"Act natural!": Exchanging Private Messages on Public Blockchains

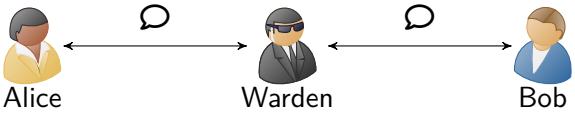
Thore Tiemann, Sebastian Berndt, Thomas Eisenbarth, Maciej Liśkiewicz

University of Lübeck, Lübeck, Germany

EuroS&P 2023, July 3–7 2023

UNIVERSITÄT ZU LÜBECK
INSTITUTE FOR IT SECURITY

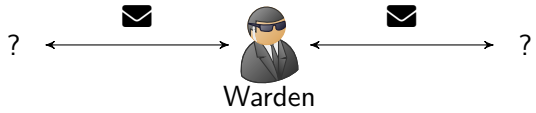
Motivation



Motivation

- Encryption hide the *contents*

Motivation



- Encryption — hide the *contents*
- Anonymity systems — hide the *identities*

Motivation


Warden

- Encryption — hide the *contents*
- Anonymity systems — hide the *identities*
- Steganography — hide the *presence*

Motivation

Warden

- Encryption — hide the *contents*
- Anonymity systems — hide the *identities*
- Steganography — hide the *presence*

Motivation


Warden

- Encryption — hide the *contents*
- Anonymity systems — hide the *identities*
- Steganography — hide the *presence*

Motivation

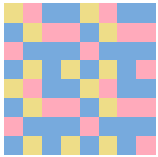
Steganography

- Multimedia applications

Motivation

Steganography

- Multimedia applications
- Cryptographic systems



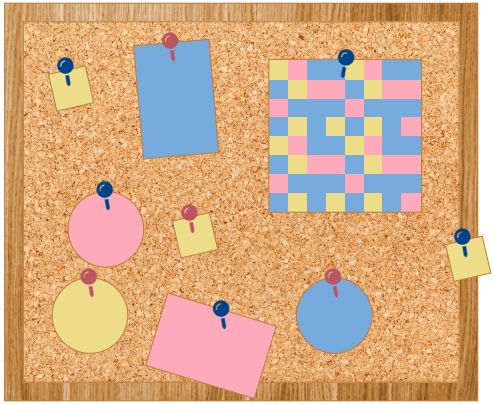
Motivation

Steganography

- Multimedia applications
- Cryptographic systems

Blockchain bulletin board

- Transaction scripts



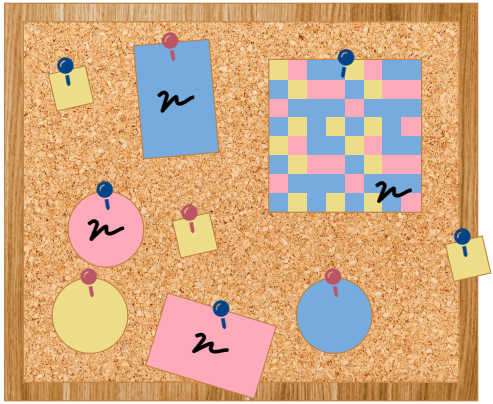
Motivation

Steganography

- Multimedia applications
- Cryptographic systems

Blockchain bulletin board

- Transaction scripts
- Digital signatures



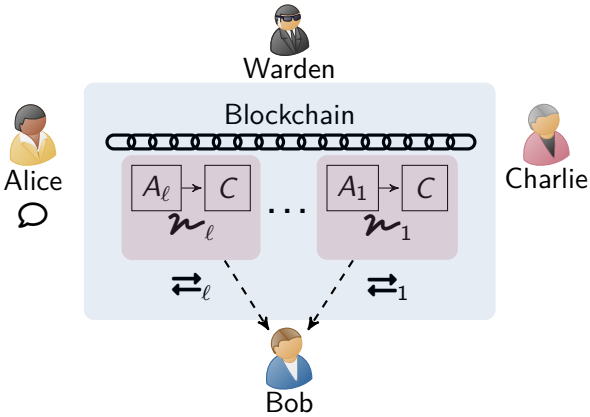
Motivation

Our goal

Hide messages in digital signatures on public blockchains

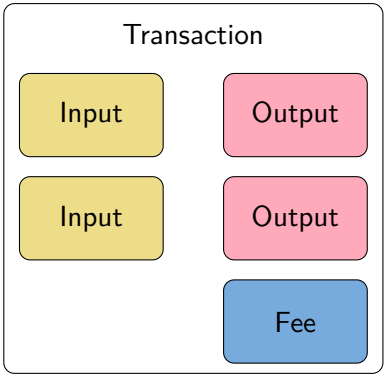
Motivation

Scenario



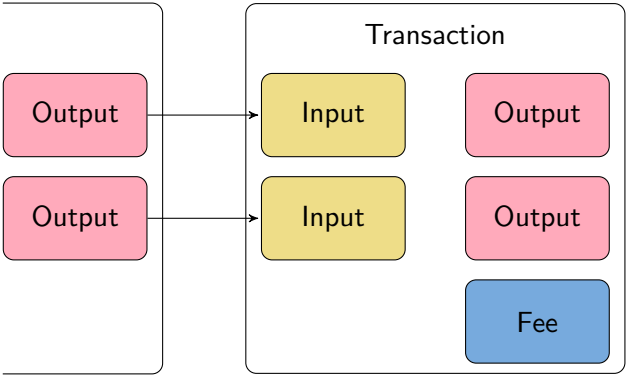
Background

Bitcoin Transactions



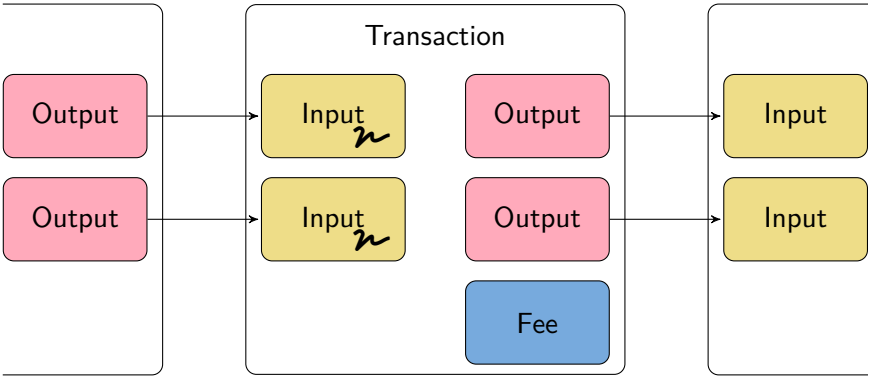
Background

Bitcoin Transactions



Background

Bitcoin Transactions



Background

Splittable signature schemes

- Signature has randomness- and message-binding part

Y. Wang et al., "Asymmetric subversion attacks on signature and identification schemes", 2022

D. Frkat et al., "ChainChannels: Private botnet communication over public blockchains", 2018

Background

Splittable signature schemes

- Signature has randomness- and message-binding part
- Randomness exchangeability

Y. Wang et al., "Asymmetric subversion attacks on signature and identification schemes", 2022

D. Frkat et al., "ChainChannels: Private botnet communication over public blockchains", 2018

Background

Splittable signature schemes

- Signature has randomness- and message-binding part
- Randomness exchangeability
- Signing key recoverability

Y. Wang et al., "Asymmetric subversion attacks on signature and identification schemes", 2022

D. Frkat et al., "ChainChannels: Private botnet communication over public blockchains", 2018

Background

Splittable signature schemes

- Signature has randomness- and message-binding part
- Randomness exchangeability
- Signing key recoverability

ECDSA, Schnorr, MLSAG
Used by 98 of top-100 blockchains

Y. Wang et al., "Asymmetric subversion attacks on signature and identification schemes", 2022

D. Frkat et al., "ChainChannels: Private botnet communication over public blockchains", 2018

Background

Splittable signature schemes

- Signature has randomness- and message-binding part
- Randomness exchangeability
- Signing key recoverability

ECDSA, Schnorr, MLSAG
Used by 98 of top-100 blockchains

ECDSA Sign

Y. Wang et al., "Asymmetric subversion attacks on signature and identification schemes", 2022

D. Frkat et al., "ChainChannels: Private botnet communication over public blockchains", 2018

Background

Splittable signature schemes

- Signature has randomness- and message-binding part
- Randomness exchangeability
- Signing key recoverability

ECDSA, Schnorr, MLSAG
Used by 98 of top-100 blockchains

ECDSA Sign

1. Choose (pseudo-) random nonce k

Y. Wang et al., "Asymmetric subversion attacks on signature and identification schemes", 2022

D. Frkat et al., "ChainChannels: Private botnet communication over public blockchains", 2018

Background

Splittable signature schemes

- Signature has randomness- and message-binding part
- Randomness exchangeability
- Signing key recoverability

ECDSA, Schnorr, MLSAG
Used by 98 of top-100 blockchains

ECDSA Sign

1. Choose (pseudo-) random nonce k
2. Compute $(x, y) = k \cdot G$

Y. Wang et al., "Asymmetric subversion attacks on signature and identification schemes", 2022

D. Frkat et al., "ChainChannels: Private botnet communication over public blockchains", 2018

Background

Splittable signature schemes

- Signature has randomness- and message-binding part
- Randomness exchangeability
- Signing key recoverability

ECDSA, Schnorr, MLSAG
Used by 98 of top-100 blockchains

ECDSA Sign

1. Choose (pseudo-) random nonce k
2. Compute $(x, y) = k \cdot G$
3. Compute $s = (\rightleftarrows + x \cdot$  $) \cdot k^{-1}$

Y. Wang et al., "Asymmetric subversion attacks on signature and identification schemes", 2022

D. Frkat et al., "ChainChannels: Private botnet communication over public blockchains", 2018

Background

Splittable signature schemes

- Signature has randomness- and message-binding part
- Randomness exchangeability
- Signing key recoverability

ECDSA, Schnorr, MLSAG
Used by 98 of top-100 blockchains

ECDSA Sign

1. Choose (pseudo-) random nonce k
2. Compute $(x, y) = k \cdot G$
3. Compute $s = (\rightleftarrows + x \cdot$  $) \cdot k^{-1}$
4. Publish signature $\mathscr{n} = (x, s)$

Y. Wang et al., "Asymmetric subversion attacks on signature and identification schemes", 2022

D. Frkat et al., "ChainChannels: Private botnet communication over public blockchains", 2018

Background

Splittable signature schemes

- Signature has randomness- and message-binding part
- Randomness exchangeability
- Signing key recoverability

ECDSA, Schnorr, MLSAG
Used by 98 of top-100 blockchains

ECDSA Sign

1. Choose (pseudo-) random nonce k
2. Compute $(x, y) = k \cdot G$
3. Compute $s = (\rightleftarrows + x \cdot$  $) \cdot k^{-1}$
4. Publish signature $\mathcal{N} = (x, s)$

Embedding

- Replace k with pseudo-random ciphertext

Y. Wang et al., "Asymmetric subversion attacks on signature and identification schemes", 2022

D. Frkat et al., "ChainChannels: Private botnet communication over public blockchains", 2018

Background

Splittable signature schemes

- Signature has randomness- and message-binding part
- Randomness exchangeability
- Signing key recoverability

ECDSA, Schnorr, MLSAG
Used by 98 of top-100 blockchains

ECDSA Sign

1. Choose (pseudo-) random nonce k
2. Compute $(x, y) = k \cdot G$
3. Compute $s = (\rightleftarrows + x \cdot$  $) \cdot k^{-1}$
4. Publish signature $\mathcal{N} = (x, s)$

Embedding

- Replace k with pseudo-random ciphertext

Extraction

- Leak  to recover k

Y. Wang et al., "Asymmetric subversion attacks on signature and identification schemes", 2022

D. Frkat et al., "ChainChannels: Private botnet communication over public blockchains", 2018

Background

Problems

- How to leak  ?
- Nonce reuse possible

Construction

- RFC6979

NonceGenChat(⇄, 🔑₿)

1 :
2 : $k \leftarrow$ HMAC(🔑₿ ‖ ⇄)
3 :
4 : **return** k
5 :
6 :

🔑: Secret key 🔑: Public key

Construction

Exchanged out-of-band

- RFC6979
- Chat key pair ( , )

NonceGenChat(⇄ , )

1 :  , 

2 : $k \leftarrow$ HMAC( $\|$ ⇄)

3 :

4 : **return** k

5 :

6 :

 : Secret key  : Public key

Construction

- RFC6979
- Chat key pair ($\bigcirc$, $\bigcirc$)
- Non-interactive key exchange

Computable by receiver
Allows $\bigcirc$ recovery

NonceGenChat($\rightleftarrows$, $\bigcirc$)

1 : $\bigcirc_A$, $\bigcirc_B$, $\bigcirc$
2 : $k \leftarrow \mathrm{H}(\mathrm{ECDH}(\bigcirc_A, \bigcirc_B) \| \bigcirc)$
3 :
4 : **return** k
5 :
6 :

$\bigcirc$: Secret key $\bigcirc$: Public key

Construction

- RFC6979
- Chat key pair ($\overset{\bigcirc}{\blacksquare}$, $\overset{\bigcirc}{\blacksquare}$)
- Non-interactive key exchange
- Embed message

NonceGenChat($\rightleftarrows$, $\overset{\bigcirc}{\blacksquare}^{B}$)

1 : $\overset{\bigcirc}{\blacksquare}_A, \overset{\bigcirc}{\blacksquare}_B, \bigcirc$

2 : $k \leftarrow \mathrm{H}(\mathrm{ECDH}(\overset{\bigcirc}{\blacksquare}_A, \overset{\bigcirc}{\blacksquare}_B) \| \overset{\bigcirc}{\blacksquare}^{B})$

3 : **if** $\bigcirc = \emptyset$:

4 : **return** k

5 : $iv \leftarrow \mathrm{H}(\bigcirc)$

6 : **return** $\mathrm{AES}(\bigcirc, k, iv)$

$\overset{\bigcirc}{\blacksquare}$: Secret key $\overset{\bigcirc}{\blacksquare}$: Public key

Construction

- RFC6979
- Chat key pair ($\chat_A$, $\chat_B$)
- Non-interactive key exchange
- Embed message
- Prevent nonce reuse

NonceGenChat($\rightleftarrows$, $\bitcoin$)

1 : $\chat_A, \chat_B, \chat$
2 : $k \leftarrow \mathrm{H}(\mathrm{ECDH}(\chat_A, \chat_B) \| \bitcoin)$
3 : **if** $\chat = \emptyset$:
4 : **return** k
5 : $iv \leftarrow \mathrm{H}(\mathrm{H}(\rightleftarrows) \| k)$
6 : **return** $\mathrm{AES}(\chat, k, iv)$

: Secret key : Public key

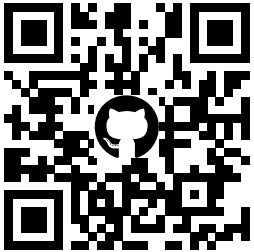
Evaluation

Algorithm	min (μs)	avg (μs)	max (μs)
AES-NI-CBC ENC (w/ KE)	0.0612	0.0631	0.0691
AES-NI-CBC DEC (w/ KE)	0.0611	0.0622	0.0639
SHA256	0.525	0.529	0.546
ECDH	49.2	50.2	51.9
NonceGenRFC6979	6.22	6.37	6.56
NonceGenChat	55.2	56.7	58.1
SignBTC	41.5	42.4	43.5
SignChat	90.9	92.9	93.9

1,000,000 runs on an Intel Core i5-7600 CPU

Conclusions

- Embedding into splitable signatures
- Bi-directional communication
- Constant overhead
- Reusable communication keys
- Optimal embedding rate
- Provably undetectable



Conclusions

- Embedding into splitable signatures
- Bi-directional communication
- Constant overhead
- Reusable communication keys
- Optimal embedding rate
- Provably undetectable

Thore Tiemann
@ t.tiemann@uni-luebeck.de
@ThoreTiemann
https://www.its.uni-luebeck.de/en/staff/thore-tiemann.html

Thank you for your attention!