E-voting modellek matematikája

Dr. Huszti Andrea

Tartalom

Szavazás folyamata

Szavazó hitelesítése

Szavazat leadása

Szavazatok összeszámlálása

Elektronikus szavazás

A szavazás adatait **elektronikusan**

- rögzítik,
- tárolják,
- feldolgozzák.

Formái:

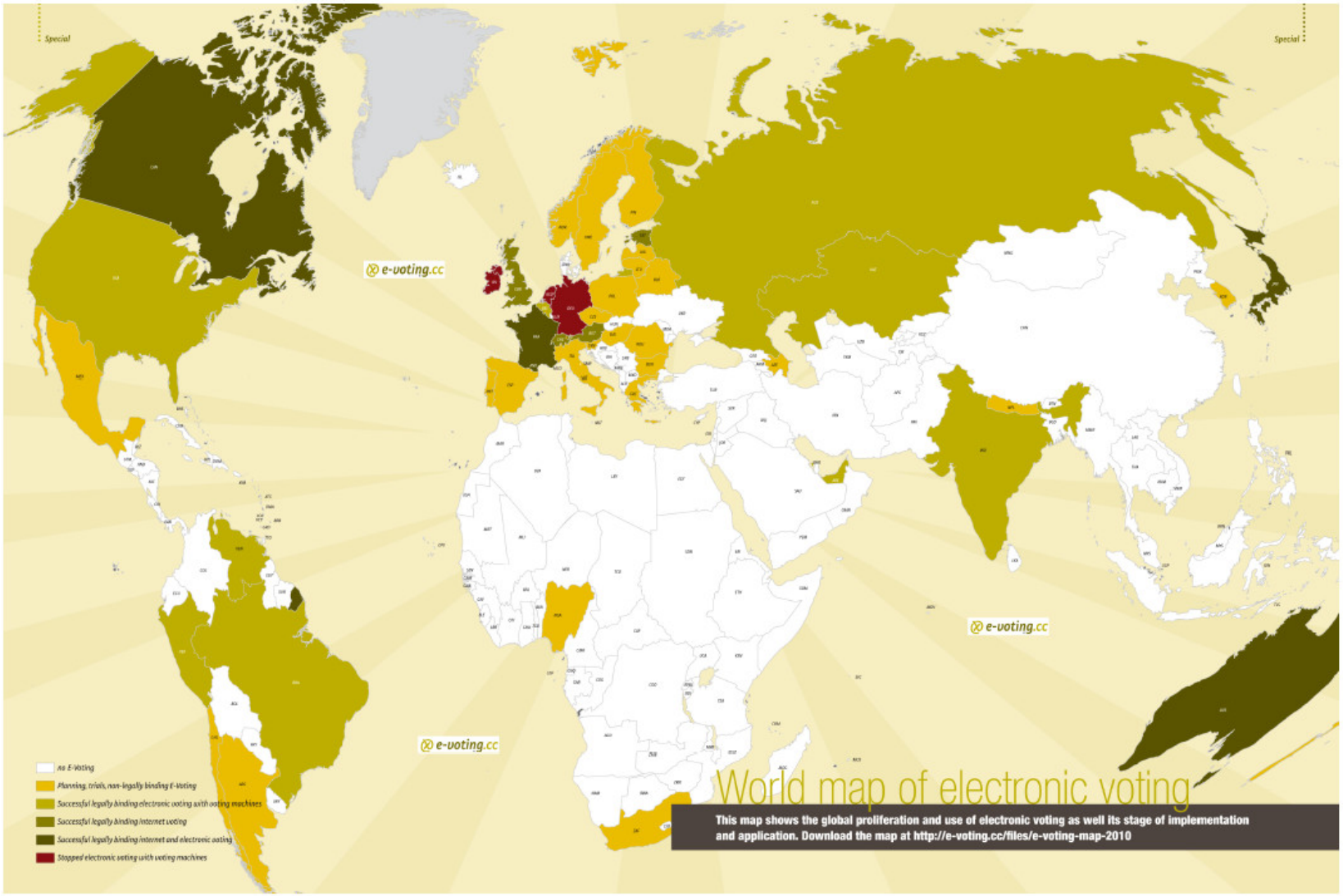
- *Internet szavazás* (I-szavazás): távoli elektronikus szavazás, nem kontrollált környezetben
- *Kiosk szavazás*: szavazógép segítségével, nem kontrollált környezetben (pl. áruházak), szavazó hitelesítését hivatalos személyzet végzi a helyszínen
- *Szavazógépek* (**D**irect-**R**ecording **E**lectronic machine): szavazóhelyiségeken, érintőképernyős/nyomógombos, sok esetben papír alapú igazolást ad
- *Scanner*: a szavazólapot elektronikusan rögzíti és összeszámlálja a szavazatokat, az eredeti szavazólap felhasználható újraszámlálásra

Elektronikus szavazás formái

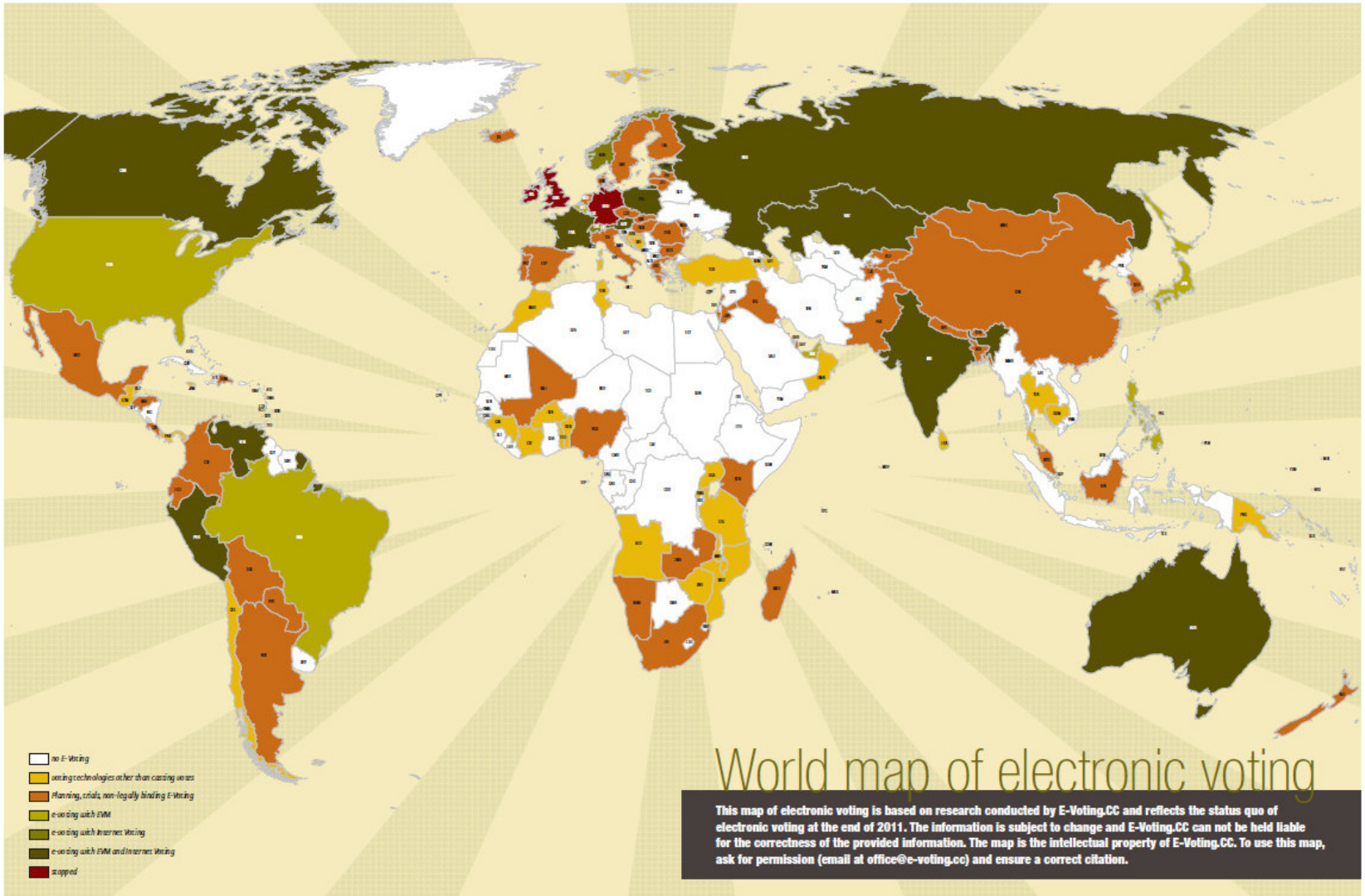
Scanner (dreamstime.com)

DRE (wikipedia)

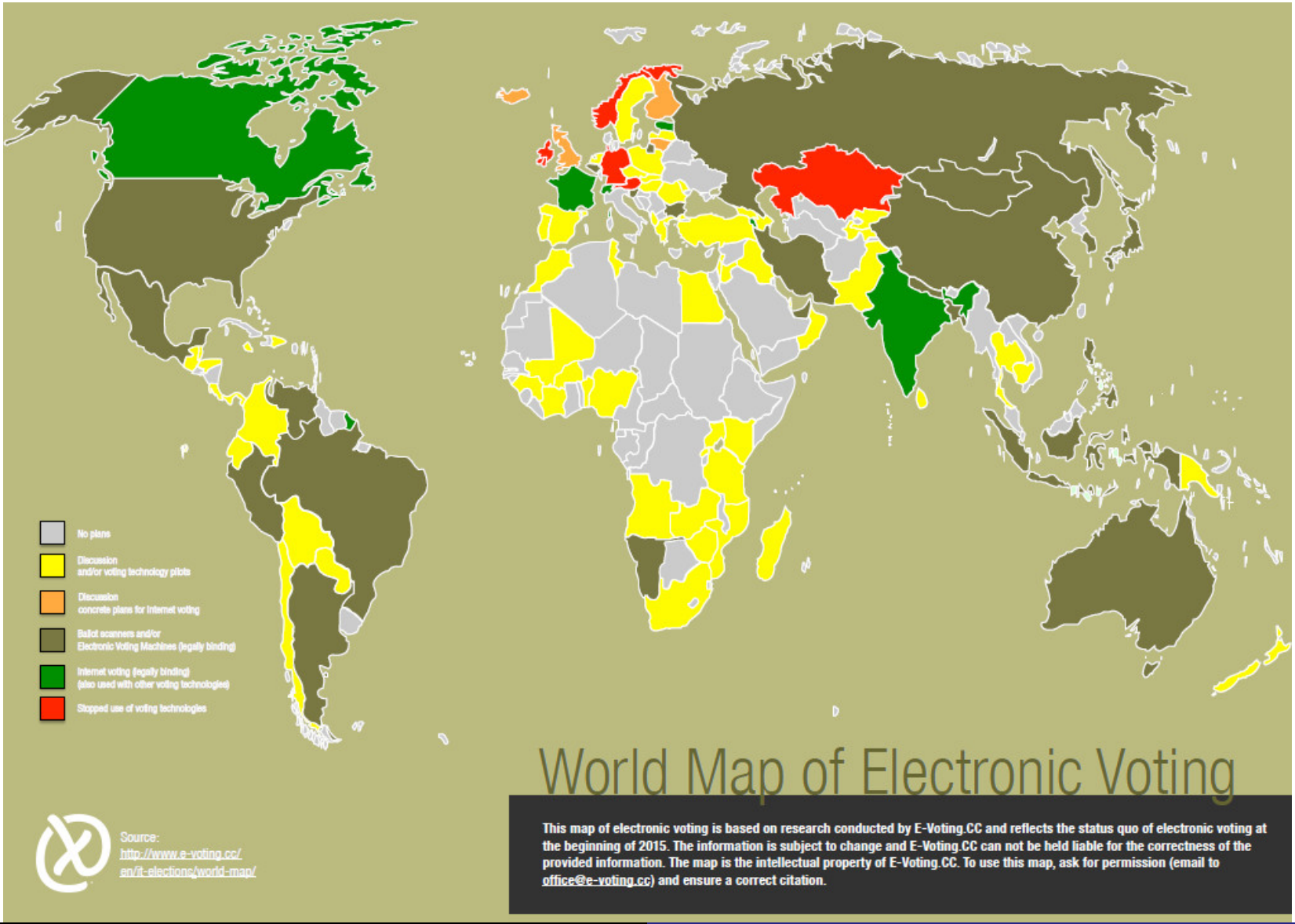
I-szavazás a világon 2009 (evoting.cc)



I-szavazás a világon 2011 (evoting.cc)



I-szavazás a világon 2015 (evoting.cc)



Biztonsági elvárások

- titkosság (privacy): titokban marad ki mire szavazott
- jogosultság (eligibility): csak az arra jogosult szavazhat
- egyszer-szavazhatóság (unreusability): mindenki csak legfeljebb egyszer szavazhat
- igazságosság (fairness): részeredmények nem befolyásolhatják a végleges eredményt
- személyes ellenőrizhetőség(individual verifiability): szavazó ellenőrizheti, hogy megfelelően számolták -e be a szavazatát
- univerzális ellenőrizhetőség(global verifiability): bárki, akár egy külső megfigyelő is ellenőrizheti, hogy a rendszer megfelelően működik

Biztonsági elvárások

- zsarolhatatlanság, megvesztegethetetlenség: nincs bizonyíték arról, hogy a szavazó hogy szavazott
  - igazolásmentes (receipt-freeness): a támadó megfigyelésből és az együttműködő szavazó titkaiból nyer információt
  - kényszeríthetetlen (uncoercibility): a támadó együttműködik a szavazóval a szavazó fázisban (megadhatja az üzeneteket)

Kategóriák

Vak aláíráson alapuló sémák

- regisztrációs fázis : rendszer-paraméterek generálása, token (azonosító, titkosított szavazat) hitelesítése
- szavazó fázis : szavazat és a hitelesített token elküldése anonim csatornán keresztül
- összeszámlálási fázis : hitelesített szavazatok visszafejtése, összeszámlálása

Homomorf titkosításon alapuló sémák

- regisztrációs fázis : azonosító generálása
- szavazó fázis: titkosított szavazat érvényességének vizsgálata és elküldése
- összeszámlálási fázis: az eredmény meghatározása

Kategóriák

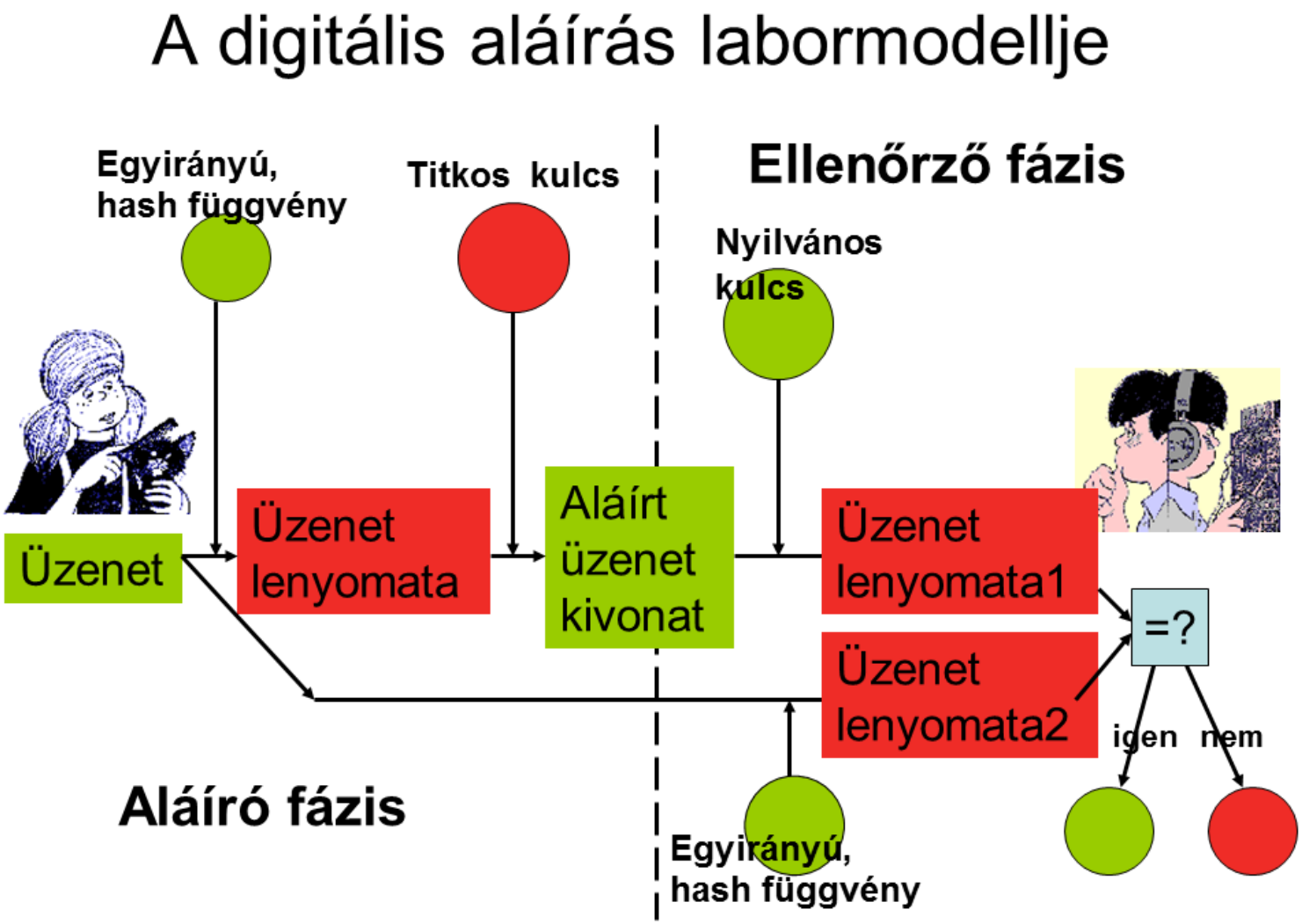
Mix-neten alapuló sémák

- minden szervezet megkapja a jelöltek listáját véletlenszerűen permutálja és titkosítja, majd az így kapott listát nyilvánosságra hozza a következő szervezet számára
- a permutációt elküldi titkos csatornán keresztül a szavazónak
- a szavazó az utolsó szervezet által készített listából kiválaszt egyet (az összes permutáció ismeretében)

FOO séma

- Atsushi Fujioka, Tatsuaki Okamoto, Kazuo Ohta (Nippon Telegraph and Telephone Corporation, Japan, 1992)
- Résztvevők: Szavazó, Adminisztrátor, Számláló
- Kommunikációs csatornák: anonim csatorna, nyilvános csatorna
- Kriptográfiai sémák: aláírási séma, vak aláírási, bit-commitment

Digitális aláírás



RSA-FDH aláírás

Aláírási séma: $\{\mathcal{K}, \mathcal{S}ign, \mathcal{V}er\}$
$\mathcal{P} = \mathcal{A} = \mathbb{Z}_n$, ahol n az RSA modulus, $H : \mathbb{Z}_n \mapsto \mathbb{Z}_n$ hash

$\mathcal{K}$:

1. p és q véletlen, nagy prímek választása
2. $n = p \cdot q$, $\phi(n) = (p-1)(q-1)$
3. $1 < e < \phi(n)$ választása, ahol $(e, \phi(n)) = 1$
4. $1 < d < \phi(n)$ kiszámítása $ed \equiv 1 \mod n$ alapján
5. $PK = (n, e)$
   $SK = d$, titkos paraméterek:$p, q, \phi(n)$

$$\mathcal{S}ign_{SK}(m) = s = [H(m)]^d \mod n$$

$$\mathcal{V}er_{PK}(m, s) = \begin{cases} 1, & s^e \equiv H(m) \mod n; \\ 0, & \text{egyébként.} \end{cases}$$

Vak aláírás

Vak aláírások

Alice

Hitelesítő Szervezet

- véglegesíti a dokumentumot
- belehelyezi egy átlátszatlan, indigós borítékba
- lezárja a borítékot és elküldi aláírásra

- aláírja a lezárt borítékot és visszaküldi a feladónak

- kiveszi a borítékból a dokumentumot
- az aláírás ellenőrizhető

Nem tudja mit írt alá!!

A Hitelesítő Szervezet hitelesen aláírja a dokumentumot anélkül, hogy ismerné annak tartalmát.

RSA-FDH vak aláírás

$\mathcal{P} = \mathcal{A} = \mathbb{Z}_n$, ahol n az RSA modulus, $H : \mathbb{Z}_n \mapsto \mathbb{Z}_n$ hash
$PK = (n, e)$, $SK = d$, titkos paraméterek: $p, q, \phi(n)$

Alice ($\mathcal{B}lind$):

- $m \in \mathcal{P}$ üzenet, $r \in \mathbb{Z}_n$ véletlen,
- $m' \equiv H(m) \cdot r^e \mod n$
- m' elküldése

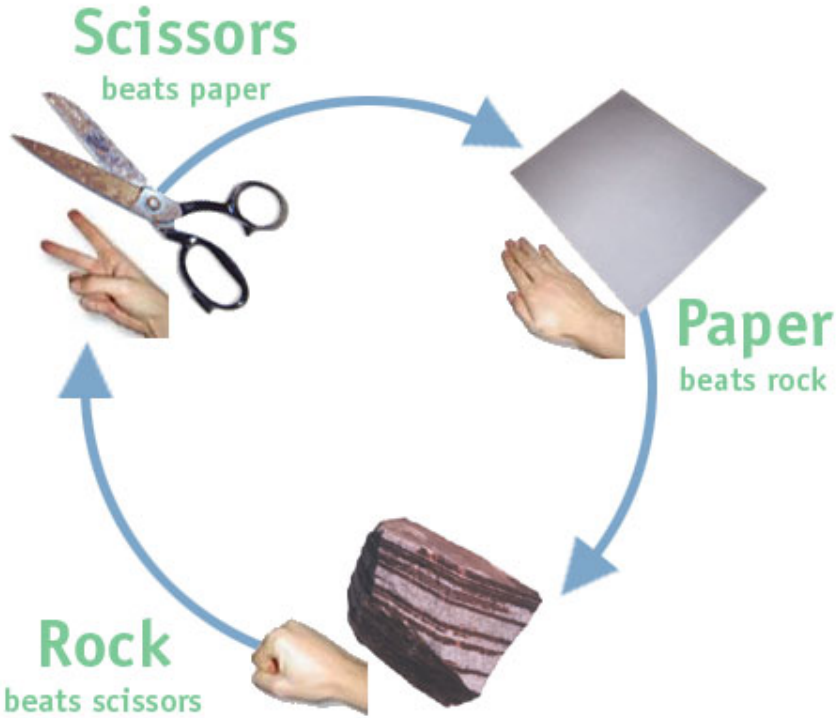
Bob (Aláírás):
$\mathcal{S}ign_{SK}(m') = s' = (m')^d \mod n$

Alice ($\mathcal{U}nblind$, ellenőrzés):
$s \equiv s' \cdot r^{-1} \mod n$, hiszen $H(m)^d \cdot r^{e \cdot d} \cdot r^{-1} \equiv [H(m)]^d \mod n$

$$\mathcal{V}er_{PK}(m, s) = \begin{cases} 1, & s^e \equiv H(m) \mod n; \\ 0, & \text{egyébként.} \end{cases}$$

Bit-commitment

Kő-papír-olló játék telefonon:



(wikipedia)

Nem tudjuk biztosan a másik nem gondolta -e meg magát.

Bit-commitment

Cél: "Elkötelezze" magát valami mellett úgy, hogy a másik ne tudja meg mi az.

Elkötelezettségi séma: $\{\mathcal{S}etup, \mathcal{C}ommit, \mathcal{O}pen\}$
$\mathcal{P}$: üzenetek halmaza

- $K = \mathcal{S}etup(1^k)$, k biztonsági paraméter,
- $(c, d) = \mathcal{C}ommit_K(m)$, ahol $m \in \mathcal{P}$,
  c: elkötelezettségi érték, d: nyitó érték,
- $m' = \mathcal{O}pen_K(c, d)$, ahol $m' \in \mathcal{P} \bigcup \{\perp\}$
  $\perp$: c nem kötelezettségi értéke egy lehetséges üzenetnek sem

Biztonsági elvárások:

-kötés (binding): nehéz találni olyan d' nyitó értéket, melyre
$(c, d) = \mathcal{C}ommit_K(m)$ és $(c, \hat{d}) = \mathcal{C}ommit_K(\hat{m})$

-elrejtés (hiding): (c, d) nem árul el információt az m üzenetről

Bit commitment

Kő-papír-olló játék telefonon:

- A: $(c, d) = \mathcal{C}ommit_K(\text{papír})$
- $A \to B$: c
- $B \to A$: olló
- $A \to B$: d, papír
- B: $\mathcal{O}pen_K(c, d) =$ papír ellenőrzése

Megjegyzés: Ha legfeljebb egy nyílt üzenete lehet egy adott titkosított üzenetnek, akkor az aszimmetrikus titkosítási séma *elkötelezettségi*. Ha CPA biztonságos, akkor használható elkötelezettségi sémaként is. A nyitó fázisban is titkosítunk, tehát nincs szükség titkos kulcsra. Egyszerűbb megoldások is vannak.

Pedersen egy-bit séma

$\mathcal{P} = \{0, 1\}$

- $\mathcal{S}etup(1^k)$:
  1. p prím
  2. $y \in \mathbb{Z}_p^*$ véletlen
  3. g generátor eleme $\mathbb{Z}_p^*$-nak
  4. $K = (p, g, y)$
- $\mathcal{C}ommit_K(b)$:
  1. $r \in \mathbb{Z}_p^*$ véletlen
  2. $c = g^r y^b \mod p$
  3. $(c, (r, b))$
- $\mathcal{O}pen_K(c, (r, b))$:
  1. IF $c = g^r y^b \mod p$
     THEN $m' = b$
     ELSE $m' = \perp$.

FOO séma

Résztvevők: Szavazó (V), Adminisztrátor (A), Számláló (C)

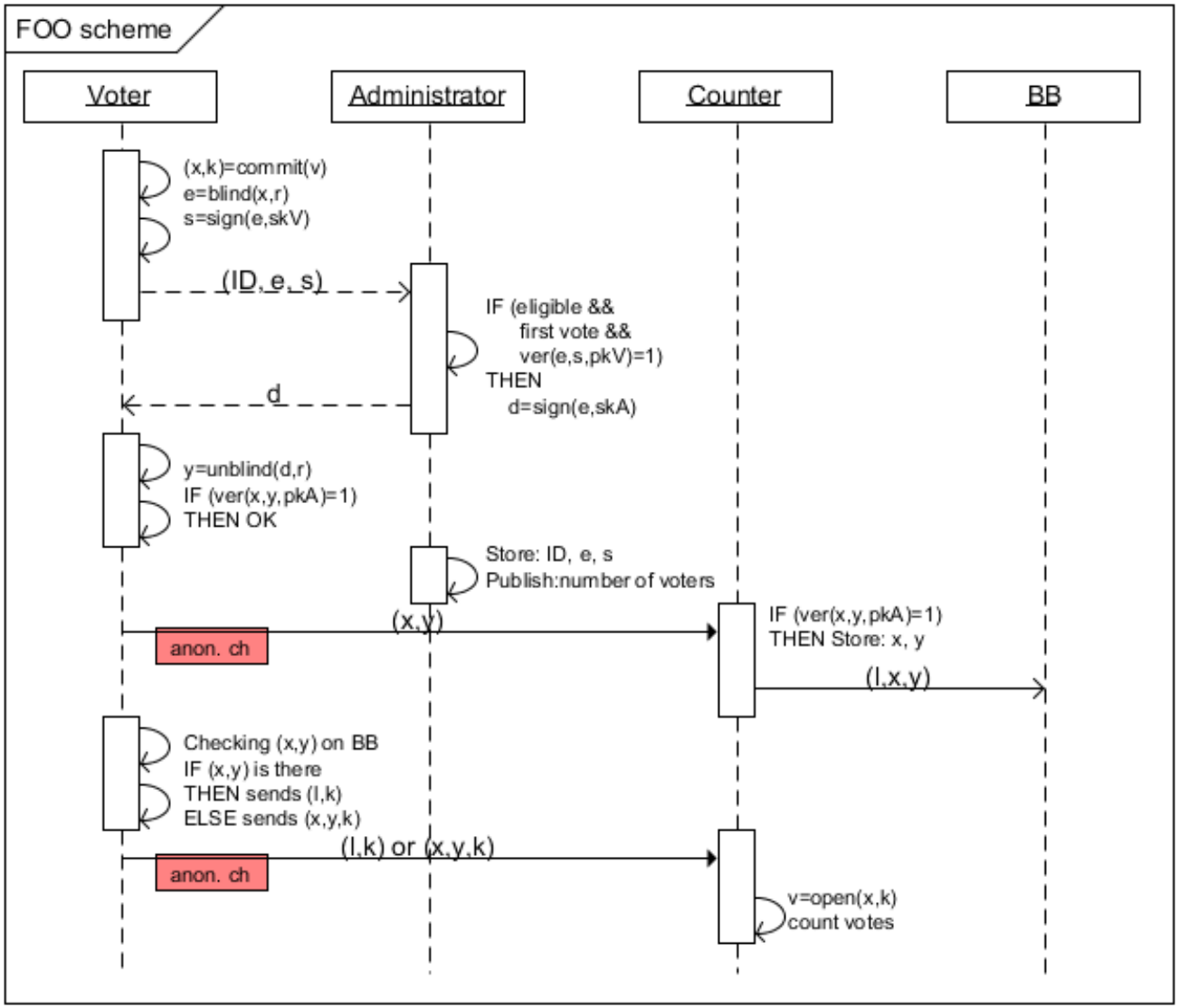
Fázisok:

- Regisztráció:
  1. Szavazó elkészíti *e-szavazatát*, melyben a tényleges szavazata rejtett:$(x, k) = \mathcal{C}ommit_K(v)$, $e = \mathcal{B}lind(x, r)$,
  2. Szavazó digitálisan aláírja: $\mathcal{S}ign_{SK_V}(e)$,
  3. Szavazó elküldi az aláírt e-szavazatot az Adminisztrátornak,
  4. Adminisztrátor vakon aláírja, ha a Szavazó jogosult szavazni, még nem hitelesítette korábban és a Szavazó aláírása érvényes: $d = \mathcal{S}ign_{SK_A}(e)$,
  5. Adminisztrátor nyilvánossá teszi a szavazók számát és a (ID, e, s) listát.
- Szavazó:
  1. Szavazó az aláírt e-szavazatát elküldi a Számlálónak anonim csatornán keresztül:(x, y),
  2. Számláló ellenőrzi az aláírás érvényességét,
  3. Határidő után az érvényes aláírt e-szavazatokat a hirdetőtáblán nyilvánosságra hozza :(l, x, y).

FOO séma

- Összeszámláló:
  1. Szavazó ellenőrzi, hogy a szavazók és szavazatok száma megegyezik -e,
  2. Szavazó ellenőrzi, hogy szavazata szerepel -e BB-n, ha nem elküldi: (x, y),
  3. Szavazó elküldi anonim csatornán keresztül: (l, k),
  4. Számláló kinyitja az e-szavazatokat: $\mathcal{O}pen_K(x, k)$,
  5. Számláló összeadja az érvényes szavazatokat.

FOO séma


FOO scheme
Voter
Administrator
Counter
BB
(x,k)=commit(v)
e=blind(x,r)
s=sign(e,skV)
(ID, e, s)
IF (eligible &&
first vote &&
ver(e,s,pkV)=1)
THEN
d=sign(e,skA)
d
y=unblind(d,r)
IF (ver(x,y,pkA)=1)
THEN OK
Store: ID, e, s
Publish:number of voters
(x,y)
anon. ch
IF (ver(x,y,pkA)=1)
THEN Store: x, y
(l,x,y)
Checking (x,y) on BB
IF (x,y) is there
THEN sends (l,k)
ELSE sends (x,y,k)
(l,k) or (x,y,k)
anon. ch
v=open(x,k)
count votes

FOO séma - Jellemzők

- titkosság (privacy): anonim csatorna, A és C összefogása mellett is
- jogosultság (eligibility): digitális aláírás + vak aláírás
- egyszer-szavazhatóság (unreusability): vak aláírás
- igazságosság (fairness): határidő után számolják a szavazatokat
- személyes ellenőrizhetőség(individual verifiability): szavazó ellenőrizheti BB-n a szavazatát
- univerzális ellenőrizhetőség(global verifiability): bárki, akár egy külső megfigyelő is ellenőrizheti a szavazók számát és a szavazatokat, feltéve, hogy minden szavazó szavaz, ha regisztrált (C feltehet szavazatot)
- megvesztegethetetlenség, zsarolhatatlanság (receipt-freeness, uncoercibility): nem teljesül (támadó ismeri e, x értékeket)

Észt szavazó séma

- észt személyi igazolvány képes digitális aláírásra és autentikációra (2 tanúsítvány)
- kb. 1.3 millió lakos
- 2005: 765 000 db személyi igazolvány
- 2010: 1.1 millió db személyi igazolvány
- szavazás napja előtt 4-10 nappal lehet e-szavazni
- a szavazó megváltoztathatja e-szavazatát: újra elküldi a szavazás napja előtt 4-10 nappal elektronikusan vagy papíron
- az utolsó szavazatot veszik figyelembe
- Résztvevők: szavazók(PC), Nemzeti Választási Bizottság(szerverek)
- szavazó PC-je a leggyengébb pont, a szerverek felügyelet alatt állnak (felkészültség biztosítható)

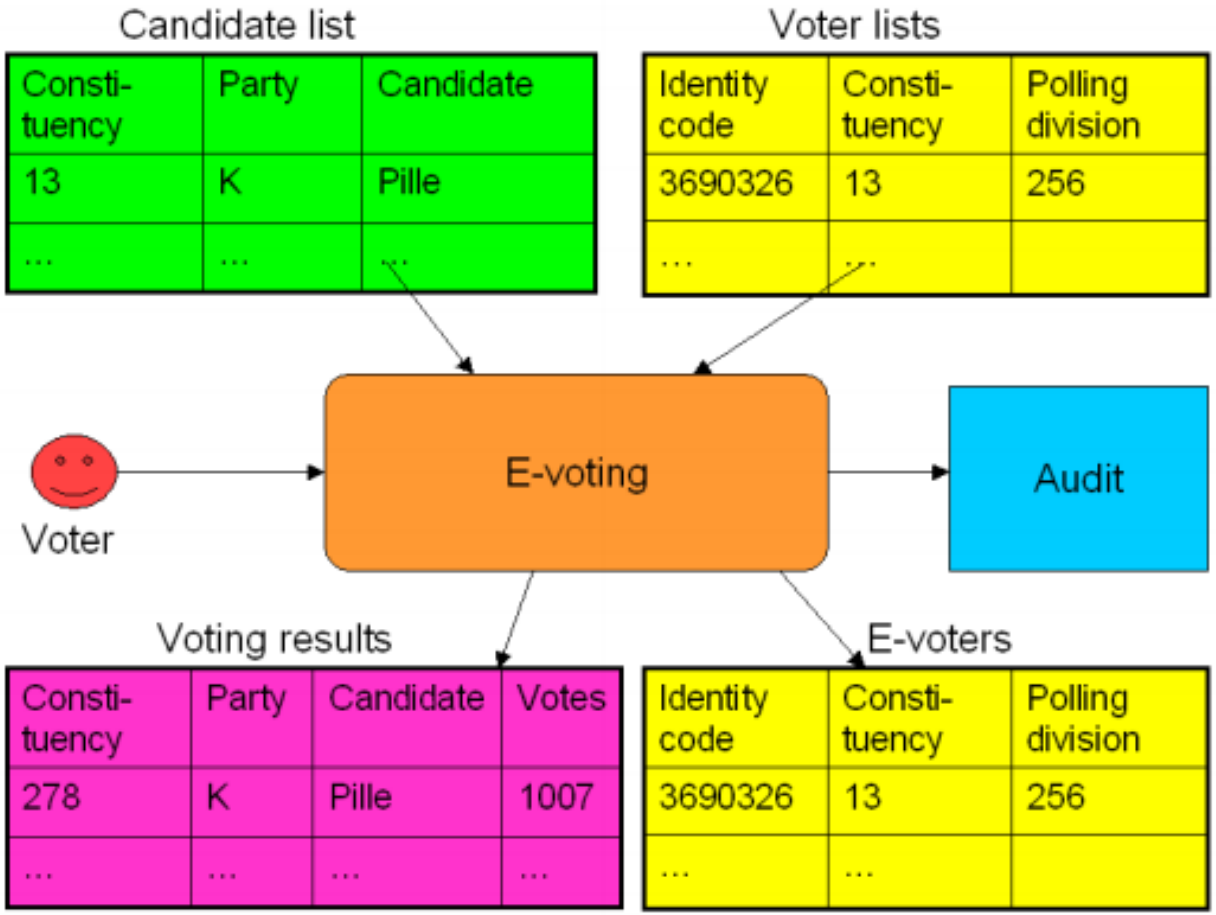


Fig. 1 The scope of e-voting: input and output

Estonian National Electoral Committee

A protokoll váza

- minél egyszerűbb és érthetőbb legyen
- legalább olyan biztonságos legyen, mint a hagyományos
- alapötlet: mozgó szavazóurna modellje
- Működés:
  1. Nemzeti Választási Bizottság honlapján a szavazónak magának kell szavaznia
  2. szavazó hitelesíti magát személyi igazolványa segítségével
  3. megfelelő jelöltek listája megjelenik
  4. szavazó kiválasztja a jelöltet és aláírásával hietlesíti
  5. honlap megjeleníti a kiválasztott jelöltet a szavazónak

Mozgó szavazóurna modell

- szavazó hitelesíti magát a szavazó bizottságnak
- berakja a kitöltött szavazólapját egy jelöletlen borítékba
- a boríték belekerül egy másik borítékba, melyre rákerül a szavazó adata
- a borítékot elviszik a választó helyiségbe
- ellenőrzik a szavazó jogosultságát a borítékon levő adatok alapján
- ha jogosult a belső boríték az urnába kerül
- külső boríték: digitális aláírás
- belső boríték: titkosítás (jelölt+véletlen szám)

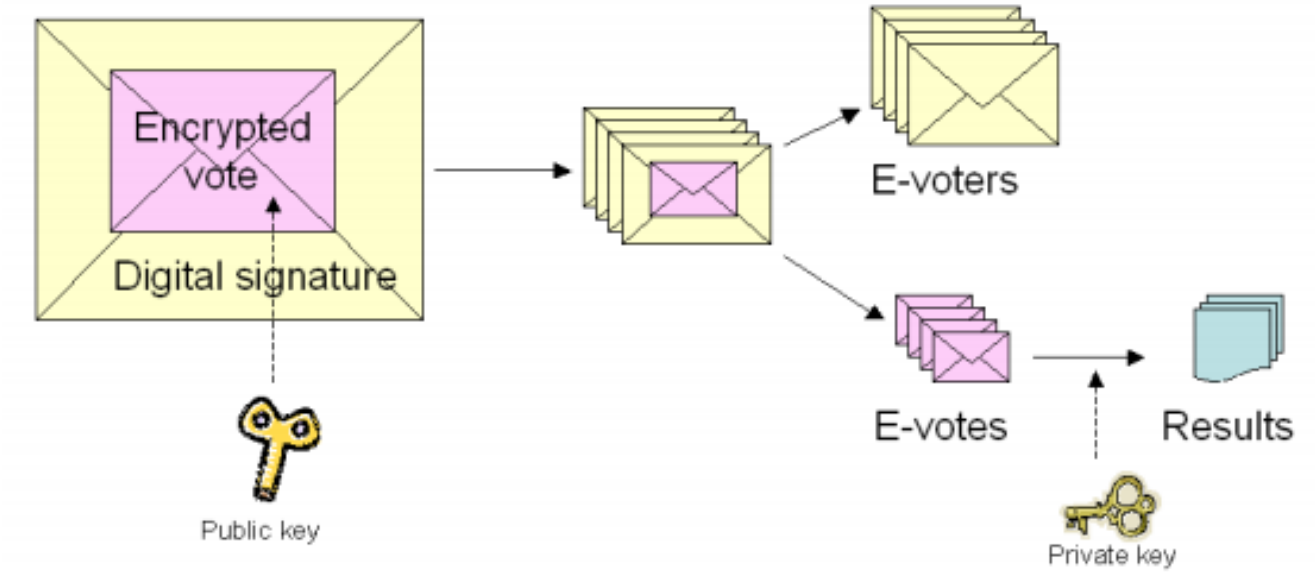


Fig. 2. The envelope method

Estonian National Electoral Committee

Feltételezzük: egy résztvevő sem rendelkezhet az aláírt szavazattal és a titkos visszafejtő kulccsal egyszerre

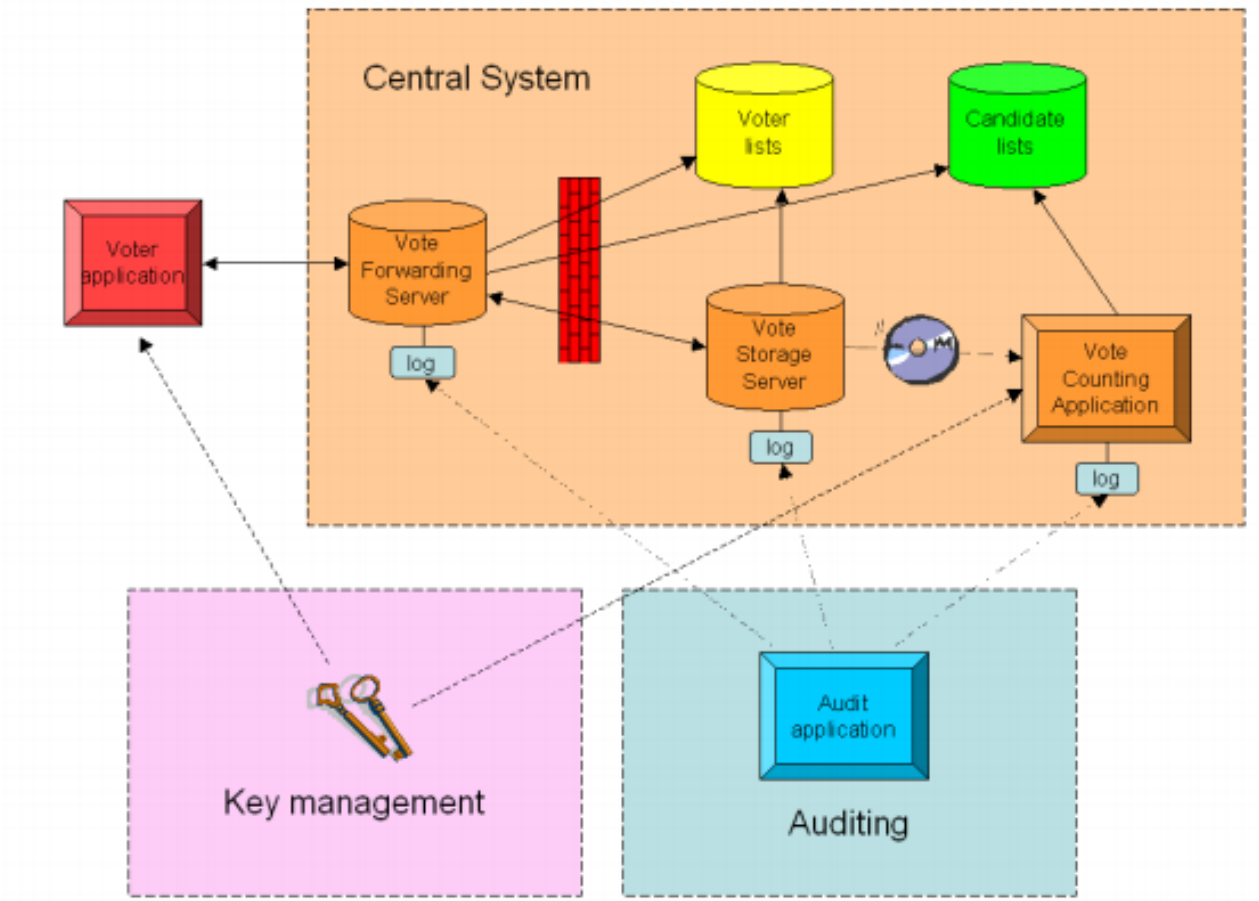


Fig. 3. Election System's general architecture

VFS: szavazó hitelesítése
VSS:jogosulatlan és dupla szavazatok törlése
VCA: visszafejti a titkosított szavazatokat

Észt séma - Jellemzők

- titkosság (privacy): egy résztvevő sem rendelkezhet az aláírt szavazattal és a titkos visszafejtő kulccsal egyszerre
- jogosultság (eligibility): digitális aláírás
- egyszer-szavazhatóság (unreusability): digitális aláírás
- igazságosság (fairness): határidő után számolják a szavazatokat, addig titkosított
- személyes és univerzális ellenőrizhetőség: LOG állományok tartalmazza a szavazat és egy véletlen titkosításának hash értékét (szavazó és bárki ellenőrizhet)
- megvesztegethetetlenség, zsarolhatatlanság (receipt-freeness, uncoercibility): szavazó újra elküldheti szavazatát (akár papíron is)

Homomorf titkosítás

- $\mathcal{E}nc_{PK}(m_1, k_1) \cdot \mathcal{E}nc_{PK}(m_2, k_2) = \mathcal{E}nc_{PK}(m_1 \cdot m_2, k_1 + k_2)$
- ElGamal titkosítás: $\mathcal{E}nc_{PK}(m) = (g^k, m \cdot h^k)$, ahol $PK = (g, p, h = g^a)$
- $\mathcal{E}nc_{PK}(m_1) \cdot \mathcal{E}nc_{PK}(m_2) = (g^{k_1+k_2}, m_1 m_2 \cdot h^{k_1+k_2})$
- Alapötlet:
  1. $SK = a$ megosztva több szervezet között
  2. igen/nem szavazat: $(m_0, m_1) = (g, g^{-1})$
  3. $\mathcal{E}nc_{PK}(m_b) = (x, y) = (g^k, m_b \cdot h^k)$, $b \in \{0, 1\}$ titkosított szavazat elküldése
  4. kapott titkosított szavazatok összeszorzása: $\prod(g^{k_i}, g^{t_i} \cdot h^{k_i}) = (g^{\sum k_i}, g^{\sum t_i} \cdot h^{\sum k_i})$, ahol $t_i \in \{1, -1\}$
  5. A szervezetek közösen fejtik vissza az eredményt (g^T, amiből T kiszámítható).
  6. Nulla-ismeretű protokoll szükséges, mely bizonyítja a beküldött titkosított szavazat helyességét: $dlog_g x = dlog_h y g^{-1}$ vagy $dlog_g x = dlog_h y g$
- Globálisan egyszerűen ellenőrizhető

Nulla-ismeretű protokoll

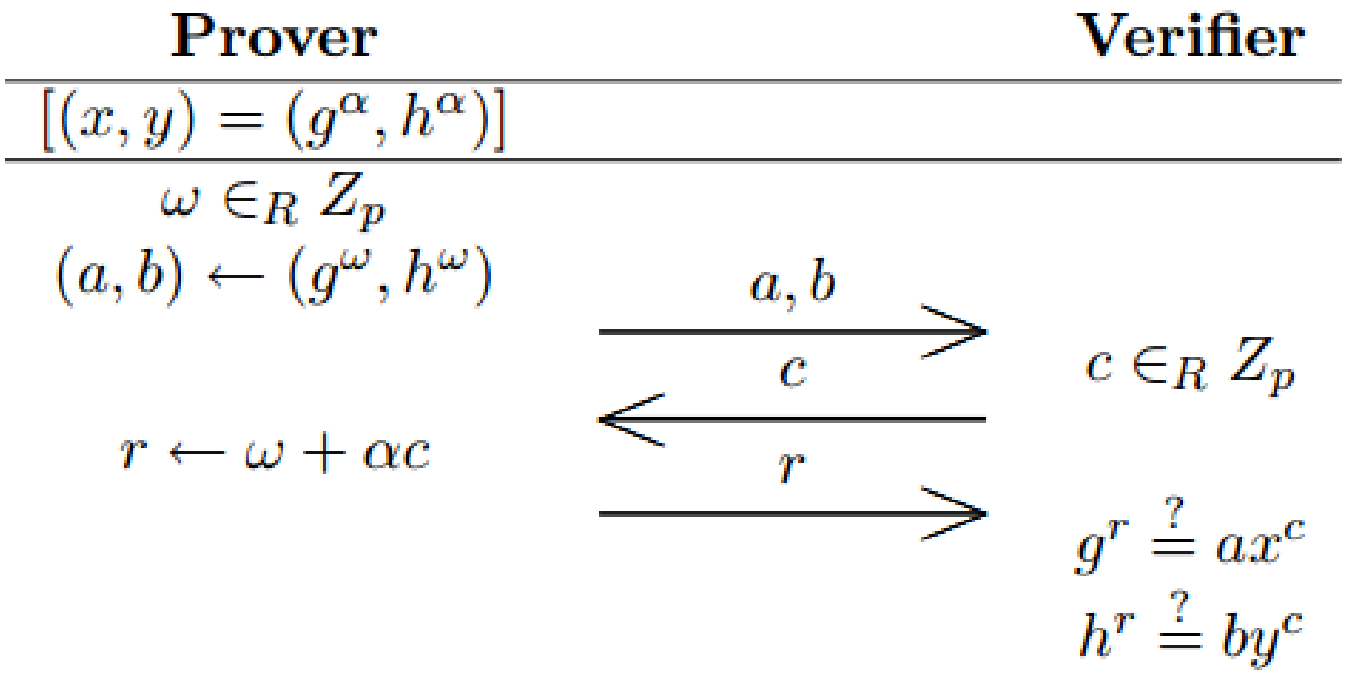


Figure 2: Proof of knowledge for $\log_g x = \log_h y$

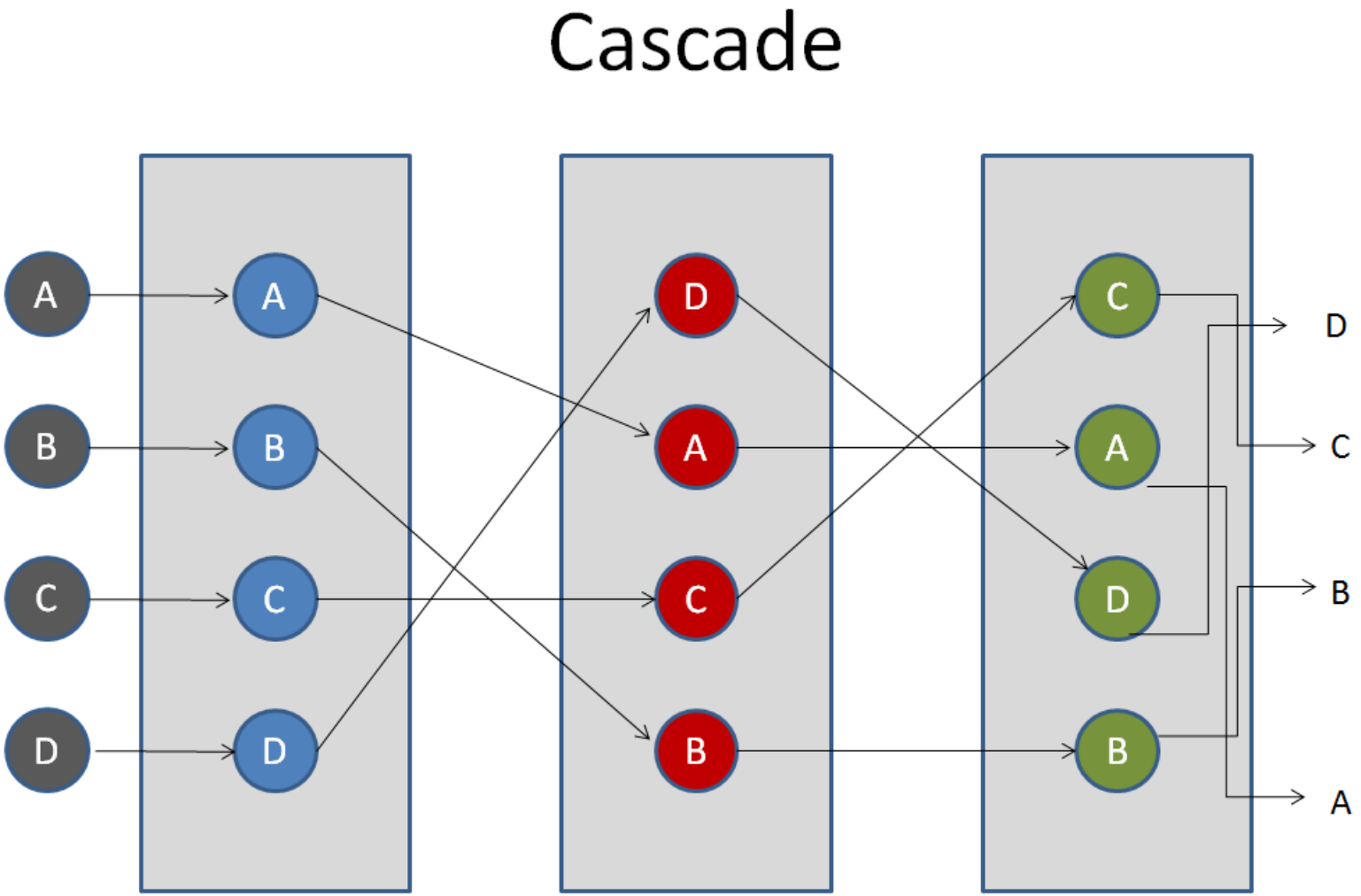
Mix-net

- Mix szerverek láncolata
- cél: anonim kommunikáció biztosítása
- Mix műveletei:
  1. összegyűjti a bejövő üzeneteket
  2. kriptográfiai primitív + permutáció
  3. az üzeneteket vagy a következő mix-nek vagy a címzettnek küldi

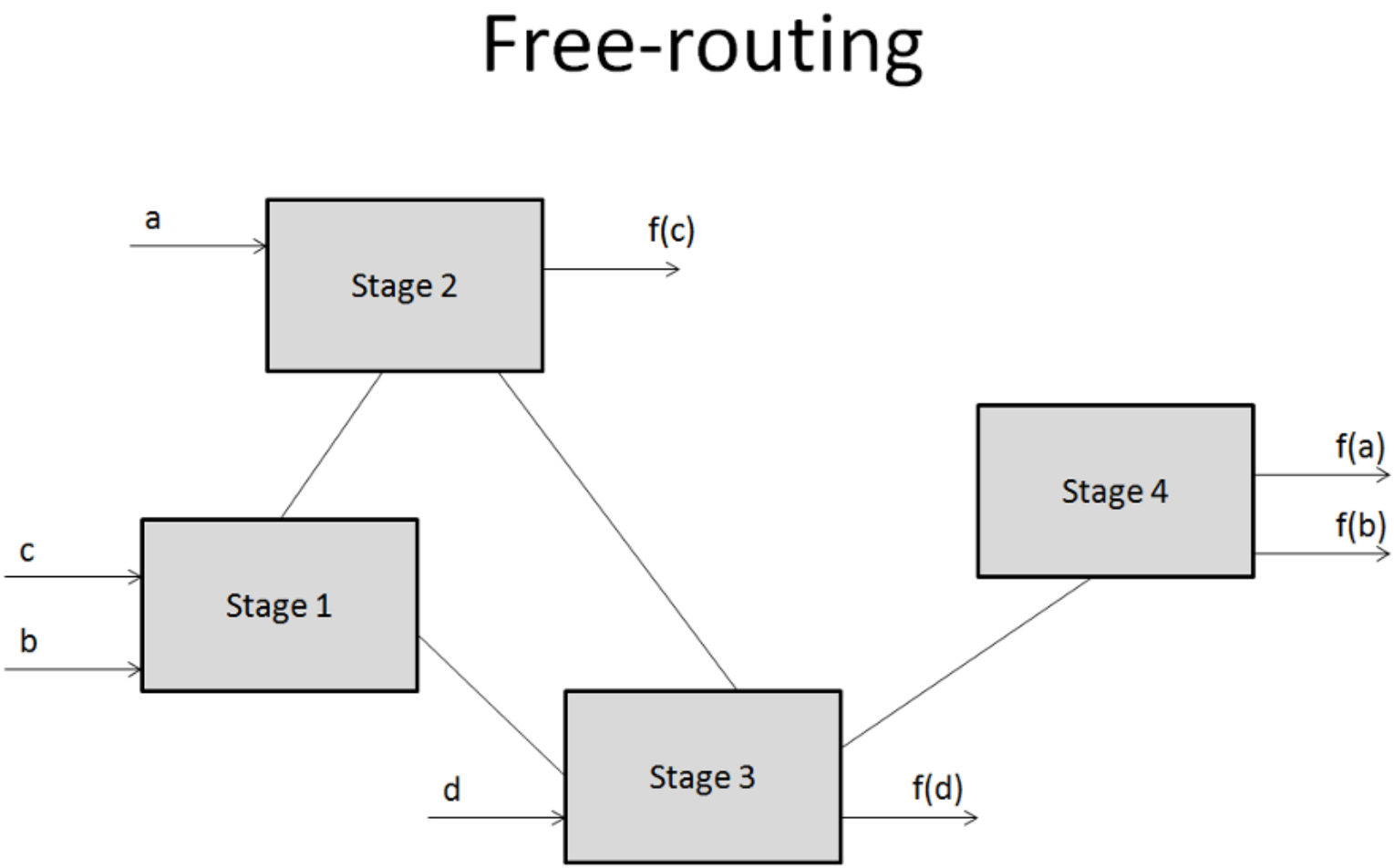
Szabad útválasztásos mix-net: a szerverek sorrendje tetszőleges
Cascade mix-net:

- Szerverek sorrendje kötött
- Visszafejtő mix-net
- (Újra)titkosító mix-net
- Hybrid mix-net

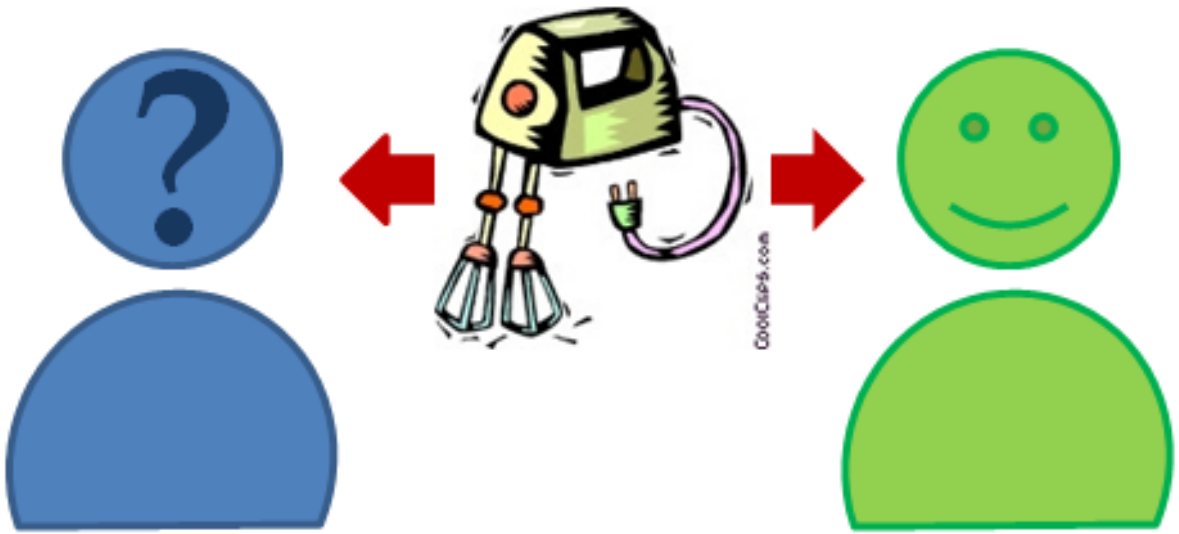
Cascade


Cascade
A
B
C
D
A
B
C
D
D
A
C
B
C
A
D
B
D
C
B
A
Color change: cryptographic operation

Szabad útválasztásos



Egyirányú mix-net



Hybrid: tetszőleges hosszú üzenetek
Jogosultság
Anonim válasz
Anonimitás visszavonása

Definition

Let G_1 and G_2 be two groups of order q for some large prime q. A map $e : G_1 \times G_1 \to G_2$ is an **admissible bilinear map** if satisfies the following properties:

1. **Bilinear**: We say that a map $e : G_1 \times G_1 \to G_2$ is bilinear if $e(aP, bQ) = e(P, Q)^{ab}$ for all $P, Q \in G_1$ and all $a, b \in Z_q^*$.
2. **Non-degenerate**: The map does not send all pairs in $G_1 \times G_1$ to the identity in G_2. Since G_1, G_2 are groups of prime order, if P is a generator of G_1 then $e(P, P)$ is a generator of G_2.
3. **Computable**: There is an efficient algorithm to compute $e(P, Q)$ for any $P, Q \in G_1$.

The Weil and Tate pairings prove the existence of such constructions. Typically, G_1 is an elliptic-curve group and G_2 is a finite field.

The following properties of bilinear pairings can be easily verified. Property (5) is another way of defining non-degeneracy. For all $S, T \in G_1$:

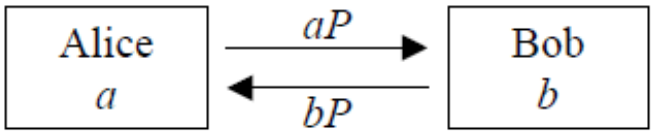
1. $e(S, \infty) = 1$ and $e(\infty, S) = 1$.
2. $e(S, -T) = e(-T, S) = e(S, T)^{-1}$
3. $e(aS, bT) = e(S, T)^{ab}$ for all $a, b \in Z$.
4. $e(S, T) = e(T, S)$.
5. If $e(S, R) = 1$ for all $R \in G_1$, then $S = \infty$.

Definition

Discrete Logarithm Problem (DLP) in an additively-written group $G =< P >$ of order q is the problem, given P and Q, of finding the integer $x \in [0, q-1]$ such that $Q = xP$.

Definition

Computational Diffie-Hellman problem (CDHP) is the problem, given P, aP and bP, of computing abP.



Definition

Let e be a bilinear pairing on (G_1, G_2). The **bilinear Diffie-Hellman problem** (BDHP) is the following: Given P, aP, bP, cP, compute $e(P, P)^{abc}$.

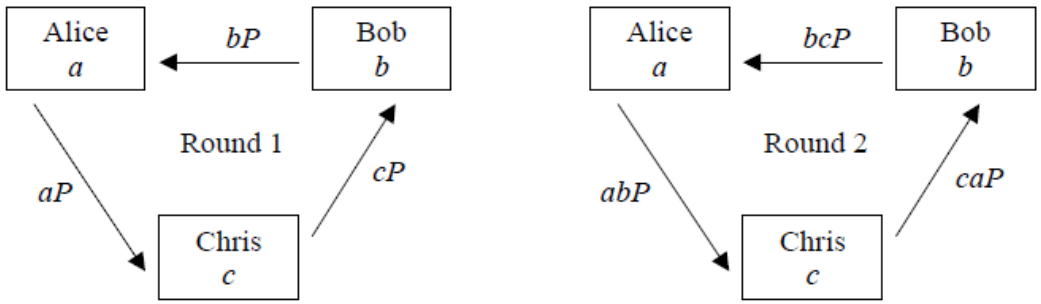


FIGURE 2. Three-party two-round key agreement protocol.

Ehelyett: $K = e(bP, cP)^a = e(aP, cP)^b = e(aP, bP)^c$

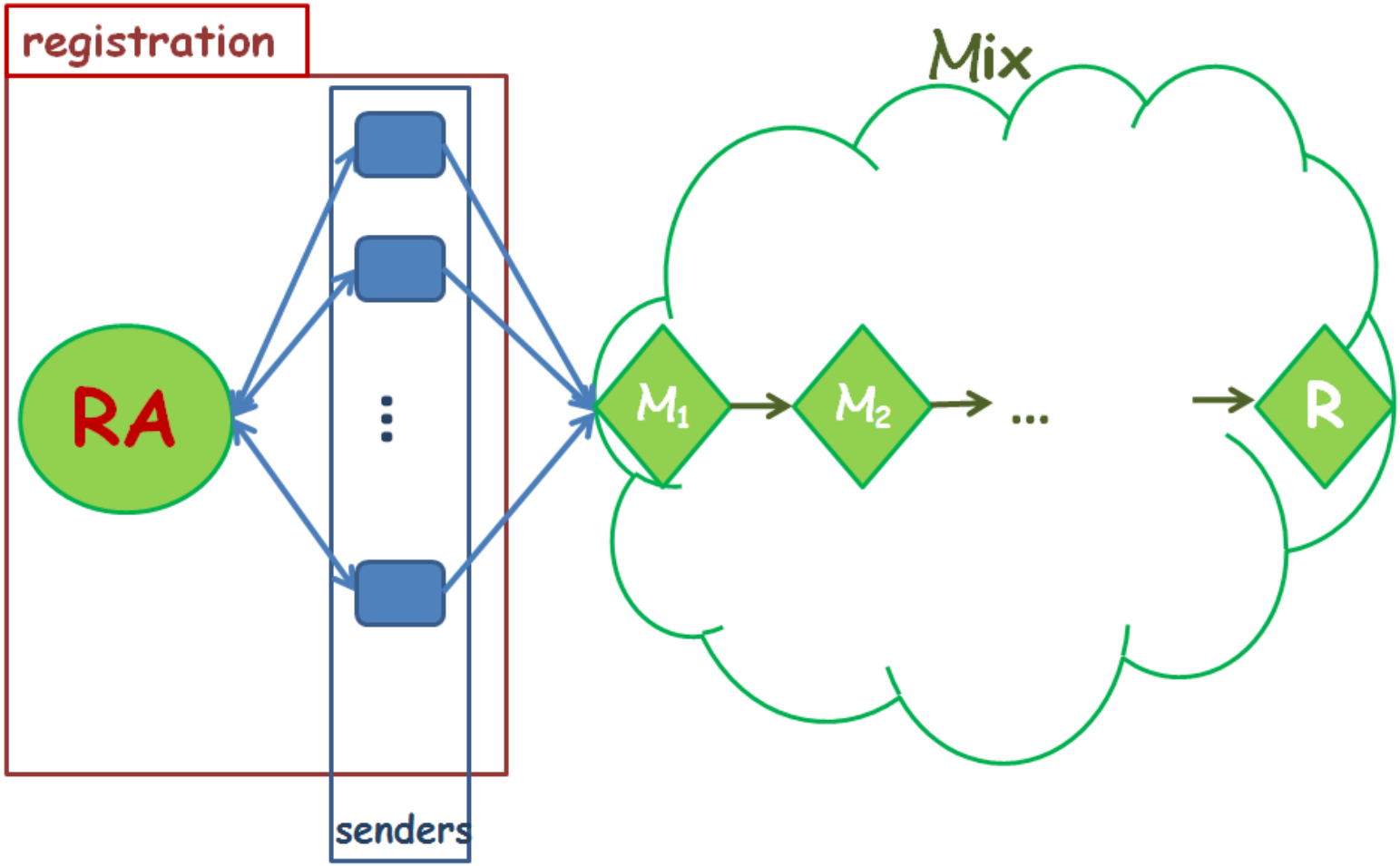
Hardness of the BDHP implies the hardness of the CDHP in both G_1 and G_2.

Definition

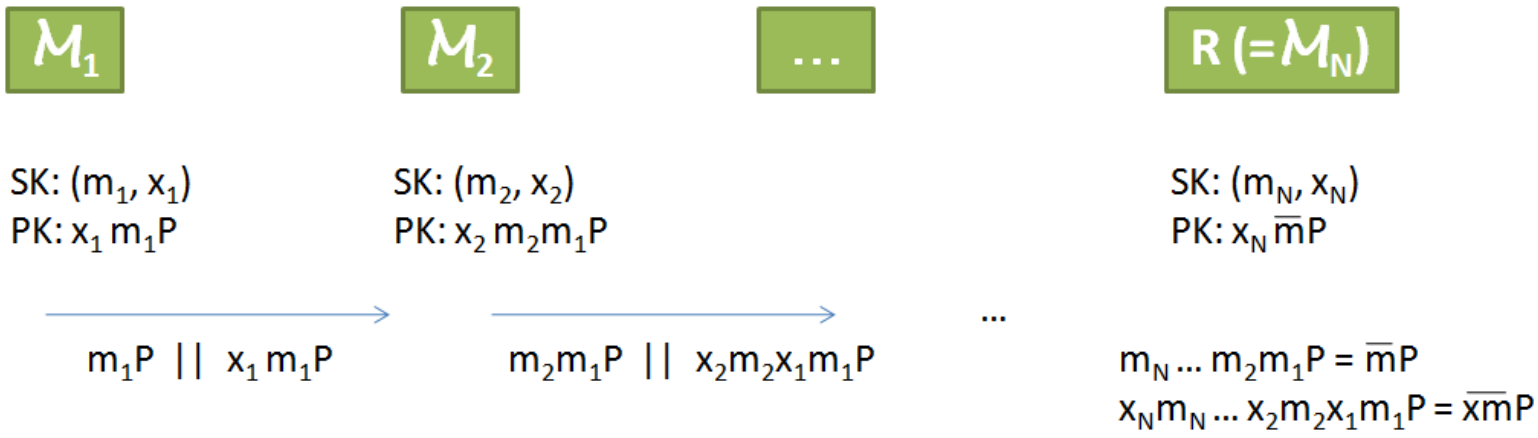
Decisional Diffie-Hellman problem (DDHP) is the problem, given P, aP, bP and cP, of deciding whether $cP = abP$.

In G_1 it is easy.
Calculating: $e(P, cP) = e(P, P)^c$ and $e(aP, bP) = e(P, P)^{ab}$

Protokoll

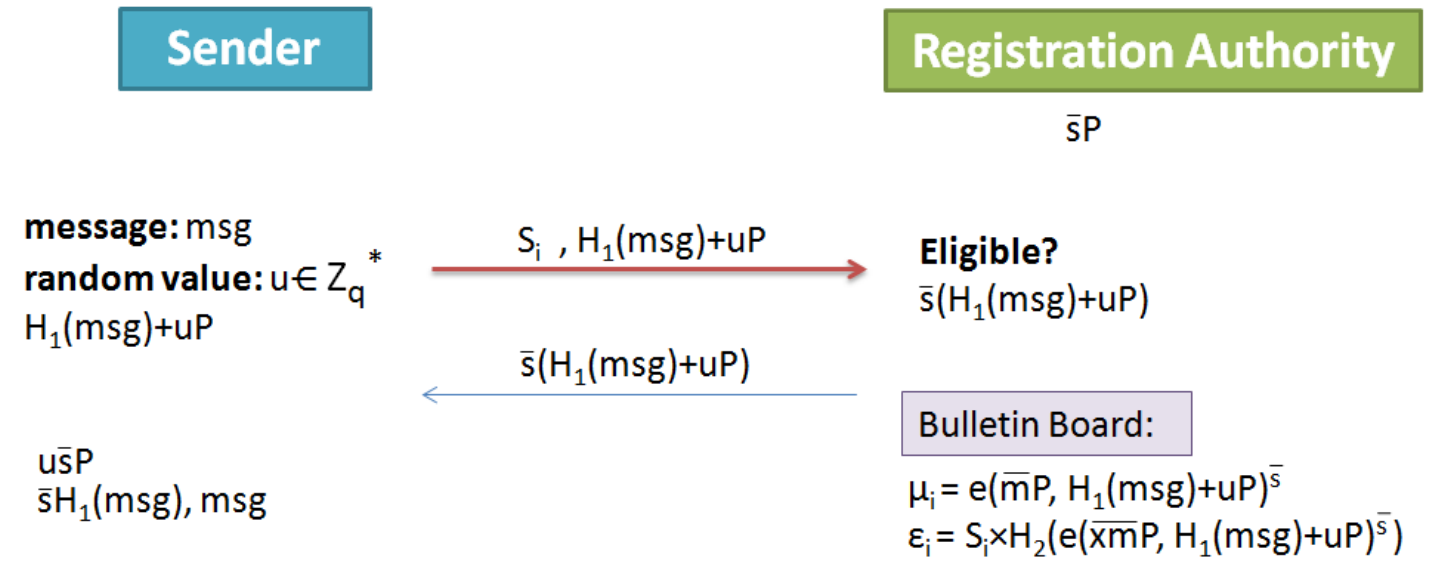


Kulcsgenerálás



Regisztráció

Registration



Verification: $e(\bar{s}H_1(msg),P)=e(\bar{s}P,H_1(msg))$

RA does not have information about *msg*.
μ_i is a commitment value for *u*
ε_i is the encrypted identity
$\bar{s}\,H_1(msg)$ ->eligibility

Üzenet elküldése

S_i **message:** msg **secret random value:** $a_{s_i} \in Z_q^*$

$$\mathbf{p} = \text{msg} \,||\, \bar{s}H_1(\text{msg}) \,||\, a_{s_i} P$$

symmetric encryption keys:

$K_1^{(i)} = H_2(e(PK_{\mathcal{M}1}, \bar{s}P)^{u^{(i)}})$
$K_2^{(i)} = H_2(e(PK_{\mathcal{M}2}, \bar{s}P)^{u^{(i)}})$
...
$K_{N-1}^{(i)} = H_2(e(PK_{\mathcal{M}N-1}, \bar{s}P)^{u^{(i)}})$
$K_R^{(i)} = H_2(e(PK_R, \bar{s}P)^{u^{(i)}})$

encryption:

$$\mathbf{M_1^{(i)}} = Enc_{K1}^{(i)}(Enc_{K2}^{(i)}(...Enc_{KR}^{(i)}(p)))$$

secret random values: $u_1^{(i)}, u_2^{(i)} \in Z_q^*$
such that: $\mathbf{u^{(i)} = u_1^{(i)} * u_2^{(i)}}$

$$\mathbf{v_1^{(i)} = u_1^{(i)} P \,||\, w_1^{(i)} = u_2^{(i)} \bar{s}P \,||\, M_1^{(i)}} \rightarrow \mathcal{M}_1$$

Mix

Mix Server *j*

PK_j: $x_j \prod_{k=1}^{j} m_k P$ $\quad m_j = a_j^{(i)} b_j^{(i)} \quad (a_j^{(i)}, b_j^{(i)} \in Z_q^*)$

$(v_j^{(i)}, w_j^{(i)}, M_j^{(i)})$ →

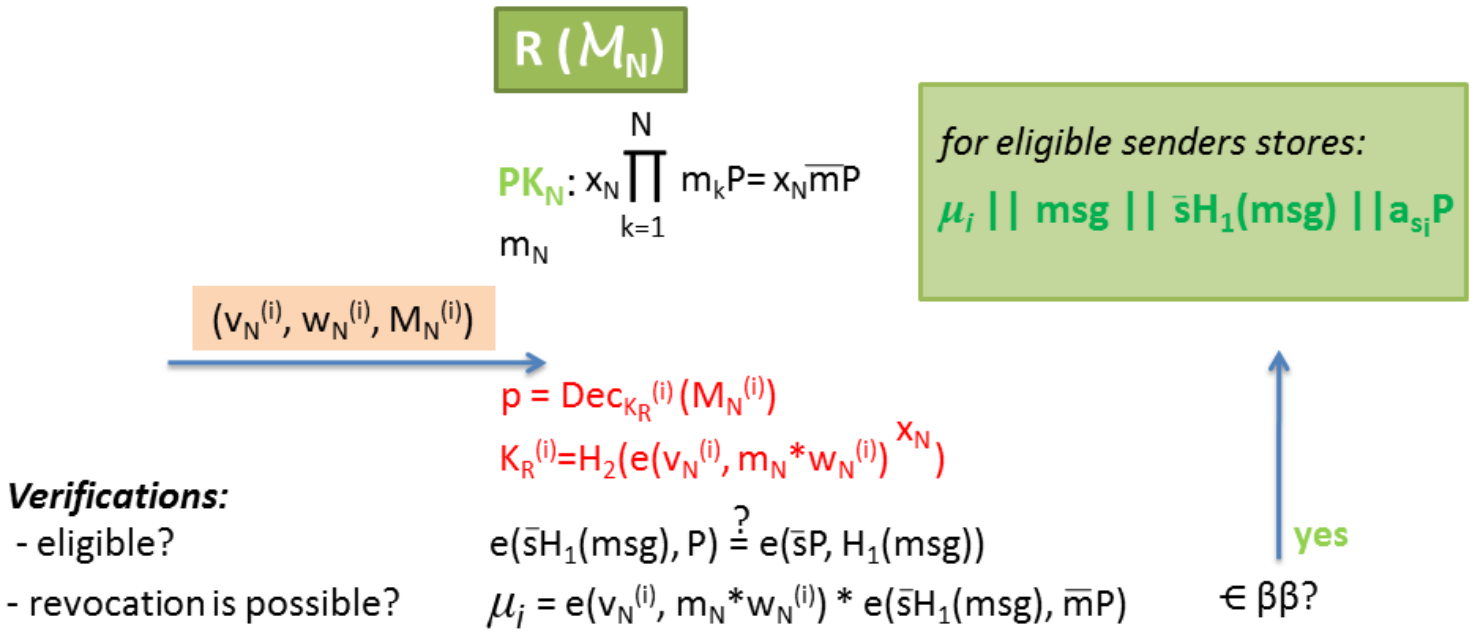
$$= \left(\prod_{k=1}^{j-1} a_k^{(i)} u_1^{(i)} P \, , \prod_{k=1}^{j-1} b_k^{(i)} u_2^{(i)} \bar{s} P, M_j^{(i)} \right)$$

$$K_j^{(i)} = H_2\left(e\left(\prod_{k=1}^{j} a_k^{(i)} u_1^{(i)} P, \prod_{k=1}^{j} b_k^{(i)} u_2^{(i)} \bar{s} P\right)^{x_j}\right)$$

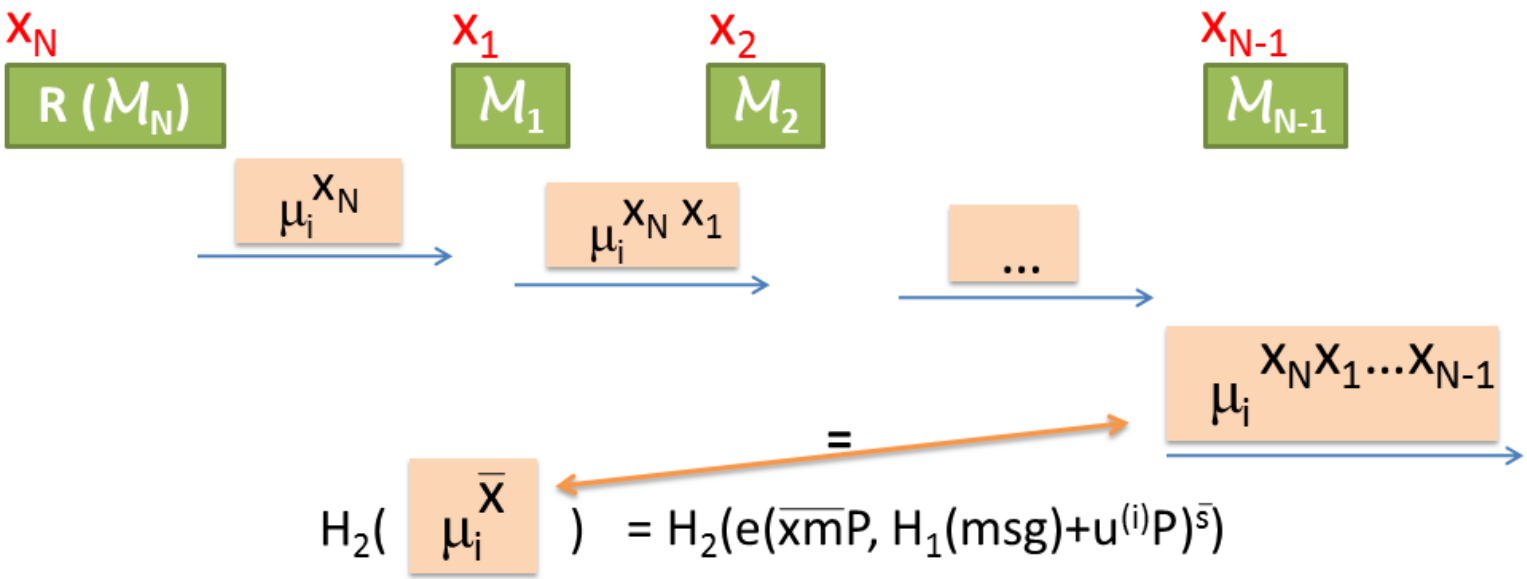
$$M_{j+1}^{(i)} = Dec_{K_j}^{(i)}(M_j^{(i)})$$

$(v_{j+1}^{(i)} = a_j^{(i)} v_j^{(i)}, w_{j+1}^{(i)} = b_j^{(i)} w_j^{(i)}, M_{j+1}^{(i)})$ →

Üzenetek feldolgozása



Anonimitás visszavonása



RA tárolja: $\varepsilon_i = S_i \otimes H_2(e(x\bar{m}P, H_1(msg) + u^{(i)}P)^{\bar{s}})$

S ellenőrzi(visszavonja):

$$\varepsilon_i = S_i \otimes H_2(e(\bar{s}H_1(msg), x\bar{m}P) \cdot e(\bar{s}P, x\bar{m}P)^{u^{(i)}})$$

R visszavonja: $\varepsilon_i = S_i \otimes H_2(e(\bar{s}u^{(i)}P, \bar{m}P) \cdot e(\bar{s}H_1(msg), \bar{m}P)^{\bar{x}})$

Jellemzők

- titkosság (privacy): anonim csatorna (μ_i és ε_i nélkül)
- jogosultság (eligibility): vak aláírás
- egyszer-szavazhatóság (unreusability): vak aláírás
- igazságosság (fairness): határidő után számolják a szavazatokat
- személyes ellenőrizhetőség(individual verifiability): szavazó ellenőrizheti BB-n a szavazatát
- univerzális ellenőrizhetőség(global verifiability): ha minden szavazó szavaz, ha regisztrált (R feltehet szavazatot)
- megvesztegethetetlenség, zsarolhatatlanság (receipt-freeness, uncoercibility): nem teljesül (támadó ismeri $a_{S_i}P$ értéket)

Köszönöm a figyelmet!