腾讯云数盾

量子时代的隐私保护利器

演讲者 彭思翔博士

目录

新时代的数据安全挑战

隐私保护法规趋严

中国：等级保护 2.0时代

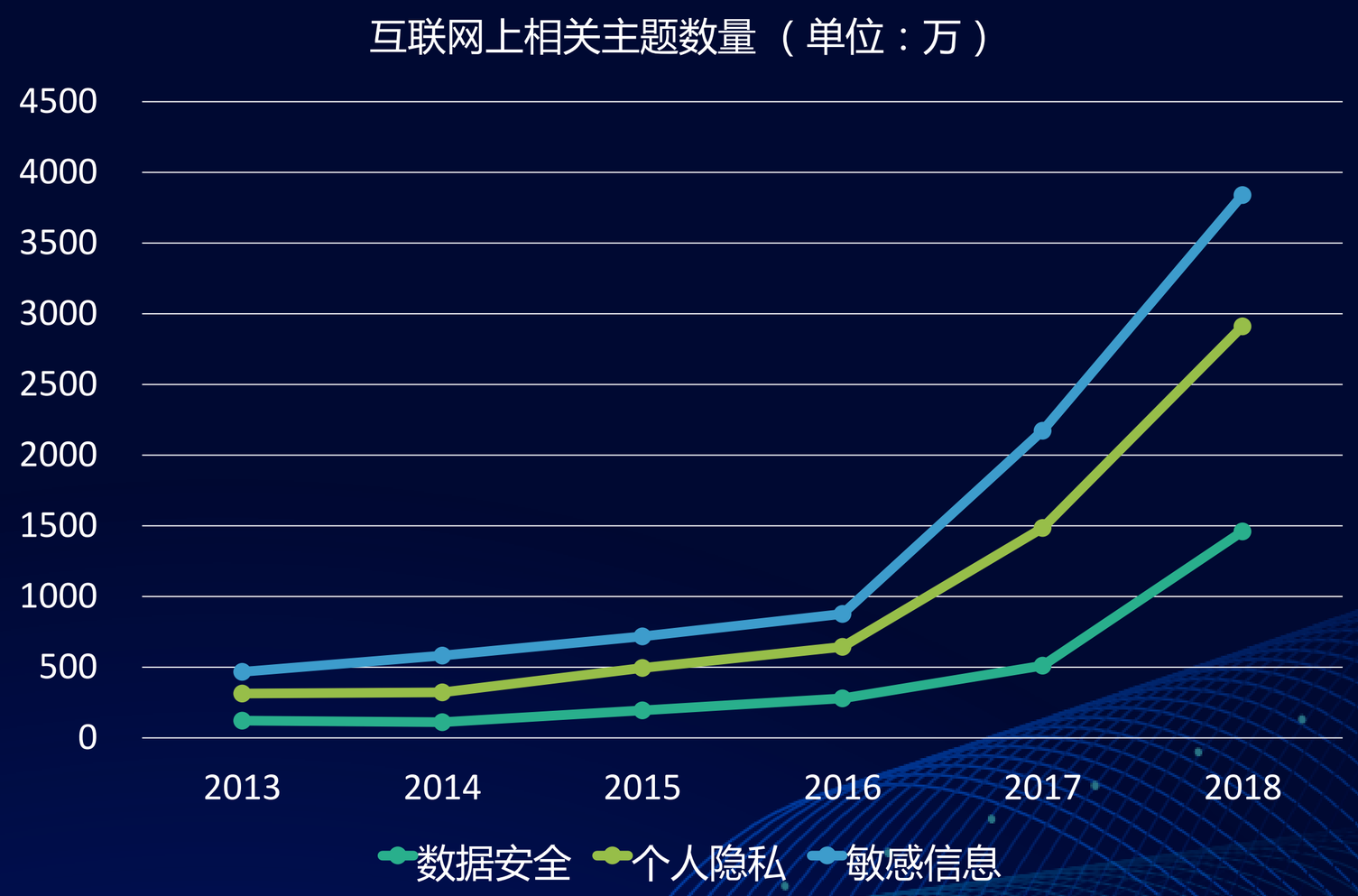
欧盟：GDPR 5月25日

美国：TrustArc 20+年

个人隐私保护意识觉醒

近两年半隐私保护受关注度

增长 **80%**



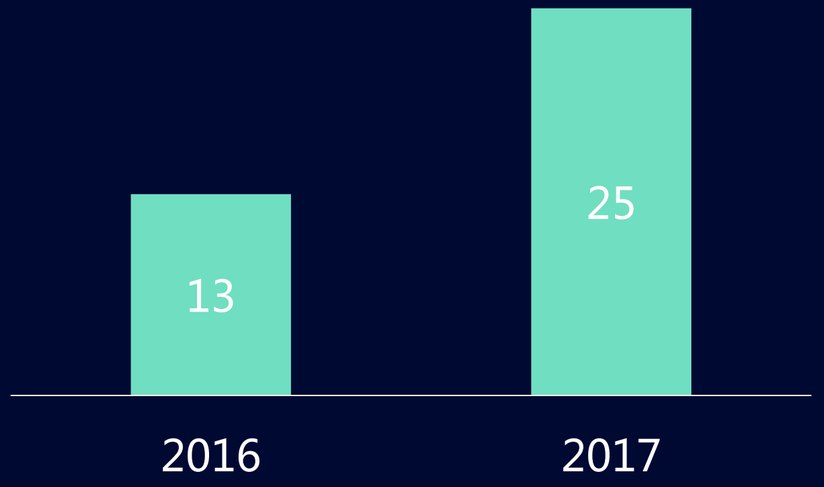
数据来源：Google Trend

数据安全态势越发严峻

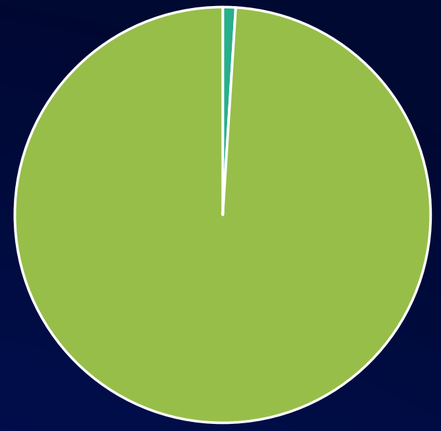
发生过数据泄漏的企业

占比 **80%**

泄漏数据增长88%（单位：亿）



泄漏的数据中仅1%经过加密



已加密 未加密

数据来源：Gemalto / Gatner

量子技术破解数据加密

量子计算机破解Https“安全”信道将仅用

4.8小时

RSA密码长度		1024bits	2048bits	4096bits
传统计算机	2006年水平	10^5 年	$5*10^{15}$年	$3*10^{29}$年
	2042年水平	3 天	$3*10^8$年	$2*10^{22}$年
量子计算机	5124 qubit	5124 分	10^{244}分	20484 小时
	20484 qubit	4.5 分	36分	4.8小时

传统计算机与量子计算机破解RSA所需时间对比

数据来源：R.J. Hughes, LA-UR-97-4986

腾讯云数盾：新时代的数据全流程保护方案（DCAP）

操作审计

亿级样本训练AI风险识别引擎
十亿数据操作记录秒级检索
完全符合等保数据安全要求

隐私保护

多达29类隐私数据智能发现能力
数据分析/共享安全的高级脱敏/水印
满足中美欧多国隐私保护法规要求

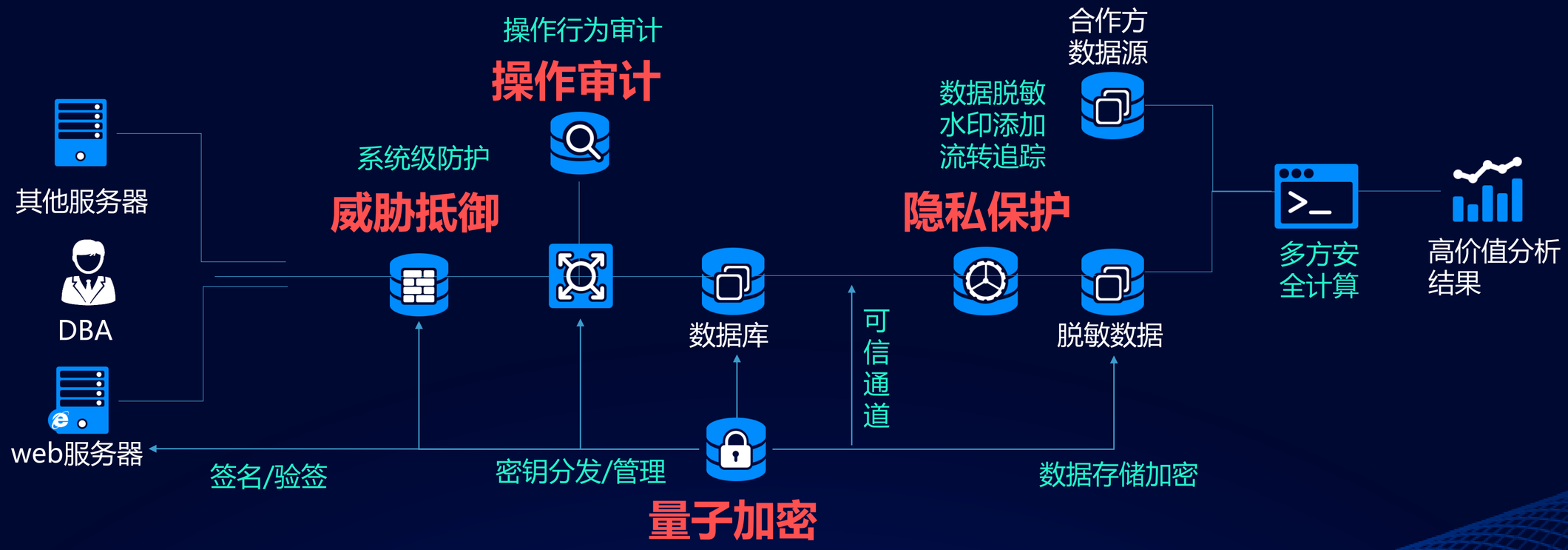
量子加密

量子随机密钥，无法窃听/预测
可抵御量子计算攻击的加密算法
集成国产密码技术

威胁抵御

SQL注入风险检出率高达97%
数据访问多因子控制
数据加密+漂白多重防护

腾讯云数盾：全景


操作行为审计
操作审计
合作方
数据源
数据脱敏
水印添加
流转追踪
系统级防护
威胁抵御
隐私保护
其他服务器
DBA
web服务器
数据库
可信通道
脱敏数据
多方安全计算
高价值分析结果
签名/验签
密钥分发/管理
数据存储加密
量子加密

操作审计：基于AI的数据库审计

操作审计：合规的基石

腾讯云 | 连接智能未来

安全合规

- 定期报表展示
- 实时视图展示
- 留存期限合规
- 审计内容合规

事件追溯

- 问题事故追责
- 内部泄密取证
- 恶意操作溯源
- 安全事件还原

风险监测

- SQL注入识别
- 非法语句告警
- 语句压力监控
- 风险AI识别
- 异常操作告警
- 高危语句监控

等保合规

事故定责

防统方

泄密取证

操作审计：全景视图，态势感知

腾讯云 | 连 接 智 能 未 来

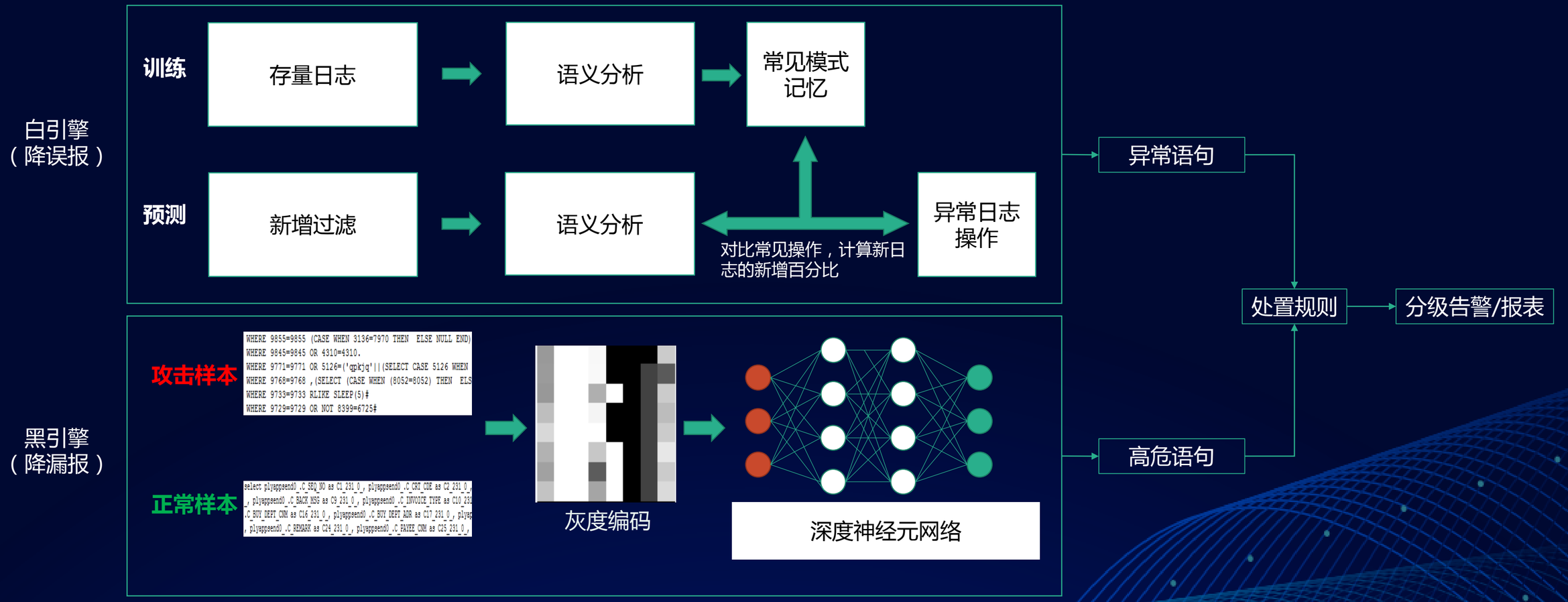
智能审计，掌控全局

- 语句压力预警：数据库性能问题预测
- 业务审计：全量会话审计，快速追溯
- AI审计：AI双引擎，未知操作风险识别
- 风险报表：自定义操作风险报表，等保报表
- 威胁告警：多途径分级实时告警

操作审计：AI赋能，精准发现

腾讯云 | 连接智能未来

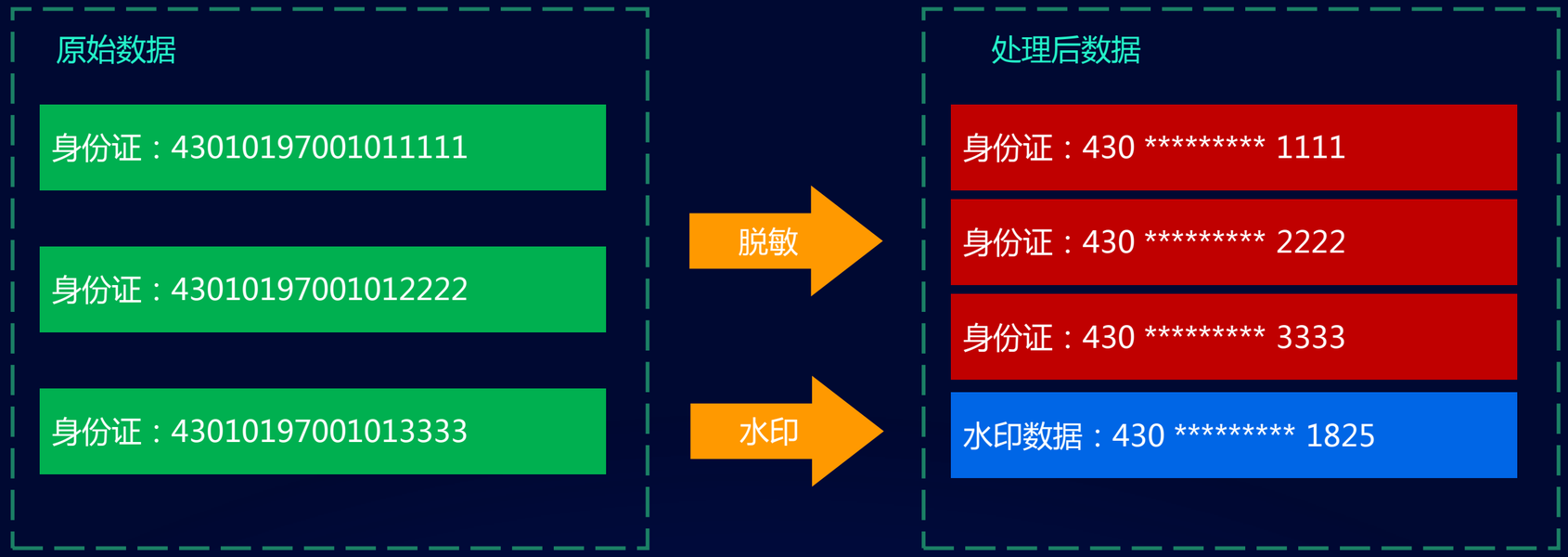
独创AI双引擎综合判断，自动适配用户操作特征，误报率/漏报率双低



隐私保护：数据分析/共享中的敏感信息特殊处理

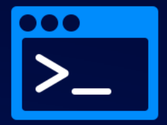
隐私保护：数据脱敏、水印

对敏感数据进行脱敏和水印处理，同时保持数据统计学价值
满足数据分析/共享环境中的隐私保护需求



系统测试

数据分析

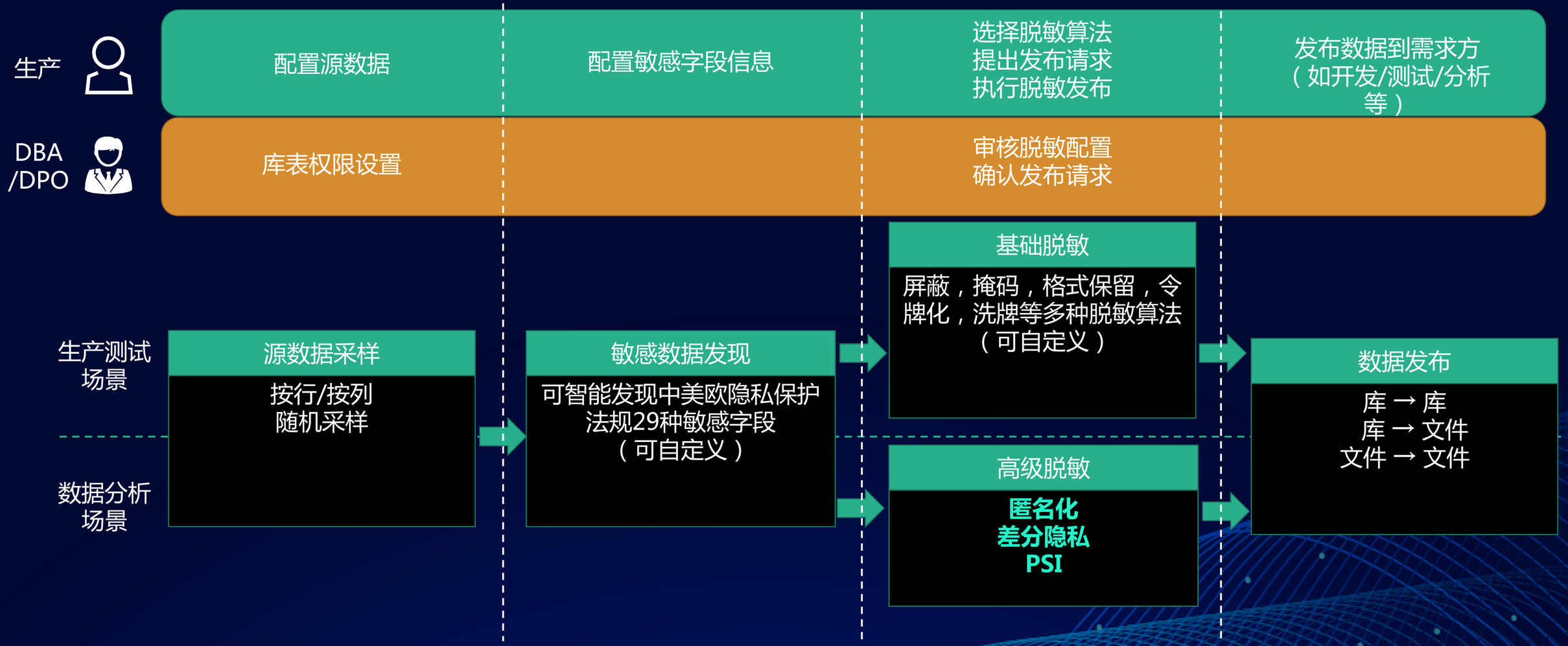


应用开发

业务培训

隐私保护：智能高效

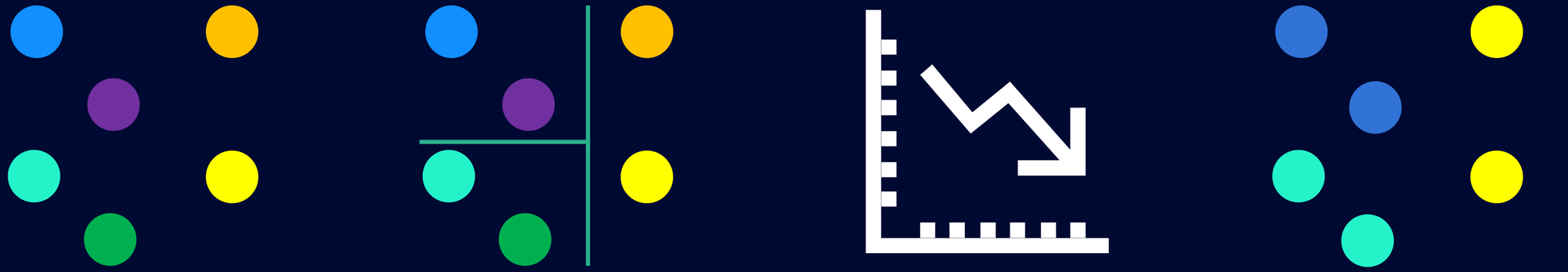
一键智能脱敏，满足生产数据用于测试、开发、培训和大数据分析场景中的数据脱敏需求



隐私保护：平衡隐私保护与数据挖掘价值

匿名化：通过聚合与泛化使得脱敏后数据无法被唯一对应，同时保证统计分析可用性

适合离线数据批量脱敏，支持多种数据类型，各种业务通用



拓扑关系分析

(拓扑树构造，语义分析)

聚类

（K-means, DBSCAN,Birch等多种聚类方式 ）

误差分析

（欧式距离收敛）

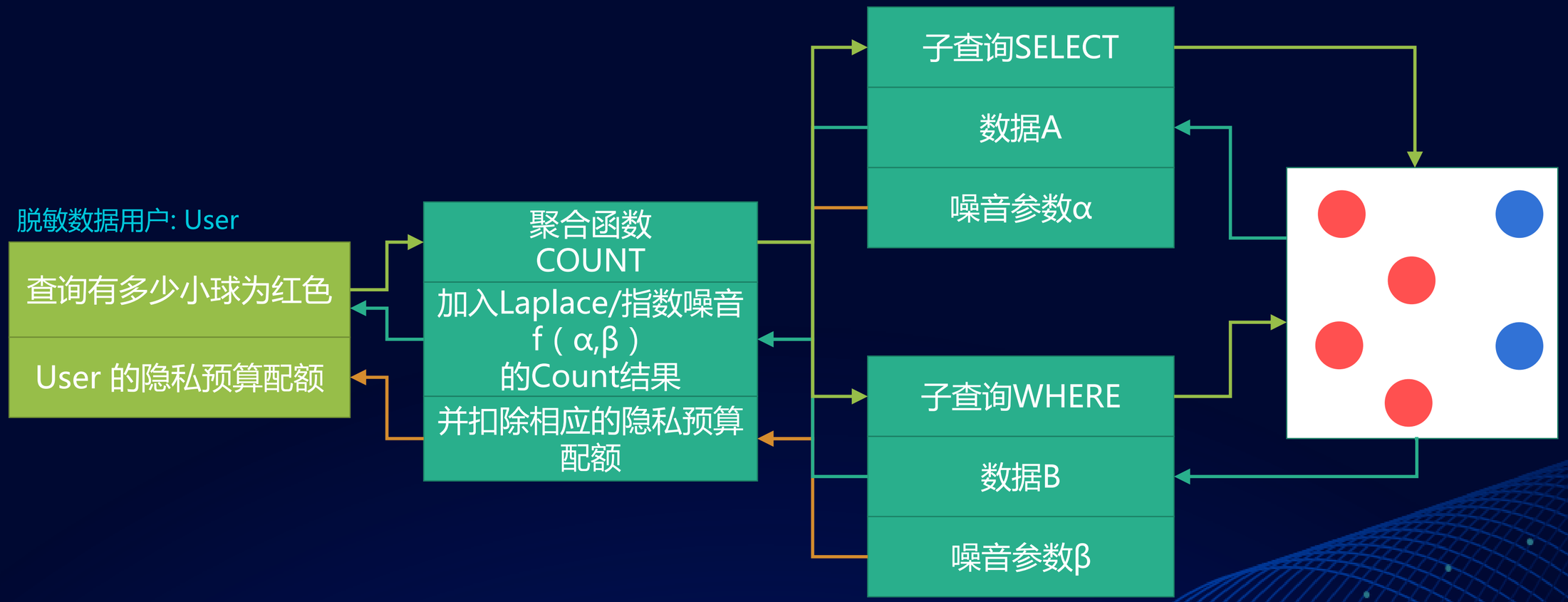
泛化结果

（保留格式，泛化数值）

隐私保护：平衡隐私保护与数据挖掘价值

差分隐私：通过语义分析，对结果加入噪声，平衡隐私安全与数据可用性

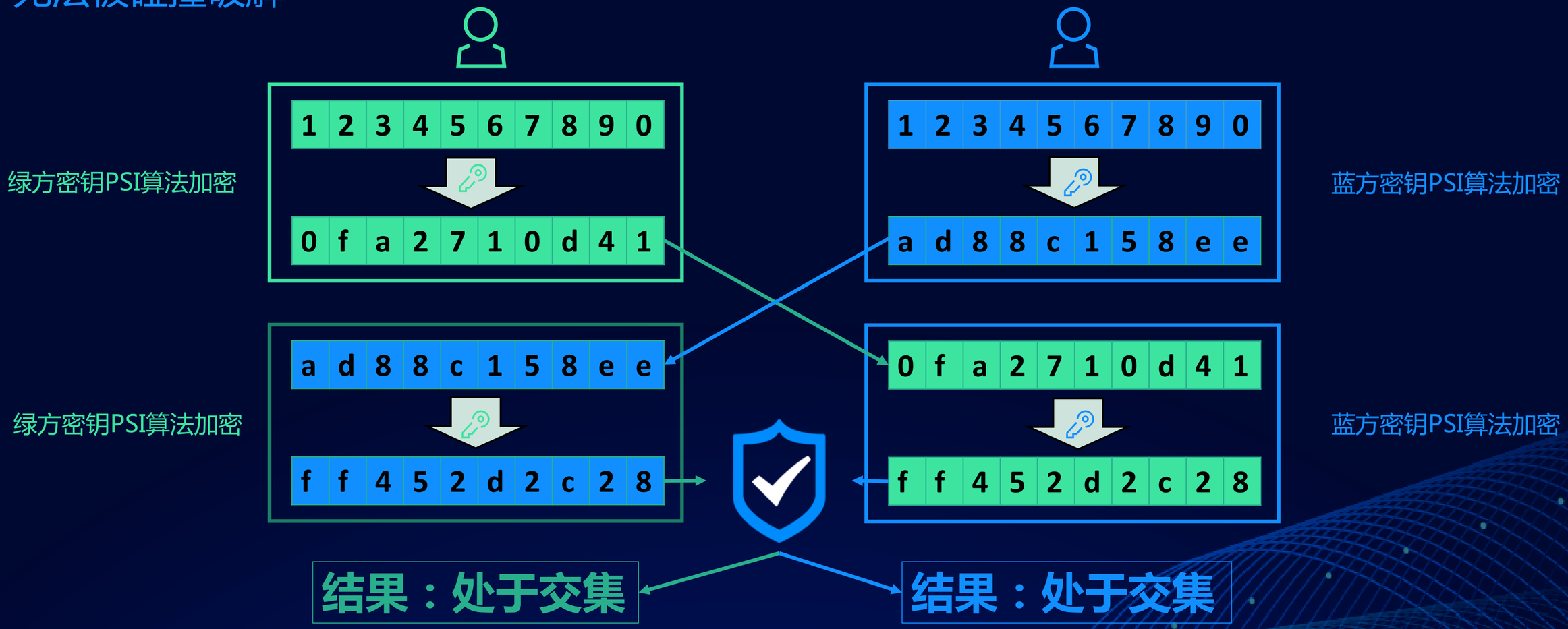
适合实时数据查询结果脱敏，具备高保护等级，低数据分析误差



隐私保护：平衡隐私保护与数据挖掘价值

安全多方计算框架：针对多方互不信任但需要共享数据的场景，解决安全分析问题

数隐采用Private Set Intersection(PSI) 共享安全算法，各方地位平等，线性计算复杂度，无法被碰撞破解



量子加密：量子时代的数据加密方案

量子加密：量子时代的数据加密方案

腾讯云 | 连接智能未来

量子技术对现有密码安全影响巨大

算法类型	受到的影响
对称加密	加密强度降低
非对称加密	可破解
散列计算	无影响

对四个主要场景的影响

量子加密：量子时代的数据加密方案

利用量子技术应对量子时代的挑战

腾讯云 | 连接智能未来

数盾

量子技术	特点
量子随机数发生器 **QRNG**	真随机、不可预测
量子密钥分发 **QKD**	无法复制，窃听

数盾独有方案	特点
抗量子加密算法 **PQC**	基于量子安全的散列运算

对四个主要场景的影响

加密传输
- 对称加密
- 通过加长密钥提高安全性✓

密钥协商
- 使用非对称加密
- 可破解✗

身份认证
- 使用非对称加密，摘要计算
- 可破解✗

数字签名
- 使用非对称加密，摘要计算
- 可破解✗

量子加密：基于量子密码技术的数据加密解决方案

应用层	抗量子数字签名	量子传输加密	抗量子身份认证	传统加密场景
服务层	量子密钥管理/分发	抗量子加密	密钥管理/分发	加解密计算
算法层	基于散列	多变量密码	量子傅里叶变换	大数分解	椭圆曲线
	纠错码	格密码		区块置换	加盐散列
物理层	量子真随机数发生器			噪音随机数发生器	
	量子密码技术			传统密码技术	

文件校验

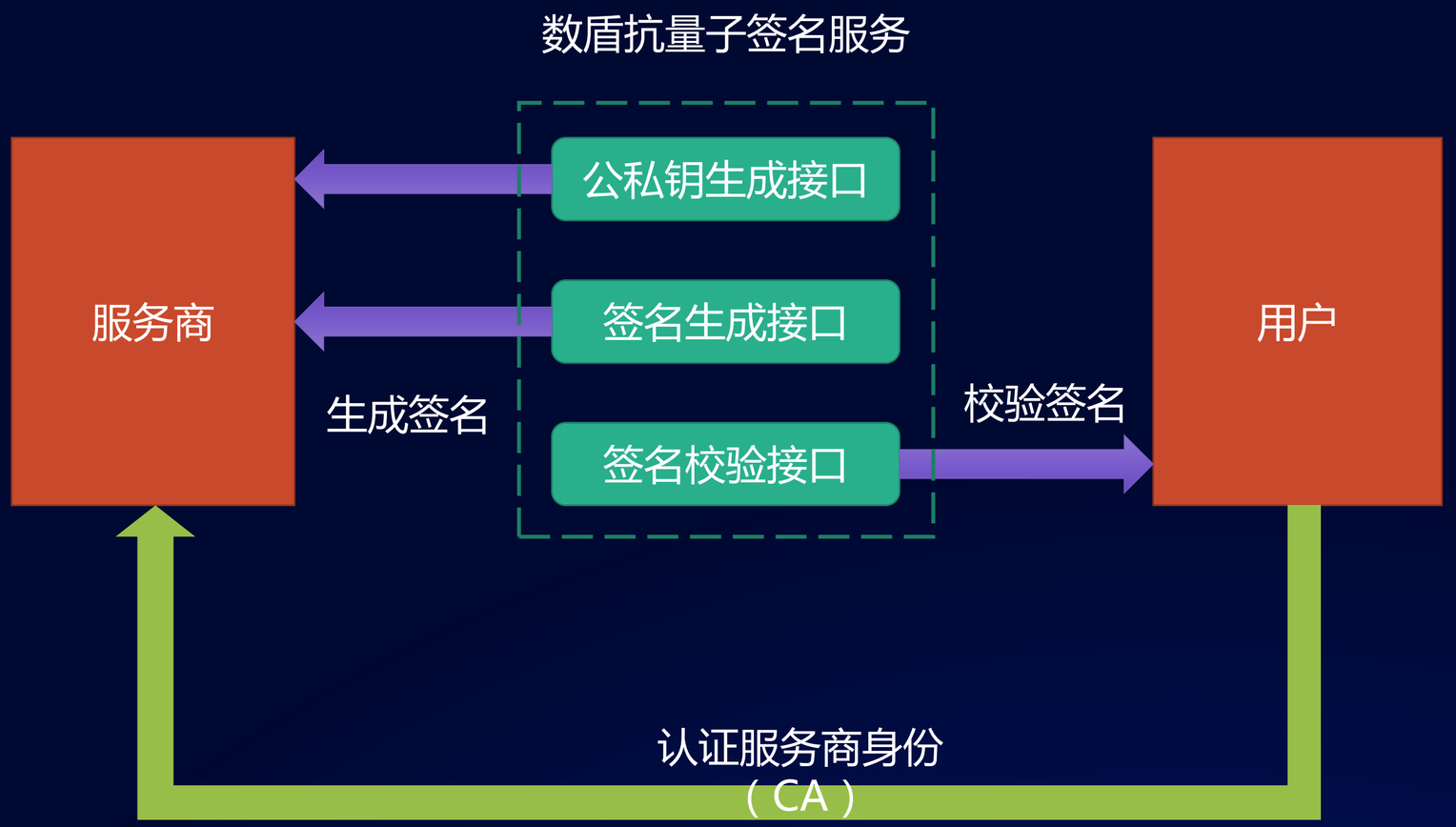
应用签名

安全存储

身份鉴定

量子加密：抗量子签名服务

基于量子安全的散列运算，可抵抗量子攻击



腾讯云数盾，助力各行各业数据安全建设

互联网个人信息泄露事故追溯

满足金融安全合规

全流程防护智慧零售数据分析

医疗信息系统

企业敏感数据安全管理

政务网络国产密码服务


以我所能 为你而+
腾讯云 | 连接智能未来