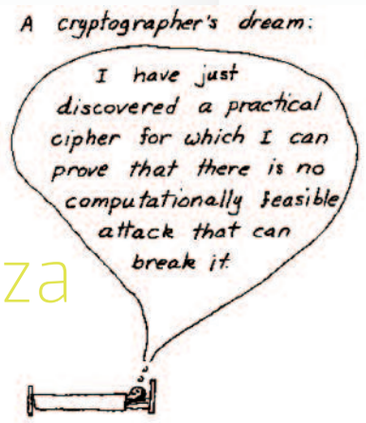
Cifratura del cloud e crittografia quantistica

Due balzi di conoscenza



Massimiliano Sala

La pervasività di sistemi informatici basati sul cloud è ormai assodata. Ogni sistema cloud-based necessita della gestione sicura dei dati da parte del cloud provider e presenta il problema della tutela della loro privacy nei suoi confronti. Questi aspetti rallentano la diffusione del cloud in settori che coinvolgono grandi volumi di dati sensibili, tra cui quello sanitario. Nello sforzo di superare tali limitazioni, sono stati progettati nuovi algoritmi crittografici dalle proprietà sorprendenti, chiamati 'cifrature omomorfe'. Altrettanto stupefacenti sono le proprietà della cosiddetta 'crittografia quantistica', che risolverebbe un problema antichissimo e cruciale nella crittografia: lo scambio della chiave in maniera pienamente sicura. Sebbene i primi dispositivi commerciali siano già sottoposti ad attacchi di 'Quantum Hacking', questa tecnologia si avvicina alla piena maturità. L'articolo presenta due evoluzioni recenti della crittografia, relative ad applicazioni in ambiti diversi, accomunate dalla medesima caratteristica: sciolgono problemi ritenuti irrisolvibili.

Cloud e cifrature omomorfe

Supponiamo la disponibilità di dati da proteggere che, per qualche motivo, non vogliamo (o possiamo) conservare sui nostri computer. Potremmo cifrarli con chiave simmetrica (impiegando Aes, ad esempio) e pagare qualcuno per ospitarceli. Qualora ci servissero, basterebbe farsi ridare il cifrato e decifrarlo. Nel 'basterebbe' sono nascoste due difficoltà: chi accoglie i nostri dati deve essere disponibile a renderceli in qualunque

I disegni sono tratti dalla *Distinguished Lecture*, tenuta all'International Association for Cryptologic Research nel 1996 da James Lee Massey, professore emerito di Digital Technology all'Eth di Zurigo. Nel disegno sopra, *Il sogno del crittografo moderno: la cifra dimostrabilmente rompibile*; a pagina 145, *L'incubo del crittografo moderno: gli attacchi nascosti.*

momento e dovremmo poi custodirli nei nostri server (dove non volevamo o potevamo salvarli) almeno per il tempo necessario a decifrarli. Il primo scoglio è superabile usando un cloud provider, facilmente accessibile ovunque sia presente una connessione internet e che disponga di memoria abbondante. Purtroppo, la seconda difficoltà appare insuperabile perché l'enorme sforzo di decifratura dei dati riscaricati vanificherebbe il vantaggio di aver utilizzato il cloud. Proviamo a immaginare di essere una banca dati di analisi mediche e di annoverare milioni di pazienti, ognuno con numerosi file. Invece di tenerli sui nostri server, collochiamo sul cloud tante cartelline, ognuna corrispondente a un soggetto, contenenti i file cifrati con nostra chiave simmetrica (che ovviamente conserviamo segreta e protetta). Quando ci servono i referti di una persona, basterà scaricare i file cifrati corrispondenti e decifrarli, operazione veloce e leggera perché si tratta di un singolo paziente. In questa situazione sono precluse operazioni più sofisticate, come il controllo delle analisi del sangue effettuate l'anno scorso su 'tutti i pazienti che quest'anno registrano il colesterolo alto'. Questa ricerca potrebbe fornirci preziose indicazioni per prevenire l'insorgere della patologia. Il problema che dobbiamo affrontare è che 'non sappiamo' quali pazienti abbiano il colesterolo alto quest'anno! Per saperlo, infatti, dovremmo scaricare le analisi del sangue cifrate di 'tutti i pazienti, decifrarle tutte' e poi selezionare i soggetti interessati. Queste operazioni, ovviamente, vanificherebbero l'uso del cloud. In alternativa, potremmo condividere la chiave di cifratura con il cloud provider ed eseguire la ricerca direttamente, sacrificando la privacy dei pazienti. Entrambe le soluzioni sono inaccettabili. Di conseguenza, ci servirebbe un cloud che possa operare sui dati, ma 'senza' vederli e, anzi, senza ricavarne informazioni.

La soluzione al problema, che si riteneva irrisolvibile, è stata prospettata nella tesi di dottorato di Craig Gentry presentata nel 2009. Gentry crea un'intera nuova famiglia di algoritmi crittografici, denomimati Fully Homomorphic Encryption (Fhe) – che chiameremo semplicemente 'cifrature omomorfe' – i quali permettono di eseguire direttamente 'operazioni sui cifrati'. Torniamo allora all'esempio. Se avessimo cifrato i dati sanitari con cifrature omomorfe, potremmo chiedere al cloud di cercare, tra tutti i file cifrati, quelli relativi al 2016 che contengono valori alti di colesterolo. Servendoci della cifratura omomorfa, la nostra richiesta è tale che:

- mentre elabora i file, il cloud 'non ne capisce' il contenuto, perché essi rimangono cifrati;
- il cloud 'non sa' nemmeno cosa gli sia stato chiesto e non ha idea dei valori che sta cercando (il colesterolo alto);
- al termine dell'elaborazione, il cloud ci restituisce un elenco di numeri, 'senza poterne ricostruire' il significato;
- l'elenco inviatoci dal cloud, anche se intercettato da nemici, è protetto dalla stessa cifratura omomorfa e 'solo noi' siamo in grado di decifrarlo (oltre a essere gli unici a sapere cosa rappresenti).

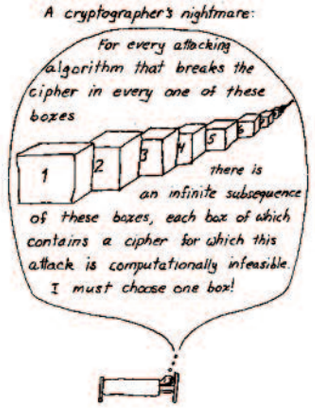
Una volta decifrato l'elenco, potremmo chiedere al cloud di ricercare correlazioni statistiche (sempre sfruttando la cifratura omomorfa) all'interno delle analisi risalenti al 2015, e ancora una volta sarebbero soddisfatte le quattro proprietà listate in precedenza.

I LIMITI ATTUALI DELLE CIFRATURE OMOMORFE

L'idea magnifica di Gentry – attualmente Research Scientist nei laboratori dell'Ibm – è stata destinataria di vari riconoscimenti, tra cui il prestigioso premio della MacArthur Foundation 'Genius' con la seguente motivazione: «Craig Gentry is a computer scientist fueling a 'revolution' in cryptography and theoretical computer science through 'his elegant solutions' to some of the discipline's most challenging open problems».

Sfortunatamente, nelle applicazioni pratiche, il primo schema proposto da Gentry richiede risorse computazionali sproporzionate ed è inefficiente. Negli ultimi anni la ricerca – pubblicata in centinaia di articoli da parte di scienziati di tutto il mondo – si è rivolta a trovare sia cifrature omomorfe migliori sia cifrature che diano risposte parziali (Somewhat Homomorphic Encryption) ma che siano sicuramente più efficienti.

I notevoli miglioramenti apportati negli ultimi anni (operazioni che richiedevano giorni, vengono ora eseguite in pochi minuti) non bastano ancora a ottenere algoritmi che possano essere sfruttati commercialmente (se non, forse, per applicazioni critiche in cui bisogna proteggere per poco tempo dati di enorme valore). Tuttavia rimango fiducioso che, seguendo la strada tracciata da Gentry, si possa giungere a innovazioni radicali nel cloud.



CRITTOGRAFIA QUANTISTICA NELLO SCAMBIO CHIAVI

Spesso si adoperano termini derivati da 'quantum' discutendo di tematiche correlate, anche solo vagamente, alla crittografia. In questo articolo ci soffermiamo sulla cosiddetta Quantum Key Distribution (Qkd), qui chiamata semplicemente 'crittografia quantistica'.

Il problema più antico nella crittografia è lo scambio delle chiavi crittografiche (simmetriche), di cui si è parlato estesamente nei precedenti articoli dedicati su questa rivista alla crittografia. La soluzione matematicamente più elegante coincide con quella più diffusa

al momento, consistendo nell'utilizzo di funzioni one-way, come il logaritmo discreto sulle curve ellittiche, ampiamente discusso nell'articolo I *pratici effetti dell'astrazione matematica nella crittografia* apparso sul n. 4 di «Gnosis» del 2015. Volendo riassumere l'idea in maniera semplice, si può dire che lo scambio delle chiavi tramite funzioni one-way equivale a generare l'istanza di un problema matematico da parte di Alice e Bob mentre comunicano su un canale non protetto (i.e., internet), in maniera che loro ne conoscano la soluzione (avendo costruito assieme l'istanza del problema) ma nessun altro la sappia. La sicurezza del metodo si basa sulla difficoltà della risoluzione del problema matematico sottostante (o, a essere precisi, dell'istanza generata). Non si conoscono, però, problemi matematici impiegati in crittografia che siano 'dimostrabilmente' difficili. In altre parole, esistono di certo molti problemi matematici – tra questi il logaritmo discreto – che 'si suppone' siano difficili e che sono utilizzati in crittografia, sebbene non si possegga alcuna dimostrazione della loro difficoltà. L'uso (ora universale) di funzioni one-way lascia perciò il crittografo coscienzioso con una forte inquietudine, suscitata sia dal dubbio che il nemico conosca un metodo veloce per risolvere il problema matematico sia dalla certezza che, in tal caso, egli si guardi bene dal divulgarne la conoscenza.

Recentemente, a questo scenario classico si è affiancata la possibilità di fare ricorso a tratti ereditati dalla Meccanica Quantistica, branca della Fisica che propone la spiegazione di fenomeni singolari e la formulazione di paradossi, come quello famoso 'del gatto di Schrödinger'. Naturalmente, ogni teoria fisica si basa su principi coerenti con le osservazioni sperimentali (da cui spesso sono derivati), che potrebbero essere abbandonati o rivisti al sopraggiungere di esperimenti in loro contraddizione. D'altro canto, le prove che avallano i principi della Meccanica Quantistica sono così numerose da lasciare solo un dubbio filosofico residuo sulla loro validità, mentre nessuna conferma l'esistenza di funzioni one-way. Al contrario, nei pochi casi che si riescono a studiare esaurientemente al computer, tali funzioni non sono mai state individuate.

Utilizzando i principi della Meccanica Quantistica è possibile progettare dispositivi, quali il Cerberis di IdQuantique o la Q-Box di MagicQ, che Alice e Bob usano per scambiarsi fotoni su un canale quantistico e bit su un canale classico, canali teoricamente leggibili da un nemico. Il protocollo impiegato ottiene i seguenti risultati:

- alla fine dell'interazione, con alta probabilità, Alice e Bob si ritrovano con una 'chiave condivisa';
- qualora il nemico intercetti anche tutta la trasmissione sul canale pubblico, è 'dimostrabile' che egli non ottenga alcuna informazione sulla chiave;
- se il nemico tenti di leggere il canale quantistico, Alice o Bob 'se ne accorgono' e quindi la chiave generata viene scartata.

Già adesso, pertanto, è possibile valersi di questi dispositivi e ottenere chiavi teoricamente al sicuro da 'sguardi' indiscreti.

I LIMITI ATTUALI DELLO SCAMBIO DI CHIAVI QUANTISTICO

Il primo protocollo di scambio di chiavi a giovarsi di questa idea fu ideato da Charles H. Bennett e Gilles Brassard nel 1984, nella cui nomina a Fellow of the Royal Society of London è scritto, tra l'altro: «... is one of the earliest pioneers of quantum information science in the world. His most celebrated breakthroughs are the invention of quantum cryptography and quantum teleportation, both universally recognized as fundamental cornerstones of the entire discipline».

Rispetto all'idea originale di Bennet e Brassard, negli anni sono stati proposti numerosi miglioramenti, variazioni e alternative. L'aspetto più interessante, a mio parere, è l'esistenza di aziende che costruiscono il loro modello di business basandosi sulla commercializzazione di siffatti dispositivi, la cui realizzazione ha condotto a problemi inaspettati: gli attacchi di Quantum Hacking. L'esponente di punta di questa recentissima disciplina è probabilmente Vadim Makarov, dell'University of Waterloo. L'hackeraggio dei sistemi quantistici si basa sul principio fondamentale che, indipendentemente da quanto perfetto possa essere un principio fisico, qualunque dispositivo cerchi di metterlo in pratica sarà costruito con dei difetti microscopici che porteranno a deviazioni rispetto al comportamento atteso. Il gruppo di Makarov ha studiato i principali dispositivi commerciali basati sulla crittografia quantistica ed è riuscito a inserirsi nel canale quantistico sfruttandone alcune leggerissime imperfezioni. In risposta, le aziende stanno sviluppando dei dispositivi che riescano a resistere perlomeno ai primi attacchi pubblicati dal gruppo di Makarov.

CONCLUSIONI

Le idee brillantissime compendiate in questo articolo possono portare a rivoluzioni tecnologiche con ricadute enormi, rivoluzioni tuttavia frenate nella loro realizzazione pratica da ostacoli possenti. Nel caso delle cifrature omomorfe la barriera è costituita dall'inefficienza del software che esegue gli algoritmi, mentre nel caso della crittografia quantistica è posta dai difetti dell'hardware che implementa il protocollo. Anche se si tratta di sfide ardue, credo fermamente che entrambi gli ostacoli siano superabili, considerato l'enorme potenziale applicativo che spingerà costantemente la comunità scientifica a occuparsene attivamente

G