QuietPrint：防范针对 3D 打印机的声学侧信道攻击

Seyed Ali Ghazi Asgar 德
克萨斯农工大学，美国德克
萨斯州大学城
alighazi@tamu.edu

Narasimha Reddy
德克萨斯农工大学，美国
德克萨斯州大学城
reddy@tamu.edu

arXiv:2602.02198v1 [cs.CR] 2 Feb 2026

摘要
近年来，3D打印市场显著增长，预计2025年收入将达到150亿美元。针对3D打印过程的网络攻击日益常见，攻击途径包括机器本身、供应链或制造出的部件。其中一个主要隐患是知识产权（IP）盗窃，即恶意攻击者获取设计文件。实施此类盗窃的一种方法是发动侧信道攻击。本文研究了通过声学侧信道窃取知识产权的可能性，并提出一种防范此类攻击的新方法。我们的方法主要优势在于无需添加大型扬声器或降噪设备等硬件，而是通过对G代码进行少量修改来保护打印部件。

CCS 概念
•**安全与隐私 → 隐私保护协议**; **硬件逆向工程**; **防篡改与抗篡改设计**; **侧信道分析与对策**.

关键词
侧信道攻击、增材制造安全、3D打印安全、声学侧信道攻击、声学防护

1 引言
3D 打印或增材制造（AM）是一种通过逐层沉积特定材料来制造组件的方法。多年来，由于 3D 打印机成本低廉，这项技术已为更广泛的群体所用；截至 2025 [1, 28]，其预计收入已超过 150 亿美元。此外，这种打印技术适合用于快速原型制造复杂几何形状的物体，同时保持其质量 [11, 14, 33]。和每一项能为世界带来诸多益处的新技术一样，它也伴随着各种风险。增材制造同样面临许多网络安全威胁。针对 3D 打印机的一类攻击旨在损坏打印出的组件[24, 31]。在这种情况下，攻击者会设法篡改计算机辅助设计（CAD）文件或 G代码文件，导致制造出的零件缺乏必要的机械强度 [25, 26, 34]。例如， [22] 的作者展示了一种攻击：3D 打印机的开源固件遭到感染，随后自动降低组件的强度。另一种攻击则直接针对机器本身。例如， [2] 的研究人员模拟了一种情景：攻击者篡改固件，绕过用于防止喷嘴过热并超过安全限值的安全功能，从而引发火灾隐患。 [23] 的类似研究展示了一种名为*Print Your Own Grave*的攻击。在这种攻击中，恶意框架会迫使 3D 打印机的喷嘴压向打印平台（某些型号的打印平台由玻璃制成），持续施压 30 分钟后便会导致玻璃破裂。3D 打印领域的另一个问题是在同一地点管理多台打印机。物联网（IoT）协议（例如 MQTT）可用于监控 3D打印机群 [4, 12]；然而，这种协议存在安全弱点，可能被利用来破坏机器[5, 21]。此外，设计人员也担心与制造商共享设计文件。由于恶意内部人员和与员工相关的威胁可能构成漏洞，因此人们提出了多种解决方案。其中一种方法是由设计人员将 G代码文件直接流式传输至机器 [7, 32]。虽然这种方法消除了内部人员威胁，却给制造机器带来了重大风险。如果攻击者拦截传输过程，并在传输期间开始注入恶意 G代码指令，就可能损坏增材制造机器。 [6], 提出的研究解决了这一问题：不再传输 G代码文件，而是先将 STL文件拆分成多个数据块，再依次传输。由于这些 STL片段只包含不具备执行能力的设计数据，不含机器指令，因此这种方法也缓解了制造商的顾虑。

1.1 先前研究与侧信道泄漏
先前研究表明，3D打印机容易受到多种侧信道攻击的影响，这些攻击可能危及设计文件的机密性。在这些攻击中，攻击者利用打印过程中产生的间接物理信号，推断运动模式，并最终重建打印对象或其底层G代码。

一种常见的侧信道泄漏源于光学信号。许多现代3D打印机都配备了摄像头，以便进行远程监控或自动故障检测。虽然这些摄像头提升了易用性和可靠性，但一旦遭到入侵，也会带来隐私风险。先前的研究表明，分析打印过程中采集的视觉数据，可以重建执行的G代码，进而导致知识产权泄漏 [9, 19]。

基于电源的侧信道也被证明会泄露敏感信息。通过测量步进电机汲取的电流，研究人员能够推断运动状态，例如启动、停止和方向变化。这些推断出的状态随后可在多个轴之间同步，以重建运动轨迹并恢复原始G代码 [13]。尽管功耗侧信道信息主要从攻击角度进行研究，但它也可以被重新用于防御性应用。

预期电流模式与观测电流模式之间的偏差可能表明异常或恶意固件行为。

步进电机产生的机械振动是侧信道泄漏的另一来源。以往研究人员将加速度计安装在打印机机架上，并分析振动频谱图，以识别振动模式与喷嘴运动之间的强相关性。利用这些信息，研究人员成功重建了打印出的几何形状，凸显了振动信号对打印机运动的敏感性 [30]。

最后，磁侧信道攻击利用通电的步进电机线圈产生的电磁场。随着电机相位依次激活，它们会引起周围磁场可测量的变化。多项研究表明，这些磁辐射可以通过商用传感器捕获，例如使用放置在打印机附近的智能手机内置传感器，随后用于重建打印物体 [16, 27]。

1.2 声学侧信道

3D 打印机运行时，会产生来自多个来源的噪声，其中步进电机和喷嘴风扇是主要噪声源 [8]。在 [3, 10], 开展的研究中，研究人员将一台专业音频录音机（Zoom H6）放置在 3D 打印机附近。通过提取音频特征，并训练多个机器学习模型来预测运动速度和方向，研究人员证明可以利用音频信号重建 G代码。在另一项研究中， [18], 将两台专业麦克风（Behringer C-1U）分别放置在 3D 打印机的左侧和右侧。随后，对两个声道的音频频谱图进行进一步处理，以完成重建。为解决这一问题， [29] 提议在打印机后方放置一个配有适当放大器的扬声器，以产生足够的噪声，使录制声音的信噪比（SNR）变得无法辨识。尽管这种方法有效，但成本高昂，预计费用约为 1000 欧元，而且需要占用大量空间。

本研究的重点是保护 3D打印机免受声学侧信道攻击。尽管已有多种概念验证攻击场景 [3, 10, 18], , 但据我们所知，目前尚无可行的解决方案能够保护 3D打印机免受此类攻击。在本研究中，我们首先分析 3D打印机中声学噪声的不同来源。然后，评估每种声源的有效性及其对重建打印对象的贡献。最后，我们将提供防御机制，以混淆声学信息，使其无法再被重建。

本文其余部分安排如下。我们首先在第 2 节回顾相关技术术语。接下来，我们在第 3 节介绍威胁模型，随后说明硬件细节。然后，我们在第 5 节提供一种概念验证方法，通过音频重建位置。之后，我们将在第 6 节探讨不同的防御方法并评估其性能。最后，我们在第 7 节进行总结。

2 增材制造中的术语

设计人员使用 3D CAD 应用程序将概念构想转化为数字模型。由于每种 CAD 软件都有自己的专有文件格式，因此需要一种标准化格式，以确保各种制造系统之间的兼容性。顾名思义，标准三角语言（STL）文件会将原始 CAD 模型转换为由三角形构成的网格，用于重建整个物体。每个三角形都包含特定的坐标和几何属性。3D打印机无法直接执行 STL 文件。首先，使用切片软件对 STL文件进行切片，并以 G代码指令的形式依次指定打印过程的轨迹。每条 G 代码指令在机器上执行时都有特定用途。例如，“G0 X6”会使喷嘴沿 X 轴移动到 X= 6 mm 处，但不会挤出耗材丝；而指令“M106 S100”可将喷嘴风扇转速设为 100%（见表 1）。

3 威胁模型

在本研究中，我们关注这样一种场景：具备音频录制功能的设备位于 3D打印机附近。该设备可能已遭入侵，使攻击者能够访问其麦克风；也可能是恶意内部人员（例如工作人员）故意放置的。在本研究中，我们致力于保护 3D打印机免受声学泄漏，确保即使攻击者录制了音频信号，也无法重建原始打印模型（例如 G代码）。

4 数据采集设置

4.1 硬件

我们使用 Elegoo Neptune 3 FDM 3D 打印机作为数据采集和打印测试物体的测试设备。为模拟真实场景进行音频录制，我们使用了 Microsoft Surface Pro 7+笔记本电脑内置的麦克风，而此前的一些研究则使用了专业麦克风，这在现实的攻击场景中可能并不实用。

4.2 声学信息来源

4.2.1 电源。如图1所示，声学噪声主要有三个来源。第一个来源几乎不包含有用信息，就是电源散热风扇。该风扇运行时

表 1：G代码指令示例

指令	示例	描述
G1	G1 X1.0 Y3.3	移动到以下位置： X轴上 1.0mm，Y轴上 3.3mm 并开启挤出
G28	G28 X Y	将 X 轴和 Y轴归零
M106	M106 S50	将风扇转速设为 50 %
M104	M104 S235	设置热端温度 至 235 ◦C
M997	M997	从 SD 卡更新固件 card
M999	M999	重新启动机器

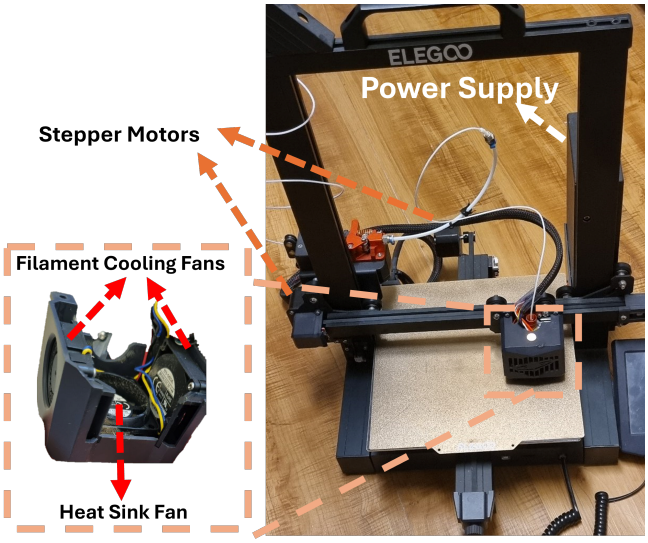

图1：声学噪声来源。

会散去电源电路产生的热量，与G代码指令和运动无关。

4.2.2 步进电机。 步进电机的工作原理基于电磁学。磁芯（称为转子）位于中心，周围环绕着多个线圈。线圈通电时，转子会在磁吸引力的作用下朝线圈旋转。按照特定顺序为线圈通电，转子便会进行步进运动，同时产生大量声学噪声 [3]。3D打印机的每个轴都由一个独立的步进电机控制。如图1所示，X 轴和 Y 轴分别由各自的步进电机驱动。因此，通过分析录制的音频中的模式并分离各个电机的声学特征，就可以估算转速，并将其转换为相应的线性距离。

4.2.3 冷却风扇。 另一种音频来源是安装在 3D打印机喷嘴上方的风扇。如图1所示，喷嘴上通常安装有三个风扇。其中两个是耗材冷却风扇，安装在两侧，出风口朝向 3D打印机平台。这些风扇的主要作用是冷却熔融耗材。散热风扇也安装在挤出机上，有助于防止耗材在挤出管内熔化。

为了研究重要声学特征对信息泄露的影响，首先要回答的问题是：是否可以仅利用风扇产生的噪声来重建喷嘴的位置？在我们的 3D 打印机配置中，喷嘴沿 X 轴移动，而打印床沿 Y轴移动。因此，我们着重分析能否仅凭风扇噪声推断喷嘴沿 X 轴的移动。为实现这一目标，我们设计了一项实验。首先，我们以 500 mm/min 的速度将喷嘴从 $x = 0$ cm 移动到 $x = 18$ cm。我们应用了四阶巴特沃斯高通滤波器。随后，我们按照以下公式计算每 100 ms 音频片段的能量（为降低复杂度，我们使用绝对值之和，而不是平方和）：

$$E = \frac{1}{N}\sum_{i=1}^{N}|x_i|$$

然后，我们使用 $\log(E)$ 进行插值，得到一条直线，该直线表明 $\log(E)$ 与水平移动呈线性相关（见图 2）。

接下来，我们将插值得到的直线用于下一项实验。实验采用自定义的 G代码序列：首先将喷嘴移动到 X = 0 cm，并在该位置停留 10 秒；随后依次移动到 X = 10 cm、X = 5 cm。接着移动到 X = 12 cm，短暂停留后移动到 X = 8 cm，再移动到 X = 16 cm，最后返回 X = 0 cm。每一步中，喷嘴都会暂停 5 秒。移动速度设为 F500，即 500 mm/min。如图 3 所示，攻击者仅凭一个特征（能量），利用我们在上一步（从 X = 0 cm 移动到 X = 18 cm）得到的简单插值直线，就能轻松预测喷嘴的位置。因此，如果攻击者能够根据挤出机风扇产生的音频能量估算出正确的插值直线，就可能准确确定喷嘴的当前位置。更令人担忧的是，在 CoreXY打印机中，喷嘴可以沿 X 轴和 Y 轴移动；若攻击者能够使用两个音频录制设备，就有可能确定性地重建喷嘴在两个轴上的位置。

4.3 将位置与音频同步

声学侧信道攻击的主要目标是根据录制的音频重建喷嘴位置。为此，需要一个以音频为输入并预测相应

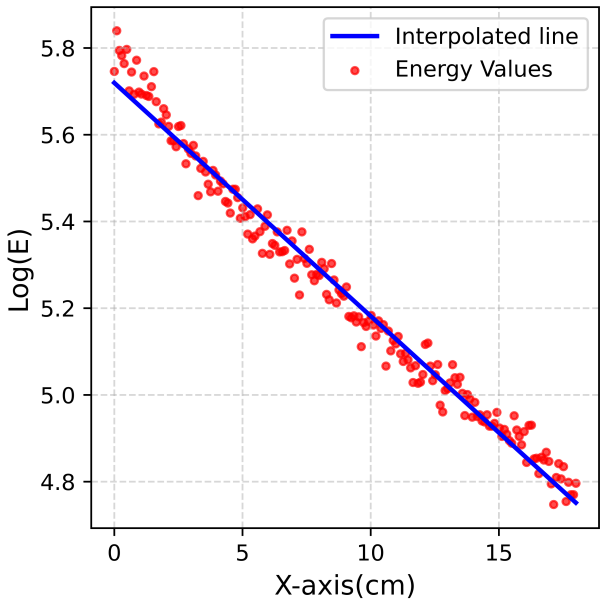

图 2：将音频能量线性插值到水平运动。

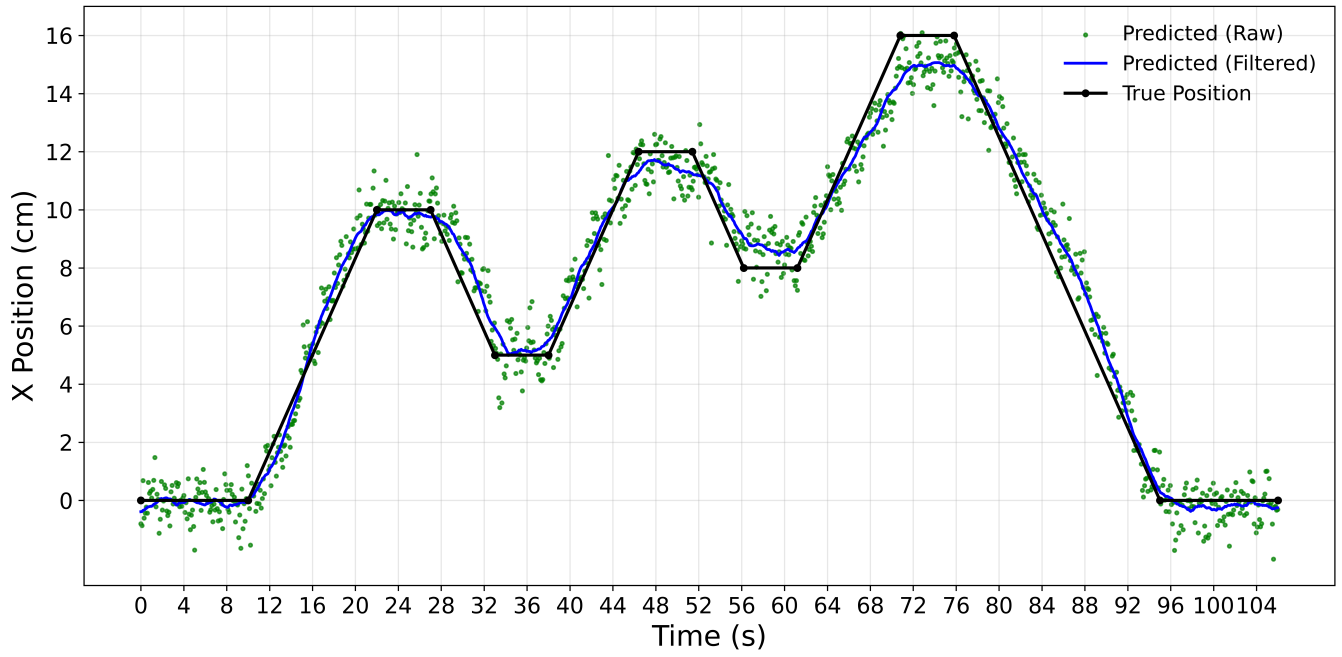

图 3：使用随机运动预测沿 X 轴的喷嘴运动。

位置的模型。这需要知道音频中的哪个点与喷嘴在任意给定时刻的位置相对应。

在最近的一项研究中，[20], 研究人员发布了一个包含 3D 打印物体音频录音的数据集。然而，该数据集的一个关键局限是音频与喷嘴位置之间缺乏同步。因此，由于缺少时间对齐数据，研究界难以训练将音频映射到精确位置的机器学习模型。

为了解决这一问题，我们开发了一种自定义同步方法，如算法 1 所示。我们首先与 3D 打印机建立串行连接。在工艺开始时，我们同时开始音频录制并初始化计时器。然后，我们向打印机发送第一条 G代码指令。打印机接收到第一行 G代码后，我们利用 M400 指令。该指令可确保在当前运动完成之前，不会执行任何后续运动指令。通过从上一行 G代码中提取坐标，我们可以确定当前的喷嘴位置。随后，我们记录喷嘴的坐标以及当前时间戳。由于音频录制和计时器是同时启动的，因此我们实现了位置数据与录制的音频之间的一致计时。我们数据采集过程的最终输出包括喷嘴位置、时间点和录制的音频。

为了评估最终结果，我们设计了一个如图 4 所示的测试物体。切片角度设为 90 度，因此沿 X 轴生成水平刀具路径。用于音频录制的笔记本电脑放置在 3D 打印机左侧。因此，我们预计，当喷嘴位于最左侧（最靠近麦克风）时，观测到的音量会更高；而当喷嘴位于最右侧（离麦克风最远）时，音量会更低。我们

算法 1音频和位置同步

```
初始化串行连接
设置音频录制参数
位置 ← [ ]
时间 ← [ ]
函数发送_G代码_到_打印机(G代码_文件_路径)
    打开G代码文件
    启动音频录音和计时器
    对于所有文件中的行执行
        如果行 =" 或行[0] = ' ; ' 则
            继续
        结束 if
        发送行 并等待“ok”
        发送“M400”并等待“ok”
        使用 extract_xyz_Gcode 提取 x、y、z
        获取当前经过的_时间
        如果 x ≠ None 或 y ≠ None 或 z ≠ None 则
            将 [x,y,z] 追加到位置
            将已用_时间追加到时间
        结束 if
    结束 for
结束函数
调用 send_gcode_至_打印机（文件名）
调用 stop_音频_recoding()
将 (locations, times) 保存到 'loc_time.pkl'
```

图 5 展示了录制的音频频谱图，以及喷嘴的 X 轴位置（以绿色绘制）。为便于观察，省略了与喷嘴运动没有明显相关性的中频。

根据我们的观察，出现了两种显著模式，证明了我们的同步方法有效。第一种模式出现在 6 kHz 至 9 kHz 的频段，来源于喷嘴的风扇。如图 5(b) 所示，当喷嘴位于最左侧（离麦克风最近）时，频谱图显示的能量较高；相反，当喷嘴位于最右侧时，能量最低。此外，我们还在 0 至 1 kHz 的频段观察到第二种模式。这种音频模式由喷嘴路径的突然变化产生。例如，当喷嘴到达最右侧并迅速反向以开始新的一行时，会产生一种独特的运动声。图中白色箭头所示的这些尖锐峰值与喷嘴方向的变化同步。

5 从音频重建位置

根据音频信号重建位置的一种方法，是利用步进电机产生的噪声。当步进电机到达最终位置并开始新的运动时，由于运动方向突然改变，会产生一个突发尖峰（见图6）。假设步进电机以恒定的打印速度运行，则两个连续点之间的时间差可用于估算移动距离。将时间差乘以速度，即可计算出移动的距离。结合所有这些距离，我们便可以重建整体形状。为了证明可以基于这些尖峰重建形状，我们重建了沿 X 轴的数据点。由于采用水平切片，我们假设 Y轴移动以恒定距离递增。首先，我们对音频信号中 100 至 600 Hz 的频率范围进行滤波，然后放大信号。滤波后的音频信号如图6所示。接下来，我们对数据进行归一化，并识别可接受范围内的峰值。其中一些峰值对应的是环境噪声，而不是突然的运动，因此我们将其忽略。随后，我们利用路径中连续变化之间的时间差来计算运动长度。具体而言，我们获取了每个峰值之间的时间差，应用 Savitzky–Golay滤波器，并进一步对数据进行平滑处理。最后，我们将每个

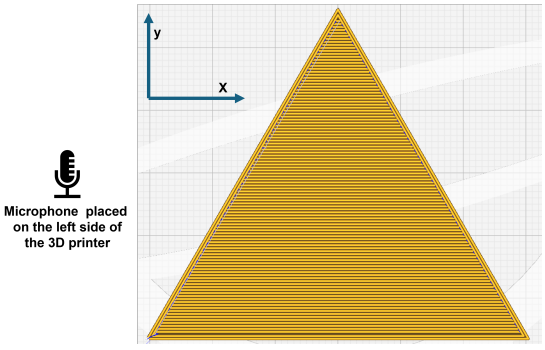

图 4：测试物体的 G代码，以及水平切片角度和麦克风的位置。

时间差值乘以恒定速度（1200 mm/min），并通过改变速度的符号，在从左向右和从右向左之间切换运动方向。根据步进电机产生的突发声学尖峰得到的 X 轴位置预测结果如图7所示。与步进电机产生的突发尖峰类似，也可以利用风扇产生的噪声重建物体。根据我们的实验，耗材冷却风扇还会产生独特的高频（8 kHz）噪声。这种噪声的频谱图如图6所示。

6 防御方法

为了混淆步进电机和风扇产生的噪声，我们提出了隐蔽式打印头运动（SHM）的概念。该方法通过延长 3D 打印机打印头的常规运动，使得即使攻击者能够解码声学信号并还原形状，所还原出的形状也会与原始形状不同。如图9所示，我们首先获取原始 G代码文件，并用矩形边界框定物体。然后，将所有运动延长至这一最大长度。我们找到一个与前一条路径共线的点，并延长这条线段，直到形状仍处于由最大和最小边界所限定的矩形内。添加新点后，还会在 G代码文件中加入一行新的 G代码，使喷嘴能够返回下一个点。该方法有几项优势。首先，如图6所示，喷嘴改变方向时可能会产生突发的声学尖峰。然而，采用我们提出的方法后，由于喷嘴路径是在矩形边界处改变的，即使出现这种突发尖峰，攻击者也无法还原原始形状的位置。相反，如果不进行这种延长运动，攻击者一旦检测到这些尖峰，就可能重建原始形状。其次，即使攻击者利用冷却风扇产生的声学辐射来推断位置，恢复出的也会是经过混淆的形状，而非原始形状。为了进一步研究这一方法，我们提出两个主要研究问题。第一个问题是，在转折点处——即将延长运动加入 G代码指令的位置——是否存在攻击者能够检测到的可识别音频特征，从而识别转折点并区分原始运动与延长运动。第二个问题是，如何移除部分延长运动，以优化打印时间并消除不必要的额外运动。我们首先展示该方法的有效性，随后将在以下小节中探讨这些问题。

6.1 转折点处可区分的音频模式

为了评估我们的方法对音频模式的影响，我们首先在有界矩形的起点和终点（见图9(a)）处分割频谱图，这两个点分别是最左侧和最右侧的点。然后，我们确定正常打印与延长打印之间发生转换的位置。我们对不同片段进行了目视检查，但没有发现任何可识别的模式，能够将转折点与周围部分区分开来。

为进一步验证我们的论点，我们将所有片段调整为相同大小，将频谱图展平，并训练了一个 XGBoost

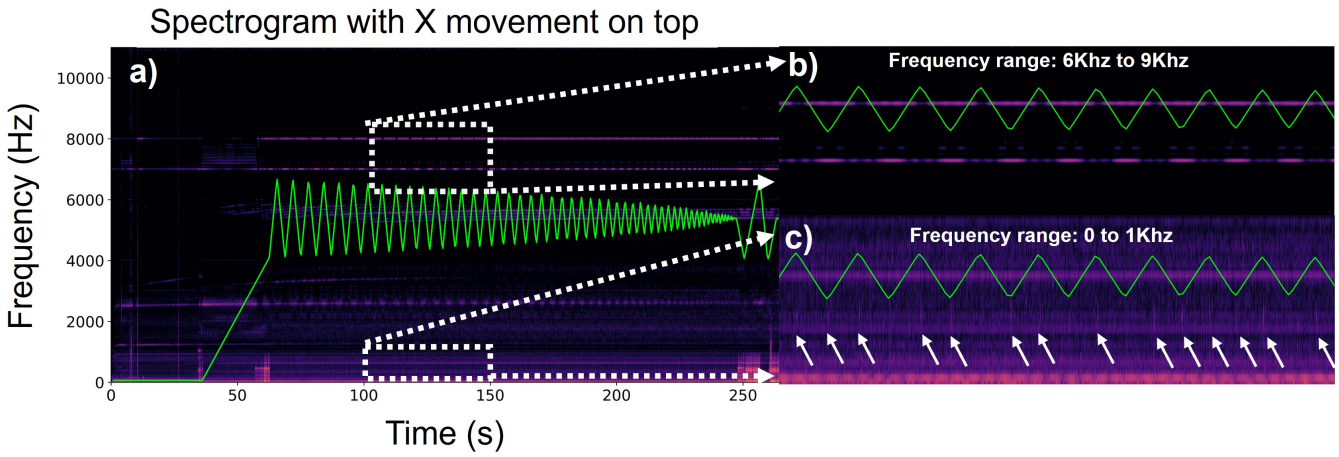

图 5：(a) 沿 X 轴的喷嘴位置叠加在相应音频的频谱图上。(b) 时间范围 100 至 150 秒、频率范围 6 kHz 至 9 kHz 的放大视图。(c) 时间范围 100 至 150 秒、频率范围 0 至 1 kHz 的放大视图。沿 X 轴的喷嘴位置以绿色显示。

回归模型来预测过渡位置。我们使用了 300 个片段，其中 30% 作为测试集，且不进行随机打乱，以避免数据泄露。该模型的平均绝对百分比误差高达 33.79%，皮尔逊相关系数则低至 0.4。这些结果表明，攻击者无法识别转折点（见图8）。

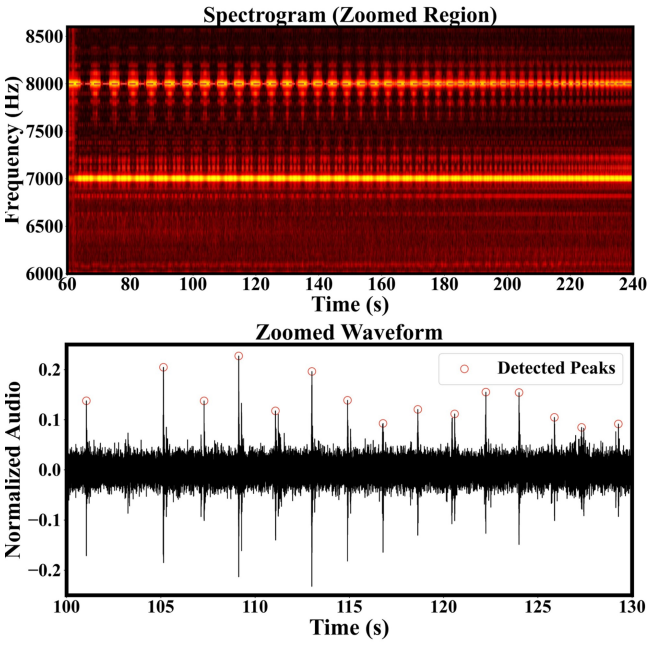

图6：频谱图显示了风扇产生的噪声，其主导频率分量为 8,000 Hz。时域图显示了步进电机产生的突然尖峰。这些峰值出现在电机改变方向时，并使用峰值检测算法进行识别。

6.2 优化扩展路径

虽然将形状限制在矩形内可以对其进行混淆，但这可能并非最优方案。例如，对于图9(a)所示的三角形，由于扩展路径区域的面积与三角形相同，打印时间会增加到三倍（扩展区域的面积与三角形相同，而且每次移动到边缘后都要返回）。因此，有必要进一步优化扩展路径区域。如算法2所示，我们首先为对象拟合一个凸包。目标是移除凸包的部分区域，以尽量减小优化形状与原始形状之间的面积差异。不过，原始形状与优化形状之间的差异度必须保持较高；否则，攻击者可能能够

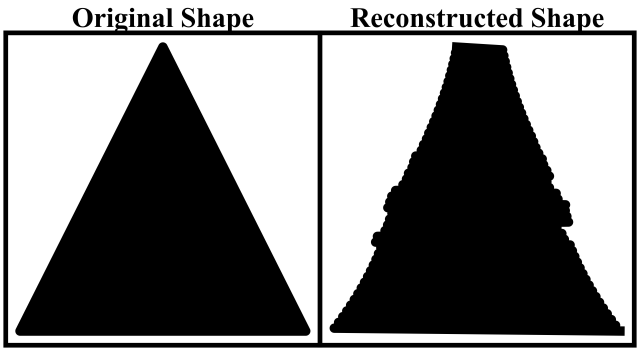

图7：真实形状显示在左侧，基于步进电机突然运动预测的形状显示在右侧。

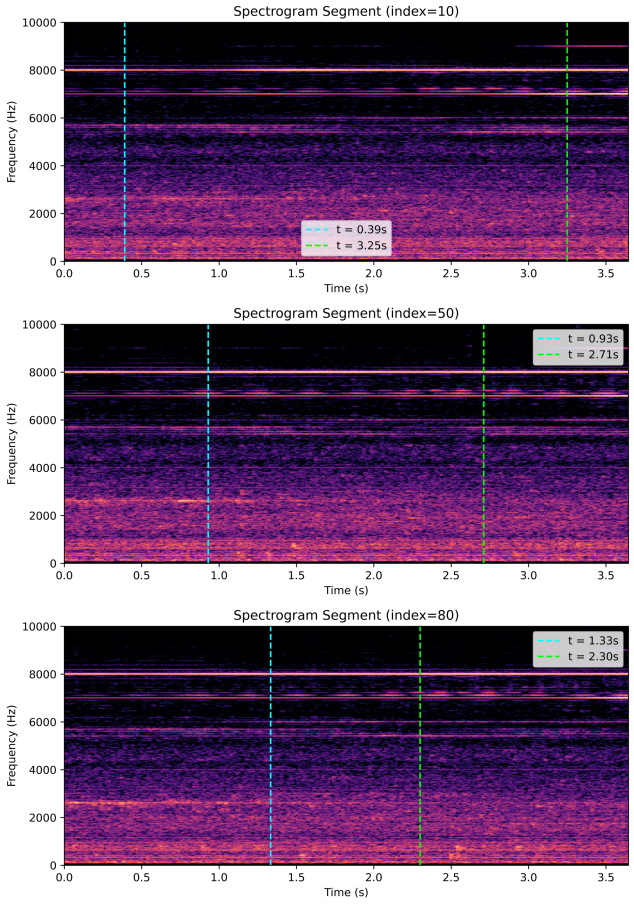

图8：不同片段的频谱图，以及正常路径与扩展路径之间发生转换的位置。

重建原始形状。我们可以将问题表述如下：

$$R(\mathbf{x}) = D(\mathbf{x}) - A(\mathbf{x})$$

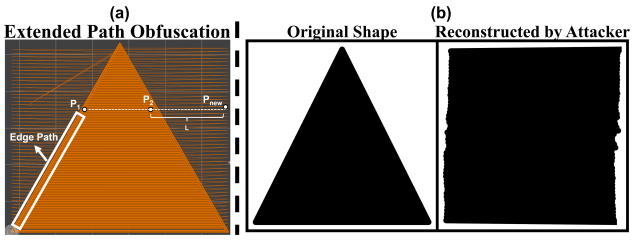

图9：(a) 沿同一方向添加一个共线点，将每条路径延伸至矩形边界，以混淆物体。(b) 左侧显示原始三角形，右侧显示攻击者从音频文件中解读出的结果。

优化形状的索引可通过以下方式求得：

$$\arg\max_{\mathbf{x}} \; R(\mathbf{x})$$

其中， D 表示优化形状与原始形状之间的差异度， A 表示优化形状中添加的白色点数量。我们选用普罗克拉斯提斯分析作为衡量两个形状差异度的指标。该算法使用缩放、旋转和平移等线性变换，将形状 Z 与形状 W 对齐 [15, 17]，并给出差异度指标；指标值越高，表示两个形状之间的差异越大。矩阵 Z 和 W 的大小相同，通过对第二个矩阵应用线性变换，我们的目标是最小化以下数值：

$$\mathrm{D} = \sum_{i=1}^{n} (\mathbf{Z}_i - \mathbf{T}(\mathbf{W}_i))^2,$$

值得注意的是，我们的两个指标 A 和 B 都是无量纲的，因为 A 是点的总数，而 D 是平方误差的最小总和。如算法2所示，我们首先获取原始形状及其凸包。然后，在满足两个条件的情况下，将随机矩形添加到随机位置。首先，矩形必须与凸包相交，并与原始形状重叠。其次，新添加的矩形必须与原始形状连通，以避免产生孤立连通分量。每次添加后，我们都会记录面积和差异度。此过程持续进行，直到修改后形状的面积超过凸包的面积。根据记录的数据，我们选择奖励最高的形状作为优化形状。我们还应用二值闭运算算法来填充形状内部的间隙和孔洞。尽管该算法对凹形效果良好，但可能不适用于凸形。例如，矩形或三角形的凸包就是其自身。在这种情况下，我们首先通过随机延长其长和宽，将形状包在一个更大的外接矩形内。然后，不再添加点，而是从外接矩形与原始形状之间的区域中随机移除点。算法结果如图10所示。如奖励曲线所示，奖励函数在某处达到峰值，此时新增面积较小，而差异度足够高。作为示例，我们对图10所示的钥匙对象应用了组合方法进行模糊处理。如图所示，使用SHM方法成功模糊了钥匙齿的重要信息。这个三层对象的正常打印时间约为258秒。SHM方法增加了约143秒，使打印时间延长了55%。我们还在图11中比较了钥匙示例的打印时间。打印时间是根据不同的进给速度计算的。进给速度是指喷嘴移动的速度。如图11所示，在较低速度下，SHM方法始终会带来线性开销，无论速度如何，因为总路径长度保持不变，且不需要恢复时间。

6.3 评估所提出的混淆方法

为了评估我们的方法，我们重新采用了之前的三角形示例，但这次将该形状包围在一个矩形多边形内（图

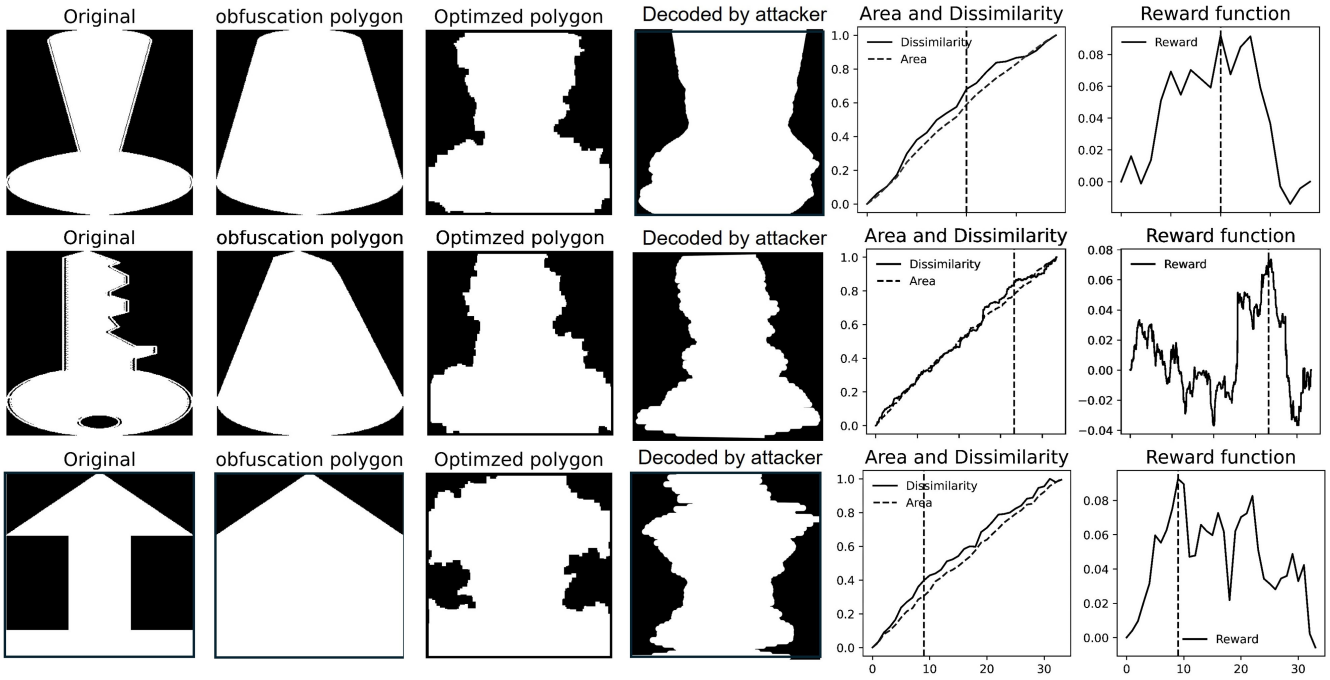

图10：该图展示了混淆算法的结果。第一列为原始形状，接下来依次是朴素混淆和优化混淆多边形。第四列展示了攻击者根据录制的音频重建出的形状。图中还显示了优化多边形的面积、差异度和奖励值。

9(a))，以屏蔽风扇噪声和突发的声学尖峰。录制并预处理音频后，我们检测出转折点并重建了对象。攻击者只能还原出外接矩形（图9(b)），而无法还原原始三角形。这表明，即使拥有完整的音频访问权限，原始对象仍然处于隐藏状态。优化后的隐蔽头部运动结果如图10所示。我们使用这一优化后的多边形进行混淆，打印该对象并录制音频，攻击者重建出的结果如图10所示。

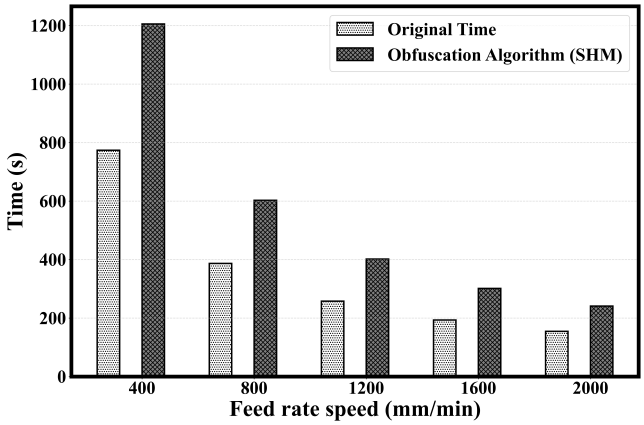

图11：比较了在不同打印速度下，针对钥匙样本的隐蔽头部运动算法的时间开销。

7 结论

在本研究中，我们首先考察了冷却风扇和步进电机噪声对数据泄露的影响。随后，我们采用尖峰检测方法重建基准形状。接着，我们提出了隐蔽式打印头运动（SHM）混淆算法，以隐藏运动模式。该方法确保即使攻击者检测到步进电机的突然运动或方向变化，也仍然无法重建完整物体。随后，我们对该方法进行了形式化描述，并给出了优化方案，以尽量缩短打印时间。我们方法的主要优势在于无需额外硬件，且与现有3D打印机完全兼容。实现时只需对G代码文件进行少量修改，以加入SHM算法，无需任何额外设置，例如降噪或噪声生成设备。

致谢

本研究得到了美国国家科学基金会资助项目 CCRI 2234972 的支持。本研究所表达的任何观点、结论、发现或建议均不一定反映资助机构的立场。

参考文献

[1] [全球3D打印市场规模、份额、最新趋势与增长分析（2024—2029年）— marketsandmarkets.com。https://www.marketsandmarkets.com/Market-Reports/3d-printing-market-1276.html。 [访问日期：14-07-2025]。[2] Muhammad Ahsan 和 Irfan Ahmed。2025年。WattShield：一种用于检测熔融长丝制造中恶意固件的功耗侧信道框架。

算法2 SHM算法 1：函数 AddRects($img,\ img_neg,\ n,$) 2：$out \leftarrow img$3：$(h, w) \leftarrow$ Shape(img) 4：for $i = 1$ to n do 5：for $j = 1$ to $attempt$ do 6：$rw \leftarrow$ RandInt(min_s, max_s) 7：$rh \leftarrow$ RandInt(min_s, max_s) 8：$x \leftarrow$ RandInt(0, $w - rw$) 9：$y \leftarrow$ RandInt(0, $h - rh$) 10：$r \leftarrow out[y{:}y{+}rh,\ x{:}x{+}rw]$11：$r2 \leftarrow img_neg[y{:}y{+}rh,\ x{:}x{+}rw]$12：if (Sum($r2$) $\wedge$Sum(r)) then 13：$out[y{:}y{+}rh,\ x{:}x{+}rw] \leftarrow$ 114：break 15：end if 16：end for 17：end for 18：return out19：end function 20：$convex_mask \leftarrow$凸_包络(img) 21：$img_neg \leftarrow \sim$ ($convex_mask$ & img_points) 22：$prev_i \leftarrow -$123：for $i = Start$ to $Stop$ step $Step$ do 24：if $prev_i <$ 0then 25：$prev_i \leftarrow Start -$ 10026：end if 27：$n \leftarrow i - prev_i$28：$result_img \leftarrow$AddRects($result_img,\ img_neg,\ n$) 29：$result_img \leftarrow$二值闭运算($result_img$) 30：$area_img \leftarrow$Sum($result_img$) 31：$area_convex \leftarrow$Sum($convex_mask$) 32：if $area_img > area_convex$ then 33：break 34：end if 35：$disp \leftarrow$普罗克拉斯提斯($result_img,\ img_points$) 36：$r2 \leftarrow result_img$ & img_neg37：$area \leftarrow$Sum($r2$) 38：Append($all_score,\ disp$) 39：Append($all_area,\ area$) 40：Append($all_shapes,\ result_img$) 41：$prev_i \leftarrow i$42：end for 43：$reward \leftarrow all\ \ area - all\ \ score_$ _44：$Optimized_idx \leftarrow arg$max($reward$) 45：$Optimized_shape \leftarrow all_shapes[Optimized_idx]$

载于*2025*年*IEEE*硬件导向安全与可信国际研讨会（*HOST*）。*IEEE*。[3] Mohammad Abdullah Al Faruque、Sujit Rokka Chhetri、Arquimedes Canedo和Jiang Wan。2016年。针对增材制造系统的声学侧信道攻击。载于*2016*年*ACM/IEEE*第七届信息物理系统国际会议（*ICCPS*）。IEEE，第1–10页。[4] Osama T AlShaheen、Zeashan H Khan和Samir N Mekid。2024。RDM-3D：用于3D打印机性能监控的远程仪表板。载于*2024*年创新工程科学与技术研究第一届国际会议（*ICIESTR*）。IEEE，第1–5页。

[5] Seyed Ali Ghazi Asgar 和 Narasimha Reddy。2025。配置错误的物联网 MQTT 部署分析及轻量级暴露检测系统。载于网络与分布式系统安全（NDSS）研讨会、标准化物联网安全与隐私研讨会（SDIoTSec）。[6] Seyed Ali Ghazi Asgar、Narasimha Reddy 和 Satish T. S. Bukkapatnam。2025。永不信任制造商，永不信任客户端：一种用于安全增材制造的 STL 文件流传输新方法。arXiv:2507.06421 [cs.CR] https://arxiv.org/abs/2507 06421。[7] F W Baumann、T Ludwig、N Darwin Abele、S Hoffmann 和 D Roller。2017。用于增材制造的模型数据流传输：保护知识产权。《智能与可持续制造系统》1，1（2017），142–152。[8] Christian Bayens、Tuan Le、Luis Garcia、Raheem Beyah、Mehdi Javanmard 和 Saman Zonouz。2017。非视、非听、非感、非打印？增材制造中恶意填充图案的检测。载于第 26 届 USENIX 安全研讨会（USENIX Security 17）。1181–1198。[9] Twisha Chattopadhyay、Fabricio Ceschin、Marco E Garza、Dymytriy Zyunkin、Animesh Chhotaray、Aaron P Stebner、Saman Zonouz 和 Raheem Beyah。2025。一段视频窃取一切：通过光学侧信道窃取 3D 打印知识产权。arXiv 预印本 arXiv:2506.21897（2025）。[10] Sujit Rokka Chhetri、Arquimedes Canedo 和 Mohammad Abdullah Al Faruque。2017。信息物理增材制造系统中通过声学侧信道造成的机密性泄露。《ACM 信息物理系统汇刊》2，1（2017），1–25。[11] Tarasankar DebRoy、Huiliang L Wei、James S Zuback、Tuhin Mukherjee、John W Elmer、John O Milewski、Allison Michelle Beese、A de Wilson-Heid、Amitava De 和 Wei Zhang。2018。金属部件的增材制造——工艺、结构与性能。《材料科学进展》92（2018），112–224。[12] Tonica P Garcia、Aimee Rachel O Aguilar、Juliah Faye T Dela Vega、Mary Mar-garette S Macatumpag、Mhikaella Mae M Vaay、Richard Josiah C Tan Ai、Ryan Rhay P Vicerra、Argel A Bandala 和 Elmer P Dadios。2023。通过 MQTT Sparkplug B 协议将 3D 打印机接入工业物联网（IIoT）。载于 2023 IEEE 第 15 届人形机器人、纳米技术、信息技术、通信与控制、环境及管理国际会议（HNICEM）。IEEE，1–6。[13] Jacob Gatlin、Sofia Belikovetsky、Yuval Elovici、Anthony Skjellum、Joshua Lubell、Paul Witherell 和 Mark Yampolskiy。2021。加密无济于事：利用功耗侧信道重建 3D 打印模型。载于第 24 届攻击、入侵与防御研究国际研讨会论文集。135–147。[14] Ian Gibson、David W Rosen、Brent Stucker、Mahyar Khorasani、David Rosen、Brent Stucker 和 Mahyar Khorasani。2021。增材制造技术。第 17 卷。Springer。[15] John C Gower。2010。普罗克鲁斯忒斯方法。《Wiley 跨学科评论：计算统计》2，4（2010），503–508。[16] Amirhossein Jamarani、Yazhou Tu 和 Xiali Hei。2025。实践者论文：解码知识产权：针对 3D 打印机的声学与磁性侧信道攻击。载于信息物理系统与智能车辆安全和隐私国际会议。Springer，54–74。[17] Wojtek Krzanowski。2000。多变量分析原理。第 23 卷。牛津大学出版社。[18] Ireneusz Kubiak、Artur Przybysz 和 Andrzej Stańczak。2020。3D 打印机的声学声音在窃听过程及打印形状重建中的用途。《电子学》9，2（2020），297。[19] Sizhuang Liang 和 Raheem Beyah。 [无日期]。隐藏真实的自我！保护增材制造系统中的知识产权免受光学侧信道攻击。[20] Christos Madamopoulos 和 Nektarios Georgios Tsoutsos。2024。用于增材制造安全漏洞研究的 3D 打印机音频与振动侧信道数据集。《数据简报》57（2024），111002。[21] Zahid Mohammed、Abdullah Shahwan、Ali Alazawi 和 Wael Elmedany。2025。增强物联网通信安全：MQTT、CoAP 和 XMPP 协议中的漏洞分析与缓解。[22] Hammond Pearce、Kaushik Yanamandra、Nikhil Gupta 和 Ramesh Karri。2022。FLAW3D：针对增材制造物理结果的特洛伊木马网络攻击。《IEEE/ASME 机电一体化汇刊》27，6（2022），5361–5370。doi:10.1109/TMECH.2022.3179713[23] Muhammad Haris Rais、Muhammad Ahsan 和 Irfan Ahmed。2024。SOK：针对熔融长丝制造的 3D 打印机固件攻击。载于第 18 届 USENIX 攻击性技术会议论文集（美国宾夕法尼亚州费城）（WOOT'24）。USENIX 协会，美国，第 18 篇文章，共 20 页。[24] Muhammad Haris Rais、Muhammad Ahsan 和 Irfan Ahmed。2025。通过低幅度动力学操纵攻击破坏材料挤出式 3D 打印部件。《ACM 信息物理系统汇刊》9，1（2025），1–26。[25] Jost Rossel、Vladislav Mladenov 和 Juraj Somorovsky。2023。3MF 数据格式的安全性分析。载于第 26 届攻击、入侵与防御研究国际研讨会论文集。179–194。

[26] Jost Rossel、Vladislav Mladenov、Nico Wördenweber 和 Juraj Somorovsky。[无日期]。3D 打印中恶意 G 代码的安全影响。（[无日期]）。[27] Chen Song、Feng Lin、Zhongjie Ba、Kui Ren、Chi Zhou 和 Wenyao Xu。2016年。我的智能手机知道你打印的内容：探索针对 3D 打印机的基于智能手机的侧信道攻击。载于*2016 年 ACM SIGSAC 计算机与通信安全会议论文集*。895–907。[28] Keval K Sonigara、Jayraj V Vaghasiya、Carmen C Mayorga-Martinez 和 Martin Pumera。2025年。将 3D 打印废料在使用点升级再造，以开发 3D 打印锌碘电池。《材料化学*A*辑》13，16（2025），11804–11816。[29] Andrzej Stańczak 和 Ireneusz Kubiak。2023。评估保护三维打印机免受声学渗透的有效性。《电子学》12，22（2023），4641。[30] Andrzej Stańczak、Ireneusz Kubiak、Artur Przybysz 和 Anna Witenberg。2021。根据打印机振动重建物体形状的可能性

在增材打印过程中。《应用科学》11, 11（2021），5305。[31] Shubham Bhaskar Thakare 和 Sanjay Poddar。2025年。安全的机械设计与制造：通过网络安全防止知识产权盗窃。《国际科学与研究档案期刊》14, 2（2025年），638–645。[32] Akash Tiwari、A L Narasimha Reddy 和 Satish T S. Bukkapatnam。2020年。新兴制造即服务（制造即服务）范式中的网络安全保障：来自视频流媒体行业的经验。《智能与可持续制造系统》4, 3（2020），324–329。[33] Syed A M Tofail、Elias P Koumoulos、Amit Bandyopadhyay、Susmita Bose、Lisa O'Donoghue 和 Costas Charitidis。2018年。增材制造：科学与技术挑战、市场应用及机遇。《今日材料》21, 1（2018），22–37。[34] Steven Eric Zeltmann、Nikhil Gupta、Nektarios Georgios Tsoutsos、Michail Ma- niatakos、Jeyavijayan Rajendran 和 Ramesh Karri。2016年。3D 打印中的制造与安全挑战。《JOM》68, 7（2016），1872–1881。