June 6, 2025. 4:55pm – 5:20pm
The 3rd IEEE International Workshop on Cryptocurrency Exchanges (CryptoEx 2025)

IEEE ICBC

Not Your MPC, Not Your Coin

Yuto TAKEI

Security Researcher
Mercari, Inc.

mercari

Outline

1. Research Motivation
2. Background and Related Work
3. Comparison: Non-MPC vs. MPC Wallet
4. Attack Vectors
5. Security Measures
6. Conclusion

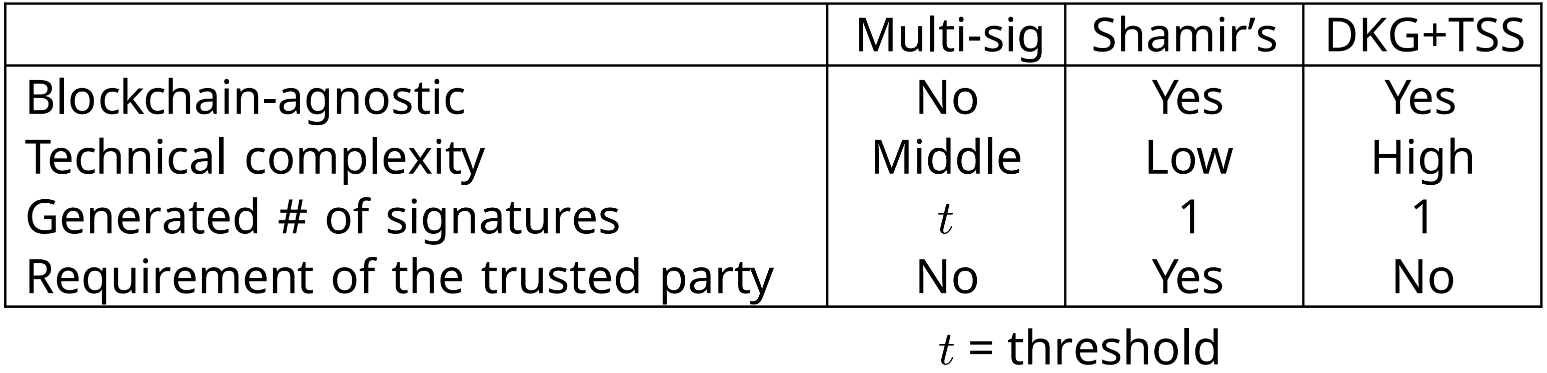
Research Motivation

To understand the security characteristics and implications when using an MPC wallet at cryptocurrency exchanges:

- Compare with air-gapped or secret-sharing wallets
- Understand potential attack vectors when operating in real-world settings
- Propose necessary security management measures for using vendor solutions

Background : Withdrawal Power Segregation

Powers are often split to eliminate a single point of failure at financial institutions.



	Multi-sig	Shamir's	DKG+TSS
Blockchain-agnostic	No	Yes	Yes
Technical complexity	Middle	Low	High
Generated # of signatures	t	1	1
Requirement of the trusted party	No	Yes	No

t = threshold

MPC wallets (DKG+TSS) are becoming popular.

Multiple vendors provide solutions out of the box.

Related Work

Securing Crypto-Wallets

- Takei et al. Pragmatic analysis of key management. ICBC 2024.

Cryptology behind MPC

- Verifiable Secret Sharing
- Threshold Signing Scheme
- Distributed Key Generation

MPC Wallets and Attacks

EdDSA (e.g. Solana)

- A Schnorr variant, and TSS -friendly. E.g. MuSig, FROST.

ECDSA (e.g. Bitcoin, Ethereum)

- Multiple studies since 2018 E.g. GG18, DKL19.

Attack methods

- Improper verifications E.g. Aumasson et al.

Comparison: Non-MPC versus MPC wallet

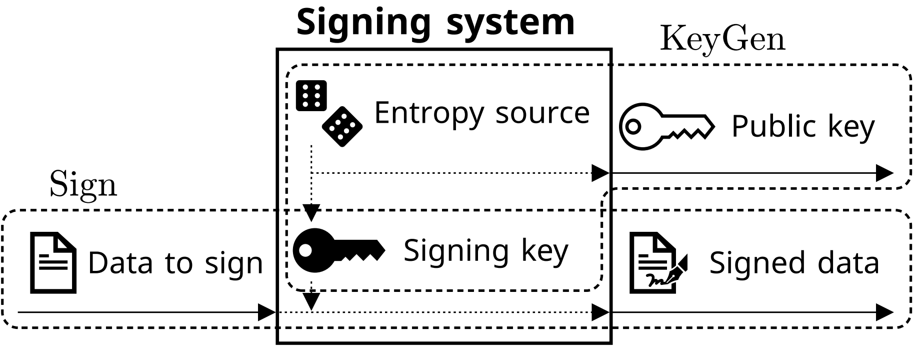
Conventional Cold Wallets / Secret Sharing Wallets

The key is securely stored in the system:

- Hardware wallets or HSMs
- Secret sharing among devices in a closed-circuit network

To prevent key leakage:

- Eliminate side channels
- Inspect output for validation



We do not assume an external vendor to be the trusted party.

Comparison: Non-MPC versus MPC wallet

MPC Wallet with Vendor Holding Key Share

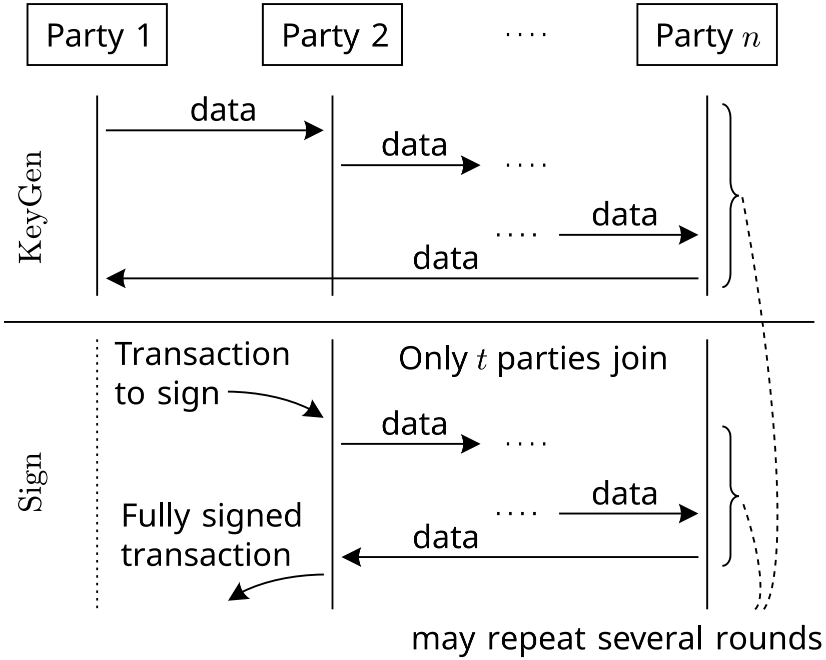
Key exists among multiple parties.

- In vendor-provided settings, one of the parties = vendor.
- The system may run over an open network.

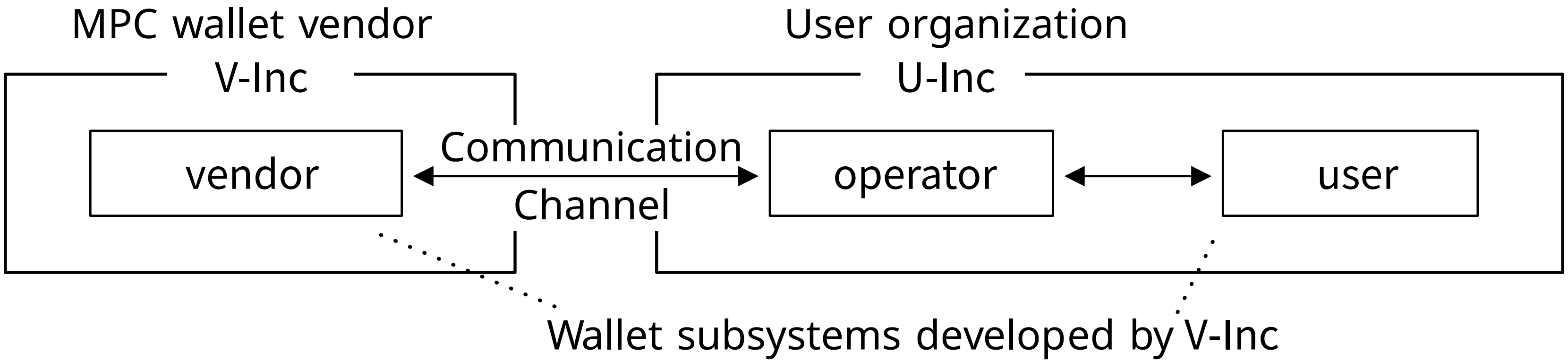
To prevent key leakage:

- Sanitize all communication

Is the external vendor trustworthy?

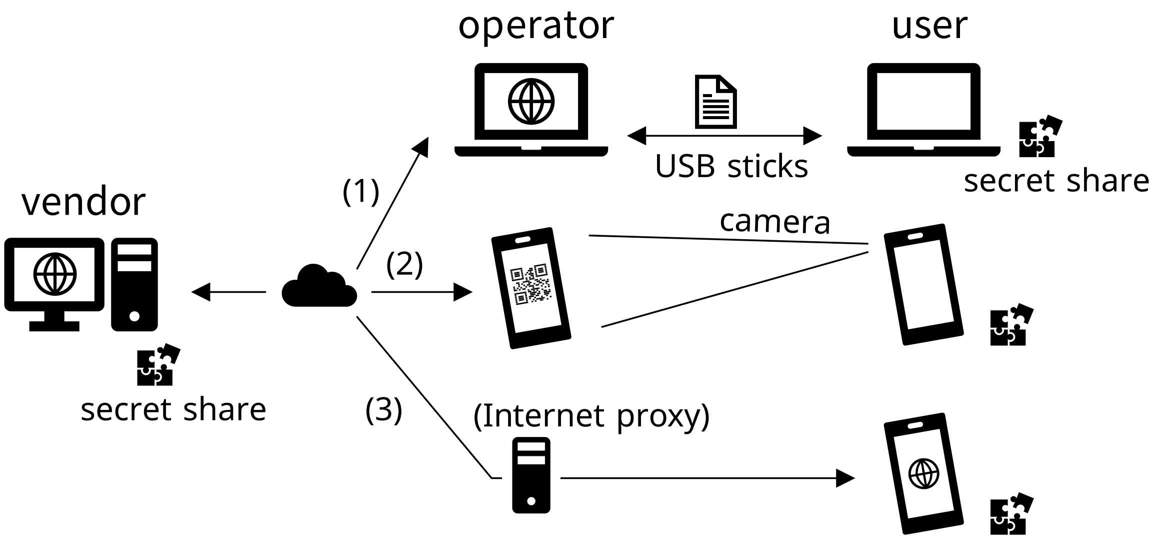


Attack Target: Model of MPC-Wallet



- U-Inc (user exchange) uses vendor-provided system
- One of the shares is managed by V-Inc (Vendor), i.e., Not all shares are under U-Inc's control.

Communication Between user and vendor

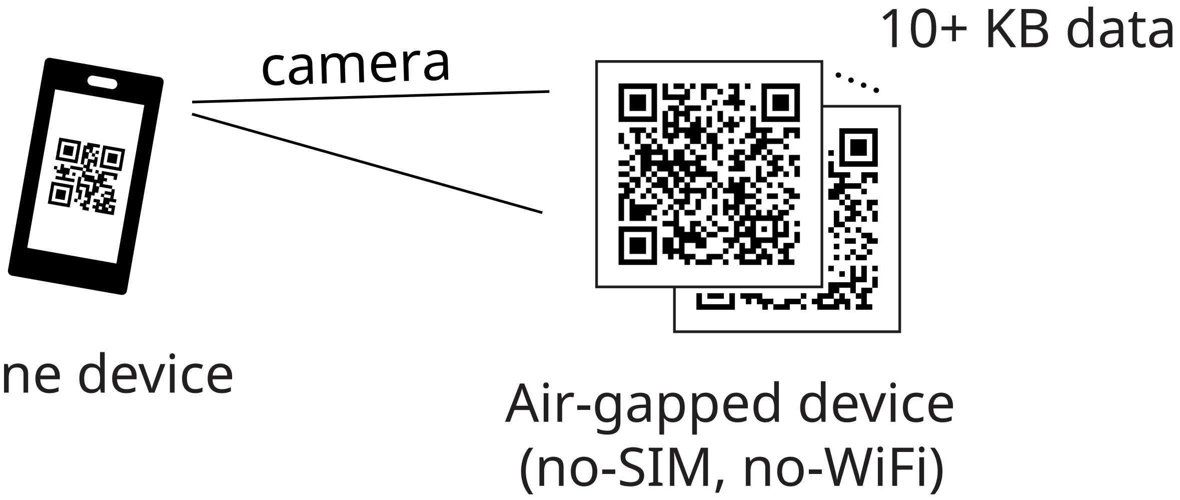


(1) Using media (e.g. USB sticks, SD cards) over air gap

(2) Showing and scanning multiple QR codes

(3) Online device with key share direct contact via API

In Case of (2) QR Code Channel



10+ KB data

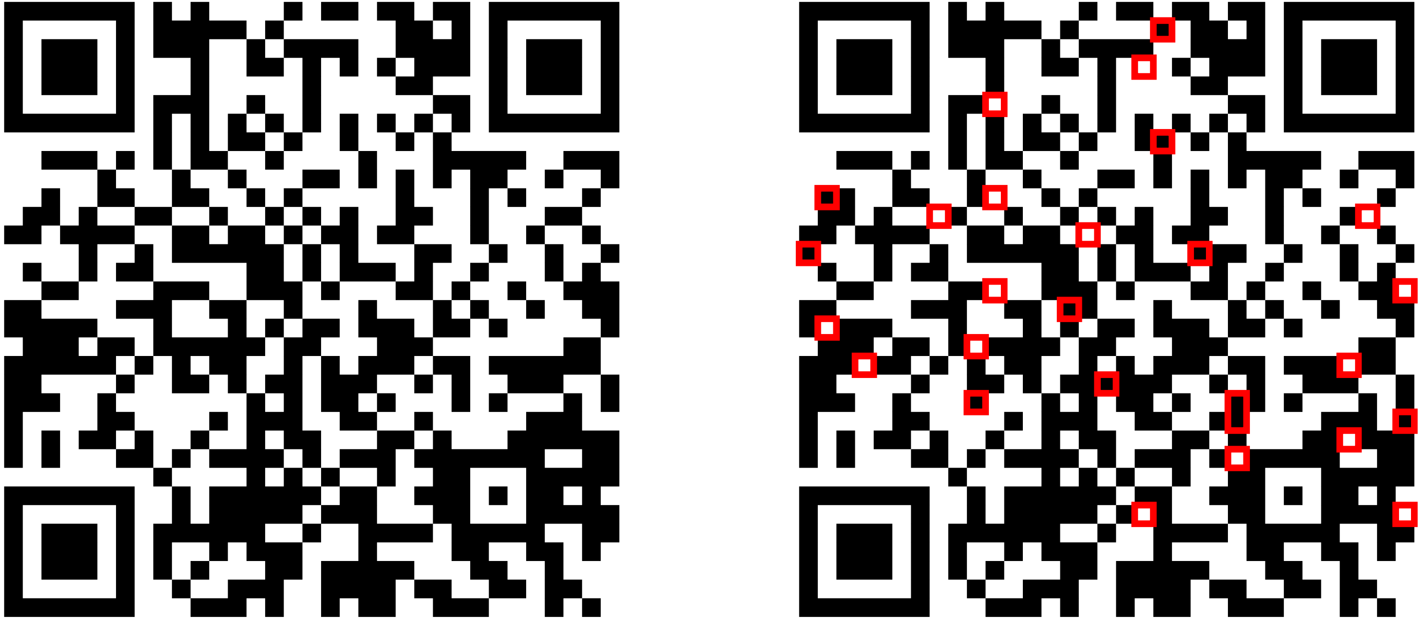
camera

Online device

Air-gapped device
(no-SIM, no-WiFi)

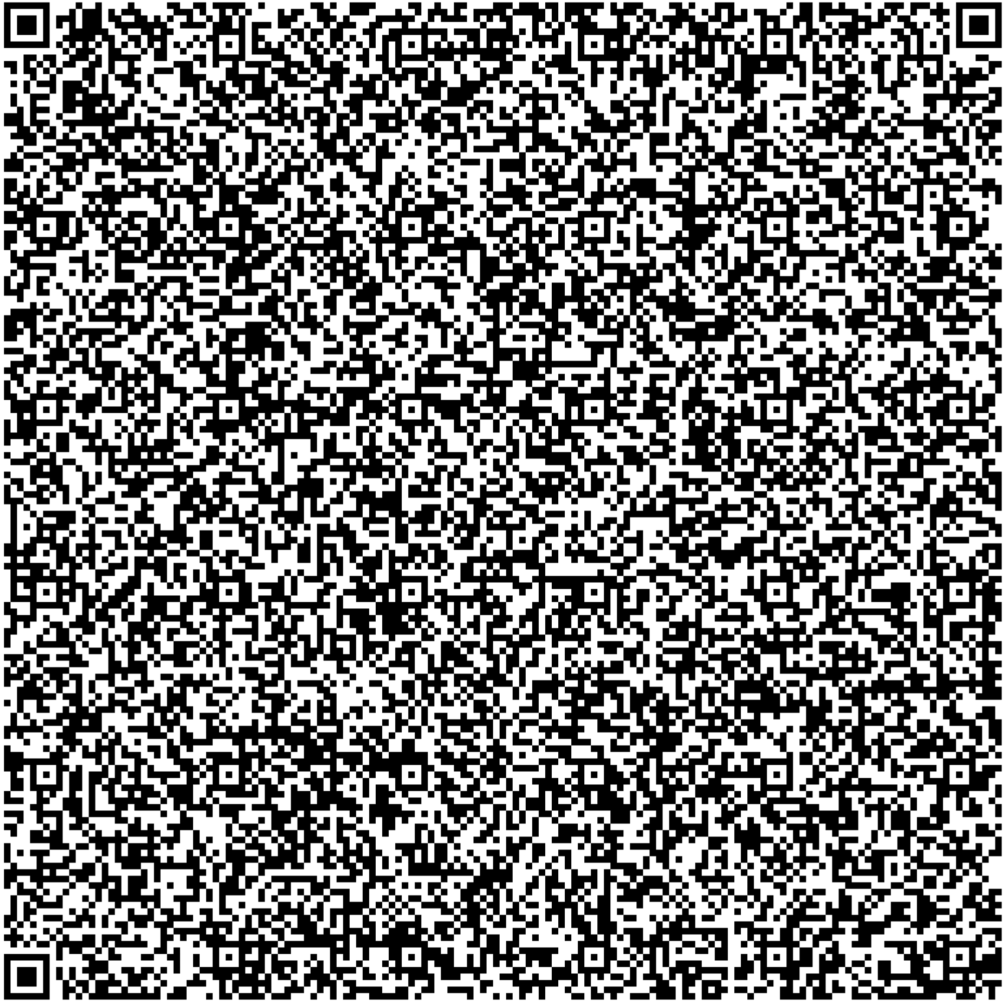
🧩 Key share = 256 bits

Example of Data Embedding in QR Codes

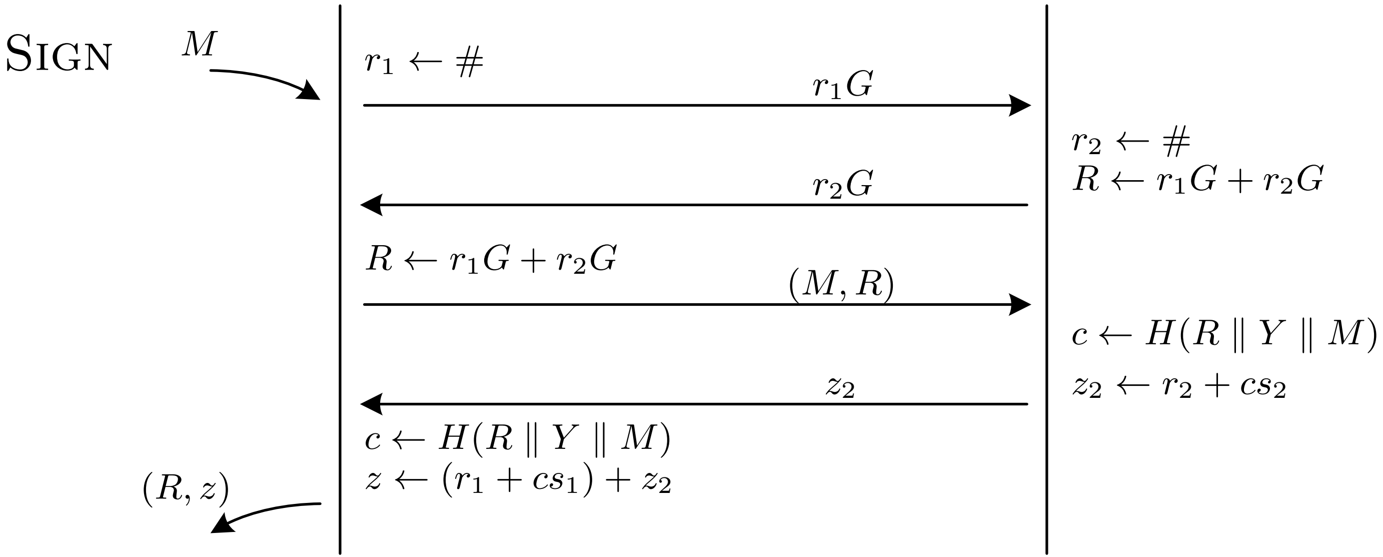


Demo at https://takeiyuto.github.io/qr

300 bytes Embedded in 1024 bytes



Secret Injection in Random Numbers



SIGN M

$r_1 \leftarrow \#$

r_1G

$r_2 \leftarrow \#$
$R \leftarrow r_1G + r_2G$

r_2G

$R \leftarrow r_1G + r_2G$

(M, R)

$c \leftarrow H(R \parallel Y \parallel M)$
$z_2 \leftarrow r_2 + cs_2$

z_2

$c \leftarrow H(R \parallel Y \parallel M)$
$z \leftarrow (r_1 + cs_1) + z_2$

(R, z)

s_2 (secret share) are random bits 01001011...
r_2G also contains random bits 11010101...

Choose r_2 so that certain bit of r_2G matches the bit from s_2

Extending to Real-World Case

Number of key shares:

- As long as a vendor holds 1 key share, not limited to $n = 2$. Applies to the case with $n > 2$ shares as well.

Communication between user and vendor:

- If plaintext: Fault injection is feasible as demonstrated.
- If encrypted: Even more direct attacks can be done.

Countermeasures and Security Management

Data sanitization

- Eliminate the potential for fault injection.

Code audit

- Checks for vulnerabilities and potential backdoors in the code.
- Includes external dependency libraries.

Open-source MPC implementation

- Allows for community review and transparency.

Summary

MPC wallet has a security advantage without a trusted party.

However:

- Do not blindly trust vendor implementations.
- Ensure to use implementations with security due diligence.

Otherwise:

- Same as “Not Your Key, Not Your Coin”, where you entrust your keys without knowing how they are treated.