

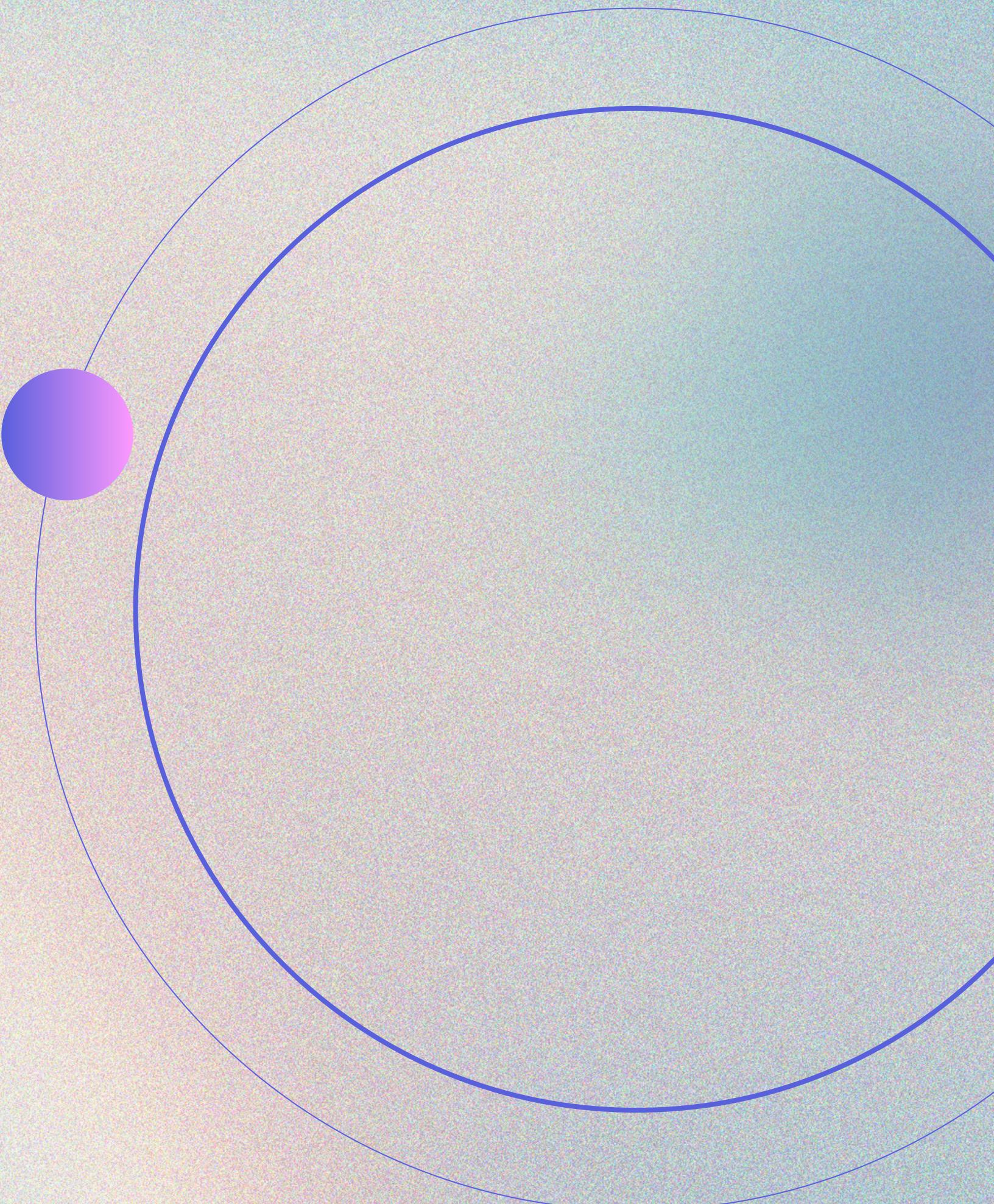
VULNERABILITY ASSESSMENT SU LIBRERIA PYTHON CHE IMPLEMENTA SECURE MULTI-PARTY COMPUTATION

Di Giada Rossana Margarone

A.A. 2023/2024
Relatore: Prof. Giampaolo Bella

OBIETTIVO

Analizzare una libreria Python, MPyC, la quale implementa Secure Multi-Party Computation, per verificarne la robustezza ad attacchi malevoli.





COS'È SMPC?

È un protocollo crittografico, così definito:

- Le parti coinvolte posseggono un'input privato;
 - L'obiettivo è calcolare una funzione $f(x_1, x_2, \dots, x_n) = y$;
 - Le parti ottengono y senza conoscere gli input.
- 

PROPRIETÀ DI SMPC

Privacy

Correctness

**Indipendence
of
inputs**

**Guaranteed
output
delivery**

Fairness

TECNICHE

CRITTOGRAFIA OMOMORFICA

Permette di eseguire operazioni direttamente sui dati cifrati, senza bisogno di decifratura.

CIRCUITI GARBLED

Rappresentazione crittografica di un circuito logico, in cui gli input e gli output sono codificati.



TECNICHE

SECRET SHARING

Divide un segreto in n parti in modo tale che solo un insieme di almeno t parti consenta di ricostruire il segreto.

OBLIVIOUS TRANSFER

Trasmissione sicura di più messaggi da parte di un mittente, il quale non sarà a conoscenza di quale dei tanti il ricevente ha ricevuto.

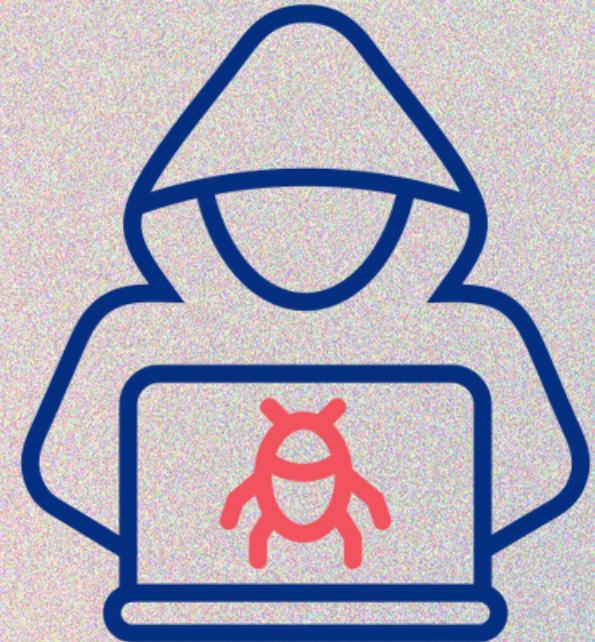


TIPI DI AVVERSARI

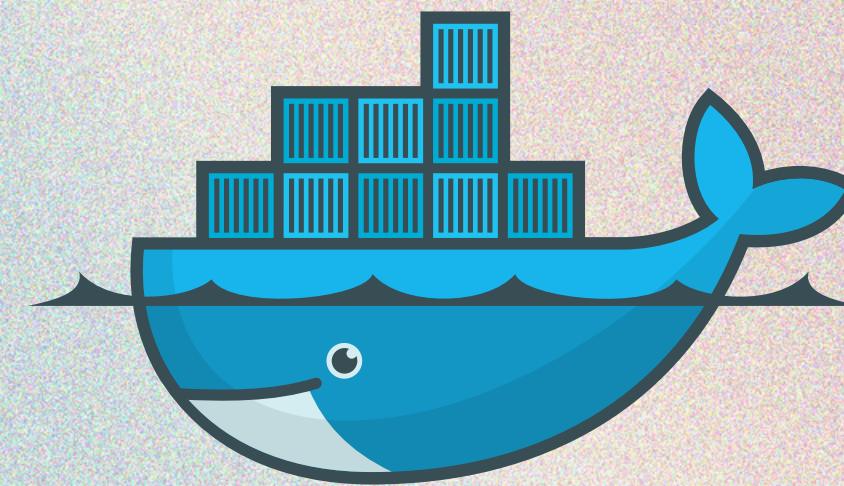
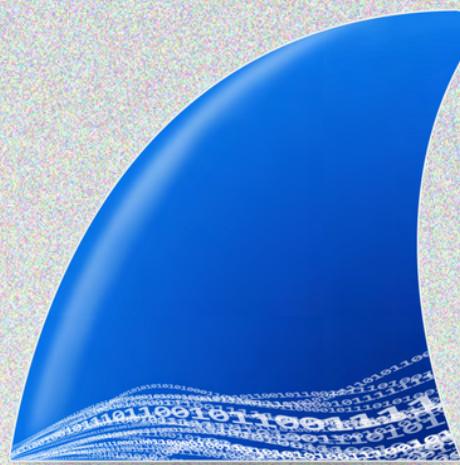
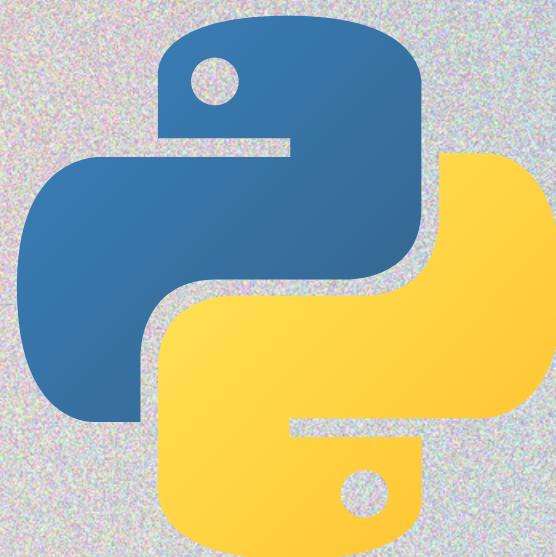
CURIOSO



MALEVOLO

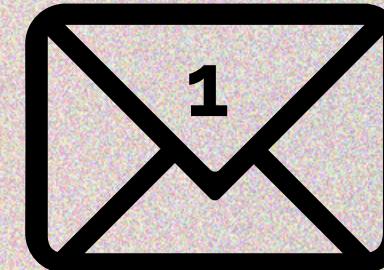
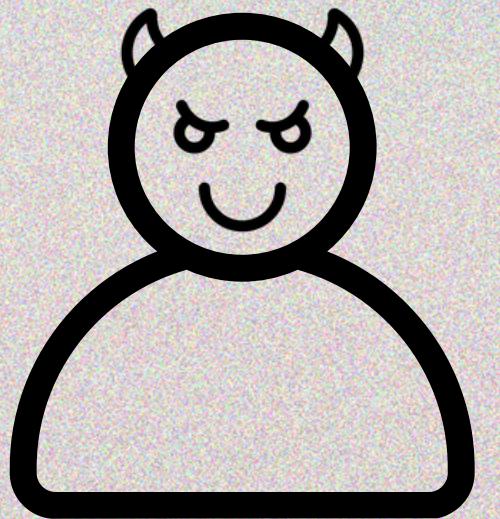
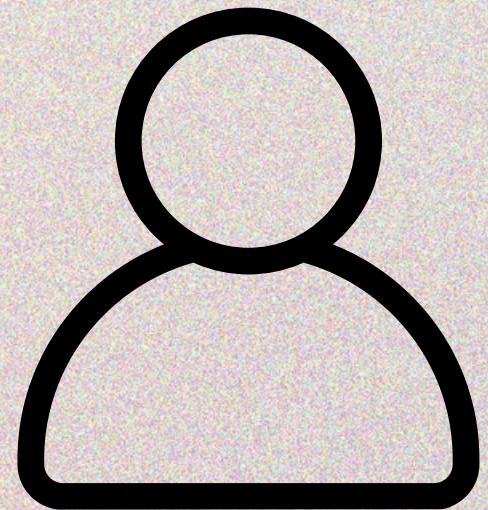


STRUMENTI UTILIZZATI

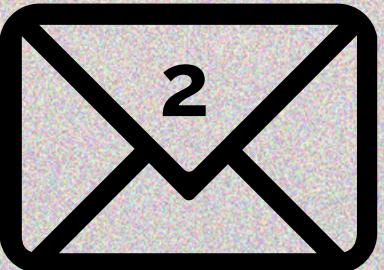
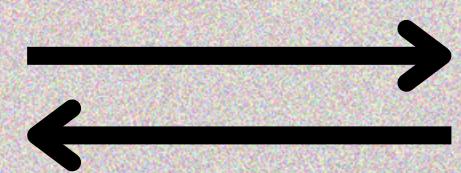


ATTACCO 1: INPUT RIVELATI

L'attaccante è "solo" curioso e si attiene al protocollo, ma ottiene più informazioni di quante previste.



MAX : 2

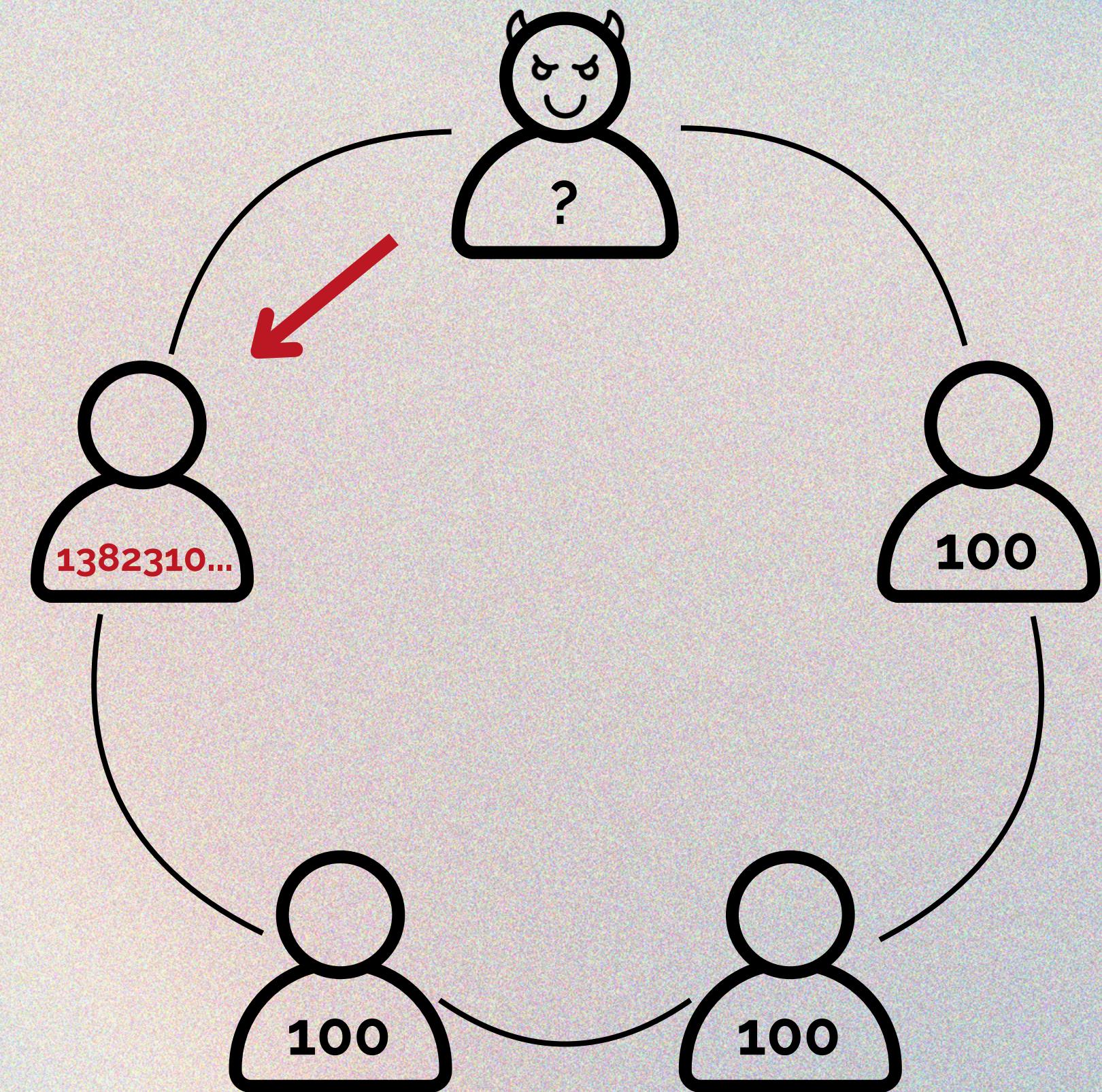


MAX : 2

INPUT: [1,2]

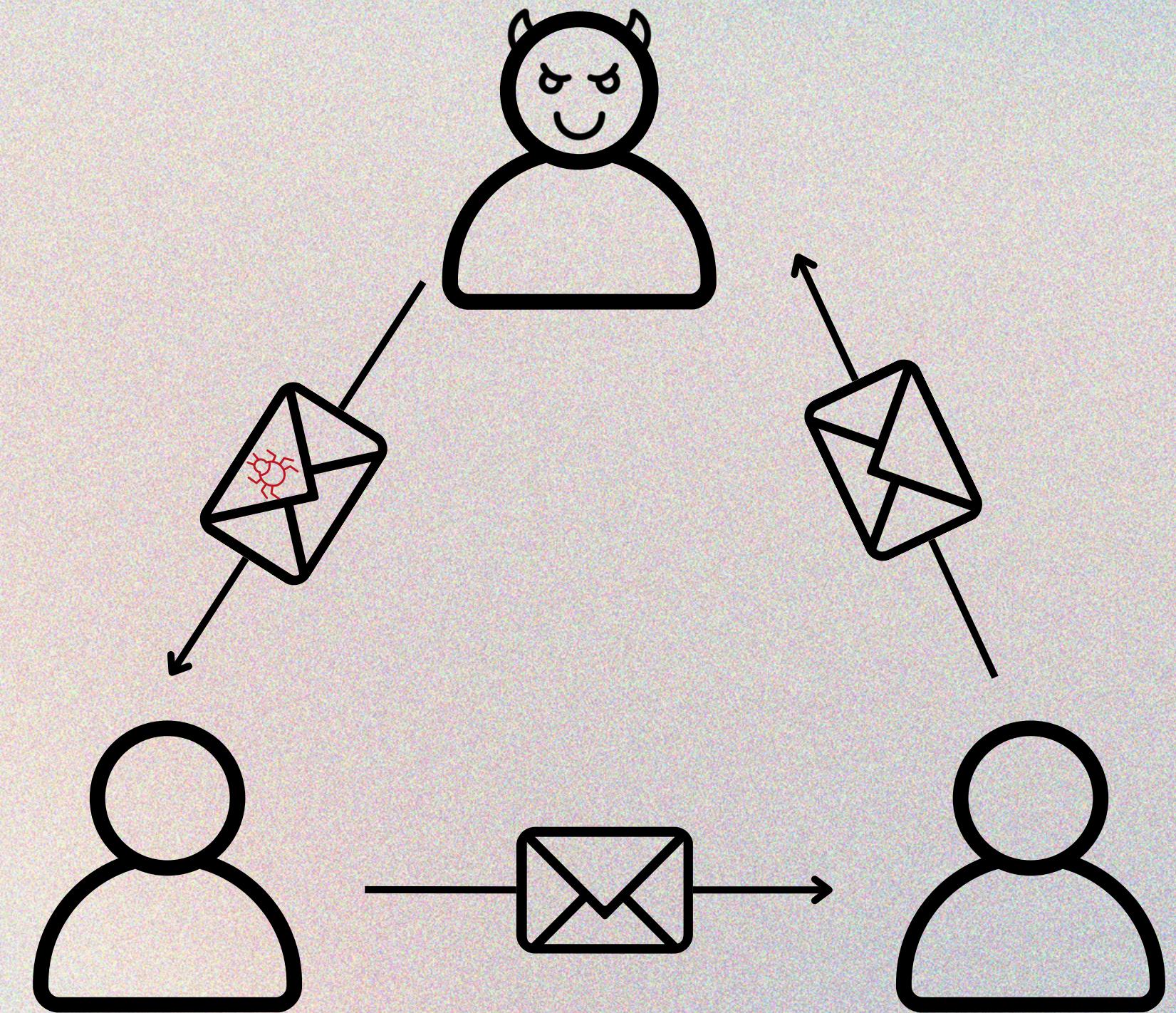
ATTACCO 2: SOMMA MANIPOLATA

Il nodo malevolo, effettuando azioni aggiuntive non concordate, riesce ad alterare l'output ad uno dei partecipanti.



ATTACCO 3: CATEGNA INTERROTTA

Dopo un'analisi dettagliata dei messaggi scambiati, è stato possibile decifrare quali pacchetti trasportavano i messaggi di output. È stata quindi creata una funzione che invia messaggi alterati con l'obiettivo di falsare i risultati sui nodi non malevoli.



CONCLUSIONI

Sono state rilevate vulnerabilità nella libreria MPyC in scenari semi-onesti e malevoli, con evidenza di manipolazione dei dati e decryption non sicura. Proposte soluzioni come zero-knowledge proofs e crittografia avanzata per migliorare affidabilità e sicurezza.



**GRAZIE
PER L'ATTENZIONE**