BANCA D'ITALIA
EUROSISTEMA

La crittografia nell'evoluzione digitale: nuovi orizzonti tra opportunità e sfide tecnologiche

Intervento di apertura di Alessandra Perrazzelli
Vice Direttrice Generale della Banca d'Italia

CIFRIS24 – National Conference on Cryptography
Roma, 25 settembre 2024

Signore e Signori, buongiorno[*].

Sono lieta di aprire la seconda edizione di CIFRIS24.

Ringrazio gli organizzatori per aver coinvolto la Banca d'Italia nel dialogo accademico, istituzionale e industriale che avverrà in questo convegno di rilevanza internazionale. Si tratta di un'importante occasione di riflessione e discussione degli avanzamenti scientifici su tematiche che si dimostrano sempre più essenziali nel contesto odierno.

1. Pervasività della crittografia

La crittografia è una disciplina antica, sviluppata per garantire la protezione delle informazioni riservate. Nel tempo, ha subito una costante evoluzione: dai primi cifrari, come quello di Cesare utilizzato a scopi militari, ai più complessi sistemi crittografici del Medioevo, sino ad arrivare al XX secolo, dove la crittografia ha assunto un ruolo cruciale: pensiamo ad esempio alla macchina Enigma e agli sforzi compiuti per decrittarne i messaggi durante la Seconda Guerra Mondiale.

In un'epoca profondamente influenzata dall'innovazione digitale, la crittografia ha una rilevanza senza precedenti. Essa rappresenta non solo un elemento chiave per la salvaguardia della privacy e della sicurezza globale, ma anche un motore di sviluppo economico e tecnologico.

Un esempio lampante è l'*e-commerce*: nel 2023, il 70 per cento dei cittadini dell'Unione Europea tra i 16 e i 74 anni ha acquistato beni e servizi online[1]. Dietro a questo successo si nasconde l'efficacia dei protocolli crittografici, che garantiscono transazioni sicure e proteggono i dati sensibili, come i numeri di carta di credito, creando un clima di fiducia nei confronti del commercio digitale.

---

[*] Desidero ringraziare Giuseppe Zingrillo, Claudia Biancotti e Michela Iezzi per i loro contributi al presente intervento.

[1] Eurostat, Statistic Explained, "*E-commerce statistics for individuals*", aprile 2024.

2. Sistemi di pagamento

Il funzionamento dei mercati e dei sistemi di pagamento è stato profondamente rivoluzionato dalle soluzioni tecnologiche basate sulla crittografia.

Si pensi alle cripto-attività, ovvero rappresentazioni digitali di valore che possono essere emesse, trasferite e conservate digitalmente, utilizzando le *distributed ledger technologies*, le quali si fondano sui principi della crittografia e del consenso distribuito. Risulta evidente come l'utilizzo di queste tecnologie apra le porte a un più ampio insieme di intermediari finanziari, prospettando al contempo guadagni di efficienza in termini di costi e di tempi di esecuzione delle operazioni.

In questo contesto di decentralizzazione, le garanzie di sicurezza delle transazioni sono affidate alla crittografia. Tuttavia, pur conferendo maggiore dinamicità e competitività al panorama finanziario, questo fermento richiede un'attenta valutazione dei nuovi rischi e delle sfide che ne derivano.

Pertanto, è compito delle autorità e delle istituzioni garantire un equilibrio tra l'innovazione tecnologica e la necessità di assicurare sistemi finanziari e di pagamento stabili e sicuri per il bene di cittadini e imprese.

Sebbene un approccio regolamentare più tradizionale possa contribuire a mantenere tale equilibrio, è importante riconoscere che la regolamentazione e l'innovazione tecnologica evolvono a ritmi differenti, con la prima che tende a "inseguire" la seconda.

È dunque indispensabile che anche le Istituzioni considerino le opportunità offerte dalla crittografia, per rispondere tempestivamente all'evoluzione del contesto esterno.

3. *Post-Quantum Cryptography*

Un'evoluzione tempestiva è richiesta anche a fronte della necessità di attuare una transizione post-quantistica delle comunicazioni e delle transazioni digitali.

La crittografia a chiave pubblica si è finora dimostrata efficace nel proteggere le comunicazioni e le transazioni, sia su Internet sia sulle reti private. La sicurezza degli algoritmi crittografici è di tipo computazionale: in altri termini, risiede sull'ipotesi che i computer classici non siano in grado di compromettere tali algoritmi, poiché il costo computazionale sarebbe troppo elevato.

Tuttavia, i computer quantistici operano in modo differente e possono violare gli algoritmi e i protocolli su cui abbiamo fatto affidamento negli ultimi decenni.

Sebbene un computer quantistico con tali capacità non sia ancora disponibile, i rapidi progressi nel campo del *quantum computing* lasciano presagire che entro il prossimo decennio possa essere realizzato un dispositivo in grado di minacciare la sicurezza e la privacy di individui, organizzazioni e intere nazioni. In un futuro non troppo lontano, potremmo trovarci nell'impossibilità di garantire la segretezza e l'integrità delle nostre transazioni e comunicazioni digitali.

Già oggi non devono essere sottovalutate le minacce del tipo "*Harvest now, decrypt later*", in cui un attore ostile potrebbe raccogliere e immagazzinare dati cifrati, attualmente inutilizzabili, con la prospettiva di decifrarli e impiegarli non appena un computer quantistico sarà disponibile.

Non tutta la crittografia è vulnerabile alle minacce derivanti dal quantum computing: una soluzione mitigativa è costituita dallo sviluppo della cosiddetta crittografia post-quantum, la quale utilizza algoritmi matematici differenti che, allo stato dell'arte, non sono violabili da un computer quantistico.

Di recente, il *National Institute of Standards and Technology* statunitense (NIST) ha annunciato l'approvazione di tre nuovi algoritmi di crittografia post-quantum, due basati su reticoli e uno basato su funzioni di *hash*[2]. Questi standard offrono protezione a una vasta gamma di informazioni digitali, dai messaggi di posta elettronica riservati alle transazioni di *e-commerce* che alimentano l'economia moderna.

Risulta evidente come sia necessaria una rapida e proattiva transizione verso algoritmi crittografici resistenti ai computer quantistici.

4. *Privacy-Enhancing Technologies (PETs)*

Non meno rilevante è l'applicazione della crittografia per la condivisione delle informazioni con garanzia di privacy.

In qualità di Banca Centrale, disponiamo di molteplici fonti di dati riservati – sia strutturati, sia non strutturati – derivanti dalla natura variegata dei servizi che offriamo. Ogni singola fonte informativa è gestita da un diverso *data owner*, il che comporta l'esistenza di differenti livelli di accesso volti a controllare e prevenire l'elaborazione e la diffusione non autorizzate.

La condivisione di dati tra Istituzioni e con la comunità accademica potrebbe consentire l'ottenimento di risultati di pubblica utilità che sarebbero difficilmente raggiungibili adottando una logica a silos informativi. Questo favorirebbe inoltre l'integrazione con altri ambiti di conoscenza, fungendo da catalizzatore per l'innovazione e la competizione. Inoltre, il potenziale offerto dalle tecnologie *cloud*, quali l'archiviazione di grandi volumi di dati e l'elaborazione ad alte prestazioni, potrebbe essere sfruttato in modo più completo.

D'altro canto, la condivisione dei dati con terze parti comporta rischi di violazione della privacy. Bilanciare l'urgente necessità di analisi di dati per il progresso tecnologico e sociale con la protezione della privacy degli individui rappresenta una sfida complessa.

Le tecnologie orientate alla protezione della privacy, note come *Privacy-Enhancing Technologies*, svolgono un ruolo cruciale nel bilanciare queste due esigenze contrapposte.

---

2 NIST, "*Announcing Approval of Three Federal Information Processing Standards (FIPS) for Post-Quantum Cryptography*", 13 agosto 2024.

Tecniche come la *secure multi-party computation*, la crittografia omomorfica, il *secure federated learning* e la generazione di dati sintetici possono fungere da strumenti abilitanti per la condivisione sicura dei dati sensibili, preservando al contempo la privacy. Su tutti questi fronti la Banca è attivamente impegnata.

4.1 *Homomorphic encryption (HE) e Secure Multi-Party Computation (SMPC)*

In particolare, lo sviluppo e la standardizzazione di algoritmi omomorfici consentirebbero un'adozione sicura e ampia dei servizi di *cloud computing* da parte delle istituzioni e delle aziende.

La crittografia omomorfica permette di effettuare calcoli complessi su dati cifrati, senza la necessità di decifrarli, estendendo così i concetti già noti di cifratura *at-rest* e *in-transit* a quello di cifratura *in-use*. Tali elaborazioni complesse possono includere analisi statistiche e algoritmi di intelligenza artificiale. Sin dalla sua introduzione nel 2009, sono stati compiuti notevoli avanzamenti in termini di tempi di computazione e usabilità.

L'adozione della crittografia omomorfica consentirebbe di delegare le elaborazioni più sofisticate a terze parti, garantendo simultaneamente la piena riservatezza dei dati, anche in presenza di una minaccia quantistica.

Compiti analoghi in tale ambito di utilizzo sono svolti dalla *secure multi-party computation*, la quale consente a più entità di collaborare nell'esecuzione di calcoli su un insieme di dati condivisi, senza rivelare le informazioni sottostanti a nessuna delle parti coinvolte.

4.2 *Synthetic Data*

Tra le *Privacy-Enhancing Technologies*, la generazione di dati sintetici riveste un ruolo significativo nella protezione dei dati sensibili.

I dati sintetici sono progettati per replicare le proprietà statistiche dei dati originali, pur non includendo dettagli che possono ricondurre agli individui appartenenti alla popolazione originaria. Grazie a queste caratteristiche, le analisi condotte sui dati sintetici dovrebbero fornire risultati molto simili a quelle effettuate sui dati originali, rendendoli uno strumento prezioso nelle fasi di addestramento dei modelli di intelligenza artificiale e di *testing* delle applicazioni informatiche.

4.3 *Challenges delle PETs*

L'adozione delle *Privacy-Enhancing Technologies* presenta non poche complessità; diversi fattori possono ostacolare il loro utilizzo. Tra le principali barriere, si annoverano la mancanza di standardizzazione, le difficoltà nell'identificazione di casi d'uso efficaci, nonché le difficoltà nel reperire le necessarie competenze tecniche.

5. Come vogliamo rapportarci col mondo accademico

Sebbene la crittografia sia ancora frequentemente percepita come un settore riservato esclusivamente agli specialisti, è fondamentale riconoscere che essa costituisce una risorsa strategica non solo per la protezione del sistema finanziario, ma anche per la salvaguardia della nostra società nella sua interezza.

Per affrontare le sfide poste dagli avanzamenti tecnologici e per sfruttare appieno le opportunità offerte dalla crittografia e dalle tecnologie a essa correlate, è essenziale che le istituzioni finanziarie collaborino strettamente con il mondo accademico. Solo attraverso tale collaborazione si potrà creare un ambiente favorevole in cui matematici, crittografi, ingegneri, economisti e giuristi possano confrontarsi e sviluppare soluzioni innovative e sicure.

È nostro compito dimostrare lungimiranza nell'accogliere l'innovazione tecnologica. La crittografia, con le sue molteplici e sempre più diffuse applicazioni, riveste un ruolo centrale nella transizione verso un futuro in cui le istituzioni assumeranno una dimensione digitale. Queste iniziative non solo promuovono la ricerca scientifica, ma incoraggiano anche la condivisione della conoscenza, permettendoci di progredire insieme, con sana curiosità, verso un futuro solido, consapevole tanto dei rischi quanto anche delle grandi opportunità.

* * *

Concludo esprimendo il mio sincero ringraziamento a tutti voi per l'attenzione e un sentito apprezzamento agli organizzatori e al comitato scientifico per aver creato un programma ricco di contenuti stimolanti.

Grazie dell'attenzione e buon lavoro.

Grafica a cura della Divisione Editoria e stampa della Banca d'Italia