Fully Homorphic Encryption

Giulia Droandi

Dipartimento di Ingegneria dell'Informazione e Scienze Matematiche,
University of Siena, ITALY

Somewhat homomorphic

Chiavi

- *Segreta*: scelgo p dispari
- *Pubblica*: $x_0 = pq_0 + 2r_i$ dispari, $\{x_i = pq_i + r_i; i \in [0, \tau]\}$,

cifratura

$m \in \{0, 1\}$ messaggio scelgo $s \subseteq \{1, \ldots \tau\}$

$$c = \left[m + 2r + 2 \sum_{i \in S} x_i \right]_{x_0}$$

decifratura

$$m = \Big[[c]_p \Big]_2 \approx \left[c - \left\lfloor \frac{c}{p} \right\rfloor \right]_2$$

parametri

λ parametro di sicurezza
$\gamma = \omega(\eta^2 \log \lambda)$ lunghezza in bit chiave pubblica
$\eta \geq \rho \cdot O(\lambda \log^2 \lambda)$ lunghezza in bit chiave privata
$\rho = \omega(\log \lambda)$ lunghezza in bit del rumore
$\tau \geq \lambda + \omega(\log \lambda)$ numero interi chiave pubblica
$\theta = \lambda$ cardinalità di S
$k = \frac{\gamma\eta}{\rho}$ cifre binarie dopo la virgola
$\Theta = \omega(k \cdot \log \lambda)$

parametri da tenere a mente
$\rho = \lambda$
$\eta = O(\lambda^2)$
$\gamma = O(\lambda^5)$
$\tau = \gamma + \lambda$
$k = \gamma + 2$

Full Homomoriphic encription

Chiavi

- *Segreta*: scelgo $S \subseteq \{1 \dots \theta\}$ indici
- *Pubblica*: $x_0 = pq_0 + 2r_i$ dispari e $\{x_i = pq_i + r_i; i \in [0, \tau]\}$ e $\{y_1 \dots y_l\}$ tali che:
  sia $x_p = \left\lfloor \frac{2^k}{p} \right\rceil$,
  $\forall j = 1 \dots \theta : u_j \in [\mathbb{Z} \cap 2^{k+1})$

$$\sum_{i \in S} u_i = x_p (mod 2^{k+1})$$

$y_i \in [0, 2]$, $y_i = \frac{u_i}{2^k}$ tali che $[\sum_{i \in S} yi]_2 \approx \frac{1}{p}$

y_i sono numeri razionali con k bit di precisione dopo la virgola

cifratura

$m \in \{0,1\}$ messaggio scelgo $s \subseteq \{1, \ldots \Theta\}$

$$c^* = \left[m + 2r + 2 \sum_{i \in S} x_i \right]_{x_0}$$

$\forall i = \ldots \Theta$, $z_i = [c^* \cdot y_i]_2$ razionali con $n = \lceil \log \theta \rceil + 3$ bit di precisione dopo la virgola
cifrato coppia $c = (c^*, \mathbf{z})$

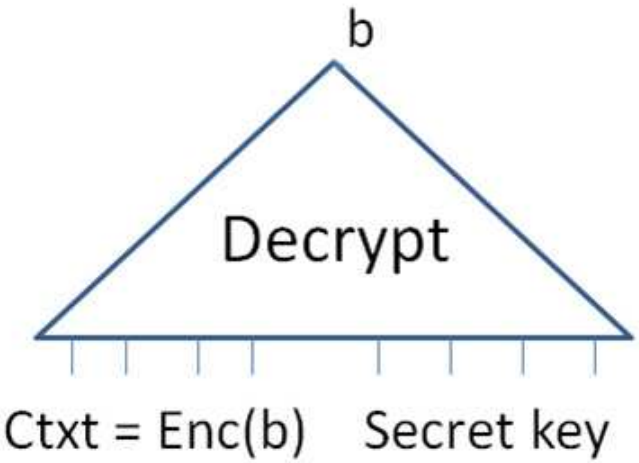
decifratura

$$m = \left[c^* - \left\lfloor \sum_{i=1}^{\tau} s_i z_i \right\rfloor \right]_2$$

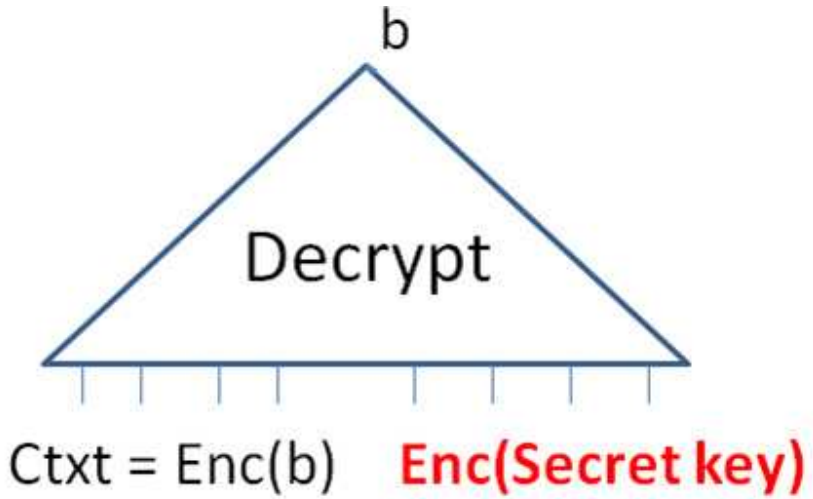
$s_i = 1$ sse $i \in S$, $s_i = 0$ altrimenti

Bootstrapping

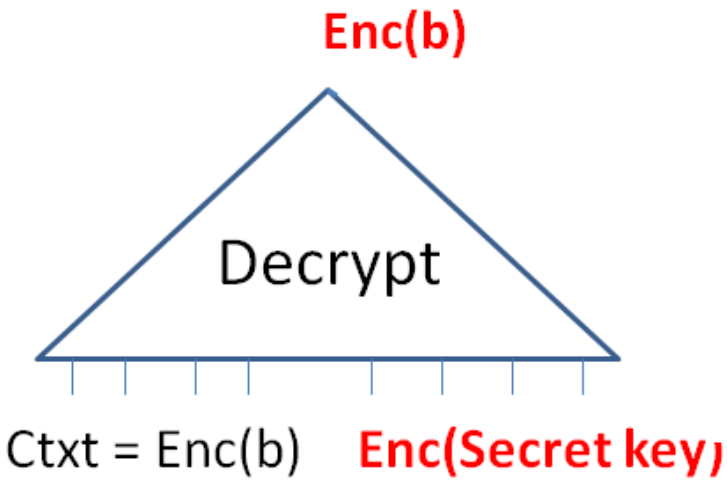
Qualsiasi schema di cifratura omomorfa è basato sul rumore.
Ogni operazione lo fa aumentare
Cosa diminuisce il rumore e fa recuperare il messaggio?
LA DECIFRATURA



Non posso dare la chiave segreta a tutti, quindi aggiungo un *indizio di chiave segreta* nella chiave pubblica



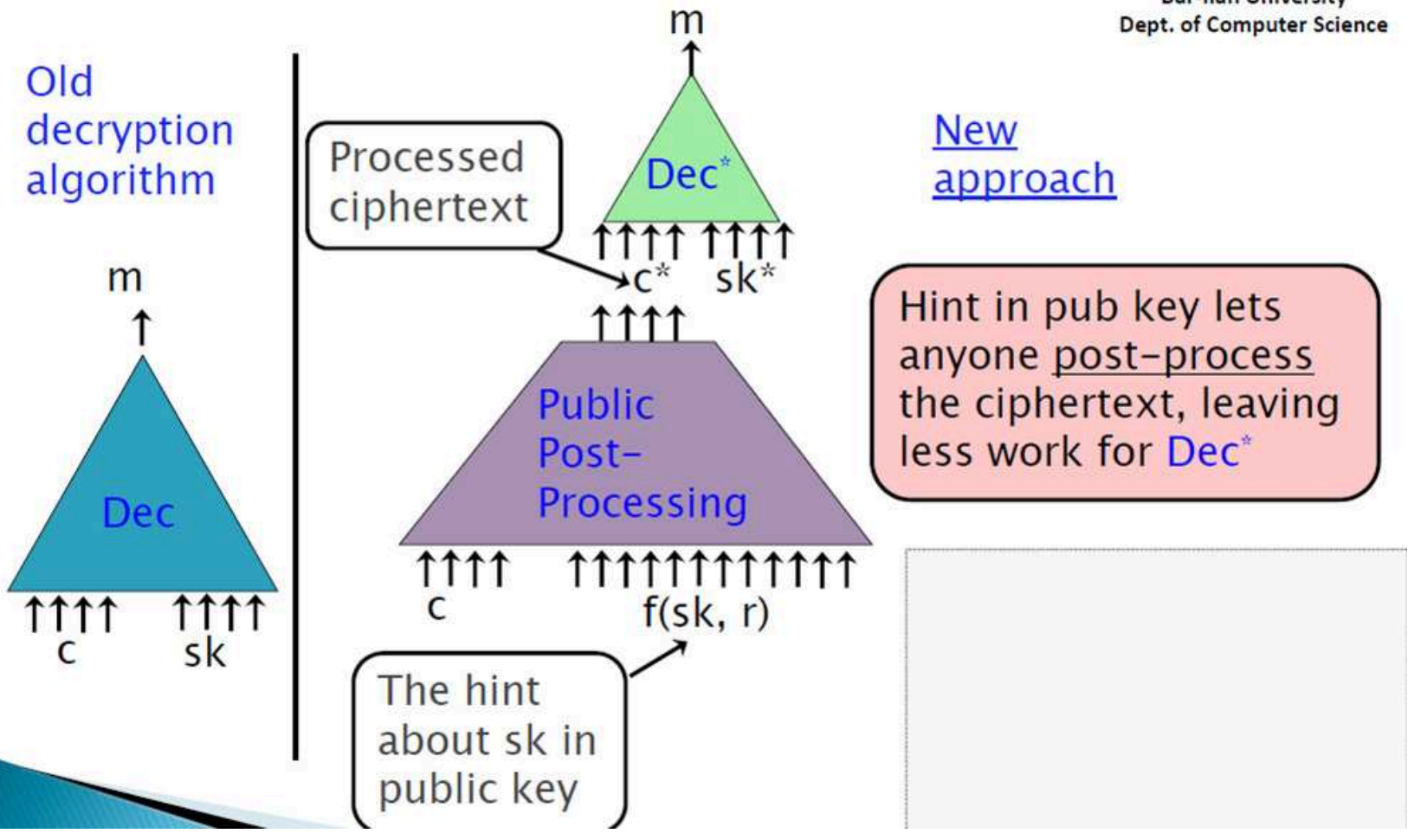
Non posso dare la chiave segreta a tutti, quindi aggiungo un *indizio di chiave segreta* nella chiave pubblica



Il messaggio in entrata e uscita è lo stesso, e rimane cifrato.
Cambia il livello di rumore della cifratura.

How to"simplify" decryption?

Bar-Ilan University
Dept. of Computer Science



Teorema bootstrapping di Gentry

Se uno schema di cifratura può valutare omomorficamente il suo stesso circuito di decifratura, allora può valutare qualsiasi cosa.

Ovvero il circuito di decifratura deve essere esprimibile come un polinomio valutabile omomorficamente all'interno del sistema stesso

fhe modificato

Genero $\sigma_i = q_i p - \epsilon_i p + 2r_i + s_i$ cifratura dei bit della chiave segreta.
Memorizzo i σ_i nel vettore σ
$\epsilon_i \in [0, 2^{(\gamma+\eta)/p}[$

$$Decrypt(sk, c^*, \mathbf{z}) = \left[c^* - \left\lfloor \sum_{i=1}^{\tau} s_i z_i \right\rfloor \right]_2$$

Quando il rumore cresce troppo applico

$$c_{new} = recrypt(\sigma, c^*, \mathbf{z}) = \left[c^* - \left\lfloor \sum_{i=1}^{\tau} \sigma_i z_i \right\rfloor \right]_2$$

ottenendo un nuovo testo cifrato c_{new}


Van Dijk, M. and Gentry, C. and Halevi, S. and Vaikuntanathan, V., *Fully homomorphic encryption over the integers*, Advances in Cryptology–EUROCRYPT 2010, pages 24-43, year 2010, Springer


Coron, J.S. and Mandal, A. and Naccache, D. and Tibouchi, M., *Fully homomorphic encryption over the integers with shorter public keys*, Advances in Cryptology–CRYPTO 2011, 487–504, 2011, Springer


Coron, J.S. and Naccache, D. and Tibouchi, M., *Public Key Compression and Modulus Switching for Fully Homomorphic Encryption over the Integers*, Advances in Cryptology–EUROCRYPT 2012, 446–464, 2012, Springer

Grazie per l'attenzione.