GC57 – L’estensione degli scomparti

Nel contesto del metodo di fattorizzazione GC57, basato sulla chiave B−1, si introduce un’estensione fondamentale: quella degli scomparti, ovvero contenitori logici costruiti sull’intervallo deterministico I.

Questo concetto è stato accennato nel documento *GC57: Metodo Alternativo per la Fattorizzazione Ultra-Rapida di Semiprimi con Applicazioni in Crittografia*, disponibile su: https://zenodo.org/records/15640331

In questo nuovo documento, il meccanismo degli scomparti viene analizzato nel dettaglio. Si mostrerà come la struttura del metodo GC57, già solida nella costruzione delle basi A e B, si estenda in modo deterministico anche a scomparti diversi da quello di origine.

Nel documento *GC57 – Dentro il meccanismo del metodo* (https://zenodo.org/records/15742011) è stato formalizzato il cuore del sistema attraverso la relazione:

$$\mathbf{MCD(S, S \bmod C) = A + x}$$

Qui tale formulazione verrà generalizzata nella forma:

$$\mathbf{MCD(S, S \bmod C + k \cdot C) = A + x}$$

per ogni scomparto k>0, dove la massima estensione è raggiunta quando si verifica la disuguaglianza $\mathbf{k \cdot C \neq k \cdot I}$

Questo punto rappresenta il limite operativo oltre il quale la proprietà GC57 non è più in grado di gestire correttamente la fattorizzazione, poiché i contenitori risultano sfasati.

Nei contenitori inferiori, in cui $k \cdot C = k \cdot I$, la fattorizzazione avviene invece senza alcuna necessità di ricerca, trattandosi di **contenitori equivalenti e allineati**.

Indice

1. Introduzione: Contesto generale del metodo GC57

Il metodo GC57 nasce come un approccio deterministico alla fattorizzazione di semiprimi della forma:

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

in cui:

- A e B sono interi positivi scelti con $B \gg A$
- x e y sono scarti positivi che appartengono a un intervallo definito,
- $C=B-1$ è la chiave modulare centrale del metodo.

Il punto di forza di GC57 risiede nel fatto che, per ogni semiprimo costruito secondo questo schema, è possibile recuperare il fattore A+x tramite una semplice operazione di massimo comune divisore:

$$MCD(S, S \bmod C)=A+x$$

Questa proprietà si basa sulla riduzione del semiprimo modulo C, che isola la parte contenente A+x in modo diretto. La logica modulare, combinata con la condizione di coprimalità

$$MCD(B+y,\ y+1)=1$$

rende l'estrazione del fattore immediata, anche per numeri di dimensione elevatissima.

📌 Riferimenti ai documenti precedenti

La struttura e le fondamenta teoriche del metodo GC57 sono state illustrate nei seguenti documenti:

- **GC57: Metodo Alternativo per la Fattorizzazione Ultra-Rapida di Semiprimi con Applicazioni in Crittografia**, disponibile su Zenodo: https://zenodo.org/records/15640331
- **GC57 – Dentro il meccanismo del metodo**, documento di approfondimento tecnico sulle proprietà modulari e sull'intervallo deterministico I, disponibile su: https://zenodo.org/records/15742011

Il presente documento si propone come estensione diretta del secondo, affrontando la generalizzazione della formula nei contenitori successivi allo scomparto base, attraverso la relazione:

$$MCD(S, S \bmod C+k \cdot C)$$

dove k rappresenta uno scomparto arbitrario in cui il semiprimo può essere stato generato.

2. Definizione degli scomparti

Nel contesto del metodo GC57, il termine **scomparto** (o contenitore) indica un segmento dell'intervallo numerico deterministico I, suddiviso in zone adiacenti. Ogni scomparto rappresenta un intervallo di valori in cui possono essere selezionati gli scarti x e y per costruire il semiprimo:

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

📌 Struttura dello scomparto

Dato l'intervallo deterministico:

$$I=2\cdot\left[\frac{C}{((A+1)\cdot(B+1))\,mod\,C}\right] \quad \text{con } C=B-1$$

uno scomparto generico di indice $k\in\mathbb{N}$ definito come scomparto $k=[k\cdot I,(k+1)\cdot I)$

Selezione dei valori x e y:

Invece di selezionare x e y nell'intervallo base [0,I), è possibile costruire il semiprimo scegliendoli all'interno di uno scomparto arbitrario:

$$\mathbf{x\in[k\cdot I,\ (k+1)\cdot I),\ y\in[k\cdot I,\ (k+1)\cdot I)}$$

per un valore di k sufficientemente grande.

Questa costruzione è significativa perché dimostra che:

- Il metodo GC57 **non è limitato al primo contenitore**;
- La proprietà modulare $MCD(S,S \bmod C)=A+x$ può essere estesa, come si vedrà nella sezione successiva.

3. Costruzione del semiprimo nello scomparto

Una delle caratteristiche distintive del metodo GC57 è la possibilità di generare il semiprimo **S=(A+x)(B+y)** partendo da uno **scomparto arbitrario**, non necessariamente **quello base (contenitore 0).**

In GC57, i valori x e y non sono scelti casualmente all'interno dell'intero spazio dei numeri naturali, ma sono **selezionati da uno specifico scomparto** di indice k, secondo la regola:

$$\mathbf{x\in[k\cdot I,\ (k+1)\cdot I),\ \ y\in[k\cdot I,\ (k+1)\cdot I)}$$

Nota: In questo contesto, il metodo GC57 opera su un livello modulare diverso, espresso dal contenitore I, cioè da 0 a I. L'indice k è tipicamente maggiore di 0 e può estendersi fino a un valore

massimo K max, compatibilmente con la capacità della proprietà MCD di recuperare il fattore primo corretto.

Dopo aver selezionato x e y in modo deterministico o pseudocasuale all'interno dello scomparto:

$$x = random\left(k \cdot I, (k+1) \cdot I\right), y = random\left(k \cdot I, (k+1) \cdot I\right)$$

si costruiscono i due fattori:

$$\mathbf{p = NextPrime(A+x), \quad q = NextPrime(B+y)}$$

In questo modo, il semiprimo generato risulta:

$$\mathbf{S = p \cdot q}$$

con entrambi i fattori scelti da una zona specifica del dominio definita dallo scomparto k.

📌 Importanza dello scomparto

La costruzione nei contenitori alti (cioè con $k \gg 0$) è fondamentale per validare il comportamento **scalabile** di GC57: il metodo continua a funzionare anche quando i fattori si trovano **a distanza enorme** dal punto di origine, a condizione che venga gestita correttamente la componente modulare nella fase di fattorizzazione.

4. Estensione della formula GC57

Nel teorema base, la proprietà fondamentale del metodo GC57 è:

$$\mathbf{MCD(S,\ S \bmod C) = A + x}$$

dove:

- $S = (A+x)(B+y)$
- $C = B - 1$
- $x \in [0, I)$

Questa relazione funziona perfettamente quando il valore x viene scelto all'interno del contenitore base (scomparto k=0). Ma la vera forza del metodo GC57 emerge quando questa proprietà si **estende** anche ai contenitori superiori, dove $x \in [k \cdot I, (k+1) \cdot I)$

In questi casi, la proprietà GC57 assume la forma estesa:

$$\mathbf{MCD(S,\ S \bmod C + k \cdot C) = A + x}$$

Questa relazione afferma che è possibile recuperare il fattore A+x **anche se esso si trova in uno scomparto diverso da quello base**, purché si compensi la parte mancante dell'intervallo con un termine $\mathbf{k \cdot C}$ aggiunto al modulo.

Il valore $\mathbf{k \cdot C}$ rappresenta l'**offset modulare** necessario per spostarsi nel dominio del modulo da uno scomparto all'altro. Infatti, poiché:

$$\mathbf{S \bmod C = (A+x)(y+1) \bmod C}$$

e poiché $\mathbf{x \in [k \cdot I, (k+1) \cdot I)}$, l'informazione contenuta in $\mathbf{S \bmod C}$ non è più sufficiente per isolare **A+x** direttamente. Aggiungendo $\mathbf{k \cdot C}$, si ristabilisce il giusto "contenitore di ricerca".

Risultato

Il metodo GC57 risulta quindi **funzionale anche a grandi distanze**, se la fattorizzazione è eseguita secondo la formula:

$$\mathbf{MCD(S, S \bmod C + k \cdot C) = A + x}$$

5. Condizione di validità dell'estensione

La formula estesa del metodo GC57:

$$MCD(S, S \bmod C + k \cdot C) = A + x$$

è valida solo **entro un certo limite**, che dipende direttamente dalla relazione tra lo scarto x e l'intervallo deterministico I.

Analisi del comportamento

Durante la costruzione del semiprimo: $x \in [k \cdot I, (k+1) \cdot I)$, ma la formula GC57 funziona solo se $k \cdot C$ mantiene l'allineamento con $k \cdot I$, e cioè $k \cdot C = k \cdot I$

se questa condizione è rispettata, il sistema riesce ancora a recuperare correttamente il valore A+x usando la formula estesa.

5. Limite operativo dell’estensione: inizio dello sfasamento

La formula estesa del metodo GC57:

$$\mathbf{MCD(S, S \bmod C + k \cdot C) = A + x}$$

rappresenta una scoperta significativa: la proprietà osservata nella formula base,

$$\mathbf{MCD(S, S \bmod C) = A + x}$$

estende naturalmente anche agli scomparti successivi a quello iniziale (contenitore 0), puntando al contenitore $k \cdot I$

Tuttavia, questa estensione presenta **un limite operativo** che si manifesta con l’insorgere di uno **sfasamento crescente**, il quale può compromettere la corretta fattorizzazione.

📉 Origine dello sfasamento

Nelle prove effettuate, ho osservato che l’intervallo prodotto da C **non è perfettamente proporzionale** all’intervallo I. Questo comporta uno **sfasamento** tra il contenitore $k \cdot C$ puntato dalla formula e il contenitore numerico reale $k \cdot I$ in cui si trovano i fattori.

Da un certo punto in avanti, questo sfasamento **non cresce più in modo lineare**, ma assume un comportamento **esponenziale**. La causa non è solo la precisione numerica, ma anche il modo in cui vengono esplorati i contenitori.

Infatti, per evitare di scandire tutti i numeri naturali in sequenza (1, 2, 3, …), il sistema applica direttamente **potenze** E^n (es. E^2, E^3 ...), che saltano interi blocchi di contenitori.

In questo scenario:

- Se un contenitore analizzato con indice k soddisfa la condizione $k \cdot C = k \cdot I$, allora **tutti i contenitori inferiori** a k sono necessariamente **allineati**.
- Se invece si verifica $k \cdot C \neq k \cdot I$, significa che è stato raggiunto il **limite operativo** dell’estensione: Quando questo avviene la fattorizzazione non è più garantita

6. Esempi numerici

In questa sezione verranno presentati esempi numerici concreti che mostrano il comportamento della proprietà GC57 estesa ai contenitori superiori.

Per ogni esempio verranno riportati:

- Il valore della chiave $C = B - 1$
- Il valore dell’intervallo deterministico I

- I valori selezionati di x e y nei contenitori di indice k
- Il risultato della formula MCD(S, $S \bmod C + k \cdot C$)
- La verifica che il risultato corrisponde effettivamente a A+x

Questi esempi dimostreranno sperimentalmente:

- il corretto funzionamento del metodo per $k \cdot C = k \cdot I$
- e la perdita di efficacia per $k \cdot C \neq k \cdot I$

Esempio 1

Chiave C = B - 1 = 48387791486053370476040093095151087430126111095621367578657510

Intervallo deterministico I = 130249422027793725102

Differenza in cifre tra p e q: 20

MCD(B+y, y+1) = 1

MCD(B+y, y+1 + k·I/(A+x)) = 1

Divisore trovato da GC57 : 37150100732019909529427493886397816897787 7

Test primo (p): True

Test primo (q): True

Contenitore individuato da GC57 (k·C) : 8589934592

Contenitore di ricerca x,y (k·I) : 8589934592

Valore X (offset su A): 11188340159185441261019343992 50

Valore Y (offset su B): 11188340158908370538659247791 60

Semiprimo analizzato (cifre: 104):

17976113279068580644715272686 6 ... 97769015064149402723886952746 7

Esempio 2

Chiave C = B - 1 = 48387791486053370476040093095151087430126111095621367578657510

Intervallo deterministico I = 130249422027793725102

Differenza in cifre tra p e q: 20

MCD(B+y, y+1) = 1

MCD(B+y, y+1 + k·I/(A+x)) = 1

Divisore trovato da GC57 : 37150100732131792931011041250199967496762 3

Test primo (p): True

Test primo (q): True

Contenitore individuato da GC57 (k·C) : 17179869185

Contenitore di ricerca x,y (k·I) : 17179869184

Valore X (offset su A): 22376680317540177641234403889 96

Valore Y (offset su B): 22376680318512156482783652595 28

Semiprimo analizzato (cifre: 104):

17976113279122718551781023319 8 ... 27102361356951247823612302829 7

Nota: In questi due esempi viene elaborato lo stesso numero dove il primo mostra che nel comparto 2^{33} i contenitori $k \cdot C$ e $k \cdot I$ sono ancora allineati, mentre nel secondo esempio con 2^{34} i contenitori $k \cdot C$ e $k \cdot I$ sono disallineati. *Il motivo del perché comunque viene risolta la fattorizzazione sta nel fatto che ho inserito un ciclo che sonda da -3 a +3 i contenitori adiacenti a quello impostato. Essendo questo disallineato di solo 1, viene intercettato comunque dal programma il quale svela subito il divisore del semiprimo. Questo è possibile nelle prime diseguaglianze, ma crescendo questa in modo esponenziale, basta poco per aumentare a dismisura la distanza*

Esempio 3

Chiave C = B - 1 =
113294128110630314714867356208750405325369921676815711248628863563698134063558505478490378171568291561425313502099927018566007488082265347129523226612512950243910781088821918866533923830

Intervallo deterministico I =
220966997475172242605112905881478790734362181241965363422931O

Differenza in cifre tra p e q: 61

MCD(B+y, y+1) = 1

MCD(B+y, y+1 + k·I/(A+x)) = 1

Divisore trovato da GC57 :
512719679432490793234412844100792768525703414123511300686044900932458896081037137581915163473731407258190838496955491338759 73

Test primo (p): True

Test primo (q): True

Contenitore individuato da GC57 (k·C): 202824096036516704239472512860 16

Contenitore di ricerca x,y (k·I) : 202824096036516704239472512860 16

Valore X (offset su A):
448174315168050790441598443901160561369420649639515838237287010019839547153025698906396980 90

Valore Y (offset su B):
448174315168050790441598443901155343791451031217428502313988556661718466474370636061597092 86

Semiprimo analizzato (cifre: 310):

580881290464659187836434627341 ... 325824624469675702297443397841

Nota: L’esempio 3 dimostra che basta aumentare anche di poco i numeri che già gli scomparti aumentano a 2^{104} prima di arrivare al disallineamento k·C e k·I

7. Conclusioni

L’estensione dei contenitori nel metodo GC57 conferma la straordinaria capacità del sistema di individuare i fattori di un semiprimo anche quando la costruzione avviene in scomparti superiori al dominio iniziale [0,I).

Abbiamo osservato che:

- Ogni contenitore è logicamente definito sull’intervallo I con un errore trascurabile ma che aumenta con il crescere degli scomparti
- La formula **$MCD(S, S \bmod C + k \cdot C)$** permette di estendere la ricerca ai contenitori successivi
- Il metodo mantiene la validità finché è soddisfatta la condizione $k \cdot C = k \cdot I$ che delimita il massimo valore di k gestibile da **$MCD(S, S \bmod C + k \cdot C) = A + x$** estrae il fattore A+x senza ambiguità e senza necessità di ricerca nei contenitori vicini.

Questa proprietà non solo amplia il campo di applicazione della formula originale GC57, ma dimostra anche che la relazione tra fattori e modulo C, con C=B-1, possiede una struttura modulare stratificata, di grande interesse teorico e applicativo.

Nota dell'autore

l presente lavoro è stato sviluppato in autonomia, con l’intento di condividere un’osservazione matematica emersa da un’indagine sperimentale sul comportamento dei semiprimi nel contesto della proprietà GC57.

Pur avendo prestato la massima attenzione nella redazione del testo e nella verifica delle formule, non si esclude la presenza di refusi, imperfezioni formali o imprecisioni minori.

Rimango pienamente disponibile a fornire chiarimenti, ricevere osservazioni e discutere eventuali suggerimenti che possano contribuire al miglioramento del contenuto, nella convinzione che il confronto aperto sia parte integrante della ricerca.

Eventuali segnalazioni possono essere inviate tramite i contatti riportati nel profilo Zenodo o per email a claugoru@yahoo.it

- **È obbligatoria la citazione dell’autore** (“Claudio Govi”) e della formula **GC57** in ogni forma di utilizzo, sia essa pubblica, privata, accademica, sperimentale o editoriale.
- **È vietato attribuire altro nome** o marchio alla formula o alle sue implementazioni: essa può essere menzionata solo come **“GC57”**.
- L’opera **non è soggetta a copyright restrittivo**: può essere condivisa, stampata o distribuita, **anche a pagamento**, purché vengano rispettate le condizioni sopra esposte.
- **Qualsiasi uso commerciale o accademico** deve comunque mantenere il riferimento integrale alla formula GC57 e al suo autore.