ARTICOLO DI PUNTOSICURO

Anno 22 - numero 4811 di Venerdì 06 novembre 2020

E' quasi pronta una nuova famiglia di algoritmi crittografici

La sicurezza degli algoritmi crittografici deve costantemente rincorrere la crescente potenza di calcolo dei moderni computer. L'arrivo dei computer quantistici ha obbligato gli esperti a compiere un gigantesco salto di qualità.

Il NIST, National Institute for standards and technology ha lanciato qualche tempo fa un bando di gara per la messa punto di algoritmi criptografici di altissimo livello, in grado di resistere anche agli attacchi portati con i potentissimi computer quantici.

Vale forse la pena di offrire ai lettori una breve panoramica di come si sono evoluti di algoritmi crittografici ed i metodi di attacco.

Il primo algoritmo criptografico, messo pubblicamente a disposizione degli utenti, nacque nel 1970 e venne chiamato DES digital encryption standard. Questo algoritmo crittografico utilizzò una chiave a 56 bit, ritenuta da molti non molto robusta, ma venne ufficialmente approvato nel 1976 e fu lo standard di riferimento per tutti coloro che avevano bisogno di un efficiente ed efficace algoritmo criptografico.

La crescente potenza di calcolo dei computer permise però di migliorare le tecniche di attacco, tant'è vero che nel 1999 venne pubblicamente dimostrata una tecnica di violazione di questo algoritmo, utilizzando un potente computer nell'arco di 22 ore.

Ci si rese conto quindi che questo algoritmo aveva compiuto il suo periodo di vita utile e il NIST si attivò per sviluppare un nuovo algoritmo, che venne pubblicamente approvato nel 2001: siamo davanti allo Advanced Encryption Standard, AES, con chiave a 128 bit. Ai tempi, si ritenne che questo algoritmo per qualche tempo avrebbe potuto essere considerato di difficilissima violazione.

Purtroppo, l'algoritmo rimase immutato, mentre i computer effettuavano un salto di qualità gigantesco, con l'arrivo sul mercato dei computer a tecnica quantistica. Il NIST si rese allora conto che doveva avviare un processo di individuazione ed approvazione di un nuovo algoritmo, in grado di resistere alle potentissime capacità di decifrazione, tipiche dei computer quantistici.

Il bando di gara è stato mirato alla individuazione di algoritmi per criptografie post quantum (PQE). Adesso il NIST sta valutando le offerte pervenute da varie parti, soprattutto dall'Europa. Ad oggi, sembra vi siano sette aziende, che vanno da laboratori privati ad università di ricerca, che hanno presentato delle soluzioni meritevoli di approfondimento.

Questi algoritmi sono stati sviluppati dai più esperti crittografi del mondo, provenienti da Zurigo, dal Giappone, dall'Inghilterra e da molti altri paesi, che si sono resi conto come la disponibilità di un algoritmo a prova di attacchi quantistici rappresenti una necessità indispensabile nel mondo della sicurezza informatica.

Oltre ad un primo gruppo di sette candidati, il NIST ha selezionato altri otto algoritmi, che potrebbero essere presi in esame se l'analisi approfondita dei primi sette non porterà a risultati soddisfacenti.

La fase di analisi da parte del NIST durerà almeno 12 mesi e si prevede che possa essere presentato uno standard è di tipo PQE ad una conferenza, pianificata per la seconda metà del 2021.

Per i lettori che vogliono saperne di più su questo bando di gara, che è di una incredibile raffinatezza e che comporta requisiti oltremodo stringenti, è possibile accedere al bando di gara al sito www.nist.gov/pqcrypto.

Adalberto Biasiotti