chaincode

Schnorr Signatures

Digital Signatures

1976 - “New Directions in Cryptography” - Whitfield Diffie & Martin Hellman.

“Widening applications of teleprocessing have given rise to a need for new types of cryptographic systems,... and supply the equivalent of a written signature…
A second problem, amenable to cryptographic solution, which stands in the way of replacing contemporary business communications by teleprocessing systems is authentication…
It must be easy for anyone to recognize the signature as authentic, but impossible for anyone other than the legitimate signer to produce it”

1977 - “A Method for Obtaining Digital Signatures and Public-Key Cryptosystems” - Rivest & Shamir & Adleman.

History of Digital signatures

Elgamal Signatures (1985) - $sk = e - kG_x d$

ECDSA - NIST/ANSI (1997) - $sk = e + kG_x d$

Schnorr Signatures (1991) - $s = k + ed$
(patent expired 2008)

$$Sig(s, kG)$$
$$Sig(s, R)$$

Glossary
m - Message.
$e = H(m)$
d = Private Key.
k = Random nonce
G = Generator Point.
Point = scalar*G = (x,y)
Public key = dG

© Elichai Turkel

chaincode

Now the fun begins

Multi Signatures

$$P_1 = d_1 G, \quad P_2 = d_2 G$$

$$s_1 = k_1 + ed_1, \quad s_2 = k_2 + ed_2$$

$$s_1 + s_2 = (k_1 + k_2) + e(d_1 + d_2)$$

$$s' = k' + ed'$$

$$P' = (d_1 + d_2)G$$

Glossary

m - Message.

$e = H(m)$

d = Private Key.

k = Random nonce

G = Generator Point.

Point = scalar*G = (x,y)

Public key = dG

Pay to Contract

$$P' = P + H(P||s)G$$

$$d' = d + H(P||s)$$

Glossary

m - Message.

$$e = H(m)$$

d = Private Key.

k = Random nonce

G = Generator Point.

Point = scalar*G = (x,y)

Public key = dG

Sign to contract

$$\boldsymbol{s = k + ed}$$

$$k' = k + H(R||c)$$

$$R' = R + H(R||c)G$$

Glossary

m - Message.

$e = H(m)$

d = Private Key.

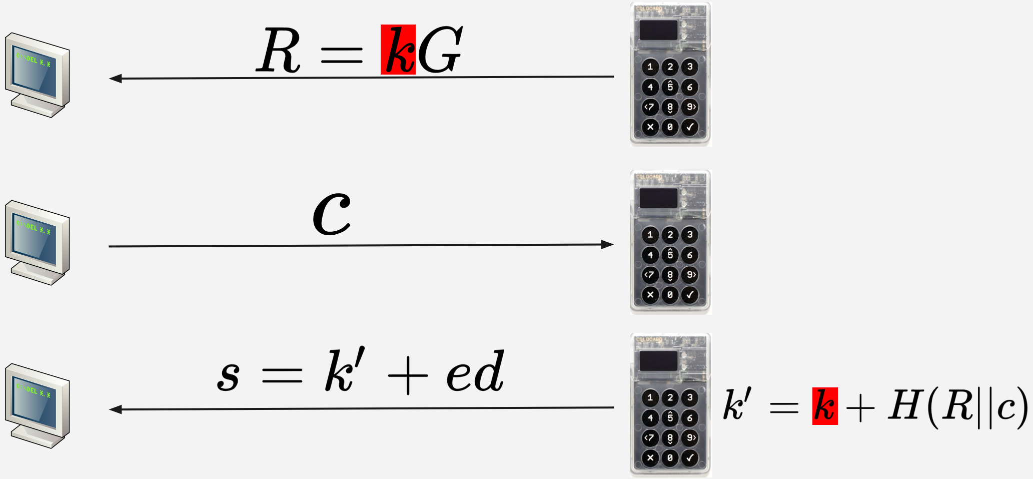
k = Random nonce

G = Generator Point.

Point = scalar*G = (x,y)

Public key = dG

Anti Nonce Covert Channel



$$R = kG$$

$$c$$

$$s = k' + ed$$

$$k' = k + H(R||c)$$

Glossary

m - Message.

$$e = H(m)$$

d = Private Key.

k = Random nonce

G = Generator Point.

Point = scalar*G = (x,y)

Public key = dG

Adaptor Signatures

$$s'_1 = k_1 + ed_1 + t$$

$$AdapSig(s', kG, tG)$$

$$s_2 = k_2 + ed_2$$

$$s' = (k_1 + k_2) + e(d_1 + d_2)$$

$$t = s' - s2 - s'_1 \quad s_1 = s'_1 - t$$

Glossary

m - Message.

$$e = H(m)$$

d = Private Key.

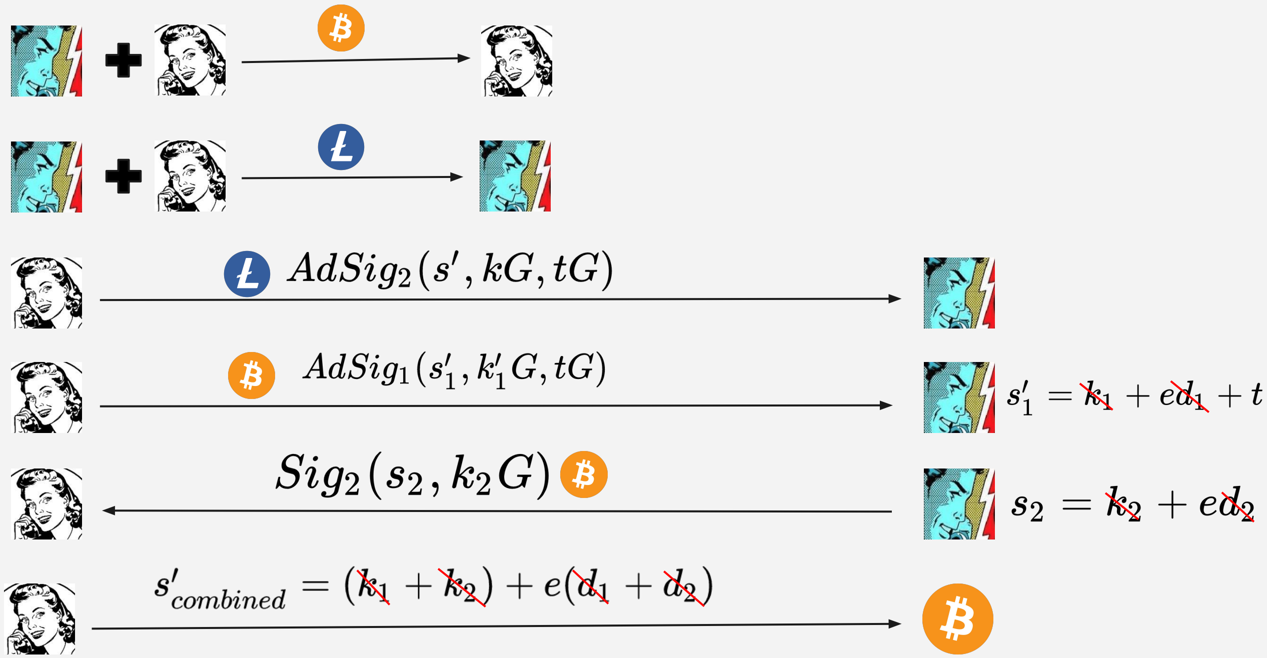
k = Random nonce

G = Generator Point.

Point = scalar*G = (x,y)

Public key = dG

Atomic Swap



$$AdSig_2(s', kG, tG)$$

$$AdSig_1(s'_1, k'_1G, tG)$$

$$s'_1 = \cancel{k_1} + e\cancel{d_1} + t$$

$$Sig_2(s_2, k_2G)$$

$$s_2 = \cancel{k_2} + e\cancel{d_2}$$

$$s'_{combined} = (\cancel{k_1} + \cancel{k_2}) + e(\cancel{d_1} + \cancel{d_2})$$

Glossary

m - Message.

$$e = H(m)$$

d = Private Key.

k = Random nonce

G = Generator Point.

Point = scalar*G = (x,y)

Public key = dG

chaincode

Thank you and questions?

chaincode