

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(21)(22) Заявка: 2011104883/28, 09.02.2011

(24) Дата начала отсчета срока действия патента:
09.02.2011

Приоритет(ы):

(22) Дата подачи заявки: 09.02.2011

(45) Опубликовано: 10.07.2012 Бюл. № 19

(56) Список документов, цитированных в отчете о
поиске: US 7880248 B1, 01.02.2011. US 7489013 B1,
10.02.2009. US 7705439 B2, 27.04.2010. US
2007/0189055 A1, 16.08.2007. US 5233505 A,
03.08.1993. DE 10252329 A1, 27.05.2004. RU
2251153 C2, 27.04.2005.

Адрес для переписки:

111123, Москва, Е-123, ФГУП "18 ЦНИИ"
МО РФ, руководителю

(72) Автор(ы):

Боярков Вадим Сергеевич (RU),
Горбась Андрей Витальевич (RU),
Семенов Антон Валерьевич (RU),
Федорец Владимир Николаевич (RU)

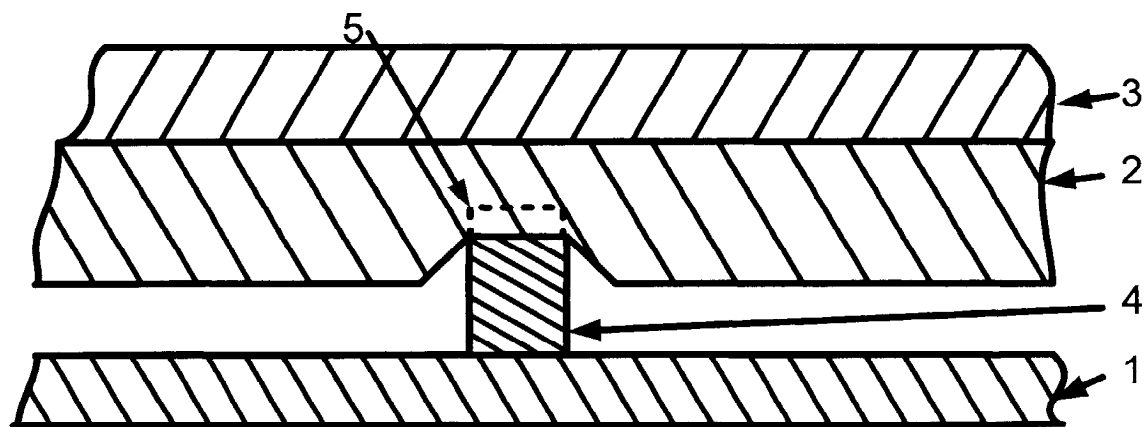
(73) Патентообладатель(и):

Федеральное государственное унитарное
предприятие "18 Центральный научно-
исследовательский институт" Министерства
обороны Российской Федерации (RU)(54) ПОЛУПРОВОДНИКОВЫЙ ПРИБОР С ЗАЩИТОЙ ОБЛАСТЕЙ ТОПОЛОГИИ
КРИСТАЛЛА, СОДЕРЖАЩИХ КОНФИДЕНЦИАЛЬНЫЕ ДАННЫЕ, ОТ ОБРАТНОГО
ПРОЕКТИРОВАНИЯ

(57) Реферат:

Изобретение относится к области микроэлектроники, а именно к изделиям электронной техники, например микросхемам, содержащим конфиденциальные сведения, записанные в области памяти, которые необходимо защитить от незаконного считывания. Сущность изобретения: полупроводниковый прибор конструктивно состоит из кристалла, содержащего область топологии с конфиденциальными данными, корпуса, вставки из материала с эффектом памяти формы, размещенной под областью топологии в месте механического ослабления,

и полимеризованного наполнителя. При воздействии на него специальными методами обратного проектирования будет разрушена именно та область, которая содержит конфиденциальные данные. Техническим результатом изобретения является обеспечение возможности защиты областей топологии кристалла, содержащих конфиденциальные данные от обратного проектирования, путем механического разрушения именно того участка топологии, который содержит конфиденциальную информацию. 2 з.п. ф-лы, 2 ил.



Фиг. 1

RU 2 4 5 5 7 2 9 C 1

RU 2 4 5 5 7 2 9 C 1



FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY

(12) ABSTRACT OF INVENTION(21)(22) Application: **2011104883/28, 09.02.2011**(24) Effective date for property rights:
09.02.2011

Priority:

(22) Date of filing: **09.02.2011**(45) Date of publication: **10.07.2012 Bull. 19**

Mail address:

**111123, Moskva, E-123, FGUP "18 TsNII" MO
RF, rukovoditelju**

(72) Inventor(s):

**Bojarkov Vadim Sergeevich (RU),
Gorbas' Andrej Vital'evich (RU),
Semenov Anton Valer'evich (RU),
Fedorets Vladimir Nikolaevich (RU)**

(73) Proprietor(s):

**Federal'noe gosudarstvennoe unitarnoe
predpriyatie "18 Tsentral'nyj nauchno-
issledovatel'skij institut" Ministerstva oborony
Rossijskoj Federatsii (RU)****(54) SEMICONDUCTOR DEVICE HAVING REVERSE ENGINEERING PROTECTION OF CHIP PATTERN REGIONS CONTAINING CONFIDENTIAL DATA**

(57) Abstract:

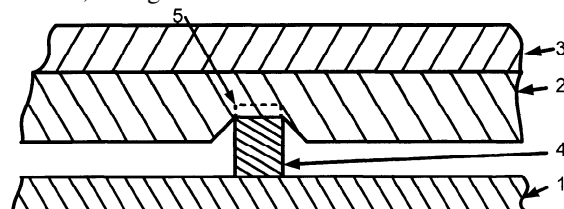
FIELD: physics.

SUBSTANCE: semiconductor device consists of a chip having a chip pattern with confidential data, a housing, inserts made from material with shape memory effect placed under the chip pattern at the mechanically weak point, and a polymerised filler. When subjected to special reverse engineering techniques, that region containing confidential data will be destroyed.

EFFECT: protection of chip pattern regions

containing confidential data from reverse engineering through mechanical destruction of that area of the pattern containing confidential information.

3 cl, 2 dwg



Фиг. 1

Настоящее изобретение относится к области микроэлектроники, а именно к изделиям электронной техники, например микросхемам, содержащим конфиденциальные сведения, записанные в области памяти, которые необходимо защитить от незаконного считывания (например, коды кредитных карт, ключи шифрования).

В патенте US №7005733 [1] рассматривается микросхема шифрования, в которой в пассивирующий (защитный) слой вводится цепь, ответственная за считывание ключей шифрования или дешифрования, чувствительная по крайней мере к свойствам одного из параметров упомянутого слоя, так что его нарушение, при попытке вскрытия микросхемы, приводит к ошибкам процесса шифрования. Недостатком данного способа защиты является введение лишнего слоя (или слоев), что усложняет конструкцию и топологию кристалла микросхемы.

В патентах US №7008873 [2], US №7294935 [3] рассматриваются метод и структура камуфлирования структуры интегральной микросхемы, по принципу создания «ложных» межсоединений и специфического расположения окисла. Предлагаемые способы не защищают микросхему от полунинвазивных методов (частичное вскрытие корпуса) считывания и применимы только для специфической топологии интегральных микросхем, не могут распространяться, например, на такой класс интегральных схем, как программируемые логические интегральные схемы. Кроме того, такой способ защиты не применим при изготовлении по так называемой fabless-технологии, когда на фабрику производителя передается полное описание топологии прибора.

В патентах US №5783846 [4], US №5930663 [5] предлагаются варианты топологии, в которых все логические элементы практически одинаковы и визуально неразличимы, что затрудняет интерпретацию реальной блок-схемы прибора. Данный способ защиты подразумевает использование только на ограниченном множестве микросхем (простые логические схемы), поэтому не обладает универсальностью.

В патенте US №7295455 [6] рассмотрена защита структуры и памяти микросхемы от считывания конфиденциальных данных, записанных в ее память, путем введения многочисленных фоточувствительных элементов, что приводит к изменению ее внутренней структуры при вскрытии ее непрозрачного корпуса. Недостатком данного решения является введение лишних фоточувствительных элементов в топологию микросхемы, значительно усложняющих конструкцию и технологию ее изготовления из-за введения дополнительного слоя топологии.

Наиболее близким к заявленному техническому решению является патент US №7489013 [7], который описывает полупроводниковый прибор, включающий основание корпуса и кристалл интегральной схемы, содержащий электрический или термический реактивный слой, расположенный между верхней поверхностью основания корпуса и нижней поверхностью кристалла интегральной схемы, в которой упомянутый реактивный слой организован таким образом, что обнаружение вмешательства в полупроводниковый прибор задействует этот реактивный слой электрически или термически и по крайней мере частично разрушает полупроводниковый прибор. Такой реактивный слой может быть выполнен, в частности, из материала с эффектом памяти формы (shape memory alloy), п.п.20, 21, 31, 37 патентной формулы этого патента. Недостатком данного технического решения является отсутствие гарантий разрушения/повреждения областей кристалла, содержащих конфиденциальную информацию, что в значительном количестве случаев может сделать возможным использование, по крайней мере, одного из современных

методов считывания конфиденциальной информации с неокончательно разрушенной области памяти. Проведенные предварительные опыты показали, что прямое применение данного изобретения затруднено по двум выявленным причинам: первое - отслаивание кристалла микросхемы без разрушения при деформации корпуса, второе - малое число обломков при деформации кристалла по оси, перпендикулярной плоскости скола, - плоскости 110 кремния при базовой ориентации пластины 011, что приводит к тому, что защищаемое место кристалла остается неповрежденным.

Из существующего уровня техники известны материалы, обладающие эффектом памяти формы, в частности сплавы на основе титана и никеля, содержащие в качестве добавки гафний, которые имеют температуру трансформации в диапазоне температур от 100 до 300°C в зависимости от процентного содержания гафния в сплаве [8], что выше типичных рабочих температур полупроводниковых приборов -60 ÷ +125°C.

Задачей, на решение которой направлено заявляемое изобретение, является устранение недостатков прототипа, а именно целенаправленной защиты областей топологии кристалла, содержащих конфиденциальные данные от обратного проектирования путем механического разрушения именно того участка топологии, который содержит конфиденциальную информацию.

Данная задача решается за счет того, что заявленный полупроводниковый прибор, содержащий конфиденциальные данные, включающий корпус с кристаллом интегральной схемы и вставку из материала с эффектом памяти формы, размещенную внутри, которая при детектировании нарушения целостности корпуса целенаправленно разрушает область кристалла, содержащую конфиденциальную информацию. Вставка из материала с эффектом памяти формы имеет температуру трансформации выше максимальной рабочей температуры прибора; внутренний объем прибора заполняется полимеризованным наполнителем с температурой размягчения выше температуры трансформации упомянутой вставки с эффектом памяти формы, что и обеспечивает деформацию упомянутой вставки и соответственно разрушение кристалла прибора. При этом защищаемая область кристалла прибора выполняется механически ослабленной, а форма вставки из материала с эффектом памяти формы и способ ее крепления выбираются таким образом, чтобы обеспечить разрушение упомянутого защищаемого участка кристалла полупроводникового прибора.

Целесообразно выполнить механическое ослабление защищаемой области, осуществлять структуру мембраны, изготовленной на обратной стороне кристалла прибора точно под областью топологии, которую мы защищаем, а вставка из материала с эффектом памяти формы представляет собой цилиндр, расположенный внутри мембраны между кристаллом прибора и корпусом, в частности в виде сплошной пластины по размеру кристалла прибора, в которой имеется цилиндрическая выпуклость в области входящей мембранной уплотняющей структуры. Применение такой вставки из материала с эффектом памяти формы значительно затрудняет рентгеноструктурные исследования прибора и обнаружение вставки из материала с эффектом памяти формы (как правило, сплава на основе никеля, титана, меди) до момента вскрытия корпуса полупроводникового прибора.

Техническим результатом, обеспечиваемым приведенной совокупностью признаков, является целенаправленное разрушение участка кристалла интегральной схемы полупроводникового прибора, компактно содержащего конфиденциальную информацию, при обнаружении нарушения целостности корпуса полупроводникового прибора.

Сущность изобретения поясняется чертежами, на которых изображено:

На фиг.1 схематично изображено поперечное сечение полупроводникового прибора с вставкой из материала с эффектом памяти формы;

На фиг.2 - поперечное сечение прибора с вариантом крепления в корпус.

5 Полупроводниковый прибор состоит из корпуса (металлокерамический, пластмассовый) (1 на фиг.1, 2), внутри которого располагается кристалл (2 на фиг.1, 2), содержащий участок топологии (область памяти и т.п.), в котором содержится конфиденциальная информация (в том или ином виде), подлежащая защите от считывания. Кристалл закрыт специализированным рабочим слоем из полимеризованного материала с температурой размягчения выше, чем температура трансформации вставки из материала с эффектом памяти формы рабочего слоя (3 на фиг.1, 2). Вставка из материала с эффектом памяти формы (4 на фиг.1, 2) и с температурой трансформации ниже, чем у рабочего слоя, расположена вплотную к кристаллу таким образом, чтобы при трансформации происходило механическое разрушение кристалла, по крайней мере, по двум непараллельным осям. Возможны различные варианты размещения такой вставки с различной геометрией трансформации (5 фиг.1, 2). Удлинение цилиндра из материала с эффектом памяти формы может достигать 7%, что при длине цилиндра составляет величину в 70 мкм, и что обеспечивает разрушение мембранной структуры толщиной порядка 10÷15 мкм при толщине кристалла микросхемы до 300÷400 мкм. Диаметр такой мембранной структуры может быть порядка 1 мкм или меньше. Для преодоления эффекта адгезии при срабатывании вставки из материала с памятью формы возможно введение дополнительных вставок, в частности, и из материала с эффектом памяти формы в конструкцию полупроводникового прибора (6 фиг.2), которая может образовывать полость, внутри которой размещен кристалл полупроводникового прибора.

Важной особенностью применения способа целенаправленной защиты областей топологии кристалла, содержащих конфиденциальные данные от обратного проектирования, является возможность внедрения вставок из материала с эффектом памяти формы или нанесения мембран на кристаллы на этапе, когда кристалл полупроводникового прибора уже изготовлен и остается только этап сборки прибора, что отвечает всем требованиям на выполнение технологических процедур наиболее широко применяющейся в настоящее время fabless-технологии производства полупроводниковых приборов. Мембранная структура может быть выполнена путем травления обратной стороны кристалла при совмещении места расположения мембраны и защищаемой области кристалла. Также могут быть выполнены ложные мембраны, затрудняющие определение реально защищаемой области топологии кристалла.

Работает система целенаправленной защиты от обратного проектирования следующим образом: при детектировании нарушения целостности корпуса полупроводникового прибора и вмешательства в рабочий слой из полимеризованного наполнителя (1 на фиг.1, 2) происходит изменение температуры внутри полупроводникового прибора, что, в свою очередь, приводит к восстановлению трансформированной вставкой из материала с эффектом памяти формы (3 на фиг.1, 2) своей первоначальной формы, при этом геометрия вставки меняется установленным образом, происходит целенаправленное разрушение области топологии, компактно содержащей конфиденциальную информацию.

ИСТОЧНИКИ ИНФОРМАЦИИ

1. Anti tamper encapsulation for an integrated circuit. Патент US №7005733, МПК H01L

23/02, опубликован 28.02.2006.

2. *Integrated circuit with reverse engineering protection.* Патент US №7008873, МПК H01L 21/44, H01L 21/00, H01L 21/84, H01L 21/338, H01L 21/4763, опубликован 28.07.2005.

3. *Integrated circuits protected against reverse engineering and method for fabricating the same using an apparent metal contact line terminating on field oxide.* Патент US №7294935, МПК H01L 23/52, H01L 29/40, опубликован 25.07.2002.

4. *Digital circuit with transistor geometry and channel stops providing camouflage against reverse engineering.* Патент US №5783846, МПК H01L 27/10, опубликован 21.07.1998.

5. *Digital circuit with transistor geometry and channel stops providing camouflage against reverse engineering.* Патент US №5930663, МПК H01L 27/10, опубликован 27.07.1999.

6. *Semiconductor integrated circuit with photo-detecting elements for reverse-engineering protection.* Патент US №7295455, МПК G11C 13/04, опубликован 16.08.2007.

7. *Destructor integrated circuit chip, interposer electronic device and methods.* Патент US №7489013, МПК H01L 23/06, опубликован 10.02.2009.

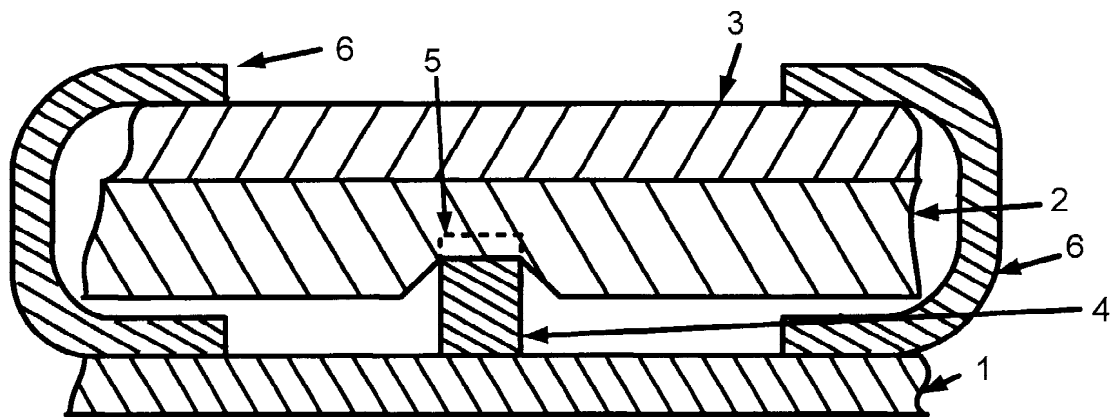
8. *High Transformation Temperature Shape Memory Alloy.* Патент US №5114504. 148/402, МПК C22C 19/00, опубликован 19.05.1992.

Формула изобретения

1. Полупроводниковый прибор, содержащий конфиденциальные данные, включающий корпус с кристаллом интегральной схемы и вставку из материала с эффектом памяти формы, размещенную внутри, которая при детектировании нарушения целостности корпуса, целенаправленно разрушает область кристалла, содержащую конфиденциальную информацию, отличающийся тем, что, с целью целенаправленной защиты областей топологии кристалла, вставка из материала с эффектом памяти формы имеет температуру трансформации выше максимальной рабочей температуры прибора; внутренний объем прибора заполняется полимеризованным наполнителем с температурой размягчения выше температуры трансформации упомянутой вставки с эффектом памяти формы, причем, защищаемая область кристалла прибора выполняется механически ослабленной, а форма вставки из материала с эффектом памяти формы выбирается таким образом, чтобы обеспечить разрушение упомянутого защищаемого участка кристалла полупроводникового прибора.

2. Полупроводниковый прибор по п.1, отличающийся тем, что механическое ослабление защищаемой области осуществляется структурой мембраны, изготовленной методом травления после изготовления кристалла на обратной стороне упомянутого кристалла прибора точно под областью топологии, которую мы защищаем, а вставка из материала с эффектом памяти формы представляет собой цилиндр, расположенный внутри мембраны между кристаллом прибора и корпусом.

3. Полупроводниковый прибор по п.1, отличающийся тем, что вставка из материала с эффектом памяти формы представляет собой сплошную пластину по размеру кристалла прибора, в которой имеется цилиндрическая выпуклость в области входящей в упомянутую мембранную структуру, изготовленную на обратной стороне упомянутого кристалла прибора точно под областью топологии, которую мы защищаем.



Фиг.2