Provas de Conhecimento Zero: Um Estudo sobre zk-SNARKs e sua Aplicação em Sistemas de Autenticação

Alex Davis Neuwiem da Silva

Ciências da Computação | INE | CTC

UNIVERSIDADE FEDERAL
DE SANTA CATARINA

Introdução

1. **Estudo Teórico**
   - Realizar uma análise aprofundada dos principais protocolos zk-SNARKs.
   - Foco em **Pinocchio** e **Groth16**.
2. **Aplicação Prática**
   - Desenvolver de um sistema de autenticação biométrica facial que preserva a privacidade.
   - Utiliza **Groth16**.

Estrutura

Provas de Conhecimento

zk-SNARKs

Pinocchio

Groth16

Autenticação Biométrica

O que é uma Prova de Conhecimento?

É um protocolo computacional entre duas partes:

- **Provador (P):** A parte que alega conhecer uma informação.
- **Verificador (V):** A parte que valida a alegação.

Satisfazendo as seguintes propriedades:

- **Completude:** Se P é honesto, V sempre aceitará a prova.
- **Solidez:** Se P é desonesto, V só aceitará a prova com uma probabilidade negligenciável.

Formalizando uma prova de conhecimento

1. "Estar convencido"
   - P e V são modelados como máquinas de Turing interativas.
   - São definidos o parâmetro público x e a testemunha privada w.
   - V é "convencido"quando chega em seu estado de aceitação.

2. "Saber algo"
   - Se P conhece uma solução válida, então ela pode ser extraída de P.
   - **Extrator de conhecimento:** Dispositivo hipotético capaz de extrair w de P.

O que é uma Prova de Conhecimento Zero?

- A propriedade de **conhecimento zero** garante que o verificador seja convencido sem revelar nenhuma informação adicional além da veracidade dessa afirmação
- É formalmente definido em termos de um **simulador**: uma máquina que pode gerar uma prova "falsa" sem ter acesso à testemunha real do provador. Se a prova gerada pelo provador real for computacionalmente indistinguível da prova gerada pelo simulador, então o verificador não aprendeu nada além da verdade da afirmação. (A transcrição da conversa é trivial que um simulador também pode gerá-la)

Exemplo Interativo: Coloração de Grafos

- **Objetivo:** O Provador (P) quer provar ao Verificador (V) que conhece uma coloração de três cores válida para um grafo G, sem revelar tal coloração.
- **Protocolo:**
  1. **Compromisso:** P permuta aleatoriamente as cores (π), criptografa a cor de cada vértice ($F_v = f(\pi(\phi(v)), r_v)$) e envia todos os F_v para V.
  2. **Desafio:** V escolhe uma aresta aleatória (u, v) e a envia para P.
  3. **Resposta:** P revela as cores permutadas $\pi(\phi(u))$, $\pi(\phi(v))$ e as chaves de criptografia r_u, r_v.
  4. **Verificação:** V checa se as chaves abrem os compromissos F_u, F_v e se $\pi(\phi(u)) \neq \pi(\phi(v))$.
- O processo é repetido m^2 vezes para garantir a solidez.

Propriedades da Prova Interativa

- **Completude:** Se P conhece a coloração e segue o protocolo, V sempre aceitará a prova.
- **Solidez:** Se P não conhece a coloração, V irá rejeitar com alta probabilidade.
- **Conhecimento Zero:** V não aprende nada sobre a coloração. A permutação aleatória π a cada rodada garante que as cores reveladas não tenham correlação com a coloração original de P.

Propriedades da Prova Interativa

- **Completude:** Se P conhece a coloração e segue o protocolo, V sempre aceitará a prova.
- **Solidez:** Se P não conhece a coloração, V irá rejeitar com alta probabilidade.
- **Conhecimento Zero:** V não aprende nada sobre a coloração. A permutação aleatória π a cada rodada garante que as cores reveladas não tenham correlação com a coloração original de P.

Problema: Este protocolo é **interativo**. Requer múltiplas rodadas de comunicação e é modelado especificamente para um único problema.

Estrutura

Provas de Conhecimento

zk-SNARKs

Pinocchio

Groth16

Autenticação Biométrica

O que é um zk-SNARK?

Uma classe especial de Prova de Conhecimento Zero:

- **S**uccinct (Sucinto):
  - A prova é muito pequena (tamanho constante ou logarítmico).
  - A verificação é muito rápida.
- **N**on-interactive (Não-interativo):
  - O Provador envia uma única mensagem para o Verificador.
  - Geralmente requer uma Cerimônia de Confiança inicial.
- **AR**gument of **K**nowledge (Argumento de Conhecimento):
  - A solidez é *computacional* (baseada em problemas difíceis, ex: logaritmo discreto) e não estatística.

Exemplo de um circuito

Uma **prova de conhecimento** permite que um provador convença um verificador de que conhece um valor w tal que:

$$C(x, w) = 0$$

Onde:

- C é o circuito da condição a ser satisfeita
- x é o parâmetro público
- w é o valor privado

A propriedade **conhecimento zero** garante que o verificador não aprende nada sobre w

Pré-processamento do circuito

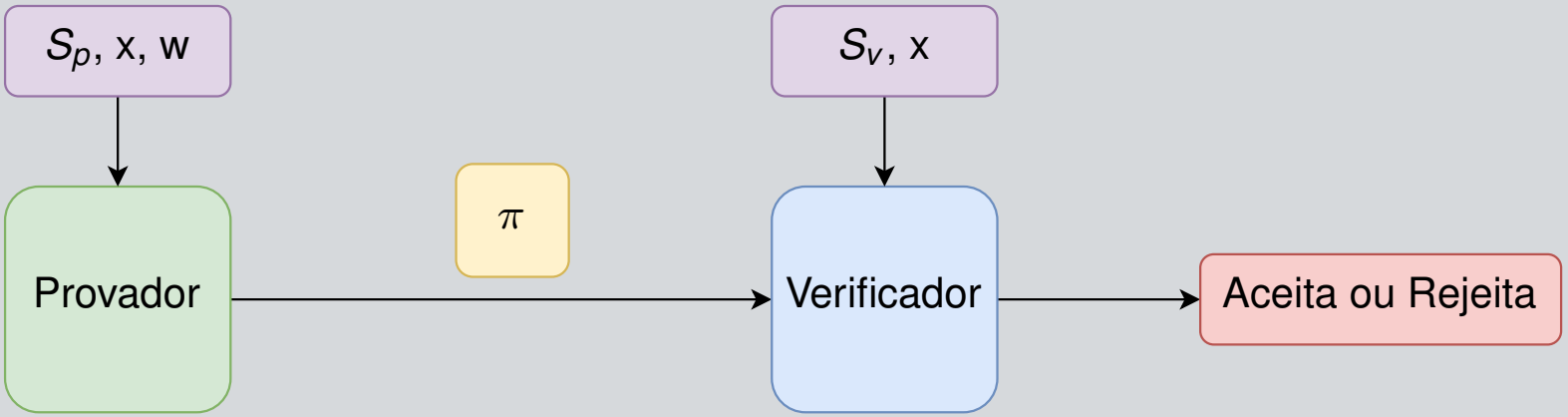
Cerimônia de Confiança sobre o circuito $C(x, w)$:

$$S(C) \rightarrow (S_p, S_v)$$

Um algoritmo que gera:

- Chave de Prova: S_p
- Chave de Verificação: S_v

Processamento de uma prova



Estrutura

Provas de Conhecimento

zk-SNARKs

Pinocchio

Groth16

Autenticação Biométrica

Estrutura

Provas de Conhecimento

zk-SNARKs

Pinocchio

Groth16

Autenticação Biométrica

Estrutura

Provas de Conhecimento

zk-SNARKs

Pinocchio

Groth16

Autenticação Biométrica

Reconhecimento Facial com Similaridade de Cossenos

O reconhecimento facial pode ser modelado como uma tarefa de comparação entre vetores:

- Cada rosto é representado por um vetor de características (*embedding*)
- Vetores são gerados por redes neurais treinadas para extrair feições únicas

A comparação é feita utilizando a **similaridade de cossenos**.

O que é a Similaridade de Cossenos?

A **similaridade de cossenos** mede o ângulo entre dois vetores:

$$\cos(\theta) = \frac{\vec{A} \cdot \vec{B}}{\|\vec{A}\| \cdot \|\vec{B}\|}$$

- Varia entre -1 (opostos) e 1 (iguais)
- Se $\cos(\theta) \approx 1$, vetores são semelhantes $\rightarrow$ rostos parecidos

Autenticação com Similaridade de Cossenos

1. A imagem de entrada é convertida em vetor $\vec{A}$
2. Vetor $\vec{B}$ é previamente armazenado durante a etapa de registro
3. Se $\cos(\vec{A}, \vec{B}) > \tau$, a autenticação é aceita

Nota: τ é um limiar definido com base no modelo de IA (ex: 0.7)

Problemas em Armazenar *Embeddings* Sem Proteção

Embeddings faciais são representações vetoriais únicas do rosto de uma pessoa. Armazená-las sem proteção apresenta riscos sérios:

- **Embeddings são identificadores biométricos:** um atacante pode usar *embeddings* roubadas para reconstruir um rosto e se autenticar como outra pessoa
- **Vazamentos são irreversíveis:** diferente de senhas, as representações vetoriais são insubstituíveis

Problemas em Armazenar *Embeddings* Sem Proteção

Embeddings faciais são representações vetoriais únicas do rosto de uma pessoa. Armazená-las sem proteção apresenta riscos sérios:

- **Embeddings são identificadores biométricos:** um atacante pode usar *embeddings* roubadas para reconstruir um rosto e se autenticar como outra pessoa
- **Vazamentos são irreversíveis:** diferente de senhas, as representações vetoriais são insubstituíveis

Solução: usar **provas de conhecimento zero** para provar correspondência sem expor o vetor.

Integração com Provas de Conhecimento Zero

O cálculo da similaridade de cosseno pode ser embutido no circuito de prova de conhecimento zero:

- $\cos(\vec{A}, \vec{B}) > \tau$ é o circuito a ser verificado
- O limiar de similaridade τ é o parâmetro público
- As *embeddings* faciais representam os valores privados

Isso permite autenticação facial **sem revelar** os vetores faciais.

Vantagens do Método Proposto

O sistema de autenticação com provas de conhecimento zero traz benefícios significativos:

- **Privacidade Total:** o verificador não sabe quem é o usuário, apenas verifica se a prova é válida.
- **Resistência a Vazamentos:** nenhum dado biométrico é armazenado no sistema, por isso não há o que ser vazado ou roubado.

Referências


Nir Bitansky, Ran Canetti, Alessandro Chiesa, and Eran Tromer.
From extractable collision resistance to succinct non-interactive arguments of knowledge, and back again.
In *Proceedings of the 3rd Innovations in Theoretical Computer Science Conference*, ITCS '12, page 326–349, New York, NY, USA, 2012. Association for Computing Machinery.


Shafi Goldwasser, Silvio Micali, and Charles Rackoff.
The knowledge complexity of interactive proof systems.
SIAM Journal on Computing, 18(1):186–208, 1989.


Florian Schroff, Dmitry Kalenichenko, and James Philbin.
Facenet: A unified embedding for face recognition and clustering.
In *2015 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, page 815–823. IEEE, June 2015.

Muito obrigado!

UNIVERSIDADE FEDERAL
DE SANTA CATARINA