
29岁成武大最年轻正教授！当事人希望“先埋头做事”

作者：writer 来源：科学网

本文原地址：<https://www.iikx.com/news/progress/32237.html>

本文仅供学习交流之用，版权归原作者所有，请勿用于商业用途！

29岁成武大最年轻正教授！当事人希望“先埋头做事”。文 | 《中国科学报》记者李思辉
实习生 张曦月

3月15日，武汉大学发布消息，29岁赵莽获聘为该校教授。这位刚刚结束8年海外求学、回国任教的青年学者成为武汉大学最年轻的正教授。

面对外界的关注，赵莽告诉《中国科学报》：“毕竟刚回来，希望先埋头做些事情。”



赵莽签约入职武汉大学 武汉大学供图

“ 95后 ”

作为“ 95后 ”的赵莽，2016年前往德国萨尔大学求学，主修计算机科学，同时辅修数学。

本科毕业后，他获得硕博连读资格，师从国际密码学权威、前牛津大学终身教授Cas Cremers。在Cremers的课题组里，他深入研究通信安全、身份认证等关键领域，主导多个国际前沿项目，并与全球顶尖学者展开合作。

赵莽的研究方向——应用密码学，听起来高深莫测，但其实与每个人的日常生活息息相关。从社交软件的聊天加密到网上银行的安全交易，再到无密码认证系统，每一个环节都离不开密码学的保障。

“ 密码学就像是在解一道永远没有标准答案的数学题。你知道它存在解法，但你需要不断探索、尝试，才能找到最优解。 ” 赵莽介绍。



赵莽 武汉大学供图

学成

在博士期间，赵莽主导并参与了非对称认证算法、带有关联数据的认证加密算法、无密码认证协议、多方实时通信协议、即时通信协议等多个课题，并多次在国际顶级安全会议上发表论文。

其中，最具突破性的一项研究是针对FIDO2（WebAuthn 2与CTAP 2.1）协议的安全性分析。

这项协议旨在替代传统的密码系统，实现更安全的无密码认证。然而，赵莽发现，尽管这一协议在应对传统攻击方面表现出色，但其在抵御量子计算攻击方面仍存在隐患。

为此，赵莽提出了WebAuthn 2和CTAP 2.1的全球第一个后量子实例化扩展，在国际学术界引起广泛关注。这项研究为未来网络安全提供了重要保障，也获得了微软安全响应中心的资助支持。

除了研究密码协议的安全性，赵莽还积极推动学术研究与现实应用的结合。例如，他的团队在对Ed25519数字签名算法进行安全性分析时，发现不同版本的算法在安全性上存在显著差异。

最终，这项研究成果被IEEE Symposium on Security and Privacy（IEEE SP）接收，并被万维网联盟（W3C）认可为Ed25519签名安全性的权威分析。

这些研究让赵莽在密码领域声名鹊起。

回国

2023年1月，赵莽受邀回国，在武汉大学做了一场学术报告。在与武大国家网络安全学院的老师们深入交流后，他惊喜地发现，这里的研究方向与自己高度契合。

而更让他心动的是，学院对密码学研究的重视程度，以及希望推动中国在这一领域取得更多自主突破的决心。

当武大向他抛出橄榄枝时，他几乎没有犹豫——回国，成为一名教师和研究者。

武大为赵莽提供了优厚的待遇和科研支持，包括60万年薪、30万雷军教育基金支持、200万的安家费以及8个博士生指标等。对于他而言，这不仅是待遇上的保障，更是一种科研环境的承诺——他可以迅速建立自己的研究团队，继续推进密码学研究的前沿探索。

尽管从博士生到教授的“跨越式”身份转变带来了不小的挑战，“最年轻教授”的名头也给他增加了曝光度，但他更希望安静下来，先埋头做些事情。

作者：李思辉，张曦月 来源：科学网微信公众号

更多 科学进展 请访问 <https://www.iikx.com/news/progress/>

本文版权归原作者所有，请勿用于商业用途，[爱科学iikx.com](https://www.iikx.com)转发