La percezione dell’equazione (A+x)(B+y)

teoria, apparenza e realtà computazionale

Obiettivo del documento:

Questo documento intende analizzare la percezione, spesso fuorviante, che si ha dell’equazione di tipo ***S=(A+x)(B+y)*** *quando viene discussa nel contesto della fattorizzazione dei semiprimi, soprattutto in ambito teorico matematico. Esamineremo alcune trasformazioni classiche dell’espressione, mostreremo come queste possano dare l'illusione di una semplificazione risolutiva, e contrapporremo questa percezione alla realtà computazionale legata all’uso di numeri molto grandi.*

1. La forma strutturata del semiprimo

Nel metodo GC57, un semiprimo viene costruito esplicitamente come: *S=(A+x)(B+y)*
con A e B scelti tali che B>>A , e con $x, y \in \mathbb{N}$ *selezionati in un intervallo definito da una chiave modulare.*

Tuttavia, in contesto matematico classico, questa equazione è spesso considerata risolvibile (almeno in linea di principio), attraverso una serie di trasformazioni algebriche.

2. La trasformazione e la riduzione apparente

Una delle strategie teoriche più note è la seguente

$$S = (A + x)(B + y) = AB + Ay + Bx + xy$$

Sostituendo:

$$x = w - z, \quad y = w + z$$

si ottiene:

$$S = AB + (A + B)w + (A - B)z + w^2 - z^2$$

Successive sostituzioni del tipo:

$$w = r - \frac{A + B}{2}, \quad z = s + \frac{A - B}{2}$$

portano infine a una forma del tipo:

$$r^2 - s^2 = \text{costante}$$

da cui si deduce la somiglianza con un'equazione di tipo Fermat-Pell

3. Il limite computazionale di queste trasformazioni

Tutto ciò è formalmente corretto e utile per classificare il tipo di equazione, ma non implica affatto che la fattorizzazione di S sia semplice.

La conoscenza di B (come nella costruzione **GC57**, in cui B è nota a chi genera S) non aiuta chi deve fattorizzare S, perché il valore di x e y sono sconosciuti. Le variabili possono essere enormi (anche centinaia o migliaia di bit). La forma finale è ancora un'equazione diofantea di difficile risoluzione.

La realtà è che nella pratica anche se l'equazione può essere ridotta in una forma nota, non esiste un algoritmo generale veloce per risolverla con numeri molto grandi. Le variabili non sono facilmente isolabili, e il numero di possibilità cresce esponenzialmente

4. Conclusione: la divergenza tra percezione e realtà

La tentazione di ridurre a una forma gestibile è forte, e spesso viene presa come indicazione che il problema della fattorizzazione sia, in fondo, solo una questione di algebra.

Ma nella realtà della crittografia e della computazione, queste semplificazioni non forniscono strumenti concreti per l'attacco. La struttura modulare del metodo GC57 sfrutta proprio queste illusorie semplificazioni per creare una funzione che sembra semplice, ma è risolvibile solo in condizioni determinate.

In sintesi: la percezione teorica è una cosa, la computabilità reale è un'altra. Ed è proprio nella distanza tra queste due che nasce la forza del metodo GC57.

5. Confronto tra approccio teorico e metodo applicato, con numeri reali medio grandi GC57

5.1 – Approccio teorico mediante trasformazione algebrica

Poniamo:

A=9863856354654348763247615728926535252 31

B=34897623846029346576325673267873878638266525072967862519376246554 1

x=?

y=?

S=(A+x)(B+y)=

3442251487360036156816990009299878822771065764099613728476170602144210434906001704155802111657216335344 89

$$S = AB + Ay + Bx + xy$$

Un possibile tentativo di semplificazione è la sostituzione:

$$x = w - z, \quad y = w + z$$

che porta a:

$$S = AB + (A + B)w + (A - B)z + w^2 - z^2$$

Ulteriori sostituzioni del tipo:

$$w = r - \frac{A + B}{2}, \quad z = s + \frac{A - B}{2}$$

riconducono infine a un'equazione della forma:

$$r^2 - s^2 = \text{costante}$$

Formalmente corretta, questa trasformazione mira a ricondurre il problema a una forma diofantea nota. Tuttavia, la soluzione pratica dell'equazione per valori di molto grandi è computazionalmente inapplicabile, poiché:

1) Il numero di combinazioni possibili per le variabili r e s è enorme ;

2) La costante risultante è fuori scala;

3) Nessun algoritmo noto consente di risalire in tempo utile ai fattori originali.

5.2 – Risoluzione diretta con GC57

Prendiamo gli stessi parametri sopra e avremo:

S=(A+x)(B+y)=

344225148736003615681699000929987882277106576409961372847617060214421043490600170415580211165721633534489

C=B-1 = 34897623846029346576325673267873878638266525072967862519376246554 0

MCD(S,S mod C)= A+x = 98638563546546327590994474685275677374 7

x=(A+x)-A=2839958518317396010324851 6

$$(B+y)=\frac{S}{(A+x)}$$

y= (B+y)-B =3008390526160000247121700 46

La funzione agisce direttamente sull’aritmetica costruttiva del semiprimo e consente il recupero immediato di uno dei due fattori, senza ricorrere ad alcuna forma di trasformazione o ricerca.

Conclusione del confronto

Entrambi gli approcci partono dalla stessa equazione iniziale, ma mentre il primo tenta una semplificazione teorica priva di sbocco pratico su numeri grandi, il secondo imposta una costruzione deterministica che consente una estrazione diretta del fattore tramite una funzione modulare. Questo confronto rende evidente la divergenza tra forma risolta e risolubilità reale.