Seminar, 17.3.22

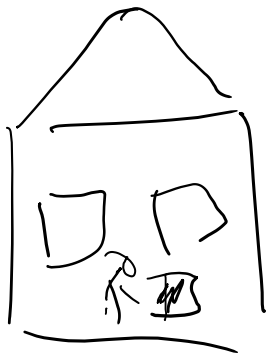
Covert channel in Monero

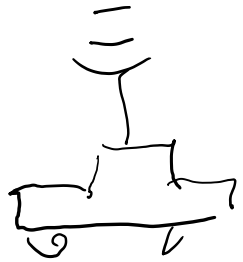
Spy

Enc(M)

Headquarters

traffic

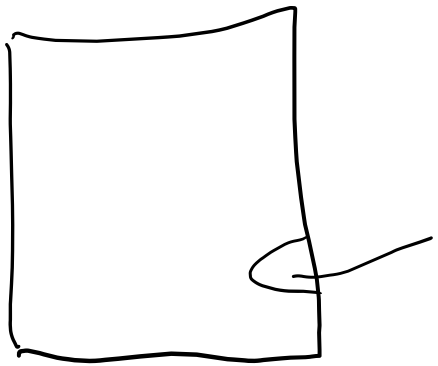




Today:

FB account

pictures from vacation



Stego$_K$

Still:

Jan Kowalski

↓

downloads 10 KGB

Goal make spying easy

and undetectable with traffic analysis

Monero ring signature

$q_i, w_i : i \in n$,

P_s, x_s - pair of keys used to sign

$$L_i = \begin{cases} q_i \cdot G & i = s \\ q_i \cdot G + w_i \cdot P_i & i \neq s \end{cases}$$

$$R_i = \begin{cases} q_i \cdot H(P_i) & i = s \\ q_i \cdot H(P_i) + w_i \cdot I & \end{cases}$$

$$c = Hash(M, L_1, \ldots, L_n, R_1, \ldots, R_n)$$

$$c_i = \begin{cases} w_i & i \neq s \\ c - \sum_{i \neq s} c_i & i = s \end{cases}$$

$$r_i = \begin{cases} q_i & i \neq s \\ q_s - c_s \cdot x_s & i = s \end{cases}$$

Trick

c_i, r_i : for $i \neq s$

$(= q_i, w_i)$

↑ ↑

ciphers of PK scheme

use PK of destination

to encode any plaintext

$n = 10$

$q_i, w_i \approx 2^{256}$

over 2K bits

Now: destination point fetches transactions

⟷ not suspicious

Monero framework for spying and covert transmissions!

Countermeasures

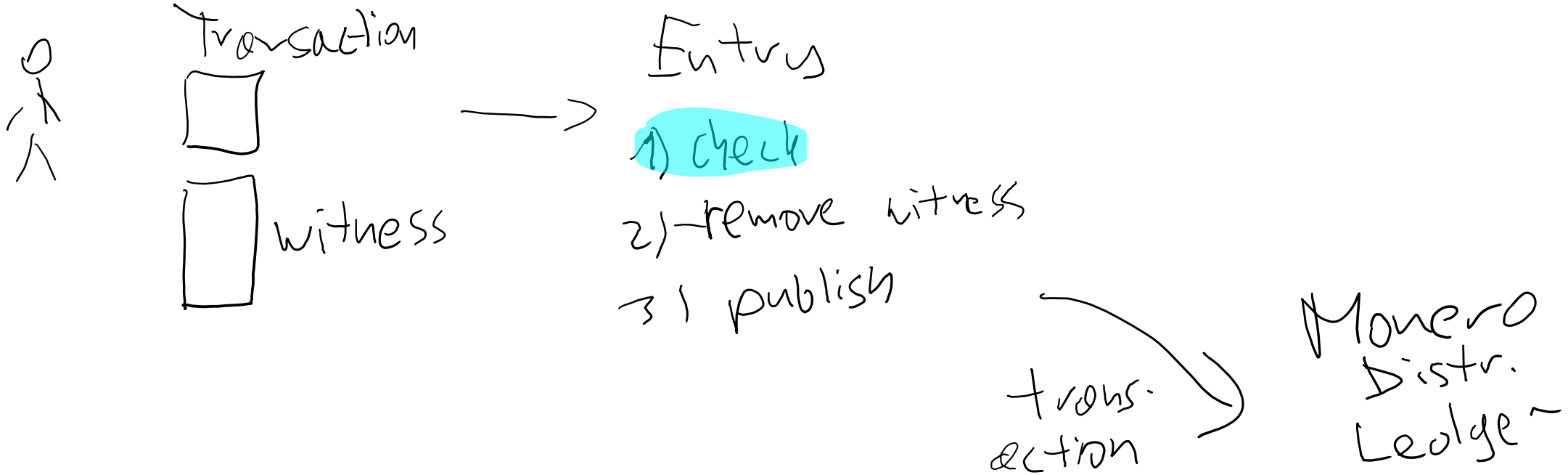
P_i

$(G, P_i, k_i \cdot G, k_i \cdot P_i)$

$Q_i \rightsquigarrow q_i$

$\Rightarrow$ cryptographic channel is narrow

$NZKP(k_i : (G, P_i, A, B);\ A = k_i \cdot G,\ B = k_i \cdot P_i)$


Transaction
witness
Entry
1) check
2) remove witness
3) publish
trans-
action
Monero
Distr.
Ledger

NZKP for DH tuple, Chaum-Pedersen signature

$$(g, h, g^k, h^k) = (g, h, A, B)$$

1) $r_g = g^u$ u-random

$r_h = h^u$

2) c = challenge , $c = \text{Hash}(\dots r_g, r_h \dots)$

3) $s = u + c \cdot k$

Test $\begin{cases} g^s = g^u \cdot g^{ck} = r_g \cdot A^c \\ h^s = h^u \cdot h^{ck} = r_h \cdot B^c \end{cases}$

cheating g, h, g^{k_1}, h^{k_2}

$r_g = g^{u_1}, \quad r_h = g^{u_2}$

$$\begin{cases} s = u_1 + c \cdot k_1 \\ s = u_2 + c \cdot k_2 \end{cases}$$

if linearly independant $\Rightarrow$ one solution for (s, c)

$i \simeq S$

$(G, P_i, \frac{1}{x_i} \cdot C_S, C_S)$ — DH tuple, as before

$$\begin{cases} k \cdot G = \frac{1}{x} \cdot C_S \\ k \cdot P_i = C_S \end{cases}$$

(g, h, A, B)

$h = g^x, \quad B = A^x$

& the same NIZKP works

Challenge we show NZKP for each i,
but ... we cannot betray s

(g, h, A, B):

$$NZKP(k \text{ or } x : (g^k = A \;\&\; h^k = B) \text{ OR } (g^x = h \;\&\; A^x = B))$$

OR - NZKP

c - challenge

$c = c_1 + c_2$ ← computed after c

↑ chosen in advance

Helpful, because if we know c_1 in advance we can simulate ZKP

$$\begin{cases} r_g \cdot A^{c_1} = g^s \\ r_h \cdot B^{c_1} = h^s \end{cases}$$

1) choose s, c_1

2) $r_g \cdot r_h$ as above

Ring signature:

$B \rightarrow q_i$

i: (G, P_i, A, B)

NZKP: ① knows k: $A = k \cdot G$, $B = k \cdot P_i$

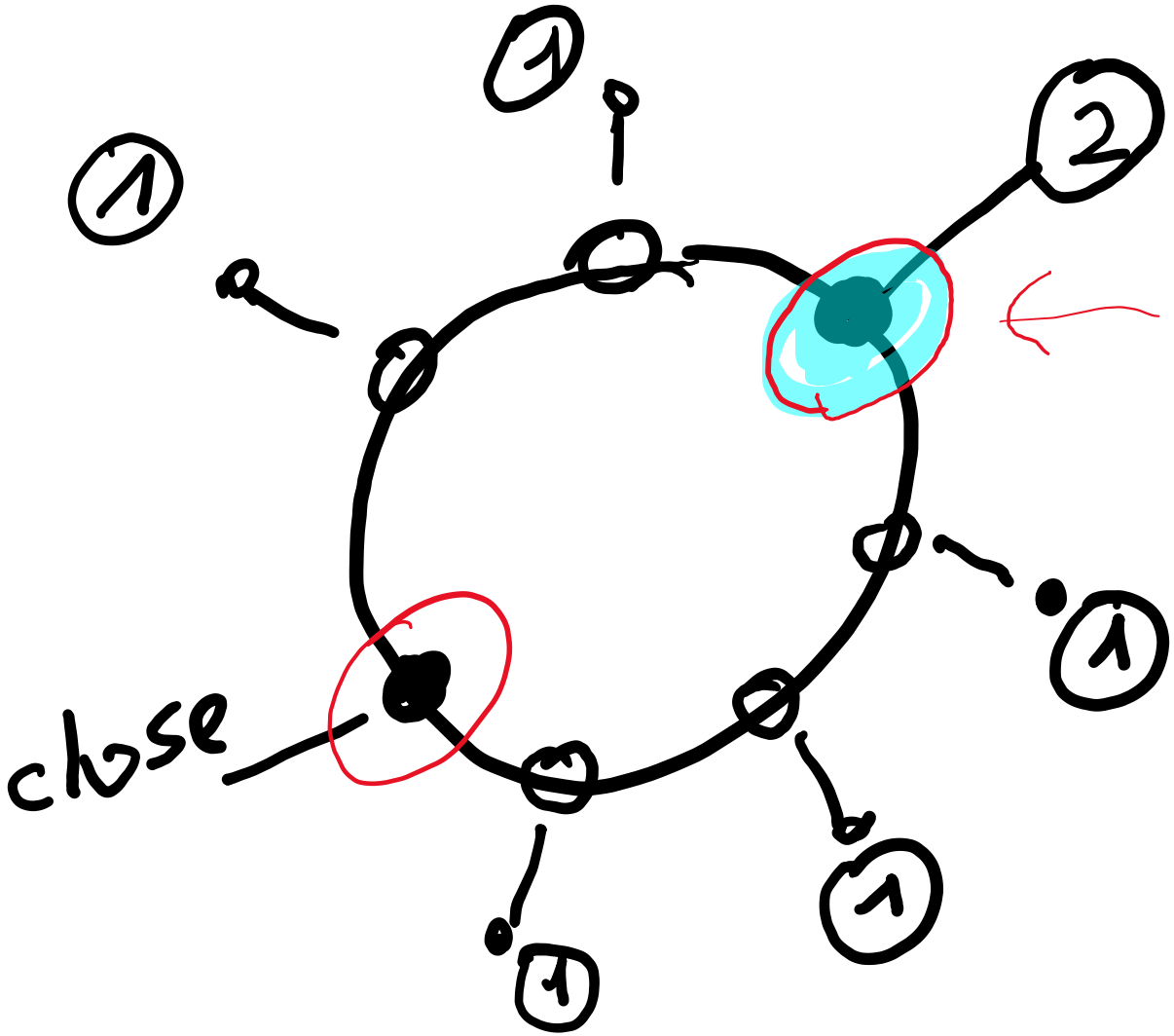
OR

② knows x_i: $P_i = x_i \cdot G$, $B = x_i \cdot A$

Now $i \neq s$: kleptographic channel is narrow

$i = s$: deterministic

Fine, but adversary may hold >1 private key



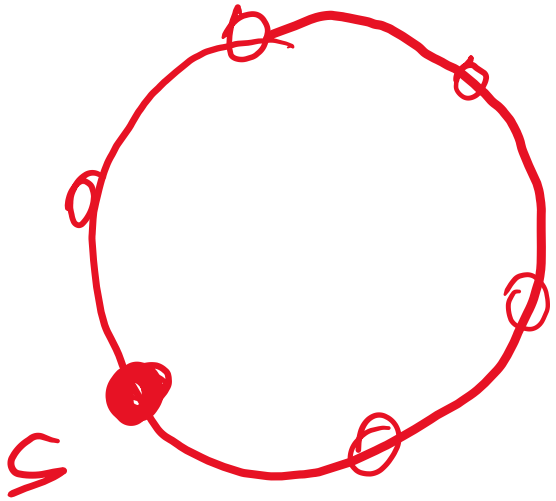
ciphertext

σ

$(G, P_j, x_j^{-1} \cdot \sigma, \sigma)$

Defense is not effective

what to do ?

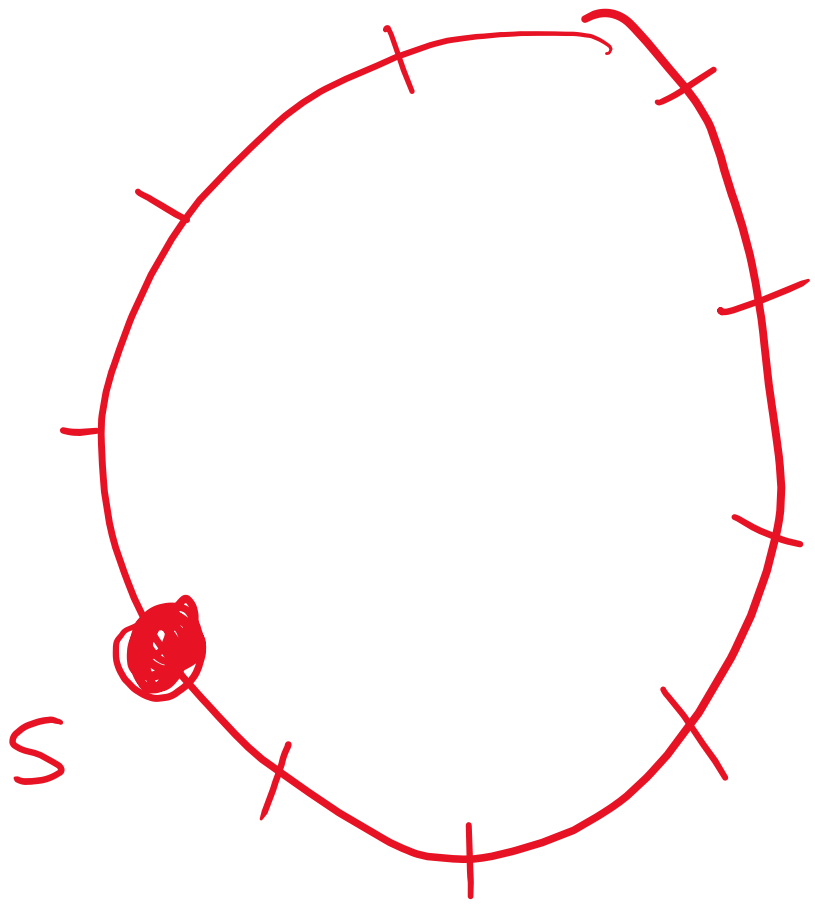


NZKP( ) OR
$s=1$

NZKP( ) OR
$s=2$

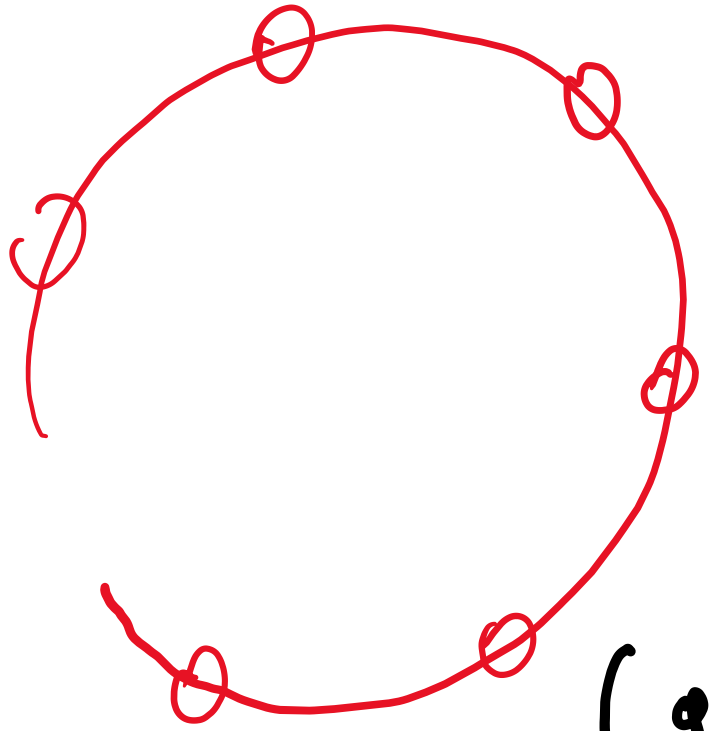
⋮

NZKP (. . . .)
$s=n$



$(g, h, A, B) = (g, h, g^k, h^k)$

How to prove that



$(g, P_i, g^{k_i}, P_i^{k_i})$

$(g, P_j, g^{k_j}, P_j^{k_j})$

Problem

$g^{k_1}, g^{k_2}, \ldots, g^{k_{n-1}}$

show that I know $k_1, k_2, \ldots k_{n-1}$

Ad hoc solution

$c_1, \dots c_{n-1}$ - challenge (Fiat-Shamir)

$A' = \prod A_i^{c_i}$

NZKP of $\log_g A'$

A_i, A_i^{-1}

$A_i^{c_i}, A_i^{-c_i}$

Challenge

1) concise proof

2) details for Monero (choice of the group, EC arithmetic)

3) demonstration

? 'invitation to cooperation

— MA dissertation is also an option!