La crittografia omomorfa

Federico Giacon, 1059578
Università degli Studi di Padova

federico.giacon.1@studenti.unipd.it

Torre Archimede, aula 1AD100
25 luglio 2014,
ore 9:00

Sommario

La crittografia omomorfa è stata per molto tempo un obiettivo ambito da ogni crittografo, per via delle sue numerose applicazioni. Tuttavia solo recentemente il primo algoritmo di cifratura omomorfa è stato pubblicato: la tesi di dottorato del 2009 di Gentry [2] descrive una procedura generale per ottenere uno schema completamente omomorfo a partire da algoritmi con proprietà più deboli.

In questo seminario definirò la cifratura omomorfa e le sue applicazioni, e tramite esempi presenterò le idee sottostanti il lavoro di Gentry per la creazione di schemi di cifratura omomorfa.

Riferimenti bibliografici

[1] Vaikuntanathan, Vinod. Computing Blindfolded: New Developments in Fully Homomorphic Encryption. In *Foundations of Computer Science (FOCS), 2011 IEEE 52nd Annual Symposium on*, vol., no., pp.5,16, 22-25 Oct. 2011.

[2] Gentry, Craig. Fully Homomorphic Encryption Using Ideal Lattices. In *Symposium on the Theory of Computing (STOC)*, 2009, pp. 169-178..