(19)中华人民共和国国家知识产权局

(12)实用新型专利

(10)授权公告号 CN 202711261 U
(45)授权公告日 2013.01.30

(21)申请号 201220405921.2

(22)申请日 2012.08.16

(73)专利权人 北京江南天安科技有限公司
地址 100088 北京市海淀区马甸东路 17 号金澳国际大厦 1110 室

(72)发明人 闫鸣生 王冠 李国 赵志国

(74)专利代理机构 北京轻创知识产权代理有限公司 11212
代理人 杨立

(51)Int.Cl.
G06F 21/62(2013.01)
G06F 21/77(2013.01)

(ESM)同样的发明创造已同日申请发明专利

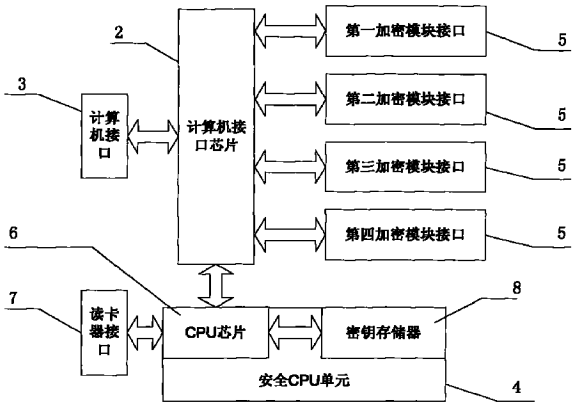
权利要求书 1 页 说明书 5 页 附图 2 页

(54)实用新型名称

一种加密卡

(57)摘要

本实用新型涉及一种加密卡，包括焊接在印制线路板上的计算机接口芯片、计算机接口、安全 CPU 单元和至少一个加密模块接口，所述计算机接口芯片通过印制线分别与所述计算机接口、所述安全 CPU 单元以及所述各加密模块接口相连。本加密卡可以根据不同使用需求和加解密运算的需要，更换或增减不同算法的加密模块，因为加密卡的各个加密模块接口具有统一的管脚结构，为实际应用提供了标准化的选择，使得加密卡具有充分的灵活性和便利性，大大减少了不同加密模块的产品设计工作，因而具有充分的灵活性和便利性，为实际设备的应用提供了标准化的选择，大大减少了产品设计工作。



CN 202711261 U

1. 一种加密卡，其特征在于：包括焊接在印制线路板上的计算机接口芯片、计算机接口、安全 CPU 单元和至少一个加密模块接口，所述计算机接口芯片通过印制线分别与所述计算机接口、所述安全 CPU 单元以及所述各加密模块接口相连；

所述计算机接口芯片，用于与计算机接口、安全 CPU 单元、各加密模块交换数据，并执行各种逻辑与时序控制功能；

所述计算机接口，用于实现加密卡和计算机之间交换数据；

所述安全 CPU 单元，用于实现加密卡的安全管理和密钥管理功能；

所述加密模块接口，用于与加密模块连接，通过加密模块实现多种不同的密码算法的运算。

2. 根据权利要求 1 所述一种加密卡，其特征在于：所述印制线路板上具有至少两个加密模块接口，所述各加密模块接口的管脚相同。

3. 根据权利要求 1 或 2 所述一种加密卡，其特征在于：所述安全 CPU 单元包括 CPU 芯片和密钥存储器，所述 CPU 芯片通过印制线分别与所述计算机接口芯片、所述密钥存储器相连；

所述 CPU 芯片，用于对加密卡安全管理功能的控制；

所述密钥存储器，用于存储密钥。

4. 根据权利要求 3 所述一种加密卡，其特征在于：所述 CPU 芯片还通过印制线与一个读卡器接口相连；

所述读卡器接口，用于连接读卡器，来读取或存放卡片中的外部安全数据。

5. 根据权利要求 1 或 2 所述一种加密卡，其特征在于：所述印制线路板上设有 4 个加密模块接口，所述每个加密模块接口具有 64 个 IO 管脚，所述印制线路板上的计算机接口芯片为具有 256 个数据管脚的现场可编程门阵列芯片，所述 4 个加密模块接口共计的 256 个 IO 管脚通过印制线与现场可编程门阵列芯片的 256 个数据管脚分别一一对应相连。

6. 根据权利要求 5 所述一种加密卡，其特征在于：所述每个加密模块接口有 80 个管脚，其中包括 3 个 1.2 伏电源线管脚、3 个 3.3 伏电源线管脚、3 个 5 伏电源线管脚、5 个地线管脚、1 个电源供电控制信号管脚、1 个复位信号管脚和 64 个 IO 管脚。

7. 根据权利要求 1 或 2 所述一种加密卡，其特征在于：所述每个加密模块接口有 80 个管脚，包括 3 个 1.2 伏电源线管脚、3 个 3.3 伏电源线管脚、3 个 5 伏电源线管脚、5 个地线管脚、1 个电源供电控制信号管脚、1 个复位信号管脚和 64 个 I O 管脚。

8. 根据权利要求 7 所述一种加密卡，其特征在于：所述每个加密模块接口的 80 个管脚按从上到下分成 4 行，每行 20 个管脚排列在印制线路板上。

9. 根据权利要求 1 或 2 所述一种加密卡，其特征在于：所述计算机接口为 PCI Express 接口。

一种加密卡

技术领域

[0001] 本实用新型涉及信息安全领域，特别是涉及一种加密卡。

背景技术

[0002] 国家密码局根据我国安全需要先后颁布了国产密码算法，包括 SM1、SM2、SM3、SM4 及祖冲之序列密码算法等，为支持不同的国产密码算法，就需要设计各种加密卡来满足支持这些国产密码算法的硬件插卡。

[0003] 采用加密卡结构的密码设备是在计算机上通过安装带密码功能的插卡方式实现的硬件平台。目前加密卡普遍采用专用加解密芯片来实现，而安全芯片受到实际应用限制，一般采用设计不同的板卡来为不同密码产品量身定做，其主要缺点是：单芯片的运算速度受到芯片的限制，加解密速度很慢；多芯片结构随意，不标准，实际使用受到局限；不同应用场合需要设计不同的板卡，设计工作量大。

实用新型内容

[0004] 本实用新型所要解决的技术问题是提供一种具有模块结构并可更换加密模块的加密卡。

[0005] 本实用新型解决上述技术问题的技术方案如下：一种加密卡，包括焊接在印制线路板上的计算机接口芯片、计算机接口、安全 CPU 单元和至少一个加密模块接口，所述计算机接口芯片通过印制线分别与所述计算机接口、所述安全 CPU 单元以及所述各加密模块接口相连；

[0006] 所述计算机接口芯片，用于与计算机接口、安全 CPU 单元、各加密模块交换数据，并执行各种逻辑与时序控制功能；

[0007] 所述计算机接口，用于实现加密卡和计算机之间交换数据；

[0008] 所述安全 CPU 单元，用于实现加密卡的安全管理和密钥管理功能；

[0009] 所述加密模块接口，用于与加密模块连接，通过加密模块实现多种不同的密码算法的运算。

[0010] 本实用新型的有益效果是：提供了一种支持国产密码算法的加密卡通用结构，使用时只需增减或更换加密模块，以满足加解密运算的不同使用需要，使用方便。

[0011] 在上述技术方案的基础上，本实用新型还可以做如下改进。

[0012] 进一步，所述印制线路板上具有至少两个加密模块接口，所述各加密模块接口的管脚相同。采用本结构的有益效果是可以各加密模块可以彼此通用，包括各种算法的加密模块可任意插在加密卡不同的加密模块接口上，具有较好的通用性和扩展性。

[0013] 进一步，所述安全 CPU 单元包括 CPU 芯片和密钥存储器，所述 CPU 芯片通过印制线分别与所述计算机接口芯片、所述密钥存储器相连；所述 CPU 芯片，用于对加密卡安全管理功能的控制；所述密钥存储器，用于存储密钥。采用上述结构可方便进行密钥管理及安全性管理等功能实现，密钥存储器用于存储各种应用密钥，使得加密卡具备了更加完善的密钥

管理功能，同时也方便在不同应用需要时所需做的更改，因为这些涉及管理与密钥的更改只需修改安全 CPU 单元内的软件即可完成。

[0014] 进一步，所述 CPU 芯片还通过印制线与一个读卡器接口相连；所述读卡器接口，用于连接读卡器，来读取或存放卡片中的外部安全数据。通过读卡器接口可方便的用于读取应用中所需的外部安全数据，这些安全数据可存放在智能 IC 的卡片中，如密钥要素、密码要素、安全数据的全部或部分数据等；也可以用于登录、权限管理及密钥管理等需要外部输入的项目，这些项目可存放在智能 IC 卡中，可以是数据，也可以是文件形式。

[0015] 进一步，所述印制线路板上设有 4 个加密模块接口，所述每个加密模块接口具有 64 个 IO 管脚，所述印制线路板上的计算机接口芯片为具有 256 个数据管脚的现场可编程门阵列芯片，所述 4 个加密模块接口共计的 256 个 IO 管脚通过印制线与现场可编程门阵列芯片的 256 个数据管脚分别一一对应相连。采用上述进一步方案的有益效果是芯片具有 256 个数据管脚，4 个加密模块每个加密模块具有 64 个 IO 管脚，设计标准、合理，具备较好扩展性。

[0016] 进一步，所述每个加密模块接口有 80 个管脚，其中包括 3 个 1.2 伏电源线管脚、3 个 3.3 伏电源线管脚、3 个 5 伏电源线管脚、5 个地线管脚、1 个电源供电控制信号管脚、1 个复位信号管脚和 64 个 IO 管脚。考虑到多种供电管脚，每个加密模块可以根据密码芯片的需要选择所需电源供电的种类和数量，而数据、地址、控制等信号可在 64 个 IO 管脚中根据需要选择，也可根据需要选择是否使用所提供的复位信号及电源控制管脚。这种灵活性的选择方式既满足了不同的设计使用要求，又具备一定扩展性。

[0017] 进一步，所述每个加密模块接口的 80 个管脚按从上到下分成 4 行，每行 20 个管脚排列在印制线路板上。这样设计的管脚布置较为整齐美观，方便利于用两个双排插座插接。

[0018] 进一步，所述计算机接口为 PCI Express 接口。优选采用这种本领域常用的计算机接口，以支持高速数据传输。

[0019] 本实用新型的有益效果是这种具有模块化结构的密码卡，可以根据不同使用需求和加解密运算的需要，使用加密卡时只需增减或更换加密模块即可；因为这种加密卡的各个加密模块接口具有统一的管脚结构，为实际应用提供了标准化的选择，使得加密卡具有充分的灵活性和便利性，大大减少了不同加密模块的产品设计工作；另外本实用新型优选实施例中的各元件管脚设计合理，具备较宽的应用性和拓展性，易于标准化生产。

附图说明

[0020] 图 1 为本实用新型组成示意模块图；

[0021] 图 2 为加密卡电路板示意图；

[0022] 图 3 为本实用新型加密模块接口管脚排列示意图。

[0023] 附图中，各标号所代表的部件列表如下：

[0024] 1、印制线路板，2、计算机接口芯片，3、计算机接口，4、安全 CPU 单元，5、加密模块接口，6、CPU 芯片，7、读卡器接口，8、密钥存储器。

具体实施方式

[0025] 以下结合附图对本实用新型的原理和特征进行描述，所举实例只用于解释本实用

新型，并非用于限定本实用新型的范围。

[0026] 如图 1、图 2 所示，本实用新型包括在印制线路板 1 上焊接的计算机接口芯片 2、计算机接口 3、安全 CPU 单元 4 和至少一个加密模块接口 5，当加密卡具有多个加密模块接口 5 时，这些加密模块接口 5 应具有相同的管脚结构，使得具有相配合插脚的加密模块可通用的插到任一加密模块接口上，当然如果只有一个加密模块接口，同样优选与具有多个加密模块接口 5 具有统一相同的管脚结构，通过更换加密模块接口 5 上的加密模块实现不同的使用需求，这就使得具备这种可更换模块结构的加密卡具有良好的通用性和扩展性，计算机接口芯片 2 通过印制线分别与所述计算机接口 3、所述安全 CPU 单元 4 以及所述各加密模块接口 5 相连并实现数据交换，其中 ：

[0027] 计算机接口 3 用于实现加密卡和计算机之间交换数据，可选用本领域常用的 PCI Express(PCIE) 高速接口，可根据实际需要配置 1X、2X、4X 等不同的接口速率 ；

[0028] 安全 CPU 单元 4 包括 CPU 芯片 6、密钥存储器 8，用于实现加密卡的安全管理和密钥管理功能 ；CPU 芯片 6 通过印制线分别与计算机接口芯片 2、密钥存储器 8 相连，用于对加密卡安全管理功能的控制 ；CPU6 还可以跟一个读卡器接口 7 相连，读卡器接口 7 用于连接读卡器，来读取或存放卡片中的外部安全数据 ；这里 CPU 芯片 6 可以是一个 32 位单片机，支持外部存储器访问方式，并使用存储器方式访问计算机接口芯片 2 编程的 RAM 接口，用于与各加密模块的通信，同时采用 CPU 芯片 6 的 SPI（串行外设接口）总线访问串行 FLASH 闪存，用于读、写、删除密钥数据 ；CPU 芯片 6 通过 RS232 接口访问读卡器，用于密钥导入、导出，配置的导入、导出及身份管理等加密卡的管理 ；

[0029] 计算机接口芯片 2 用于与计算机接口、安全 CPU 单元、各加密模块交换数据，并执行各种逻辑与时序控制功能，计算机接口芯片 2 可采用现场可编程门阵列芯片 FPGA，这里选用 Altera 公司的 Cyclone IV 系列的 GX 芯片，该芯片自带支持 PCI Express 的高速串行收发器模组，利用此高速串行收发器模组实现计算机接口 3 的功能，可方便的实现与计算机的高速通信。该 FPGA 具有 256 个数据管脚，将 256 个数据管脚分为 4 组，每组 64 个数据管脚。当然，该 FPGA 也可以选择具有 256 个以上数据管脚的规格，并用其中的 256 个数据管脚与 4 个加密模块接口 5 的 256 个 IO 管脚一一相连 ；

[0030] 所述印制线路板 1 上设有至少一个加密模块接口 5，加密模块接口 5 用于与加密模块的连接，加密模块用于执行多种不同的密码算法的运算，这些加密模块接口 5 的管脚结构均相同，也就是说具有相配插脚的加密模块可以插在任一加密模块接口 5 上 . 为满足实际需要例如对加解密速度的要求，并与前面选择 FPGA 数据管脚数量匹配，可在印制线路板上设有 4 个加密模块接口 5，每个加密模块接口 5 具有 80 个管脚，其中包括 3 个 1.2 伏电源线管脚、3 个 3.3 伏电源线管脚、3 个 5 伏电源线管脚、5 个地线管脚、1 个电源供电控制信号管脚、1 个复位信号管脚和 64 个 IO 管脚。加密模块接口管脚的上述定义如表 1 所示 ：

[0031] 表 1

[0032]

A1	VCC1.2	B1	GND	C1	VCC5.0	D1	GND
A2	VCC1.2	B2	VCC1.2	C2	VCC5.0	D2	VCC5.0

A3	IOx_00	B3	IOx_16	C3	IOx_32	D3	IOx_48
A4	IOx_01	B4	IOx_17	C4	IOx_33	D4	IOx_49
A5	IOx_02	B5	IOx_18	C5	IOx_34	D5	IOx_50
A6	IOx_03	B6	IOx_19	C6	IOx_35	D6	IOx_51
A7	IOx_04	B7	IOx_20	C7	IOx_36	D7	IOx_52
A8	IOx_05	B8	IOx_21	C8	IOx_37	D8	IOx_53
A9	IOx_06	B9	IOx_22	C9	IOx_38	D9	IOx_54
A10	IOx_07	B10	IOx_23	C10	IOx_39	D10	IOx_55
A11	IOx_08	B11	IOx_24	C11	IOx_40	D11	IOx_56
A12	IOx_09	B12	IOx_25	C12	IOx_41	D12	IOx_57
A13	IOx_10	B13	IOx_26	C13	IOx_42	D13	IOx_58
A14	IOx_11	B14	IOx_27	C14	IOx_43	D14	IOx_59
A15	IOx_12	B15	IOx_28	C15	IOx_44	D15	IOx_60
A16	IOx_13	B16	IOx_29	C16	IOx_45	D16	IOx_61
A17	IOx_14	B17	IOx_30	C17	IOx_46	D17	IOx_62
A18	IOx_15	B18	IOx_31	C18	IOx_47	D18	IOx_63
A19	RESET	B19	PWRON	C19	VCC3.3	D19	VCC3.3
A20	GND	B20	GND	C20	GND	D20	VCC3.3

[0033] 其中：

[0034] GND：地线

[0035] VCC1.2：1.2V 电源线

[0036] VCC3.3：3.3V 电源线

[0037] VCC5.0：5V 电源线

[0038] RESET：复位信号，低电平有效；

[0039] PWRON：电源供电控制信号，高电平有效；

[0040] IOx_yy：第 x 个模块，第 yy 个 IO 端口，x = 0-3，yy = 0-63

[0041] 如图 3 所示，每个加密模块接口的 80 个管脚可以按从上到下分成 4 行，每行 20 个的方式排列在印制线路板上。

[0042] 然后将前述的计算机接口芯片 2 上的分成 4 组每组 64 个数据管脚与 4 个加密模块接口 5，其中每个加密模块 5 具有 64 个 IO 管脚通过印制线一一对应相连，即形成了 4 个加密模块接口共计的 256 个 IO 管脚通过印制线与计算机接口芯片 2 的 256 个数据管脚一一对应相连。

[0043] 将具有不同算法的算法制成具有统一管脚结构的加密模块，根据加密内容的不同在加密模块接口 5 处更换不同的与加密模块，可选择的加密模块包括但不限于：

[0044] 非对称密码模块，用于 RSA 公钥算法、SM2 国产公钥密码算法、ECC 国际标准椭圆算法等非对称加解密运算；

[0045] 分组对称密码模块，用于 DES(Data Encryption Standard) 数据加密标准算法、3DES(3Data Encryption Standard) 三重数据加密标准算法、SM1 国产对称密码算法、AES(Advanced Encryption Standard) 先进加密标准算法等分组对称加解密运算；

[0046] 可编程密码模块，用于支持新公布的密码算法或无合适密码芯片支持但可以通过 FPGA 编程实现的密码算法，如 SM4 国产对称密码算法、祖冲之序列密码算法的加解密运算。

[0047] 利用 FPGA 的可编程性，通过对 FPGA 加载不同的程序来完成最对不同的加密模块的加解密算法支持，编程的程序包括但不限于：接口 IO 的输入输出定义；接口的实现，包括先入先出存储器、随机存储器、状态寄存器及中断处理等固件模块；时序控制器、时钟及访问控制逻辑。

[0048] 以上所述仅为本实用新型的较佳实施例，本实用新型不局限于上述具体实施方式，在本领域普通技术人员所具备的知识范围内，还可以在不脱离本发明宗旨的前提下做出各种结构变化，例如加密模块的数量不同以及带来的计算机接口芯片管脚数量的变化；采用其他类型或型号的可编程芯片、计算机接口等等；还有仅管脚数量不同的等同变化等，均落在本实用新型的保护范围之中。

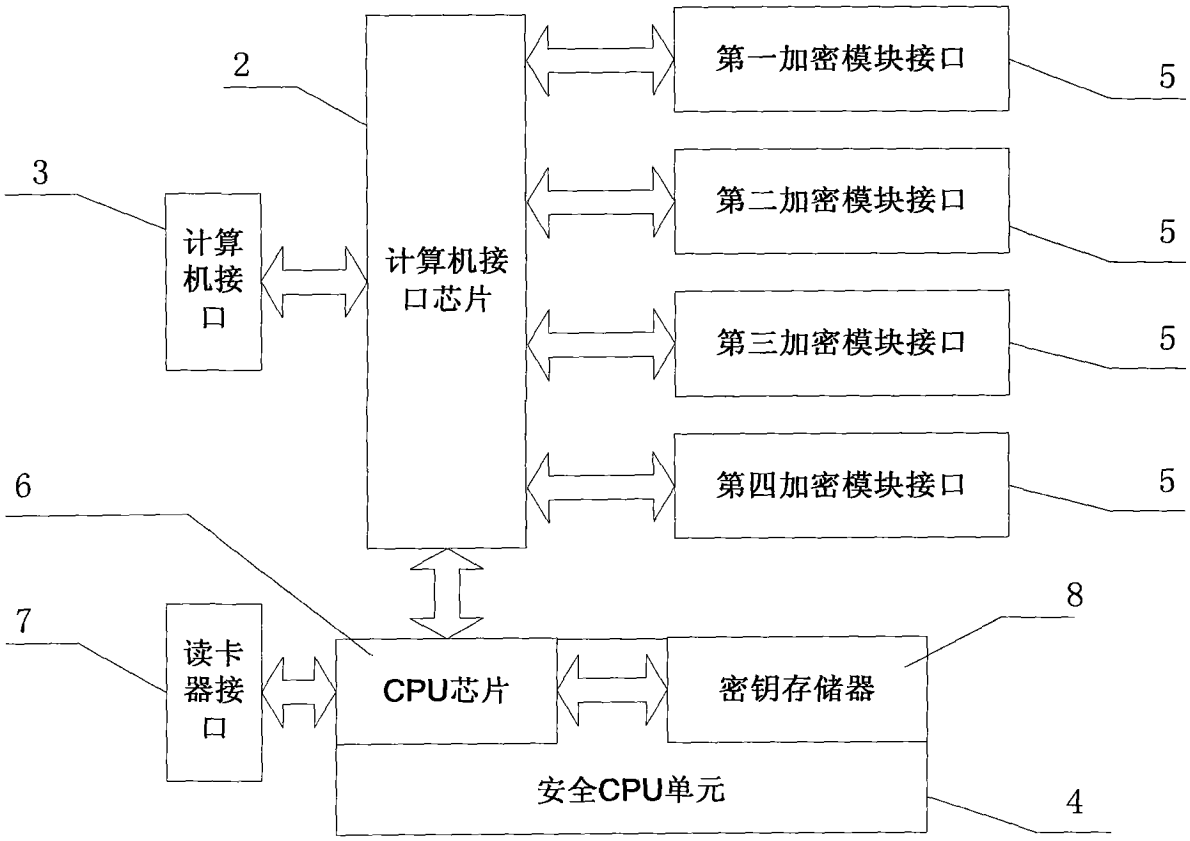

2
第一加密模块接口
5
3
第二加密模块接口
5
计算机接口
计算机接口芯片
第三加密模块接口
5
第四加密模块接口
5
6
8
7
读卡器接口
CPU芯片
密钥存储器
安全CPU单元
4

图 1

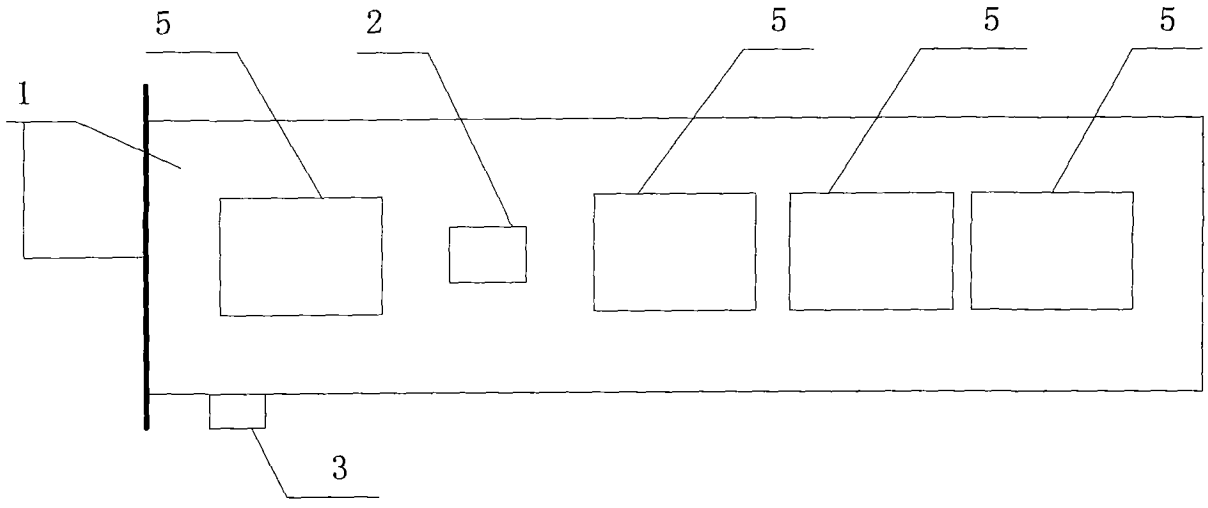

5
2
5
5
5
1
3

图 2

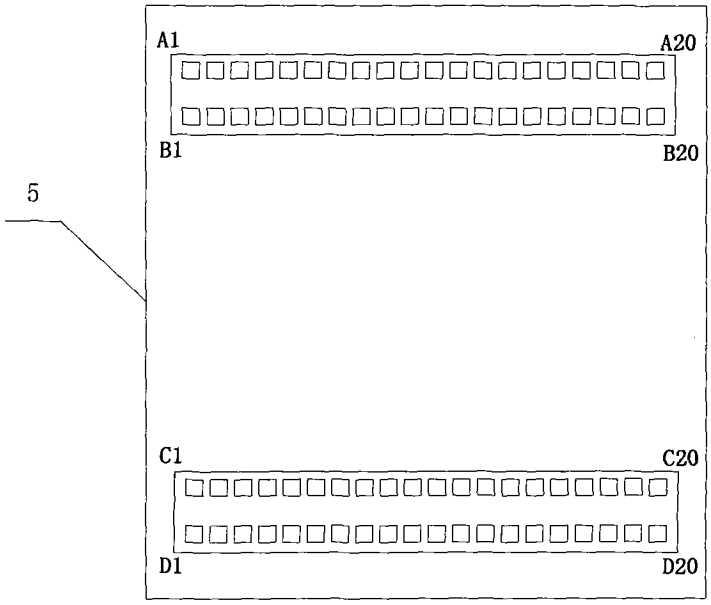


图 3