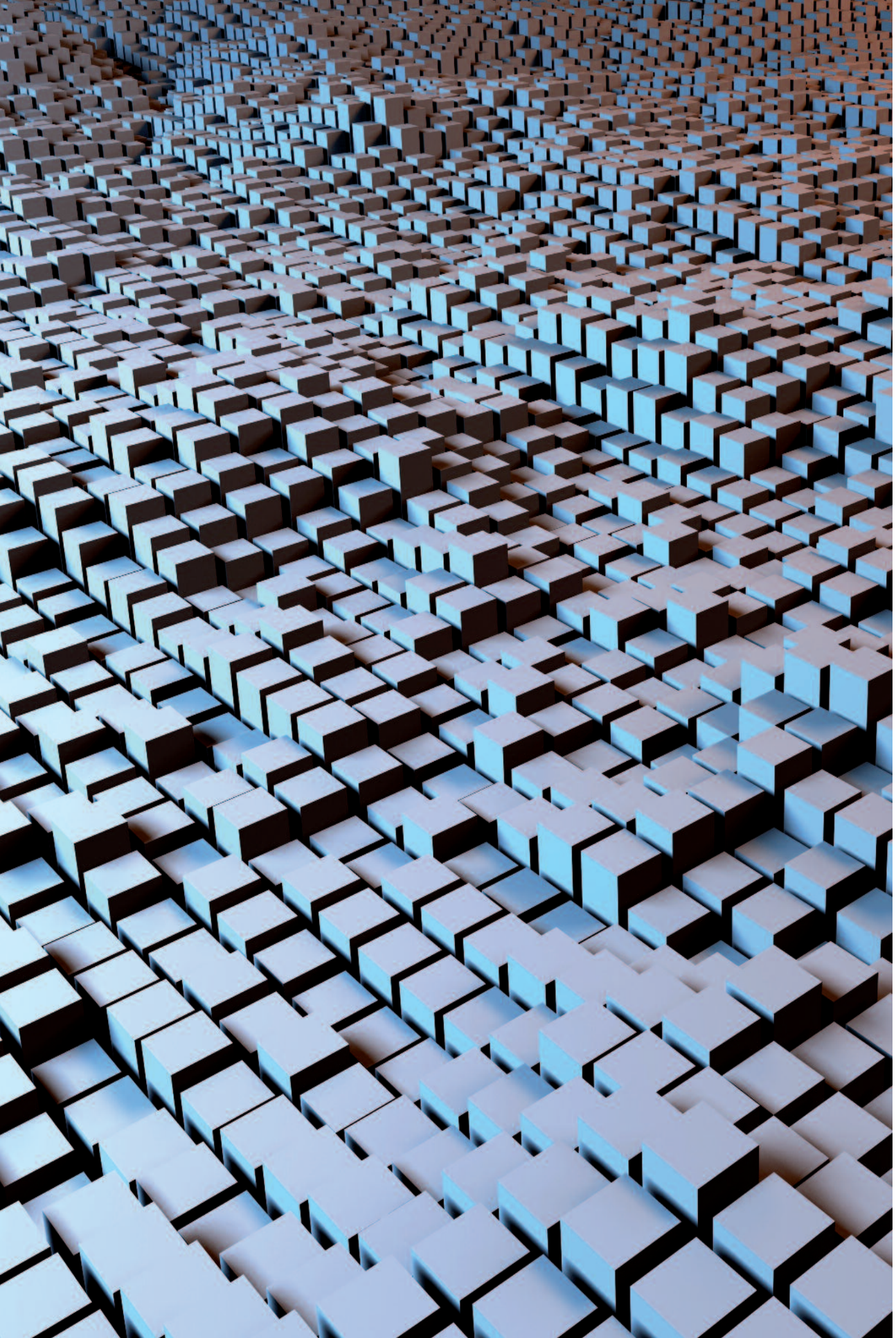

Il futuro della crittografia teorica e pragmatica e il post quantum

Marco Baldi – Michele Elia – Massimiliano Sala

In questo articolo si tenta di tratteggiare i futuri sviluppi teorici e pratici della crittografia anche in conseguenza dell'incremento delle tecnologie microelettroniche volte alla realizzazione di microprocessori sempre più veloci e del recente potenziamento degli elaboratori basati sulla meccanica quantistica.

Thus we may have knowledge of the past but cannot control it; we may control the future but have no knowledge of it.

Claude Elwood Shannon

Nella sua millenaria storia, la crittografia è passata da impieghi quasi esclusivamente in questioni di governo, diplomazia o militari, a un uso pervasivo e indispensabile nella vita quotidiana delle persone. Anche se nella sua evoluzione ha raggiunto un soddisfacente grado di formalizzazione, sono ancora molti gli aspetti che vanno completati e le direzioni in cui ragguardevoli miglioramenti sono attesi; si stanno delineando, inoltre, nuove vie secondo cui investigare alla ricerca di paradigmi sfuggiti alle pur attente, acute e profonde ricerche condotte, nei secoli scorsi, dalle migliori menti.
Le definitive basi assiomatiche della crittografia poste dallo statunitense Claude Elwood Shannon (1916-2001) hanno consentito di precisare i limiti delle cifrature in chiave segreta. Tuttavia, la crittografia in chiave pubblica (che si è poi sviluppata e che prevede

scenari completamente diversi) non ha ancora trovato una propria definitiva e soddisfacente sistemazione teorica. In particolare, la nozione di *funzione one-way* (ossia facile da calcolare in un verso ma difficile da invertire[1]) non ha ancora una definizione rigorosa.
Di tutte quelle oggi largamente impiegate come funzioni one-way, sia in ambito civile che militare, di nessuna è stata ancora dimostrata, in modo rigoroso, la pretesa proprietà – poiché non è ancora comprovata la difficoltà del sottostante problema matematico – per cui si dovrebbe parlare, più precisamente, di funzioni *one-way putative*. È prevedibile che in un futuro, magari lontano, i fondamenti della crittografia in chiave pubblica ricevano un'accettabile sistemazione teorica, determinando condizioni favorevoli per sostanziali perfezionamenti applicativi. Nello stesso tempo, i progressi della tecnologia elettronica offrono enormi capacità di calcolo che, a loro volta, richiedono sviluppi teorici apportatori di nuove idee e di nuovi algoritmi. Peraltro, l'avvento di tecnologie basate sulla meccanica quantistica ha fatto emergere due aspetti correlati, ma ben distinti. Per un verso, tecniche crittografiche che sfruttano direttamente i principi quantistici hanno determinato una rapida obsolescenza degli algoritmi classici, soppiantandoli con protocolli ad hoc[2]; per un altro, il *quantum computing* impone la proposizione di algoritmi crittografici che gli possano resistere, i cosiddetti *post quantum*[3]. Su questi ultimi osserviamo che il National Institute of Standards and Technology (Nist) ha appena pubblicato un primo report nel quale lo sviluppo di tali algoritmi s'identifica come una direzione prioritaria per il futuro della crittografia.
Tra le classi di algoritmi post-quantum che oggi paiono le più promettenti si annoverano gli algoritmi basati sui codici correttori d'errore che – introdotti nel 1978 dall'americano Robert McEliece per la crittografia in chiave pubblica – non ebbero molta fortuna per via dell'eccessiva dimensione della chiave. Gli stessi, oggi contano varianti capaci di offrire dimensioni delle chiavi notevolmente ridotte e competitive. Questi algoritmi si basano sulla difficoltà di compiere ricerche all'interno di un insieme enorme non-ordinato di numeri. È stato teoricamente provato, altresì, che essi appartengono alla classe di problemi cosiddetti NP (N*on-deterministic* P*olynomial*) che potrebbero resistere al quantum computing. Una seconda classe si basa sulla difficoltà di risolvere sistemi di equazioni algebriche quadratiche in molte variabili (precisamente, sulla NP-*hardness*).

1. «Gnosis» 4/2015.
2. «Gnosis» 3/2016.
3. «Gnosis» 4/2015.

Una terza classe di algoritmi crittografici a chiave pubblica candidata alle applicazioni post quantum è quella fondata sul concetto algebrico di reticolo, comprese le varianti basate sul problema del *learning with errors*, che consiste nella ricostruzione di una funzione da alcune sue imprecise valutazioni. Tale formulazione ha consentito di definire taluni algoritmi innovativi per la crittografia asimmetrica, corredati di severe dimostrazioni di sicurezza. Infine, sistemi di cifratura in chiave privata, con la dimensione della chiave sufficientemente grande, sono sicuri anche rispetto ad attacchi con calcolatori quantistici. Ad esempio, una versione del sistema A*dvanced* E*ncryption* S*tandard* (AES) chiamata AES256 rimarrebbe sicura[4], mentre le altre cadrebbero (AES128 e AES192).

LA METAMORFOSI DELLA DICOTOMIA CRITTOGRAFIA-APPLICAZIONI

Recentemente si è imposto un trend imprevisto, determinato da una metamorfosi subita dalla dicotomia crittografia-applicazioni. Fino a non più di vent'anni fa le applicazioni utilizzavano la crittografia nota a quel momento per raggiungere gli obiettivi di sicurezza e in gran parte è ancora così. Ad esempio, la comunicazione tra il proprio computer e il server di home banking dell'istituto di credito è protetta dalla crittografia contro i tentativi d'infiltrazione da parte di malfattori, semplici curiosi o avversari. Ma se si pensa alla cifratura specializzata usata per proteggere i dati biometrici[5] o a quella omomorfa impiegata nel cloud, ad esempio per i dati sanitari[6], ci si rende conto che sono le applicazioni a generare nuova crittografia, ribaltando completamente la dicotomia.
Nuovi esempi di questo genere sono forniti dagli schemi crittografici basati su identità (*identity-based encryption*) o su attributi (*attribute-based encryption*), i quali hanno per scopo principale una gestione delle chiavi private tesa a superare le problematiche dovute alla distribuzione e all'integrità delle chiavi pubbliche. Questi schemi sono basati su una vecchia idea del crittografo israeliano Adi Shamir per l'uso di chiavi condivise – rivisitata in tempi recenti con dimostrazioni di sicurezza – peraltro ancora

4. «Gnosis» 4/2015.
5. «Gnosis» 1/2016.
6. «Gnosis» 3/2016.

solo parzialmente risolti. In altre parole, le applicazioni, la cui lunghissima lista è destinata a crescere indefinitamente, si sono trasformate da soggetto che usa crittografia a oggetto stesso di crittografia, perché le metodologie d'uso richiedono non solo un esperto utilizzo degli schemi disponibili, ma addirittura la creazione di nuovi algoritmi e paradigmi.
Tra le applicazioni più promettenti si possono citare sia realizzazioni di attività ludiche – come i giochi delle carte a distanza – sia pratici servizi che puntano a cambiare la vita di ogni giorno, come la moneta elettronica anonima, la votazione elettronica a distanza, la gestione delle bio-impronte. Ma anche quelle che ormai diamo per scontate, come la geo-localizzazione, possono dare sviluppi imprevisti (come, ad esempio, permettere a due agenti in territorio nemico di conoscere la reciproca posizione senza rivelare la loro posizione assoluta agli avversari, grazie alla cifratura omomorfa).

IL VIAGGIO È APPENA INIZIATO

Oltre l'orizzonte che siamo in grado di osservare, s'intravede la ricerca di fondamenti teorici incontrovertibili e validi per i nuovi paradigmi crittografici, necessariamente non solo basati sull'ipotetica complessità di problemi che sono difficili da risolvere. Lo sviluppo di nuovi algoritmi post quantistici, oltre a quelli prima ricordati, resta una sfida per l'inventiva e lo spirito di avventura dell'uomo.
Forse saranno gli sviluppi tecnologici a imporre nuove vie alla crittografia, ma su questo sentiero – guardando i pochi millenni che riusciamo a scorgere e la prodigiosa evoluzione che la creatività umana ha viepiù accelerato – è difficile fare previsioni anche di sola fantasia nello stile leggero, ma in concreto profetico, di Jules Verne.
Prosaicamente, oltre non riusciamo a scorgere il futuro della crittografia ma solo a intuire la ciclopica ricerca che sarà dispiegata nello sviluppo di nuove applicazioni, convenendo con le parole attribuite a Winston Churchill, per il quale: «Success is not final, failure is not fatal: it is the courage to continue that counts»