Fully Homomorphic Encryption over Integers

Stefania Lippiello

3 febbraio 2013

Dopo l'avvento del "cloud computing" si è avvertita la necessità di sviluppare nuove tecniche crittografiche che garantiscano un alto grado di affidabilità dal punto di vista della sicurezza dei dati e che, d'altra parte, non limitino la possibilità di operare sui dati stessi. Dati c_1 e c_2 le rispettive codifiche dei messaggi m_1 e m_2, calcoliamo $C = c_1 * c_2$, dove $*$ è un'operazione "semplice" che viene eseguita direttamente sui messaggi cifrati (si noti che si deve poter eseguire $*$ senza conoscere i messaggi in chiaro soggiacenti a c_1 e c_2); ciò che vogliamo è che, decodificando C, si ottenga $m_1 * m_2$, ossia che l'operazione $*$ sia compatibile con le trasformazioni di cifratura e decifratura del crittosistema utilizzato.
Un crittosistema che possiede le suddette caratteristiche viene definito *pienamente omomorfo*; tale proprietà fu ipotizzata nel 1978 da Rivest, Adleman e Dertouzos [1], pochi mesi dopo la prima implementazione di RSA, senza tuttavia che essi riuscissero a fornirne un esempio sicuro. Tale risultato è stato raggiunto nel 2009 grazie al lavoro di Gentry [4]; successivamente, nel 2011, Gentry, in collaborazione con van Dijk, Halevi e Vaikuntanathan [3], ha sviluppato un crittosistema pienamente omomorfo più semplice di quello originale e basato solamente sull'aritmetica modulare. La rilevanza teorica di questi risultati è notevole sebbene vi sia ancora molta strada da fare per ridurre le, attualmente eccessive, richieste di complessità spaziale e temporale che rendono al momento praticamente inutilizzabili i crittosistemi pienamente omomorfi.

In questo seminario analizzeremo i concetti di base necessari alla comprensione del problema e, riferendoci al metodo sviluppato in [3], mostreremo i meccanismi su cui si fonda un crittosistema pienamente omomorfo.

Riferimenti bibliografici

[1] R. L. Rivest, L. Adleman, M. L. Dertouzos, *On data banks and privacy homomorphism*, in "Foundations of Secure Computation" (1978), 169-180.

[2] C. Gentry, *Computing arbitrary functions of encrypted data*, in Comm. of ACM **53** (2010), 97-105.

[3] M. van Dijk, C. Gentry, S. Halevi, V. Vaikuntanathan, *Fully homomorphic encryption over the integers*, in Advances in Cryptology LNCS 6110 (2010), 24-53.

[4] C. Gentry, *A fully homomorphic encryption scheme*, PhD thesis, Stanford University, 2009.