



Finanziato
dall'Unione europea
NextGenerationEU



Ministero
dell'Università
e della Ricerca



Italiadomani
PIANO NAZIONALE
DI RIPRESA E RESILIENZA



SERICS
SECURITY AND RIGHTS IN THE CYBERSPACE



CrypTO

CONFERENCE



Politecnico
di Torino



Telsy

A TIM
ENTERPRISE
BRAND



Enhancing the generation of parameters for BGV

Matilda Urani

In collaborazione con Beatrice Biasioli, Chiara Marcolla e Nadir Murru

23 Maggio 2025



La **crittografia omomorfa** consente di eseguire operazioni **direttamente su dati cifrati** senza la necessità di decifrarli precedentemente.

$$\text{Enc}_{pk}(m_1) \times \text{Enc}_{pk}(m_2) = \text{Enc}_{pk}(m_1 \times m_2)$$

$$\text{Enc}_{pk}(m_1) + \text{Enc}_{pk}(m_2) = \text{Enc}_{pk}(m_1 + m_2)$$

Definizione

Sia m un intero positivo. L' m -esimo polinomio ciclotomico è definito come

$$\Phi_m(x) = \prod_{\substack{1 \leq i < m \\ \gcd(i, m) = 1}} (x - \zeta^i)$$

dove ζ è una radice m -esima primitiva dell'unità.

Questo polinomio ha grado $\phi(m)$, dove ϕ denota la funzione di Eulero.

Definizione

Dati $d, m \in \mathbb{N}$, denotiamo con R_d l'anello

$$R_d = \frac{\mathbb{Z}_d[x]}{\Phi_m(x)}$$

Si fissano i seguenti parametri:

- $m \in \mathbb{N}$, che determina il **polinomio ciclotomico** $\Phi_m(x)$
- $t \in \mathbb{N}$, il **modulo del plaintext**
- $q \in \mathbb{N}$, il **modulo del ciphertext**

Si fissano i seguenti parametri:

- $m \in \mathbb{N}$, che determina il **polinomio ciclotomico** $\Phi_m(x)$
- $t \in \mathbb{N}$, il **modulo del plaintext**
- $q \in \mathbb{N}$, il **modulo del ciphertext**

BGV è composto da tre funzioni principali:

- **Key Generation**
- **Encryption**
- **Decryption**

Key Generation

La **chiave segreta** sk e la **chiave pubblica** pk sono generate come segue:

$$\begin{cases} sk = s \\ pk = (b, a) \equiv (-a \cdot s + te, a) \pmod{q} \end{cases}$$

dove $s \leftarrow \chi_s$, $a \leftarrow \mathcal{U}_q$ ed $e \leftarrow \chi_e$.

Solitamente

- $\chi_s = \mathcal{U}_3$
- $\chi_e = \mathcal{DG}_q(3.19^2)$
- $\mathcal{U}_q$ è la *distribuzione uniforme* su $\mathbb{Z}/q\mathbb{Z}$
- $\mathcal{DG}_q(\sigma^2)$ è la *distribuzione gaussiana discreta*, con media 0 e varianza σ^2

Encryption

Dato:

- un plaintext $m \in R_t$
- la chiave pubblica $pk = (b, a)$

La funzione di cifratura restituisce il ciphertext

$$c = (c_0, c_1) \equiv (b \cdot u + te_0 + m, a \cdot u + te_1) \mod q$$

dove:

- $u \leftarrow \chi_s$
- $e_0, e_1 \leftarrow \chi_e$

Decryption

Dato un ciphertext c e la rispettiva chiave segreta s , il plaintext viene recuperato effettuando i seguenti calcoli

$$m = \left[[c_0 + c_1 \cdot s]_q \right]_t$$

dove $[x]_q$ è la *rappresentazione centrata* di x modulo q .

La correttezza segue da

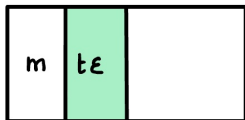
$$\begin{aligned} [c_0 + c_1 \cdot s]_q &= [(b \cdot u + te_0 + m) + (a \cdot u + te_1) \cdot s]_q \\ &= [(-a \cdot s + te) \cdot u + te_0 + m + (a \cdot u + te_1) \cdot s]_q \\ &= [m + t(e \cdot u + e_1 \cdot s + e_0)]_q \\ &= [m + t\epsilon]_q \end{aligned}$$

Questa quantità viene detta la **quantità critica** del ciphertext

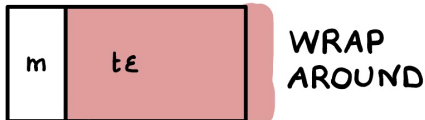
$$\nu = [c_0 + c_1 \cdot s]_q$$

Fallimenti della Decryption

Può la decryption fallire? Sì



↓ DEC
m ✓



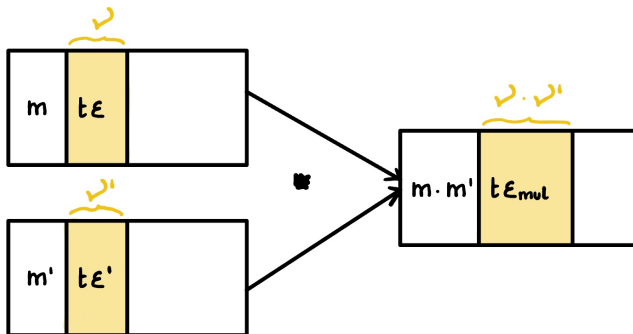
↓
random
quantity ✗

Per evitare che ciò accada, la seguente condizione deve essere soddisfatta:

$$\|\nu\|_{\infty} < \frac{q}{2}$$

Moltiplicazione Omomorfa

Ad ogni operazione omomorfa, il rumore aumenta, raggiungendo eventualmente un punto in cui **non è più possibile** recuperare il messaggio originale.



Obiettivo: Selezionare Correttamente q

Il modulo q deve essere:

- **sufficientemente grande**, per garantire la correttezza
- **il più piccolo possibile**, per migliorare l'efficienza

Per farlo, è fondamentale stimare con precisione la magnitudine della quantità critica, chiamata **rumore**, derivante dalle operazioni coinvolte nel circuito che vogliamo valutare.

Ad oggi, due approcci principali:

- Il **worst-case approach**, che consiste nello stimare il rumore tramite la sua norma.
- L'**average-case approach**, che consiste nel trattare i coefficienti della quantità critica come variabili aleatorie e studiarne la varianza.

L'approccio average-case è ritenuto più promettente, poiché offre stime che si avvicinano maggiormente ai dati sperimentali.

Tuttavia, il metodo attuale [2] tende a **sottostimare il rumore**, introducendo vulnerabilità nella sicurezza.

La Nostra Proposta

Abbiamo dimostrato che la causa di questa sottostima è l'**assunzione che i coefficienti del polinomio errore siano tra loro indipendenti**.

Seguendo un approccio simile a quello presentato in [1] per BFV, abbiamo sviluppato un metodo che tiene conto di queste dipendenze, le quali, in BGV, risultano particolarmente impattanti, rendendo l'**analisi più complessa**.

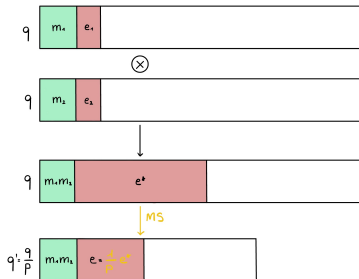
La Nostra Proposta

Abbiamo dimostrato che la causa di questa sottostima è l'**assunzione che i coefficienti del polinomio errore siano tra loro indipendenti**.

Seguendo un approccio simile a quello presentato in [1] per BFV, abbiamo sviluppato un metodo che tiene conto di queste dipendenze, le quali, in BGV, risultano particolarmente impattanti, rendendo l'**analisi più complessa**.

Abbiamo analizzato due diversi scenari:

- Circuiti **senza modulo switch**
- Circuiti **con modulo switch**



Il Nostro Scenario

Assumiamo di voler valutare un circuito di $L - 1$ moltiplicazioni utilizzando lo schema BGV.

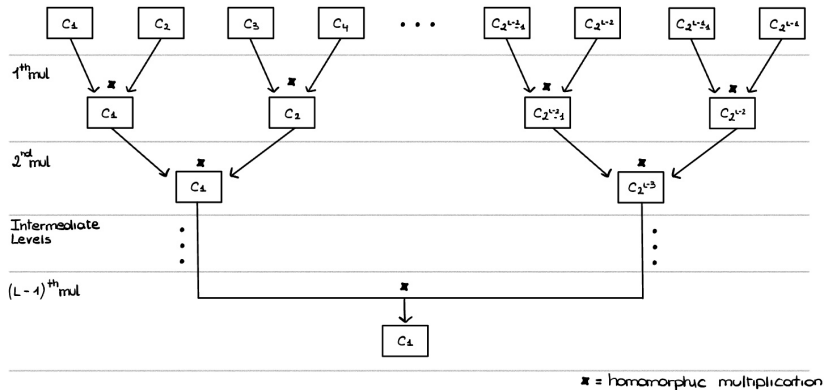


Figura: Circuito di riferimento

Obiettivo: Stimare la varianza V_ℓ dei coefficienti della quantità critica al termine di ogni livello ℓ .

Limiti dell'approccio attuale:

- L'approccio **average-case** [2] approssima V_ℓ come:

$$V_\ell \leq \phi(m) V_{\ell-1}^2$$

Questo porta a una sottostima della varianza sperimentale, introducendo potenziali **vulnerabilità**.

Contributo della nostra ricerca:

- Abbiamo dimostrato che:

$$V_\ell \leq \phi(m) h(\ell) V_{\ell-1}^2$$

dove la funzione $h(\ell)$ è costruita in modo da tener conto delle dipendenze tra i coefficienti dell'errore.

Ogni quantità critica ν può essere espressa come

$$\nu = \sum_{\iota} a_{\iota} s^{\iota} = \sum_{\iota} \sum_{\mu} b_{\mu}(\iota) e^{\mu} s^{\iota}$$

dove:

- e è il polinomio coinvolto nella generazione della chiave pubblica;
- s è la chiave segreta;
- $b_{\mu}(\iota)$ non contiene potenze di s ed e ;

Ogni quantità critica ν può essere espressa come

$$\nu = \sum_{\iota} a_{\iota} s^{\iota} = \sum_{\iota} \sum_{\mu} b_{\mu}(\iota) e^{\mu} s^{\iota}$$

dove:

- e è il polinomio coinvolto nella generazione della chiave pubblica;
- s è la chiave segreta;
- $b_{\mu}(\iota)$ non contiene potenze di s ed e ;

Lemma

Sia $\nu = \sum_{\iota} \sum_{\mu} b_{\mu}(\iota) e^{\mu}$ una quantità critica generica. Allora

- $\text{Cov}(b_{\mu_1}(\iota_1)|_{j_1}, b_{\mu_2}(\iota_2)|_{j_2}) = 0$ per $\mu_1 \neq \mu_2$ o $j_1 \neq j_2$, $\forall \iota_1, \iota_2$;*
- $\mathbb{E}[b_{\mu}(\iota)|_i] = 0$, $\forall \iota, \mu, i$;*

Il Nostro Teorema Principale

Teorema

Siano $\nu = \sum_{\ell} a_{\ell} s^{\ell}$, $\nu' = \sum_{\ell} a'_{\ell} s^{\ell}$ le quantità critiche di due ciphertext, definite rispetto allo stesso modulo q . Allora

$$\text{Var}((a_{\ell_1} s^{\ell_1} a'_{\ell_2} s^{\ell_2})|_i) \leq \phi(m) \text{Var}((a_{\ell_1} s^{\ell_1})|_i) \text{Var}((a'_{\ell_2} s^{\ell_2})|_i) F_s(\ell_1, \ell_2) F_e(K_1, K_2)$$

dove K_1, K_2 derivano dalle espansioni

$$a_{\ell_1} = \sum_{\mu_1=0}^{K_1} b_{\mu_1}(\ell_1) e^{\mu_1}, \quad a'_{\ell_2} = \sum_{\mu_2=0}^{K_2} b'_{\mu_2}(\ell_2) e^{\mu_2}$$

e rappresentano, rispettivamente, la più grande potenza di e che compare in a_{ℓ_1} , a'_{ℓ_2} .

Una definizione di F_s, F_e si può trovare in [1].

Confronto Tra Approcci

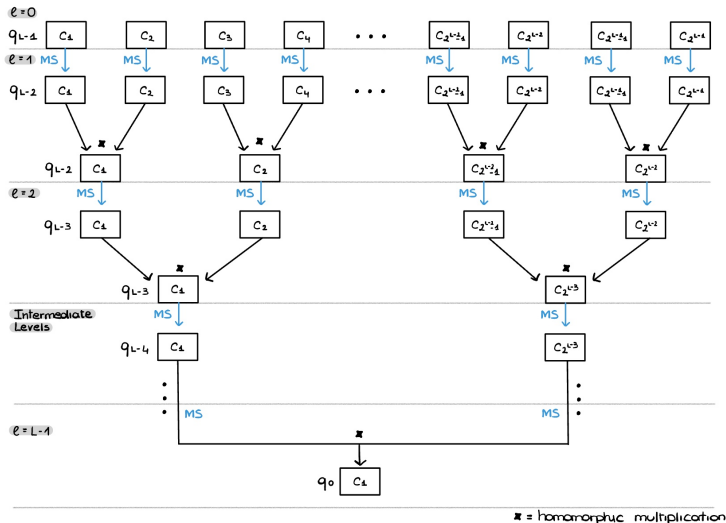
ℓ	0	1	2	3	4	5
[2]	19.9	52.9	118.7	250.5	513.9	1040.8
<i>exp</i>	19.9	53.5	121.6	260.2	541.3	1101.4
<i>our</i>	19.9	53.6	121.9	261.1	546.5	1131.1

Tabella: Confronto delle varianze per circuiti senza modulo switch

Nella tabella sono riportati i valori di $\log_2(V_\ell)$ per un circuito con sei livelli. Nello specifico:

- [2] rappresenta le stime fornite dall'approccio **average-case** attuale
- *exp* rappresenta i **valori sperimentali** ottenuti da 1000 campioni
- *our* fa riferimento ai risultati ottenuti utilizzando il **nostro bound**

Circuiti con Modulo Switch



Stima delle Varianze e Selezione dei Moduli

ℓ	0	1	2	3	4	5
[2]	19.9	38.8	37.0	37.0	37.0	37.0
<i>exp</i>	19.9	39.5	38.0	38.0	38.0	38.0
<i>our</i>	19.9	39.6	38.1	38.1	38.1	40.7

Tabella: Confronto delle varianze per circuiti con modulo switch

ℓ	0	1	2	3	4	5
[2]	23.6	37.1	50.6	64.1	77.6	81.7
<i>can</i>	58.2	87.8	117.3	146.9	176.5	184.4
<i>our</i>	35.4	53.8	72.2	90.6	109.1	113.2

Tabella: Confronto di $\log_2(q_\ell)$

I Nostri Risultati:

- **Dimostrazione dell'importanza di considerare le dipendenze** tra i coefficienti delle quantità critiche.
- **Sviluppo di un nuovo metodo per stimare le varianze**, sia per circuiti *senza* che *con* modulo switch.
- **Costruzione di un metodo per selezionare correttamente i moduli del ciphertext**.

La nostra soluzione garantisce che **il rumore non sia mai sottostimato**, fornendo stime molto vicine ai dati sperimentali e migliorando significativamente l'efficienza del sistema.

Grazie per l'attenzione!

- [1] Beatrice Biasioli, Chiara Marcolla, Marco Calderini e Johannes Mono. *Improving and Automating BFV Parameters Selection: An Average-Case Approach*. Cryptology ePrint Archive, Paper 2023/600. 2023. URL: <https://eprint.iacr.org/2023/600>.
- [2] Sean Murphy e Rachel Player. *A Central Limit Framework for Ring-LWE Noise Analysis*. Cryptology ePrint Archive, Paper 2019/452. 2019. URL: <https://eprint.iacr.org/2019/452>.