

I NUMERI CASUALI E LA CRITTOGRAFIA

Gruppo ERATOSTENE

Introduzione

I numeri casuali, com'è noto, sono utilizzati in crittografia, ma finora è difficile trovare algoritmi veramente efficaci per trovarli. Ma ora questo problema sembra avviato a soluzione

Qui, dopo la definizione di Wikipedia, riportiamo l'articolo "Numeri casuali per davvero", di Michele Catanzaro, dalla rivista "LE SCIENZE" di giugno 2010.

Definizione di "numero casuale da Wikipedia"

In [statistica](#), un numero casuale è una singola osservazione (risultato)

di una specifica [variabile casuale](#). Dove non viene specificata alcuna

distribuzione, si intende usualmente la [distribuzione continua uniforme](#) nell'intervallo [0,1]. In un senso informale, c'è una certa circolarità in questa definizione poiché l'idea stessa di variabile casuale si basa sul concetto di [casualità](#).

Un [numero](#) di per sé stesso non può essere casuale, eccetto nel senso del modo in cui è stato generato. Informalmente, generare un numero

casuale significa che prima di essere generato, tutti gli [elementi](#) di un

certo [insieme](#) siano egualmente [probabili](#) come risultato. In particolare, questo significa che la conoscenza dei numeri generati da questo processo, o da un qualunque altro processo, non porta informazioni aggiuntive al riguardo del prossimo numero generato. Questo è equivalente alla [indipendenza statistica](#).

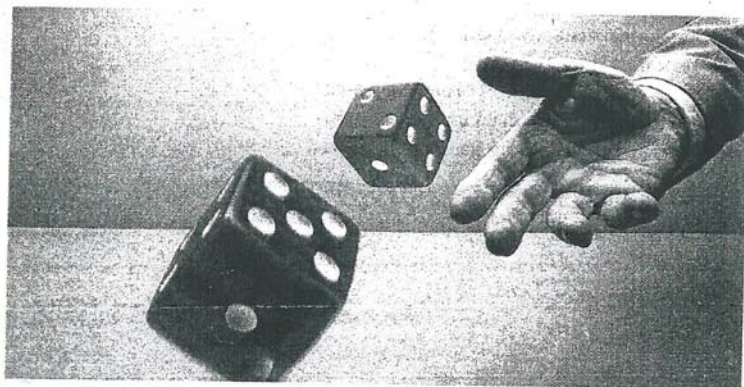
Dalla rivista "Le Scienze" giugno 2010, l'articolo accennato all'inizio:

■ FISICA QUANTISTICA

Numeri casuali per davvero

Sviluppato un metodo per ottenere un'estrazione di cifre veramente casuale

È stato finalmente creato il «dado perfetto». Un articolo pubblicato su «Nature» ha reso noto un sistema per generare una serie di numeri veramente casuali. Con i sistemi attuali, infatti, è impossibile generare una sequenza di cifre con la piena sicurezza che siano davvero casuali. Come in un dado truccato, c'è sempre la possibilità di prevedere



RISULTATO IMPREVEDIBILE.

Se i dadi non sono truccati il risultato del lancio non è prevedibile, contrariamente a quanto avviene con l'estrazione di numeri da algoritmi.

Ora però un gruppo internazionale di ricerca ha risolto questo problema.

i risultati. Ed è un problema per la crittografia, che ha bisogno di serie imprevedibili al 100 per cento per codificare messaggi impossibili da decifrare.

Grazie a un sistema di ottica quantistica, un gruppo internazionale di fisici ha sviluppato un metodo che non ha questi difetti. Per ora, però, è riuscito a generare solo 42 numeri in un mese.

Un compito apparentemente semplice come produrre una sequenza di numeri casuali è in realtà un

grattacapo per gli scienziati. Attualmente si usano i cosiddetti «pseudo-generatori», cioè algoritmi che producono sequenze dall'aspetto casuale, che sono utilizzate, per esempio, per cifrare le transazioni su Internet. Se però un malintenzionato riesce a identificare l'algoritmo di partenza, ha tutto il necessario per decodificare il messaggio. In termini scientifici, il problema consiste nel fatto che è impossibile essere sicuri al 100 per cento che una serie di numeri è del tutto casuale. In natura, gli unici fenomeni veramente non deterministici sono quelli che avvengono nel mondo microscopico.

Secondo la meccanica quantistica, è impossibile prevedere con certezza il comportamento di una particella. Quindi se si usa questo comportamento per ottenere dei numeri si può, in teoria, generare una sequenza del tutto imprevedibile. Gli autori dello studio hanno usato coppie di atomi distanti un metro, legati fra loro dall'*entanglement*, un fenomeno caratteristico del mondo quantistico. Dopo aver analizzato oltre 3000 coppie, sono riusciti a estrarre 42 cifre, scelte fra 0 e 1. Quindi hanno applicato un test che permette di garantire che la sequenza è davvero casuale.

Il metodo, sviluppato per la prima volta, si basa su una nota relazione della meccanica quantistica, la disuguaglianza di Bell. Questo sistema potrebbe essere usato per codificare messaggi in modo indecifrabile. Ma è necessario migliorarne l'efficienza per generare più numeri e più rapidamente.

Michele Catanzaro

Cortesia European Southern Observatory (foto F-ELT); John Smith/Cortis (dadi)

Conclusione

Si va quindi verso una crittografia quantistica più completa ed efficiente per quanto riguarda la comunicazione riservata di informazioni.

Altri passi si fanno ogni tanto anche verso la realizzazione del computer quantistico, in grado di scomporre i numeri RSA (Rif.1 e 2), prodotti tra due numeri primi di qualche centinaio (o a volte anche un migliaio) di cifre ciascuno, alla base dell'omonimo sistema crittografico.

Il sistema crittografico ECC si basa invece sulle curve ellittiche, ma ha

chiavi più corte e più adatte a telefonini, palmari, ecc.

Si va quindi verso una crittografia quantistica più completa ed efficiente per quanto riguarda la comunicazione riservata di informazioni.

Altri passi si fanno ogni tanto anche verso la realizzazione del computer quantistico, in grado di scomporre i numeri RSA (Rif.1 e 2), prodotti tra due numeri primi di qualche centinaio (o a volte anche un migliaio) di cifre ciascuno, alla base dell'omonimo sistema crittografico. Il sistema crittografico ECC si basa invece sulle curve ellittiche, ma ha chiavi più corte e più adatte a telefonini, palmari, ecc.

Riferimenti

- 1) “ Crittografia RSA”“Articoli su Problemi del Millennio” sul nostro sito
- 2) “Articoli sulla fattorizzazione”, idem

Caltanissetta, 1.7.2010