东南大学专利申请信息页

申请专利名称：一种可高效提取的改进型 BRPUF 电路及 FPGA IP 核部署方案

申请专利类型：　国家发明专利

申请人：　东南大学

发明人:李冰(101003988)、葛文杰(220226080)、宋宏展(220226329)、李宜、赵蕃菁（220226054）、姜子威（220225822）、何煌（220226006）

发明人所在学院：　无锡分校

第一发明人身份证号：　320102196810061631

第一发明人座机：_____ 手机：　15365045432

E-mail: bernie_seu@seu.edu.cn

联系人座机：_____ 手机：**18362405376**

E-mail: 220226080@seu.edu.cn

备注：申请人地址：无锡市新吴区菱湖大道 99 号 邮编：214135

（若学生是第一发明人，必须要有老师的联系电话和邮箱）

若有共同申请单位，则需提供以下信息：

共同申请人地址：_____

共同申请人邮编：_____

共同申请人法人代码：_____

专利代理委托书（向代理人索要或在专利局网站下载）

以下是提交的专利申请材料

著录信息

发明名称：一种可高效提取的改进型 BRPUF 电路及 FPGA IP 核部署方案

发明人：李冰、葛文杰、宋宏展 、李宜、赵蕃菁、姜子威、何煌
第一发明人身份证号： 320102196810061631
申请人： 东南大学
申请人地址：无锡市滨湖区状元路 5 号 邮编：214082

说明书摘要

本发明提出了一种 BRPUF 电路的改进型结构和其在 FPGA 上的部署方案，提出将标准 BRPUF 电路的长反相器环截成多个短反相器环，每个反相器环由四个 SRAM 单元组成，并保留了标准 BRPUF 的路径选择功能，从而减小振荡时间。并且该改进型 BRPUF 电路理论上能够产生2^{64}个不同响应，因此该结构 BRPUF 也可应用与设备认证，实验结果表明改进型 BRPUF 电路的振荡时间小于 18ns，且其随机性、可靠性和唯一性分别达到了 98.88%，98.67%，31.8%，并且该改进型 BRPUF 电路以纯软核形式提供，能够依靠 EDA 工具的自动布线得到电路，不需要任何调整单元，且能够在多数开发平台上综合，其具有较高的灵活性。

权利要求书

1．一种可高效提取的改进型 BRPUF 电路及 FPGA IP 核部署方案，其特征在于：

所述改进型 BRPUF 电路结构提出将 SRAM 单元与 BRPUF 结构相结合，改进后的电路中反相器环由 4 个 SRAM PUF 单元组成，并保留了标准 BRPUF 的路径选择功能。

所述 FPGA IP 核部署方案为一 AXI 接口协议标准的封装 IP 核，其具有通信接口部分、加速器部分、PUF 电路部分、寄存器组部分；其中，

通信接口为 AIX4-Lite 接口协议标准，实现 IP 核与处理器的互连，提供处理器与 IP 核之间的交互通路；处理器可通过该通信接口来完成对本 IP 核的上电、调电时间配置，工作基频率的配置，编解码数据、激励数据的写入，辅助数据、响应数据、真随机数数据的读出；

加速器部分实现对 HASH 算法的硬件加速、ReedMuller 与 Repetition 算法的加速，其中 HASH 加速器通过写入的编码数据生成 HASH 摘要，ReedMuller 与 Repetition 用于辅助数据产生，其二级级联输出将直接与 PUF 响应异或得到辅助数据；

PUF 电路为一 128bit 激励，64bit 响应的改进型 BRPUF 电路，能够提供 64bit 的可信根；

寄存器组用于 CPU 与本 IP 核的交互，可分为配置寄存器与数据寄存器，CPU 通过读写配置寄存器完成对 PUF 电路上电、掉电时间的配置，IP 核工作频率的配置，通过读写数据寄存器可完成编解码数据、激励数据的写入，辅助数据、响应数据、真随机数数据的读出；

2．根据权利要求 1 所述的一种可高效提取的改进型 BRPUF 电路及 FPGA IP 核部署方案，其特征在于，所述改进型 BRPUF 设计结合了 SRAM 单元和标准型 BRPUF 电路的路径选择功能，其具有 128bit 的激励输入，对应产生 64bit 的 PUF 响应，其激励输入至产生响应的时间小于 18ns；

3．根据权利要求 1 所述的一种可高效提取的改进型 BRPUF 电路及 FPGA IP 核部署方案，其特征在于，ReedMuller 码所采取的参数为 K=3，R=1，Repetition 码所采取的参数为 N=8，M=1，由 ReedMuller 码与 Repetition 码共同实现 PUF 响应中噪声的纠错。其中在编码阶段 128bit 消息首先通过 ReedMuller 编码器再通过 Repetition 编码器产生 2048bit 数据，然后与 BRPUF 响应异或生成辅助数据，存储

至 IP 核内 RAM 中；

4．根据权利要求 1 所述的一种可高效提取的改进型 BRPUF 电路及 FPGA IP 核部署方案，其特征在于，所述 HASH 算法采用了 SHA-1 算法，其产生 160bit 定长摘要；

5．根据权利要求 1 所述的一种可高效提取的改进型 BRPUF 电路及 FPGA IP 核部署方案，其特征在于，用于提取改进型 BRPUF 响应时，步骤如下：

步骤（1）、复位并初始化本 IP 核，通过置位 CTL0 寄存器的第 3 比特位解锁分频寄存器，并通过配置分频寄存器 DIV0 至 DIV1 配置 IP 核工作基频率，然后复位 CTL0 寄存器的第 3 比特位上锁分频寄存器，然后置位 CTL0 第 0 比特位进行复位，最后复位 CTL0 第 0 比特位并置位第二比特位使能 IP 核；

步骤（2）、配置 CINx（x=0，1，2，3）寄存器向 IP 核写入激励，然后置位 CTL0 寄存器第 3 比特位开始一次 PUF 事件，查询 IFG0 寄存器第 2 比特位是否置位，若置位则读取 RBUFx（x=0，1）寄存器得到 PUF 响应；

6．根据权利要求 5 所述的一种可高效提取的改进型 BRPUF 电路及 FPGA IP 核部署方案，其特征在于，在此基础上进行辅助数据及信息摘要的产生，步骤如下：

步骤 A、复位 CTL0 第 4 比特位将 IP 核配置为编码模式，进行一次权利要求 5 中的一次 BRPUF 响应过程；

步骤 B、配置 EMSGx（x=0，1，2，3）向 IP 核写入 128bit 编码数据；

步骤 C、置位 CTL0 寄存器第 4 比特位开始一次 PUF 事件，查询 IFG0 寄存器第 2 比特位是否置位，若置位则读取辅助数据核信息摘要；

步骤 D、配置 ASSAR 寄存器，向 IP 核写入当前读取的辅助数据 RAM 地址，读取 ASSISx（x=0,1）读取 64 位辅助数据；

步骤 E、重复步骤 D，向 ASSAR 写入地址 0 至 32，直至读满 2048bit 辅助数据；

步骤 F、读取 DIGx（x=0，1，2，3，4）寄存器，读出信息摘要；

7．根据权利要求 5 所述的一种可高效提取的改进型 BRPUF 电路及 FPGA IP 核部署方案，其特征在于，在此基础上进行辅助数据解码及信息摘要的重建，步骤如下：

步骤 i、置位 CTL0 第 4 比特位将 IP 核配置为解码模式，进行一次权利要求 5 中的一次 BRPUF 响应过程；

步骤 ii、将权力要求 6 中得到的辅助数据写入 IP 核，通过分别向 EMSGAR 寄存器写入 0 至 32，确定辅助数据暂存寄存器的地址，然后向 ECODEx（x=0，1）寄存器写入辅助数据，直至写满 2048bit；

步骤 iii、将权力要求 6 中得到的辅助数据写入 IP 核，通过分别向 EMSGAR 寄存器写入 0 至 32，确定辅助数据暂存寄存器的地址，然后向 ECODEx（x=0，1）寄存器写入辅助数据，直至写满 2048bit；

步骤 iiii、置位 CTL0 寄存器第 3 比特位开始一次 PUF 事件，查询 IFG0 寄存器第 2 比特位是否置位，若置位则读取 DIGx（x=0，1，2，3，4）寄存器，读出重建后的信息摘要；

8．根据权利要求 1 所述的一种可高效提取的改进型 BRPUF 电路及 FPGA IP 核部署方案，其特征在于，作为本发明中对标准型 BRPUF 的结构优化，该改进型 BRPUF 结构能够大幅缩减其响应的提取时间，对于需要快速认证的系统，能够缩短响应提取过程需要的时间，提高改进型 BRPUF 响应的提取效率。

9．根据权利要求 1 所述的一种可高效提取的改进型 BRPUF 电路及 FPGA IP 核部署方案，其特征在于，作为本发明中对标准型 BRPUF 的结构优化，改进型 BRPUF 保留了 BRPUF 的路径选择功能，并采用了 SRAM 的结构单元，在 FPGA 上的部署过程中，SRAM 结构单元使得部署过程完全依靠 EDA 工具的自动布局布线完成，BRPUF 路径选择功能保证了改进型 BRPUF 的足够多的激励响应对，因此该改进型 BRPUF 电路完全可以应用于设备认证、信息加密、密钥提取等场合。

说明书

一种可高效提取的改进型 BRPUF 电路及 FPGA IP 核部署方案

技术领域

本专利涉及数据安全、网络信息安全领域，可应用于需要数据加密、设备认证的应用场景。

背景技术

随着对信息安全的重视，对安全芯片的大规模使用，人们对安全芯片的可靠性也提出了更高的要求。传统的安全防护方法是将密钥存储在存储器中，这种防护措施不能提供绝对安全的保护，最大的脆弱点就密钥的存储易受到攻击。

物理不可克隆函数（Physically Unclonable Functions, PUFs）的使用可解决上述问题，利用映射关系避免密钥的直接存储。PUFs 是一种内嵌于物理实体的噪声函数，其利用 IC 不可控的随机工艺制造差异（如沟道长度、沟道宽度、阈值电压、氧化层厚度以及金属线的形状等）实现输入到输出的映射。这种映射关系具有随机性和唯一性，类似于人的指纹，因此 PUFs 也被称为芯片指纹。PUFs 根据实现原理不同可以分为存储类 PUFs 和延时类 PUFs。存储类 PUFs 包括 SRAM PUFs、DRAM PUFs、Flash PUFs 和 Memristor PUFs 等，而延时类 PUFs 包括 APUFs 和 Ring Oscillator PUFs。

目前在 PUF 技术中能够成熟商用的 PUF 为 SRAM PUF，但 SRAM PUF 为一种弱 PUF，常用于密钥生成，能够在设备认证中成熟商用的强 PUF 电路较少。且在嵌入式系统或 SOC 中实现 SRAM PUF 需要外接一块 SRAM 芯片，一方面会消耗很多 IO 资源，另一方面外接的 SRAM 芯片只能用于 PUF 响应的产生，不能再用于数据存储，浪费资源。

除了 SRAM 以外，类似 RO PUF、Arbiter PUF、标准型 BR PUF 虽为强 PUF，但在实现过程中的布局布线产生的路径延迟要求较高，往往由于设计者无法控制路径延迟导致最终的 PUF 响应随机性、稳定性较差。

在 FPGA 中，上述的 RO PUF、Arbiter PUF、标准型 BR PUF 存在的路径延迟问题可以通过增加多级调整单元来解决，其结构上的对称性也可通过直接例化底层 LUT 资源实现，但这种方式实现的 PUF 往往可移植性较差，不同平台不同类型的 FPGA 可能面临 LUT 资源不通用的问题，并且在不同 FPGA 上部署，其需要的调整单元个数也不同，以上这些问题需要设计者不停地进行上板测试得到最优部署方案，耗费时间和精力。

如果在 FPGA 上使用 SRAM，同样需要外接 SRAM 器件，耗费大量 IO 资源，并非部署 PUF 的最优方案。

发明内容

标准 Bistable Ring PUFs（BRPUF）具有过长的振荡时间的限制（128 位标准 BRPUFs 的平均振荡时间为 23.08us），这限制了其在秘钥生成场景的应用。本发明针对现有 PUF 存在的问题，提出将标准 BRPUF 的长反相器环截成多个短反相器环，每个反相器环由四个 SRAM 单元组成，并保留了标准 BRPUF 的路径选择功能，从而减小振荡时间。并且该改进型 BRPUF 理论上能够产生 2^{64} 个不同响应，因此该结构 PUF 也可应用与设备认证，实验结果表明改进型 BRPUF 的振荡时间小于 18ns，且其随机性、可靠性和唯一性均有明显提升，并且该改进型 BRPUF 可以纯软核形式提供，能够依靠 EDA 工具的自动布线得到电路，不需要任何调整单元，其具有较高的灵活性。

针对上述的改进型 BRPUF，本发明提出一种集成了该改进型 BRPUF 的加解密 IP 核，该 IP 核以软核和固核形式提供，软核可以部署于任何 FPGA 平台，固核可以在 Vivado 平台上实现增量编译，利于产品的快速更新迭代；

本发明采用的技术方案如下：

根据本发明提出的一种可高效提取的改进型 BRPUF 电路及 FPGA IP 核部署方案，其特征在于：该进型 BRPUF 电路结构提出将 SRAM 单元与 BRPUF 结构相结合，改进后的电路中反相器环由 4 个 SRAM PUF 单元组成，并保留了标准 BRPUF 的路径选择功能。

根据本发明提出的一种可高效提取的改进型 BRPUF 电路及 FPGA IP 核部署方案，以改进型 BRPUF 为基础的加解密 IP 核具有通信接口部分、加速器部分、PUF 电路部分、寄存器组部分；其中，

通信接口为 AIX4-Lite 接口协议标准，实现 IP 核与处理器的互连，提供处理器与 IP 核之间的交互通路；处理器可通过该通信接口来完成对本 IP 核的上电、调电时间配置，工作基频率的配置，编解码数据、激励数据的写入，辅助数据、响应数据、真随机数数据的读出；

加速器部分实现对 HASH 算法的硬件加速、ReedMuller 与 Repetition 算法的加速，其中 HASH 加速器通过写入的编码数据生成 HASH 摘要，ReedMuller 与 Repetition 用于辅助数据产生，其二级级联输出将直接与 PUF 响应异或得到辅助数

据；

PUF 电路为一 128bit 激励，64bit 响应的改进型 BRPUF 电路，能够提供 64bit 的可信根；

寄存器组用于 CPU 与本 IP 核的交互，可分为配置寄存器与数据寄存器，CPU 通过读写配置寄存器完成对 PUF 电路上电、掉电时间的配置，IP 核工作频率的配置，通过读写数据寄存器可完成编解码数据、激励数据的写入，辅助数据、响应数据、真随机数数据的读出；

改进型 BRPUF 设计结合了 SRAM 单元和标准型 BRPUF 电路的路径选择功能，其具有 128bit 的激励输入，对应产生 64bit 的 PUF 响应，其激励输入至产生响应的时间小于 18ns；

ReedMuller 码所采取的参数为 K=3，R=1，Repetition 码所采取的参数为 N=8，M=1，由 ReedMuller 码与 Repetition 码共同实现 PUF 响应中噪声的纠错。其中在编码阶段 128bit 消息首先通过 ReedMuller 编码器再通过 Repetition 编码器产生 2048bit 数据，然后与 BRPUF 响应异或生成辅助数据，存储至 IP 核内 RAM 中；

HASH 算法采用了 SHA-1 算法，其产生 160bit 定长摘要；

用于提取改进型 BRPUF 响应时，步骤如下：

步骤（1）、复位并初始化本 IP 核，通过置位 CTL0 寄存器的第 3 比特位解锁分频寄存器，并通过配置分频寄存器 DIV0 至 DIV1 配置 IP 核工作基频率，然后复位 CTL0 寄存器的第 3 比特位上锁分频寄存器，然后置位 CTL0 第 0 比特位进行复位，最后复位 CTL0 第 0 比特位并置位第二比特位使能 IP 核；

步骤（2）、配置 CINx（x=0，1，2，3）寄存器向 IP 核写入激励，然后置位 CTL0 寄存器第 3 比特位开始一次 PUF 事件，查询 IFG0 寄存器第 2 比特位是否置位，若置位则读取 RBUFx（x=0，1）寄存器得到 PUF 响应；

在此基础上进行辅助数据及信息摘要的产生，步骤如下：

步骤 A、复位 CTL0 第 4 比特位将 IP 核配置为编码模式，进行一次步骤（1）至步骤（2）BRPUF 响应过程；

步骤 B、配置 EMSGx（x=0，1，2，3）向 IP 核写入 128bit 编码数据；

步骤 C、置位 CTL0 寄存器第 4 比特位开始一次 PUF 事件，查询 IFG0 寄存器第 2 比特位是否置位，若置位则读取辅助数据核信息摘要；

步骤 D、配置 ASSAR 寄存器，向 IP 核写入当前读取的辅助数据 RAM 地址，

读取 ASSISx（x=0,1）读取 64 位辅助数据；

步骤 E、重复步骤 D，向 ASSAR 写入地址 0 至 32，直至读满 2048bit 辅助数据；

步骤 F、读取 DIGx（x=0，1，2，3，4）寄存器，读出信息摘要；

在此基础上进行辅助数据解码及信息摘要的重建，步骤如下：

步骤 i、置位 CTL0 第 4 比特位将 IP 核配置为解码模式，进行一次步骤（1）至步骤（2）BRPUF 响应过程；

步骤 ii、将权力要求 6 中得到的辅助数据写入 IP 核，通过分别向 EMSGAR 寄存器写入 0 至 32，确定辅助数据暂存寄存器的地址，然后向 ECODEx（x=0，1）寄存器写入辅助数据，直至写满 2048bit；

步骤 iii、将步骤 E 中得到的辅助数据写入 IP 核，通过分别向 EMSGAR 寄存器写入 0 至 32，确定辅助数据暂存寄存器的地址，然后向 ECODEx（x=0，1）寄存器写入辅助数据，直至写满 2048bit；

步骤 iiii、置位 CTL0 寄存器第 3 比特位开始一次 PUF 事件，查询 IFG0 寄存器第 2 比特位是否置位，若置位则读取 DIGx（x=0，1，2，3，4）寄存器，读出重建后的信息摘要；

作为本发明中对标准型 BRPUF 的结构优化，该改进型 BRPUF 结构能够大幅缩减其响应的提取时间，对于需要快速认证的系统，能够缩短响应提取过程需要的时间，提高改进型 BRPUF 响应的提取效率。

作为本发明中对标准型 BRPUF 的结构优化，改进型 BRPUF 保留了 BRPUF 的路径选择功能，并采用了 SRAM 的结构单元，在 FPGA 部署过程中，SRAM 结构单元使得部署过程完全依靠 EDA 工具的自动布局布线完成，BRPUF 路径选择功能保证了改进型 BRPUF 的足够多的激励响应对，因此该改进型 BRPUF 电路完全可以应用于设备认证、信息加密、密钥提取等场合。

附图说明

图 1 为本发明提出的一种可高效提取的改进型 BRPUF 电路及 FPGA IP 核部署方案中改进型 BRPUF 电路中一个基本单元 BRPUF-cell 的结构。

图 2 为本发明提出的一种可高效提取的改进型 BRPUF 电路及 FPGA IP 核部署方案中改进型 BRPUF 电路中 BRPUF 电路设计。

图 3 为本发明提出的一种可高效提取的改进型 BRPUF 电路及 FPGA IP 核部署方案中基于改进型 BRPUF 的 IP 核设计。

图 4 为本发明提出的一种可高效提取的改进型 BRPUF 电路及 FPGA IP 核部署方案中基于改进型 BRPUF 的 IP 核中寄存器组的名称及类型，其中 offset 为偏移地址，Register 为寄存器名，Type 为寄存读写类型，可以是只读（R）、只写（W）、可读可写（RW），Reset 为该寄存器复位后的值，图中列出的寄存器默认位宽均为 32bit。

图 5 为本发明提出的一种可高效提取的改进型 BRPUF 电路及 FPGA IP 核部署方案中基于改进型 BRPUF 的 IP 核中关于改进型 BRPUF 的分数汉明距离测试，总采样比特数为 320000，其中 1bit 数为 171011,0bit 数为 148989，1bit 占比百分之 53.44%，0bit 占比 46.56%，采用的分数汉明计算公式为$H_{fra} = \frac{M}{N}$，其中 N 为采集的总响应比特数，M 为响应中为 0bit 的数量，其值越接近 50%说明 PUF 的随机性越好，0,1 分布越均匀。

图 6 为本发明提出的一种可高效提取的改进型 BRPUF 电路及 FPGA IP 核部署方案中基于改进型 BRPUF 的 IP 核中关于改进型 BRPUF 的分数汉明距离测试可视化图。

图 7 为本发明提出的一种可高效提取的改进型 BRPUF 电路及 FPGA IP 核部署方案中基于改进型 BRPUF 的 IP 核中关于改进型 BRPUF 的片内汉明距离测试可视化图，其平均片内汉明距离为 0.011209027777777776，计算片内汉明距离的公式为 $\mu_{intra} = \frac{2}{N(N-1)} \sum_{j=1}^{N-1} \sum_{k=j+1}^{N} \frac{HD(R_j, R_k)}{l} \cdot 100\%$，N 表示采集响应总数，$R_j$，$R_k$为总次数 N 中第 j 次与第 k 次生成响应，其值越小，PUF 稳定性越好。

具体实施方式

为了使本发明的目的、技术方案和优点更加清楚，下面将结合附图及具体实施例对本发明进行详细描述。

改进型 BRPUF 标准单元如图 1 所示，每个标准单元由 8 个或非门，2 个二选一数组选择器和 1 个异或门组成。其中 power 信号为控制信号，power 置 1 时电路输出为 0，power 置 0 时电路正常工作。c[i]为二选一数据选择器的输入信号，其来源为输入激励。out[i]为 BR 单元最终输出信号。

改进型 BR-PUFs 由 128 个 BR 单元组成阵列，如果资源允许，改进型 BRPUF

可以有更多的 BR 单元，其结构如图 2 所示。

每个 BR 单元需要 2bit 激励，所以图 2 所示的改进型 BR-PUFs 的激励长度为 128 比特，其激励空间是 2^{128}，根据 c[i]与 c[i+1]的取值不同，共有 4 种不同的环路组合。

如果直接读取所有 BR 单元的输出作为响应，全‘0’和全‘1’激励便可以遍历所有 BR 单元的所有取值，在知道输入激励的情况下，攻击者可以快速推断出响应。

为应对上述问题，改进型 BRPUF 相邻的两个环路的输出进行异或处理生成 1 位响应，从而其响应长度为 n/2 比特。对于此种响应生成方式，当施加全‘0’或全‘1’激励时，攻击者只能获取异或之后的值，这 n 个 BR 单元由 2n 种排列方式。因此攻击者不可能通过输出响应反向推断出 BR 单元的输出，从而无法预测改进型 BR-PUFs 的响应。

改进型 BRPUF 产生响应得到可信根的过程如下：

步骤 A1：将 power 信号置 1，模拟 SRAM 掉电。

步骤 A2：等待改进型 BRPUF 单元振荡结束。

步骤 A3：设置改进型 BRPUF 阵列的激励。

步骤 A4：将 power 信号置 0，模拟 SRAM 上电。

步骤 A5：等待改进型 BRPUF 单元振荡结束。

步骤 A6：读取改进型 BRPUF 阵列的响应。

使用如图 3 所示的 IP 核进行提取改进型 BRPUF 响应时，步骤如下：

步骤 B1：复位并初始化本 IP 核，通过置位 CTL0 寄存器的第 3 比特位解锁分频寄存器，并通过配置分频寄存器 DIV0 至 DIV1 配置 IP 核工作基频率，然后复位 CTL0 寄存器的第 3 比特位上锁分频寄存器，然后置位 CTL0 第 0 比特位进行复位，最后复位 CTL0 第 0 比特位并置位第二比特位使能 IP 核；

步骤 B2:：配置 CINx（x=0，1，2，3）寄存器向 IP 核写入激励，然后置位 CTL0 寄存器第 3 比特位开始一次 PUF 事件，查询 IFG0 寄存器第 2 比特位是否置位，若置位则读取 RBUFx（x=0，1）寄存器得到 PUF 响应；

使用如图 3 所示的 IP 核进行辅助数据及信息摘要的产生，步骤如下：

步骤 C1：复位 CTL0 第 4 比特位将 IP 核配置为编码模式，按照步骤 B1 至步骤 B2 进行一次 BRPUF 响应过程；

步骤 C2：配置 EMSGx（x=0，1，2，3）向 IP 核写入 128bit 编码数据。

步骤 C3：置位 CTL0 寄存器第 4 比特位开始一次 PUF 事件，查询 IFG0 寄存器第 2 比特位是否置位，若置位则读取辅助数据核信息摘要。

步骤 C4：配置 ASSAR 寄存器，向 IP 核写入当前读取的辅助数据 RAM 地址，读取 ASSISx（x=0,1）读取 64 位辅助数据。

步骤 C5：重复步骤 D，向 ASSAR 写入地址 0 至 32，直至读满 2048bit 辅助数据。

步骤 C6：读取 DIGx（x=0，1，2，3，4）寄存器，读出信息摘要。

使用如图 3 所示的 IP 核进行辅助数据解码及信息摘要的重建，步骤如下：

步骤 D1：置位 CTL0 第 4 比特位将 IP 核配置为解码模式，按照步骤 B1 至步骤 B2 进行一次 BRPUF 响应过程；

步骤 D2：将权力要求 6 中得到的辅助数据写入 IP 核，通过分别向 EMSGAR 寄存器写入 0 至 32，确定辅助数据暂存寄存器的地址，然后向 ECODEx（x=0，1）寄存器写入辅助数据，直至写满 2048bit；

步骤 D3：将权力要求 6 中得到的辅助数据写入 IP 核，通过分别向 EMSGAR 寄存器写入 0 至 32，确定辅助数据暂存寄存器的地址，然后向 ECODEx（x=0，1）寄存器写入辅助数据，直至写满 2048bit；

步骤 D4：置位 CTL0 寄存器第 3 比特位开始一次 PUF 事件，查询 IFG0 寄存器第 2 比特位是否置位，若置位则读取 DIGx（x=0，1，2，3，4）寄存器，读出重建后的信息摘要；

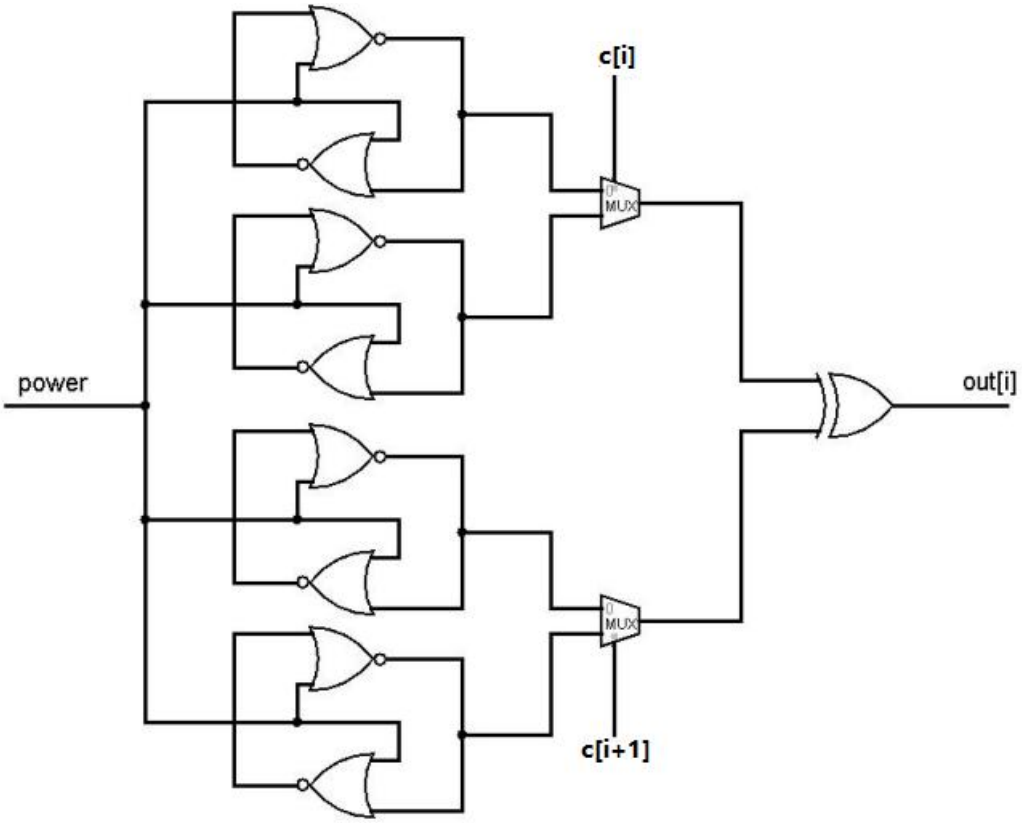
c[i]
power
out[i]
MUX
MUX
c[i+1]

图 1

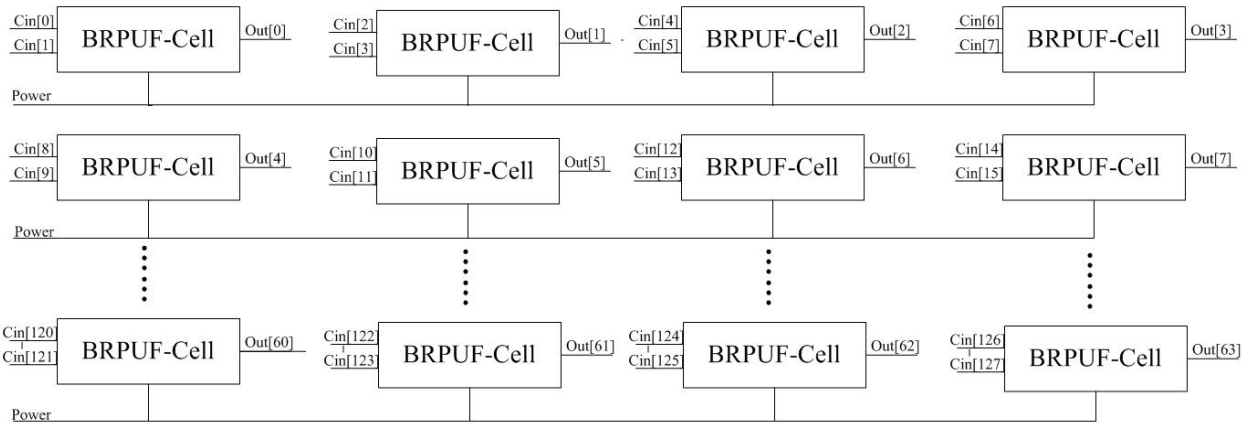
Cin[0]
Cin[1]
BRPUF-Cell
Out[0]
Cin[2]
Cin[3]
BRPUF-Cell
Out[1]
Cin[4]
Cin[5]
BRPUF-Cell
Out[2]
Cin[6]
Cin[7]
BRPUF-Cell
Out[3]
Power
Cin[8]
Cin[9]
BRPUF-Cell
Out[4]
Cin[10]
Cin[11]
BRPUF-Cell
Out[5]
Cin[12]
Cin[13]
BRPUF-Cell
Out[6]
Cin[14]
Cin[15]
BRPUF-Cell
Out[7]
Power
Cin[120]
Cin[121]
BRPUF-Cell
Out[60]
Cin[122]
Cin[123]
BRPUF-Cell
Out[61]
Cin[124]
Cin[125]
BRPUF-Cell
Out[62]
Cin[126]
Cin[127]
BRPUF-Cell
Out[63]
Power

图 2

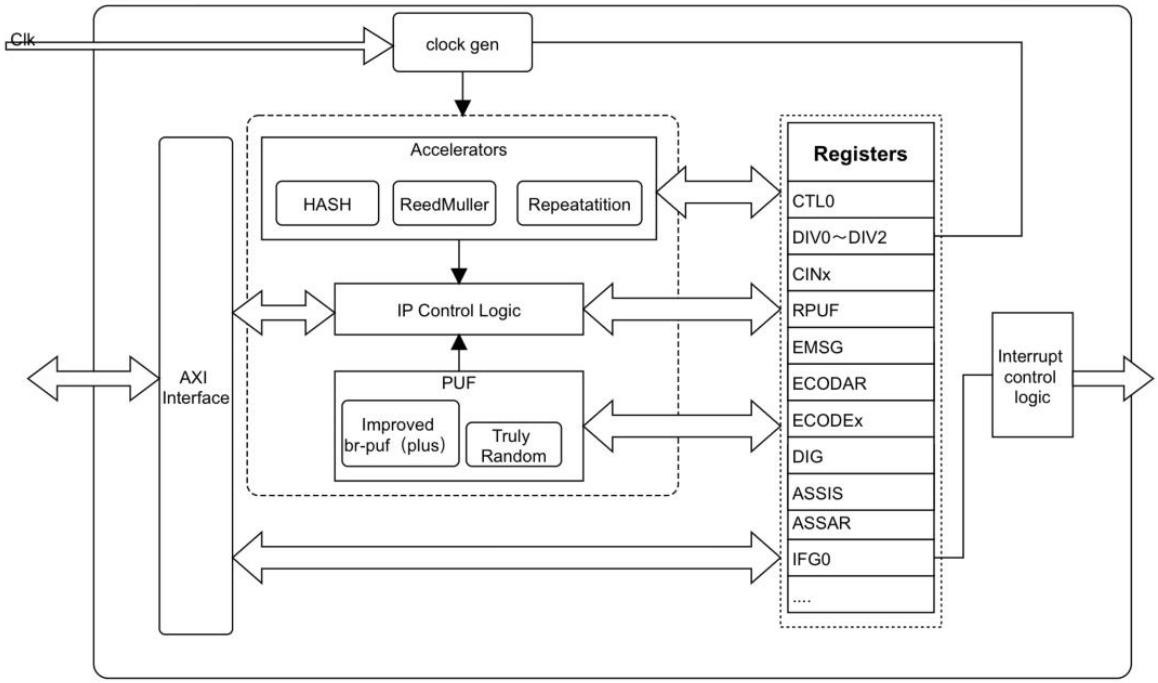

图 3

Offset	Register	Type	Reset
00	PUF_KEY_CTL0	RW	(0)h
04	PUF_KEY_DIV0	RW	(0)h
08	PUF_KEY_DIV1	RW	(0)h
0C	PUF_KEY_DIV2	RW	(0)h
10	PUF_KEY_CIN0	RW	(0)h
14	PUF_KEY_CIN1	RW	(0)h
18	PUF_KEY_CIN2	RW	(0)h
1C	PUF_KEY_CIN3	RW	(0)h
20	PUF_KEY_RBUF0	R	(0)h
24	PUF_KEY_RBUF1	R	(0)h
28	PUF_KEY_IFG0	R	(0)h
2C	PUF_KEY_EMSG0	RW	(0)h
30	PUF_KEY_EMSG1	RW	(0)h
34	PUF_KEY_EMSG2	RW	(0)h
38	PUF_KEY_EMSG3	RW	(0)h
3C	PUF_KEY_ECODAR	RW	(0)h
40	PUF_KEY_ECODE0	R	(0)h
44	PUF_KEY_ECODE1	R	(0)h
48	PUF_KEY_DIG0	R	(0)h
4C	PUF_KEY_DIG1	R	(0)h
50	PUF_KEY_DIG2	R	(0)h
54	PUF_KEY_DIG3	R	(0)h
58	PUF_KEY_DIG4	R	(0)h
5C	PUF_KEY_ASSIS0	RW	(0)h
60	PUF_KEY_ASSIS1	RW	(0)h
64	PUF_KEY_ASSAR	RW	(0)h

图 4

Total	1 bit	0 bit	1 bit rate	0bit rate
320000	171011	148989	53.44%	46.56%

图 5

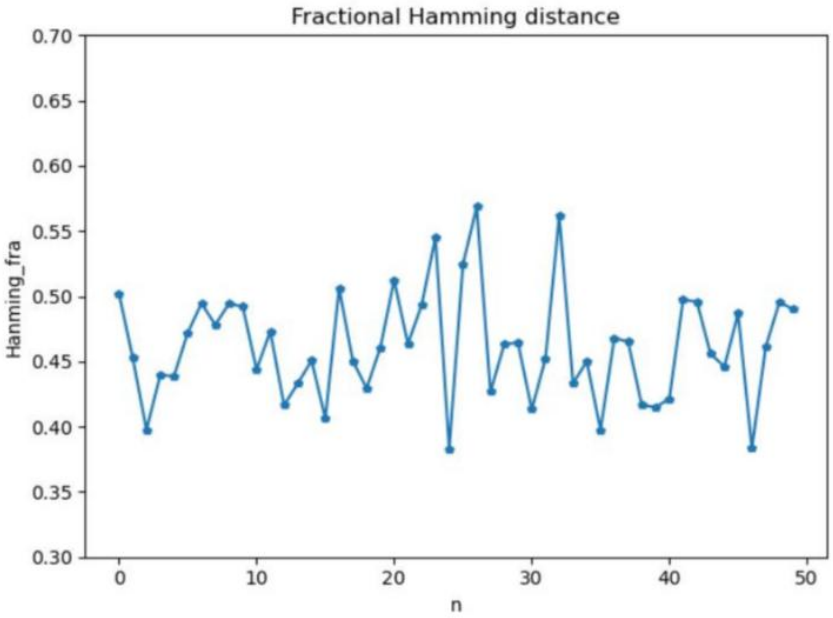
Fractional Hamming distance
Hanming_fra
n
0.70
0.65
0.60
0.55
0.50
0.45
0.40
0.35
0.30
0
10
20
30
40
50

图 6

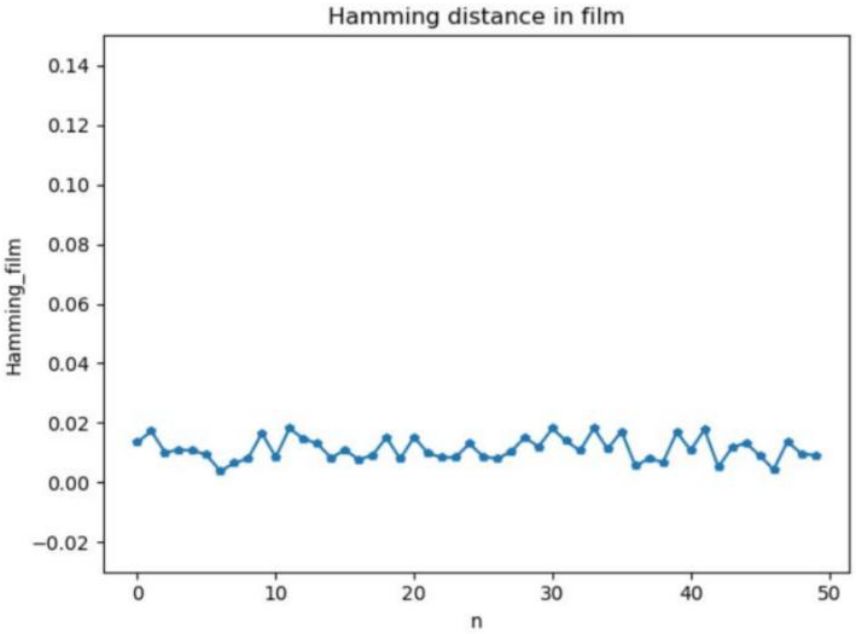
Hamming distance in film
Hamming_film
n
0.14
0.12
0.10
0.08
0.06
0.04
0.02
0.00
−0.02
0
10
20
30
40
50

图 7