Scuola di Ingegneria e Architettura
Dipartimento di Informatica · Scienza e Ingegneria · DISI
Corso di Laurea in Ingegneria Informatica

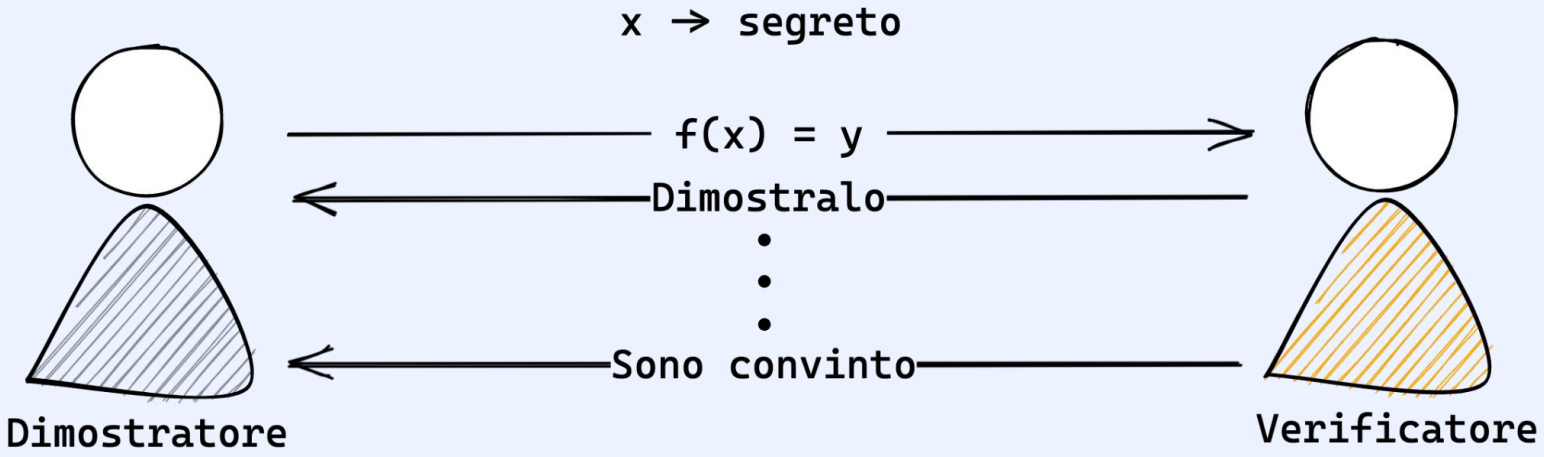
SISTEMI ANTI-DENIAL OF SERVICE IN AMBIENTI ANONIMI BASATI SU ZK-SNARK

Relatore:
Prof. Paolo Bellavista

Presentata da:
Straccali Leonardo

Zero Knowledge Proof

Capacità di dimostrare l'esecuzione corretta di un algoritmo senza dover rivelare i dati in ingresso



zk-SNARK

Zero-Knowledge Succinct Non-Interactive Argument of Knowledge

Tempo creazione

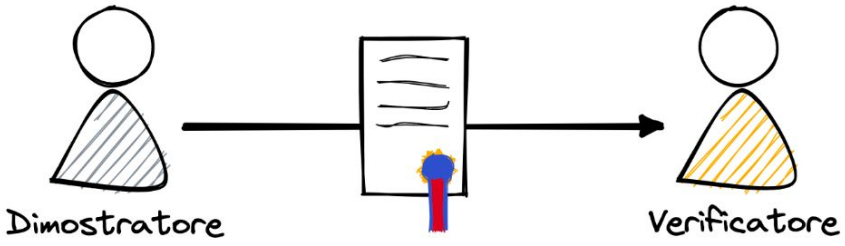
2.3 s

Tempo Verifica

10 ms

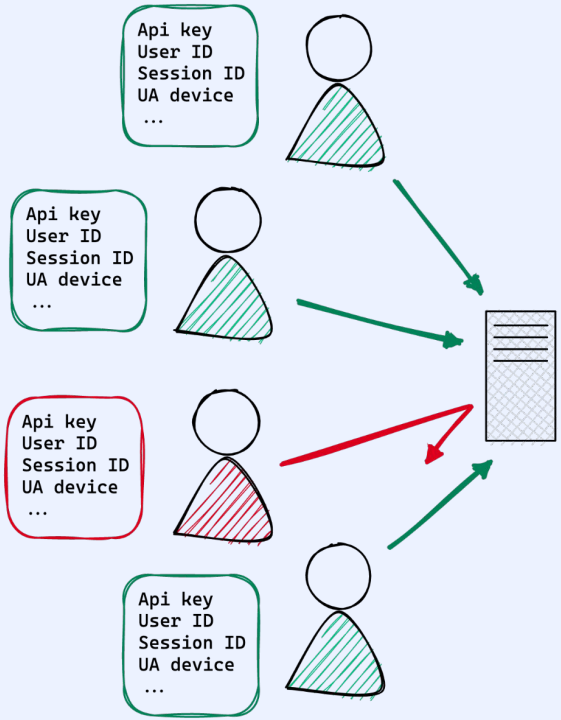
Dimensione prova

288 byte

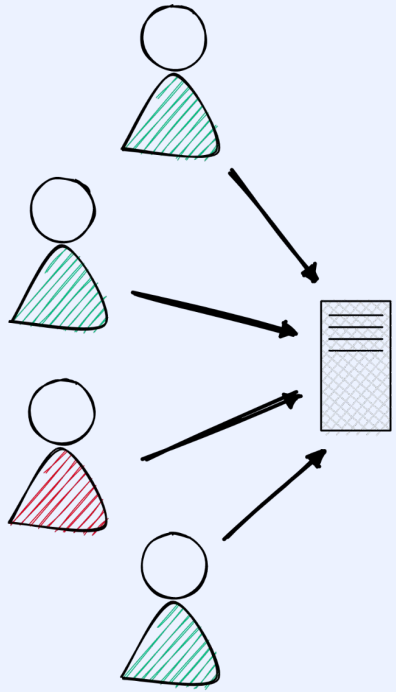


Anti-DoS in ambiente anonimo

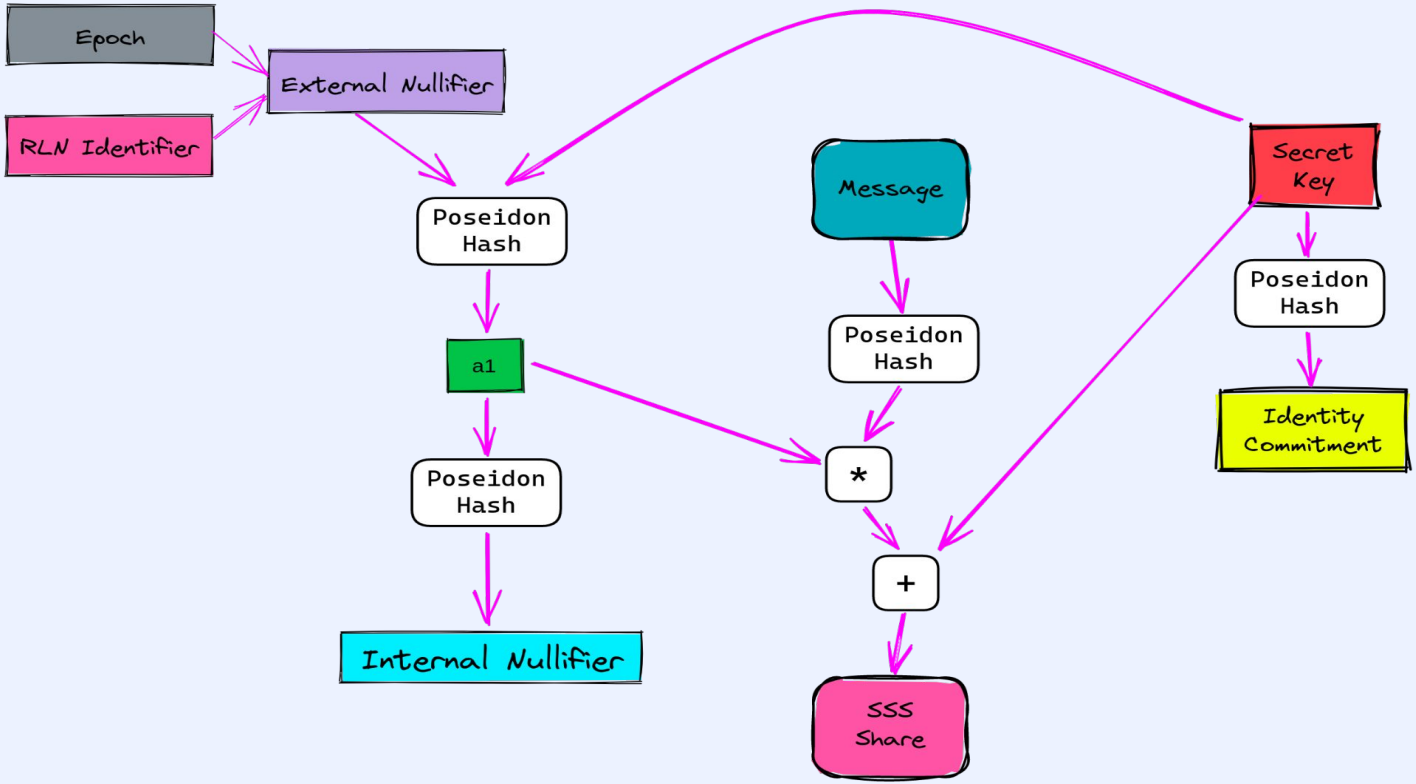
ambiente ordinario



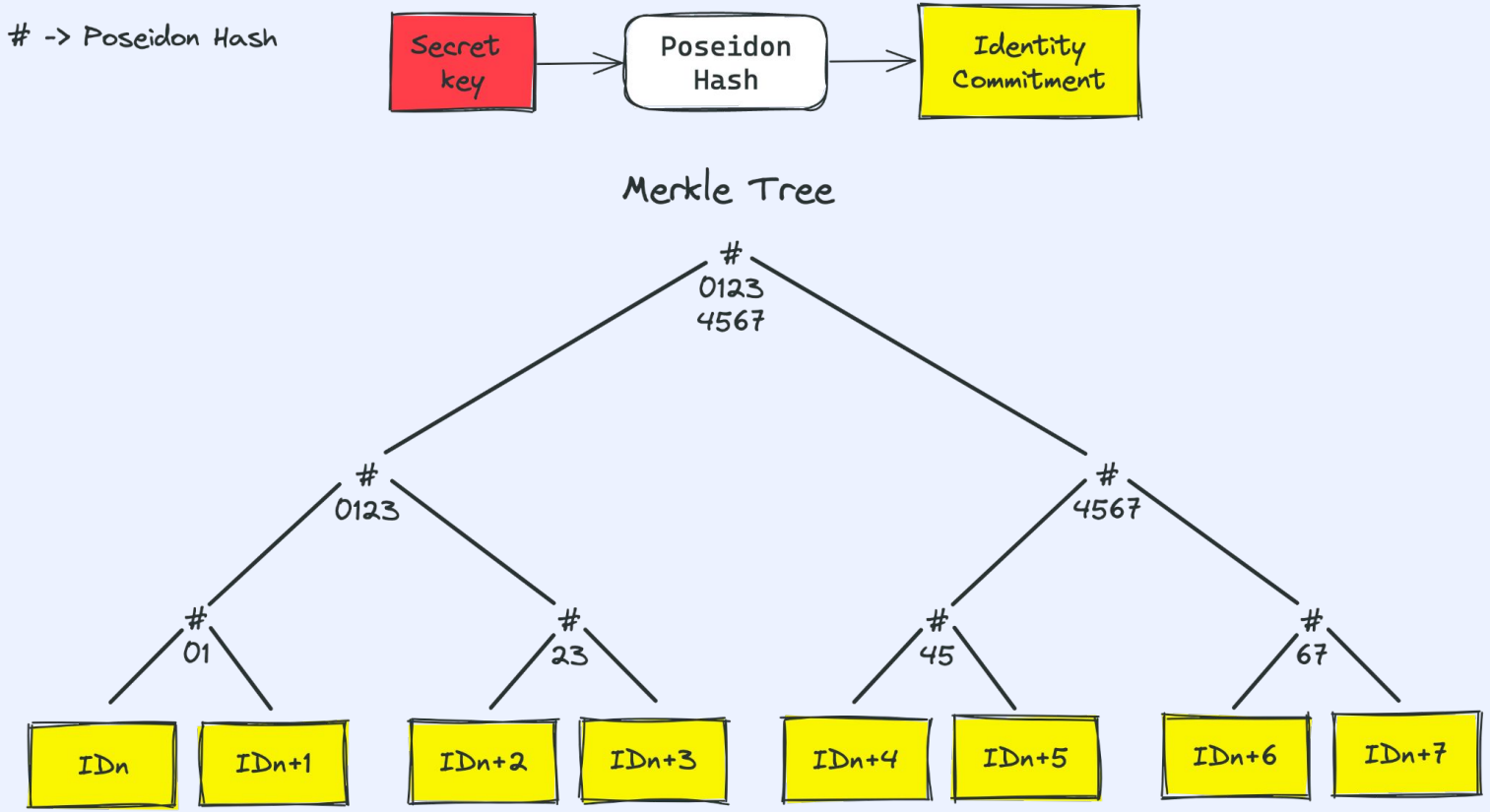
ambiente anonimo



RLN

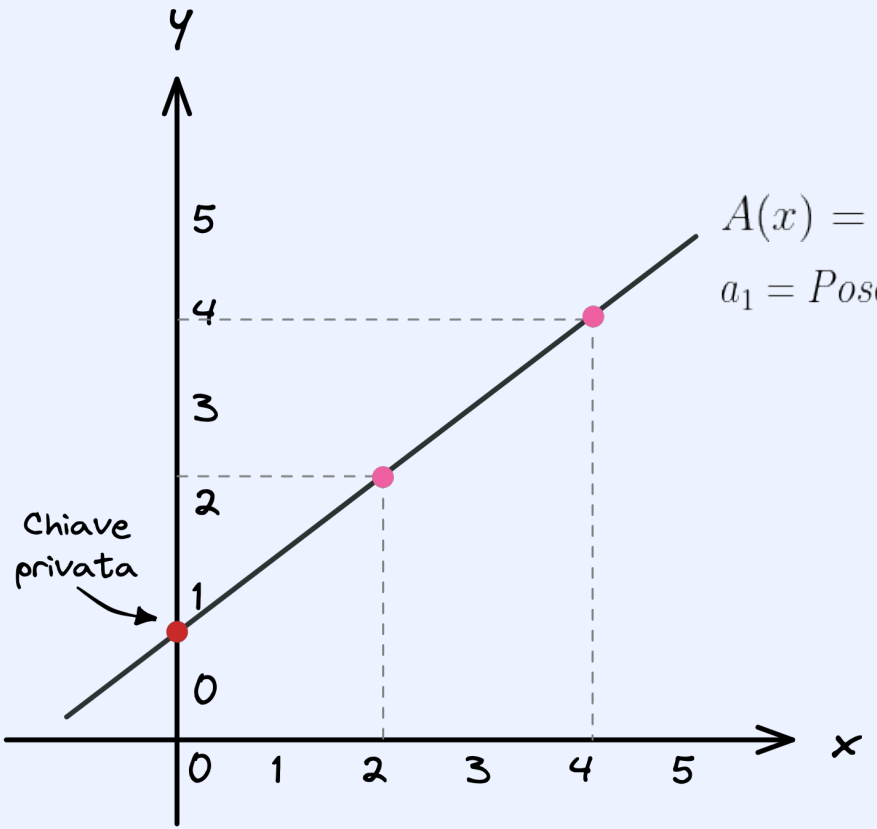

Epoch
External Nullifier
RLN Identifier
Poseidon Hash
a1
Poseidon Hash
Internal Nullifier
Message
Poseidon Hash
*
+
SSS Share
Secret Key
Poseidon Hash
Identity Commitment

RLN - Registrazione



RLN - Interazione

SSS Share

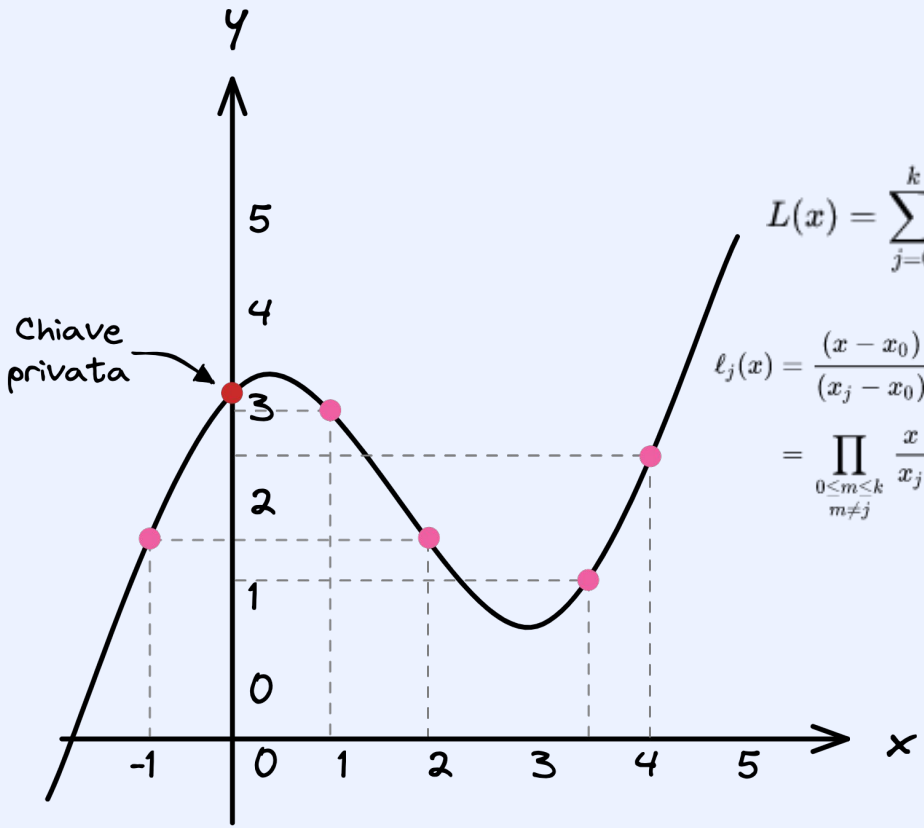


$$A(x) = a_1 * x + a_0$$

$$a_1 = Poseidon(a_0, external\_nullifier)$$

RLN - Interazione

SSS Share



$$L(x) = \sum_{j=0}^{k} y_j \ell_j(x).$$

$$\ell_j(x) = \frac{(x - x_0)}{(x_j - x_0)} \cdots \frac{(x - x_{j-1})}{(x_j - x_{j-1})} \frac{(x - x_{j+1})}{(x_j - x_{j+1})} \cdots \frac{(x - x_k)}{(x_j - x_k)}$$

$$= \prod_{\substack{0 \le m \le k \\ m \ne j}} \frac{x - x_m}{x_j - x_m}.$$

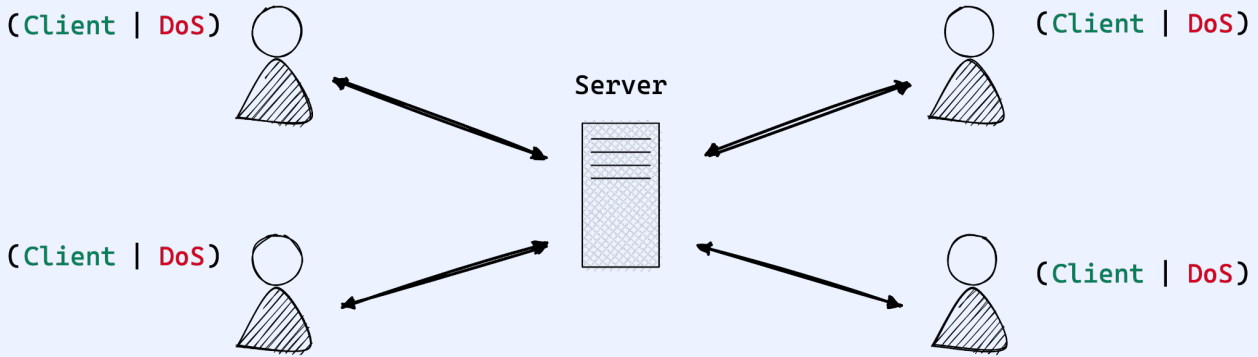
Prototipo

Obbiettivo: Applicare il protocollo RLN a una struttura di tipo Client/Server in ambiente anonimo*

Linguaggi usati: TypeScript, Circom

Librerie usate: Rlnjs, Rln-circuit, Socket.IO, Circom lib

Tecnologie usate: Node.js, Web Assembly, Web Socket, Eslint, Git



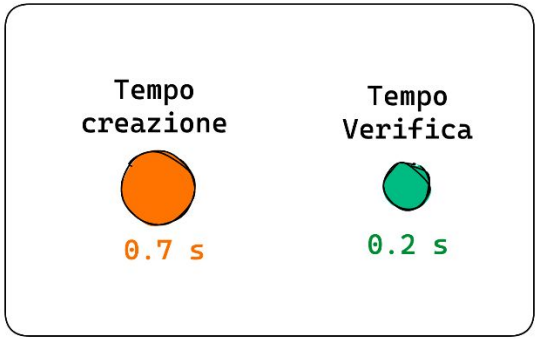
Prototipo - Esecuzione

RLN : OFF

```
Signal: 4124889358320442841707057036539213410598335664943159828119778691355697372 05
Signal: 1467277834811643929285454601632814245264857717925107032771764723151022375 97
Signal: 2556067988658861861192961389152796229917812376284881132368798493163577786 20
Signal: 4020439317225922297514424153805387708029950835211889469743232299545421508 60
Signal: 3022765250307670248611012791474851284733139230997510748894928430032757135 06
Signal: 1819249405857342238834984347958572420316656837555864752562582173597490856 45
Signal: 2194227084833782696675124620809521859900088047885175894274982767031015179 57
Signal: 3182989482022490645468545697357633351393748910181472316271878675236898880 31
Signal: 4260697181138068485219820514288942693051527860093829846689570365916321419 10
Signal: 2384077255109443329568833309820908801358363577503767607917003699129506886 73
Signal: 1823566811065283571897792500390977789985814946091039495813921652070709193 6
Signal: 4096085833616286261222997025174337110817795650409651542727302383535563048 88
Signal: 2726866521666193883934892739964787220447136080127472564570865818421037798 21
Signal: 2454894319600026573893714059131057794546152759621359198794411574868848608 24
Signal: 1313035110969963527351958926690839978371290347441820710423263986755746888 28
Signal: 3841807711091507572979382006163350988788252356470300538251208201368942314 14
Signal: 4121977563342890121435582832079789644024317181879640773614941330442797127 93
Signal: 9419335504851762696504277120992339343013474045331787969260444696965844547
Signal: 9367787659136536145275246257095906270074744726004336938143554746283729878 1
Signal: 1971644955040075476052731592940504733202165698821576210571434066149150076 35
Signal: 4203430852981919664503005496126613352099400931578869116298101919372187793026
Signal: 1980820974744157732179991991437280964434563927101673024640597899474995 1487
Signal: 4124889358320442841707057036539213410598335664943159828119778691355697372 05
Signal: 5295964316241093332487027739555562824052865484664542158544429778048505665 1
Signal: 2760701545625016262606733812142918232967574523420019303795304175488060679 04
Signal: 4020439317225922297514424153805387708029950835211889469743232299545421508 60
Signal: 1279140221563075301105609639382860176516552752700173410497309634886825285 17
Signal: 2719043587282523951111309147656284989994794256873887698671030571656233372 74
Signal: 2194227084833782696675124620809521859900088047885175894274982767031015179 57
Signal: 3480851892266718764057644984229295301317791206403795004537222464722711944 77
Signal: 2761888802395732868420864693750023975030104342138489489837483479460773840 2
Signal: 2384077255109443329568833309820908801358363577503767607917003699129506886 73
Signal: 4360211434858356742312681215793712914597245832626518750930562092356047742 51
Signal: 2063868910726683800986497491183102174895743292467800407981321590644023245 46
Signal: 2726866521666193883934892739964787220447136080127472564570865818421037798 21
```

RLN : ON

```
Signal: 2556067988658861861192961389152796229917812376284881132368798493163577786 20
Breach detected : Rate limit breach, secret attached
Signal: 2556067988658861861192961389152796229917812376284881132368798493163577786 20
Breach detected : Rate limit breach, secret attached
Signal: 2556067988658861861192961389152796229917812376284881132368798493163577786 20
Breach detected : Rate limit breach, secret attached
Signal: 2556067988658861861192961389152796229917812376284881132368798493163577786 20
Breach detected : Rate limit breach, secret attached
```



Conclusione

+ Il protocollo risolve corettamente e con affidabilità il problema dell'attuazione di regole di rate-limiting in ambiente anonimo.

- Eredità molte delle criticità della tecnologia zk-SNARK, come la necessità di un trusted setup e i tempi di generazione delle prove elevati.

- È inoltre un protocollo molto nuovo, ideato nel 2019 che deve essere ancora utilizzato in applicazioni fuori dall'ambiente di testing.

+ Ottimo esempio di come è possibile utilizzare traendone beneficio, la tecnologia Zero Knowledge Proof in situazioni conosciute ma attualmente irrisolte.