Contribution ID: **19** Type: **not specified**

量子通信中高速并行真随机数发生器设计

随机数正被广泛应用于通信、信息安全、统计决策、程序设计以及娱乐博彩等诸多领域中。通常情况下，仅在一定周期内具有随机性的伪随机数序列就能满足大多数应用的需求，但在如通信安全等特殊领域中，需要通过随机物理过程产生具有真正意义上的随机性的真随机数序列。量子通信中的安全性核心技术量子密钥分发（QKD）系统由于其通信协议和硬件技术的限制，需要使用高速、高集成度的真随机数发生器。而商用真随机数发生器速度无法满足 QKD 系统的需求，如果使用大量芯片并行来追求高产码率，又会导致成本上升和设备体积过于庞大。基于上述原因，针对量子通信中对真随机发生器的特殊需求，本文介绍了一种基于 ASIC 技术的高速并行真随机数发生器芯片——TRNG2014 的设计方案。

本文中真随机数发生器计划采用结构较容易实现的数字电路的振荡环信号抖动作为物理熵源，通过高速时钟信号进行采样，引入后处理结构，提供十路并行真随机数高速连续输出，目标输出数据率为 250Mbps。通过 SPI 总线可以实现对发生器使能、振荡环起振数目和后处理结构选通等进行配置，实现性能与功耗之间的平衡。

基于高速和高集成度的要求，FPGA 由于其成本低、设计周期短、体积小等优势，成为真随机数发生器 TRNG2014 设计载体的第一选择。但 FPGA 对于电路设计的实现是基于其底层逻辑单元对设计方案进行的等价的逻辑替换，并不是对设计结构的绝对复现，因而得到的随机数序列并不是完全按照设计原理生成的。而 ASIC 技术虽然具有成本高昂、设计周期长等劣势，但同时也具有高性能、高集成度的优势，最关键的是 ASIC 技术可以对电路的设计结构实现绝对的复现，从而保证了发生器原理的确定性。因而我们在使用 FPGA 对设计方案进行原理验证的基础上，选择 ASIC 芯片作为高速真随机数发生器 TRNG2014 的实现载体。

本文将着重介绍真随机数发生器 TRNG2014 的设计方案、在 FPGA 上的方案验证以及 ASIC 设计的实现。

作者简介：王鑫🄵（1991-），男，山东德州人，现为中国科学技术大学近代物理系物理电子学硕士研究生，主要从事 ASIC 芯片设计工作。

基金项目：国家自然科学基金资助（编号：61401422）

Primary author: Mr 王, 鑫🄵 (中国科学技术大学)

Presenter: Mr 王, 鑫🄵 (中国科学技术大学)