Interactive ZK is Blazingly Fast

Weikeng Chen, Research Partner

L2IV

Disclaimer

This presentation is prepared by L2 Iterative Ventures ("L2IV") for informational purposes only.

All information contained in this presentation is not intended for use by persons located in or residing in jurisdiction that restricts the distribution of such information by L2IV. The information contained in this presentation does not constitute a distribution, an offer to buy or the solicitation of any offer to buy or sell any securities in any jurisdiction where such a distribution or offer would be illegal.

The products and services mentioned in this presentation (the "Product") have not been authorized by Securities and Futures Commission (the "SFC") to be marketed to the general public. Information contained herein this presentation has not been reviewed by the SFC.

None of the information contained in this presentation constitute an invitation or solicitation to invest in any shares of units of the Products; nor does it constitute any investment advice or recommendation to acquire or dispose of any investment or to engage in any transactions. Before acting on any information in this presentation, you should consider whether any investment, security or strategy is suitable for your particular circumstances and, if necessary, seek independent professional advice.

Investment involves risks. The price of units or shares of the Products may go up as well as down. Past performance is not indicative of future results. The value of the Products can be volatile and could go down substantially within a short period of time. It is possible that the entire value of your investment could be lost. Please read the Products' relating documents for details and risk factors of the Products.

All information contained in this presentation is published to the best of the knowledge and belief of L2IV to be accurate at the time it was posted. No representation or warranty, expressed or implied is made by L2IV as to its accuracy or completeness of the information. L2IV, its affiliates, directors, officers or employees accept no liability for any errors or omissions relating to information available in this presentation and will not be liable for any damages or costs arising out of or in anyway connected with the use of the information provided in this presentation.

Note: Cover photos are generated from Midjourney AI.

L2IV

01 | What is IZK? P.5

02 | Advances in IZK research P.10

03 | Application: verifying Web2 data P.15

04 | Application: detecting bias in confidential computing P.24

05 | Future directions P.28

Content

01| What is IZK?

Interactive zero-knowledge proofs

A “magical” cryptographic tool to prove without revealing secrets

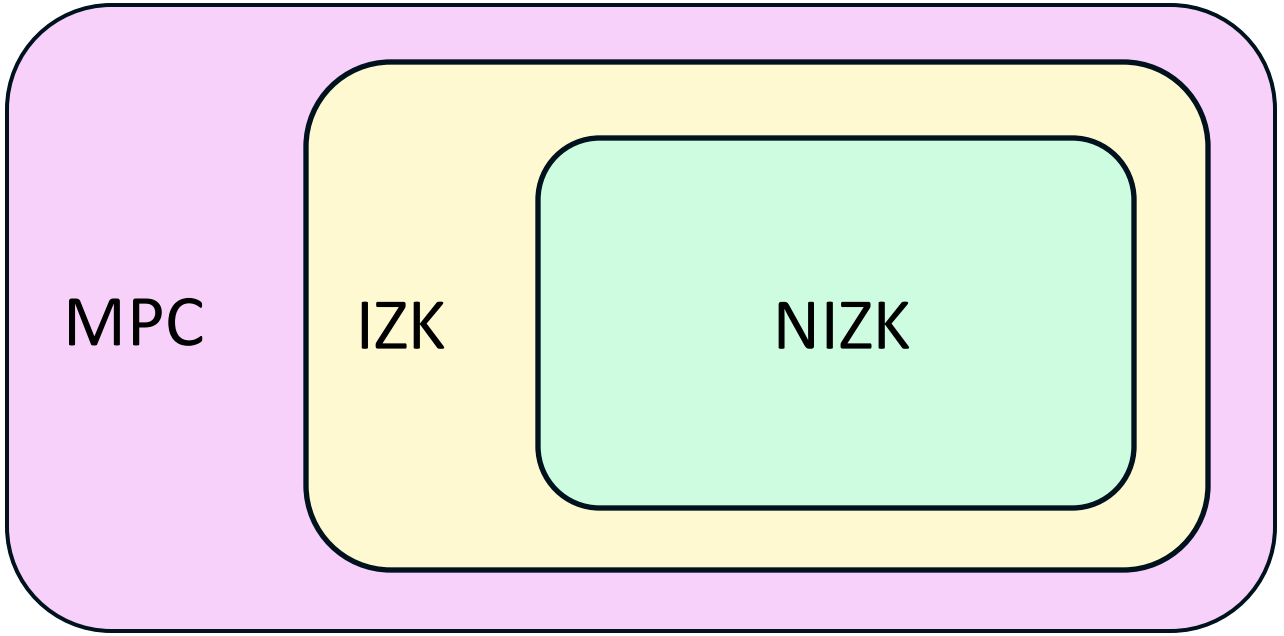
(source: https://bit.ly/izk-logo)

Interactive:
A phone call, not an email. It is a conversation happening between two parties in real time.

Zero-knowledge:
Prover can hide certain information even if it is needed for proving.

Proofs:
Prover cannot lie.

Compare IZK with MPC and NIZK



IZK is a special case of MPC:

- IZK has only two parties.
- IZK only allows one party (“Prover”) to give data.
- Anything that IZK can do, MPC can do.

NIZK is a special case of IZK:

- NIZK is “email”, which can be considered as a special case of a “phone call”.
- Anything that NIZK can do, IZK can do.

Why do we need IZK?

One can argue that:

- Most ZK use cases can be proven in NIZK. One can just use **NIZK**.
- Any IZK can be instantiated with MPC. One can just use **MPC**.

The reason is **performance**.

The paper [CSCKP23] "HOLMES: Efficient Distribution Testing for Secure Collaborative Learning" (USENIX Security 2023) gives the following benchmark.

Type	Time (s)	Compared with IZK
IZK (using QuickSilver)	57.3	1x
NIZK (using Spartan)	2602	45x
SNARK (using Spartan)	20752	362x
MPC (using MP-SPDZ + SCALE-MAMBA)	2064	36x

Limitations of IZK

IZK is only for proving, but not confidential computing.

MPC can compute on both parties (or more parties)' confidential data.

$$y = f(x_{\text{Alice}}, x_{\text{Bob}})$$

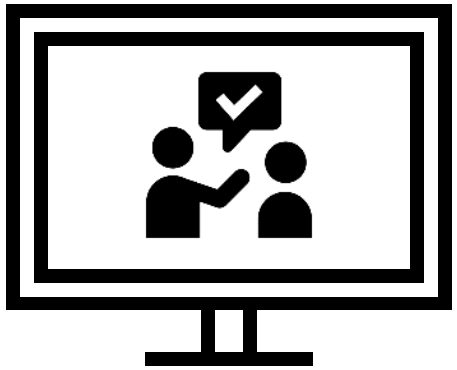
IZK is one party proving to another party.

$$g(x_{\text{Alice}}, y) = 1$$

Limitations of IZK

IZK is interactive, which limits its usage in blockchain.

Only the verifier presented at the time of the interaction of IZK can trust the results.



A third party, not involved in the interaction, cannot be convinced by a transcript of the conversations. This is similar to a video recording that can be deepfaked and not realiable.

This can be both an advantage or a disadvantage.

02| Advances in IZK research

Earliest ZK work is IZK

[GMR86] The Knowledge Complexity of Interactive Proof Systems (FOCS 1986)
Shafi Goldwasser, Silvio Micali, Charles Rackoff

[IY87] Direct Minimum-Knowledge Computations (CRYPTO 1987)
Russell Impagliazzo, Moti Yung

[GMW86] Proofs that Yield Nothing But Their Validity All Languages in NP Have Zero-Knowledge Proof Systems (FOCS 1986)
Oded Goldreich, Silvio Micali, Avi Wigderson

[BGGHKMR88] Everything Provable is Provable in Zero-Knowledge (CRYPTO 1988)
Michael Ben-Or, Oded Goldreich, Shafi Goldwasser, Johan Hastad, Joe Kilian, Silvio Micali, Phillip Rogaway

IZK

NIZK

[BFM88] Non-Interactive Zero-Knowledge and its Applications (STOC 1988)
Manuel Blum, Paul Feldman, Silvio Micali

SNARK

[Micali94] Computationally Sound Proofs (FOCS 1994)
Silvio Micali

Resurgence of IZK

[JKO13] Zero-Knowledge Using Garbled Circuits, or How to Prove Non-Algebraic Statements Efficiently (CCS 2013)
Marek Jawurek, Florian Kerschbaum, Claudio Orlandi

[ZER15] Two Halves Make a Whole: Reducing Data Transfer in Garbled Circuits using Half Gates (EUROCRYPT 2015)
Samee Zahur, Mike Rosulek, David Evans

[FNO14] Privacy-free garbled circuits with applications to efficient zero-knowledge (EUROCRYPT 2014)
Tore Kasper Frederiksen, Jesper Buus Nielsen, Claudio Orlandi

[HK20] Stacked Garbling for Disjunctive Zero-Knowledge Proofs (EUROCRYPT 2020)
David Heath and Vladimir Kolesnikov

Before silent vector oblivious linear evaluation

After silent vector oblivious linear evaluation

[DIO21] Line-Point Zero Knowledge and Its Applications
(ITC 2021) **Samuel Dittmer, Yuval Ishai, and Rafail Ostrovsky**

[WYKW21] Wolverine: Fast, Scalable, and Communication-Efficient Zero-Knowledge Proofs for Boolean and Arithmetic Circuits
(S&P 2021) **Chenkai Weng, Kang Yang, Jonathan Katz, Xiao Wang**

[BMRS21] Mac'n'Cheese: Zero-Knowledge Proofs for Boolean and Arithmetic Circuits with Nested Disjunctions
(CRYPTO 2021) **Carsten Baum, Alex J. Malozemoff, Marc B. Rosen, Peter Scholl**

…and then more optimization toward real-world applications

Instead of multiplication gates, think **low-degree polynomials**, e.g., $f(x_1, x_2, x_3) = x_1 x_2 x_3 + 2x_1 x_3 + x_2$.

[YSWW21] QuickSilver: Efficient and Affordable Zero-Knowledge Proofs for Circuits and Polynomials over Any Field (CCS 2021)
Kang Yang, Pratik Sarkar, Chenkai Weng, Xiao Wang

Switch prime fields during proof generation

[BBMRS21] Appenzeller to Brie: Efficient Zero-Knowledge Proofs for Mixed-Mode Arithmetic and F2k (CCS 2021)
Carsten Baum, Lennart Braun, Alexander Munch-Hansen, Benoit Razet, Peter Scholl

[WYXKW21] Mystique: Efficient Conversions for Zero-Knowledge Proofs with Applications to Machine Learning (USENIX Security 2021)
Chenkai Weng, Kang Yang, Xiang Xie, Jonathan Katz, Xiao Wang

Handling **repeated** computation

[WYYXW22] AntMan: Interactive Zero-Knowledge Proofs with Sublinear Communication (CCS 2022)
Chenkai Weng, Kang Yang, Zhaomin Yang, Xiang Xie, Xiao Wang

Source: **[BDSW23]** SoK: Vector OLE-Based Zero-Knowledge Protocols. (Designs, Codes and Cryptography 2023)
Carsten Baum, Samuel Dittmer, Peter Scholl, Xiao Wang

Two papers to discuss

Application: verifying Web2 data

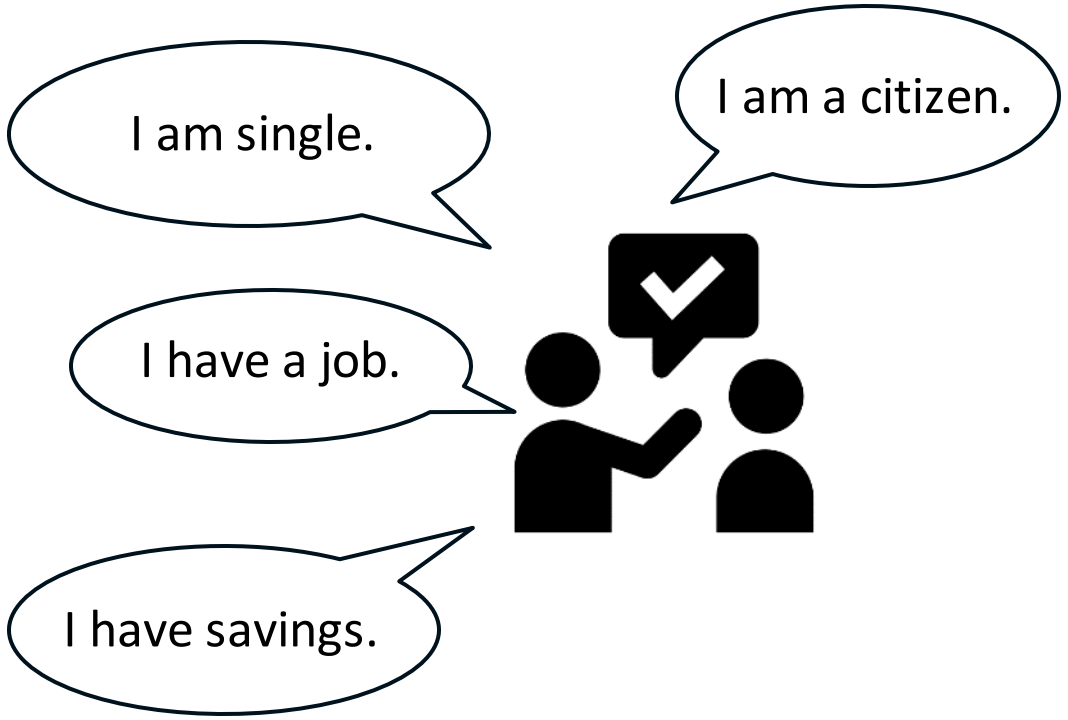
Lightweight Authentication of Web Data via Garble-Then-Prove (in submission to USENIX Security 2024)
Xiang Xie, Kang Yang, Xiao Wang, Yu Yu

Application: detecting bias in federated learning

HOLMES: Efficient Distribution Testing for Secure Collaborative Learning (USENIX Security 2023)
Ian Chang, Katerina Sotiraki, Weikeng Chen, Murat Kantarcioglu, Raluca Ada Popa

03| Application: verifying Web2 data

What is zero-knowledge in the real world?



Many are provable from Web2 using MPC with IZK

I am single.

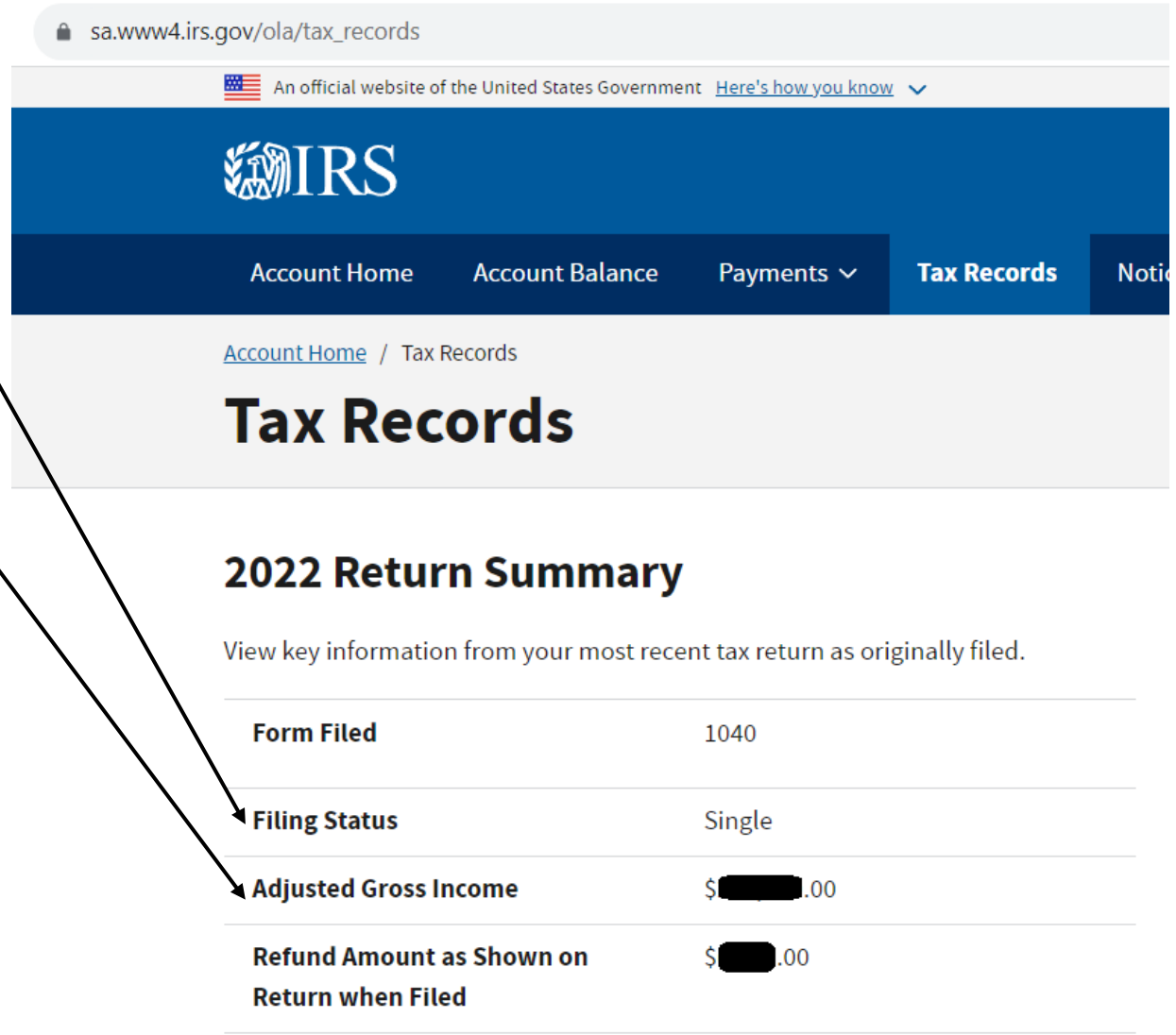
- verify IRS tax return's filing status (single or head of household vs. married filing jointly/separately)

I have a job.

- verify IRS tax return's income.

Recipe:

- Prove the ownership of a unique account on the IRS website
- Prove the HTTPS response from the IRS server showing the claimed data



Many are provable from Web2 using MPC with IZK

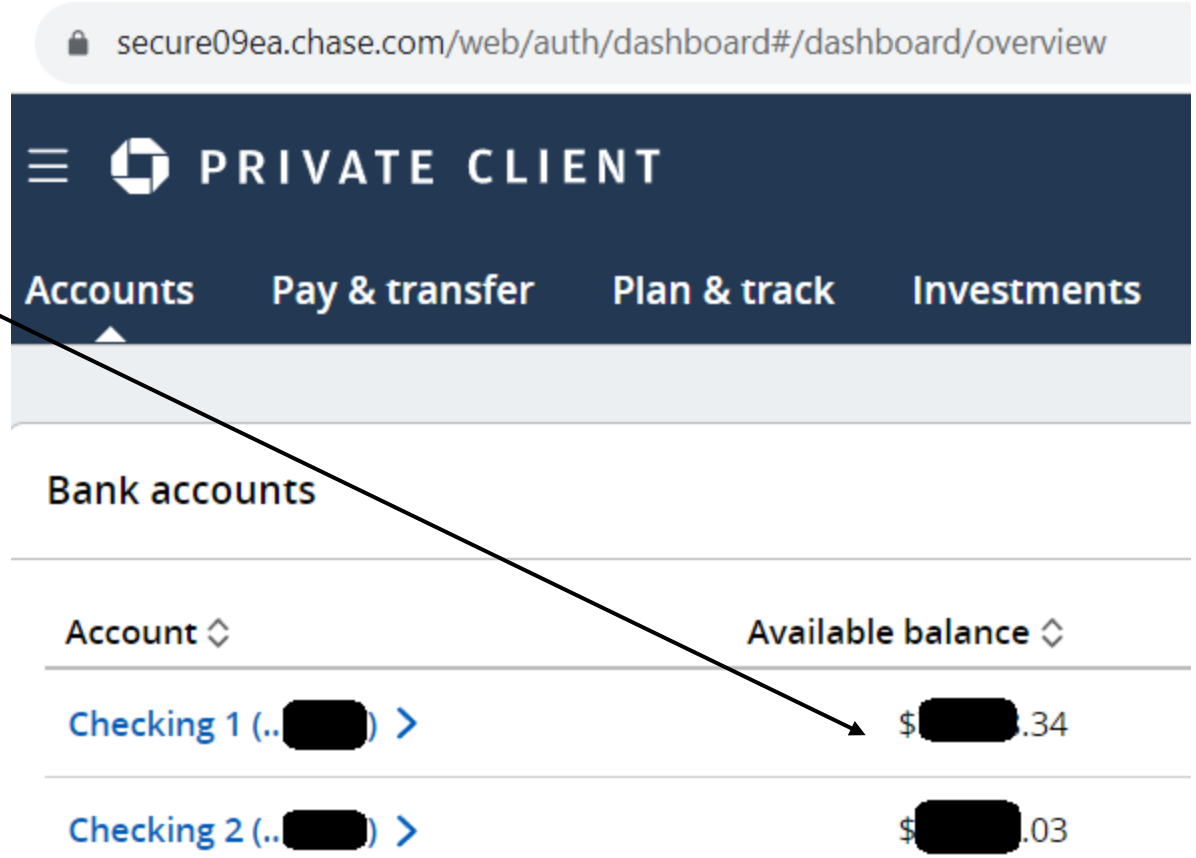
I have savings.

- prove the account balances in the bank website after the user logs in

Recipe:

- Prove the ownership of a unique bank account
- Prove the HTTPS response from the bank's web server showing the claimed data

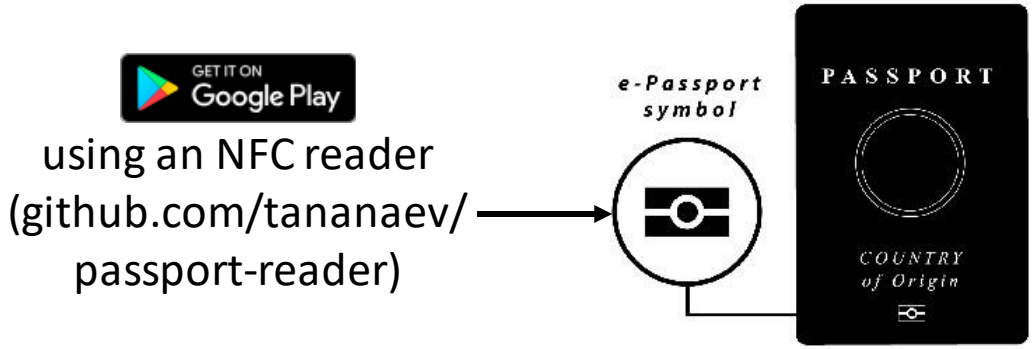
Although JP Morgan Chase does have developer API (https://developer.chase.com/), the permission is not fine-grained -- authorized apps can see the customer's home address, phone number, and email address, and it is currently available to existing partners only.



Citizenship can be proven using IZK

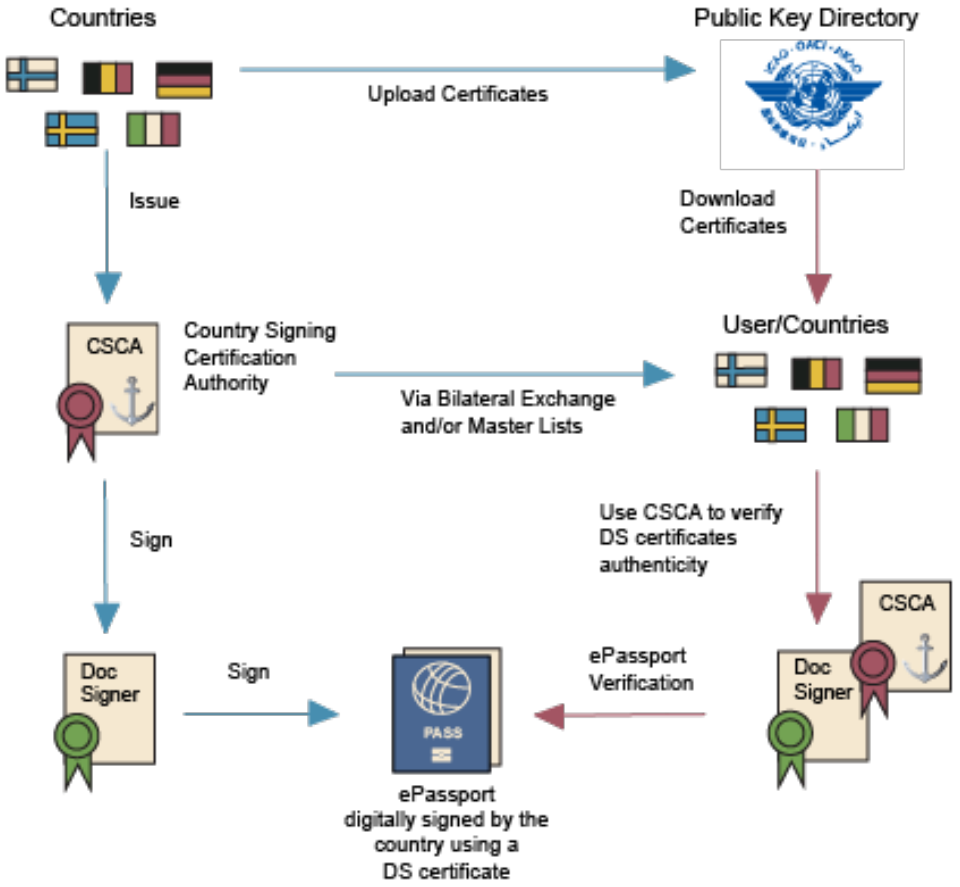
I am a citizen.

- prove a valid e-passport (now in 173 countries)



Recipe:

- Prove that the passport is issued by a country, by using IZK (or NIZK, or SNARK)
  Prove only necessary data



[RWGM23] zk-creds: Flexible Anonymous Credentials from zkSNARKs and Existing Identity Infrastructure (IEEE S&P 2023)
Michael Rosenberg, Jacob White, Christina Garman, Ian Miers

Source: International Civil Aviation Organization. https://www.icao.int/Security/FAL/PKD/Pages/ePassport-Basics.aspx

Technology

(The landmark paper)

[ZMMGJ20] DECO: Liberating Web Data Using Decentralized Oracles for TLS (CCS 2020)
Fan Zhang, Sai Krishna Deepak Maram, Harjasleen Malvai, Steven Goldfeder, Ari Juels

DECO consists of **MPC** and **NIZK**.

Replace NIZK with IZK, 45x improvement

[WYKW21] Wolverine: Fast, Scalable, and Communication-Efficient Zero-Knowledge Proofs for Boolean and Arithmetic Circuits (S&P 2021)
Chenkai Weng, Kang Yang, Jonathan Katz, Xiao Wang

Improvement on IZK, 7x improvement

[YSWW21] QuickSilver: Efficient and Affordable Zero-Knowledge Proofs for Circuits and Polynomials over Any Field (CCS 2021)
Kang Yang, Pratik Sarkar, Chenkai Weng, Xiao Wang

Replace MPC with semi-honest MPC + IZK, 15x improvement

[XYWY24] Lightweight Authentication of Web Data via Garble-Then-Prove (in submission to USENIX Security 2024)
Xiang Xie, Kang Yang, Xiao Wang, Yu Yu

Concurrently, in the industry…

Brave Browser has been working on this for two years and…

> **[CDHPR24]** DiStefano: Decentralized Infrastructure for Sharing Trusted Encrypted Facts and Nothing More (in submission)
> **Sofía Celi, Alex Davidson, Hamed Haddadi, Gonçalo Pestana, Joe Rowell**

…they might be able to ship it to production in one year or two.

TLS Notary, under Privacy & Scaling Exploration, is a grant recipient from Etherum Foundation.

The core contributor, Dan  (GitHub: themighty1) has been working on this project for 9 years, starting from 2014.

Applications in Web3

Preventing airdrop Sybil attack:
Making it difficult for a user to create multiple identities.
Very important for protecting token prices.

APTOS
ARBITRUM

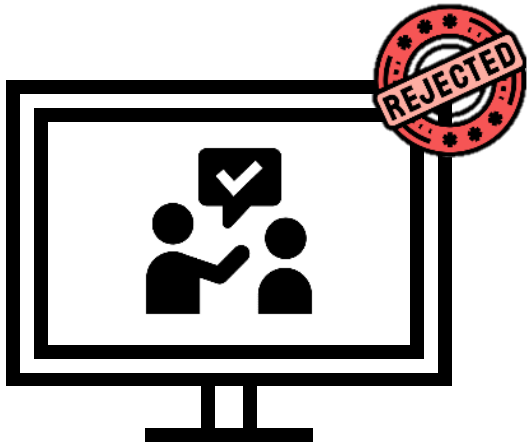
ZK-ID or ZK-KYC:
Proving that the user can legally use this DeFi services and is not on any sanction list, without sending photos of IDs.

polygon ID
WORLDCOIN

IPs and other real-world assets on chains:
Establishing the offchain identities with the onchain identities in a decentralized manner.

STORY PROTOCOL
Chainlink

Why interaction can be an advantage over NIZK/SNARK?



IZK is not “recordable”. A transcript of the conversations in the IZK protocol does not prove anything.

↓

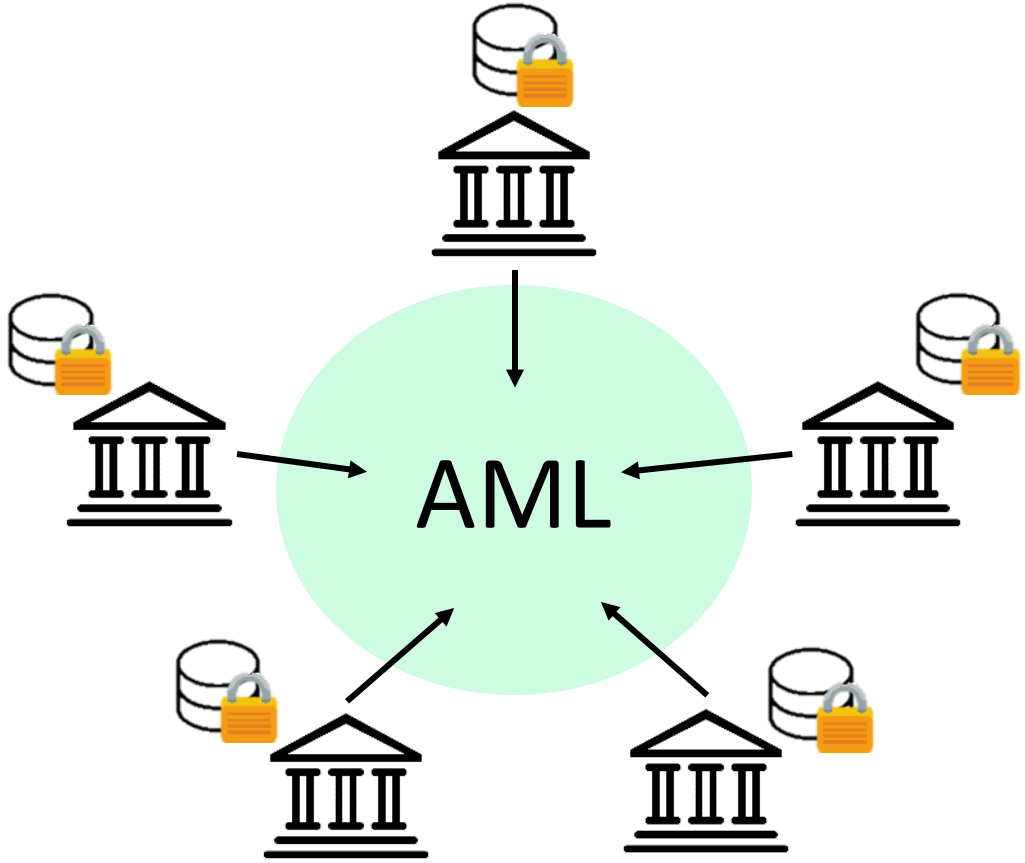
The verifier cannot convince a third party with the conversations.

↓

Off-the-record, deniability

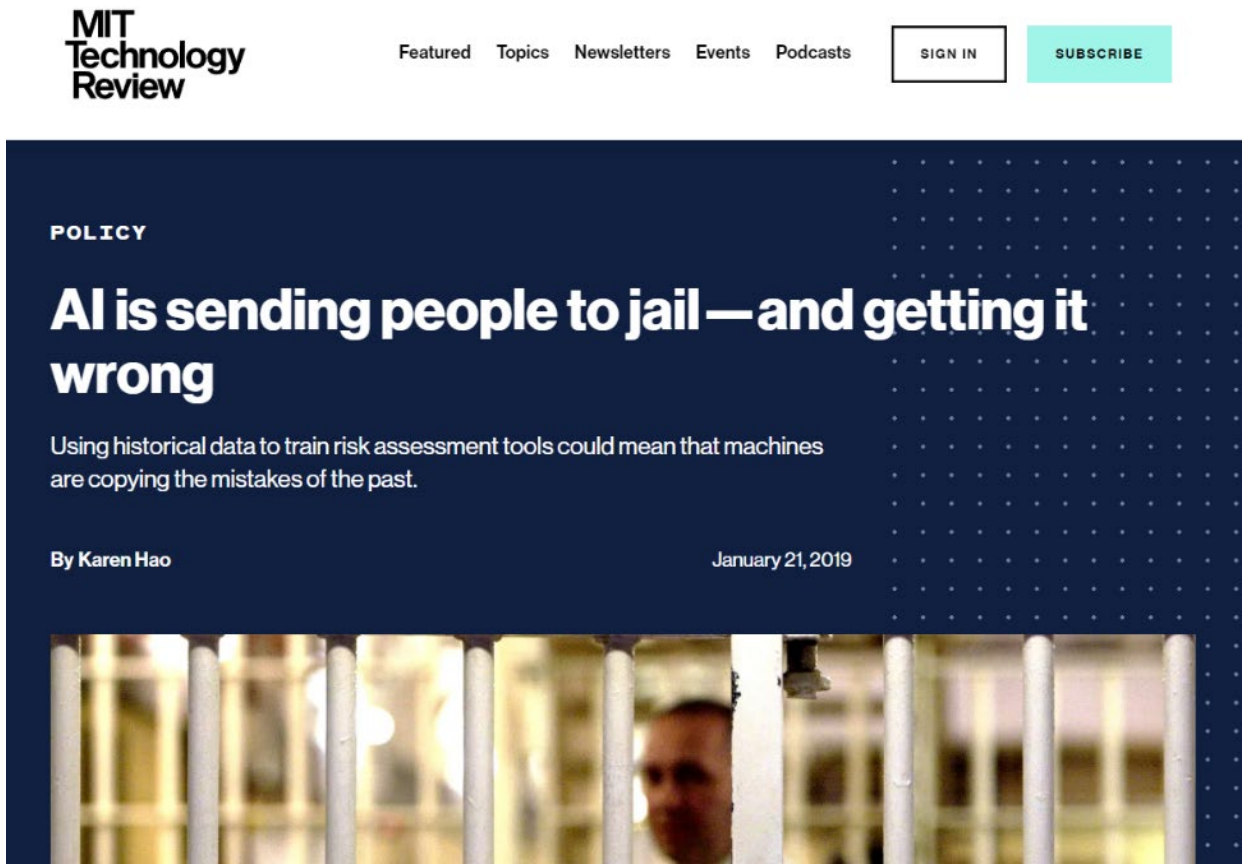
04| Application: detecting bias in confidential computing

Secure federated learning, inference, or data analytics



Source: Ernst & Young's Presentation "Application of confidential computing to Anti Money Laundering in Canada" in Confidential Computing Summit. https://drive.google.com/file/d/19TRiKjmVlPXPBsYtLc_CGcEU_wLe44ML/view

Bias detection



A critical question when AI models are used to affect human beings

fairness

⇩

Training data must be **balanced**: different groups are represented in the dataset appropriately.

IZK for detecting bias

[CSCKP23] HOLMES: Efficient Distribution Testing for Secure Collaborative Learning (USENIX Security 2023)
Ian Chang, Katerina Sotiraki, Weikeng Chen, Murat Kantarcioglu, Raluca Ada Popa

Baseline: about 19 years

↓ Replace MPC with IZK, 186x improvement

IZK: about 41 days

↓ Use mathematical sketching in IZK, 11678x improvement

IZK + Application-specific IZK protocols: about 5 minutes

IZK provides a playground for new, emerging application-specific protocols.

Benchmark is done with 10 parties on four-dimensional dataset consisting of 500k records, with 50 classes per dimension.

05| Future Directions

Hardware acceleration for IZK verifiers

Very soon when IZK applications start to emerge, scalability would be an issue.

APTOS

ARBITRUM

polygon ID

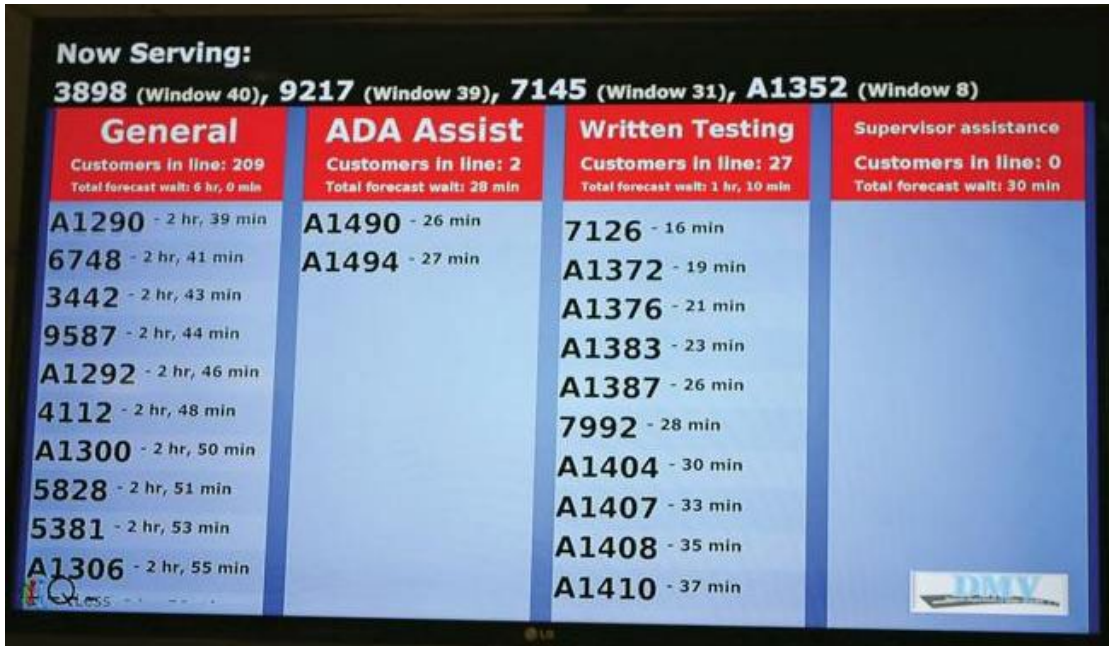
WORLDCOIN

STORY PROTOCOL

Chainlink

Hardware acceleration for IZK verifiers

Interaction can mean **wait**



Working hours and Types of Service

	General Service Hours
11/09 (Monday)	Full
12/09 (Tuesday)	Full
13/09 (Wednesday)	Full
14/09 (Thursday)	Full
15/09 (Friday)	Full
16/09 (Saturday)	Full
18/09 (Monday)	Full
19/09 (Tuesday)	Full
20/09 (Wednesday)	Full
21/09 (Thursday)	Full
22/09 (Friday)	Full

Our take: MPC and IZK are currently fully in CPU. Our experience in ZKP hardware acceleration on GPU suggests that there can be a significant performance improvement with GPU and FPGA.

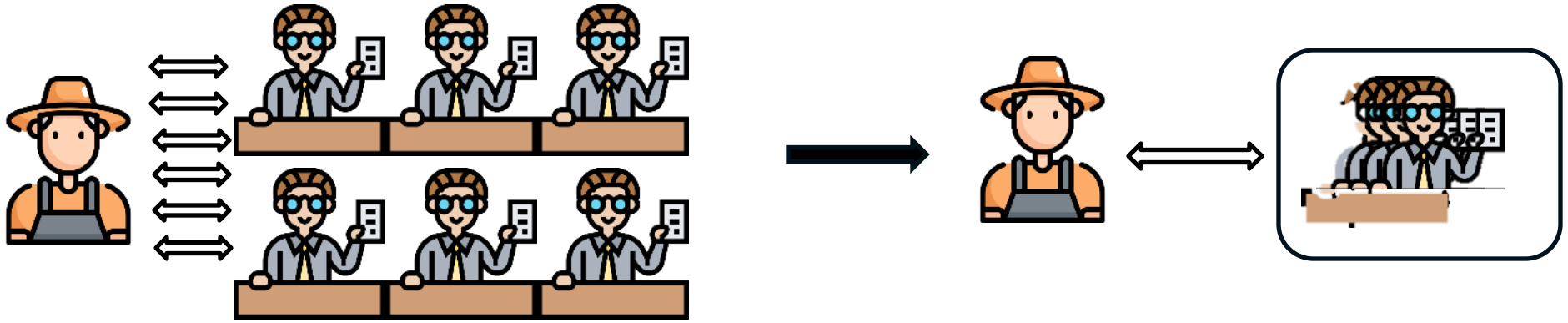
There is a strong preference on Apple's UMA architecture, M3 chips, as shown by RISC Zero's performance data. Other research directions include bypassing the CPU in the network and a very high level of programmability.

Stacking MPC in IZK

To be decentralized, a user needs to repeat the IZK with **multiple** notary nodes.

If we want a user to get digital IDs after being verified by 20 notary nodes (likely elected through PoS), the user needs to repeat the same process for 20 times.

A way to avoid such overhead for the user is to let servers do more work by **stacking MPC in IZK**.



New academic research directions. Non-trivial. Needs new techniques.
Immediate adoption.

IZK in post-quantum Internet

August 15, 2023 marks a special day for the Internet.

Google Chrome Adds Support for a Hybrid Post-Quantum Cryptographic Algorithm

If you've been waiting to put quantum-resistant encryption to work to protect your organization's infrastructure and data, then your wait is over. Chrome rolled out a quantum hybrid key agreement mechanism in its latest release (version 116) on Aug. 15.

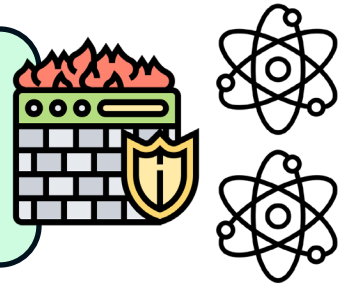
And IZK is just a family member of the post-quantum cryptography.

LHE-based MPC

FSS-based IZK

GC-based MPC

FRI-based NIZK



Important for financial institutions. Moving toward *fully* post-quantum Internet.

IZK in post-quantum Internet

Like FRI-based NIZK, post-quantum may be ***faster*** than pre-quantum.
Example for TLS 1.3:

		Size keyshares(in bytes)		Ops/sec (higher is better)	
Algorithm	PQ	**Client**	**Server**	**Client**	**Server**
Kyber512	✅	800	768	50,000	100,000
Kyber768	✅	1,184	1,088	31,000	70,000
X25519	❌	32	32	17,000	17,000

We expect to see more application-specific IZK protocols for post-quantum cryptography and post-quantum applications that leverage IZK.

Source: Cloudflare. Defending against future threats: Cloudflare goes post-quantum. https://blog.cloudflare.com/post-quantum-for-all/

Website: www.l2iterative.com
Email: team@l2iterative.com
Twitter: https://twitter.com/l2iterative
Telegram: https://t.me/+8uyDw7uz7iI4ZWIx
LinkedIn: https://www.linkedin.com/company/l2iv/

San Francisco | Hong Kong

L2IV