(19) Bundesrepublik Deutschland
Deutsches Patent- und Markenamt

(10) **DE 103 47 301 A1** 2005.05.25

(12) # Offenlegungsschrift

(21) Aktenzeichen: **103 47 301.7**
(22) Anmeldetag: **08.10.2003**
(43) Offenlegungstag: **25.05.2005**

(51) Int Cl.[7]: **H04L 12/22**
H04L 12/40

(71) Anmelder:
Infineon Technologies AG, 81669 München, DE

(74) Vertreter:
Schoppe, Zimmermann, Stöckeler & Zinkler, 82049 Pullach

(72) Erfinder:
Klug, Franz, 81739 München, DE; Künemund, Thomas, Dr., 80337 München, DE

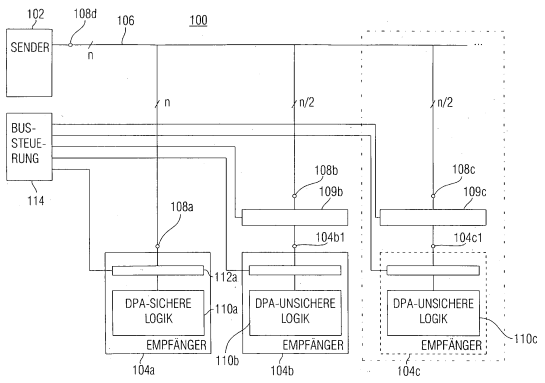
(56) Für die Beurteilung der Patentfähigkeit in Betracht gezogene Druckschriften:
BENINI,L. et al.: Energy-Aware Design Techniques for Differential Power Analysis Protection. In: Proc. Design Automation Conf., Juni 2003, S.36-41;

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

Prüfungsantrag gemäß § 44 PatG ist gestellt.

(54) Bezeichnung: **Schaltung mit einem Bus mit mehreren Empfängern**

(57) Zusammenfassung: Vorliegend wird von der bisherigen Vorgehensweise bei Bussen mit mehreren Empfängern, nämlich ein auf dem Bus (106) augegebenes Signal zunächst einmal an alle Empfänger (104a-c) und nicht nur an den Adressaten weiterzuleiten, abgegangen, da die Verarbeitung des Signals bereits mit der Eintragung des Signals an den Eingangsregistern (112a-c) der Empfängerschaltungsteile (104a-c) beginnt und damit potentiellen Angreifern bereits Möglichkeiten zum Ausspionieren der Schaltung (100) bietet. Der Mehraufwand, der damit verbunden ist, eine Verarbeitung eines Signals auf dem Bus (106) durch einen nichtadressierten Empfängerschaltungsteil zu verhindern, wird in der Gesamtbetrachtung dadurch ausgeglichen, dass dieser Empfängerschaltungsteil nicht oder weniger DPA-sicher ausgeführt sein muss, wenn er nicht zur Verarbeitung sicherheitskritischer bzw. mit einer höheren Geheimhaltungsstufe als einer vorbestimmten Schwelle vorgesehen ist. Sicherheitskritische Daten können diejenigen sein, die einen DPA-Angriff ermöglichen, wenn sie in DPA-unsicherer Logik verarbeitet werden bzw. sich korrelativ im Stromverbrauch niederschlagen, aber auch andere, insbesondere Klartextdaten, wie z. B. Geldbeträge, Kontonummern, Identifikationsnummern etc.



Beschreibung

[0001] Die vorliegende Erfindung bezieht sich allgemein auf Bussysteme bzw. Schaltungen mit einem Bus, ein wenig spezifischer auf Schaltungen mit einem Bus mit mehreren Empfängern und insbesondere auf Bussysteme, bei denen auf dem Bus zumindest unter anderem geheime Daten, wie z.B. Geldbeträge, kryptographische Schlüssel oder dergleichen, übertragen werden, wie es beispielsweise bei Kryptocontrollern in Chipkarten oder Smartcards der Fall ist.

Stand der Technik

[0002] Ein exemplarisches Beispiel für ein mögliches Bussystem bzw. eine Schaltung mit einem Bus ist in **Fig.** 5 gezeigt. Die Schaltung, die allgemein mit **900** angezeigt ist, umfasst einen Senderschaltungsteil **902** und drei Empfängerschaltungsteile **904a**, **904b** und **904c**. Jeder Schaltungsteil **902** bzw. **904a**–**904c** umfasst einen n-Bit-Dateneingang. Jeder Schaltungsteil **902**, **904a**–**904** ist über seinen Dateneingang mit einem Bus **906** gekoppelt. Insbesondere ist der Empfängerschaltungsteil **904a** mit einem n-Bit-Anschluss **908a**, der Empfängerschaltungsteil **904b** mit einem n-Bit-Anschluss **908b**, der Empfängerschaltungsteil **904c** mit einem n-Bit-Anschluss **908c** und der Senderschaltungsteil **902** mit einem n-Bit-Busanschluss **908d** des Busses **906** verbunden. Jeder Empfängerschaltungsteil **904a**–**904c** umfasst eine Logik **910a**, **910b** bzw. **910c**, deren n-Bit-Dateneingang über ein n-Bit-Eingangsregister **912a**, **912b** bzw. **912c** mit dem jeweiligen Dateneingang des Empfängerschaltungsteils **904a**–**904c** bzw. dem Busanschluss **908a**–**908c** verbunden ist. Jedes Register **912a**–**912c** weist einen Freigabe- (Enable-) bzw, einen Umschalt- (Toggle-) Eingang auf, der mit einer Bussteuerung **914** verbunden ist.

[0003] Bei dem exemplarischen Bussystem **900** von **Fig.** 5 gibt der Senderschaltungsteil **902** ein Daten repräsentierendes Signal ungezielt auf dem Bus **906** aus. Das Signal gelangt zu jedem Busanschluss, insbesondere jedem Busanschluss **908a**–**908c** der Empfängerschaltungsteile **904a**–**904c**. Von dort aus gelangt das Signal ungehindert in die Eingangsregister **912a**–**912c** der einzelnen Empfängerschaltungsteile **904a**–**904c**, um dort zwischengespeichert bzw. eingetragen zu werden. Im nächsten Taktzyklus sorgt die Bussteuerung **914** dafür, dass unter den Eingangsregistern **912a**–**912c** nur diejenigen ihren Registerinhalt an die nachfolgende Logik **910a**–**910c** ausgeben, die zu dem Empfängerschaltungsteil **904a**–**904c** gehören, der Adressat des durch den Sender **902** auf dem Bus **906** ausgegebenen Signals ist. Hierzu sendet die Bussteuerung **914** an das Eingangsregister bzw. die Eingangsregister des Adressaten bzw. der Adressatenschaltungsteile das Enable- bzw. Toggle-Signal.

[0004] Ein Bussystem wie dasjenige von **Fig.** 5 kann nicht ohne weiteres eingesetzt werden, wenn über den Bus **906** sowohl nichtsicherheitskritische als auch sicherheitskritische Daten übertragen werden. Bei der Kryptographie beispielsweise werden in Chipkarten, Smartcards oder dergleichen Daten verarbeitet, welche für eine DPA-Attacke verwendet werden können. Bei DPA-Angriffen wird sich der Umstand zunutze gemacht, dass eine Verarbeitung eines Signals in einer Schaltung den Stromverbrauch der Schaltung beeinflusst, d.h. dass der Stromverbrauch mit den Eingangsdaten korreliert. Bei DPA-Angriffen werden nun der Schaltung, wie z.B. dem Kryptocontroller einer Chipkarte, nacheinander mehrere unterschiedliche Daten zugeführt, die dieselbe dann auf dieselbe Art und Weise und beispielsweise mit dem selben Kryptoschlüssel verarbeitet. Bei jedem Mal wird der Stromverbrauchsverlauf der Schaltung gemessen. Anhand der Messergebnisse wird dann die Korrektheit einer Hypothese für geheime Daten, wie z.B. des Kryptoschlüssels einer durch die Schaltung implementierten Verschlüsselung, überprüft, indem eine statistische Analyse der Strom- bzw. Leistungsmessung verwendet wird.

[0005] Bei der Schaltung **900** von **Fig.** 5 ist es nun so, dass alle Daten, die auf dem Bus **906** ausgegeben werden, auf jeden Fall zunächst einmal in den Eingangsregistern **912a**–**912c** gespeichert werden. Diese Zwischenspeicherungsvorgänge schlagen sich in dem Strom- bzw. Leistungsverbrauch der Schaltung **900** durch Überlagerung nieder, beispielsweise aufgrund der Schaltvorgänge in verwendeten Transistoren von den den Registern zugrundeliegenden D-Flip-Flops. Verarbeitet die Schaltung **900** einen anderen von dem Angreifer zugeführten Eingangswert, so ändern sich bei der Verarbeitung durch die Schaltung **900** die auf dem Bus **906** ausgegebenen Signale bzw. Daten. Wenn bei dem Bussystem **900** von **Fig.** 5 keine Gegenmaßnahmen getroffen werden, ist eine DPA-Attacke erfolgreich, selbst wenn die Logiken **910a**–**910c** selbst DPA-sicher ausgeführt sind.

[0006] Eine Möglichkeit zur Abwehr von DPA-Angriffen ist die Verwendung einer Dual-Rail-Precharge-Logik und -Busses. Bei diesen Logiken wird jedes Bit auf zwei Bitleitungen übertragen. Der Bitwert **0** entspricht einer logischen 1 auf der einen und einer logischen 0 auf der anderen Bitleitung bzw. Schiene (Rail), während der

Bitwert **0** der umgekehrten Verteilung entspricht, d.h. eine logische 0 auf der einen und eine logische 1 auf der anderen Rail. Ein Bitwechsel führt folglich immer zu sowohl einer Änderung von logisch hoch zu logisch niedrig und umgekehrt. Dementsprechend umfassen Register in der Dual-Rail-Logik doppelt so viele Zellen bzw. Flip-Flops wie normalerweise, d.h. 2n Zellen für einen n-Bit-Wert, und der Bus ist doppelt so breit, 2n Bit breit. Die Hälfte aller Registerzellen weisen, wenn sie einen n-Bit-Wert zwischenspeichern, stets einen logisch niedrigen und die andere Hälfte einen logisch hohen Zustand auf. Um nun auch dem Angreifer die Möglichkeit zu nehmen, festzustellen, welche Bits sich zwischen aufeinanderfolgenden in das Register gespeicherten n-Bit-Werten ändern, wird vor jedem Registereintrag ein Precharge durchgeführt, bei dem alle Registerzellen auf einen logisch niedrigen oder logisch hohen Zustand gebracht werden. Folglich erfolgen bei jedem Registereintrag immer n Registerzellenzustandsänderungen.

[0007] Wie bereits erwähnt, ist es nicht ausreichend, bei der Schaltung **900** diejenigen Logiken DPA-sicher in Dual-Rail-Precharge-Logik auszuführen, welche die sicherheitskritischen Daten, welche für eine DPA-Attacke verwendet werden können, den eigentlichen Operationen unterziehen. Vielmehr werden die Daten ja bereits früher in den Eingangsregistern **912a**–**912c** „verarbeitet". Eine Möglichkeit, die Schaltung **900** DPA-sicher zu implementieren, besteht nun darin, alle Eingangsregister **912a**–**912c** an den Eingangsstufen der Empfängerschaltungsteile **904a**–**904c** DPA-sicher in Dual-Rail-Precharge-Logik auszuführen. Ein Nachteil an dieser Lösung besteht jedoch darin, dass damit ein erheblicher Mehraufwand an Fläche, Entwicklungszeit und Strombedarf verbunden ist. Wie bereits erwähnt, müsste die doppelte Anzahl an Registerzellen für die Eingangsregister verwendet werden. Zudem müsste vor jeder Registereintragung ein Precharge-Zyklus durchgeführt werden, d.h. vor jeder Datenausgabe auf dem Bus **906**, was einen zusätzlichen Stromverbrauch bedeutet.

Aufgabenstellung

[0008] Die Aufgabe der vorliegenden Erfindung besteht darin, eine Schaltung mit einem Bus und zwei Empfängerschaltungsteilen bzw. ein Verfahren zur Steuerung derselben bereitzustellen, die bzw. das bei gleicher oder sogar höherer Sicherheit gegenüber DPA-Angriffen hardwaretechnisch unaufwendiger ist und/oder einen geringeren Stromverbrauch aufweist.

[0009] Diese Aufgabe wird durch eine Schaltung gemäß Anspruch 1 und ein Verfahren gemäß Anspruch 17 gelöst.

[0010] Die Erkenntnis der vorliegenden Erfindung besteht darin, dass von der bisherigen Vorgehensweise bei Bussen mit mehreren Empfängern, nämlich ein auf dem Bus ausgegebenes Signal zunächst einmal an alle Empfänger und nicht nur an den Adressaten weiterzuleiten, abgegangen werden muss, da die Verarbeitung des Signals bereits mit der Eintragung des Signals an den Eingangsregistern oder -zwischenspeichern der Empfängerschaltungsteile beginnt und damit potentiellen Angreifern bereits Möglichkeiten zum Ausspionieren der Schaltung bietet.

[0011] Eine weitere Erkenntnis der vorliegenden Erfindung bestand nun darin, erkannt zu haben, dass der Mehraufwand, der damit verbunden ist, eine Verarbeitung eines Signals auf dem Bus durch einen nichtadressierten Empfängerschaltungsteil zu verhindern, in der Gesamtbetrachtung dadurch ausgeglichen wird, dass dieser Empfängerschaltungsteil nicht oder weniger DPA-sicher ausgeführt sein muss, wenn er nicht zur Verarbeitung sicherheitskritischer bzw. mit einer höheren Geheimhaltungsstufe als einer vorbestimmten Schwelle vorgesehen ist. Sicherheitskritische Daten können diejenigen sein, die einen DPA-Angriff ermöglichen, wenn sie in DPA-unsicherer Logik verarbeitet werden bzw. sich korrelativ im Stromverbrauch niederschlagen, aber auch andere, insbesondere Klartextdaten, wie z.B. Geldbeträge, Kontonummern, Identifikationsnummern etc.

[0012] Ein Vorteil der vorliegenden Erfindung besteht folglich darin, dass basierend auf derselben eine Schaltung mit einem Bus und zwei oder mehr Empfängern erzielbar ist, die bei zumindest gleicher DPA-Sicherheit weniger Stromverbrauch aufweist, da die Empfängerschaltungsteile, deren Verarbeitung des Datums auf dem Bus verhindert werden kann, nicht DPA-sicher ausgeführt sein müssen, sofern dieselben nicht zur Verarbeitung von sicherheitskritischen Daten vorgesehen sind, d.h. schaltungsbedingt nie Empfänger von sicherheitskritischen Daten sind.

[0013] Ein weiterer Vorteil der vorliegenden Erfindung besteht darin, dass bei gleicher oder sogar höherer DPA-Sicherheit eine Schaltung mit geringerem Hardwareaufwand erzielt werden kann, da diejenigen Empfängerschaltungsteile, bei denen eine Verarbeitung des Signals auf dem Bus verhindert werden kann, einfacher implementiert werden können, sofern sie nicht zur Verarbeitung von sicherheitskritischen Daten vorgesehen sind.

[0014] Ein weiterer Vorteil der vorliegenden Erfindung besteht darin, dass dieselbe einen höheren Grad an DPA-Sicherheit liefern kann, wenn ein sicherheitskritisches Datum auf dem Bus erst gar nicht zu einem nicht-DPA-sicheren Empfängerschaltungsteil durchgelassen wird.

[0015] Ein weiterer Vorteil der vorliegenden Erfindung besteht darin, dass dieselbe deshalb einen geringeren Stromverbrauch ermöglicht, weil der Empfängerschaltungsteil, der an der Verarbeitung des Signals auf dem Bus gehindert wird, in den Fällen der Verhinderung gar keinen Strom verbraucht, auch nicht durch ein gegebenenfalls vorhandenes Eingangs- bzw. Empfangsregister.

[0016] Gemäß einem Ausführungsbeispiel der vorliegenden Erfindung ist es zur Verhinderung der Verarbeitung des Signals auf dem Bus durch einen jeweiligen Empfängerschaltungsteil vorgesehen, dass eine ansonsten bestehende elektrische Kontinuität zwischen dem Bus und dem Empfängerschaltungsteil unterbrochen wird, so dass in dem Fall der Verhinderung das Signal erst gar nicht zu dem Empfängerschaltungsteil gelangt, und zwar weder im elektrischen Sinne noch im inhaltlichen Sinne, also durch ein dem Signal entsprechendes, da gleichen Wert anzeigendes, Signal. Eine Einrichtung wird beispielsweise zwischen Busanschluss und Empfängerschaltungsteil geschaltet, um in dem Fall keiner Verhinderung bzw. bei Nichtvorliegen eines Steuersignals Strom zwischen Bus und Empfängerschaltungsteil zu leiten, und bei Verhinderung bzw. Vorliegen eines Steuersignals den Stromfluss zwischen Bus und Empfängerschaltungsteil zu unterbinden. Hierzu könnte beispielsweise ein Tristate-Buffer bzw. eine Tristate-Pufferlogik oder ein Tristate-Transistor verwendet werden. Alternativ könnte beispielsweise ein Multiplexer verwendet werden, der zwischen dem Signal auf dem Bus und einem unbeachtlichen, beispielsweise zufälligen oder konstanten, aber sicherheitsunkritischen Datum hin- und herschaltet, wobei der Multiplexer in diesem Fall vorzugsweise als Analog-Multiplexer/Demultiplexer ausgebildet ist.

[0017] Gemäß einem alternativen Ausführungsbeispiel der vorliegenden Erfindung ist es vorgesehen, dass zur Verhinderung der Verarbeitung durch einen jeweiligen Empfängerschaltungsteil derselbe von einer Versorgungsspannung getrennt wird.

Ausführungsbeispiel

[0018] Bevorzugte Ausführungsbeispiele der vorliegenden Erfindung werden nachfolgend Bezug nehmend auf die beiliegenden Zeichnungen näher erläutert. Es zeigen:

[0019] Fig. 1 ein Blockschaltbild einer Schaltung gemäß einem Ausführungsbeispiel der vorliegenden Erfindung;

[0020] Fig. 2 ein Blockschaltbild eines Ausschnitts der Schaltung von Fig. 1 zur Veranschaulichung eines Ausführungsbeispiels für eine Implementierung der Einrichtung zum Verhindern einer Verarbeitung;

[0021] Fig. 3 ein Blockschaltbild eines Ausschnitts der Schaltung von Fig. 1 zur Veranschaulichung eines weiteren Ausführungsbeispiels für eine Implementierung der Einrichtung zum Verhindern einer Verarbeitung;

[0022] Fig. 4 ein Blockschaltbild, das einen an einem Bus hängenden Empfängerschaltungsteil darstellt, gemäß einem weiteren Ausführungsbeispiel der vorliegenden Erfindung; und

[0023] Fig. 5 ein Blockschaltbild eines Ausschnitts aus dem Schaltungsteil von Fig. 2 zur Veranschaulichung eines alternativen Ausführungsbeispiels für eine Implementierung der Einrichtung zum Verhindern einer Verarbeitung;

[0024] Fig. 6 ein Blockschaltbild eines herkömmlichen Bussystems.

[0025] Bevor Bezug nehmend auf die Fig. 1–Fig. 4 Ausführungsbeispiele der vorliegenden Erfindung näher erläutert werden, wird darauf hingewiesen, dass gleiche Elemente in diesen Figuren mit gleichen oder ähnlichen Bezugszeichen versehen sind und dass eine wiederholte Beschreibung dieser Elemente weggelassen wird.

[0026] Fig. 1 zeigt eine Schaltung **100** gemäß einem Ausführungsbeispiel der vorliegenden Erfindung. Die in Fig. 1 dargestellte Schaltung **100** könnte beispielsweise Teil eines Kryptocontrollers einer Chipkarte oder einer Smartcard sein. Die Schaltung **100** umfasst einen Senderschaltungsteil **102** und drei Empfängerschaltungsteile **904a**, **904b** und **904c**. Die Empfängerschaltungsteile **904a**, **904b** und **904c** sowie der Senderschaltungsteil

102 sind mit einem Bus **106** gekoppelt bzw. hängen (hook to) an dem Bus. Genauer ausgedrückt umfasst der Bus **106** zumindest vier Busanschlüsse **108a**, **108b**, **108c** und **108d**, wobei der Bus **106** noch weitere Busanschlüsse in einem in Fig. 1 nicht gezeigten Teil von Schaltung **100** aufweisen kann. Der Empfängerschaltungsteil **904a** ist mit dem Busanschluss **108a** direkt verbunden. Der Empfängerschaltungsteil **104b** ist über eine Verarbeitungsverhinderungseinrichtung **109b** mit dem Busanschluss **108b** verbunden, die zwischen den Busanschluss **108b** und einen Dateneingang **104b1** des Empfängerschaltungsteils **104b** geschaltet ist. Auf ähnliche Weise ist auch der Empfängerschaltungsteil **104c** nicht unmittelbar sondern über eine Verarbeitungsverhinderungseinrichtung **109c** mit dem Busanschluss **108c** verbunden, die zwischen den Busanschluss **108c** und einen Dateneingang **104c1** des Empfängerschaltungsteils **104c** geschaltet ist.

[0027] Jeder Empfängerschaltungsteil **904a**–**904c** umfasst eine Logik **110a**, **110b** und **110c** sowie als eine Eingangsstufe ein Empfangs- bzw. Eingangsregister **112a**, **112b** bzw. **112c**. Jedes Register **112a**–**112c** umfasst einen Registereingang und einen Registerausgang sowie einen Registersteuereingang. Der Registereingang jedes Eingangsregisters **112a**–**112c** bildet gleichzeitig den Dateneingang des jeweiligen Empfängerschaltungsteils **104a**–**104c**. Der Registerausgang ist mit der jeweiligen nachgeschalteten Logik **110a**–**110c** verbunden. Der Registersteuereingang ist mit einer Bussteuerung **114** verbunden, um von derselben Enable- bzw. Toggle-Signale zu erhalten, die anzeigen, dass das entsprechende Eingangsregister seinen Registerinhalt an die nachgeordnete Logik ausgeben soll, wie es im folgenden noch näher erörtert werden wird.

[0028] Neben einem Dateneingang und einem Datenausgang, mit welchen die Verarbeitungsverhinderungseinrichtungen **900b** und **900c** zwischen Busanschluss und Dateneingang geschaltet sind, umfassen dieselben ferner einen Steuereingang, der ebenfalls mit der Bussteuerung **114** verbunden ist, um von derselben ein Steuersignal zu erhalten, das der jeweiligen Verarbeitungsverhinderungseinrichtung anzeigt, dass dieselbe verhindern soll, dass ein Signal auf dem Bus **106** zu dem jeweiligen mit dem Bus **106** gekoppelten Empfängerschaltungsteil **104b** bzw. **104c** gelangt, wie es ebenfalls im folgenden noch näher erörtert werden wird.

[0029] Obwohl die Schaltung **100** von Fig. 1 jegliche elektronische Schaltung sein kann, wird die Schaltung von Fig. 1 im folgenden vor dem Hintergrund beschrieben, dass dieselbe Teil eines Kryptocontrollers bildet, der beispielsweise in einer Chipkarte oder einer Smartcard verwendet wird, um die Vorzüge der Schaltung besser veranschaulichen zu können. Dabei kann der in Fig. 1 dargestellte Schaltungsteil **100** beispielsweise eine obere Hierarchieebene des Mikrocontrollers darstellen, wobei beispielsweise der Sender **102** die CPU darstellte, während die Empfängerschaltungsteile **104a**–**104c** ein DES-Modul, ein Sende/Empfangsmodul, einen Speicher, ein kryptographisches Modul, einen Zufallsgenerator oder dergleichen darstellten. Der in Fig. 1 dargestellte Schaltungsteil **100** kann aber auch ein Detail in einer niedrigeren Hierarchieebene eines Kryptocontrollers darstellen, wobei beispielsweise der Senderschaltungsteil **102** einem Cachespeicher, der Empfängerschaltungsteil **104a** einer Verschlüsselungseinheit, der Empfängerschaltungsteil **104b** einem EEPROM und der Empfängerschaltungsteil **104c** einem anderen Schaltungsteil entspräche.

[0030] Es wird zu Veranschaulichungszwecken ferner davon ausgegangen, dass auf dem Bus **106** sicherheitskritische Daten ausgegeben werden, was in vorliegendem Ausführungsbeispiel bedeuten soll, dass dieselben für eine DPA-Attacke verwendet werden können. Das bedeutet, dass sich ihre Verarbeitung in dem Stromverbrauch der Schaltung **100** niederschlagen würde, und dieselben durch Korrelation zwischen einem geheimen Datum, wie z.B. einem kryptographischen Schlüssel, und dem Stromverbrauch bzw. Leistungsverbrauch der Schaltung **100** Rückschlüsse auf das geheime Datum bzw. Aussagen über die Richtigkeit einer Hypothese über das geheime Datum zuließen, wenn die Schaltung **100** mehrere Male mit mehreren unterschiedlichen Eingangsdaten betrieben wird. Daneben werden auf dem Bus **106** auch sicherheitsunkritische Daten übertragen, d.h. Daten, deren Verarbeitung sich ruhig auf den Gesamtstromverbrauch der Schaltung **100** auswirken darf, da er einem Angreifer keine Rückschlüsse auf ein geheimes Datum zulässt. Bezug nehmend auf das vorhergehende Beispiel könnten auf dem Bus **106** beispielsweise gleichzeitig Adressen, die sicherheitsunkritisch sind, und Daten, die sicherheitskritisch sind, übertragen werden. Das wäre beispielsweise in dem Fall des Cachespeichers als Senderschaltungsteil **102** und einem EEPROM und einer Speicherverschlüsselungseinheit als Empfängerschaltungsteile der Fall.

[0031] Es wird ferner davon ausgegangen, dass es sich, da auf dem Bus **106** sicherheitskritische Daten übertragen werden, bei dem Bus **106** um einen DPA-sicheren Bus handelt, d.h. einen Bus, der DPA-sicher implementiert ist. Exemplarisch wird davon ausgegangen, dass der Bus als Dual-Rail-Precharge-Bus (dual rail with precharge Bus) implementiert ist. Das bedeutet, dass, obwohl der Bus in Fig. 1 als n-Bit-breiter Bus dargestellt ist, derselbe nur n/2-Bit-Werte überträgt, wobei n eine geradzahlige Ganzzahl ist. Abwechselnd werden auf dem Bus **106** ein n-Bit-Nutzsignal und ein n-Bit-Precharge-Signal angelegt, wobei ein n-Bit-Nutzsignal n/2 logisch hohe und n/2 logisch niedrige und ein Precharge-Signal n logisch hohe oder n logisch niedrige Zustände

aufweist. In Hinblick auf eine detailliertere Beschreibung der Dual-Rail-Precharge-Logik wird noch auf die Beschreibungseinleitung verwiesen.

[0032] Ferner wird bei der nachfolgenden Beschreibung davon ausgegangen, dass es sich bei der Logik **110a** um eine DPA-sichere Logik handelt, während es sich bei den Logiken **110b** und **110c** um DPA-unsichere Logiken handelt. Die DPA-sichere Logik **110a** ist beispielsweise in Dual-Rail-Precharge-Logik ausgeführt. Dementsprechend ist auch das Register **112a** DPA-sicher ausgeführt, während die Register **112b** und **112c** einfach ausgeführt sind. Genauer ausgedrückt bedeutet dies, dass das Eingangsregister **112a** ein n-Bit-Register ist, dessen n-Bit-Registereingang unmittelbar mit dem n-Bit-Busanschluss **108a** verbunden ist. Die Eingangsregister **112b** und **112c** sind demgegenüber n/2-Bit-Register. Jede der n/2-Registerzellen dieser Register umfasst einen Registereingang, der einer vorbestimmten Rail jedes Railpaars des Busses **106** zugeordnet ist. Genauer ausgedrückt sind die Busanschlüsse **108b** und **108c** n/2-Bit-Anschlüsse, zu denen nur jeweils die vorbestimmte Rail jedes Railpaars, das ein logisches Bit des über den Bus **106** übertragenen n/2-Bit-breiten Datums darstellt, geführt ist.

[0033] Nachdem im Vorhergehenden der Aufbau der Schaltung **100** beschrieben worden ist sowie ein mögliches Anwendungsbeispiel für dieselbe, wird noch vor der Beschreibung ihrer Funktionsweise kurz erläutert, was in der vorliegenden und insbesondere in der nachfolgenden Beschreibung unter „Verarbeitung eines Signals" verstanden wird. Unter Verarbeitung eines Signals soll jeglicher elektronischer Vorgang bezeichnet werden, bei dem eine elektrische Zustandsänderung in Abhängigkeit von dem Signal durchgeführt wird bzw. bei dem der Stromverbrauch von einem Wert das Signals abhängt. Insbesondere umfasst der Ausdruck „Verarbeiten eines Signals" folglich das Anlegen eines Signals an einen Steuereingang eines Transistors oder das Zwischenspeichern eines Datums in einem Register, da das Umschalten eines Transistors in Abhängigkeit vom Signal auf dem Bus beispielsweise in der CMOS-Technologie zu Stromverbrauchsspitzen führt. Demgegenüber soll das Verarbeiten eines Signals nicht einen Vorgang bezeichnen, bei dem das Signal entweder durchgelassen oder nicht durchgelassen wird, da dies vorliegend lediglich als Weiterleitung zu einer nachfolgenden Verarbeitung oder Abhalten von einer nachfolgenden Verarbeitung betrachtet wird und bei diesem Vorgang wiederum der Stromverbrauch nicht vom Wert des Signals abhängt.

[0034] Wenn nun der Sender **102** ein Signal auf dem Bus **106** ausgibt, dem dann bereits ein Precharge-Signal vorausgegangen ist, dann ist dieses Signal auf dem Bus **106** für einen bestimmten der Empfängerschaltungsteile **104a**–**104c** bestimmt, dem sogenannten Adressaten. Trotzdem gelangt, wie es bereits beschrieben worden ist, das Signal an alle Busanschlüsse **108a**–**108c** der Empfängerschaltungsteile **104a**–**104c** unabhängig davon, ob der jeweilige Schaltungsteil nun Empfänger oder nicht Empfänger ist. Der Bus **106** bildet somit eine elektrische Kontinuität, aufgrund welcher sich das Signal auf dem Bus bis zu allen Busanschlüssen ausbreiten kann und von dort aus zu dem Eingangsregister **112a** bzw. den Verarbeitungsverhinderungseinrichtungen **109b**, **109c**.

[0035] Es können nun vier Fälle unterschieden werden:

1. Das Signal auf dem Bus **106** ist ein sicherheitskritisches Datum, d.h. es ermöglicht eine DPA-Attacke, wenn es DPA-unsicher verarbeitet wird, und Adressat ist eine DPA-sichere Logik, d.h. Empfänger **104a**.
2. Das Signal auf dem Bus betrifft ein DPA-unkritisches Datum, das keine DPA-Attacke bei DPA-unsicherer Verarbeitung ermöglicht, und Adressat ist eine DPA-sichere Logik, d.h. Empfänger **104a**.
3. Das Datum ist ein sicherheitsunkritisches Datum und Empfänger ist eine DPA-unsichere Logik, d.h. Empfängerschaltungsteil **104b** oder Empfängerschaltungsteil **104c**.
4. Das Signal auf dem Bus betrifft ein sicherheitskritisches Datum und der Adressat ist eine DPA-unsichere Logik, d.h. Empfängerschaltungsteil **104b** oder **104c**.

[0036] Bei dem vierten Fall wird davon ausgegangen, dass dieser Fall bereits bei Entwurf der Schaltung **100** bzw. des Kryptocontrollers, in den dieselbe integriert ist, ausgeschlossen worden ist und deshalb nicht auftritt bzw. vermieden wird. Im nachfolgenden werden deshalb nur die drei anderen Fälle erläutert.

[0037] Es wird zunächst mit dem Fall **3** begonnen, d.h. das Signal auf dem Bus **106** stellt ein sicherheitsunkritisches Datum dar. Adressat sei der Empfängerschaltungsteil **104b**. Das Augenmerk sei nun zunächst auf das Eintreffen des Signals am Busanschluss **108a** gerichtet. Der mit demselben direkt verbundene Empfängerschaltungsteil **104a** ist DPA-sicher, aber nicht Adressat. Da der Empfängerschaltungsteil **104a** direkt mit dem Bus **100** verbunden ist und eine elektrische Kontinuität zwischen Sender **102** und Registereingang des Eingangsregisters **112a** vorliegt, wird das Signal bzw. das sicherheitsunkritische Datum unmittelbar in dem durch vorhergehenden Precharge-Zyklus rückgesetzten Eingangsregister **112a** zwischengespeichert. Diese Verarbeitung des sicherheitsunkritischen Datums durch Zwischenspeicherung schlägt sich zwar als Überlagerung

in dem Gesamtstromverbrauch der Schaltung **100** bzw. dem Kryptocontroller nieder, verhilft dem DPA-Angreifer jedoch nicht zum Erfolg, da das Datum ja Sicherheitsunkriestisch ist. Die Bussteuerung **114** sendet dem Registersteuereingang des Eingangsregisters **112a** kein Enable- bzw. Toggle-Signal, um die beispielsweise als Flip-Flops ausgeführten Registerzellen des Eingangsregisters **112a** zur Weitergabe des gespeicherten Signals bzw. sicherheitsunkritischen Datums an die nachgeschaltete DPA-sichere Logik **110a** zu bewegen, da der Empfänger **104a** ja nicht Adressat des Signals ist.

[0038] Das sicherheitsunkritische Datum gelangt aber auch zum Busanschluss **108c**, d.h. einem Busanschluss, der ebenfalls einem Empfänger **104c** zugeordnet ist, der kein Adressat des Signals ist. Da das Signal sicherheitsunkritisch ist, bestünde nun keine Notwendigkeit, das Signal an der Weiterleitung zum Register **112c** zu hindern, wo dasselbe, wie Bezug nehmend auf das Eingangsregister **112** beschrieben, zwischengespeichert aber nicht weitergeleitet werden würde. Dennoch sendet die Bussteuerung **114** gemäß dem vorliegenden Ausführungsbeispiel an den Steuereingang der Verarbeitungsverhinderungseinrichtung **109c** ein Signal, das anzeigt, dass dieselbe verhindern soll, dass das Signal auf dem Bus **106** zu dem Dateneingang **104c1** des Empfängerschaltungsteils **104c** gelangt, bzw. dass dieselbe die elektrische Kontinuität zwischen Busanschluss **108c** und Dateneingang **104c1** unterbrechen soll. Der Vorteil hierin besteht darin, dass aufgrund dieser Vorgehensweise das Signal auf dem Bus **106**, das ja nicht für den Empfängerschaltungsteil **104c** bestimmt ist, nicht zu stromverbrauchenden Umschaltvorgängen in dem Eingangsregister **112c** führt, wodurch eine Stromersparnis erzielt wird. Effektiv wird dadurch der Empfängerschaltungsteil **104c** hierdurch von dem Bus **106** getrennt bzw. „abgeklemmt".

[0039] Das Signal **106** gelangt aber natürlich auch zu dem Busanschluss **108b**, mit welchem der Adressat **104b** gekoppelt ist. Die Bussteuerung **114** sendet der Verarbeitungsverhinderungseinrichtung **109b** kein Steuersignal, das ihr anzeigte, sie solle das Signal nicht durchlassen. Da kein Steuersignal von der Bussteuerung **114** kommt, stellt die Verarbeitungsverhinderungseinrichtung **109b** eine elektrische Kontinuität zwischen dem Busanschluss **108b** und dem Dateneingang **104b1** her und leitet das Signal elektrisch vom Bus **106** zum Empfängerschaltungsteil **104b**. Dort gelangt das Signal zu dem Eingangsregister **112b**, wo es zwischengespeichert wird. Die Bussteuerung **114** sendet nun an das Eingangsregister **112b** des Adressaten das Enable- bzw. Toggle-Signal, damit dasselbe das empfangene Signal bzw. das empfangene Datum an die nachgeschaltete Logik weitergibt. In diesem Fall ist dies das Empfangsregister **112b**. Die DPA-unsichere Logik **110b** führt nun anhand des sicherheitsunkritischen Datums eine vorbestimmte Operation durch, wie z.B. einen Speichervorgang, einen Lesevorgang, eine Rechenoperation oder dergleichen, und gibt das Ergebnis an einen geeigneten Empfänger aus, wobei die Rückgabe des Signals auch über den Bus **106** laufen kann, wobei dies jedoch aus Übersichtlichkeitsgründen in Fig. 1 nicht dargestellt ist. Die Ausführung der Operation an dem sicherheitsunkritischen Datum durch die DPA-unsichere Logik **110b** ist unbedenklich, da das Datum ja sicherheitsunkritisch ist und somit definitionsgemäß einem DPA-Angreifer keine DPA-verwertbaren Informationen liefert.

[0040] Im folgenden sei nun der zweite Fall nach obiger Auflistung betrachtet. Danach repräsentiert das auf dem Bus **106** befindliche Signal ein sicherheitsunkritisches Datum, wobei der Adressat DPA-sicher ist, d.h. Empfängerschaltungsteil **104a**. In diesem Fall sendet die Bussteuerung **114** zur Stromersparnis Steuersignale an sowohl den Steuereingang der Verarbeitungsverhinderungseinrichtung **109b** als auch der Verarbeitungsverhinderungseinrichtung **109c**. Das Signal auf dem Bus gelangt folglich zu den Busanschlüssen **108b** und **108c**, jedoch von dort aus nicht weiter zu den Dateneingängen **104b1** und **104c1** der nichtadressierten Empfängerschaltungsteile **104b** und **104c**. Da der DPA-sichere Empfängerschaltungsteil **104a** unmittelbar mit dem Busanschluss **108a** verbunden ist, gelangt das Signal ohne weiteres zu dem Eingangsregister **112a**, wo es zwischengespeichert wird. Da das Eingangsregister **112a** das Eingangsregister des Adressaten ist, sendet die Bussteuerung **114** an dieses Eingangsregister das Freigabesignal, woraufhin das Eingangsregister **112a** das Signal bzw. das durch dasselbe repräsentierte sicherheitsunkritische Datum an die DPA-sichere Logik **110a** weitergibt, die an demselben dann eine vorbestimmte Operation auf DPA-sichere Weise durchführt.

[0041] Der in der vorhergehenden Auflistung zuerst genannte Fall betrifft den Fall, dass das Signal auf dem Bus **106** ein sicherheitskritisches Datum betrifft und der Adressat auch der DPA-sichere Empfänger **104a** ist. Ohne die Verarbeitungsverhinderungseinrichtungen **109b** und **109c** würde nun dieses Signal ohne weiteres in elektrischer Kontinuität zu den Dateneingängen der Empfängerschaltungsteile **104b** und **104c** gelangen, wo dasselbe in den Eingangsregistern **112b** und **112c** zwischengespeichert werden würde, was, wie im Vorhergehenden beschrieben, eine DPA-Attacke ermöglichen würde, da die Register **112b** und **112c** DPA-unsicher implementiert sind und somit den DPA-ausgewerteten Stromverbrauch der Schaltung **100** Signalabhängig beeinflussen würden, und diese Beeinflussungen bei unterschiedlichen Gesamteingangsdaten der Schaltung **100** wiederum eine Überprüfung einer Hypothese über ein Geheimnis ermöglichen. Die Bussteuerung **114** steuert deshalb in diesem Fall beide Verarbeitungsverhinderungseinrichtungen **109b** und $\mathbf{109}_{\mathbf{c}}$ mit einem Steuersignal

an, das denselben anzeigt, dass dieselben eine Verarbeitung durch die ihnen zugeordneten Empfängerschaltungsteile **104b** bzw. **104c** verhindern sollen. Es findet folglich keine Verarbeitung in den nicht adressierten Empfängerschaltungsteilen **109b** und **104c** statt. Da auch die Verarbeitungsverhinderungseinrichtungen **109b** und **109c**, wie oben ausgeführt und wie es im folgenden noch näher beschrieben werden wird, keine Verarbeitung des sicherheitskritischen Datums durchführen, sondern lediglich die elektrische Kontinuität zwischen Busanschluss **108b** bzw. **108c** und **104b1** und **104c1** auf Signalwert unabhängige Weise unterbrechen, führt das Signal auch in den Verarbeitungsverhinderungseinrichtungen **109b** und **109c** nicht zu einer DPA-verwertbaren Auswirkung auf den Gesamtstromverbrauch. Anders ausgedrückt bewirkt das Signal auf dem Bus **106** an keiner der Verarbeitungsverhinderungseinrichtungen **109b**, **109c** und der Empfängerschaltungsteile **104b**, **104c** zu einer elektrischen Zustandsänderung bzw. einem Umschaltvorgang. Da der Empfängerschaltungsteil **104a** Adressat des Signals auf dem Bus **106** ist, steuert die Bussteuerung **114** das Eingangsregister **112a** mit einem Freigabesignal an, das deshalb das sicherheitskritische Datum zwischenspeichert und auf das Freigabesignal hin an die DPA-sichere Logik **110a** zur Durchführung einer Operation an demselben aus DPA-sichere Weise weitergibt.

[0042] Bezug nehmend auf das vorhergehende Ausführungsbeispiel wird darauf hingewiesen, dass im Vorhergehenden der Bus **106** lediglich als unidirektionaler Bus beschrieben worden ist, obwohl derselbe freilich auch bidirektional verwendet werden kann. Die Rollen, die die einzelnen Schaltungsteile **102**, **104a**, **104b**, **104c** in der vorhergehenden Beschreibung eingenommen haben, können sich in einem nachfolgenden Taktzyklus folglich ändern, so dass beispielsweise einer der Empfängerschaltungsteile die Rolle des Senderschaltungsteils einnehmen könnte, während dann der Senderschaltungsteil **102** die Rolle eines Empfängerschaltungsteils einnimmt.

[0043] Ferner wurde die Bussteuerung **114** als getrennter Block dargestellt. Es sei jedoch darauf hingewiesen, dass die Bussteuerung **114** nicht tatsächlich im physikalischen Sinne eine getrennte Einheit darstellen muss. Vielmehr können die Signale, die in Fig. 1 von der Bussteuerung **114** ausgegeben werden, auch von den einzelnen Schaltungsteilen, beispielsweise immer dem Senderschaltungsteil, ausgegeben werden. Im unidirektionalen Fall wäre dann die Bussteuerung **114** in dem Senderschaltungsteil **102** integriert.

[0044] Ferner wird darauf hingewiesen, dass die vorhergehende Beschreibung sich lediglich illustrativ auf einen Bus mit einem Sender und drei Empfängern bezog. Die vorliegende Erfindung ist freilich auch bei Bussen mit nur einer Anordnung aus einem Sender und zwei Empfängern anwendbar.

[0045] Bezug nehmend auf Fig. 2 wird im folgenden ein Ausführungsbeispiel für eine Verarbeitungsverhinderungseinrichtung beschrieben. Fig. 2 stellt beispielsweise den in Fig. 1 mit Strichpunktlinien umrandeten Teil gemäß einer speziellen Implementierung gemäß einem Ausführungsbeispiel der vorliegenden Erfindung dar.

[0046] Fig. 2 zeigt einen Ausschnitt des Busses **106**, der lediglich illustrativ die Busanschlüsse **108b** und **108a** umfasst. Gezeigt sind ferner der Empfängerschaltungsteil **104c**, der über seinen Dateneingang **104c1** über die Verarbeitungsverhinderungseinrichtung **109c** mit dem Busanschluss **108c** verbunden ist. Gemäß diesem Implementierungsbeispiel ist die Verarbeitungsverhinderungseinrichtung **109c** in Form eines Tristate-Buffers implementiert. Genauer ausgedrückt, umfasst die Verarbeitungsverhinderungseinrichtung **109c** n/2-Tristate-Buffer oder -Transistoren **200**. Jeder Tristate-Buffer **200** umfasst einen Eingang, einen Ausgang und einen Steuereingang. Der Eingang jedes Tristate-Buffers **200** ist über den Busanschluss **108c** mit einer unterschiedlichen Rail **202** des Busses **106** verbunden, nämlich einer vorbestimmten Rail aus einem unterschiedlichen Railpaar des Busses **106**. Der Ausgang jedes Tristate-Buffers **200** ist mit einem Registereingang einer unterschiedlichen der n/2-Registerzellen 204 des Eingangsregisters **112c** verbunden. Die Steuereingänge der Tristate-Buffer **200** werden über einen gemeinsamen Steuereingang **206** angesteuert, der mit der Bussteuerung **114** (Fig. 1) verbunden ist, um gegebenenfalls das Steuersignal zu erhalten, das anzeigt, dass dieselben eine Signalverarbeitung durch die nachgeschaltete Logik **110c** verhindern sollen. Fig. 2 zeigt auch den gemeinsamen Registerschaltungseingang für die Registerschaltungseingänge der Registerzellen **204** des Eingangsregisters **112c**, der ebenfalls mit der Bussteuerung **114** (Fig. 1) verbunden ist.

[0047] Die Tristate-Buffer **200** sind beispielsweise Aktiv-Hoch-Tristate-Buffer, deren Schaltverhalten durch folgende Wahrheitstabelle beschrieben wird, in der 0 für einen logisch niedrigen und 1 für einen logisch hohen Zustand steht, Z eine hohe Impedanz bedeutet, c den logischen Zustand am gemeinsamen Steuereingang **206** repräsentiert, x den logischen-Zustand am Dateneingang eines Tristate-Buffers **200** und z den logischen Zustand am Datenausgang des Tristate-Buffers bedeutet.

c	x	z
0	0	Z
0	1	Z
1	0	0
1	1	1

[0048] Alternative könnte der Baustein **300** als Aktiv-Niedrig-Tristate-Buffer ausgebildet sein, dessen Wahrheitstabelle aus obiger Tabelle durch vertauschen der Einsen und Nullen in der Spalte c erhalten wird.

[0049] Anders ausgedrückt bedeutet Z nicht nur hohe Impedanz, sondern eben auch das Vorliegen von weder einer logischen 0 noch einer logischen 1. Der Stromfluss zwischen Eingang und Ausgang des Tristate-Buffers ist in diesem Fall unterbrochen. Sendet folglich die Bussteuerung **114** (Fig. 1) das Steuersignal c = 0 zu den Tristate-Buffern **200**, so verhindern dieselben, wie erwünscht, dass das Signal auf dem Bus **106** zu dem nachgeschalteten Empfängerschaltungsteil **104c** gelangt. Für Zeiten, in denen das die Verarbeitungsverhinderung anzeigende Steuersignal nicht gesendet wird, liegt c = 1 vor, und das Signal auf dem Bus passiert den Tristate-Baustein **200** in elektrische Kontinuität ohne weiteres.

[0050] Fig. 3 stellt ein anderes Ausführungsbeispiel für eine Implementierung der Verarbeitungsverhinderungseinrichtung **109c** dar. Gemäß dem Ausführungsbeispiel von Fig. 3 umfasst die Verarbeitungsverhinderungseinrichtung **109c** einen n/2-Bit-2-auf-1-Multiplexer **300**, der einen ersten Multiplexereingang, der mit dem Busanschluss **108c** verbunden ist, einen zweiten Multiplexereingang, der mit einem Fake- bzw. Verwirrungssignaleingang **302** verbunden ist, einen Multiplexerausgang, der mit dem Dateneingang **104c1** verbunden ist, und einen Steuereingang **304**, der mit der Bussteuerung **114** verbunden ist.

[0051] Der Multiplexer **300** ist vorzugsweise als Analog-Multiplexer/Demultiplexer ausgebildet. Der Multiplexer umfasst beispielsweise Analogschalter bzw. Transmission-Gates, von denen n/2 zwischen erstem Multiplexereingang und Multiplexerausgang und die anderen n/2 zwischen zweitem Multiplexereingang und Multiplexerausgang geschaltet sind, und von denen selektiv entweder die erste Hälfte oder die zweite Hälfte durch einen 1-aus-2-Decoder (nicht gezeigt) in einen leitenden Zustand versetzt wird, während die jeweils anderen in einen nichtleitenden Zustand versetzt werden. In dem Fall, dass die Bussteuerung **114** an den Steuereingang **304** das Steuersignal sendet, das anzeigt, dass eine Verarbeitung durch die nachgeschaltete Empfängerschaltung **104c** verhindert werden soll, sorgt der Multiplexer **300** für eine elektrische Kontinuität zwischen Fakesignaleingang **302** und Dateneingang **104c1**.

[0052] An dem Fakesignaleingang **302** liegt entweder ein konstantes Signal an, das keine weitere Bedeutung hat und insbesondere sicherheitsunkritisch im oben genannten Sinne ist, oder ein$_e$ durch einen Zufallsgenerator erzeugte Zufallszahl. Bei Nichtvorliegen des Steuersignals sorgt der Multiplexer **300** für eine elektrische Kontinuität zwischen dem Busanschluss **108c** und dem Dateneingang **104c1**. Das Vorhandensein des Steuersignals entspricht beispielsweise einem logisch hohen Zustand am Steuereingang **304**, während das Nichtvorhandensein des Steuersignals einem logisch niedrigen Zustand entspricht.

[0053] Bezug nehmend auf die vorhergehende Beschreibung wird noch darauf hingewiesen, dass im Vorhergehenden lediglich Empfängerschaltungsteile beschrieben wurden, die in der Eingangsstufe ein Eingangsregister umfassten. Die vorliegende Erfindung ist aber auch in Fällen anwendbar, bei denen ein Empfängerschaltungsteil kein Eingangsregister aufweist. Dieser Fall ist in Fig. 4 dargestellt. Es sei darauf hingewiesen, dass das Fehlen eines Eingangsregisters freilich auch bei der DPA-sicheren Logik **110a** vorgesehen sein könnte, wenn der Empfängerschaltungsteil **104a** bei jeder Signalausgabe auf dem Bus **106** Empfänger wäre, oder aber wenn die ständige Durchführung der Operation durch die Logik **110a** auch in Fällen, da der Empfängerschaltungsteil **104a** nicht Adressat ist, in Kauf genommen würde.

[0054] Bezugnehmend auf das Ausführungsbeispiel von Fig. 2 sei darauf hingewiesen, dass dort in dem Fall eines Dual-Rail-Precharge-Bus als dem Bus **106** in den Precharge-Phasen bzw. Zyklen des Busses **106** die Tristate-Buffer **200** mittels des Freigabesignals an dem Steuereingang **206** durch die Bussteuerung **114** derart gesteuert werden, dass sie das Precharge-Signal, bei dem beispielsweise beide Rails, die zu einem logischen Bit gehören in einen logisch hohen Zustand versetzt werden, nicht hindurchlassen, so dass keine Zustandsänderung in dem Eingangsregister **112c** eintritt. Die Steuerung des Freigabesignals auf diese Weise, nämlich auch in den Precharge-Phasen, erhöht jedoch den Aufwand zur Steuerung. In einigen Anwendungen kann es

deshalb vorteilhafter sein, das Freigabesignal nur in Nicht-Precharge- bzw. Daten-Zyklen zur Steuerung des Hindurch- und Nicht-Hindurchlassens des Signals auf dem Bus **106** zu verwenden, während dasselbe in den Precharge-Zyklen Werte annimmt, die unkorreliert bzw. unbeachtlich zu dem gewollten Hindurchlassverhalten sind. In diesem Fall könnten die Tristate-Buffer **200** von Fig. 2 durch Bridge- bzw. Dual-Auf-Single-Schaltungen ersetzt werden, wie es im folgenden bezugnehmend auf Fig. 5 beschrieben wird.

[0055] Fig. 5 zeigt stellvertretend eine solche Bridge-Schaltung **400** in angeschlossenem Zustand innerhalb der Umgebung der Schaltung von Fig. 2, wobei sie einen der Tristate-Buffer **200** von

[0056] Fig. 2 ersetzt. Die Bridge **400** umfasst zwei Raileingänge **108c1** und **108c2**, von denen jede mit einer unterschiedlichen von zwei zusammengehörenden Bit-Rails eines n-Bit breiten Busanschlusses **108a** des n Bit breiten Busses **106** verbunden ist, einen Single-Rail-Ausgang, der mit einer Bitleitung des n/2-Bit breiten Single-Rail-Eingangs **104c1** des angeschlossenen Empfängers **104c** verbunden ist, und einen Steuereingang, der mit dem gemeinsamen Steuereingang **206** verbunden ist, um das Signal zu erhalten, dass während der Datenzyklen anzeigt, dass eine Verarbeitung des Datums auf dem Bus **106** verhindert werden soll und in Precharge-Phasen beliebige Werte annimmt. Wie es durch Punkte innerhalb von **109c** angedeutet ist, ersetzt eine Brücke alle Tristate-Buffer **200** von Fig. 2.

[0057] Wie vorher beschrieben wird bei dem Ausführungsbeispiel von Fig. 5 angenommen, dass das Freigabesignal an dem gemeinsamen Steuereingang **206** während der Precharge-Phasen nur unbestimmte Wert annimmt. Die Bridge **400** weist deshalb folgendes Schaltverhalten auf, um auch in den Precharge-Phasen sicherzustellen, dass hier aufgrund des Precharge-Signals auf den Rails keine ungewollte verräterische Zustandsänderung in dem nachfolgenden DPA-unsicheren Eingangsregister **204** ergibt, das sich an den Ausgang der Bridge **400** anschließt:

Wert	bit	bitq	enable	out
Precharge	1	1	X	Alter Wert
Precharge/1/0	X	X	0	Alter Wert
1	1	0	1	1
0	0	1	1	0

[0058] Die Tabelle zeigt in der linken Spalte den auf den beiden Railleitungen, die mit den Eingängen **108c1** und **108c2** der Bridge **400** verbunden sind, und übertragenen Wert an, der durch die logischen Zustand bit auf der Rail **108c1** und dem logischen Zustand bitq auf der Rail **108c2** bestimmt ist. Ein großes X in der Tabelle bedeutet, dass der logische Zustand der entsprechenden Leitung unbeachtlich ist bzw. einen logisch hohen oder einen logisch niedrigen Zustand einnehmen kann, und trotzdem die anderen Werte in der selben Zeile zutreffen. Die zweite Spalte zeigt den logischen Zustand bit an, der sich auf der Rail **108c2** einstellt. Die dritte Spalte zeigt den logischen Zustand bitq an, der sich auf der Rail **108c1** einstellt. Die vierte Spalte zeigt, welchen Zustand das Freigabesignal annimmt, der sich an dem Steuereingang **206** einstellt, wobei der Zustand mit enable bezeichnet ist. Die letzte Spalte zeigt an, welcher Zustand sich an dem Anschluss **104c1** einstellt, wobei dieser Zustand mit Out bezeichnet ist.

[0059] Wie es zu erkennen ist, verhält sich die Bridge **400** derart, dass, wenn ein Precharge-Signal auf den Rails **108c1** und **108c2** übertragen wird, d.h. ein Precharge-Zyklus vorliegt, unabhängig von dem Zustand des Freigabesignals, der ja, wie im vorhergehenden beschrieben, in diesem Zyklus ohnehin undefiniert ist, der Zustand am Ausgang der Bridge **400** eingefroren wird und auf dem alten Wert verbleibt. Das nachgeschaltete Eingangsregister **204** ändert folglich seinen Zustand nicht sondern erhält ein unverändertes Signal von der Bridge **400**. Ist das Freigabesignal auf einen logisch niedrigen Zustand, nämlich 0, geschaltet, so sorgt auf jeden Fall, nämlich unabhängig von den Zuständen auf den Rails **108c1** und **108c2**, die Bridge **400** dafür, dass der Wert am Ausgang **104c1** der Bridge-Schaltung **400** unverändert bleibt, wodurch das nachgeschaltete Eingangsregister seinen Wert wiederum nicht ändert. Dieses Verhalten der Bridge **400** ermöglicht es, in den Daten-Zyklen des Busses **106** die in den vorhergehenden Ausführungsbeispielen beschriebene Sperrung bzw. Verhinderung der Verarbeitung eines Signals auf dem Bus **106** vorzunehmen.

[0060] Liegt ein Bitwert und nicht ein Precharge-Signal auf den Rails **108c1** bzw. **108c2** vor, nämlich eine logische 1 oder eine logische 0, in welchem ersten Fall die Rail **108c2** einen logisch hohen Zustand (bit = 1) aufweist, während die Rail **108c1** den logisch niedrigen Zustand (bitq = 0) aufweist, und in welchem zweiten Fall die Rail **108c2** ein logisch niedrigen Zustand (bit = 0) und die Rail **108c1** einen logisch hohen Zustand (bitq =

1) aufweist, und weist gleichzeitig das Freigabesignal enable einen logisch hohen Zustand auf, wird am Datenausgang der Brücke **400** einfach ein entsprechender Bitwert ausgegeben, wodurch sich der entsprechende Zustand des nachgeschalteten Registers **204** je nach dem, welcher Wert darin zuvor gespeichert war, ändert oder nicht ändert. Dies ermöglicht es, wie im vorhergehenden beschrieben, den Daten-Zyklen ein Signal auf dem Bus **106** zum Eingangsregister durchzulassen bzw. eine Verarbeitung durch den Empfänger **104c** zu ermöglichen.

[0061] Wie es aus vorhergehender Beschreibung hervorgegangen ist, wirkt folglich die Bridge **400** wie ein Zwischenspeicher, der jedoch seinen Wert in dem Fall, dass das Freigabesignal einen logisch niedrigen Zustand aufweist und somit signalisiert, dass das Signal auf dem Bus **106** nicht hindurch gelassen werden soll, nicht ändert. Zudem ändert sie ihren gespeicherten Zustand aber auch dann nicht, wenn ein Precharge-Zyklus vorliegt, und zwar unabhängig von dem gegebenenfalls in diesen Zyklen undefinierten enable-Signal.

[0062] Eine Implementierung der Bridge **400** könnte beispielsweise einen Zwischenspeicher mit einem Eingang und einem Ausgang umfassen. Zwischen Eingang des Zwischenspeichers und dem Dateneingang **108c2** wäre ein erster Tristate-Buffer geschaltet, dessen Steuereingang mit dem Steuereingang **206** verbunden wäre. Zwischen Eingang **108c2** und Zwischenspeicher wäre aber ferner ein weiterer Tristate-Buffer geschaltet, dessen Steuereingang von dem Ausgangssignal eines UND-Gatters gesteuert würde, dessen beide Dateneingänge mit dem Eingang **108c1** bzw. **108c2** verbunden wären. Der Ausgang des Zwischenspeichers wäre mit dem Anschluss **104c1** verbunden. Der Schaltvorgang in dem UND-Gatter, der ja bei jedem Signal auf dem Bus **106** auftreten würde, hätte keine Auswirkungen im Hinblick auf die Sicherheit vor Angriffen, da zwischen den einzelnen Daten- und Precharge-Zyklen ja immer genau ein Zustandswechsel eintritt, und somit keine Rückschlüsse auf den Dateninhalt in den Daten-Zyklen geschlossen werden kann. Folglich verhindert die Bridge **400** zwar nicht gänzlich jegliche Verarbeitung, da sie ja selbst eine in Abhängigkeit der Eingangssignale bit und bitq auf dem Bus **106** durchführt, aber sie verhindert jegliche DPA-unsichere Verarbeitung im sich anschließenden Teil. Im Unterschied zu einem Eingangsregister sorgt folglich die Bridge-Schaltung dafür, dass sich der Inhalt bzw. Zustand des Zwischenspeichers am Ausgang bzw. der Masterstufe nicht in verräterischen Situationen, d.h. bei sicherheitskritischen Daten, ändert, während ja bei Eingangsregistern sich der Zustand der Masterstufe auf jeden Fall ändert, nur eventuell nicht an die nachfolgende Slave-Stufe weitergegeben wird.

[0063] Nachdem im Vorhergehenden Bezug nehmend auf die Figuren die vorliegende Erfindung anhand von Ausführungsbeispielen näher beschrieben worden ist, wird darauf hingewiesen, dass die vorliegende Erfindung nicht nur auf das Gebiet der Kryptocontroller begrenzt ist, sondern ferner auch auf andere Sicherheitsmodule anwendbar ist, wie z.B. TPMs (Trusted Platform Modules). Natürlich ist die vorliegende Erfindung aber auch bei Anwendungen anwendbar, bei denen keine geheimen Daten der Gefahr des Ausspähens durch DPA-Angriffe ausgesetzt sind, wie z.B. bei Mikrocontrollern oder dergleichen, wie wohl dort die Vorteile im Hinblick auf die erhöhte Sicherheit wegfallen und nur noch diejenigen im Hinblick auf die Stromersparnis verbleiben.

[0064] Ferner wird noch darauf hingewiesen, dass die oben verwendete Definition sicherheitskritischer Daten in anderen Fällen auch anders aussehen kann. Sicherheitskritische Daten können beispielsweise auch Klartextdaten sein, die an sich bereits geheim sind, wie z.B. ein Guthaben oder dergleichen. Anderenfalls könnte es nämlich einem Angreifer beispielsweise durch einen DPA-Angriff gelingen, durch Beobachtung des Stromverbrauches eventuell eine Vermutung über das geheime Datum zu bestätigen.

[0065] Die Unterteilung der Daten muss auch nicht dual in zwei Teile erfolgen. Ebenso ist es möglich die Daten in mehreren Geheimhaltungsstufen zu untergliedern.

[0066] Ferner wird Bezug nehmend auf die vorhergehende Beschreibung darauf hingewiesen, dass, obwohl bei Fig. 1 der DPA-sichere Empfängerschaltungsteil **104a** direkt mit dem Bus **106** verbunden war, zwischen Busanschluss **108a** und Empfängerschaltungsteil **104a** ebenfalls eine Verarbeitungsverhinderungseinrichtung geschalten sein könnte. Dies führt jedoch insofern nicht zu einem Vorteil, als dass das Eingangsregister **112a** sowie die DPA-sichere Logik **110a** ja ohnehin DPA-sicher ausgeführt sein müssen, da der Empfängerschaltungsteil **104a** zur Durchführung von Operationen an sicherheitskritischen Daten vorgesehen ist.

[0067] Zusammenfassend ausgedrückt betrafen die vorhergehenden Ausführungsbeispiele ein Demultiplexing von nichtsicherheitsrelevanten und sicherheitsrelevanten Daten auf einem gemultiplexten Bus, um DPA-Attacken auf nachfolgende Speicher und/oder Logikschaltungen zu verhindern. Die Informationen des Busses wurden vor ihrer Verarbeitung getrennt. Diese Trennung sorgte dafür, dass sicherheitskritische Daten in DPA-resistenten Systemteilen ankommen und verarbeitet werden, während in den nichtresistenten Teilen

ein Verarbeiten und/oder Speichern der Daten nur möglich ist, wenn diese nicht sicherheitsrelevant sind. Funktional wurde dies durch ein Abkoppeln der Speicherzelle bzw. Logikschaltung mittels einer „Isolierschicht" erzielt, wobei als Beispiel in Fig. 3 Tristate-Buffer bzw. Tristate-Transistoren verwendet wurden.

[0068] Im Bereich von Sicherheitsanwendungen, wie z.B. Geldkarten oder dergleichen, lösen die obigen Ausführungsbeispiele damit auf elegante Weise das Problem der DPA-Anfälligkeit. Aus Flächengründen werden Datenpfadbusse oft für unterschiedlichste Zwecke genutzt. Es können beispielsweise in einer CPU Adressen (sicherheitsunkritisch) und Daten (sicherheitskritisch) über einen gemeinsamen Bus übertragen werden. Dabei gibt es verschiedene Empfänger für diese Informationen. Die Daten können beispielsweise in einer Recheneinheit verarbeitet und dann gespeichert werden. Bei obigen Ausführungsbeispielen von Fig. 1–Fig. 3 wurden jeweils Eingangsspeicher betrachtet. Gleiches galt jedoch auch für nachfolgende Logik, welche nur an der Auswertung unkritischer Daten interessiert ist, wie es bei Fig. 4 der Fall ist. Dies erfolgt aus Flächengründen. Das jedoch ermöglicht einen DPA-Angriff auf das Gesamtsystem, wie oben beschrieben, da jedes Datum in den Speicher geschrieben wird. Dadurch erfolgt ein signifikant unterschiedlicher Stromverbrauch beim Umladen der sicherheitskritischen Daten. Eine mögliche Schutzmaßnahme wäre die Verwendung von DPA-sicheren Speichereinheiten für die Eingangsregister gewesen, jedoch sind diese flächen- und energieaufwendig, wie es in der Beschreibungseinleitung der vorliegenden Anmeldung beschrieben wurde.

[0069] Die obigen Ausführungsbeispiele stellten deshalb eine elegante Lösung dar: Werden nur die sicherheitsunkritischen Daten weiter benötigt, dann kann durch ein Demultiplexing der unterschiedlichen, über den Bus übertragenen Daten eine Datenkorrelation im nachfolgenden Speicher, d.h. dem Eingangsregister, verhindert werden. Das erlaubt die Benutzung einfacher, kleiner Speicherzellen, d.h. **112b**, **112c**. Es ist durch die Verwendung der Isolierschicht (**109b**, **109c**) möglich, die ausgewählten Daten dann weiter über Single-Rail-Busse (**104b1**, **104c1**) zu übertragen und in Single-Rail-Speicherzellen (**112b**, **112c**) abzulegen. All die hier getroffenen Aussagen gelten auch für unkritische Logikteile (Fig. 4).

[0070] Bereits im Vorhergehenden wurde darauf hingewiesen, dass die vorliegende Erfindung auch auf bidirektionale Busse anwendbar ist. In diesem Fall könnte es vorgesehen sein, dass die Verarbeitungsverhinderungseinrichtungen durch zwei Freigabesignale ansteuerbar sind, eines, das das Gelangen eines Signals von dem Bus zum angehängten Schaltungsteil ermöglicht bzw. verhindert, und das andere, das umgekehrt das Gelangen eines Signals von dem an dem Bus angeschlossenen Schaltungsteil zum Bus ermöglicht bzw. verhindert.

[0071] Ferner wird darauf hingewiesen, dass im Vorhergehenden nur Ausführungsbeispiele beschrieben wurden, bei denen die Verhinderung der Verarbeitung dadurch erzielt wurde, dass das Signal auf dem Bus nicht bis zu dem Dateneingang der jeweiligen Empfängerschaltung durchgelassen wurde. Freilich wäre es auch möglich, als Verarbeitungsverhinderungseinrichtung eine Einrichtung vorzusehen, die den jeweiligen Empfängerschaltungsteil von einer Versorgungsspannung trennt, so dass derselbe deaktiviert wird und somit auch nicht in einer von dem Signal auf dem Bus abhängigen Weise zum Gesamtstromverbrauch beiträgt. Insbesondere wäre es hier natürlich möglich, lediglich die Eingangsstufe, nämlich das Eingangsregister, von der Versorgungsspannung zu trennen.

[0072] In Bezug auf die vorbeschriebenen Ausführungsbeispiele wird darauf hingewiesen, dass die vorbeschriebenen Register, wie z.B. die Eingangsregister, auch als Latches oder in anderer Form als Zwischenspeicher ausgebildet sein können.

[0073] Insbesondere wird darauf hingewiesen, dass abhängig von den Gegebenheiten das erfindungsgemäße Schema zur Bus- bzw. Schaltungssteuerung auch in Software implementiert sein kann. Die Implementation kann auf einem digitalen Speichermedium, insbesondere einer Diskette oder einer CD mit elektronisch auslesbaren Steuersignalen erfolgen, die so mit einem programmierbaren Computersystem zusammenwirken können, dass das entsprechende Verfahren ausgeführt wird. Allgemein besteht die Erfindung somit auch in einem Computerprogrammprodukt mit auf einem maschinenlesbaren Träger gespeicherten Programmcode zur Durchführung des erfindungsgemäßen Verfahrens, wenn das Computerprogrammprodukt auf einem Rechner abläuft. In anderen Worten ausgedrückt kann die Erfindung somit als ein Computerprogramm mit einem Programmcode zur Durchführung des Verfahrens realisiert werden, wenn das Computerprogramm auf einem Computer abläuft.

Bezugszeichenliste

100	Schaltung
102	Senderschaltungsteil
104a	Empfängerschaltungsteil
104b	Empfängerschaltungsteil
104b1	Dateneingang
104c	Empfängerschaltungsteil
104c1	Dateneingang
106	Bus
108a	Busanschluss
108b	Busanschluss
108c	Busanschluss
108c1	Railanschluss
108c2	Railanschluss
108d	Busanschluss
109b	Verarbeitungsverhinderungseinrichtung
109c	Verarbeitungsverhinderungseinrichtung
110a	DPA-sichere Logik
110b	DPA-unsichere Logik
110c	DPA-unsichere Logik
112a	Eingangsregister
112b	Eingangsregister
112c	Eingangsregister
114	Bussteuerung
200	Tristate-Buffer
202	Single-Rail-Bus
204	Registerzelle
206	gemeinsamer Steuereingang
208	gemeinsamer Steuereingang
300	Analog-Multiplexer
302	Fakesignaleingang
304	gemeinsamer Steuersignaleingang
400	Bridge
900	Schaltung
902	Senderschaltungsteil
904a	Empfängerschaltungsteil
904b	Empfängerschaltungsteil
904c	Empfängerschaltungsteil
906	Bus
908a	Busanschluss
908b	Busanschluss
908c	Busanschluss
908d	Busanschluss
910a	Logik
910b	Logik
910c	Logik
912a	Eingangsregister
912b	Eingangsregister
912c	Eingangsregister
914	Bussteuerung

Patentansprüche

1. Schaltung mit
einem Bus (**106**);
einem ersten Empfängerschaltungsteil (**104c**), der mit dem Bus (**106**) gekoppelt ist, zum Verarbeiten eines Signals auf dem Bus (**106**);
einem zweiten Empfängerschaltungsteil (**104a**), der mit dem Bus (**106**) gekoppelt ist, zum Verarbeiten eines Signals auf dem Bus (**106**);

einem Senderschaltungsteil (**102**), der mit dem Bus (**106**) gekoppelt ist, zum Ausgeben eines Signals auf dem Bus (**106**); und
einer Einrichtung (**109c**) zum, ansprechend auf ein Steuersignal, Verhindern einer Verarbeitung eines Signals auf dem Bus (**106**) durch den ersten Empfängerschaltungsteil (**104c**).

2. Schaltung gemäß Anspruch 1, bei der die Einrichtung (**109c**) zum Verhindern ausgebildet ist, um die Verhinderung derart vorzunehmen, dass das Signal auf dem Bus (**106**) zu keiner elektrischen Zustandsänderung in dem ersten Empfängerschaltungsteil (**104c**) führt.

3. Schaltung gemäß Anspruch 1 oder 2, bei der die Einrichtung (**109c**) zum Verhindern folgendes Merkmal aufweist:
eine Einrichtung (**109c**) zum Verhindern, dass das Signal auf dem Bus zu dem ersten Empfängerschaltungsteil (**104c**) gelangt, ohne dass in derselben das Signal zu einem Umschaltvorgang führt.

4. Schaltung gemäß einem der vorhergehenden Ansprüche, bei der die Einrichtung (**109c**) zum Verhindern folgendes Merkmal aufweist:
eine Einrichtung (**200**, **300**), die einen Dateneingang, der mit dem Bus (**106**) verbunden ist, einen Datenausgang, der mit dem ersten Empfängerschaltungsteil (**104c**) verbunden ist, und einen Steuereingang (**206**, **304**) aufweist, zum, bei Nichtvorliegen des Steuersignals am Steuereingang, Leiten von Strom zwischen Dateneingang und Datenausgang, und, bei Vorliegen des Steuersignals am Steuereingang, Unterbinden eines Stromflusses zwischen Dateneingang und Datenausgang.

5. Schaltung gemäß einem der vorhergehenden Ansprüche, bei der die Einrichtung (**109c**) zum Verhindern folgendes Merkmal aufweist:
einen Tristate-Buffer (**200**), der einen Dateneingang, einen Datenausgang und einen Steuereingang aufweist und mit Dateneingang und Datenausgang zwischen den Bus (**106**) und den ersten Empfängerschaltungsteil (**104c**) geschaltet ist, wobei der Steuereingang angeschlossen ist, um das Steuersignal zu empfangen.

6. Schaltung gemäß Anspruch 1, bei der die Einrichtung zum Verhindern folgendes Merkmal aufweist:
eine Einrichtung zum Entkoppeln des ersten Empfängerschaltungsteils oder eines Teils davon von einer Versorgungsspannung.

7. Schaltung gemäß einem der vorhergehenden Ansprüche, bei der der erste Empfängerschaltungsteil (**104c**) folgendes Merkmal aufweist:
einen Empfangszwischenspeicher (**112c**) mit einem Zwischenspeichereingang, der mit dem Bus (**106**) gekoppelt ist.

8. Schaltung gemäß Anspruch 7, bei der der Empfangszwischenspeicher (**112c**) des ersten Empfängerschaltungsteils (**104c**) einen Registerausgang und einen Zwischenspeichersteuereingang aufweist, zum Zwischenspeichern des Signals auf dem Bus (**106**) und Ausgeben desselben am Zwischenspeicherausgang auf ein Aktivierungssignal am Zwischenspeichersteuereingang hin, wobei die Schaltung ferner folgendes Merkmal aufweist:
eine Bussteuerung (**114**) zum Senden des Aktivierungssignals an den Zwischenspeichersteuereingang des Empfangszwischenspeichers (**112c**) des ersten Empfängerschaltungsteils (**104c**) und Nichtsenden des Steuersignals an die Einrichtung (**109c**) zum Verhindern, falls der erste Empfängerschaltungsteil (**104c**) Adressat des Signals auf dem Bus (**106**) ist, und zum Senden des Steuersignals an die Einrichtung (**109c**) zum Verhindern, falls der erste Empfängerschaltungsteil (**104c**) nicht Adressat des Signals auf dem Bus (**106**) ist.

9. Schaltung gemäß Anspruch 8, bei dem die Bussteuerung (**114**) ausgebildet ist, um das Steuersignal in dem Fall, dass der erste Empfängerschaltungsteil (**104c**) nicht Adressat des Signals auf dem Bus (**106**) ist, nur zu senden, wenn ein Signal auf dem Bus ein Geheimnis betrifft, und in dem Fall, dass das Signal auf dem Bus kein Geheimnis betrifft, das Aktivierungssignal nicht an den Empfangszwischenspeicher (**102c**) des ersten Empfängerschaltungsteils (**104c**) und das Steuersignal nicht an die Einrichtung (**109c**) zum Verhindern zu senden.

10. Schaltung gemäß einem der Ansprüche 1 bis 6, bei der der erste Empfängerschaltungsteil (**104c**) folgendes Merkmal aufweist:
eine Logik (**110c**, **104c**) mit einem Logikeingang, der mit dem Bus (**106**) unmittelbar verbunden ist.

11. Schaltung gemäß einem der Ansprüche 1 bis 10, bei der der zweite Empfängerschaltungsteil (**104a**)

folgendes Merkmal aufweist:
einen Empfangszwischenspeicher (**102a**), das einen Zwischenspeichereingang, der mit dem Bus (**106**) gekoppelt ist, einen Zwischenspeicherausgang und einen Zwischenspeichersteuereingang aufweist, zum Zwischenspeichern des Signals auf dem Bus (**106**) und Ausgeben desselben am Zwischenspeicherausgang auf ein Aktivierungssignal am Zwischenspeichersteuereingang hin, und bei der die Schaltung ferner folgendes Merkmal aufweist:
eine Bussteuerung (**114**) zum Senden des Aktivierungssignals an den Zwischenspeichersteuereingang des Empfangszwischenspeichers (**112a**) des zweiten Empfängerschaltungsteils (**104a**), falls der zweite Empfängerschaltungsteil (**104a**) Adressat des Signals auf dem Bus (**106**) ist.

12. Schaltung gemäß einem der Ansprüche 1 bis 11, bei der der zweite Empfängerschaltungsteil (**104a**) ein Dual-Rail-Precharge-Empfangszwischenspeicher (**102a**) aufweist.,

13. Schaltung gemäß einem der Ansprüche 1 bis 12, bei der der zweite Empfängerschaltungsteil (**104a**) DPA-sicherer implementiert ist als der erste Empfängerschaltungsteil (**104c**).

14. Schaltung gemäß einem der vorhergehenden Ansprüche, bei der der erste und der zweite Empfängerschaltungsteil derart mit dem Bus (**106**) verbunden sind, dass sie in dem Fall keiner Verhinderung das Signal auf dem Bus ohne Zwischenspeicherung erhalten.

15. Schaltung gemäß einem der vorhergehenden Ansprüche, bei der die Einrichtung zum Verhindern einen Analog-Multiplexer/Demultiplexer aufweist.

16. Schaltung gemäß einem der vorhergehenden Ansprüche, bei der der Bus ein Dual-Rail-Precharge-Bus ist.

17. Verfahren zur Steuerung einer Schaltung mit einem Bus (**106**), einem ersten Empfängerschaltungsteil (**104c**), der mit dem Bus (**106**) gekoppelt ist, zum Verarbeiten eines Signals auf dem Bus (**106**), einem zweiten Empfängerschaltungsteil (**104a**), der mit dem Bus (**106**) gekoppelt ist, zum Verarbeiten eines Signals auf dem Bus (**106**) und einem Senderschaltungsteil (**102**), der mit dem Bus (**106**) gekoppelt ist, zum Ausgeben eines Signals auf dem Bus (**106**), wobei das verfahren folgendes Merkmal aufweist:
eine Einrichtung (**109c**) zum, ansprechend auf ein Steuersignal, Verhindern einer Verarbeitung eines Signals auf dem Bus (**106**) durch den ersten Empfängerschaltungsteil (**104c**).

18. Computer-Programm mit einem Programmcode zur Durchführung des Verfahrens nach Anspruch 17, wenn das Computer-Programm auf einem Computer abläuft.

Es folgen 4 Blatt Zeichnungen

Anhängende Zeichnungen

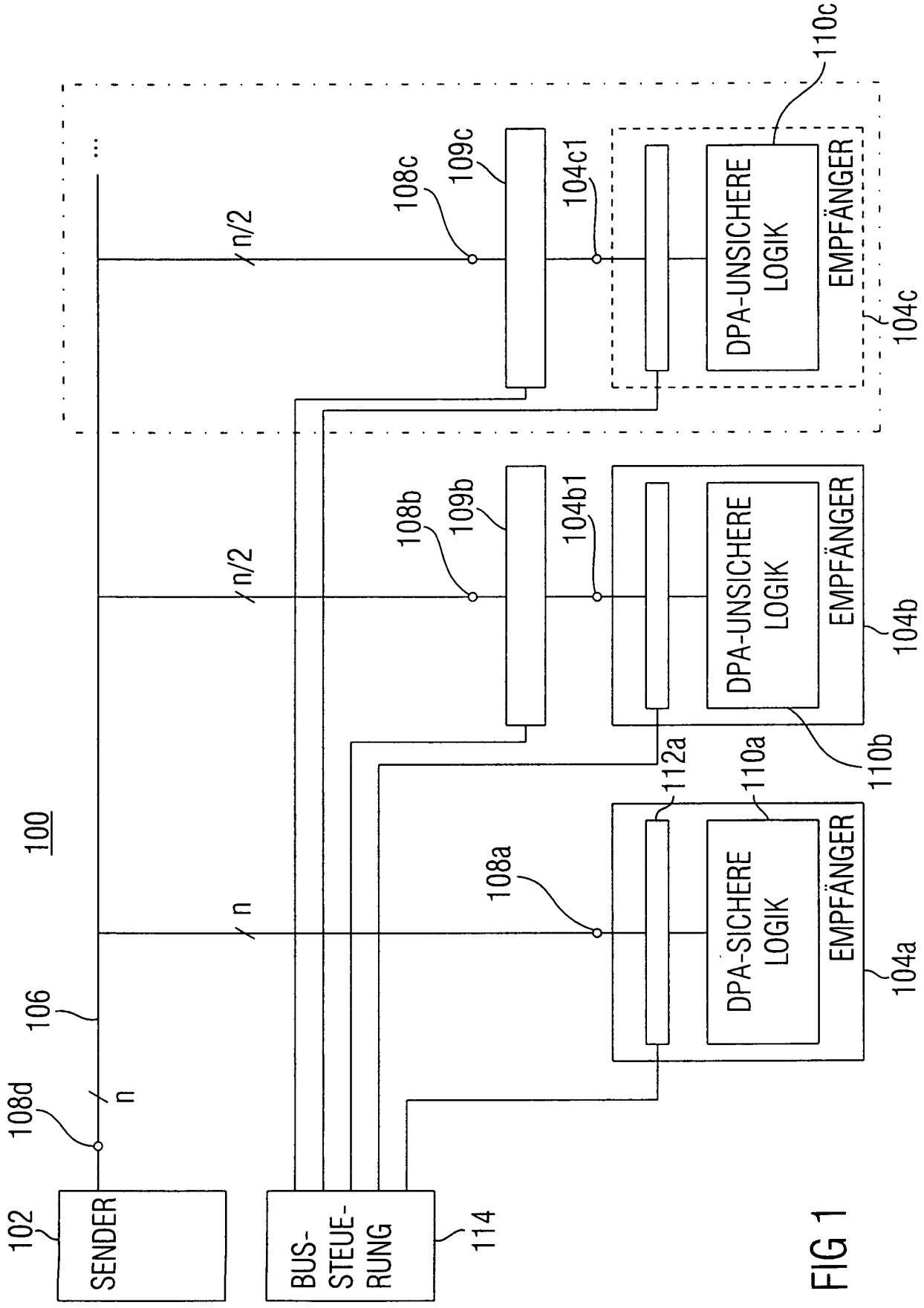


FIG 1

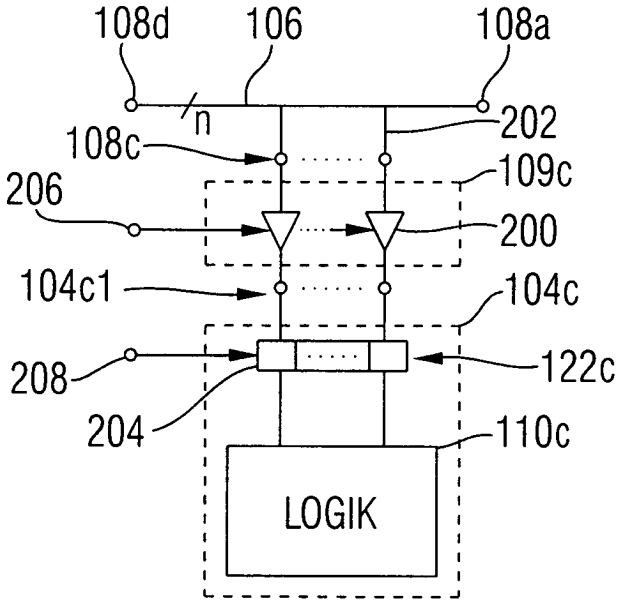


FIG 2

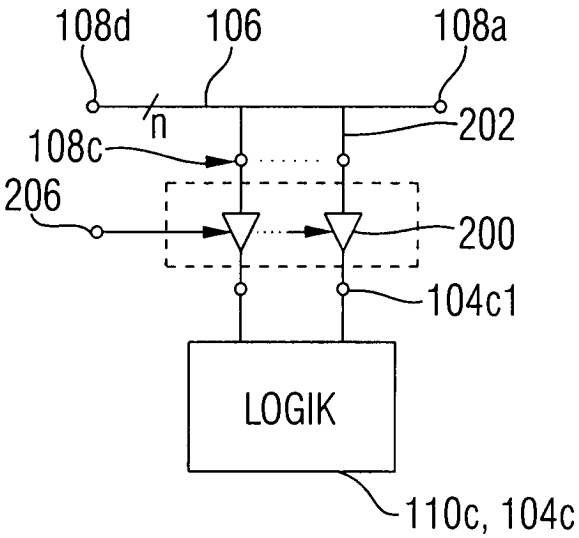


FIG 4

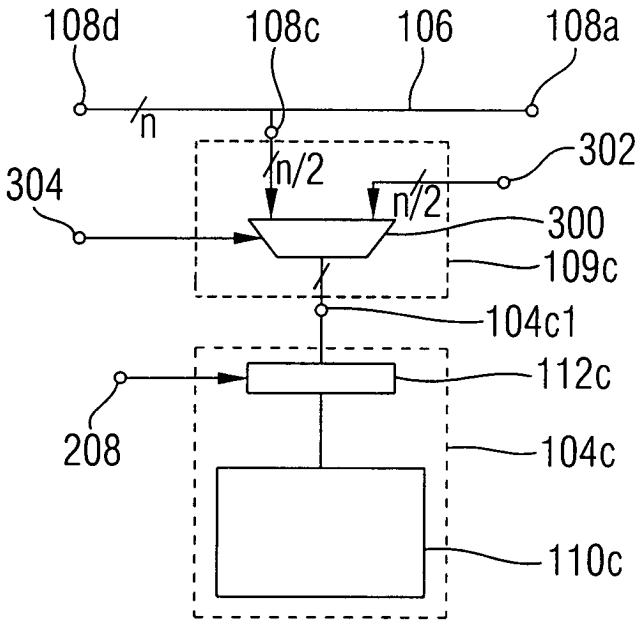


FIG 3

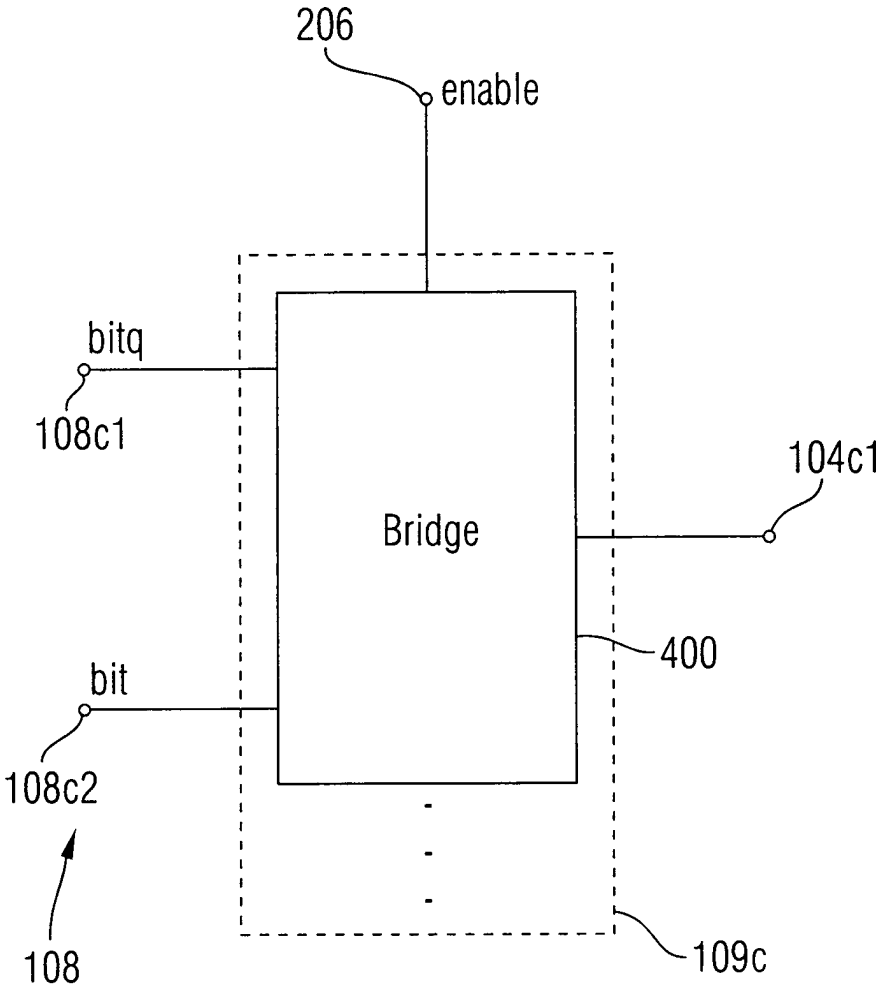


FIG 5

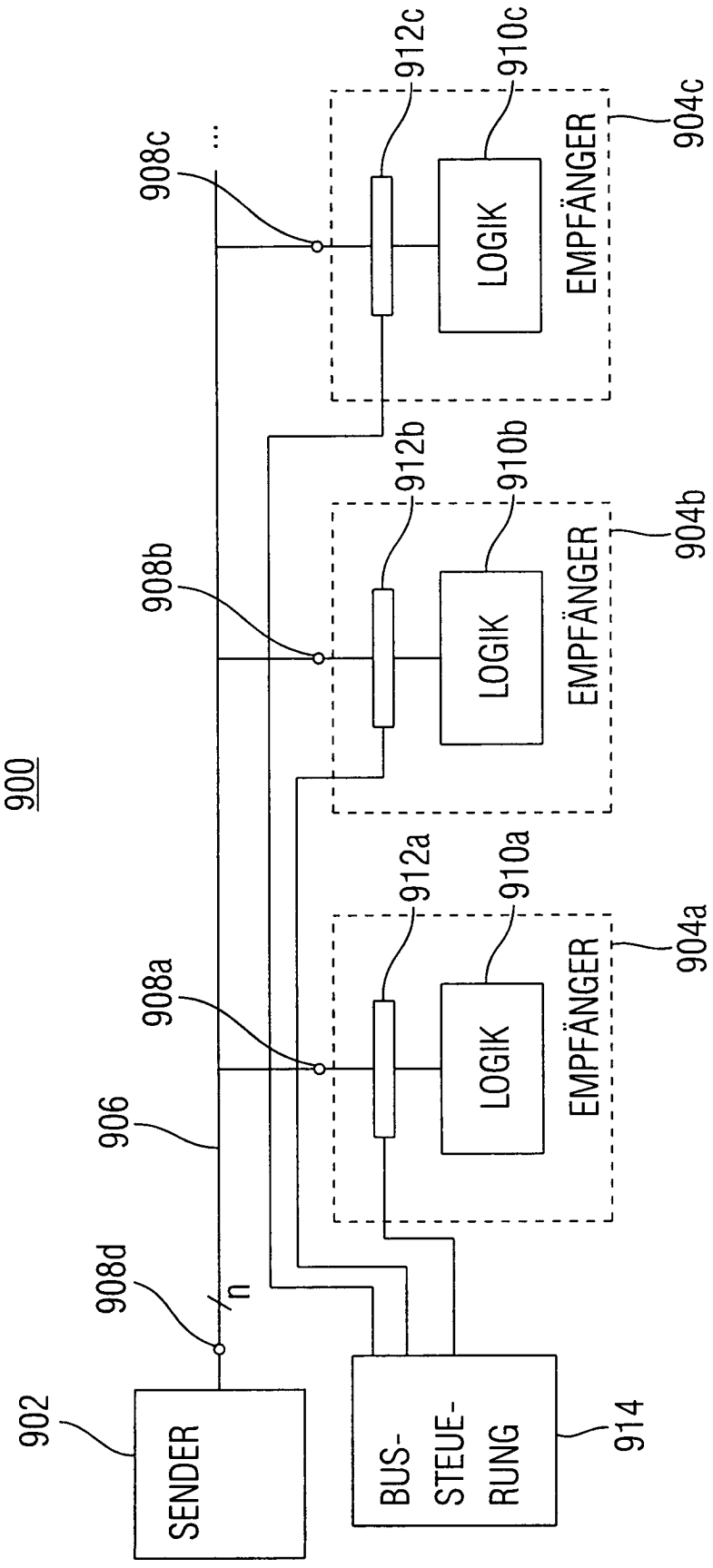

900
902
SENDER
908d
n
906
908a
908b
908c
...
912a
910a
LOGIK
EMPFÄNGER
904a
912b
910b
LOGIK
EMPFÄNGER
904b
912c
910c
LOGIK
EMPFÄNGER
904c
BUS-
STEUE-
RUNG
914

FIG 6