

Verlässliche Echtzeitsysteme

Übungen zur Vorlesung

Codierung

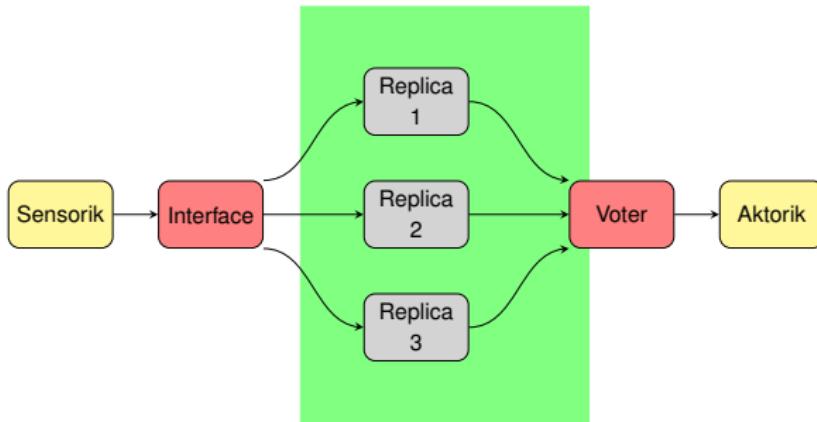
Phillip Raffeck, Florian Schmaus, Simon Schuster

Friedrich-Alexander-Universität Erlangen-Nürnberg
Lehrstuhl Informatik 4 (Verteilte Systeme und Betriebssysteme)
<https://www4.cs.fau.de>

Sommersemester 2020



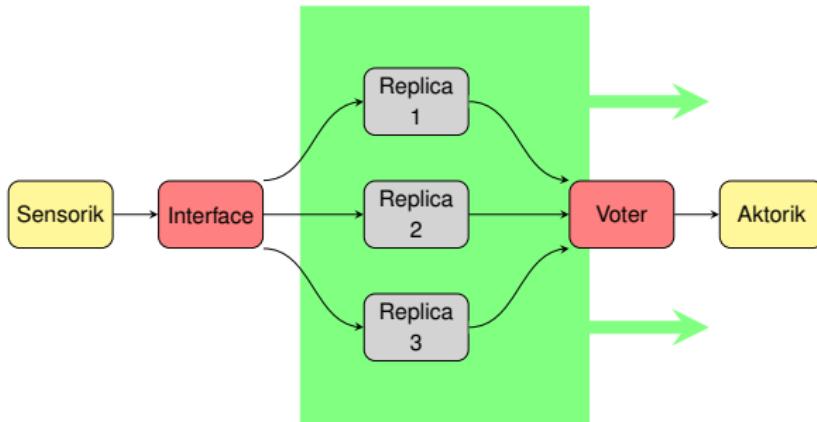
Klassische “Triple Modular Redundancy” (TMR)



- Schnittstelle sammelt Eingangsdaten (Replikdeterminismus)
- Verteilt Daten und aktiviert Replikate
- Mehrheitsentscheider (Voter) wählt Ergebnis
- Ergebnis wird an Aktuator versendet



Klassische “Triple Modular Redundancy” (TMR)



Redundanzbereich

Ausschließlich Replikatausführung

- ~ Erweiterung der Ausgangsseite mit Informationsredundanz
- ~ Mehrheitsentscheid über codierte Prüfsumme



nach Forin 1989: "Vital coded microprocessor principles and application for various transit systems" [1]

- Arithmetisch codierter Wert V_C
- Ausgangswert

$$V_C = V * A + B_V + D$$

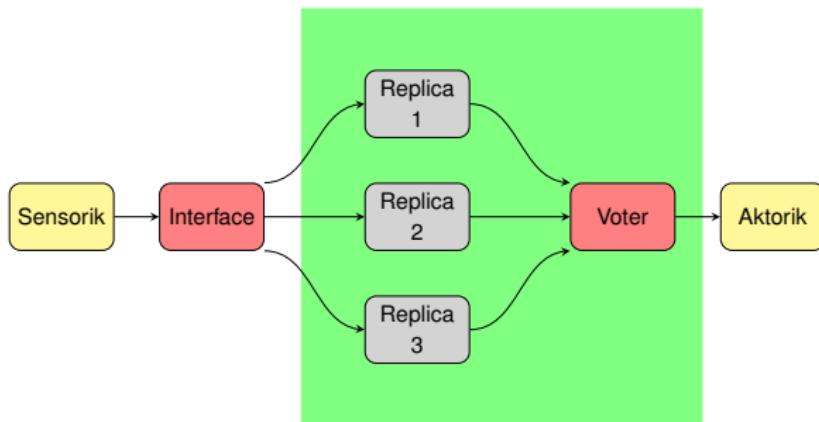
- Schlüssel
- Variablenspezifische Signatur
- Zeitstempel



- Schlüssel A sollte so groß wie möglich sein:
 - ↝ Möglichst geringe Restfehlerwahrscheinlichkeit ($P = 1/A$)
- Wertebereich des dynamischen Zeitstempels
 - $D = \{x \mid x \in \mathbb{N}_0 \wedge x \leq D_{max}\}$
 - Zeitstempel darf überlaufen: $D_{max} + 1 = 0$
- Für jede Signatur $B_* \in \mathbb{N}$ muss dann gelten
 - $B_* + D_{max} < A$
 - Die minimale Distanz zwischen jeweils zwei Signaturen im System muss größer D_{max} sein: $\forall i, j : |B_i - B_j| > D_{max}$
 - Sämtliche Distanzen zwischen jeweils zwei Signaturen müssen unterschiedlich sein: $\forall i : \forall j, k : |B_i - B_j| = |B_k - B_j| \Rightarrow i = k$



Erweiterung I – codierte Ausgangswerte



- Replikate liefern arithmetisch codierte Ergebnisse
- Mehrheitsentscheid auf codierten Prüfsummen
- Übertragung codierter Ergebnisse

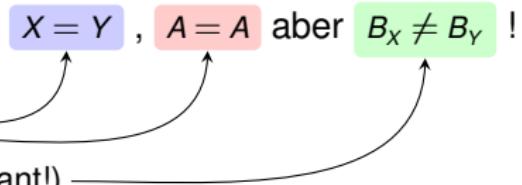


Vereinfachung für diese Übungsaufgabe

- Kein Zeitstempel
- Voting basiert auf codierter Vergleichsoperation:
 $\leadsto X_C = Y_C \Rightarrow X * A + B_X = Y * A + B_Y$
- Im fehlerfreien Fall gilt:

- *Rohwerte* sind identisch
- Schlüssel ist per Definition identisch
- Signaturen sind unterschiedlich (aber konstant!)

$X = Y$, $A = A$ aber $B_X \neq B_Y$!

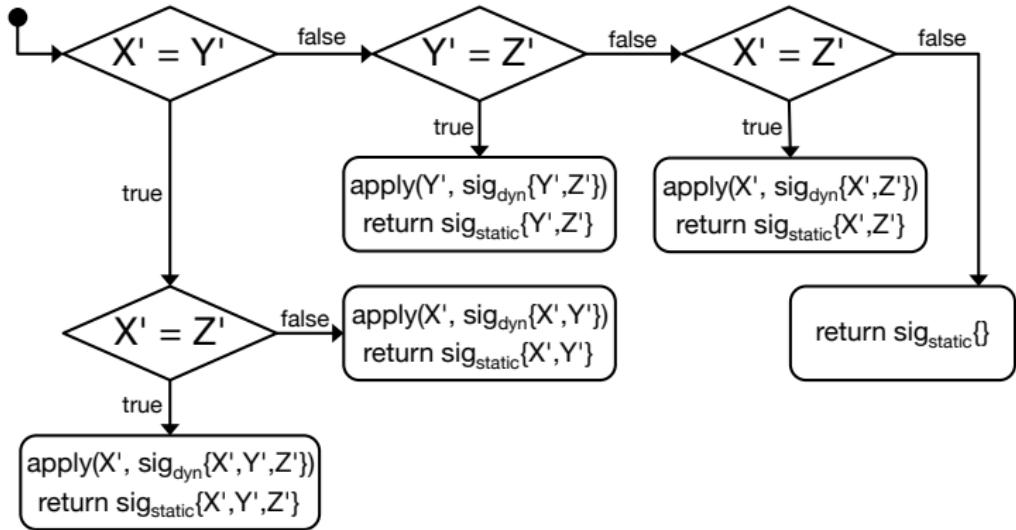


Bestimmung der Gleichheit durch Differenzbildung:

$$\leadsto X_C - Y_C = B_X - B_Y = \text{const.}$$



Codierter Mehrheitsentscheid



- Bestimmung von dynamischer und statischer Signatur:
 - $sig_{dyn}(X', Y') : X' = Y' \Rightarrow X' - Y'$
 - $sig_{static}(X', Y') : X' = Y' \Rightarrow B_X - B_Y$
- Für die Signaturen muss gelten: $B_X > B_Y > B_Z$

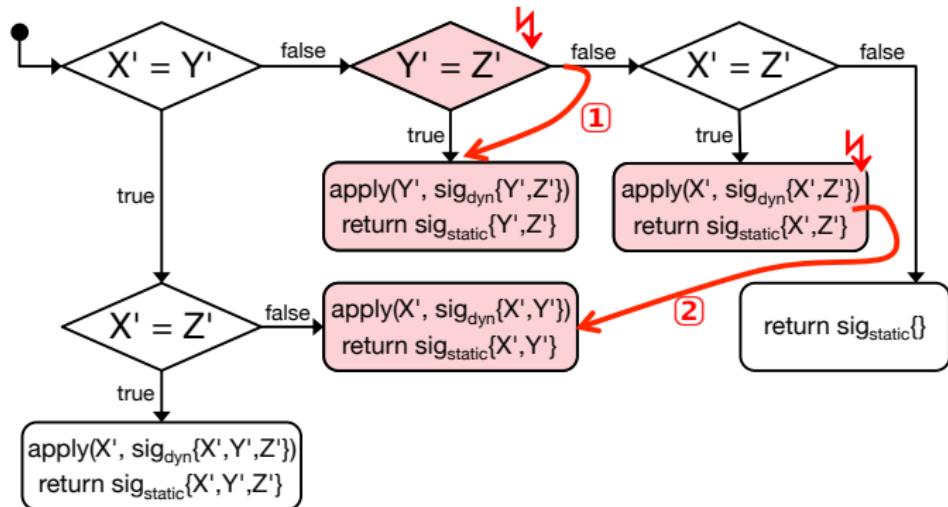


1. Vergleichsoperation wird durchgeführt (z. B. $X' = Y' \wedge X' = Z'$)
 - Berechnung von sig_{dyn}
 - Vergleich mit $\text{sig}_{\text{static}}$
2. Verzweigungsentscheidung wird nachberechnet:
 - Wiederholte (redundante) Berechnung von sig_{dyn}
 - Erneuter Vergleich: $\text{sig}_{\text{dyn}} = \text{sig}_{\text{static}}$
 - Addiere sig_{dyn} (*apply*) zum gewählten Ergebnis
3. Konstante Signatur des durchlaufenen Zweiges identifiziert Gewinner (Rückgabewert: $\text{sig}_{\text{static}}$)
 - Aktor wählt entsprechendes Replikatergebnis
 - Führt inverse Operation zu *apply* durch

Im Voter wurde die *dynamisch berechnete Signatur der Verzweigungsentscheidung* hinzu addiert. Im Aktor wird mit der entsprechenden *konstanten Signatur zurückgerechnet*.



Codierter Mehrheitsentscheid - Fehlerfall



1. Falsche Verzweigungsentscheidung: ($Y' \neq Z'$)

- Y' wird als korrekt angenommen, sig_{dyn} wird berechnet
- allerdings ist sig_{dyn} tatsächlich $\neq sig_{static}$
- Fehler wird vor dem *apply* erkannt

2. Falscher (plötzlicher) Sprung

- X' wird als korrekt erkannt, sig_{dyn} wird erneut berechnet



Ausgangslage

- Wähle $A = 601$
- Initiale Ergebniskodierung in den Replikaten:

	X	Y	Z
Wert	7	5	7
B	37	23	5
Kodiert	$X' = A * 7 + 37$ $= 4244$	$Y' = A * 5 + 23$ $= 3028$	$Z' = A * 7 + 5$ $= 4212$

- Berechnung der statischen Signaturen **vorab, statisch**:

$$\text{sig}_{\text{static}} \{X', Y', Z'\} = (B_X - B_Y) + (B_X - B_Z) = 46$$

$$\text{sig}_{\text{static}} \{X', Y'\} = (B_X - B_Y) = 14$$

$$\text{sig}_{\text{static}} \{Y', Z'\} = (B_Y - B_Z) = 18$$

$$\text{sig}_{\text{static}} \{X', Z'\} = (B_X - B_Z) = 32$$



Regulärer Durchlauf

- Das eigentliche Voting geschieht dann zur Laufzeit:

- $X' = Y'?$

$$X' - Y' \stackrel{?}{=} \text{sig}_{\text{static}} \{ X', Y' \} \Leftrightarrow 4244 - 3028 = 1216 \stackrel{?}{=} 14 \Leftrightarrow \text{false}$$

- $Y' = Z'?$

$$Y' - Z' \stackrel{?}{=} \text{sig}_{\text{static}} \{ Y', Z' \} \Leftrightarrow 3028 - 4212 = -1184 \stackrel{?}{=} 18 \Leftrightarrow \text{false}$$

- $X' = Z'?$

$$X' - Z' \stackrel{?}{=} \text{sig}_{\text{static}} \{ X', Z' \} \Leftrightarrow 4244 - 4212 = 32 \stackrel{?}{=} 32 \Leftrightarrow \text{true}$$

- Berechnung der dynamischen Signaturen zur Laufzeit:

$$\text{sig}_{\text{dyn}} \{ X', Z' \} = (X' - Z') = (4244 - 4212) = 32$$



5. $\text{sig}_{\text{dyn}} \{X', Z'\} \stackrel{?}{=} \text{sig}_{\text{static}} \{X, Z\} \Leftrightarrow 32 \stackrel{?}{=} 32 \Leftrightarrow \text{true}$
6. $X' = \text{apply}(X', \text{sig}_{\text{dyn}} \{X', Z'\}) = 4276$
7. $B_E \leftarrow \text{sig}_{\text{static}} \{X', Z'\} = 32$
8. $\text{return}(32)$
9. Nachschlagen der zugrundeliegenden Variable mittels $B_{\text{dyn}} = 32$ (erste Variable der Konsensmenge), basierend auf den vorberechneten statischen Werten:
$$(\text{result}_{\text{variable}}, \text{result}_{\text{extrasignature}}) \leftarrow (X', B_X)$$
10. $\text{inv_apply}(\text{result}_{\text{variable}}, B_{\text{dyn}}) = \text{inv_apply}(4276, 32) = 4276 - 32 = 4244$

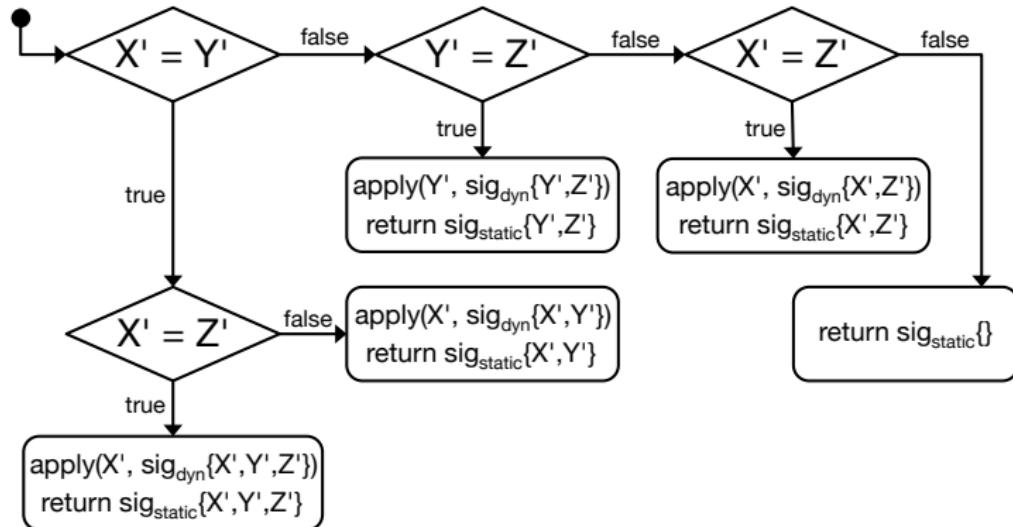


Regulärer Durchlauf (III)

11. Signaturverifikation:

$$check(4244, A, B_X): \frac{4244 - B_X}{A} = 7 \text{ Rest: } 0$$

12. Ergebnis erfolgreich dekodiert: 7



Es hat somit eine erfolgreiche Einigung auf die Konsensmenge $\{X', Z'\}$ stattgefunden.



Ausgangslage (unverändert)

- Wähle $A = 601$
- Initiale Ergebniskodierung in den Replikaten:

	X	Y	Z
Wert	7	5	7
B	37	23	5
Kodiert	$X' = A * 7 + 37$ $= 4244$	$Y' = A * 5 + 23$ $= 3028$	$Z' = A * 7 + 5$ $= 4212$

- Berechnung der statischen Signaturen **vorab, statisch**:

$$\text{sig}_{\text{static}} \{X', Y', Z'\} = (B_X - B_Y) + (B_X - B_Z) = 46$$

$$\text{sig}_{\text{static}} \{X', Y'\} = (B_X - B_Y) = 14$$

$$\text{sig}_{\text{static}} \{Y', Z'\} = (B_Y - B_Z) = 18$$

$$\text{sig}_{\text{static}} \{X', Z'\} = (B_X - B_Z) = 32$$



Fehlerszenario ①

1. $X' = Y'?$

$$X' - Y' \stackrel{?}{=} \text{sig}_{\text{static}} \{ X', Y' \} \Leftrightarrow 4244 - 3028 = 1216 \stackrel{?}{=} 14 \Leftrightarrow \text{false}$$

2. $Y' = Z'?$

$$Y' - Z' \stackrel{?}{=} \text{sig}_{\text{static}} \{ Y', Z' \} \Leftrightarrow 3028 - 4212 = -1184 \stackrel{?}{=} 18 \Leftrightarrow \text{false}$$

3. Hier tritt nun der Operatorfehler ein, die falsche Verzweigung ① wird ausgewählt
4. Berechnung der dynamischen Signaturen zur Laufzeit:

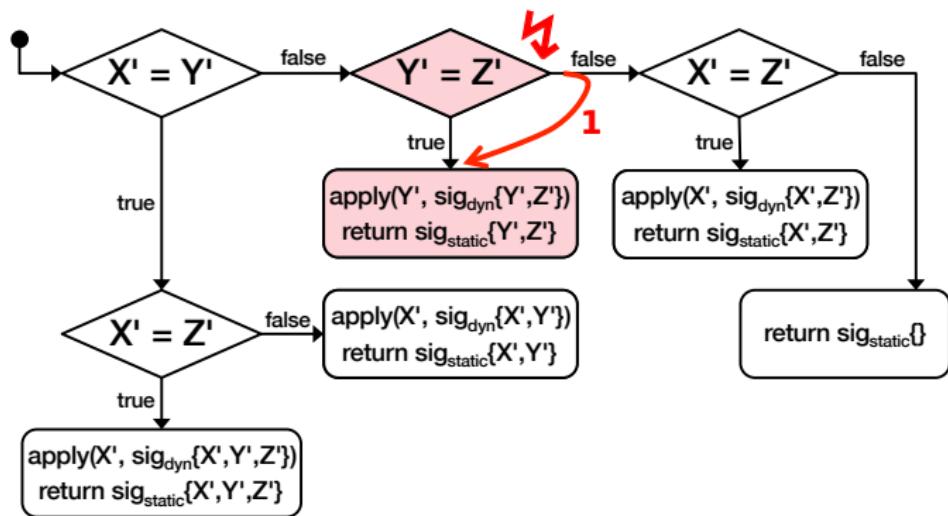
$$\text{sig}_{\text{dyn}} \{ Y', Z' \} = (Y' - Z') = (3028 - 4212) = -1184$$

5. $\text{sig}_{\text{dyn}} \{ Y', Z' \} \stackrel{?}{=} \text{sig}_{\text{static}} \{ Y, Z \} \Leftrightarrow -1184 \stackrel{?}{=} 18 \Leftrightarrow \text{false}$



Fehlerszenario ① (II)

6. Fehler erfolgreich detektiert: Vergleich zwischen sig_{dyn} und $\text{sig}_{\text{static}}$ für Konsensmenge $\{Y', Z'\}$ fehlgeschlagen



Ausgangslage (unverändert)

- Wähle $A = 601$
- Initiale Ergebniskodierung in den Replikaten:

	X	Y	Z
Wert	7	5	7
B	37	23	5
Kodiert	$X' = A * 7 + 37$ $= 4244$	$Y' = A * 5 + 23$ $= 3028$	$Z' = A * 7 + 5$ $= 4212$

- Berechnung der statischen Signaturen **vorab, statisch**:

$$\text{sig}_{\text{static}} \{X', Y', Z'\} = (B_X - B_Y) + (B_X - B_Z) = 46$$

$$\text{sig}_{\text{static}} \{X', Y'\} = (B_X - B_Y) = 14$$

$$\text{sig}_{\text{static}} \{Y', Z'\} = (B_Y - B_Z) = 18$$

$$\text{sig}_{\text{static}} \{X', Z'\} = (B_X - B_Z) = 32$$



1. $X' = Y'$?

$$X' - Y' \stackrel{?}{=} \text{sig}_{\text{static}} \{ X', Y' \} \Leftrightarrow 4244 - 3028 = 1216 \stackrel{?}{=} 14 \Leftrightarrow \text{false}$$

2. $Y' = Z'$?

$$Y' - Z' \stackrel{?}{=} \text{sig}_{\text{static}} \{ Y', Z' \} \Leftrightarrow 3028 - 4212 = -1184 \stackrel{?}{=} 18 \Leftrightarrow \text{false}$$

3. $X' = Z'$?

$$X' - Z' \stackrel{?}{=} \text{sig}_{\text{static}} \{ X', Z' \} \Leftrightarrow 4244 - 4212 = 32 \stackrel{?}{=} 32 \Leftrightarrow \text{true}$$

4. Berechnung der dynamischen Signaturen zur Laufzeit:

$$\text{sig}_{\text{dyn}} \{ X', Z' \} = (X' - Z') = (4244 - 4212) = 32$$



5. $\text{sig}_{\text{dyn}} \{X', Z'\} \stackrel{?}{=} \text{sig}_{\text{static}} \{X, Z\} \Leftrightarrow 32 \stackrel{?}{=} 32 \Leftrightarrow \text{true}$
6. $X' = \text{apply}(X', \text{sig}_{\text{dyn}} \{X', Z'\}) = 4276$
7. Hier tritt nun der Kontrollflussfehler ② ein
8. $B_E \leftarrow \text{sig}_{\text{static}} \{X', Y'\} = 14$
9. $\text{return}(14)$
10. Nachschlagen der zugrundeliegenden Variable mittels $B_{\text{dyn}} = 14$ (erste Variable der Konsensmenge), basierend auf den vorberechneten statischen Werten:
$$(\text{result}_{\text{variable}}, \text{result}_{\text{extrasignature}}) \leftarrow (X', B_X)$$
11. $\text{inv_apply}(\text{result}_{\text{variable}}, B_{\text{dyn}}) = \text{inv_apply}(4276, 14) = 4276 - 14 = 4262$

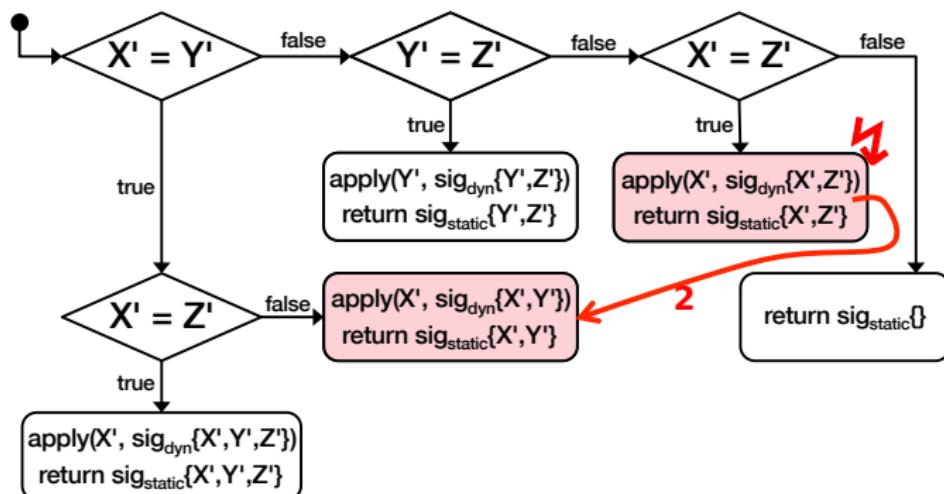


Fehlerszenario ② (II)

12. Signaturverifikation:

$$check(4262, A, B_X): \frac{4262 - B_X}{A} = 7 \text{ Rest: } 18$$

13. Fehler erfolgreich detektiert: Dekodieren schlägt fehl



Aufgabe

- Absichern des Voters per EAN mittels CoRed-Ansatz
- Berechnungen mit codierten Werten
 - Berücksichtigung der (statischen) Signaturen
 - ~ Eigene Operationen mit konstanten Signaturwerten notwendig
 - ~ bspw. eigenes equals anstatt ==
- Jedes Replikat hat genau einen Ausgabewert ($\text{integer} \mapsto \text{enc_t}$): eine codierte Prüfsumme des Ergebnisses
 - ~ Festlegung für jeden der drei Ausgabewerte (X', Y', Z') jeweils *unterschiedliche* aber *konstante* Signatur (SIG_X, SIG_Y, SIG_Z)
- Nutzung des nächstgrößeren Datentyps X für den ursprünglichen Wert X'
 - ~ Wahl einer Zahl A mit möglichst großem Hamming-Abstand unter *Vermeidung* möglicher *Überläufe bei der Codierung*
 - ~ Handhabbarkeit: **nicht** Super-As





Forin.

Vital coded microprocessor principles and application for various transit systems.

IFA-GCCT, pages 79–84, 1989.