PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 25 - numero 5448 di Lunedì 28 agosto 2023

Quanti conoscono l'algoritmo criptografico omomorfico?

Un algoritmo, attualmente sotto esame per la pubblicazione di una norma specifica, che può offrire eccezionali garanzie di trattamento protetto dei dati.

Lo ISO/IEC JTC 1/SC 27 Information security, cybersecurity and privacy protection ha da poco cominciato a lavorare su una proposta di norma così classificata:

ISO/IEC WD 18033-8 -Information security ? Encryption algorithms ? Part 8: Fully Homomorphic Encryption

Questa proposta in norma internazionale illustra i meccanismi crittografici che permettono di calcolare una funzione, relativa ai dati crittografati, pur conservando un elevato livello di riservatezza sui dati in ingresso, i dati intermedi e il risultato del calcolo. Questo particolare algoritmo crittografico si chiama Fully Homomorphic Encryption- FHE.

Il documento normativo in corso di sviluppo offre le definizioni ed i vari formati. Viene illustrato un modello di sicurezza, nonché altri aspetti del meccanismo criptografico, che possono permettere di sviluppare un modello normalizzato.

Vediamo perché questo particolare algoritmo ha destato immediatamente l'attenzione di tutti gli esperti di protezione dei dati personali.

Questo algoritmo, che appartiene alla sempre più numerosa famiglia delle PET-privacy enhancing technologies, permette di utilizzare dei dati e trattarli, senza però avere conoscenza del dato in chiaro.

Forse un semplice esempio può essere utile per meglio comprendere la natura di questo algoritmo criptografico. Supponiamo di avere a disposizione un database con alcune decine di migliaia di nomi di persone fisiche.

Il nostro desiderio è di sapere quante persone fisiche hanno come nome di battesimo "Maria".

Grazie a questo algoritmo, è possibile analizzare tutti i dati nel data base, estrarre tutti i nomi "Maria" e presentare un totale a chi ha richiesto la informazione. La informazione viene fornita senza che il richiedente abbia preso alcuna conoscenza del data base, sia in fase di acquisizione di dati, sia in fase di trattamento di dati stessi.

Non per nulla, attualmente sono in corso numerose discussioni, fra gli esperti di sicurezza, circa il fatto che questi algoritmi FHE possano essere interpretati alla luce di tecniche che riguardano la anonimizzazione e la de-identificazione di dati personali. Ecco, tra l'altro, la ragione per la quale si spera che presto gli enti regolatori possano mettere in chiaro il fatto che l'utilizzo di questo algoritmo soddisfi appieno alle esigenze di trattamento anonimo dei dati, che sono spesso diverse in numerosi paesi europei e in vari contesti legislativi.

È in questo contesto che diventa importante l'opera normativa del comitato, sopra richiamato, perché è bene ricordare a tutti i lettori che la fornitura di un prodotto o la prestazione di servizio, in conformità ad una vigente norma nazionale, europea od internazionale, costituisce fornitura o prestazione conforme alla regola d'arte.

Inoltre, l'utilizzo di una norma internazionale può migliorare la interoperabilità e la compatibilità dei sistemi di trattamento, utilizzati da diversi titolari.

Alcuni produttori di circuiti elettronici aspettano con impazienza la pubblicazione della norma, per sviluppare circuiti elettronici, che possano rendere più rapido ed efficace l'utilizzo di questo algoritmo.

Non mancheremo di tenere aggiornati i lettori su questo affascinante argomento, che consente di offrire elevate garanzie di sicurezza, nel trattamento dei dati, senza comprometterne l'utilizzo corretto dei dati stessi.

Adalberto Biasiotti