PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 20 - numero 4193 di Venerdì 09 marzo 2018

Computer potenti possono violare sofisticati algoritmi crittografici

L'aumento della potenza di calcolo dei computer, cresciuta in modo esponenziale con lo sviluppo dei computer quantici, ha reso facilmente violabili gli algoritmi crittografici, che per decenni sono stati considerati punto di riferimento quasi assoluto.

Negli anni recenti, c'è stato un incremento costante delle ricerche dirette sui computer quantici (quantum computer), vale a dire macchine che utilizzano i fenomeni meccanici dei quanti per risolvere problemi matematici, che sono difficili o quasi irrisolubili per computer convenzionali.

Poiché la potenza di calcolo dei computer quantici continua a crescere, è da ritenere del tutto probabile che nel giro di una decina di anni saranno disponibili dei computer quantici di grande dimensione, che potranno violare la maggior parte degli algoritmi criptografici a chiave pubblica, che correntemente sono in uso. Ciò porterebbe ad una compromissione drammatica della riservatezza ed integrità delle comunicazioni digitali via Internet ed altrove.

L'obiettivo di sviluppare algoritmi crittografici che siano resistenti ad un attacco con computer quantici, oltre evidentemente a computer tradizionali, deve sposarsi con la capacità di interoperare con gli esistenti protocolli e reti di comunicazione.

Il rapporto sviluppato dall'Istituto nazionale per le normative e le tecnologie fa il punto su questa situazione e mette in evidenza come sia indispensabile muoversi verso nuove infrastrutture criptografiche. In chiusura di questo articolo vedremo come il problema viene oggi tempestivamente affrontato.

Tanto per cominciare, è bene fare presente che in passato si riteneva che dei computer quantici di grandi dimensioni potessero essere teoricamente realizzabili, ma che in realtà questa specifica architettura fosse più teorica che pratica. Oggi tutti i tecnici sono convinti che si tratta solo di superare problemi di natura tecnologica, ma senza ostacoli insuperabili.

Alcuni esperti addirittura predicono che entro i prossimi 20 anni, ed anche meno, potranno essere disponibili dei computer quantici di potenza tale da poter violare tutti gli algoritmi crittografici a chiave pubblica che oggi sono correntemente utilizzati.

D'altro canto, non dimentichiamo che vent'anni è il periodo che è stato effettivamente utilizzato per giungere all'attuale infrastruttura di criptografia a chiave pubblica.

Occorre quindi affrontare fin da adesso il problema di migrare le esistenti reti ed applicazioni criptografiche verso nuove formulazioni, che possano dare un sufficiente livello di garanzia contro un attacco con computer quantici.

Pertanto, indipendentemente del fatto che si possa valutare con esattezza il tempo nel quale questi computer di grande potenza saranno disponibili, è meglio avere fin da adesso un quadro della situazione per la maggior parte degli algoritmi crittografici oggi utilizzati.

L'impatto dei computer quantici sui più comuni algoritmi crittografici

algoritmo crittografico	tipo	finalità	livello di impatto nell'uso di potenti computer quantici
AES - advanced encryption standard	Chiave simmetrica	Crittografia	Servono chiavi di maggiori dimensioni
SHA-2, SHA-3 (secure Hash Algorithm)	-------	Funzioni hash	Servono un punto di maggiori dimensioni
RSA-Rivest Shamir Aldeman	Chiave pubblica	Firme elettroniche, costruzione di chiavi di cifratura	L'algoritmo non è più sicuro
ECDSA, ECDH (crittografia a curva ellittica)	Chiave pubblica	Firme elettroniche, scambio di chiavi	L'algoritmo non è più sicuro
DSA (crittografia a campo finito)	Chiave pubblica	Firme elettroniche, scambio di chiavi	L'algoritmo non è più sicuro

Davanti a questi risultati, non deve stupire il fatto che il mondo accademico abbia già avviato gli studi in una nuova scienza, chiamata criptografia post quantum. È un'area di ricerca assai attiva, che è cominciata nel 2006 e che sta ricevendo un significativo supporto da agenzie nazionali, di vari paesi, interessate alla sicurezza dei sistemi informativi e delle reti di comunicazione. L'Europa ha già sviluppato due progetti specifici su questo argomento, insieme al Giappone.

Gli accademici si impegnano per avanzamenti significativi nella ricerca di base, tanto è vero che lo stesso NIST si è deciso finalmente a lanciare un bando di gara per sollecitare, valutare e standardizzare degli algoritmi crittografici a chiave pubblica, resistenti ad attacchi quantici.

L'obiettivo di questo bando di gara è quello di sviluppare delle normative criptografiche a chiave pubblica, di tipo pubblico e non classificato, da poter utilizzare per firme digitali, criptografia a chiave pubblica e algoritmi per la costruzione e lo scambio di chiavi. Questi algoritmi devono essere disponibili in tutto il mondo e devono essere in grado di proteggere informazioni governative sensibili nel prossimo futuro, anche dopo che i computer quantici saranno di uso se non proprio corrente, almeno allargato.

Come primo passo in questo processo, NIST ha sollecitato dei commenti pubblici sulla bozza di bando di gara, soprattutto facendo riferimento ai criteri di valutazione per gli algoritmi che verranno presentati dai concorrenti.

È stata stabilita la data finale del 30 novembre 2017 per sottoporre degli algoritmi candidati alla valutazione della commissione di gara.

Non mancheremo di tenere aggiornati i lettori sull'evoluzione di questo affascinante settore, tenendo presente che le prime informazioni potranno aversi nella conferenza sulla standardizzazione degli algoritmi post quantum computer, prevista per la metà di aprile del 2018.

Adalberto Biasiotti

Report on Post-Quantum Cryptography (pdf)

---

www.puntosicuro.it