

Crittografia omomorfica e voto elettronico



Giulio Golinelli 20/07/2021
Relatore: Luciano Margara
Università di Bologna
Ingegneria e scienze informatiche

Che cos'è la crittografia omomorfica?

$$D_{k^-}(f_1(E_{k^+}(m_1), E_{k^+}(m_2))) = f_2(m_1, m_2)$$

**Moltiplicazione
omomorfica**

$$D_{k^-}(f_1(c_1, c_2)) = m_1 \cdot m_2$$

**Addizione
omomorfica**

$$D_{k^-}(f_2(c_1, c_2)) = m_1 + m_2$$

Parzialmente omomorfica

- Fine degli anni settanta, con la scoperta di RSA
- Un numero illimitato di una particolare operazione
- Sfrutta proprietà omomorfe intrinseche del proprio schema
- Veloce, sicura

Esempi: RSA, **Paillier**, Damgård-Jurik..

Pienamente omomorfica

- Prima generazione nel 2009, Craig Gentry
- un numero illimitato di qualsiasi operazione
- Schemi complessi e funzioni di bootstrapping
- Lenta, sicura

Esempi: TFHE, CKKS, GSW..

Schema crittografico di Paillier: 1

Formule e algoritmi:

$$G_{k^+, k^-}, E_{k^+}, D_{k^-}$$

Cifratura:

$$E_{k^+}(m) = g^m r^n \bmod n^2$$

Decifratura:

$$d_{k^-}(c) = \frac{L(c^\lambda \bmod n^2)}{L(g^\lambda \bmod n^2)} \bmod n$$

Schema crittografico di Paillier: 2

Proprietà omomorfica 1:

$$\begin{aligned}c_1 \cdot c_2 &= g^{m_1} r_1^n g^{m_2} r_2^n \bmod n^2 \\&= g^{m_1 + m_2} r_1^n r_2^n \bmod n^2 \\&= g^{m_1 + m_2} (r_1 r_2)^n \bmod n^2\end{aligned}$$

Proprietà omomorfica 2:

$$c^{m_2} = \left(E_{k^+}(m_1) \right)^{m_2} = g^{m_1 m_2} r^{n m_2} \bmod n^2$$

Voto elettronico: Minosse

Minosse

Electronic voting

Funzionamento




1. Raccolta voti criptati
2. Moltiplicazione con peso
3. Conteggio dei voti
4. Presentazione dei risultati

Features

1. Responsive
2. Accessibile
3. Reattivo
4. Sicuro

Minosse si basa sulla **trasparenza** delle elezioni! 🙌🙌

Stato dell'arte e sviluppi futuri

- La crittografia omomorfica rimane una cifratura sperimentale e molto recente su cui la ricerca scientifica sta progredendo molto velocemente! 
- Tra qualche anno la crittografia omomorfica rivoluzionerà il cloud computing e il concetto di saas a cui siamo abituati. 
- Al momento non esiste nessuna piattaforma di voto elettronico **trasparente** e **sicura** in grado di essere utilizzata in produzione, anche se molti paesi stanno investendo moltissimo in questo campo e si stanno muovendo verso questa direzione. 
- Minosse rimane una piattaforma puramente dimostrativa ma con ulteriore lavoro e ricerca potrebbe essere impiegata per una vera elezione. 