From RSA to Camenisch-Lysyanskaya in 5 minutes

Maja Reißner

October 18, 2022

Privacy - Selective Disclosure And Unlinkability

Coronavirus pass

Maja Reißner
has a vaccination proof
which expires 30.10.2022.

Privacy - Selective Disclosure And Unlinkability

Coronavirus pass

Maja Reißner
has a vaccination proof
which expires 30.10.2022.

sign

Coronavirus pass

Maja Reißner
has a **xxxxxxxxx** proof
which expires 30.10.2022.

sign

RSA $\Rightarrow$ Camenisch-Lysyanskaya

Textbook RSA:

$$A = M^d \bmod n$$

Verify with:

$$A^e = M \bmod n$$

Coronavirus pass

Maja Reißner
has a vaccination proof
which expires 30.10.2022.

sign

RSA $\Rightarrow$ Camenisch-Lysyanskaya

Textbook RSA:

$$A = M^d \bmod n$$

Verify with:

$$A^e = M \bmod n$$

Camenisch-Lysyanskaya signature scheme:

$$M = \frac{Z}{S^v R_1^{a_1} R_2^{a_2} R_3^{a_3}}$$

Coronavirus pass

Maja Reißner
has a vaccination proof
which expires 30.10.2022.

sign

Coronavirus pass

name: **Maja Reißner**,
type: **vaccination**,
expiration: **30.10.2022**

A, e, v

RSA $\Rightarrow$ Camenisch-Lysyanskaya

Textbook RSA:

$$A = M^d \bmod n$$

Verify with:

$$A^e = M \bmod n$$

Camenisch-Lysyanskaya signature scheme:

$$M = \frac{Z}{S^v R_1^{a_1} R_2^{a_2} R_3^{a_3}}$$

$$\boldsymbol{A^e = \frac{Z}{S^v R_1^{a_1} R_2^{a_2} R_3^{a_3}} \bmod n}$$

Coronavirus pass

Maja Reißner
has a vaccination proof
which expires 30.10.2022.

sign

Coronavirus pass

name: **Maja Reißner**,
type: **vaccination**,
expiration: **30.10.2022**

A, e, v

Selective Disclosure

$$A^e = \frac{Z}{S^v R_1^{a_1} R_2^{a_2} R_3^{a_3}} \bmod n$$

$$H = R_2^{a_2}$$

Coronavirus pass

name: **Maja Reißner**,
type: **xxxxxxxx**,
expiration: **30.10.2022**

A, e, v

Selective Disclosure

$$A^e = \frac{Z}{S^v R_1^{a_1} R_2^{a_2} R_3^{a_3}} \bmod n$$

$$H = R_2^{a_2}$$

$$\boldsymbol{A^e = \frac{Z}{S^v R_1^{a_1} H R_3^{a_3}} \bmod n}$$

Coronavirus pass

name: **Maja Reißner**,
type: **xxxxxxxx**,
expiration: **30.10.2022**

A, e, v

Unlinkability

$$A^e = \frac{Z}{S^v R_1^{a_1} H R_3^{a_3}} \bmod n$$

Coronavirus pass

name: **Maja Reißner**,
type: **xxxxxxxx**,
expiration: **30.10.2022**

A, e, v

Unlinkability

$$\tilde{A}^e = \frac{Z}{S^{\tilde{v}} R_1^{a_1} H R_3^{a_3}} \bmod n$$

Modify equation:

$$\tilde{A} = AS^r \bmod n \qquad \tilde{v} = v - er$$

Coronavirus pass

name: **Maja Reißner**,
type: **xxxxxxxx**,
expiration: **30.10.2022**

RSA $\Rightarrow$ Camenisch-Lysyanskaya

$$A^e = M \bmod n$$

$$\Downarrow$$

$$\boldsymbol{A^e = \frac{Z}{S^v R_1^{a_1} R_2^{a_2} R_3^{a_3}} \bmod n}$$

Coronavirus pass

Maja Reißner
has a vaccination proof
which expires 30.10.2022.

sign

Coronavirus pass

name: **Maja Reißner**,
type: **xxxxxxxx**,
expiration: **30.10.2022**

$\tilde{A}, x, x$

The end.