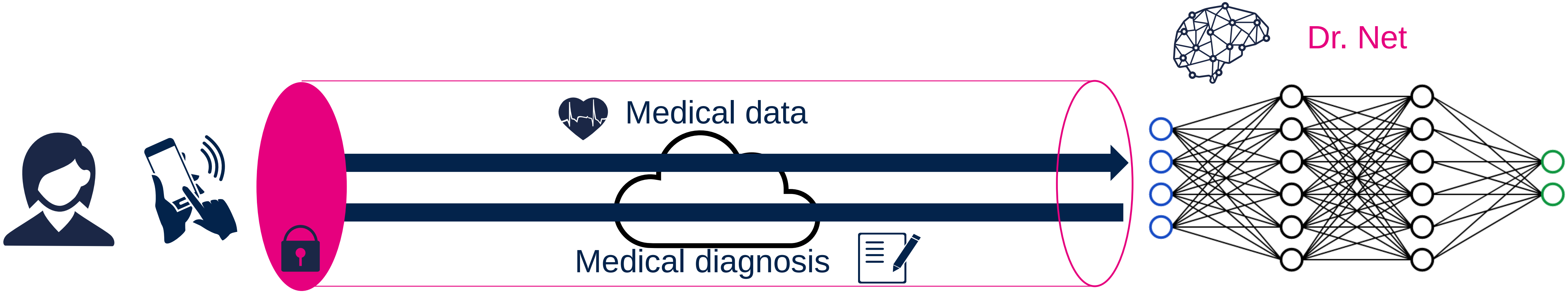
Privacy data have higher management cost

For sensitive data user confidence is required

Regulation becomes more and more demanding

HTTPs is not the cure

Creating a secure channel



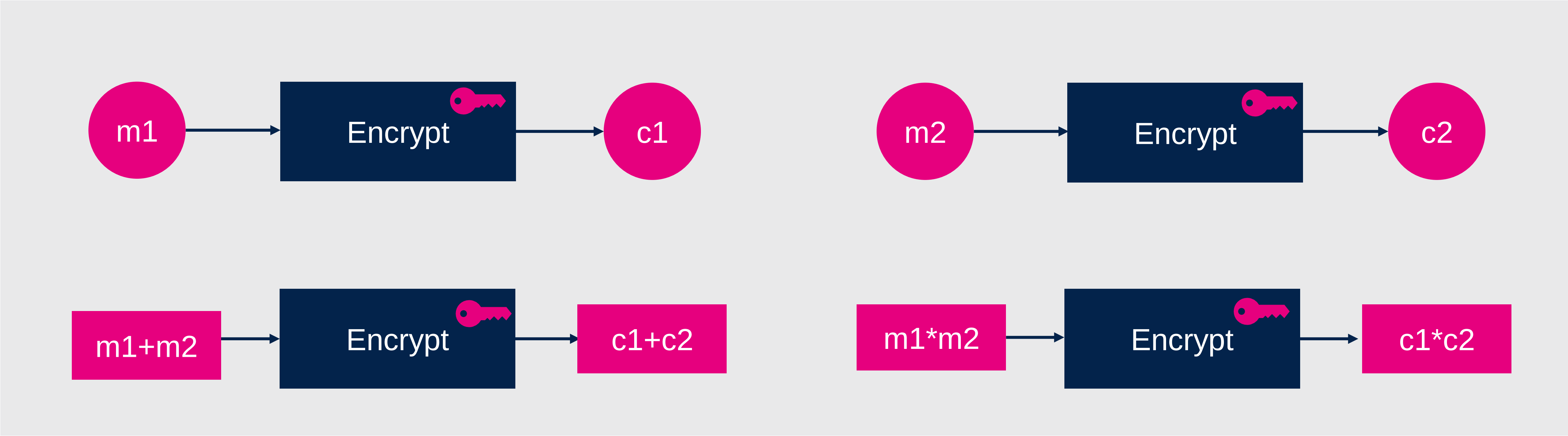
“Traditional” cryptography (symmetric, asymmetric…) may be applied to protect the data

It protects from malicious third parties…

…but Dr. Net needs to decrypt the data for the diagnosis – you always have to trust Dr. Net!

life.augmented

Full Homomorphic Encryption



m1 → Encrypt → c1

m2 → Encrypt → c2

m1+m2 → Encrypt → c1+c2

m1*m2 → Encrypt → c1*c2

Input data are encrypted by user secret key

Operations are performed "blindly" on encrypted data

Result can be decrypted only by user key

e-Voting

Outsourced computation

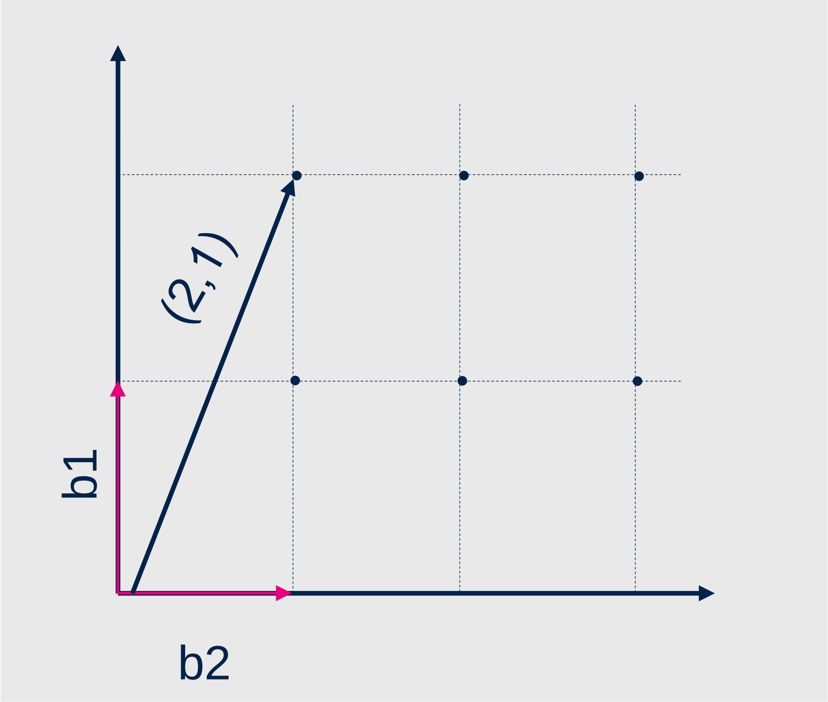
Private biometry

Machine Learning

life.augmented

Lattice cryptography

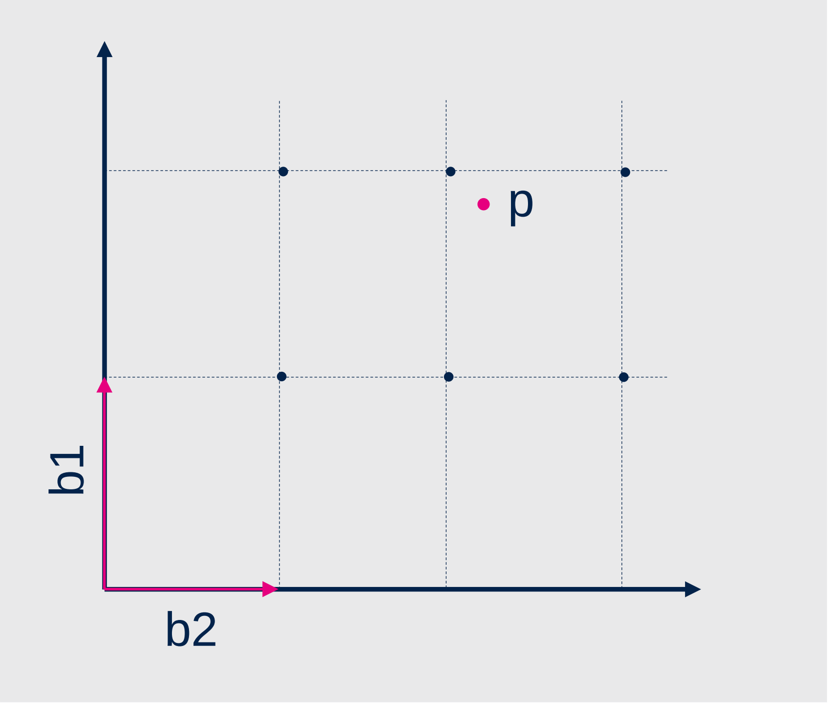
Take a lattice…



A set of points obtained multiplying vectors by integers

The same lattice may be generated by different basis

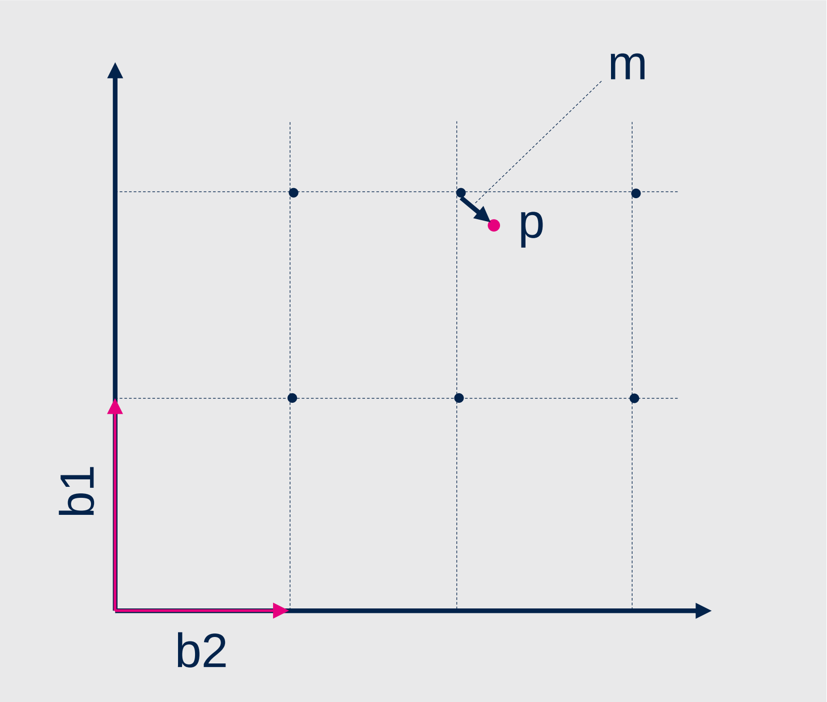
…that creates a (np) problem!



Closest Vector Problem

Which is the lattice point closest to P?

Lattice cryptography



The *closest vector problem* complexity depends on the basis

For some basis (Euclidean) it’s easy, for others it’s not

“message” is the distance of *p* from the closest vector

A cryptosystem is born!

s = an Euclidean basis
m = message
(A, p) = Ciphertext (*A* is a different basis for the same lattice)
The cryptosystem is Full Homomorphic
(and post-quantum…)

life.augmented

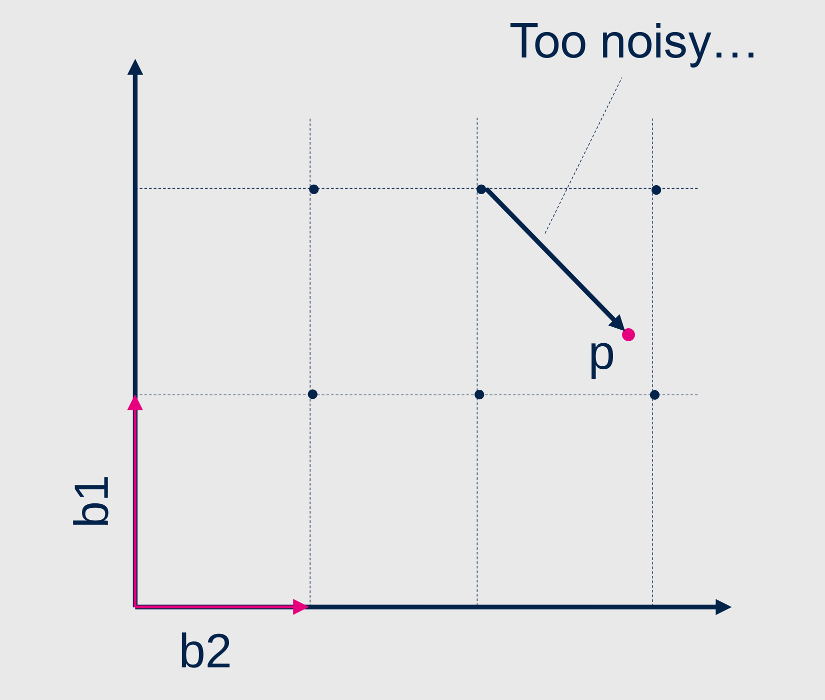
Hear some noise?

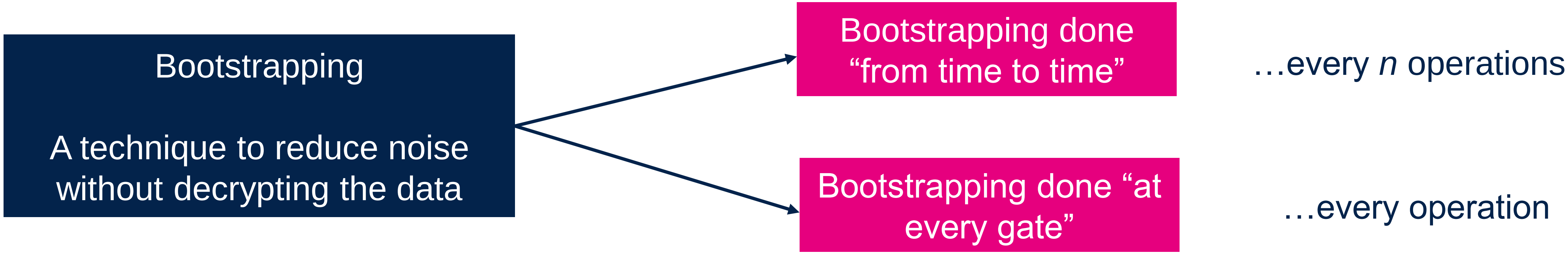
When we perform homomorphic encryption, we add noise

When we perform operations, we increase noise

Noise(A+B) ~ Noise(A)+Noise(B)
Noise(A*B) ~ Noise(A)*Noise(B)

…until there is too much noise…





Bootstrapping

A technique to reduce noise without decrypting the data

Bootstrapping done "from time to time"

…every *n* operations

Bootstrapping done "at every gate"

…every operation

life.augmented

Some nice FHE library

Many different FHE cryptosystems are currently developing:

TFHE

BFV

BGV

CKKS

and many FHE open-source libraries… you can play with them

Concrete

PALISADE

SEAL

HeLib

nuFHE

http://homomorphicencryption.org

A consortium to standardize homomorphic encryption

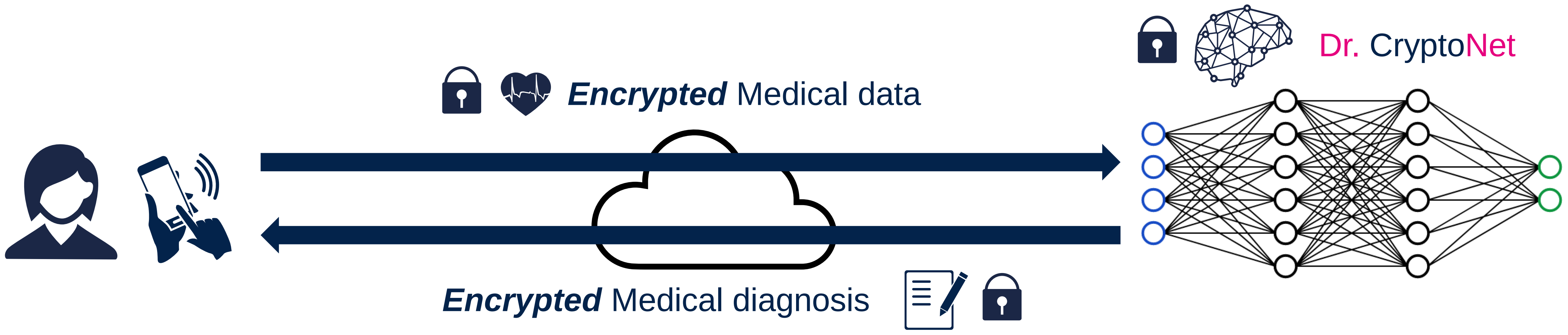
Security

Speed

Memory footprint

Meet Dr. CryptoNet

Neurons are replaced by homomorphic neurons



Client encrypts with a FHE key

Neural operations are replaced by their FHE equivalent

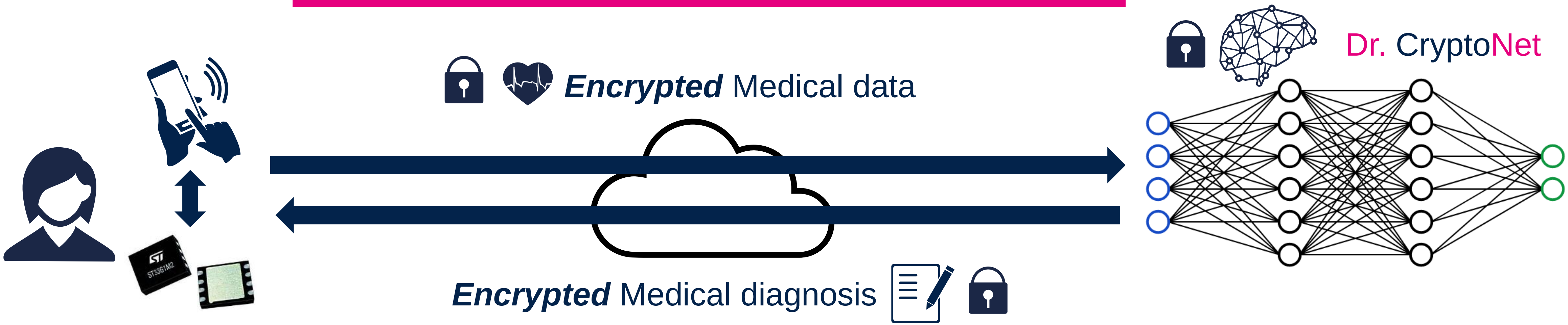
Bootstrapping is done at every neuron or at different stages

Dr. CryptoNet doesn't know the data, doesn't know the diagnosis but he does its job!

life.augmented

And on the client?

Life is more secure with Secure Elements



Encrypted Medical data

Dr. CryptoNet

Encrypted Medical diagnosis

High end devices (PC, smartphones, tablet…) often contain a secure element, a chip protected “by design”

Tamper resistant

Cryptographic accelerated

Internal secure storage

Anti-clone features

ST is working to a FHE cryptosystem based on “TFHE” (FHE over the Torus) with:

- Secret keys stored on secure element
- High speed performances

Thank you

life.augmented