

2026

2026

*A Fantastical Journey into AI
Exploration and Security*

AI探秘与安全守 护的奇幻漂流



07.18 — 07.19



AI EXPLORATION & SECURITY

Zhejiang University. Harbin Institute of Technology, Shenzhen. Renmin University of China

Chapter 1

AI大模型科普

AI朋友本领大，隐私秘密要藏好。真假对错要分辨，独立思考不能少。爸妈陪伴更安心，快乐学习没烦恼！

CONTENTS

01

认识AI大模型

揭开AI大模型的神秘面纱，探索其核心定义与技术本质

03

我们常用的AI大模型

认识ChatGPT、文心一言等热门AI模型，领略技术风采与特色

05

AI使用安全手册

了解AI使用的伦理边界、隐私保护与安全规范，健康探索智能

02

呢

解密AI的学习机制，从海量数据训练到模型迭代进化的奥秘

04

AI指令的魔法

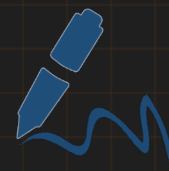
掌握提示词工程核心技巧，解锁与AI高效交互的实用秘诀

AI大模型如何学习



01

认识AI大模型



- 它就像一个超级爱读书的机器人学霸，从诞生起就沉浸在海量的知识海洋中不断学习
- 它不是真正的人类，但却比任何单一个体更“博学”，能快速整合并应用全球海量信息



AI：超级学霸机器人

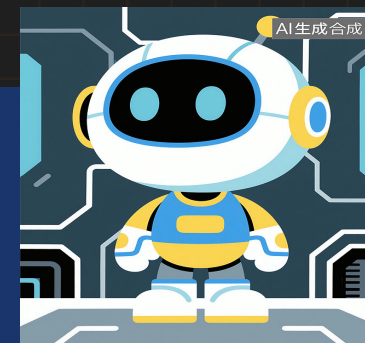
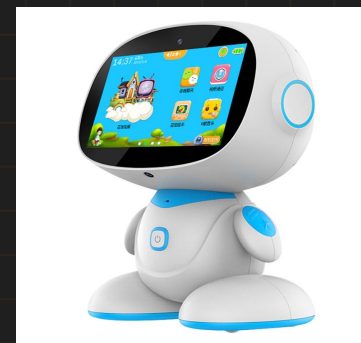
它是从出生就开始疯狂阅读的机器人，知识量远超人类总和！

想象一下，有个机器人从诞生起就泡在书海里，读的书比全人类加起来还多！语文、数学、科学课本是它的基础，连菜谱、新闻、漫画都不放过。

它的大脑装着整个世界的知识，问它恐龙灭绝、月亮的奥秘，它都能秒答，就像一部行走的超级百科全书，无所不知，无所不晓！

它还是个“超级模仿大师”，解锁超多有趣技能！

看了无数人类作品，它学会了像人一样写字、画画、聊天。写的作文生动又新奇，画的画脑洞大开超奇妙，聊天时还能接住你的所有梗，像个懂你的好朋友。



它不是真正的人，但比你更“博学”

虽然AI大模型看起来无所不知、十分聪明，但它和我们人类有着本质的不同，并不是真正有生命的“人”哦！

首先，它没有真正的大脑和意识。AI的“智慧”来自超级电脑集群和复杂算法，它不会像我们一样思考、感受情绪，也不会做梦或产生自我意识，只是在高速处理和匹配数据而已。

其次，它的知识全靠“海量阅读”。它知道的一切都来自人类投喂的海量信息，如果学习的资料里有错误，AI也会跟着学到错误的内容，甚至会一本正经地“胡编乱造”，也就是出现我们所说的“AI幻觉”，所以它的答案不一定全是对的。

最后，它需要你的指令驱动。AI就像一个安静的魔法精灵，不会主动做任何事，必须等你下达清晰的指令，它才会根据要求去生成内容或解决问题，没有你的指挥，它就只是一个沉睡的程序。



02

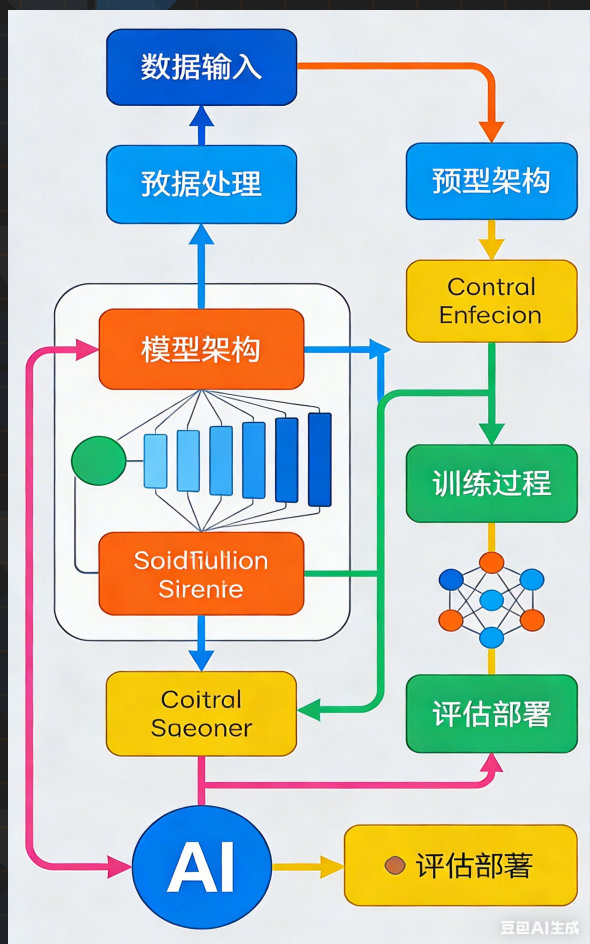
AI模型如何学习呢

- AI的学习三部曲：海量阅读、做练习题、老师打分
- 揭秘AI变得越来越聪明的核心秘密



学霸养成记：AI学习三部曲

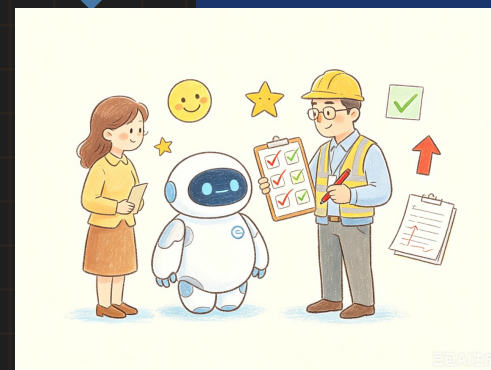
AI的学习过程就像小朋友上学一样，有着趣味十足的“学习三部曲”，一步步从懵懂变得博学：



01 海量阅读：如同小朋友学认字、读绘本，AI会“啃”下亿万级的书籍和资料，疯狂汲取各类词语、知识与世间万象的信息。

02 做练习题：就像我们写课后作业，AI会通过回答海量的问题来练习，把学到的知识反复运用，不断巩固和熟练掌握。

03 老师打分：工程师叔叔阿姨扮演“老师”的角色，给AI的答案打分、纠错，告诉它哪里回答得好，哪里有问题，帮助它不断修正进步。



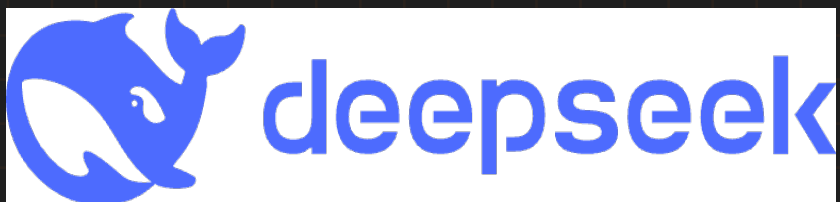
03

我们常用的AI大模型

- 豆包：懂你的智能助手
- 文心一言：知识渊博的伙伴
- ChatGPT：全能对话专家
- 各具所长的AI “尖子生”

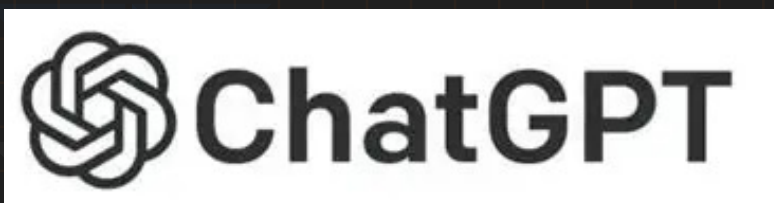


认识几位AI学霸明星



01. 豆包 (Doubao) —— 懂你的全能伙伴

它是最懂中文的AI小能手，不仅能像朋友一样陪你聊天谈心，还能帮你**拍照改作文、规划周末活动、解答生活里的各种小疑问**，是学习和生活中贴心又靠谱的好帮手。



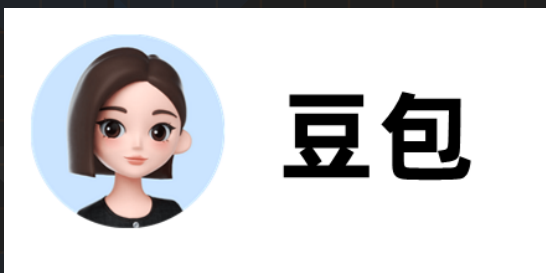
02. ChatGPT —— 创意满分的知识大师

这位AI拥有超丰富的知识储备，就像一个装满智慧的百宝箱。无论是回答天文地理的问题，还是帮你**编写童话、创作诗歌，甚至是出谋划策想点子**，它都能给你带来满满的惊喜和灵感。



03. 文心一言 —— 严谨耐心的学习辅导员

它像一位认真负责的老师，严谨又细致。遇到不会的难题，**它会一步步帮你梳理思路、讲解答案**；学习上需要**总结知识点**，它也能帮你整理得清清楚楚，是辅导我们高效学习的好助手。



04

AI指令的魔法

- 学会“指挥”你的学霸朋友
- 神奇的Prompt四要素



神奇的Prompt四要素

一个好的Prompt，就像给AI一张清晰的地图，它才能准确理解需求并抵达目标。掌握这四大核心要素，你就能精准指挥AI！

01 明确角色：赋予AI身份定位

先告诉AI它需要扮演什么角色，比如“一位温柔的幼儿园老师”“专业的美食家”或“资深的产品经理”。清晰的角色设定能让AI的回答贴合场景，语气和视角也会更精准。

02 下达任务：提出具体行动指令

清晰说明你希望AI完成的**具体工作**，比如“为春游写一首儿童诗”“设计一份减脂餐食谱”或“分析这篇新闻的核心观点”。任务越具体，AI的产出就越不容易偏离你的预期。

03 补充要求：细化结果的标准

给结果加上**具体的约束条件**，比如“诗歌要押韵、语言活泼”“食谱要包含早餐和晚餐、做法简单”“分析内容分三点、不超过300字”。这些细节能让AI的回答更符合你的实际需求。

04 规定格式：指定答案的呈现形式

告诉AI你想要的**输出形式**，比如“用分点列表呈现”“以对话形式展开”“写成一段优美的散文”或“整理成对比表格”。合适的格式能让信息更易读，也更便于你后续使用。



有趣的Prompt应用实例（一）

01. 专属私教模式

💡 **核心指令：**“请扮演耐心的小学数学老师，用最通俗的语言，一步步教我计算长方形面积，还要举个生活里的例子帮助我理解。”

✨ **应用效果：**化繁为简的知识陪伴

“请扮演耐心的小学数学老师，用最通俗的语言，一步步教我计算长方形面积，还要举个生活里的例子帮助我理解。”

长方形面积超通俗讲解（小学数学版）

第一步：先搞懂两个基础词

1. **长：**长方形横着那条长边的长度
2. **宽：**长方形竖着那条短边的长度
3. **面积：**这个长方形平平的表面，到底有多大（不是边长多长，是整块平面大小）

第二步：最简单的道理 —— 用小方块理解

咱们拿边长 1 厘米的小正方形当“标准小块”，1 个小方块的面积就是 1 平方厘米。

- 一个长 3 厘米、宽 2 厘米的长方形：
横着能摆 3 个小方块，竖着能摆 2 排
总块数 = 一排数量 × 排数 = $3 \times 2 = 6$ 块
一共 6 个小方块，面积就是 6 平方厘米

💡 **关键技巧：**指定身份 + 要求通俗 + 结合实例，让知识不再“高冷”。

02. 视频创作大师

🎬 **核心指令：**“请生成一个10秒的短视频。主题是一只可爱的小猫在阳光下追逐蝴蝶。风格要求：治愈系动画，色彩明亮温暖，镜头缓慢推进，最后有小猫打哈欠的可爱特写。”

🎥 **应用效果：**生成符合描述的视频



💡 **关键技巧：**明确主题 + 指定风格 + 描述镜头，让视频更具电影感。



有趣的Prompt应用实例（一）



04. 音乐创作大师



核心指令：“请为一段关于春天的视频生成背景音乐。风格要求：轻松、愉悦的钢琴曲，节奏明快，有鸟鸣和流水的声音作为点缀。”

春之愉悦乐章

“请为一段关于春天的视频生成背景音乐。风格要求：轻松、愉悦的钢琴曲，节奏明快，有鸟鸣和流水的声音作为点缀。”



关键技巧：AI能理解文字描述的情绪和场景，生成符合氛围的背景音乐，为视频增添感染力。关键技巧：描述场景 + 指定风格 + 加入音效，让音乐更生动。



05. 绘本插画大师



核心指令：“请生成一张儿童绘本风格的插画。画面中有一只穿着红色斗篷的小兔子，在森林里提着一盏灯笼。风格要求：色彩温暖，线条柔和，充满童话感。”



关键技巧：AI能根据描述生成符合绘本风格的可爱插画，让故事有生动画面。关键技巧：明确主体 + 描述场景 + 指定风格，让画面更具艺术感。



05

AI使用安全手册

- 和AI安全地玩耍
- 建立AI使用安全底线
- 记住你的“安全魔法口诀”
- 守护个人隐私不泄露



如何和AI安全地玩耍？

记住下面几条“安全魔法口诀”，让AI成为你的好伙伴

！

01 守护秘密

不告诉AI真实姓名、住址、电话、学校等私密信息，把隐私牢牢锁在心里。



02 火眼金睛

AI说的话不一定全对，遇到不懂或重要信息，要查课本、问老师或爸妈确认。



03 拒绝作弊

写作业、做卷子要自己动脑，不用AI直接写答案，让AI帮你解释难题才是正确用法。



04 遵守“红绿灯”

看到奇怪、吓人的内容立刻喊“停”，使用AI时要在爸妈看得见的地方，让他们把关。



安全小口诀

AI朋友本领大，
隐私秘密要藏好，
真假对错要分辨，
独立思考不能少，
爸妈陪伴更安心，
快乐学习没烦恼！
安全用AI，快乐成长！

让我们一起做一个聪明、安全的AI小用户吧！



特别提醒：小学生需家长陪同

根据国家《指南》：小学阶段的小朋友不可独自使用AI大模型哦！

为什么需要陪伴？

这就像我们过马路需要大人牵着，使用AI这个强大的工具也需要爸爸妈妈的陪伴与指导。有了家长的把关，我们才能更好地分辨信息真假，避免受到不良内容的影响，让AI真正成为学习的好帮手。

陪伴的意义

这不仅是规则的要求，更是给我们的安全保护，就像雨天的小伞，为我们挡住数字世界里可能出现的“风雨”。让我们在爸爸妈妈的守护下，和AI一起健康成长！



豆包AI生成



Chapter 2

数字世界安全通关课

AI 让数字世界更好玩了，但也让骗子更“聪明”了。这一站，我们不当“数字小白”，要当“安全小卫士”——四道关卡，一层层打通，拿到你的通关护照。

CONTENTS

01

信息安全

我在网上留下了什么

02

网络文明

网上说话也要像面对面一样礼貌

03

反诈防骗

看到诱惑先停一下

04

守法公民

网上线下都守规则



第1关：信息安全

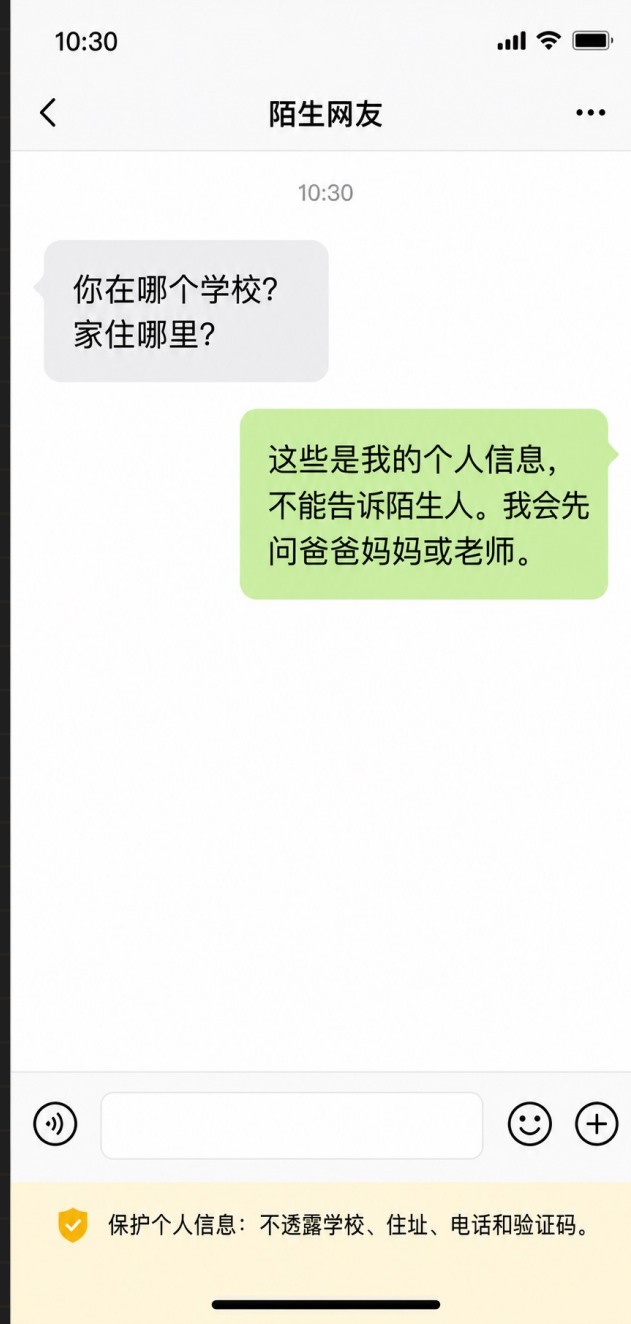


第1关：信息安全

哪些信息可以说，哪些信息要保护？

如果陌生网友问你：
“你在哪个学校？家住哪里？”

答案不是“赶紧回复”，
而是：先停下，问大人。



那些属于个人信息？

不是只有身份证号才叫隐私

- 姓名、学校、班级、家庭住址、电话
- 照片、定位、家门口/小区门牌号
- 账号密码、验证码、支付信息
- 家长电话、家人工作单位、出行安排

！红色提醒

验证码、密码、支付信息：绝对不能告诉别人。

照片和定位：发之前想一想，会不会暴露自己在哪里。



关系	姓名	出生年月日	家庭现住住址	婚否	联系电话
父亲	3				0
母亲					
兄/弟 姐/妹					
兄/弟					

口诀：要信息、要密码、要验证码，先停下，问大人。



情景判断：这些能不能告诉别人？

举手回答：可以 / 要小心 / 绝对不行

网友问：你在哪个学校？可以说吗？

判断：要小心

网友说送你游戏皮肤，让你发验证码。可以发吗？

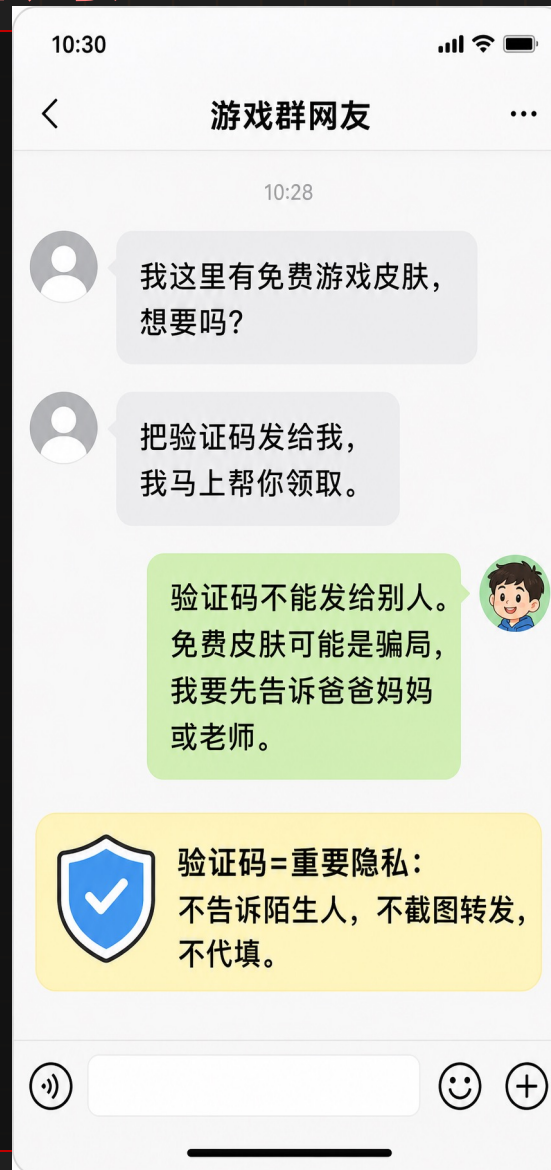
判断：绝对不行

领奖页面让填爸爸电话。可以直接填吗？

判断：要问大人

告诉同学今天午饭吃什么。可以说吗？

判断：通常可以



第2关：网络文明



网上说话也要像面对面一样文明



礼：网络不是“没人管的地方”

屏幕对面也是真实的人。
一句嘲笑、一张丑照、
一次跟风转发，
都可能伤害别人。



文明表达三件事

- 1 不骂人，不起侮辱性外号。
- 2 不曝光别人照片。
- 3 不转发未经确认的消息。

谢谢提醒！
我会注意的~ 😊



?

如果别人把你的丑照发到群里，你会是什么感受
屏幕对面也是人，网上也要讲礼貌



这是玩笑，还是伤害？

红灯绿灯：大家一起判断

01



把同学照片做成
表情包发群里



红灯：可能伤害别人



建议：不拍、不传、不起哄。

02



游戏输了
就在聊天框骂队友



红灯：不文明



建议：冷静表达，不能骂人。

03



看到消息
先问老师再转发



绿灯：会核实



建议：不确定，先求证。

04



提醒同学不要
公开别人隐私



绿灯：会保护



建议：隐私信息，不随便发。



第3关：反诈防骗



看到这些“好事”，先亮“**红灯**”



! 只要听到这些词，就先停一下：是真的吗？要不要问老师





AI EXPLORATION & SECURITY

Zhejiang University, Harbin Institute of Technology, Shenzhen, Renmin University of China

看到这些“好事”，先亮“红灯”

01 扫码领免费游戏皮肤



情景：有人私信：
扫码领免费游戏皮肤。

正确做法：
不扫码，告诉家长或老师。



02 先交手续费才能领奖



情景：页面提示：
先交手续费才能领奖。

正确做法：
不交钱，退出页面。



03 这是秘密，别告诉爸妈



情景：陌生人说：
这是秘密，别告诉爸妈。

正确做法：

越说保密，越要告诉大人。



04 群里发来陌生链接



情景：群里发来
陌生链接让你点。

正确做法：
不点、不转发、不好奇。



先停一下，再问大人：不扫码，不交钱，不保密，不乱点。。。



第4关：网上也要守规则



网上也要守规则

小小守法公民：线上线下一个样

- 不能冒用别人的账号
- 不能造谣、传谣、恶意辱骂
- 不能随便传播别人照片和视频
- 不能私自充值、打赏、转账
- 遇到危险信息，要截图保存并告诉大人

法律不是离我们很远。
它保护我们，
也提醒我们：
自由上网，要
守规则。



三不三要：今天带走的安全口诀

遇到拿不准的事，不逞强，找大人

三不

× 不泄露隐私

× 不伤害别人

× 不相信骗局

三要

✓ 要文明表达

✓ 要学会求助

✓ 要遵守规则

安全口诀：验证码，不出口；陌生链，不乱走；网上说话要礼貌；遇到危险找大人。



★ 通关承诺卡 ★

1
承诺



我不随便告诉陌生人
自己的个人信息。

2
承诺



我不在网上伤害别人，
也不转发未经确认的消息。

3
承诺



我遇到可疑链接、二维码、
验证码、转账要求，会马上
告诉家长或老师。



Conclusion

AI 是工具，不是大脑
数字世界很精彩，安
全带你玩得更久



THANKS FOR LISTENING!

感谢您的垂听!



07.18 — 07.19

BY

浙江大学
哈尔滨工业大学 (深圳)
中国人民大学



AI EXPLORATION & SECURITY

Zhejiang University. Harbin Institute of Technology, Shenzhen. Renmin University of China