# An introduction to Fully Homomorphic Encryption

Marco Rinaudo

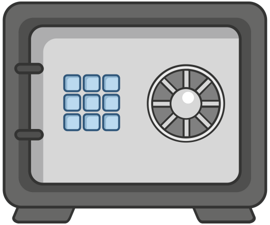
Telsy | A TIM ENTERPRISE BRAND

May 26, 2023

# Encryption for data protection

Using encryption schemes we are able to protect

- **Data-in-transit**
- **Data-at-rest**



**Warning**

In order to process data (**data-in-use**) we have to decrypt it, exposing the cleartext information!



Telsy A TIM ENTERPRISE BRAND

# A solution: Homomorphic Encryption

**Homomorphic Encryption (HE)** allows a third party to perform some computations directly on encrypted data.

HE was first theorized in 1978 by Rivest, Adleman and Dertouzos [RAD78].

# A solution: Homomorphic Encryption

**Homomorphic Encryption (HE)** allows a third party to perform some computations directly on encrypted data.

HE was first theorized in 1978 by Rivest, Adleman and Dertouzos [RAD78].

## Definition

Let $\mathcal{M}$ be the set of plaintexts, $\mathcal{C}$ the set of ciphertexts and

$$*\colon \mathcal{M} \times \mathcal{M} \to \mathcal{M} \qquad \text{and} \qquad \bullet\colon \mathcal{C} \times \mathcal{C} \to \mathcal{C},$$

two operations.
An encryption scheme $E\colon \mathcal{M} \to \mathcal{C}$ is called **homomorphic** with respect to $*$ and $\bullet$ if it holds:

$$E(m_1) \bullet E(m_2) = E(m_1 * m_2) \qquad \forall m_1, m_2 \in \mathcal{M}.$$



Telsy A TIM ENTERPRISE BRAND

# Different families of HE

We can divide HE cryptosystems in three families:

- **Partially Homomorphic Encryption (PHE)** schemes (e.g. RSA [RSA78], ElGamal [Elg85])
- **Somewhat Homomorphic Encryption (SHE)** schemes (e.g. BGN [BGN05])
- **Fully Homomorphic Encryption (FHE)** schemes (e.g. BGV [BGV12], TFHE [Chi+19], CKKS [Che+17])

FHE has been called the **"Holy Grail of cryptography"** because of its groundbreaking potential

# RSA - Partially Homomorphic Encryption

Introduced in 1978 by Rivest, Shamir, Adleman [RSA78].

- **KeyGen**:

$$\mathbf{PK} = (e, n = p \cdot q) \quad \mathbf{SK} = d$$

  where $p, q$ are primes and $ed \equiv 1 \mod \phi(n)$.

- **Enc**: Given a message $0 \leq m < n$, compute ciphertext $c$ as

$$c \equiv m^e \mod n$$



Telsy A TIM ENTERPRISE BRAND

# RSA - Partially Homomorphic Encryption

Introduced in 1978 by Rivest, Shamir, Adleman [RSA78].

- **KeyGen**:

$$\textbf{PK} = (e, n = p \cdot q) \quad \textbf{SK} = d$$

  where $p, q$ are primes and $ed \equiv 1 \mod \phi(n)$.
- **Enc**: Given a message $0 \leq m < n$, compute ciphertext $c$ as

$$c \equiv m^e \mod n$$

## Homomorphic property

$$\begin{aligned} E(m_1) \cdot E(m_2) &= (m_1^e \, mod \, n) \cdot (m_2^e \, mod \, n) = \\ &= (m_1 \cdot m_2)^e \, mod \, n = \\ &= E(m_1 \cdot m_2) \end{aligned}$$



Telsy A TIM ENTERPRISE BRAND

# BGN - Somewhat Homomorphic Encryption

Proposed in 2005 by Boneh, Goh, Nissim [BGN05].

- **KeyGen**: Choose primes $p_1, p_2$ and output $(n, G, G_1, e, g, h)$ where
  - $n = p_1 p_2$
  - $G, G_1$ cyclic groups of order $n$
  - $g$ generator of $G$
  - $e \colon G \times G \to G_1$ bilinear map s.t. $e(g, g)$ generator of $G_1$
  - $h = u^{p_2}$, with $u \neq g$ another generator of $G$

$$\mathbf{PK} = (n, G, G_1, e, g, h) \quad \mathbf{SK} = p_1$$



Telsy A TIM ENTERPRISE BRAND

# BGN - Somewhat Homomorphic Encryption

Proposed in 2005 by Boneh, Goh, Nissim [BGN05].

- **KeyGen**: Choose primes $p_1, p_2$ and output $(n, G, G_1, e, g, h)$ where
  - $n = p_1 p_2$
  - $G, G_1$ cyclic groups of order $n$
  - $g$ generator of $G$
  - $e\colon G \times G \to G_1$ bilinear map s.t. $e(g, g)$ generator of $G_1$
  - $h = u^{p_2}$, with $u \neq g$ another generator of $G$

$$\mathbf{PK} = (n, G, G_1, e, g, h) \quad \mathbf{SK} = p_1$$

- **Enc**: Given a message $0 \leq m < p_2$, compute ciphertext $c$ as

$$c = g^m h^r \in G$$

with $r \in \{0, \ldots, n-1\}$ random.



Telsy A TIM ENTERPRISE BRAND

# BGN - Somewhat Homomorphic Encryption

Proposed in 2005 by Boneh, Goh, Nissim [BGN05].

- **KeyGen**: Choose primes $p_1, p_2$ and output $(n, G, G_1, e, g, h)$ where
  - $n = p_1 p_2$
  - $G, G_1$ cyclic groups of order $n$
  - $g$ generator of $G$
  - $e\colon G \times G \to G_1$ bilinear map s.t. $e(g, g)$ generator of $G_1$
  - $h = u^{p_2}$, with $u \neq g$ another generator of $G$

$$\mathbf{PK} = (n, G, G_1, e, g, h) \quad \mathbf{SK} = p_1$$

- **Enc**: Given a message $0 \leq m < p_2$, compute ciphertext $c$ as

$$c = g^m h^r \in G$$

  with $r \in \{0, \dots, n-1\}$ random.
- **Dec**: Given ciphertext $c$ recover $m$ by computing

$$c' = c^{p_1} \quad \text{and} \quad g' = g^{p_1}$$

  and solving

$$m = \log_{g'}(c')$$



Telsy A TIM ENTERPRISE BRAND

# BGN - Somewhat Homomorphic Encryption

- **Enc**: Given a message $0 \leq m < p_2$, compute ciphertext $c$ as

$$c = g^m h^r \in G$$

with $r \in \{0, \ldots, n-1\}$ random.

## Homomorphic properties

**Addition**: take $r \in \mathbb{Z}_n$ random

$$E(m_1)E(m_2)h^r = \overbrace{(g^{m_1}h^{r_1})}^{\in G}\overbrace{(g^{m_2}h^{r_2})}^{\in G}h^r = g^{m_1+m_2}h^{r'} = \overbrace{E(m_1+m_2)}^{\in G}$$

**Multiplication**: compute $g_1 = e(g,g)$ and $h_1 = e(g,h)$, pick $r \in \mathbb{Z}_n$ random

$$e(E(m_1),E(m_2))h_1^r = \underbrace{e(g^{m_1}h^{r_1}, g^{m_2}h^{r_2})}_{\in G_1}h_1^r = g_1^{m_1 m_2}h_1^{r'} = \underbrace{E(m_1 \cdot m_2)}_{\in G_1}$$


Telsy A TIM ENTERPRISE BRAND

# LWE and error growth in FHE

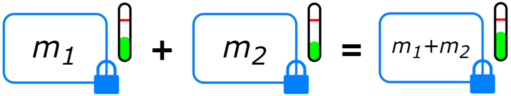
The majority of FHE schemes base their security on hard problems on lattices also used in **Post-Quantum Cryptography (PQC)**.

Many Fully Homomorphic Encryption schemes are based on the **Learning With Error (LWE)** problem and its variants.

# LWE and error growth in FHE

The majority of FHE schemes base their security on hard problems on lattices also used in **Post-Quantum Cryptography (PQC)**.

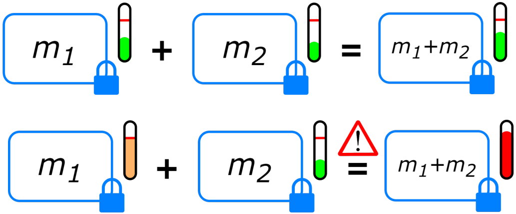
Many Fully Homomorphic Encryption schemes are based on the **Learning With Error (LWE)** problem and its variants.



# LWE and error growth in FHE

The majority of FHE schemes base their security on hard problems on lattices also used in **Post-Quantum Cryptography (PQC)**.

Many Fully Homomorphic Encryption schemes are based on the **Learning With Error (LWE)** problem and its variants.



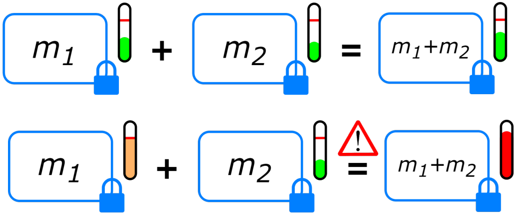



Telsy A TIM ENTERPRISE BRAND

# LWE and error growth in FHE

The majority of FHE schemes base their security on hard problems on lattices also used in **Post-Quantum Cryptography (PQC)**.

Many Fully Homomorphic Encryption schemes are based on the **Learning With Error (LWE)** problem and its variants.




Two possible approaches to deal with error growth:

- Leveled FHE schemes
- **Bootstrapping**



Telsy A TIM ENTERPRISE BRAND

# Bootstrapping

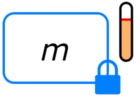
Technique introduced by Craig Gentry [Gen09] and used in many schemes nowadays.

Consists in homomorphically evaluating the decryption function to reduce the error.

# Bootstrapping

Technique introduced by Craig Gentry [Gen09] and used in many schemes nowadays.

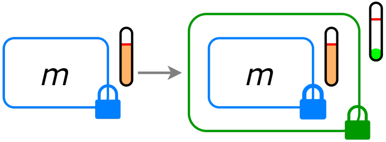
Consists in homomorphically evaluating the decryption function to reduce the error.



# Bootstrapping

Technique introduced by Craig Gentry [Gen09] and used in many schemes nowadays.

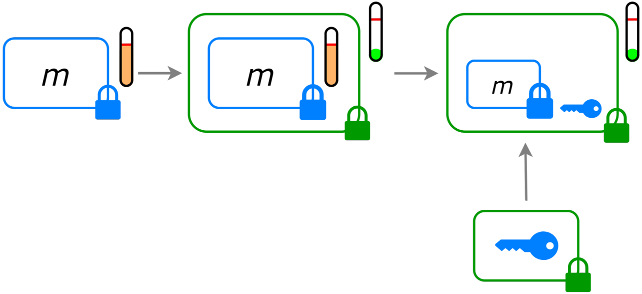
Consists in homomorphically evaluating the decryption function to reduce the error.



# Bootstrapping

Technique introduced by Craig Gentry [Gen09] and used in many schemes nowadays.

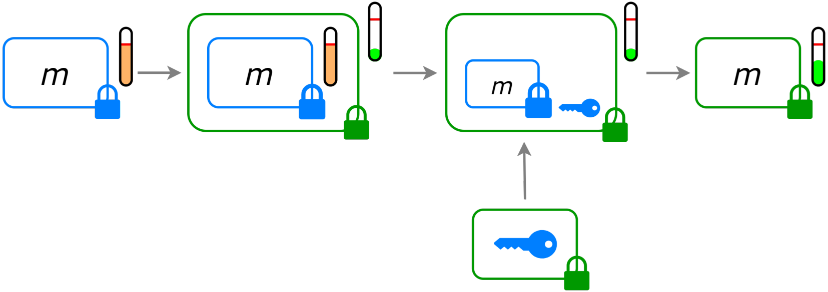
Consists in homomorphically evaluating the decryption function to reduce the error.



# Bootstrapping

Technique introduced by Craig Gentry [Gen09] and used in many schemes nowadays.

Consists in homomorphically evaluating the decryption function to reduce the error.






Telsy A TIM ENTERPRISE BRAND

# FHE timeline

The first Fully Homomorphic Encryption scheme was described in 2009 by Craig Gentry in his PhD thesis [Gen09].

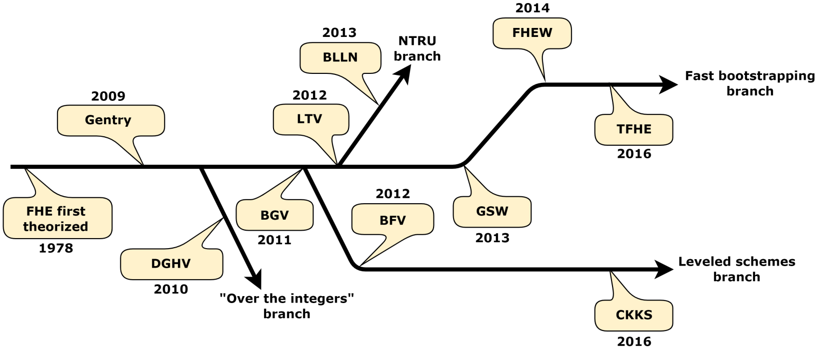



Image taken from [Chi21]



Telsy A TIM ENTERPRISE BRAND

# Performance and future perspectives



Telsy A TIM ENTERPRISE BRAND

# Performance and future perspectives

- Big computational overhead, but improved a lot since 2009
- Gap between FHE and cleartext operations is narrowing thanks to
  - Academic research (Hybrid Homomorphic Encryption)
  - Funded projects (DARPA DPRIVE)
  - Industry involvement (Zama, IBM, Google)

# Use cases

WORLD ECONOMIC FORUM

**Fully homomorphic encryption is the Holy Grail**

Forbes

**What Is Homomorphic Encryption? And Why Is It So Transformative?**

Digital Health, HealthTech, Cyber Security, Life Sciences & BioTech innovation since 2016

Homepage

Digital Health Hype Circles

London, England, UK

Search...

Lloyd Price · 2 min read

Fully Homomorphic Encryption: the next big thing for Healthcare data

- Cloud computing
- Machine Learning training and inference
- Medical research
- Stock market predictions
- Electronic voting
- Supply Chain

# Tools for Homomorphic Encryption

- Zama TFHE-rs, Concrete Python, Concrete ML
- OpenFHE
- Microsoft SEAL
- IBM HElib
- Google FHE C++ Transpiler



Telsy A TIM ENTERPRISE BRAND

# References I


[BGN05] D. Boneh, E. Goh, and K. Nissim. "Evaluating 2-DNF Formulas on Ciphertexts". In: *TCC*. Vol. 3378. 2005.

[BGV12] Z. Brakerski, C. Gentry, and V. Vaikuntanathan. "(Leveled) Fully Homomorphic Encryption without Bootstrapping". In: *Proceedings of the 3rd Innovations in Theoretical Computer Science Conference*. ITCS '12. 2012.

[Che+17] J. Cheon, A. Kim, M. Kim, and Y. Song. "Homomorphic Encryption for Arithmetic of Approximate Numbers". In: *International Conference on the Theory and Application of Cryptology and Information Security*. 2017.

[Chi+19] I. Chillotti, N. Gama, M. Georgieva, and M. Izabachène. "TFHE: Fast Fully Homomorphic Encryption Over the Torus". In: *Journal of Cryptology* 33 (2019).

[Chi21] I. Chillotti. "TFHE Deep Dive". `https://www.youtube.com/watch?v=npoHSR6-oRw&ab_channel=FHE_org`. 2021.

[Elg85] T. Elgamal. "A public key cryptosystem and a signature scheme based on discrete logarithms". In: *IEEE Transactions on Information Theory* 31.4 (1985).

# References II


[Gen09] C. Gentry. “A fully homomorphic encryption scheme”. PhD thesis. Stanford University, 2009.

[RAD78] R. L. Rivest, L. Adleman, and M. L. Dertouzos. “On data banks and privacy homomorphisms”. In: *Foundations of secure computation* 4.11 (1978).

[RSA78] R. L. Rivest, A. Shamir, and L. Adleman. “A Method for Obtaining Digital Signatures and Public-Key Cryptosystems”. In: *Commun. ACM* 21 (1978).

# Thank you

marco.rinaudo@telsy.it