Testkatalog

Aus all den zu prüfenden Daten galt es nun einen Testkatalog zu erstellen. Dieser ist in fünf Kategorien unterteilt, welche später im Detail erklärt werden. Das Endergebnis des Verifiers ist also die Summe aus allen fünf Ergebnissen der jeweiligen Kategorie.

Später in der Bachelor-Thesis muss ersichtlich sein. Welcher Test welchem Programm Code entspricht. Aus diesem Grund wurde jedem Test eine Eindeutige Nummer zugewiesen. Damit man diese Später im Programm Code verwenden kann.

Wie auch schon beim Bulletin Board wurden die Test auch hier teilweise den 3 Phasen der Spezifikation zugewiesen. Diese ermöglicht eine bessere Übersicht über die Tests.

Um die Integritäts- und Konsistenz Tests durchführen zu können, müssen noch folgende Parameter definiert werden.

- $\omega = max(\mathbf{w})$
- $t = |\mathbf{n}|$
- $N_E = |\mathbf{v}|$
- $s = |\hat{\boldsymbol{D}}|$
- $n = \sum_{j=1}^{t} n_j$
- $N = |\mathbf{e}_1|$
- $k = \sum_{j=1}^{t} k_j$

1 Vollständigkeit

In diesem Teil wird überprüft, ob alle erforderlichen Daten vorhanden sind. Denn nur so kann man eine lückenlose Verifizierung gewährleisten. Es werden hier also einfach nochmal alle Daten aufgeführt. Jeder Test überprüft ob ein Parameter vorhanden ist oder nicht. Der Output ist also entweder wahr oder falsch.

1.1 Vor der Wahl

1.1.1 Check for election identifier U

1.1.2 Check for vector of number of candidates in each election $\mathbf{n}$

1.1.3 Check for vector of candidate description $\mathbf{c}$

1.1.4 Check for vector of number of selection in each election $\mathbf{k}$

1.1.5 Check for vector of voter description $\mathbf{v}$

1.1.6 Check for vector of assigned counting circles $\mathbf{w}$

1.1.7 Check for eligibility matrix $\mathbf{E}$

1.1.8 Check for vector of public voter credentials $\hat{\mathbf{D}}$

1.1.9 Check for vector of public keys of Authorities $\mathbf{pk}$

1.1.10 Check for signature of full election parameters σ_1^{param}

1.1.11 Check for signature of part of election parameters σ_2^{param}

1.1.12 Check for signature of other part of election parameters σ_3^{param}

1.1.13 Check for vector of signature of public credentials $\mathbf{s}_{prep}$

1.1.14 Check for vector of signature of public keys $\mathbf{s}_{kgen}$

1.2 Während der Wahl

1.2.1 Check for ballot list $\langle(v, \alpha)\rangle$

1.2.2 Ballot Tests $\mathbf{A}$

1.2.2.1 For all elements check for voter ID ballot v

1.2.2.2 For all elements check ballot α

1.2.3 Check for OT-response list $\langle(v, \beta_j, \sigma_{ij}^{cast})\rangle$

1.2.4 Responses Tests $\mathbf{B}$

1.2.4.1 For all elements check for voter ID v

1.2.4.2 For all elements check for OT-response β_j

1.2.4.3 For all elements check for signature σ_{ij}^{cast}

1.2.5 Check for confirmation list $\langle(v, \gamma)\rangle$

1.2.6 Confirmation Tests $\mathbf{C}$

1.2.6.1 For all elements check for voter ID v

1.2.6.2 For all elements check for confirmation γ

1.2.7 Check for finalization list $\langle(v, \delta_j, \sigma_{ij}^{cast})\rangle$

1.2.8 Finalization Tests $\mathbf{D}$

1.2.8.1 For all elements check for voter ID v

1.2.8.2 For all elements check for finalization δ_j

1.2.8.3 For all elements check for signature σ_{ij}^{cast}

1.3 Nach der Wahl

1.3.1 Check for mixed and re-encrypted Ballot lists $\mathbf{E}'$

1.3.2 Check for vector of Shuffle Proofs $\boldsymbol{\pi}$

1.3.3 Check for vector of partial decrypted Ballot lists $\mathbf{B}'$

1.3.4 Check for vector of decryption Proofs $\boldsymbol{\pi}'$

1.3.5 Check for election result matrix $\mathbf{V}$

1.3.6 Check for counting circle matrix $\mathbf{E}$

1.3.7 Check for signature of tallying result σ^{tally}

1.3.8 Check for vector of signatures of mixed re-encryptions $\mathbf{s}_{mix}$

1.3.9 Check for vector of signatures of partial decryption's $\mathbf{s}_{dec}$

2 Integrität

In diesem Teil wird die Integrität der Parameter geprüft. Es wird also geprüft ob die Parameter in sich schlüssig sind. Beispielweise wird geprüft ob sie sich im geforderten Wertebereich befinden. Der Output ist wieder entweder wahr oder falsch.

2.1 Vor der Wahl

2.1.1 Check if $U \in A_{\mathbf{ucs}}^*$

2.1.2 Check if $\omega \geqslant 1$

2.1.3 Check if $t \geqslant 1$

2.1.4 Check if $N_E \geqslant 0$

2.1.5 Check if $s \geqslant 1$

2.1.6 For all $j \in \{1, ..., t\}$, check if $n_j \geqslant 2$

2.1.7 For all $j \in \{1, ..., t\}$, check if $k_j \geqslant 1$

2.1.8 EligibilityMatrix Tests

2.1.8.1 For all $j \in \{1, ..., t\}$, $i \in \{1, ..., N_E\}$, check if $e_{ij} \in \mathbb{B}$

2.1.8.2 Check if $\sum_{j=1}^{t} e_{ij} \geqslant 1$

2.1.9 For all $i \in \{1, ..., n\}$, check if $C_i \in A_{\mathbf{ucs}}^*$

2.1.10 For all $i \in \{1, ..., N_E\}$, check if $V_i \in A_{\mathbf{ucs}}^*$

2.1.11 For all $i \in \{1, ..., N_E\}$, check if $\omega_i \in \{1, ..., \omega\}$

2.1.12 For all $j \in \{1, ..., s\}$, $i \in \{1, ..., N_E\}$, check if $\hat{d}_{ij} = (\hat{x}_{ij}, \hat{y}_{ij})$

2.1.13 For all $j \in \{1, ..., s\}$, check if $pk_j \in \mathbb{G}_q$

2.1.14 Check if $\sigma_1^{param} \in \mathbb{B} \times \mathbb{Z}_q$

2.1.15 Check if $\sigma_2^{param} \in \mathbb{B} \times \mathbb{Z}_q$

2.1.16 Check if $\sigma_3^{param} \in \mathbb{B} \times \mathbb{Z}_q$

2.1.17 For all $j \in \{1, ..., s\}$, check if $\sigma_j^{prep} \in \mathbb{B} \times \mathbb{Z}_q$

2.1.18 For all $j \in \{1, ..., s\}$, check if $\sigma_j^{kgen} \in \mathbb{B} \times \mathbb{Z}_q$

2.2 Während der Wahl

2.2.1 Ballot Tests $\mathbf{A}$

2.2.1.1 For all elements check if $v \in \{0, ..., N_E\}$

2.2.1.2 For all elements in α, check if $\hat{x}_v \in \mathbb{G}_{\hat{q}}$

2.2.1.3 For all elements in α, check if $a_j = (a_{j,1}, a_{j,2}) \in \mathbb{G}_q^2$

2.2.1.4 For all elements in α, check if $\pi_\alpha \in (\mathbb{G}_{\hat{q}} \times \mathbb{G}_q^2) \times (\mathbb{Z}_{\hat{q}} \times \mathbb{G}_q \times \mathbb{Z}_q)$

2.2.2 Response Tests $\mathbf{B}$

2.2.2.1 For all elements check if $v \in \{0, ..., N_E\}$

2.2.2.2 For all elements check if $\beta_j \in \mathbb{G}_q^{k'_v} \times (\mathcal{B}^{L_M})^{nk'_v} \times \mathbb{G}_q$

2.2.2.3 For all elements check if $\sigma_{vj}^{cast} \in \mathbb{B}^\ell \times \mathbb{Z}_q$

2.2.3 Confirmation Tests $\mathbf{C}$

2.2.3.1 For all elements if $v \in \{0, ..., N_E\}$

2.2.3.2 For all elements in γ, check if $\hat{y}_v \in \mathbb{G}_{\hat{q}}$

2.2.3.3 For all elements in γ, check if $\pi_\beta \in \mathbb{G}_{\hat{q}} \times \mathbb{Z}_{\hat{q}}$

2.2.4 Finalization Tests $\mathbf{D}$

2.2.4.1 For all elements check if $v \in \{0, ..., N_E\}$

2.2.4.2 For all elements check if $\delta_j \in \mathcal{B}^{L_F} \times \mathbb{Z}_q^2$

2.2.4.3 For all elements check if $\sigma_{vj}^{\text{conf}} \in \mathbb{B}^\ell \times \mathbb{Z}_q$

2.3 Nach der Wahl

2.3.1 For all $j \in \{1, ..., s\}$ check if $\mathbf{e}_j \in (\mathbb{G}_q^2)^{N*}$

2.3.2 For all $j \in \{1, ..., s\}$ check if $\pi_j \in (\mathbb{G}_q^3 \times \mathbb{G}_q^2 \times \mathbb{G}_q^N) \times (\mathbb{Z}_q^4 \times \mathbb{Z}_q^N \times \mathbb{Z}_q^N) \times \mathbb{G}_q^N \times \mathbb{G}_q^N$

2.3.3 For all $j \in \{1, ..., s\}$ check if $\mathbf{b}'_j \in \mathbb{G}_q^N$

2.3.4 For all $j \in \{1, ..., s\}$ check if $\pi'_j \in (\mathbb{G}_q \times \mathbb{G}_q^N) \times \mathbb{Z}_q$

2.3.5 For all $j \in \{1, ..., s\}$, $i \in \{1, ..., N\}$ check if $v_{ij} \in \mathbb{B}$

2.3.6 For all $j \in \{1, ..., s\}$, $i \in \{1, ..., N\}$ check if $\omega_{ij} \in \mathbb{B}$

2.3.7 For all $j \in \{1, ..., s\}$ check if $\sigma_j^{mix} \in \mathbb{B} \times \mathbb{Z}_q$

2.3.8 For all $j \in \{1, ..., s\}$ check if $\sigma_j^{dec} \in \mathbb{B} \times \mathbb{Z}_q$

2.3.9 Check if $\sigma^{tally} \in \mathbb{B} \times \mathbb{Z}_q$

3 Konsistenz

In diesem Teil wird geprüft ob die Parameter zu den anderen konsistent sind. Wir haben zu Beispiel zwei Vektoren, welche die gleiche Länge haben sollten. Nun wird geprüft ob diese wirklich die gleiche Länge haben. Auch hier ist der Output wahr oder falsch.

3.1 Vor der Wahl

3.1.1 Check if $|\mathbf{n}| = t$

3.1.2 Check if $|\mathbf{k}| = t$

3.1.3 Check if $|\mathbf{E}| = N_E$

3.1.4 For all $i \in \{1, ..., N_E\}$ check if $|\mathbf{e}_i| = t$

3.1.5 Check if $|\mathbf{c}| = n$

3.1.6 Check if $|\mathbf{v}| = N_E$

3.1.7 Check if $|\mathbf{w}| = N_E$

3.1.8 Check if $|\hat{\mathbf{D}}| = s$

3.1.9 For all $j \in \{1, ..., s\}$, check $|\hat{\mathbf{d}}_j| = N_E$

3.1.10 Check if $|\mathbf{pk}| = s$

3.1.11 Check if $p_{n+w} \prod_{j=1}^{k} p_{n-j+1} < p$

3.2 Während der Wahl

3.2.1 For all elements in $\mathbf{A}$, for all α, check if $|\mathbf{a}| = k$

3.2.2 Response Tests $\mathbf{B}$

3.2.2.1 For all elements, for $\boldsymbol{\beta}_v = \{\beta_{v,1}, ..., \beta_{v,s}\}$, check if $|\boldsymbol{\beta}_v| = s$

3.2.2.2 For all elements, for $\mathbf{S}_{cast_v} = \{\sigma_{v,1}^{cast}, ...\sigma_{v,s}^{cast}\}$, check if $|\mathbf{S}_{cast_v}| = s$

3.2.3 Finalization Tests $\mathbf{D}$

3.2.3.1 For all elements, for $\boldsymbol{\delta}_v = \{\delta_{v,1}, ..., \delta_{v,s}\}$, check if $|\boldsymbol{\delta}_v| = s$

3.2.3.2 For all elements, for $\mathbf{S}_{\text{conf}_v} = \{\sigma_{v,1}^{\text{conf}}, ...\sigma_{v,s}^{\text{conf}}\}$, check if $|\mathbf{S}_{\text{conf}_v}| = s$

3.3 Nach der Wahl

3.3.1 Check if $|\mathbf{E}'| = s$

3.3.2 For all $j \in \{1, ..., s\}$, check if $|\mathbf{e}'_j| = N$

3.3.3 Check if $|\boldsymbol{\pi}| = s$

3.3.4 Check if $|\mathbf{B}'| = s$

3.3.5 For all $j \in \{1, ..., s\}$, check if $|\mathbf{b}'_j| = N$

3.3.6 Check if $|\boldsymbol{\pi}'| = s$

3.3.7 Check if $|\mathbf{V}| = N$

3.3.8 For all $i \in \{1, ..., N\}$, check if $|\mathbf{v}_i| = n$

3.3.9 Check if $|\mathbf{W}| = (N, \omega)$

3.3.10 For all $i \in \{1, ..., N\}$, check if $|\omega_i| = \omega$

3.3.11 Check if $|\mathbf{s}_{mix}| = s$

3.3.12 Check if $|\mathbf{s}_{dec}| = s$

4 Evidenz

In diesem Teil wird geprüft ob die verschieden kryptographischen Beweisen stimmen.
Dazu wird eine Verifizierungsfunktion aufgerufen, die wahr oder falsch zurückgibt.

Es handelt sich hierbei um sogenannte Nicht-Interaktive Zero-Knowledge-Beweise. Sie dienen dazu, zu beweisen, dass man Kenntnis von gewissen Parameter oder Schlüsseln hat.Beispiel „proof of confirmation“ : Hier wir der Beweis erbracht, dass man sowohl das öffentliche „confirmation credential“ und auch das private „vote validity credential“ kennt.

4.1 Proof Tests

4.1.1 For all elements in α, check proof of validity of ballot π_α

4.1.2 For all elements in $\mathbf{C}$, check proof of confirmation π_β

4.1.3 For all $j \in \{1, ..., s\}$, check shuffle proof π_j

4.1.4 For all $j \in \{1, ..., s\}$, check decryption proof π'_j

5 Authentizität

In diesem Teil wird die Gültigkeit der Zertifikate und Signaturen überprüft.
Auch hier wird eine Verifizierungsfunktion aufgerufen, welche wiederum wahr oder falsch zurückgibt.
Jedes Zertifikat besitzt einen Gültigkeitszeitraum sowie einen öffentlichen Schlüssel. Mit dem öffentlichen Schlüssel kann dann die Signatur des Zertifikates überprüft werden.

5.1 Zertifikate

5.1.1 Check validity of Certificate of election administrator C_{Admin}

5.1.2 For all $j \in \{1, ..., s\}$, check validity of the Certificates of authorities C_{Auth_j}

5.2 Siganturen

5.2.1 Check signature of full election parameters σ_1^{param}

5.2.2 Check signature of part of election parameters σ_2^{param}

5.2.3 Check signature of other part of election parameters σ_3^{param}

5.2.4 Check signature of tallying result σ^{tally}

5.2.5 For all $j \in \{1, ..., s\}$, check signature of public credentials σ_j^{prep}

5.2.6 For all $j \in \{1, ..., s\}$, check signature of public keys σ_j^{kgen}

5.2.7 For all elements in $\mathbf{B}$, for $j \in \{1, ..., s\}$, $i \in \{1, ..., N\}$ check σ_{ij}^{cast}

5.2.8 For all elements in $\mathbf{D}$, for $j \in \{1, ..., s\}$,$i \in \{1, ..., N\}$ check $\sigma_{ij}^{\text{conf}}$

5.2.9 For all $j \in \{1, ..., s\}$, signatures of mixed re-encryption's check σ_j^{mix}

5.2.10 For all $j \in \{1, ..., s\}$, check signatures of partial decryption's σ_j^{dec}