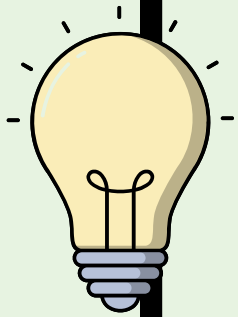
# Project Work
## Algoritmi e Protocolli per la Sicurezza


Docenti:
Carlo Mazzocca,
Francesco Cauteruccio

**Gruppo 6** - Studenti:
Francesco Pio Cirillo,
Alessandra Fasolino


Dipartimento di Ingegneria dell'Informazione ed Elettrica e Matematica Applicata

# Overview

## 01 Threat Model

Contestualizzazione dei treat model e Analisi della sicurezza

## 02 Prestazioni

Analisi dell'overhead spaziale e dei tempi

## 03 Schema

Interazioni e gestione dello scambio di messaggi

## 04 Merkle Tree

Gestione della privacy dello studente

## 05 Blockchain

Gestione della revoca dei certificati

# 01. Threat Model

## TM4 - Man in the middle durante lo scambio di chiavi

### Risorse
Accesso attivo alla comunicazione

### Obbiettivo
Ottenere la chiave di sessione

### Impatto
Perdita di sicurezza nello scambio di informazioni da ambo le parti oneste.

### Attaccante
Hacker professionista

### Asset
Chiave di sessione per la comunicazione simmetrica

### Security Analysis
Le parti oneste coinvolte devono dimostrare la loro identità per mezzo della decrittazione di Nonce crittografati con la chiave pubblica.

Dipartimento di Ingegneria dell'Informazione ed Elettrica e Matematica Applicata

# 01. Threat Model

## TM7 - Cambio dello stato di revoca di un certificato revocato

### Risorse

Essere un proponente della blockchain che ospita la lista delle revoch

### Obbiettivo

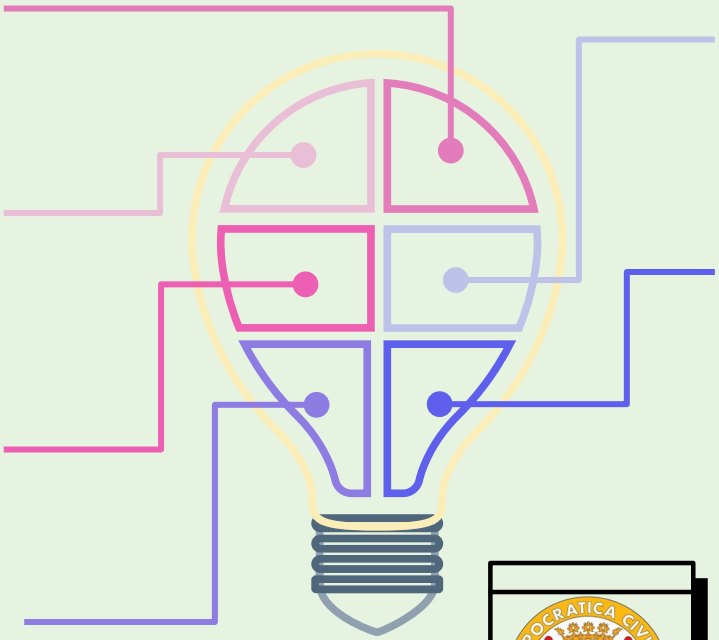
Modificare lo stato di revoca di un certificato per fare in modo da far risultare non revocato un certificato revocato

### Impatto

Perdita di fiducia nell'università e nei certificati da essa rilasciati

### Attaccante

Terza parte malintenzionata



### Asset

Credibilità dell'università e credibilità delle certificazioni

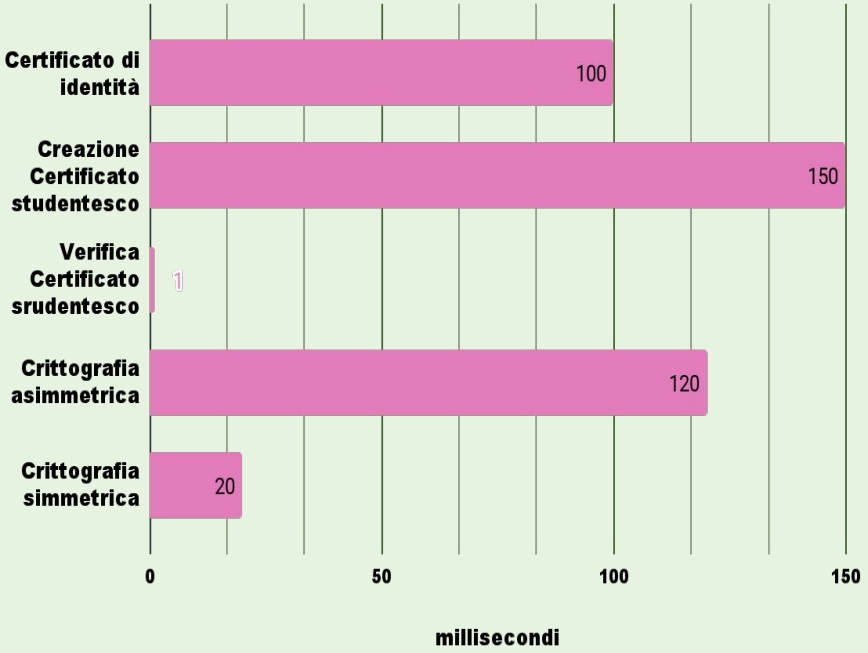
### Security Analysis

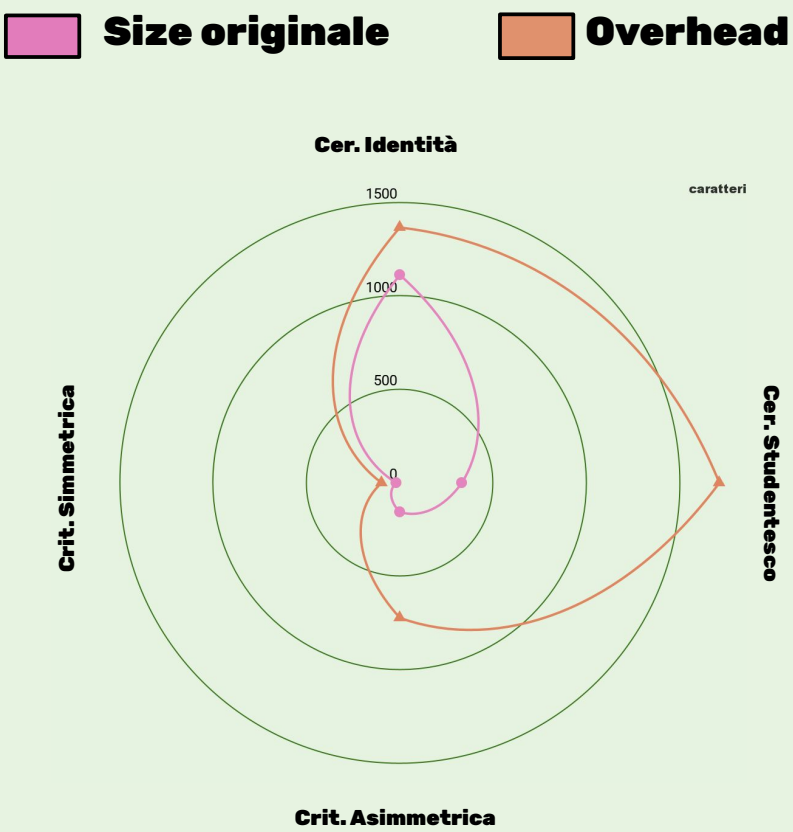
Essendo un proponente per la blockchain, si tratta di una struttura dati append-only e non sono quindi possibili modifiche a dati già aggiunti.

Dipartimento di Ingegneria dell'Informazione ed Elettrica e Matematica Applicata

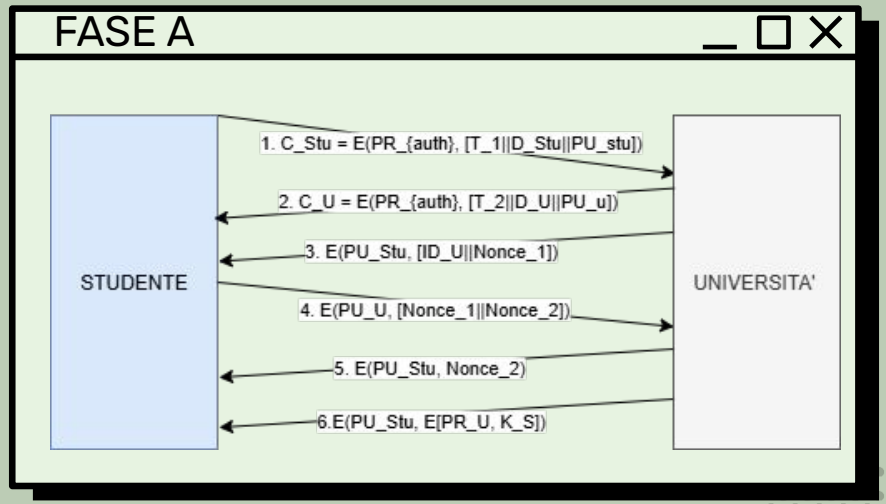
# 02. Prestazioni

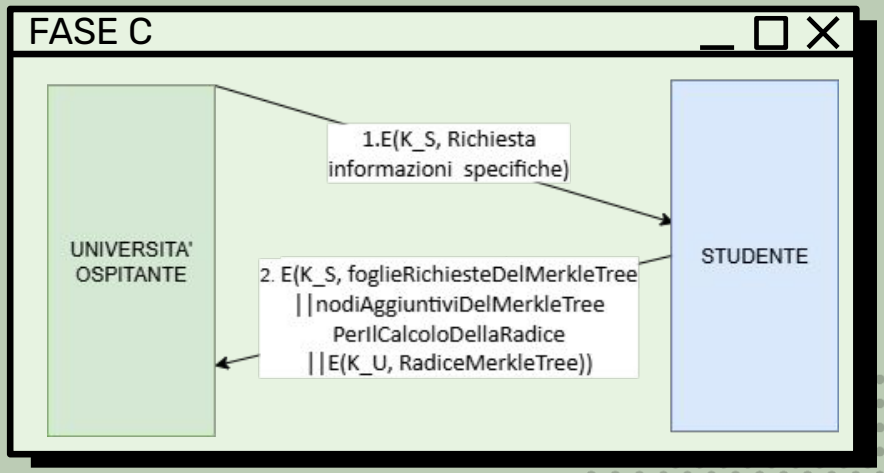
## Latenza

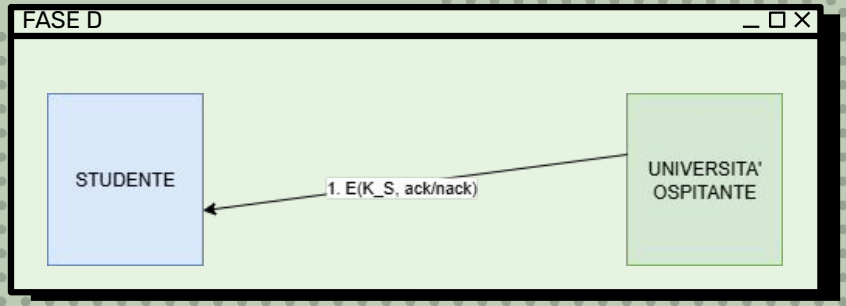


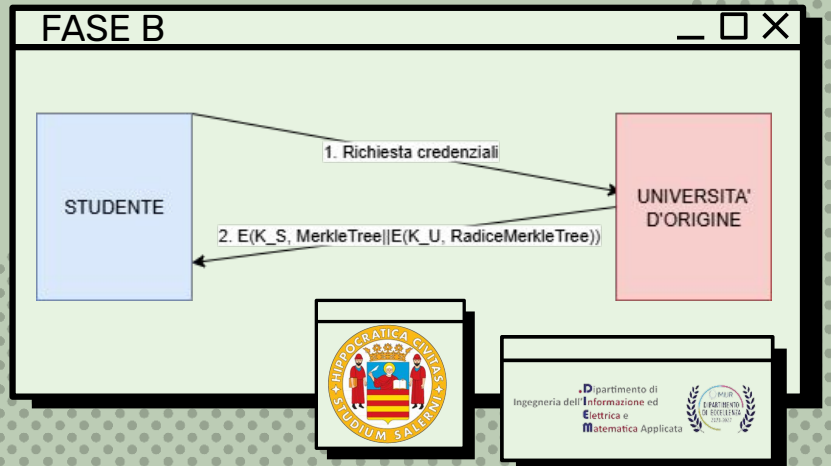



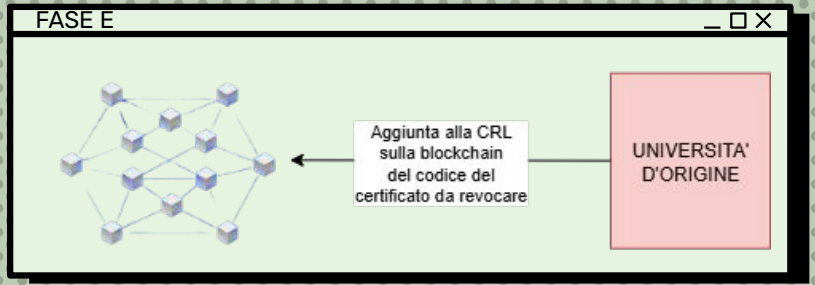
# 03. Schema


FASE A
STUDENTE
UNIVERSITA'
1. C_Stu = E(PR_{auth}, [T_1||D_Stu||PU_stu])
2. C_U = E(PR_{auth}, [T_2||D_U||PU_u])
3. E(PU_Stu, [ID_U||Nonce_1])
4. E(PU_U, [Nonce_1||Nonce_2])
5. E(PU_Stu, Nonce_2)
6.E(PU_Stu, E[PR_U, K_S])

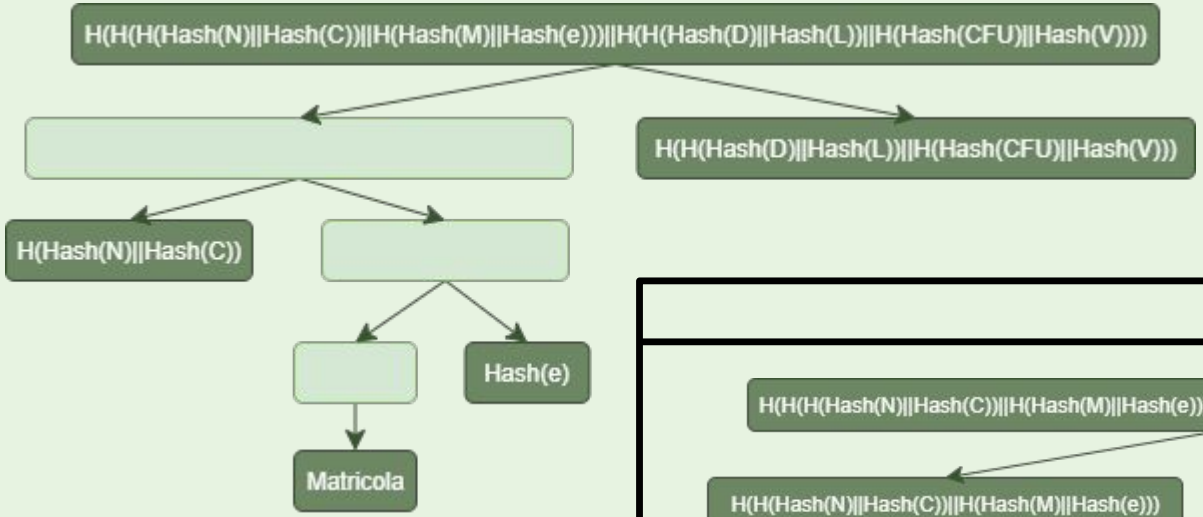

FASE C
UNIVERSITA' OSPITANTE
1.E(K_S, Richiesta informazioni specifiche)
STUDENTE
2. E(K_S, foglieRichiesteDelMerkleTree ||nodiAggiuntiviDelMerkleTree PerIlCalcoloDellaRadice ||E(K_U, RadiceMerkleTree))

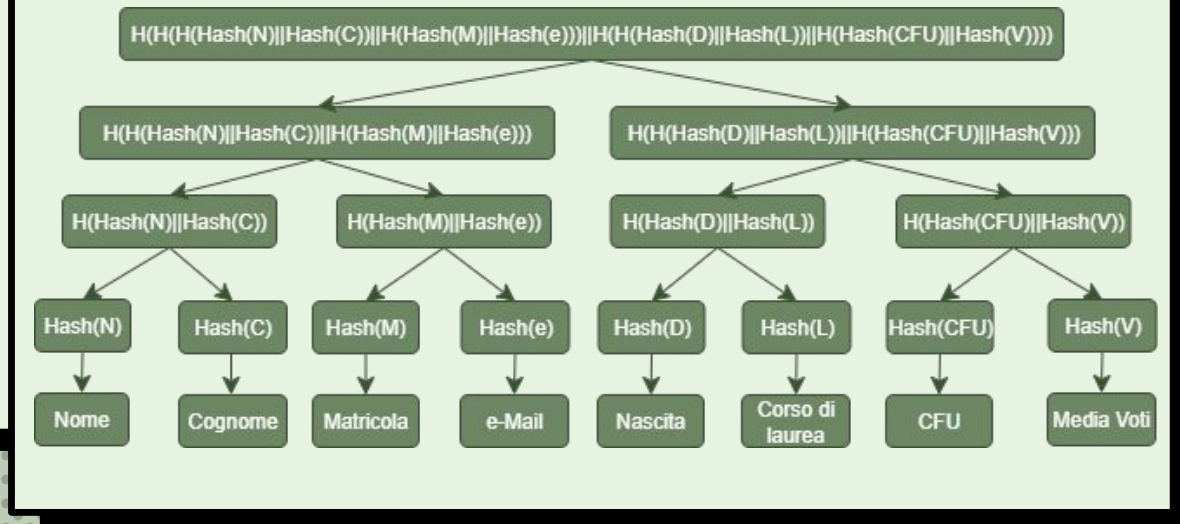

FASE D
STUDENTE
1. E(K_S, ack/nack)
UNIVERSITA' OSPITANTE


FASE B
STUDENTE
1. Richiesta credenziali
2. E(K_S, MerkleTree||E(K_U, RadiceMerkleTree))
UNIVERSITA' D'ORIGINE
Dipartimento di Ingegneria dell'Informazione ed Elettrica e Matematica Applicata


FASE E
Aggiunta alla CRL sulla blockchain del codice del certificato da revocare
UNIVERSITA' D'ORIGINE

# 04. Merkle Tree





Dipartimento di Ingegneria dell'Informazione ed Elettrica e Matematica Applicata

# 05. Blockchain

## SMART CONTRACT


PARTIES SMART CONTRACT EXECUTION

Dipartimento di Ingegneria dell'Informazione ed Elettrica e Matematica Applicata

# Grazie per l'attenzione