

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

Alex Davis Neuwiem da Silva

Novembro de 2025

O que é uma Prova de Conhecimento Zero?

- ▶ Permitem que uma parte (o provador) demonstre para outra (o verificador) que uma afirmação é verdadeira
- ▶ A propriedade de **conhecimento zero** garante que o verificador seja convencido sem revelar nenhuma informação adicional além da veracidade dessa afirmação

Exemplo de uma Prova de Conhecimento Zero

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

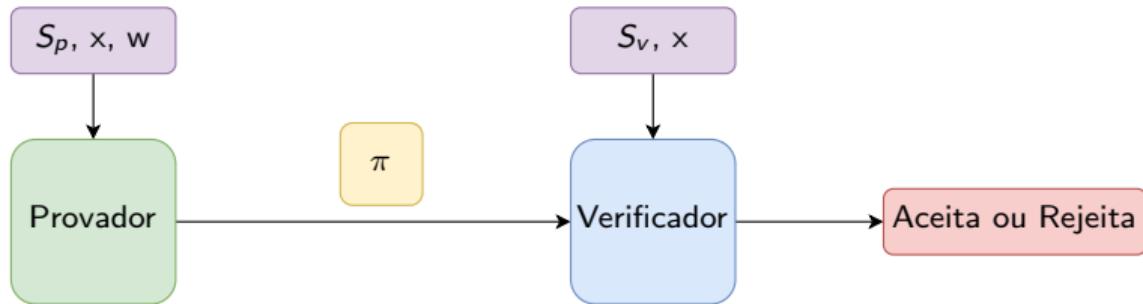
Cerimônia de Confiança sobre o circuito $C(x, w)$:

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

Um algoritmo que gera:

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

Processamento de uma prova



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.