Mixnetid - miks, mis ja kuidas?

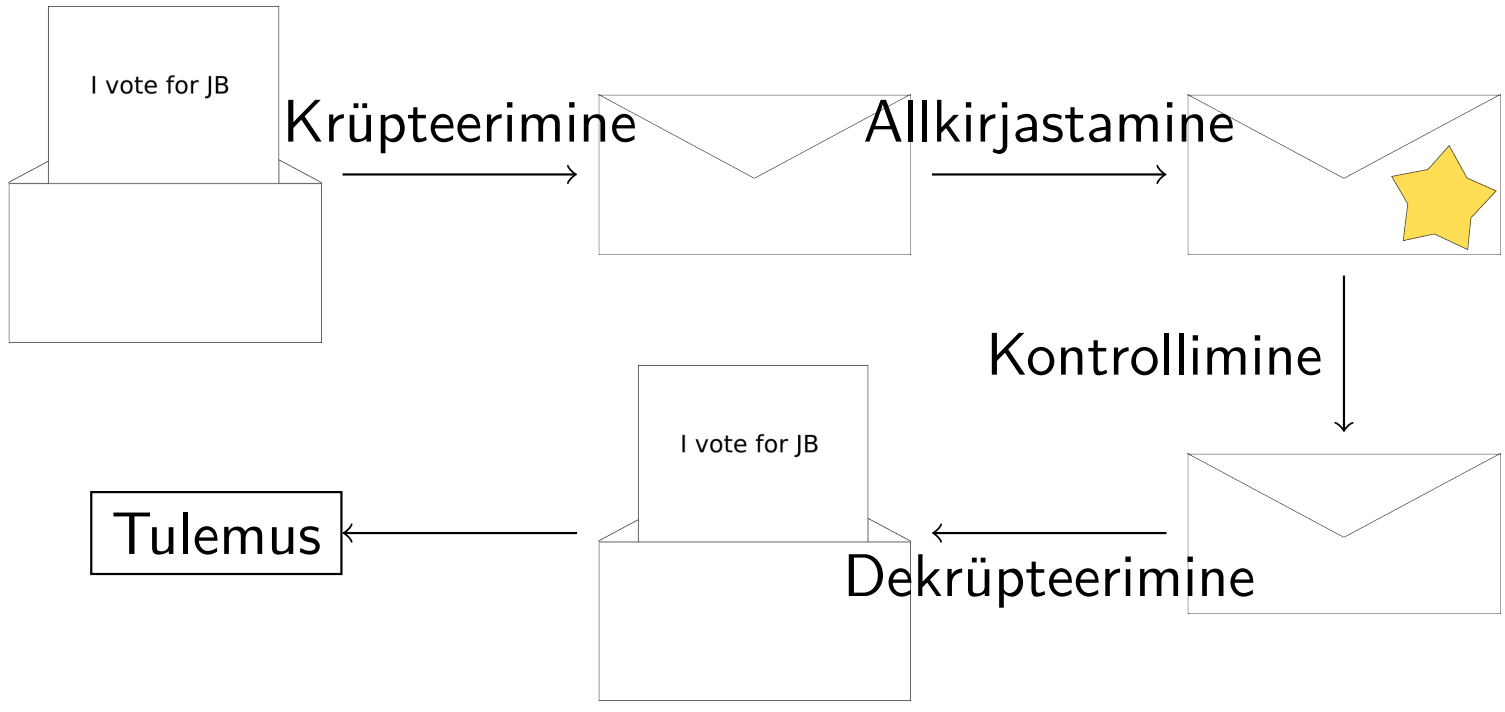
Ivo

18. juuni 2015

Eesmärk

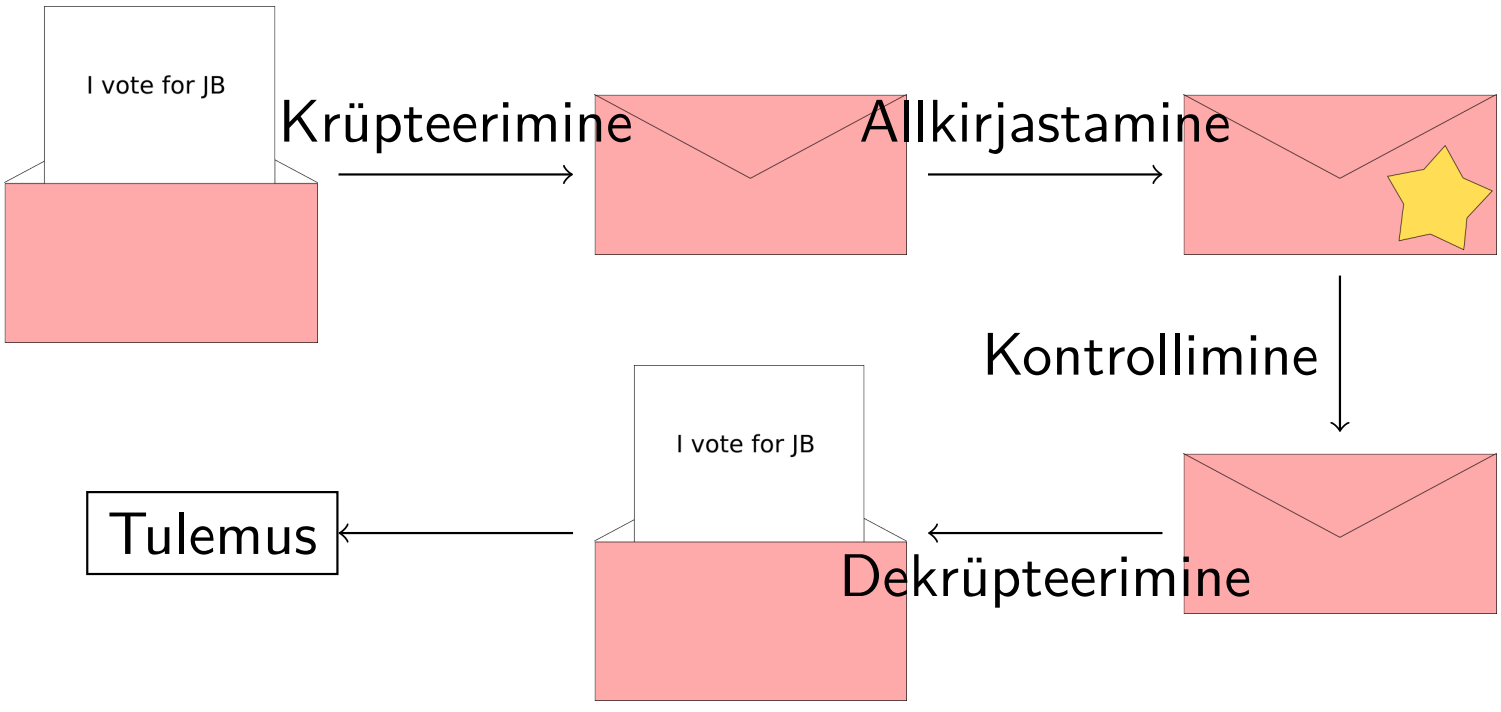
- Hetkel ei ole võimalik tõestada HLR-i korrektset tegevust;
- tervikluse ja korrektsuse auditeerimine rikuks hetkel paratamatult valija privaatsust;
- eesmärk - tervikluse ja korrektsuse tõestus säilitades valija privaatsust.

Stsenaarium



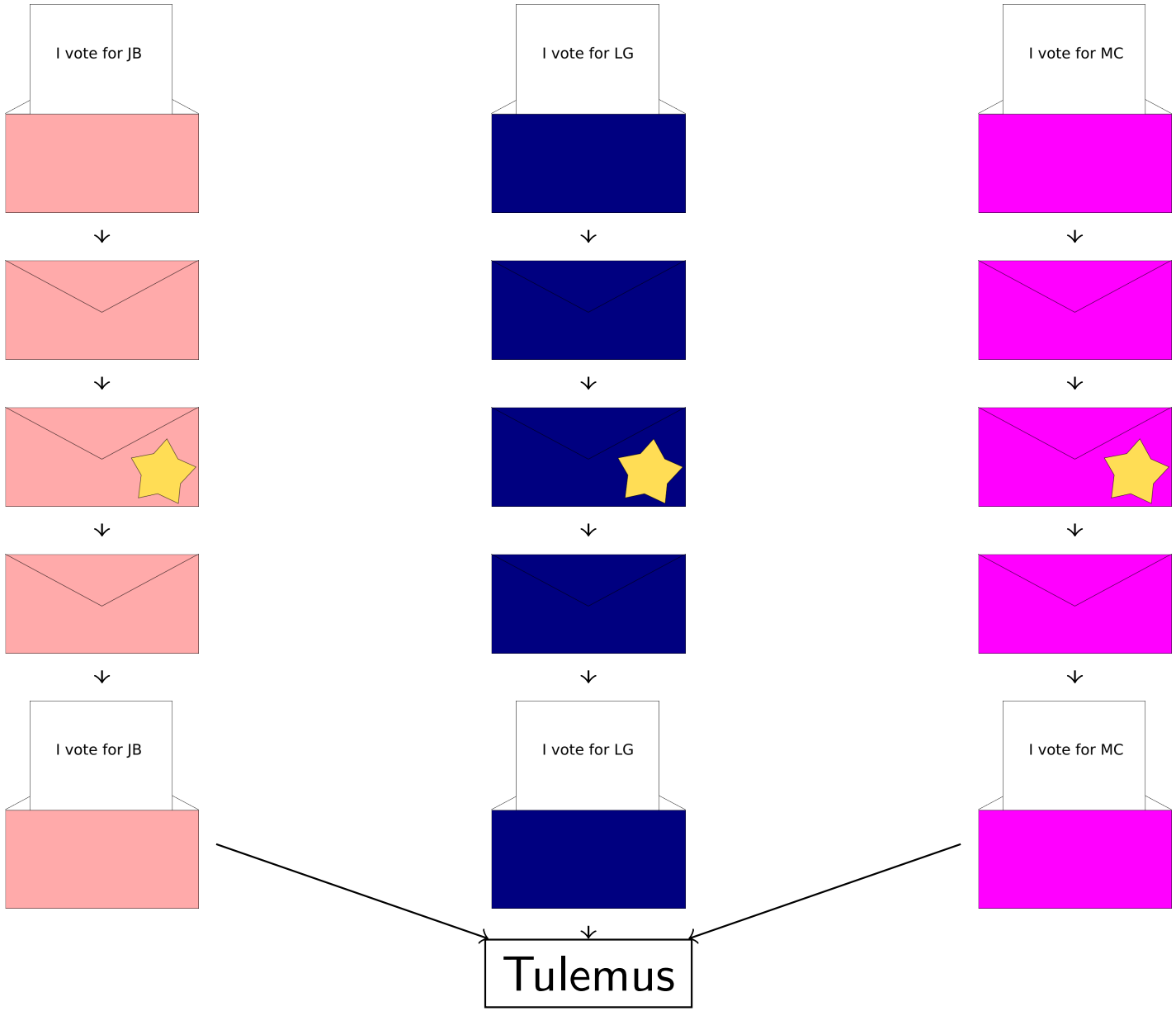
Joonis: Internetivalimiste protokoll praegu (lihtsustatud)

Stsenaarium

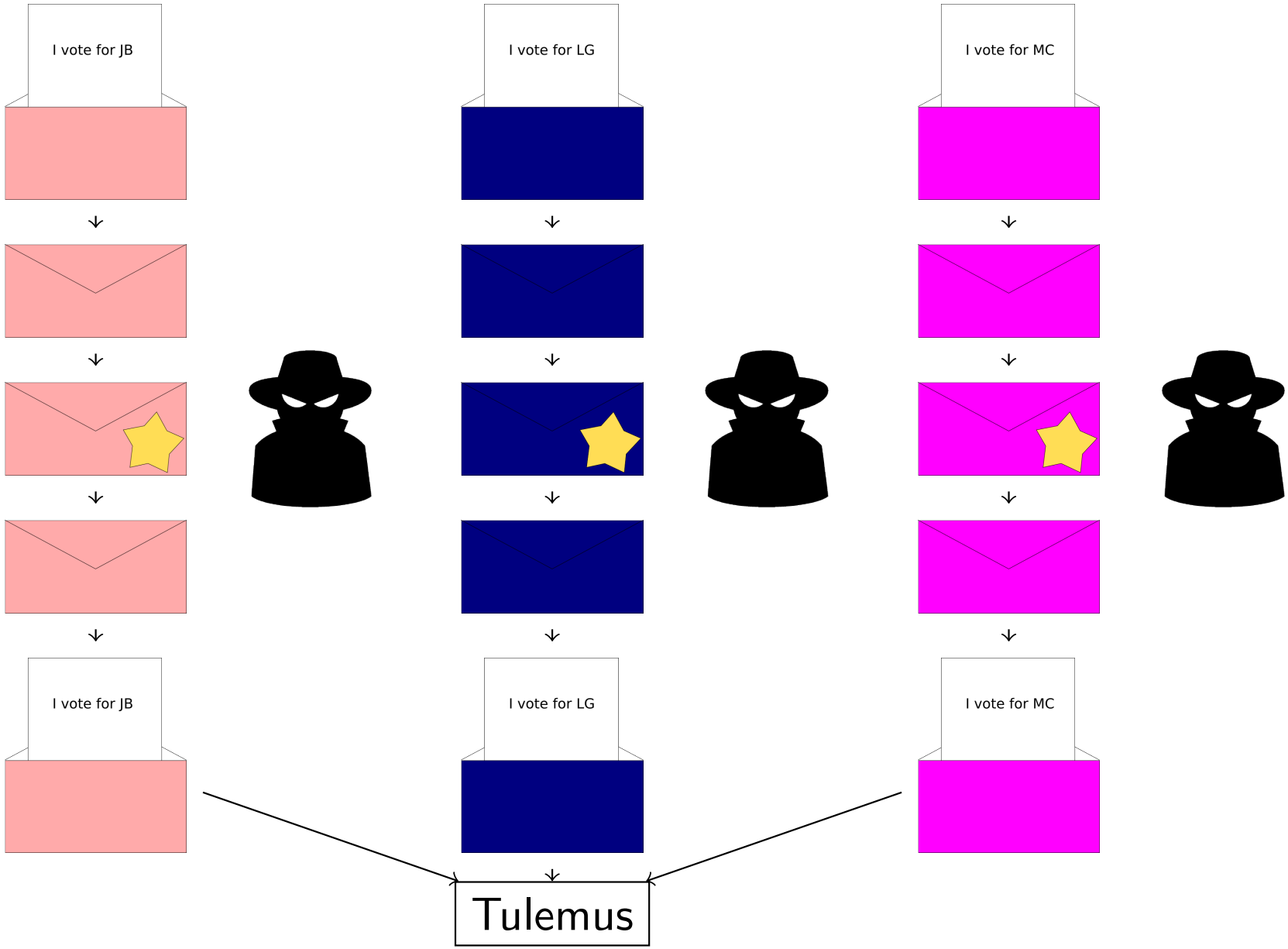


Joonis: Internetivalimiste protokoll praegu (krüptogrammi unikaalsus)

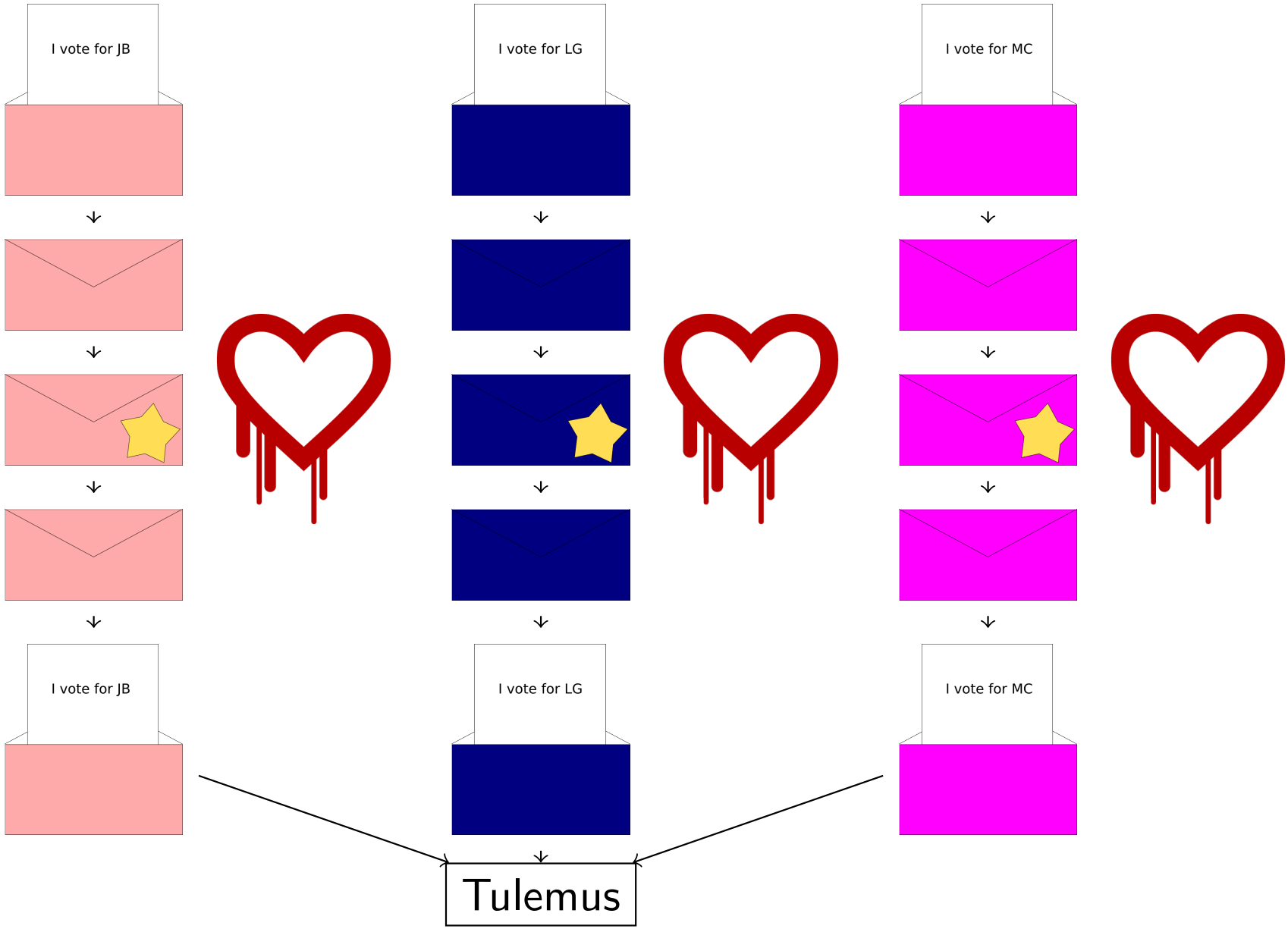
Stsenaarium



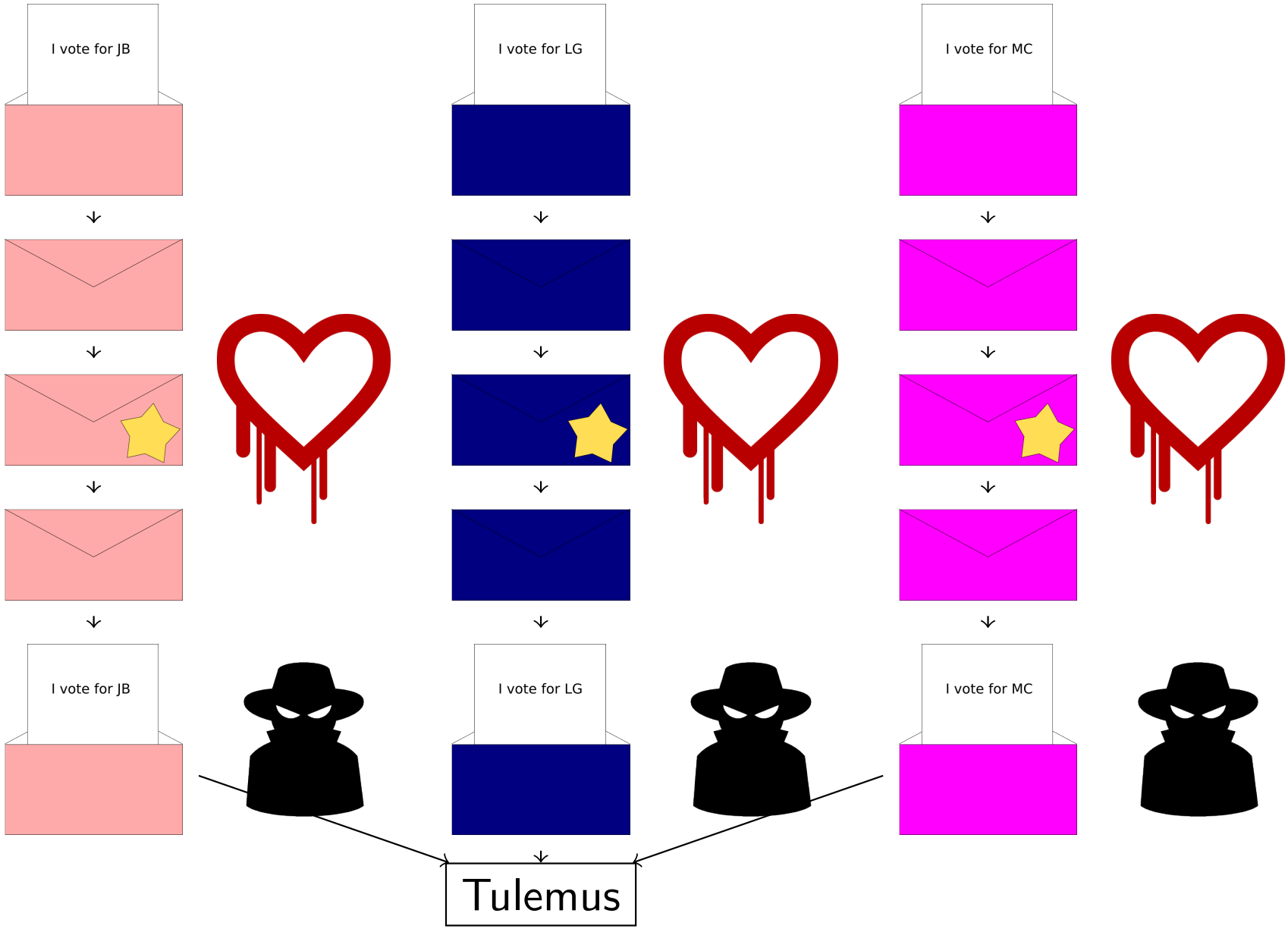
Stsenaarium



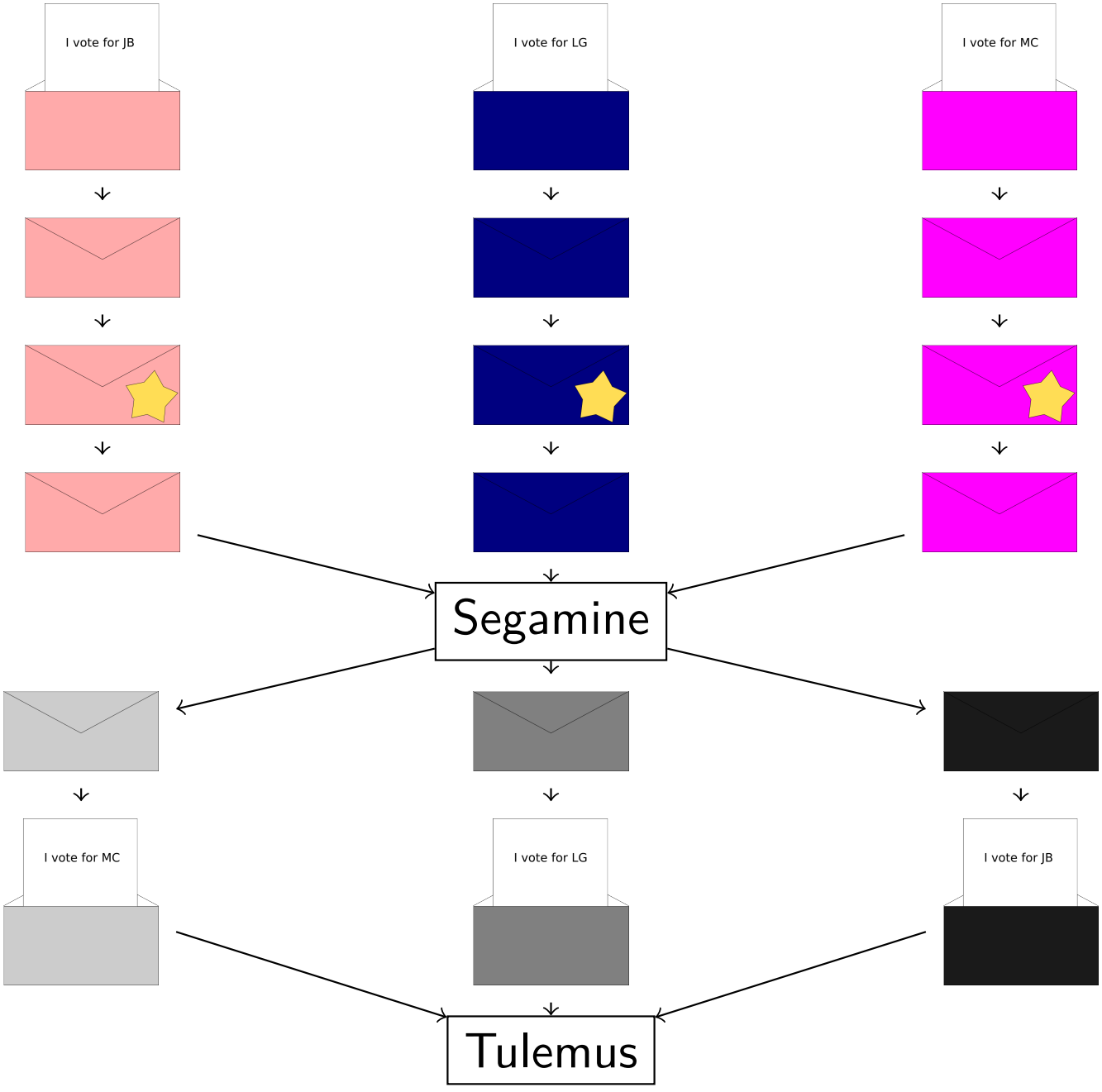
Stsenaarium



Stsenaarium



Lahendus - segamine



Segamine

Vajalik:

- krüptogrammide permuteerimine;
- krüptogrammide taas-randomiseerimine;
- tegevuse korrektsuse tõestus;

Segamine

Vajalik:

- krüptogrammide permuteerimine;
- krüptogrammide taas-randomiseerimine;
- tegevuse korrektsuse tõestus;
- arvutuslik efektiivsus.

Homomorfne krüptosüsteem

Definitsioon

Krüptosüsteem on multiplikatiivselt homomorfne kui iga $m_1, m_2 \in \mathcal{M}$ ja iga $\rho_1, \rho_2 \in \Omega$ korral

$$\mathcal{E}_{\mathrm{pk}}(m_1 m_2; \rho_1 + \rho_2) = \mathcal{E}_{\mathrm{pk}}(m_1; \rho_1)\mathcal{E}_{\mathrm{pk}}(m_2; \rho_2).$$

- multiplikatiivne homomorfism lubab teostada operatsioone krüptogrammidel;
- võimaldab taas-randomiseerimist:

$$\mathcal{E}_{\mathrm{pk}}(m_1; \rho_1)\mathcal{E}_{\mathrm{pk}}(1; \rho_2) = \mathcal{E}_{\mathrm{pk}}(m_1; \rho_1 + \rho_2).$$

Näide

ElGamali krüptosüsteem on multiplikatiivselt homomorfne.

Saame

- Valija privaatsustaseme kasv;
- võimalik anda tõestus korrektse dekrüpteerimise kohta;
- ElGamaliga võimalik kasutada elliptkõveraid (RIA krüptouuring 2015);
- (vajadusel) avalik auditeeritavus.

Eksperimendid

- Olemas teostus Pythonis
- Olemas teostus C-s
- Lisaks kommertsiaalsed teostused
- Numbrilised tulemused:

krüptogrammide arv	segamise aeg (s)	tõestuse kontrolli aeg (s)
100	0.45	0.11
500	2.15	0.54
10000	42.58	10.58
50000	233.06	52.47
100000	418.12	104.00
200000	839.02	208.19