

IL FUTURO DELLA CRITTOANALISI

CRITTOGRAFI 

**protezione dei
segreti**

CRITTOANALISTI 

**disvelamento
dei segreti**

IL FUTURO DELLA CRITTOANALISI

ATTUALE SITUAZIONE

CRITTOGRAFIA A CHIAVE PUBBLICA

**DIBATTITO INTORNO ALL'USO DELLE
CIFRATURE FORTI**

IL FUTURO DELLA CRITTOANALISI

DIBATTITO INTORNO ALL'USO DELLE CIFRATURE FORTI

Esistono due campi contrapposti:

i difensori delle libertà civili e mondo degli affari sono favorevoli alle cifrature forti, mentre i tutori dell'ordine sostengono la necessità di significative limitazioni

IL FUTURO DELLA CRITTOANALISI

DIBATTITO INTORNO ALL'USO DELLE CIFRATURE FORTI

L'opinione pubblica sembra propendere per lo schieramento favorevole alle cifrature forti, che gode della simpatia dei media e ha avuto l'appoggio di un paio di importanti pellicole hollywoodiane

Codice Mercury

Nemico Pubblico

IL FUTURO DELLA CRITTOANALISI

**DIBATTITO INTORNO ALL'USO DELLE
CIFRATURE FORTI**

Compromesso

Key escrow

(deposito della chiave)

IL FUTURO DELLA CRITTOANALISI

Phil Zimmermann

La moderna crittografia consente di effettuare cifrature molto ma molto al di là della portata di tutte le forme di decifratura oggi conosciute

IL FUTURO DELLA CRITTOANALISI

William Crowell

(vicedirettore della NSA)

Se tutti i computer del mondo fossero impiegati simultaneamente per la decifrazione di un solo crittogramma PGP, si stima che per venirne a capo impiegherebbero un tempo pari a circa 12 milioni di volte l'età dell'universo

IL FUTURO DELLA CRITTOANALISI

Tuttavia ...

L'esperienza passata ci dice che tutte le scritture segrete ritenute inviolabili prima o poi hanno ceduto alla decifrazione

Dietro il velo del segreto di Stato possono già nascondersi importanti progressi dei metodi di decifrazione

IL FUTURO DELLA CRITTOANALISI

Solo una parte delle informazioni che transitano nel mondo sono cifrate in modo sicuro; il resto è debolmente crittato o non crittato

Ciò dipende tra l'altro dalla circostanza che gli utenti di Internet sono sempre più numerosi e pochi di loro prendono precauzioni adeguate in fatto di privacy

IL FUTURO DELLA CRITTOANALISI

**Tecniche per l'accesso a
informazioni riservate**

Analisi del traffico

**Perfino quando il contenuto di un
messaggio è inaccessibile, può essere
importante sapere chi lo invia e chi lo
riceve**

IL FUTURO DELLA CRITTOANALISI

**Tecniche per l'accesso a
informazioni riservate**

Tempest attack

(approccio tempesta elettromagnetica)

**Implica il rilevamento dei segnali
elettromagnetici che accompagnano la
pressione di ogni pulsante di una tastiera
di computer e che permettono di
identificarla**

IL FUTURO DELLA CRITTOANALISI

Tempest attack

(approccio tempesta elettromagnetica)

Per difendersi dall'approccio "tempesta elettromagnetica" sono nate società che forniscono materiali capaci di assorbire i segnali elettromagnetici, applicabili alle pareti di una stanza

In America, per acquistare e installare schermature di questo tipo occorre l'autorizzazione dello Stato; ciò suggerisce che forze di polizia come FBI ricorrano spesso a questa forma di sorveglianza

IL FUTURO DELLA CRITTOANALISI

**Tecniche per l'accesso a
informazioni riservate**

Cavalli di troia

- 1. Eva potrebbe progettare un virus informatico capace di penetrare silenziosamente nel personal computer di Alice e infettare programmi come PGP**

Non appena Alice usasse la sua chiave privata per decifrare il messaggio, il virus la memorizzerebbe; poi, al primo collegamento di Alice con Internet, il virus approfitterebbe della rete per inviare la chiave a Eva

IL FUTURO DELLA CRITTOANALISI

**Tecniche per l'accesso a
informazioni riservate**

Cavalli di troia

- 2. Alice potrebbe credere di aver scaricato da Internet una copia autentica del PGP e aver invece installato sul suo computer una versione "troiana" del programma che potrebbe contenere istruzioni extra per l'invio surrettizio a Eva di copie non crittate di messaggi di Alice**

IL FUTURO DELLA CRITTOANALISI

Tecniche per l'accesso a
informazioni riservate

Backdoor

Una variazione sul tema del cavallo di Troia è rappresentata da un programma crittografico originale, affidabile in condizioni normali ma munito di backdoor (porta di servizio): un gruppo di istruzioni che permettono ai creatori del programma, o a chi conosce l'esistenza e le proprietà della porta, di accedere ai messaggi in chiaro degli utenti

IL FUTURO DELLA CRITTOANALISI

Tempest attack

Cavalli di troia

Backdoor

... ma la vera sfida dei crittoanalisti è trovare il punto debole della cifratura RSA, cardine della crittografia contemporanea

... occorrono grandi passi in avanti sia **teorici** che **tecnologici**

IL FUTURO DELLA CRITTOANALISI

Approccio teorico

L'unico passo avanti teorico che sia dato immaginare è un nuovo procedimento matematico per la scoperta della chiave pubblica di Alice

Essa consiste nei numeri primo p e q e la possibilità di calcolarli è legata alla scomposizione in fattori primi di N , la chiave pubblica di Alice

IL FUTURO DELLA CRITTOANALISI

Approccio teorico

I sistemi adoperati a questo scopo comportano l'esame di un numero primo per volta, per controllare se divide N senza resto; ma questo approccio è troppo lento

I decrittatori hanno quindi cercato una scorciatoia della scomposizione in fattori primi – un metodo che riduca drasticamente i passi necessari all'individuazione di p e q

Finora, però, nessun tentativo in questa direzione ha avuto buon esito

IL FUTURO DELLA CRITTOANALISI

Approccio tecnico

Se ridurre i passi necessari alla scomposizione in fattori primi sembra difficile o impossibile, la decrittazione ha bisogno di una tecnologia che li esegua più rapidamente

I circuiti integrati di silicio diventano più potenti anno dopo anno, raddoppiano la propria velocità di elaborazione all'incirca ogni diciotto mesi, ma un simile ritmo non può avere conseguenze rilevanti per la scomposizione di numeri grandi come le chiavi pubbliche RSA; per rendere obsoleta questa cifratura, occorrerebbero circuiti integrati miliardi di volte più veloci di quelli attuali

IL FUTURO DELLA CRITTOANALISI

Approccio tecnico

Gli esperti di decifrazione hanno riposto le loro speranze in un tipo di calcolatore radicalmente diverso da quelli attuali: il computer quantistico

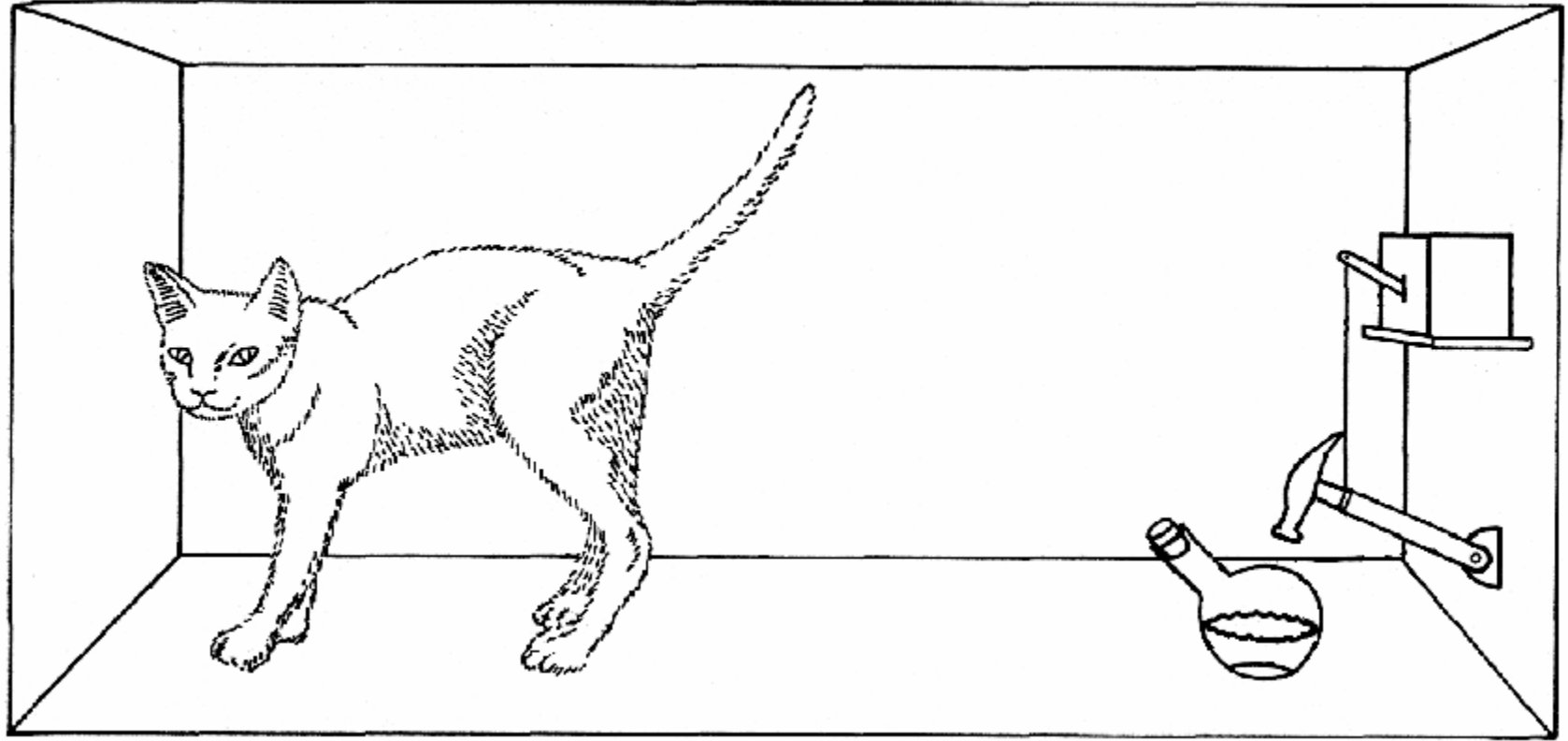
IL FUTURO DELLA CRITTOANALISI

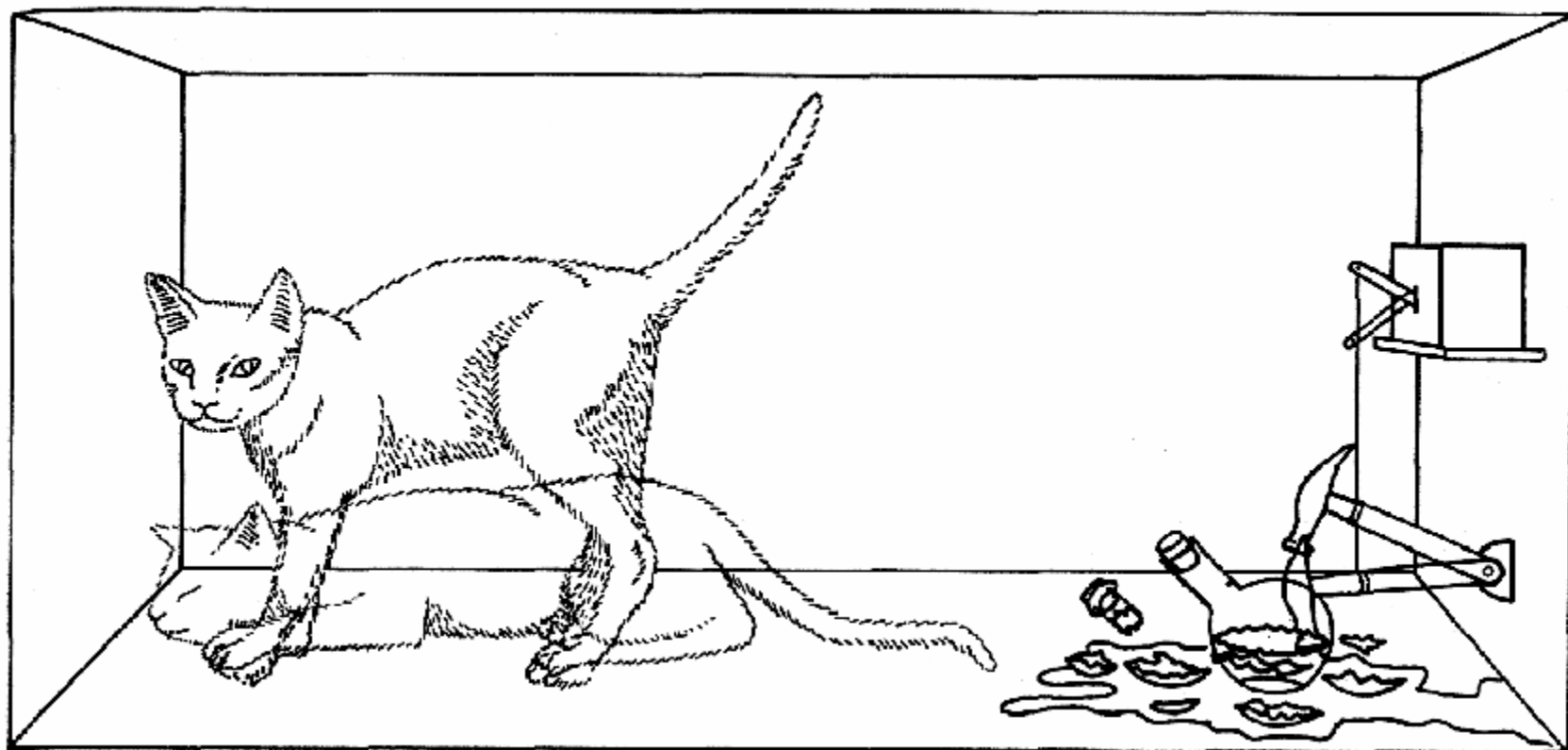
La meccanica quantistica lascia disorientati

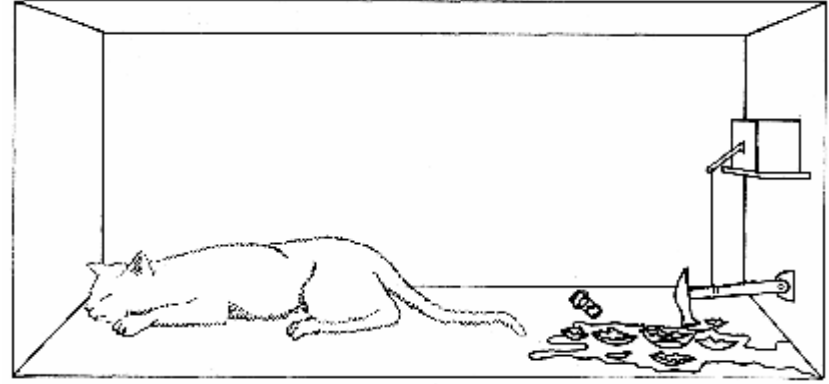
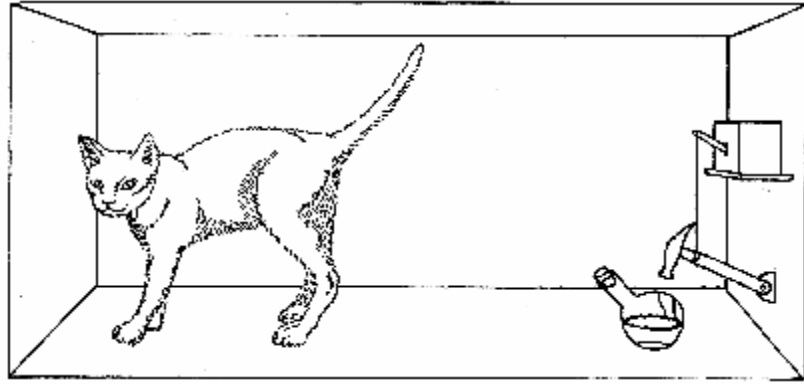
Ma essa si è dimostrata una delle teorie scientifiche più corrette e potenti che l'uomo abbia concepito

Essa spiega un numero impressionante di fenomeni naturali

Per esempio, solo la meccanica quantistica ha permesso ai fisici di calcolare le conseguenze delle reazioni nucleari che hanno luogo nel nocciolo di reattori atomici, ai chimici di dar conto dei minimi dettagli della struttura del DNA, agli astrofisici di capire come avviene la combustione del sole, agli ingegneri di progettare i laser per la lettura dei CD degli impianti stereofonici







L'amico di Wigner

