专栏

创新型企业如何通过安全的机器学习在竞争中胜出

在瞬息万变、竞争日益激烈的数字经济时代，新的解决方案可帮助创新型企业取得成功。这些解决方案通过保护客户和员工的隐私，使企业能够激活并挖掘敏感数据的价值，促进相互信任。这样，企业便可以有效地使用私有数据（包括这些数据在高级分析、机器学习 (ML) 和人工智能 (AI) 方面的应用），而无需担心给客户、员工或知识产权带来风险。

企业通过深刻了解以下方面，可获得优势，从而领先于创新能力较弱的竞争对手：如何对受保护数据使用 ML 而获益，量子计算领域最新的进步会如何显著影响新数据和历史数据面临的机会和威胁，当前和未来技术以及涉及未来技术的长期路线图如何优化和保护 ML 代码。上述所有方面都给企业提供了竞争优势，使他们领先于创新能力较弱的竞争对手，从而推动企业向前发展。

安全 AI 从受保护数据中获取价值

安全 AI 解决方案创造了机会，让企业可以利用那些已证明在激活高级分析和 ML 方面最为有效的敏感数据。由于企业对保护敏感数据充满信心，因此可以快速获取价值，实时运用洞察并预测结果，从而加速发展。敏感数据应该得到安全保护，无论它们存储在何处（云或本地），也无论它们处于什么状态（静态或使用中），以便整个企业的一线员工、分析团队以及需要相关信息才能做出业务决策的任何人员都能利用这些数据。数据没有边界，数据保护也不应有边界。无论是加密、令牌化还是应用隐私方法，解决方案都应确保数据安全，数据支撑着推动企业日常运作的许多操作系统以及决策制定、个性化客户体验和 AI 建模背后的分析系统。

案例研究：使用数据保护工具减少金融科技风险
匿名化是一种最大限度地降低身份识别风险的方法。

匿名化是一种不可逆的数据保护方法，通过使用差分隐私或 k-匿名性推动数据密集型业务应用（如分析）向前发展。

在**图 1** 的示例中，相比初始 ML 模型，需要对客户提交的交易进行信用卡审批的银行将隐私风险从 26% 降至 8%，并提供 98% 的准确性。

此方法可用于分析、洞察、制作仪表板、报告、预计、预测、模拟和优化预期的储蓄和收入增加额。

Ulf Mattsson，MSE
担任 Protegrity 的首席安全战略官，为支付卡行业数据安全标准 (PCI DSS)、美国国家标准协会 (ANSI) ANSI X9 和云安全联盟 (CSA) 的发展做出了杰出贡献。在任职于 IBM、Protegrity 及其他科技公司期间，他还开发出了机器人、企业资源规划、数据加密和令牌化、数据发现、云应用安全代理、Web 应用防火墙、托管安全服务以及安全运营中心等领域的产品和服务。Mattsson 曾在多个不同的国家/地区开展数据保护项目，包括为欧盟跨境数据保护法律提供合规性解决方案。他经常在国际安全会议上发表演讲，曾为美国电气和电子工程师协会 (IEEE) Xplore、IBM 期刊、ISACA® 期刊以及信息系统安全协会 (ISSA) 期刊撰写过 100 多篇文章。他还是一位发明家，拥有 70 多个已发布的美国专利。您可通过 ulf@ulfmattsson.com 与他联系。.

在 ML 模型中，另一种数据保护技术是假名化，这是一种基于加密或令牌化技术的可逆方法。加密使用数学算法和加密密钥将数据更改为二进制密文，令牌化使用确定性随机字符串替换明文数据。**图 2** 说明对不同保护方法一些特征的定位。

差分隐私

差分隐私是一种字段级数据掩码形式，以便数据可用于查询汇总的统计数据，同时限制暴露个人的具体信息。[1] 差分隐私是严谨的数学定义，是在将算法思想运用到隐私研究的漫长工作中产生的。在最简单的环境中，该算法分析数据集并计算这些数据的统计信息（如数据集的均值、方差、中值和模式），它是差分私有的 — 通过查看输出无法判断原始数据集中是否包含任何个人的数据。换言之，差分私有算法可保证在数据集中添加或删除个人数据时，行为几乎不会出现任何变化；在包含个人信息的数据库上算法可能输出的任何内容与不含个人信息的数据库输出的内容几乎相同。这种保证适用于任何个人及任何数据集；因此，无论任何个人的详细信息以及数据库中任何其他人的详细信息有多么奇怪，仍可保持差分隐私保证。这就意味着该数据库中参与者的个人信息不会遭到泄露。此方法为数据共享场景提供支持，可用于在不受信任的环境中处理数据。[2]

图 1 — 降低身份识别风险的匿名化流程

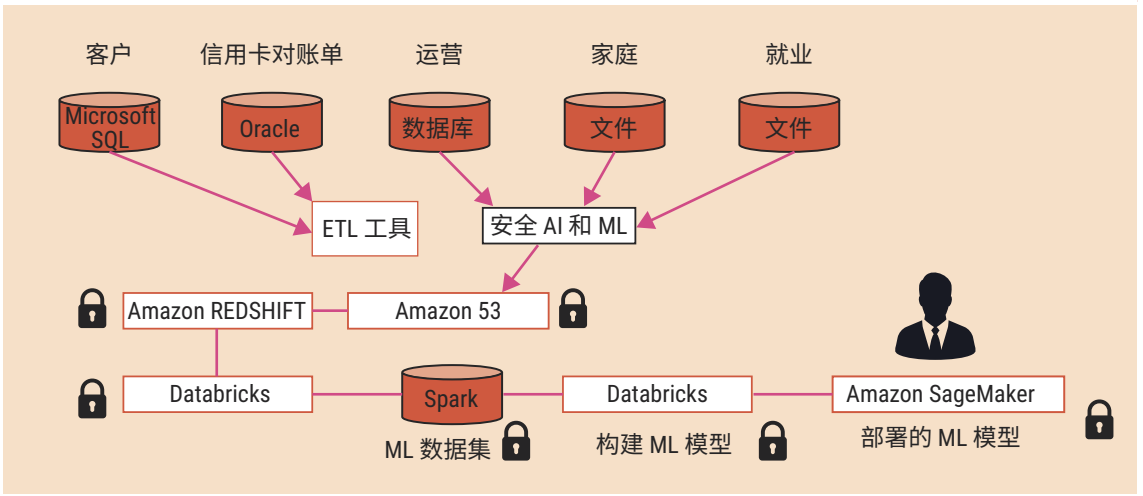
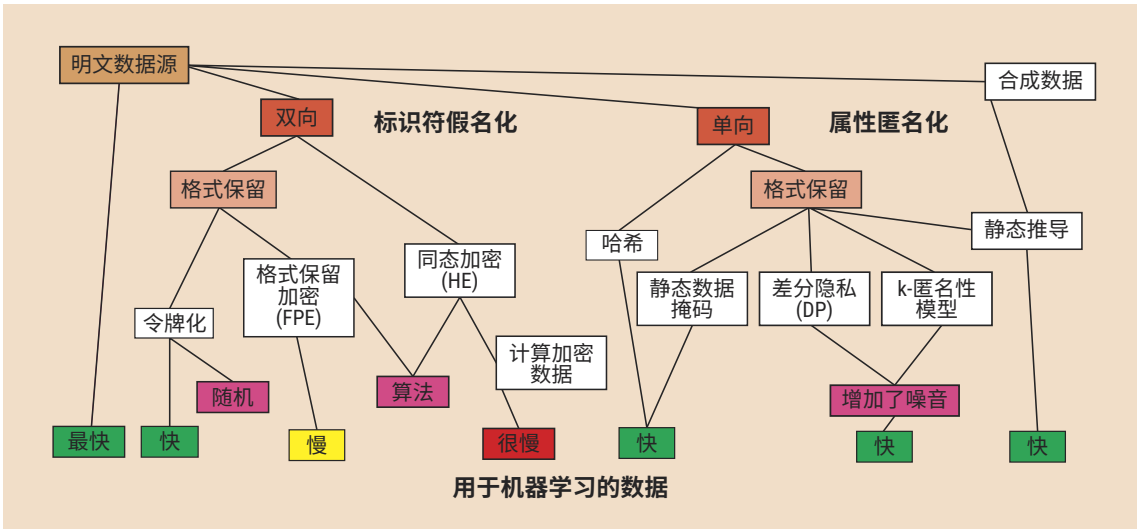


图 2 — 定位不同的数据保护技术的特征



合成数据

合成数据是一种不可逆方法，用于通过人工方式生成微数据以代表预定义的统计数据模型。[3] 根据定义，合成数据集不包含从现有数据主体那里收集的任何数据或关于现有数据主体的任何数据，但对预期目的来说，这些数据看起来是真实的。如果合成数据拟合过于接近原始数据，则会透露有关真实数据主体的信息，如个人数据。合成数据有多种创建方式。从理论上来说，可以根据大量选定的统计属性随机生成数据。此类模型的关键特征包括每个属性的分布（整体和在子总体中的分布情况）以及各属性的内部关系。在实践中，要生成合成数据，需要使用随机化技术和抽样，对真实数据集进行多次或连续转换。通常，合成数据用于测试工具和应用程序，在某些应用中用于开发查询，并且可用于替代真实数据。数据监护者应在真实数据上再现对合成数据执行的查询，以确保从合成数据得出的推论对真实数据而言是正确的。合成数据的隐私保证可以使用差分隐私模型评估。[4]

医疗保健领域的匿名化

k-匿名性可用于对数据进行泛化处理。k-匿名性模型可确保无法识别小于“k”个个体的群体。查询将至少返回“k”个记录。k-匿名性是一种正式的隐私衡量模型，可确保对于每个标识符，存在包含至少“k”个记录的相应等价类。要实现 k-匿名性，数据集需要包含至少“k”个个体，这些个体共享可用于识别每个个体的属性集。[5] **图 3** 显示了 k-匿名性示例。

k-匿名性可描述为“隐藏于人群中”保证：如果每个人都是大群体的一部分，那么这个群体中的任何记录都可能对应一个人。[6] **图 4** 显示经过匿名化处理的数据。通过泛化一些准标识符属性和编辑其他属性可以实现匿名化处理。

金融科技领域的合成数据

当历史数据不可用或由于缺乏质量或多样性而导致可用数据不足时，组织会依靠合成数据构建模型。组织可以生成任意分布的随机样本。合成数据的效用取决于分析师对特定数据环境的了解程度。通过生成合成数据将真实数据拟合到已知分布，从而生成合成数据。此外，还有各种工具可用于生成数据，例如 CA Technologies Datamaker 和 Informatica 测试数据管理工具。真实数据到合成数据的静态推导可提供不受监管但与第三方共享时非常有用的数据（**图 5**）。[7]

量子计算：利与弊

使用量子计算机有利有弊。量子计算机可以提高计算性能，部分量子 ML 算法可以针对量子计算机进行优化，并且量子计算机可以打破加密数据中的算法和模式，特别是打破公钥加密。**图 6** 展示了这些技术之间的关系。当组织在 ML 模型中使用分析时，组织可能希望保护在云端运行的一些敏感数据 ML 模型。这可以通过可信执行环境 (TEE) 实现。

> “合成数据集不包含从现有数据主体那里收集的任何数据或关于现有数据主体的任何数据，但对预期目的来说，这些数据看起来是真实的。”

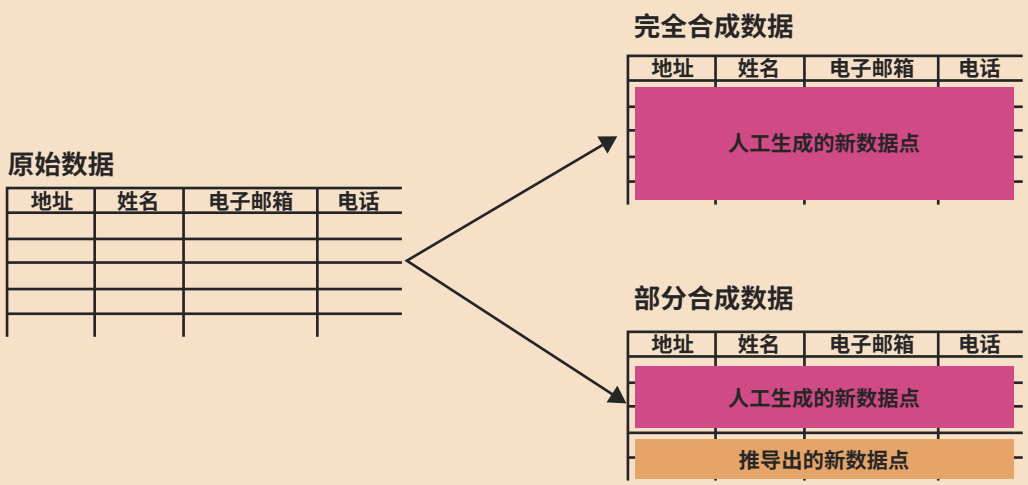
图 3 — 示例数据集

标识符	准标识符			机密属性	
门牌号	性别	年龄	邮政编码	工资	派别
123-55-1321	男	22	94123	22	社会主义者
321-33-4321	女	26	94321	33	保守主义者
876-89-6543	男	24	94654	44	保守主义者
345-56-6789	男	40	90222	55	社会主义者
876-34-4322	女	38	90654	43	保守主义者
837-45-1256	女	42	90876	32	社会主义者

图 4 — 应用于数据集的 k-匿名性

标识符	准标识符			机密属性	
门牌号	性别	年龄	邮政编码	工资	派别
*	男	40	94***	22	社会主义者
*	男	38	94***	33	保守主义者
*	男	42	94***	44	保守主义者
*	女	22	90***	55	社会主义者
*	女	26	90***	43	保守主义者
*	女	24	90***	32	社会主义者

图 5 — 真实数据到合成数据的静态推导



Enjoying this article?

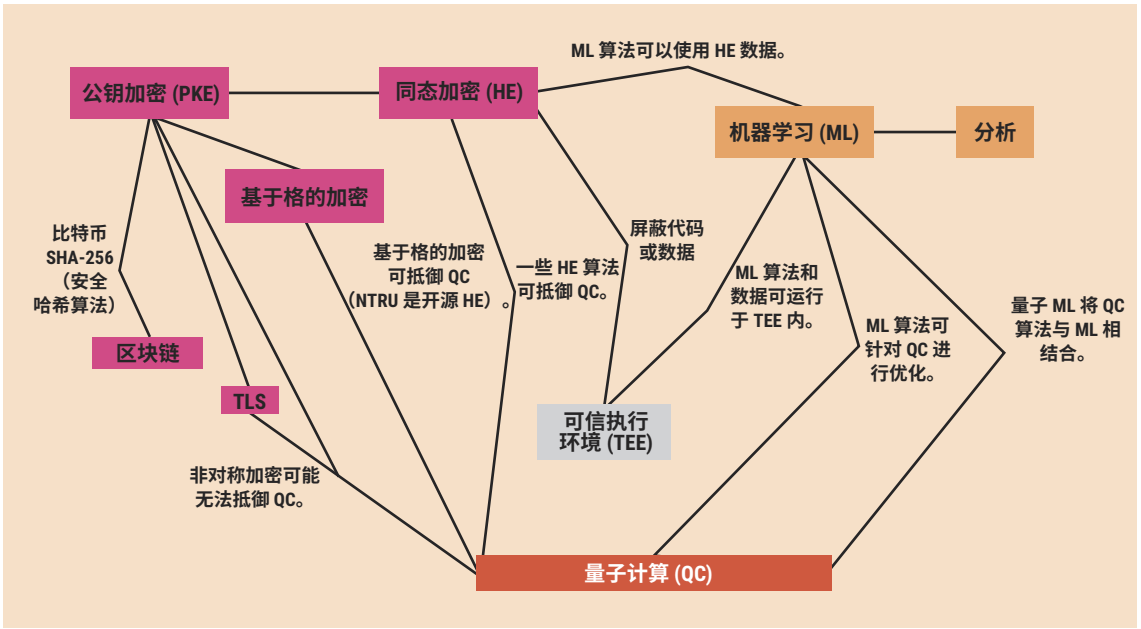
- Read *Privacy by Design and Default. www.isaca.org/Privacy-by-Design*
- Learn more about, discuss and collaborate on privacy in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

> “云可以与 AI 结合重塑组织制定决策的方式。”

同态加密和量子计算

新的同态加密 (HE) 算法可以抵御量子计算机的攻击，并且 ML 算法可以针对量子计算机进行优化。[8] HE 允许对加密数据进行计算，并且 ML 的普及程度越来越高。HE 和量子计算都可以应用于提供隐私性和安全性，以便在易受攻击的环境（如不同的云模型）中保护敏感数据和机密 ML 模型。欧盟《通用数据保护条例 (GDPR)》、美国《加州消费者隐私法案 (CCPA)》以及实行的其他法规（日后肯定还会制定更多相关法规）只强调了企业保护其数据的需求。数据必须通过企业的很多混合云数据库和应用程序以受保护的形式移动。云可以与 AI 结合重塑组织制定决策的方式。对于通过高级分析、ML 和 AI 推动创新至关重要的数据类型，会被视为最敏感的数据，因此必须保障其安全。其中的 ML 模型和数据可以在 TEE 中予以屏蔽。TEE 类似于硬件安全模块 (HSM)，但速度更快，并且通常不会根据美国国家标准与技术研究院 (NIST) 联邦信息处理标准 (FIPS) 140 要求进行评估。这是通过加密非线性 ML 模型和用于不同的云模型和 IoT 设备等外包环境的数据提供的补充保护。HE 可通过合理的性能降级保护线性 ML 模型。非线性 ML 模型受到同态加密的保护时，速度会变得非常慢。

图 6 – 数据保护分析场景



量子计算带来的机会

HE 和 ML 允许企业使用敏感数据助力高级分析、ML 和 AI，即使这些计划迁移到云环境也不例外。[9]这给当前和未来的计算机带来机会的同时也造成了威胁。

量子计算机可以破坏区块链和公钥加密

数字科技面临的最严峻的挑战之一就是保障系统和数据的安全。几十年来，计算机科学家们努力开发出越来越复杂的算法，旨在加密数据并通过公钥加密 (PKE)（也被称为“非对称加密”）等框架保护数据。[10]这些框架的运行情况相对良好，每天有数十亿的事务和交互使用这些算法。

随着量子计算机不断发展并逐渐成为主流，它们将计算能力提高到新的水平的同时也带来了风险。[11] 虽然量子计算机具有许多潜在的好处，但它的一个重大缺点是能够破解如今的 PKE，包括广泛使用的 Rivest-Shamir-Adleman (RSA) 和 Diffie-Hellman 框架。从路由器和虚拟私有网络 (VPN) 到验证数字签名的能力，量子计算机的影响无处不在。

2016 年，美国国家安全局 (NSA) 发布警报，建议组织想办法转换为更先进的加密技术。一年后，为对抗量子计算机破解密码的威胁，NIST 开始征求更先进的新算法，并将该算法设置为标准。[12]

量子计算机不具备对古典加密算法成功发起暴力攻击的处理能力。但短短几年后，一旦这些计算机达到约 1000 万物理量子比特的阈值，它们将具备这样的处理能力。对企业、大学和政府而言，风险尤为明显。如果量子计算机破解了 PKE 算法，不止设备会受到影响，企业的历史数据也有可能泄露。因此，数学家和计算机科学家正在开发更先进的新加密算法，这些算法使用古典框架和基于格的框架。[13]前者依赖于非兼容代码；后者使用数学公式或证明确保算法的完整性。实际上，向正式（已验证）软件进行更广泛的迁移时，需要使用基于格的算法。

> “量子霸权，描述了量子计算机的性能远远超出经典计算机的时代即将来临。”

当前计算机造成的威胁

除了量子计算机之外，当前的英特尔至强计算机也会对 RSA 加密造成威胁。RSA 的安全性依赖于对两个大素数的乘积进行分解的实际难度（分解问题）。破解 RSA 加密被称为 RSA 问题。分解可通过一个含 240 个十进制位且大小为 795 位的 RSA 密钥展示。[14]

从短期看，企业可以改为使用最少 2048 位 RSA、Diffie-Hellman 或 DSA 密钥，通过英特尔处理器和类似处理器的改进保持安全。尽管传输层安全协议 (TLS) 因采用较大的密钥而导致协商时间较慢，但只对繁忙的站点有明显影响。对因速度变慢而受影响的大多数繁忙站点来说，它们可能买得起或租得起所需的硬件来帮助提供支持。从短期使用情况来看，可以使用 Curve25519；它的速度很快，并且与 NIST 毫无关联。这种加密算法约等同于 128 位高级加密标准 (AES) 加密。

> “在许多情况下，企业需要更新证书管理框架、设备和软件以支持新的算法。”

区块链安全性

尽管韧性不像有些人认为的那样与生俱来，但该能力是促使企业使用区块链技术的主要动机之一。[15] 区块链依赖于互联网连接性和基于 RSA 算法等对称加密的公钥基础设施 (PKI)。区块链框架依赖于基础加密流程的安全性。没有受信任的哈希函数和公钥签名就没有区块链。量子计算机会威胁到区块链中使用的几个加密基元。攻击加密基元背后的数学问题必须使用可扩展的量子计算机，虽然目前还没有，但一些企业和政府已经制造出小型量子计算机。有些量子计算机甚至可通过互联网访问，可用于测试量子算法。量子霸权，描述了尽管目前尚未实现，但量子计算机的性能远远超出经典计算机的时代即将来临。因此，必须了解对区块链构成的威胁并概括介绍可能的解决方案。

量子韧性算法

在接下来的几年内，NIST 预计将最终敲定量子韧性算法的新标准。

目前，企业可以通过随时了解 NIST 举措的最新动态和留意该领域的突破性新闻，为加密技术下一阶段的发展做好充分准备。现在开始评估系统和设备并思考量子弹性算法何时何地发挥作用不算过早。在许多情况下，企业需要更新证书管理框架、设备和软件以支持新的算法。此外，将旧系统升级为 256 位密钥以最大限度地提高数据保护水平，也是个好主意。

幸运的是，对称式密钥加密法（依赖于私钥）并不容易被量子计算破解，因此暂时不会被视为风险。不过，要依赖对称式密钥加密法处理当今计算环境中发生的许多交互和事务并不可行。一旦出现量子安全算法，尽快迁移才是明智之举。

许多 PKE 算法依赖于极大的数字，即两个素数的乘积。其他加密算法根据解决特定离散对数问题的困难程度提供安全性。密钥足够大时，没有已知的方法破解它们提供的加密。大数的分解和离散对数的计算会破坏给定密钥大小的加密保证，并迫使用户逐渐增加使用的熵位数。

后量子加密研究侧重于六种不同的方法：[16]

1. **基于格的加密** — 这种方法包括以下加密系统：容错学习 (LWE)、环上容错学习、环上容错学习密钥交换、环上容错学习签名、旧的 NTRU 或 Goldreich-Goldwasser-Halevi (GGH) 加密方案，以及较新的 NTRU 签名和双峰格签名方案 (BLISS) 签名。
2. **多变量加密** — 包括 彩虹不平衡油醋 (UOV) 方案等加密系统，该方案基于解决多变量方程系统的困难程度。构建安全的多变量方程加密方案的各种尝试均以失败告终。
3. **基于哈希函数的加密** — 包括以下加密系统：Lamport 签名和 Merkle 签名方案以及较新的扩展 Merkle 签名方案 (XMSS) 和 SPHINCS 方案。20 世纪 70 年代晚期，发明了基于哈希函数的数字签名，并且自那以后，开始研究 RSA 和数字签名算法 (DSA) 等基于数字理论的数字签名的有趣替代方案。
4. **基于代码的加密** — 包括依赖于纠错代码的加密系统，如 McEliece 和 Niederreiter 加密算法以及相关的 Courtois、Finiasz 和 Sendrier 签名方案。使用 Goppa 随机码的原始 McEliece 签名经受了 30 多年的审查。
5. **超奇异椭圆曲线同源加密** — 此加密系统依赖于超奇异椭圆曲线和超奇异同源图形的属性，创建使用前向保密的 Diffie-Hellman 替代品。
6. **抗量子对称密钥** — 如果使用的密钥足够大，则高级加密标准 (AES) 和 SNOW 3G 等对称密钥加密系统可抵御量子计算机的攻击。

超越可破解的加密

美国国务院及其他一些美国政府机构要求从 128 位 AES 迁移至 256 位 AES，并停止使用与 256 位 AES 关联的特定安全哈希函数。[17] **图 7** 展示了为量子计算做准备的加密路线图示例。

实现随机化的道路

量子计算机及其他功能强大的计算机可以破解加密数据的算法和模式。或者，可以使用随机数保护敏感数据的安全，因为它们不基于算法或模式。

随机数应通过适用于随机数的 NIST 统计测试套件验证。NIST 特别出版物 (SP) 800-22 提供 15 个统计测试，评估是否存在某种模式，如果检测到，则表示序列是非随机的。18 测试的重点是整个序列中 0 和 1 的比例。测试的目的是确定序列中 0 和 1 的数量是否和真正随机序列的预期大致相同。测试套件包括对频率和近似熵的测试。

> “蓝色令牌代表临时结果，最终令牌值显示为绿色。”

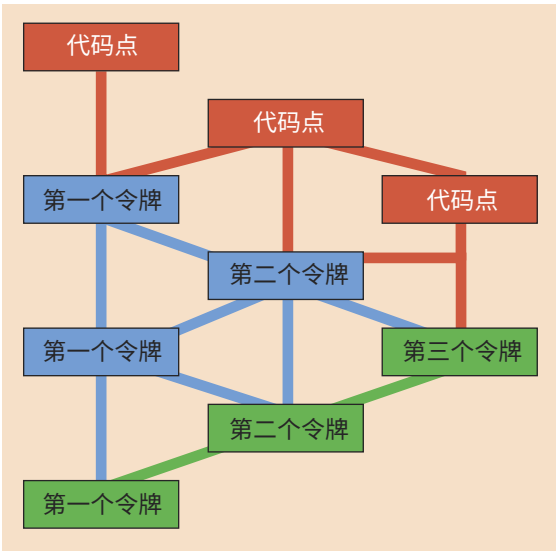
构建受保护数据元素的令牌结构

保护短数据总是充满挑战性，这是因为可能值的熵或变化很小。结构可用于在保护短数据的同时增加熵。因此可以创建用于替换明文数据的中间数据令牌的结构。这些是随机生成的值，其中每一层逐渐增加每个最终令牌的熵，这些值将取代原始输入数据。**图 8** 展示了中间令牌的结构示例。蓝色令牌代表临时结果，最终令牌值显示为绿色。

图 7 — 加密路线图示例

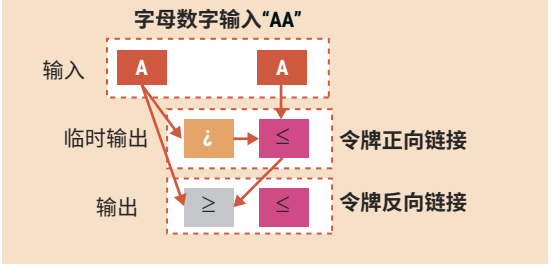
时间范围	领域	备注
短	升级为 AES，最好是具有强大随机种子的 AES-256	立即-中期采取的中间步骤
短	使用 SHA-512 作为哈希算法	立即采取的步骤
短	短期使用基于有状态哈希的签名进行签名	立即审查
短	使用混合加密以避免 RSA/ECC 中的弱点以及后量子算法中的潜在弱点	立即采取的步骤
中	基于格的算法	工具研究和整合计划
中	HE	工具及合作伙伴整合
中	在加密数据上运行	协议的整合
中	安全多方计算 (SMPC)	协议的整合
中	2022 年 NIST 要完成安全算法的审查	工具整合
中	待发布的 2022 年 NIST 标准	工具整合
长	基于 NIST 标准中的 NIST 算法的 2024 年行业标准	工具整合
长	分析和 ML	针对量子处理器进行了优化的 ML 算法
长	2019 年以后全行业采用	工具整合

图 8 – 中间令牌的结构示例



我们可以使用基于随机查找表的令牌化功能。令牌的链接可以通过额外的输入数据将熵添加到每一步的令牌化流程。**图 9** 展示了包含双字符输入字符串（“AA”）的短数据示例，这些数据将生成表示临时结果的中间层令牌以及底层的最终令牌。每个令牌都基于唯一的初始化值，并与其他令牌呈正向链接和反向链接关系，以增加高熵和随机性。特定设计和实施的安全性必须由领先的专家和大学验证。

图 9 – 将熵添加到令牌化流程的链接示例



结论

创新型企业可以通过实施有助于从敏感数据获取价值的解决方案保持竞争力。借助 TEE 和令牌化结构等新技术，企业能够安全地使用私有信息，包括这些信息在高级分析、ML 和 AI 方面的应用，而无需担心给客户、员工或知识产权带来风险。

常用的解决方案无法像量子计算机一样提供强有力的保护。适当规划并了解可用的技术，例如通过不断演变的量子计算机技术提供的令牌化结构和增强选项，可以提供实际的数据保护方法，使企业能够获得竞争优势，从而领先于创新能力较弱的竞争对手。

> “常用的解决方案无法像量子计算机一样提供强有力的保护。”

尾注

1 Zhao, J.; T. Jung; Y. Wang; X. Li; “Achieving Differential Privacy of Data Disclosure in the Smart Grid,” IEEE Conference on Computer Communications，加拿大多伦多，2014 年 4 月

2 Nayak, C.; “New Privacy-Protected Facebook Data for Independent Research on Social Media’s Impact on Democracy,” Facebook Research，2020 年 2 月 13 日，*https://research.fb.com/blog/2020/02/new-privacy-protected-facebook-data-for-independent-research-on-social-medias-impact-on-democracy/*

3 Reiter, J. P.; “Using CART to Generate Partially Synthetic, Public Use Microdata,” *Journal of Official Statistics*，第 21 卷，第3 期，2005 年 1 月

4 Watson, A.; "Using Generative, Differentially-Private Models to Build Privacy-Enhancing, Synthetic Datasets From Real Data," *Medium*，2020 年 3 月 2 日，*https://medium.com/gretel-ai/using-generative-differentially-private-models-to-build-privacy-enhancing-synthetic-datasets-c0633856184*

5 Privitar, "K – Anonymity: An Introduction,"2017 年 4 月 7 日，*https://www.privitar.com/blog/k-anonymity-an-introduction/*

6 *同上*

7 Sarkar, T.; "Synthetic Data Generation—A Must-Have Skill for New Data Scientists," *Towards Data Science*，2018 年 12 月 19 日，*https://towardsdatascience.com/synthetic-data-generation-a-must-have-skill-for-new-data-scientists-915896c0c1ae*

8 Mattsson, U.; "New Technologies for Data Protection That Arm Innovative Businesses to Win," ISACA® San Francisco Chapter (California USA)，美国，2021 年 4 月 21 日，*https://engage.isaca.org/sanfranciscochapter/events/eventdescription?CalendarEventKey=7fc789f0-0538-4887-a6e0-8668bcdc68c1&CommunityKey=f510bd50-4fdc-46b1-a329-d6ce8a64bae7&Home=%2Fcommunities%2Fcommunity-home%2Frecent-community-events*

9 Mattsson, U.; "Homomorphic Encryption Will Take on the Challenge of AI," RSA Conference，2021 年 2 月 25 日，*https://www.rsaconference.com/Library/blog/Homomorphic%20Encryption%20Will%20Take%20on%20the%20Challenge%20of%20AI*

10 The National Academies Press, *Decrypting the Encryption Debate: A Framework for Decision Makers*，美国，2018 年

11 IBM, "Quantum Computing: Tomorrow's Computing Today," *https://www.ibm.com/quantum-computing/?p1=Search&p4=43700050386405608&p5=b&gclsrc=aw.ds&gclid=EAIaIQobChMIuLe0jcOR8AIVhrLICh1ICQZ0EAAYASAAEgI2avD_BwE*

12 National Institute of Standards and Technology (NIST), "NIST Kicks Off Effort to Defend Encrypted Data From Quantum Computer Threat,"美国，2016 年 4 月 28 日，*https://www.nist.gov/news-events/news/2016/04/nist-kicks-effort-defend-encrypted-data-quantum-computer-threat*

13 The National Academies Press, *Quantum Computing: Progress and Prospects*，美国，2019 年

14 Goodin, D.; "New Crypto-Cracking Record Reached, With Less Help Than Usual From Moore's Law," *Ars Technica*，2019 年 3 月 12 日，*https://arstechnica.com/information-technology/2019/12/new-crypto-cracking-record-reached-with-less-help-than-usual-from-moores-law/*

15 Deloitte, "Security Controls for Blockchain Applications," *https://www2.deloitte.com/ch/en/pages/risk/articles/security-controls-for-blockchain-applications.html*

16 Raffaelli, F.; R. Denman; R. Collins; J. C. Faugere; G. De Martino; C. Shaw; J. Kennard; R. Sibson; L. Perret; C. Erven; "Combining a Quantum Random Number Generator and Quantum-Resistant Algorithms Into the GnuGPG Open-Source Software," *Advanced Optical Technologies*，第 9 卷，第5 期，2020 年

17 *Op cit Goodin*

18 Rukhin, A.; J. Soto; J. Nechvatal; M. Smid; E. Barker; S. Leigh; M. Levenson; M. Vangel; D. Banks; *A. Heckert; J. Dray; S. Vo; A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*, National Institute of Standards and Technology (NIST) Special Publication (SP) 800-22，美国，2010 年，*https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-22r1a.pdff*