Foundations of Coin Mixing Services

PRESENTER: Noemi Glaeser

BACKGROUND

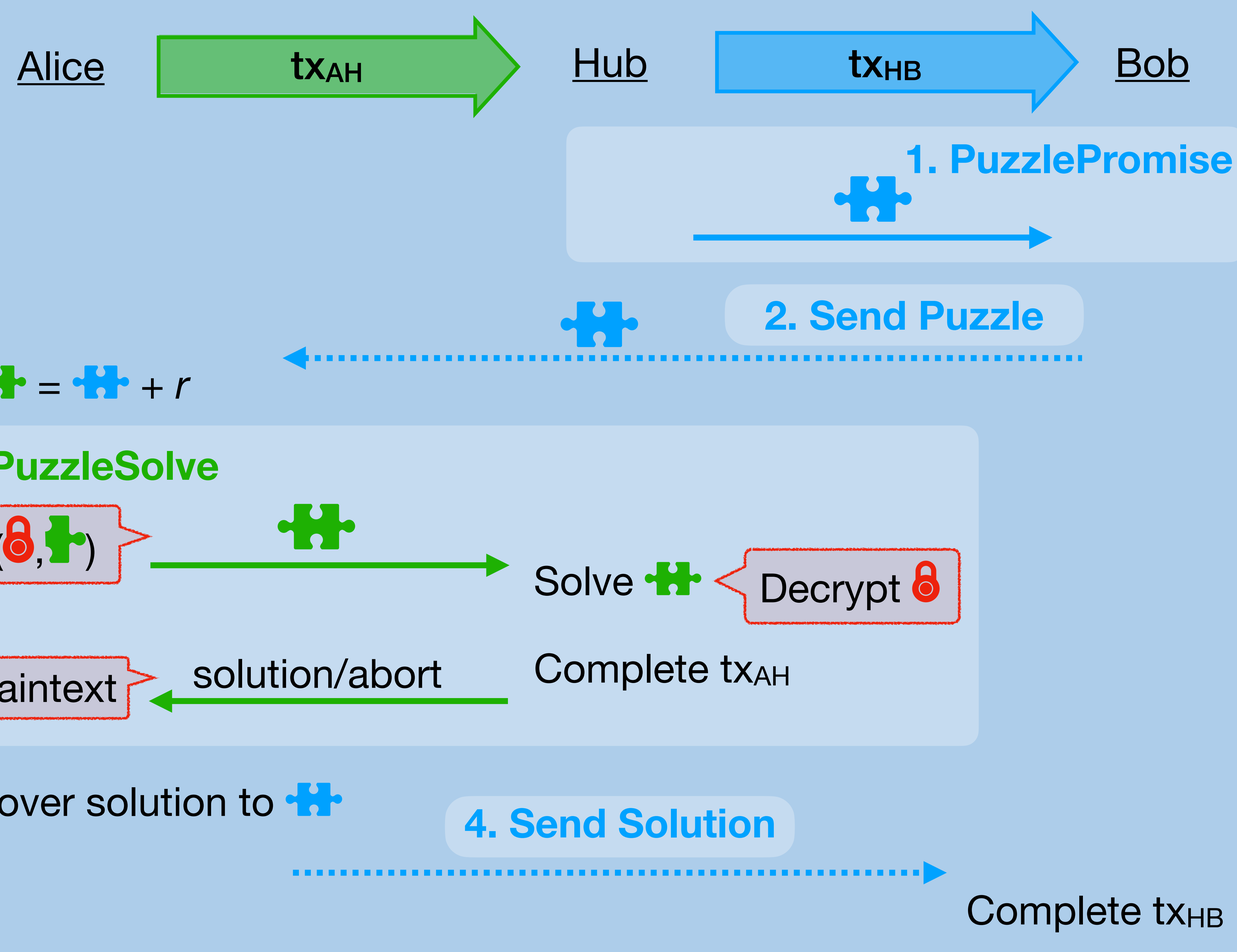
- Blockchains have a **scalability problem** (time per transaction & transactions per second).
- For scalability, two users can use a *payment channel* to pay each other off-chain. Many payment channels are usually **connected via central hubs**.
- A²L [S&P'21]: protocol for **atomic** and **private** payment hubs with formal security guarantees.

RESULTS

- A²L's security model flawed, as shown by **2 counterexamples**:
  1. Key Recovery: Learn full decryption key → unlimited free money!
  2. One-more Signature: Steal 1 coin for every q successful payments
- New framework: **blind conditional signatures (BCS)** with precise security definitions, can be used to analyse payment hubs in *all* cryptocurrencies
- We give a fixed version of A²L called **A²L⁺** which is **provably secure** and requires only **minimal overhead**

The coin mixing protocol A²L **is not provably secure.** We fixed it.

In A²L, the payer Alice sends a ciphertext to the hub and receives a decryption or abort based on the plaintext. This **"decryption oracle" is unaccounted for** in A²L's security proof.



Π_{BCS} := (Setup, PPromise, PSolve, Open)

Game-based security for A²L⁺

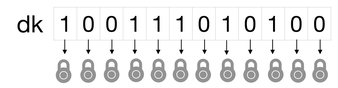
- **Blindness** (vs. H): Hub can't link its session with Alice to its session with Bob
- **Unlockability** (vs. H): hard for Hub to complete a payment from Alice that doesn't result in a payment to Bob
- **Unforgeability** (vs. A+B): Alice and Bob can't get q+1 payments from Hub while only completing q payments

Protocol	Signature	Exp (CL)	Op (CL)	Inv (CL)	DLog (CL)
A²L (insecure)	Schnorr	18	12	1	1
	ECDSA	18	12	1	1
A²L⁺	Schnorr	28	20	2	2
	ECDSA	28	20	2	2
A²L vs. A²L⁺	Schnorr	+10	+8	+1	+1
	ECDSA	+10	+8	+1	+1

Exp (𝔾)	Op (𝔾)	× mod q	+ mod q	#H	WAN (s)	LAN (s)
13	8	4	9	6	2.292	0.580
27	8	17	10	11	2.327	0.483
14	9	5	9	6	~3.438	~0.87
32	10	21	12	11	~3.491	~0.725
+1	+1	+1	+0	+0	+1.146	+0.290
+5	+2	+4	+2	+0	+1.164	+0.242

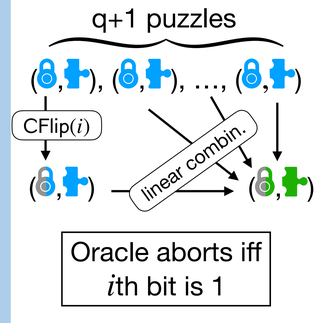
Key Recovery

- Linearly hom.
- Circular sec. for bit encr.
- Bit encr. of dk
- A* opens a new session with hub for each bit (cryptocurrency layer has one-time keys)



← Enc(ek, x) +
Compute for x

Oracle aborts iff encrypts 1



Oracle aborts iff ith bit is 1

One-More Sig

- Linearly hom.
- Conditional bit flip
- Make q non-⊥ queries → learn plaintext 1
- Solve system of eqns for remaining q plaintexts

linktr.ee/coinmixing

Noemi Glaeser, Matteo Maffei, Giulio Malavolta, Pedro Moreno-Sanchez, Erkan Tairi, Sri AravindaKrishnan Thyagarajan

UNIVERSITY OF MARYLAND · TU WIEN · Carnegie Mellon University · institute IMDEA software · CDL-BOT · MAX PLANCK INSTITUTE FOR SECURITY AND PRIVACY