



(10) **DE 10 2016 204 055 B4** 2019.04.04

(12) **Patentschrift**

(21) Aktenzeichen: **10 2016 204 055.3**
 (22) Anmeldetag: **11.03.2016**
 (43) Offenlegungstag: **14.09.2017**
 (45) Veröffentlichungstag
 der Patenterteilung: **04.04.2019**

(51) Int Cl.: **G06F 21/73 (2013.01)**
H03M 1/12 (2006.01)
H03M 1/66 (2006.01)
H03M 3/00 (2006.01)

Innerhalb von neun Monaten nach Veröffentlichung der Patenterteilung kann nach § 59 Patentgesetz gegen das Patent Einspruch erhoben werden. Der Einspruch ist schriftlich zu erklären und zu begründen. Innerhalb der Einspruchsfrist ist eine Einspruchsgebühr in Höhe von 200 Euro zu entrichten (§ 6 Patentkostengesetz in Verbindung mit der Anlage zu § 2 Abs. 1 Patentkostengesetz).

(73) Patentinhaber:
Universität Ulm, 89081 Ulm, DE

(74) Vertreter:
**Pfenning, Meinig & Partner mbB Patentanwälte,
 10719 Berlin, DE**

(72) Erfinder:
**Herkle, Andreas, 89081 Ulm, DE; Ortmanns,
 Maurits, Prof. Dr.-Ing., 89075 Ulm, DE; Becker,
 Joachim, Dr.-Ing., 89179 Beimerstetten, DE**

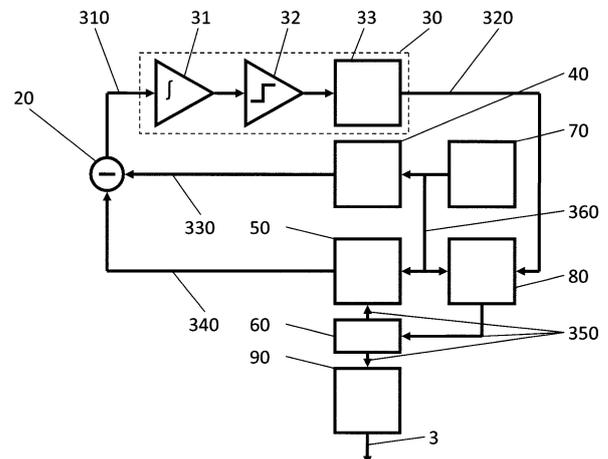
(56) Ermittelter Stand der Technik:

DE	199 40 341	A1
US	8 850 281	B2
US	2012 / 0 321 077	A1
US	2014 / 0 108 786	A1
US	2015 / 0 195 088	A1
US	5 612 729	A

**T. Addabbo, A. Fort, M. Di Marco, L. Pancioni
 and V. Vignoli, "Physically Unclonable Functions
 Derived From Cellular Neural Networks," in IEEE
 Transactions on Circuits and Systems I: Regular
 Papers, vol. 60, no. 12, pp. 3205-3214, Dec. 2013.**

(54) Bezeichnung: **Verfahren und Vorrichtung zur Erzeugung einer digitalen Signatur**

(57) Zusammenfassung: Gemäß einiger Ausführungsformen weist eine Vorrichtung zur Erzeugung einer digitalen Signatur einen ersten D/A-Wandler auf, der ausgebildet ist, eine Sequenz digitaler Daten zu empfangen und die Sequenz digitaler Daten in ein erstes analoges Signal zu wandeln, sowie einen zweiten D/A-Wandler, der ausgebildet ist, eine Sequenz digitaler Daten und digitale Korrekturdaten zu empfangen und die Sequenz digitaler Daten in Abhängigkeit von den digitalen Korrekturdaten in ein zweites analoges Signal zu wandeln, wobei das erste analoge Signal und das zweite analoge Signal einem Knoten zugeführt werden, der ausgebildet ist, die analogen Signale zu kombinieren und an den Eingang eines A/D-Wandlers weiterzuleiten, der die kombinierten analogen Signale in eine Sequenz digitaler Ausgangsdaten wandelt. Die Vorrichtung weist weiterhin eine Korrekturdaten-Erzeugungseinheit auf, die ausgebildet ist, mehr als eine Sequenz digitaler Daten zu empfangen. Der erste D/A-Wandler, der zweite D/A-Wandler und die Korrekturdaten-Erzeugungseinheit sind derart angeordnet, dass diesen eine Testsequenz digitaler Daten zuführbar ist. Die Korrekturdaten-Erzeugungseinheit ist ferner derart angeordnet, dass dieser die Sequenz digitaler Ausgangsdaten des A/D-Wandlers zuführbar ist, wobei die Korrekturdaten-Erzeugungseinheit derart eingerichtet ist, dass aus der Testsequenz digitaler Daten und der Sequenz digitaler Ausgangsdaten des A/D-Wandlers digitale Korrekturdaten generiert werden, wobei die digitalen Korrekturdaten eine digitale Signatur bilden.



Beschreibung

[0001] Die Erfindung betrifft eine Vorrichtung und ein Verfahren zur Erzeugung einer digitalen Signatur.

Hintergrund

[0002] Digitale Signaturen finden beispielsweise Verwendung als Identifikationsnummern für die Absicherung von elektronischen Bausteinen oder Schaltungen oder auch von Software. Weiterhin werden digitale Signaturen in kryptographischen Anwendungen verwendet.

[0003] Eine digitale Signatur sollte zumindest individuell und nicht duplizierbar sein. Da eine gespeicherte digitale Signatur leicht duplizierbar oder veränderbar ist, wird häufig die digitale Signatur erst auf eine Anforderung hin generiert, wobei das Verfahren zur Generierung der digitalen Signatur derart ausgestaltet ist, dass die digitale Signatur ohne Kenntnis des Verfahrens zur Generierung oder der Verfahrensparameter zur Generierung nicht dupliziert werden kann.

Zusammenfassung

[0004] Eine Möglichkeit zur Erzeugung von digitalen Signaturen ist die Anwendung von so genannten physikalisch unklonbaren Funktionen (PUF). Eine PUF ist ausgebildet, auf einen Stimulus hin eine oder mehrere Antworten zu generieren, wobei die Antworten auf den Stimulus reproduzierbar und individuell sind, die PUF selbst aber nicht duplizierbar ist. Der Stimulus und die Antwort können beispielsweise analoge oder digitale Daten oder Signale sein. So genannte schwache PUF generieren lediglich eine begrenzte Anzahl von Antworten oder auch nur eine einzige Antwort. Bekannte PUF basieren auf der Messung und Auswertung von Fertigungstoleranzen eines Bauteils, wobei die jeweiligen PUF durch die Fertigungstoleranzen des Bauteils einen zufälligen Charakter haben, eindeutig reproduzierbar sind, individuell für das Bauteil sind und sich nicht vorhersagen lassen. Damit sind PUF geeignet, eine digitale Signatur zu bilden.

[0005] Aus der US 8,938,792 B2 sind verschiedene Verfahren und Vorrichtungen zur Bildung einer PUF bekannt.

[0006] Eine mögliche Ausführungsform basiert auf Ringoszillatoren, wobei die Schwingungsfrequenzen der Ringoszillatoren durch die Fertigungstoleranzen zufällig, aber reproduzierbar sind. Die Frequenzverhältnisse verschiedener Ringoszillatoren zueinander werden mit einer Auswerteschaltung bestimmt um daraus die PUF zu bilden. Nachteilig ist dabei die Abhängigkeit der Schwingungsfrequenzen von der Umgebungstemperatur, die entweder zusätzlichen Auf-

wand zur Temperaturkompensation erfordert oder die Nutzbarkeit auf einen begrenzten Temperaturbereich einschränkt. Weiterhin ist zusätzlicher Schaltungsaufwand für die Auswerteschaltung erforderlich.

[0007] Eine weitere mögliche Ausführungsform einer PUF basiert auf SRAM Speicherzellen, deren logischer Zustand nach dem Einschalten allein durch die Fertigungstoleranzen der Speicherzellen bestimmt ist. Die logischen Zustände für bestimmte SRAM Speicherzellen werden mit einer Auswerteschaltung bestimmt und bilden die PUF. Nachteilig ist hier, dass die SRAM Speicherzellen nicht für andere Zwecke nutzbar sind und zusätzlicher Schaltungsaufwand für die Auswerteschaltung erforderlich ist.

[0008] Die Offenlegungsschrift DE 199 40 341 A1 beschreibt ein Signaturverfahren zum Schutz von Daten, bei dem ein privater oder geheimer Signaturschlüssel mit Daten kodiert beziehungsweise verschlüsselt wird, die aus einem biometrischen Merkmal des Besitzers des geheimen Schlüssels gewonnen werden. Die veröffentlichte Patentanmeldung US 2012/0321077 A1 offenbart ein kryptographisches Kommunikationssystem bestehend aus zwei Geräten, wobei das erste Gerät einen gemeinsamen Schlüssel mittels einer physikalisch unklonbaren Funktion generiert, den gemeinsamen Schlüssel mit dem öffentlichen Schlüssel des zweiten Gerätes verschlüsselt und an das zweite Gerät übermittelt. Die veröffentlichte Patentanmeldung US 2014/0108786 A1 beschreibt die Verwendung einer physikalisch unklonbaren Funktion zur Bereitstellung eines manipulationssicheren Halbleitermoduls.

[0009] Der Erfindung liegt damit die Aufgabe zugrunde, ein Verfahren und eine Vorrichtung zur Erzeugung einer digitalen Signatur zu schaffen, die diese Nachteile verringert.

[0010] Erfindungsgemäß wird die Aufgabe durch eine Vorrichtung und ein Verfahren mit den Merkmalen der unabhängigen Patentansprüche gelöst. Zweckmäßige Ausgestaltungen sind Gegenstand der Unteransprüche.

[0011] Das erfindungsgemäße Verfahren erzeugt eine digitale Signatur auf Basis von Korrekturdaten, die herstellungsbedingte Abweichungen von Komponenten einer analogen elektronischen Schaltung korrigieren. Die Nutzung der Korrekturdaten sowohl für die Korrektur der Schaltungskomponenten als auch für die Bildung der digitalen Signatur minimiert den zusätzlichen Hardwareaufwand für die Bildung der digitalen Signatur mit einer elektronischen Schaltung, da die erforderlichen Komponenten in der Schaltung bereits vorhanden sind. Die Schaltungskomponenten bleiben weiterhin bestimmungsgemäß nutzbar. Weiterhin sind die Korrekturdaten im Ausgangssignal der elektronischen Schaltung nicht nachweisbar. Da die

zu korrigierenden Abweichungen erst bei der Herstellung auftreten, die Korrekturdaten erst durch die Schaltung selbst erzeugt werden und herstellungsbedingte Abweichungen mehrerer verschiedener Komponenten in die Korrekturdaten eingehen, ist die Erzeugung der digitalen Signatur selbst mit Kenntnis der elektronischen Schaltung und ihrer Komponenten nicht nachvollziehbar. Die Korrekturdaten in Teilen oder ihrer Gesamtheit bilden eine PUF, aus der eine digitale Signatur generiert wird.

[0012] Digitale Korrekturdaten werden beispielsweise in Analog-Digital-Wandlern (A/D-Wandler) und Digital-Analog-Wandlern (D/A-Wandler) verwendet, um deren herstellungsbedingte Abweichungen vom idealen Ausgangssignal zu kompensieren. Dies betrifft insbesondere, aber nicht ausschließlich, die Verschiebung (Offset), die Verstärkung (Gain) und die Linearität der zu erzeugenden Ausgangskurve.

[0013] Eine weitere beispielhafte Anwendung von digitalen Korrekturdaten findet sich in programmierbaren Phasenschiebern, die beispielsweise bei der Linearisierung von Transkonduktanzverstärkern Anwendung finden. Hierbei werden verschiedene Signalpfade dadurch zeitlich angeglichen, dass jeder Signalpfad einen programmierbaren RC-Phasenschieber aufweist, dessen Phasenverschiebung über den Wert des Widerstands und/oder der Kapazität variabel eingestellt werden kann.

[0014] Eine weitere beispielhafte Anwendung von digitalen Korrekturdaten findet sich in In-Phase-&-Quadratur-Empfängern (I/Q-Receiver). Um die Auswirkungen von herstellungsbedingten Abweichungen in deren grundlegenden Schaltungsteilen zu verringern, wird häufig ein digitaler Signalprozessor (DSP) verwendet. Während einer Initialisierungsphase werden Verstärkungs- und Phasenungenauigkeiten gemessen und daraus digitale Korrekturwerte erzeugt. Diese werden dann verwendet, um analoge Korrekturschaltungen zu steuern, welche die grundlegenden Schaltungsteile linearisieren um Nichtidealitäten zwischen Gesamteingang- und Ausgang zu eliminieren.

[0015] Die vorgehend genannten A/D-Wandler, D/A-Wandler, programmierbaren Phasenschieber oder I/Q Receiver sind als Beispiele für die vorgehend genannte und auch in **Fig. 6** gezeigte analoge elektronische Schaltung zu verstehen.

[0016] Die Wirkung von Korrekturdaten wird nachfolgend am Beispiel einer D/A-Wandlung mit digitalen Korrekturdaten kurz erläutert.

[0017] Digitale Korrekturdaten können beispielsweise eine D/A-Wandlung derart beeinflussen, dass die D/A-Wandlung ein abweichendes Ergebnis anstelle des ursprünglichen Ergebnisses ohne Einfluss der digitalen Korrekturdaten liefert. Die digitalen Korrektur-

daten können entweder die D/A-Wandlung der Daten über den gesamten Wertebereich der Eingangsdaten gleichermaßen beeinflussen oder auch nur bestimmte Eingangswerte oder Eingangswertebereiche beeinflussen. Die digitalen Korrekturdaten werden durch einen oder mehrere digitale Korrekturwerte repräsentiert, die beispielsweise durch eine bestimmte Anzahl von Bits dargestellt werden können. Der Wert eines digitalen Korrekturwertes ist das Maß für die durch den Korrekturwert verursachte Abweichung des Ausgangssignals des D/A-Wandlers. Empfängt ein entsprechend ausgestalteter D/A-Wandler einen digitalen Korrekturwert für den gesamten Eingangswertebereich mit einem Wert, dem eine Korrektur des Ausgangssignals von +0,1 Volt zugeordnet ist, so korrigiert dieser D/A-Wandler das ursprüngliche Ausgangssignal um +0,1 Volt.

[0018] Korrekturdaten für eine elektronische Schaltung können mit einer Korrekturwert-Erzeugungseinheit bestimmt werden. Der Korrekturwert-Erzeugungseinheit werden beispielsweise ein Eingangssignal der Schaltung, für die Korrekturwerte zu erzeugen sind, das Ausgangssignal der Schaltung und gegebenenfalls ein Referenzsignal zugeführt, wobei das Referenzsignal auch in der Korrekturwert-Erzeugungseinheit generiert werden kann. Die Korrekturwert-Erzeugungseinheit generiert Korrekturwerte für die Schaltung, die ein Maß des Verhältnisses des Eingangssignals zum Ausgangssignal sind und gegebenenfalls ein Verhältnis des Ausgangssignals zum Referenzsignal mit einbeziehen. Das Generieren der Korrekturdaten kann auf vielfältige Art und Weise erfolgen, beispielsweise durch Vergleich der Signale, Summenbildung, Differenzbildung, Gewichtung, Korrelation und dergleichen. Die vorgehend genannten Eingangssignale, Ausgangssignale, Referenzsignale und Korrekturdaten können dabei sowohl analoger oder digitaler Art sein. Die genannten Korrekturdaten können durch einen einzelnen Korrekturwert gebildet werden oder auch eine Vielzahl von Korrekturwerten umfassen, die in Ihrer Gesamtheit Korrekturdaten bilden.

[0019] Eine Ausführungsform umfasst eine Vorrichtung zur Erzeugung einer digitalen Signatur eine analoge Schaltung, die bedingt durch Herstellungstoleranzen, eindeutige Nichtidealitäten aufweist und eine Korrekturdaten-Erzeugungseinheit, die ausgebildet ist, digitale Korrekturdaten, die herstellungsbedingte Abweichungen von Komponenten der analogen Schaltung korrigieren, zu generieren; wobei die analoge Schaltung ausgebildet ist, mittels der digitalen Korrekturdaten die analogen Nicht-idealitäten am Ausgang zu minimieren und die digitale Signatur auf Basis der digitalen Korrekturdaten (**606**) erzeugt wird.

[0020] Eine Ausführungsform einer Vorrichtung zur Erzeugung einer digitalen Signatur weist einen ersten D/A-Wandler auf, der ausgebildet ist, eine Sequenz

digitaler Daten zu empfangen und die Sequenz digitaler Daten in ein erstes analoges Signal zu wandeln, sowie einen zweiten D/A-Wandler, der ausgebildet ist, eine Sequenz digitaler Daten und digitale Korrekturdaten zu empfangen und die Sequenz digitaler Daten in Abhängigkeit von den digitalen Korrekturdaten in ein zweites analoges Signal zu wandeln, wobei das erste analoge Signal und das zweite analoge Signal einem Knoten zugeführt werden, der ausgebildet ist, die analogen Signale zu kombinieren und an den Eingang eines A/D-Wandlers weiterzuleiten, der die kombinierten analogen Signale in eine Sequenz digitaler Ausgangsdaten wandelt. Die Vorrichtung weist weiterhin eine Korrekturdaten-Erzeugungseinheit auf, die ausgebildet ist, mehr als eine Sequenz digitaler Daten zu empfangen. Der erste D/A-Wandler, der zweite D/A-Wandler und die Korrekturdaten-Erzeugungseinheit sind derart angeordnet, dass diesen eine Testsequenz digitaler Daten zuführbar ist. Die Korrekturdaten-Erzeugungseinheit ist ferner derart angeordnet, dass dieser die Sequenz digitaler Ausgangsdaten des A/D-Wandlers zuführbar ist, wobei die Korrekturdaten-Erzeugungseinheit derart eingerichtet ist, dass aus der Testsequenz digitaler Daten und der Sequenz digitaler Ausgangsdaten des A/D-Wandlers digitale Korrekturdaten generiert werden, wobei die digitalen Korrekturdaten eine digitale Signatur bilden.

[0021] In einer Ausbildungsform weist die Vorrichtung einen Korrekturdatenspeicher auf, der ausgebildet ist, die digitalen Korrekturdaten zu speichern. Dadurch können die digitalen Korrekturdaten während eines Initialisierungsvorganges, beispielsweise nach dem Einschalten erzeugt werden, so dass die Komponenten der Vorrichtung anschließend für andere Anwendungen verfügbar sind.

[0022] In einer weiteren Ausbildungsform weist die Vorrichtung eine Generatoreinheit auf, die ausgebildet ist, eine Testsequenz digitaler Daten zu erzeugen. Dies ermöglicht in vorteilhafter Weise die Erzeugung der Testsequenz digitaler Daten mit der Vorrichtung selbst. Damit ist die Testsequenz digitaler Daten nur für die Vorrichtung selbst verfügbar.

[0023] In einer weiteren Ausbildungsform weist die Vorrichtung eine Kodiereinheit auf, die ausgebildet ist, die digitalen Korrekturdaten zu kodieren.

[0024] Vorzugsweise wird die Kodierung so gewählt, dass die Hamming-Distanz verschiedener, mit gleichartigen Vorrichtungen generierter Signaturen erhalten bleibt und gleichzeitig Fehlerwahrscheinlichkeiten, beispielsweise verursacht durch Bit-Aliasing, reduziert werden, wodurch die Unterscheidbarkeit verschiedener, mit gleichartigen Vorrichtungen generierter Signaturen erhalten bleibt.

[0025] In einer weiteren Ausbildungsform ist die Korrekturdaten-Erzeugungseinheit ausgebildet, die digitalen Korrekturdaten mittels einer Korrelationsoperation zu generieren. Eine digitale Korrelationsoperation, beispielsweise eine digitale Kreuzkorrelation ermöglicht es in vorteilhafter Weise, Sequenzen digitaler Daten zu vergleichen und das Ergebnis des Vergleichs in digitale Korrekturdaten zu überführen.

[0026] In einer weiteren Ausbildungsform ist die Generatoreinheit ausgebildet, eine pseudo-zufällige Datenfolge als Testsequenz digitaler Daten zu generieren. Durch eine pseudo-zufällige Datenfolge wird statistische Unabhängigkeit von dem durch die Schaltung zu wandelnden Eingangssignal erreicht. Das Ergebnis der digitalen Kreuzkorrelation wird damit nicht durch Anteile des Eingangssignals und des Quantisierungsrauschens beeinflusst, so dass das Ergebnis der digitalen Kreuzkorrelation nur die relativen Abweichungen des D/A-Wandlers enthält. Daher kann die Testsequenz in-band platziert werden, wodurch die Präzision der Messung erhöht wird.

[0027] In einer weiteren Ausbildungsform ist der Knoten ausgebildet, eine Differenz der analogen Eingangssignale zu bilden.

[0028] In einer weiteren Ausbildungsform ist der A/D Wandler als Multi-Bit A/D-Wandler ausgebildet, und der erste D/A Wandler sowie der zweite D/A Wandler (50) sind als Multi-Bit D/A-Wandler ausgebildet. Die Verwendung von Multi-Bit Wandlern ermöglicht es insbesondere, eine digitale Signatur größerer Länge zu generieren.

[0029] Ein vorteilhaftes Verfahren erzeugt eine digitale Signatur mittels einer Vorrichtung, die einen ersten D/A-Wandler aufweist, der ausgebildet ist, eine Sequenz digitaler Daten zu empfangen und die Sequenz digitaler Daten in ein erstes analoges Signal zu wandeln und die einen zweiten D/A-Wandler aufweist, der ausgebildet ist, eine Sequenz digitaler Daten und digitale Korrekturdaten zu empfangen und die Sequenz digitaler Daten in Abhängigkeit von den digitalen Korrekturdaten in ein zweites analoges Signal zu wandeln, wobei das erste analoge Signal und das zweite analoge Signal einem Knoten zugeführt werden, der ausgebildet ist, die analogen Signale zu kombinieren und an den Eingang eines A/D-Wandlers weiterzuleiten, der die kombinierten analogen Signale in eine Sequenz digitaler Ausgangsdaten wandelt. Die Vorrichtung weist weiterhin eine Korrekturdaten-Erzeugungseinheit auf, die ausgebildet ist, mehr als eine Sequenz digitaler Daten zu empfangen und daraus digitale Korrekturdaten zu generieren. Das vorteilhafte Verfahren umfasst die Verfahrensschritte:

- Zuführen einer Testsequenz digitaler Daten an den ersten D/A-Wandler, den zweiten D/A-Wandler und die Korrekturdaten-Erzeugungseinheit;
- Zuführen der Sequenz digitaler Ausgangsdaten des A/D-Wandlers an die Korrekturdaten-Erzeugungseinheit;
- Generieren von digitalen Korrekturdaten aus der Testsequenz digitaler Daten und der Sequenz digitaler Ausgangsdaten des A/D-Wandlers;
- Ausgeben der digitalen Korrekturdaten als digitale Signatur.

[0030] In einer Ausbildungsform des Verfahrens werden die digitalen Korrekturdaten in einem Korrekturdatenspeicher gespeichert.

[0031] In einer weiteren Ausbildungsform des Verfahrens werden die digitalen Korrekturdaten vor dem Ausgeben als digitale Signatur kodiert.

[0032] In einer weiteren Ausbildungsform des Verfahrens erfolgt das Generieren der digitalen Korrekturdaten durch eine Korrelationsoperation.

[0033] In einer weiteren Ausbildungsform des Verfahrens wird vor dem Zuführen der Testsequenz digitaler Daten den digitalen Korrekturdaten ein vordefinierter Wert zugewiesen.

[0034] In einer weiteren Ausbildungsform des Verfahrens wird die Testsequenz digitaler Daten durch eine pseudo-zufällige Datenfolge gebildet.

[0035] In einer weiteren Ausbildungsform des Verfahrens sind bei der Vorrichtung der Ausgang des A/D-Wandlers mit den Eingängen des ersten D/A-Wandlers und des zweiten D/A-Wandlers verbunden, so dass der Knoten, der A/D-Wandler, der erste D/A-Wandler und der zweite D/A-Wandler einen Delta-Sigma A/D-Wandler bilden, dessen Eingang mit dem Knoten verbunden ist und dessen Ausgang mit dem Ausgang des A/D-Wandlers verbunden ist, wobei vor dem Zuführen der Testsequenz digitaler Daten an den ersten D/A-Wandler:

- die Verbindungen zwischen dem Eingang und dem Knoten sowie zwischen dem Ausgang und dem Ausgang des A/D-Wandlers geöffnet werden, und
- die Verbindungen zwischen dem Ausgang des A/D-Wandlers und den Eingängen des ersten D/A-Wandlers und des zweiten D/A-Wandlers geöffnet werden.

[0036] Damit kann in vorteilhafter Weise ein A/D-Wandler der beschriebenen Art in die Vorrichtung zur Erzeugung einer digitalen Signatur überführt werden.

[0037] In einer weiteren Ausführungsform umfasst ein Verfahren zur Erzeugung einer digitalen Signatur eine analoge Schaltung, die bedingt durch Herstellungstoleranzen, eindeutige Nichtidealitäten aufweist und eine Korrekturdaten-Erzeugungseinheit, die ausgebildet ist, digitale Korrekturdaten, die herstellungsbedingte Abweichungen von Komponenten der analogen Schaltung korrigieren, zu generieren; wobei die analoge Schaltung ausgebildet ist, mittels der digitalen Korrekturdaten die analogen Nicht-idealitäten am Ausgang zu minimieren, wobei die digitale Signatur auf Basis der digitalen Korrekturdaten erzeugt wird.

Figurenliste

Fig. 1 ist ein Blockschaltbild eines Delta-Sigma Analog-DigitalWandlers,

Fig. 2 ist ein Blockschaltbild eines Delta-Sigma Analog-DigitalWandlers gemäß einiger Ausführungsformen,

Fig. 3 ist ein Blockschaltbild einer vorteilhaften Vorrichtung,

Fig. 4 ist eine Darstellung von differentiellen Nichtlinearitäten (DNL) und von integralen Nichtlinearitäten (INL),

Fig. 5 ist eine Darstellung des Ablaufes zur Bestimmung einer physikalisch unklonbaren Funktion (PUF),

Fig. 6 ist ein Blockschaltbild einer erfindungsgemäßen Vorrichtung.

Beschreibung

[0038] Die Erfindung wird nachstehend anhand von Ausführungsbeispielen näher erläutert.

[0039] In mehreren Ausführungsbeispielen nutzt die vorteilhafte Vorrichtung Komponenten eines Sigma-Delta A/D-Wandlers, die in ihrem Zusammenwirken eine analoge Schaltung, wie in **Fig. 6** gezeigt, bilden. Ein Sigma-Delta A/D-Wandler ist in **Fig. 1** dargestellt. Der Eingang **1** des Sigma-Delta A/D-Wandlers empfängt ein analoges Eingangssignal **100**, welches dem Knoten **20** zugeführt wird. Das Ausgangssignal **310** des Knoten **20** wird von einem A/D-Wandler **30** in eine Sequenz digitaler Daten **320** gewandelt, die am Ausgang **2** als digitales Ausgangssignal **200** zur Verfügung stehen. Der A/D-Wandler **30** umfasst eine Reihenschaltung aus einem Integrator **31**, einem Komparator **32** und einem taktgesteuerten Speicher **33**, wobei die Zuführung des Taktsignals an den taktgesteuerten Speicher **33** in **Fig. 1** nicht dargestellt ist. Somit ist der A/D-Wandler **30** ausgebildet, ein Taktsignal zu empfangen, dass die Bitrate der vom A/Wandler **30** erzeugten Sequenz digitaler Daten **320** vorgibt. Ein Rückführungsweig, umfassend einen D/A-Wandler **40** und den Knoten **20**, führt die Sequenz digitaler Daten **320** vom Ausgang des A/D-Wandlers

30 als analoges Rückführungssignal **330** zurück auf den Knoten **20**, wobei der Knoten **20** eine Differenz des analogen Eingangssignals **100** und des analogen Rückführungssignals **330** bildet, die dann dem A/D-Wandler **30** zugeführt wird. In **Fig. 1** nicht dargestellt ist, dass das Taktsignal des A/D-Wandlers **30** ebenfalls dem D/A-Wandler **40** zugeführt wird, um eine der Bitrate angepasste D/A-Wandlung der dem D/A-Wandler **40** zugeführten Sequenz digitaler Daten **320** zu gewährleisten.

[0040] In einer Ausführungsform des Delta-Sigma A/D-Wandlers beträgt die Verarbeitungsbreite des Komparators **32**, des taktgesteuerten Speichers **33** und des D/A-Wandlers **40** genau 1 Bit, das heißt die Sequenz digitaler Daten **320** am Ausgang des A/D-Wandlers **30** und am Eingang des D/A-Wandlers **40** ist eine 1-Bit breite Sequenz. Wird die Verarbeitungsbreite des Komparator **32**, des taktgesteuerten Speichers **33** und des D/A-Wandlers **40** auf mehrere Bit vergrößert, dann werden diese auch als Multi-Bit Komparator, Multi-Bit taktgesteuerter Speicher und Multi-Bit D/A-Wandler bezeichnet. Gleichermaßen wird dann der von Integrator **31**, Komparator **32** und taktgesteuerten Speicher **33** gebildete A/D-Wandler **30** als Multi-Bit A/D-Wandler bezeichnet. Beträgt die Verarbeitungsbreite des A/D-Wandlers **30** und des D/A-Wandlers **40** beispielsweise 4 Bit, so besteht die Sequenz digitaler Daten **320** am Ausgang des A/D-Wandlers **30** und am Eingang des D/A-Wandlers **40** aus Wörtern mit einer Breite von 4 Bit.

[0041] **Fig. 2** zeigt eine weitere Ausführungsform eines Delta-Sigma A/D-Wandlers.

[0042] Zusätzlich zu den bereits in **Fig. 1** dargestellten Komponenten weist der Sigma-Delta A/D-Wandler gemäß **Fig. 2** einen zweiten A/D-Wandler **50** und optional einen Korrekturdatenspeicher **60** auf. Der zweite A/D-Wandler **50** ist ausgebildet, digitale Korrekturdaten **350** zu empfangen und die seinem Eingang zugeführte Sequenz digitaler Daten **320** in Abhängigkeit von den digitalen Korrekturdaten in ein zweites analoges Signal zu wandeln. Das zweite analoge Signal wird über einen zweiten Rückführungszweig dem Knoten **20** als zweites analoges Rückführungssignal **340** zugeführt, wobei der Knoten **20** das analoge Eingangssignal **100**, das erste analoge Rückführungssignal **330** des ersten D/A-Wandlers **40** und das zweite analoge Rückführungssignal **340** des zweiten D/A-Wandlers **50** kombiniert und dann dem A/D-Wandler **30** zugeführt. Die Kombination der analogen Signale **100**, **330** und **340** im Knoten **20** kann beispielsweise durch eine Summenbildung, eine Differenzbildung oder eine Kombination von Summen- und Differenzbildung erfolgen.

[0043] Das zweite analoge Rückführungssignal **340** bildet ein Korrektursignal, mit dem herstellungsbedingte Abweichungen des A/D-Wandlers, des ersten

D/A-Wandlers **40** und des zweiten D/A-Wandlers **50** korrigiert werden.

[0044] **Fig. 3** zeigt eine vorteilhafte Vorrichtung. Zusätzlich zu den bereits in **Fig. 1** oder **Fig. 2** dargestellten Komponenten weist die Vorrichtung eine Korrekturdaten-Erzeugungseinheit **80** auf. Abweichend zu **Fig. 3** ist der Ausgang des A/D-Wandlers **30** nicht mit den Eingängen der D/A-Wandler **40** und **50** verbunden. Statt dessen ist der Ausgang des A/D-Wandlers **30** mit einem Eingang der Korrekturdaten-Erzeugungseinheit **80** verbunden. Ein zweiter Eingang der Korrekturdaten-Erzeugungseinheit **80** ist mit den Eingängen der D/A-Wandler **40** und **50** verbunden, so dass die D/A-Wandler **40** und **50** und die Korrekturdaten-Erzeugungseinheit **80** eingerichtet sind, die gleiche Sequenz digitaler Daten zu empfangen. Wie aus **Fig. 3** ersichtlich ist, ist die Vorrichtung nicht mit einem Eingang zum Empfang eines analogen Eingangssignals verbunden. Ebenso ist kein Ausgang für die Ausgabe eines digitalen Ausgangssignals vorhanden. Dadurch wird gewährleistet, dass die von der Vorrichtung generierten Signale innerhalb der Vorrichtung verbleiben und von außerhalb der Vorrichtung nicht zugänglich sind. Der in **Fig. 2** dargestellte Sigma-Delta A/D-Wandler kann in die Vorrichtung gemäß **Fig. 3** überführt werden, indem die Verbindungen zwischen dem Eingang **1** und dem Knoten **20** sowie zwischen dem Ausgang **2** und dem Ausgang des A/D-Wandlers **30** geöffnet werden; die Verbindungen zwischen dem Ausgang des A/D-Wandlers **30** und den Eingängen des ersten D/A-Wandlers **40** und des zweiten D/A-Wandlers **50** geöffnet werden und ein Eingang einer Korrekturdaten-Erzeugungseinheit **80** mit dem Ausgang des A/D-Wandlers **30** verbunden wird und ein weiterer Eingang der Korrekturdaten-Erzeugungseinheit **80** mit den Eingängen der D/A-Wandler **40** und **50** verbunden wird.

[0045] Für die Generierung der digitalen Korrekturdaten wird den Eingängen des ersten D/A-Wandlers **40**, des zweiten D/A-Wandlers **50** und einem Eingang der Korrekturdaten-Erzeugungseinheit **80** eine Testsequenz digitaler Daten **360** zugeführt. Die Testsequenz digitaler Daten **360** kann beispielsweise durch eine pseudo-zufällige Datenfolge gebildet werden. In einer bevorzugten Ausführungsform ist die Testsequenz digitaler Daten **360** mit einem Taktsignal synchronisiert, dass dem A/D-Wandler **30** und den D/A-Wandlern **40** und **50** zugeführt wird. In einem Ausführungsbeispiel wird die Testsequenz digitaler Daten **360** durch eine Generatoreinheit **70** generiert, die ausgebildet ist, eine solche Testsequenz digitaler Daten **360** zu generieren. Die Testsequenz digitaler Daten **360** durchläuft den D/A-Wandler **40** und wird vom D/A-Wandler **40** in ein erstes analoges Signal **330** umgesetzt. Die Testsequenz durchläuft ebenfalls den D/A-Wandler **50** und wird vom D/A-Wandler **50** in ein zweites analoges Signal **340** umgesetzt. Das erste analoge Signal **330** und das zweite analoge Signal

340 werden dem Knoten **20** zugeführt. Der Knoten **20** kombiniert die analogen Signale und führt die kombinierten analogen Signale **310** dem Eingang des A/D-Wandlers **30** zu. Die Kombination **310** der analogen Signale kann durch eine Addition, eine Subtraktion, eine Mittelwertbildung oder dergleichen erfolgen. Der A/D-Wandler **30** wandelt die kombinierten analogen Signale **310** in eine Sequenz digitaler Ausgangsdaten **320**. Die Korrekturdaten-Erzeugungseinheit **80** empfängt die Testsequenz digitaler Daten **360** und ebenfalls die vom A/D-Wandler **30** erzeugte Sequenz digitaler Ausgangsdaten **320**. Die Korrekturdaten-Erzeugungseinheit **80** generiert aus der Testsequenz digitaler Daten **360** und der Sequenz digitaler Ausgangsdaten **320** des A/D-Wandlers **30** digitale Korrekturdaten **350**. Auf die Generierung der digitalen Korrekturdaten **350** durch die Korrekturdaten-Erzeugungseinheit **80** wird nachfolgend noch genauer eingegangen. Die digitalen Korrekturdaten **350** werden dem zweiten D/A-Wandler **50** zugeführt. Der zweite D/A-Wandler **50** setzt die seinem Eingang zugeführte Sequenz digitaler Daten **360** in Abhängigkeit von den digitalen Korrekturdaten **350** in das zweite analoge Signal **340** um, so dass die vom A/D-Wandler **30** erzeugte Sequenz digitaler Ausgangsdaten **320** von den digitalen Korrekturdaten **350** beeinflusst wird. In einer Ausführungsform wird den digitalen Korrekturdaten **350** vor dem Zuführen der Testsequenz digitaler Daten ein vordefinierter Wert zugewiesen. In einer weiteren Ausführungsform wird die Testsequenz digitaler Daten **360** so lange zugeführt, bis sich die von der Korrekturdaten-Erzeugungseinheit **80** generierten digitalen Korrekturdaten **350** nicht mehr verändern.

[0046] Die Generierung der digitalen Korrekturdaten **350** durch die Korrekturdaten-Erzeugungseinheit **80** umfasst die Verarbeitung der Testsequenz digitaler Daten **360** und die Verarbeitung der vom A/D-Wandler **30** erzeugten Sequenz digitaler Ausgangsdaten **320**. Da diese Daten sowohl den A/D-Wandler **30** als auch die D/A-Wandler **40** und **50** durchlaufen haben, bewirken die von der Korrekturdaten-Erzeugungseinheit **80** generierten digitalen Korrekturdaten **350** eine Korrektur der herstellungsbedingten Abweichungen sowohl des A/D-Wandlers **30** und der D/A-Wandler **40** und **50**. Dadurch gehen herstellerbedingte Abweichungen von drei verschiedenen Komponenten in die aus den digitalen Korrekturdaten **350** hervorgehende digitale Signatur **3** ein, was die Wahrscheinlichkeit, weiter verringert, dass durch zwei gleichartige Vorrichtungen identische digitale Signaturen generiert werden. Gleichzeitig wird die Duplizierbarkeit der digitalen Signatur weiter erschwert. In einem Ausführungsbeispiel generiert die Korrekturdaten-Erzeugungseinheit **80** die digitalen Korrekturdaten **350** in Abhängigkeit des Ergebnisses des Vergleichs der Testsequenz digitaler Daten **360** und der vom A/D-Wandler **30** erzeugten Sequenz digitaler Ausgangsdaten **320**. In einem weiteren Ausführungsbeispiel führt die Korrekturdaten-Erzeugungseinheit **80** eine

Korrelationsoperation mit der Testsequenz digitaler Daten **360** und der vom A/D-Wandler **30** erzeugten Sequenz digitaler Ausgangsdaten **320** aus und generiert die digitalen Korrekturdaten **350** in Abhängigkeit vom Ergebnis der Korrelation. In einer Ausführungsform ist die Korrelationsoperation eine digitale Kreuzkorrelation.

[0047] Die digitale Kreuzkorrelation liefert für jede der Wandlerstufen einen eindeutigen, charakteristischen Wert, der als einheitsloser Faktor ein Maß der Abweichung der Wandlerstufe zu einer Referenz darstellt.

[0048] Wie vorgehend erwähnt, können in einigen Ausführungsformen der A/D-Wandlers **30** und die D/A-Wandler **40** und **50** als Multi-Bit Wandler ausgeführt sein. In diesen Ausführungsformen umfassen die Wandler mehrere gekoppelte Wandlerstufen. Die herstellungsbedingten Abweichungen einer jeder Wandlerstufe führen zu differentiellen Nichtlinearitäten (DNL). Die differentiellen Nichtlinearitäten bewirken nur kleine Abweichungen der einzelnen Wandlerstufe. Durch die Koppelung der Wandlerstufen summieren sich die differentiellen Nichtlinearitäten zu einer integralen Nichtlinearität (INL).

[0049] Anhand von **Fig. 4** und **Fig. 5b** und **Fig. 5c** sollen nachstehend Ausführungsformen zur Bestimmung der PUF des Systems der **Fig. 3** erläutert werden.

[0050] **Fig. 5a** und **Fig. 5b** erläutern in Verbindung mit **Fig. 4** die Funktion der Korrekturdaten-Erzeugungseinheit **80** aus **Fig. 3**. In **Fig. 4a** sind beispielhaft die differentiellen Nichtlinearitäten DNL **41, 42, 43, 44** der ersten bis vierten Wandlerstufe eines 4-Bit Wandlers dargestellt. **Fig. 4b** zeigt die daraus resultierenden integralen Nichtlinearitäten INL. Die Y-Achse in **Fig. 4a** und **Fig. 4b** zeigt ein Maß der Abweichung jeder Wandlerstufe vom Sollwert. Die in **Fig. 4b** dargestellte INL **41'** der ersten Wandlerstufe entspricht der DNL **41** aus **Fig. 4a**. Die in **Fig. 4b** dargestellte INL **42'** der zweiten Wandlerstufe ist die Summe der in **Fig. 4a** gezeigten DNL **41** und **42** und so weiter. Durch das vorgehend beschriebene Verfahren können in vorteilhafter Weise durch die digitale Kreuzkorrelation einer pseudo-zufälligen Testsequenz die differentiellen Nichtlinearitäten DNL der einzelnen Wandlerstufen bestimmt werden.

[0051] Die in **Fig. 5a** gezeigten Signale der Schaltung werden durch die Testsequenz digitaler Daten **360** und die vom A/D-Wandler **30** erzeugte Sequenz digitaler Ausgangsdaten **320** gebildet. Die Korrekturdaten-Erzeugungseinheit **80** bestimmt eine oder mehrere der vorgehend beschriebenen DNL und bestimmt aus der oder den DNL die digitalen Korrekturdaten **350**. Aus Teilen der digitalen Korrekturdaten **350** oder deren Gesamtheit wird die PUF gebildet.

[0052] Die in **Fig. 5b** gezeigten Signale der Schaltung werden ebenfalls durch die Testsequenz digitaler Daten **360** und die vom A/D-Wandler **30** erzeugte Sequenz digitaler Ausgangsdaten **320** gebildet. Wie in **Fig. 5b** dargestellt, werden zuerst die differentiellen Nichtlinearitäten DNL für die Wandlerstufen bestimmt. Aus den differentiellen Nichtlinearitäten DNL der Wandlerstufen werden mit Kenntnis der Koppelung der Wandlerstufen dann die integralen Nichtlinearitäten INL der Wandlerstufen bestimmt und nachfolgend die digitalen Korrekturdaten **350** generiert, die die integralen Nichtlinearitäten INL aller Wandler kompensieren. Aus Teilen der digitalen Korrekturdaten **350** oder deren Gesamtheit wird die PUF gebildet.

[0053] Die digitalen Korrekturdaten **350** basieren auf den herstellungsbedingten Abweichungen mehrerer Wandlerstufen und sind damit nicht duplizierbar.

[0054] In einer weiteren Ausführungsform werden die digitalen Korrekturdaten **350** vor dem Ausgeben als digitale Signatur **3** kodiert, beispielsweise in der in **Fig. 3** dargestellten Kodiereinheit **90**. Durch eine geeignete Kodierung kann die Wahrscheinlichkeit erhöht werden, dass auch bei einer Vielzahl der in **Fig. 3** dargestellten Vorrichtungen keine identischen Signaturen generiert werden. In vorteilhafter Weise kann die Kodierung mittels einer Gray-Kodierung erfolgen.

[0055] **Fig. 6** zeigt eine Ausführungsform **600** einer Vorrichtung zur Ausführung des Verfahrens. Die Vorrichtung weist eine analoge Schaltung **602** auf. Die analoge Schaltung **602** ist so zu verstehen, dass sie zumindest eine Schaltungskomponente oder Teilschaltung aufweist, die ein analoges Signal generiert und/oder der ein analoges Signal zugeführt wird.

[0056] Die analoge Schaltung **602** kann eine oder mehrere Teilschaltungen aufweisen, die digitale Signale in analoge Signale umsetzen. Die analoge Schaltung **602** kann eine oder mehrere Teilschaltungen aufweisen, die analoge Signale in digitale Signale umsetzen. Die analoge Schaltung **602** kann eine oder mehrere Teilschaltungen aufweisen, die digitale Signale generieren und/oder denen digitale Signale zugeführt werden. Die vorgehend beschriebenen Teilschaltungen können auch miteinander verbunden sein.

[0057] Zumindest eine der vorgehend beschriebenen Teilschaltungen ist mit einem Ausgang **603** der analogen Schaltung **602** verbunden. Zusätzlich kann die analoge Schaltung einen oder mehrere Eingänge **601** aufweisen.

[0058] Die analoge Schaltung **602** weist, bedingt durch Herstellungstoleranzen, eindeutige Nichtidealitäten auf. Diese Nichtidealitäten sind als herstellungs-

bedingte Abweichungen von einem Soll-Verhalten der analogen Schaltung **602** zu verstehen, beispielsweise Abweichungen eines von der analogen Schaltung **602** generierten Signalwertes von einem Sollwert. Sie werden auch als Mismatch bezeichnet.

[0059] Die Vorrichtung weist weiterhin eine mit der analogen Schaltung **602** verbindbare oder verbundene Korrekturdaten-Erzeugungseinheit **605** auf. Der Korrekturdaten-Erzeugungseinheit **605** werden ein oder mehrere Signale **604** der analogen Schaltung **602** zugeführt, die eine oder mehrere Messgrößen von herstellungsbedingten Abweichungen bilden oder aus denen eine oder mehrere Messgrößen herstellungsbedingte Abweichungen ableitbar sind. Die Signale **604** können analoger oder digitaler Natur sein. Der Korrekturdaten-Erzeugungseinheit **605** können auch weitere analoge oder digitale Signale zugeführt werden, beispielsweise Referenzsignale.

[0060] Die Korrekturdaten-Erzeugungseinheit **605** ist ausgebildet, Korrekturdaten **606** zur Reduktion der Nichtidealitäten der analogen Schaltung **602** zu generieren, und diese der analogen Schaltung **602** zuzuführen. Die analoge Schaltung **602** ist ausgebildet, mittels der Korrekturdaten **606** die Nichtlinearitäten am Ausgang zu minimieren. Die Korrekturdaten **606** können durch digitale Korrekturdaten gebildet werden. Teile der Korrekturdaten **606** oder deren Gesamtheit bilden eine digitale Signatur.

[0061] **Fig. 5c** erläutert die Funktion der Korrekturdaten-Erzeugungseinheit **605** aus **Fig. 6**. Die Korrekturdaten-Erzeugungseinheit **605** bestimmt aus einem Signal oder Signalen der analogen Schaltung **602** Korrekturdaten. Aus Teilen der Korrekturdaten oder deren Gesamtheit wird die PUF gebildet.

Patentansprüche

1. Vorrichtung zur Erzeugung einer digitalen Signatur, **gekennzeichnet durch**

- eine analoge Schaltung (602), die bedingt durch Herstellungstoleranzen, eindeutige Nichtidealitäten aufweist;

- eine Korrekturdaten-Erzeugungseinheit (605), die ausgebildet ist, digitale Korrekturdaten (606), die herstellungsbedingte Abweichungen von Komponenten der analogen Schaltung (602) korrigieren, zu generieren; wobei die analoge Schaltung (602) ausgebildet ist, mittels der digitalen Korrekturdaten (606) die analogen Nichtidealitäten am Ausgang (603) zu minimieren und dass die digitale Signatur auf Basis der digitalen Korrekturdaten (606) erzeugt wird.

2. Vorrichtung zur Erzeugung einer digitalen Signatur die aufweist:

- einen ersten D/A-Wandler (40), der ausgebildet ist, eine Sequenz digitaler Daten zu empfangen und die

Sequenz digitaler Daten in ein erstes analoges Signal zu wandeln,
 einen zweiten D/A-Wandler (50), der ausgebildet ist, eine Sequenz digitaler Daten und digitale Korrekturdaten zu empfangen und die Sequenz digitaler Daten in Abhängigkeit von den digitalen Korrekturdaten in ein zweites analoges Signal zu wandeln,
 wobei das erste analoge Signal und das zweite analoge Signal einem Knoten (20) zugeführt werden, der ausgebildet ist, die analogen Signale zu kombinieren und an den Eingang eines A/D-Wandlers (30) weiterzuleiten, der die kombinierten analogen Signale in eine Sequenz digitaler Ausgangsdaten wandelt,
 einer Korrekturdaten-Erzeugungseinheit (80), die ausgebildet ist, mehr als eine Sequenz digitaler Daten zu empfangen,
dadurch gekennzeichnet, dass:
 der erste D/A-Wandler (40), der zweite D/A-Wandler (50) und die Korrekturdaten-Erzeugungseinheit (80) derart angeordnet sind, dass diesen eine Testsequenz digitaler Daten zuführbar ist,
 die Korrekturdaten-Erzeugungseinheit (80) ferner derart angeordnet ist, dass dieser die Sequenz digitaler Ausgangsdaten des A/D-Wandlers (30) zuführbar ist,
 die Korrekturdaten-Erzeugungseinheit (80) derart eingerichtet ist, dass aus der Testsequenz digitaler Daten und der Sequenz digitaler Ausgangsdaten des A/D-Wandlers (30) digitale Korrekturdaten generiert werden, wobei die digitalen Korrekturdaten eine digitale Signatur bilden.

3. Vorrichtung nach Anspruch 2, die einen Korrekturdatenspeicher (60) aufweist, der ausgebildet ist, die digitalen Korrekturdaten zu speichern.

4. Vorrichtung nach einem der Ansprüche 2 oder 3, die eine Generatoreinheit (70) aufweist, die ausgebildet ist, eine Testsequenz digitaler Daten zu erzeugen.

5. Vorrichtung nach einem der Ansprüche 2 bis 4, die eine Kodiereinheit (90) aufweist, die ausgebildet ist die digitalen Signaturdaten zu kodieren.

6. Vorrichtung nach einem der Ansprüche 2 bis 5, **dadurch gekennzeichnet**, dass die Korrekturdaten-Erzeugungseinheit (80) ausgebildet ist, die digitalen Korrekturdaten mittels einer Korrelationsoperation zu generieren.

7. Vorrichtung nach einem der Ansprüche 4 bis 6, **dadurch gekennzeichnet**, dass die Generatoreinheit (70) ausgebildet ist, eine pseudo-zufällige Datenfolge als Testsequenz digitaler Daten zu generieren.

8. Vorrichtung nach einem der Ansprüche 2 bis 7, **dadurch gekennzeichnet**, dass der Knoten (20) ausgebildet ist, eine Differenz der analogen Eingangssignale zu bilden.

9. Vorrichtung nach einem der Ansprüche 2 bis 8, **dadurch gekennzeichnet**, dass der A/D Wandler (30) als Multi-Bit A/D-Wandler ausgebildet ist und dass der erste D/A Wandler (40) und der zweite D/A Wandler (50) als Multi-Bit D/A-Wandler ausgebildet sind.

10. Verfahren zur Erzeugung einer digitalen Signatur mittels einer Vorrichtung, die aufweist:
 einen ersten D/A-Wandler (40), der ausgebildet ist, eine Sequenz digitaler Daten zu empfangen und die Sequenz digitaler Daten in ein erstes analoges Signal zu wandeln,
 einen zweiten D/A-Wandler (50), der ausgebildet ist, eine Sequenz digitaler Daten und digitale Korrekturdaten zu empfangen und die Sequenz digitaler Daten in Abhängigkeit von den digitalen Korrekturdaten in ein zweites analoges Signal zu wandeln,
 wobei das erste analoge Signal und das zweite analoge Signal einem Knoten (20) zugeführt werden, der ausgebildet ist, die analogen Signale zu kombinieren und an den Eingang eines A/D-Wandlers (30) weiterzuleiten, der die kombinierten analogen Signale in eine Sequenz digitaler Ausgangsdaten wandelt,
 eine Korrekturdaten-Erzeugungseinheit (80), die ausgebildet ist, mehr als eine Sequenz digitaler Daten zu empfangen und daraus digitale Korrekturdaten zu generieren,
 mit den Verfahrensschritten:

- Zuführen einer Testsequenz digitaler Daten an den ersten D/A-Wandler (40), den zweiten D/A-Wandler (50) und die Korrekturdaten-Erzeugungseinheit (80);
- Zuführen der Sequenz digitaler Ausgangsdaten des A/D-Wandlers (30) an die Korrekturdaten-Erzeugungseinheit (80);
- Generieren von digitalen Korrekturdaten aus der Testsequenz digitaler Daten und der Sequenz digitaler Ausgangsdaten des A/D-Wandlers (30);
- Ausgeben der digitalen Korrekturdaten als digitale Signatur.

11. Verfahren nach Anspruch 10, **dadurch gekennzeichnet**, dass die digitalen Korrekturdaten in einem Korrekturdatenspeicher (60) gespeichert werden.

12. Verfahren nach einem der Ansprüche 10 oder 11, **dadurch gekennzeichnet**, dass die digitalen Korrekturdaten vor dem Ausgeben als digitale Signatur kodiert werden.

13. Verfahren nach einem der Ansprüche 10 bis 12, **dadurch gekennzeichnet**, dass das Generieren der digitalen Korrekturdaten durch eine Korrelationsoperation erfolgt.

14. Verfahren nach einem der Ansprüche 11 bis 13, **dadurch gekennzeichnet**, dass vor dem Zuführen der Testsequenz digitaler Daten den digitalen Korrekturdaten ein vordefinierter Wert zugewiesen wird.

15. Verfahren nach einem der Ansprüche 10 bis 14, **dadurch gekennzeichnet**, dass das die Testsequenz digitaler Daten durch eine pseudo-zufällige Datenfolge gebildet wird.

16. Verfahren nach einem der Ansprüche 10 bis 15,

wobei der Ausgang des A/D-Wandlers (30) mit den Eingängen des ersten D/A-Wandlers (40) und des zweiten D/A-Wandlers (50) verbunden ist, so dass der Knoten (20), der A/D-Wandler (30), der erste D/A-Wandler (40) und der zweite D/A-Wandler (40) einen Delta-Sigma A/D-Wandler bilden, dessen Eingang (1) mit dem Knoten (20) verbunden ist und dessen Ausgang (2) mit dem Ausgang des A/D-Wandlers (30) verbunden ist,

gekennzeichnet dadurch, dass

vor dem Zuführen der Testsequenz digitaler Daten an den ersten D/A-Wandler (40):

- die Verbindungen zwischen dem Eingang (1) und dem Knoten (20) sowie zwischen dem Ausgang (2) und dem Ausgang des A/D-Wandlers (30) geöffnet werden,
- die Verbindungen zwischen dem Ausgang des A/D-Wandlers (30) und den Eingängen des ersten D/A-Wandlers (40) und des zweiten D/A-Wandlers (50) geöffnet werden.

17. Verfahren zur Erzeugung einer digitalen Signatur, **gekennzeichnet durch**

- eine analoge Schaltung (602), die bedingt durch Herstellungstoleranzen, eindeutige Nichtidealitäten aufweist;

- eine Korrekturdaten-Erzeugungseinheit (605), die ausgebildet ist, digitale Korrekturdaten (606), die herstellungsbedingte Abweichungen von Komponenten der analogen Schaltung (602) korrigieren, zu generieren; wobei die analoge Schaltung (602) ausgebildet ist, mittels der digitalen Korrekturdaten (606) die analogen Nichtidealitäten am Ausgang (603) zu minimieren und dass die digitale Signatur auf Basis der digitalen Korrekturdaten (606) erzeugt wird.

Es folgen 3 Seiten Zeichnungen

Anhängende Zeichnungen

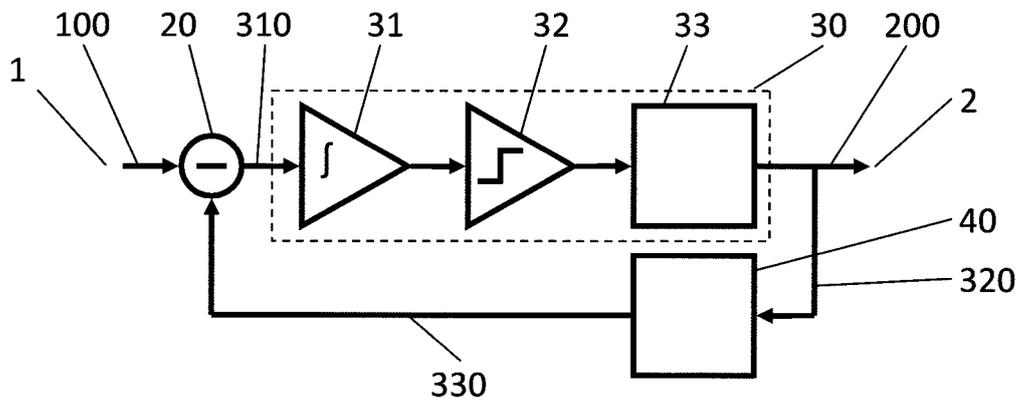


FIG. 1

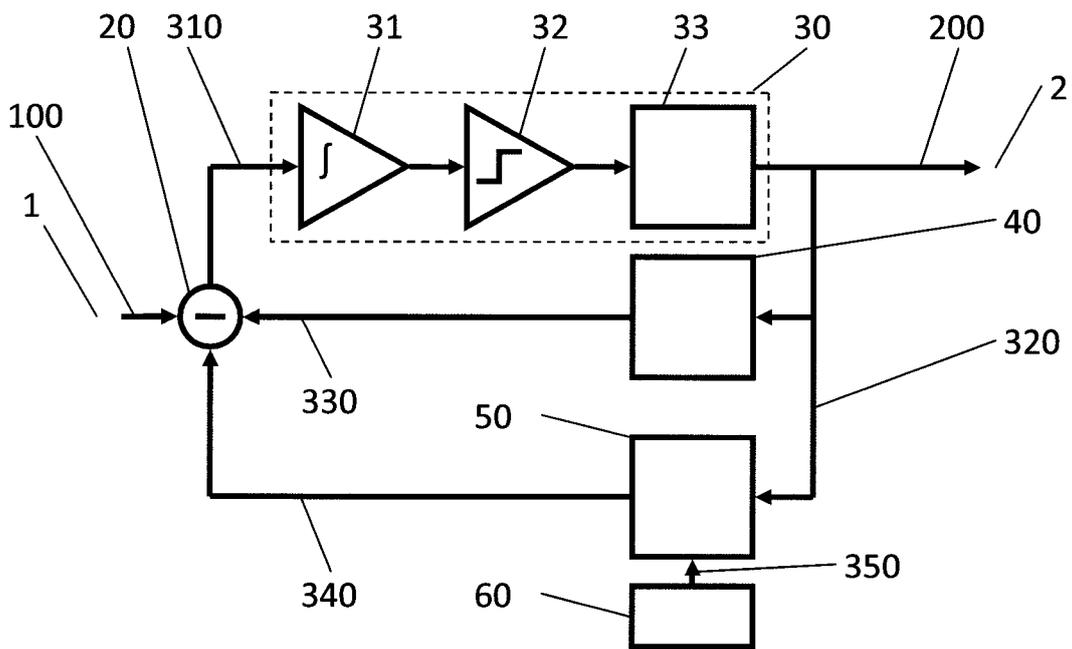


FIG. 2

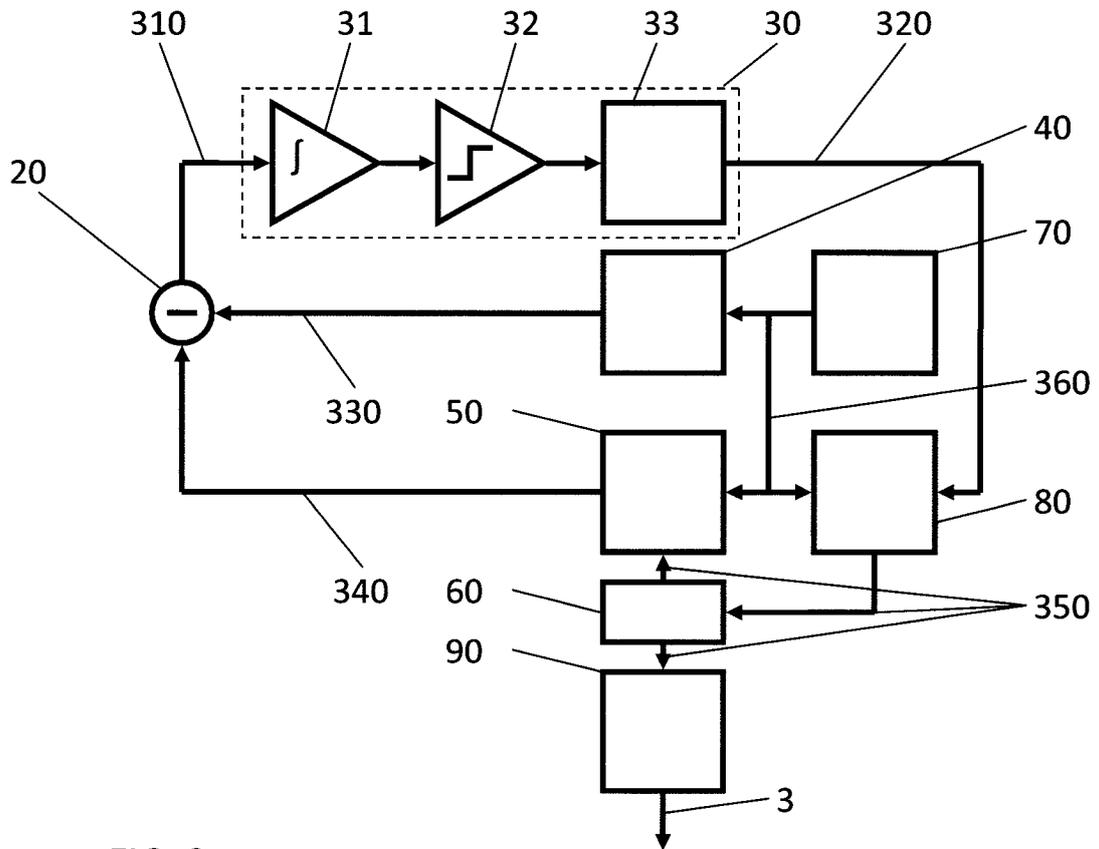


FIG. 3

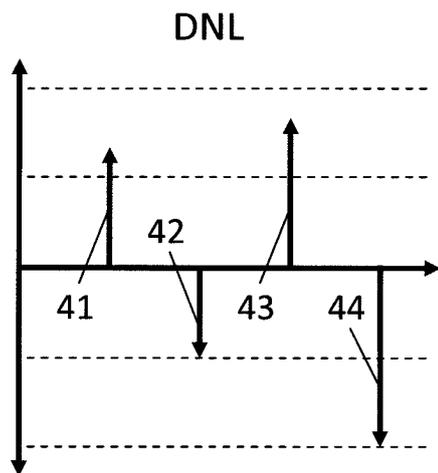


FIG. 4a

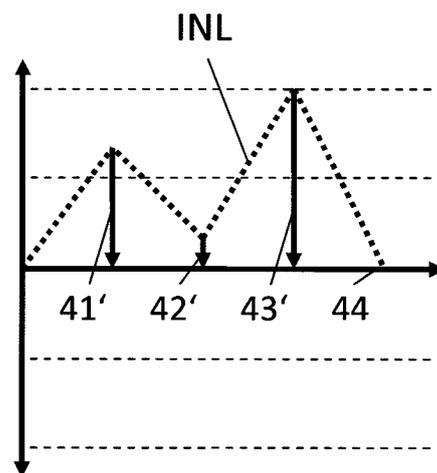


FIG. 4b

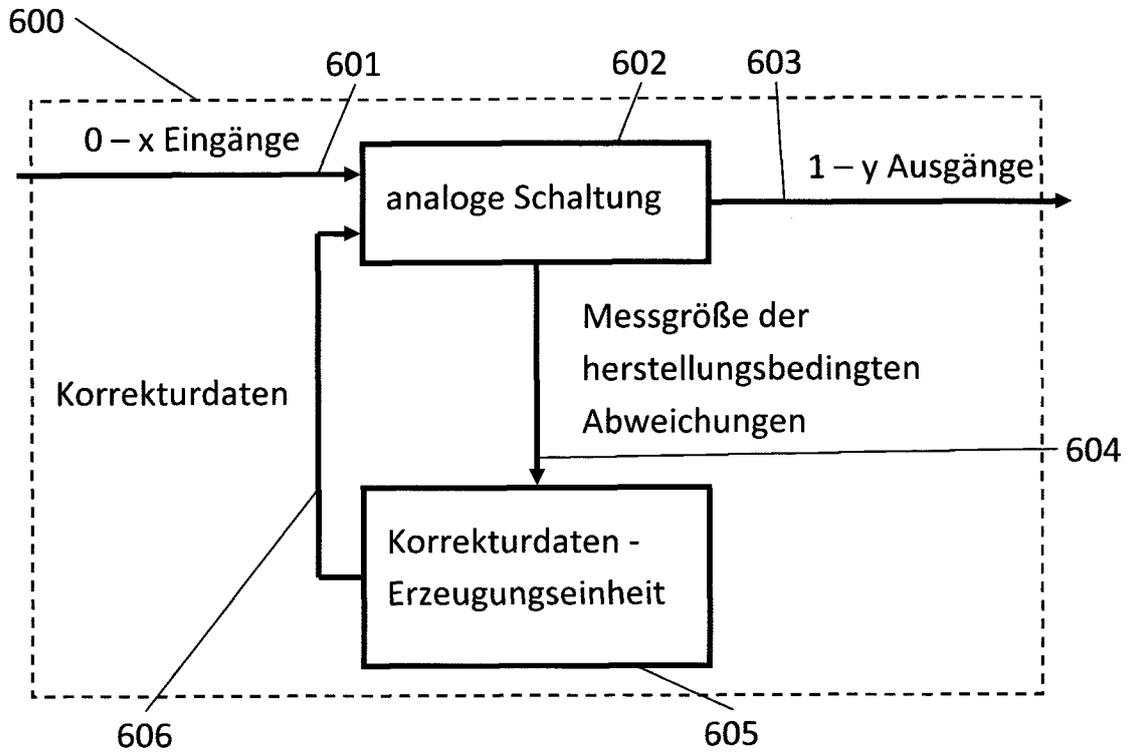
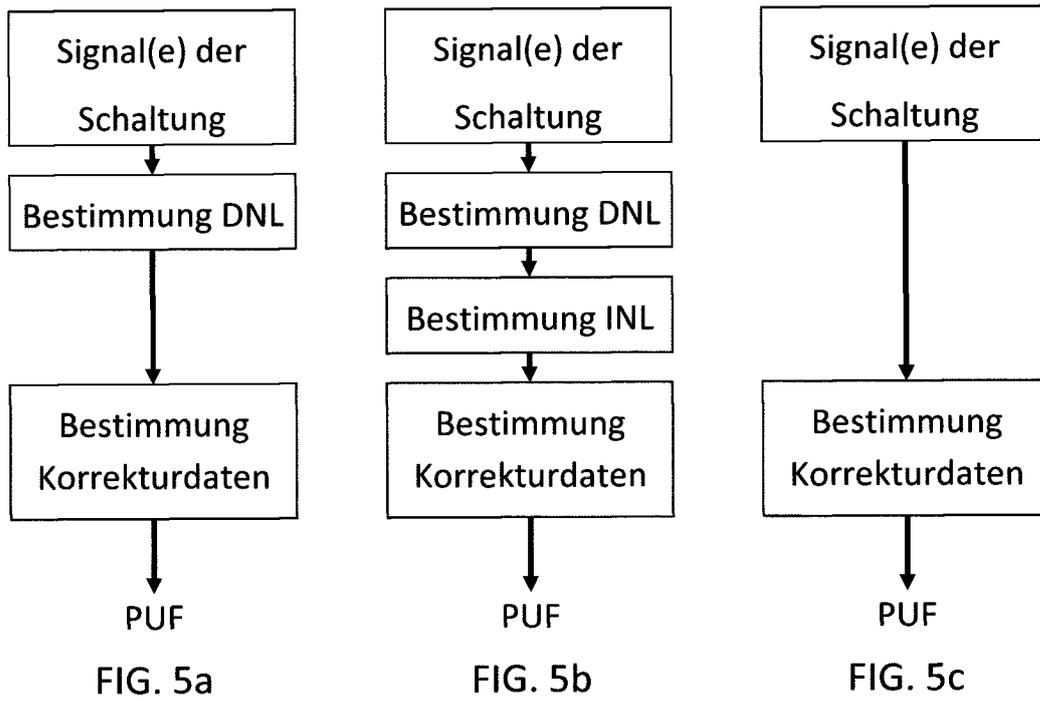


FIG. 6