The Incognito Conundrum

Challenges in Managing Private Identities

THE UNIVERSITY OF SYDNEY

Sam Polgar

spol2078@uni.sydney.edu.au

Supervisor: Qiang Tang

';--have i been pwned?

Check if your email address is in a data breach

sampolgar@gmail.com pwned?

Oh no — pwned!

Pwned in 8 data breaches and found no pastes (subscribe to search sensitive breaches)

Agenda

1. Privacy & Anonymous Credentials
2. Usecase Tradeoff between Usability and Privacy
3. Our Research

Why Privacy is Important

Incessant Phishing & SPAM

87% Population Identifiable by DOB, ZIP, Gender*

Cybercrime $10.5T P/A by 2025**

*https://privacytools.seas.harvard.edu/sites/projects.iq.harvard.edu/files/privacytools/files/paper1.pdf

**https://www.globenewswire.com/news-release/2020/11/18/2129432/0/en/Cybercrime-To-Cost-The-World-10-5-Trillion-Annually-By-2025.html

Anonymous Credentials aren’t new

Problem Identified
[Chaum, 1984]

324,000 Academic
Ref, Google Scholar

Commercialised
Products

Anonymous Credentials aren’t widely used

Additional Infrastructure

Behaviour Change

Our Goals

Privacy

- Unlinkability
- Selective Disclosure
- ZK Predicate Proofs

Private Accountability

- KYC Compliance
- Revocation

Usability

- Minimal Behaviour Change
- Minimal Infrastructure change
- Efficiency

Our Research

		Identity Provider	Anonymous Credentials	Our Research
Privacy	Unlinkability		✓	✓
	Anonymity		✓	✓
	Selective Disclosure		✓	✓
	ZK Predicate Proofs		✓	✓
Accountability	KYC Compliance	✓	✓	✓
	Revocation	✓	✓	✓
Usability	Min Behaviour Change	✓		✓
	Min Additional Infrastructure	✓		✓
	Efficiency	✓		✓

Agenda

1. Privacy & Anonymous Credentials
2. Usecase Tradeoff between Usability and Privacy
3. Our Research

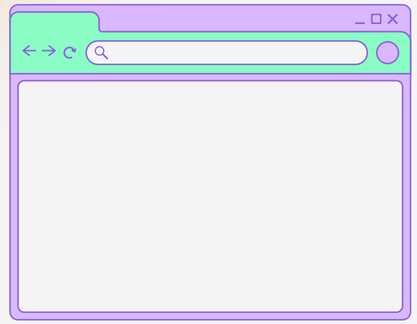
Scenario

A user accessing a R18+ movie online needs to prove they’re over 18 years old and Australian

User

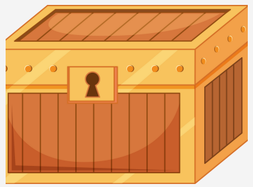
Issuer

Service NSW



Verifier

Cryptography



Commitment

“Locked box” for securely hiding user attributes. Once locked it can’t be changed, but can be opened by a user

Digital Signature

Verifiable signature over messages

Blind Signature

Verifiable signature over hidden messages

Zero Knowledge Proof (ZKP)

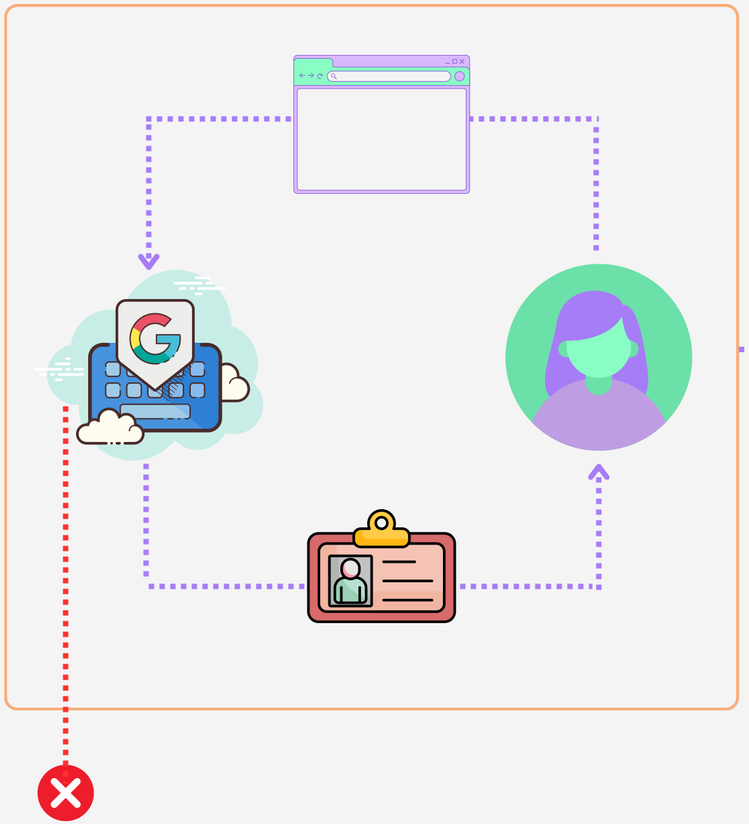
Used to prove your credential attributes without sharing information about them. E.g. “age over 18”

zkSNARK (Succinct ZKP)

Used to prove large computations with a small proof

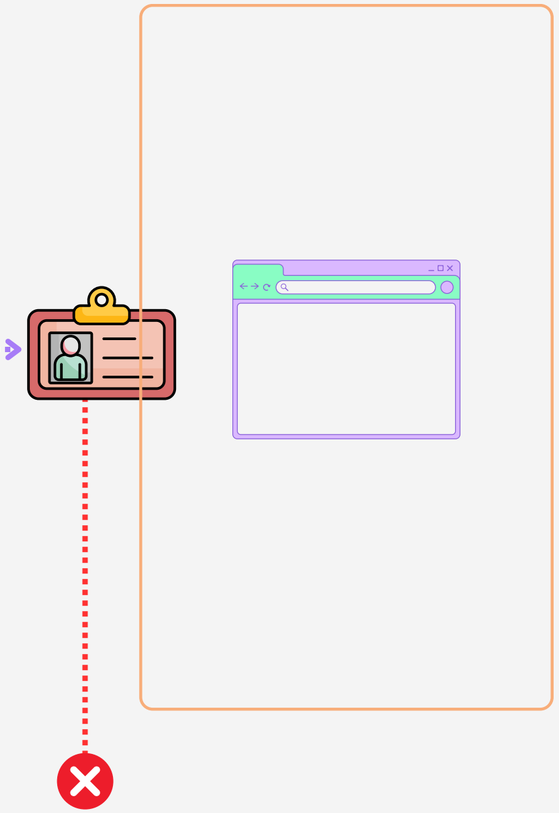
Identity Provider: 3 Party Protocol

Login



Issuer Unlinkability

Verify



Verifier Unlinkability
+ Selective Disclosure
+ Expressive Verification

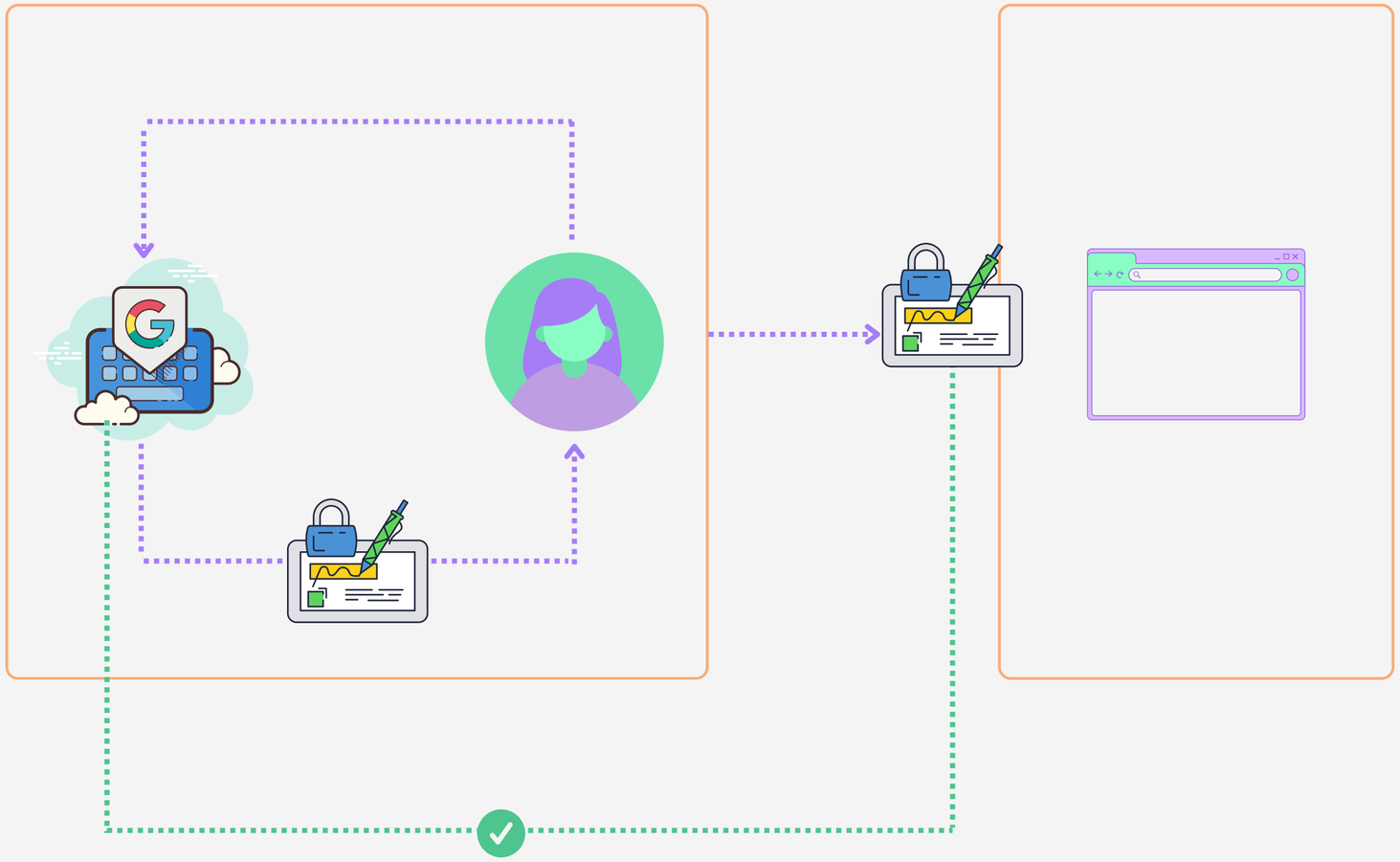
Properties

Unlinkability	✗
Anonymity	✗
Selective Disclosure	✗
ZK Predicate Proofs	✗
KYC Compliance	✓
Revocation	✓
Min Behaviour Change	✓
Min Additional Infrastructure	✓
Efficiency	✓

Privacy Improvement - Digital Signature

Issue

Verify

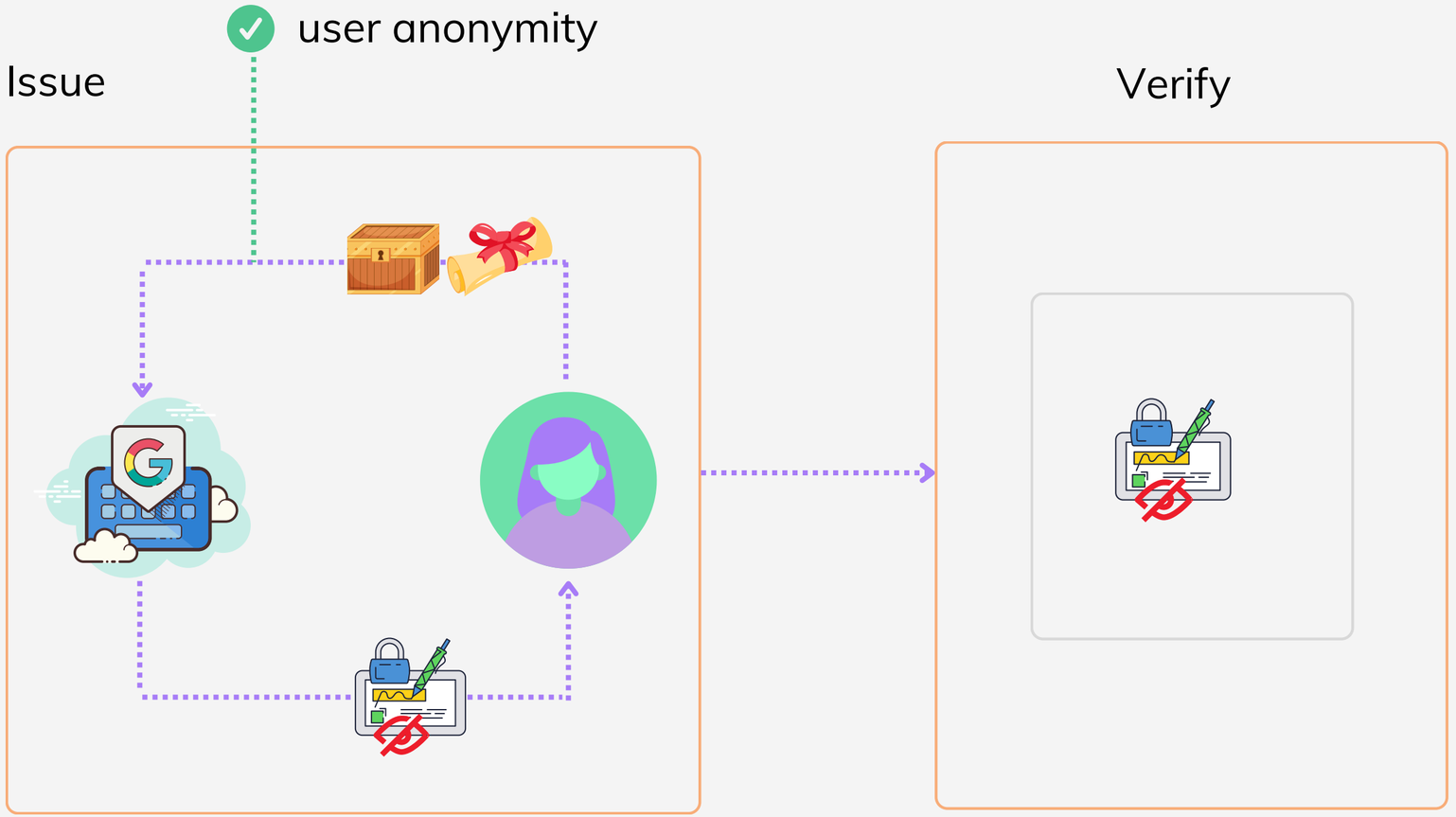


Issuer can’t track credential usage

Properties

Unlinkability	✓
Anonymity	✗
Selective Disclosure	✗
ZK Predicate Proofs	✗
KYC Compliance	✗
Revocation	✗
Min Behaviour Change	✗
Min Additional Infrastructure	✗
Efficiency	✗

Privacy Improvement - Blind Signature



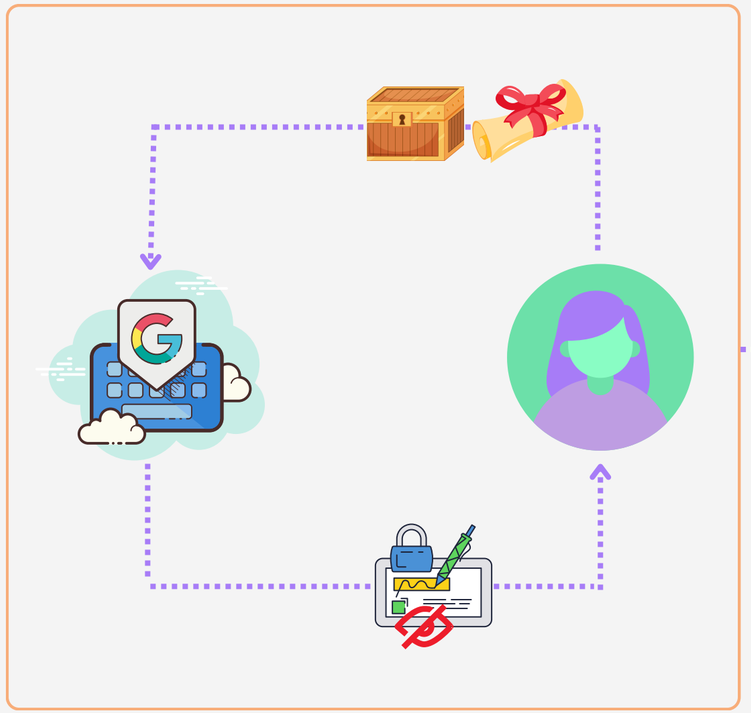
Properties

Unlinkability	✓
Anonymity	✓
Selective Disclosure	✗
ZK Predicate Proofs	✗
KYC Compliance	✗
Revocation	✗
Min Behaviour Change	✗
Min Additional Infrastructure	✗
Efficiency	✗

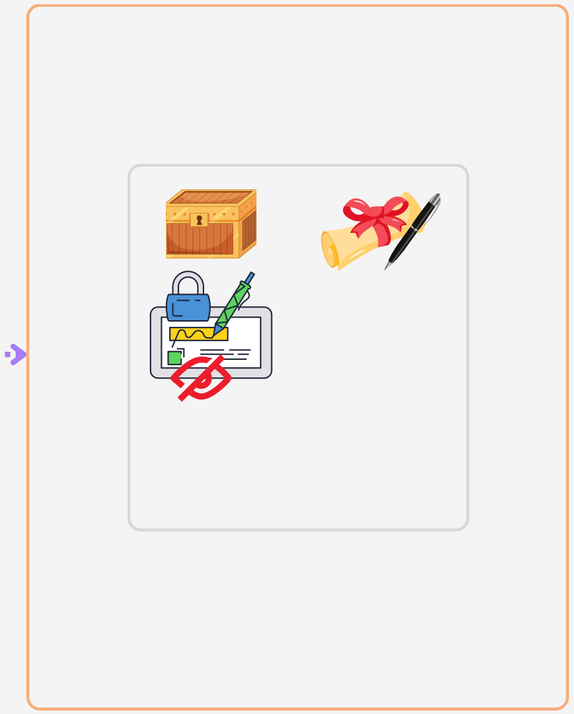
Privacy Improvement - Selective Disclosure

Blind Signature + ZK Proofs

Issue



Verify



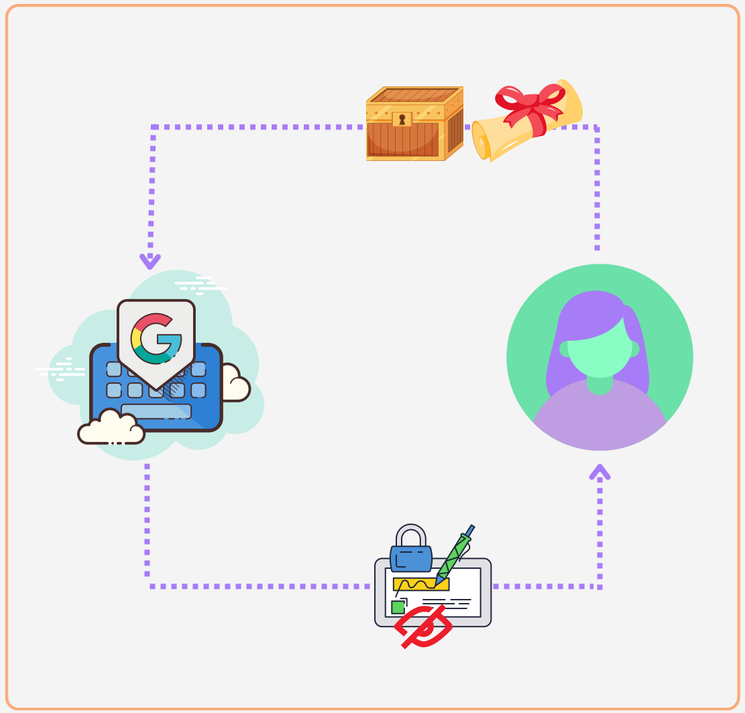
Properties

Unlinkability	✓
Anonymity	✓
Selective Disclosure	✓
ZK Predicate Proofs	✗
KYC Compliance	✗
Revocation	✗
Min Behaviour Change	✗
Min Additional Infrastructure	✗
Efficiency	✗

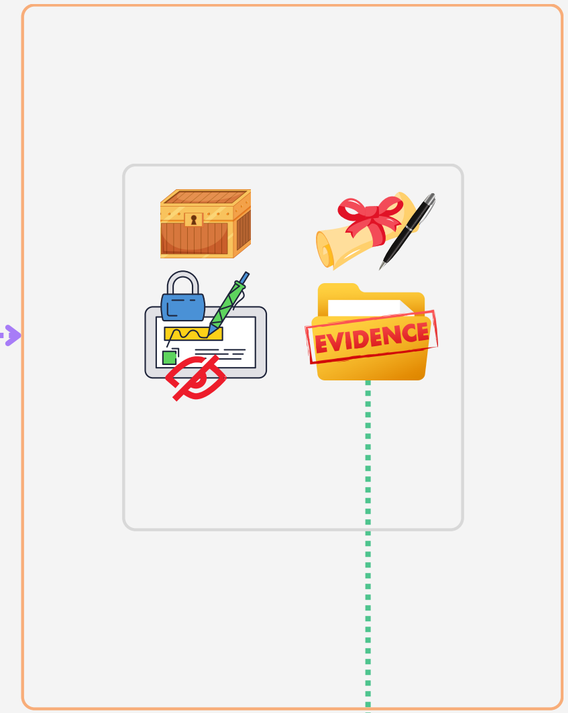
Privacy Improvement - ZK Predicate Proofs

Blind Signature + ZK Proofs + zkSNARK Proof

Issue



Verify

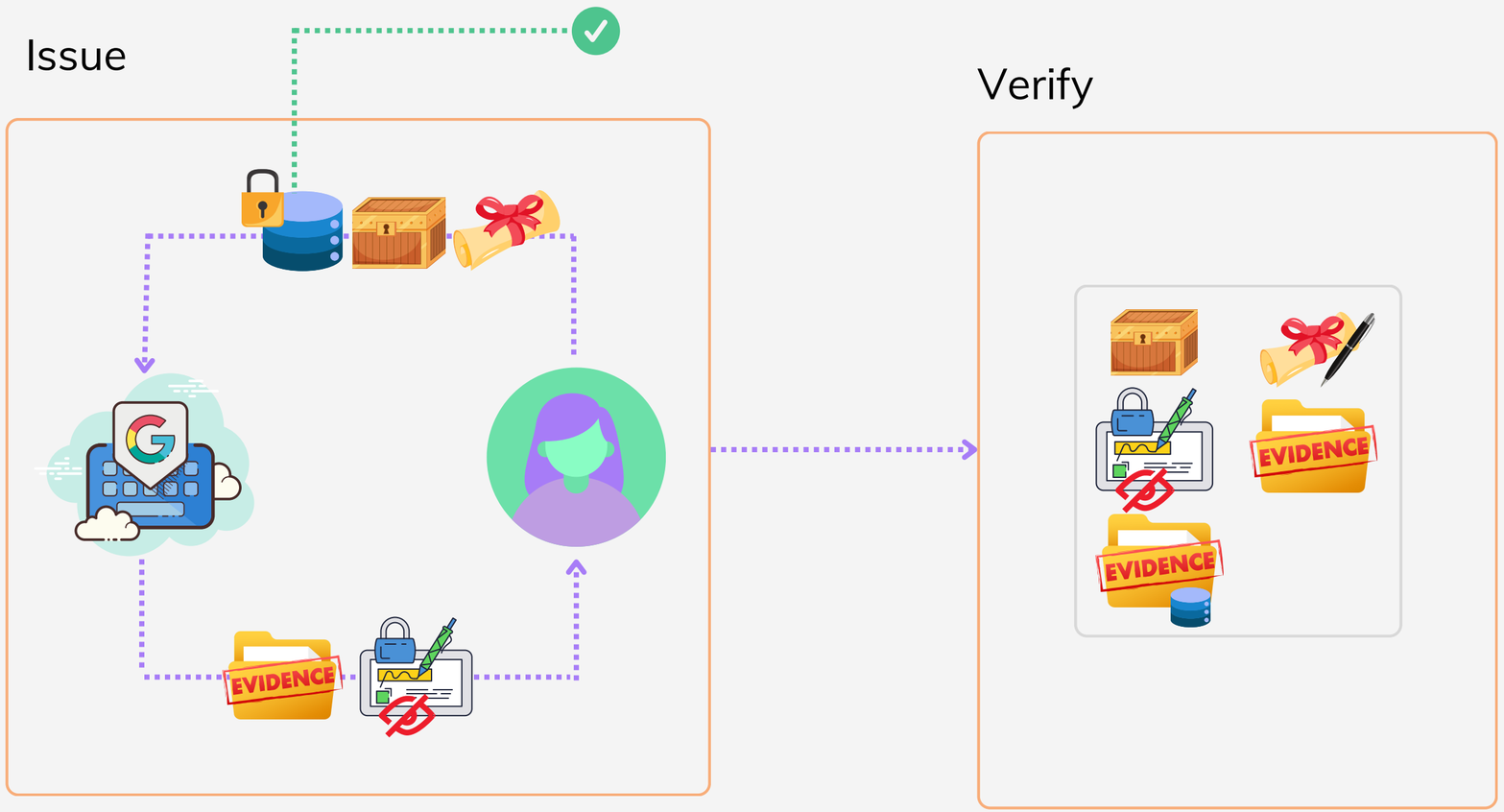


Properties

Unlinkability	✓
Anonymity	✓
Selective Disclosure	✓
ZK Predicate Proofs	✓
KYC Compliance	✗
Revocation	✗
Min Behaviour Change	✗
Min Additional Infrastructure	✗
Efficiency	✗

Accountability Improvement - KYC Compliance

Blind Signature + ZK Proofs + zkSNARK Proofs + Private Computation



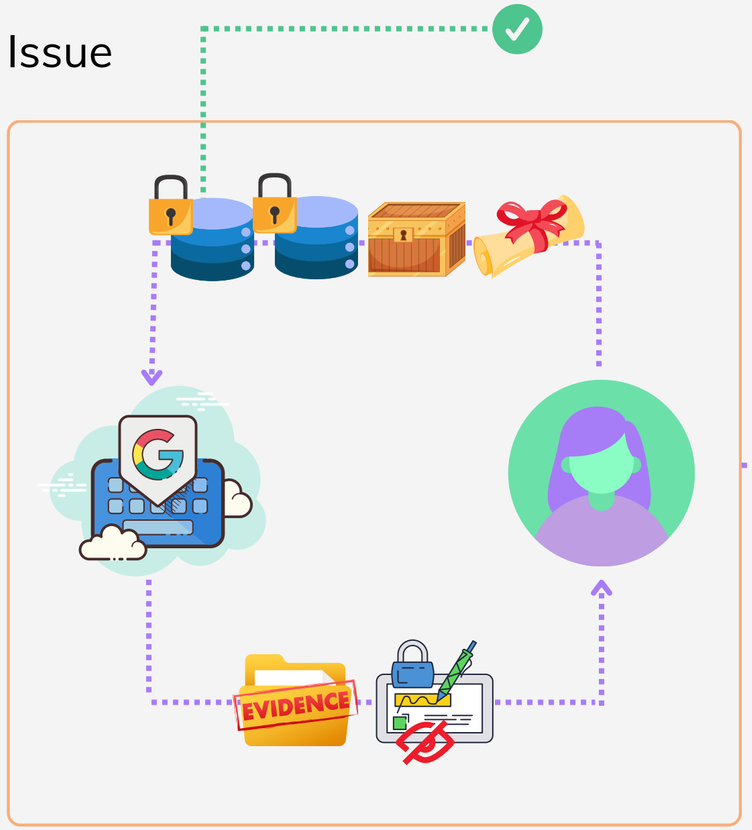
Properties

Unlinkability	✓
Anonymity	✓
Selective Disclosure	✓
ZK Predicate Proofs	✓
KYC Compliance	✓
Revocation	✗
Min Behaviour Change	✗
Min Additional Infrastructure	✗
Efficiency	✗

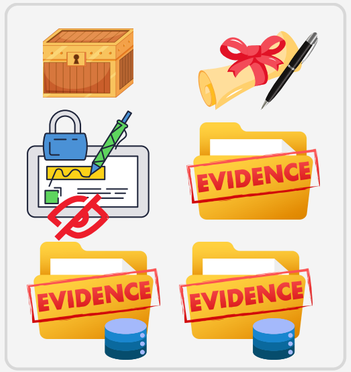
Accountability Improvement - Revocation

Blind Signature + ZK Proofs + zkSNARK Proofs + Private Computation

Issue



Verify

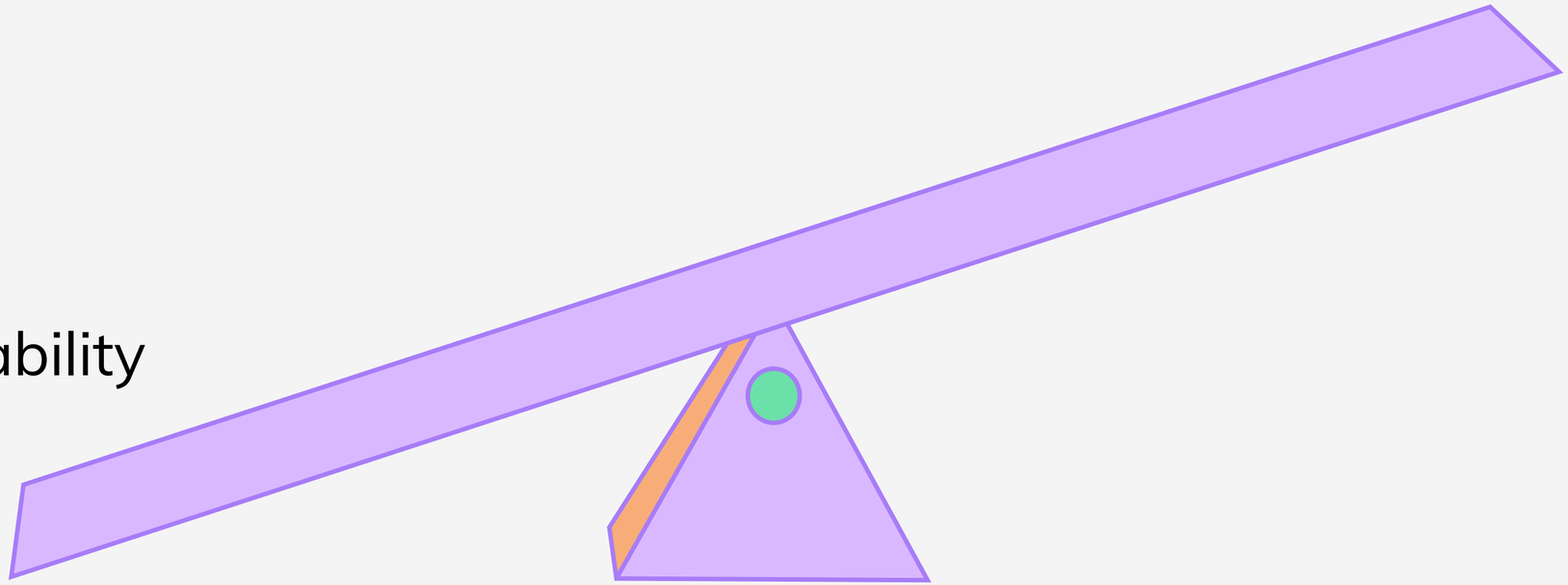


Properties

Unlinkability	✓
Anonymity	✓
Selective Disclosure	✓
ZK Predicate Proofs	✓
KYC Compliance	✓
Revocation	✓
Min Behaviour Change	✗
Min Additional Infrastructure	✗
Efficiency	✗

The Incognito Conundrum

Privacy +
Accountability



Usability

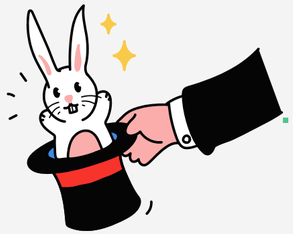
Agenda

1. Privacy & Anonymous Credentials
2. Usecase Tradeoff between Usability and Privacy
3. Our Research

Our Research

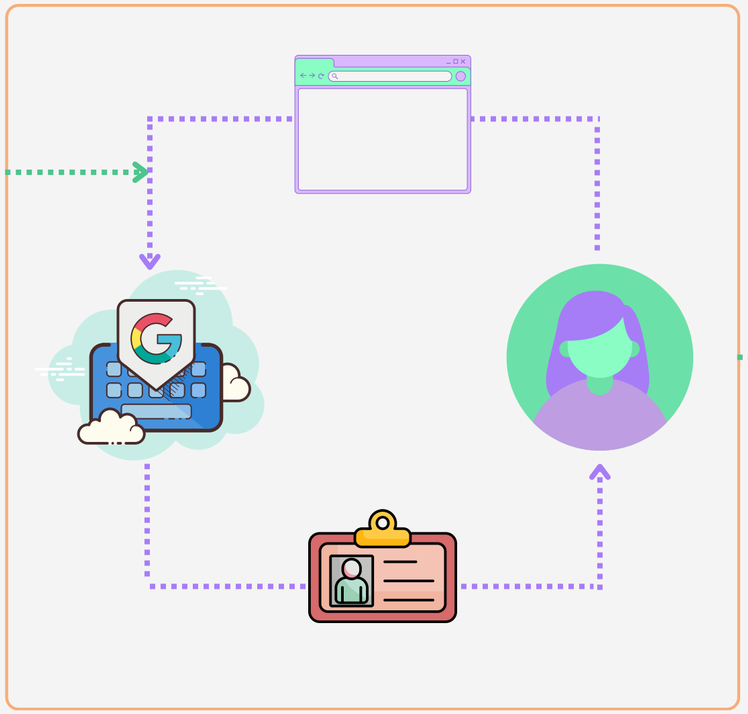
	Identity Provider	Anonymous Credentials	Our Research
Unlinkability		✓	✓
Anonymity		✓	✓
Selective Disclosure		✓	✓
ZK Predicate Proofs		✓	✓
KYC Compliance	✓	✓	✓
Revocation	✓	✓	✓
Min Behaviour Change	✓		✓
Min Additional Infrastructure	✓		✓
Efficiency	✓		✓

Our Research



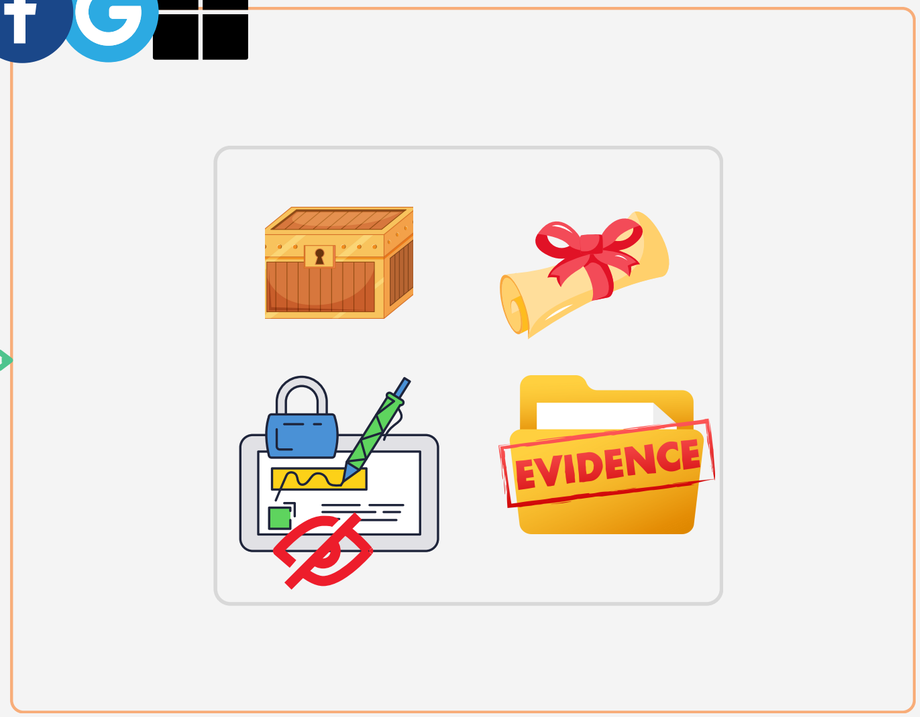
Nonce trick

zkLogin [BKJ, 2024]



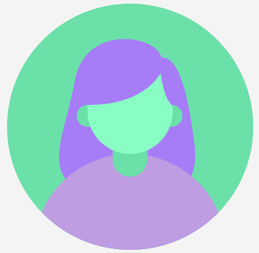
Generate anonymous signing key
from existing OAuth provider

My Contribution



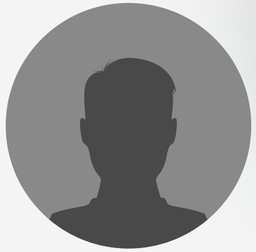
Generate fully featured Anonymous Credential
from multiple identity providers

Summary and Conclusion



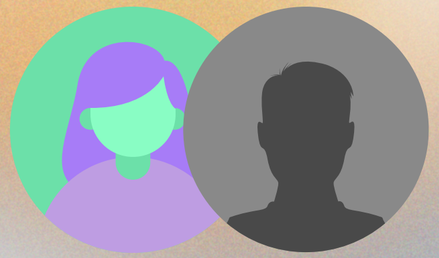
zkLogin [BKJ, 2024]

Solves the usable privacy problem
Creates Anonymous Signing Key & partial credential from Existing OAuth Infrastructure piggy-backing on Trust and Accountability



Enhance with Anonymous Credentials

Solves the privacy functionality problem
By aggregating zkLogin tokens and compiling into a fully featured Anonymous Credential



zkLogin Credentials

Usable Anonymous Credentials without additional infrastructure or major behaviour change.

Questions

Thank you to

- Dr Qiang Tang
- Dr Alberto Sonnino - Mysten Labs for the idea to blend zkLogin with Coconut Credentials
- Everyone who helped review and improve this presentation

THE UNIVERSITY OF SYDNEY

Sam Polgar

spol2078@uni.sydney.edu.au

Supervisor: Qiang Tang