E-Voting Remote (unsupervised)

Usability
How the f*ç@ does it work? What am I supposed to do here?

Efficiency
Will there ever be a result?

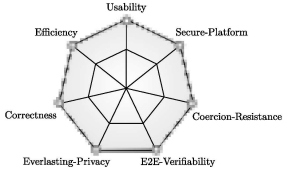
Secure-Platform
"All your data are belong to us" (sic.)

Correctness
My neighbour had the NSA vote instead?!

Coercion Resistance
We know your kid's location... vote 'yes' and all is well!

Everlasting Privacy
Your family is punished as your grandfather voted 'yes'!

E2E-Verifiability
I do not have a clue if my intention made it to the final tally?!



Berner Fachhochschule

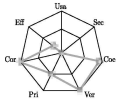
Protocol Enhancments

Voter casts with genuine intention
Real ballot $(A_1, B, \pi)|A_1 = Enc_y(\sigma_a, r_1), B = Enc'_y(v, r'_1), \pi = zkp(r_1, r'_1 : A_1, B)$
Simulated ballot $(A_2, B, \pi)|A_2 = Enc_y(\sigma_{a_i}, r_2), B = Enc'_y(v, r'_2), \pi = zkp(r_2, r'_2 : A_2, B)$

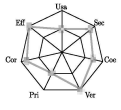
Voter casts with genuine intention
Duplicate ballot $(A_3, B, \pi)|A_3 = Enc_y(\sigma_a, r_3)$
Unintended voter error
Credential stolen -> Attack

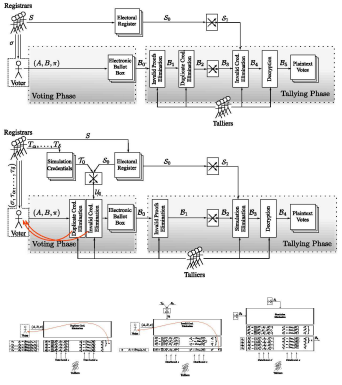
Voter / Someone casts
Invalid ballot $(A_4, B, \pi)|A_4 = Enc_y(\chi, r_4)$
Unintended voter error
Voter cannot remember
Board Flooding -> Attack

JCJ-05
Darmstadt -> Civitas



KHF-11

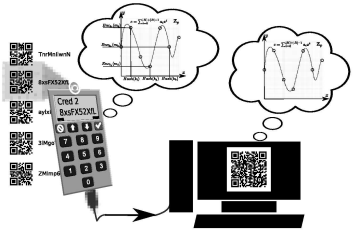




Multi Secret Management

Voter must be able to...

.... manage multiple credentials seamlessly (no search)
.... hide the true amount of credentials (chaffing)
.... having access to the credentials (non-challengeable)



Usability Studies

Secure Platform

The Secure Platform Module must
... be restricted in its usage (finite state machine / software close)
... provide trust (analyzable down to the metal by 'experts')
... indicate tampering
... make the calculation for the cryptographic aspects
... make the calculation of the E2E-verification aspects
... provide entropy to the rest of us (not to the user)
... intuitive to use
... easily replacable (no secrets within)

E-Voting Remote (unsupervised)

Usability
How the f*ç@ does it work? What am I supposed to do here?

Efficiency
Will there ever be a result?

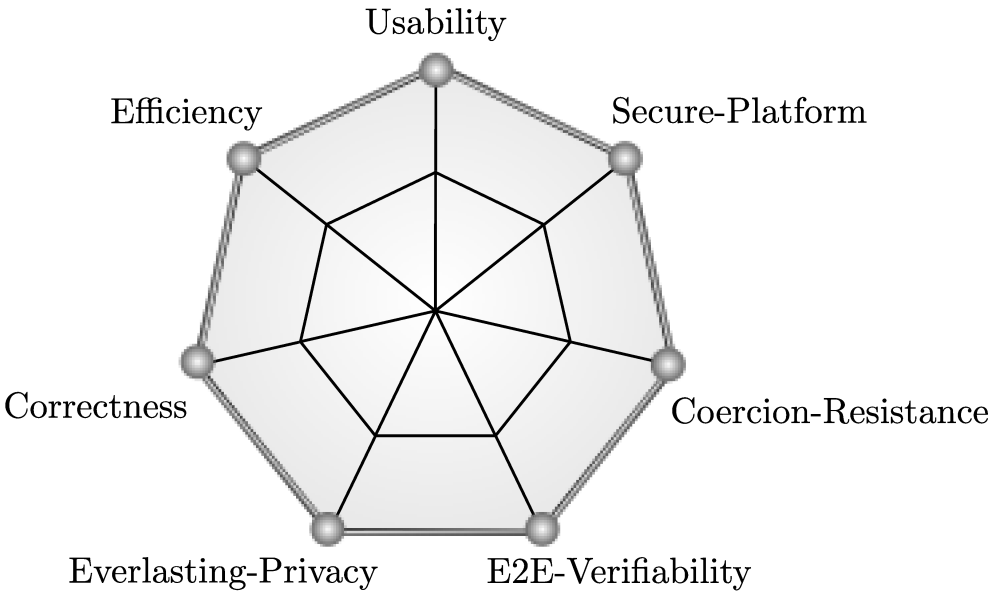
Secure-Platform
"All your data are belong to us" (sic.)

Correctness
My neighbour had the NSA vote instead?!

Coercion Resistance
We know your kid's location... vote 'yes' and all is well!

Everlasting Privacy
Your family is punished as your grandfather voted 'yes'!

E2E-Verifiability
I do not have a clue if my intention made it to the final tally?!



Usability

How the f*ç@ does it work? What am I supposed to do here?

Efficiency

Will there ever be a result?

Secure-Platform

"All your data are belong to us" (sic.)

Correctness

My neighbour had the NSA vote instead?!

Coercion Resistance

We know your kid's location... vote 'yes' and all is well!

Everlasting Privacy

Your family is punished as your grandfather voted 'yes'!

E2E-Verifiability

I do not have a clue if my intention made it to the final tally?!

E-Voting Remote (unsupervised)

Usability
How the f*ç@ does it work? What am I supposed to do here?

Efficiency
Will there ever be a result?

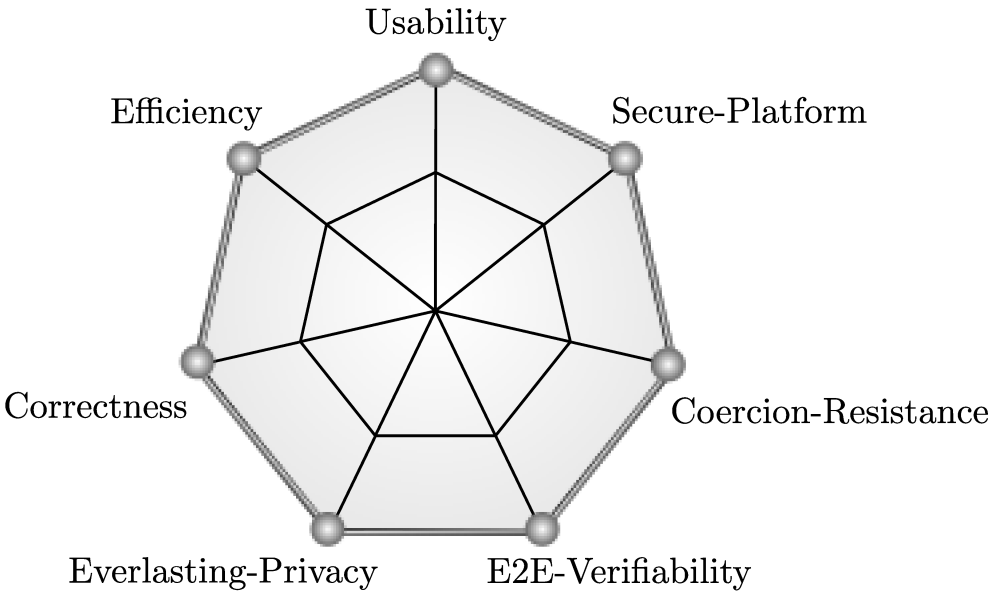
Secure-Platform
"All your data are belong to us" (sic.)

Correctness
My neighbour had the NSA vote instead?!

Coercion Resistance
We know your kid's location... vote 'yes' and all is well!

Everlasting Privacy
Your family is punished as your grandfather voted 'yes'!

E2E-Verifiability
I do not have a clue if my intention made it to the final tally?!



E-Voting Remote (unsupervised)

Usability
How the f*ç@ does it work? What am I supposed to do here?

Efficiency
Will there ever be a result?

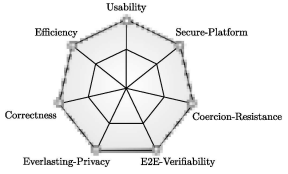
Secure-Platform
"All your data are belong to us" (sic.)

Correctness
My neighbour had the NSA vote instead?!

Coercion Resistance
We know your kid's location... vote 'yes' and all is well!

Everlasting Privacy
Your family is punished as your grandfather voted 'yes'!

E2E-Verifiability
I do not have a clue if my intention made it to the final tally?!



Berner Fachhochschule

Protocol Enhancments

Voter casts with genuine intention

Real ballot $(A_1, B, \pi)|A_1 = Enc_y(\sigma_a, r_1), B = Enc'_y(v, r'_1), \pi = zkp(r_1, r'_1 : A_1, B)$

Simulated ballot $(A_2, B, \pi)|A_2 = Enc_y(\sigma_a, r_2), B = Enc'_y(v, r'_2), \pi = zkp(r_2, r'_2 : A_2, B)$

Voter casts with genuine intention

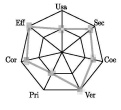
Duplicate ballot $(A_3, B, \pi)|A_3 = Enc_y(\sigma_a, r_3)$
Unintended voter error
Credential stolen -> Attack

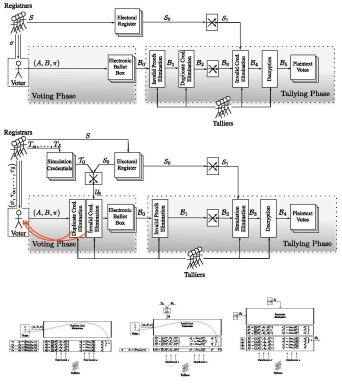
Voter / Someone casts

Invalid ballot $(A_4, B, \pi)|A_4 = Enc_y(\chi, r_4)$
Unintended voter error
Voter cannot remember
Board Flooding -> Attack

JCJ-05

KHF-11

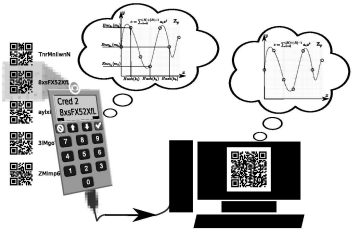




Multi Secret Management

Voter must be able to...

.... manage multiple credentials seamlessly (no search)
.... hide the true amount of credentials (chaffing)
.... having access to the credentials (non-challengeable)



Usability Studies

Secure Platform

The Secure Platform Module must
... be restricted in its usage (finite state machine / software close)
... provide trust (analyzable down to the metal by 'experts')
... indicate tampering
... make the calculation for the cryptographic aspects
... make the calculation of the E2E-verification aspects
... provide entropy to the rest of us (not to the user)
... intuitive to use
... easily replacable (no secrets within)

Protocol Enhancments

Voter casts with genuine intention

Real ballot $(A_1, B, \pi)|A_1 = Enc_y(\sigma_a, r_1), B = Enc'_y(v, r'_1), \pi = zkp(r_1, r'_1 : A_1, B)$

Simulated ballot $(A_2, B, \pi)|A_2 = Enc_y(\tau_{a_\alpha}, r_2), B = Enc'_y(v, r'_2), \pi = zkp(r_2, r'_2 : A_2, B)$

Voter casts with genuine intention

Duplicate ballot $(A_3, B, \pi)|A_3 = Enc_y(\sigma_a, r_3)$

- Unintended voter error
- Credential stolen -> Attack

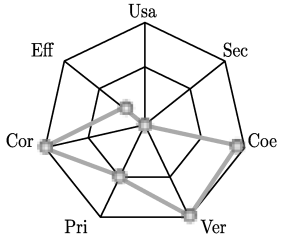
Voter / Someone casts

Invalid ballot $(A_4, B, \pi)|A_4 = Enc_y(\chi, r_4)$

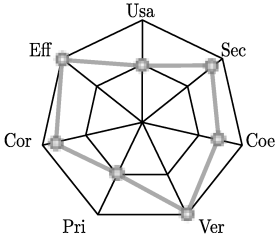
- Unintended voter error
- Voter cannot remember
- Board Flooding -> Attack

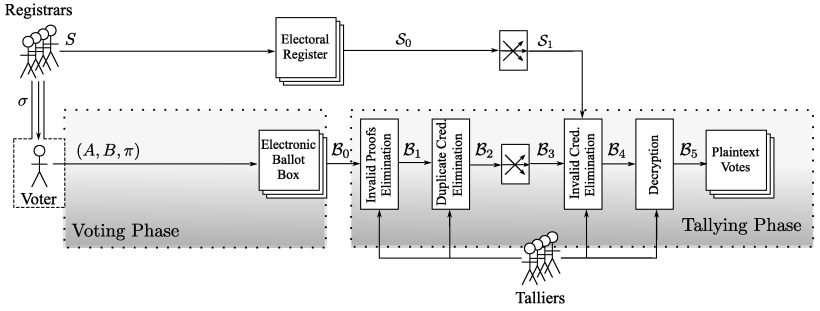
JCJ-05

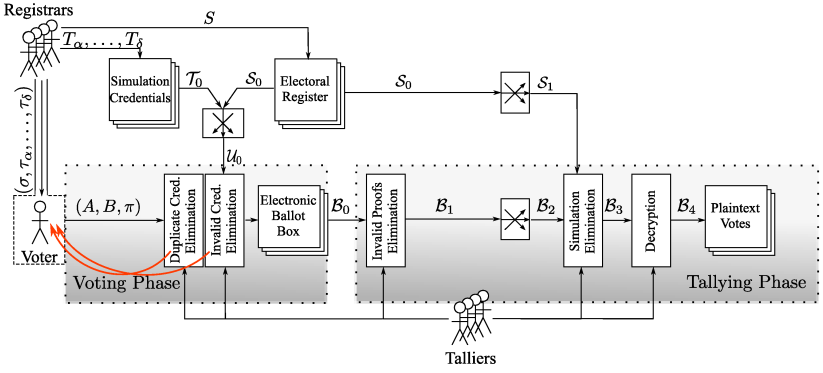
Darmstadt -> Civitas

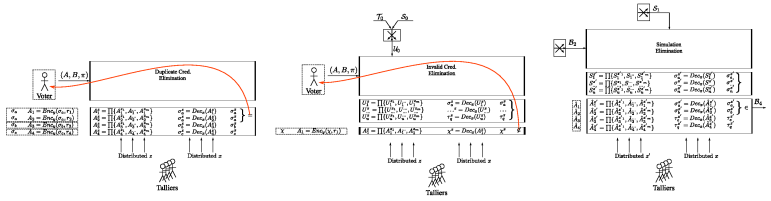


KHF-11



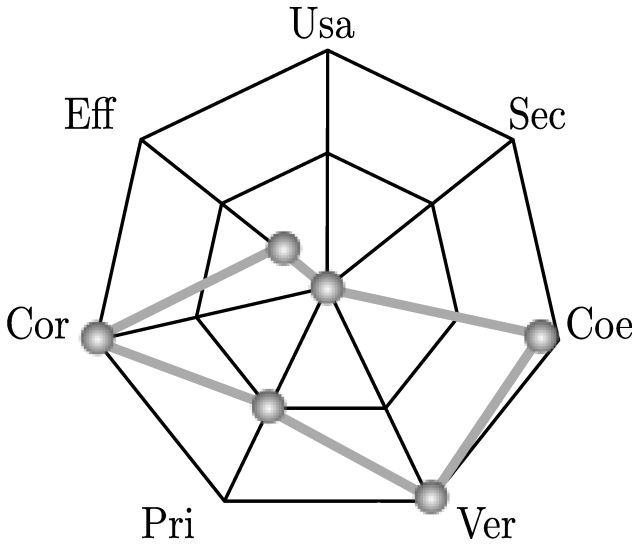




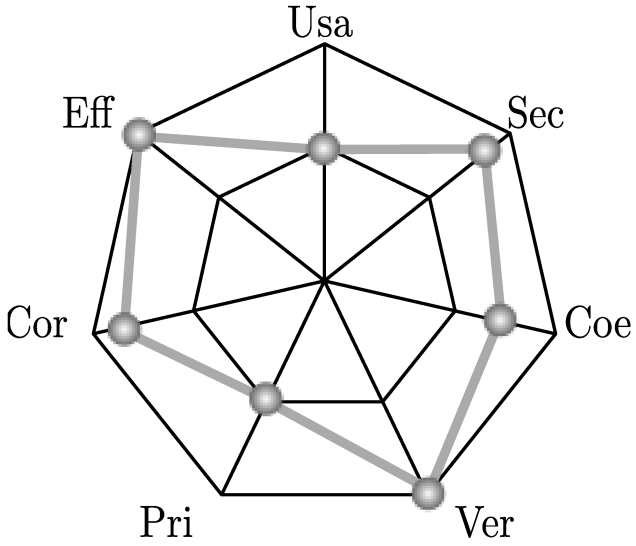


JCJ-05

Darmstadt -> Civitas

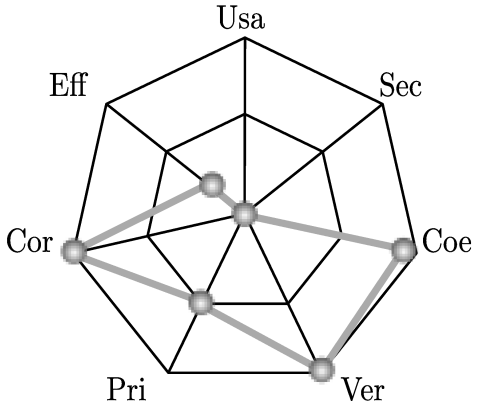


KHF-11

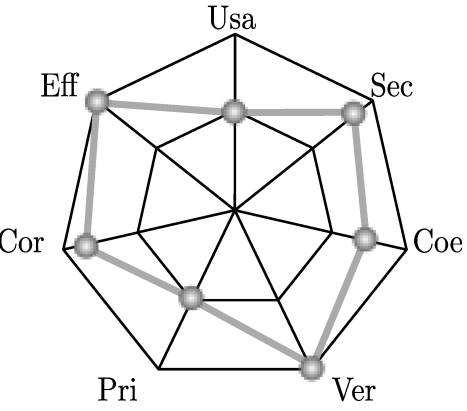


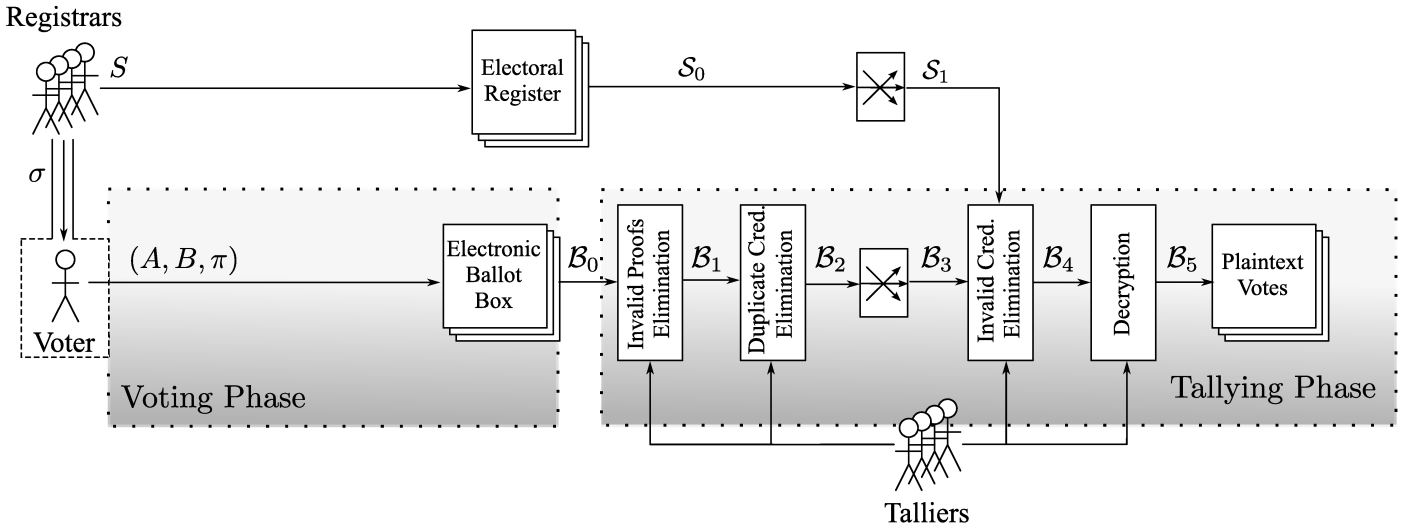
JCJ-05

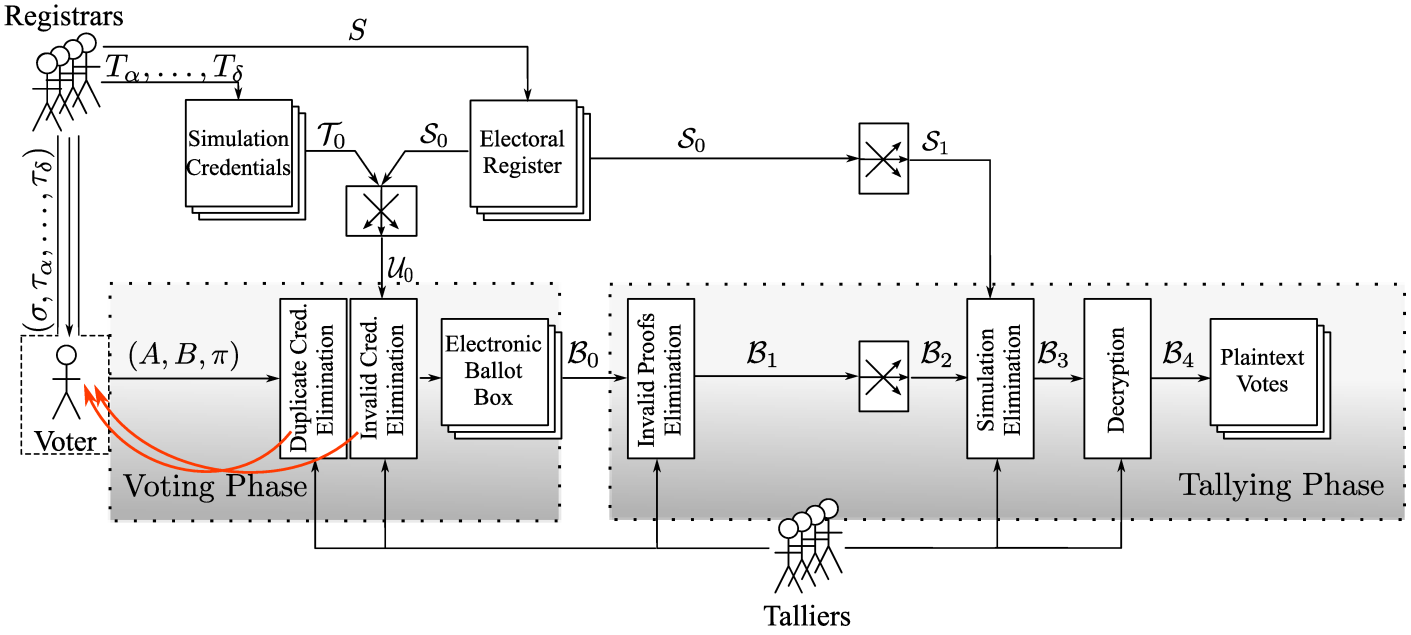
Darmstadt -> Civitas

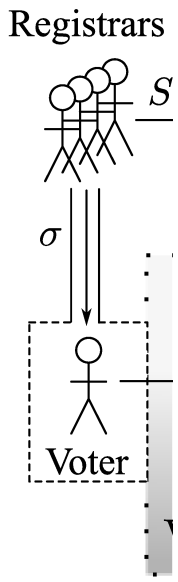


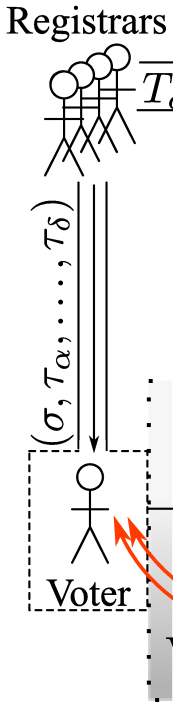
KHF-11

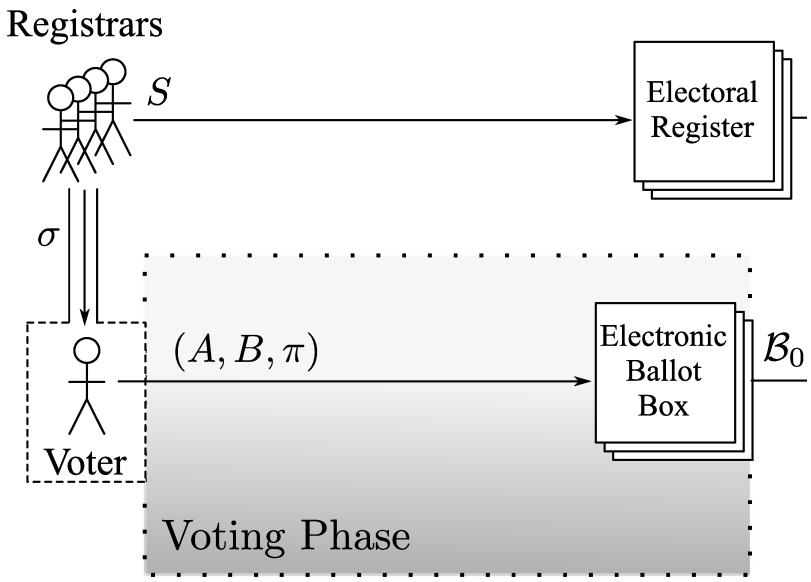


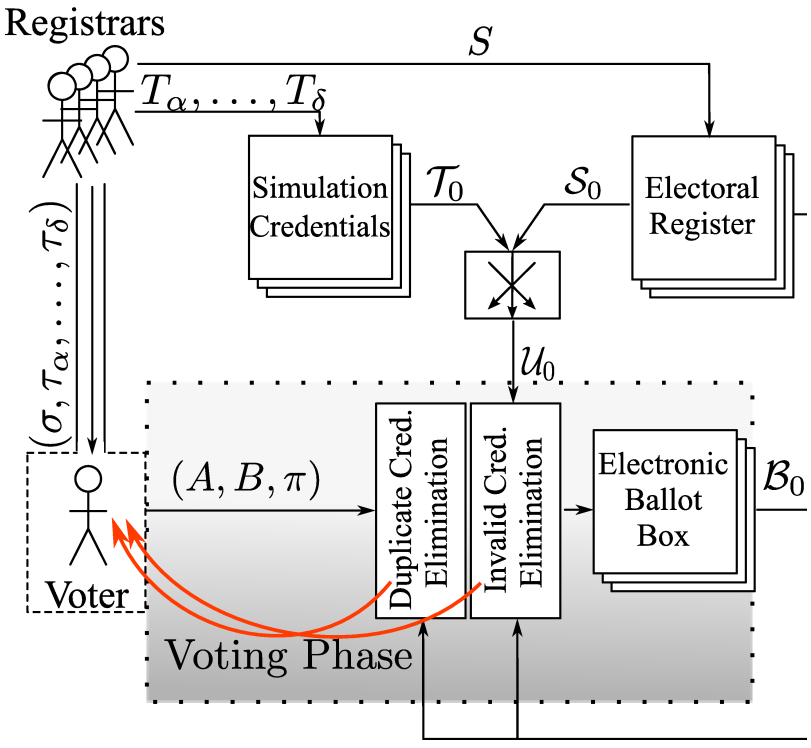


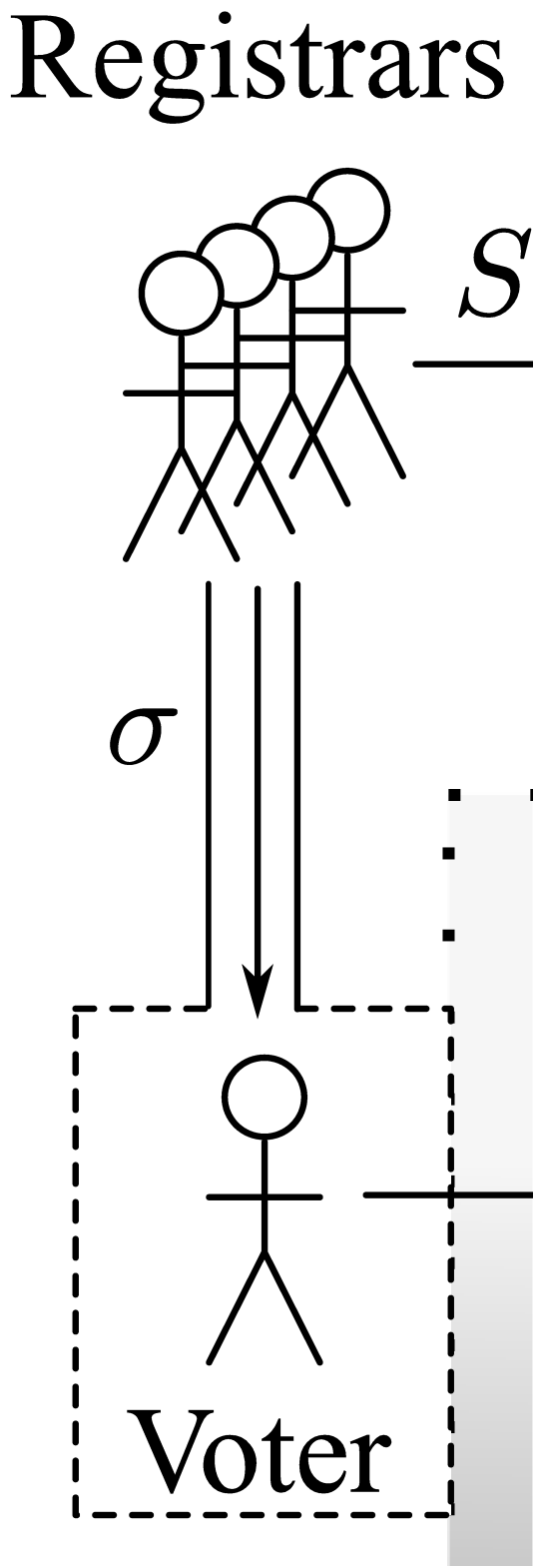



Registrars
S
σ
Voter

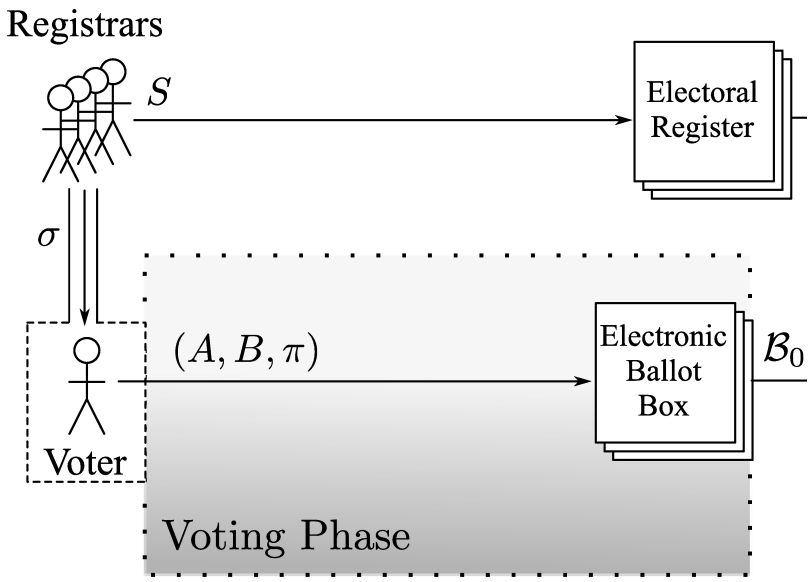

Registrars
T
$(\sigma, \tau_\alpha, \ldots, \tau_\delta)$
Voter

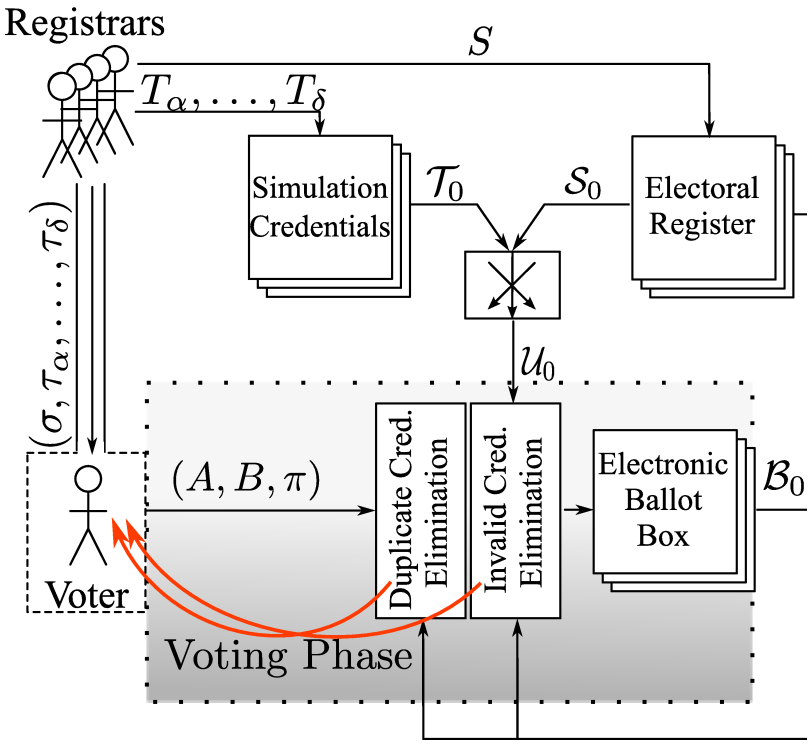

Registrars
S
Electoral Register
σ
(A, B, π)
Electronic Ballot Box
$\mathcal{B}_0$
Voter
Voting Phase

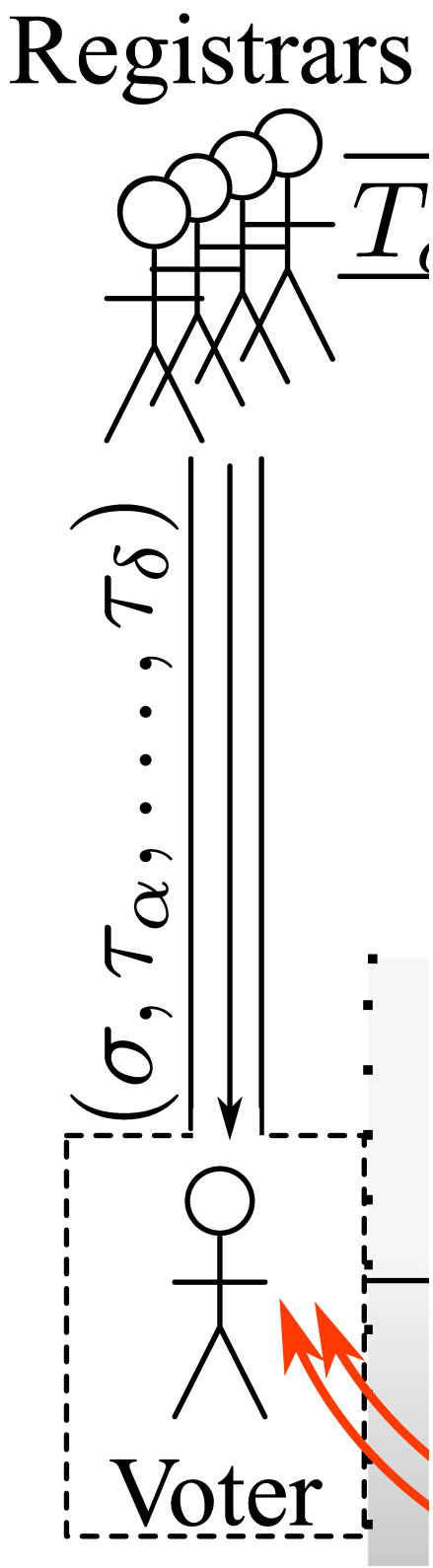

Registrars
S
$T_\alpha, \ldots, T_\delta$
Simulation Credentials
$\mathcal{T}_0$
$\mathcal{S}_0$
Electoral Register
$(\sigma, \tau_\alpha, \ldots, \tau_\delta)$
$\mathcal{U}_0$
(A, B, π)
Duplicate Cred. Elimination
Invalid Cred. Elimination
Electronic Ballot Box
$\mathcal{B}_0$
Voter
Voting Phase

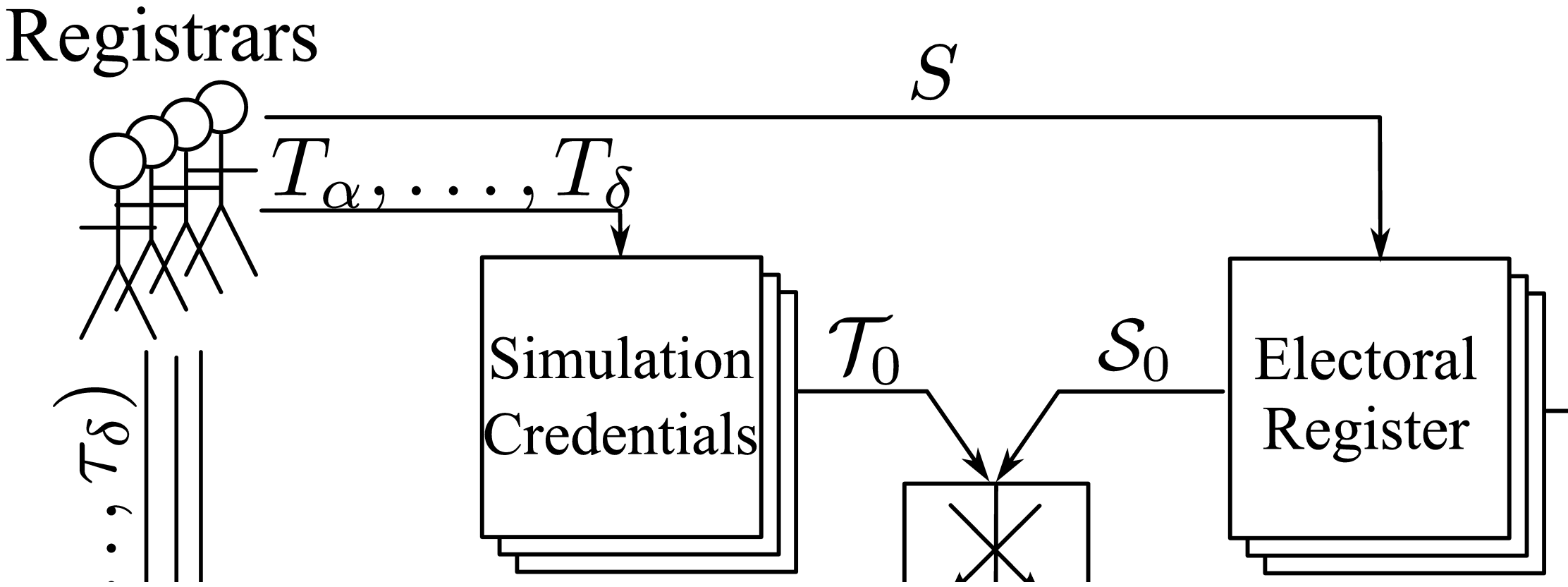

Registrars
S
σ
Voter

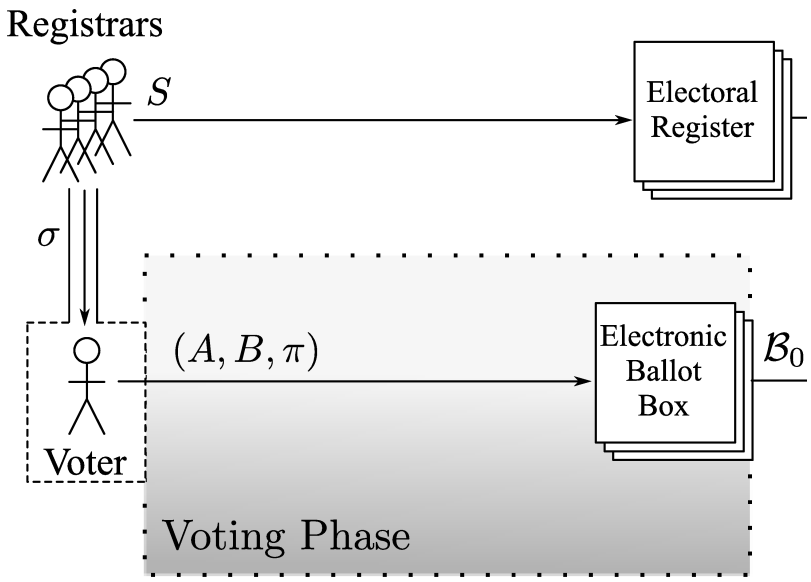

Registrars
S
σ
Electoral
Register

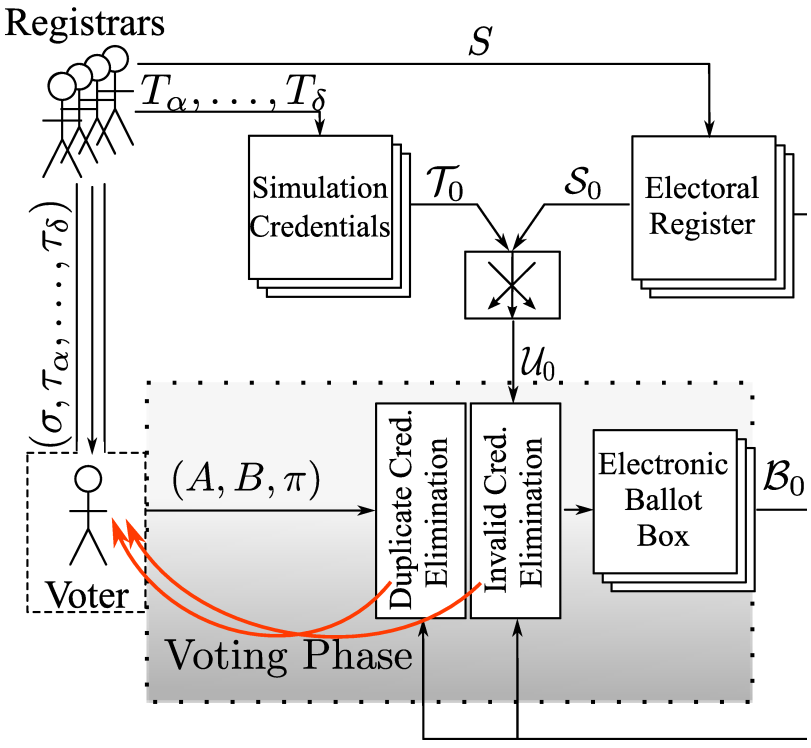

Registrars
S
Electoral Register
σ
(A, B, π)
Electronic Ballot Box
$\mathcal{B}_0$
Voter
Voting Phase

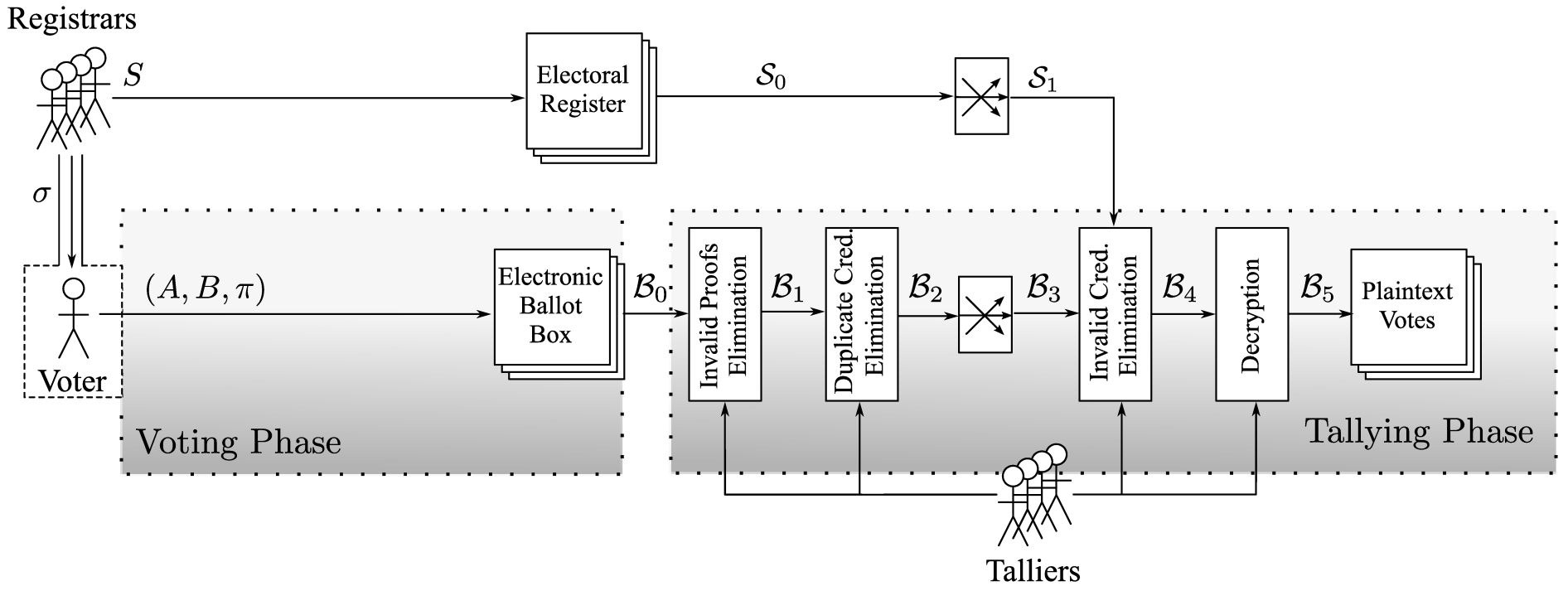

Registrars
S
$T_\alpha, \ldots, T_\delta$
Simulation Credentials
$\mathcal{T}_0$
$\mathcal{S}_0$
Electoral Register
$(\sigma, \tau_\alpha, \ldots, \tau_\delta)$
$\mathcal{U}_0$
(A, B, π)
Duplicate Cred. Elimination
Invalid Cred. Elimination
Electronic Ballot Box
$\mathcal{B}_0$
Voter
Voting Phase

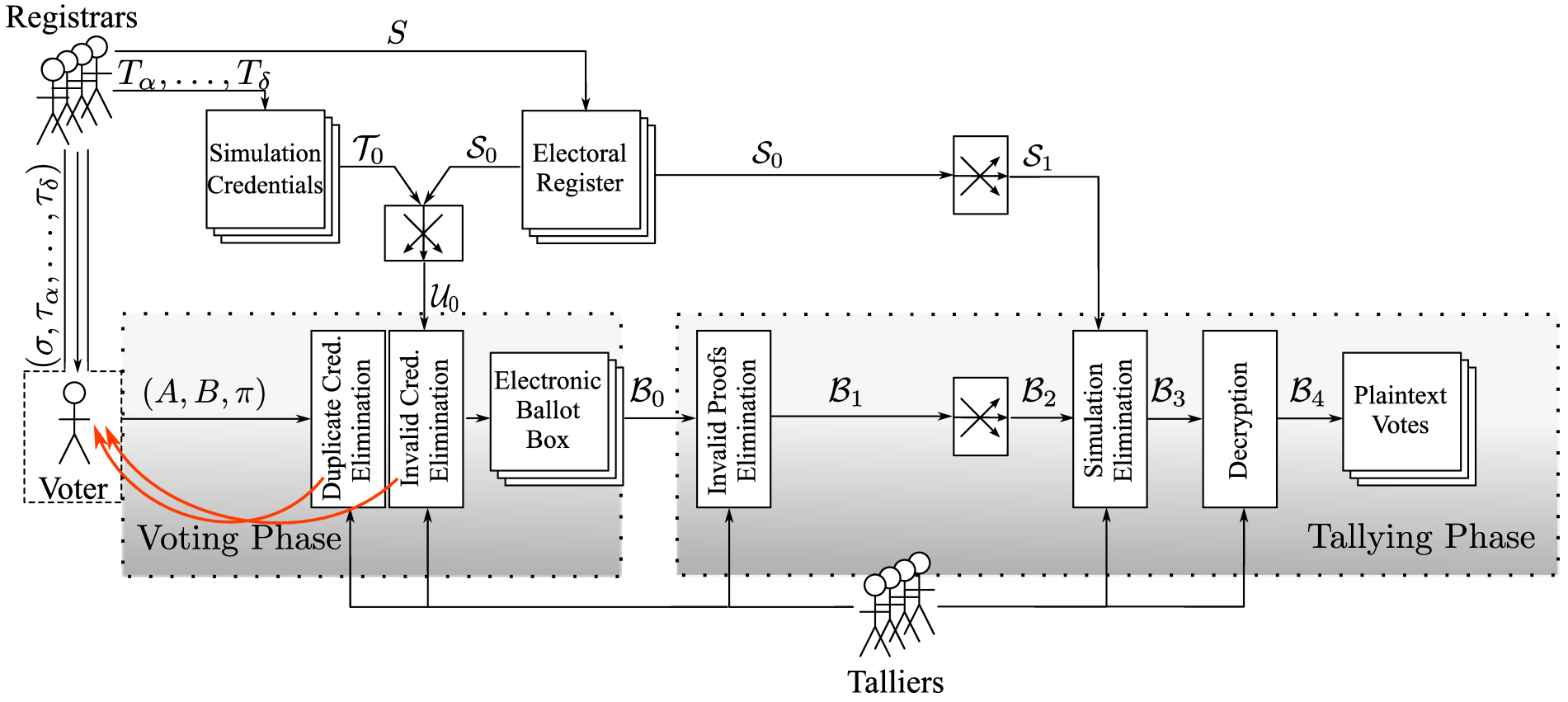

Registrars
$\overline{T_\delta}$
$(\sigma, \tau_\alpha, \ldots, \tau_\delta)$
Voter

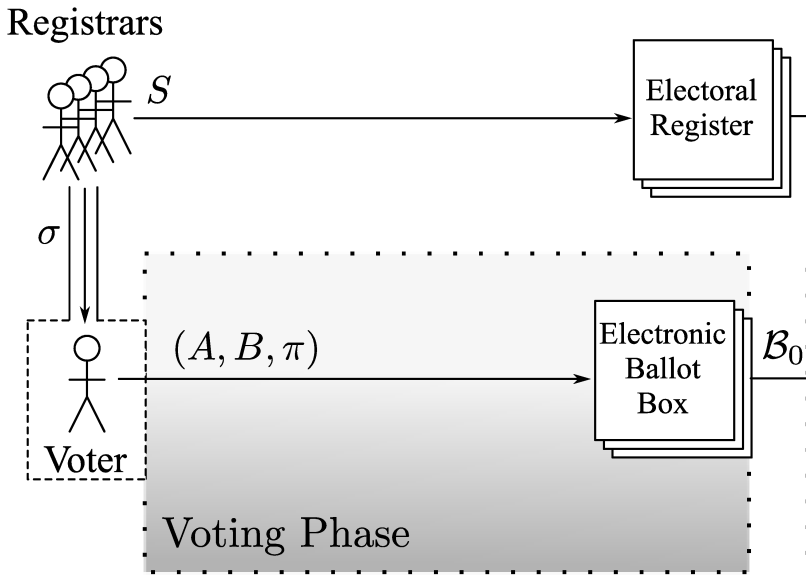

Registrars
S
$T_\alpha, \ldots, T_\delta$
$(\ldots, \tau_\delta)$
Simulation Credentials
$\mathcal{T}_0$
$\mathcal{S}_0$
Electoral Register

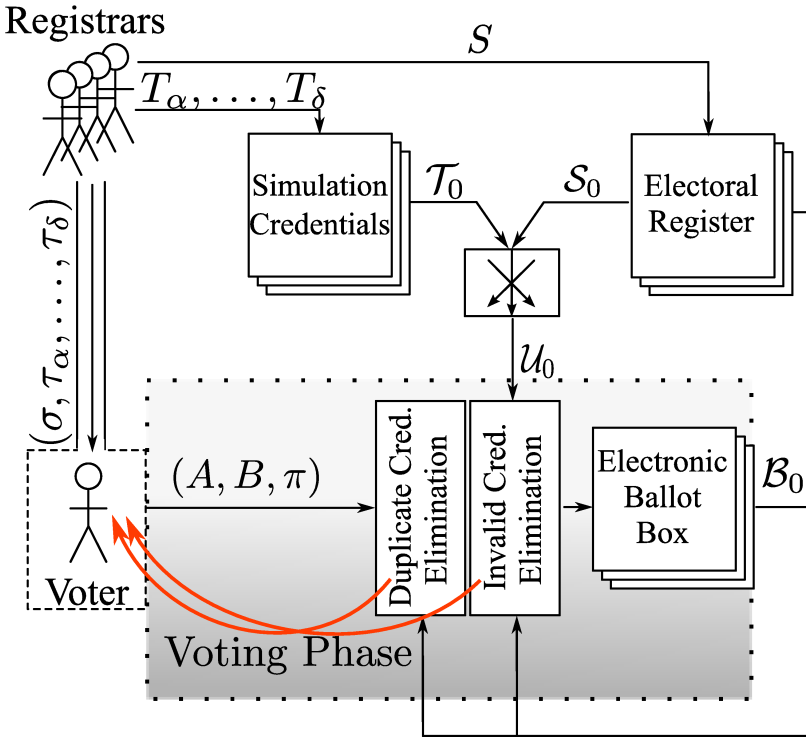

Registrars
S
Electoral Register
σ
(A, B, π)
Electronic Ballot Box
$\mathcal{B}_0$
Voter
Voting Phase


Registrars
S
$T_\alpha, \ldots, T_\delta$
Simulation Credentials
$\mathcal{T}_0$
$\mathcal{S}_0$
Electoral Register
$(\sigma, \tau_\alpha, \ldots, \tau_\delta)$
$\mathcal{U}_0$
(A, B, π)
Duplicate Cred. Elimination
Invalid Cred. Elimination
Electronic Ballot Box
$\mathcal{B}_0$
Voter
Voting Phase


Registrars
S
Electoral Register
$\mathcal{S}_0$
$\mathcal{S}_1$
σ
(A, B, π)
Voter
Electronic Ballot Box
$\mathcal{B}_0$
Invalid Proofs Elimination
$\mathcal{B}_1$
Duplicate Cred. Elimination
$\mathcal{B}_2$
$\mathcal{B}_3$
Invalid Cred. Elimination
$\mathcal{B}_4$
Decryption
$\mathcal{B}_5$
Plaintext Votes
Voting Phase
Tallying Phase
Talliers


Registrars
S
$T_\alpha, \ldots, T_\delta$
Simulation Credentials
$\mathcal{T}_0$
$\mathcal{S}_0$
Electoral Register
$\mathcal{S}_0$
$\mathcal{S}_1$
$\mathcal{U}_0$
$(\sigma, \tau_\alpha, \ldots, \tau_\delta)$
(A, B, π)
Voter
Duplicate Cred. Elimination
Invalid Cred. Elimination
Electronic Ballot Box
$\mathcal{B}_0$
Invalid Proofs Elimination
$\mathcal{B}_1$
$\mathcal{B}_2$
Simulation Elimination
$\mathcal{B}_3$
Decryption
$\mathcal{B}_4$
Plaintext Votes
Voting Phase
Tallying Phase
Talliers


Registrars
S
Electoral Register
σ
(A, B, π)
Electronic Ballot Box
$\mathcal{B}_0$
Voter
Voting Phase


Registrars
S
$T_\alpha, \ldots, T_\delta$
Simulation Credentials
$\mathcal{T}_0$
$\mathcal{S}_0$
Electoral Register
$\mathcal{U}_0$
$(\sigma, \tau_\alpha, \ldots, \tau_\delta)$
(A, B, π)
Duplicate Cred. Elimination
Invalid Cred. Elimination
Electronic Ballot Box
$\mathcal{B}_0$
Voter
Voting Phase

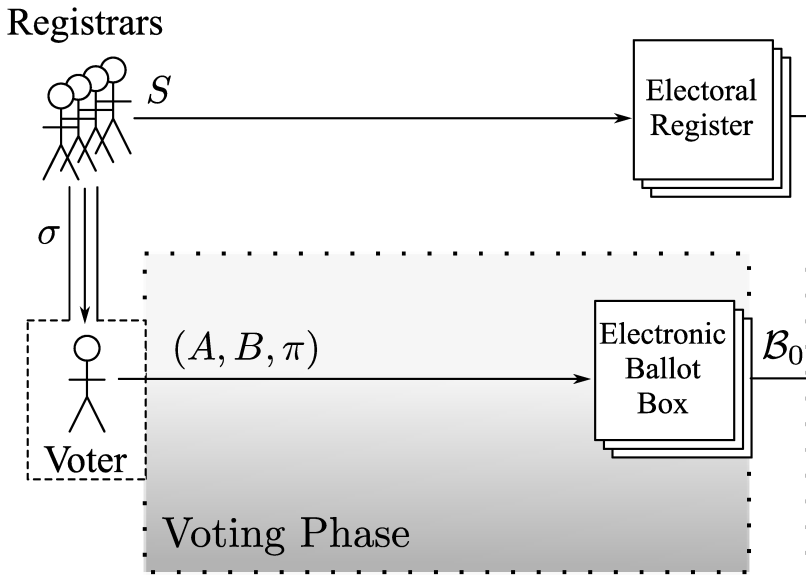
Voter casts with genuine intention

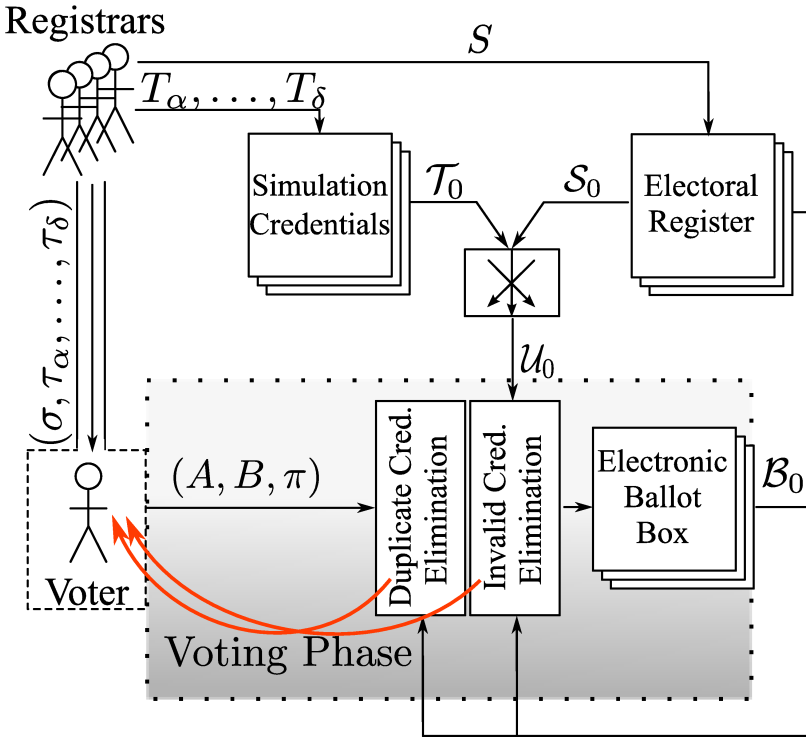
Real ballot $(A_1, B, \pi) | A_1 = Enc_y(\sigma_a, r_1), B = Enc'_y(v, r'_1), \pi = zkp(r_1, r'_1 : A_1, B)$

Voter casts with genuine intention

Real ballot $(A_1, B, \pi) | A_1 = Enc_y(\sigma_a, r_1), B = Enc'_y(v, r'_1), \pi = zkp(r_1, r'_1 : A_1, B)$

Simulated ballot $(A_2, B, \pi) | A_2 = Enc_y(\tau_{a_\alpha}, r_2), B = Enc'_y(v, r'_2), \pi = zkp(r_2, r'_2 : A_2, B)$


Registrars
S
Electoral Register
σ
(A, B, π)
Electronic Ballot Box
$\mathcal{B}_0$
Voter
Voting Phase


Registrars
S
$T_\alpha, \ldots, T_\delta$
Simulation Credentials
$\mathcal{T}_0$
$\mathcal{S}_0$
Electoral Register
$(\sigma, \tau_\alpha, \ldots, \tau_\delta)$
$\mathcal{U}_0$
(A, B, π)
Duplicate Cred. Elimination
Invalid Cred. Elimination
Electronic Ballot Box
$\mathcal{B}_0$
Voter
Voting Phase

Voter casts with genuine intention

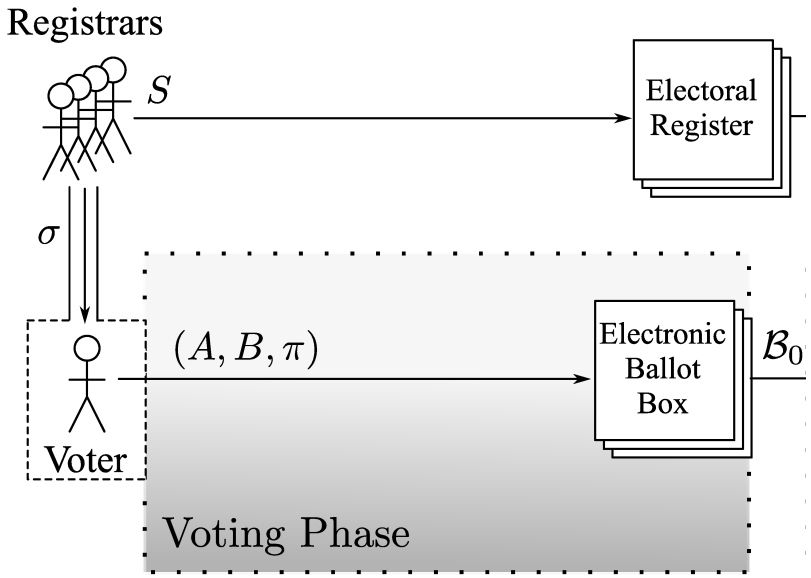
Duplicate ballot $(A_3, B, \pi)|A_3 = Enc_y(\sigma_a, r_3)$

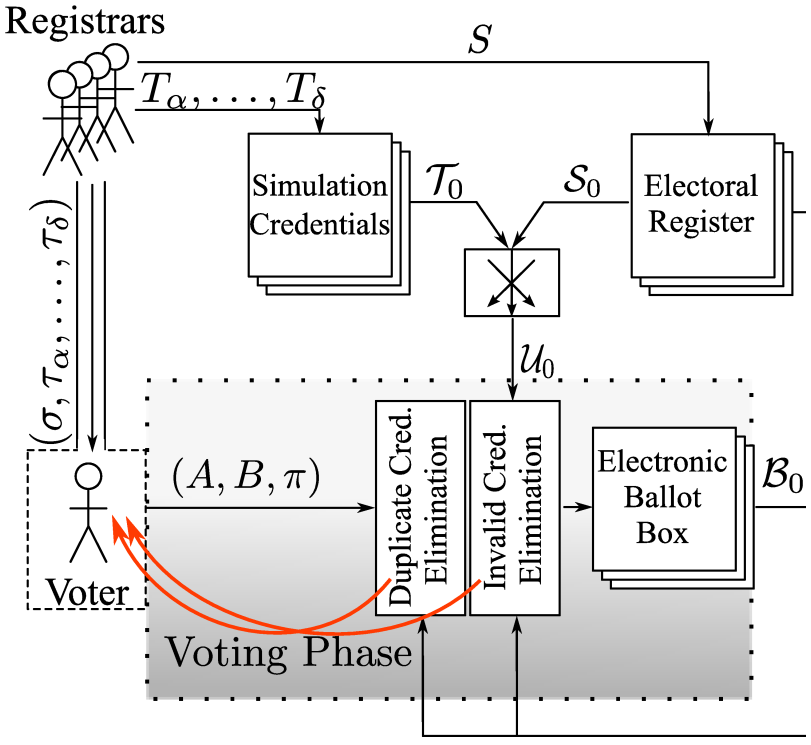
Voter casts with genuine intention

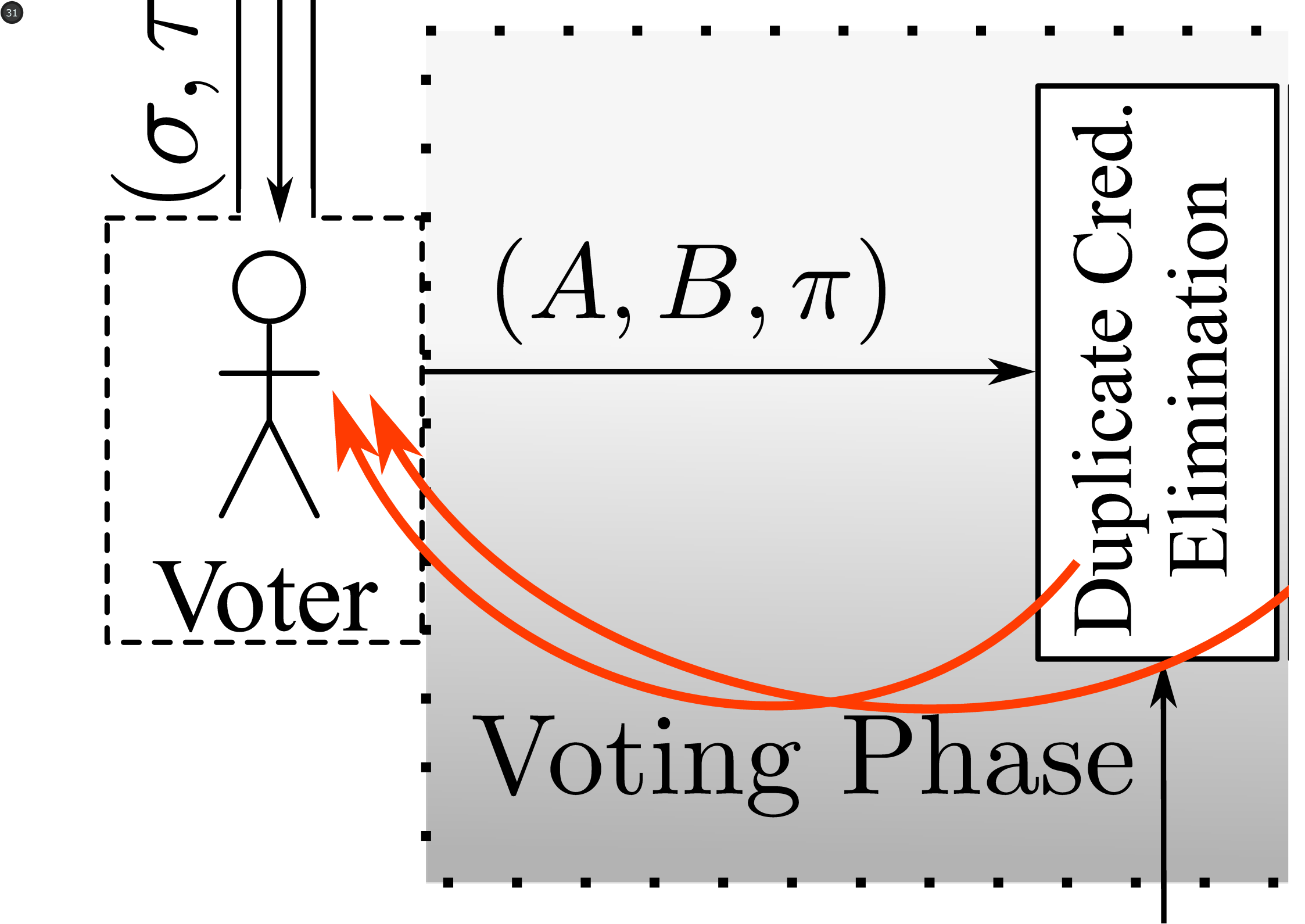
Duplicate ballot $(A_3, B, \pi)|A_3 = Enc_y(\sigma_a, r_3)$

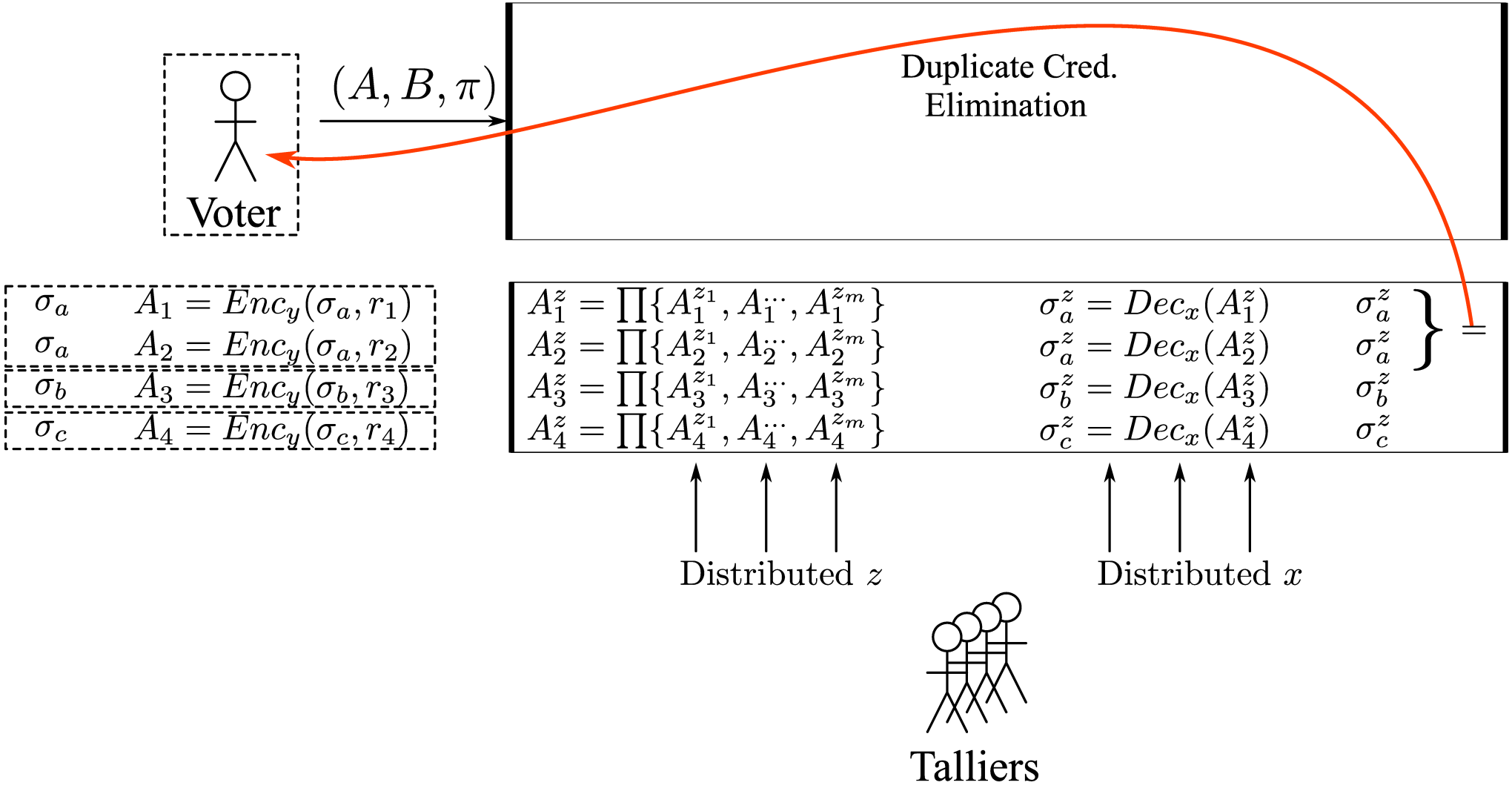
Unintended voter error

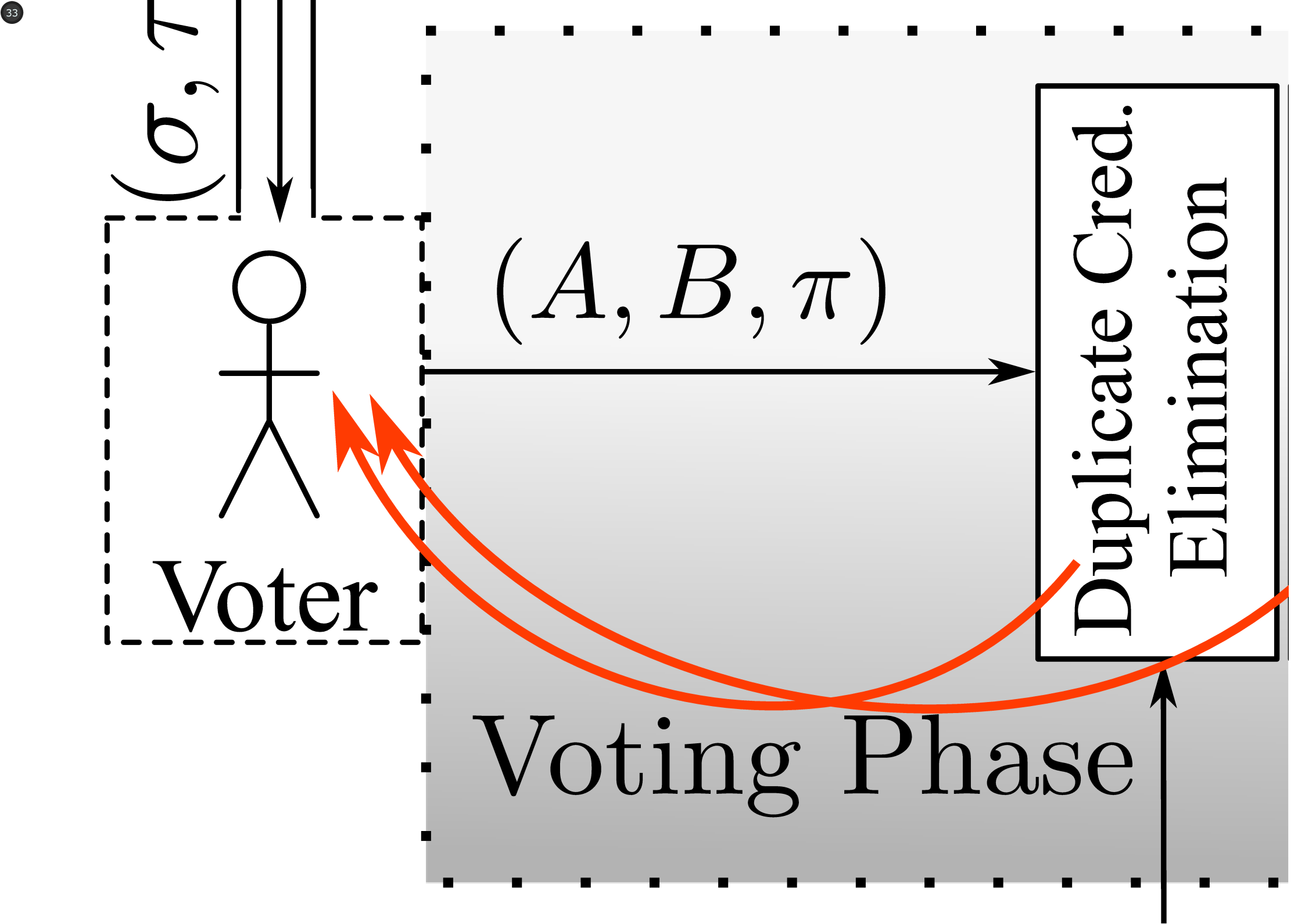
Credential stolen -> Attack

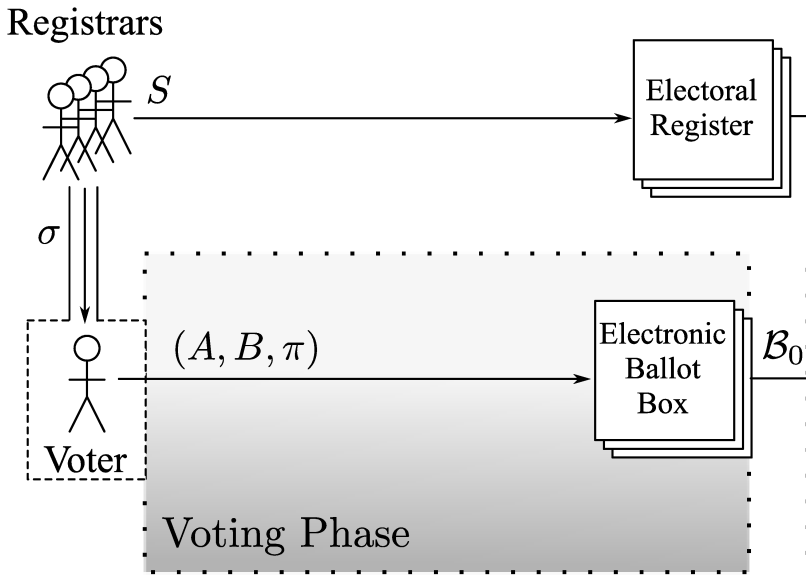

Registrars
S
Electoral Register
σ
(A, B, π)
Electronic Ballot Box
$\mathcal{B}_0$
Voter
Voting Phase

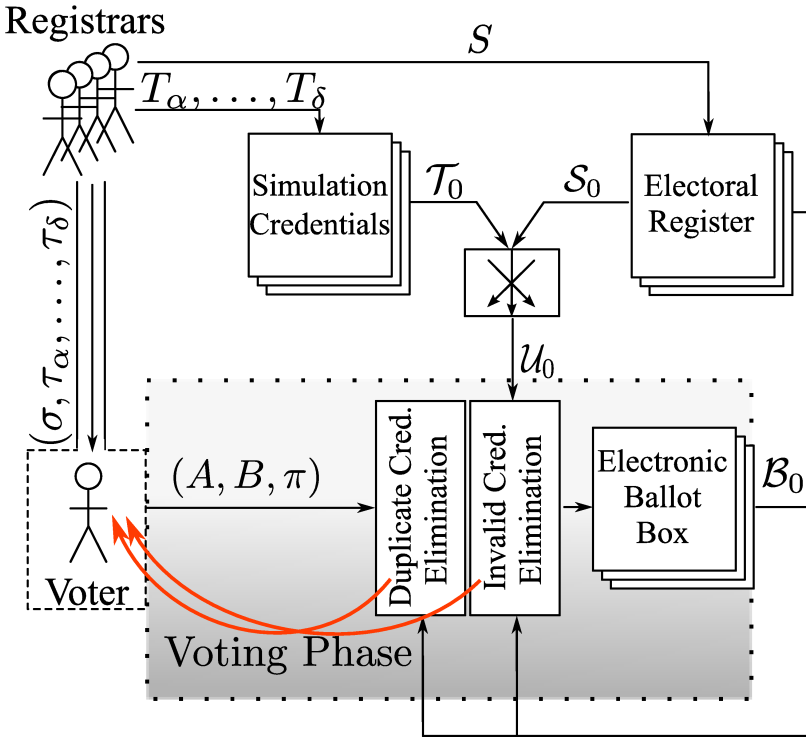

Registrars
S
$T_\alpha, \ldots, T_\delta$
Simulation Credentials
$\mathcal{T}_0$
$\mathcal{S}_0$
Electoral Register
$\mathcal{U}_0$
$(\sigma, \tau_\alpha, \ldots, \tau_\delta)$
(A, B, π)
Duplicate Cred. Elimination
Invalid Cred. Elimination
Electronic Ballot Box
$\mathcal{B}_0$
Voter
Voting Phase


$(\sigma, \tau$
(A, B, π)
Voter
Duplicate Cred. Elimination
Voting Phase


Voter
(A, B, π)
Duplicate Cred.
Elimination
$\sigma_a \quad A_1 = Enc_y(\sigma_a, r_1)$
$\sigma_a \quad A_2 = Enc_y(\sigma_a, r_2)$
$\sigma_b \quad A_3 = Enc_y(\sigma_b, r_3)$
$\sigma_c \quad A_4 = Enc_y(\sigma_c, r_4)$
$A_1^z = \prod\{A_1^{z_1}, A_1^{\cdots}, A_1^{z_m}\} \quad \sigma_a^z = Dec_x(A_1^z) \quad \sigma_a^z$
$A_2^z = \prod\{A_2^{z_1}, A_2^{\cdots}, A_2^{z_m}\} \quad \sigma_a^z = Dec_x(A_2^z) \quad \sigma_a^z$
$A_3^z = \prod\{A_3^{z_1}, A_3^{\cdots}, A_3^{z_m}\} \quad \sigma_b^z = Dec_x(A_3^z) \quad \sigma_b^z$
$A_4^z = \prod\{A_4^{z_1}, A_4^{\cdots}, A_4^{z_m}\} \quad \sigma_c^z = Dec_x(A_4^z) \quad \sigma_c^z$
$=$
Distributed z
Distributed x
Talliers


$(\sigma, \tau$
(A, B, π)
Voter
Duplicate Cred. Elimination
Voting Phase


Registrars
S
Electoral Register
σ
(A, B, π)
Electronic Ballot Box
$\mathcal{B}_0$
Voter
Voting Phase


Registrars
S
$T_\alpha, \ldots, T_\delta$
Simulation Credentials
$\mathcal{T}_0$
$\mathcal{S}_0$
Electoral Register
$\mathcal{U}_0$
$(\sigma, \tau_\alpha, \ldots, \tau_\delta)$
(A, B, π)
Duplicate Cred. Elimination
Invalid Cred. Elimination
Electronic Ballot Box
$\mathcal{B}_0$
Voter
Voting Phase

Voter / Someone casts

Invalid ballot $(A_4, B, \pi)|A_4 = Enc_y(\chi, r_4)$

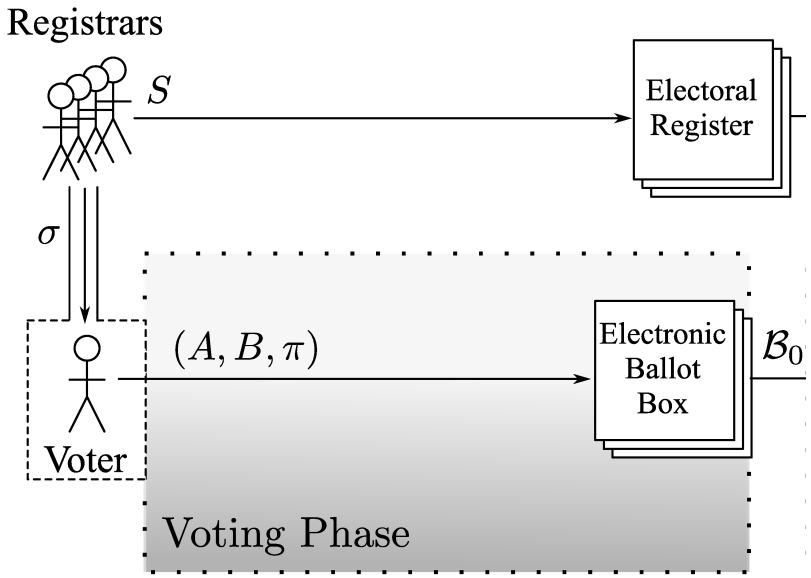
Voter / Someone casts

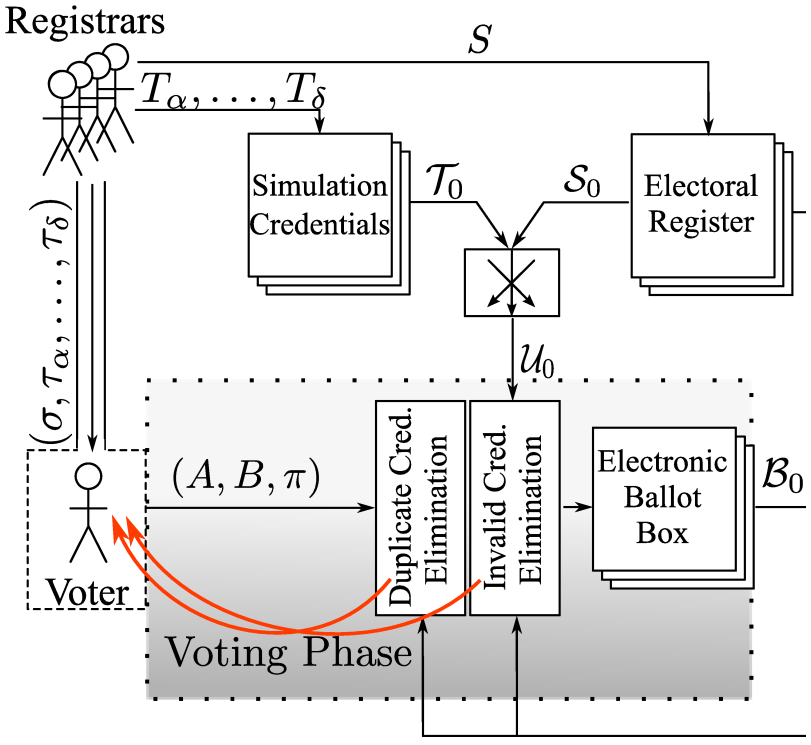
Invalid ballot $(A_4, B, \pi)|A_4 = Enc_y(\chi, r_4)$

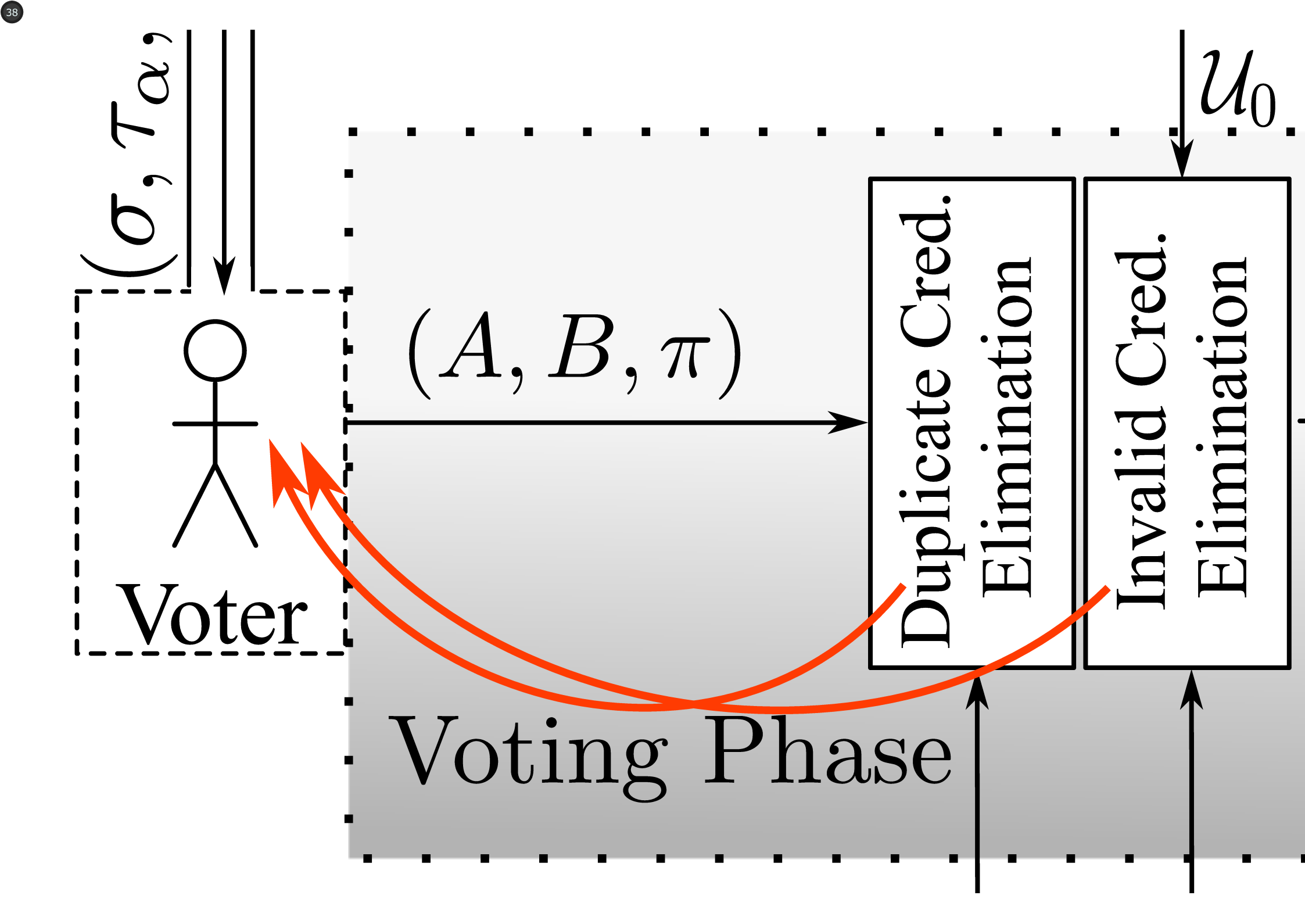
Unintended voter error

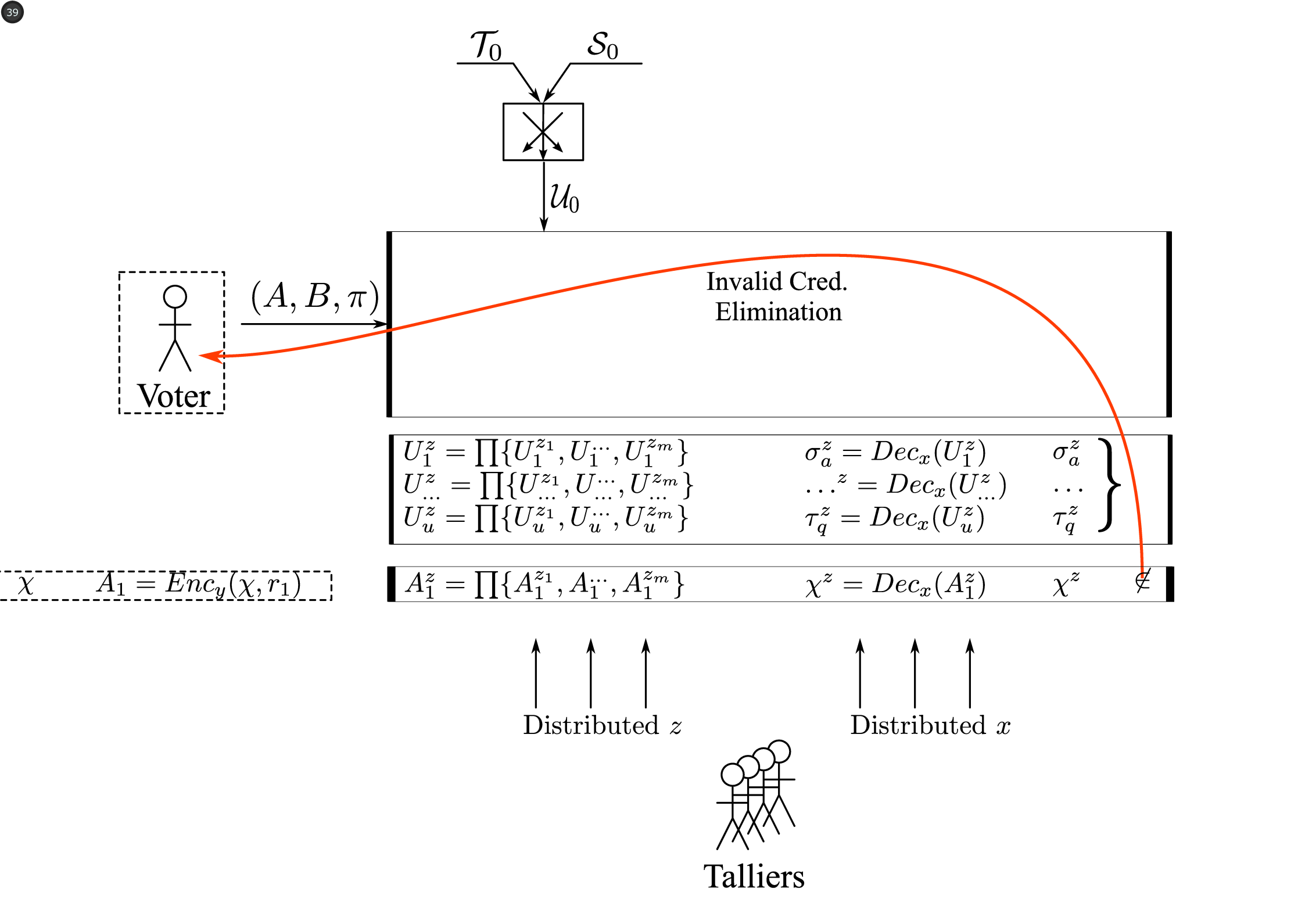
Voter cannot remember

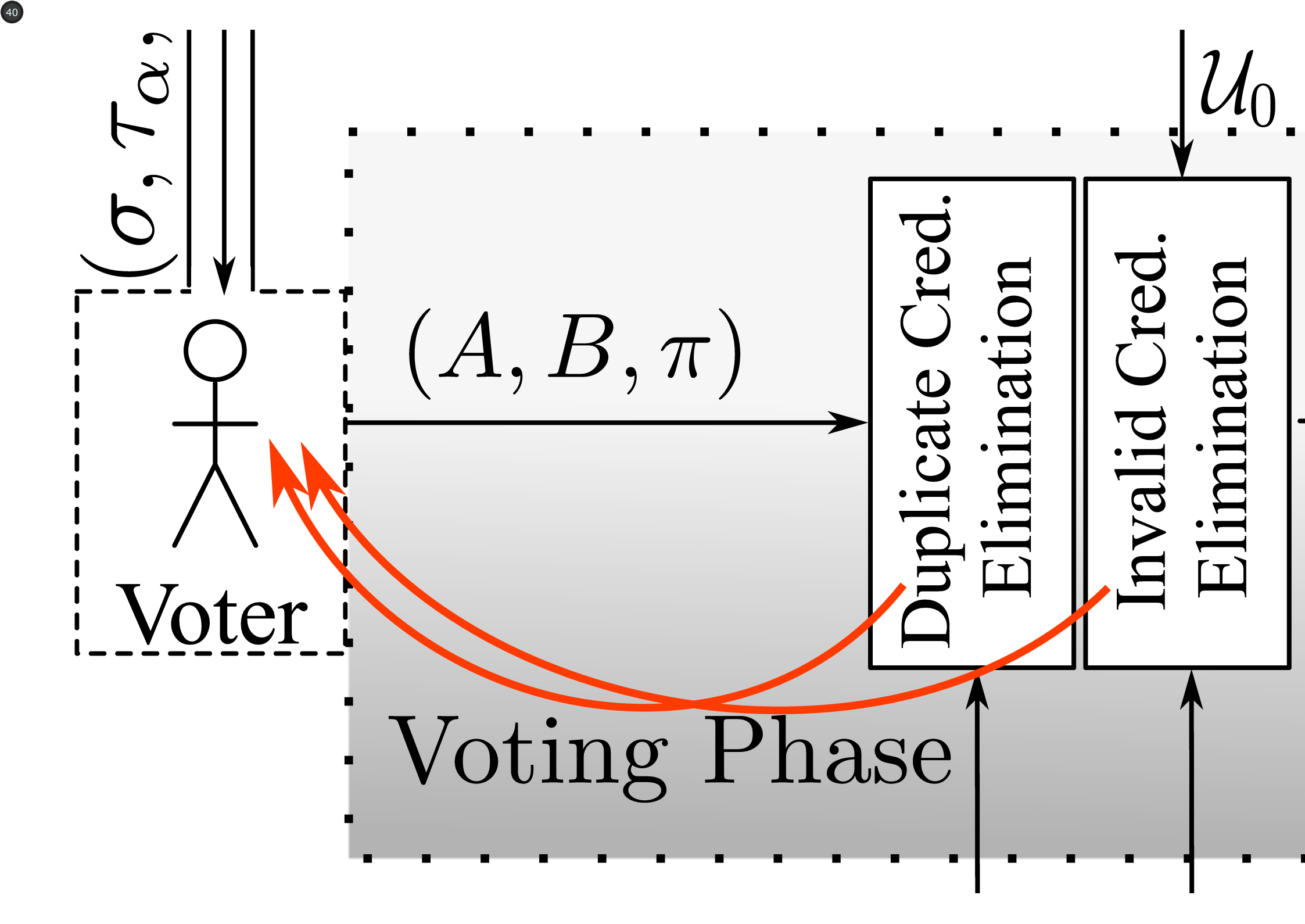
Board Flooding -> Attack

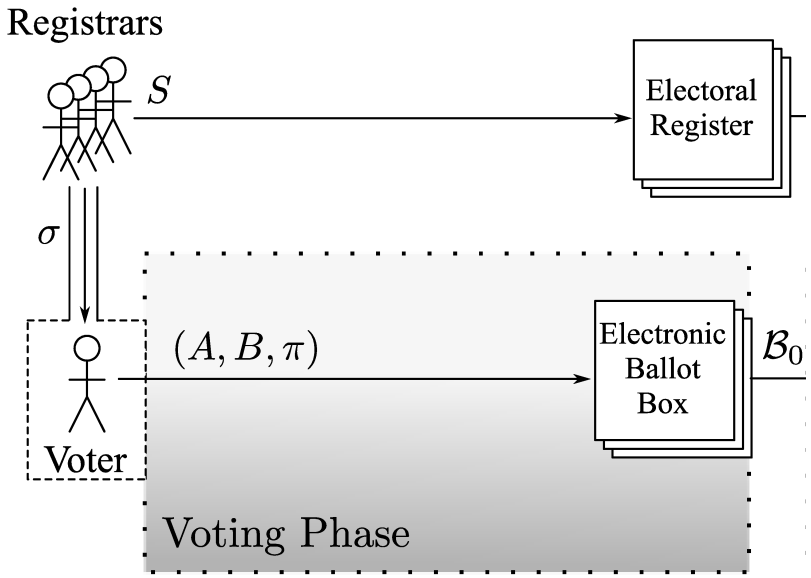

Registrars
S
Electoral Register
σ
(A, B, π)
Electronic Ballot Box
$\mathcal{B}_0$
Voter
Voting Phase

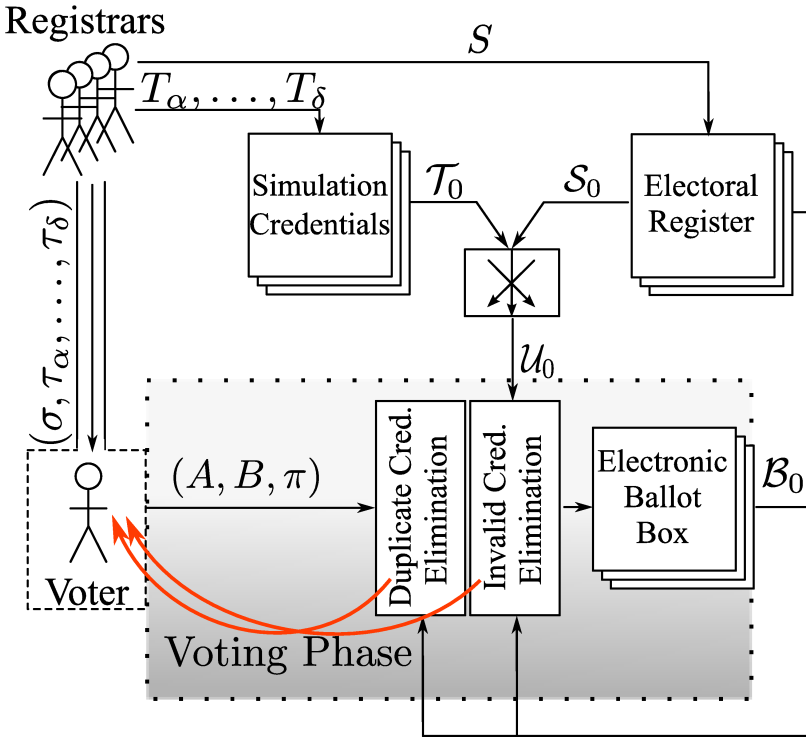

Registrars
S
$T_\alpha, \ldots, T_\delta$
Simulation Credentials
$\mathcal{T}_0$
$\mathcal{S}_0$
Electoral Register
$\mathcal{U}_0$
$(\sigma, \tau_\alpha, \ldots, \tau_\delta)$
(A, B, π)
Duplicate Cred. Elimination
Invalid Cred. Elimination
Electronic Ballot Box
$\mathcal{B}_0$
Voter
Voting Phase

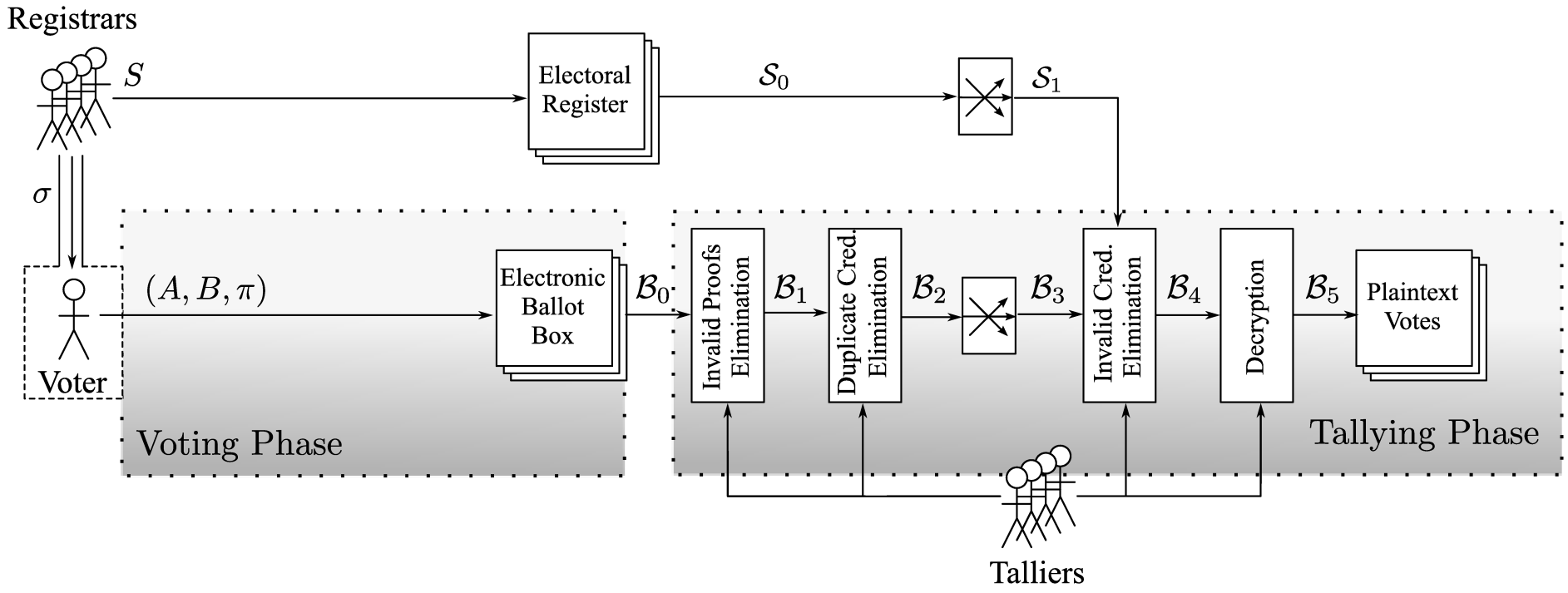

(σ, τ_α)
$\mathcal{U}_0$
(A, B, π)
Voter
Duplicate Cred. Elimination
Invalid Cred. Elimination
Voting Phase

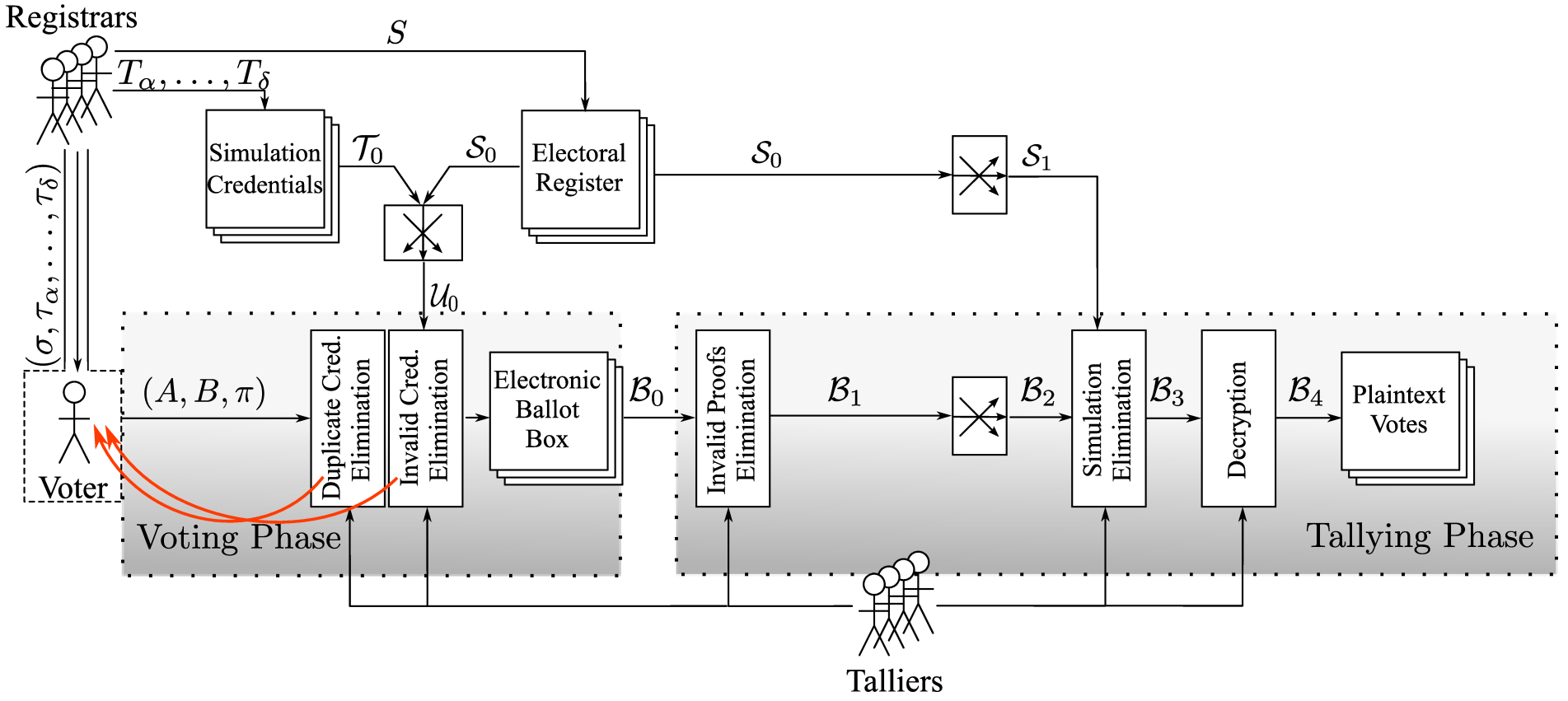

$\mathcal{T}_0$
$\mathcal{S}_0$
$\mathcal{U}_0$
Invalid Cred. Elimination
(A, B, π)
Voter
$U_1^z = \prod\{U_1^{z_1}, U_1^{\cdots}, U_1^{z_m}\}$
$U_{\cdots}^z = \prod\{U_{\cdots}^{z_1}, U_{\cdots}^{\cdots}, U_{\cdots}^{z_m}\}$
$U_u^z = \prod\{U_u^{z_1}, U_u^{\cdots}, U_u^{z_m}\}$
$\sigma_a^z = Dec_x(U_1^z)$
$\ldots^z = Dec_x(U_{\cdots}^z)$
$\tau_q^z = Dec_x(U_u^z)$
σ_a^z
$\ldots$
τ_q^z
χ
$A_1 = Enc_y(\chi, r_1)$
$A_1^z = \prod\{A_1^{z_1}, A_1^{\cdots}, A_1^{z_m}\}$
$\chi^z = Dec_x(A_1^z)$
χ^z
$\notin$
Distributed z
Distributed x
Talliers

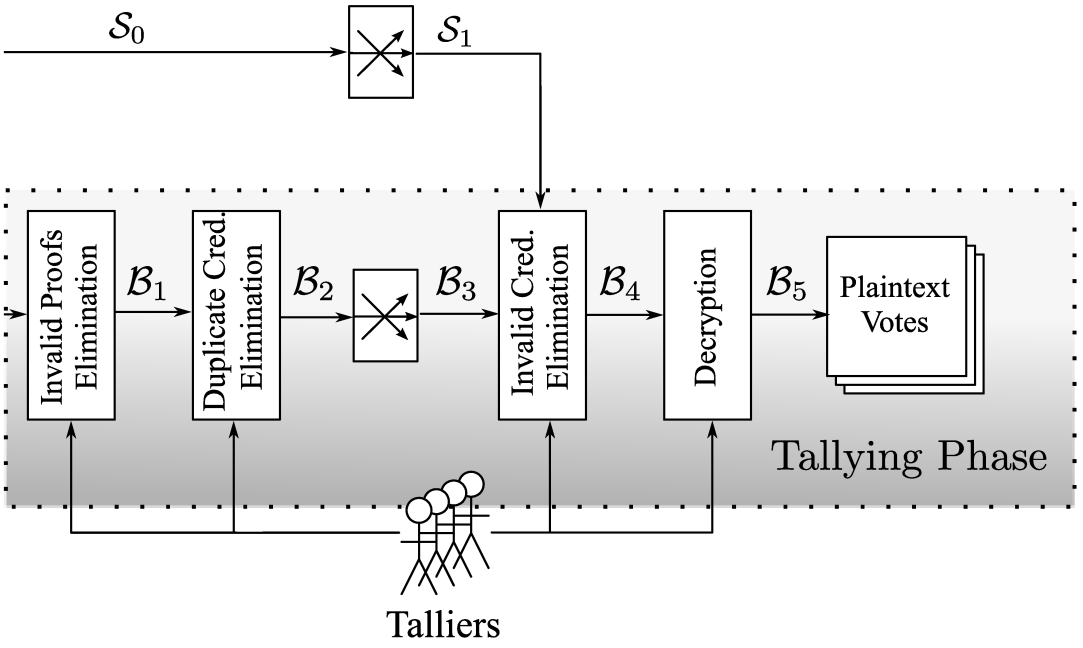

(σ, τ_α)
$\mathcal{U}_0$
(A, B, π)
Voter
Duplicate Cred. Elimination
Invalid Cred. Elimination
Voting Phase

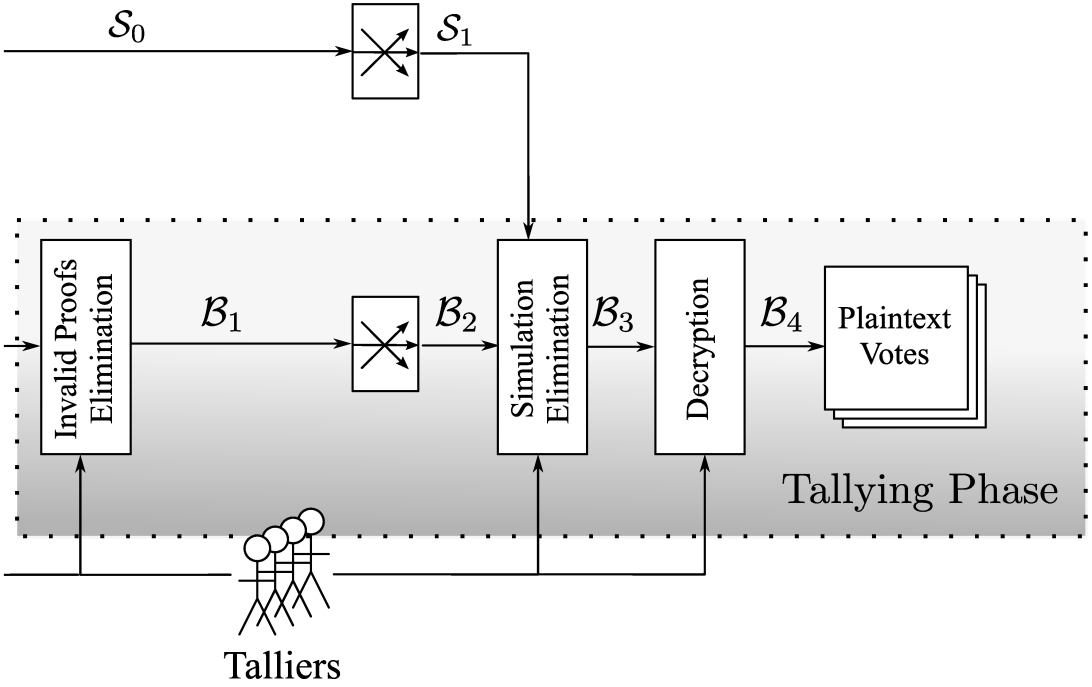

Registrars
S
Electoral Register
σ
(A, B, π)
Electronic Ballot Box
$\mathcal{B}_0$
Voter
Voting Phase


Registrars
S
$T_\alpha, \ldots, T_\delta$
Simulation Credentials
$\mathcal{T}_0$
$\mathcal{S}_0$
Electoral Register
$\mathcal{U}_0$
$(\sigma, \tau_\alpha, \ldots, \tau_\delta)$
(A, B, π)
Duplicate Cred. Elimination
Invalid Cred. Elimination
Electronic Ballot Box
$\mathcal{B}_0$
Voter
Voting Phase

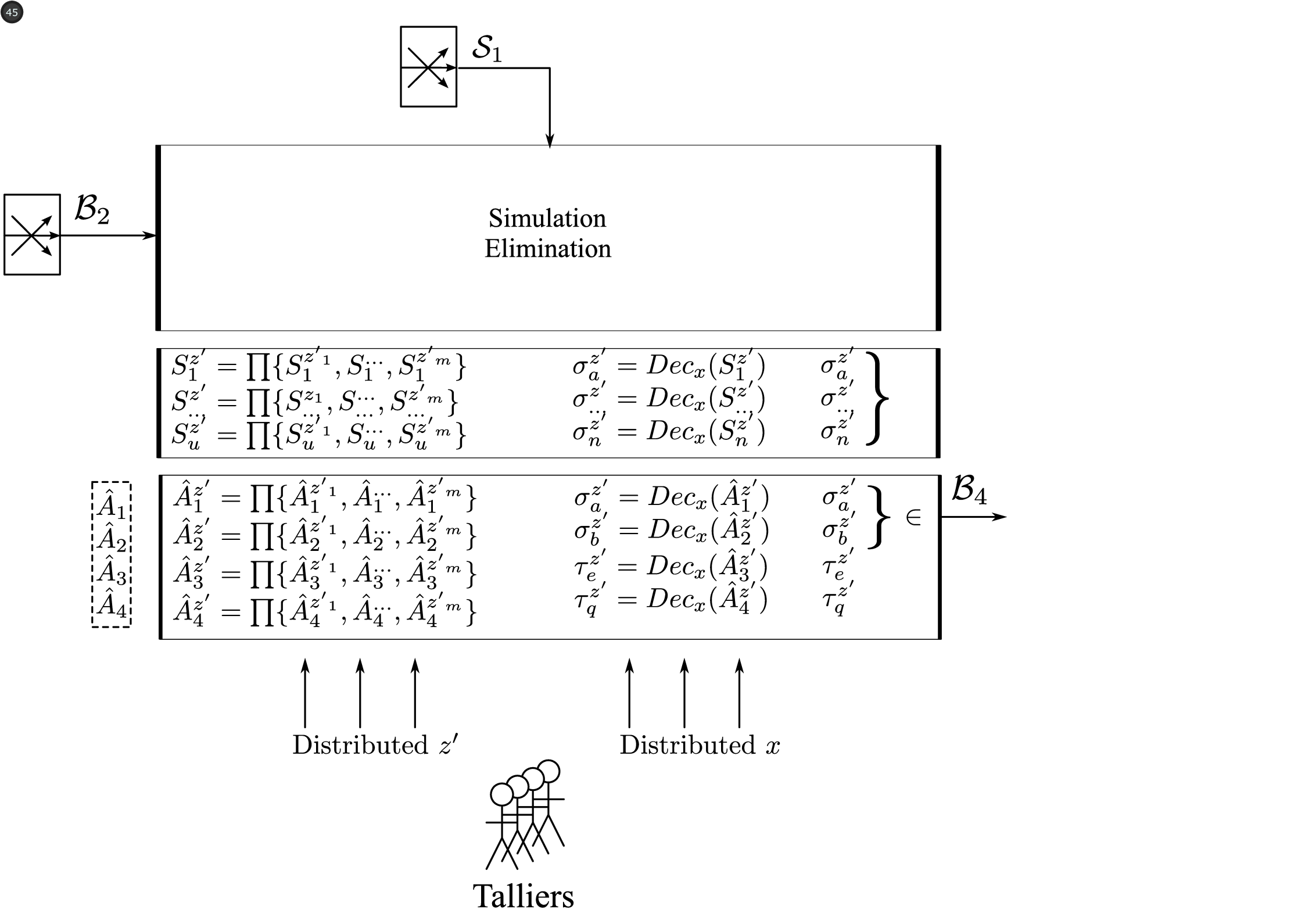

Registrars
S
Electoral Register
$\mathcal{S}_0$
$\mathcal{S}_1$
σ
(A, B, π)
Voter
Electronic Ballot Box
$\mathcal{B}_0$
Invalid Proofs Elimination
$\mathcal{B}_1$
Duplicate Cred. Elimination
$\mathcal{B}_2$
$\mathcal{B}_3$
Invalid Cred. Elimination
$\mathcal{B}_4$
Decryption
$\mathcal{B}_5$
Plaintext Votes
Voting Phase
Tallying Phase
Talliers


Registrars
S
$T_\alpha, \ldots, T_\delta$
Simulation Credentials
$\mathcal{T}_0$
$\mathcal{S}_0$
Electoral Register
$\mathcal{S}_0$
$\mathcal{S}_1$
$\mathcal{U}_0$
$(\sigma, \tau_\alpha, \ldots, \tau_\delta)$
(A, B, π)
Voter
Duplicate Cred. Elimination
Invalid Cred. Elimination
Electronic Ballot Box
$\mathcal{B}_0$
Invalid Proofs Elimination
$\mathcal{B}_1$
$\mathcal{B}_2$
Simulation Elimination
$\mathcal{B}_3$
Decryption
$\mathcal{B}_4$
Plaintext Votes
Voting Phase
Tallying Phase
Talliers


$\mathcal{S}_0$
$\mathcal{S}_1$
Invalid Proofs Elimination
$\mathcal{B}_1$
Duplicate Cred. Elimination
$\mathcal{B}_2$
$\mathcal{B}_3$
Invalid Cred. Elimination
$\mathcal{B}_4$
Decryption
$\mathcal{B}_5$
Plaintext Votes
Tallying Phase
Talliers


$\mathcal{S}_0$
$\mathcal{S}_1$
Invalid Proofs Elimination
$\mathcal{B}_1$
$\mathcal{B}_2$
Simulation Elimination
$\mathcal{B}_3$
Decryption
$\mathcal{B}_4$
Plaintext Votes
Tallying Phase
Talliers

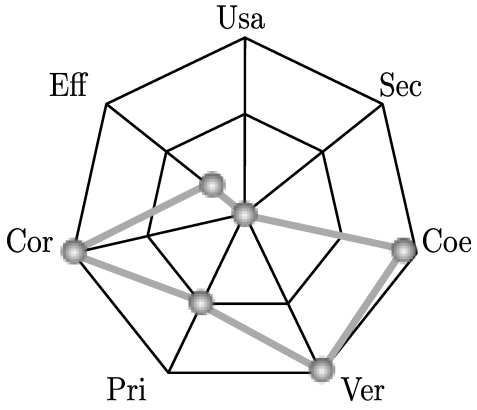
$\mathcal{S}_1$
$\mathcal{B}_2$
Simulation
Elimination
$\mathcal{B}_3$


$\mathcal{S}_1$
$\mathcal{B}_2$
Simulation
Elimination
$S_1^{z'} = \prod\{S_1^{z'1}, S_1^{\cdots}, S_1^{z'm}\}$
$S_{\cdots}^{z'} = \prod\{S_{\cdots}^{z_1}, S_{\cdots}^{\cdots}, S_{\cdots}^{z'm}\}$
$S_u^{z'} = \prod\{S_u^{z'1}, S_u^{\cdots}, S_u^{z'm}\}$
$\sigma_a^{z'} = Dec_x(S_1^{z'})$
$\sigma_{\cdots}^{z'} = Dec_x(S_{\cdots}^{z'})$
$\sigma_n^{z'} = Dec_x(S_n^{z'})$
$\sigma_a^{z'}$
$\sigma_{\cdots}^{z'}$
$\sigma_n^{z'}$
$\hat{A}_1$
$\hat{A}_2$
$\hat{A}_3$
$\hat{A}_4$
$\hat{A}_1^{z'} = \prod\{\hat{A}_1^{z'1}, \hat{A}_1^{\cdots}, \hat{A}_1^{z'm}\}$
$\hat{A}_2^{z'} = \prod\{\hat{A}_2^{z'1}, \hat{A}_2^{\cdots}, \hat{A}_2^{z'm}\}$
$\hat{A}_3^{z'} = \prod\{\hat{A}_3^{z'1}, \hat{A}_3^{\cdots}, \hat{A}_3^{z'm}\}$
$\hat{A}_4^{z'} = \prod\{\hat{A}_4^{z'1}, \hat{A}_4^{\cdots}, \hat{A}_4^{z'm}\}$
$\sigma_a^{z'} = Dec_x(\hat{A}_1^{z'})$
$\sigma_b^{z'} = Dec_x(\hat{A}_2^{z'})$
$\tau_e^{z'} = Dec_x(\hat{A}_3^{z'})$
$\tau_q^{z'} = Dec_x(\hat{A}_4^{z'})$
$\sigma_a^{z'}$
$\sigma_b^{z'}$
$\tau_e^{z'}$
$\tau_q^{z'}$
$\in$
$\mathcal{B}_4$
Distributed z'
Distributed x
Talliers

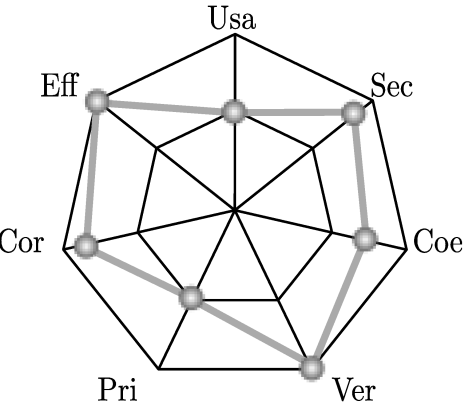
$\mathcal{S}_1$
$\mathcal{B}_2$
Simulation
Elimination
$\mathcal{B}_3$

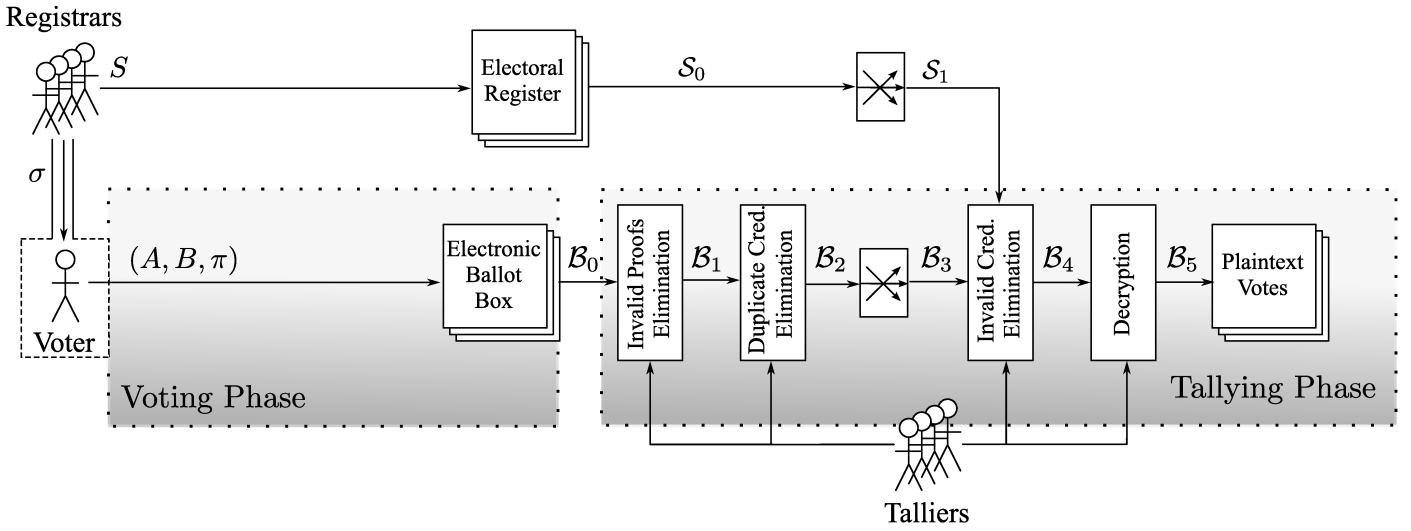
JCJ-05

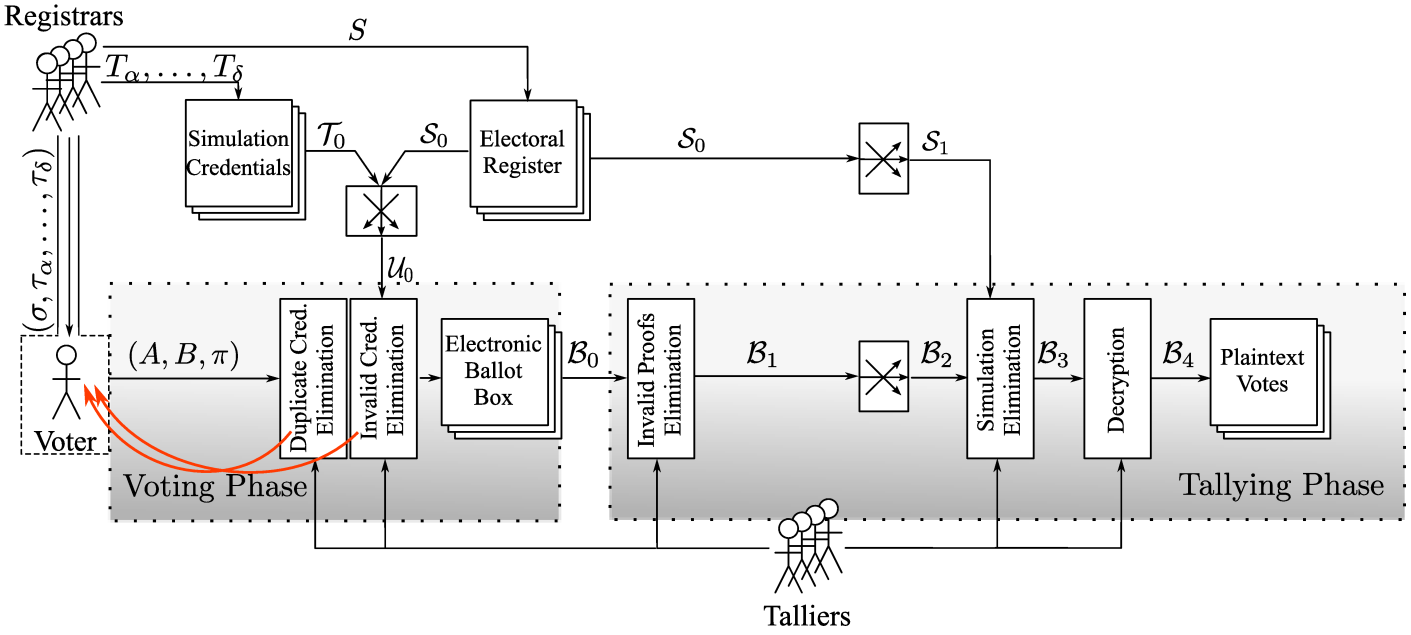
Darmstadt -> Civitas



KHF-11







E-Voting Remote (unsupervised)

Usability
How the f*ç@ does it work? What am I supposed to do here?

Efficiency
Will there ever be a result?

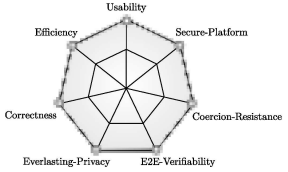
Secure-Platform
"All your data are belong to us" (sic.)

Correctness
My neighbour had the NSA vote instead?!

Coercion Resistance
We know your kid's location... vote 'yes' and all is well!

Everlasting Privacy
Your family is punished as your grandfather voted 'yes'!

E2E-Verifiability
I do not have a clue if my intention made it to the final tally?!



Berner Fachhochschule

Protocol Enhancments

Voter casts with genuine intention

Real ballot $(A_1, B, \pi)|A_1 = Enc_y(\sigma_a, r_1), B = Enc'_y(v, r'_1), \pi = zkp(r_1, r'_1 : A_1, B)$

Simulated ballot $(A_2, B, \pi)|A_2 = Enc_y(\sigma_{a_i}, r_2), B = Enc'_y(v, r'_2), \pi = zkp(r_2, r'_2 : A_2, B)$

Voter casts with genuine intention

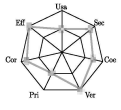
Duplicate ballot $(A_3, B, \pi)|A_3 = Enc_y(\sigma_a, r_3)$
Unintended voter error
Credential stolen -> Attack

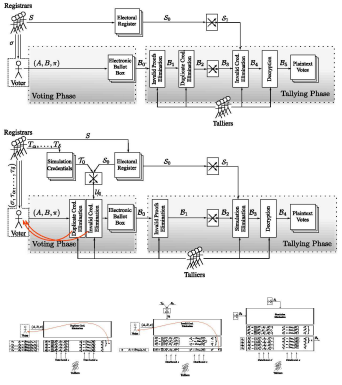
Voter / Someone casts

Invalid ballot $(A_4, B, \pi)|A_4 = Enc_y(\chi, r_4)$
Unintended voter error
Voter cannot remember
Board Flooding -> Attack

JCJ-05

KHF-11

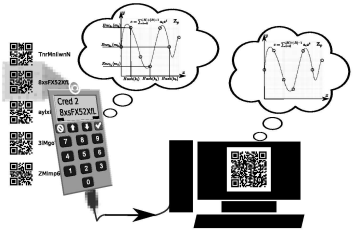




Multi Secret Management

Voter must be able to...

.... manage multiple credentials seamlessly (no search)
.... hide the true amount of credentials (chaffing)
.... having access to the credentials (non-challengeable)

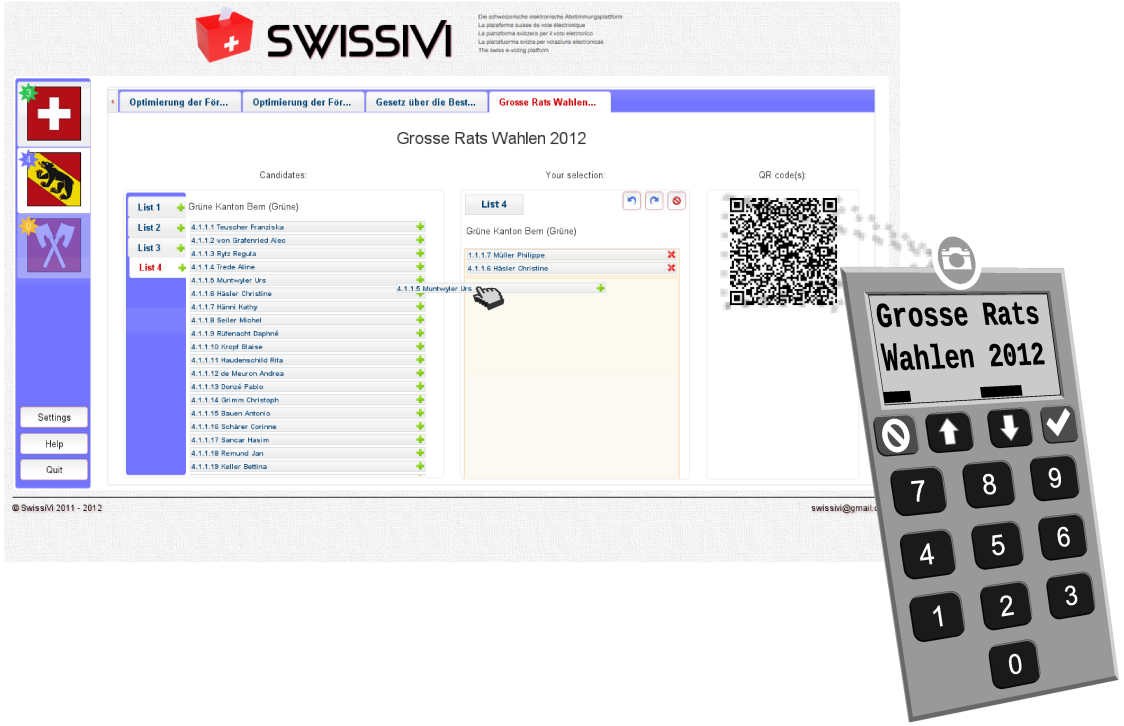


Usability Studies

Secure Platform

The Secure Platform Module must
... be restricted in its usage (finite state machine / software close)
... provide trust (analyzable down to the metal by 'experts')
... indicate tampering
... make the calculation for the cryptographic aspects
... make the calculation of the E2E-verification aspects
... provide entropy to the rest of us (not to the user)
... intuitive to use
... easily replacable (no secrets within)

Usability Studies



SWISSIVI

Die schweizerische elektronische Abstimmungsplattform
La plateforme suisse de vote électronique
La piattaforma svizzera per il voto elettronico
La plattafuorma svizra per votaziuns electronicas
The swiss e-voting platform

Bundesbeschluss üb... | Volksinitiative «Siche... | Volksinitiative «Schut...

Volksinitiative «Schutz vor Passivrauchen»

Wollen Sie die Volksinitiative «Schutz vor Passivrauchen» annehmen?

Yes | No | Uncompleted ballot

Settings
Help

SWISSIVI

Die schweizerische elektronische Abstimmungsplattform
La plateforme suisse de vote électronique
La piattaforma svizzera per il voto elettronico
La plattafuorma svizra per votaziuns electronicas
The swiss e-voting platform

Optimierung der För... | Optimierung der För... | Gesetz über die Best... | Grosse Rats Wahlen...

Grosse Rats Wahlen 2012

Candidates:

List 1 Grüne Kanton Bern (Grüne)
List 2
List 3
List 4

4.1.1.1 Teuscher Franziska
4.1.1.2 von Grafenried Alec
4.1.1.3 Rytz Regula
4.1.1.4 Trede Aline
4.1.1.5 Muntwyler Urs
4.1.1.6 Häsler Christine
4.1.1.7 Hänni Kathy
4.1.1.8 Seiler Michel
4.1.1.9 Rüfenacht Daphné
4.1.1.10 Kropf Blaise
4.1.1.11 Haudenschild Rita
4.1.1.12 de Meuron Andrea
4.1.1.13 Donzé Pablo
4.1.1.14 Grimm Christoph
4.1.1.15 Bauen Antonio
4.1.1.16 Schärer Corinne
4.1.1.17 Sancar Hasim
4.1.1.18 Remund Jan
4.1.1.19 Keller Bettina

Your selection:

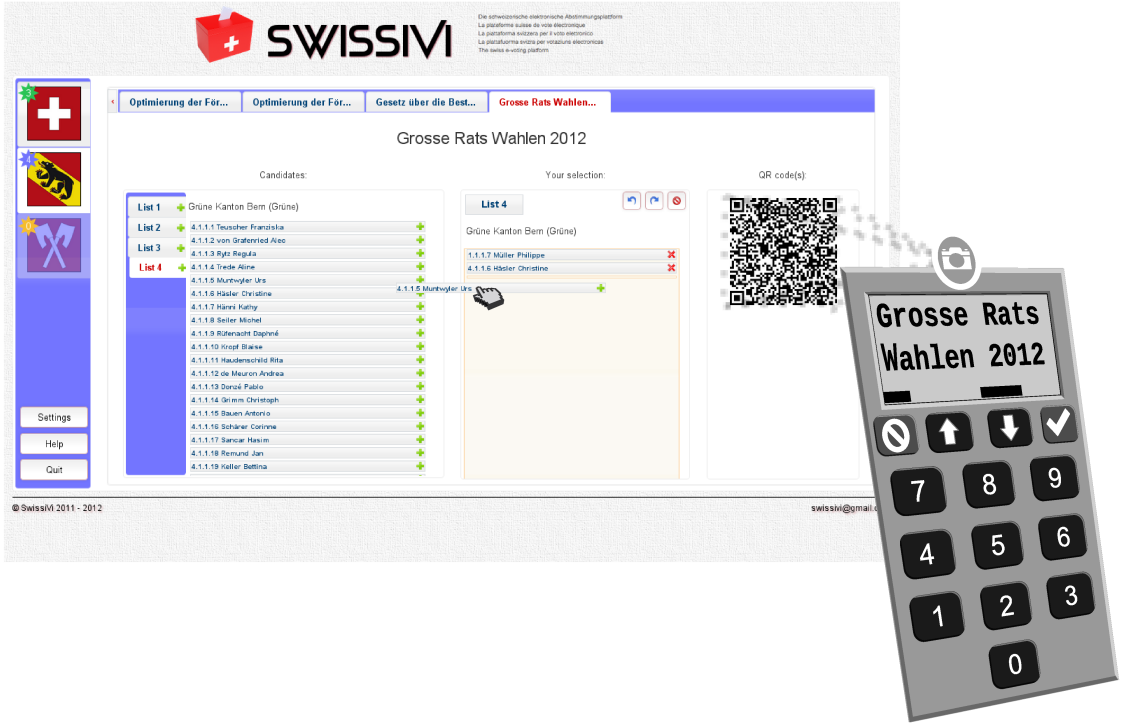
List 4
Grüne Kanton Bern (Grüne)
1.1.1.7 Müller Philippe
4.1.1.6 Häsler Christine
4.1.1.5 Muntwyler Urs

QR code(s):

Settings
Help
Quit

swissivi@gmail.c

Usability Studies



E-Voting Remote (unsupervised)

Usability
How the f*ç@ does it work? What am I supposed to do here?

Efficiency
Will there ever be a result?

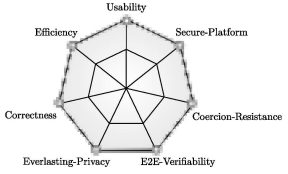
Secure-Platform
"All your data are belong to us" (sic.)

Correctness
My neighbour had the NSA vote instead?!

Coercion Resistance
We know your kid's location... vote 'yes' and all is well!

Everlasting Privacy
Your family is punished as your grandfather voted 'yes'!

E2E-Verifiability
I do not have a clue if my intention made it to the final tally?!



Berner Fachhochschule

Protocol Enhancments

Voter casts with genuine intention

Real ballot $(A_1, B, \pi)|A_1 = Enc_q(\sigma_a, r_1), B = Enc'_q(v, r'_1), \pi = zkp(r_1, r'_1 : A_1, B)$

Simulated ballot $(A_2, B, \pi)|A_2 = Enc_q(\sigma_a, r_2), B = Enc'_q(v, r'_2), \pi = zkp(r_2, r'_2 : A_2, B)$

Voter casts with genuine intention

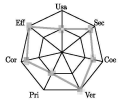
Duplicate ballot $(A_3, B, \pi)|A_3 = Enc_q(\sigma_a, r_3)$
Unintended voter error
Credential stolen -> Attack

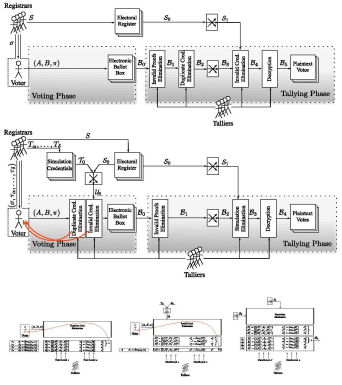
Voter / Someone casts

Invalid ballot $(A_4, B, \pi)|A_4 = Enc_q(\chi, r_4)$
Unintended voter error
Voter cannot remember
Board Flooding -> Attack

JCJ-05

KHF-11

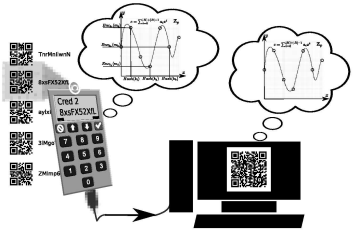




Multi Secret Management

Voter must be able to...

.... manage multiple credentials seamlessly (no search)
.... hide the true amount of credentials (chaffing)
.... having access to the credentials (non-challengeable)



Usability Studies

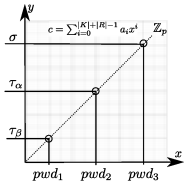
Secure Platform

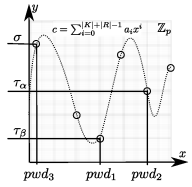
The Secure Platform Module must
... be restricted in its usage (finite state machine / software close)
... provide trust (analyzable down to the metal by 'experts')
... indicate tampering
... make the calculation for the cryptographic aspects
... make the calculation of the E2E-verification aspects
... provide entropy to the rest of us (not to the user)
... intuitive to use
... easily replacable (no secrets within)

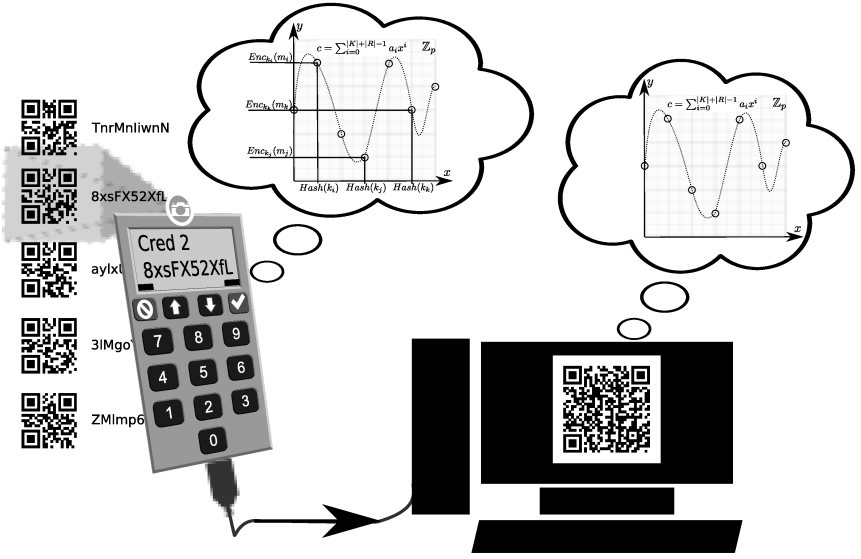
Multi Secret Management

Voter must be able to...

.... manage multiple credentials seamlessly (no search)
.... hide the true amount of credentials (chaffing)
.... having access to the credentials (non-challengeable)



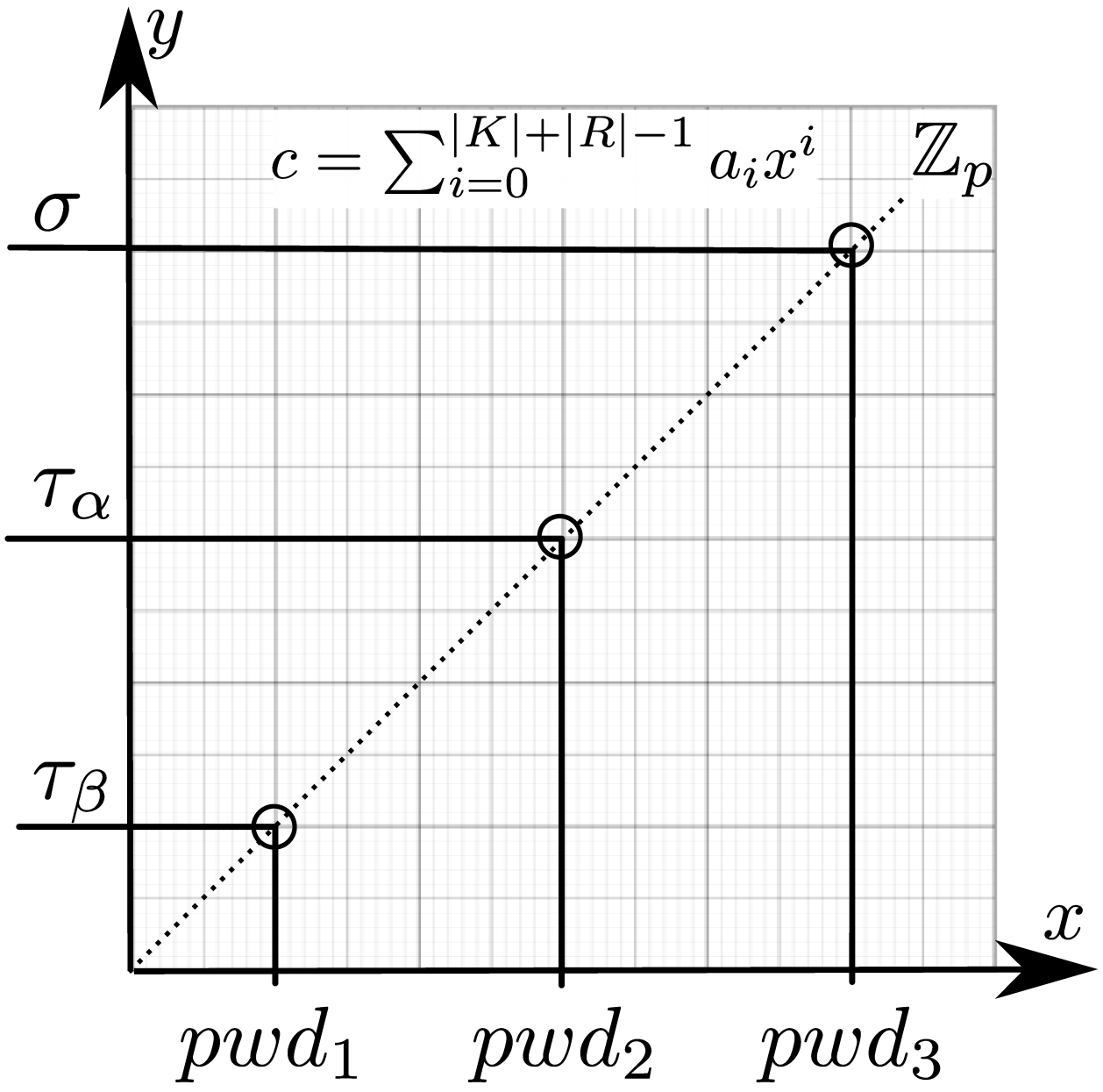


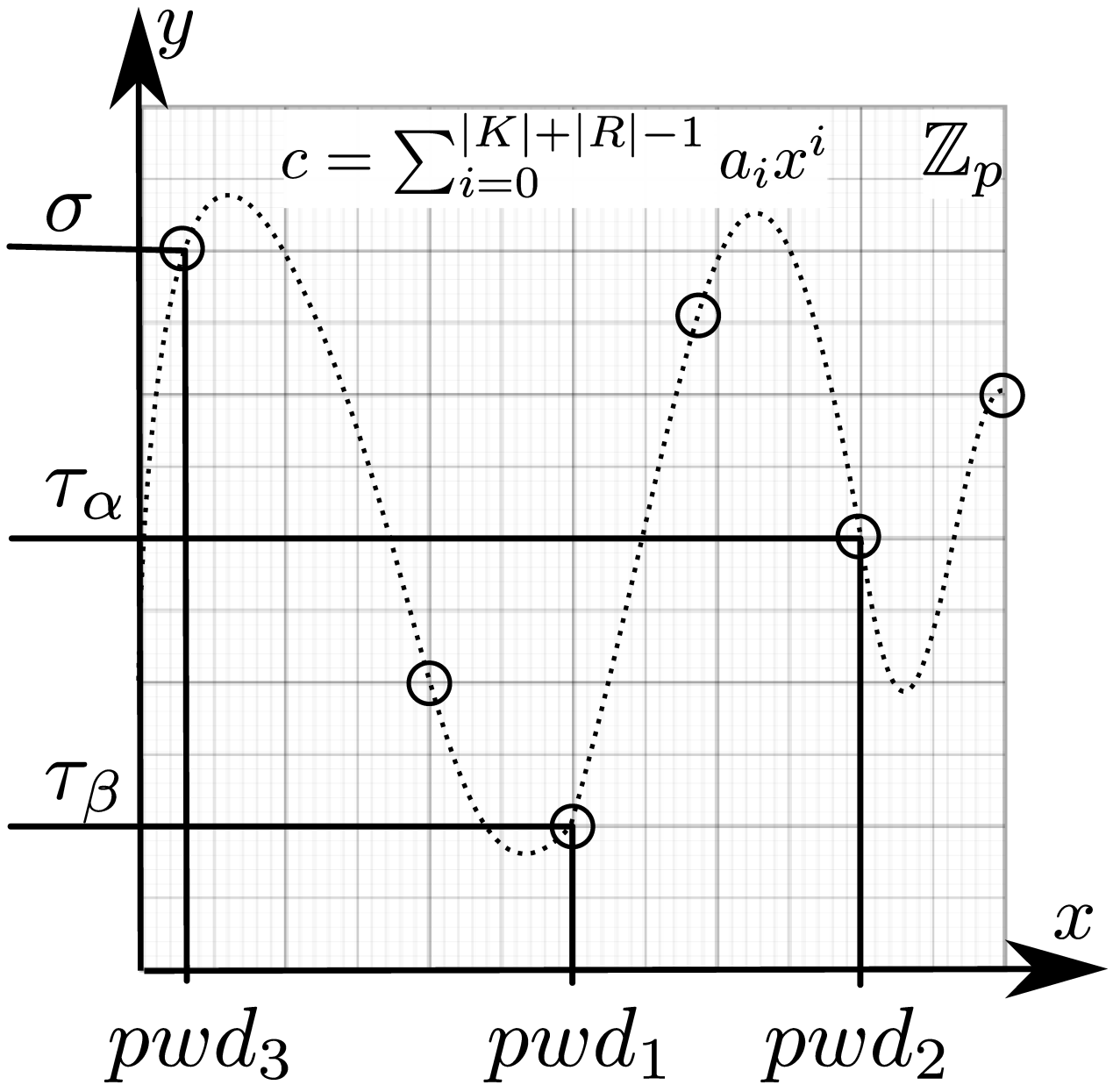


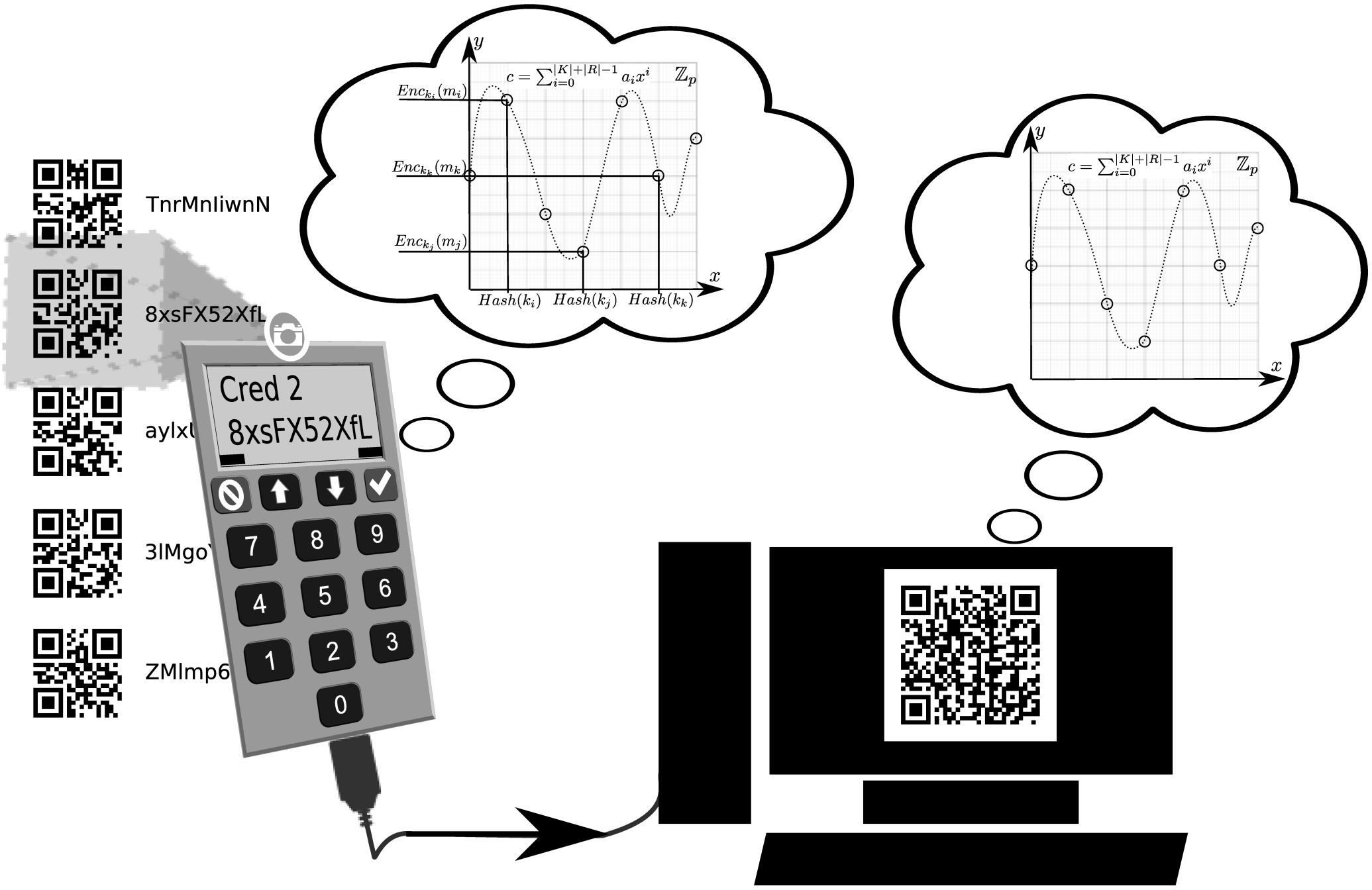
Multi Secret Management

Voter must be able to...

.... manage multiple credentials seamlessly (no search)
.... hide the true amount of credentials (chaffing)
.... having access to the credentials (non-challengeable)


y
$c = \sum_{i=0}^{|K|+|R|-1} a_i x^i$
$\mathbb{Z}_p$
σ
τ_α
τ_β
x
pwd_1
pwd_2
pwd_3

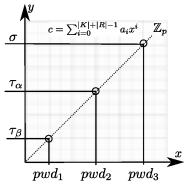

y
$c = \sum_{i=0}^{|K|+|R|-1} a_i x^i$
$\mathbb{Z}_p$
σ
τ_α
τ_β
x
pwd_3
pwd_1
pwd_2

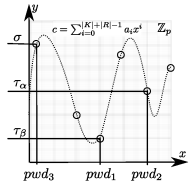

TnrMnIiwnN
8xsFX52XfL
aylxU
3lMgoY
ZMlmp6
Cred 2
8xsFX52XfL
7
8
9
4
5
6
1
2
3
0
$c = \sum_{i=0}^{|K|+|R|-1} a_i x^i$
$\mathbb{Z}_p$
$Enc_{k_i}(m_i)$
$Enc_{k_k}(m_k)$
$Enc_{k_j}(m_j)$
$Hash(k_i)$
$Hash(k_j)$
$Hash(k_k)$
x
y

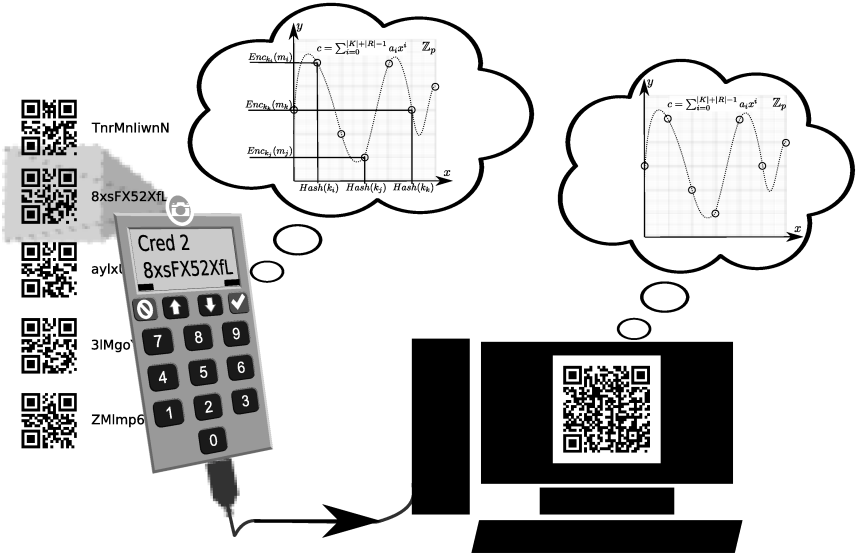
Multi Secret Management

Voter must be able to...

.... manage multiple credentials seamlessly (no search)
.... hide the true amount of credentials (chaffing)
.... having access to the credentials (non-challengeable)







E-Voting Remote (unsupervised)

Usability
How the f*ç@ does it work? What am I supposed to do here?

Efficiency
Will there ever be a result?

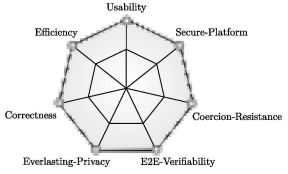
Secure-Platform
"All your data are belong to us" (sic.)

Correctness
My neighbour had the NSA vote instead?!

Coercion Resistance
We know your kid's location... vote 'yes' and all is well!

Everlasting Privacy
Your family is punished as your grandfather voted 'yes'!

E2E-Verifiability
I do not have a clue if my intention made it to the final tally?!



Berner Fachhochschule

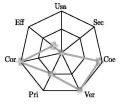
Protocol Enhancments

Voter casts with genuine intention
Real ballot $(A_1, B, \pi)|A_1 = Enc_y(\sigma_a, r_1), B = Enc'_y(v, r'_1), \pi = zkp(r_1, r'_1 : A_1, B)$
Simulated ballot $(A_2, B, \pi)|A_2 = Enc_y(\sigma_{a_i}, r_2), B = Enc'_y(v, r'_2), \pi = zkp(r_2, r'_2 : A_2, B)$

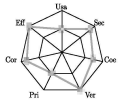
Voter casts with genuine intention
Duplicate ballot $(A_3, B, \pi)|A_3 = Enc_y(\sigma_a, r_3)$
Unintended voter error
Credential stolen -> Attack

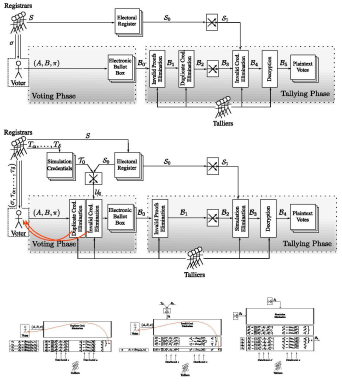
Voter / Someone casts
Invalid ballot $(A_4, B, \pi)|A_4 = Enc_y(\chi, r_4)$
Unintended voter error
Voter cannot remember
Board Flooding -> Attack

JCJ-05
Damstadt -> Civitas



KHF-11

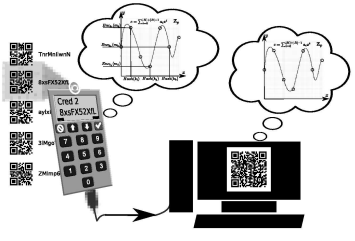




Multi Secret Management

Voter must be able to...

.... manage multiple credentials seamlessly (no search)
.... hide the true amount of credentials (chaffing)
.... having access to the credentials (non-challengeable)



Usability Studies

Secure Platform

The Secure Platform Module must
... be restricted in its usage (finite state machine / software close)
... provide trust (analyzable down to the metal by 'experts')
... indicate tampering
... make the calculation for the cryptographic aspects
... make the calculation of the E2E-verification aspects
... provide entropy to the rest of us (not to the user)
... intuitive to use
... easily replacable (no secrets within)

Secure Platform

The Secure Platform Module must
... be restricted in its usage (finite state machine / software close)
... provide trust (analyzable down to the metal by 'experts')
... indicate tampering
... make the calculation for the cryptographic aspects
... make the calculation of the E2E-verification aspects
... provide entropy to the rest of us (not to the user)
... intuitive to use
... easily replacable (no secrets within)

Secure Platform

The Secure Platform Module must
... be restricted in its usage (finite state machine / software close)
... provide trust (analyzable down to the metal by 'experts')
... indicate tampering
... make the calculation for the cryptographic aspects
... make the calculation of the E2E-verification aspects
... provide entropy to the rest of us (not to the user)
... intuitive to use
... easily replacable (no secrets within)

Secure Platform

The Secure Platform Module must
... be restricted in its usage (finite state machine / software close)
... provide trust (analyzable down to the metal by 'experts')
... indicate tampering
... make the calculation for the cryptographic aspects
... make the calculation of the E2E-verification aspects
... provide entropy to the rest of us (not to the user)
... intuitive to use
... easily replacable (no secrets within)

Secure Platform

The Secure Platform Module must
... be restricted in its usage (finite state machine / software close)
... provide trust (analyzable down to the metal by 'experts')
... indicate tampering
... make the calculation for the cryptographic aspects
... make the calculation of the E2E-verification aspects
... provide entropy to the rest of us (not to the user)
... intuitive to use
... easily replacable (no secrets within)

E-Voting Remote (unsupervised)

Usability
How the f*ç@ does it work? What am I supposed to do here?

Efficiency
Will there ever be a result?

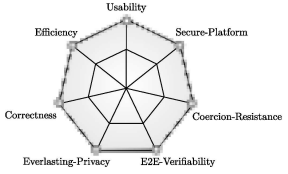
Secure-Platform
"All your data are belong to us" (sic.)

Correctness
My neighbour had the NSA vote instead?!

Coercion Resistance
We know your kid's location... vote 'yes' and all is well!

Everlasting Privacy
Your family is punished as your grandfather voted 'yes'!

E2E-Verifiability
I do not have a clue if my intention made it to the final tally?!



Berner Fachhochschule

Protocol Enhancments

Voter casts with genuine intention

Real ballot $(A_1, B, \pi)|A_1 = Enc_y(\sigma_a, r_1), B = Enc'_y(v, r'_1), \pi = zkp(r_1, r'_1 : A_1, B)$

Simulated ballot $(A_2, B, \pi)|A_2 = Enc_y(\sigma_{a_i}, r_2), B = Enc'_y(v, r'_2), \pi = zkp(r_2, r'_2 : A_2, B)$

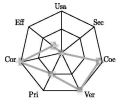
Voter casts with genuine intention

Duplicate ballot $(A_3, B, \pi)|A_3 = Enc_y(\sigma_a, r_3)$
Unintended voter error
Credential stolen -> Attack

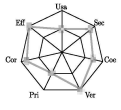
Voter / Someone casts

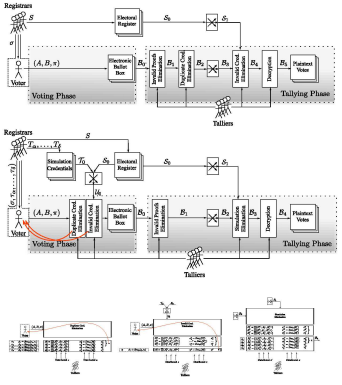
Invalid ballot $(A_4, B, \pi)|A_4 = Enc_y(\chi, r_4)$
Unintended voter error
Voter cannot remember
Board Flooding -> Attack

JCJ-05



KHF-11

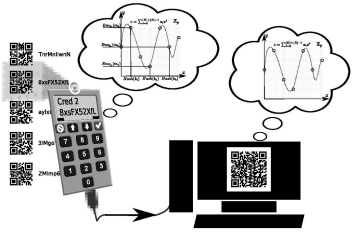




Multi Secret Management

Voter must be able to...

.... manage multiple credentials seamlessly (no search)
.... hide the true amount of credentials (chaffing)
.... having access to the credentials (non-challengeable)



Usability Studies

Secure Platform

The Secure Platform Module must
... be restricted in its usage (finite state machine / software close)
... provide trust (analyzable down to the metal by 'experts')
... indicate tampering
... make the calculation for the cryptographic aspects
... make the calculation of the E2E-verification aspects
... provide entropy to the rest of us (not to the user)
... intuitive to use
... easily replacable (no secrets within)