(19) Deutsches Patent- und Markenamt

(10) **DE 10 2015 103 640 A1** 2016.09.15

(12) # Offenlegungsschrift

(21) Aktenzeichen: **10 2015 103 640.1**
(22) Anmeldetag: **12.03.2015**
(43) Offenlegungstag: **15.09.2016**

(51) Int Cl.: ***G06F 21/44*** (2013.01)

(71) Anmelder:
Universität Rostock, 18055 Rostock, DE

(74) Vertreter:
Gulde & Partner Patent- und Rechtsanwaltskanzlei mbB, 10179 Berlin, DE

(72) Erfinder:
Salomon, Ralf, Prof. Dr., 18119 Rostock, DE;
Joost, Ralf, Dr., 18225 Kühlungsborn, DE

(56) Ermittelter Stand der Technik:

US	2013 / 0 194 886	A1
US	4 431 928	A
EP	2 191 410	B1

Flip-flop (electronics). In: Wikipedia, The Free Encylopedia. Bearbeitungsstand: 7. März 2015. URL: https://en.wikipedia.org/wiki/Flip-flop_(electronics)?oldid=650252772 [abgerufen am 1. August 2016]

MAES, R.: Physically Unclonable Functions. Constructions, Properties and Applications. Berlin, Heidelberg : Springer, 2013. S. 11–48. - ISBN 978-3-642-41394-0. DOI: 10.1007/978-3-642-41395-7

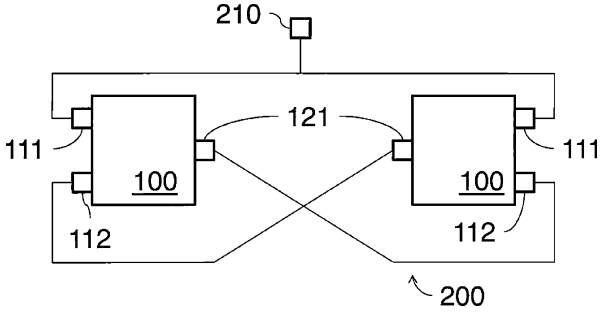
SU, Y ; HOLLEMAN, J ; OTIS, B.: A 1.6pJ/bit 96% Stable Chip-ID Generating Circuit using Process Variations. In: IEEE International Solid-State Circuits Conference 2007 (ISSCC 2007), 2007, S. 406, 407, 611. - ISSN 0193-6530. DOI: 10.1109/ISSCC.2007.373466

Prüfungsantrag gemäß § 44 PatG ist gestellt.

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

(54) Bezeichnung: **Vorrichtung umfassend logische Elemente**

(57) Zusammenfassung: Die vorliegende Erfindung betrifft eine Vorrichtung umfassend logische Elemente. Insbesondere betrifft die vorliegende Erfindung eine Zertifizierung der Echtheit der Vorrichtung.
Die Vorrichtung (400) umfasst logische Elemente (100, 100'), von denen mindestens zwei zu einem Schaltelement (200) verschaltet sind, wobei ein Antwortverhalten eines Ausgangssignals des Schaltelements auf zumindest einen Zustandsübergang theoretisch unvorhersagbar ist.
Die Vorrichtung ist dadurch gekennzeichnet, dass durch ein tatsächliches Antwortverhalten des Ausgangssignals auf den zumindest einen Zustandsübergang eine physikalisch nichtnachbildbare Funktion für eine Zertifizierung der Echtheit der Vorrichtung (400) definiert ist.



Beschreibung

TECHNISCHES GEBIET

[0001] Die vorliegende Erfindung betrifft eine Vorrichtung umfassend logische Elemente. Insbesondere betrifft die vorliegende Erfindung eine Zertifizierung der Echtheit der Vorrichtung.

STAND DER TECHNIK

[0002] Die Zertifizierung der Echtheit einer technischen Vorrichtung, beispielsweise ein Speicherbaustein, ein Prozessor oder ein Field-Programmable Gate Array (FPGA), ist in vielen Anwendungen von Interesse. Durch die Zertifizierung kann sichergestellt werden, dass mit einer konkreten technischen Vorrichtung (derselben Vorrichtung) und nicht mit einem Replikat bzw. einer Fälschung (einer gleichen Vorrichtung) interagiert wird.

[0003] Eine Möglichkeit, Echtheit zu zertifizieren, besteht in physikalisch nichtnachbildbaren Funktionen.

[0004] Da die Herstellung jeder Vorrichtung stets geringfügigen, nicht kontrollierbaren Variationen unterworfen ist, unterscheiden sich auch zwei nach demselben Verfahren hergestellte Vorrichtungen in physikalischen Eigenschaften, die für jede der Vorrichtungen eine Art Fingerabdruck definieren. Diese physikalischen Eigenschaften werden auch als physikalisch nichtnachbildbare Funktionen bezeichnet. Beispielsweise unterscheiden sich baugleiche Transistoren durch inhärente physikalische Variationen wie etwa die Lage und Konzentration der Dotierungsatome. Dadurch entstehen auch minimale Unterschiede in abstrakteren technischen Parametern wie beispielsweise der Schaltgeschwindigkeit eines Transistors oder Logikgatters. Diese Variationen sind aufgrund oben erwähnter (zufallsbehafteter) Produktionsprozesse nicht vollständig kontrollierbar und somit auch nicht vollständig reproduzierbar.

[0005] Beispiele physikalisch nichtnachbildbarer Funktionen sind Signallaufzeiten in Abhängigkeit von einer Konfigurationseingabe und die Frequenzverhältnisse von auf der Vorrichtung implementierten Oszillatoren.

OFFENBARUNG DER ERFINDUNG

[0006] Die vorliegende Erfindung befasst sich mit der Aufgabe, eine Vorrichtung anzugeben, deren Echtheit besonders einfach zertifiziert werden kann.

[0007] Erfindungsgemäß wird daher eine Vorrichtung gemäß Anspruch 1 vorgeschlagen. Bevorzugte Ausführungsformen sind in den abhängigen Ansprüchen angegeben.

[0008] Die Vorrichtung umfasst logische Elements, von denen mindestens zwei zu einem Schaltelement verschaltet sind, wobei ein Antwortverhalten eines Ausgangssignals des Schaltelements auf zumindest einen Zustandsübergang theoretisch unvorhersagbar ist.

[0009] Die Vorrichtung ist dadurch gekennzeichnet, dass durch ein tatsächliches Antwortverhalten des Ausgangssignals auf den zumindest einen Zustandsübergang eine physikalisch nichtnachbildbare Funktion für eine Zertifizierung der Echtheit der Vorrichtung definiert ist.

[0010] In einer bevorzugten Ausführungsform sind die logischen Elemente des Schaltelements bezüglich eines weiteren logischen Elements, von dem ein Kontrolldraht, über den ein Zustandsübergangssignal an die logischen Elements des Schaltelements geliefert werden kann, ausgeht, symmetrisch angeordnet.

[0011] Die symmetrische Anordnung ist der theoretischen Unvorhersagbarkeit zuträglich.

[0012] Die logischen Elements des Schaltelements können so bezüglich des weiteren logischen Elements angeordnet sein, dass eine Zeitdifferenz, mit der das Zustandsübergangssignal eines der logischen Elemente gegenüber einem anderen der logischen Elements früher oder später erreicht, geringstmöglich ist.

[0013] Dies ist eine einfach realisierbare symmetrische Anordnung.

[0014] Die logischen Elements der Vorrichtung können in Reihen und Spalten angeordnet sein und genau zwei logische Elemente können zu einem Schaltelement verschaltet sein, die dann entweder in einer selben Spalte und unterschiedlichen Reihen oder in einer selben Reihe und unterschiedlichen Spalten angeordnet

sein können, wobei sich dann zwischen den unterschiedlichen Reihen bzw. Spalten mindestens eine weitere Reihe bzw. mindestens eine weitere Spalte befinden kann.

[0015] Es ist auch möglich, dass jeweils genau die zwei logischen Elemente zu einem Schaltelement verschaltet sein können, die je durch eine Anzahl Spalten und eine Anzahl Reihen von dem weiteren logischen Element beabstandet sind, wobei die Summen der Anzahl Spalten und der Anzahl Reihen der miteinander verschalteten logischen Elemente gleich sind. Insbesondere können die Anzahlen Spalten der miteinander verschalteten logischen Elemente gleich sein und die Anzahlen Reihen der miteinander verschalteten logischen Elemente können gleich sein.

[0016] Diese Formen der Anordnung bewirken besonders signifikante physikalisch nichtnachbildbare Funktionen.

[0017] Das weitere logische Element kann sich in einer von den unterschiedlichen Reihen gleichweit beabstandeten mittleren Reihe bzw. in einer von den unterschiedlichen Spalten gleichweit beabstandeten mittleren Spalte befinden.

[0018] So wird die symmetrische Anordnung sichergestellt.

[0019] Weitere von der Vorrichtung umfasste logische Elemente können zu weiteren Schaltelementen verschaltet sein, wobei dann durch das tatsächliche Antwortverhalten von Ausgangssignalen der weiteren Schaltelemente auf den zumindest einen Zustandsübergang weitere physikalisch nichtnachbildbare Funktionen für die Zertifizierung der Echtheit definiert sein können.

[0020] Die Vorrichtung kann weiterhin einen Soft-Core Prozessor umfassen, der eine Schnittstelle zwischen der physikalisch nichtnachbildbaren Funktion und einem Host-Computer bereitstellt.

[0021] Der Soft-Core Prozessor kann auf einen kleinen Fußabdruck hin optimiert sein und/oder kann keine Verzweigungsvorhersage (branch prediction), keinen zusätzlichen Pufferspeicher (Cache) oder keinen Vervielfacher (Multiplier) umfassen.

[0022] Das tatsächliche Antwortverhalten kann in „stabile Nullantwort”, „stabile Einsantwort” und „unstabile Antwort” klassifiziert sein.

[0023] Das Schaltelement kann ein Flipflop sein.

ZEICHNUNGEN

[0024] Ausführungsbeispiele der Erfindung werden anhand der Zeichnungen und der nachfolgenden Beschreibung näher erläutert. Es zeigen, schematisch:

[0025] **Fig.** 1 ein Schaltelement, wie es in einem Ausführungsbeispiel der erfindungsgemäßen Vorrichtung Verwendung finden kann,

[0026] **Fig.** 2 ein Ausführungsbeispiel der erfindungsgemäßen Vorrichtung,

[0027] **Fig.** 3 Messergebnisse von 1000 theoretisch unvorhersagbaren Zustandsübergängen einer ersten erfindungsgemäßen Vorrichtung,

[0028] **Fig.** 4 Messergebnisse von 100000 theoretisch unvorhersagbaren Zustandsübergängen der ersten erfindungsgemäßen Vorrichtung, und

[0029] **Fig.** 5 die Messergebnisse aus **Fig.** 4 überlagert mit Messergebnissen von 100000 theoretisch unvorhersagbaren Zustandsübergängen einer zweiten, mit der ersten erfindungsgemäßen Vorrichtung baugleichen (hardware-identischen) Vorrichtung.

AUSFÜRUNGSFORMEN DER ERFINDUNG

[0030] **Fig.** 1 zeigt ein aus zwei logischen Elementen **100** zusammengesetztes Schaltelement **200** (Schaltwerk). Die logischen Elemente **100** weisen je zwei Eingänge **111**, **112**, und einem Ausgang **121** auf. Dabei

ist jeweils der Ausgang **121** des einen logischen Elements **100** mit einem der Eingänge **112** des anderen logischen Elements **100** verschaltet. Die jeweils anderen Eingänge **111** der logischen Elemente **100** sind mit einem Schaltelementeingang **210** des Schaltelements **200** verschaltet und damit mit einander verschaltet.

[0031] im gezeigten Beispiel sind die logischen Elemente **100** NOR-Gatter, die genau dann am Ausgang **121** ein Signal ausgeben, wenn an keinen der Eingänge **111**, **112** ein Signal anliegt. **Fig.** 1 zeigt also ein RS-Flipflop (RS-Latch). Die Eingänge eines RS-Flipflops werden auch als R und S bezeichnet, Q und $\overline{Q}$ sind die Bezeichnungen der Ausgänge, sie entsprechen den Ausgängen der verschalteten logischen Elemente **100**. RS-Latches haben folgende Wahrheitswert Tabelle:

S	R	Q	$\overline{Q}$	Beschreibung
0	0	Q'	$\overline{Q}$'	Speichern
0	1	0	1	Setzen
1	0	1	0	Rücksetzen
1	1	1	1	Ungültig

Tabelle 1

[0032] RS-Latches besitzen also einen Zustand, der in der Regel als ”Ungültig” bezeichnet. Ein weiterer Zustand dieser Latches wird als ”Speichern” bezeichnet, da ein vorher hineingeschriebener Wert erhalten bleibt. Aus RS-Latches lassen sich daher Arbeitsspeicher (RAM) bilden.

[0033] Der Zustandsübergang von ”Ungültig” zu ”Speichern” ist in gewisser Weise randomisiert, so dass ein Signal am Ausgang des RS-Latches häufig nicht vorhersagbar ist: Unter anderem hängt das tatsächlich am Ausgang anliegende Signal von technischen Parametern wie der Schaltgeschwindigkeit der verwendeten Transistoren, der benötigten Leitungslängen sowie den charakteristischen Eigenschaften der Leitungstreiber ab. Mit anderen Worten, erfolgt der Zustandsübergang von „Ungültig” zu „Speichern” durch eine quasi-gleichzeitige Änderung der Signale „S” und „R”, so ist das Ausgangsignal „Q” derart randomisiert, das der endgültige Signalpegel nicht vorhersagbar ist.

[0034] Die vorliegende Erfindung baut auf diesem, zumindest teilweise nicht vorhersagbaren Verhalten auf. In einer beispielhaften Ausführungsform werden eine Zahl n, beispielsweise n = 256, von RS-Latches auf einem Gerät konfiguriert. Dann werden alle diese Latches vom Zustand ”Ungültig” direkt in den Zustand ”Speichern” überführt. Nach einer kurzen Relaxationszeit besteht der sich ergebende Zustand aus n Bits. Jedes dieser Bits kann den Wert ”0” oder ”1” haben.

[0035] Dieser Zustand lässt sich auf ein und demselben Gerät nahezu vollständig reproduzieren, wohingegen sich diese Zustände von Gerät zu baugleichem Gerät (beispielsweise Field-Programmable Gate Arrays) deutlich voneinander unterscheiden. Insofern lasst sich dieser Zustand direkt oder als Grundlage eines gerätespezifischen Fingerabdrucks verwenden.

[0036] Liegt also am Schaltelementeingang **210** ein EINS-Signal an, so wird das Ausgangssignal des Schaltelements **200** theoretisch unvorhersagbar, wenn ein Wechsel zu einem NULL-Signal am Schaltelementeingang **210** erfolgt. Das sich tatsächlich einstellende Ausgangssignal hängt von den individuellen physikalischen Eigenschaften des Elements ab, die sich aus nicht kontrollierbaren Schwankungen im Herstellungsprozess in der Herstellung für jedes Element ergeben.

[0037] Es ist auch möglich, anstelle von NOR-Gattern NAND-Gatter oder andere Arten logischer Elemente zu verwenden, sofern sich je mindestens zwei logische Elemente zu einem Schaltelement verschalten lassen, dessen Antwortverhalten im Ausgangssignal auf zumindest einen Zustandsübergang theoretisch unvorhersagbar ist. Insbesondere ist eine Verschaltung von logischen Elementen unterschiedlichen Typs möglich.

[0038] **Fig.** 2 zeigt ein Ausführungsbeispiel der erfindungsgemäßen Vorrichtung **400**. Die Vorrichtung **400** umfasst in Reihen und Spalten angeordnete logische Elemente. Zwei Gruppen A, B logischer Elemente befinden sich in gegenüberliegenden äußersten Spalten.

[0039] Jedes logisches Element aus Gruppe A ist je mit einem logischen Element aus der Gruppe B zu einem Schaltelement verschaltet. Dabei sind beispielsweise immer logische Elements aus derselben Reihe mit einander verschaltet.

[0040] Die Eingänge der logischen Elements in den Gruppen A und B sind alle mit einem weiteren logischen Element **100'** in einer Mittelspalte der Vorrichtung **400** verschaltet. Die Ausgänge der logischen Elemente in den Gruppen A und B sind mit einem Soft-Core **300** verschaltet, der eine Schnittstelle zu einem Computer bereitstellt. Über die Schnittstelle lässt sich das tatsächliche Antwortverhalten der Ausgangssignale der Schaltelemente auf einen theoretisch unvorhersagbaren Zustandsübergang für eine Auswertung auslesen.

[0041] Ein Beispiel für einen Soft-Core ist Nios II, eine 32-bit embedded Prozessor Architektur, die für die Altera Familie von FPGAs entworfen wurde. Nios II ist für die Implementierung einer Vielfalt von Rechneranwendungen geeignet, beispielsweise digitale Signalprozessoren oder Systemkontrolle. Ein anderes Soft-Corebeispiel ist MicroBlaze für die Xilinx Familie von FPGAs.

[0042] In einem Ausführungsbeispiels eines Verfahrens im Rahmen der Erfindung werden folgende Schritte ausgeführt:

1. Zurücksetzen der Schaltelemente durch ein Eingangssignal am jeweiligen Eingang der Schaltelemente, welches die Schaltelemente den Zustand „Ungültig" überführt.
2. Änderung des Eingangssignals am jeweiligen Eingang der Schaltelemente, welches die Schaltelemente in den Zustand „Speichern" überführt, und Abwarten einer Relaxationszeit, z. B. 300 Zyklen (clock cycles). Die Schaltelemente nehmen in der Relaxationszeit einen stabilen Zustand an.
3. Auslesen der Ausgänge der Schaltelemente. Dabei kann durch Vergleich der Ausgänge eines Schaltelements miteinander festgestellt werde, ob das Schaltelement schon einen stabilen Zustand erreicht hat, da dann Q = not $\overline{Q}$.

[0043] Die **Fig.** 3 bis **Fig.** 5 zeigen Ergebnisse von 1000 bzw. 100.000 Einzelmessungen. In **Fig.** 3 und **Fig.** 4 werden Einzelmessungen für ein und dasselbe CycloneIV FPGA mit 265 RS-Latches dargestellt. **Fig.** 5 vergleicht Messungen für zwei unterschiedliche CycloneIV FPGA mit 265 RS-Latches. Erkennbar sind die unterschiedlichen CycloneIV FPGA anhand der Messungen unterscheidbar.

[0044] Eine Unterscheidung zweier gleicher Vorrichtungen kann beispielsweise anhand von einem Vektor, der für jede der Vorrichtungen anhand von wiederholten Messungen bestimmt wird, vorgenommen werden. Jedes Bit des Vektors entspricht einem Schaltelement. Beispielsweise werden Bits des Vektors, die Schaltelementen entsprechen, die in den Messungen stets ein Signal am Ausgang aufgewiesen haben, gleich EINS gesetzt. Bits des Vektors, die Schaltelementen entsprechend, die in den Messungen stets kein Signal am Ausgang aufgewiesen haben, werden gleich NULL gesetzt. Und Bits, die Schaltelementen entsprechend, die in den Messungen manchmal ein und manchmal kein Signal am Ausgang aufgewiesen haben, werden gleich X gesetzt. Unterscheiden sich zwei Vektoren nun mindestens in einer Mindestmenge von Bits, beispielsweise 10% der Bits, so können die Vektoren als unterschiedlich klassifiziert werden. Entsprechend kann geschlossen werden, dass die Messungen für die beiden Vektoren nicht an derselben Vorrichtung durchgeführt wurden. Es kann auch anhand der Anzahl unterschiedlicher Bits eine Wahrscheinlichkeit dafür bestimmt werden, dass die Vektoren aus Messungen an derselben Vorrichtung bzw. aus Messungen an zwei gleichen Vorrichtungen stammen.

Patentansprüche

1. Vorrichtung (**400**) umfassend logische Elemente (**100**, **100'**), von denen mindestens zwei zu einem Schaltelement (**200**) verschaltet sind, wobei ein Antwortverhalten eines Ausgangssignals des Schaltelements (**200**) auf zumindest einen Zustandsübergang theoretisch unvorhersagbar ist, **dadurch gekennzeichnet,** dass durch ein tatsächliches Antwortverhalten des Ausgangssignals auf den zumindest einen Zustandsübergang eine physikalisch nichtnachbildbare Funktion für eine Zertifizierung der Echtheit der Vorrichtung (**400**) definiert ist.

2. Vorrichtung nach Anspruch 1, wobei die logischen Elemente (**100**) des Ausgangssignals bezüglich eines weiteren logischen Elements (**100'**), von dem ein Kontrolldraht, über den ein Zustandsübergangssignal an die logischen Elemente (**100**) des Schaltelements (**200**) geliefert werden kann, ausgeht, symmetrisch angeordnet ist.

3. Vorrichtung nach Anspruch 1 oder 2, wobei die logischen Elemente (**100**) des Schaltelements (**200**) so bezüglich des weiteren logischen Elements (**100'**) angeordnet sind, dass eine Zeitverzögerung, mit der das

Zustandsübergangssignal eines der logischen Elemente (**100**) des Schaltelements (**200**) gegenüber einem anderen der logischen Elemente (**100**) des Schaltelements (**200**) erreicht, geringstmöglich ist.

4. Vorrichtung nach einem der vorangehenden Ansprüche, wobei die logischen Elements der Vorrichtung (**400**) in Reihen und Spalten angeordnet sind und wobei genau zwei logische Elements zu einem Schaltelement verschaltet sind, die entweder in einer selben Spalte und unterschiedlichen Reihen oder in einer selben Reihe und unterschiedlichen Spalten angeordnet sind, wobei sich zwischen den unterschiedlichen Reihen bzw. Spalten mindestens eine weitere Reihe bzw. mindestens eine weitere Spalte befindet.

5. Vorrichtung nach Anspruch 4, wobei sich das weitere logische Element (**100'**) in einer von den unterschiedlichen Reihen gleichweit beabstandeten mittleren Reihe bzw. in einer von den unterschiedlichen Spalten gleichweit beabstandeten mittleren Spalte befindet.

6. Vorrichtung nach einem der vorangehenden Ansprüche, umfassend weitere, zu weiteren Schaltelementen verschaltete logischer Elemente, wobei durch tatsächliche Antwortverhalten von Ausgangssignalen der weiteren Schaltelemente auf den zumindest einen Zustandsübergang weitere physikalisch nichtnachbildbare Funktionen für die Zertifizierung der Echtheit definiert sind.

7. Vorrichtung nach einem der vorangehenden Ansprüche, weiterhin umfassend einen Soft-Core Prozessor (**300**), der eine Schnittstelle zwischen der physikalisch nichtnachbildbaren Funktion und einem Host-Computer bereitstellt.

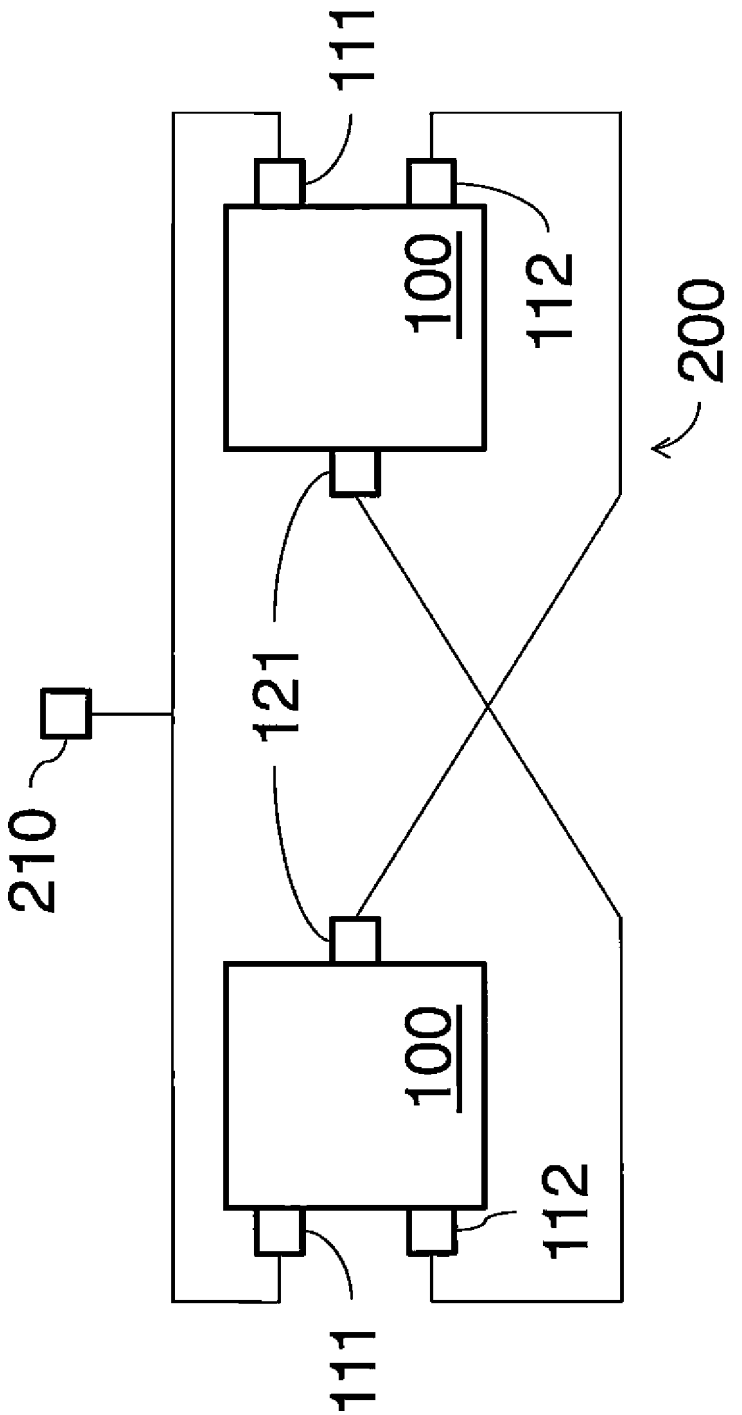
8. Vorrichtung nach Anspruch 7, wobei der Soft-Core Prozessor (**300**) auf einen kleinen Fußabdruck hin optimiert ist und keine Verzweigungsvorhersage, keinen zusätzlichen Pufferspeicher oder keinen Vervielfacher umfasst.

9. Vorrichtung nach einem der vorangehenden Ansprüche, wobei das tatsächliche Antwortverhalten in „stabile Nullantwort”, „stabile Einsantwort” und „unstabile Antwort” klassifiziert ist.

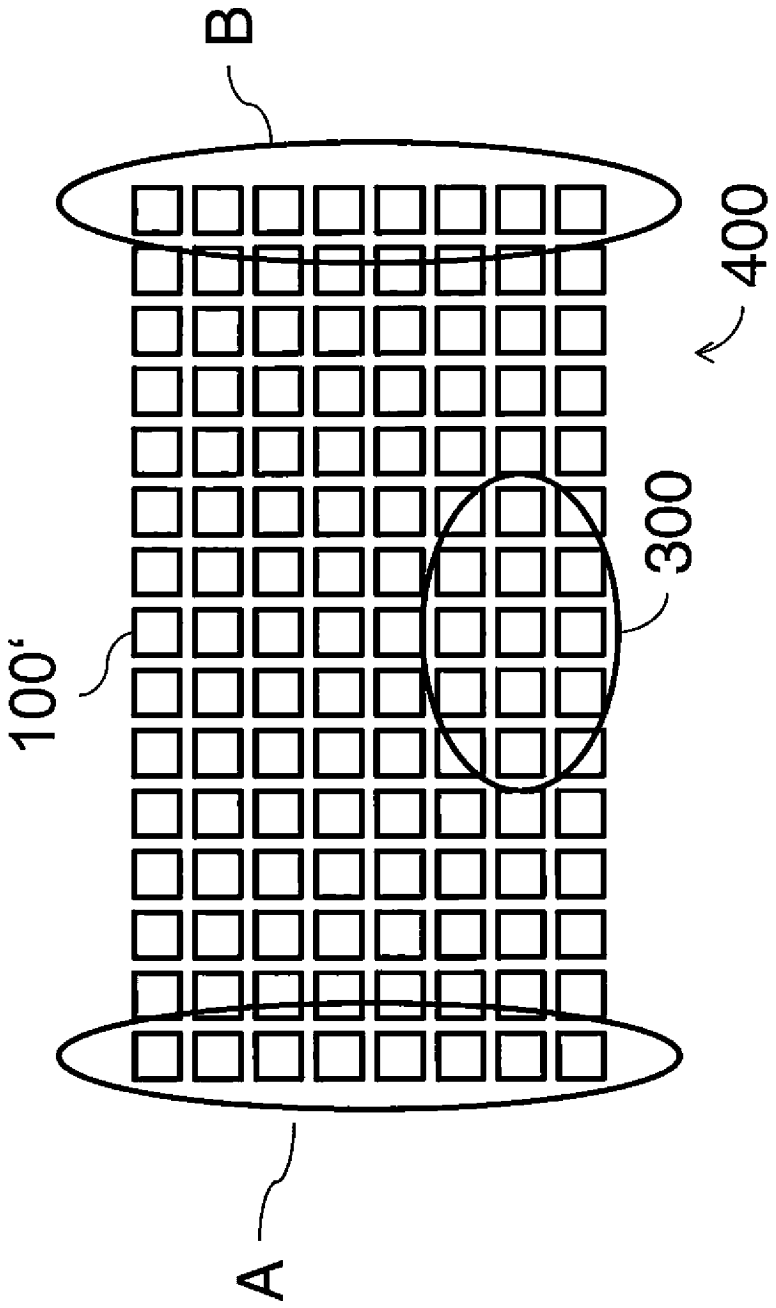
10. Vorrichtung nach einem der vorangehenden Ansprüche, wobei das Schaltelement ein Flipflop ist.

Es folgen 5 Seiten Zeichnungen

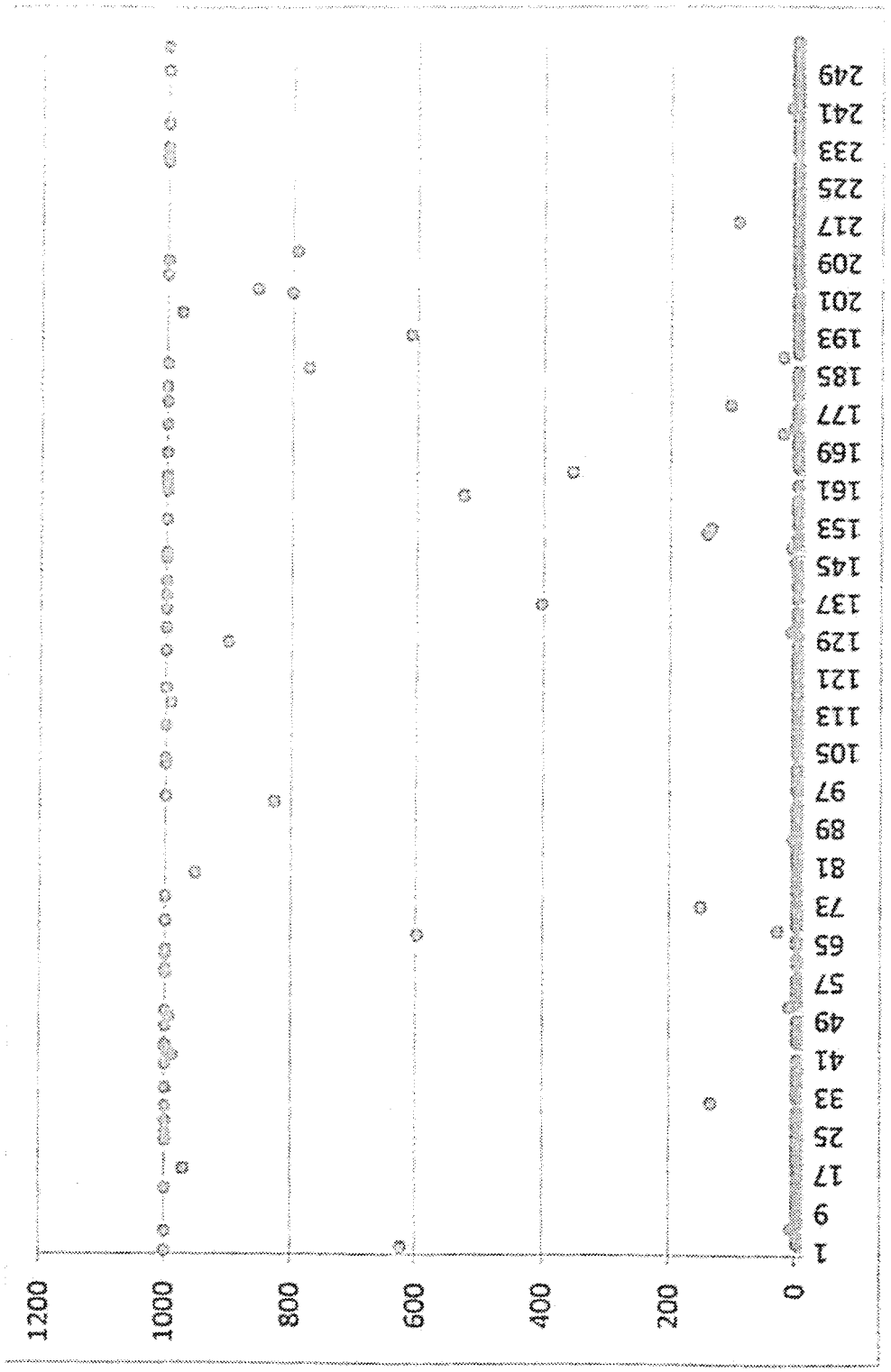
Anhängende Zeichnungen



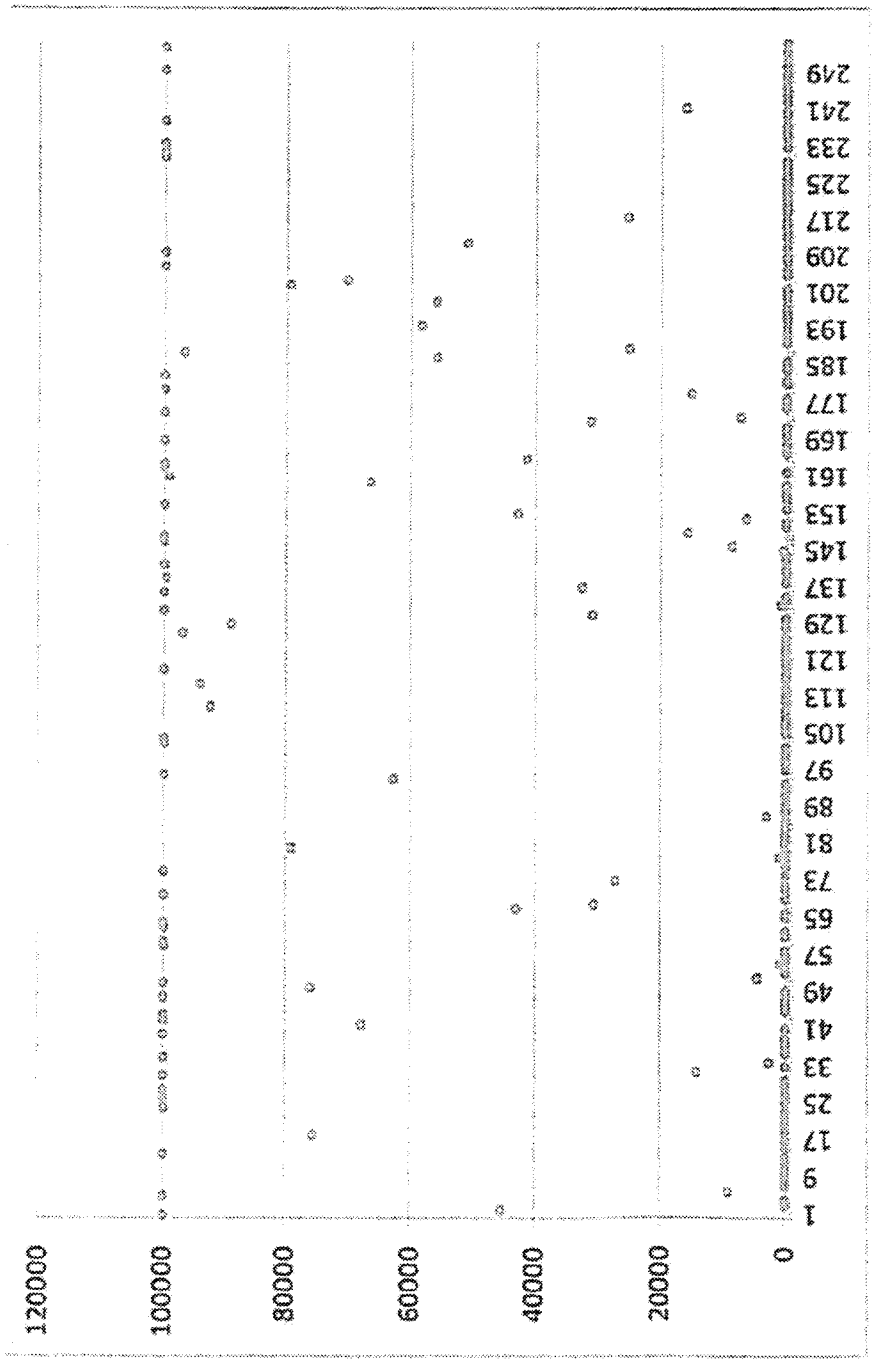
Figur 1



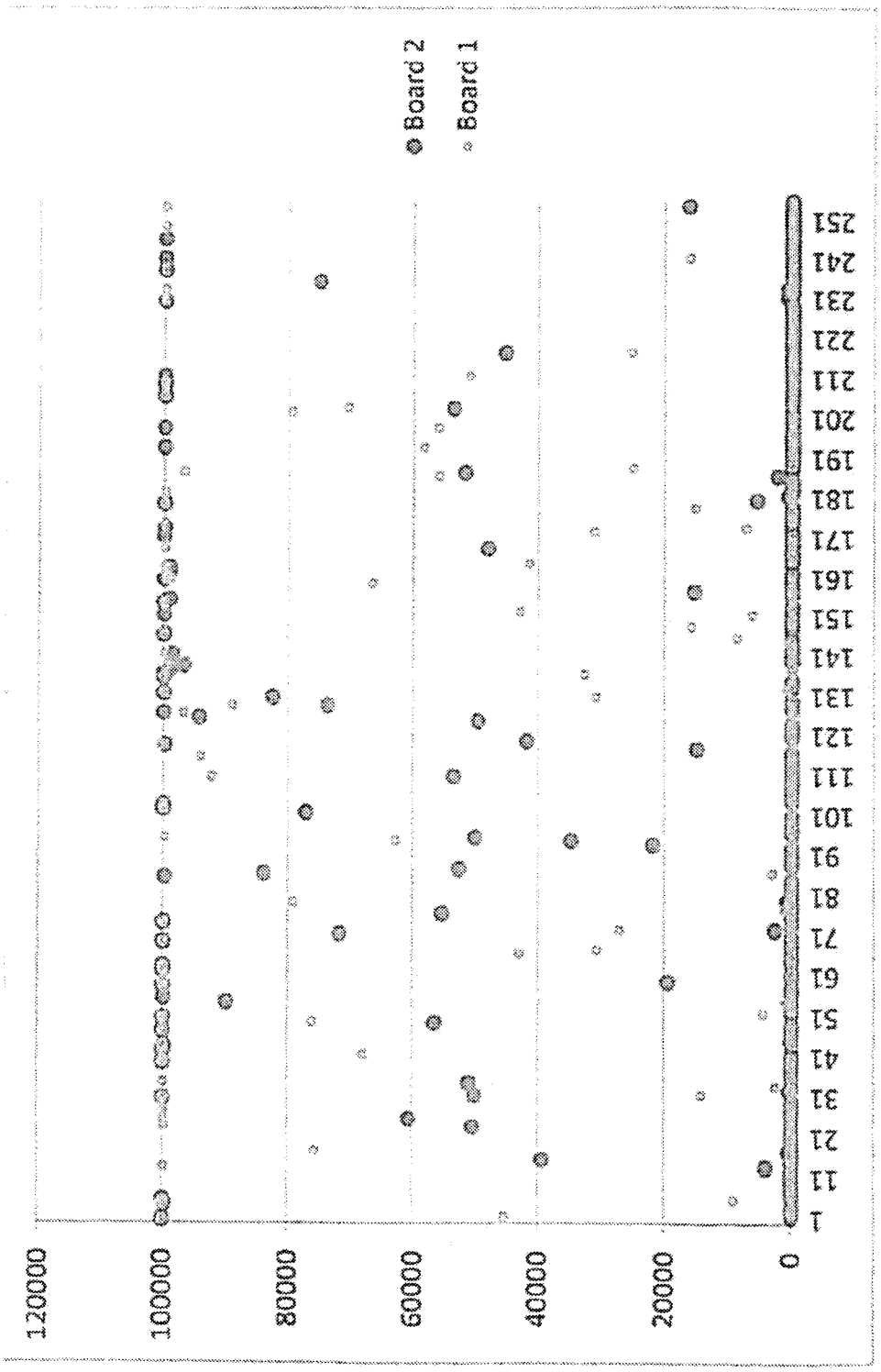
Figur 2


1200
1000
800
600
400
200
0
1
9
17
25
33
41
49
57
65
73
81
89
97
105
113
121
129
137
145
153
161
169
177
185
193
201
209
217
225
233
241
249

Figur 3


120000
100000
80000
60000
40000
20000
0
1
9
17
25
33
41
49
57
65
73
81
89
97
105
113
121
129
137
145
153
161
169
177
185
193
201
209
217
225
233
241
249

Figur 4


Board 2
Board 1
120000
100000
80000
60000
40000
20000
0
1
11
21
31
41
51
61
71
81
91
101
111
121
131
141
151
161
171
181
191
201
211
221
231
241
251

Figur 5