Paper Reading on Timing Violation Induced Faults in Multi-Tenant FPGAs

3200105787 张云策

该论文[1]主要介绍了对多用户FPGA的时序违反故障的故障攻击方法，这种攻击由于其导致的暂时性的错误，所以该攻击很难被发现。作者在论文中演示了对一套自定时真随机生成数（STRNGs）进行攻击，发现攻击时的随机数发生偏差，失去了随机性，并且在攻击后恢复了原本的性质。

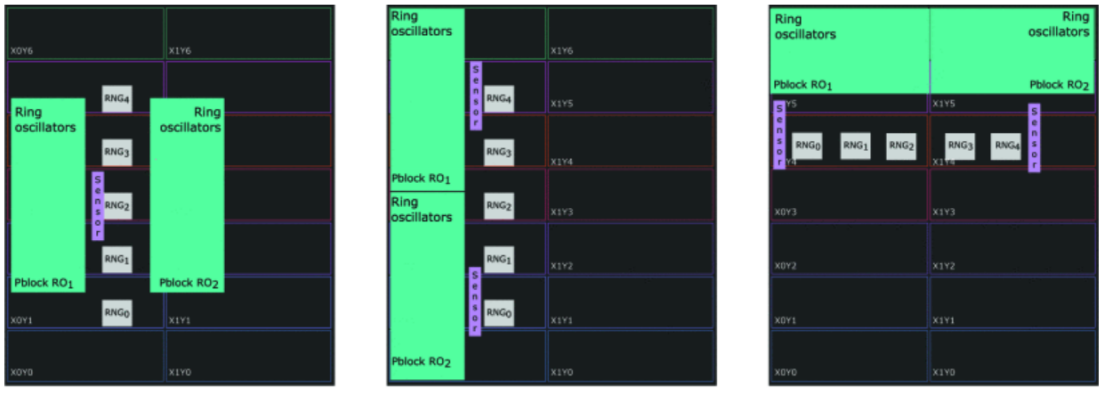
作者实现这种故障攻击原理是利用其它研究人员对于FPGA内部电压的变化攻击[2]，通过设置一个电压供应的低落，使得FPGA出现重置，在论文研究中，作者使用这个特性提高FPGA的逻辑时延，从而使得STRNGs的输出出现偏差。

首先，作为一个FPGA的用户，是没有劝降来控制时间毛刺的生成，但是由于电源供应故障和时钟毛刺会导致时序违反的故障，用户可以利用电源变化来实现这种攻击。首先是制造电压毛刺，作者参考了[^3]中的方法，利用环形振荡器在FPGA内部产生电压振荡，如图1显示的电路进行控制。如果 RO 使用高频信号激活，则配电电路会补偿压降，而压降本身不会持续足够长的时间以导致复位。相反，如果使用低频信号激活 RO，电压降会更高，但电源往往会从冲击中恢复，如果电压降持续时间不长，则不会发生复位。从而实现控制电压毛刺持续时间。

为了评估和监控电压降对 FPGA 逻辑延迟的影响，作者实现了一个基于集成延迟线的传感器。传感器由一系列由时钟信号驱动的缓冲器组成。缓冲器输出连接到寄存器，时钟频率相同但相移 90°。因此，当缓冲器输出被寄存时，时钟下降沿在四分之一周期内通过延迟线传播。实际上，传感器记录延迟线传播深度。电压变化会影响传感器输出，因为它也会影响缓冲延迟

$$d \propto \frac{1}{V_{dd} - V_{drop}}. \tag{1}$$

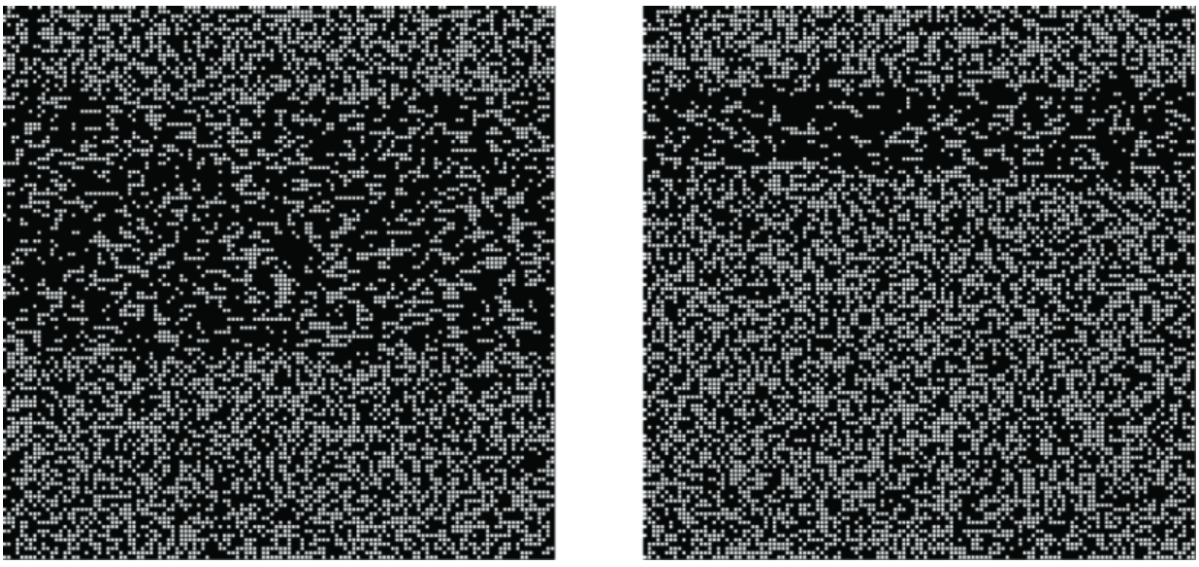
实验设置部分，作者设置了三组实验，每组有着不同的对照组，作者首先从随机数生成器的两边同时进行时序故障攻击，从而观察环形振荡器的电压毛刺。第二组是将环形振荡器放置于RNGs的左边，并且放置两个电压传感器进行观察，随后将传感器和RO的距离不断延长，分为近中远三个组。第三组是将RO放置在FPGA的顶部，RO与随机数生成器对齐，并且也按照两者之间的距离由远及近分为五组，分别测量。对于每个 RNG，作者收集了 20 个输出比特流，每个比特流为 214 (16,384) 位：十次没有 RO 处于活动状态，十次有 RO 处于活动状态（在这种情况下，在攻击开始之前收集了 100 位），并测试了两者的随机性。



实验结果上，也按照上面三组的划分分别介绍。如上图(a)所示，作者改变了 RO 的数量并观察了 RNG 输出和电压传感器输出。所有 RNG 都有 512 个阶段。当 RO 的数量达到 140,000 时，可以通过查看输出比特流直观地检测到所有五个 RNG 的输出都存在偏差。在大多数试验中，偏向于“1”；在第二组的时侯也出现了偏差。从左边和顶部进行故障攻击时，改变 RO 的位置和 RNG 的位置会影响输出比特流的可观察偏差和随机性。根据它们的位置，RNG 要么受到影响，要么不受到影响：当受到影响时，它们将无法通过统计测试（有时有，有时没有可观察到的偏差）。为了测试攻击的持续时间是否影响可观察偏差的持续时间，作者使用了t_B和t_D之间的时间减半进行重复测试，有测试结果显示，RO持续时间会影响偏差的持续时间。作者随后设置了更高的时钟频率，增加到180MHz.

	Output bitstream properties				
Location	**RNG0**	**RNG1**	**RNG2**	**RNG3**	**RNG4**
X-left	–	⋆	×	⋆	–
X-middle	–	⋆	⋆	×	n/a
X-right	⋆	n/a	n/a	×	⋆
Y4	⋆	–	–	–	⋆
Y3	⋆	×	×	⋆	–
Y2	–	⋆	⋆	⋆	n/a
Y1	⋆	⋆	⋆	⋆	–
Y0	⋆	⋆	⋆	×	n/a

RO对从左侧攻击和从顶部攻击场景的五个RNG的影响



应用自顶而下攻击场景时$RNG2$输出的位图

在实验过程中，RO的数量、功率、攻击方式和时间都是不变的，目标的放置位置、数量、以及抑或树的执行方式都是一定的。

由于作者在实验中利用了所有可控因素，RNG 之间的可观察偏差存在差异。差异出现在不同的 RNG 和 RO 和 RNG 的不同相对位置之间。这可能是由于各种原因造成的。首先，RNG 相对于 RO 的放置具有显着效果。作者分析了瞬态电压降的空间影响，并提出活动的位置会对芯片上的延迟增加产生不同的影响。在本文的实验设置中，作者测量了 RNG 附近的延迟增加，发现它始终足以使通过 XOR 链的关键路径延迟超过时钟周期。

可变性的另一个原因可能是目标相对于 FPGA 上也消耗电流的其他组件的放置，例如 PLL、ILA、复位系统处理器。随着 RO 的激活，RO 块和其他工作逻辑的影响可能会累积并影响随机位输出。

最后作者提出了三个可供继续研究的方向，首先是自动化攻击，作者在实验中改变了攻击者和受害者的相对位置，并使用传感器输出作为选择激活波形参数和设置所需 RO 数量的指导。实际上，所有这些都可以自动化；在自动攻击中，不是使用两个块的许多 RO，而是可以将它们分成许多较小的组，并为每个组提供一个激活信号。然后，根据目标延迟增量 ΔS，传感器读数可用于即时决定激活多少 RO、何时激活以及激活多长时间。二是研究攻击目标所处位置以及攻击者位置对攻击效果的影响。三是研究如何检测到这种故障攻击，人们也许能够设计一个电路来检测潜在的危险情况。例如，对于给定的关键路径和设计时钟频率，可以使用相同的电压传感器来估计是否可能发生时序故障。如果发生时序错误的可能性很高，则可以选择丢弃前一个时钟周期的数据（如果可能的话），或者重新开始计算。

在文章中，作者描述了恶意 FPGA 用户如何在共享同一 FPGA 芯片的电路中制造微妙的时序错误。作为攻击者，作者使用了大量环形振荡器作为武器，使用了自定时真随机数生成器为目标。通过实验证明，在攻击发生时，RO 会产生电压骤降，从而导致逻辑延迟增加。延迟如果足够高，会导致 RNG 的关键路径变得比时钟周期长，通常会导致非随机且明显有偏差的输出。未来的工作将侧重于攻击的自动化、检测和防御。

---

1. D. Mahmoud and M. Stojilović, "Timing Violation Induced Faults in Multi-Tenant FPGAs," 2019 Design, Automation & Test in Europe Conference & Exhibition (DATE), Florence, Italy, 2019, pp. 1745-1750, doi: 10.23919/DATE.2019.8715263. ↩

2. D. R. Gnad, F. Oboril and M. B. Tahoori, "Voltage drop-based fault attacks on FPGAs using valid bitstreams", *Proceedings of the 27th International Conference on Field-Programmable Logic and Applications*, pp. 1-7, Sep. 2017. ↩