(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
11. Dezember 2003 (11.12.2003)

PCT

(10) Internationale Veröffentlichungsnummer
WO 03/102786 A2

(51) Internationale Patentklassifikation[7]: G06F 13/00

(21) Internationales Aktenzeichen: PCT/EP03/05641

(22) Internationales Anmeldedatum:
28. Mai 2003 (28.05.2003)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
102 24 742.0 4. Juni 2002 (04.06.2002) DE

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: **INFINEON TECHNOLOGIES AG** [DE/DE]; St.-Martin-Str. 53, 81669 München (DE).

(72) Erfinder; und

(75) Erfinder/Anmelder *(nur für US)*: **ELBE, Astrid** [DE/DE]; Am Stadtpark 40 B, 81243 München (DE). **JANSSEN, Norbert** [DE/DE]; Innere Wiener Str. 13 A, 81667 München (DE). **SEDLAK, Holger** [DE/DE]; Kramergasse 2 A, 82054 Sauerlach (DE).

(74) Anwälte: **ZINKLER, Franz** usw.; Schoppe, Zimmermann, Stöckeler & Zinkler, Postfach 246, 82043 Pullach bei München (DE).

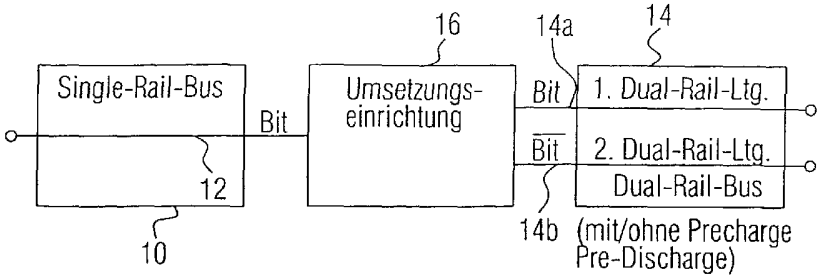
(81) Bestimmungsstaaten *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Bestimmungsstaaten *(regional)*: ARIPO-Patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), eurasisches Patent (AM, AZ, BY, KG, KZ, MD, RU, TJ,

[Fortsetzung auf der nächsten Seite]

(54) Title: DATA PROCESSING CIRCUIT AND METHOD FOR TRANSMITTING DATA

(54) Bezeichnung: DATENVERARBEITUNGSSCHALTUNG UND VERFAHREN ZUM ÜBERTRAGEN VON DATEN



A... SINGLE RAIL BUS
B... BIT
C... CONVERSION DEVICE
D... DUAL RAIL LINE
E... DUAL RAIL BUS
F... (WITH/WITHOUT PRECHARGE PRE-DISCHARGE)

(57) Abstract: The invention relates to a data processing circuit comprising a single rail bus (10) having a single rail line (12), a dual rail bus (14) having a first dual rail line (14a) for data bits and a second dual rail line (14b) for inverted data bits, and a conversion device (16) for converting signals on the single rail bus into signals on the dual rail bus and vice versa. By using both the single rail technique and the dual rail technique with precharge or pre-discharge or without pre-charge in a data processing circuit, an optimum compromise is achieved between security on the one hand and chip surface consumption and power consumption on the other. According to the invention, regions in which security-critical data is processed are embodied according to the dual rail technique, whereas regions in which less security-critical data is processed are embodied according to the single rail technique, and interfaces located between said regions are provided with a conversion device.

[Fortsetzung auf der nächsten Seite]

WO 03/102786 A2

TM), europäisches Patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI-Patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Veröffentlicht:

— *ohne internationalen Recherchenbericht und erneut zu veröffentlichen nach Erhalt des Berichts*

Zur Erklärung der Zweibuchstaben-Codes und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

(57) Zusammenfassung: Eine Datenverarbeitungsschaltung umfaßt einen Single-Rail-Bus (10) mit einer Single-Rail-Leitung (12), einen Dual-Rail-Bus (14) mit einer ersten Dual-Rail-Leitung (14a) für Datenbits und einer zweiten Dual-Rail-Leitung (14b) für invertierte Datenbits sowie eine Umsetzungseinrichtung (16) zum Überführen von Signalen auf dem Single-Rail-Bus in Signale auf dem Dual-Rail-Bus und umgekehrt. Durch Einsetzen sowohl der Single-Rail-Technik als auch der Dual-Rail-Technik mit Precharge oder Pre-Discharge oder ohne Precharge in einer Datenverarbeitungsschaltung wird ein optimaler Kompromiß zwischen Sicherheit einerseits und Chipflächenverbrauch und Leistungsverbrauch andererseits erreicht, indem Bereiche, in denen sicherheitskritische Daten verarbeitet werden, in Dual-Rail-Technik ausgeführt werden, während Bereiche, in denen weniger sicherheitskritische Daten verarbeitet werden, in Single-Rail-Technik ausgeführt werden, und wobei Schnittstellen zwischen diesen Bereichen mit einer Umsetzungseinrichtung versehen werden.

Beschreibung

Datenverarbeitungsschaltung und Verfahren zum Übertragen von Daten

Die vorliegende Erfindung bezieht sich auf Prozessorarchitekturen und insbesondere auf eine Datenverarbeitungsschaltung und auf ein Verfahren zum Übertragen von Daten, bei denen die Sicherheit gegenüber externen Angriffen zum Ausspähen von Daten erhöht ist.

Kryptographische Algorithmen zeichnen sich im allgemeinen dadurch aus, daß sicherheitsrelevante Daten verarbeitet werden. Solche sicherheitsrelevanten Daten sind beispielsweise ein privater Schlüssel bei einem asymmetrischen Kryptographiealgorithmus, wie z. B. dem RSA-Algorithmus. Der private Schlüssel wird dazu verwendet, Daten zu entschlüsseln, die mit einem entsprechenden öffentlichen Schlüssel verschlüsselt worden sind. Alternativ wird der private Schlüssel dazu verwendet, eine digitale Signatur zu Authentifizierungszwecken mit dem dazugehörigen öffentlichen Schlüssel zu verarbeiten.

Solche Prozessoren verarbeiten jedoch nicht nur Daten unter Verwendung privater bzw. geheimer Schlüssel, sondern umfassen typischerweise auch personenbezogene Daten, die gegenüber Angriffen geschützt werden müssen, wie z. B. persönliche Daten oder Guthaben, wenn an eine Geldkarte gedacht wird. Selbstverständlich gehört auch die PIN einer ec-Karte zu solchen geheimen Daten, die unbedingt gegenüber externen Angriffen zu schützen sind, um eine Akzeptanz eines solchen kryptographischen Systems am Markt zu erreichen.

Ein spezielles Gebiet, auf dem Kryptographiealgorithmen immer mehr zum Einsatz kommen, sind Chipkarten oder Sicherheits-ICs. Insbesondere bei Chipkarten besteht eine weitere Anforderung dahingehend, daß der Platz für ein Chipkarten-Prozessorsystem begrenzt ist. Die zur Verfügung stehende

Chipfläche, die typischerweise vorgegeben ist, muß möglichst gut genutzt werden, um zum einen ein Rechenwerk und einen Arbeitsspeicher sowie einen nicht-flüchtigen Speicher unterzubringen, und um zum anderen auch die zu einem Kryptographieprozessorsystem gehörenden Peripherieelemente unterzubringen, wie z. B. einen Krypto-Coprozessor, einen Zufallszahlengenerator, einen Eingabe/Ausgabe-Port, etc.

Bekannte Attacken auf kryptographische Systeme sind die sogenannten Power-Analysis-Attacken. Nachdem Kryptographieprozessoren typischerweise in CMOS-Technik realisiert werden, haben solche Schaltungen, wenn keine besonderen Gegenmaßnahmen getroffen werden, einen stark inhomogenen Leistungsverbrauch. Bekannterweise verbrauchen CMOS-Schaltungen nahezu keine Leistung, wenn sich Zustände auf einem Bus bzw. in einem Rechenwerk nicht ändern. Ändern sich jedoch Zustände in einem Rechenwerk oder auf einem Bus, so fließt während des Umschaltens einer CMOS-Schaltung von einem Zustand in einen anderen Zustand ein Strom, der von einer Leistungsquelle eingespeist werden muß. Insbesondere gilt dies für Bus-Treiberschaltungen, die insbesondere dann, wenn die Datenbusse lang sind, neben dem eigentlichen Stromverbrauch, den die CMOS-Schaltung hat, auch einen Strom zum Umladen von Leitungskapazitäten liefern müssen, die bei solchen langen Bussen ganz erhebliche Werte einnehmen können.

Hinzu kommt, daß für Kryptographieprozessoren zum einen aus Sicherheitsgründen und zum anderen aus Performance-Gründen Langzahlrechenwerke eingesetzt werden. Solche Langzahlrechenwerke haben mitunter eine Datenbreite von z. B. mehr als 1024 oder - in jüngster Zeit - mehr als 2048 Bits. Ein solches Langzahlrechenwerk umfaßt eine entsprechende Anzahl von Bit-Slices, wobei ein Bit-Slice neben der eigentlichen arithmetischen Einheit, die typischerweise zumindest eine Volladdiererfunktion umfaßt, auch Registerzellen für mehrere Register hat, die zum Ausführen einer kryptographischen Operation, wie z. B. einer modularen Multiplikation, benötigt werden.

In der DE 3631992 C1 ist ein Langzahlrechenwerk offenbart, das zur Ausführung einer modularen Exponentiation, die für den RSA-Algorithmus benötigt wird, als zentrales Element einen Langzahl-3-Operanden-Addierer umfaßt. Die modulare Exponentiation wird in eine Vielzahl modularer Multiplikationen zerlegt, welche wiederum in eine Vielzahl von 3-Operanden-Additionen zerlegt werden. Unter Verwendung eines Multiplikations-Vorausschau-Algorithmus und eines damit gekoppelten Reduktions-Vorausschau-Algorithmus ergibt sich eine 3-Operanden-Operation, bei der ein Zwischenergebnis, der Multiplikand und der Modul, möglicherweise mit Verschiebungswerten und Look-Ahead-Parametern multipliziert, addiert werden, um ein neues Zwischenergebnis zu ergeben.

Innerhalb einer Bit-Slice existiert ein sogenannter Slice-interner Bus, der die Registerplätze innerhalb der Bit-Slice und das Slice-Rechenwerk miteinander verbindet. Die Bit-Slices des Rechenwerks sind über einen Rechenwerks-internen Bus, welcher typischerweise lediglich eine Datenbreite von z. B. acht Bit hat, miteinander und mit den anderen Elementen des Kryptographie-Datenverarbeitungssystems z. B. über einen externen Bus verbunden.

In Anbetracht der Tatsache, daß ein Langzahlrechenwerk aus sehr vielen Bit-Slices besteht, ist dieser Rechenwerks-interne Bus, der außerhalb der Bit-Slices verläuft, ein sehr langer Datenbus, welcher eine Länge von mehreren Millimetern aufweist und als sehr regelmäßige Struktur auf der integrierten Schaltung erkennbar ist. Dasselbe gilt für das Langzahlrechenwerk selbst, das aus einem oder mehreren Stapeln von Bit-Slices besteht.

In Anbetracht der Tatsache, daß bei typischen Sicherheits-ICs die Chipfläche selbst begrenzt ist, und zudem auch der Stromverbrauch eine Rolle spielt, die besonders dann wesentlich ist, wenn Kontaktlosanwendungen betrachtet werden, bei denen

die Chipkarte selbst keine eigene Leistungsversorgung hat, sondern ihre Leistung aus dem umgebenden HF-Feld bezieht, ergeben sich Anforderungen an den Rechenwerks-internen Bus einerseits und die Bit-Slices andererseits, daß sowohl Chipfläche gespart wird als auch der Stromverbrauch niedrig zu halten ist.

Andererseits existieren bei Sicherheits-ICs Anforderungen, daß Maßnahmen gegenüber externen Angriffen, wie z. B. Leistungsattacken, von denen die einfachen Leistungsattacken (SPA) oder die differentiellen Leistungsattacken (DPA) die bekanntesten Vertreter sind, zu treffen sind. Ohne solche Maßnahmen könnte ein Angreifer durch eine Leistungsanalyse beispielsweise auf dem Rechenwerks-Bus oder auf einem Slice-internen Bus jeden Umschaltvorgang mit verfolgen und bräuchte dann nur noch einen Anfangszustand oder Zwischen-Datenzustand ermitteln, um sämtliche verarbeiteten Daten mitprotokollieren zu können, um so unter Kenntnis des ausgeführten Algorithmus und weiterer Randbedingungen geheime Daten, wie z. B. geheime Schlüssel, PINs, Guthaben-Beträge, etc. eruieren zu können.

Eine hinsichtlich der Sicherheit optimale Methode besteht darin, jeden Datenbus - bezogen auf eine Bitleitung - nicht mehr als eine einzige Datenleitung auszuführen, sondern als zwei Datenleitungen. Diese sogenannte Dual-Rail-Technik basiert darauf, daß zu einem Zeitpunkt auf den beiden Daten komplementäre Zustände übertragen werden. Liegt auf einer ersten Dual-Rail-Leitung für einen bestimmten Zeitpunkt ein Spannungszustand an, der eine logische „1" darstellt, so liegt auf der zweiten Dual-Rail-Leitung der komplementäre Zustand an, also im Beispiel ein Spannungszustand, der einer logischen „0" entspricht. Damit wird bereits die Sicherheit dahingehend erhöht, daß bei jeder Umschaltung von einem Zustand zu einem anderen Zustand beide Leitungen schalten, so daß durch eine Leistungsanalyse nicht mehr ermittelbar ist, in welcher Richtung umgeschaltet worden ist, da immer beide Umschaltrichtungen gleichzeitig auftreten.

Obgleich bereits ein Sicherheitszuwachs erhalten worden ist, wird dennoch anhand der Leistungsanalyse erkennbar sein, ob in aufeinanderfolgenden Zyklen umgeschaltet worden ist, oder nicht. Liegen nämlich beispielsweise fünf aufeinanderfolgende logische „1"-Zustände an, so wird in der Leistungscharakteristik kein Stromverbrauch erkennbar sein, so daß ein Angreifer immer noch die Information erhalten kann, daß sich in diesen fünf Zyklen in den Daten auf dem Dual-Rail-Bus nichts geändert hat.

Um auch dieses Sicherheitsleck zu eliminieren, wird die sogenannte Dual-Rail-Technik mit Precharge verwendet. Hier wird zwischen jedem Datentakt ein sogenannter Precharge-Takt eingespeist. In diesen Precharge-Takt werden sowohl die erste Dual-Rail-Leitung als auch die zweite Dual-Rail-Leitung auf einen logisch hohen Zustand gebracht, so daß immer, also wenn von einem Daten-Takt zu einem Precharge-Takt gegangen wird, oder wenn von einem Precharge-Takt zu einem Daten-Takt gegangen wird, und unabhängig davon, ob die Daten sich von einem Takt zum nächsten ändern, eine einzige Umschaltung im Stromprofil erkennbar sein wird.

Obgleich die Dual-Rail-Technik mit Precharge eine maximale Sicherheit liefert, wird hierfür dennoch mit maximalem Aufwand bezahlt. Nachdem jede Bitleitung doppelt ausgeführt werden muß, führt die Dual-Rail-Technik zu einem doppelten Chipflächenverbrauch für die Übertragungsbusse. Nachdem ferner nach jedem Datentakt ein Precharge-Takt eingestreut wird, führt diese Technik auch zu einer halb so großen Verarbeitungsgeschwindigkeit, da in den Precharge-Takten keine Nutzdaten verarbeitet werden.

Nachdem ferner zwei Datenleitungen umgeladen werden müssen und dafür zwei Leitungstreiber - statt einem Leitungstreiber bei Single-Rail - existieren, ist auch der Stromverbrauch doppelt so groß. Die maximale Sicherheit wird somit teuer er-

kauft, nämlich durch einen doppelt so großen Chipflächenverbrauch, einen halb so großen Nutzdatendurchsatz und einen doppelten Stromverbrauch.

Aus diesen Gründen kommt die Dual-Rail-Technik mit Precharge trotz der bereitgestellten überlegenen Sicherheit gegenüber Leistungs-Angriffen typischerweise nicht bei Sicherheits-ICs zum Einsatz.

Typischerweise werden daher alternativ Lösungen eingesetzt, wie z. B. Dummy-Berechnungen zum Verschleiern des Leistungsprofils, Software-technische Algorithmen, die - unabhängig von den verarbeiteten Daten - die gleiche Anzahl von Zyklen erfordern, etc. Allen diesen Maßnahmen ist gemeinsam, daß sie gegenüber komplexeren Angriffsalgorithmen keine maximale Sicherheit liefern bzw. Eingriffe in bereits bestehende Routinen erfordern, die dazu führen, daß für die Routinen wieder aufwendige Tests etc. gefahren werden müssen, so daß sich zum einen die Kosten erhöhen und zum anderen die Zeit erhöht, in der ein neues Produkt auf den Markt gebracht werden kann. Diese beiden Punkte sind zusätzlich zu bestimmten Sicherheitsanforderungen wesentlich dafür, ob sich ein Kryptographie-Prozessorchip auf dem sehr wettbewerbsintensiven Markt durchsetzt oder nicht.

Die Aufgabe der vorliegenden Erfindung besteht darin, ein Konzept für eine sichere und dennoch wirtschaftliche Datenverarbeitung zu schaffen.

Diese Aufgabe wird durch eine Datenverarbeitungsschaltung nach Patentanspruch 1 oder durch ein Verfahren zum Übertragen von Daten nach Patentanspruch 20 gelöst.

Der vorliegenden Erfindung liegt die Erkenntnis zugrunde, daß aus Sicherheitsgründen bestimmte Teile eines Sicherheits-ICs in Dual-Rail-Technik mit oder ohne Precharge bzw. Pre-Discharge ausgeführt werden, während andere Bereiche, auf de-

nen nicht derart Sicherheits-relevante Daten verarbeitet werden nach wie vor in Single-Rail-Technik auszuführen sind. An der Schnittstelle zwischen dem Single-Rail-Bus und dem Dual-Rail-Bus wird erfindungsgemäß eine Umsetzungseinrichtung plaziert, um Signale auf dem Single-Rail-Bus in Signale auf dem Dual-Rail-Bus oder umgekehrt umzusetzen.

Die erfindungsgemäße Kombination eines Single-Rail-Busses und eines Dual-Rail-Busses aufgrund der dazwischenliegenden Umsetzungseinrichtung ermöglicht es, in einem Sicherheits-ICs beide Bus-Typen zu verwenden, um einen optimalen Kompromiß zwischen Sicherheit einerseits und Wirtschaftlichkeit andererseits zu erreichen.

Bei einem bevorzugten Ausführungsbeispiel der vorliegenden Erfindung werden die Slice-internen Busse in Dual-Rail-Technik mit oder ohne Pre-Charge/Dis-Charge ausgeführt, während der in seiner Länge und damit in seinem Flächenverbrauch ganz erhebliche Rechenwerks-interne Bus, welcher extern der Slices verläuft und die Slices miteinander verbindet, nach wie vor in Single-Rail-Technik ausgeführt wird, so daß jeder Bit-Slice ferner eine eigene Umsetzungseinrichtung zugeordnet ist. Alternativ kann die Umsetzungseinrichtung auch am Eingang des Multiplexers zum Verbinden des Rechenwerks-Busses, der typischerweise eine kleine Bandbreite hat, wie z. B. lediglich acht Bits, mit den Rechenwerks-Slices, die z. B. mehr als 2048 in ihrer Anzahl sein können, vorgesehen. In diesem Fall wäre der gesamte Multiplexer in Dual-Rail-Technik ausgeführt. Im anderen Ausführungsbeispiel, bei dem die Umsetzungseinrichtung direkt am Eingang der Bit-Slices angeordnet ist, muß der Multiplexer lediglich in Single-Rail-Technik ausgeführt werden, da erst am Ausgang des Multiplexers umgesetzt wird.

Das erfindungsgemäße Konzept ist dahingehend vorteilhaft, daß die sicherheitsmäßig optimale Dual-Rail-Technik mit Precharge nunmehr auch in einem Sicherheits-IC einsetzbar ist, der

strengen Chipflächenanforderungen und strengen Leistungsverbrauchanforderungen genügen muß. Erfindungsgemäß werden somit die Sicherheitsvorteile der Dual-Rail-Technik mit Precharge mit den Flächen- und Stromvorteilen der Single-Rail-Lösung kombiniert, indem eine Umsetzung von Dual-Rail auf Single-Rail und umgekehrt innerhalb eines Sicherheits-ICs an einer oder beliebig vielen Stellen eingesetzt wird. Diese Lösung macht kaum Abstriche von der Sicherheit des Systems, wenn die sich ständig ändernden Daten auf der Dual-Rail-Seite liegen, während die Single-Rail-Seite für seltenere Abläufe, wie z. B. das Lesen und Schreiben von sich nicht ändernden Daten, wie z. B. Initialisierungswerte, Endergebnis, etc., verwendet wird. Dies wird vorzugsweise dadurch erreicht, daß die Slice-internen Busse als Dual-Rail-Busse ausgeführt werden, während alle anderen Busse in der erfindungsgemäßen Datenverarbeitungsschaltung in Single-Rail-Technik auszuführen sind, um Platz und Strom zu sparen, ohne daß nennenswerte Sicherheitsabstriche hingenommen werden müssen, da die sicherheitsmäßig-hochrelevanten Slice-internen Busse in sicherer Dual-Rail-Technik mit Precharge ausgeführt sind.

Bevorzugte Ausführungsbeispiele der vorliegenden Erfindung werden nachfolgend Bezug nehmend auf die beiliegenden Zeichnungen detailliert erläutert. Es zeigen:

Fig. 1 ein Prinzip-Blockschaltbild einer erfindungsgemäßen Datenverarbeitungsschaltung;

Fig. 2 ein bevorzugtes Ausführungsbeispiel der vorliegenden Erfindung am Beispiel eines Langzahlrechenwerks mit Rechenwerks-internem Bus in Single-Rail und Bitslice-internem Bus in Dual-Rail;

Fig. 3 eine Detaildarstellung eines Bit-Slices in Dual-Rail-Technik;

Fig. 4 eine Umsetzungseinrichtung gemäß einem bevorzugten Ausführungsbeispiel für Dual-Rail mit Precharge; und

Fig. 5 eine Umsetzungseinrichtung gemäß einem alternativen Ausführungsbeispiel in Dual-Rail-Technik ohne Precharge.

Fig. 1 zeigt eine erfindungsgemäße Datenverarbeitungsschaltung mit einem Single-Rail-Bus 10, wobei der Single-Rail-Bus eine Single-Rail-Leitung 12, die in Fig. 1 auch als Bit-Leitung bezeichnet ist, für eine Folge von Datenbits aufweist.

Die erfindungsgemäße Datenverarbeitungsschaltung umfaßt ferner einen Dual-Rail-Bus, der zwei Dual-Rail-Leitungen 14a, 14b für die Folge von Datenbits aufweist, wobei eine erste Dual-Rail-Leitung 14a für eine Folge von Datenbits vorgesehen ist, und wobei eine zweite Dual-Rail-Leitung 14b für eine Folge von invertierten Datenbits vorgesehen ist.

Die erfindungsgemäße Datenverarbeitungsschaltung umfaßt ferner eine Umsetzungseinrichtung 16 zum Überführen von Signalen auf dem Single-Rail-Bus 12 in Signale auf den Dual-Rail-Bus 14 und umgekehrt.

Fig. 2 zeigt eine Datenverarbeitungsschaltung gemäß einem bevorzugten Ausführungsbeispiel der vorliegenden Erfindung, die als Single-Rail-Bus 12 einen Rechenwerks-Bus umfaßt. Aus Einfachheitsgründen ist der Rechenwerksbus 12 in Fig. 2 lediglich als eine einzige Leitung gezeichnet, wobei jedoch der Rechenwerks-Bus 12 insgesamt ein paralleler Bus ist und k Datenleitungen umfaßt, wobei k beispielsweise gleich 8 oder 16 ist.

Der Rechenwerks-Bus 12 ist über einen Multiplexer 18 mit der Umsetzungseinrichtung 16 verbunden, die wiederum mit Dual-

Rail-Bussen für jede Bit-Slice 1, ..., n eines Langzahlrechenwerks 20 verbunden ist. Das Langzahlrechenwerk umfaßt eine Anzahl von n Bit-Slices, die größer als 2048 ist und beispielsweise 2100 oder auch 2300 Bit-Slices umfaßt. Erfindungsgemäß sind die Slice-internen Busse als Dual-Rail-Busse ausgeführt, während der Rechenwerks-Bus, der die einzelnen Slices untereinander bzw. die einzelnen Slices mit anderen Komponenten des Sicherheits-ICs verbindet, in Single-Rail-Technik ausgeführt ist. Bei dem in Fig. 2 gezeigten Ausführungsbeispiel der vorliegenden Erfindung ist jeder Bit-Slice eine eigene Single-Rail/Dual-Rail-Umsetzungseinrichtung 16 zugeordnet, derart, daß der Multiplexer 18 in Single-Rail-Technik ausgeführt ist. Bei einem alternativen Ausführungsbeispiel könnte jedoch auch der Multiplexer-Eingang, der bei dem in Fig. 2 gezeigten Ausführungsbeispiel acht Bit breit ist, bereits mit einer Umsetzungs-Einrichtung für jede Bitleitung versehen sein, wobei der Multiplexer dann komplett in Dual-Rail-Technik ausgeführt sein müßte. Diese Lösung kann unter Umständen günstiger sein, da wesentlich weniger Umsetzungseinrichtungen benötigt werden, nämlich bei dem in Fig. 2 gezeigten Beispiel lediglich 8 anstatt von 2100 Umsetzungseinrichtungen.

Fig. 3 zeigt eine schematische Darstellung einer Bit-Slice i. Jede Bit-Slice umfaßt eine arithmetische Einheit AU_i, die in Fig. 3 mit dem Bezugszeichen 22 bezeichnet ist, sowie eines oder mehrere Registerplätze $R1_i$, $R2_i$, $R3_i$, wobei die Registerplätze mit 24a, 24b, 24c bezeichnet sind. Jedes Register-Bit ist untereinander und mit der arithmetischen Einheit 22 in der Bit-Slice über einen Dual-Rail-Bus verbunden, der die erste Dual-Rail-Leitung 14a und die zweite Dual-Rail-Leitung 14b für die invertierten Bits ($\overline{BIT}$) aufweist. Die Ausführung jeder Bit-Slice i in Dual-Rail-Technik stellt sicher, daß die Daten, die zwischen den Registern 24a, 24b, 24c und der arithmetischen Einheit 22 kommuniziert werden, für eine Leistungsanalyse unangreifbar sind. Diese Daten sind typischer-

weise sensible Daten und werden erfindungsgemäß stark geschützt.

Dagegen sind die Daten, die auf dem Rechenwerks-Bus 12 transportiert werden, typischerweise keine derart Sicherheitssensitiven Daten, so daß die Ausführung des Rechenwerks-Busses 12 in Single-Rail-Technik zu keinen besonders großen Sicherheitsabstrichen führt, jedoch zu erheblichen Einsparungen an Chipfläche, Leistungsverbrauch und Verarbeitungszeit.

Im nachfolgenden wird Bezug nehmend auf Fig. 4 auf ein bevorzugtes Ausführungsbeispiel einer Umsetzungseinrichtung 16 Bezug genommen, die für eine Dual-Rail-Technik mit Precharge geeignet ist, während Bezug nehmend auf Fig. 5 auf eine Umsetzungseinrichtung 16 Bezug genommen wird, die für eine Dual-Rail-Technik ohne Precharge vorgesehen ist.

Die Umsetzungseinrichtung 16 in Fig. 4 ist an ihrem Eingang mit der Bitleitung 12 des Single-Rail-Busses verbunden. Ausgangsseitig ist sie mit der ersten Dual-Rail-Leitung 14a für Datenbits und mit der zweiten Dual-Rail-Leitung für invertierte Datenbits (14b) verbunden.

Die Single-Rail-Leitung 12 ist mit einem ersten Knoten 40 verbunden, welcher mit einem Ausgang eines Lesen-Treibers 42 einerseits und mit einem Eingang eines Schreiben-Treibers 44 verbunden ist. In den Lesen-Treiber 42 wird als Eingangssignal 46 ein Lesen-Treiber-Steuersignal eingespeist. In den Schreiben-Treiber 44 wird ebenfalls ein Schreiben-Treiber-Steuersignal 48 eingespeist. Ein weiterer Eingang der Lesen-Treiber-Schaltung 42 ist mit der ersten Dual-Rail-Leitung 14a verbunden.

Die erste Dual-Rail-Leitung 14a ist ferner über einen Knoten 50 sowohl mit einem Ausgang des Schreiben-Treibers 44 verbunden als auch stellt ein Steuersignal für einen ersten Schalter 52 dar. Ein zweiter Schalter 54 ist ferner vorgesehen, um

mit dem Schreiben-Steuersignal 48 gesteuert zu werden, wie es aus Fig. 4 ersichtlich ist.

Die in Fig. 4 gezeigte Umsetzungseinrichtung umfaßt ferner eine Prechargeeinrichtung 56 mit zwei Schaltern 56a, 56b sowie einem Precharge-Takt-Eingang PCH 56c. Beide Schalter werden mit dem Precharge-Steuersignal 56c angesteuert und sind wirksam, um das Potential V_{DD} 58, das bei einem bevorzugten Ausführungsbeispiel der vorliegenden Erfindung einem logisch hohen Zustand, also einem Zustand einer logischen „1" entspricht, sowohl auf die erste Dual-Rail-Leitung 14a als auch auf die zweite Dual-Rail-Leitung 14b zu legen.

Ein zweites niedriges Potential V_{SS} 60 wird auf die zweite Dual-Rail-Leitung 14b gelegt, wenn sowohl der erste Schalter 52 als auch der zweite Schalter 54 durchgeschaltet sind. Ist jedoch einer der Schalter 52, 54 nicht durchgeschaltet, so existiert keine leitfähige Verbindung zwischen dem Potential V_{SS} 60 und der zweiten Dual-Rail-Leitung 14b. Das zweite niedrige Potential V_{SS} kann das Massepotential sein und entspricht bei dem beschriebenen Ausführungsbeispiel dem logisch niedrigen Zustand bzw. dem logischen „0"-Zustand.

In Fig. 5 tragen dieselben Elemente wie in Fig. 4 dieselben Bezugszeichen. Fig. 5 umfaßt keine Precharge-Einrichtung 56, da Fig. 5 für eine Dual-Rail-Technik ohne Precharge vorgesehen ist. Als zusätzliches Element umfaßt Fig. 5 einen dritten Schalter 64, der, wie es aus dem Symbol in Fig. 5 zu erkennen ist, im Gegensatz zu den anderen auftretenden Schaltern als PMOS-Transistor ausgeführt ist, während die Schalter 52, 54 als NMOS-Transistoren ausgeführt sind. NMOS-Transistoren sind durchgeschaltet, wenn das Steuersignal einen hohen Spannungszustand hat, und sperren, wenn das Steuersignal einen niedrigen Zustand hat. Dagegen sind PMOS-Transistoren durchgeschaltet, wenn das Steuersignal einen niedrigen Zustand hat. Die PMOS-Transistoren sperren dagegen, wenn das Steuersignal einen hohen Spannungszustand aufweist.

Im nachfolgenden wird Bezug nehmend auf Fig. 4 die Funktion der erfindungsgemäßen Umsetzungseinrichtung dargestellt. Im Falle des Lesens von der Bit-Slice auf den Rechenwerks-Bus ist das Lesen-Steuersignal 46 aktiv, so daß das Signal auf der ersten Dual-Rail-Leitung 14a - unabhängig davon, ob es eine „1" oder eine „0" ist - auf die Single-Rail-Leitung 12 durchgeschaltet wird. Es sei darauf hingewiesen, daß die Lesen-Treiberschaltung 42 genauso wie die Schreiben-Treiberschaltung 44 z. B. als UND-Gatter ausgeführt sein können, das nur dann ein Ausgangssignal erzeugt, wenn beide Eingangssignale einen „1"-Zustand haben. Die in Fig. 4 gezeigte Schaltung bewirkt, daß das Signal auf der zweiten Dual-Rail-Leitung 14b im Falle des Lesens von der Bit-Slice auf den Rechenwerksbus, also im Falle einer Datenübertragung von rechts nach links in Fig. 4 ignoriert wird.

Das Schreiben-Steuersignal ist im Falle des Lesens gleich 0, was bedeutet, daß der zweite Schalter 54 von Fig. 4 offen ist, d. h. sperrt, so daß die zweite Dual-Rail-Leitung 14b nicht mit dem Massepotential 60 verbunden ist. Dies stellt sicher, daß in einem darauffolgenden Precharge-Takt, in dem beide Schalter 56a, 56b geschlossen werden, um beide Dual-Rail-Leitungen in einen logisch hohen Zustand zu bringen, eine Spannung angelegt werden kann, ohne daß ein Kurzschluß mit dem Massepotential 60 erzeugt wird.

Im Falle des Precharge-Taktes ist das Lesen-Steuersignal 46 gleich 0, so daß verhindert wird, daß der Precharge-Zustand auf der zweiten Dual-Rail-Leitung 14a auf die Single-Rail-Leitung 12 übertragen wird.

Die in Fig. 4 gezeigte Schaltung stellt somit sicher, daß im Falle des Lesens, also im Falle einer Umsetzung von Dual-Rail mit Precharge auf Single-Rail - lediglich im Datentakt und nicht im Precharge-Takt - der Zustand auf der ersten Dual-Rail-Leitung 14a auf die Single-Rail-Leitung 12 durchgeschal-

tet wird, daß im Precharge-Takt keine Datenübertragung von der ersten Dual-Rail-Leitung auf die Single-Rail-Leitung auftritt, und daß ferner die zweite Dual-Rail-Leitung 14b von dem Massepotential 60 (V_{SS}) abgetrennt ist, damit die zweite Dual-Rail-Leitung ebenso wie die erste Dual-Rail-Leitung im Precharge-Takt auf einen hohen Zustand geladen werden können.

Im nachfolgenden wird die Umsetzung eines Single-Rail-Signals in ein Dual-Rail-Signal, also die Datenübertragung von links nach rechts in Fig. 4, die auch mit „Schreiben" bezeichnet ist, beschrieben.

Im Falle des Schreibens ist, wie es aus der in Fig. 4 gezeigten Tabelle ersichtlich ist, der Lesen-Treiber 42 durch eine „0" am Steuersignaleingang deaktiviert. Dagegen ist der Schreiben-Treiber 44 durch eine „1" an seinem Steuereingang aktiviert. Dies führt dazu, daß das auf der Bit-Leitung anliegende Signal in einem Datentakt unmittelbar auf die erste Dual-Rail-Leitung 14a durchgeschaltet wird. Liegt am Ausgang des Schreiben-Treibers 44 ein logisch hoher Zustand, also eine „1" an, so ist der Schalter 52 geschlossen. Aufgrund des Schreiben-Steuersignals gleich „1" ist auch der Schalter 54 geschlossen, so daß das Massepotential V_{SS} 60 mit der zweiten Dual-Rail-Leitung 14b verbunden wird, so daß der invertierte Zustand, also eine „0" auf der zweiten Dual-Rail-Leitung erzeugt wird.

Liegt dagegen eine 0 am Ausgang des Schreiben-Treibers 44 an, so liegt diese 0 auch auf der ersten Dual-Rail-Leitung 14a an. Aufgrund der 0 ist jedoch der erste Schalter 52 offen, so daß das Massepotential 60 nicht mit der zweiten Dual-Rail-Leitung 14b verbunden ist, sondern von derselben abgetrennt ist. Der aus dem vorhergehenden Precharge-Takt bestehende „1"-Zustand auf der zweiten Dual-Rail-Leitung 14b bleibt somit erhalten, was dazu führt, daß auf der zweiten Dual-Rail-Leitung 14b nunmehr wieder der komplementäre Wert zur ersten Dual-Rail-Leitung anliegt.

Die erfindungsgemäße Umsetzungseinrichtung von Fig. 4 stellt somit sicher, daß im Falle einer Umwandlung von Single-Rail in Dual-Rail zum einen der Single-Rail-Zustand auf die erste Dual-Rail-Leitung 14a gelegt wird, daß im Falle eines Precharge-Taktes nichts vom Eingang zum Ausgang übertragen wird, und daß im Falle eines Single-Rail-„1"-Zustands die zweite Dual-Rail-Leitung mit dem Massepotential kurzgeschlossen wird oder im Falle eines Single-Rail-„0"-Zustands der hohe Zustand der zweiten Dual-Rail-Leitung aufgrund des vorhergehenden Precharge-Taktes beibehalten wird.

Im nachfolgenden wird auf die Funktion der Umsetzungseinrichtung von Fig. 5 eingegangen, die eine Umsetzungseinrichtung für Single-Rail auf Dual-Rail ohne Precharge darstellt. Aus diesem Grund ist in Fig. 5 keine Precharge-Einrichtung 56 vorgesehen. Statt dessen wird der dritte Schalter 64 eingesetzt, durch den das hohe Potential V_{DD} 58 auf die zweite Dual-Rail-Leitung gelegt werden kann, und zwar dann, wenn das Schreiben-Steuersignal 48 hoch ist, also der zweite Schalter 54 geschlossen ist und der erste Schalter 52 offen ist (eine „0" am Ausgang des Schreiben-Treibers 44). Dies wird dadurch erreicht, daß der dritte Schalter 64 als PMOS-Transistor ausgeführt ist, so daß das Potential V_{DD} dann mit der zweiten Dual-Rail-Leitung 14b verbunden wird, wenn am Ausgang des Schreiben-Treibers 44 eine „0" anliegt.

Wird bei dem in Fig. 5 gezeigten Ausführungsbeispiel im nächsten Arbeitszyklus am Single-Rail-Bus eine „1" eingespeist, so wird diese wiederum ohne weiteres auf die erste Dual-Rail-Leitung 14a durchgeschaltet. Nunmehr ist der dritte Schalter 64 jedoch offen, und sind der erste und der zweite Schalter 52, 54 geschlossen, so daß der hohe Zustand aus dem vorherigen Zyklus auf der zweiten Dual-Rail-Leitung über das Massepotential 60 (V_{SS}) entladen wird, um die zweite Dual-Rail-Leitung 14b auf den niedrigen Potentialzustand zu ziehen.

Obgleich das in Fig. 4 gezeigte Ausführungsbeispiel für Dual-Rail mit Precharge beschrieben worden ist, sind die Modifikationen für Dual-Rail mit Pre-Discharge für Fachleute ohne weiteres ersichtlich. Anstatt des Potentials V_{DD} 58 von Fig. 4 könnte das Potential V_{SS} eingesetzt werden. Anstatt des Potentials V_{SS} 60 könnte dann das Potential V_{DD} genommen werden, wobei die Schalter 52 und 54 derart zu modifizieren sind, daß der logisch niedrige Zustand aus dem vorherigen Precharge-Zyklus im Falle einer „1" auf der Single-Rail-Leitung 12 beibehalten wird.

Alternative Ausgestaltungen für den Lesen-Treiber 42 und den Schreiben-Treiber 44 sind für Fachleute ebenfalls ersichtlich, so lange die Funktionen des Lesens und Schreibens sichergestellt werden und während des Precharge-Taktes beide Treiber gesperrt werden, so daß keine Datenübertragung vom einen Ende zum anderen Ende der Schaltung stattfindet.

Bei dem in Fig. 4 gezeigten Ausführungsbeispiel, bei dem eine Dual-Rail-Technik mit Precharge eingesetzt wird, ist die Datenrate am Dual-Rail-Ausgang aufgrund des Precharge-Taktes bei gleichem Arbeitszyklus auf beiden Seiten halb so hoch wie am Single-Rail-Eingang. Dieser Datenratenunterschied kann ausgenutzt werden, um die Datenrate auch auf dem Single-Rail-Bus zu halbieren, um Sicherheitsverbesserungen zu erreichen. Dies kann dadurch geschehen, daß eine Verschlüsselung bzw. Codierung der Daten auf dem Single-Rail-Bus vorgenommen wird. In diesem Fall würde die Umsetzungseinrichtung eingangsseitig einen Speicher zum Speichern von zwei aufeinanderfolgenden Bits haben sowie eine Entschlüsselungseinrichtung bzw. Decodiereinrichtung, um das unverschlüsselte bzw. decodierte Single-Rail-Bus-Bit zu erhalten, das dann in ein unverschlüsseltes Dual-Rail-Bit umgesetzt wird. Zur Erhöhung des Sicherheitsstandards auch auf dem Single-Rail-Bus kann somit eine Datencodierung bzw. Datenverschlüsselung eingesetzt werden, die zu einer Halbierung der Nutzdatenrate führt. In diesem

Fall laufen der Single-Rail-Bus und der Dual-Rail-Bus wieder synchron, jedoch mit unterschiedlichen Maßnahmen zur Sicherheitserhöhung.

Bezugszeichenliste

10 Single-Rail-Bus
12 Single-Rail-Leitung
14 Dual-Rail-Bus
14a erste Dual-Rail-Leitung
14b zweite Dual-Rail-Leitung
16 Umsetzungseinrichtung
18 Multiplexer
20 Langzahlrechenwerk
22 arithmetische Einheit einer Bit-Slice
24a erstes Register einer Bit-Slice
24b zweites Register einer Bit-Slice
24c drittes Register einer Bit-Slice
40 Eingangsknoten
42 Lesen-Treiber
44 Schreiben-Treiber
46 Lesen-Steuersignal
48 Schreiben-Steuersignal
50 Ausgangsknoten
52 erster Schalter
54 zweiter Schalter
56 Initialisierungseinrichtung
56a Initialisierungs-Schalter
56b Initialisierungs-Schalter
56c Precharge-Takt
58 Einrichtung zum Anlegen eines hohen Potentials V_{DD}
60 Einrichtung zum Anlegen eines niedrigen Potentials V_{SS}
64 dritter Schalter

Patentansprüche

1. Datenverarbeitungsschaltung mit folgenden Merkmalen:

einem Single-Rail-Bus (10) mit einer Single-Rail-Leitung (12) für eine Folge von Datenbits;

einem Dual-Rail-Bus (14) mit zwei Dual-Rail-Leitungen für die Folge von Datenbits, wobei eine erste Dual-Rail-Leitung (14a) für die Datenbits vorgesehen ist, und wobei eine zweite Dual-Rail-Leitung (14b) für invertierte Datenbits vorgesehen ist; und

einer Umsetzungseinrichtung (16) zum Überführen von Signalen auf dem Single-Rail-Bus (10) in Signale auf dem Dual-Rail-Bus (14) und umgekehrt.

2. Datenverarbeitungsschaltung nach Patentanspruch 1, bei der die Umsetzungseinrichtung (16) folgende Merkmale aufweist:

einen Lesen-Treiber (42) zum Überführen von Signalen auf der ersten Dual-Rail-Leitung (14a) auf den Single-Rail-Bus (10);

einem Schreiben-Treiber (44) zum Überführen der Signale auf dem Single-Rail-Bus auf die erste Dual-Rail-Leitung (14a);

einer Erzeugungseinrichtung (52, 54, 60) zum Erzeugen der Signale auf der zweiten Dual-Rail-Leitung (14b) aus den Signalen auf der ersten Dual-Rail-Leitung; und

einer Steuereinrichtung (46, 48) zum Steuern des Lesen-Treibers (42) und des Schreiben-Treibers (44) über ein Lesen-Steuersignal (46) und ein Schreiben-Steuersignal (48), so daß höchstens entweder der Lesen-Treiber (42) oder der Schreiben-Treiber (44) aktiv ist.

3. Datenverarbeitungsschaltung nach Patentanspruch 2,

bei der der Schreiben-Treiber (44) eine UND-Funktion aufweist, wobei ein erster Eingang des Schreiben-Treibers (44) mit der Single-Rail-Leitung (12) verbunden ist, ein zweiter Eingang des Schreiben-Treibers (44) mit dem Schreiben-Steuersignal (48) verbunden ist, und ein Ausgang des Schreiben-Treibers (44) mit der ersten Dual-Rail-Leitung (14a) verbunden ist.

4. Datenverarbeitungsschaltung nach Patentanspruch 2 oder 3,

bei der der Lesen-Treiber (42) eine UND-Funktion aufweist, wobei ein erster Eingang des Lesen-Treibers (42) mit der ersten Dual-Rail-Leitung (14a) verbunden ist, wobei ein zweiter Eingang des Lesen-Treibers (42) mit dem Lesen-Steuersignal (46) verbunden ist, und wobei ein Ausgang des Lesen-Treibers (42) mit der Single-Rail-Leitung (12) verbunden ist.

5. Datenverarbeitungsschaltung nach Patentanspruch 3 oder 4, bei der die Umsetzungseinrichtung (16) ferner folgende Merkmale aufweist:

eine Einrichtung (60) zum Anlegen eines ersten Potentials (V_{SS}), das einem niedrigen Spannungszustand zugeordnet ist; und

einen ersten Schalter (54), der zwischen die zweite Dual-Rail-Leitung (14b) und die Einrichtung (60) zum Anlegen des ersten Potentials geschaltet ist, wobei der erste Schalter (54) durch das Schreiben-Steuersignal (48) steuerbar ist.

6. Datenverarbeitungsschaltung nach Anspruch 5, bei der die Umsetzungseinrichtung (16) ferner folgendes Merkmal aufweist:

einen zweiten Schalter (52), der zwischen die zweite Dual-Rail-Leitung (14) und die Einrichtung (60) zum Anlegen des ersten Potentials (V_{SS}) geschaltet ist, wobei der zweite

Schalter (54) durch ein Ausgangssignal des Schreiben-Treibers (44) steuerbar ist.

7. Datenverarbeitungsschaltung nach einem der vorhergehenden Ansprüche,

bei der der Dual-Rail-Bus (14) ein Dual-Rail-Bus mit Precharge oder Pre-Discharge ist, so daß zwischen jedem Datentakt auf der ersten und zweiten Dual-Rail-Leitung (14a, 14b) ein Initialisierungstakt eingefügt ist, in dem die erste Dual-Rail-Leitung (14a) und die zweite Dual-Rail-Leitung (14b) auf denselben Spannungszustand bringbar sind.

8. Datenverarbeitungsschaltung nach Anspruch 7,

bei der die zwei Dual-Rail-Leitungen (14a, 14b) mit einer Initialisierungseinrichtung (56) verbunden sind, wobei die Initialisierungseinrichtung (56) wirksam ist, um in dem Initialisierungstakt die beiden Dual-Rail-Leitungen auf denselben Spannungszustand zu bringen.

9. Datenverarbeitungsschaltung nach Anspruch 8, bei der der Spannungszustand ein hoher Spannungszustand ist, wobei die Initialisierungseinrichtung (56) eine Einrichtung (58) zum Anlegen eines zweiten Potentials (V_{DD}), das höher als das erste Potential (V_{SS}) ist, aufweist, um in dem Initialisierungstakt die beiden Dual-Rail-Leitungen (14a, 14b) auf das zweite Potential zu bringen.

10. Datenverarbeitungsschaltung nach einem der Ansprüche 3 bis 6, bei der die Umsetzungseinrichtung (16) folgende Merkmale aufweist:

eine Einrichtung (58) zum Anlegen eines zweiten Potentials (V_{DD}), das größer als das erste Potential (V_{SS}) ist; und

einen dritten Schalter (64), der zwischen die Einrichtung (58) zum Anlegen des zweiten Potentials und den zweiten Dual-Rail-Bus (14b) geschaltet ist, und der von einem Ausgangssignal des Schreiben-Treibers (44) steuerbar ist.

11. Datenverarbeitungsschaltung nach einem der Ansprüche 6 bis 9,

bei der die Umsetzungseinrichtung (16) ausgebildet ist, um den Lesen-Treiber (42) und den Schreiben-Treiber (44) in einem Initialisierungstakt zu deaktivieren.

12. Datenverarbeitungsschaltung nach einem der vorhergehenden Ansprüche, die auf einem Halbleitersubstrat integriert ausgeführt ist.

13. Datenverarbeitungsschaltung nach einem der vorhergehenden Ansprüche,

bei der der Single-Rail-Bus ein Teil eines Mehrfach-Single-Rail-Busses ist, dessen Anzahl von Single-Rail-Bussen kleiner ist als eine Anzahl von Dual-Rail-Bussen in einem Mehrfach-Dual-Rail-Bus.

14. Datenverarbeitungsschaltung nach einem der vorhergehenden Ansprüche,

bei dem der Dual-Rail-Bus ausgebildet ist, um Komponenten innerhalb einer Bit-Slice eines Rechenwerks miteinander zu verbinden, und wobei der Single-Rail-Bus ausgebildet ist, um die Bit-Slices des Rechenwerks untereinander oder mit externen Komponenten zu verbinden.

15. Datenverarbeitungsschaltung nach Anspruch 14,

bei der der Single-Rail-Bus ausgebildet ist, um Daten für eine Initialisierung von Bit-Slices oder Endergebnisdaten von den Bit-Slices zu übertragen.

16. Datenverarbeitungseinrichtung nach einem der Ansprüche 14 oder 15,

bei der die Anzahl von Bit-Slices in dem Rechenwerk größer als 1000 ist, und

bei der die Anzahl von Single-Rail-Bussen in einem Mehrfach-Single-Rail-Bus kleiner oder gleich 64 ist.

17. Datenverarbeitungsschaltung nach einem der vorhergehenden Ansprüche,

bei der eine physikalische Länge des Single-Rail-Busses größer als eine physikalische Länge des Dual-Rail-Busses ist.

18. Datenverarbeitungsschaltung nach einem der vorhergehenden Ansprüche,

bei der ferner eine Einrichtung zum Verschlüsseln oder Codieren von Daten auf dem Single-Rail-Bus oder zum Ausführen eines Precharge- oder Pre-Discharge-Betriebs auf dem Single-Rail-Bus vorgesehen ist.

19. Datenverarbeitungsschaltung nach einem der vorhergehenden Ansprüche,

die in einer Chipkarte oder einem Sicherheits-IC ausgebildet ist.

20. Verfahren zum Übertragen von Daten von einem Single-Rail-Bus mit einer Single-Rail-Leitung zu einem Dual-Rail-Bus mit zwei Dual-Rail-Leitungen, wobei eine erste Dual-Rail-Leitung für eine Folge von Datenbits vorgesehen ist, und eine zweite

Dual-Rail-Leitung für eine Folge von invertierten Datenbits vorgesehen ist, mit einem Schritt des Überführens von Signalen auf dem Single-Rail-Bus in Signale auf dem Dual-Rail-Bus und umgekehrt.

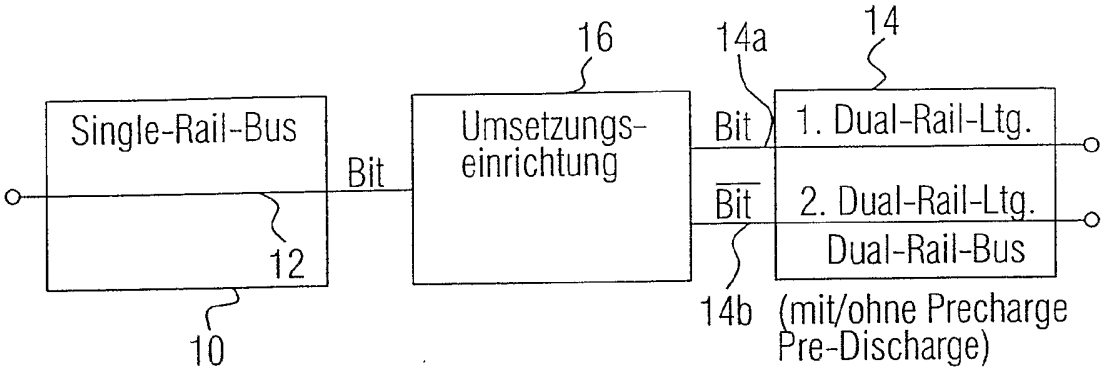

16
14a
14
Single-Rail-Bus
Bit
Umsetzungs-
einrichtung
Bit
1. Dual-Rail-Ltg.
Bit
2. Dual-Rail-Ltg.
Dual-Rail-Bus
12
10
14b
(mit/ohne Precharge
Pre-Discharge)

FIG 1

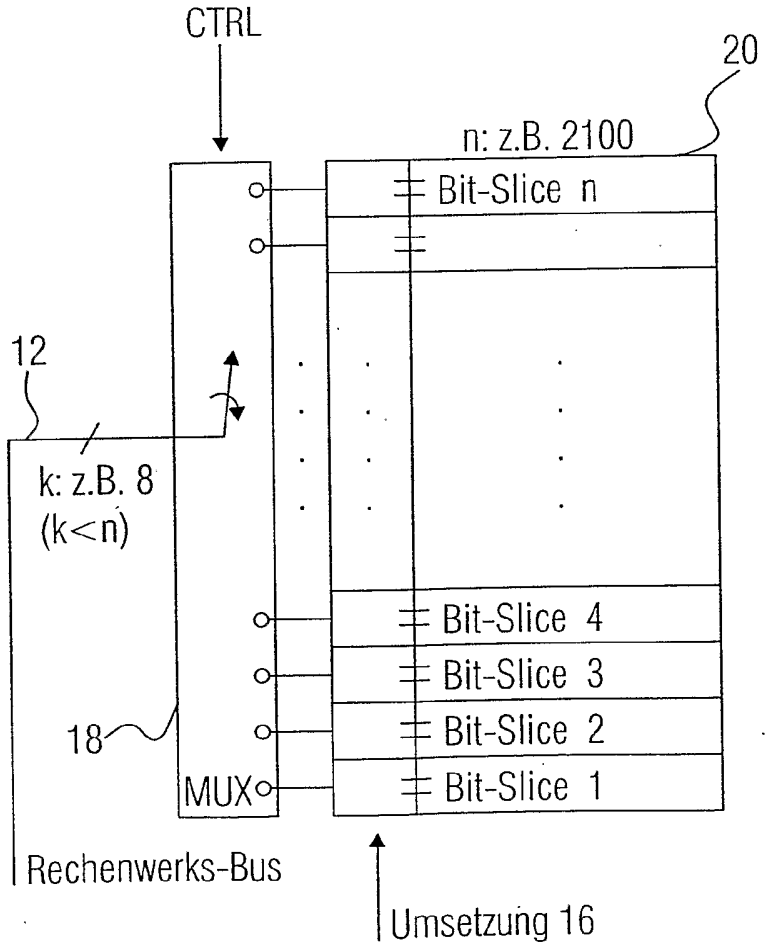

CTRL
20
n: z.B. 2100
Bit-Slice n
12
k: z.B. 8
(k<n)
Bit-Slice 4
Bit-Slice 3
Bit-Slice 2
Bit-Slice 1
18
MUX
Rechenwerks-Bus
Umsetzung 16

FIG 2

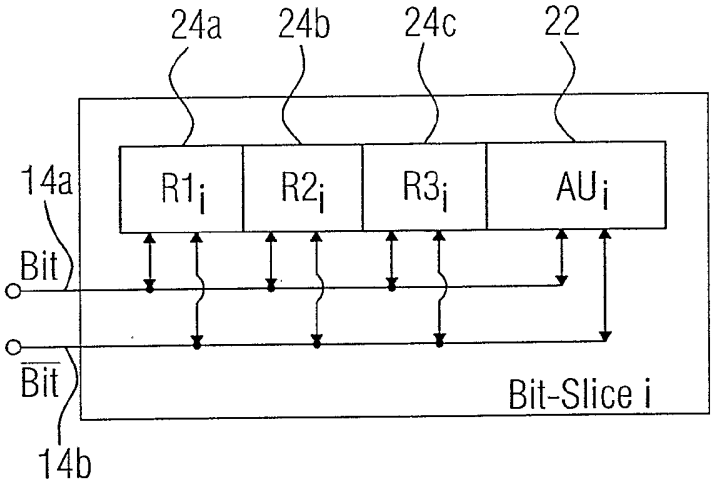
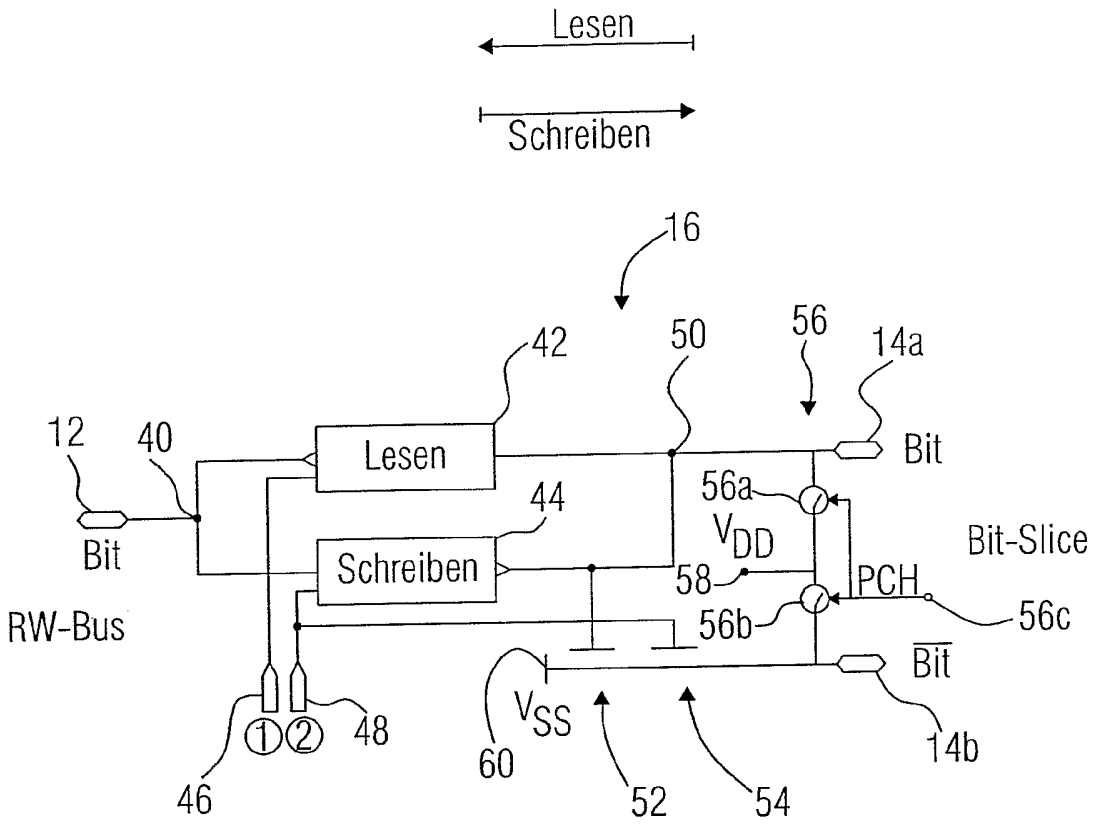


FIG 3



	①	②
Schreiben	0	1
Lesen	1	0
Prech.	0	0

FIG 4 (mit Precharge)

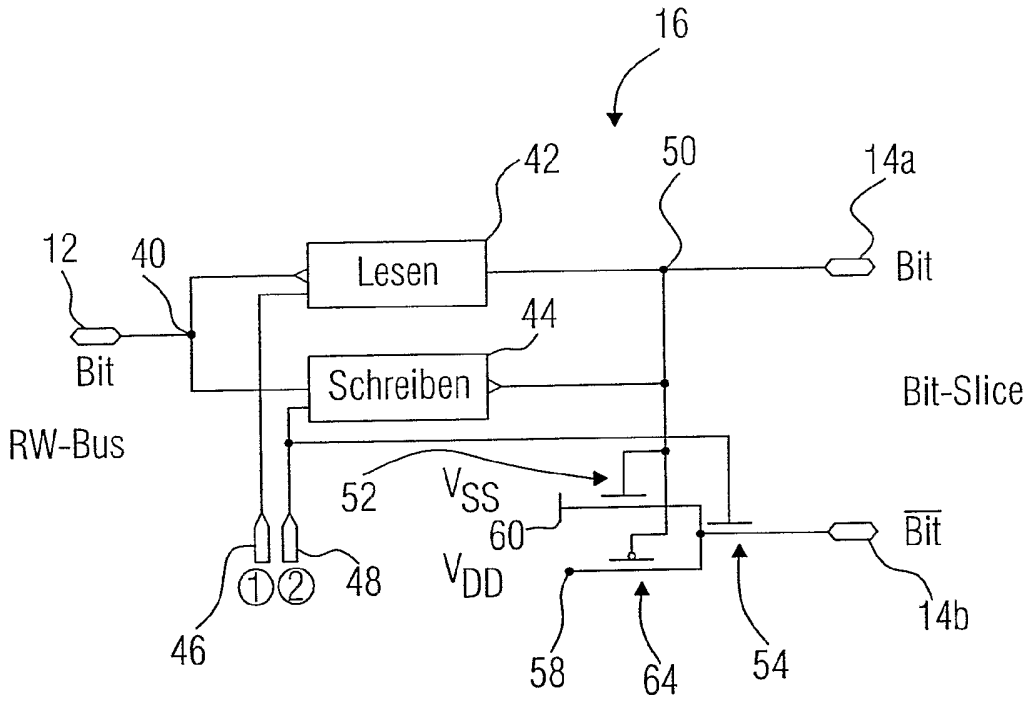


FIG 5 (ohne Precharge)