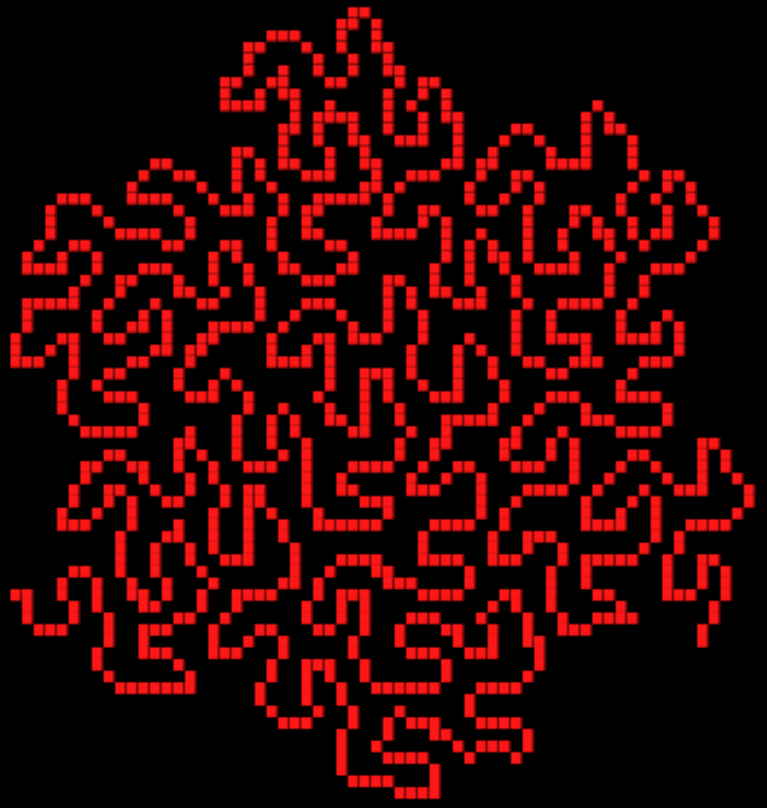


rmxwallet.io

i_a@rmxwallet.io

Line-up:

(1) Keep the project going

(2) HW messenger

(3) Monero implementation

(4) HW Security

rmxwallet.io

(1) Keep it going

- Building hardware is challenging itself
- Thinking about next step(s)
- Avoiding burn-outs
- Contributors, motivations
- Funding

(2) HW messenger

- RMX to RMX encrypted
- XMPP as a transport protocol
- Any XMPP server..?
- 256B long messages, (user experience close to SMS)
- Messages are encrypted, then sent as a plaintext
- Each message is symmetrically encrypted with a one-time key

(3)Monero wallet

<secret view key>

036de964247a6 …

<secret spend key>

90a77cbf807c8f ...

[Create tx→

sign→broadcast]

<Monero blockchain>

Bdaa1036de964247a6a6686adda42edd5
73a90a77cbf807c8fb37bdaa1036de9642
07c847a6a60ef9b4194686adda42ed0ef9
b4194d573a90a77cbf807c8fb37bdaa103
6de964247a6a6686adda42ed0ef9b4194
d573a90a77cbf807c8fb37bd07c8aa1036
de96424707c866573a90a77cbf807c8fb3
7bdaa103607c8de964247a6a60ef9b4194
686adda42ed0ef9b4194d573a90a77cbf8
07c8fb37bdaa1036de964247a6a6686add
a4964247a6a637bd07c8aa10363a90a77
cbf807c8fb37bdaa1036de964247a6a668
6adda42ed0ef9b4194d573a90a77cbf807
c8fb37...

rmxwallet.io

(3)Monero wallet

<secret view key>

036de964247a6 ...

<secret spend key>

90a77cbf807c8f ...

– > incomming txs

– > outcomming txs, spending (signing txs)

[Create tx→

sign→broadcast]

rmxwallet.io

(3)Monero wallet

- Monero has encrypted blockchain
- viewkey, spendkey – functions segregation

SCANNING:

- Tx: Output's public key P, Tx's public key R
- P - H(aR)G
- 2x Ed25519 Elliptic curve multiplication, one SHA-3 hash, one point substraction for each Tx's output
- Check if the result == with public spend key

rmxwallet.io

(3)Monero wallet

- Public scanning – offloading viewkey to PC
- If match, unmasking

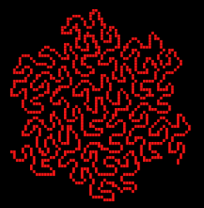
- Private scanning
- Too heavy for arm cortex m3/4
- Need for faster ed25519 multiplications

rmxwallet.io

(3)Monero wallet

- Microchip CEC1702
- Cortex M4F + hardware accelerator
- Scanning one output in 4ms (100 Tx/s*)
- 8 Txs in a block every 2 minutes
- One day scanned in 46s, one year in 5h

**one Tx contains two outputs*



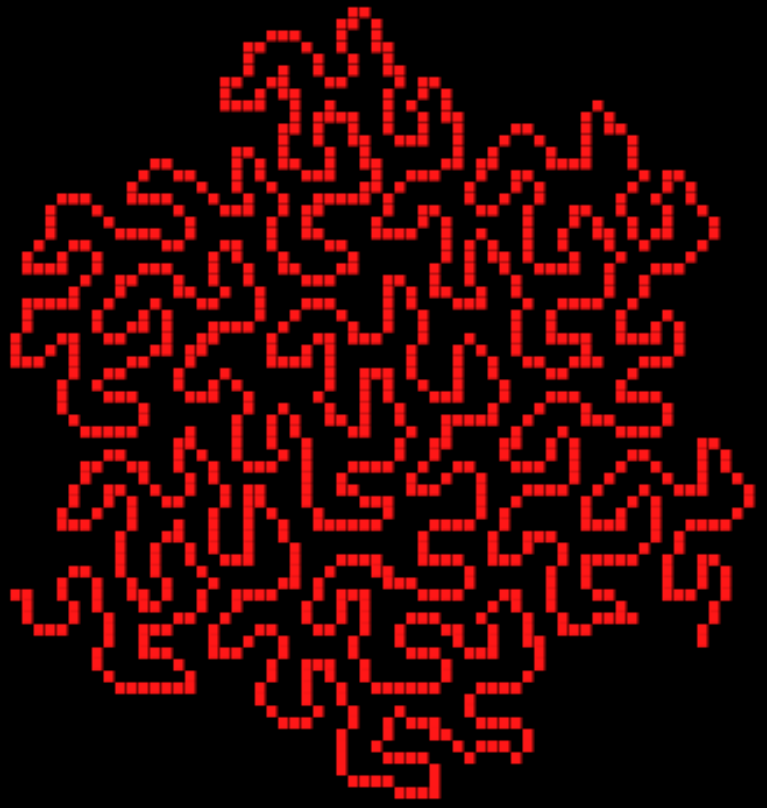
rmxwallet.io

(4)HW security

- Secure boot feature
- Only signed images
- Cortex m4 -Fault injections? Glitches?
- Passphrase?
- Source of random
- Secure element versus encrypted secret

rmxwallet.io

rmxwallet.io



rmxwallet.io

i_a@rmxwallet.io

(2) HW messenger

- Encryption variables:

  1. Get one time random r [32B]

  2. Get recipient’s pubkey P (query XMPP server)

- Creating encryption key

  1. Creating one time encryption key K = rP [32B]

  2. X = rG (ed25519) – will be added to encrypted payload

- Encryption

  symmetric AES encryption, CBC MODE,

  Randomization vector SHA3(K)

- Payload

  [encrypted string 256B || X]

- Receiving

  K’ = privkeyX

rmxwallet.io