著名密码学算法获得升级

原文： Celebrated Cryptography Algorithm Gets an Upgrade

作者： Madison Goldberg

译者： Mengce Zheng

日期： 2024 年 11 月 25 日

两位研究人员改进了一种众所周知的格基约化技术，为密码学和数学的实际实验开辟了新的途径。

在我们日益数字化的生活中，安全性取决于密码学。发送私人消息或在线支付账单，您所依赖的算法是为了确保数据保密。自然，有些人想要揭开这些秘密——因此研究人员努力测试这些系统的强度，以确保它们不会在聪明的攻击者手中崩溃。

这项工作中的一个重要工具是 LLL 算法，该算法以 1982 年发表该算法的研究人员 Arjen Lenstra、Hendrik Lenstra Jr. 和 László Lovász 的名字命名。LLL 及其许多后继算法在某些情况下可以破坏加密方案；研究它们的行为方式有助于研究人员设计不易受到攻击的系统。

而多年来，研究人员已经打磨了 LLL 的变体，以使得该方法更加实用——但仅限于一定程度。现在，一对密码学家构建了一种新的 LLL 类型算法，效率显著提高。这项新技术在 2023 年国际密码学会议（Crypto 2023）上获得了最佳论文奖，拓宽了计算机科学家和数学家可以使用类似 LLL 的方法的场景范围。

“这真的很令人兴奋，”密歇根大学（University of Michigan）的密码学家克里斯 • 佩克特（Chris Peikert）说，虽然他没有参与这篇论文。他说，几十年来，该工具一直是研究的重点。“当一个已经努力了这么久的目标..... 表明仍然有惊喜等待发现。”

LLL 类型的算法在格的世界中运行：规则间隔点的无限集合。作为可视化的一种方式，假设您正在平铺地板。你可以用方形瓷砖覆盖它，这些瓷砖的角将构成一个格。或者，您可以选择不同的图块形状（例如，长平行四边形）来创建不同的格。

格可以使用其“基”来描述。这是一组向量（本质上是包含数字的列表），您可以以不同的方式组合它们以获得格中的每个点。让我们想象一个基由两个向量组成的格：$[3, 2]$ 和 $[1, 4]$。格就是您可以通过添加和减去这些向量的复制来获得的所有点。

这对向量并不是格的唯一基。每个至少具有二维的格都有无限多个可能的基。但并

非所有基都是平等的。向量更短且彼此更接近直角的基通常更容易使用，并且对于解决某些计算问题更有用，因此研究人员称这些基为“好”。由较长且较不正交的向量组成的基可以被视为“坏”。

这就是 LLL 的工作：输入给定一个多维格的基，它会输出一个更好的基。这个过程称为格基约化。

这一切与密码学有什么关系？事实证明，在某些情况下，破解密码系统的任务可以改写为另一个问题：在格中找到一个相对较短的向量。有时，该向量可以从 LLL 类型算法生成的约化基中提取。这种策略帮助研究人员推翻了从表面上看似乎与格无关的系统。

从理论上讲，原始的 LLL 算法运行速度很快：运行所需的时间不会随输入的大小——格的维度和基向量中数字的大小，呈指数级增长。但时间复杂度确实以一个多项式函数形式增加，“如果你真的想这样做，多项式时间并不总是那么可行，”荷兰国家研究机构 CWI 的密码学家，利奥·杜卡斯（Léo Ducas）说。

实际上，这意味着原始 LLL 算法无法处理太大的输入。“数学家和密码学家希望能够做更多的事情，”加州大学圣地亚哥分校（University of California, San Diego）的博士生基冈·瑞安（Keegan Ryan）说。研究人员致力于优化 LLL 类型的算法以适应更大的输入，通常可以取得良好的性能。尽管如此，一些任务仍然顽固地遥不可及。

这篇新论文由瑞安和他的导师纳迪亚·海宁格（Nadia Heninger）一同撰写，结合了多种策略来提高其 LLL 类型算法的效率。首先，该技术使用递归结构将任务分解为更小的块。另一方面，该算法会仔细管理所涉及数字的精度，在速度和正确结果之间找到平衡。这项新工作使研究人员能够约化具有上千维数的格基。

过去的工作遵循了类似的方法：2021 年的一篇论文同样结合了递归结构和精度管理，以快速处理大维数的格，但它仅适用于特定类型的格，而不适用于密码学中重要的所有格。新算法在更广泛的范围内表现良好。“我真的很高兴有人做到了，”PQShield 公司的密码学研究员，同时也是上述论文的作者——托马斯·埃斯皮陶（Thomas Espitau）说，他们团队的工作提供了‘概念验证’，新结果表明：你可以通过合理的方式进行非常快速的格基约化。”

这项新技术已经开始被证明是有用的。法国国家研究机构 Inria 的数学家奥雷尔·佩奇（Aurel Page）表示，他和他的团队已经对该算法进行了改编，以完成一些计算数论任务。

LLL 类型的算法还可以在与基于格的加密系统相关研究中发挥作用，格密码系统设计目标在于即使在拥有强大量子计算机的未来也能保持安全。但它们不会对此类系统构成威胁，因为要摧毁它们需要找到比这些算法所能达到的更短的向量。但研究人员所知

道的最好的攻击是使用 LLL 类型的算法作为“基本构建模块”，波尔多大学（University of Bordeaux）的密码学家韦塞尔·范·沃尔登（Wessel van Woerden）说。在研究这些攻击的实际实验中，该构建模块可以减慢一切速度。使用新工具，研究人员可能能够扩大他们可以对攻击算法进行的实验范围，从而更清楚地了解它们的性能。

注：本文为基于人工智能技术的翻译，若需了解详细信息，请参考原文出处。