(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 105184191 A
(43)申请公布日 2015.12.23

(21)申请号 201510491295.1

(22)申请日 2015.08.12

(71)申请人 苏州芯动科技有限公司
地址 215021 江苏省苏州市工业园区独墅湖高教区仁爱路99号西交大科技园D栋608

(72)发明人 敖海 李伟

(74)专利代理机构 苏州市新苏专利事务所有限公司 32221
代理人 徐鸣

(51)Int.Cl.
G06F 21/72(2013.01)
G06F 21/76(2013.01)
G06F 21/77(2013.01)

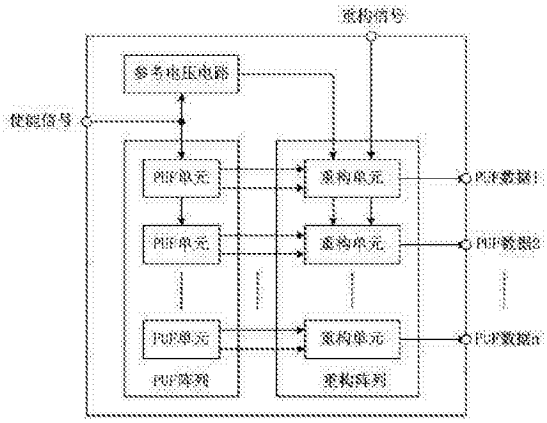
权利要求书2页 说明书5页 附图2页

(54)发明名称

一种可重构物理不可克隆功能电路

(57)摘要

本发明公开了一种可重构物理不可克隆功能电路，该功能电路包括具有至少1个PUF单元、该PUF单元包括至少两个电阻分压单元的PUF阵列，每个电阻分压单元产生并输出一个PUF电压信号至重构阵列，该重构阵列包括至少1个重构单元，PUF阵列以及重构阵列分别与参考电压电路相连，使能信号连接至该参考电压电路以及PUF阵列中的每个PUF单元，重构信号连接至重构阵列中的每个重构单元控制其对PUF数据进行重构。本发明相比现有不可重构PUF电路，电路成本低，节省电路功耗。芯片掉电，PUF数据消失，即使芯片不掉电，通过关闭使能信号亦可删除PUF数据，提高系统安全性。



CN 105184191 A

1. 一种可重构物理不可克隆功能电路，其特征在于，所述功能电路包括 PUF 阵列、重构阵列、参考电压电路，其中：

所述 PUF 阵列包括至少 1 个 PUF 单元，该 PUF 单元包括至少两个电阻分压单元，每个电阻分压单元产生并输出一个 PUF 电压信号至所述的重构阵列，该重构阵列包括至少 1 个重构单元，所述的 PUF 阵列以及所述的重构阵列分别与所述的参考电压电路相连，使能信号连接至该参考电压电路以及所述 PUF 阵列中的每个 PUF 单元，重构信号连接至所述重构阵列中的每个重构单元控制其对 PUF 数据进行重构。

2. 根据权利要求 1 所述的可重构物理不可克隆功能电路，其特征在于：所述电阻分压单元包括电阻 1、电阻 2、开关 1 和开关 2，电阻 1 与电阻 2 串联连接，该电阻 1 与该电阻 2 连接端通过开关 2 连接至所述的 PUF 电压信号，电阻 1 未与电阻 2 连接的一端通过开关 1 连接至电源，电阻 2 未与电阻 1 连接的一端连接至地，开关 1 和开关 2 由所述的使能信号控制开关。

3. 根据权利要求 2 所述的可重构物理不可克隆功能电路，其特征在于：所述电阻分压单元中开关 1 和开关 2 由使能信号控制，当使能信号有效时，开关 1 和开关 2 导通，电阻分压单元打开，电阻 1 通过开关 1 接通电源，电阻分压单元产生一个由工艺偏差决定的 PUF 电压，PUF 电压通过开关 2 连接至对应的重构单元；使能信号无效时，开关 1 和开关 2 关断，电阻分压单元关闭。

4. 根据权利要求 2 所述的可重构物理不可克隆功能电路，其特征在于：所述电阻分压单元中电阻 1 和电阻 2 采用相同的尺寸、类型和版图设计，该电阻 1 和电阻 2 的类型为多晶硅电阻、阱电阻或者热电阻。

5. 根据权利要求 1 所述的可重构物理不可克隆功能电路，其特征在于：所述参考电压电路包括电阻 3、电阻 4 和开关 3，电阻 3 与电阻 4 串联连接，该电阻 3 和该电阻 4 连接端与参考电压信号相连，该电阻 3 未与该电阻 4 连接的一端通过开关 3 连接至电源，电阻 4 未与电阻 3 连接的一端连接至地，开关 3 由所述的使能信号控制开关。

6. 根据权利要求 5 所述的可重构物理不可克隆功能电路，其特征在于：所述的参考电压电路中电阻 3 和电阻 4 采用相同的尺寸和类型，且采用版图匹配设计。

7. 根据权利要求 1 所述的可重构物理不可克隆功能电路，其特征在于：所述 PUF 阵列由包含 m 行、n 列的任意矩阵构成，其中，m 和 n 为≥ 1 的整数，所述的 PUF 单元的个数等于 m×n，所述的重构阵列中重构单元的个数等于 n，PUF 阵列产生 m×n 位 PUF 数据信号；每一列 PUF 单元中的每个 PUF 单元产生的至少两个 PUF 电压信号连接至所述重构阵列中与该列 PUF 单元对应的一个重构单元，该重构单元对单个 PUF 单元产生的至少两个 PUF 电压进行比较，产生 1 位 PUF 数据。

8. 根据权利要求 1 所述的可重构物理不可克隆功能电路，其特征在于：所述重构单元包括一个多选二电路和一个比较器，对 PUF 数据进行提取，与重构单元相对应的 PUF 单元输出的至少两个 PUF 电压信号以及参考电压电路输出的参考电压信号分别连接至该多选二电路，该多选二电路输出的两个电压信号分别连接至所述比较器的正负输入端，该比较器输出端连接至 PUF 数据信号，多选二电路由重构信号控制。

9. 根据权利要求 1 所述的可重构物理不可克隆功能电路，其特征在于：所述重构单元中多选二电路由重构信号控制，从输入的至少两个 PUF 电压和参考电压信号中选择其中两

个电压信号输出到比较器正负输入端；比较器对多选二电路输出的两个电压信号进行比较，产生一位 PUF 数据；若比较器正端输入电压高于负端，则输出 PUF 数据 1，反之，则输出 PUF 数据 0；在不同的重构信号控制下，重构单元可以从单个 PUF 单元产生的多个 PUF 电压以及参考电压之中选择不同的两个电压进行比较，从同一个 PUF 单元中提取出多个不同的 PUF 数据，实现 PUF 数据的重构，若 PUF 单元中电阻分压单元的个数为 k，k 为≥ 2 的整数，重构单元中多选二电路为 (k+1) 选二电路，则 PUF 数据的可重构数目为 0.5×k×(k+1)。

10. 根据权利要求 1 所述的可重构物理不可克隆功能电路，其特征在于：所述的功能电路 PUF 数据的提取和重构的步骤包括：

步骤一，外部控制电路开始提取 PUF 数据，发出有效的使能信号和重构信号，若需要重构 PUF 数据，则使用与上次提取不同的重构信号，若不需要重构 PUF 数据，则使用相同的重构信号；

步骤二，参考电压电路接收到使能信号，产生参考电压，连接至每个重构单元，PUF 阵列接收到使能信号，打开 PUF 单元，每个 PUF 单元产生多个 PUF 电压信号，连接至对应的重构单元；

步骤三，重构阵列接收到重构信号，重构单元根据重构信号从 PUF 单元产生多个 PUF 电压信号以及参考电压中选择对应的两个电压信号进行比较，产生 PUF 数据；

步骤四，外部控制电路读取重构阵列产生的所有 PUF 数据，完成 PUF 数据的提取后，关闭使能信号，电路关断，PUF 数据消失。

一种可重构物理不可克隆功能电路

技术领域

[0001] 本发明涉及物理不可克隆技术和信息安全技术，具体涉及一种可重构物理不可克隆功能电路。

背景技术

[0002] 物理不可克隆技术(Physical Unclonable Function, PUF)是近年来不断发展的一种信息安全技术。该技术具有不可预测、不可复制、不可篡改等众多优点，可以极大地提高系统在加密、防伪等方面的安全性。因此，PUF 技术在信息安全领域将具有广阔的应用前景。

[0003] PUF 技术主要分为非电子类 PUF 和电子类 PUF。非电子类 PUF 包括光学 PUF 等。电子类 PUF 基于集成电路(Integrated Circuit)制造技术，使用各种集成电路器件来构成其实施电路，并利用集成电路制造工艺的随机偏差，来实现其唯一且不可复制的特性。因此，电子类 PUF 可以在各种集成电路工艺下实现，并集成到芯片之中。

[0004] 除了可靠性之外，许多应用场合对 PUF 电路的面积、功耗也有着严格的要求，并且一些应用系统在不同时刻需要使用不同的 PUF 数据，即需要对 PUF 数据进行重构。传统上通过增加 PUF 电路模块的数量来实现 PUF 数据的重构，但这种方法增加了芯片的成本和功耗。因此，设计一种低成本、低功耗且可重构的 PUF 电路具有重要的应用意义。

发明内容

[0005] 针对上述现有技术存在的不足，本发明提供了一种可重构物理不可克隆功能电路，利用电阻的工艺偏差来产生 PUF 数据，具有可靠性高、功耗低等优点，且以较小的电路成本实现 PUF 电路的可重构功能，不需要增加整个 PUF 电路模块，可降低芯片的成本。

[0006] 本发明提供的可重构物理不可克隆功能电路的特征在于：所述功能电路包括 PUF 阵列、重构阵列、参考电压电路，其中：

所述 PUF 阵列包括至少 1 个 PUF 单元，该 PUF 单元包括至少两个电阻分压单元，每个电阻分压单元产生并输出一个 PUF 电压信号至所述的重构阵列，该重构阵列包括至少 1 个重构单元，所述的 PUF 阵列以及所述的重构阵列分别与所述的参考电压电路相连，使能信号连接至该参考电压电路以及所述 PUF 阵列中的每个 PUF 单元，重构信号连接至所述重构阵列中的每个重构单元控制其对 PUF 数据进行重构。

[0007] 所述电阻分压单元包括电阻 1、电阻 2、开关 1 和开关 2，电阻 1 与电阻 2 串联连接，该电阻 1 与该电阻 2 连接端通过开关 2 连接至所述的 PUF 电压信号，电阻 1 未与电阻 2 连接的一端通过开关 1 连接至电源，电阻 2 未与电阻 1 连接的一端连接至地，开关 1 和开关 2 由所述的使能信号控制开关。

[0008] 所述参考电压电路包括电阻 3、电阻 4 和开关 3，电阻 3 与电阻 4 串联连接，该电阻 3 和该电阻 4 连接端与参考电压信号相连，该电阻 3 未与该电阻 4 连接的一端通过开关 3 连接至电源，电阻 4 未与电阻 3 连接的一端连接至地，开关 3 由所述的使能信号控制开关。

[0009] 所述重构单元包括一个多选二电路和一个比较器，对 PUF 数据进行提取，与重构单元相对应的 PUF 单元输出的至少两个 PUF 电压信号以及参考电压电路输出的参考电压信号分别连接至该多选二电路，该多选二电路输出的两个电压信号分别连接至所述比较器的正负输入端，该比较器输出端连接至 PUF 数据信号，多选二电路由重构信号控制。

[0010] 进一步的，所述 PUF 阵列由包含 m 行、n 列的任意矩阵构成，其中，m 和 n 为≥ 1 的整数，所述的 PUF 单元的个数等于 m×n，所述的重构阵列中重构单元的个数等于 n，PUF 阵列产生 m×n 位 PUF 数据信号。每一列 PUF 单元中的每个 PUF 单元产生的至少两个 PUF 电压信号连接至所述重构阵列中与该列 PUF 单元对应的一个重构单元，该重构单元对单个 PUF 单元产生的至少两个 PUF 电压进行比较，产生 1 位 PUF 数据。提取 PUF 数据时，所述的使能信号依次选择上述 PUF 阵列中的一行 PUF 单元连接至重构阵列，重构阵列对该行 PUF 数据进行提取，提取完成后使能信号则选择下一行 PUF 单元进行提取，直至所有 PUF 数据被提取。

[0011] 进一步的改进方案为，所述电阻分压单元中开关 1 和开关 2 由使能信号控制，当使能信号有效时，开关 1 和开关 2 导通，电阻分压单元打开，电阻 1 通过开关 1 接通电源，电阻分压单元产生一个由工艺偏差决定的 PUF 电压，PUF 电压通过开关 2 连接至对应的重构单元。使能信号无效时，开关 1 和开关 2 关断，电阻分压单元关闭，节省功耗。电阻 1 和电阻 2 采用相同的尺寸、类型和版图设计。上述电阻的类型为多晶硅电阻、阱电阻或热电阻等。

[0012] 进一步的改进方案为，所述重构单元中多选二电路由重构信号控制，从输入的至少两个 PUF 电压和参考电压信号中选择其中两个电压信号输出到比较器正负输入端。比较器对多选二电路输出的两个电压信号进行比较，产生一位 PUF 数据。若比较器正端输入电压高于负端，则输出 PUF 数据 1，反之，则输出 PUF 数据 0。在不同的重构信号控制下，重构单元可以从单个 PUF 单元产生的多个 PUF 电压以及参考电压之中选择不同的两个电压进行比较，从同一个 PUF 单元中提取出多个不同的 PUF 数据。因此，重构阵列可以从同一个 PUF 阵列中提取出多组不同的 PUF 数据，实现 PUF 数据的重构。若 PUF 单元中电阻分压单元的个数为 k，k 为≥ 2 的整数，重构单元中多选二电路为 (k+1) 选二电路，则 PUF 数据的可重构数目为 0.5×k×(k+1)。通过增加 PUF 单元中电阻分压单元的个数，可增加 PUF 数据的可重构数目。

[0013] 所述的参考电压电路中电阻 3 和电阻 4 采用相同的尺寸和类型，且采用较大的宽度和长度尺寸设计和版图匹配设计，使该电阻 3 和电阻 4 的工艺偏差最小化，以产生一个精确的参考电压信号。

[0014] 所述的 PUF 数据的提取和重构的步骤包括：

步骤一，外部控制电路开始提取 PUF 数据，发出有效的使能信号和重构信号，若需要重构 PUF 数据，则使用与上次提取不同的重构信号，若不需要重构 PUF 数据，则使用相同的重构信号；

步骤二，参考电压电路接收到使能信号，产生参考电压，连接至每个重构单元，PUF 阵列接收到使能信号，打开 PUF 单元，每个 PUF 单元产生多个 PUF 电压信号，连接至对应的重构单元；

步骤三，重构阵列接收到重构信号，重构单元根据重构信号从 PUF 单元产生多个 PUF 电压信号以及参考电压中选择对应的两个电压信号进行比较，产生 PUF 数据；

步骤四，外部控制电路读取重构阵列产生的所有 PUF 数据，完成 PUF 数据的提取后，关

闭使能信号，电路关断，PUF 数据消失。

[0015] 本发明提供的可重构物理不可克隆功能电路，相比现有不可重构 PUF 电路，通过增加一个参考电压电路或者在 PUF 单元中增加一个电阻分压单元，即可实现可重构 PUF 电路，进一步增加电阻分压单元的个数则可获得近似具有平方关系的可重构数目，电路成本低。不使用的电路可被使能信号关闭，节省电路功耗。可根据实际应用需求灵活设计 PUF 电路的结构，以实现最低的成本和功耗。芯片掉电，PUF 数据消失，即使芯片不掉电，通过关闭使能信号亦可删除 PUF 数据，提高系统安全性。

附图说明

[0016] 图 1 为本发明实施例的电路结构示意图；

图 2 为本发明实施例中 PUF 单元示意图；

图 3 为本发明实施例中电阻分压单元示意图；

图 4 为本发明实施例中参考电压电路示意图；

图 5 为本发明实施例中重构单元示意图。

具体实施方式

[0017] 下面结合附图及实施例对本发明的具体实施方式进一步加以描述，以使本发明所属技术领域的技术人员能够容易实施本发明。

[0018] 请参见图 1 所示，本实施例提供的可重构物理不可克隆功能电路，包括 PUF 阵列、重构阵列和参考电压电路，所述的 PUF 阵列以及重构阵列分别与所述的参考电压电路相连。所述的 PUF 阵列包括至少 1 个 PUF 单元，该 PUF 单元包括至少两个电阻分压单元，每个电阻分压单元产生一个 PUF 电压信号至所述的重构阵列，使能信号连接至该 PUF 单元控制其打开或关闭。使能信号同时连接至所述参考电压电路，控制参考电压电路的打开或关闭。所述的重构阵列包括至少 1 个重构单元，该重构单元包括 1 个多选二电路和 1 个比较器，对 PUF 数据进行提取，重构信号连接至重构单元控制其对 PUF 数据进行重构。参考电压电路包括两个串联分压电阻，输出参考电压信号。

[0019] 本实施例电路中，若 PUF 阵列采用 1×n 的矩阵结构，该 PUF 阵列具有 1×n 个 PUF 单元，每个 PUF 单元包含两个电阻分压单元，重构阵列包括 n 个重构单元，且重构单元中多选二电路为三选二电路，则可得到如图 1 所示的本发明实施例。

[0020] 如图 1 所示，所述的 PUF 阵列由 n 个 PUF 单元组成，所述的重构阵列由 n 个重构单元组成，n 为≥ 1 的整数，n 的大小可根据实际应用对 PUF 数据位数的需求来确定。PUF 阵列中每个 PUF 单元输出的至少两个 PUF 电压信号连接至所述重构阵列中与该列 PUF 单元对应的重构单元。该重构单元包括一个多选二电路和一个比较器，对 PUF 数据进行提取，该重构单元对单个 PUF 单元产生的至少两个 PUF 电压进行比较，产生 1 位 PUF 数据。外部输入的使能信号连接至 PUF 阵列中的每个 PUF 单元和参考电压电路。外部输入的重构信号连接至重构阵列中的每个重构单元。提取 PUF 数据时，所述的使能信号依次选择上述 PUF 阵列中的一行 PUF 单元连接至重构阵列，重构阵列对该行 PUF 数据进行提取，提取完成后使能信号则选择下一行 PUF 单元进行提取，直至所有 PUF 数据被提取。重构单元对 PUF 单元进行提取后可输出 1 位 PUF 数据，整个重构阵列对 PUF 阵列进行提取后输出 n 位 PUF 数据。参

考电压电路输出的参考电压信号也连接至该多选二电路，该多选二电路输出的两个电压信号分别连接至所述比较器的正负输入端，该比较器输出端连接至 PUF 数据信号。

[0021] 图 2 为上述 PUF 单元的示意图，其包括电阻分压单元 1 和电阻分压单元 2，该电阻分压单元 1 和电阻分压单元 2 的电路相同。电阻分压单元 1 产生并输出 PUF 电压 1，电阻分压单元 2 产生并输出 PUF 电压 2。使能信号连接至电阻分压单元 1 和电阻分压单元 2，控制该两个电阻分压单元的打开或关闭。

[0022] 图 3 为上述电阻分压单元 1 或电阻分压单元 2 的示意图，其包括电阻 1、电阻 2、开关 1 和开关 2。电阻 1 与电阻 2 串联连接，该电阻 1 与电阻 2 连接端连接至开关 2 的一端，开关 2 的另一端连接至 PUF 电压信号，电阻 1 未与电阻 2 连接的另一端连接至开关 1 的一端，开关 1 的另一端连接至电源，电阻 2 未与电阻 1 连接的另一端连接至地。使能信号连接至开关 1 和开关 2，控制上述两个开关的导通和关断。当使能信号有效时，开关 1 和开关 2 导通，电阻分压单元 1 或电阻分压单元 2 打开，电阻 1 通过开关 1 接通电源，电阻 1 和电阻 2 通过分压产生一个有效的 PUF 电压信号，该 PUF 电压信号由集成电路制造工艺偏差决定，该 PUF 电压信号通过开关 2 连接输出至对应的重构单元。开关 1 和开关 2 的导通电阻远小于电阻 1 和电阻 2 的阻值。使能信号无效时，开关 1 和开关 2 关断，电阻分压单元 1 或电阻分压单元 2 关闭，输出的 PUF 电压无效。电阻 1 和电阻 2 采用相同的类型、尺寸和版图设计，电阻 1 和电阻 2 的类型为多晶硅电阻、阱电阻或热电阻等。电阻分压单元产生的 PUF 电压的大小由电阻 1 和电阻 2 的阻值决定，而电阻 1 和电阻 2 的阻值大小由电阻的工艺偏差决定。因此，上述 PUF 电压的大小由电阻的工艺偏差决定，具有随机性，不可预测且不可复制，或高于理想值，或低于理想值，与理想值存在一定的偏差，且不同电阻分压单元产生的 PUF 电压之间也存在一定的偏差。

[0023] 图 4 为上述参考电压电路的示意图，其包括电阻 3、电阻 4 和开关 3。电阻 3 与电阻 4 串联连接，该电阻 3 和电阻 4 连接端连接至输出的参考电压信号，电阻 3 未与电阻 4 连接的另一端连接至开关 3 的一端，开关 3 的另一端连接至电源。电阻 4 未与电阻 3 连接的另一端连接至地。使能信号连接至开关 3，控制开关 3 的导通和关断。当使能信号有效时，开关 3 导通，电阻 3 通过开关 3 接通电源，电阻 3 和电阻 4 通过分压产生一个有效的参考电压信号并连接至输出。开关 3 的导通电阻远小于电阻 3 和电阻 4 的阻值。使能信号无效时，开关 3 关断，输出的参考电压无效。电阻 3 和电阻 4 在电路实现上采用相同的类型和尺寸，且采用较大的宽度和长度尺寸，版图设计上进行严格匹配，如采用共质心等版图匹配技术，尽量减小上述两个电阻在制造过程中产生的工艺偏差，通过分压产生一个较为精确的参考电压，该参考电压的大小近似等于上述电阻分压单元产生的 PUF 电压的理想值。

[0024] 图 5 为所述重构单元的示意图，其包括一个三选二电路和一个比较器。该三选二电路接收所述 PUF 单元输出的 PUF 电压 1、PUF 电压 2 以及参考电压电路输出的参考电压，作为三个输入信号。重构信号连接至三选二电路，控制三选二电路从三个输入信号中选择对应的两个电压信号，分别连接至比较器的正负输入端。比较器对三选二电路输出的两个电压信号进行比较，若正输入端的电压信号高于负输入端，则比较器输出数据 1，反之，则输出数据 0，重构单元按照上述方法产生 1 位 PUF 数据。三选二电路从三个输入信号中选出两个信号进行比较共有三种有效选择：参考电压和 PUF 电压 1、参考电压和 PUF 电压 2、PUF 电压 1 和 PUF 电压 2。因此，重构单元在不同的重构信号的控制下，可从一个 PUF 单元中提

取 3 个不同的 PUF 数据，重构阵列可从 PUF 阵列提取 3 组不同的 PUF 数据，通过改变重构信号，可实现对 PUF 数据的重构。由于 PUF 单元输出的 PUF 电压 1、PUF 电压 2 以及参考电压的相对大小由电阻制造过程中产生的随机工艺偏差决定，重构单元提取的 PUF 数据也由上述工艺偏差决定，具有唯一性，不可预测，且不可复制和篡改。

[0025] 下面对 PUF 数据提取和重构的过程进行说明：

（1）外部控制电路需要使用 PUF 数据，开始提取 PUF 数据，发出有效的使能信号和重构信号。若需要重构 PUF 数据，则使用与上次提取不同的重构信号，若不需要重构 PUF 数据，则使用相同的重构信号。

[0026] （2）PUF 阵列接收到使能信号，打开其内部的每个 PUF 单元。PUF 单元在使能信号的控制下，打开其内部的电阻分压单元 1 和电阻分压单元 2。每个电阻分压单元在使能信号的控制下，内部的开关 1 和开关 2 导通，电阻 1 接通电源，电阻 1 和电阻 2 通过分压产生一个 PUF 电压信号，并通过开关 2 连接至输出。PUF 单元通过电阻分压单元 1 和电阻分压单元 2 分别产生 PUF 电压 1 和 PUF 电压 2，连接到重构阵列中对应的重构单元。上述两个 PUF 电压信号的大小由电阻的工艺偏差决定，与理想值之间存在一定的偏差。

[0027] （3）参考电压电路接收到使能信号，内部的开关 3 导通，电阻 3 接通电源，电阻 3 和电阻 4 通过电阻分压产生一个参考电压信号，连接到重构阵列中的每个重构单元。上述参考电压近似等于 PUF 单元产生的 PUF 电压信号的理想值。

[0028] （4）重构阵列中每个重构单元接收到重构信号。重构单元中三选二电路根据重构信号，从 PUF 电压 1、PUF 电压 2 和参考电压三个输入信号中选择对应的两个电压信号，并输出到比较器的正负输入端。例如，若外部控制电路发出第一重构信号，三选二电路选择参考电压和 PUF 电压 1 输出。发出第二重构信号，三选二电路选择参考电压和 PUF 电压 2 输出。发出第三重构信号，三选二电路选择 PUF 电压 1 和 PUF 电压 2 输出。比较器对输入的两个电压信号进行比较，产生 1 位 PUF 数据。若比较器正输入端的电压信号高于负输入端，则比较器输出 PUF 数据 1，反之，则输出 PUF 数据 0。重构阵列对 PUF 阵列中每个 PUF 单元进行提取，产生与当前重构信号对应的一组 PUF 数据。

[0029] （5）外部控制电路读取重构阵列产生的所有 PUF 数据，完成 PUF 数据的提取后，外部控制电路关闭使能信号，电路关断，PUF 数据消失。

[0030] 若外部控制电路需要提取不同的 PUF 数据，通过在步骤（1）中设置不同的重构信号，然后重复步骤（2）、（3）、（4）、（5），则可提取出与当前设置的重构信号对应的一组 PUF 数据，实现对 PUF 数据的重构。

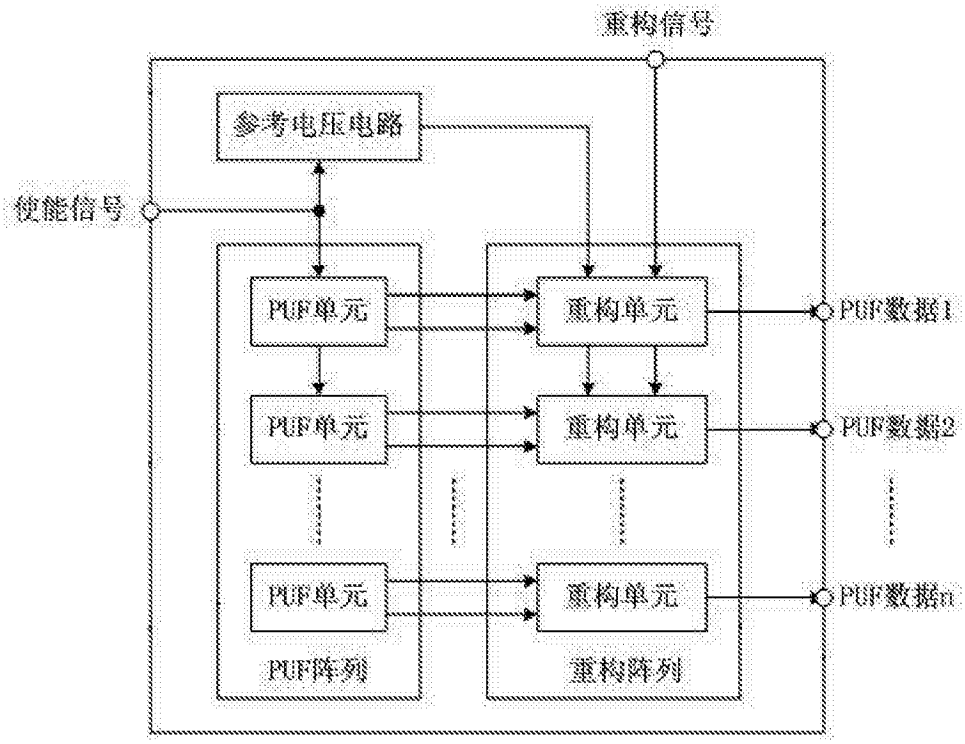

重构信号
参考电压电路
使能信号
PUF单元
PUF单元
PUF单元
重构单元
重构单元
重构单元
PUF数据1
PUF数据2
PUF数据n
PUF阵列
重构阵列

图 1

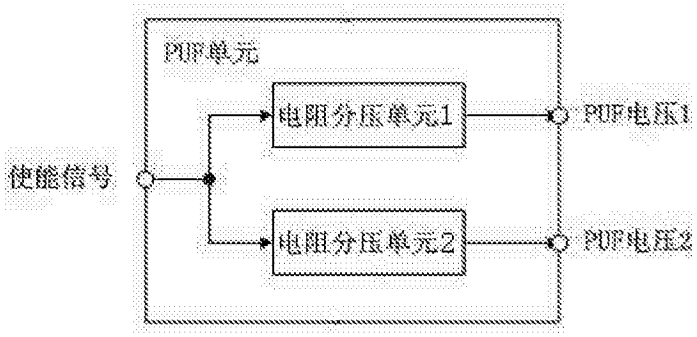

PUF单元
电阻分压单元1
电阻分压单元2
使能信号
PUF电压1
PUF电压2

图 2

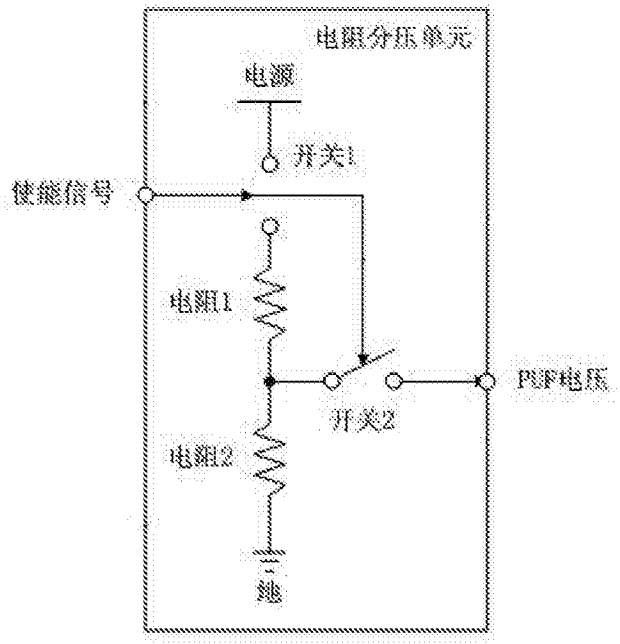

电阻分压单元
电源
开关1
使能信号
电阻1
开关2
PUF电压
电阻2
地

图 3

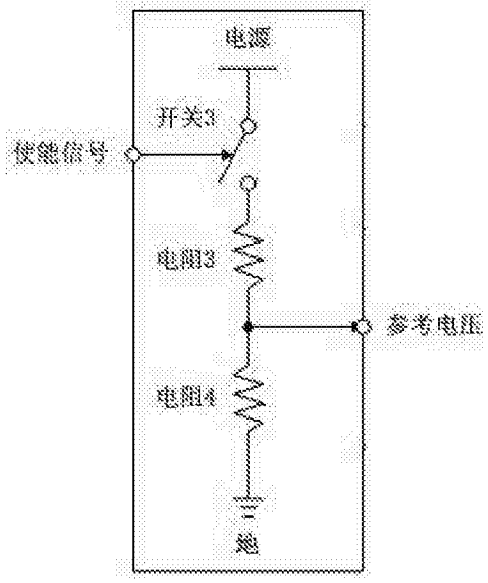

电源
开关3
使能信号
电阻3
参考电压
电阻4
地

图 4

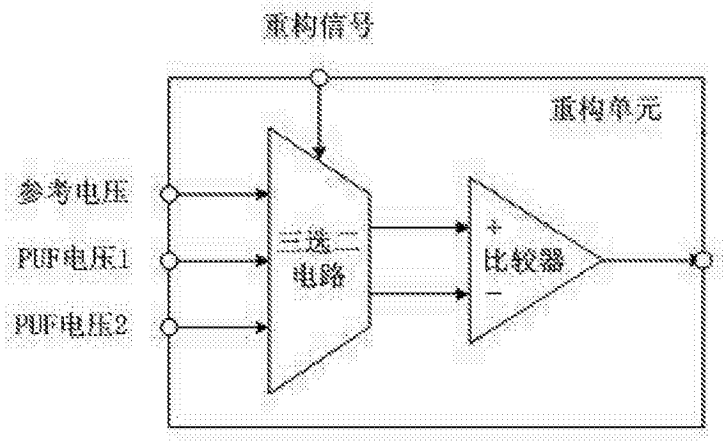

重构信号
重构单元
参考电压
PUF电压1
PUF电压2
三选二电路
+
比较器
-

图 5