(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 102119390 A
(43)申请公布日 2011.07.06

(21)申请号 200980131328.4

(22)申请日 2009.07.30

(30)优先权数据
0855536 2008.08.12 FR

(85)PCT申请进入国家阶段日
2011.02.11

(86)PCT申请的申请数据
PCT/EP2009/059891 2009.07.30

(87)PCT申请的公布数据
WO2010/018072 FR 2010.02.18

(71)申请人 法国电信教育集团－巴黎电信学院
地址 法国巴黎

(72)发明人 S·吉耶 J-L·当热 L·绍瓦热

(74)专利代理机构 永新专利商标代理有限公司 72002
代理人 刘瑜 王英

(51)Int.Cl.
G06F 21/02(2006.01)
G06F 21/00(2006.01)

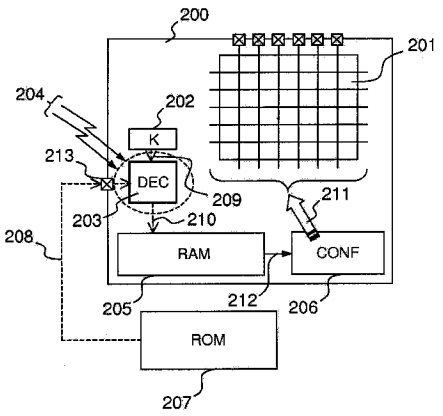
权利要求书 1 页 说明书 4 页 附图 2 页

(54)发明名称

防止可编程逻辑电路的配置文件被解密的方法以及实现该方法的电路

(57)摘要

本发明的主题是用于保护可编程逻辑电路(100,200)的方法,其特征在于:用于配置所述电路的可编程资源的一个或多个数据文件在被加密(112)后存储在非易失性存储器(107,207)中,所述电路内部的解密模块(103,203)负责使用存储在所述电路中的秘密密钥(102,202)来解密所述一个或多个文件,通过配置至少一个对抗技术保护解密模块在解密操作期间不受目的为获取密钥的攻击。本发明的主题还可以是FPGA类型的可编程逻辑电路,通过使用根据前面权利要求中的一个的方法来保护其在解密操作期间不受通过观察和/或故障注入的攻击。



CN 102119390 A

1. 用于保护可编程逻辑电路 (100,200) 的方法,其特征在于 :

用于所述电路的可编程资源的配置的数据文件在被加密 (112) 之后存储在非易失性存储器 (107,207) 中,所述电路内部的解密模块 (103,203) 负责通过使用存储在所述电路中的秘密密钥 (102,202) 来解密所述文件,通过实现至少一个对抗技术来保护所述解密模块在所述解密操作期间不受目的为获取所述密钥的隐藏信道攻击或基于故障的攻击,所述对抗技术包括 :差分逻辑保护、掩码保护和故障检测保护。

2. 根据权利要求 1 所述的方法,其特征在于 :所述可编程逻辑电路 (100,200) 是 FPGA 类型的。

3. 根据权利要求 1 或 2 中任一个所述的方法,其特征在于 :所述解密模块 (103,203) 是所述可编程逻辑电路 (100,200) 内部的专用逻辑电路。

4. 根据权利要求 1 或 2 中任一个所述的方法,其特征在于 :通过编程所述可编程逻辑电路 (100,200) 的所述可配置资源来实例化所述解密模块 (103,203)。

5. FPGA 类型的可编程逻辑电路 (100,200),其特征在于 :其包括所述电路内部的至少一个解密模块 (103,203),所述解密模块负责通过使用存储在所述电路中的秘密密钥 (102,202) 来解密用于所述电路的可编程资源的配置文件,通过使用根据前述权利要求中的一个所述的方法保护所述解密模块在所述解密操作期间不受观察和 / 或故障注入攻击。

防止可编程逻辑电路的配置文件被解密的方法以及实现该方法的电路

技术领域

[0001] 本发明涉及用于保护 FPGA 类型的可编程逻辑电路的配置文件的解密的方法，以及实现该方法的电路。

[0002] 本发明特别地应用于电子领域和可编程逻辑电路的安全领域。

背景技术

[0003] 电子元件市场的经济模型经历价值转换已经十多年了。因此，例如使用 VHDL 或 Verilog 语言生成的硬件的高级描述是最战略的部分，并且因此需要保护其不被伪造。

[0004] 此外，一些电路被嵌入秘密实现。对于诸如卫星电视或具有机密算法和协议的军事的内容分发市场部分的情况就是这样。

[0005] 因此，考虑到打击盗版的原因，需要使电路的逆向工程不可能进行，或至少是难于进行。在诸如 ASIC 电路的定制设计的产品中，随着性能尺寸 (characteristic dimensions) 的减少（目前是纳米量级），逆向工程变得愈加困难。然而，仍然使用特别的方法来保护具有高战略价值或存储 / 处理机密数据的敏感部分，所述特别的方法例如：

[0006] - 用金属化层遮蔽以阻止直接的显微镜观察；

[0007] - 使资源的可视标识复杂化的逻辑的处置；

[0008] - 扰频数据总线，其需要光密码分析方法以便能够解译任何标识的资源。

[0009] 相反地，在可重新配置的部件（例如，FPGA）中，要保护的信息是以通常用术语“比特流”描述的配置文件的形式可获得的。在一些 FPGA 系列中，该配置文件存储在例如 PROM 的非易失性存储器中，因为所述非易失性存储器是焊接的，所以其可以轻易地被抽取并且因此是完全可读的。由于该存储器不在 FPGA 产品设计者的价值链上，因此需要使其成本尽可能地低。因此，这些部件通常没有安全保护。在其他的 FPGA 系列中，配置文件被直接存储在 FPGA 矩阵中，使得对其进行访问更加复杂。

[0010] 然而，存在使用例如移位寄存器以对该文件进行写入和有时还进行读取的方法。因为 FPGA 特别容易受到目的为找到其配置文件的攻击，所以大型制造商提供集成在电路中的对抗方案。

[0011] 在当前实现中，通过使用例如 3DES 和 AES 算法的对称方法加密配置文件以使得配置文件的读取变得困难。此外，所述存储器和可编程逻辑电路之间的通信也受到保护，因为解密通常是在所述电路的芯片上执行的。

[0012] 解密逻辑操作本身未被保护来防止对其物理实现的攻击。因此，聪明的攻击可能找到加密密钥，然后因此访问包含在配置文件中的数据。

[0013] 要找到该加密密钥，可以实现两个系列的攻击：观察攻击和干扰或故障注入攻击。

[0014] 第一个系列的攻击，即观察攻击，利用处理加密的电路的瞬间的电耗特别地依赖于所处理的数据的事实。已知若干种类型的观察攻击。SPA（简单功率分析）试图基于在加密操作期间测量的中央单元的电耗的测量，来区分由该中央单元执行的操作。差分消耗分

析 DPA（差分功率分析）使用对在对随机消息进行加密操作的期间执行的大量电耗测量进行的统计操作，并且使用常量密钥来确认或否认关于密钥受限部分做出的假设。“模板”类型攻击在第一阶段使用与正在被攻击的设备相同的设备（除了该相同的设备不包含秘密的事实之外）以构建由密钥的受限部分的值索引的消耗模型，并且在第二阶段使用对正被攻击的设备的消耗的一些测量以确定与所测量的消耗最接近的模型并且因此确定子密钥的值。此外，导体中的任何电流流动产生电磁场，对其测量可以进行与特别由 DPA 进行的依靠电耗的攻击原理上相同的攻击。

[0015] 第二系列的攻击，即干扰或故障注入攻击，通过例如温度或电压变化、电源上的强伪造信号的功效或通过电磁场、激光射击等将干扰引入到系统中。所生成的错误导致正在被攻击的电路的节点的值被修改。取决于对硅的影响，它们可以是单一的或多次的、永久的或暂时的。暂时故障注入的灵活性通过进行多次测试引起更强烈的攻击并且增加成功的机会。使用单一故障的攻击简化了攻击过程。基于故障的攻击是基于非错误的加密输出和具有错误的输出之间的差分分析的。

[0016] 针对可编程部件的配置文件的安全模型正在失效：虽然通过加密防止了对包含文件的非易失性存储器的物理攻击，但是可编程部件上的解密电路未受保护并且可能遭受物理攻击。因此可以例如通过使用配置时钟上的触发器和测量瞬时磁场特征潜在地隔离配置文件的数据块的加密。该分析使得可以重新编制加密密钥，并且因此重新编制解密的配置文件。

发明内容

[0017] 本发明的一个目的是特别地克服上述缺点。

[0018] 为此，本发明的主题是用于保护可编程逻辑电路的方法。用于电路的可编程资源的配置的数据文件在被加密之后存储在非易失性存储器中，电路内部的解密模块负责通过使用存储在所述电路中的秘密密钥来解密文件，通过实现至少一个对抗技术来保护解密模块在解密操作期间不受目的在于获取密钥的隐藏信道攻击或基于故障的攻击，所述对抗技术包括：差分逻辑保护、掩码保护和故障检测保护。

[0019] 所述可编程逻辑电路例如是 FPGA 类型。

[0020] 解密模块例如可以是可编程逻辑电路内部的专用逻辑电路或通过编程可编程逻辑电路的可配置资源来实例化 (instantiate)。

[0021] 本发明的另一主题是 FPGA 类型的可编程逻辑电路，其特征在于其包括电路内部的至少一个解密模块，所述解密模块负责通过使用存储在所述电路中的秘密密钥来解密用于所述电路的可编程资源的配置文件，通过使用根据前面权利要求中的一个所述的方法来保护解密模块在解密操作期间不受观察和 / 或故障注入攻击。

附图说明

[0022] 通过结合附图以说明性和非限制性的例子的形式提供的以下描述，本发明的其他特性和优点将会变得显而易见，其中：

[0023] 图 1 说明了用于配置 FPGA 类型的可编程逻辑电路的示例过程；

[0024] 图 2 说明了用于初始化 FPGA 类型的可编程逻辑电路的示例过程和根据本发明保

护解密电路的方式。

具体实施方式

[0025] 图 1 说明了用于配置 FPGA 类型的可编程逻辑电路的示例过程。在该例子中，FPGA 100 包括可编程资源区域 101。一旦被编程，所述区域可以用于生成设计者针对的应用程序所需要的功能。可编程资源区域特别地包括可配置的逻辑块和这些逻辑块之间互连资源。可编程资源区域还包括通常被称为输入 / 输出块 (IOB) 的部件。这些块通过编程互连，IOB 使得可以定义 FPGA 的输入和输出端口 118 的使用。FPGA 100 包括特别地用于存储配置文件的 RAM 易失性存储器 104。配置逻辑模块 105 用于根据包含在配置文件中的易失性存储器 104 中的程序将逻辑块和 IOB 连接在一起。FPGA 100 包括可以用于解密配置文件的解密模块 103 和包含解密所需要的密钥的非易失性存储器 102 的区域。例如，PROM 类型的非易失性存储器 107 用于存储加密的配置文件。因此，即使当系统断电时，配置信息也被保存在存储器中并且被保护以防止任何攻击者。

[0026] 在系统的设计期间，FPGA 电路被编程以使得生成根据针对的应用程序的一个或多个功能。为此，设计者使用例如具有计算机辅助设计软件 (CAO) 的计算机 108。设计者使用诸如 VHDL 语言的高级硬件描述语言来编程所述一个或多个功能 110。对应的程序和数据 111 产生存储在计算机的存储器中的配置文件。设计者可选择来定义加密密钥 K 109 以保护所述配置数据。将该密钥作为参数 113 输入。使用例如 AES 或 3DES 的加密算法、利用密钥 K 113 来加密包含在配置文件中配置数据 111。然后将加密的配置文件放置到非易失性存储器 107 中 (116)。另一个方法是经由输入端口 114 将加密的配置文件直接地放置到 FPGA 内部的易失性存储器 104 中 (117)，这样做是为了例如系统测试的目的。为了配置可编程的资源区域 101，需要由 FPGA 解密配置文件。为此，将密钥 K 存储在部件内部 (102) 并且在设计阶段经由 FPGA 的端口 106 发送密钥 K(115)。

[0027] 图 2 说明了用于初始化 FPGA 类型的可编程逻辑电路的示例过程和根据本发明保护解密电路的方式。如先前所述，加密的配置文件通常存储在 FPGA 200 外部的非易失性存储器 207 中。当系统加电时，下载加密的配置文件 (208) 并将其作为输入经由例如输入端口 213 呈现给 FPGA 内部的解密模块 203。模块 203 使用密钥 K 202(209) 来解密文件并且将所述文件发送到内部的易失性存储器 205(210)。然后配置逻辑模块 206 使用配置文件 (212) 来配置可编程的资源区域 201(211)。

[0028] 在每次系统加电时系统地触发上文描述的初始化过程。目的在于识别存储在 FPGA 中的密钥 K(202) 并且然后解密配置文件的攻击者可以选择在系统的初始化期间研究解密模块 203 的操作。攻击者通过例如 ROM 207 和 FPGA200 之间的通信协议使用的同步时钟的使用来监视该初始化。然后通过观察或干扰注入来攻击解密模块 (204)。

[0029] 为了保护不受这些攻击 (204)，解密模块 203 可以实现各种对抗方法。

[0030] 例如，通过使用差分逻辑来保护解密模块不受观察攻击，特别是 DPA 类型的观察攻击。在最常见的差分逻辑中特别地存在以下几种 :

[0031] -WDDL(波动态差分逻辑)，其由 K.Tiri 和 I.Verbauwhede 在 2004 年 2 月巴黎的 date '04 上第 246-251 页、题名为“A Logic Level Design Methodology for a Secure DPA Resistant ASIC or FPGA Implementation”的文章中详述。该例子中的解密模块由两

个双重逻辑阵列构成，所述两个双重逻辑阵列通过互补逻辑工作，以使得模块的消耗几乎不变；

[0032] -SECLIB（安全库），其由 S.Guilley、P.Hoogvorst、Y.Mathieu、R.Pacalet、J.Provost 在 2004 年 2 月巴黎的 date '04 上第 1414-1415 页、题名为"CMOS structures suitable for secured Hardware"的文章中描述；

[0033] -SABL，其由 K.Tiri、M.Akmal 和 I.Verbauwhede 在 2002 年 9 月的 ESSCIRC 上第 403-406 页、题名为"A dynamic and Differential CMOS Logic with Signal Independant Power Consumption to Withstand Differential Power Analysis on Smart Cards"的文章中描述；

[0034] -MCML，其由 F.Regazzoni 等在 2007 年 7 月的 SAMOS IC 上、题名为"A Simulation-Based Methodology for Evaluating DPA-Resistance of Cryptographic Functional Units with Application to CMOS and MCML Technologies"的文章中描述；

[0035] -DyMCL，其由 M.W.Allam 和 M.I.Elmasry 在 2000 年的 10.1109/CICC.2000.852699 的第 421-424 页、题名为"Dynamic Current Mode Logic(DyMCL)，a new low-power/high-performancelogic family"的文章中描述；

[0036] -TDPL，其由 M.Burcci、L.Giancane、R.Luzzi 和 A.Trifiletti 在 Springer 2006 的 CHESS 的 LNCS 的 4249 卷的第 232-241 页、题名为"Three-phase dual-rail pre-charge logic"的文章中描述。

[0037] 防止隐藏信道上的攻击的另一种安全措施是对变量使用掩码。该掩码具有随机的值并且可以在诸如逻辑门的功能层使用。

[0038] 由 Mangard Stefan、Oswald Elisabeth 和 Popp Thomas 在 Springer 2007、名称为"Power Analysis Attacks：Revealing the Secrets of Smart Cards"的书中特别地描述了基于差分逻辑或掩码的对抗技术。

[0039] 为了保护不受故障注入类型干扰攻击，可以通过使用例如以下文章中描述的故障检测技术来保护解密电路：

[0040] -2002 年 12 月的 IEEE 计算机辅助设计会刊的 21(12) 的第 1509-1517 页、作者为 Y.Kim、R.Karri 和 K.Wu、题名为"Concurrent Error Detection Schemes for Fault Based Side-Channel Cryptanalysis of Symmetric Block Ciphers"的文章；

[0041] -2004 年 5 月的 IEEE 计算机辅助设计会刊的 21(2) 上的、作者为 M.Karpovsky、K.Kulikowski 和 A.Taubin、题名为"Robust Protection against Fault-Injection Attacks on Smart Cards Implementing the Advanced Encryption Standard"的文章；

[0042] -2003 年 4 月的 IEEE 计算机辅助设计会刊的 52(4) 上的、作者为 G.Bertoni、L.Breveglieri、I.Koren、P.Maistri 和 V.Piuri、题名为"Error Analysis and Detection Procedures for a Hardware Implementation of the Advanced Encryption Standard"的文章。

[0043] 通过使用上述技术中的一个或多个，增强了解密模块的保护并且这弥补了现有 FPGA 中观察到的失效。因此，用于可编程逻辑电路的保护机制的安全规范与嵌入式加密处理器的保护相互补充以处理物理观察或故障注入攻击。

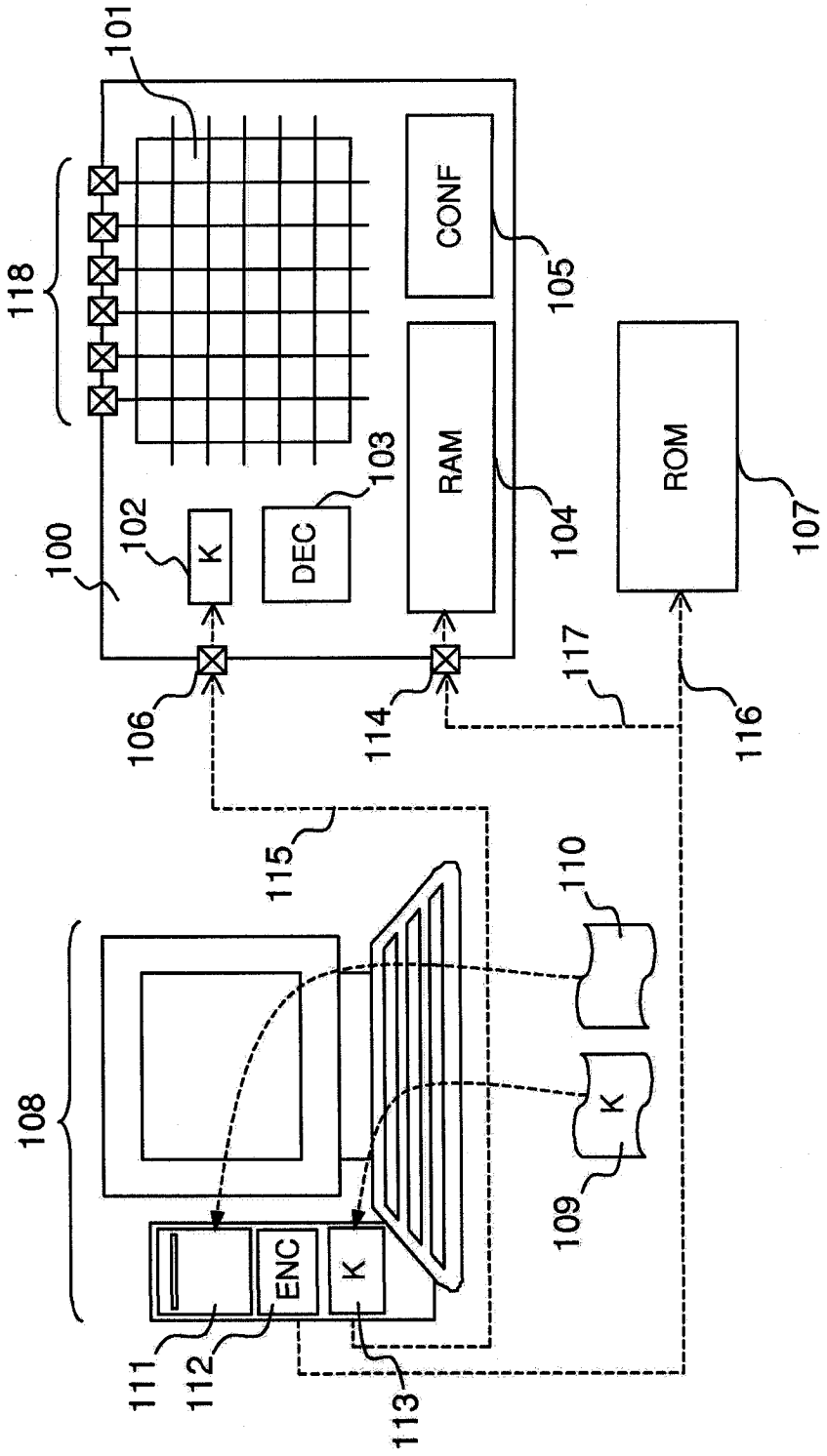

101
118
CONF
105
RAM
104
ROM
107
103
DEC
102
K
100
106
114
117
116
115
110
108
K
109
ENC
K
111
112
113

图 1

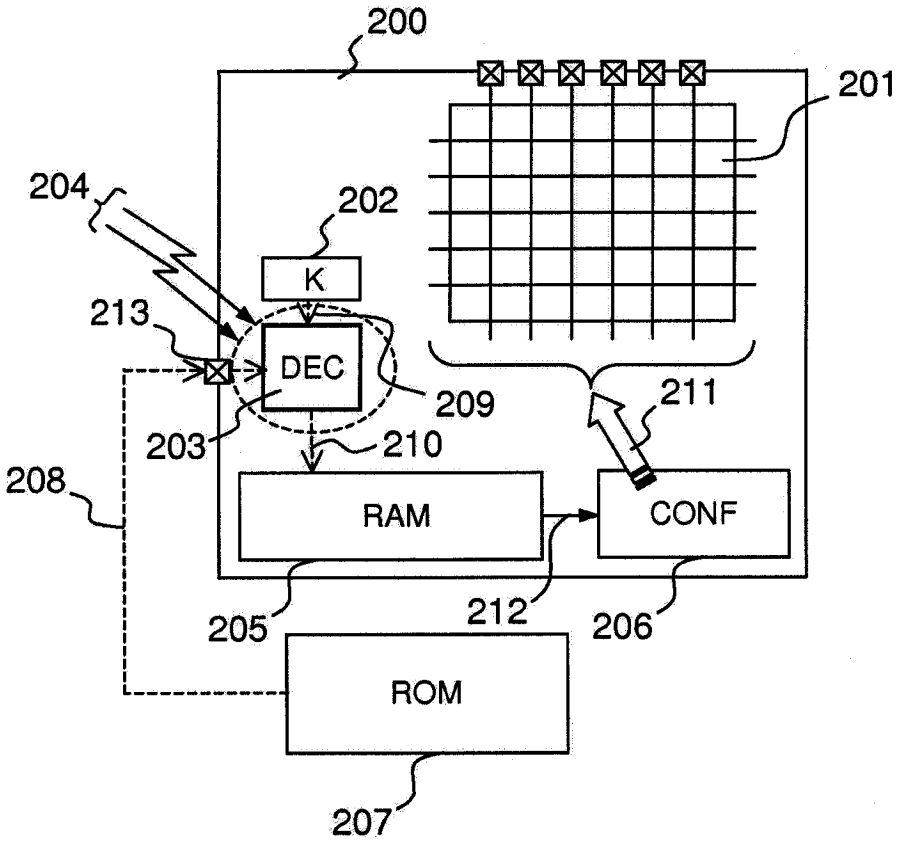

200
201
204
202
K
213
DEC
209
211
203
210
208
RAM
CONF
205
212
206
ROM
207

图 2