AI 数据革命：没有可信密码，何来真正智能？

2026 年 1 月 19 日

我们正全速驶向一个由 AI 智能体驱动的未来，从日常办公、生活规划、到更复杂的自动驾驶汽车规划路径、医疗 AI 分析影像、金融模型评估风险、智能制造质量管控等等，智能决策的触角正延伸至社会经济的每个关键领域。然而，在这场以 AI 算法复杂度和算力规模为标尺的狂热竞赛中，一个更为根本的命题被严重忽视了：我们倾尽所有资源构建的智能巨塔，其根基—“投喂”给 AI 的数据是否真实可信？如果驱动一切智能的“数据燃料”来源可疑、不可信赖，那么我们最终得到的，究竟是一座通向未来的智慧圣殿，还是一座建立在流沙之上、随时可能倾覆的危楼？

问题的根源在于当前 AI 范式中一个近乎悖论的脆弱性：AI 智能体展现出愈加强大的“思考”能力，但其“认知”的起点，却建立在对输入数据无条件的、盲目的信任之上。AI 缺乏人类与生俱来的质疑与溯源本能，这导致了我们在追求智能高度时，却容忍了数据信度的致命短板。在开放、复杂且存在对抗的真实世界，这种“垃圾进，垃圾出”的逻辑，就等于给一个无知的孩子灌输了一堆错误的观点，这个孩子当然会做出错误的决策，其后果远不止于模型精度下降几个百分点。

一、从智能驾驶到生命健康：系统性信任危机的缩影

仅以智能驾驶为例，便可管中窥豹。一辆自动驾驶汽车若无法验证感知数据的真实来源（是否来自可信传感器？）、时效（高精地图是否已更新？）及传输安全（指令是否在途中被篡改？），它就可能在关键时刻做出灾难性误判。过时或伪造的数据，对 AI 而言就是绝对的“事实”，其输出的“智能”决策，轻则失效，重则致命。

这一逻辑放之四海而皆准：在医疗领域，如果用于辅助诊断的医学影像数据被恶意污染或标注错误，AI 给出的“良性”判断可能延误救治；在金融领域，如果用于风险评估的交易数据身份不明、时间不清，模型可能会纵容欺诈或错杀良企；在工业制造中，如果生产线传感器的读数无法被可信地追溯和验证，所谓的“智能质检”将失去所有质量基础。这揭示了一个残酷的真相：在构建可信 AI 的征途上，任何单一的、孤立的“安全措施”都如同断线的珍珠，无法形成有效防御。 AI 所面临的，是一个贯穿数据身份、数据时效、数据传输乃至未来安全的系统性

信任危机。

二、构建 AI 数据信任基石：四位一体的可信密码应用体系

我们必须发起一场根本性的数据“投喂”革命。这场革命的基石，不再是某一项炫酷的孤立的 AI 模型和算法，而是一套系统性的、贯穿数据从“出生”到“被消费”全生命周期的可信密码应用体系。这套体系如同为数据世界建立了一套不可伪造的“法律、公证、流通与未来安全”，它由四大支柱协同构成，缺一不可：

(1) 第一支柱：HTTPS 加密 — 数据的“防弹运钞车”与“机密通道”。

HTTPS 加密确保数据在漫长的网络旅程中的传输安全。当客户端与服务端建立连接时，通过密钥交换算法协商出仅有双方知晓的会话密钥，随后所有数据都用此密钥加密传输。这实现了：(1) 机密性：即便数据被截获，也无法被解密阅读。(2) 完整性：内置的消息认证机制能检测传输过程中的任何篡改。它完美保障了数据的“在途”安全，是连接可信数据源头与可信 AI 的安全桥梁。

(2) 第二支柱：数字签名 — 数据的“法定身份证”与“责任钢印”。

数字签名的作用远不止于“加密”。基于公钥基础设施（PKI），数据生产者用其私钥对数据生成一段独特的“签名”。任何接收者都可用公开的公钥验证此签名。若验证通过，则百分百证明：(1) 数据来源身份可信：该数据确由该私钥持有者（生产者）创建。(2) 数据完整性：数据自签名后，哪怕一个比特都未被篡改。这从根本上解决了身份假冒和内容篡改问题，并为事后审计追责提供了不可抵赖的电子证据。

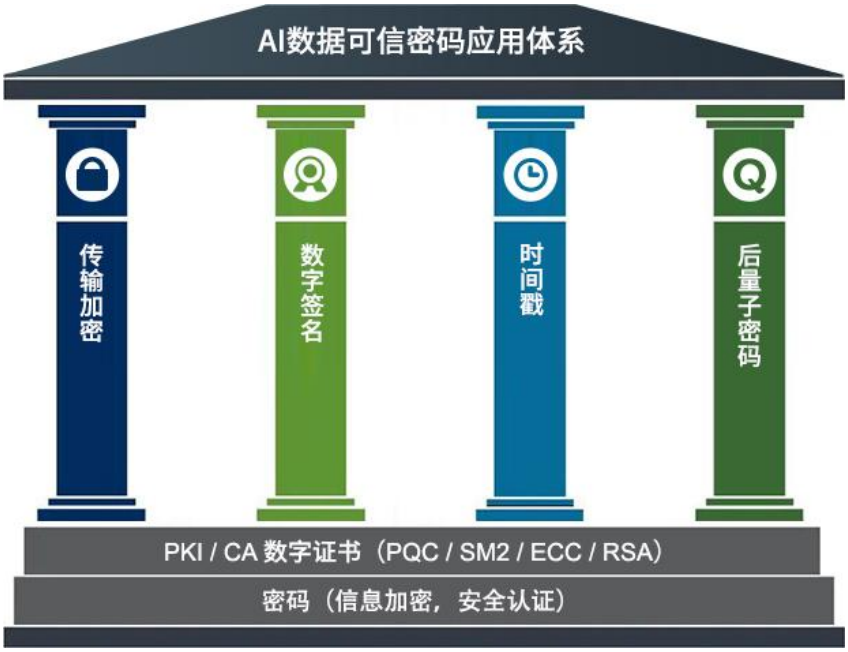
(3) 第三支柱：时间戳 — 数据的“权威出生证明”与“时效公证”。

时间戳由权威可信的时间戳服务（TSA）提供。过程是：将数据的哈希值（数据的数字指纹）发送给 TSA，TSA 将收到该哈希的权威时间（如 UTC 时间）与哈希值本身一并签名，生成时间戳签名，这权威地证明了该数据在“那个”时间点已经存在。AI 系统可据此轻松判断数据是否在有效时间窗内，自动过滤过期信息，杜绝因数据陈旧导致的决策失误。时间戳还可以为数据的使用时间提供可信证明。

(4) 第四支柱：后量子密码算法 — 面向未来的“抗量子安全锁”。

这是应对“Q-Day”（量子计算机破解现有密码算法之日）的前瞻布局。后量子密码（PQC）基于量子计算机难以解决的数学问题（如格问题、多变量方程等）设计的新算法，全球标准机

构（如 NIST）正加速推进 PQC 算法标准化。将其用于数字签名和密钥交换，意味着我们今天为智能汽车、医疗档案、金融合约等生成的数据凭证及流通传输，在未来数十年内依然能抵御最强大的计算攻击，实现信任的长期保值。



以上四大支柱并非简单堆叠，而是有机融合，共同将数据从原始、匿名、易腐、易受攻击的“原料”，转化为身份明确、时间确凿、传输安全(防篡改、防窃取)、未来可信的“标准智能养料”。这是一场 AI 数据“投喂”革命，是 AI 真正成为安全可用的 AI 的关键，是 AI 智能体的制胜法宝。

三、重新定义 AI 友好数据：从格式友好到信任友好

基于以上系统性认知，我们必须对“AI 友好数据”的定义进行一次彻底的范式升维。它绝不能继续停留在“格式规整、标签清晰、便于模型读取”的初级阶段。真正的、面向严峻现实挑战的 AI 友好数据，其核心标准应表述为一个乘数效应模型：

真正的 AI 友好数据 = 结构化机器可读 × 可信密码应用（身份可信 × 时间可信 × 传输可信 × 未来可信）

这里的“乘号”意味着，任何一个可信维度的缺失（值为零），整个数据的可信度总值将归零，无论其他维度有多强。只有所有维度同时得到满足，数据才能释放出其全部价值，AI 智能体才能生成可信的可靠的结果。

当这一模型成为行业共识与实践，将为 AI 生态带来根本性变革：

(1) **安全模式进化**：从“出现漏洞-紧急打补丁”的被动反应式，转变为“系统免疫”。可信密码体系在数据入口就构建了主动验证与过滤屏障。

(2) **责任界定清晰化**：从事故后难以厘清的“模糊地带”，走向全流程“可审计、可追溯”。基于数字签名和时间戳，任何输出都能追溯到其输入数据的源头和状态。

(3) **行业协作成为可能**：从根本上打破“数据孤岛”。当所有参与方都遵循统一的可信密码标准，跨机构、跨行业的数据共享流通与联合建模将在一个预设的信任框架内安全进行，催生更强大的可信生态。

四、可信密码应用是 AI 智能时代的“价值锚点”

综上所述，AI 数据“投喂”急需一场可信密码应用革命：系统性的全面的可信密码应用，必须从 AI 项目的“可选项”变为智能时代发展的“必选项”，是 AI 价值得以实现的“锚点”。

没有可信密码应用作为基石，投喂给 AI 的数据将永远是来源可疑、时效不明、路径存疑的“垃圾数据”。在这样的垃圾数据泛滥基础上，无论 AI 算法如何精妙，其生成的“智能”也必然根基不稳、逻辑扭曲、危机四伏，无法承担关键使命的。这样的 AI，不是伙伴，而是负担；不是进步，而是倒退。

因此，笔者大声疾呼：整个 AI 产业界、密码产业界、网安产业界都必须立即行动，将可信密码应用体系的构建与集成，提升至 AI 基础设施的战略核心地位。这需要算法科学家、密码学家、网安工程师、软硬件工程师、标准制定者和政策监管者的共同协作。

没有可信密码应用，就没有可信数据来源；没有可信数据来源，何来真正可信的人工智能？唯有在密码学为我们共同铸就的这片坚实、透明、面向未来的信任基石之上，AI 智能体才能彻底摆脱“高级盲从者”的困境，真正进化成为与人类文明协同进化、值得完全托付的、可靠的智慧伙伴。

这，已不仅是一条技术路径的选择，更是我们作为 AI 创造者，对这个智能时代所必须履行的、最根本的伦理与安全责任。

王高华

2026 年 1 月 19 日于深圳

欢迎关注零信技术公众号，实时推送每篇精彩 CEO 博客文章。
已累计发表中文 258 篇(共 75 万 5 千多字)和英文 115 篇(15 万 7 千多单词)。