新闻动态
图片新闻
头条新闻
综合新闻
学术活动
科研动态

研究院十年庆典
研究院电子政务平台
用户名:
密码:
登录
中科院邮件系统
国家自然科学基金委

SEARCH
GO
院长信箱
地理位置

潘彦斌、邓映蒲完全攻破Cai-Cusick格密码体制

2011-10-08 | 编辑：

2011年3月，国际著名期刊IEEE Transactions on Information Theory刊登了国家数学与交叉科学中心潘彦斌和邓映蒲关于Cai-Cusick格密码体制的论文，其审稿意见认为该密码体制已被完全攻破。Cai和 Cusick于1998年提出的一个基于格的可实用的公钥密码体制，十余年来许多密码学家包括Shamir都曾试图攻击它，但都没有成功。潘彦斌和邓映蒲给出了它的一个唯密文攻击，时间复杂性是多项式的，从而彻底攻破了该存在有十多年的密码体制。

在当今互联网时代,各个国家都非常重视密码学的理论和技术的研究。现代密码学由对称密码学和公钥密码学组成，对称密码包括流密码和分组密码，对称密码由于速度快、安全性高而用来加密海量的信息，而公钥密码用来加密对称密码体制的密钥，两者在解决信息安全问题时都是非常重要、不可或缺的。

目前流行的公钥体制主要包括基于大整数分解问题的RSA和基于椭圆曲线上离散对数问题的公钥体制，即ECC。这些体制有一个共同的弱点，即不能抵抗量子攻击。因此，一旦实用的量子计算机出现，这些体制将可能被攻破，从而被淘汰。而且随着计算机技术的飞速发展，这些体制也逐渐遭受一些新的威胁。因此，寻找新的公钥体制，特别是能抵抗量子攻击的公钥体制，便成为一件重要而迫切的工作。

而格密码恰恰被认为是后量子时代最主要的公钥体制之一，它以能抵抗量子攻击、平均安全性可以建立在格问题最坏情况复杂性及快速的加解密速度等优点受到了广泛的关注。Cai-Cusick格密码体制是蔡进一和Cusick于1998年在加拿大的国际会议SAC上提出的，他们认为Cai-Cusick体制具有合理的密钥规模，并讨论了Cai-Cusick体制的参数设置，以使得该体制能够抵抗一些已有的和潜在的攻击，并能有效防止信息的统计泄漏。

国际上很多密码分析学者都曾试图攻击Cai-Cusick格密码体制，但都没有取得成功。潘彦斌和邓映蒲改变了以往密码分析学者试图恢复私钥的做法，直接从恢复消息入手，成功地给出了十余年来首个对Cai-Cusick体制的有效的唯密文攻击，彻底攻破了该体制。

密码学中对公钥密码体制的攻击有几种，包括唯密文攻击，选择密文攻击，广播攻击等，其中最难的就是唯密文攻击，因为它需要的条件最少，要求只通过公钥和密文就把消息恢复出来，而获得公钥和密文也是在现实攻击中最容易满足的条件。因此，一旦唯密文攻击成功，其它的攻击就不需要了，也就宣告该公钥体制被彻底攻破了。从复杂性的角度来看，所提的攻击防范可以在多项式时间内完成，是可以具体实施的彻底而有效的攻击。

另外，这种攻击所提出的算法也可以作为衡量新的格密码体制安全性的一个标准，并用于攻击一些类似的格密码体制。

[关闭窗口]