使用示波器
查找并消除电路设计中的串扰

陆秋捷
高级应用工程师
028-83108615
qiu-jie_lu@keysight.com

Mar. 31, 2016

助您做出正确的重要设计决策，寻回被串扰侵占的设计裕量！

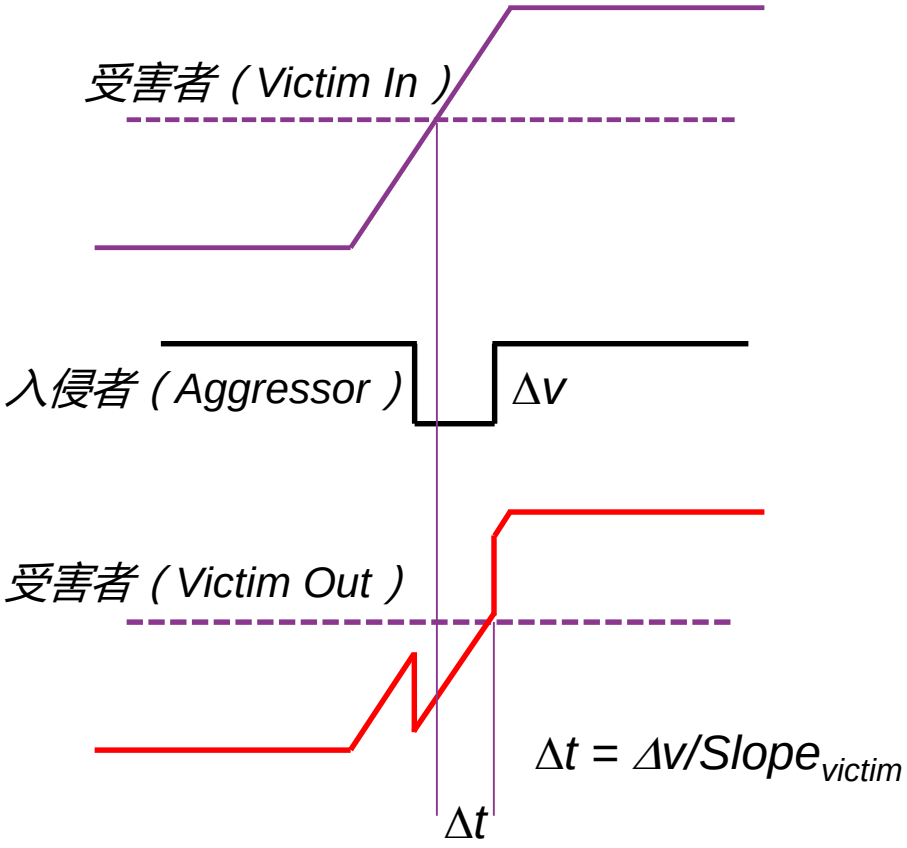
KEYSIGHT TECHNOLOGIES

目录

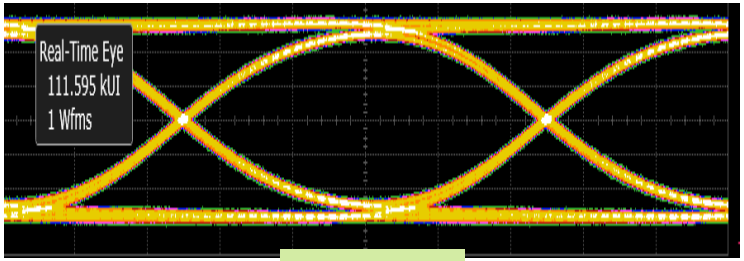
目录

串扰

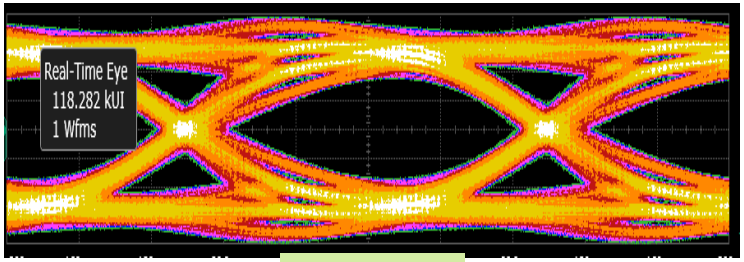
与数据码型不相关的幅度干扰



对眼图的影响



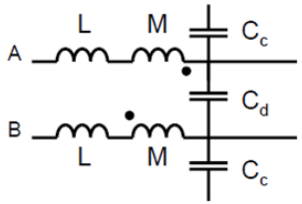
无串扰



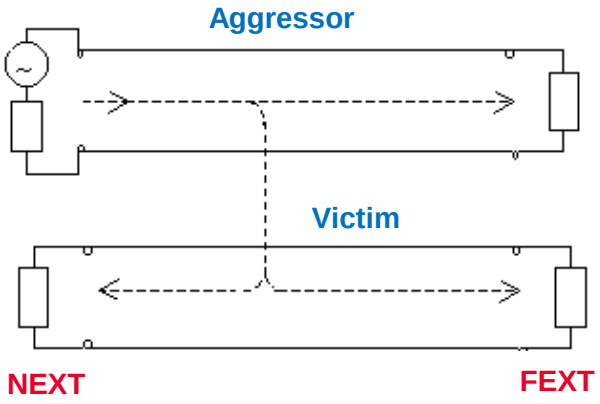
有串扰

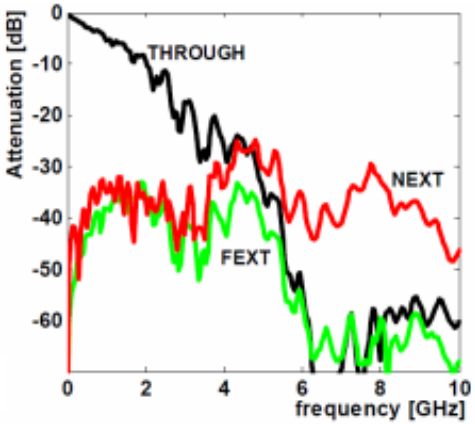
传输线串扰

- 随着数据速率越来越快，以及多个数据通路之间的间距越来越小，串扰导致的影响越来越严重。例如：
  - 100G 标准 （ 4 路并行的25 Gb/s链路 ）
  - 多达 100 路 SerDes 的 ASIC
- 传输线串扰由电路元件间的电磁干扰引起
- 主要由多路信号间的容性或感性耦合导致
- 两种主流类型：
  - 近端串扰（ NEXT ）
  - 远端串扰（ FEXT ）



两路传输线间的
互感和互容

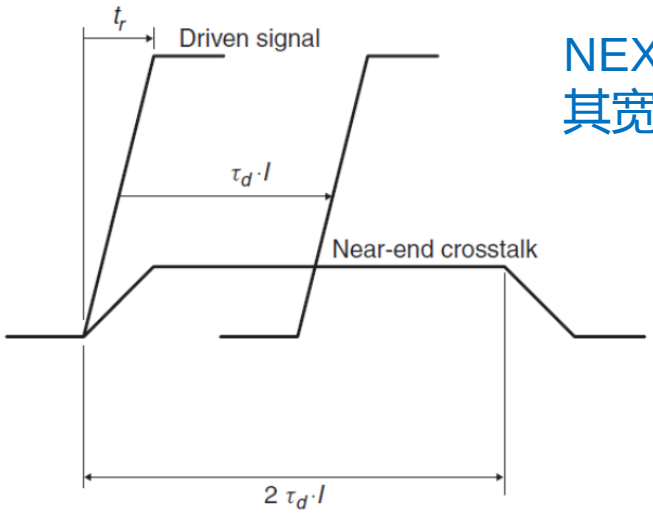




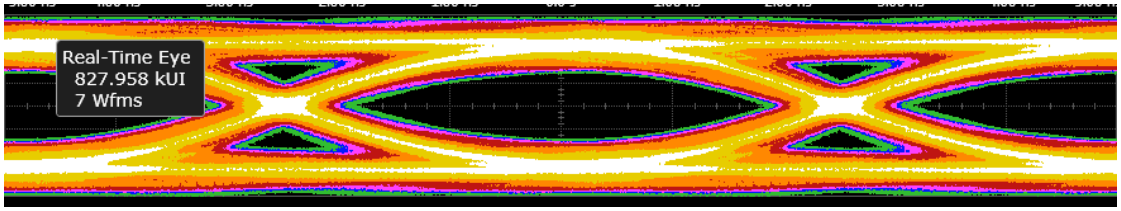
传输函数举例：
- 插入损耗 Insertion Loss
- 近端串扰 NEXT
- 远端串扰 FEXT

近端串扰（NEXT）

- 入侵者信号的边沿一旦离开发射机，干扰即开始产生，并且一直持续到入侵信号边沿到达其远端的接收机
- 反向传输的干扰波形一旦产生，即朝着不断远离入侵者边沿的方向移动，因此其展开的范围更广
- 即使是在远端产生的干扰信号，也需要反向传回近端，因此近端接收到的串扰脉冲波形的宽度是信号传输时延的2倍。



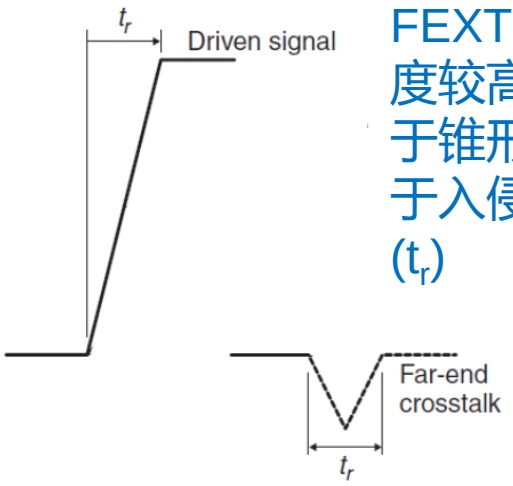
NEXT 是幅度较小的宽脉冲，
其宽度等于信号在该线路上传输时延(t_d)的2倍



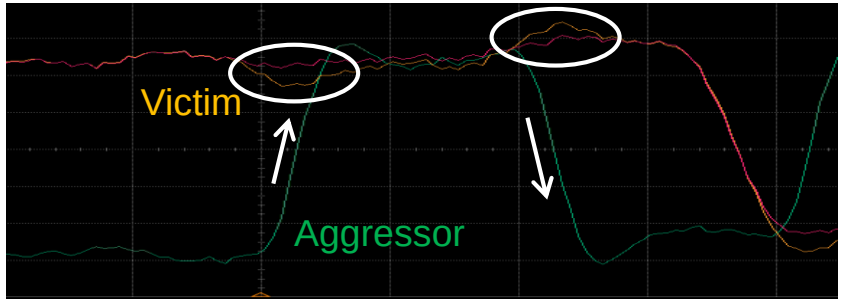
NEXT使得受害者的眼图看上去变得更加模糊

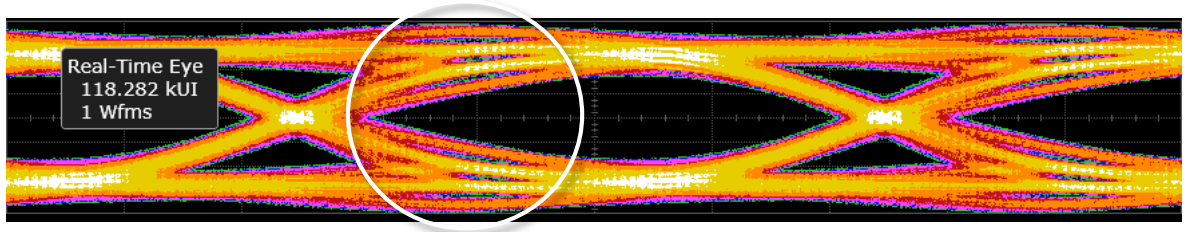
远端串扰（FEXT）

- 前向传输串扰和入侵者信号的传输方向相同，干扰能量会随着脉冲向远端的传播不断累加，所以幅度会变大
- 更快的上升时间会产生更多的串扰
- FEXT通常是幅度较高但宽度较窄的，类似于锥形的脉冲，其宽度等于入侵者信号边沿的上升时间



FEXT 通常表现为一个幅度较高但宽度较窄的类似于锥形的脉冲，其宽度等于入侵者信号的上升时间 (t_r)



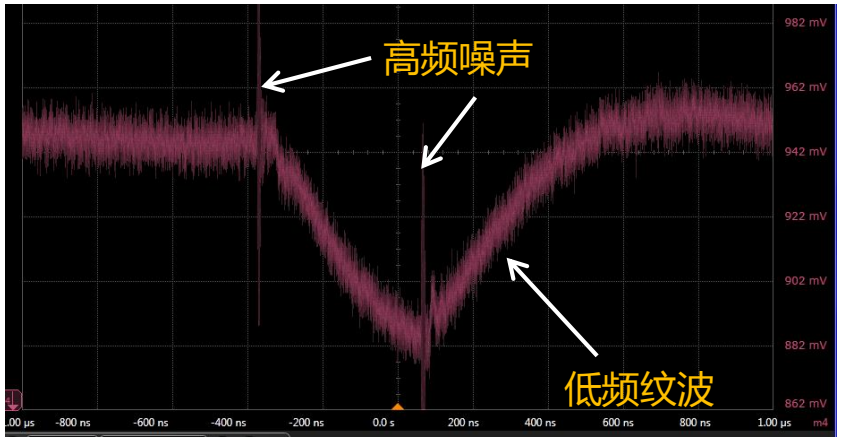


如果入侵者和受害者的数据速率相同， FEXT会使得受害者的眼图看上去有凸起的形状

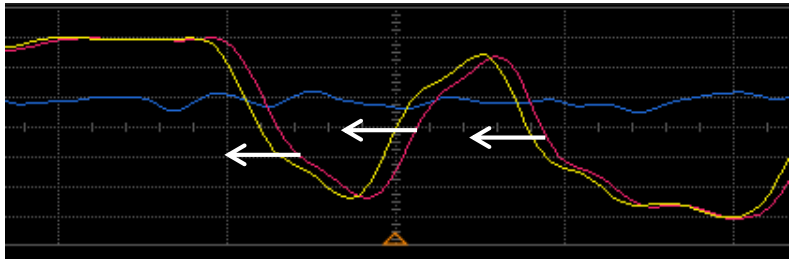
电源入侵者 – PSIJ

电源噪声引起的串扰

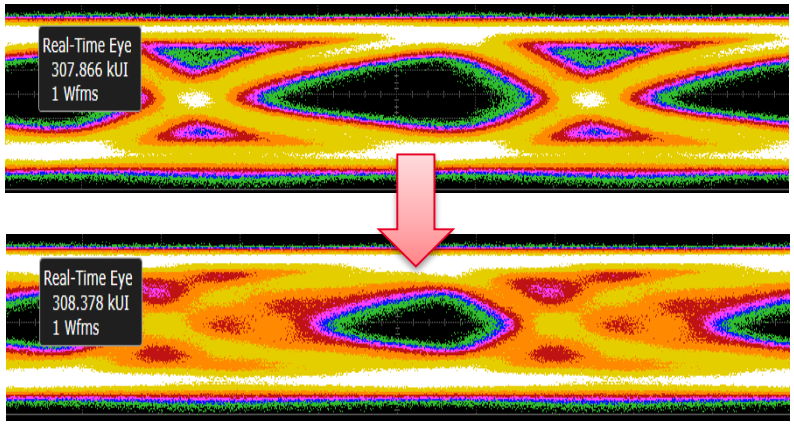
- 电源引入的抖动 (PSIJ) 是由电源轨上的噪声引起的，其通过锁相环路PLL 转移到串行信号上，引起信号的相位变化或抖动



包含低频纹波与高频噪声的电源波形



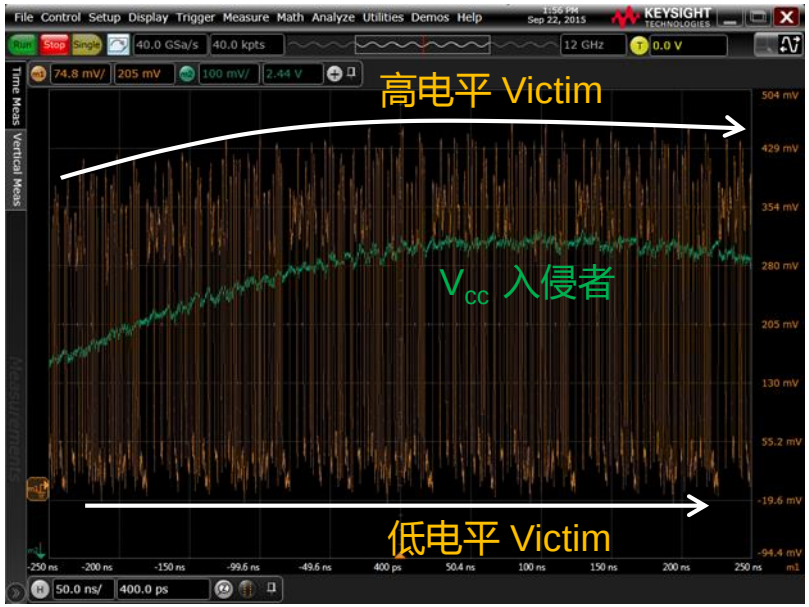
电源上的低频纹波使串行信号的边沿由红色的原始轨迹左移为黄色轨迹，这导致眼图在水平方向上的闭合

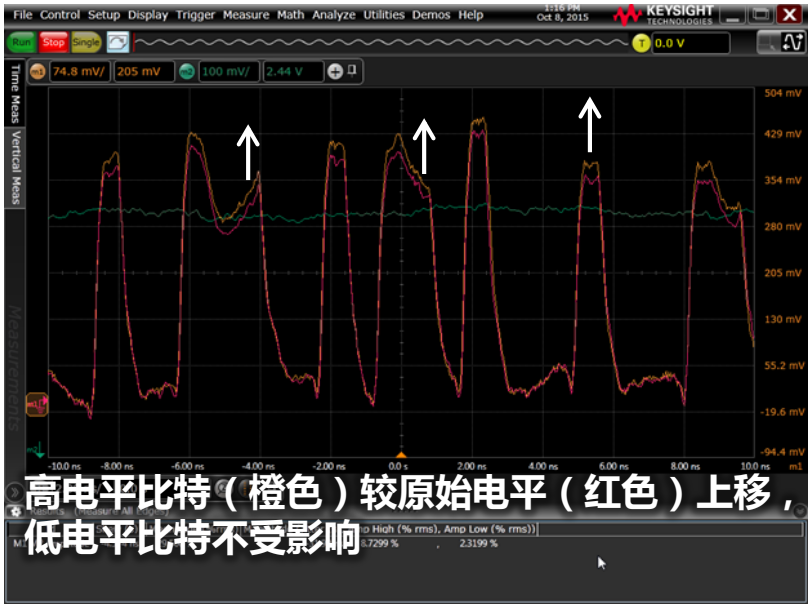


电源入侵者 – VDAN

电源噪声引起的串扰

- 电压相关幅度噪声 (VDAN) 通过电源轨（V_{cc}，Ground, etc）叠加噪声至逻辑高电平和逻辑低电平
- 与传输线串扰不同，VDAN是非线性的，其对不同逻辑电平所产生影响通常是不同的

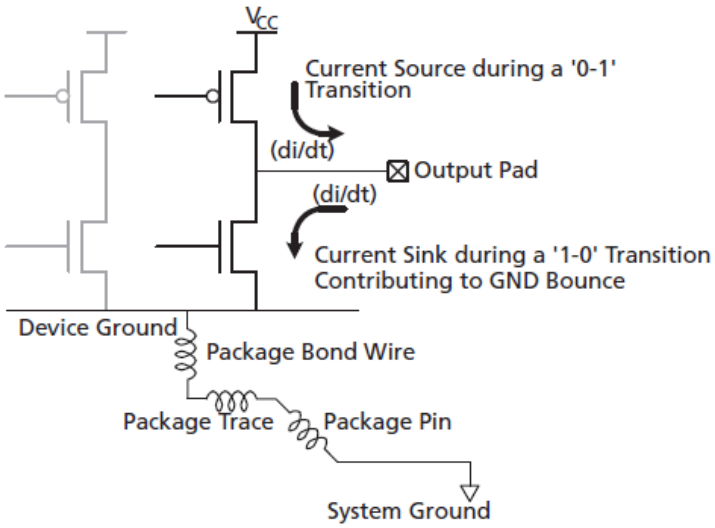




V_{cc} 的噪声传递至逻辑高电平的比特上，但不影响共地的低电平比特

电源受害者

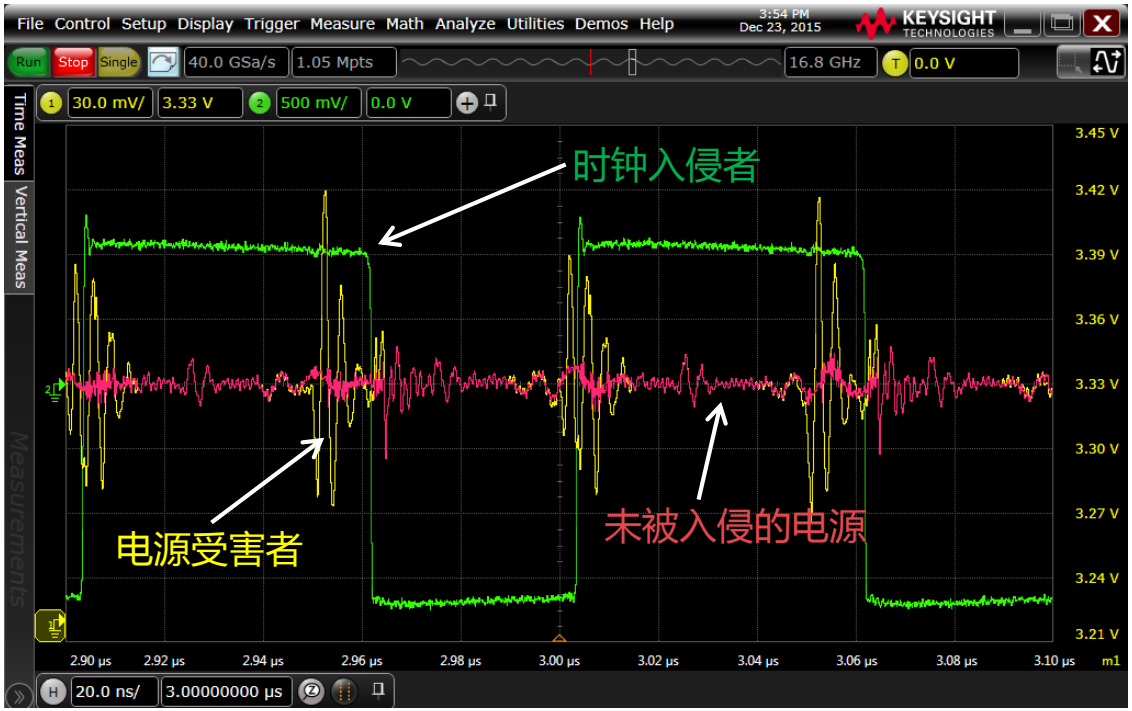
- 电源也可能是受害者，此时串行数据成为入侵者。典型的例子就是同步开关噪声（SSN）导致地弹效应的出现（高电压轨也可能“反弹”，称为“V_{CC}下跌”）
- SSN 是由器件（如芯片）地和系统（电路板）地之间的寄生电感引起的。当一个串行数据链路出现状态切换时，电流通过这些寄生电感引起压降。同时切换状态的数据链路越多，压降越大



寄生电感引起地弹效应的示意图

电源受害者

时钟边沿引起电源受串扰的示例

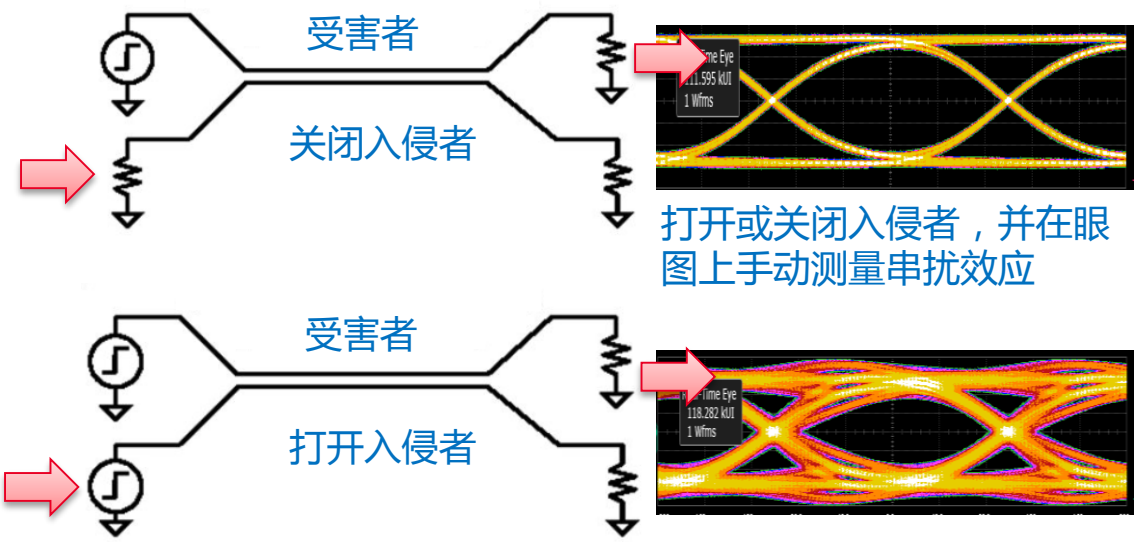


黄色迹线示出的电源信号上所具有的大幅度振铃，是与时钟边沿相关的

目录

测量串扰的传统方法

- 查找和表征串扰并不是新提出的要求，但数字通信系统中传统的串扰测量方法通常需要在有选择的打开某些通道的同时，关闭另外一些通道
- 这种方法必然要求在测量串扰影响的时候系统必须工作在特殊的测试模式下，意味着要在系统非正常工作的条件下进行测量。更坏的情况，有些系统甚至不能支持运行在特殊的测试模式下。



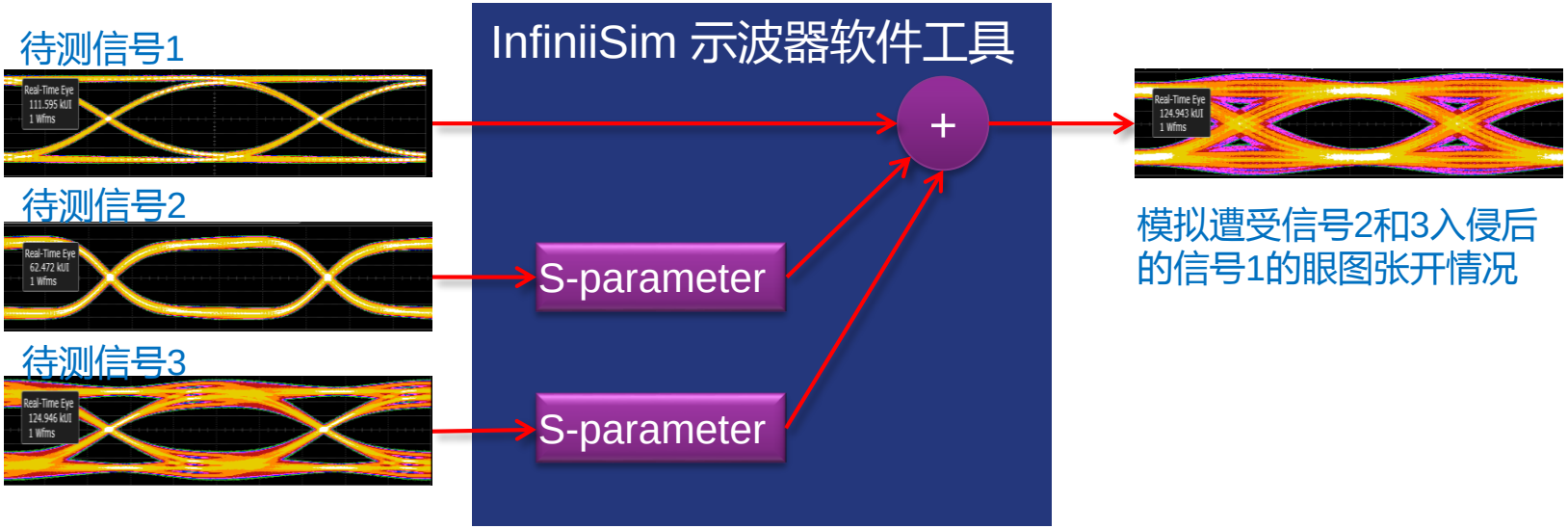
打开或关闭入侵者，并在眼图上手动测量串扰效应

其它挑战：

- 在表征多个串行信号入侵者的串扰时，需要花费大量的时间和精力
- 被测系统电源无法关闭

仿真串扰，但是不能查找并消除串扰

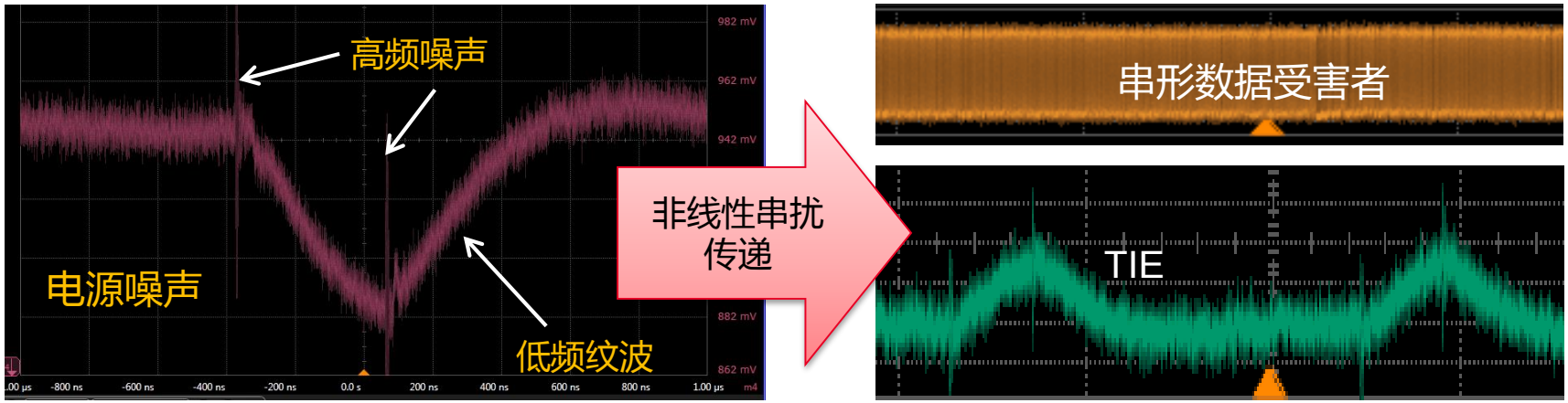
- VNA 可以表征串行数据链路间的串扰，并生成 S 参数模型
- 利用示波器及其软件工具，基于S参数模型，可以仿真波形的失真，眼图的闭合，以及信号的抖动性能



- 然而，在串扰上这些工具的功能仅限于仿真，不能查找真实系统中的串扰源，也不能分析被测信号在消除串扰后能恢复出多大的指标裕量

电源，非线性串扰

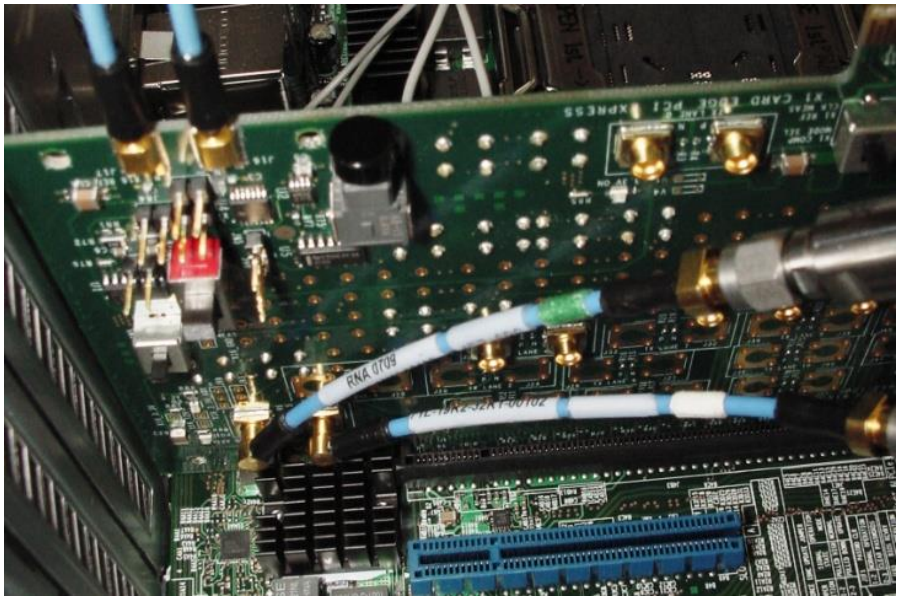
- 对于串行数据链路，由于它的网络模型是线性，因此可以使用VNA来表征串扰
- 然而，电源噪声对串行数据抖动和幅度失真的影响是非线性的，难以用VNA来表征串扰的传递情况



电源噪声与串行数据定时误差之间的传递特性是非线性，难以得出两者之间的相关性

不可探测的入侵者信号

- 并不是所以可能的入侵者都是可被探测的。串扰有可能发生在器件的封装内，但能探测到的仅仅是器件的串行数据输出。
- 是否有办法去表征或调试这种场景？
- 是否可以去除掉串行信号本身而得到残余信号，再利用FFT或放置标记点等方法做进一步分析，以缩小入侵者的可能来源范围？



很多串扰问题发生在器件封装内部，如何在无法探测到入侵者信号的情况下查找并解决串扰问题？

目录

Keysight助您轻松应对串扰分析的挑战

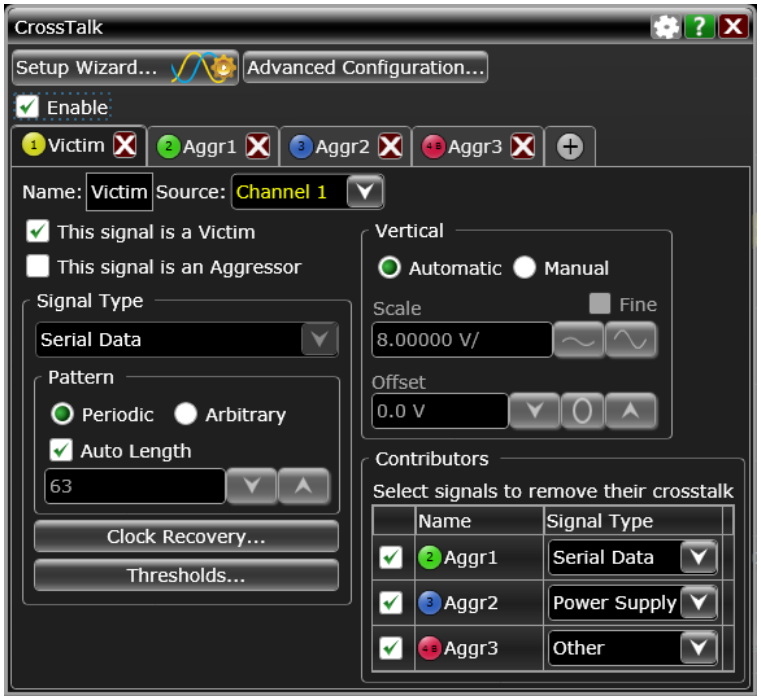
- 串扰查找
  - 哪个信号耦合到您的受害者信号上？
- 串扰量化
  - 每个入侵者信号向受害者信号添加了多少错误？
- 串扰移除分析
  - 没有串扰时，受害者信号是什么样子的？
  - 没有串扰时，受害者信号可以恢复多少指标裕量？
  - 受害者信号在存在串扰的情况下不满足测试规范要求，如果没有串扰时又是否能够满足要求？

为您的产品设计重要决策提供参考依据：

- ***在设计中，是否值得减少串扰影响？***
- ***从哪里加以改进？***

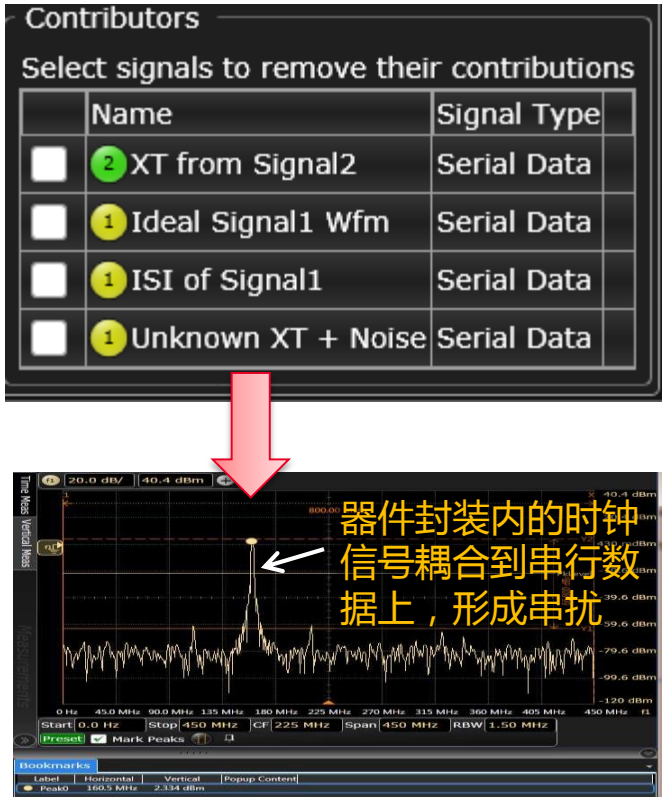
串扰分析应用软件

1. 同时分析多达4路信号（入侵者或受害者）
2. 不需要串扰模型或仿真文件
3. 通过探测不同的信号，查找并识别入侵者
4. 量化受害者所遭受的串扰大小
5. 自动分析近端串扰（NEXT）和远端串扰（FEXT）
6. 支持电源串扰分析
7. 可在示波器上显示没有受到串扰影响的受害者信号波形，并支持：
   - 使用SDA、EZJIT Complete, InfiniiSim、Equalization 和 Mask test等示波器通用分析工具与方法进行更进一步的指标分析与测试
   - 另存为波形文件



应对不可探测的入侵者信号

- 串扰应用软件可以移除理想信号波形及 ISI，得到 “未知串扰+ 噪声” 的残余波形
- 对此残余波形可以作进一步分析，例如通过FFT或放置标记点等方法，进一步查找入侵者信号来源。



串扰分析软件建立串扰网络模型

M = I + ISI + XT + UXT + N
测量波形= 理想波形 + 码间干扰 + (已知串扰) + (未知串扰 + 噪声)

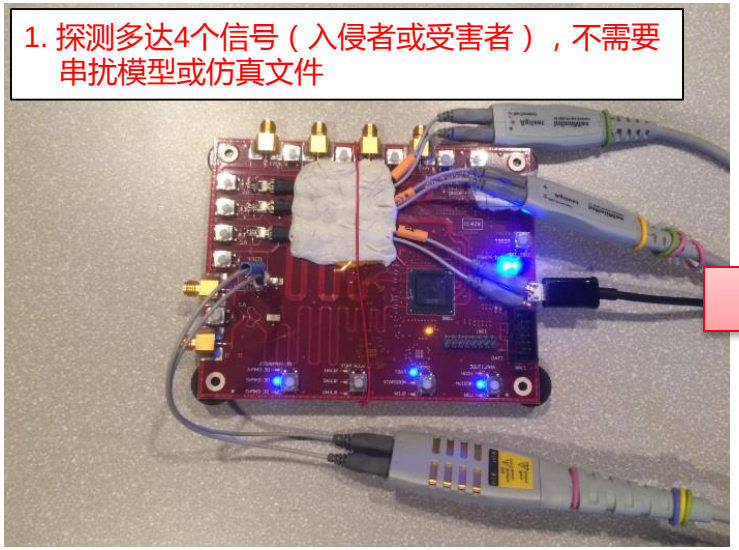
通过移除测量波形中的理想波形(I)、码间干扰(ISI)和已知串扰(XT)，得到“未知串扰 + 噪声”（即UXT + N）的波形，也就是残余波形

利用FFT分析残余波形，找出串扰源

目录

串扰分析设置

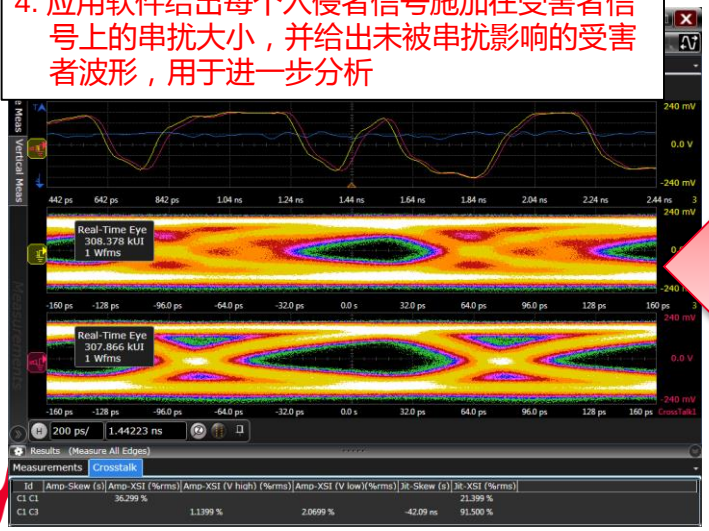
1. 探测多达4个信号（入侵者或受害者），不需要串扰模型或仿真文件



2. 设置受害者信号

3. 设置入侵者信号并配置入侵者类型

4. 应用软件给出每个入侵者信号施加在受害者信号上的串扰大小，并给出未被串扰影响的受害者波形，用于进一步分析

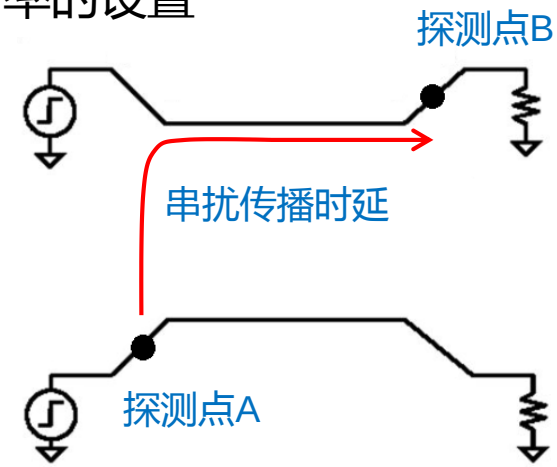


建议的探测方法

- 使用点测式探头前端快速查找并识别入侵者
- 使用焊接或ZIF式探头前端表征串扰
- 串扰分析软件允许在任意位置探测信号
- 为得出最好的结果，推荐如下：
- 串行数据串扰
  - 受害者：靠近接收端（接收端实际看到的信号）
  - 入侵者：靠近怀疑的发送端（入侵者的特征更明显）
  - 多个受害者和入侵者： 靠近接收端（接收端实际看到的信号）
- 电源入侵者
  - 受害者：靠近接收端（接收端实际看到的信号）
  - 入侵者：怀疑为入侵者的电源网络的任何位置
- 电源受害者
  - 受害者：观察到串扰失真的电源网络的任何位置（如封装 V_{cc} 或地）
  - 入侵者：靠近怀疑的发送端（入侵者的特征更明显）

同步

- 由于串扰分析软件需要寻找入侵者信号与受害者信号之间的相关性，所以需要同时捕获入侵者与受害者信号
- 串扰传播时延、信号接入点和不同的探测电缆等因素都可能引入时间偏斜即Skew
- 最小化Skew可以改善测量结果的计算时间
- 默认情况下，软件容许入侵者和受害者信号间有10ns的Skew，这大约相当于长度一米电缆的传输时延
- 在高级设置中，支持将de-skew参数设置为最大1s，但这受限于存储深度和采样率的设置



串扰应用软件可以补偿由于串扰传播时延、信号接入点位置和不同的探测电缆等因素引入的时间偏斜（skew）。

测试码型

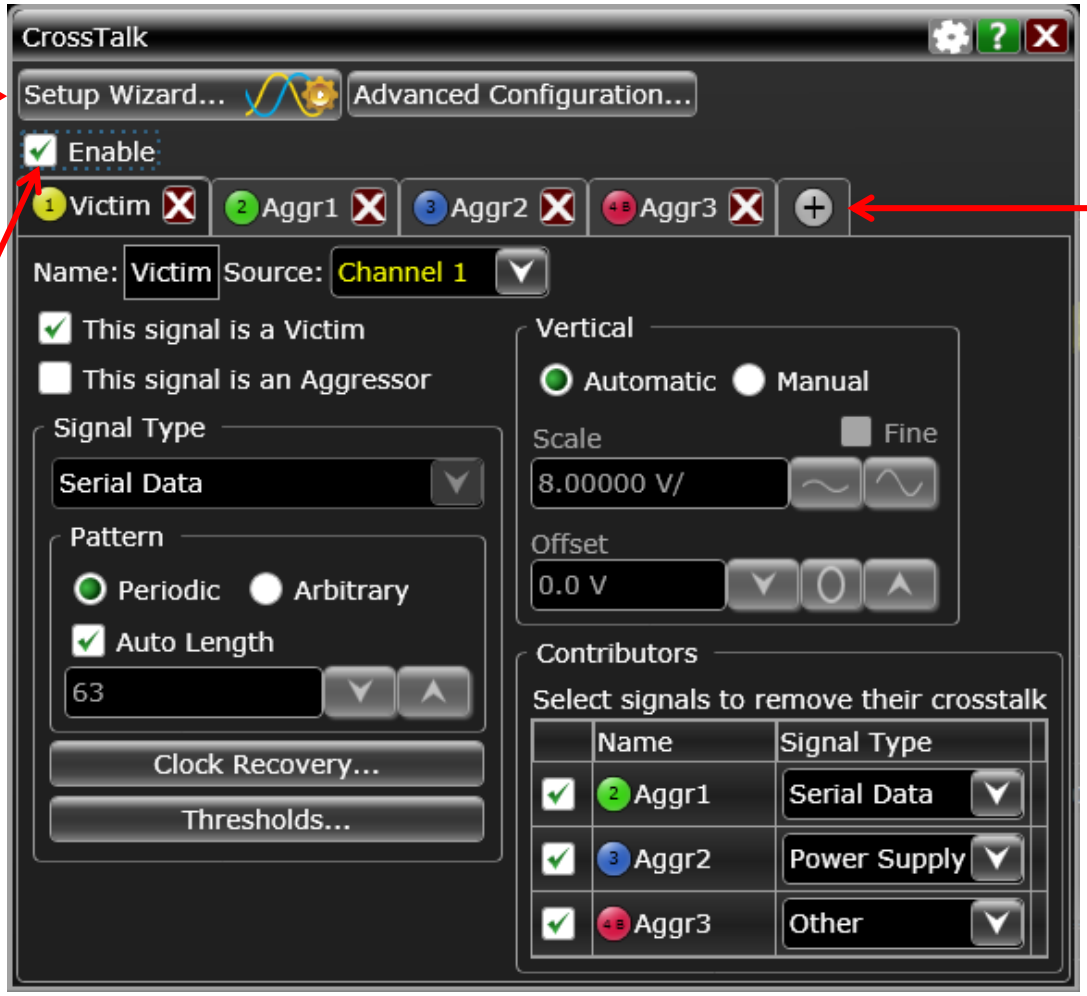
- 串扰分析软件适用于任意串行数据码型，但周期性码型的测量结果更佳，而且计算时间更短
- 为了区分由于ISI及不同的入侵者所产生的失真，每个串行数据通道必须输出不同的码型或工作在不同的数据速度上
  - 如果无法满足这一条件，在设置串行数据类型时，将受害者设置成随机数据模式，而将入侵者设置为周期性码型模式
- 长的数据码型并不能给串扰分析带来更好的效果，其原因简单来说是因为，抖动分析只注重数据的时间误差，所以在每个数据边沿只需要处理一个数据点，但串扰分析软件需要所有的波形数据
- 因此，推荐 $2^{11} - 1$ 或更短的码型

基于实用性和处理时间的考虑，推荐 $2^{11} - 1$ 或更短的测试码型

串扰设置

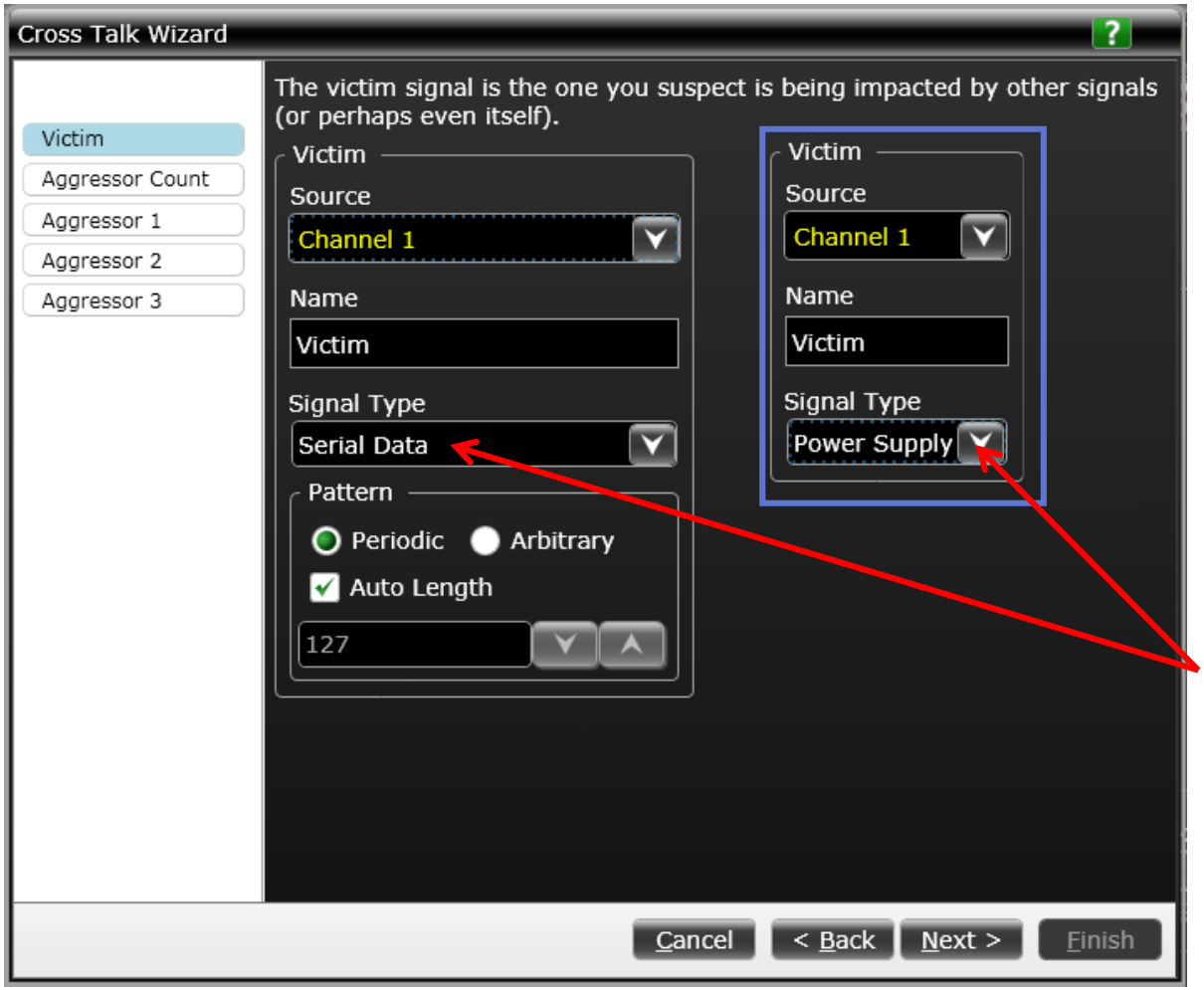
利用设置向导开始设置，或手动完成设置

激活串扰分析



分析多达4个信号

设置向导：定义受害者

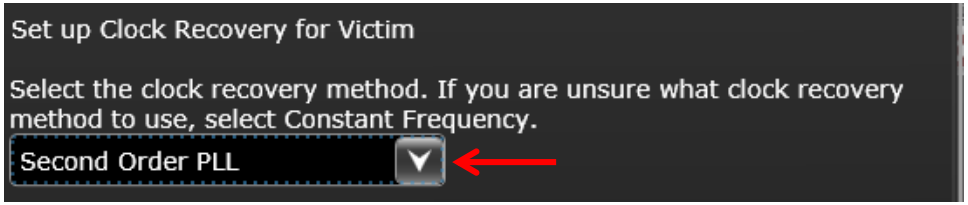


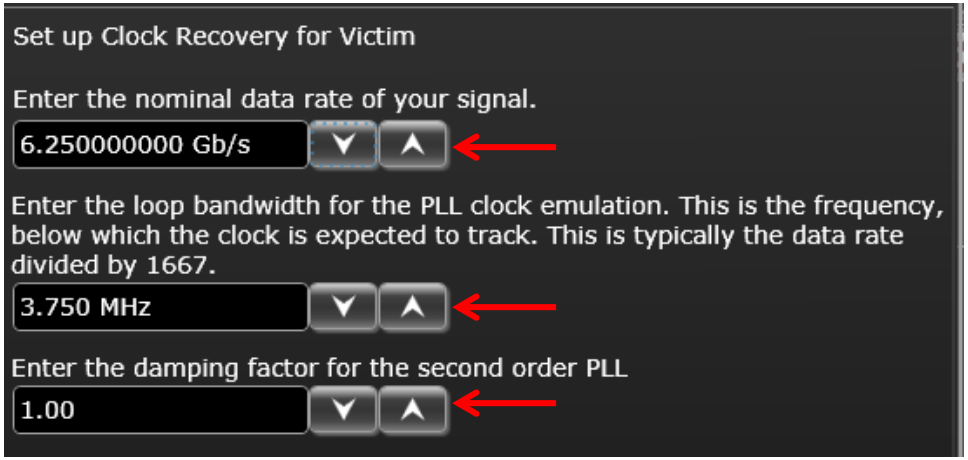
定义受害者，可以是串行数据或电源

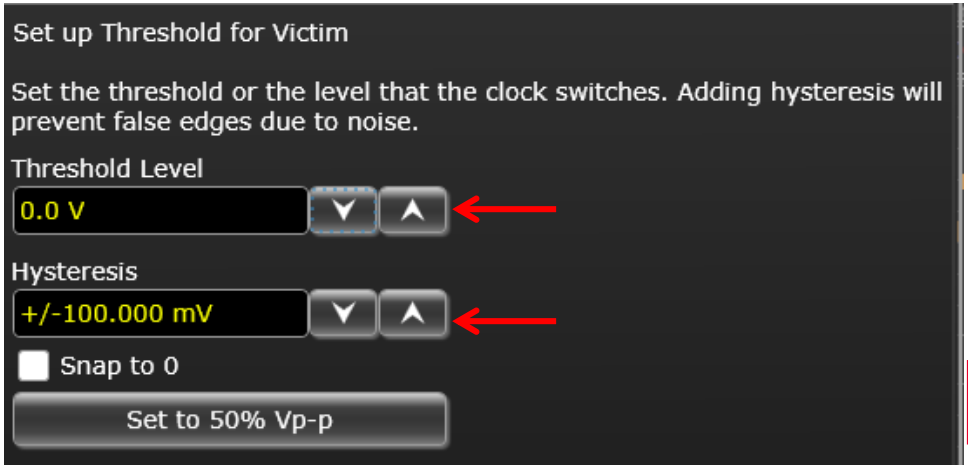
设置向导：受害者时钟恢复和门限

设置串行数据受害者的时钟恢复方式和阈值门限

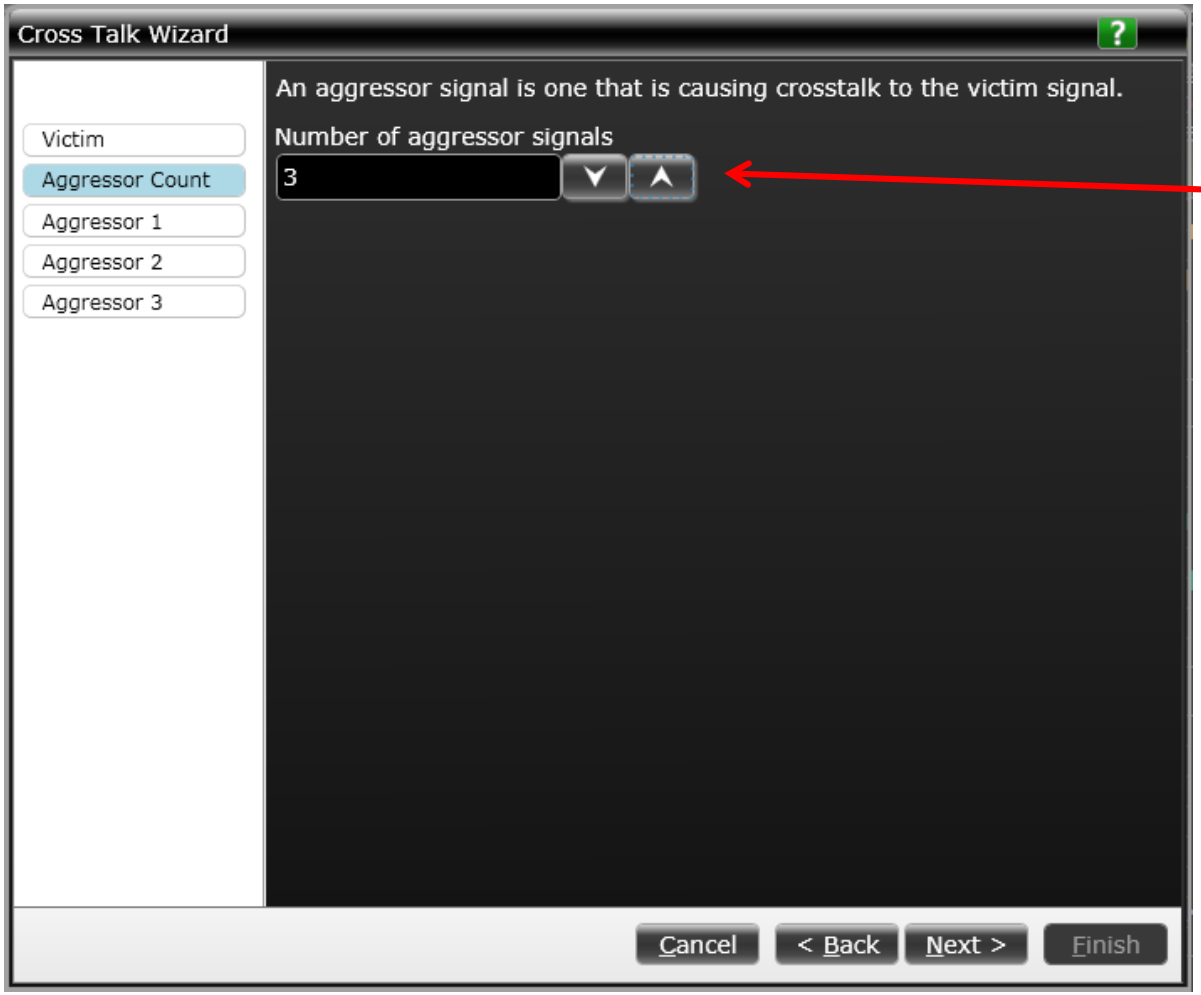
电源受害者不需要时钟恢复设置





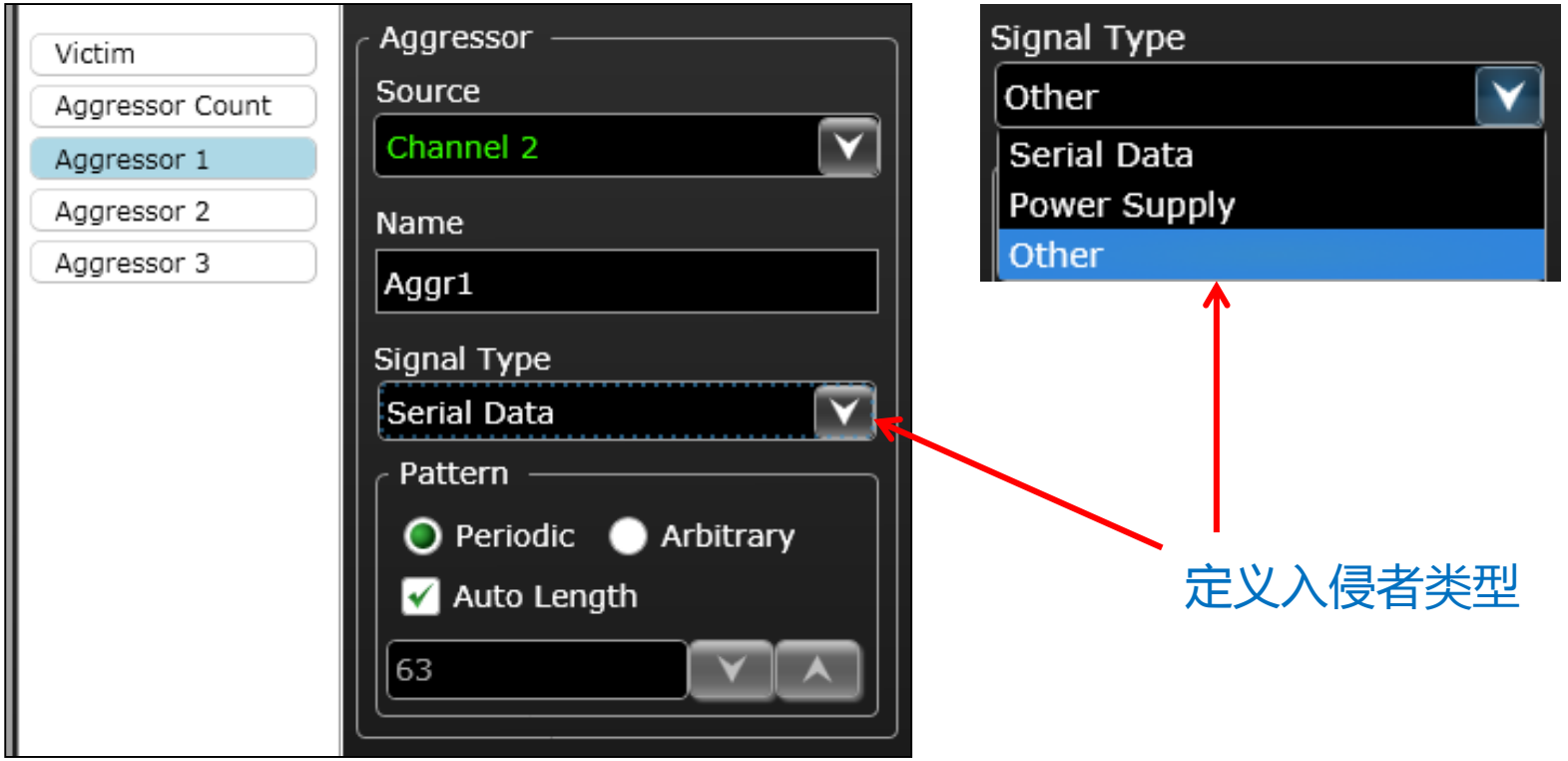


设置向导：入侵者的数量

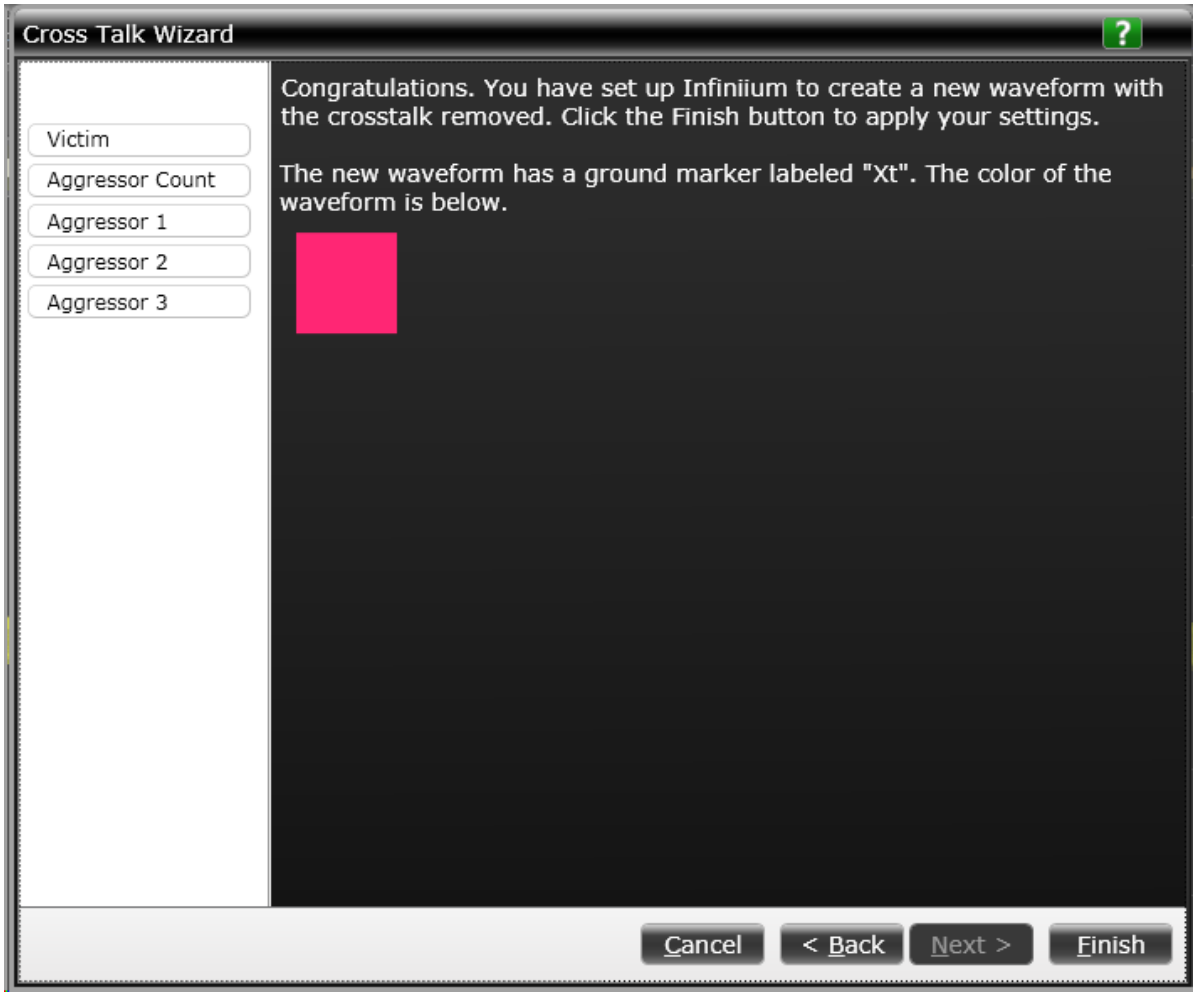


指定不超过3个的入侵者

设置向导：定义入侵者


Victim
Aggressor Count
Aggressor 1
Aggressor 2
Aggressor 3
Aggressor
Source
Channel 2
Name
Aggr1
Signal Type
Serial Data
Pattern
Periodic
Arbitrary
Auto Length
63
Signal Type
Other
Serial Data
Power Supply
Other
定义入侵者类型

设置向导：完成



将会显示出移除串扰的新波形

目录

传输线串扰分析

Id	Amp-Skew (s)	Amp-XSI (%rms)
C1 C1	0.0 s	2.2600 %
C1 C2	106.0 ps	14.100 %

包含串扰的原始串行数据受害者

移除串扰后的串行数据受害者

串行信号入侵者

包含串扰的原始串行数据眼图

移除串扰后的串行数据眼图

Victim : Aggr
C1 C1 – ISI
C1 C2 – XT

Crosstalk amplitude time skew

Amplitude External Signal Interference (Amp-XSI)
= (RMS of ISI or XT) / (RMS of victim)

与ISI（2%）相比，串扰（14%）是串行数据受害者主要的失真原因

KEYSIGHT TECHNOLOGIES

电源入侵者的串扰分析结果

电源入侵者

包含串扰的原始串行数据受害者

移除串扰后的串行数据受害者

包含串扰的原始串行数据眼图

移除串扰后的串行数据眼图

Id	Amp-Skew (s)	Amp-XSI (%rms)	Amp-XSI (V high) (%rms)	Amp-XSI (V low)(%rms)	Jit-Skew (s)	Jit-XSI (%rms)
C1 C1		36.299 %				21.399 %
C1 C3			1.1399 %	2.0699 %	-42.09 ns	91.500 %

Victim : Aggr
C1 C1 = ISI
C1 C3 = XT

ISI distortion

Aggr crosstalk on high level

Aggr crosstalk on low level

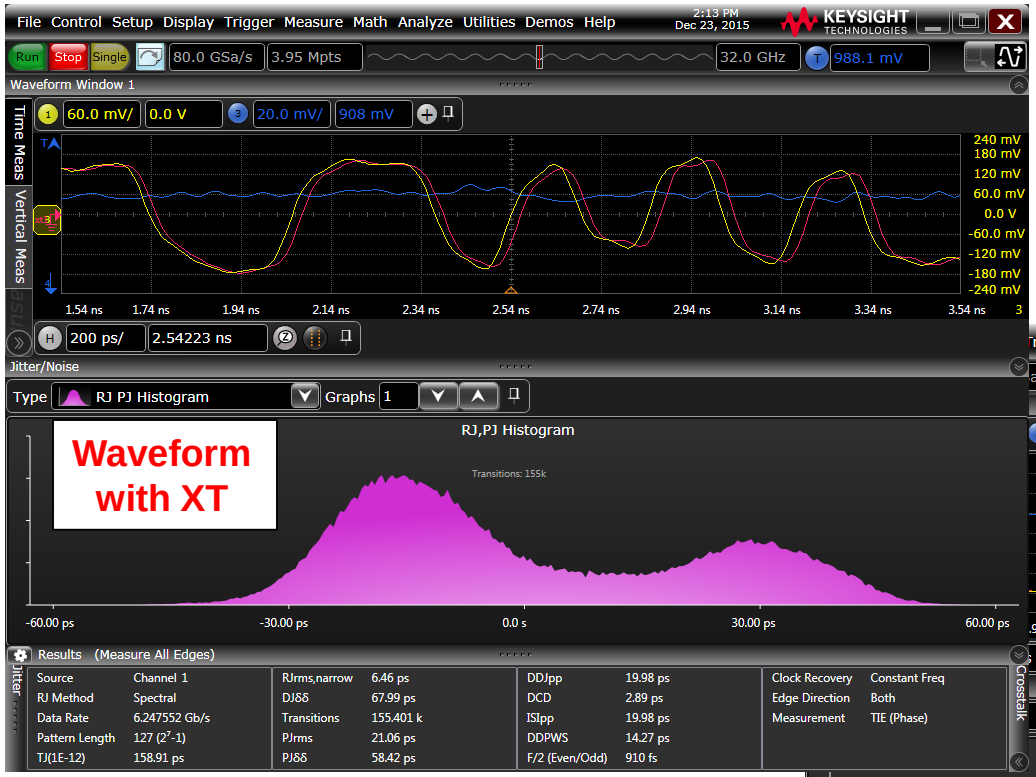
Crosstalk jitter time skew

Jitter-XSI = (RMS TIE attributed to ISI or XT) / (TIE of victim)

Amplitude External Signal Interference (Amp-XSI) = (RMS of ISI or XT) / (RMS of victim)

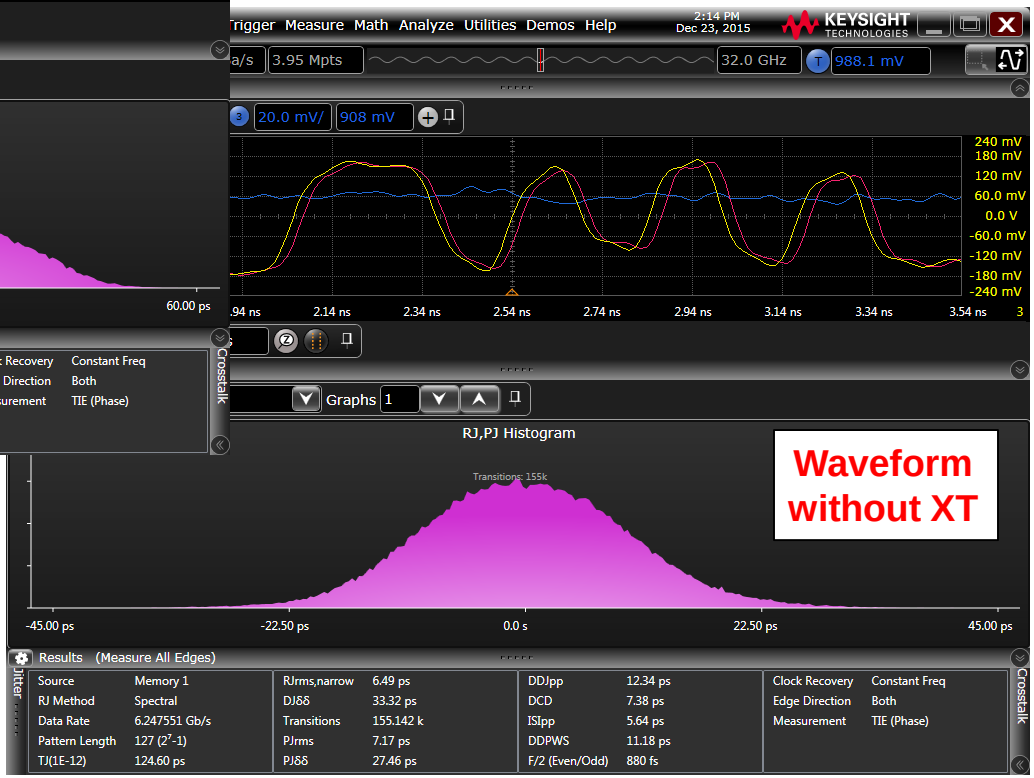
绝大部分抖动失真来源于电源（91%），电平0 和1 只有很小的失真

无电源串扰的抖动改进



TJ = 158ps
PJdd = 58ps
DJdd = 68ps

包含串扰与移除串扰后的串行数据受害者波形分别利用EZJIT Plus进行抖动分析



TJ = 124ps
PJdd = 27ps
DJdd = 33ps

移除串扰后，可以得到20%的总体抖动（TJ）的改善

KEYSIGHT TECHNOLOGIES

电源受害者的串扰分析结果

包含串扰的原始电源受害者

移除串扰后的电源受害者

时钟边沿入侵者

很显然，时钟的跳变沿导致了绝大部分的电源失真（96%的串扰）

Victim : Aggr
C1 C1 – ISI
C1 C2 – XT

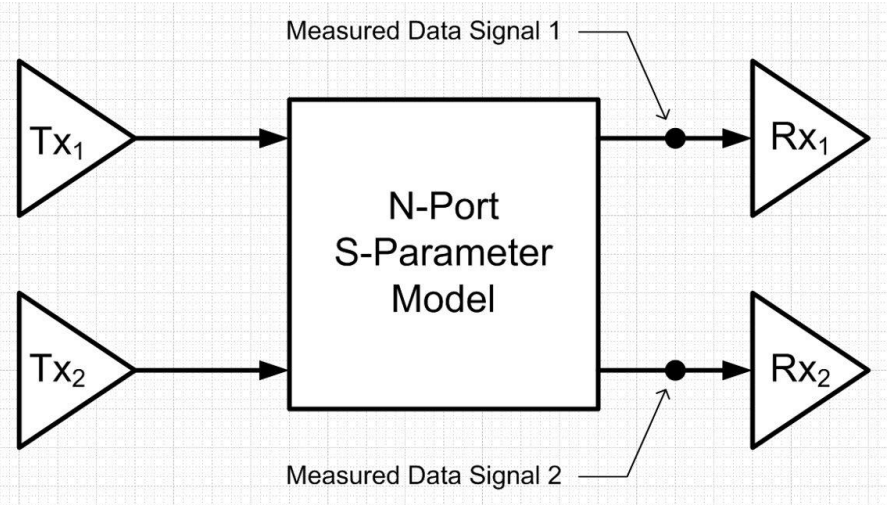
Crosstalk amplitude time skew

Amplitude External Signal Interference (Amp-XSI)
= (RMS of ISI or XT) / (RMS of victim)

目录

串扰网络模型

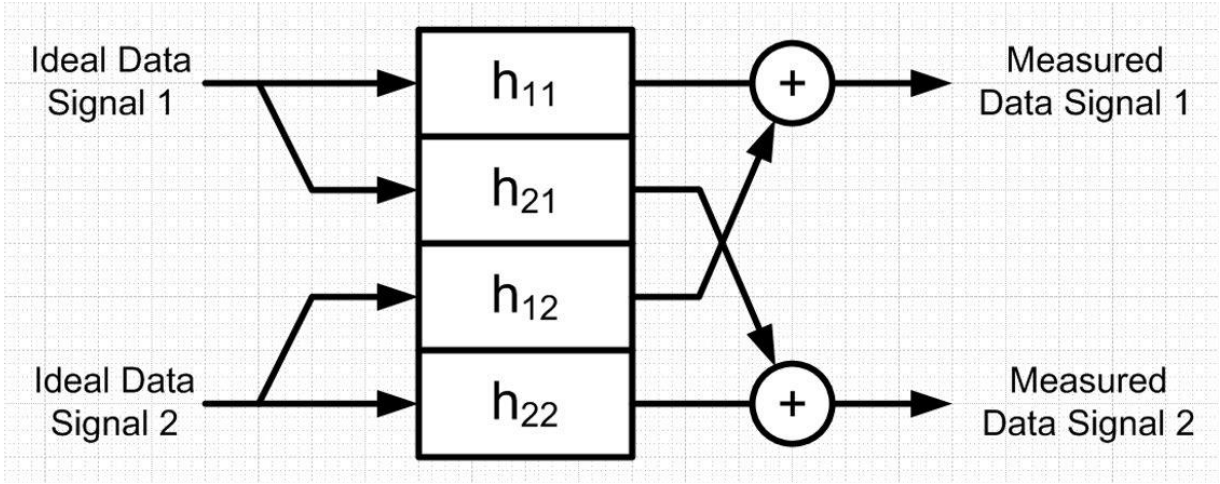
- 根据受害者与入侵者信号的不同类型，串扰分析软件基于测量波形建立不同形式的串扰模型。
- 在最简单的情况下，当受害者和入侵者信号都是串行数据信号时，串扰模型是一个线性的N端口传输函数模型
- 探测这两个串行数据通道，即可提供用于串扰分析的输入波形



两个平行传输线的 4 端口网络模型，黑色圆点表示位于远端的可能的探测点

串扰网络模型

- 作为起点，串扰分析软件首先提取每一路串行信号的时钟及数据码型
- 然后，软件使用理想的数据码型作为此4端口线性串扰模型的输入，计算最佳拟合传输函数模型，将理想的数据波形转化成实际测量到的波形
- 此模型中， h_{11} 和 h_{22} 代表信号的 ISI，h_{21} 和 h_{12} 代表两个信号之间的耦合或串扰。这种方法，使得分析软件可以从测量到的波形中移除串扰、ISI或同时移除串扰与ISI的影响



串扰分析软件计算4端口线性串扰模型，将理想的波形转化成实际的测量波形

目录

最全面的串扰分析解决方案

N8833A/B 关键特性

- 查找串扰
- 量化串扰
- 分析串扰移除后的信号
- 节省大量的调试时间和精力
- 协助您做出重要的设计决策

感谢参与今天的研讨会！

- 下面进入Q&A环节，欢迎大家踊跃提问！