前言

关于本记录

本记录用于记载 BR_PUF 电路的设计进程和改进情况，以及各种类型 BR_PUF 电路的测试情况。测试数据与激励响应对可以参考附录 I 中列出的激励响应对。还需注意的是，所有提到的关于改进型 BR_PUF 的工程均在 Zynq 平台实现与测试，在其他平台测试时需要转一下 IP，另建议使用 Micro Blaze 软核搭建测试 SOC，应用此软核则测试程序可以直接套用。

关键词声名

Key Word	Describe
HD_FIL	片内汉明距离
HD_SIL	片间汉明距离
HD_FRA	分数汉明距离
RW	读/写
R	读
W	写
()b	二进制
()h	十六进制

工程进展

Data	Work
2022.4.22	完成初步 BR_PUF 电路部署
2022.4.24	完成 BR_PUF 电路测试，稳定性差
2022.4.28	改进 BR_PUF 结构
2022.4.29	测试改进后的 BR_PUF，稳定性改善
2022.5.07	搭建加密 IP，测试性能，资源消耗过多
2022.5.12	增加随机数性算法测试
2022.5.19	进一步测试 IP 性能
2022.5.21	整理测试工程
None	None
None	None
None	None

目前遇到的问题

FPGA 开发板归还，无法进一步测试；

PUF 电路的片间汉明距离没有测试环境；

未知最终使用的 FPGA 型号，不知道 PUF 电路在该 FPGA 型号上的部署效果；

目　录

Data:2022.5.20
Recoder:Ge Wen Jie

改进型 BR_PUF 电路部署

针对陈剑师兄论文中提出的改进型 BR_PUF 进行在 FPGA 端的部署实践，在师兄的论文中通过手动例化 Slice 片中的 LUT 单元来实现整个 BR_PUF 的设计。但手动工程量较大，且不方便移植。于是我将精力集中在如何通过综合工具的自动布线功能，来实现 BR_PUF 电路的自动布局。

Topic **Page**

1.1 改进型 BR_PUF 电路

未改进前的 BR_PUF 电路如图 1.1 所示，为一链路环形结构，这也保证了其拥有丰富的激励响应对。首先其链路结构中，任意一级的激励信号 C 发生变化时，都将影响整体的输出 r。

但同时，这种环状结构也会对整体响应的稳定性带来影响，首先大量的单元互连导致震荡时间过长，其次若其中部分单元的阈值电压相近，也有可能导致整个电路始终处于震荡状态。

针对上面的问题，在陈剑师兄的论文中提及了一种改进型的 BR_PUF 电路，如图 1.2 所示。改进后的 BR_PUF 电路由多个 BR 单元组成(图 1.3)，每个单元都由 1 个二级反相器环路组成。其中，power 为掉电信号，模拟掉电过程。c 为激励信号，也可视为路径选择信号，及配置不同的反相器组成震荡环。Out 为输出。

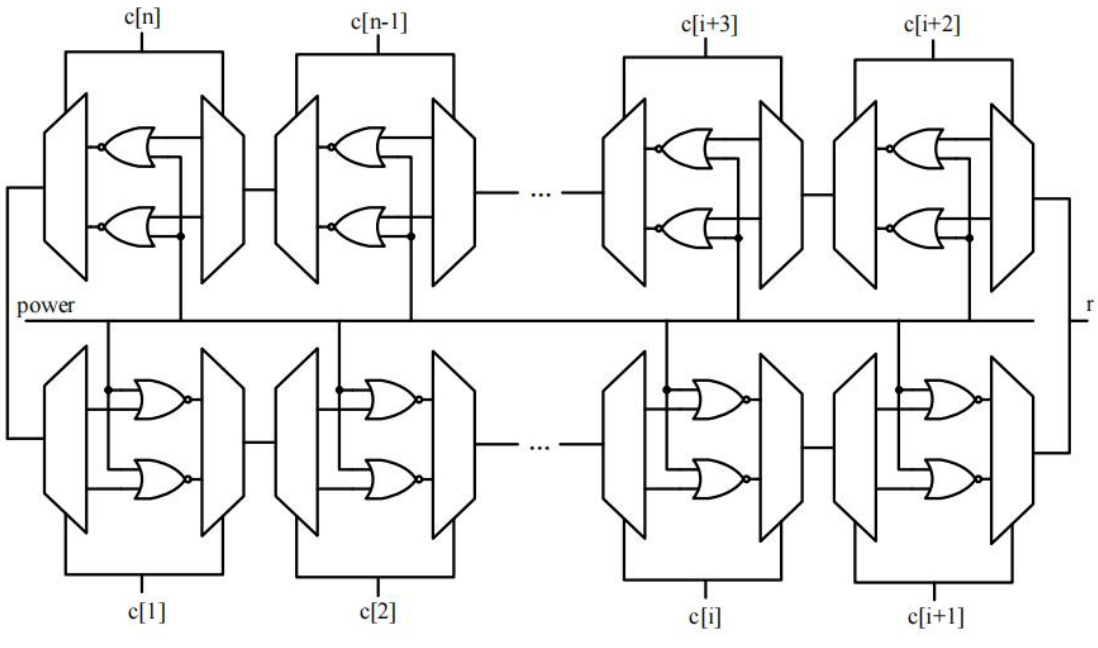


图 1.1 未改进 BR_PUF 电路

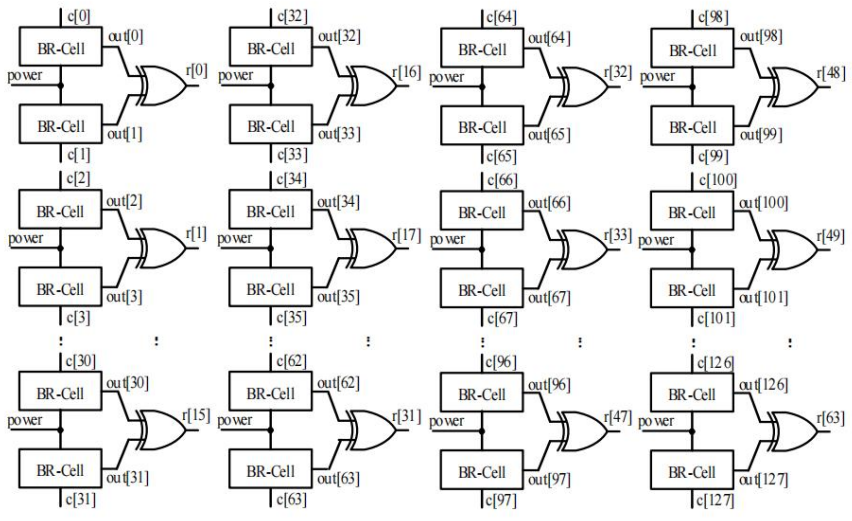


图 1.2 改进型 BR_PUF 电路

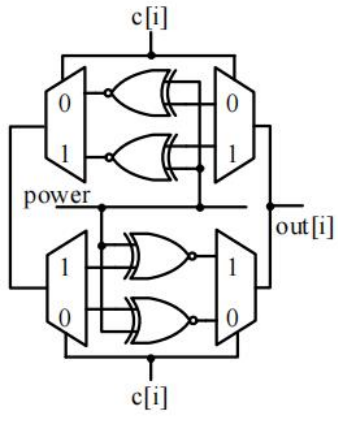


图 1.3 BR 单元

1.2 改进型 BR_PUF 电路实现

在很多论文中提到的实现方法是使用手动例化 FPGA 中 Slice 片中的 LUT 实现的，每片 Slice 片包含若干个 LUT 和若干个加减法电路、选择器资源。而上述改进型的 BR 单元单个来看资源占用很少，足够可以在 1 个 Slice 片中布局实现，这也就满足了电路良好的对称性，显然这种设计方法是最合适的。

但大量的 Slice 单元需要使用者对目标型号 FPGA 的内部结构足够熟悉，且移植性较差。如果 SOC 需要在不同型号的 FPGA 上实现，还需要重新布局，重新写 TCL 文件等等。所以我想能否通过软件自动布局布线的功能，来实现 BR_PUF 电路。

显然这是困难的，首先布局布线会经历综合布线等工作，最终产生 LUT 电路，此过程中由于工具中的各种规则，关键信号会被优化。这些问题还能够靠约束文件来解决，但自动布局产生的 LUT 电路还会带来一个不可控的问题，即电路对称性问题，这会严重影响 PUF 电路输出的稳定性。

幸运的是，改进后的 BR_PUF 电路中的 BR 单元(图 1.3)结构较为简单，所以我觉得只要按照规律严格地描述电路，由工具自动布局产生的 BR_PUF 电路性能应当可以直逼手动布局的 BR_PUF 电路。

1.2.1 电路结构部署

首先对陈剑师兄文章中提及的 BR_PUF 结构(图 1.2)进行建模。方案如图 1.4 所示。按照自顶向下的过程，首先对半个 BR_PUF 单元进行描述，然后通过例化两个这样的半个 BR_PUF 单元来完成整个 BR_PUF 单元的设计，再对这样的 BR_PUF 电路进行例化，形成 64bits 输出的 PUF 电路，最后对整个

电路进行 AXI 总线的封装得到测试 IP。

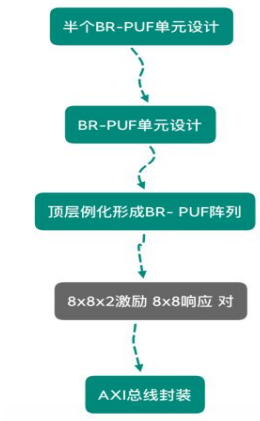


图 1.4 BR_PUF 电路实现方案

其中半个 BR_PUF 单元实现如图 1.5 所示。其中 LUT2 实现了激励信号 c 的路径选择功能。一级 BR_PUF 单元电路由四个这样的半个 BR_PUF 单元组成，如图 1.6 所示。震荡环路如图 1.6 中紫色线所示。

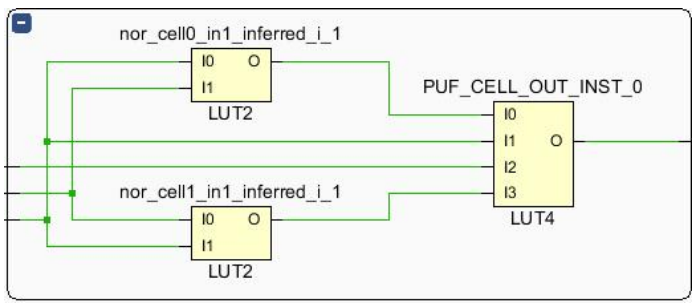


图 1.5 半个 BR_PUF LUT 实现方案

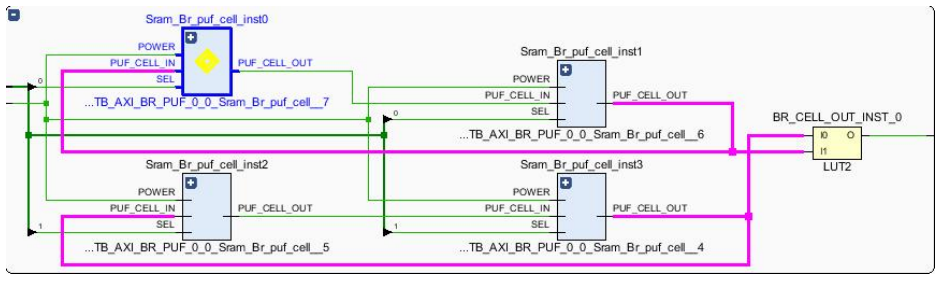


图 1.6 半个 BR_PUF LUT 实现方案

1.2.2 电路测试

对 1.2.1 小节中所提到的结构进行测试，测试过程如下，在 Zybo Z7 开发板上搭建一个 SOC，通过 AXI 总线给 BR_PUF 施加同一激励，读取响应，并观察其稳定性。最终得到的震荡环个数和 0,1 比特分布如表 1.1~1.2。

表 1.1 振荡比特分析

Total bits	Unsteady bits	ratio
64	20	31%

表 1.2 “0””1”分布

Total bits	0 bit	1 bit	0/1 distribution
3648	2462	1186	67.49%/32.51%

很显然，在 3648 采样中 0 和 1 个数相差悬殊。

1.2.3 原因分析

图 1.2.1 中的结构按理已经在电路结构上保持了对称性，因此可能是不对称的电气特性导致的振荡。我***改进***

大致想到两个可能原因。

1. 环路中存在的 MUX 单元使得阈值电压相接近。

2. 自动布局布线过程中，引入的路径延迟。

对于原因 1，在多篇文章中提到过阈值电压会导致电路始终处于振荡状态，在 1.2.1 的设计中，环路中引入的 LUT2 单元的阈值电压同样也要被纳入参考。

对于原因 2，可以参考亚稳态窗的定义。

对于时序电路中的亚稳态，如图 1.7。tsu 为建立时间，thd 为保持时间，很显然图中的采样信号采样并没有满足建立保持时间，这就导致了 OUT 端出现了一段时间的亚稳态（图中阴影）。但这种亚稳态并不会持续很久，一段时间后 OUT 也将趋于稳定的 0 或 1。

图 1.7 时序电路中的亚稳态

将 tsu 和 thd 合起来称为亚稳态窗口，这种亚稳态窗在异步时钟域数据传输中常常出现，但在时序逻辑电路中，处理的方法有很多，如使用两级同步器，异步 FIFO 等等。

将这种亚稳态窗口和 PUF 电路震荡环结合起来看，如图 1.8。换个角度看这样的电路，将 D1 看做采样信号，D0 看做输出，则构成了一级 T 触发器，将 D0 看做采样信号，D1 看做输出，构成了另一级 T 触发器，这两个触发器互连则出现了以下的结构，两级触发器的输出互为对方的驱动时钟。

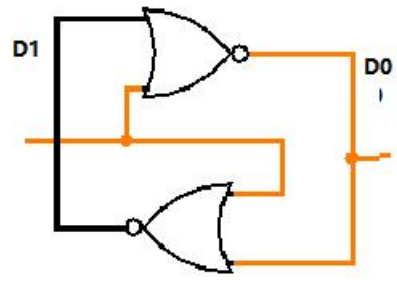


图 1.8 PUF 环路

更糟糕的是，由于自动布局布线的缺陷，D1 信号线与 D0 信号线长度长短不一，就会产生图 1.9 的情况。如果将 D0 视为 D1 的采样信号，则 D0 路径会引入一个路径延迟，同理 D1 也会引入路径延迟。这种布局布线进而进入了不同的亚稳态窗口，假设 D0 先度过了亚稳态最终到达稳态，此稳态若为 1，但此时 D1 还在亚稳态期间，若视为 1 则 D1 和 D0 相矛盾，此时电路将重新进入震荡状态。

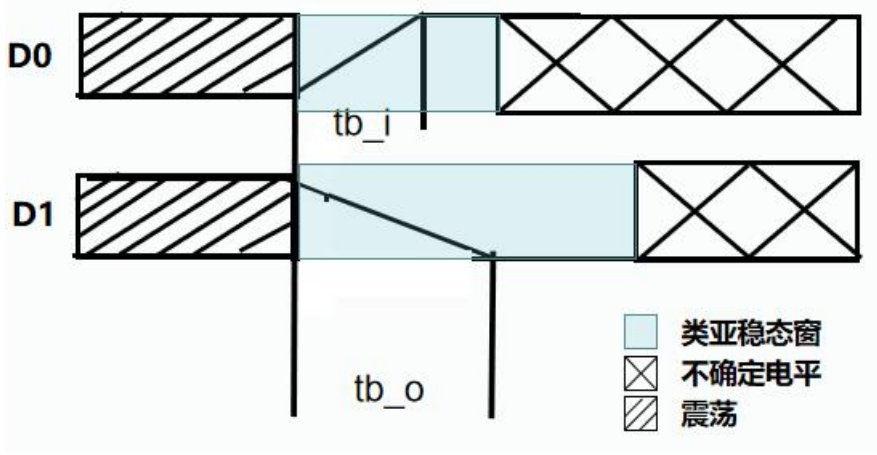


图 1.9 插入路径延迟后的情况

1.2.4 结构改进

很显然，1.1 节中提到的结构中的 MUX 模块无论在阈值电压还是路径上都会对电器上的对称性造成影响。因此将该结构继续进行改进，如图 1.10 所示。去掉了环路中插入的 MUX，激励信号用于控制选择哪个环路作为输出。其余结构不变，这就彻底去除了 MUX 模块带来的路径和阈值影响，且每个环路可由两个 LUT 实现，足够可以在一个 slice 片内实现，改善了路径上不对称的问题。

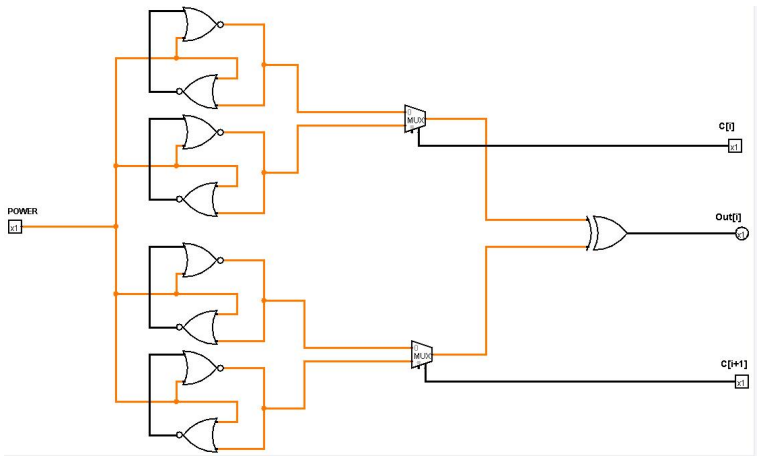


图 1.10 继续改进后的 BR_PUF 电路

1.2.5 改进后电路部署

改进后整个电路的 BD 设计如图 1.16 所示。整个电路的接口信号由一位 POWER 上电信号、128 位的激励信号和 64 位的 RES 响应信号组成。当 POWER=(1)b 时，电路处于掉电状态，RES=(00000000)h。当 POWER=(0)b 时，RES=(????????)h，RES 由激励信号 Q 决定。

每个 BR_PUF 单元如图 1.17 所示，由两个 BR_PUF_CELL 组成(br_puf_cell_inst)。

每个 BR_PUF_CELL 单元如图 1.18 所示，由两个 SRAM_BR_PUF_CELL 组成(sram_br_puf_inist)。

每个 SRAM_BR_PUF_CELL 单元如图 1.19 所示，由两个二输入 LUT 组成，这两个二输入 LUT 形成了一个环路结构。

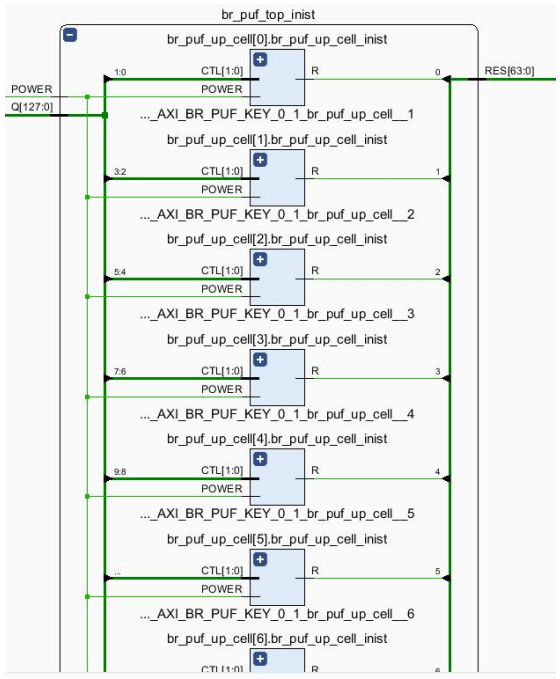


图 1.16 BR_PUF 电路 BD 设计

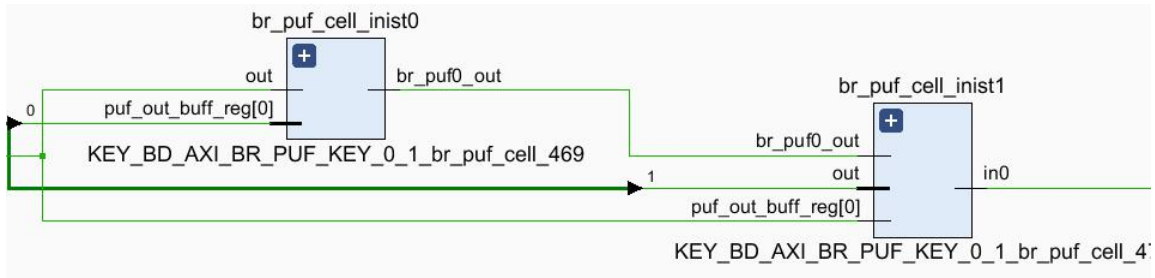


图 1.17 BR_PUF 单元

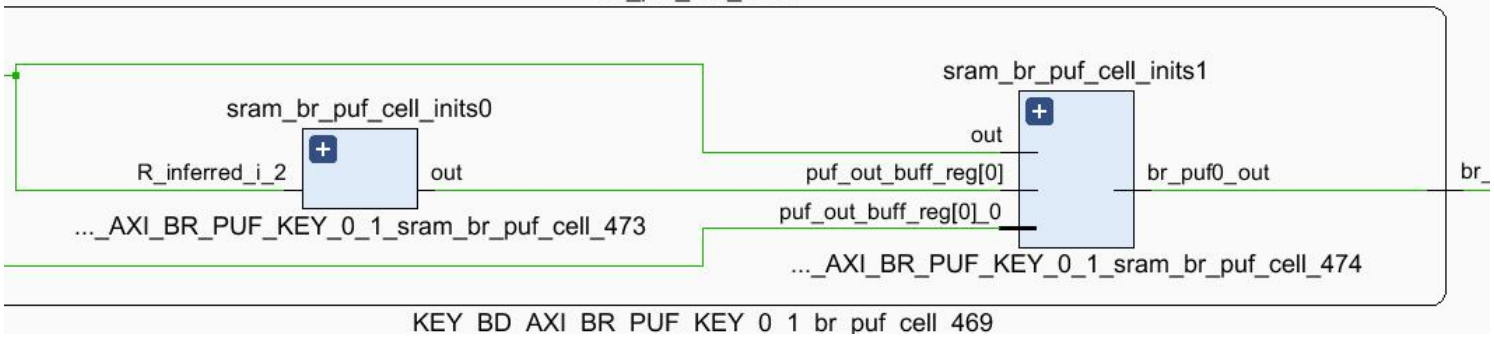


图 1.18 BR_PUF_CELL 单元

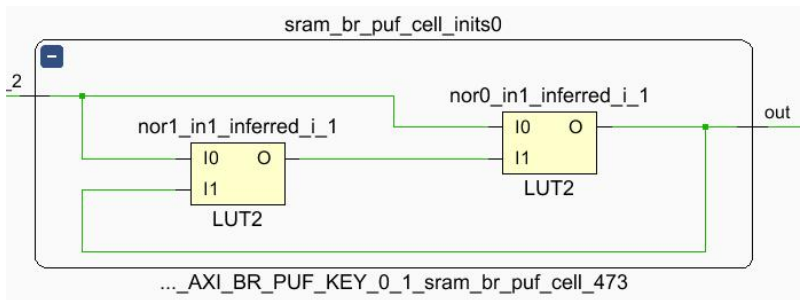


图 1.9 SRAM_BR_PUF_CELL 单元

1.2.6 改进后电路测试

如表 1.3~1.4 所示。

电路稳定性和随机性都有了很好的改善。

表 1.3 振荡比特分析

Total bits	Unsteady bits	ratio
64	7	10.9%

表 1.4 “0””1”分布分析

Total bits	1 bit	0 bit	0/1 distribution
7104	3435	3669	52%/48%

BR_PUF_KEY IP 核

本章将介绍 BR_PUF_KEY IP 核的特点和相关寄存器。

Topic **Page**

2.1 简介

BR_PUF_KEY 为 AXI4 接口协议标准的 IP 核，内部封装了 PUF 电路，时钟管理电路，密钥生成电路。BR_PUF_KEY IP 核的主要特点:

- 利用改进后的 BR_PUF 电路保护密钥。
- 使用 SHA1 加密算法。
- Reed-Muller 和 Repetition 编码级联的模糊提取算法。
- PUF 激励 128bits，对应响应 64bits。
- 加密数据 R 输入 128bits，密钥输出长度 160bits。
- 辅助数据长度 2048bits。
- 最高时钟频率 101Mhz。
- PUF 响应最高输出频率 12.636MHz。
- 密钥最高输出频率 1.232MHz。

2.2 工作模式简介

BR_PUF_KEY IP 核可工作于以下几个模式：

- PUF OUT MODE:在该模式下，BR_PUF_KEY IP 仅用作 PUF 响应的输出，此时 IP 核功耗最小。
- KEY BUILD MODE:在该模式下，BR_PUF_KEY IP 的编码功能被使能，此时模块会根据输入的原始数据 R 和激励生成一组秘钥和此秘钥对应的辅助数据。
- KEY REBUILD MODE:在该模式下，BR_PUF_KEY IP 的解码功能被使能，此时模块会根据输入的

辅助数据和激励还原秘钥。

2.3 IP 核原理框图

IP 核原理框图如图 2.1 所示，其顶层采用 AXI4 标准协议进行封装，其时钟信号 puf_clk 经过分频器为 PUF 电路的控制逻辑电路提供了基准时钟。分频器的位宽为 16bits，这里需要注意的是，分频寄存器中写入的值必须大于等于 3。

除此之外，数据输出接口 PUF、KEY 等都支持 AXI Stream 协议。其包括一个数据有效信号 qvld、最后一位数据指示信号 Tlast、以及若干位的数据。可以通过这种接口去级联其他处理 IP。

整个 IP 支持 1bit 的中断信号，puf_int 为上升沿触发，当 IP 核完成指定事件后，puf_int 会产生一上升沿作为中断信号，其高电平宽度由控制逻辑的基准时钟决定。如果基准时钟频率过高，可能导致 CPU 主频低于 IP 核中断信号频率，就可能导致 CPU 无法检测该中断，其解决方法为增加一异步同步逻辑。

数据的读写都是地址映射型。

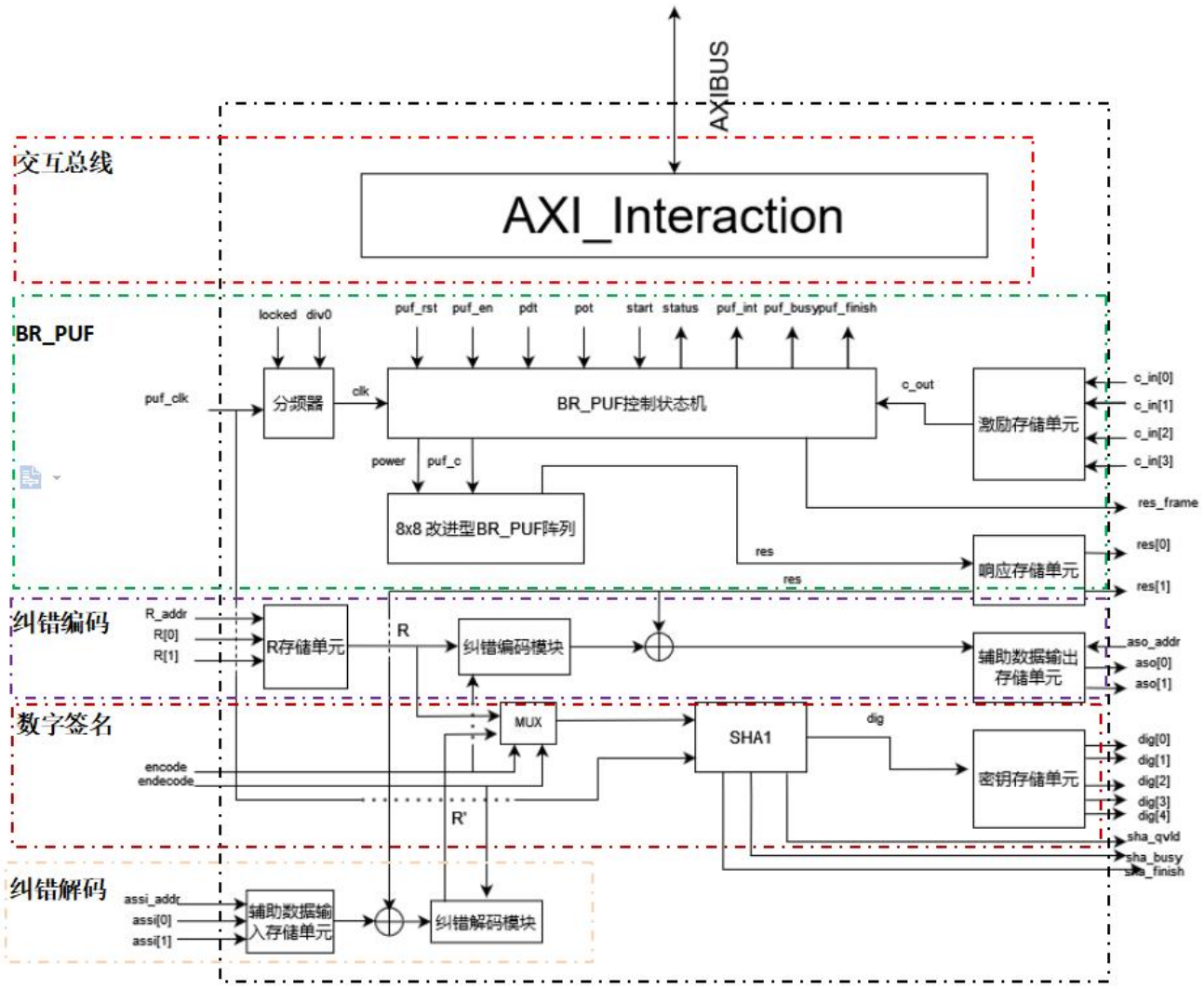


图 2.1 BR_PUF_KEY IP 原理框图

2.4 中断条件

中断信号 puf_int 为上升沿有效，其产生于:

- PUF 完成一次响应的生成。

2.5 BR_PUF_KEY 寄存器

表 2.1 中列举了 BR_PUF_KEY 所有的寄存器及其偏移地址，可通过 section 一栏快速定位其相关申明。

表 2.1 BR_PUF_KEY 寄存器表

Offset	Register	Type	Reset	Section
00	PUF_KEY_CTL0	RW	(0)h	Section 2.5.1
04	PUF_KEY_DIV0	RW	(0)h	Section 2.5.2
08	PUF_KEY_DIV1	RW	(0)h	Section 2.5.3
0C	PUF_KEY_DIV2	RW	(0)h	Section 2.5.4
10	PUF_KEY_CIN0	RW	(0)h	Section 2.5.5
14	PUF_KEY_CIN1	RW	(0)h	Section 2.5.5
18	PUF_KEY_CIN2	RW	(0)h	Section 2.5.5
1C	PUF_KEY_CIN3	RW	(0)h	Section 2.5.5
20	PUF_KEY_RBUF0	R	(0)h	Section 2.5.6
24	PUF_KEY_RBUF1	R	(0)h	Section 2.5.6
28	PUF_KEY_IFG0	R	(0)h	Section 2.5.7
2C	PUF_KEY_EMSG0	RW	(0)h	Section 2.5.8
30	PUF_KEY_EMSG1	RW	(0)h	Section 2.5.8
34	PUF_KEY_EMSG2	RW	(0)h	Section 2.5.8
38	PUF_KEY_EMSG3	RW	(0)h	Section 2.5.8
3C	PUF_KEY_ECODAR	RW	(0)h	Section 2.5.9
40	PUF_KEY_ECODE0	R	(0)h	Section 2.5.10
44	PUF_KEY_ECODE1	R	(0)h	Section 2.5.10
48	PUF_KEY_DIG0	R	(0)h	Section 2.5.11
4C	PUF_KEY_DIG1	R	(0)h	Section 2.5.11
50	PUF_KEY_DIG2	R	(0)h	Section 2.5.11
54	PUF_KEY_DIG3	R	(0)h	Section 2.5.11
58	PUF_KEY_DIG4	R	(0)h	Section 2.5.11
5C	PUF_KEY_ASSIS0	RW	(0)h	Section 2.5.12
60	PUF_KEY_ASSIS1	RW	(0)h	Section 2.5.12
64	PUF_KEY_ASSAR	RW	(0)h	Section 2.5.13

2.5.1 PUF_KEY_CTL0

Offset = (00)h

CTL0 寄存器用于整个 IP 核的功能选择、复位、数据同步信号等控制。

表 2.2 PUF_KEY_CTL0 寄存器

31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16
reserved															
rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0
15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
reserved									ASSFRAME	MODE		STA	LOCK	EN	RST
rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0

表 2.3 PUF_KEY_CTL0 寄存器描述

Bit	定义	类型	默认值	描述
31-7	Reserved	RW	0h	保留
6	ASSFRAME	RW	0h	辅助数据同步信号。 1b = 当前输入辅助数据有效 0b = 当前输入数据无效
5-4	MODE	RW	0h	工作模式选择。 00b = PUF 输出模式。 01b = 秘钥注册模式(KEY_BULID_MODE) 10b = 秘钥重建模式(KEY_REBULID_MODE) 11b = 秘钥注册模式(KEY_BULID_MODE)
3	STA	RW	0h	时间触发信号。 1b = 触发一次 PUF_KEY 事件 0b = 非触发
2	LOCK	RW	0h	分频寄存器 DIV0-DIV2 上锁信号。 1b = 分频寄存器解锁 0b = 分频寄存器上锁
1	EN	RW	0h	模块使能信号。 1b = 模块使能。 0b = 模块禁能。
0	RST	RW	0h	复位信号。 1b = 模块复位 0b = 模块正常工作

2.5.2 PUF_KEY_DIV0

Offset = (04)h

DIV0 寄存器用于参考时钟的产生。

CLK_DIV = CLK_SOURCE / DIV0

表 2.2 PUF_KEY_DIV0 寄存器

31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16
reserved															
rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0
15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
VAL															
rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0

表 2.3 PUF_KEY_DIV0 寄存器描述

Bit	定义	类型	默认值	描述
31-16	Reserved	RW	0h	保留
15-0	VAL	RW	0h	参考时钟的分配值

2.5.3 PUF_KEY_DIV1

Offset = (08)h

DIV1 寄存器用于设置 BR_PUF 电路的掉电时间。

POWER_DOWN = DIV1 • CLK_DIV

表 2.4 PUF_KEY_DIV1 寄存器

31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16
reserved															
rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0
15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
VAL															
rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0

表 2.5 PUF_KEY_DIV1 寄存器描述

Bit	定义	类型	默认值	描述
31-16	Reserved	RW	0h	保留
15-0	VAL	RW	0h	掉电时间值

2.5.4 PUF_KEY_DIV2

Offset = (0C)h

DIV2 寄存器用于设置 BR_PUF 电路的上电时间。

POWER_ON = DIV2 • CLK_DIV

表 2.6 PUF_KEY_DIV2 寄存器

31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16
reserved															
rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0
15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
VAL															
rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0

表 2.7 PUF_KEY_DIV2 寄存器描述

Bit	定义	类型	默认值	描述
31-16	Reserved	RW	0h	保留
15-0	VAL	RW	0h	上电时间

2.5.5 PUF_KEY_CINx(x=0,1,2,3)

Offset = (10)h+(x<<2)h

CINx 寄存器用于暂存 PUF 电路的激励信号。PUF 电路的激励信号长度为 128 位，由 CIN0~CIN3 指定（由低到高）。该寄存器的值将在 STA 信号为高时，重新拼接为 128 位激励，并打入至 IP 核内部激励寄存器。

表 2.8 PUF_KEY_CINx 寄存器

31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16
VAL															
rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0
15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
VAL															
rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0

表 2.9 PUF_KEY_CINx 寄存器描述

Bit	定义	类型	默认值	描述
31-0	VAL	RW	0h	激励由低到高的 32 位数据。

2.5.6 PUF_KEY_RBUFx(x=0,1)

Offset = (20)h+(x<<2)h

RBUFx 寄存器用于缓存 PUF 电路的响应信号。PUF 电路的响应长度为 64 位，由 RBUF0~RBUF1 指定

（由低到高）。

表 3.0 PUF_KEY_RBUFx 寄存器

31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16
VAL															
rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0
15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
VAL															
rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0

表 3.1 PUF_KEY_RBUFx 寄存器描述

Bit	定义	类型	默认值	描述
31-0	VAL	RW	0h	响应由低到高的 32 位数据。

2.5.7 PUF_KEY_IFG0

Offset = (28)h

状态标志寄存器，存储 IP 核的各项状态。

表 3.2 PUF_KEY_IFG0 寄存器

31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16
VAL															
rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0
15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
											SHAFINISH	SHABUSY	POWERST	FINISH	BUSY
rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0

表 3.3 PUF_KEY_IFG0 寄存器描述

Bit	定义	类型	默认值	描述
31-5	Reserved	R	0h	保留位。
4	SHAFINISH	R	0h	密钥生成完成指示信号。 1b = 密钥生成完成 0b = 密钥正在生成
3	SHABUSY	R	0h	指示 SHA 模块是否繁忙 1b = SHA 算法模块繁忙 0b = SHA 算法模块空闲
2	POWERST	R	0h	指示当前 PUF 电路的上电状态 1b = PUF 处于上电状态 0b = PUF 处于掉电状态
1	FINISH	R	0h	指示当前整个系统的工作状态 1b = 已完成一个事件 0b = 正在响应一个事件
0	BUSY	R	0h	指示当前系统是否繁忙 1b = 模块繁忙 0b = 模块空闲

2.5.8 PUF_KEY_EMSGx(x=0,1,2,3)

Offset = (2C)h+(x<<2)h

该寄存器寄存产生密钥的原始数据 R。

表 3.4 PUF_KEY_EMSG0 寄存器

31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16
VAL															
rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0
15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
VAL															
rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0

表 3.5 PUF_KEY_EMSG0 寄存器描述

Bit	定义	类型	默认值	描述
31-0	VAL	RW	0h	暂存产生密钥的原始数据 R。

2.5.9 PUF_KEY_ECODAR

Offset = (3C)h

该寄存器寄用于索引辅助数据存储寄存器。其中寄存辅助数据的地址。该寄存器中数据范围为 0-32。

表 3.6 PUF_KEY_ECODAR 寄存器

31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16
VAL															
rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0
15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
VAL															
rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0

表 3.7 PUF_KEY_ECODAR 寄存器描述

Bit	定义	类型	默认值	描述
31-0	VAL	RW	0h	存储辅助数据的索引地址。

2.5.10 PUF_KEY_ECODEx(x=0,1)

Offset = (40)h+(x<<2)h

该寄存器存储通过 ECODAR 索引的辅助数据。ECODE0~ECODE1 分别为索引的低 32 位和高 32 位。

表 3.8 PUF_KEY_ECODEx 寄存器

31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16
VAL															
rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0
15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
VAL															
rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0

表 3.9 PUF_KEY_ECODEx 寄存器描述

Bit	定义	类型	默认值	描述
31-0	VAL	RW	0h	存储辅助数据。

2.5.11 PUF_KEY_DIGx(x=0,1,2,3,4)

Offset = (48)h+(x<<2)h

该寄存器存储产生的密钥。DIG0~DIG4 由低到高存储 160 位长度的密钥。

表 3.10 PUF_KEY_DIGx 寄存器

31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16
VAL															
rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0
15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
VAL															
rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0

表 3.11 PUF_KEY_DIGx 寄存器描述

Bit	定义	类型	默认值	描述
31-0	VAL	RW	0h	32 位的密钥值。

2.5.12 PUF_KEY_ASSISx(x=0,1)

Offset = (5C)h+(x<<2)h

该寄存器存储输入的辅助数据。当 STA 信号有效时，该寄存器的数据将会被打入辅助数据寄存器中由 ASSAR 指定的地址处。

表 3.12 PUF_KEY_ASSISx 寄存器

31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16
VAL															
rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0
15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
VAL															
rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0

表 3.13 PUF_KEY_ASSISx 寄存器描述

Bit	定义	类型	默认值	描述
31-0	VAL	RW	0h	32 位的输入辅助数据值。

2.5.13 PUF_KEY_ASSAR

Offset = (60)h

用于指示 ASSISx 寄存器写入辅助数据寄存器的位置。

表 3.14 PUF_KEY_ASSAR 寄存器

31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16
VAL															
rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0
15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
VAL															
rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0	rw-0

表 3.15 PUF_KEY_ASSAR 寄存器描述

Bit	定义	类型	默认值	描述
31-0	VAL	RW	0h	ASSISx 寄存器写入辅助数据寄存器的位置。

API 接口

本章节将对 BR_PUF_KEY 软件驱动函数库中所涉及的函数进行介绍。

该函数库仅适用于 AXI 总线封装的 BR_PUF_KEY IP 核。

若使用 ARM 内核或 microblaze 的情况下，该函数库同样适用。

3.1 库函数文件简介

库函数主要早 user 和 src 目录中。

其中 user 目录下包含 BR_PUF_KEY_user.c、BR_PUF_KEY_user.h、dataconfig.h、puf_cin.h、headfile.h。

其中 src 目录中包含 BR_PUF_test.c 文件。

执行函数 main.c 文件在 src 目录下，在 mian.c 中调用 BR_PUF_test.c 中的文件完成相关数据的测试。

表 3.1 库函数文件

File name	Type	Function num	Describe
BR_PUF_KEY_user.c	C source	20	BR_PUF_KEY 的驱动函数。
BR_PUF_test.c	C source	3	BR_PUF_KEY 的测试函数。
BR_PUF_KEY_user.h	Head file		BR_PUF_KEY_user.c 头文件。
dataconfig.h	Head file		数据类型申明。
puf_cin.h	Head file		PUF 测试激励存储。
headfile.h	Head file		整个测试工程头文件。

3.2 BR_PUF_KEY API 接口表

API 接口如表 3.2 所示，可通过 section 查看。

BR_PUF_KEY API 接口表

表 3.2 API 接口表

Function name	File	Type	Section
BR_PUF_KEY_reset	BR_PUF_KEY_user.c	Void	Section3.2.1
BR_PUF_KEY_enable	BR_PUF_KEY_user.c	Void	Section3.2.2
BR_PUF_KEY_disable	BR_PUF_KEY_user.c	Void	Section3.2.3
BR_PUF_KEY_start	BR_PUF_KEY_user.c	Void	Section3.2.4
BR_PUF_KEY_POWERDOWNT_set	BR_PUF_KEY_user.c	Void	Section3.2.5
BR_PUF_KEY_POWERONT_set	BR_PUF_KEY_user.c	Void	Section3.2.6
BR_PUF_KEY_CLKDIV_set	BR_PUF_KEY_user.c	Void	Section3.2.7
BR_PUF_KEY_CIN_set	BR_PUF_KEY_user.c	Void	Section3.2.8
BR_PUF_KEY_OUT_get	BR_PUF_KEY_user.c	Void	Section3.2.9
BR_PUF_KEY_IFG_get	BR_PUF_KEY_user.c	Uint16	Section3.2.10
BR_PUF_KEY_ecode_enable	BR_PUF_KEY_user.c	Void	Section3.2.11
BR_PUF_KEY_decode_enable	BR_PUF_KEY_user.c	Void	Section3.2.12
BR_PUF_KEY_ecode_disable	BR_PUF_KEY_user.c	Void	Section3.2.13
BR_PUF_KEY_decode_disable	BR_PUF_KEY_user.c	Void	Section3.2.14
BR_PUF_KEY_read_assistance	BR_PUF_KEY_user.c	Void	Section3.2.15
BR_PUF_KEY_Rdata_set	BR_PUF_KEY_user.c	Void	Section3.2.16
BR_PUF_KEY_SHAdig_get	BR_PUF_KEY_user.c	Void	Section3.2.17
BR_PUF_KEY_write_assistance	BR_PUF_KEY_user.c	Void	Section3.2.18
Random_init	BR_PUF_KEY_user.c	Void	Section3.2.19
Random	BR_PUF_KEY_user.c	Int32	Section3.2.20
BR_PUF_out_test	BR_PUF_test.c	Void	Section3.2.21
BR_PUF_key_test	BR_PUF_test.c	Void	Section3.2.22
BR_PUF_random_test	BR_PUF_test.c	Void	Section3.2.23

3.2.1 BR_PUF_KEY_reset

API 接口描述			
函数名	BR_PUF_KEY_reset	**参数**	Base_addr：操作器件的基地址
功能描述	对 BR_PUF_KEY IP 核复位		
注意事项	无		

3.2.2 BR_PUF_KEY_enable

API 接口描述			
函数名	BR_PUF_KEY_enable	**参数**	Base_addr：操作器件的基地址
功能描述	BR_PUF_KEY IP 核使能		
注意事项	无		

3.2.3 BR_PUF_KEY_enable

API 接口描述			
函数名	BR_PUF_KEY_disable	**参数**	Base_addr：操作器件的基地址
功能描述	BR_PUF_KEY IP 核失能		
注意事项	无		

3.2.4 BR_PUF_KEY_start

API 接口描述			
函数名	BR_PUF_KEY_start	**参数**	Base_addr：操作器件的基地址
功能描述	BR_PUF_KEY 触发一次 PUF 事件		
注意事项	无		

3.2.5 BR_PUF_KEY_POWERDOWNT_set

API 接口描述			
函数名	BR_PUF_KEY_POWERDOWNT_set	**参数**	Base_addr：操作器件的基地址 time:需要等待的时间
功能描述	设置 PUF 电路的掉电等待延迟时间		
注意事项	掉电等待时间计算公式: T = time*(T_clkdiv) 其中 T_clkdiv 为基准时钟，由 DIV0 寄存器对时钟源分频得到。		

3.2.6 BR_PUF_KEY_POWERONT_set

API 接口描述			
函数名	BR_PUF_KEY_POWERONT_set	**参数**	Base_addr：操作器件的基地址 time:需要等待的时间
功能描述	设置 PUF 电路的上电等待延迟时间		
注意事项	上电等待时间计算公式: T = time*(T_clkdiv) 其中 T_clkdiv 为基准时钟，由 DIV0 寄存器对时钟源分频得到。		

3.2.7 BR_PUF_KEY_CLKDIV_set

API 接口描述			
函数名	BR_PUF_KEY_CLKDIV_set	**参数**	Base_addr：操作器件的基地址 time:分频系数
功能描述	设置 IP 核内部的基准时钟频率		
注意事项	基准时钟的频率为：f_clksource/time f_clksource 为模块的输入时钟频率。		

3.2.8 BR_PUF_KEY_CIN_set

API 接口描述			
函数名	BR_PUF_KEY_CIN_set	**参数**	Base_addr：操作器件的基地址 cin:需要写入 IP 的激励存储缓冲区
功能描述	设置 PUF 的激励信号		
注意事项	cin 可以是一个 32 位的 4 个长度的数组。 如:uint32 cin[4]={0xffffffff};		

3.2.9 BR_PUF_KEY_OUT_get

API 接口描述			
函数名	BR_PUF_KEY_OUT_get	**参数**	Base_addr：操作器件的基地址 out:存储响应的缓冲区的首指针
功能描述	读取 PUF 电路的响应		
注意事项	out 可以是一个 32 位的 2 个长度的数组。 如:uint32 out[2]={0x00};		

3.2.10 BR_PUF_KEY_IFG_get

API 接口描述			
函数名	BR_PUF_KEY_IFG_get	**参数**	Base_addr：操作器件的基地址
功能描述	读取 BR_PUF_KEY IP 核的状态寄存器		
注意事项	该函数调用时会返回一个 16 位的状态数据		

3.2.11 BR_PUF_KEY_ecode_enable

API 接口描述			
函数名	BR_PUF_KEY_ecode_enable	**参数**	Base_addr：操作器件的基地址
功能描述	使能 BR_PUF_KEY IP 核的编码功能。即将模块配置为 KEY BUILD MODE 模式。		
注意事项	无		

3.2.12 BR_PUF_KEY_decode_enable

API 接口描述			
函数名	BR_PUF_KEY_decode_enable	**参数**	Base_addr：操作器件的基地址
功能描述	使能 BR_PUF_KEY IP 核的解码功能。即将模块配置为 KEY REBUILD MODE 模式。		
注意事项	无		

3.2.13 BR_PUF_KEY_ecode_disable

API 接口描述			
函数名	BR_PUF_KEY_ecode_disable	**参数**	Base_addr：操作器件的基地址
功能描述	禁能 BR_PUF_KEY IP 核的编码功能。		
注意事项	无		

3.2.14 BR_PUF_KEY_decode_disable

API 接口描述			
函数名	BR_PUF_KEY_decode_disable	**参数**	Base_addr：操作器件的基地址
功能描述	禁能 BR_PUF_KEY IP 核的解码功能。		
注意事项	无		

3.2.15 BR_PUF_KEY_read_assistance

API 接口描述			
函数名	BR_PUF_KEY_read_assistance	**参数**	Base_addr：操作器件的基地址 as_buf：辅助数据存储缓冲区的首指针。
功能描述	读取一次 BR_PUF_KEY 生成的辅助数据。		
注意事项	as_buf 可以是一个 32 位 64 长度的数组。 如：as_buf[64] = {0x00};		

3.2.16 BR_PUF_KEY_Rdata_set

API 接口描述			
函数名	BR_PUF_KEY_Rdata_set	**参数**	Base_addr：操作器件的基地址 R：需要输入的原始数据的缓冲区首指针。
功能描述	向 BR_PUF_KEY 写入一组原始数据。		
注意事项	R 可以是一个 32 位 4 长度的数组。 如：R[4] = {0x00};		

3.2.17 BR_PUF_KEY_SHAdig_get

API 接口描述			
函数名	BR_PUF_KEY_SHAdig_get	**参数**	Base_addr：操作器件的基地址 dig：存放秘钥的缓冲区首地址。
功能描述	读取一次 BR_PUF_KEY 生成的秘钥。		
注意事项	dig 可以是一个 32 位 5 长度的数组。 如：dig[5] = {0x00};		

3.2.18 BR_PUF_KEY_write_assistance

API 接口描述			
函数名	BR_PUF_KEY_write_assistance	**参数**	Base_addr：操作器件的基地址 as_buf：需要参与秘钥重建辅助数据缓冲区指针
功能描述	向 BR_PUF_KEY 写入由 as_buf 暂存的辅助数据。		
注意事项	as_buf 可以是一个 32 位 64 长度的数组。 如：as_buf[64] = {0x00};		

3.2.19 Random_init

API 接口描述			
函数名	Random_init	**参数**	Random：随机数结构体指针
功能描述	初始化随机数结构体		
注意事项	Random 结构体在 BR_PUF_KEY_user.h 文件中定义。		

3.2.20 Random

API 接口描述			
函数名	Random	**参数**	Random：随机数结构体指针
功能描述	计算并返回一次真随机数		
注意事项	Random 结构体在 BR_PUF_KEY_user.h 文件中定义 返回的随机数大小为 32 位的整型		

3.2.21 BR_PUF_out_test

API 接口描述			
函数名	BR_PUF_out_test	**参数**	无
功能描述	对 IP 核 PUF 的响应数据进行 n 次采样并以二进制形式打印		
注意事项	无		

3.2.22 BR_PUF_key_test

API 接口描述			
函数名	BR_PUF_key_test	**参数**	无
功能描述	对 IP 核生成秘钥的过程进行测试，并进行 100 次重建，计算重建秘钥的正确率。		
注意事项	无		

3.2.23 BR_PUF_random_test

API 接口描述			
函数名	BR_PUF_random_test	**参数**	无
功能描述	对 IP 核生成的真随机数进行测试。		
注意事项	无		

Data:2022.5.20
Recoder:Ge Wen Jie

IP 核相关测试记录

在本章中对 BR_PUF_IP 核的测试数据、测试过程和测试结果进行详细记录。

在本章中首先对 PUF 电路的响应进行分析，主要分析其片内汉明距离和分数汉明距离。由于 FPGA 开发板不够，暂时无法分析片间汉明距离。

其次对整个 IP 核生成秘钥的过程进行测试，并进行了 100 重建，将每次重建后的秘钥与原始秘钥进行比较，最后得到正确率。

最后对随机数方案产生的真随机数进行测试。

并将测试结果与其他论文得到的结果进行相比较。

4.1 测试情况表

Num	HD_FIL(0/1)	HD_SIL	HD_SRA	Build_right_rate	Random_var	Random_average	FPGA	remark
1	46.56%/53.44%	1.12%		100%	75.0652062911263	-0.02499074416882636	Zynq7010	
2	46.57%/53.43%	2.07%	31.8%	100%	74.2709397636582	-0.1025735294117647	Zynq7010	
3	50.84%/49.15%	1.59%	35.72%	100%			Zynq7010	优化 LUT4 为两个 LUT2

4.2 PUF 电路激励响应对测试

对 PUF 电路响应的测试主要为片内汉明距离和分数汉明距离的计算。前者代表了 PUF 电路响应的可靠性，后者则代表了 PUF 电路的随机性。

对于片内汉明距离的测量方法如下:

1.施加同一激励。

2.对同一激励进行 n 次响应的产生并读取。

3.使用 Python 对产生的响应进行分析，得到该激励下的片内汉明距离。

4.重复 50 次 1-3 步骤，将每次获得的响应作图分析，获取大体上的片内汉明距离。

注意:

该过程已经在 BR_PUF_out_test 函数中封装。

对与分数汉明距离的测量方法如下：

1.施加一激励。

2.对该激励进行 n 次响应的产生并读取。

3.改变激励重复 2 过程。

4.将取得的所有激励计算 1 和 0 的个数，得到分数汉明距离。

4.2.1 测试函数执行情况记录

执行 BR_PUF_out_test 所打印的信息:

```
-------------------PUF TEST START!!-------------------
-------------------diffrent cin!!-------------------
1000011011111111111001100010101111110111001000111111100101100110 1
0010011011011100011000101001110101111010101110011111000111011 01
0010110001010110001010101011100100101000011100011110100010101101
1000011011110000101001101111101111001110010001111010000010011110
0011010001110100101000101101000111111001011001011011100101100001
0000011000110010101011001111111101011000010111011000100010110000
1010110011110100101000001011111111111011010101111011100100001110
1001010010011001110001011011001110001111010111111010100100110111
1000011011111010001001101111111111011100010001011011100001000100
1000011011110110010010011101101110101101010111011101101001101001
0001010001110011110001001011101110001000010111111110100101001101
1001110010010111001001111101000101111011011010011001000101011011
0010010001111011100010011011100101101000011011011110100000001110
1001110011010110000001011001100010100101101111111111000110111100 0
0011111000010010101001011001001101111010011111011011000101010101
1001110010011010100000000101100111111100001000101101110010010001 1
1011010001110100101001111111111110101110011101001100001011111101
0011110011010001000011011011001100101100011110110101011100011 01
1001111011011100111000100111110100101011000011111010000000101011
0011010000110000100110111011010111101010011101101101100110101001
0010111011110001000001111001111101101001011111101111001011111010
1010011001111011100010100011001110101101011101011011000100110101
0011110011111111110000110010110011101100001000101111110001010100 1
1011011011010011111010011111011111101011001011110101010001000 10
0010010001010110011000000000101110001101101101100110010011101111 0
0000011011011011101010100011111111001111011111001110100010011111
0011111001111111001011100111011110101001010111111111001110011001
1000111011010001001000111011011100011000011101011110100011100101
0001110001011000010001111011001111111001011010011110100000100111
1000110001010001101011101011100110111100011111011011100001111000
0011111011010001101000011101101101001100000011001011101111010111
0001010010010011011011000001110111001001011110110111001011101 10
1011011001111111111001010111101101101100011110110111001111001 01
1000110011111011001001111111000101001000010111111001000010001010
1001011000110011001000110101010110111010011110111100011101111100
1000010001011010111000010011010101011010011110101011101110000101
1010011000011111001011001111100101001011010011011111001000100011
1000011011011111110000110110101010010111100001111101100100110111 0
1001110011010000000100011100100110010101001101111111010100000111 11
1001011000011001000000001100111110000101001011011111111001110011 10
1001011000110100101000011011001101111011000001101111001101011000
1011110011111001110010001011111101111100001101011010100100101100
1000111001010111111011001011010110001011011111011011000100011000
1001111001110110100001011101011100101010000110011110100100111001
0010010000011101111001010011011100001011011101111010100101111000
1011011011110101111000000111100111101010011001101111001110110000
```

1011110000111011100001101000001110101000000001011110000100000111
0011110000111000101011011101010100101111000011011111001010110100
1010010000010011010000101110111111111110110011111010010000101 1
1000010001111101101011111001101111111000011001101110100100001000
-------------------same cin!!-------------------
1000011011111111110011000101011111101110010001111101001011001101
1000011011111111110011000111011111101110010001111111001011001100
1000011010111111110011000101011111101110010001111101001011001101
1000011011111111110011000101011111101110010001111101001011001101
1000011011111111110011000111011111101110010001111111001011001101
1000011011111111110011000111011111101110010001111111001011001101
1000011011111111110011000101011111101110010001111101001011001101
1000011011111111110011000101011111101110010001111111001011001101
1000011011111111110011000111011111101110010001111110001011001101
1000011011111111110011000101011111101110010001111101001011001101
1000011011111111110011000101011111101110010001111111001011001101
1000011011111111110011000101011111101110010000111111001011001101
1000011011111111110011000101011111101110010001111101001011001101
1000011011111111110011000101011111101110010001111101001011001101
1000011011111111110011000101011111101110010001111101001011001101
1000011011111111110011000111011111101110010001111111001011001101
1000011011111111110011000101011111101110010001111101001011001100
1000011011111111110011000101011111101110010001111111001011001101
1000011011111111110011000111011111101110010001111101001011001100
1000011011111111110011000101011111101110010001111101001011001101
1000011011111111110011000111011111101110010001111101001011001101
1000011011111111110011000101011111101110010001111111001011001101
1000011011111111110011000101011111101110010001111101001011001101
1000011011111111110011000101011111101110010001111101001011001101
1000011011111111110011000101011111101110010001111101001011001101
1000011011111111110011000101011111101110010001111101001011001101
1000011011111111110011000101011111101110010001111101001011001101
1000011011111111110011000101011111101110010001111101001011001101
1000011011111111110011000100011111101110010001111111001011001101
1000011011111111110011000101011111101110010001111101001011001101
1000011011111111110011000111011111101110010001111111001011001100
1000111011111111110011000101011111101110010001111111001011001101
1000011011111111110011000111011111101110010001111111001011001101
1000011011111111110011000101011111101110010001111101001011001101
1000011011111111110011000100011111101110010001111110001011001101
1000011011111111110011000110011111101110010001111111001011001101
1000011011111111110011000110011111101110010001111101001011001101
1000011011111111110011000101011111101110010001111111001011001100
1000011011111111110011000111011111101110010000111110001011001101
1000011010111111110011000101011111101110010001111101001011001100
1000011011111111110011000101011111101110010001111101001011001101
1000011011111111110011000101011111101110010001111101001011001101
1000011011111111110011000101011111101110010000111101001011001101
1000011011111111110011000001011111101110010000111111001011001101
1000011011111111110011000101011111101110010001111111001011001101
1000011011111111110011000101011111101110010001111101001011001101
1000011011111111110011000111011111101110010000111101001011001101
1000011010111111110011000001011111101110010001111111001011001101
1000011011111111110011000101011111101110010000111101001011001101
1000011011111111110011000101011111101110010000111111001011001101

1000011011111111111001100010101111111011100100011111111001011001101
1000011011111111111001100010101111111011100100011111111001011001101
1000011011111111111001100010101111111011100100011111111001011001101
1000011011111111111001100010101111111011100100011111101001011001101
1000011011111111111001100010101111111011100100011111101001011001101
1000011011111111111001100010101111111011100100011111111001011001101
1000011011111111111001100010101111111011100100011111101001011001100
1000011011111111111001100010101111111011100100011111111001011001101
1000011011111111111001100010101111111011100100011111111001011001101
1000011011111111111001100011101111111011100100011111111001011001101
1000011011111111111001100010101111111011100100011111101001011001101
1000011011111111111001100010101111111011100100011111000001011001100
1000011011111111111001100010101111111011100100011111111001011001101
1000011010111111111001100010101111111011100100011111111001011001101
1000011011111111111001100010101111111011100100011111111001011001101
1000011011111111111001100010101111111011100100011111111001011001100
1000011011111111111001100010101111111011100100011111110001011001101
1000011011111111111001100010101111111011100100011111111001011001100
1000011011111111111001100010101111111011100100011111111001011001101
1000011011111111111001100010101111111011100100011111101001011001101
1000011011111111111001100010001111111011100100011111111001011001100
1000011011111111111001100010101111111011100100011111111001011001101
1000011011111111111001100011101111111011100100011111111001011001101
1000011010111111111001100010101111111011100100011111101001011001101
1000011011111111111001100010101111111011100100011111101001011001101
1000011011111111111001100011101111111011100100011111111001011001101
1000011011111111111001100010101111111011100100011111101001011001100
1000011010111111111001100010101111111011100100011111111001011001101
1000011011111111111001100010101111111011100100011111111001011001100
1000011011111111111001100010101111111011100100011111111001011001101
1000011011111111111001100010101111111011100100011111111001011001101
1000011011111111111001100010101111111011100100011111101001011001101
1000011011111111111001100011101111111011100100011111111001011001101
1000011011111111111001100010101111111011100100011111101001011001101
1000011011111111111001100010101111111011100100011111000001011001101
1000011011111111111001100010101111111011100100011111111001011001100
1000011011111111111001100010001111111011100100011111111001011001101
1000011011111111111001100010101111111011100100011111111001011001100
1000011011111111111001100010101111111011100100011111111001011001101
1000011011111111111001100010101111111011100100011111111001011001101
0010011010011100010000101001110101111101010110001111110001111110 1
0010011011011100011000101001110101111101010111001111110001111110 1
0010011011011100011000101001110101111101010111001111110001111110 1
0010011011011100011000101011110101111101010111001111110001110110 1
0010011011011100010000101001110101111101010110001111110001111110 1

0010011011011100010000101001010101111101010111001111100011111101
0010011011011100011000101001110101111101010111001111100011101101
0010011010011100011000101001110101111101010110001111100011111101
0010011011011100011000101001110101111101010111001111100011111101
0010011010011100011000101001110101111101010111001111100011111101
0010011011011100010000101001110101111101010111001111100011111101
0010011011011100011000101001110101111101010111001111100011111101
0010011011011100010000101001110101111101010111001110100011101101
0010011011011100011000101001110101111101010111001111100011101101
0010011011011100010000101001110101111101010111001111100011111101
0010011011011100011000101001110101111101010111001111100011101101
0010011011011100010000101001110101111101010111001111100011111101
0010011010011100011000101001110101111101010111001111100011111101
0010011011011100010000101001110101111101010111001111100011111101
0010011010011100010000101011110101111101010111001110100011111101
0010011010011100010000101001110101111101010111001111100011111101
0010011011011100010000101001110101111101010111001111100011111101
0010011011011100010000101001110101111101010111001111100011111101
0010011011011100010000101001110101111101010111001111100011111101
0010011011011100010000101001110101111101010111001111100011101101
0010011011011100011000101001110101111101010111001111100011111101
0010011010011100010000101011110101111101010111001111100011101101
0010011011011100010000101001110101111101010111001111100011111101
0010011010011100011000101011110101111101010111001111100011101101
0010011011011100011000101011110101111101010111001111100011111101
0010011010011100010000101001110101111101010110001111100011111101
0010011011011100010000101001110101111101010111001110100011111101
0010011011011100010000101001110101111101010110001111100011101101
0010011011011100010000101001110101111101010111001111100011111101
0010011011011100011000101001110101111101010110001111100011111101
0010011011011100010000101011110101111101010111001111100011111101
0010011011011100010000101001110101111101010111001111100011101101
0010011010011100010000101001110101111101010111001111100011101101
0010011011011100010000101011110101111101010111001111100011111101
0010011011011100011000101001110101111101010111001111100011101101
0010011011011100010000101001110101111101010111001110100011111101
0010011011011100011000101001110101111101010110001111100011101101
0010011011011100010000101001110101111101010111001110100011101101
0010011011011100010000101011110101111101010111001111100011101101
0010011011011100010000101001110101111101010111001111100011111101
0010011011011100011000101001110101111101010110001111100011111101
0010011011011100010000101000110101111101010111001111100011111101
0010011011011100010000101011110101111101010111001111100011111101
0010011011011100010000101011110101111101010111001111100011111101
0010011011011100010000101001110101111101010110001111100011111101
0010011011011100010000101011110101111101010111001111100011111101
0010011010011100010000101001110101111101010111001111100011101101
0010011011011100010000101001110101111101010111001111100011101101
0010011011011100010000101011110101111101010111001111100011111101
0010011011011100011000101001110101111101010111001111100011101101
0010011011011100010000101001110101111101010111001111100011111101
0010011011011100010000101001110101111101010111001111100011111101
0010011011011100010000101001110101111101010110001111100011111101
0010011011011100010000101011110101111101010111001111100011111101
0010011011011100010000101001110101111101010110001111100011111101

00100110110111000100001010011101011111010100110011111100011111101
00100110110111000100001010111101011111010101100011111100011111101
00100110110111000110001010011101011111010101110011111100011101101
00100110110111000100001010011101011111010101100011111100011111101
00100110110111000100001010011101011111010101110011111100011111101
00100110110111000100001010011101011111010101110011111100011101101
00100110110111000100001010110101011111010101110011111100011101101
00100110110111000100001010011101011111010101110011111100011111101
00100110100111000100001010011101011111010101100011111100011111101
00100110110111000110001010011101011111010101110011111100011111101
00100110110111000100001010011101011111010101110011111100011111101
00100110110111000100001010011101011111010101110011111100011101101
00100110100111000100001010010101011111010101110011111100011111101
00100110110111000100001010011101011111010101110011111100011111101
00100110110111000100001010111101011111010101110011111100011101101
00100110110111000110001010011101011111010101110011111100011111101
00100110110111000100001010111101011111010101110011111100011111101
00100110110111000100001010011101011111010101110011111100011101101
00100110100111000100001010011101011111010101110011111100011111101
00100110110111000100001010110101011111010101110011111100011101101
00100110110111000100001010011101011111010101110011111100011111101
00100110110111000100001010011101011111010101110011111100011111101
00100110110111000100001010011101011111010101110011111100011101101
00100110110111000100001010110101011111010101110011111100011101101
00100110110111000100001010011101011111010101110011111100011111101
00100110110111000100001010011101011111010101110011111100011111101
00100110110111000100001010011101011111010101110011111100011111101
00100110110111000100001010011101011111010101110011111100011111101
00100110100111000100001010011101011111010101110011111100011111101
00100110110111000100001010111101011111010101100011101001011111101
00100110110111000110001010011101011111010101110011111100011101101
00100110110111000100001010111101011111010101100011111100011111101
00100110110111000100001010011101011111010101110011111100011111101
00100110110111000100001010011101011111010101110011111100011111101
00100110110111000100001010011101011111010101110011111100011111101
00100110110111000100001010011101011111010101110011111100011111101
00101100010101100010101010111001001010000111010111101000101011101
00101100010101100010101010111001001010000111010111101000101011101
00101100010101100010101010111001001010000111010111101000101011100
00101100000101100010101010111001001010000111010111101000101011101
00101100010101100010101010111001001010000111010111101000101011101
00101100010101100010101010111001001010000111010111101000101011101
00101100010101100010101010111000100101000011101011110100010101101
00101100000101100010101010111000100101000011101011110100010101101
00101100010101100010101010111001001010000111010111101000101011101
00101100010101100010101010111000100101000011101011110100010101101
00101100000101100010101010111000100101000011101011110100010101101
00101100010101100010101010111000100101000011101011110100010101101
00101100010101100010101010111001001010000111010111101000101011101

Data:2022.5.20

Recoder:Ge Wen Jie

PUF 电路激励响应对测试

00101100000101100010101010110001001010000111010111101000101011010010110001010101011000100101000011101011110100010101101
00101100010101100010101010110001001010000111010111101000101011010010110001010101011000100101000011101011110100010101101
00101100010101100010101010111001001010000111010111101000101011010010110001010101011100100101000011101011110100010101101
00101100010101100010101010110001001010000111010111101000101011010010110001010101011000100101000011101011110100010101101
00101100000101100010101010111001001010000111010111101000101011010010110000010101011100100101000011101011110100010101101
00101100010101100010101010111001001010000111010111101000101011010010110001010101011100100101000011101011110100010101101
00101100010101100010101010111001001010000111010111101000101011010010110001010101011100100101000011101011110100010101101
00101100010101100010101010111001001010000111010111101000101011010010110001010101011100100101000011101011110100010101101
00101100010101100010101010111001001010000111010111101000101011010010110001010101011100100101000011101011110100010101101
00101100010101100010101010101001001010000111010111101000101011010010110001010101010100100101000011101011110100010101101
00101100010101100010101010101001001010000111010111101000101011010010110001010101010100100101000011101011110100010101101
00101100010101100010101010111001001010000111010111101000101011010010110001010101011100100101000011101011110100010101101
00101100010101100010101010111001001010000111010111101000101011010010110001010101011100100101000011101011110100010101101
00101100000101100010101010111001001010000111010111101000101011010010110000010101011000100101000011101011110100010101101
00101100010101100010101010111001001010000111010111101000101011010010110001010101011100100101000011101011110100010101101
00101100010101100010101010111001001010000111010111101000101011010010110001010101011100100101000011101011110100010101101
00101100000101100010101010111001001010000111010111101000101011010010110000010101011100100101000011101011110100010101101
00101100010101100010101010111001001010000111010111101000101011010010110001010101011100100101000011101011110100010101101
00101100010101100010101010111001001010000111010111101000101011010010110001010101011100100101000011101011110100010101101
00101100010101100010101010111001001010000111010111101000101011010010110001010101011100100101000011101011110100010101101
00101100010101100010101010111001001010000111010111101000101011010010110001010101011100100101000011101011110100010101101
00101100010101100010101010111001001010000111010111101000101011010010110001010101011000100101000011101011110100010101100
00101100010101100010101010111001001010000111010111101000101011010010110001010101011100100101000011101011110100010101101
00101100000101100010101010111001001010000111010111101000101011010010110000010101011100100101000011101011110100010101101
00101100000101100010101010111001001010000111010111101000101011010010110000010101011100100101000011101011110100010101101
00101100010101100010101010111001001010000111010111101000101011010010110001010101011100100101000011101011110100010101100
00101100010101100010101010111001001010000111010111101000101011010010110001010101011000100101000011101011111100010101101
00101100010101100010101010111001001010000111010111101000101011010010110001010101011100100101000011101011110100010101101
00101100010101100010101010111001001010000111010111101000101011010010110001010101011100100101000011101011110100010101101
00101100010101100010101010111001001010000111010111101000101011010010110001010101011100100101000011101011110100010101100
00101100010101100010101010111001001010000111010111101000101011010010110001010101011100100101000011101011110100010101101
00101100010101100010101010111001001010000111010111101000101011010010110001010101011100100101000011101011110100010101101
00101100010101100010101010111001001010000111010111101000101011010010110001010101011100100101000011101011110100010101101
00101100010101100010101010111001001010000111010111101000101011010010110001010101011100100101000011101011110100010101101
00101100000101100010101010101001001010000111010111101000101011010010110001010101010100100101000011101011110100010101101
00101100010101100010101010111001001010000111010111101000101011010010110001010101011100100101000011101011110100010101101
00101100010101100010101010111001001010000111010111101000101011010010110001010101011100100101000011101011110100010101101
00101100010101100010101010111001001010000111010111101000101011010010110001010101011100100101000011101011110100010101101
00101100010101100010101010111001001010000111010111101000101011010010110001010101011100100101000011101011110100010101101
00101100000101100010101010111001001010000111010111101000101011010010110000010101011100100101000011101011110100010101101
00101100010101100010101010111001001010000111010111101000101011010010110001010101011100100101000011101011110100010101101
00101100000101100010101010111001001010000111010111101000101011010010110000010101011100100101000011101011110100010101100
00101100010101100010101010111001001010000111010111101000101011010010110001010101011100100101000011101011110100010101101

0010110001010110001010101011100100101000011101011110100010101101
0010110001010110001010101011000100101000011101011110100010101100
0010110001010110001010101011100100101000011101011110100010101101
0010110001010110001010101011000100101000011101011110100010101101
0010110000010110001010101011100100101000011101011110100010101101
0010110001010110001010101011100100101000011101011110100010101101
0010110001010110001010101011100100101000011101011110100010101101
0010110001010110001010101011100100101000011101011111100010101101
0010110001010110001010101011000100101000011101011110100010101101
0010110001010110001010101011100100101000011101011110100010101100
0010110001010110001010101011100100101000011101011110100010101101
0010110001010110001010101011100100101000011101011110100010101100
0010110000010110001010101011100100101000011101011110100010101101
0010110001010110001010101011100100101000011101011110100010101101
0010110000010110001010101011100100101000011101011110100010101101
0010110001010110001010101010100100101000011101011110100010101101
0010110000010110001010101011100100101000011101011110100010101100
0010110001010110001010101011100100101000011101011110100010101101
0010110000010110001010101011100100101000011101011110100010101101
0010110000010110001010101011100100101000011101011110100010101101
0010110001010110001010101011100100101000011101011110100010101101
0010110001010110001010101011000100101000011101011110100010101100
0010110000010110001010101011000100101000011101011110100010101101
0010110000010110001010101011000100101000011101011110100010101101
0010110000010110001010101011100100101000011101011110100010101101
0010110000010110001010101011100100101000011101011110100010101100
0010110001010110001010101011100100101000011101011110100010101101
0010110001010110001010101011000100101000011101011110100010101100
0010110001010110001010101011100100101000011101011110100010101101
0010110001010110001010101011100100101000011101011110100010101101
1000011010110000101101101111101111001110010001111010000010011110
1000011011110000101001101111001111001110010101111010000010011100
1000011010110000101001101111101111001110010000111010000010011111
1000011010110000101001101111001111001110010001111000000010011110
1000011011110000101001101111101111001110010000111010000010011100
1000011011110000101001101111101111001110010000111010000010011100
1000011011110000101001101111101111001110010000111010000010011100
1000011011110000101001101111101111001110010001111010000010011100
1000011011110000101001101111101111001110010001111011000010011100
1000011010110000101001101111101111001110010000111010000010011100
1000011011110000101001101111101111001110010000111010000010011100
1000011011110000101001101111101111001110010001111010000010011110
1000011011110000101001101111001111001110010001111010000010011100
1000011011110000101101101111101111001110010000111010000010011100

对于不同激励，PUF 产生的响应如下。

Data:2022.5.20

Recoder:Ge Wen Jie

PUF 电路激励响应对测试

激励	*响应*
74aaeabe66da35d8e59e2d035e03a191	0x86ffcc57ee47f2cd
b853d33738df565169f5d554caaf6618	0x26dc428d7d48f8ed
7952feb6abe6cf7410a5966fac82b50	0x2c562ab92875e8ad
c583b430be626bdbded972fb703f616c	0x86f0a6fbce57a09e
c6312e5eb48d5332ca46f5ac8717237e	0x347482d1f9659961
cd67bcc5208e38b7dc91f1cac00efd40	0x632acff585da8b0
4245493077891afec04dd4db62a827e	0xa4f4a097fb47b90e
9007ffa9e61f8aaf56cda202da5b50d	0x94d9c5b38f5fa935
a6256fd602437d242d671d840be8f20	0x86fa26ffdc41b844
2c6f1e06896dd6466500bff0e2ea354	0x86f649dbad5dfa69
3d2029be913e246f34ed486bf3972c65	0x1473c4bb885fe95c
14f01583247b2f93906bb4262147b775	0x9c9727d17b7db15b
e7363a203ac66f4715304066aa042125	0x247b89b96869c80e
7ffd601d2dbb925c943b0abc3f666b76	0x9cd60b314b7fe378
c8b054ee3408a26718ec55a8eb43d6e2	0x3e1285837a7db155
5a047342644c17d0d94e89b87ff4b5a4	0x9c9a80b3f845b921
bfebdcb79aa2f021c35bb8d835972fde	0xb474a7ffae74e2fd
b1db9a7d5aef297581f5aababd888ef	0x3cd10db32c79ab8d
43b77e8b15b1874b3ac62fcefd3641a	0x9edcc27d2b0fa02b
e420fe9ea6ca50edd634d2159b88fc48	0x34308bb5ea76d9a9
76baac8139cf7c9d485446d9aaec41ed	0x2ef1079f697ed2fa
d0e47d66562d5ef7d88a0929681f0105	0xa67baa33ad75b125
b277f18e734cebe4c9da3df7e7da8313	0x3cff8649d855f8b9
196f4e506949417bf8037d08550d4465	0xb6d3c9d7eb2faa22
fd0094a9bb5d857c4e0c0ba4342850	0x245660171b68e9de
f947c8337253fca1ca061ac8e29e4a83	0x6dbaa3fcf7ce89f
b888b416867fb6ac9c2a238095c32fb1	0x3e7f2e77a95ff399
3973aeff13349c065e4b589b6efc65c9	0x8ed123b71875e8e5
611333f27bfdd396b96b49ba8dc72588	0x1c5847a3f979e837
5a7220004826ac521a82fc42c4e8eb	0x8c51aeb9bc79b87a
1208e4eafe14095519c3e5fbc751bbc9	0x3e9181cb4c0cbbd5
52152ff0bd372246609116dea1a4b563	0x14936c1dc97db976
5661927ae65e709023d0387267bd0d13	0xb67fe57b6c79b9e7
dea38b81fefcda5c986bb3377ef8a203	0x8cfb27f1485bb09a
b9ac80bd5bb27e5342482c8c1f231261	0x96332375ba79e3bc
a29c9f73f3a625d387f1e94284e5a2	0x845ac1155a7ebb85
62da0d42fdf3b76392ad69e42aa01635	0xa61f2cf94b4df233
29a5e211aa149bed9da6c1d421d6437	0x86df86d52f0fb26e
a72a39bba78639b5ec756a833d6846e	0x9cd023932a6bea1f
ae34aaa01140f64c56c0d4da1fa2f429	0x9619019f0a5ff9cc
3efc28983b3389dddd4353a93d3e33de	0x9674a1b37b06d35a
5d500eb43b1402c7f7024b4067da600d	0xbcf9c8b77c25a92c
da94349482f36e743321cb8530dec851	0x8e57ecb58b7db118
eb017c0f1a4088948e3b512f432e50	0x9e7685d72a1de939
45402188c179922e336c0a89e684381f	0x241de5370b77896a
e2e9f0cd663213f9e8f239fd693c635d	0xb6f5e079ea66f3b0
6b810a63557c89d214d695b335ca12a3	0xbc3b8693a805e105
f89fc37cc5618b52c120ad94c5653f2a	0x3c38add52f0df2b4
71100a137b6133ecbbc5661961616c5	0xa41342f7ff67e909
3b044501688ef11dc39b8670100bc31b	0x847daf9bf866e91a

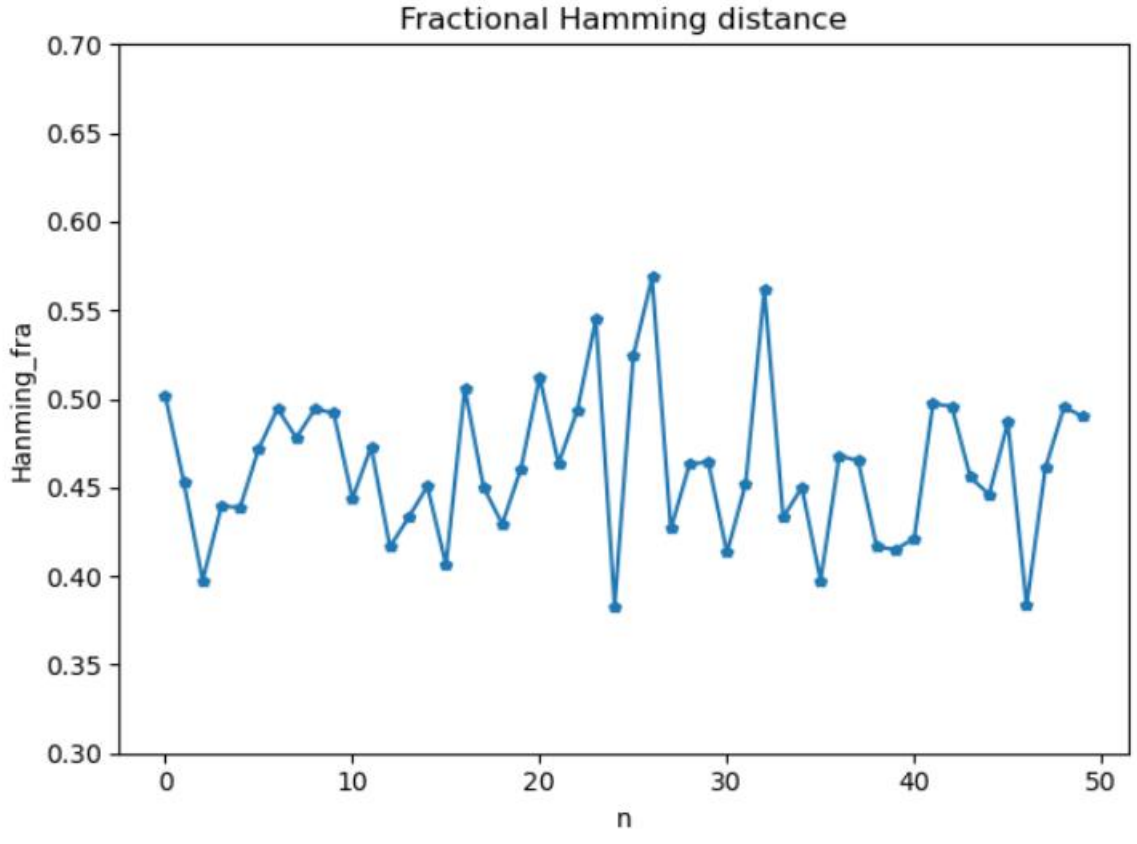
4.2.2 分数汉明距离

对每个激励读取 100 次响应并集中起来分析其中的“0”和“1”占的个数，并进行统计，得到以下结果：

激励	*分数汉明距离*
74aaeabe66da35d8e59e2d035e03a191	0.50203125
b853d33738df565169f5d554caaf6618	0.4528125
7952feb6abe6cf7410a5966fac82b50	0.3975
c583b430be626bdbded972fb703f616c	0.439375
c6312e5eb48d5332ca46f5ac8717237e	0.43875
cd67bcc5208e38b7dc91f1cac00efd40	0.47203125
4245493077891afec04dd4db62a827e	0.49453125
9007ffa9e61f8aaf56cda202da5b50d	0.47796875
a6256fd602437d242d671d840be8f20	0.494375
2c6f1e06896dd6466500bff0e2ea354	0.491875
3d2029be913e246f34ed486bf3972c65	0.44375
14f01583247b2f93906bb4262147b775	0.47296875
e7363a203ac66f4715304066aa042125	0.41640625
7ffd601d2dbb925c943b0abc3f666b76	0.433125
c8b054ee3408a26718ec55a8eb43d6e2	0.450625
5a047342644c17d0d94e89b87ff4b5a4	0.40625
bfebdcb79aa2f021c35bb8d835972fde	0.50609375
b1db9a7d5aef297581f5aababd888ef	0.45015625
43b77e8b15b1874b3ac62fcefd3641a	0.429375
e420fe9ea6ca50edd634d2159b88fc48	0.460625
76baac8139cf7c9d485446d9aaec41ed	0.51234375
d0e47d66562d5ef7d88a0929681f0105	0.4634375
b277f18e734cebe4c9da3df7e7da8313	0.493125
196f4e506949417bf8037d08550d4465	0.545
fd0094a9bb5d857c4e0c0ba4342850	0.38296875
f947c8337253fca1ca061ac8e29e4a83	0.524375
b888b416867fb6ac9c2a238095c32fb1	0.5684375
3973aeff13349c065e4b589b6efc65c9	0.4265625
611333f27bfdd396b96b49ba8dc72588	0.463125
5a7220004826ac521a82fc42c4e8eb	0.464375
1208e4eafe14095519c3e5fbc751bbc9	0.413125
52152ff0bd372246609116dea1a4b563	0.4521875
5661927ae65e709023d0387267bd0d13	0.56171875
dea38b81fefcda5c986bb3377ef8a203	0.433125
b9ac80bd5bb27e5342482c8c1f231261	0.45
a29c9f73f3a625d387f1e94284e5a2	0.3975
62da0d42fdf3b76392ad69e42aa01635	0.4678125
29a5e211aa149bed9da6c1d421d6437	0.46515625
a72a39bba78639b5ec756a833d6846e	0.41640625
ae34aaa01140f64c56c0d4da1fa2f429	0.415
3efc28983b3389dddd4353a93d3e33de	0.42125
5d500eb43b1402c7f7024b4067da600d	0.4971875
da94349482f36e743321cb8530dec851	0.49578125
eb017c0f1a4088948e3b512f432e50	0.455625
45402188c179922e336c0a89e684381f	0.44609375
e2e9f0cd663213f9e8f239fd693c635d	0.48671875
6b810a63557c89d214d695b335ca12a3	0.38328125
f89fc37cc5618b52c120ad94c5653f2a	0.46078125
71100a137b6133ecbbc5661961616c5	0.49546875
3b044501688ef11dc39b8670100bc31b	0.49

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

其图表描述如下：



4.2.3 片内汉明距离

对每个激励读取若干次响应后，求出该激励的片内汉明距离，最后对所有激励的片内汉明距离求平均，得到整体的平均片内汉明距离。

对于这样 50 组激励所采集到的片内汉明距离如下：

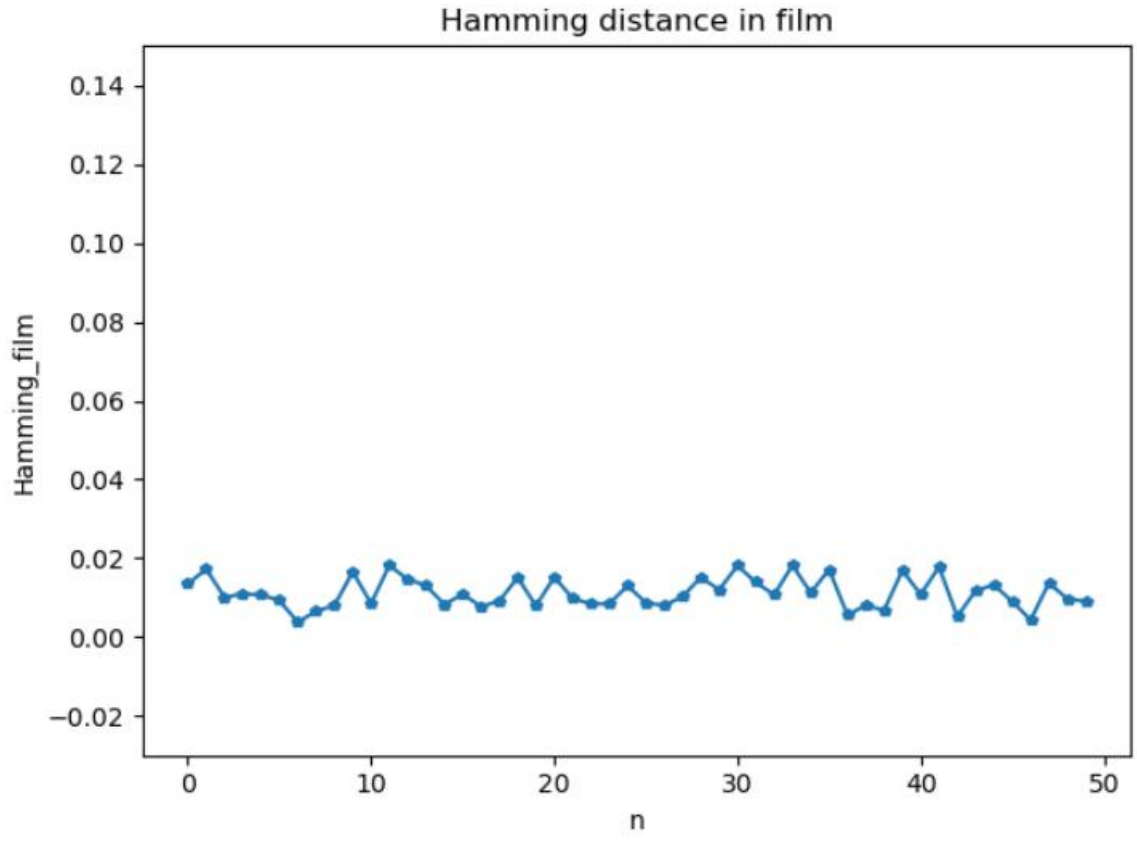
激励	*片内汉明距离*
74aaeabe66da35d8e59e2d035e03a191	0.013494318181818182
b853d33738df565169f5d554caaf6618	0.017238005050505052
7952feb6abe6cf7410a5966fac82b50	0.010129419191919191
c583b430be626bdbded972fb703f616c	0.010905934343434344
c6312e5eb48d5332ca46f5ac8717237e	0.010738636363636363
cd67bcc5208e38b7dc91f1cac00efd40	0.009242424242424243
4245493077891afec04dd4db62a827e	0.0037752525252525253
9007ffa9e61f8aaf56cda202da5b50d	0.006568813131313131
a6256fd602437d242d671d840be8f20	0.00800820707070707
2c6f1e06896dd6466500bff0e2ea354	0.01654040404040404
3d2029be913e246f34ed486bf3972c65	0.008525883838383838
14f01583247b2f93906bb4262147b775	0.01818181818181818
e7363a203ac66f4715304066aa042125	0.014627525252525253
7ffd601d2dbb925c943b0abc3f666b76	0.013093434343434343
c8b054ee3408a26718ec55a8eb43d6e2	0.00824810606060606
5a047342644c17d0d94e89b87ff4b5a4	0.010893308080808082
bfebdcb79aa2f021c35bb8d835972fde	0.007746212121212121
b1db9a7d5aef297581f5aababd888ef	0.009119318181818182
43b77e8b15b1874b3ac62fcefd3641a	0.015132575757575758
e420fe9ea6ca50edd634d2159b88fc48	0.00790719696969697

76baac8139cf7c9d485446d9aaec41ed	0.015208333333333334
d0e47d66562d5ef7d88a0929681f0105	0.009857954545454545
b277f18e734cebe4c9da3df7e7da8313	0.008352272727272727
196f4e506949417bf8037d08550d4465	0.00843118686868687
fd0094a9bb5d857c4e0c0ba4342850	0.013027146464646465
f947c8337253fca1ca061ac8e29e4a83	0.00869949494949495
b888b416867fb6ac9c2a238095c32fb1	0.008001893939393939
3973aeff13349c065e4b589b6efc65c9	0.010274621212121212
611333f27bfdd396b96b49ba8dc72588	0.01514520202020202
5a7220004826ac521a82fc42c4e8eb	0.012017045454545454
1208e4eafe14095519c3e5fbc751bbc9	0.018115530303030303
52152ff0bd372246609116dea1a4b563	0.013907828282828282
5661927ae65e709023d0387267bd0d13	0.010691287878787878
dea38b81fefcda5c986bb3377ef8a203	0.018216540404040405
b9ac80bd5bb27e5342482c8c1f231261	0.011237373737373737
a29c9f73f3a625d387f1e94284e5a2	0.017146464646464646
62da0d42fdf3b76392ad69e42aa01635	0.0056281565656565655
29a5e211aa149bed9da6c1d421d6437	0.008027146464646464
a72a39bba78639b5ec756a833d6846e	0.006799242424242425
ae34aaa01140f64c56c0d4da1fa2f429	0.016906565656565658
3efc28983b3389dddd4353a93d3e33de	0.010801767676767677
5d500eb43b1402c7f7024b4067da600d	0.01778093434343434
da94349482f36e743321cb8530dec851	0.005205176767676767
eb017c0f1a4088948e3b512f432e50	0.011811868686868687
45402188c179922e336c0a89e684381f	0.013200757575757576
e2e9f0cd663213f9e8f239fd693c635d	0.009037247474747474
6b810a63557c89d214d695b335ca12a3	0.004327651515151515
f89fc37cc5618b52c120ad94c5653f2a	0.013712121212121212
71100a137b6133ecbbc5661961616c5	0.009690656565656566
3b044501688ef11dc39b8670100bc31b	0.009075126262626262

由此得到平均片内汉明距离为:0.011209027777777776，即 1.12%

对不同激励的片

内汉明距离进行图表描述如下:



3.3 秘钥生成与重建测试

调用 BR_PUF_key_test 函数进行秘钥的生成与重建测试。

3.3.1 测试函数执行情况记录

```
--------------------KEY TEST START!!--------------------
-------------Set as build:-------------
-------------The Receive BUFs:-------------
10000110111111111100110001010111111011100100011111111001011001101
-------------------------------------------
-------------------------------------------
-------------The Receive Assistant data:-------------
 EE43C2CD,
86FFCC57,EEBC3DCD,86003357,EE43C2CD,790033A8,1143C232,79FFCCA8,EEBC3DCD,
86003357,11BC3D32,790033A8,11433DCD,8600CCA8,11BC3D32,86FFCC57,1143C232,
79FFCCA8,EEBCC232,79FF3357,1143C232,79FFCCA8,11BCC2CD,86FF33A8,11BCC2CD,
7900CC57,11BCC2CD,86FF33A8,EE433D32,7900CC57,1143C232,79FFCCA8,1143C232,
79FFCCA8,1143C232,86003357,11BCC2CD,7900CC57,EEBC3DCD,79FFCCA8,EEBCC232,
8600CCA8,EEBCC232,79FF3357,EE433D32,7900CC57,EEBCC232,79FF3357,11BC3D32,
86FFCC57,11BCC2CD,86FF33A8,11433DCD,79FF3357,11BCC2CD,86FF33A8,1143C232,
86003357,EEBC3DCD,86003357,EE43C2CD,86FFCC57,EEBC3DCD,79FFCCA8,
-----------------------------------------------------
-----------------------------------------------------
-------------The Receive SHA1 Dig:-------------
45FCCC234492FEAC821FBF0957388C809CFFF9D2
-----------------------------------------------
--------------------FINISH--------------------
-------------Set as rebuild:-------------
-------------The Rebuild SHA1 Dig:-------------
receive:45FCCC234492FEAC821FBF0957388C809CFFF9D2
rebuild:45FCCC234492FEAC821FBF0957388C809CFFF9D2
```

Check:rignt Total:1 rate:100
----------FINISH----------
----------The Rebuild SHA1 Dig:----------
receive:45FCCC234492FEAC821FBF0957388C809CFFF9D2
rebuild:45FCCC234492FEAC821FBF0957388C809CFFF9D2
Check:rignt Total:2 rate:100
----------FINISH----------
----------The Rebuild SHA1 Dig:----------
receive:45FCCC234492FEAC821FBF0957388C809CFFF9D2
rebuild:45FCCC234492FEAC821FBF0957388C809CFFF9D2
Check:rignt Total:3 rate:100
----------FINISH----------
----------The Rebuild SHA1 Dig:----------
receive:45FCCC234492FEAC821FBF0957388C809CFFF9D2
rebuild:45FCCC234492FEAC821FBF0957388C809CFFF9D2
Check:rignt Total:4 rate:100
----------FINISH----------
----------The Rebuild SHA1 Dig:----------
receive:45FCCC234492FEAC821FBF0957388C809CFFF9D2
rebuild:45FCCC234492FEAC821FBF0957388C809CFFF9D2
Check:rignt Total:5 rate:100
----------FINISH----------
----------The Rebuild SHA1 Dig:----------
receive:45FCCC234492FEAC821FBF0957388C809CFFF9D2
rebuild:45FCCC234492FEAC821FBF0957388C809CFFF9D2
Check:rignt Total:6 rate:100
----------FINISH----------
----------The Rebuild SHA1 Dig:----------
receive:45FCCC234492FEAC821FBF0957388C809CFFF9D2
rebuild:45FCCC234492FEAC821FBF0957388C809CFFF9D2
Check:rignt Total:7 rate:100
----------FINISH----------
----------The Rebuild SHA1 Dig:----------
receive:45FCCC234492FEAC821FBF0957388C809CFFF9D2
rebuild:45FCCC234492FEAC821FBF0957388C809CFFF9D2
Check:rignt Total:8 rate:100
----------FINISH----------
----------The Rebuild SHA1 Dig:----------
receive:45FCCC234492FEAC821FBF0957388C809CFFF9D2
rebuild:45FCCC234492FEAC821FBF0957388C809CFFF9D2
Check:rignt Total:9 rate:100
----------FINISH----------
----------The Rebuild SHA1 Dig:----------
receive:45FCCC234492FEAC821FBF0957388C809CFFF9D2
rebuild:45FCCC234492FEAC821FBF0957388C809CFFF9D2
Check:rignt Total:10 rate:100
----------FINISH----------
----------The Rebuild SHA1 Dig:----------
receive:45FCCC234492FEAC821FBF0957388C809CFFF9D2
rebuild:45FCCC234492FEAC821FBF0957388C809CFFF9D2
Check:rignt Total:11 rate:100
----------FINISH----------
----------The Rebuild SHA1 Dig:----------
receive:45FCCC234492FEAC821FBF0957388C809CFFF9D2
rebuild:45FCCC234492FEAC821FBF0957388C809CFFF9D2

Check:rignt Total:12 rate:100
----------FINISH----------
----------The Rebuild SHA1 Dig:----------
receive:45FCCC234492FEAC821FBF0957388C809CFFF9D2
rebuild:45FCCC234492FEAC821FBF0957388C809CFFF9D2
Check:rignt Total:13 rate:100
----------FINISH----------
----------The Rebuild SHA1 Dig:----------
receive:45FCCC234492FEAC821FBF0957388C809CFFF9D2
rebuild:45FCCC234492FEAC821FBF0957388C809CFFF9D2
Check:rignt Total:14 rate:100
----------FINISH----------
----------The Rebuild SHA1 Dig:----------
receive:45FCCC234492FEAC821FBF0957388C809CFFF9D2
rebuild:45FCCC234492FEAC821FBF0957388C809CFFF9D2
Check:rignt Total:15 rate:100
----------FINISH----------
----------The Rebuild SHA1 Dig:----------
receive:45FCCC234492FEAC821FBF0957388C809CFFF9D2
rebuild:45FCCC234492FEAC821FBF0957388C809CFFF9D2
Check:rignt Total:16 rate:100
----------FINISH----------
----------The Rebuild SHA1 Dig:----------
receive:45FCCC234492FEAC821FBF0957388C809CFFF9D2
rebuild:45FCCC234492FEAC821FBF0957388C809CFFF9D2
Check:rignt Total:17 rate:100
----------FINISH----------
----------The Rebuild SHA1 Dig:----------
receive:45FCCC234492FEAC821FBF0957388C809CFFF9D2
rebuild:45FCCC234492FEAC821FBF0957388C809CFFF9D2
Check:rignt Total:18 rate:100
----------FINISH----------
----------The Rebuild SHA1 Dig:----------
receive:45FCCC234492FEAC821FBF0957388C809CFFF9D2
rebuild:45FCCC234492FEAC821FBF0957388C809CFFF9D2
Check:rignt Total:19 rate:100
----------FINISH----------
----------The Rebuild SHA1 Dig:----------
receive:45FCCC234492FEAC821FBF0957388C809CFFF9D2
rebuild:45FCCC234492FEAC821FBF0957388C809CFFF9D2
Check:rignt Total:20 rate:100
----------FINISH----------
----------The Rebuild SHA1 Dig:----------
receive:45FCCC234492FEAC821FBF0957388C809CFFF9D2
rebuild:45FCCC234492FEAC821FBF0957388C809CFFF9D2
Check:rignt Total:21 rate:100
----------FINISH----------
----------The Rebuild SHA1 Dig:----------
receive:45FCCC234492FEAC821FBF0957388C809CFFF9D2
rebuild:45FCCC234492FEAC821FBF0957388C809CFFF9D2
Check:rignt Total:22 rate:100
----------FINISH----------
----------The Rebuild SHA1 Dig:----------
receive:45FCCC234492FEAC821FBF0957388C809CFFF9D2
rebuild:45FCCC234492FEAC821FBF0957388C809CFFF9D2

Check:rignt Total:23 rate:100
----------FINISH----------
----------The Rebuild SHA1 Dig:----------
receive:45FCCC234492FEAC821FBF0957388C809CFFF9D2
rebuild:45FCCC234492FEAC821FBF0957388C809CFFF9D2
Check:rignt Total:24 rate:100
----------FINISH----------
----------The Rebuild SHA1 Dig:----------
receive:45FCCC234492FEAC821FBF0957388C809CFFF9D2
rebuild:45FCCC234492FEAC821FBF0957388C809CFFF9D2
Check:rignt Total:25 rate:100
----------FINISH----------
----------The Rebuild SHA1 Dig:----------
receive:45FCCC234492FEAC821FBF0957388C809CFFF9D2
rebuild:45FCCC234492FEAC821FBF0957388C809CFFF9D2
Check:rignt Total:26 rate:100
----------FINISH----------
----------The Rebuild SHA1 Dig:----------
receive:45FCCC234492FEAC821FBF0957388C809CFFF9D2
rebuild:45FCCC234492FEAC821FBF0957388C809CFFF9D2
Check:rignt Total:27 rate:100
----------FINISH----------
----------The Rebuild SHA1 Dig:----------
receive:45FCCC234492FEAC821FBF0957388C809CFFF9D2
rebuild:45FCCC234492FEAC821FBF0957388C809CFFF9D2
Check:rignt Total:28 rate:100
----------FINISH----------
----------The Rebuild SHA1 Dig:----------
receive:45FCCC234492FEAC821FBF0957388C809CFFF9D2
rebuild:45FCCC234492FEAC821FBF0957388C809CFFF9D2
Check:rignt Total:29 rate:100
----------FINISH----------
----------The Rebuild SHA1 Dig:----------
receive:45FCCC234492FEAC821FBF0957388C809CFFF9D2
rebuild:45FCCC234492FEAC821FBF0957388C809CFFF9D2
Check:rignt Total:30 rate:100
----------FINISH----------
----------The Rebuild SHA1 Dig:----------
receive:45FCCC234492FEAC821FBF0957388C809CFFF9D2
rebuild:45FCCC234492FEAC821FBF0957388C809CFFF9D2
Check:rignt Total:31 rate:100
----------FINISH----------
----------The Rebuild SHA1 Dig:----------
receive:45FCCC234492FEAC821FBF0957388C809CFFF9D2
rebuild:45FCCC234492FEAC821FBF0957388C809CFFF9D2
Check:rignt Total:32 rate:100
----------FINISH----------
----------The Rebuild SHA1 Dig:----------
receive:45FCCC234492FEAC821FBF0957388C809CFFF9D2
rebuild:45FCCC234492FEAC821FBF0957388C809CFFF9D2
Check:rignt Total:33 rate:100
----------FINISH----------
----------The Rebuild SHA1 Dig:----------
receive:45FCCC234492FEAC821FBF0957388C809CFFF9D2
rebuild:45FCCC234492FEAC821FBF0957388C809CFFF9D2

Check:rignt Total:34 rate:100
----------FINISH----------
----------The Rebuild SHA1 Dig:----------
receive:45FCCC234492FEAC821FBF0957388C809CFFF9D2
rebuild:45FCCC234492FEAC821FBF0957388C809CFFF9D2
Check:rignt Total:35 rate:100
----------FINISH----------
----------The Rebuild SHA1 Dig:----------
receive:45FCCC234492FEAC821FBF0957388C809CFFF9D2
rebuild:45FCCC234492FEAC821FBF0957388C809CFFF9D2
Check:rignt Total:36 rate:100
----------FINISH----------
----------The Rebuild SHA1 Dig:----------
receive:45FCCC234492FEAC821FBF0957388C809CFFF9D2
rebuild:45FCCC234492FEAC821FBF0957388C809CFFF9D2
Check:rignt Total:37 rate:100
----------FINISH----------
----------The Rebuild SHA1 Dig:----------
receive:45FCCC234492FEAC821FBF0957388C809CFFF9D2
rebuild:45FCCC234492FEAC821FBF0957388C809CFFF9D2
Check:rignt Total:38 rate:100
----------FINISH----------
----------The Rebuild SHA1 Dig:----------
receive:45FCCC234492FEAC821FBF0957388C809CFFF9D2
rebuild:45FCCC234492FEAC821FBF0957388C809CFFF9D2
Check:rignt Total:39 rate:100
----------FINISH----------
----------The Rebuild SHA1 Dig:----------
receive:45FCCC234492FEAC821FBF0957388C809CFFF9D2
rebuild:45FCCC234492FEAC821FBF0957388C809CFFF9D2
Check:rignt Total:40 rate:100
----------FINISH----------
----------The Rebuild SHA1 Dig:----------
receive:45FCCC234492FEAC821FBF0957388C809CFFF9D2
rebuild:45FCCC234492FEAC821FBF0957388C809CFFF9D2
Check:rignt Total:41 rate:100
----------FINISH----------
----------The Rebuild SHA1 Dig:----------
receive:45FCCC234492FEAC821FBF0957388C809CFFF9D2
rebuild:45FCCC234492FEAC821FBF0957388C809CFFF9D2
Check:rignt Total:42 rate:100
----------FINISH----------
----------The Rebuild SHA1 Dig:----------
receive:45FCCC234492FEAC821FBF0957388C809CFFF9D2
rebuild:45FCCC234492FEAC821FBF0957388C809CFFF9D2
Check:rignt Total:43 rate:100
----------FINISH----------
----------The Rebuild SHA1 Dig:----------
receive:45FCCC234492FEAC821FBF0957388C809CFFF9D2
rebuild:45FCCC234492FEAC821FBF0957388C809CFFF9D2
Check:rignt Total:44 rate:100
----------FINISH----------
----------The Rebuild SHA1 Dig:----------
receive:45FCCC234492FEAC821FBF0957388C809CFFF9D2
rebuild:45FCCC234492FEAC821FBF0957388C809CFFF9D2

Check:rignt Total:45 rate:100
----------FINISH----------
----------The Rebuild SHA1 Dig:----------
receive:45FCCC234492FEAC821FBF0957388C809CFFF9D2
rebuild:45FCCC234492FEAC821FBF0957388C809CFFF9D2
Check:rignt Total:46 rate:100
----------FINISH----------
----------The Rebuild SHA1 Dig:----------
receive:45FCCC234492FEAC821FBF0957388C809CFFF9D2
rebuild:45FCCC234492FEAC821FBF0957388C809CFFF9D2
Check:rignt Total:47 rate:100
----------FINISH----------
----------The Rebuild SHA1 Dig:----------
receive:45FCCC234492FEAC821FBF0957388C809CFFF9D2
rebuild:45FCCC234492FEAC821FBF0957388C809CFFF9D2
Check:rignt Total:48 rate:100
----------FINISH----------
----------The Rebuild SHA1 Dig:----------
receive:45FCCC234492FEAC821FBF0957388C809CFFF9D2
rebuild:45FCCC234492FEAC821FBF0957388C809CFFF9D2
Check:rignt Total:49 rate:100
----------FINISH----------
----------The Rebuild SHA1 Dig:----------
receive:45FCCC234492FEAC821FBF0957388C809CFFF9D2
rebuild:45FCCC234492FEAC821FBF0957388C809CFFF9D2
Check:rignt Total:50 rate:100
----------FINISH----------
----------The Rebuild SHA1 Dig:----------
receive:45FCCC234492FEAC821FBF0957388C809CFFF9D2
rebuild:45FCCC234492FEAC821FBF0957388C809CFFF9D2
Check:rignt Total:51 rate:100
----------FINISH----------
----------The Rebuild SHA1 Dig:----------
receive:45FCCC234492FEAC821FBF0957388C809CFFF9D2
rebuild:45FCCC234492FEAC821FBF0957388C809CFFF9D2
Check:rignt Total:52 rate:100
----------FINISH----------
----------The Rebuild SHA1 Dig:----------
receive:45FCCC234492FEAC821FBF0957388C809CFFF9D2
rebuild:45FCCC234492FEAC821FBF0957388C809CFFF9D2
Check:rignt Total:53 rate:100
----------FINISH----------
----------The Rebuild SHA1 Dig:----------
receive:45FCCC234492FEAC821FBF0957388C809CFFF9D2
rebuild:45FCCC234492FEAC821FBF0957388C809CFFF9D2
Check:rignt Total:54 rate:100
----------FINISH----------
----------The Rebuild SHA1 Dig:----------
receive:45FCCC234492FEAC821FBF0957388C809CFFF9D2
rebuild:45FCCC234492FEAC821FBF0957388C809CFFF9D2
Check:rignt Total:55 rate:100
----------FINISH----------
----------The Rebuild SHA1 Dig:----------
receive:45FCCC234492FEAC821FBF0957388C809CFFF9D2
rebuild:45FCCC234492FEAC821FBF0957388C809CFFF9D2

Check:rignt Total:56 rate:100
----------FINISH----------
----------The Rebuild SHA1 Dig:----------
receive:45FCCC234492FEAC821FBF0957388C809CFFF9D2
rebuild:45FCCC234492FEAC821FBF0957388C809CFFF9D2
Check:rignt Total:57 rate:100
----------FINISH----------
----------The Rebuild SHA1 Dig:----------
receive:45FCCC234492FEAC821FBF0957388C809CFFF9D2
rebuild:45FCCC234492FEAC821FBF0957388C809CFFF9D2
Check:rignt Total:58 rate:100
----------FINISH----------
----------The Rebuild SHA1 Dig:----------
receive:45FCCC234492FEAC821FBF0957388C809CFFF9D2
rebuild:45FCCC234492FEAC821FBF0957388C809CFFF9D2
Check:rignt Total:59 rate:100
----------FINISH----------
----------The Rebuild SHA1 Dig:----------
receive:45FCCC234492FEAC821FBF0957388C809CFFF9D2
rebuild:45FCCC234492FEAC821FBF0957388C809CFFF9D2
Check:rignt Total:60 rate:100
----------FINISH----------
----------The Rebuild SHA1 Dig:----------
receive:45FCCC234492FEAC821FBF0957388C809CFFF9D2
rebuild:45FCCC234492FEAC821FBF0957388C809CFFF9D2
Check:rignt Total:61 rate:100
----------FINISH----------
----------The Rebuild SHA1 Dig:----------
receive:45FCCC234492FEAC821FBF0957388C809CFFF9D2
rebuild:45FCCC234492FEAC821FBF0957388C809CFFF9D2
Check:rignt Total:62 rate:100
----------FINISH----------
----------The Rebuild SHA1 Dig:----------
receive:45FCCC234492FEAC821FBF0957388C809CFFF9D2
rebuild:45FCCC234492FEAC821FBF0957388C809CFFF9D2
Check:rignt Total:63 rate:100
----------FINISH----------
----------The Rebuild SHA1 Dig:----------
receive:45FCCC234492FEAC821FBF0957388C809CFFF9D2
rebuild:45FCCC234492FEAC821FBF0957388C809CFFF9D2
Check:rignt Total:64 rate:100
----------FINISH----------
----------The Rebuild SHA1 Dig:----------
receive:45FCCC234492FEAC821FBF0957388C809CFFF9D2
rebuild:45FCCC234492FEAC821FBF0957388C809CFFF9D2
Check:rignt Total:65 rate:100
----------FINISH----------
----------The Rebuild SHA1 Dig:----------
receive:45FCCC234492FEAC821FBF0957388C809CFFF9D2
rebuild:45FCCC234492FEAC821FBF0957388C809CFFF9D2
Check:rignt Total:66 rate:100
----------FINISH----------
----------The Rebuild SHA1 Dig:----------
receive:45FCCC234492FEAC821FBF0957388C809CFFF9D2
rebuild:45FCCC234492FEAC821FBF0957388C809CFFF9D2

Check:rignt Total:67 rate:100
----------FINISH----------
----------The Rebuild SHA1 Dig:----------
receive:45FCCC234492FEAC821FBF0957388C809CFFF9D2
rebuild:45FCCC234492FEAC821FBF0957388C809CFFF9D2
Check:rignt Total:68 rate:100
----------FINISH----------
----------The Rebuild SHA1 Dig:----------
receive:45FCCC234492FEAC821FBF0957388C809CFFF9D2
rebuild:45FCCC234492FEAC821FBF0957388C809CFFF9D2
Check:rignt Total:69 rate:100
----------FINISH----------
----------The Rebuild SHA1 Dig:----------
receive:45FCCC234492FEAC821FBF0957388C809CFFF9D2
rebuild:45FCCC234492FEAC821FBF0957388C809CFFF9D2
Check:rignt Total:70 rate:100
----------FINISH----------
----------The Rebuild SHA1 Dig:----------
receive:45FCCC234492FEAC821FBF0957388C809CFFF9D2
rebuild:45FCCC234492FEAC821FBF0957388C809CFFF9D2
Check:rignt Total:71 rate:100
----------FINISH----------
----------The Rebuild SHA1 Dig:----------
receive:45FCCC234492FEAC821FBF0957388C809CFFF9D2
rebuild:45FCCC234492FEAC821FBF0957388C809CFFF9D2
Check:rignt Total:72 rate:100
----------FINISH----------
----------The Rebuild SHA1 Dig:----------
receive:45FCCC234492FEAC821FBF0957388C809CFFF9D2
rebuild:45FCCC234492FEAC821FBF0957388C809CFFF9D2
Check:rignt Total:73 rate:100
----------FINISH----------
----------The Rebuild SHA1 Dig:----------
receive:45FCCC234492FEAC821FBF0957388C809CFFF9D2
rebuild:45FCCC234492FEAC821FBF0957388C809CFFF9D2
Check:rignt Total:74 rate:100
----------FINISH----------
----------The Rebuild SHA1 Dig:----------
receive:45FCCC234492FEAC821FBF0957388C809CFFF9D2
rebuild:45FCCC234492FEAC821FBF0957388C809CFFF9D2
Check:rignt Total:75 rate:100
----------FINISH----------
----------The Rebuild SHA1 Dig:----------
receive:45FCCC234492FEAC821FBF0957388C809CFFF9D2
rebuild:45FCCC234492FEAC821FBF0957388C809CFFF9D2
Check:rignt Total:76 rate:100
----------FINISH----------
----------The Rebuild SHA1 Dig:----------
receive:45FCCC234492FEAC821FBF0957388C809CFFF9D2
rebuild:45FCCC234492FEAC821FBF0957388C809CFFF9D2
Check:rignt Total:77 rate:100
----------FINISH----------
----------The Rebuild SHA1 Dig:----------
receive:45FCCC234492FEAC821FBF0957388C809CFFF9D2
rebuild:45FCCC234492FEAC821FBF0957388C809CFFF9D2

Check:rignt Total:78 rate:100
----------FINISH----------
----------The Rebuild SHA1 Dig:----------
receive:45FCCC234492FEAC821FBF0957388C809CFFF9D2
rebuild:45FCCC234492FEAC821FBF0957388C809CFFF9D2
Check:rignt Total:79 rate:100
----------FINISH----------
----------The Rebuild SHA1 Dig:----------
receive:45FCCC234492FEAC821FBF0957388C809CFFF9D2
rebuild:45FCCC234492FEAC821FBF0957388C809CFFF9D2
Check:rignt Total:80 rate:100
----------FINISH----------
----------The Rebuild SHA1 Dig:----------
receive:45FCCC234492FEAC821FBF0957388C809CFFF9D2
rebuild:45FCCC234492FEAC821FBF0957388C809CFFF9D2
Check:rignt Total:81 rate:100
----------FINISH----------
----------The Rebuild SHA1 Dig:----------
receive:45FCCC234492FEAC821FBF0957388C809CFFF9D2
rebuild:45FCCC234492FEAC821FBF0957388C809CFFF9D2
Check:rignt Total:82 rate:100
----------FINISH----------
----------The Rebuild SHA1 Dig:----------
receive:45FCCC234492FEAC821FBF0957388C809CFFF9D2
rebuild:45FCCC234492FEAC821FBF0957388C809CFFF9D2
Check:rignt Total:83 rate:100
----------FINISH----------
----------The Rebuild SHA1 Dig:----------
receive:45FCCC234492FEAC821FBF0957388C809CFFF9D2
rebuild:45FCCC234492FEAC821FBF0957388C809CFFF9D2
Check:rignt Total:84 rate:100
----------FINISH----------
----------The Rebuild SHA1 Dig:----------
receive:45FCCC234492FEAC821FBF0957388C809CFFF9D2
rebuild:45FCCC234492FEAC821FBF0957388C809CFFF9D2
Check:rignt Total:85 rate:100
----------FINISH----------
----------The Rebuild SHA1 Dig:----------
receive:45FCCC234492FEAC821FBF0957388C809CFFF9D2
rebuild:45FCCC234492FEAC821FBF0957388C809CFFF9D2
Check:rignt Total:86 rate:100
----------FINISH----------
----------The Rebuild SHA1 Dig:----------
receive:45FCCC234492FEAC821FBF0957388C809CFFF9D2
rebuild:45FCCC234492FEAC821FBF0957388C809CFFF9D2
Check:rignt Total:87 rate:100
----------FINISH----------
----------The Rebuild SHA1 Dig:----------
receive:45FCCC234492FEAC821FBF0957388C809CFFF9D2
rebuild:45FCCC234492FEAC821FBF0957388C809CFFF9D2
Check:rignt Total:88 rate:100
----------FINISH----------
----------The Rebuild SHA1 Dig:----------
receive:45FCCC234492FEAC821FBF0957388C809CFFF9D2
rebuild:45FCCC234492FEAC821FBF0957388C809CFFF9D2

Check:rignt Total:89 rate:100
----------FINISH----------
----------The Rebuild SHA1 Dig:----------
receive:45FCCC234492FEAC821FBF0957388C809CFFF9D2
rebuild:45FCCC234492FEAC821FBF0957388C809CFFF9D2
Check:rignt Total:90 rate:100
----------FINISH----------
----------The Rebuild SHA1 Dig:----------
receive:45FCCC234492FEAC821FBF0957388C809CFFF9D2
rebuild:45FCCC234492FEAC821FBF0957388C809CFFF9D2
Check:rignt Total:91 rate:100
----------FINISH----------
----------The Rebuild SHA1 Dig:----------
receive:45FCCC234492FEAC821FBF0957388C809CFFF9D2
rebuild:45FCCC234492FEAC821FBF0957388C809CFFF9D2
Check:rignt Total:92 rate:100
----------FINISH----------
----------The Rebuild SHA1 Dig:----------
receive:45FCCC234492FEAC821FBF0957388C809CFFF9D2
rebuild:45FCCC234492FEAC821FBF0957388C809CFFF9D2
Check:rignt Total:93 rate:100
----------FINISH----------
----------The Rebuild SHA1 Dig:----------
receive:45FCCC234492FEAC821FBF0957388C809CFFF9D2
rebuild:45FCCC234492FEAC821FBF0957388C809CFFF9D2
Check:rignt Total:94 rate:100
----------FINISH----------
----------The Rebuild SHA1 Dig:----------
receive:45FCCC234492FEAC821FBF0957388C809CFFF9D2
rebuild:45FCCC234492FEAC821FBF0957388C809CFFF9D2
Check:rignt Total:95 rate:100
----------FINISH----------
----------The Rebuild SHA1 Dig:----------
receive:45FCCC234492FEAC821FBF0957388C809CFFF9D2
rebuild:45FCCC234492FEAC821FBF0957388C809CFFF9D2
Check:rignt Total:96 rate:100
----------FINISH----------
----------The Rebuild SHA1 Dig:----------
receive:45FCCC234492FEAC821FBF0957388C809CFFF9D2
rebuild:45FCCC234492FEAC821FBF0957388C809CFFF9D2
Check:rignt Total:97 rate:100
----------FINISH----------
----------The Rebuild SHA1 Dig:----------
receive:45FCCC234492FEAC821FBF0957388C809CFFF9D2
rebuild:45FCCC234492FEAC821FBF0957388C809CFFF9D2
Check:rignt Total:98 rate:100
----------FINISH----------
----------The Rebuild SHA1 Dig:----------
receive:45FCCC234492FEAC821FBF0957388C809CFFF9D2
rebuild:45FCCC234492FEAC821FBF0957388C809CFFF9D2
Check:rignt Total:99 rate:100
----------FINISH----------
----------The Rebuild SHA1 Dig:----------
receive:45FCCC234492FEAC821FBF0957388C809CFFF9D2
rebuild:45FCCC234492FEAC821FBF0957388C809CFFF9D2

```
Check:rignt Total:100 rate:100
------------------FINISH------------------
------------------KEY TEST FINISH!!------------------
```

3.3.2 秘钥重建正确率

据运行情况来看，在 100 次的秘钥重建过程中，正确率达到了 100%。

4.4 随机数测试

调取 BR_PUF_random_test 函数进行多轮测试。

4.4.1 测试函数执行情况记录

轮次 1：

```
------------------RANDOM TEST START!!------------------
------------------RANDOM in range (-128~127)!!------------------
-2,
-30,
29,
89,
111,
-32,
38,
-19,
34,
58,
12,
55,
4,
2,
-29,
-38,
-28,
-92,
117,
-83,
43,
-16,
-32,
-45,
59,
-76,
-72,
-79,
75,
-41,
-104,
-27,
-126,
-35,
-100,
```

-10,
48,
-77,
123,
-46,
22,
-30,
83,
4,
7,
-68,
82,
118,
-96,
57,
-46,
91,
-37,
-120,
30,
-110,
88,
54,
-107,
-116,
-101,
-92,
112,
-44,
-63,
91,
-5,
51,
37,
-113,
34,
6,
-105,
108,
66,
55,
115,
66,
-99,
105,
-27,
82,
-103,
-17,
119,
-112,
70,
-123,
-49,
-36,

41,
8,
115,
83,
24,
-92,
84,
-6,
37,
80,
----------RANDOM in range (-32768~32768)!!----------
-30819,
-15848,
-28946,
-21739,
-4951,
-14434,
25966,
6761,
-359,
-21807,
-5638,
20076,
11398,
-32616,
-26030,
-10590,
-17645,
-9561,
-7095,
28150,
-4877,
-19049,
-17015,
-9553,
-2786,
9934,
28325,
30535,
-794,
-22653,
-15051,
-2945,
-547,
23578,
14161,
21985,
32139,
-5233,
21299,
-5365,
-14991,
11860,
23937,
356,

30023,
-11899,
-1537,
-30246,
-4480,
-300,
20323,
12942,
-14468,
13038,
12501,
18830,
-15264,
-13189,
19175,
-22402,
12219,
21077,
23752,
-6612,
-9372,
21075,
-17851,
8861,
-11205,
-11661,
-21371,
22832,
-20026,
6881,
8702,
11900,
22110,
-10256,
4097,
-7021,
22392,
-246,
18850,
22509,
14686,
16417,
30383,
6901,
25607,
-30758,
4331,
691,
26443,
-32707,
-23153,
19337,
-15015,
-21903,
27610,

-1060,
----------RANDOM in range (-2147483646~2147483647)!!----------
-1575541946,
-503387164,
1187439466,
1124986635,
-234471525,
524970406,
615474310,
-1569634587,
-1032107595,
277674240,
126351679,
234922037,
-1769949119,
-1409461956,
-122881742,
1624962668,
-1764971751,
-1584159402,
-608465671,
-1360670146,
640689445,
-3968309,
-16737972,
1524430264,
1429579924,
-1212834699,
731232859,
-163838830,
-135198561,
1426961212,
1453396295,
-1151124499,
-1422031468,
-1321123258,
231076372,
1660276205,
1144396496,
576744521,
-1067620916,
1110241335,
-2025712925,
37615417,
-1926834824,
1104562989,
1276862151,
-815723327,
-204245030,
982308432,
890444786,
1835795058,
-380361006,
1444604600,
2091261886,

-30766334,
1929711241,
-768888203,
158803568,
870784505,
290421572,
780142925,
-269823009,
1486320461,
1355618220,
-1088897547,
656439567,
385450134,
289704093,
458663970,
632911758,
-29776312,
-2147407420,
155190791,
232541361,
1319914213,
1860063627,
-1655212135,
-141087601,
767767630,
-812450225,
1967643511,
1339061260,
1659633159,
-590845778,
1164458459,
-1632728947,
525484348,
-2123087826,
825339875,
1175922364,
-1526814217,
1643294909,
-649232887,
-401306197,
107420590,
1249487655,
-352729911,
-1072684873,
1317771465,
952054602,
1991683865,
----------RANDOM TEST FINISH!!----------
轮次 2：

----------RANDOM TEST START!!----------
----------RANDOM in range (-128~127)!!----------
-2,
-30,
29,

89,
-81,
-96,
22,
-3,
-90,
54,
127,
-116,
81,
60,
-116,
-92,
125,
-8,
-86,
-26,
107,
-96,
127,
-128,
-85,
61,
-120,
-33,
78,
28,
115,
16,
24,
104,
-47,
74,
-36,
62,
33,
13,
-70,
-70,
105,
13,
113,
64,
58,
-53,
-53,
-103,
-71,
106,
70,
74,
-71,
62,
-11,
16,

-118,
4,
-23,
56,
-9,
93,
-78,
16,
51,
-28,
-46,
44,
7,
42,
70,
-79,
13,
36,
-58,
66,
-113,
-8,
54,
-51,
-116,
-94,
-55,
71,
42,
11,
-4,
16,
89,
-17,
125,
-75,
113,
48,
74,
-111,
-67,
-31,
----------RANDOM in range (-32768~32768)!!----------
-18138,
-12810,
4119,
8885,
5272,
22975,
-26517,
15713,
29467,
-4286,
-472,
1271,

31917,
-26916,
-27002,
-26455,
-19996,
5959,
29391,
-30117,
32587,
-28255,
-3229,
27761,
-1939,
-1070,
23576,
6957,
27099,
5380,
-10920,
-7196,
-27845,
-27434,
25200,
-20298,
11032,
-4776,
-1336,
415,
19979,
26406,
10166,
8710,
20911,
16054,
3355,
21960,
11272,
16411,
28811,
-26942,
-6310,
-19392,
12994,
-6946,
-16562,
10659,
27201,
-10301,
1680,
21874,
7456,
-29046,
4323,
-20873,
-29394,

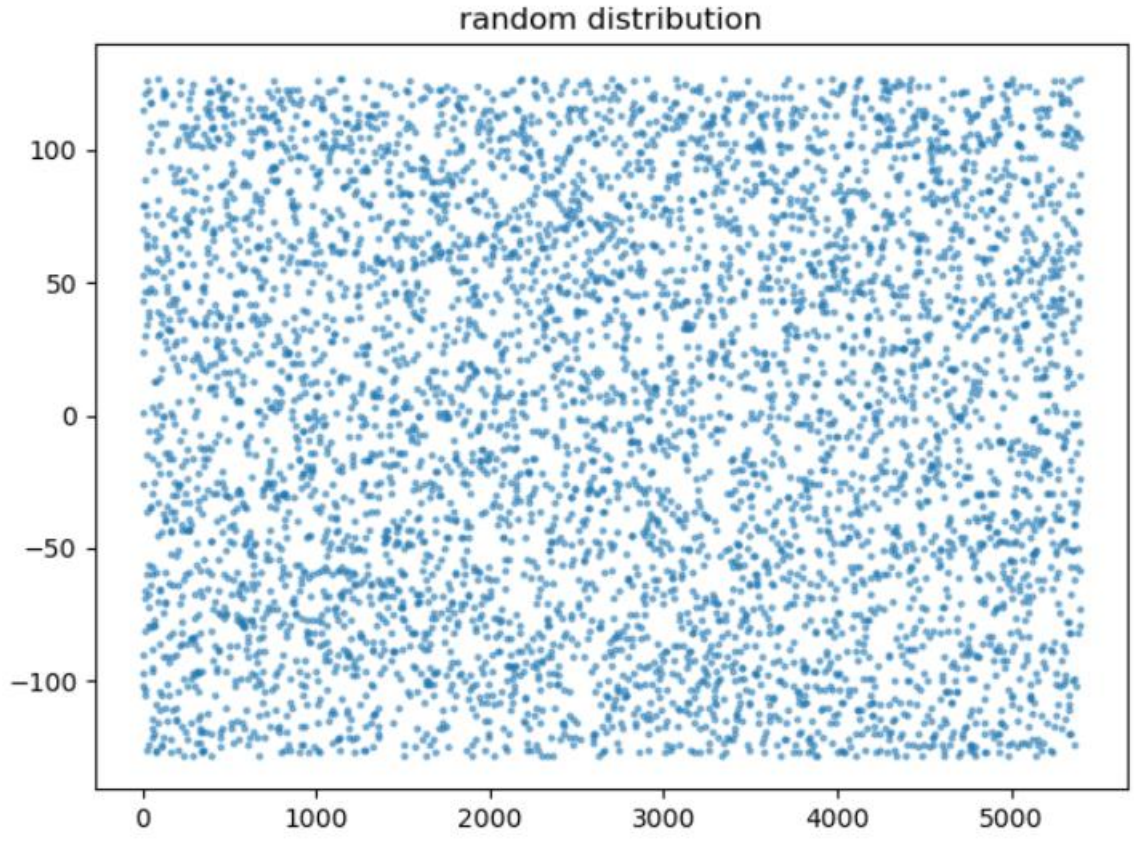
-27513,
23860,
-6379,
-31306,
19441,
-25904,
-7872,
-28969,
6601,
30337,
2039,
14821,
-16932,
-31822,
10084,
14890,
8456,
-32279,
31387,
-12409,
29142,
-16867,
26049,
13238,
-22984,
-21939,
-30968,
23988,
-21652,
-24888,
4001,
-6009,
8017,
----------RANDOM in range (-2147483646~2147483647)!!----------
-1377234909,
-319728865,
-1701000162,
1561559287,
1896612561,
1169275044,
-1073416330,
-78133846,
1033802748,
-1584984755,
569480191,
1723270415,
1105446836,
435064677,
122567893,
-1605694946,
746914665,
-1852559890,
280727186,
-341783172,
-1885802601,

1025414769,
-876842287,
-1071747448,
932409072,
826104428,
-441158233,
1984722292,
331562284,
1121864133,
-1801710026,
1502121275,
106579708,
111610906,
-594122438,
-2116283989,
1005369932,
1375764704,
-1423900159,
-479151786,
922132491,
2092650056,
-414922208,
627394383,
1789126889,
534010670,
476257241,
23472934,
-2131052177,
1856466733,
-847294378,
1539613409,
-202937188,
-80900835,
-1566534095,
-1698041629,
578177497,
1945480678,
-1287687058,
-1446955661,
1620084441,
317543681,
-1643621056,
-810156076,
1100409964,
465032147,
-1802894650,
-143549825,
371764063,
-1312573505,
-2023360734,
-458946661,
-327932203,
-1027734548,
1880984089,
1502950895,

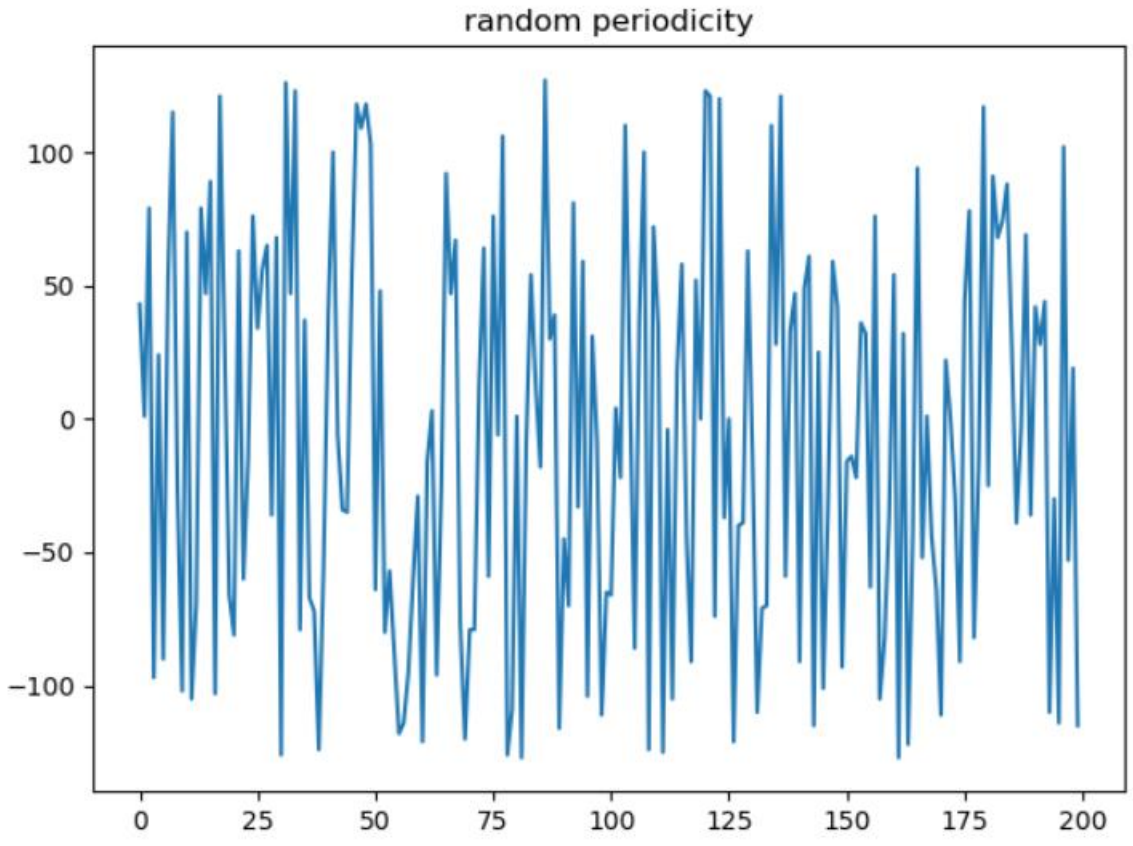
-911321144,
-380202799,
-651284417,
-1010416714,
-145203456,
1688680072,
81271551,
248610164,
2130881275,
418780869,
372478288,
157194214,
-1286241701,
-660714456,
1022222245,
-725084620,
-608687409,
155490591,
-1751249916,
42802727,
221785951,
96150697,
-2038309999,
1342555975,
----------RANDOM TEST FINISH!!----------

4.4.2 随机数分析

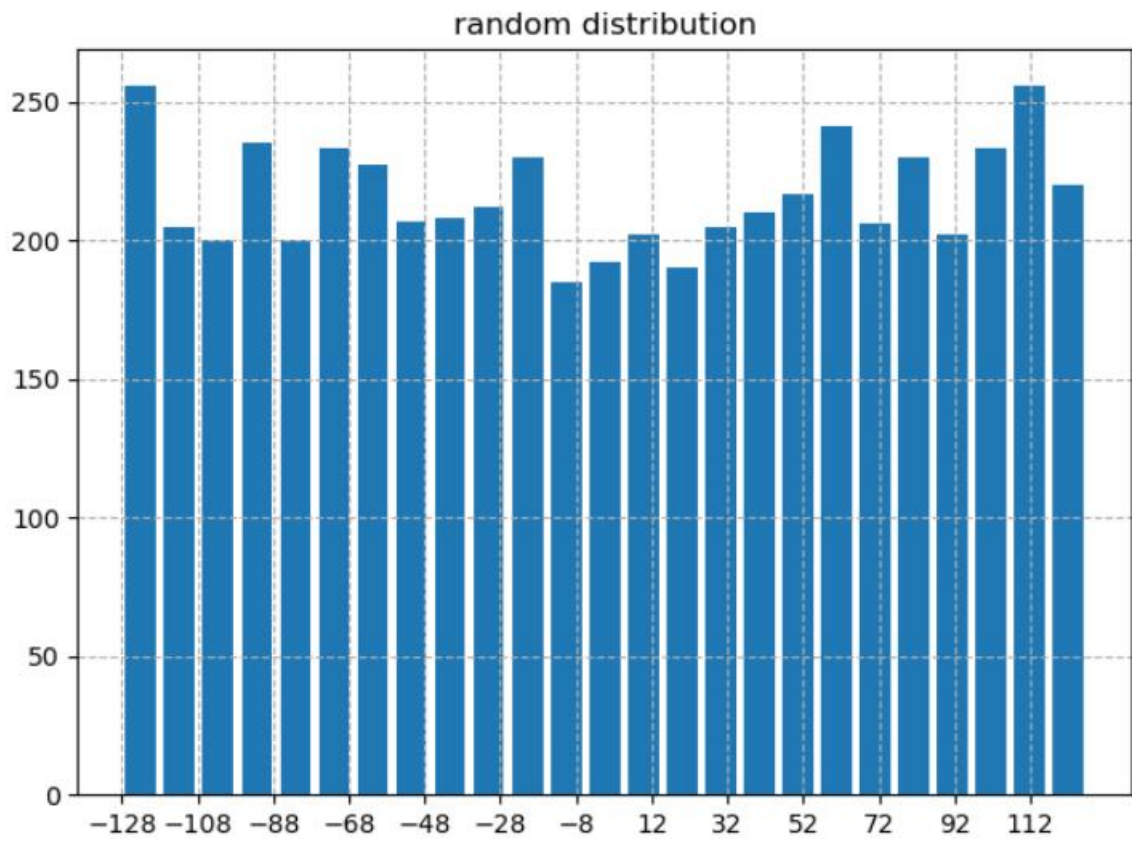
随机数分布图



随机数波形



随机数分布直方图



随机数的各项数据:

Variance	Mean value	size
75.0652062911263	-0.02499074416882636	8bits

IP 核性能对比

本章中对其他论文中提到的利用 FPGA 实现的各种类型的 PUF 进行分数汉明距离、片内汉明距离、片间汉明距离的对比。

Article	PUF type	HD_FIL	HD_SIL	HDFRA
BR_PUF_KEY	改进型 BR PUF	1.12%	31.8%	46.56%
基于 FPGA 的仲裁器 PUF 的实现_王耀冬	Arbiter PUF	4.36%	49.95%	49.98%
一种基于 FPGA 进位逻辑的 RO PUF 设计	RO PUF	1.56%	48.48%	50.56%
基于 FPGA 的低开销 RO PUF 设计	RO PUF	1.81%	50.013%	50%附近
基于延迟的 PUF 设计及其应用研究	Arbiter PUF		48.59%	
基于 FPGA 的新型强弱混合型 PUF 电路设计	Arbiter PUF	3.43%	50.18%	48.89%

附录

I 激励响应对参考表

激励（hex）	响应（hex）
74aaeabe66da35d8e59e2d035e03a191	86ffcc57ee47f2cd
b853d33738df565169f5d554caaf6618	26dc428d7d48f8ed
7952feb6abe6cf7410a5966fac82b50	2c562ab92875e8ad
c583b430be626bdbded972fb703f616c	86f0a6fbce57a09e
c6312e5eb48d5332ca46f5ac8717237e	347482d1f9659961
cd67bcc5208e38b7dc91f1cac00efd40	632acff585da8b0
4245493077891afec04dd4db62a827e	a4f4a097fb47b90e
9007ffa9e61f8aaf56cda202da5b50d	94d9c5b38f5fa935
a6256fd602437d242d671d840be8f20	86fa26ffdc41b844
2c6f1e06896dd6466500bff0e2ea354	86f649dbad5dfa69
3d2029be913e246f34ed486bf3972c65	1473c4bb885fe95c
14f01583247b2f93906bb4262147b775	9c9727d17b7db15b
e7363a203ac66f4715304066aa042125	247b89b96869c80e
7ffd601d2dbb925c943b0abc3f666b76	9cd60b314b7fe378
c8b054ee3408a26718ec55a8eb43d6e2	3e1285837a7db155
5a047342644c17d0d94e89b87ff4b5a4	9c9a80b3f845b921
bfebdcb79aa2f021c35bb8d835972fde	b474a7ffae74e2fd
b1db9a7d5aef297581f5aababd888ef	3cd10db32c79ab8d
43b77e8b15b1874b3ac62fcefd3641a	9edcc27d2b0fa02b
e420fe9ea6ca50edd634d2159b88fc48	34308bb5ea76d9a9
76baac8139cf7c9d485446d9aaec41ed	2ef1079f697ed2fa
d0e47d66562d5ef7d88a0929681f0105	a67baa33ad75b125
b277f18e734cebe4c9da3df7e7da8313	3cff8649d855f8b9
196f4e506949417bf8037d08550d4465	b6d3c9d7eb2faa22
fd0094a9bb5d857c4e0c0ba4342850	245660171b68e9de
f947c8337253fca1ca061ac8e29e4a83	6dbaa3fcf7ce89f
b888b416867fb6ac9c2a238095c32fb1	3e7f2e77a95ff399
3973aeff13349c065e4b589b6efc65c9	8ed123b71875e8e5
611333f27bfdd396b96b49ba8dc72588	1c5847a3f979e837
5a7220004826ac521a82fc42c4e8eb	8c51aeb9bc79b87a
1208e4eafe14095519c3e5fbc751bbc9	3e9181cb4c0cbbd5
52152ff0bd372246609116dea1a4b563	14936c1dc97db976
5661927ae65e709023d0387267bd0d13	b67fe57b6c79b9e7
dea38b81fefcda5c986bb3377ef8a203	8cfb27f1485bb09a
b9ac80bd5bb27e5342482c8c1f231261	96332375ba79e3bc
a29c9f73f3a625d387f1e94284e5a2	845ac1155a7ebb85
62da0d42fdf3b76392ad69e42aa01635	a61f2cf94b4df233
29a5e211aa149bed9da6c1d421d6437	86df86d52f0fb26e
a72a39bba78639b5ec756a833d6846e	9cd023932a6bea1f
ae34aaa01140f64c56c0d4da1fa2f429	9619019f0a5ff9cc
3efc28983b3389dddd4353a93d3e33de	9674a1b37b06d35a
5d500eb43b1402c7f7024b4067da600d	bcf9c8b77c25a92c
da94349482f36e743321cb8530dec851	8e57ecb58b7db118
eb017c0f1a4088948e3b512f432e50	9e7685d72a1de939
45402188c179922e336c0a89e684381f	241de5370b77896a
e2e9f0cd663213f9e8f239fd693c635d	b6f5e079ea66f3b0
6b810a63557c89d214d695b335ca12a3	bc3b8693a805e105
f89fc37cc5618b52c120ad94c5653f2a	3c38add52f0df2b4
71100a137b6133ecbbc5661961616c5	a41342f7ff67e909
3b044501688ef11dc39b8670100bc31b	847daf9bf866e91a
50~100	
c7a169caac43dd4c3ee642c4f9e6ea	AC50A4D1E865BA48
e734bb2cbc2803522ab1ac0f5c652248	8C70C8D5DE29C98C

Data:2022.5.20
Recoder:Ge Wen Jie

f8b1dfec23efcc5ef6dbfdcdf432a1d	1E5DE4FD874A265
886933badff5949bea3bc83fa144e38e	1C78CBB1195FBB3F
8abec0c2e54f0da585c3760ba5fbcfd	2EF5055BC77B2B1
5ab37677def83542b2ea7dae73c39fdf	9EB566F1A4DB005
8c7bf038a37de8a77f6b6dfe44e3fa45	AE1367D9D95D9ABE
b06fc66cdc84a0892d1fab03b2c88c9	B6D124F3A17FA84
a4633dba69e3d12478e1bd635c1738dc	841444DBEF65D82F
beec93157cca407a84e0f68c4b5da24	241A801BDA3FF3F8
4ee36b508fc91a5010f93e303d8cc950	9656A2739B599052
2879a583892567ff6bc406b2ede1b74e	1E906313AD47FBDB
75271f7250347919fd996da63f9e70e9	96B1EEF19842C877
4caa1ea6f3e0c4d7179cc23b22c9789	86998DB35E15926D
3a7d8aecdce899b6f08bce3f85ae6cd	AC51EB911E4DFB84
53ca07107dd463219e10de5ea708833f	34FD3D9DCC64A21A
3770cb8fac663d5e51cf07bec25dbc49	EB12111DC6BE999
6cce21a41dab3d4f24d704fa5ffa750c	9C98C73BF6BF27C
65fe17eadd078093a7e7975fe3ff2b98	1E5C479D939E257
168027eaedef92b08db80151cf206936	16DE2B3F4D7DB157
3e391391b9482c5d2f866557d6fbd891	2C1FEADDEA7EDB7A
1ba9bc7160d7658a88de433d53be55d9	969504B1DD4FA3B6
517913765b46c89a33fb569631e05cde	9EB4E3B5B81FABF5
dae6a29fded37890b4439fbde7e008e9	3E514191F59B0E9
ca0935486659c9476826c0550b6a676	84D648F52D7DBB00
72f01176591a383d44c6c4ced51433c5	3433029DAE56F165
369f9e7c56d856822d6a8fadec2cd43	E73E6FB2D0FAB95
e9f4abaa77b703ea83a06edd3d122bb5	965F2DFDF927E1DF
89b4bef4c405b37d987e5d2f8e8fb5e	2C548BCF1A55A1A4
b1c35baae8bc7257f51fd32cbb8fcb0f	3659CDB17879E04D
7a8d93c7b5e614eb3b5147dca9310836	365EC49DEC57F3F1
982997acbff15950d31f2077b04af545	C13AD79DB4DBBDC
29d054ebce3da6b05bdaee82ca32f274	267606D794DE157
88b04b345e860ab0764d365cc5b6c543	3453405D8819B11C
e95a8ebe979a14d683a8518a1bd727e	16B46A972B6EEAAD
8c1739942abfa96d7033495412cd8711	8EDF69BD694EB818
c04f283ce2559c8e1cc4c5a92926c9cf	B451A3934D7FBA5C
cd6f68297c91d9cdd63b04e8bee096f3	E978B1BDF42AA5E
176b453e85be28a529f93fa7ed806108	16F8C251A85C8A0D
48a3295194e21461822e98964c41ec3f	8E7D2CB5BE5CB042
9ac43c00fdeff3fe3401e1bbb834becc	24F0C8F34D67B13A
c4717ef323e2bae0f106a0d0a93b0610	345EEAFF5E559927
c29b7a11c8f45b37a3eb5c4e80e3c300	E7A679D3841B20A
e4b6d5af89282889d43ccc80b8ce7478	2E948997AE5EF0CD
ef668161f7a5343341fb63d3ff87f248	143023FF7D55C8B6
74019473c7189fbd4b1b31a755e80d9	BEF588F73E7ED9D7
57d6bf05f63d008e14358938463fd9f	2E3DE1B79F778B56
2b17d581cde59964bfc959d9dba23d2	143601951C4DB130
20a957b414493b0fee6aed3ecb6eec8d	3E79E6D13B47F34C
7f87b78e2896b5c21297cdbcfba48708	34D8AF917C45C099