Securing Bitcoin wallets: A new DSA threshold signature scheme that is usable in the real world


Rosario Gennaro, Steven Goldfeder, Arvind Narayanan
Spending bitcoins is controlled by crypto

"Pay coin c to <Bob’s address>"

Signed by Alice’s private key

Alice’s device

Bitcoin P2P network

Alice’s device containing her key is a single point of failure
Your bitcoins are as secure as your private keys
Bitcoin hacks, thefts, losses

<table>
<thead>
<tr>
<th>Rank</th>
<th>Name</th>
<th>Severity (January 2014 ₿)</th>
<th>USD Equivalent</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2014 Mt. Gox Collapse</td>
<td>850000.000 ₿</td>
<td>700258171 $</td>
</tr>
<tr>
<td>2</td>
<td>Silk Road Seizure</td>
<td>32716.283 ₿</td>
<td>26867560 $</td>
</tr>
<tr>
<td>3</td>
<td>Sheep Marketplace Incident</td>
<td>4978.276 ₿</td>
<td>4070923 $</td>
</tr>
<tr>
<td>4</td>
<td>Silk Road 2 Incident</td>
<td>4400.000 ₿</td>
<td>3624866 $</td>
</tr>
<tr>
<td>5</td>
<td>GBL Scam</td>
<td>4185.734 ₿</td>
<td>3437446 $</td>
</tr>
<tr>
<td>6</td>
<td>MintPal Incident</td>
<td>3894.492 ₿</td>
<td>3208412 $</td>
</tr>
<tr>
<td>7</td>
<td>Bitcoin Savings and Trust</td>
<td>3700.408 ₿</td>
<td>2983473 $</td>
</tr>
<tr>
<td>8</td>
<td>PicoStocks Hack</td>
<td>3679.520 ₿</td>
<td>3009397 $</td>
</tr>
<tr>
<td>9</td>
<td>MyBitcoin Theft</td>
<td>1395.691 ₿</td>
<td>1072570 $</td>
</tr>
<tr>
<td>10</td>
<td>CryptoRush Theft</td>
<td>950.000 ₿</td>
<td>782641 $</td>
</tr>
</tbody>
</table>
Almost half of exchanges hacked

45% of Bitcoin exchanges shut down over three year observation period, many due to hacks

[Moore and Christin, 2013]
Avoiding a single point of failure

- Split your key between multiple devices
- Designate your address as protected by multiple keys
Bitcoin multisignatures

• Associate $n$ keys with an address
• Specify a threshold $t$ of keys that must sign to spend from that address
Multi-sig ruins anonymity
Multi-sig ruins anonymity
Multisig at a company

Joint control between 3 employees
Imagine one employee is replaced

Money must be moved on the block chain!

Access structure is public
Multisignatures could reveal too much about security internals to external world

And they’re bad for user privacy
Splitting your key: threshold signatures
Informal definition: 
$t$-out-of-$n$ threshold signature scheme

The secret key is shared among $n$ players s.t.

- **Correctness:**
  any $t+1$ of them can jointly sign any given message

- **Security:**
  no $t$ colluding players can forge signature
Advantages of splitting your key

Threshold signature is indistinguishable from a regular signature

Address looks like a standard address
Digital Signature Algorithm (DSA)

Given

- a group $G$ of order $N$
- a generator $g$
- a private key $x$

To sign a message $m$:

- pick a nonce $k$ s.t. $1 \leq k \leq N - 1$
- $r = g^k$
- $s = k^{-1}(m + x \cdot r) \mod N$

Signature is $(r,s)$

Bitcoin uses an instantiation of DSA on elliptic curves
Nonce $k$ must be kept secret

Knowledge of $k$ together with signature leaks the key

$$r = g^k$$
$$s = k^{-1}(m + x \cdot r) \mod N$$

$$s = k^{-1}(m + x \cdot r) \mod N$$

$$\Rightarrow$$

$$x \equiv_N (s \cdot k - m) r^{-1}$$
GJKR Threshold DSA

Includes multiplication of Shamir shares

\[ r = g^k \]
\[ s = k^{-1}(m + x \cdot r) \mod N \]

Problem: Multiplication

If $a$ and $b$ are shared on degree-$t$ polynomials

$a \cdot b$ will be shared on a degree-$2t$ polynomial

$\rightarrow$ Need $2t + 1$ players to sign

BUT $t + 1$ corrupted players can compromise security!
Not useful for Bitcoin

Need $2t + 1$ players to sign
BUT $t + 1$ corrupted players can compromise security

2-out-of-2 threshold not possible
Specifically for the two party case (which was unrealizable with GJKR)

We show how this can be extended to t-of-n, but the resulting scheme is very inefficient: key size and computation time grow exponentially with $t$

Our scheme

Threshold homomorphic encryption $\rightarrow$ threshold sig
(Threshold Paillier)

Secret sharing — each player gets:
- a share of a Paillier decryption key
- $\text{Enc}(x)$ encrypted under corresponding public key

Signature: compute $\text{Enc}(s)$, then threshold decrypt

$r = g^k$
$s = k^{-1}(m + x \cdot r) \mod N$
Recall: multiplication by scalar inside additively homomorphic encryption

Additively homomorphic encryption $E$

$E(cx) = E(x + \ldots + x) = E(x + \ldots + x) \hat{\otimes} E(x + \ldots + x)$

$r = g^k$
$s = k^{-1}(m + x \cdot r) \mod N$
$r = g^k$
$s = k^{-1}(m + x \cdot r) \mod N$

Everyone knows

$\rho_1 \cdot x + \rho_2 \cdot x + \rho_3 \cdot x = \rho \cdot x$

$\rho_1 \cdot \rho_1 + \rho_2 \cdot \rho_2 + \rho_3 \cdot \rho_3 = \rho$

ZKP of consistency

ZKP of consistency

ZKP of consistency
$r = g^k$
$s = k^{-1}(m + x \cdot r) \mod N$

$\rho^{-1}k^{-1}$

ZKP of consistency
ZKP of consistency
ZKP of consistency
Every player computes

Final step: players threshold decrypt $s$. 

\[ r = g^k \]
\[ s = k^{-1}(m + x \cdot r) \mod N \]
Why is our scheme different?

**GJKR**

$t+1$ players can sign. There is no Shamir multiplication, so no need for $2t + 1$ participants.

**MR**

works for $t$-of-$n$ with constant storage, fixed number of rounds and constant per-player computation time
Dealerless protocol

How does each party initially get their share of $x$?

- **Existing key**: a trusted dealer who knows $x$ distributes shares

- **Fresh key**: Each party can independently generate their key share (for both the Paillier and DSA keys)
What if a player is replaced by another?

Still no need to reconstruct the secret!
Future Research: Building Secure protocols

How can we use threshold signatures to build secure protocols?
Building Secure Protocols: Coinbase

Could use threshold signatures for cold storage

Currently use secret-sharing based protocol that requires key reconstruction
Building Secure Protocols: Trezor

Can combine threshold signatures with secure hardware
Building Secure Protocols: OpenBazaar

- Escrow: Buyer and seller jointly choose mediator set
- Buyer and seller can jointly move money out of escrow
- buyer or seller together with a majority of mediators can move money out of escrow