Zero-Knowledge Proofs in the Wild

Anna Kaplan

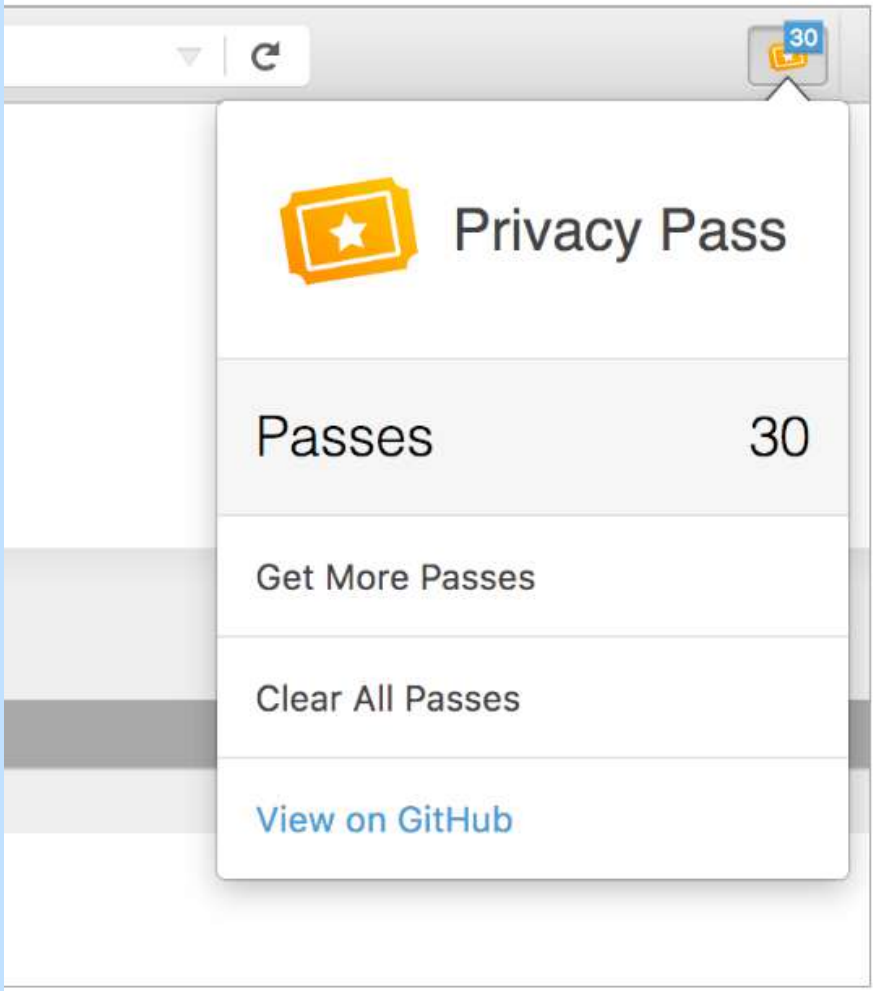
29/10/19 @ ZKProof community event


ZKPs
Signatures
Encryption

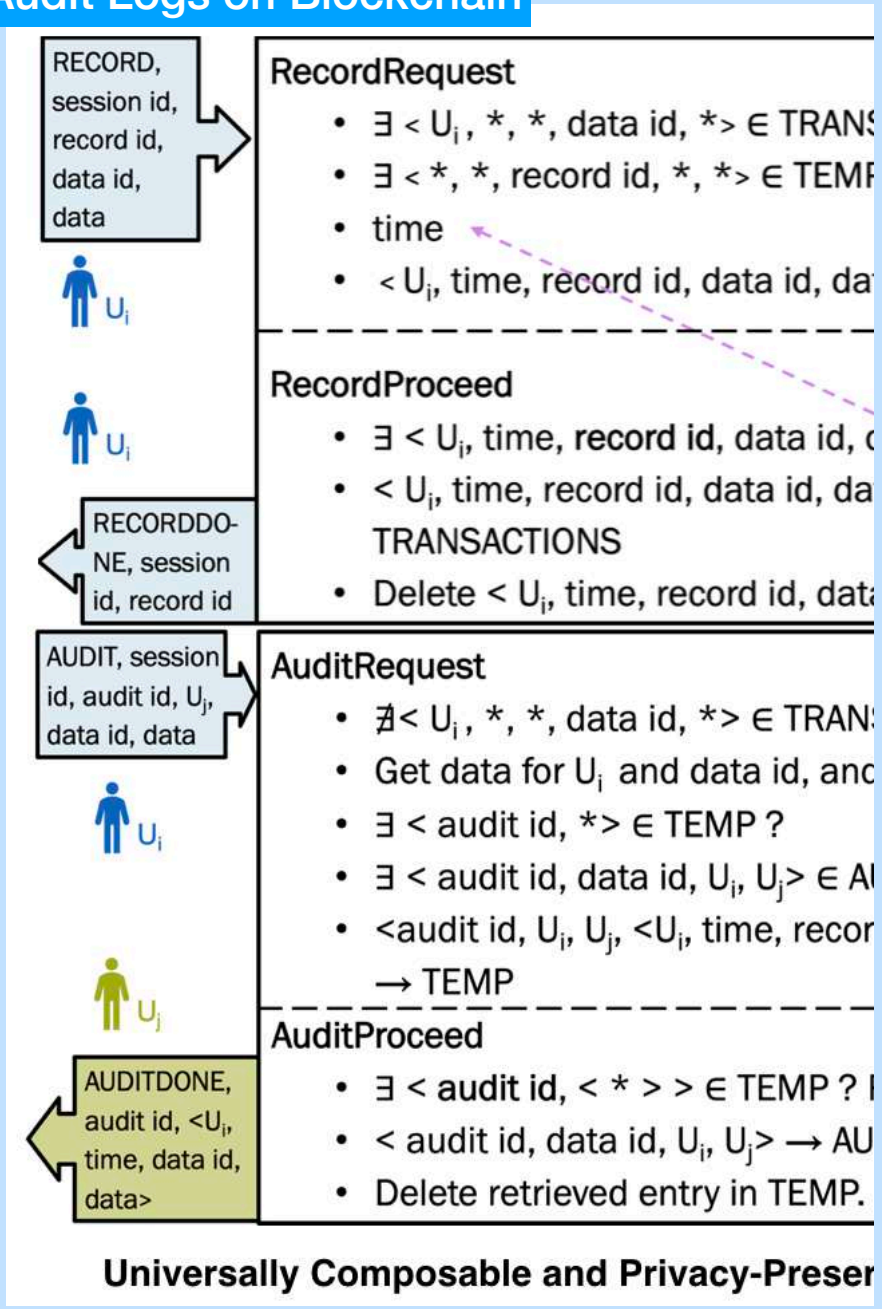

Signatures
Encryption
ZKPs


Industry
Practitioner
Protocols using
ZKPs
Protocols using
Signatures
Protocols using
Encryption

Privacy Pass



Audit Logs on Blockchain

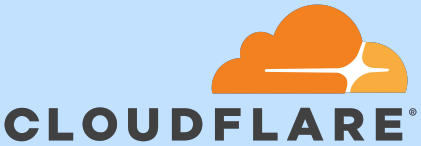


Privacy Pass

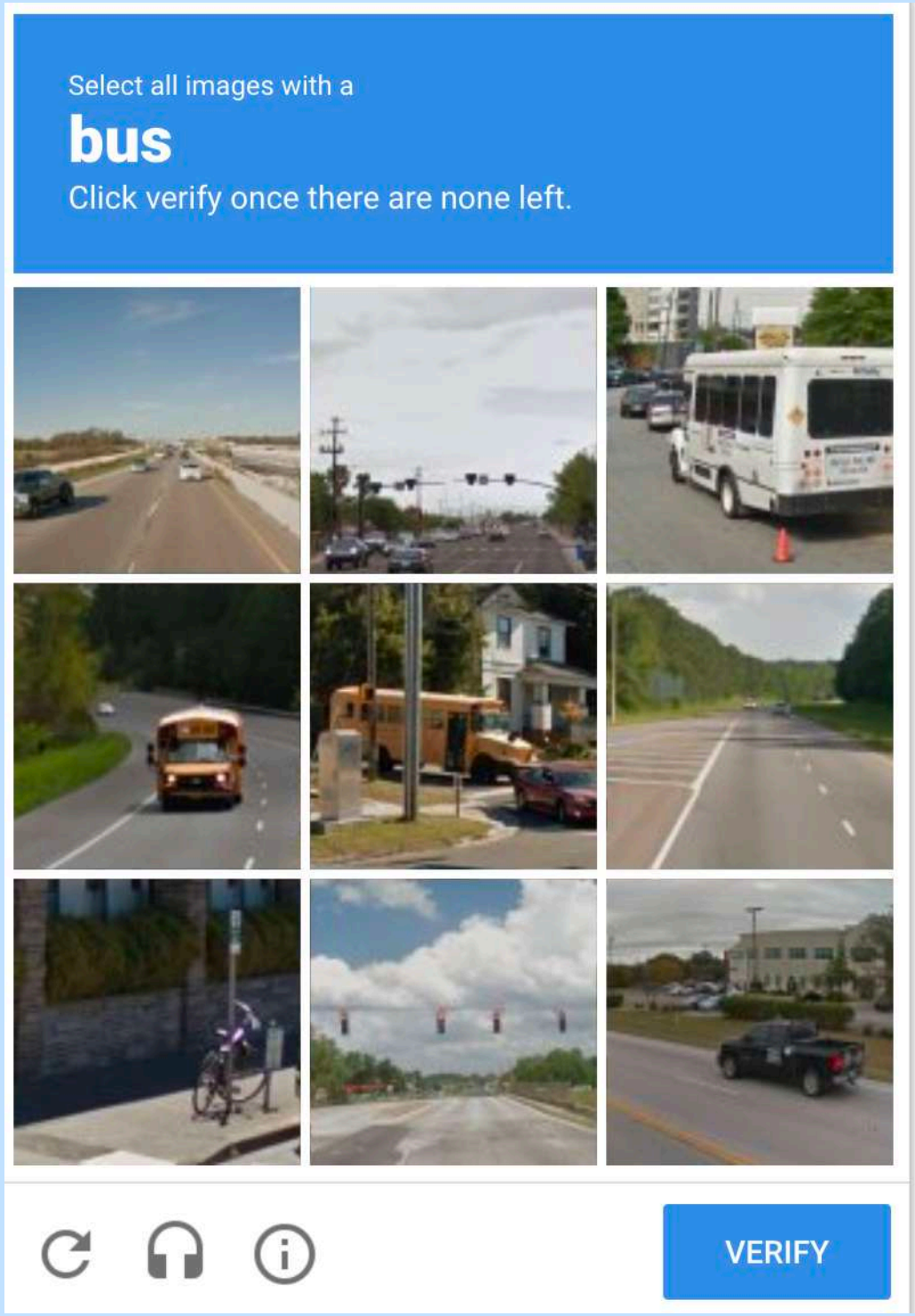
Work by Alex Davidson, Ian Goldberg, Nick Sullivan, George Tankersley, and Filippo Valsorda, 2018

https://privacypass.github.io/

What was the problem?

- Developed by 

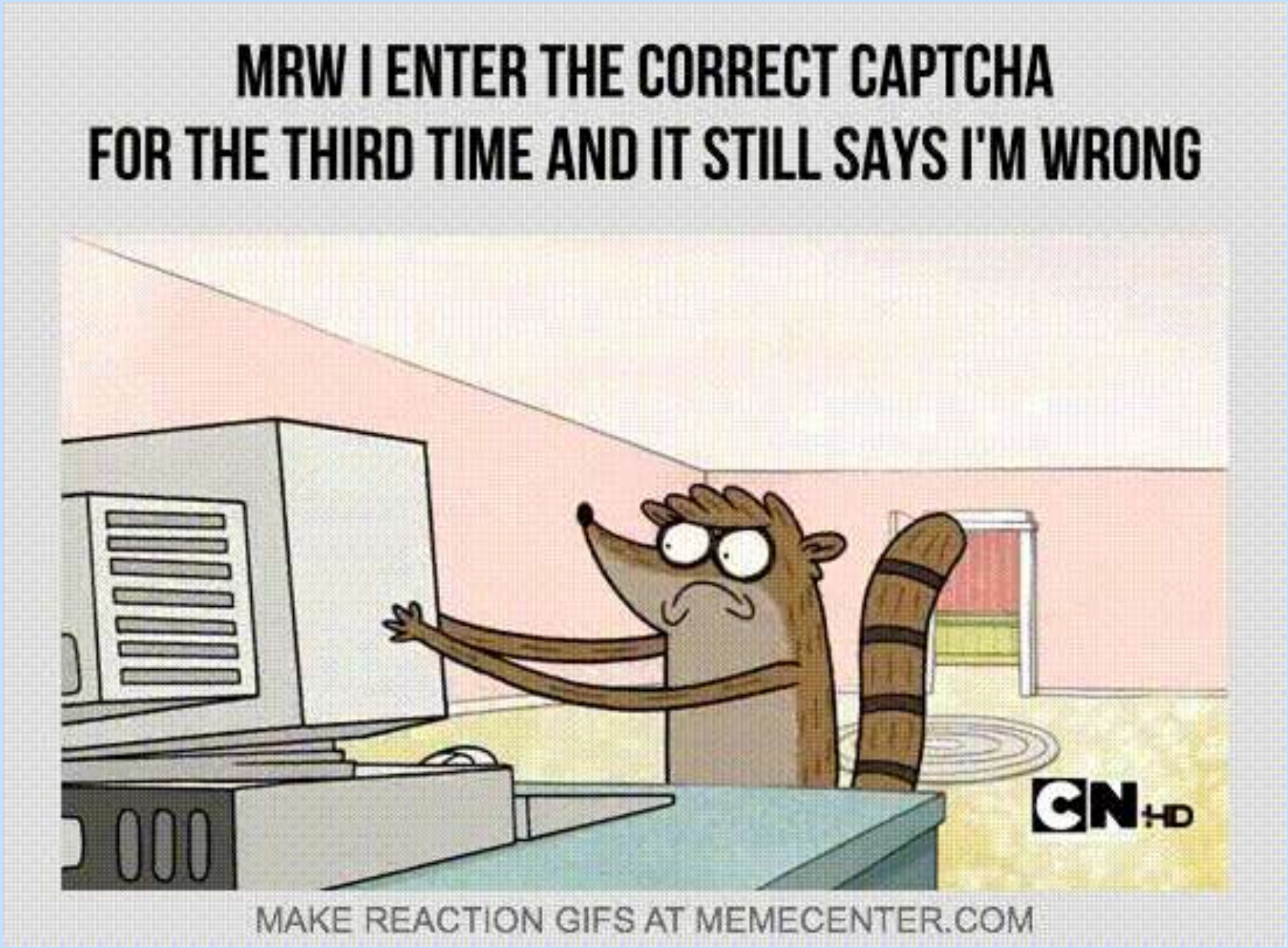
- Cloudfare needs to prevent malicious attacks, e.g. comment spam or SQL attacks, from the web
- Cloudflare does this through **IP reputation** assessment
- How to know that’s a “good" IP address? I have a great solution for you!



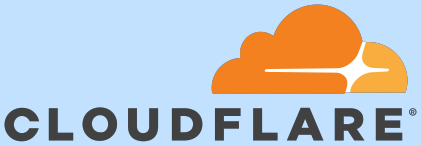
Screenshot by me, 29.10.2019


Scroll from Human to Bot
Enter the following:
Your Answer
SOLVE media
Verify
MemeCenter.com
Why can't I read that?
Am I a robot?

Failing a CAPTCHA three times because I couldn't tell what is and isn't a street sign


MRW I ENTER THE CORRECT CAPTCHA
FOR THE THIRD TIME AND IT STILL SAYS I'M WRONG
CN HD
MAKE REACTION GIFS AT MEMECENTER.COM

What was the problem?

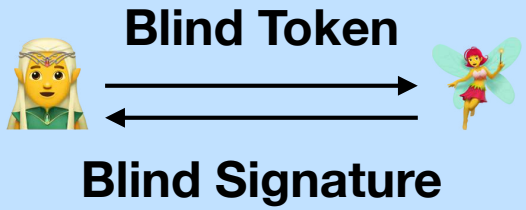
- Developed by 

- Cloudfare needs to prevent malicious attacks, e.g. comment spam or SQL attacks, from the web
- Cloudflare does this through **IP reputation** assessment
- Those who are privacy conscious are mostly affected by CAPTCHAs!

- When you solve the CAPTCHA, you get a 🍪 - but when you don’t want to be followed around you solve endless CAPTCHAs.

Idea: “Modernized Ecash” with no cash involved

- Idea based on **Ecash (Chaum 1983)**:
  - You take a token, blind it, get a blind signature
  - Issuance and Redemption are unlinkable



- After Real World Crypto 2016: How to apply the idea of **blinded signatures to not always having to solve CAPTCHAs**?
  - Filippo Valsorda and George Tankersley came up with first specification for a blinded token to be issued when a CAPTCHA is solved, and can be redeemed later
  - Take a token, blind it, send it to Cloudflare with CAPTCHA solution, get a blind signature in response, which you can later redeem
  - These are unlinkable for Cloudflare

Idea: “Modernized Ecash” with no cash involved

Token ➡️ blind it

Blind Token

Blind Signature

Make digital signature

Mint private key 🔑

Issuance

Validate

Mint public key

Token, Signature

📦

Redemption

Cryptography toolbox

- Problem: Ecash was based on RSA. 1980s cryptography is slow!
- At PETS 2016, Davidson, Tankersley, and Valsorda asked for help and Dan Boneh mentioned EC-OPRFs.
- OPRF: Oblivious Pseudo-Random Function
- **Batched Elliptic Curve VOPRF with redemption** (Tankersley)
  - Multiple simultaneous OPRFs based on Elliptic Curve multiplication
  - VRF-like public verification
  - Batched validation for more efficiency
- **VOPRFs** 🆚 **Ecash:** Ecash is publicly verifiable 🆚 VOPRFs only verifiable in the redemption phase by the issuer

Where do ZKPs come into play?

- EC-VOPRFs use a **Discrete Log Equivalence Proof**
    - Short ZKP that two pairs of points have the same Discrete Log, denounced **DLEQ(P:R == Q:S)**.

Idea: “Modernized Ecash” with no cash involved

Token ➡️ blind it

Blind Token, solved CAPTCHA

Blind Signature

Make digital signature

Mint private key 🔑

Issuance

Validate

Token, Signature

📦

Mint public key

Redemption

How does it work?

From Sullivan, 2nd ZKProof Workshop, 2019

t_1
t_2
t_3

b_1T_1, b_2T_2, b_3T_3

$sb_1T_1, sb_2T_2, sb_3T_3$

$T_1 = Hash(t_1)$
$T_2 = Hash(t_2)$
$T_3 = Hash(t_3)$

$$c_1, c_2, c_3 = H(G, sG, b_1T_1, b_2T_2, b_3T_3, s(b_1T_1), s(b_2T_2), s(b_3T_3))$$

$$DLEQ_s(c_1b_1T_1 + c_2b_2T_2 + c_3b_3T_3 : s(c_1b_1T_1 + c_2b_2T_2 + c_3b_3T_3) = = G : sG)$$

Issuance

$t_1, M, HMAC(sT_1, M)$

📦

Redemption

Current state and other ideas to think about

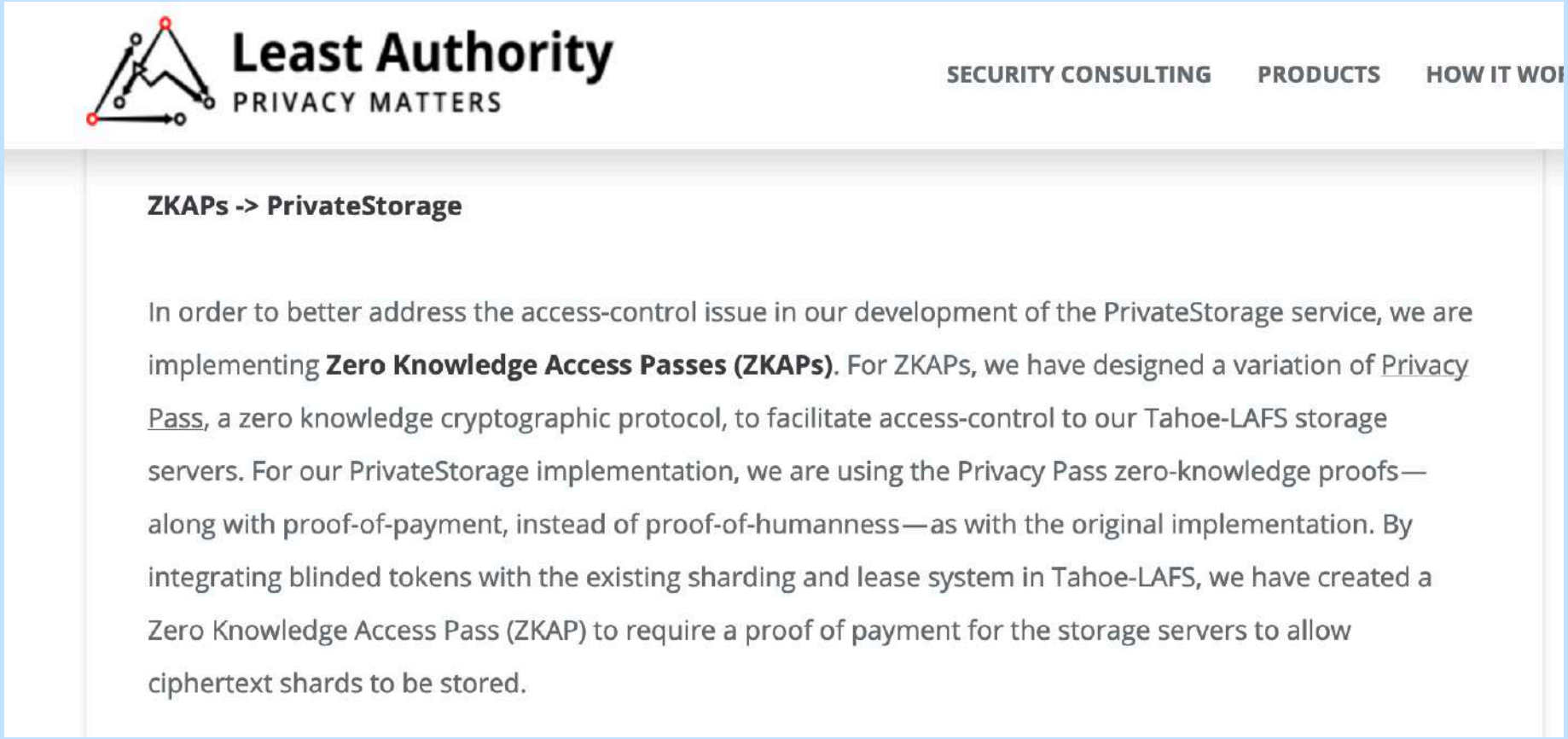
- Privacy Pass exists as an extension and Firefox or Chrome
- **Problems:**
  - Double-spending
  - Solution could be time sharding
- **Other ideas to use this idea:**
  - Anonymous session resumption for TLS
  - Anonymous referral code mechanism (e.g. discount codes) - used in Brave browser for ads
  - Single bit ZKP (e.g. Am I over 18?)

Privacy Pass - another take!

https://privatestorage.io/

What happened?

- Least Authority and Private Internet Access announce PrivateStorage (privacy focused VPN provider)
- PrivacyStorage is private, secure and end-to-end encrypted cloud storage solution, based on Least Authority's Tahoe-LAFS
- For a more robust access control method and controlling reasons, traditional accounting or subscription systems did not suit the desired privacy property
- Private Storage therefore implements **Zero Knowledge Access Passes (ZKAPs)** as a variation of Privacy Pass



https://leastauthority.com/blog/the-path-from-s4-to-privatestorage/

Auditing technology

Joint worked with Jan Camenisch, Manu Drijvers, and Maria Dubovitskaya

User i

User j

data details

data identifier

KAPLAN
0419

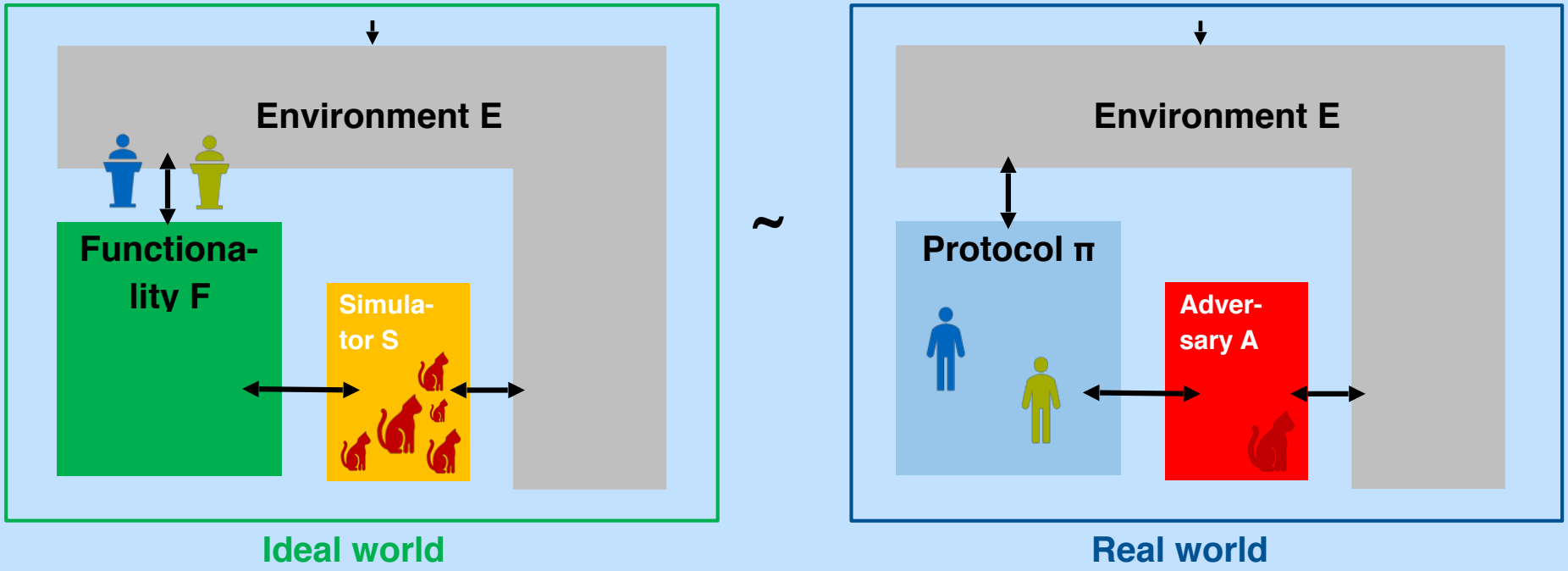
01.04. 52€ from André
02.04. -59€ to Lea
…

Time	User 1			User 2	User 3
2/17/2019 13:06:11	data identifier	data	record session identifier	…	…
…	…			…	…

How to construct such a protocol in best practice?

Modular cryptographic design,
e.g. Universal Composability framework

Universal Composability (Canetti 2001)



Proving a protocol secure means both worlds should be indistinguishable

Let π and F be ppt protocols. We say that π *UC-realizes* F if for any ppt adversary A there exists a ppt adversary S s.t. for any ppt environment E we have:

$$\mathrm{EXEC}_{F,S,E} \approx \mathrm{EXEC}_{\pi,A,E}$$

Security guarantees for our system

Transaction privacy

Transaction authentication

Transaction timestamping

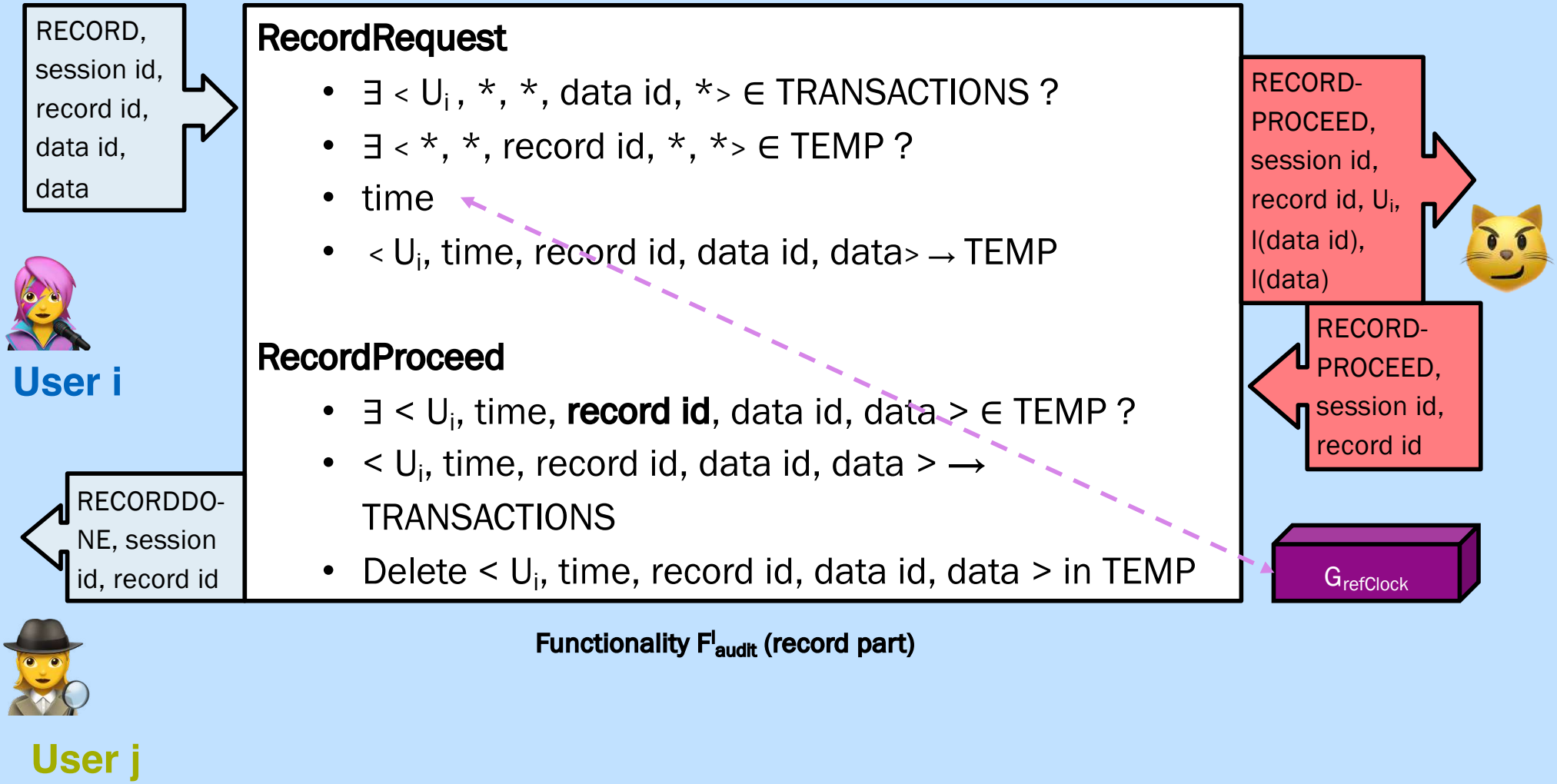
Transaction uniqueness

Record integrity

Auditor authorization

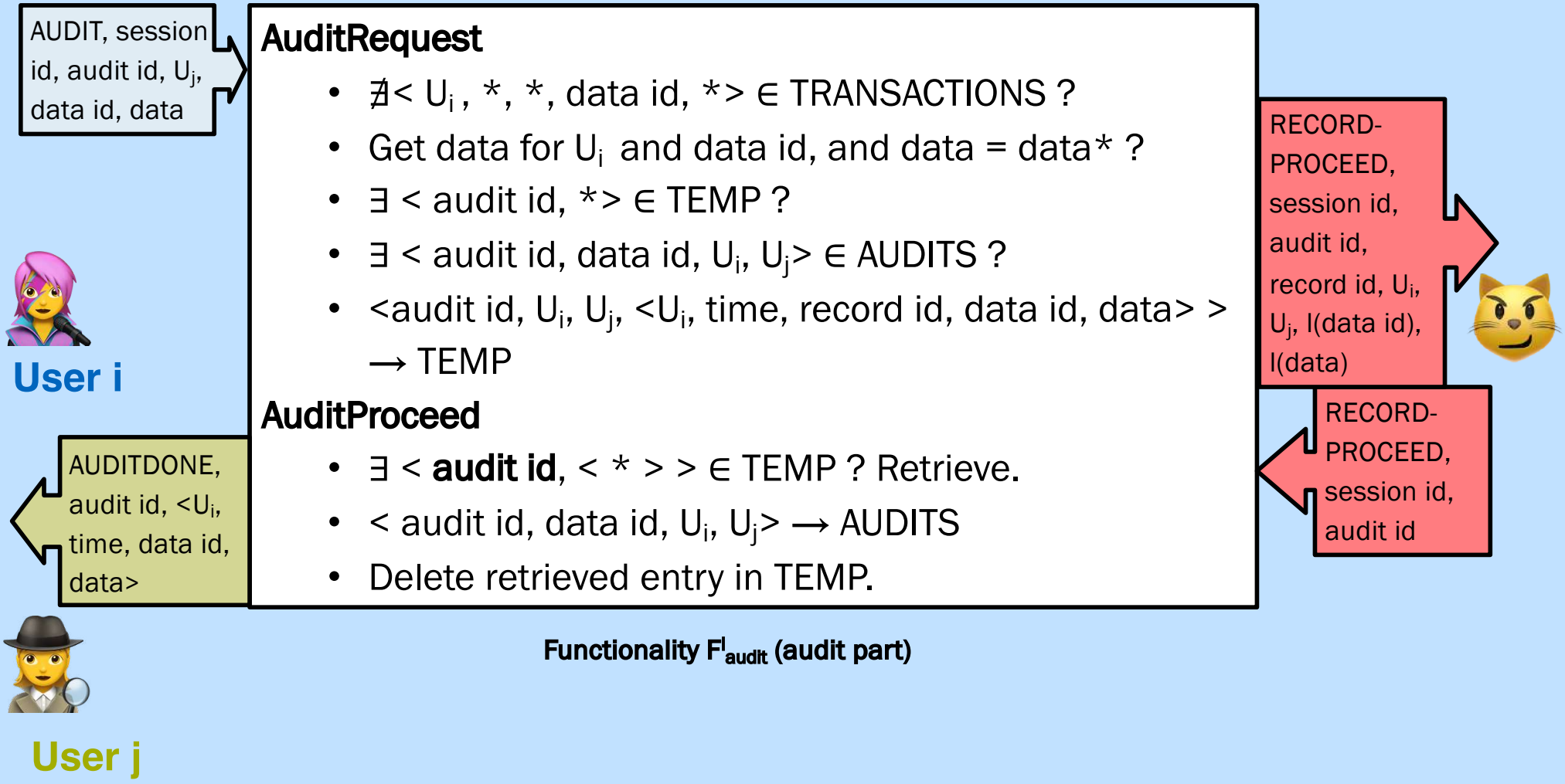
Auditing correctness

Security definition (1/2)



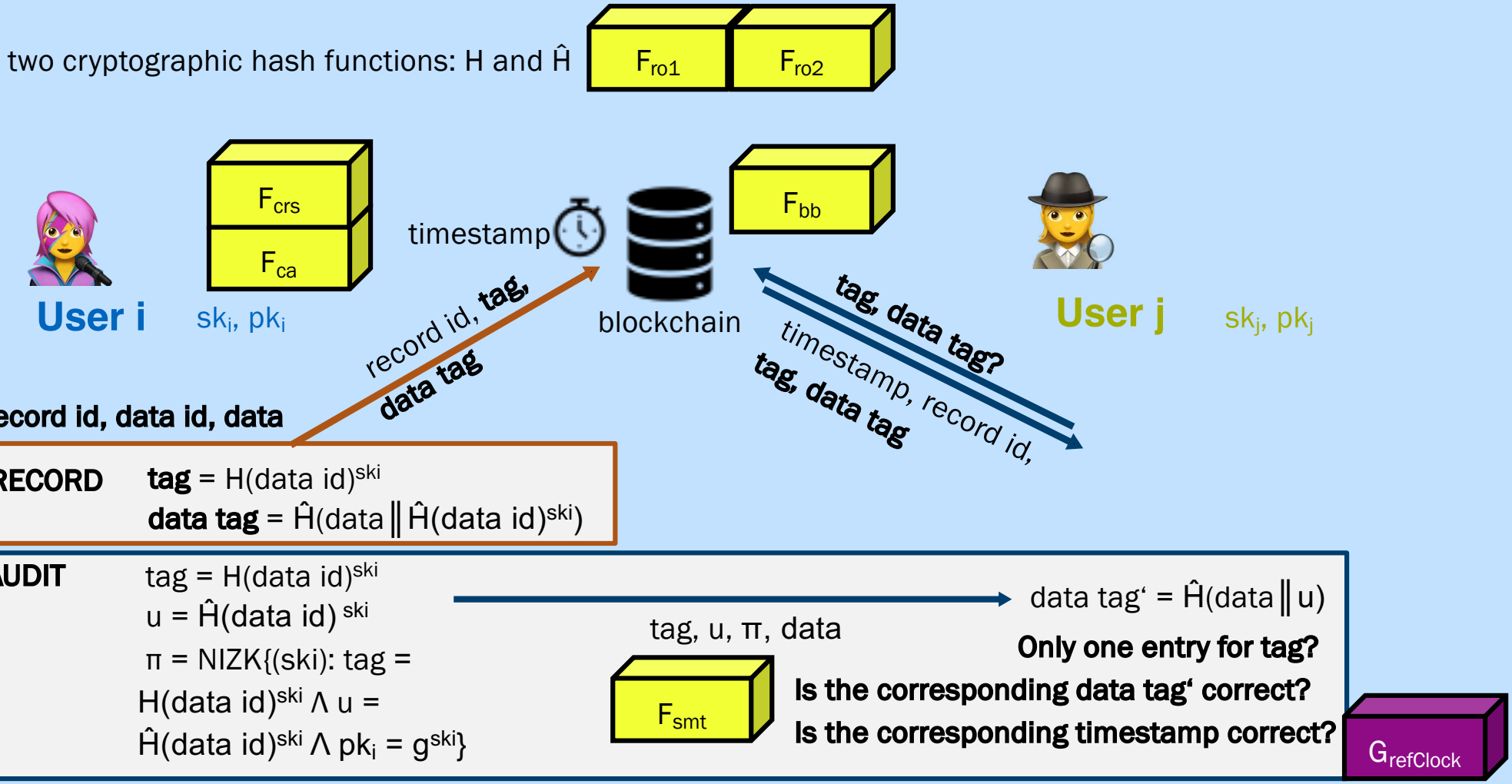
Functionality F^{I}_{audit} (record part)

Security definition (2/2)



Functionality F^{I}_{audit} (audit part)

Protocol for Audit Logs on Blockchain



Implementing

- As a feature for Identity Mixer in Hyperledger Fabric on ClientSDK in Java with the use of Apache Milagro Crypto Library (AMCL)

- Instantiating NIZKs: Schnorr's protocol with Fiat-Shamir heuristic on elliptic curve BN256 (Schnorr '91, Fiat and Shamir '86, Barreto and Naehrig '05)

for AMCL: https://github.com/miracl/amcl

Test on 2 core Intel machine with i5-7200U 2.5GHz CPU and 8GB RAM	**time in milliseconds**
Full Identity mixer benchmark test on signing and auditing	229.6
Identity mixer benchmark test on signing	35.5
Identity mixer benchmark test on auditing	**10.4**

And other wild creatures do exist!

Goldwasser and Park, 2018

Public Accountability vs. Secret Laws: Can They Coe

A Cryptographic Proposal

Shafi Goldwasser
MIT and Weizmann

Sunoo Park
MIT

TRACT

"Our Laws are not generally known; they are kept secret by the small group of nobles who rule us. We are convinced that these ancient laws are scrupulously administered; nevertheless it is an extremely painful thing to be ruled by laws that one does not know."
—Franz Kafka, Parables and Paradoxes.

t 9/11, journalists, scholars and activists have pointed out *ecret laws* — a body of law whose details and sometime mere nce is classified as top secret — were on the rise in all three nes of the US government due to growing national security rns. Amid heated current debates on governmental wishes ceptional access to *encrypted* digital data, one of the key is: which mechanisms can be put in place to ensure that ument agencies follow agreed-upon rules in a manner which ot compromise national security objectives? This promises

eventual solution, it seems clear that a key fact solution will be the ability to trust governm *transparent* about their practices to the maxim consistent with their ability to enforce laws ar Secondly, and relatedly, it is important that form that ensure that government agencies can be hel the law for their requests to access plaintext i provide the guarantee that abuse of power can *principle*.

These basic, natural requirements are further increasing governance (or lack thereof) of intelli *secret laws*: that is, where *even the details of law top secret information*.[2] The very concept of sec against the principles of accountability and tra abundant use of secret law can render entirel to the public a lawfully behaving government tonly abuses power. Indeed, recent heated disc

Metrics with ZKPs: Prio

Prio

Private, Robust, and Scalable Computation of Aggregate Statistics

Background

Prio is a privacy-preserving system for the collection of aggregate statistics. Each Prio client holds a private data value (e.g., its current location), and a small set of servers compute statistical functions over the values of all clients (e.g., the most popular location). As long as at least one server is honest, the Prio servers learn nearly nothing about the clients' private data, except what they can infer from the aggregate statistics that the system computes.

To protect functionality in the face of faulty or malicious clients, Prio uses *secret-shared non-interactive proofs* (SNIPs), a new cryptographic technique that yields a hundred-fold performance improvement over conventional zero-knowledge approaches. Prio extends classic private aggregation techniques to enable the collection of a large class of useful statistics. For example, Prio can perform a least-squares regression on high-dimensional client-provided data without ever seeing the data in the clear.

Prio provides a number of desirable properties:

- **Privacy**
  As long as at least one of the Prio servers is honest, the system leaks nearly nothing (in a precise sense) about the clients' private data.

Zcash, Mimblewimble, …

References

- David Chaum: Blind Signatures for Untraceable Payments, 1983 (https://link.springer.com/chapter/10.1007%2F978-1-4757-0602-4_18)
- Alex Davidson, Ian Goldberg, Nick Sullivan, George Tankersley, and Filippo Valsorda: Privacy Pass: Bypassing Internet Challenges Anonymously, 2018 (https://www.petsymposium.org/2018/files/papers/issue3/popets-2018-0026.pdf)
- Talk by Nick Sullivan at 2nd ZKProof Workshop in Berkeley (https://crypto.dance/projects/7128053)
- Privacy Pass: https://privacypass.github.io/
- Ran Canetti: Universally Composable Security: A New Paradigm for Cryptographic Protocols, 2001 (https://eprint.iacr.org/2000/067)
- Ran Canetti,Yevgeniy Dodis, Rafael Pass, and Shabsi Walfish: Universally Composable Security with Global Setup, 2006 (https://eprint.iacr.org/2006/432)
- Neha Narula, Willy Vasquez, and Madars Virza: zkLedger, 2018 (https://eprint.iacr.org/2018/241)
- Shafi Goldwasser and Sunoo Park: Public Accountability vs. Secret Laws: Can They Coexist?, 2018(https://eprint.iacr.org/2018/664.pdf)
- Prio: https://crypto.stanford.edu/prio/
- Mimblewimble: https://github.com/mimblewimble/
- Zcash: https://zcash.readthedocs.io/en/latest/, https://electriccoin.co/, https://www.zfnd.org/

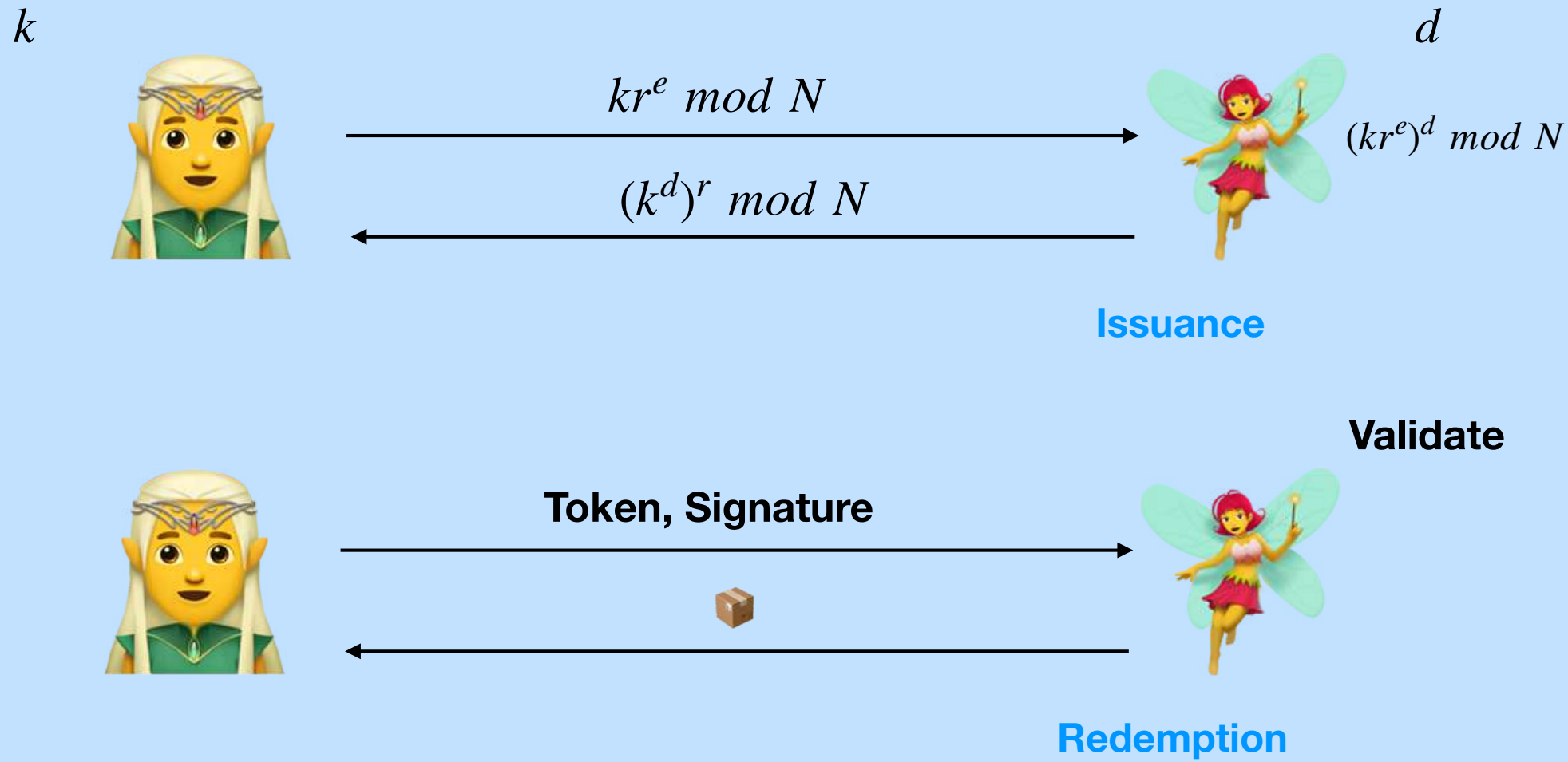
- All photos are stock photos and free to use.

Thank you!

Anna Kaplan
anna.kaplan@tum.de
@kaplannie

Backup

Ecash (Chaum 1983)



User i

User j

data details

data identifier

KAPLAN
0419

01.04. 52€ from André
02.04. -59€ to Lea
…

Time	User 1			User 2	User 3
2/17/2019 13:06:11	data identifier	data	record session identifier	…	…
…	…			…	…