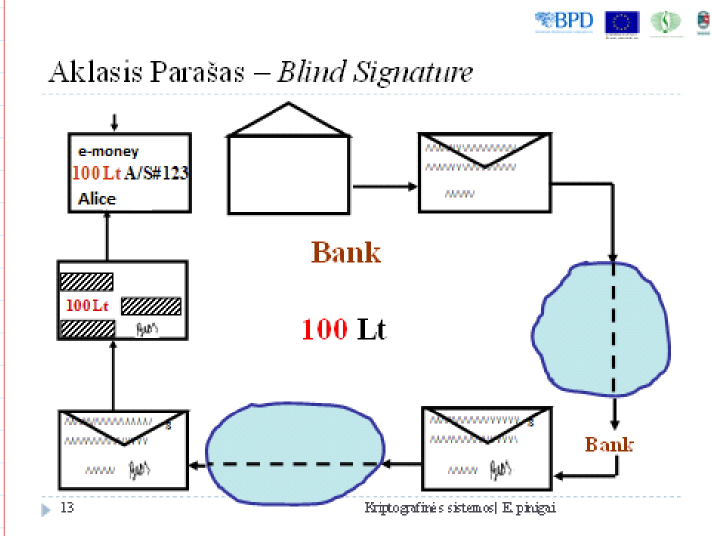
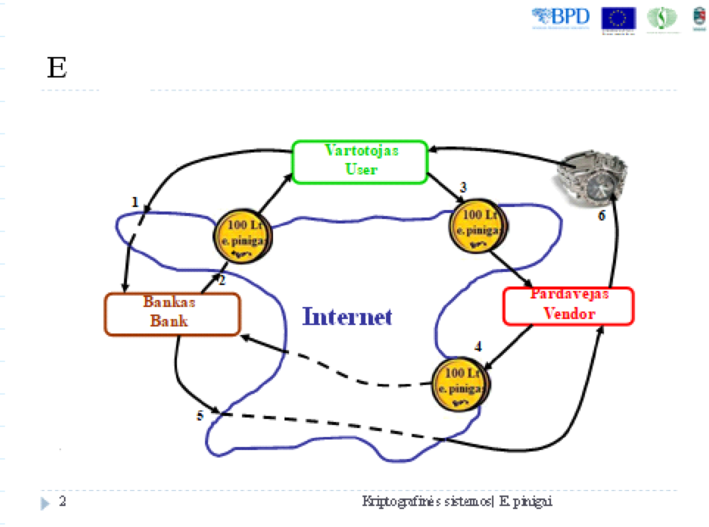
Moodle:
https://moodle.ktu.edu/pluginfile.php/739818/mod_resource/content/2/Kriptologijos%20modulio%20P170B111%20egzaminas.pdf





Withdrawal, Payment and Deposit protocols.

Property: the only customer **Alice** can create and is responsible for Random Identification String - RIS during the Withdrawal protocol.

Questions:
1.Is it possible for **Alice** to modify e-coin $\prod$.
1.How vendor **Victor** can cheat against **Bank** and how it is prevented?

E-coin properties.
1.**Anonimity**.
2.**Untraceability**.
3.**Double-spending prevention**.
4.**Divisibility**.

International Association for Cryptographic Research - IACR Barcelona, 2008, announced results:
1.Divisible e-money can be trully anonymous.
2.Divisible and trully anonymous e-money grow in size during their transfers.

Cut and choose paradigm

A : 50 claims to withdraw e-money from B.

$m_1 = 100,\ m_2 = 100, \ldots, m_{50} = 100.$

$t_1 \leftarrow randi,\ t_2 \leftarrow randi,\ t_{50} \leftarrow randi.$

$m_1' = m_1 \cdot t_1^e \bmod n, \ldots, m_{50}' = m_{50} \cdot t_{50}^e \bmod n.$

2% of A cheating $\xrightarrow{m_1', m_2', \ldots, m_{50}'}$ B: $m_i' \leftarrow \text{rand}\{m_1', \ldots, m_{50}'\}$

$\xleftarrow{m_1', \ldots, m_{i-1}', m_{i+1}', \ldots, m_{50}'}$

$Pr = \frac{1}{50} = 0.02$

$\xrightarrow{t_1, \ldots, t_{i-1}, t_{i+1}, \ldots, t_{50}}$ If $m_1' = m_1 \cdot t_1^e \bmod n$

$\xleftarrow{\sigma_i'}$ $\text{Sign}(PrK = d, m_i') = (m_i')^d \bmod n = \sigma_i'$

By collecting all m_j, $j = 1, 2, \ldots, i-1, i+1, \ldots, 50$,
B verifies: 1) if all m_j has the same value?
2) if A account sum $s > m_j$?
If Yes then B blindly signs remaining value m_i'

1 mod ϕ

$\sigma_i' = (m_i')^d \bmod n = (m_i \cdot t_i^e)^d = m_i^d\, t \bmod n$

The probability for A to cheat is: $Pr(\text{cheating}) = \frac{1}{50}$

A: is unmasking σ_i' and obtains

$\sigma_i = \sigma_i' \cdot t_i^{-1} \bmod n = m_i^d \bmod n.$

A: verifies σ_i on m_i: $Ver(PuK = (n, e), \sigma_i) = 1 \equiv T$

$m_i = (\sigma_i)^e \bmod n = m_i^{de \bmod \phi} \bmod n = m_i^1 \bmod n = m_i$
if $m_i < n$

A: creates Random Identification String RIS for every m_j':
Then A encodes her name by some binary string $A = 1010$.

$x_{j1} \leftarrow \text{randbin} \rightarrow x_{j1} = 0110$

$\rightarrow x_{j1}' = A \oplus x_{j1} \rightarrow \oplus \begin{array}{c} A \\ x_{j1} \end{array} \rightarrow \oplus \begin{array}{c} 1010 \\ 0110 \end{array}$ ✓

$x_{j1}' = 1100$ ✓

2) Payment protocol

3) Deposit protocol

A computes:

$x_{j1}, x_{j1}'; x_{j2}, x_{j2}'; \ldots; x_{j,50}, x_{j,50}'.$

If x_{jk} and x'_{jk} is revealed, then the identity of $\mathcal{A}$ will be revealed.

E.g. Let x_{j1} and x'_{j1} is known, then

$$A = x_{j1} \oplus x'_{j1} \longrightarrow \oplus \begin{array}{r} 0110 \\ 1100 \\ \hline 1010 \end{array} = A$$

$y_{j1} = H(x_{j1})$, $y'_{j1} = H(x'_{j1})$.

$m'_1 = m_1 \cdot t_1{}^e \bmod n, \ldots, m'_{50} = m_{50} \cdot t_{50}{}^e \bmod n$.

$\Pi'_1 = (m'_1; y_{11}, y'_{11}; \ldots; m'_{1,50}; y_{1,50}, y'_{1,50})$

$\Pi'_2 = ---$

$\Pi'_{50} = ----$

$$\xrightarrow{\Pi'_1, \Pi'_2, \ldots, \Pi'_{50}} \mathcal{B}: \Pi'_i \leftarrow \text{rand}\{\Pi'_1, \ldots, \Pi'_{50}\}$$

$$\xleftarrow{\Pi'_1, \ldots, \Pi'_{i-1}, \Pi'_{i+1}, \ldots, \Pi'_{50}}$$

$$\xrightarrow{t_1, \ldots, t_{i-1}, t_{i+1}, \ldots, t_{50}}$$

Verifies if:

1) all m_j have the same value
2) $\mathcal{A}$ account $s > m_j$

$\mathcal{B}$ blindly signs e-coin Π'_i

$Sig(PrK = d, \Pi'_i) = \sigma'_i$

$$\xleftarrow{\sigma'_i}$$

$\mathcal{A}$: unmasks σ'_i in the same way by computin σ_i on the sum m_i and hence $\mathcal{A}$ has e-coin Π_i consistin of the following:

$\Pi_i = (m_i, \sigma_i, y_{i1}, y'_{i1}; \ldots; y_{i,50}, y'_{i,50})$

↑ not necessary to include since having signature σ_i the value m_i can be computed during the verification phase.

$\sigma_i = M_i^d \bmod n$; $M_i = {}'m_i; y_{i1}, y'_{i1}; \ldots; y_{i,50}, y'_{i,50}{}'$

$Ver(PuK=(n,e), \sigma_i, M_i) = T$

Instead of M_i we will use the notation Π of e-coin.

$\Pi = (m; \sigma; y_1, y_1'; \ldots; y_{50}, y_{50}')$

2. Payment protocol.

$A: \xrightarrow{\Pi}$ V: Victor - vendor verifies

1) If signature on m is a valid B signature
$Ver(PuK=(n,e), \sigma, m) = T$
2) If m value is equal to the price of silver wath.

3) V generates random bit string - RBS consisting of 50 bits

A: is taking RBS $\xleftarrow{RBS}$ E.g. $RBS = '1\ 0\ 1\ 1, \ldots, 0$ ($b_1\ b_2\ b_3\ b_4 \ldots b_{50}$)

and reveals either x_1 if $b_1 = 1$ or x_1' if $b_1 = 0$

x_2 if $b_2 = 1$ or x_2' if $b_2 = 0$

- - - - - - -

x_{50} if $b_{50} = 1$ or x_{50}' if $b_{50} = 0$

$x_1, x_2', x_3, x_4, \ldots, x_{50}' \longrightarrow$ V: verifies

if $H(x_1) = y_1$

if $H(x_2') = y_2'$

- - - - - -

if $H(x_{50}') = y_{50}$

If it is T

A:  $\longleftarrow$

3. Deposit protocol.

Vendor deposits his e-coins to his bank account.

V: $\Pi(\ldots x' \ldots x \ldots x')$ B: Verifies: 1) if σ on Π is valid?

$, x_1, x_2, x_3, x_4, \dots, x_{50})$ $\longrightarrow$ $\mathcal{B}$: verifies: 1) ...

2) if the same string of $(y_1, y_1'; \dots; y_{50}, y_{50}')$ didn't deliver to him?

If it is **T**, the $\mathcal{B}$ deposits e-coin Π to the $\mathcal{V}$ account.

4. $\mathcal{I}o$ impersonates $\mathcal{A}$ and is double spending Π.

To protect $\mathcal{A}$ honour we assume that $\mathcal{I}o$ seized also $RIS = (x_1, x_1'; x_2, x_2'; \dots; x_{50}, x_{50}')$ together with Π

$\mathcal{I}o$: $\xrightarrow{\Pi}$ $\mathcal{V}$: generates a different RBS_2,

$RBS \neq RBS_2 = 1101, \dots, 0$

$\xleftarrow{RBS_2}$ $Pr(RBS = RBS_2) = 1/2^{50}$

$\mathcal{I}o$ knows the actual RIS, hence she reveals to $\mathcal{V}$ required values

$\xrightarrow{x_1,\ x_2,\ x_3',\ x_4, \dots, x_{50}'}$ $\mathcal{V}$: 1) Verifies signature σ on m

2) If m value is correct

3)

$$\left.\begin{array}{l} \text{if } H(x_1) = y_1 \\ \text{if } H(x_2) = y_2 \\ - - - - - - - \\ \text{if } H(x_{50}') = y_{50}' \end{array}\right\} \ \mathbf{T}$$

$\mathcal{I}o$ $\longleftarrow$ 

$\mathcal{V}$: $\xrightarrow{\Pi,\ (x_1,\ x_2,\ x_3',\ x_4, \dots, x_{50}')}$ $\mathcal{B}$: Verifies:

1) If σ on Π is valid? **T**

2) If the same coin Π with the same $(y_1, y_1', \dots, y_{50}, y_{50}')$ is already received previously: Yes

$\mathcal{B}$: discloses the identity of e-coin Π holder.

$$\oplus \begin{array}{l} x_1, x_2', x_3, x_4, \ldots, x_{50}' \\ x_1, x_2, x_3', x_4, \ldots, x_{50}' \\ \hline \vec{0}, A, A, \vec{0}, \ldots, \vec{0} \end{array}$$

$\mathcal{A}$ identity $A = 1010$

So $\mathcal{A}$ due to distraction has a problems with law enforcement.

Property: the only customer **Alice** can create and is responsible for Random Identification String - RIS during the Withdrawal protocol.

Questions:

1.Is it possible for **Alice** to modify e-coin $\prod$?

1.How vendor **Victor** can cheat against **Bank** and how it is prevented?

E-coin properties.

1.**Anonimity**.

2.**Untraceability**.

3.**Double-spending prevention**.

4.**Divisibility**.

International Association for Cryptographic Research - IACR Barcelona, 2008, announced results:

1.Divisible e-money can be trully anonymous.

2.Chaum: Divisible and trully anonymous e-money grow in size during their transfers.

Crypto Currences based on Blockchain.

1. Anonimity ??? Monero :	Transaction	Sender	Receiver
Anonimity	+	+	+
Bitcoin, Ethereum: Anonimity	−/+ ?	+/−	+/−

permissioned + permissionless

Homomorphic method → +

MIT Dan Boneh

Bitcoin addr. (Addr.)

Etherenm addr (Addr.)

BTC: $F(PuK) = Addr.$

Eth: — " —

$\underbrace{Tx1, Tx2, \ldots, TxN}_{Addr_i}$

$\mathcal{A}$: creates Random Identification String RIS for every m_j':
Then $\mathcal{A}$ encodes her name by some binary string $A = 1010$.

$x_{j1} \leftarrow randbin \rightarrow x_{j1} = 0110$

$\rightarrow x_{j1}' = A \oplus x_{j1} \rightarrow \oplus \begin{array}{c} A \\ x_{j1} \\ \hline x_{j1}' = \end{array} \rightarrow \oplus \begin{array}{r} 1010 \\ 0110 \\ \hline 1100 \end{array}$

2) Payment protocol

3) Deposit protocol

$\mathcal{A}$ computes:

x_{j1}, x_{j1}' ; x_{j2}, x_{j2}' ; ... ; $x_{j,50}, x_{j,50}'$.

If x_{jk} and x_{jk}' is revealed, then the identity of $\mathcal{A}$ will be revealed.

E.g. Let x_{j1} and x_{j1}' is known, then

$A = x_{j1} \oplus x_{j1}' \rightarrow \oplus \begin{array}{r} 0110 \\ 1100 \\ \hline 1010 \end{array} = A$

$y_{j1} = H(x_{j1})$, $y_{j1}' = H(x_{j1}')$.

$m_1' = m_1 \cdot r_1^e \bmod n, \ldots, m_{50}' = m_{50} \cdot r_{50}^e \bmod n$.

$\Pi_1' = (m_1'; y_{11}, y_{11}'; \ldots; m_{1,50}'; y_{1,50}, y_{1,50}')$

$\Pi_2' = \ldots$

$\ldots$

$\Pi_{50}' = \ldots$

$\xrightarrow{\Pi_1', \Pi_2', \ldots, \Pi_{50}'}$ $\mathcal{B}$: $\Pi_i' \leftarrow rand\{\Pi_1', \ldots, \Pi_{50}'\}$

$\xleftarrow{\Pi_1', \ldots, \Pi_{i-1}', \Pi_{i+1}', \ldots, \Pi_{50}'}$

$\xrightarrow{r_1, \ldots, r_{i-1}, r_{i+1}, \ldots, r_{50}}$

Verifies if:
1) all m_j have the same value
2) $\mathcal{A}$ accounts $> m_j$

$\mathcal{B}$ blindly signs e-coin Π_i'
$Sig(PrK = d, \Pi_i') = \sigma_i'$

$\xleftarrow{\quad \sigma_i' \quad}$

$\mathcal{A}$: unmasks σ_i' in the same way by computin σ_i on the sum m_i and hence $\mathcal{A}$ has e-coin Π_i consistin of the following:

$$\Pi_i = (m_i, \sigma_i, y_{i1}, y_{i1}'; \ldots; y_{i,50}, y_{i,50}')$$

not necessary to include since having signature σ_i the value m_i can be computed during the verification phase.

$\sigma_i = M^d \bmod n$; $M_i = \text{'} m_i; y_{i1}, y_{i1}'; \ldots; y_{i,50}, y_{i,50}' \text{'}$

$Ver(PuK=(n,e), \sigma_i, M_i) = T$

Instead of Π_i we will use the notation Π of e-coin.

$$\Pi = (m; \sigma; y_1, y_1'; \ldots; y_{50}, y_{50}')$$

2. Payment protocol.

$\mathcal{A}$: $\xrightarrow{\quad \Pi \quad}$ $\mathcal{V}$: Victor-vendor verifies

1) If signature on m is a valid $\mathcal{B}$ signature

$Ver(PuK=(n,e), \sigma, m) = T$

2) If m value is equal to the price of silver wath.

3) $\mathcal{V}$ generates random bit string-RBS consisting of 50 bits

E.g. $RBS = \text{'} \underset{b_1}{1}\ \underset{b_2}{0}\ \underset{b_3}{1}\ \underset{b_4}{1}, \ldots, \underset{b_{50}}{0} \text{'}$

$\mathcal{A}$: is taking RBS $\xleftarrow{\quad RBS \quad}$

and reveals either x_1 if $b_1 = 1$ or x_1' if $b_1 = 0$

x_2 if $b_2 = 1$ or x_2' if $b_2 = 0$

- - - - - -

x_{50} if $b_{50} = 1$ or x_{50}' if $b_{50} = 0$

$x_1, x_2', x_3, x_4, \ldots, x_{50}'$

$\xrightarrow{\qquad\qquad}$ $\mathcal{V}$: verifies

$\longrightarrow$ $\mathcal{V}$: verifies

$\mathcal{A}$: $\longleftarrow$

$$\left.\begin{array}{l} \text{if } H(x_1) = y_1 \\ \text{if } H(x_2') = y_2' \\ \text{- - - - - - -} \\ \text{if } H(x_{50}') = y_{50}' \end{array}\right\} \text{ If it is } \mathbf{T}$$

3. Deposit protocol. Vendor deposits his e-coins to his bank account.

$\mathcal{V}$: $\xrightarrow{\Pi, (x_1, x_2', x_3, x_4, \ldots, x_{50}')}$ $\mathcal{B}$: Verifies: 1) if σ on Π is valid?

2) if the same string of $(y_1, y_1'; \ldots; y_{50}, y_{50}')$ didn't deliver to him?

If it is **T**, the $\mathcal{B}$ deposits e-coin Π to the $\mathcal{V}$ account.

4. $\mathcal{I}o$ impersonates $\mathcal{A}$ and is double spending Π.

To protect $\mathcal{A}$ honour we assume that $\mathcal{I}o$ together with Π seized also $RIS = (x_1, x_1'; x_2, x_2'; \ldots; x_{50}, x_{50}')$

$\mathcal{I}o$: $\xrightarrow{\Pi}$ $\mathcal{V}$: generates a different RBS_2,

$RBS \neq RBS_2 = 1101, \ldots, 0$

$\xleftarrow{RBS_2}$ $Pr(RBS = RBS_2) = 1/2^{50}$

$\mathcal{I}o$ knows the actual RIS, hence she reveals to $\mathcal{V}$ required values

$\xrightarrow{x_1, x_2, x_3', x_4, \ldots, x_{50}'}$ $\mathcal{V}$: 1) Verifies signature σ on m

2) If m value is correct

3)

$\mathcal{I}o$ $\longleftarrow$

$$\left\{\begin{array}{l} \text{if } H(x_1) = y_1 \\ \text{if } H(x_2) = y_2 \\ \text{- - - - - - -} \\ \text{if } H(x_{50}') = y_{50}' \end{array}\right\} \mathbf{T}$$

$\mathcal{V}$: $\Pi, (x_1, x_2, x_3', x_4, \dots, x_{50}')$ $\xrightarrow{\qquad}$ $\mathcal{B}$: Verifies:

1) If σ on Π is valis? T

2) If the same coin Π with the same $(y_1, y_1', \dots, y_{50}, y_{50}')$ is already received previously: Yes

$\mathcal{B}$: discloses the identity of e-coin Π holder.

$$
\begin{array}{rl}
\oplus & x_1, x_2', x_3, x_4, \dots, x_{50}' \\
 & x_1, x_2, x_3', x_4, \dots, x_{50}' \\
\hline
 & \vec{0}, A, A, \vec{0}, \dots, \vec{0}
\end{array}
$$

$\mathcal{A}$ identity $A = 1010$

so $\mathcal{A}$ due to distraction has a problems with law enforcement.