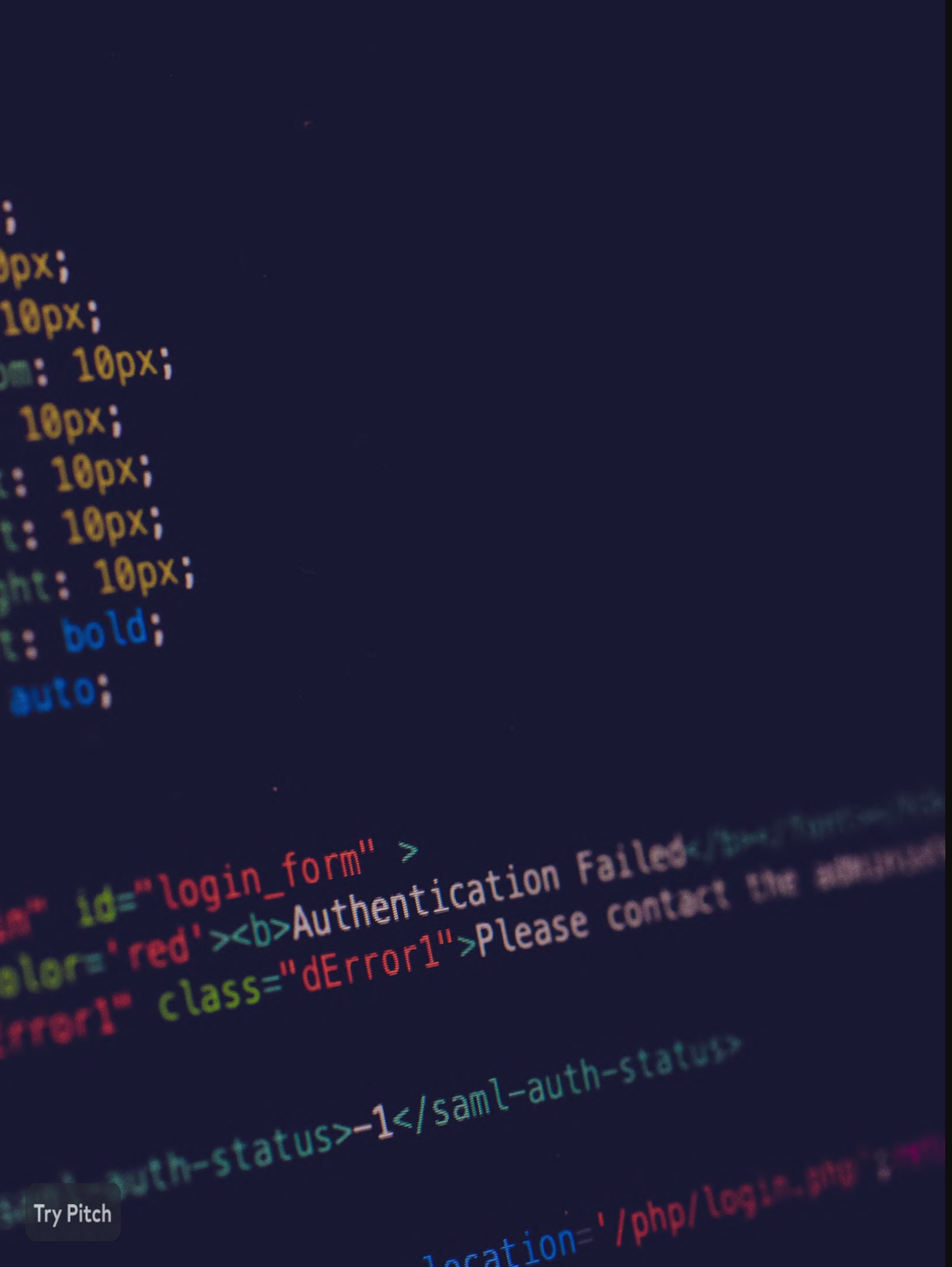
07 January 2025

Zero-Knowledge Authentication Feige-Fiat-Shamir Protocol

Șerban Tiurbe
SISC - ANUL 1



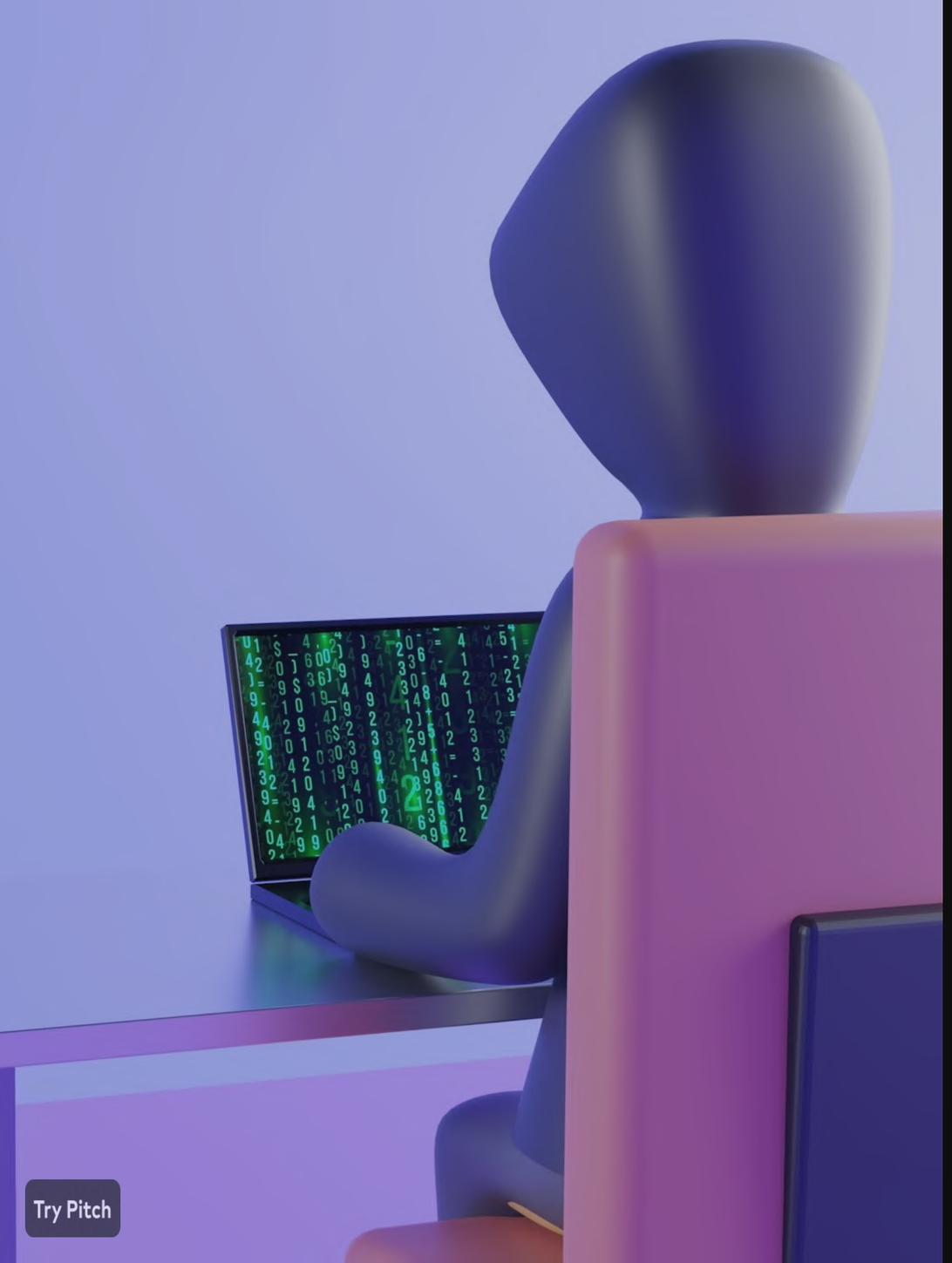
Introducere

Importanța Securității Criptografice: În contextul actual, unde amenințările cibernetice sunt în creștere, securitatea criptografică devine esențială pentru protecția datelor și comunicațiilor digitale.

Inovație în Criptografie - Protocolul Feige-Fiat-Shamir: Protocolul Feige-Fiat-Shamir se distinge prin abordarea sa unică de autentificare zero-knowledge, oferind o metodă eficientă și sigură de a confirma posesia unei cunoștințe secrete fără a expune acea informație. Aceasta tehnologie nu numai că consolidează securitatea dar și optimizează procesele prin reducerea cerințelor de procesare și de transmitere a datelor.

Scopul proiectului

Evaluarea Eficienței și Securității: Evaluarea performanței protocolului Feige-Fiat-Shamir în termeni de securitate și eficiență computațională în comparație cu metodele criptografice tradiționale precum RSA și DSA.

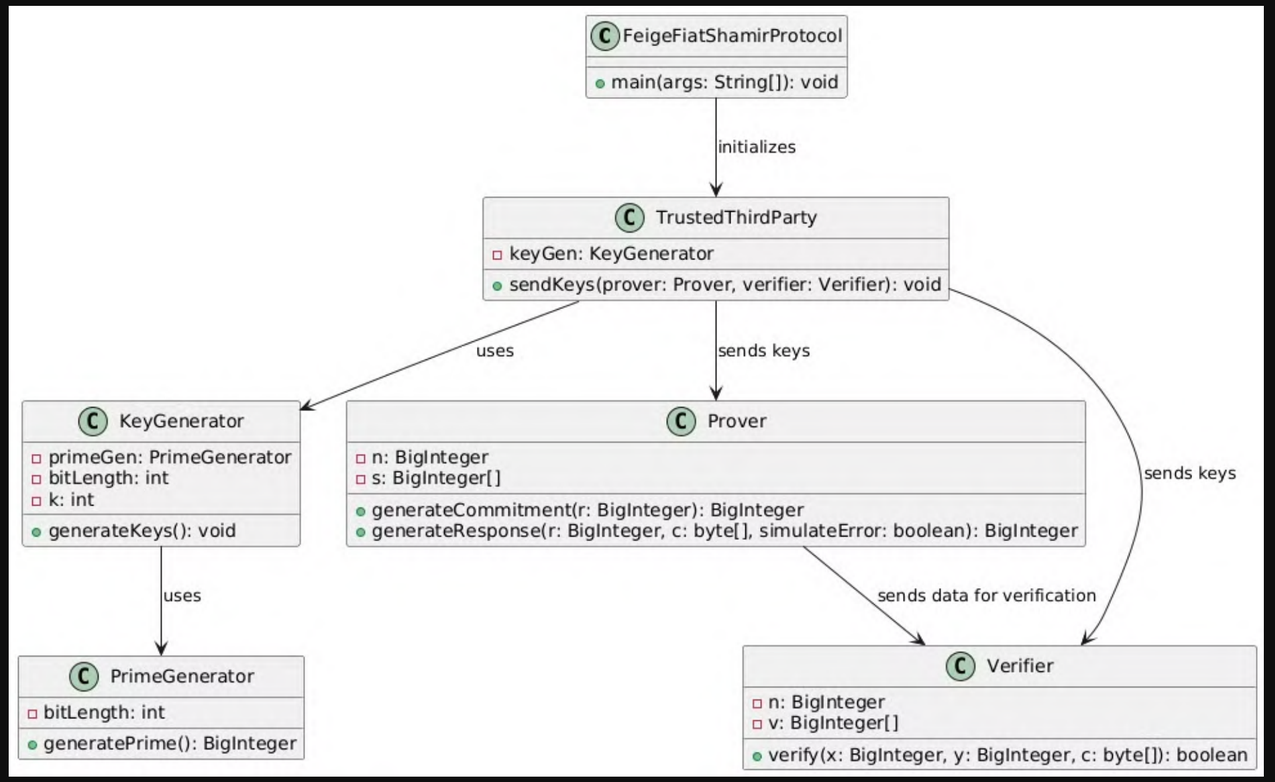


Feige-Fiat-Shamir

Descrierea Protocolului: Protocolul Feige-Fiat-Shamir este un sistem de autentificare zero-cunoștințe care permite unui prover să demonstreze că deține o anumită cunoștință secretă fără a o dezvălui verificatorului.

Funcționare: În cadrul protocolului, proverul folosește un set de chei secrete și publice generate prin procese matematice specifice pentru a crea angajamente și a răspunde la provocările verificatorului, care verifică aceste răspunsuri fără a afla cheile secrete.

Principii Criptografice de Bază: Utilizează concepte de zero-knowledge proof, unde „zero cunoștințe” înseamnă că verificatorul nu învață nimic altceva în afara faptului că afirmația proverului este adevărată, asigurând astfel un nivel înalt de securitate și confidențialitate.



Metodologie

Generarea Cheilor: Cheile secrete și publice au fost generate folosind algoritmi de generare a numerelor prime și calcule matematice specifice, asigurând unicitatea și securitatea necesară pentru fiecare sesiune de autentificare.

Configurarea Sistemului: Setările inițiale includ configurarea parametrilor criptografici și stabilirea numărului de runde de verificare, adaptate pentru a evalua performanța protocolului sub diverse scenarii de test.

Algoritmi Tradiționali

RSA (Rivest-Shamir-Adleman)

- **Securitate bazată pe numere prime**: RSA utilizează un sistem de chei publice și private bazat pe dificultatea factorizării produsului a două numere prime mari.
- **Utilizări multiple**: Folosit atât pentru criptarea datelor cât și pentru semnături digitale, asigurând confidențialitatea și integritatea informațiilor.
- **Scalabilitate**: Eficiența RSA poate scădea la chei de dimensiuni mai mari, influențând timpul de procesare necesar criptării și decriptării.

DSA (Digital Signature Algorithm)

- **Specializat în semnături digitale**: DSA este utilizat exclusiv pentru crearea semnăturilor digitale, nu pentru criptarea datelor, oferind o metodă rapidă și sigură de verificare a autenticității documentelor.
- **Eficiența semnăturilor**: Oferă semnături mai scurte comparativ cu RSA, ceea ce îl face mai eficient din punct de vedere al spațiului necesar.
- **Dependența de numere aleatorii**: Securitatea DSA este foarte dependentă de calitatea generatorului de numere aleatorii, fiind vulnerabil la atacuri dacă această componentă este slabă.

Experimente și Rezultate

Număr de Iterații	Timp de generare a cheilor (ns)	Timp de semnare (ns)	Timp mediu de verificare (ns)
10	496184400	3277100	307050
100	242638200	3983600	151024
1000	230735400	3967800	81944

TABLE II
REZULTATELE MĂSURĂTORILOR PENTRU RSA

Număr de Iterații	Timp de generare a cheilor (ns)	Timp mediu de semnare (ns)	Timp mediu de verificare (ns)
10	86015200	3863070	3119660
100	63256800	1299235	995800
1000	68530500	575856	853858

TABLE III
REZULTATELE MĂSURĂTORILOR PENTRU DSA

Număr de Iterații	Timp de generare a cheilor (ns)	Timp total de execuție (ns)	Timp mediu per rundă (ns)
10	83710600	93400700	166080
100	97861400	119591600	86555
1000	97547800	182654200	53354

TABLE I
REZULTATELE MĂSURĂTORILOR PENTRU PROTOCOLUL FEIGE-FIAT-SHAMIR

Analiza Performanței: Am evaluat și comparat timpul de generare a cheilor, timpul total de execuție, și timpul mediu pe rundă pentru protocolul Feige-Fiat-Shamir, RSA, și DSA, observând că Feige-Fiat-Shamir oferă o eficiență semnificativă în timpul de răspuns pe rundă, în special în teste cu număr mare de iterații.

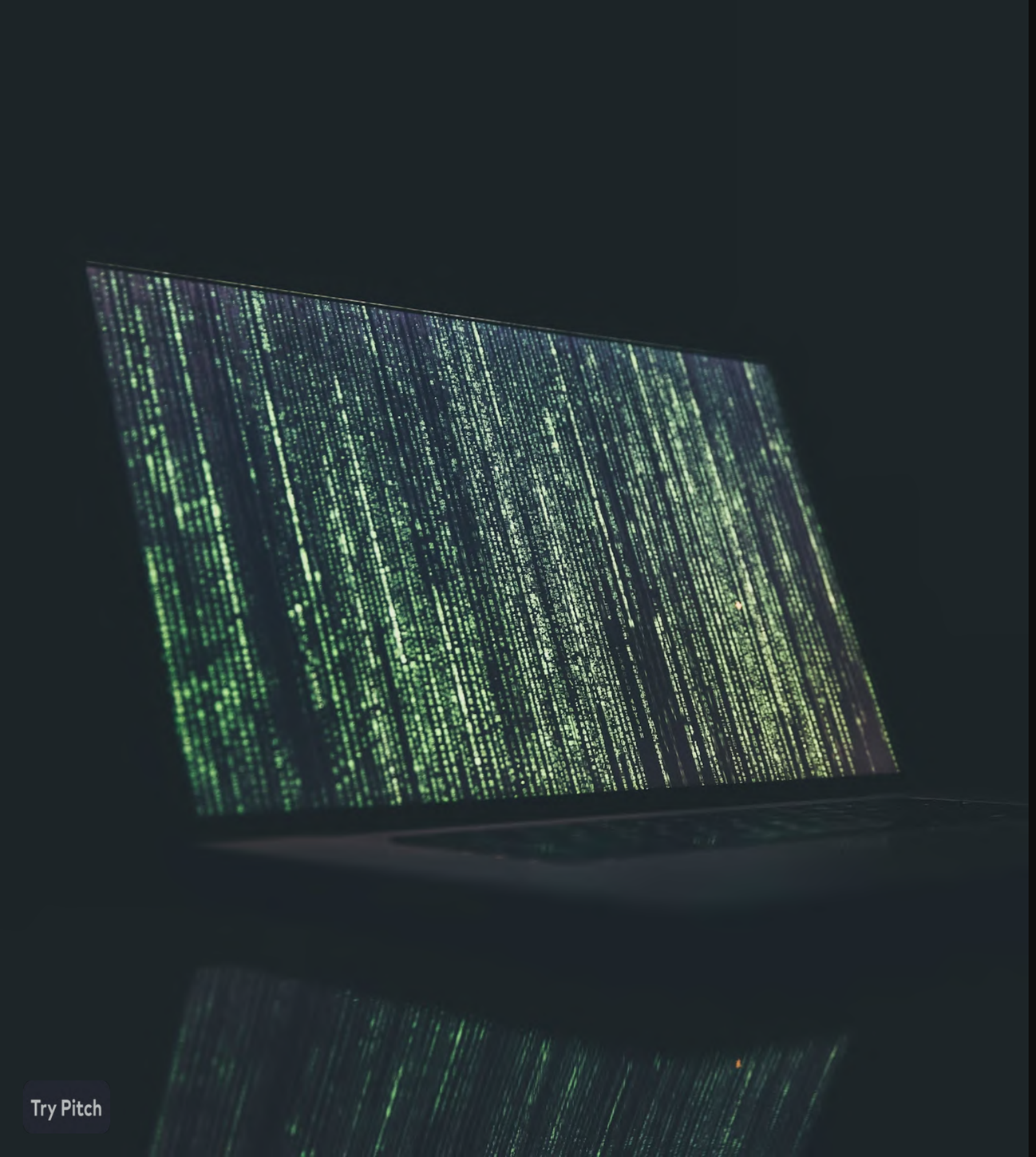
Rezultatele Comparate: Datele experimentale arată că Feige-Fiat-Shamir necesită un timp de generare a cheilor comparabil cu DSA și mai rapid decât RSA, oferind, de asemenea, o reducere substanțială a timpului de execuție per total, ceea ce demonstrează potențialul său pentru aplicabilitate în sisteme unde timpul de răspuns este critic.

Implicații și Aplicații Practice

Aplicații în Autentificarea Securizată: Protocolul Feige-Fiat-Shamir este ideal pentru sistemele care necesită autentificare securizată și rapidă, cum ar fi accesul la baze de date securizate, sisteme bancare online, și comunicații guvernamentale confidentiale.

Beneficii în Eficiență și Scalabilitate: Datorită naturii sale de zero-knowledge, protocolul reduce necesitatea schimbului de informații sensibile pe rețea, diminuând astfel riscul de interceptare a datelor și îmbunătățind viteza de procesare a autentificărilor.

Extindere în Aplicații IoT și Mobile: Utilizarea protocolului în IoT și aplicații mobile poate oferi o metodă robustă și eficientă pentru gestionarea securității dispozitivelor interconectate, de la camere inteligente la sistemele de home automation.



Concluzii

Eficacitatea Protocolului Feige-Fiat-Shamir: Studiul a confirmat superioritatea protocolului Feige-Fiat-Shamir în termeni de eficiență și securitate comparativ cu algoritmi tradiționali precum RSA și DSA, demonstrând avantajele sale în scenarii de autentificare rapidă.

Implicații pentru Securitatea Digitală: Implementarea protocolului poate transforma fundamental securitatea sistemelor digitale, oferind soluții mai rapide și mai sigure pentru protecția datelor și a comunicațiilor în era digitală.

Direcții Viitoare și Impactul Cercetării: Cercetarea deschide noi posibilități pentru optimizarea algoritmilor de autentificare și extinderea lor în diverse aplicații tehnologice, contribuind semnificativ la evoluția criptografiei moderne.

Vă mulțumesc pentru atenție!

Pitch

Want to make a presentation like this one?

Start with a fully customizable template, create a beautiful deck in minutes, then easily share it with anyone.

Create a presentation (It's free)