密码学技术如何选型？终探量子计算通信的安全模型

原创 严强 微众银行区块链 4月8日

严强，SMU信息安全方向博士，信息安全顶级国际学术会议最佳论文奖获得者；曾作为Google隐私保护基础技术架构部门唯一来自中国的早期核心成员，领导研发的技术方案在Android和Google Play生态各大门户产品中全面集成投产。

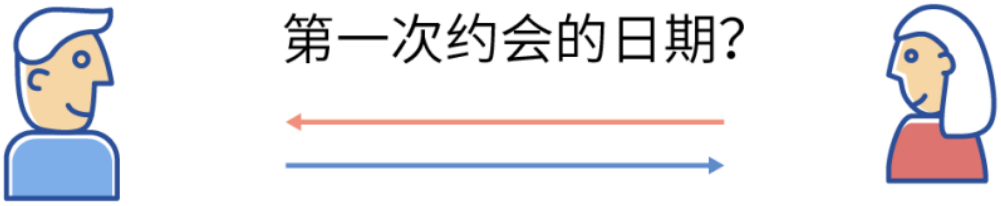
经典密码学技术的应用寿命将至？量子计算何以破解现有隐私保护方案？量子通信对隐私保护方案设计有何启示？如何有效应对量子计算通信技术给隐私保护带来的挑战？

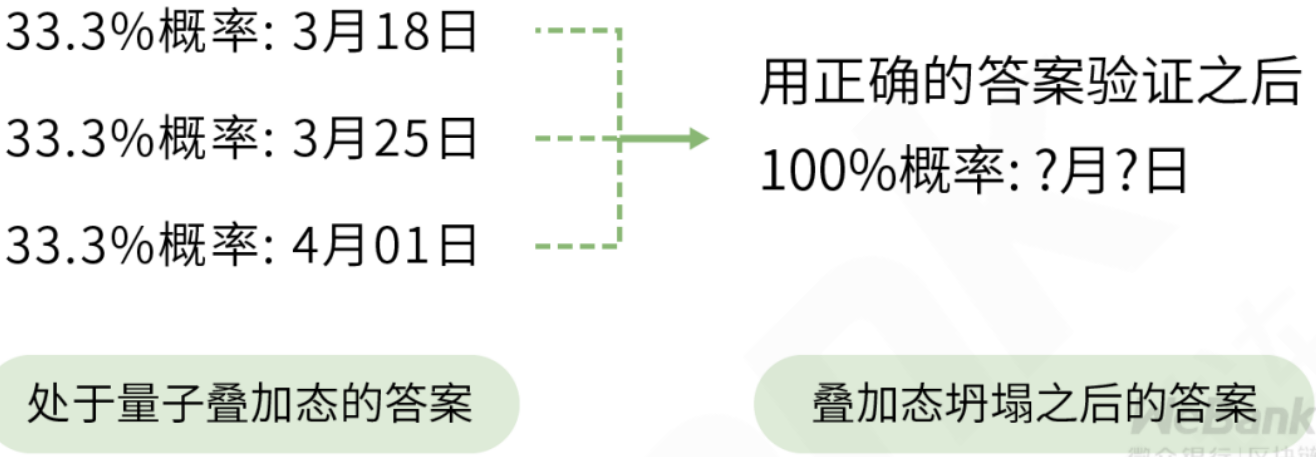
这里，我们将进入安全模型分析三部曲的最终章，跳出现有计算和通信能力的局限，着眼未来技术发展对隐私保护技术选型的启示，剖析量子计算和量子通信技术对经典密码学技术的影响，以及业务技术选型上的应对之道。

量子计算和量子通信都是基于量子力学的新兴技术。不同于经典物理理论，量子力学研究的是物质世界微观粒子运动规律的物理理论，可用来解释经典物理理论无法解释的微观系统。该理论与相对论一起并称为现代物理学的两大基本支柱。

量子力学中，最经典的故事莫过于薛定谔的猫，如果类似故事用主人公小华和好友美丽来演绎，将会是这样的：

> 小华初见美丽时，便萌生好感，经过前3论故事的“接触”，小华对美丽情有独钟。一个浪漫的午后，小华鼓起勇气向美丽告白。美丽心中早已倾慕小华，但矜持的她故意给小华一个小小的挑战，以此验证小华的真心——“我俩第一次约会的日期是哪一天？”
>
> 这可难住了小华！美丽的小剧场之前一共进行了3期，小华觉得这3个日期都有可能是正确答案。幸好，量子计算帮助小华解决了这个难题。





在传统计算模型中，小华一次只能将一个日期的结果发送给美丽，如果答案不对，美丽用正确的结果进行验证后就会出错，那么小华的表白进程就有点尴尬了。在量子计算过程中，小华的答案则会同时包含这3个日期所有的结果，当美丽用正确的答案进行验证时，便可顺利验证通过。

量子力学中，这种同时包含所有可能答案的状态就称之为**量子叠加态**。一旦结果被美丽接收，即观测后，对应的量子叠加态就会发生概率性坍塌，答案就会唯一确定为某一个具体值，美丽就可以得到与心里匹配的答案了。

这种**概率性的状态表达**，以及观测事件之间的**概率关联性**，是量子力学的核心理论要点。以此构建的量子计算和量子通信，都是利用量子的概率特征来突破现有技术的能力瓶颈。

以下将通过对比的方式，介绍经典计算机技术和量子计算机技术的差异，解析这些差异对基于密码学的隐私保护技术方案有何影响和启示。

0.1.

量子计算机 VS 冯·诺依曼计算机

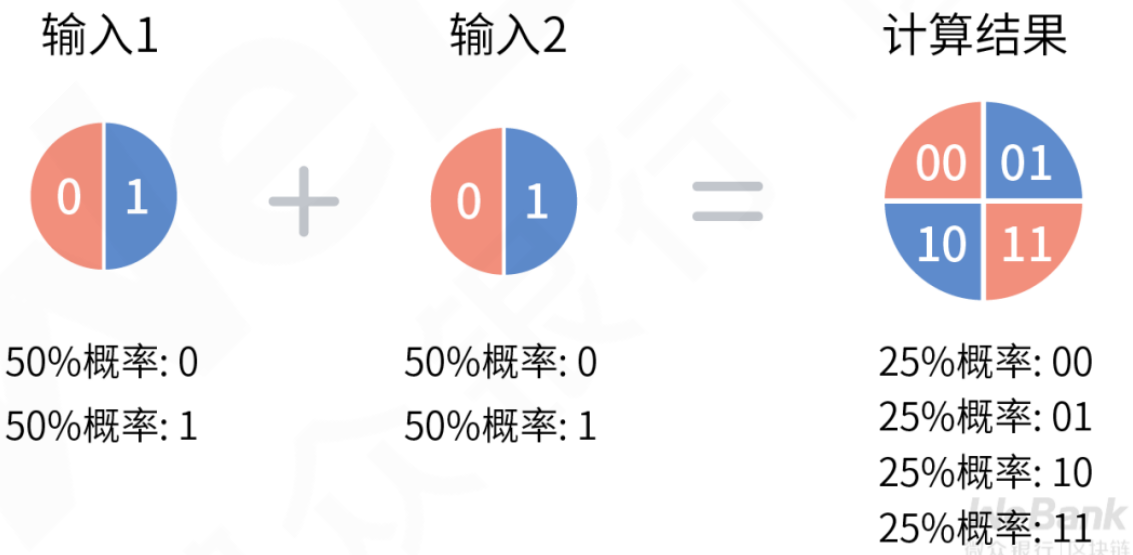
1945年，物理学家和数学家John von Neumann提出一种理论计算模型——冯·诺依曼架构，为现代计算机系统设计奠定了理论基础。

冯·诺依曼架构将计算的过程表达为数据存储过程和程序控制过程，数据和指令都以二进制的形式保存在存储介质中，并由以CPU为代表的控制器读取指令流，控制对不同数据的读写，以此串行执行程序。

尽管多核多线程CPU早已普及，但其核心执行流程依旧是在冯·诺依曼架构下的串行执行，对应的软件实现和算法设计，都是在串行执行程序的前提下进行的。

相比之下，量子计算机由于量子叠加态带来的概率不确定性，天生自带并行属性。

根据量子力学中的波粒二象性，每一个量子可以表达成符合一定概率分布的波。对应到计算机系统设计中的二进制格式，就是单独一个量子可以同时表达0和1的值，并能够同时以0和1的值与另一个量子进行交互，完成并行计算。



这样的一个量子通常被称之为qubit，由于量子态内在的不稳定性，表达一个可读取的逻辑qubit，通常需要维持多个物理qubit来实现系统容错。控制这些qubit，需要在接近绝对零度（零下273.15摄氏度）的超导环境中进行，非常具有挑战性，目前对应的工程实现尚属早期。

Google在2019年的论文中披露，已经可以一定程度上控制53个逻辑qubit的量子计算机，在3分20秒内完成对一个随机数序列是否由一个随机数生成器来生成的证明，同样的证明在现有冯·诺依曼架构下的超级计算机上执行，需要大约1万年的时间。

早在2017年，Google的合作公司D-Wave发布了D-Wave 2000Q，据称实现了2000个逻辑qubit的量子计算机，理论上可能已经具备破解当下所有经典密码学技术方案实现的技术能力。

量子计算机提供了指数级别的计算速度提升，可以打破我们在第3论中提到的计算不对称性。对于冯·诺依曼计算机，经典的NP问题是一个计算困难性问题，而对于量子计算机，理论上可以轻易实现P = NP，攻击者可以由此破解对应的经典密码学算法，提取出对应密钥和密文中的隐私数据。

根据美国国家标准与技术研究院NIST分析，**量子计算机对于非对称密码学体系冲击最大**。用来构造公钥密码算法的经典计算困难性问题，如大数分解困难问题、离散对数困难问题、椭圆曲线上的离散对数困难问题，在量子计算机上均有有效的破解算法——Shor算法及其变体。这些攻击会具体影响到现在的公钥加密、数字签名、数字证书、密钥交换等的安全性。

相比非对称密码学体系，**量子计算机对称密码学体系冲击相对较小**。只要适度增加密钥的长度，就能限制目前最有效的Grover算法攻击，但不排除将来会有更高效的量子破解算法面世。这些攻击会具体影响到对称加密、哈希，以及基于哈希的派生算法。

密码学应用	不完整举例	潜在应对策略
非对称密钥数据加密和数字签名	RSA，DSA，ElGamal，ECDSA，SM2	替换为抗量子算法
密钥交换	Diffie-Hellman密钥交换	替换为抗量子算法
数字证书	X.509，国密证书	替换为抗量子算法
加密通信	TLS，HTTPS，IPsec	替换为抗量子算法
硬件可信执行环境	SGX	替换为抗量子算法
对称密钥数据加密	AES，DES，SM4	增大安全参数值
数据摘要和哈希	SHA-3，HMAC，SM3	增大安全参数值
随机数生成器	RNG	不受直接影响
密钥生成和派生算法	KDF	不受直接影响

量子计算机对于经典密码学算法的影响，不仅作用于软件层面，对硬件层面也有很大冲击。

目前，以Intel SGX为代表的硬件可信执行环境，其内部实现的密码学算法都是不抗量子计算的。部分对性能要求高的模块，如SGX的内存加密模块（目前为AES-128），是以不能升级的硬件方式实现的。一旦量子计算机得到有效应用，相比远程替换算法软件，物理替换可信硬件可能会带来更大的代价。

为了应对量子计算对经典密码学算法的威胁，我们需要构造新的计算困难性问题。考虑到量子计算安全模型，即允许攻击者使用量子计算机的安全假设下，构造安全的密码学算法充满很多不确定性，目前尚无相关国际或国家标准。

NIST已经于2019年开始了第二轮抗量子算法标准的公开评估，预期在2021年会有一定的阶段性成果，之后会开展第三轮的公开评估流程，预期在2022年完成标准草案。时任中国科学院信息工程研究所副所长的荆继武，在2018年的新闻报道中表示，我国或将在2022年前后开展抗量子算法的标准化工作，预期2025年左右实现商业化落地。

在工程上的标准制定完成之前，须谨慎使用现有抗量子算法，即便是源自顶级学术刊物的方案也有出错的可能性。另一方面，如上一论所言，即便理论上是安全的，工程实现上的疏漏也会导致隐私数据泄露。

所以，使用经过一定时间检验的抗量子算法工程标准，是确保最终隐私保护方案有效性的必要条件。

量子通信 VS 经典通信

经典通信中的信息传递，由发送方通过传输介质向接收方发送各类信号载体的方式进行，其传输的速度受限于传输介质的传导性和信号载体的能量衰减率，根据相对论，其最高传输速度不超过光速。

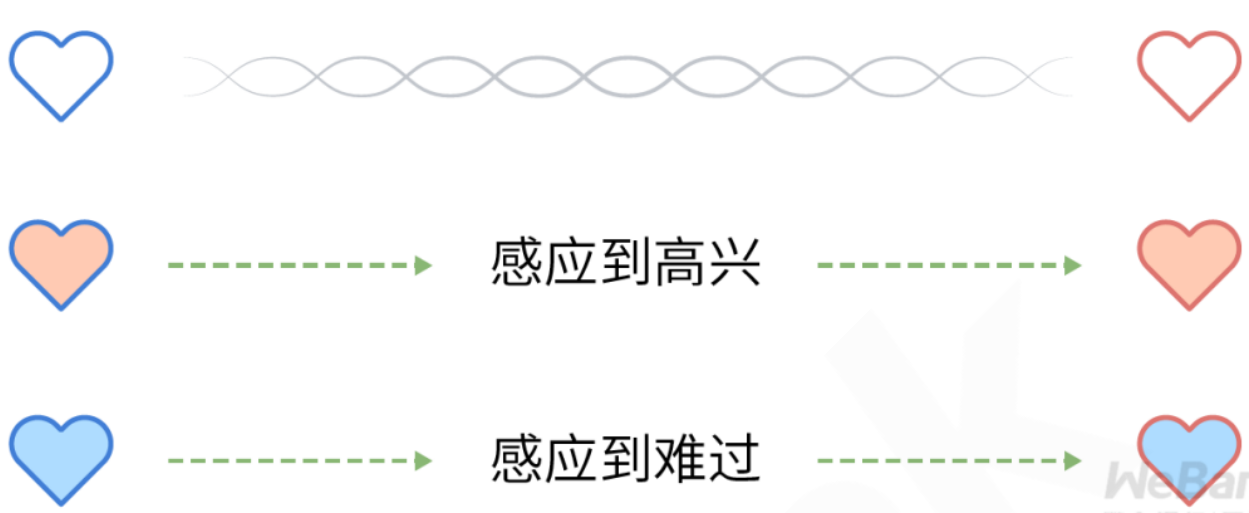
相比之下，量子通信是基于量子纠缠原理，理论上在设备初始化之后，并不需要由发送方向接收方发送任何信号载体，有实现超光速瞬时通信的可能性。

关于量子纠缠理论的解释，我们继续以小华和美丽的故事来呈现：

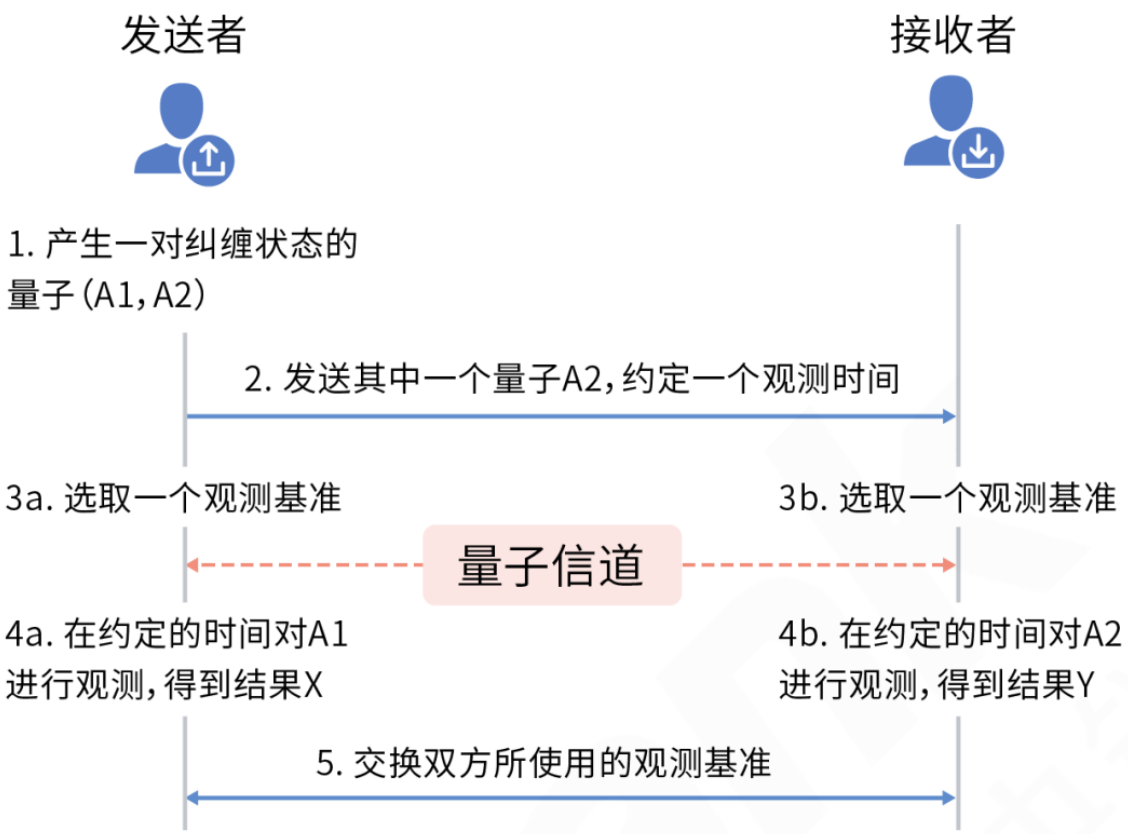
承接上面的故事，小华基于量子计算有惊无险地通过了美丽的考验，成功牵手美丽，并与之确定恋人关系。

阳光明媚的一天，两人相约在游乐场共度一个温馨的午后。临别时，美丽预感会有惊喜发生。一转身，小华正拿着自己最中意的玩偶缓缓靠近，恍惚间，美丽仿若偶像剧女主角，脸上漫开了幸福。

两人的心电感应，就类似于量子之间的纠缠态。对处于纠缠状态的量子对中的一个量子进行观测，会导致量子对中另一个量子的状态做出相应改变，这一改变与之前的观测结果有100%的关联性。小华充满爱意的心做出变化，与之对应地，美丽的内心就会有所感应。



尽管量子纠缠的特性可以无视物理距离进行信息传递，但由于目前的量子密码通信协议设计，如经典BB84协议和Ekert91协议，依旧需要配合经典通信信道来实现信息的加密传输，所以，量子密码通信实现依旧不能达到超光速传递信息。



如果发送者和接收者选用了相同的观测基准，根据量子纠缠理论，X 与 Y将严格满足如下关系：

if X = 1, Y = 0
if X = 0, Y = 1

由此发送者和接收者可以通过量子信道获得相同的随机数序列，实现后续数据加密传输所需的密钥协商。

关于量子密码通信的安全性，一个常见的观点认为它是信息论安全的，即无论攻击者拥有多少计算资源，例如量子计算机，也无法破解其安全性。对应的解释是，其安全性不是由计算困难性理论来保障，而是由物理学法则中的**测不准原理**来保障。

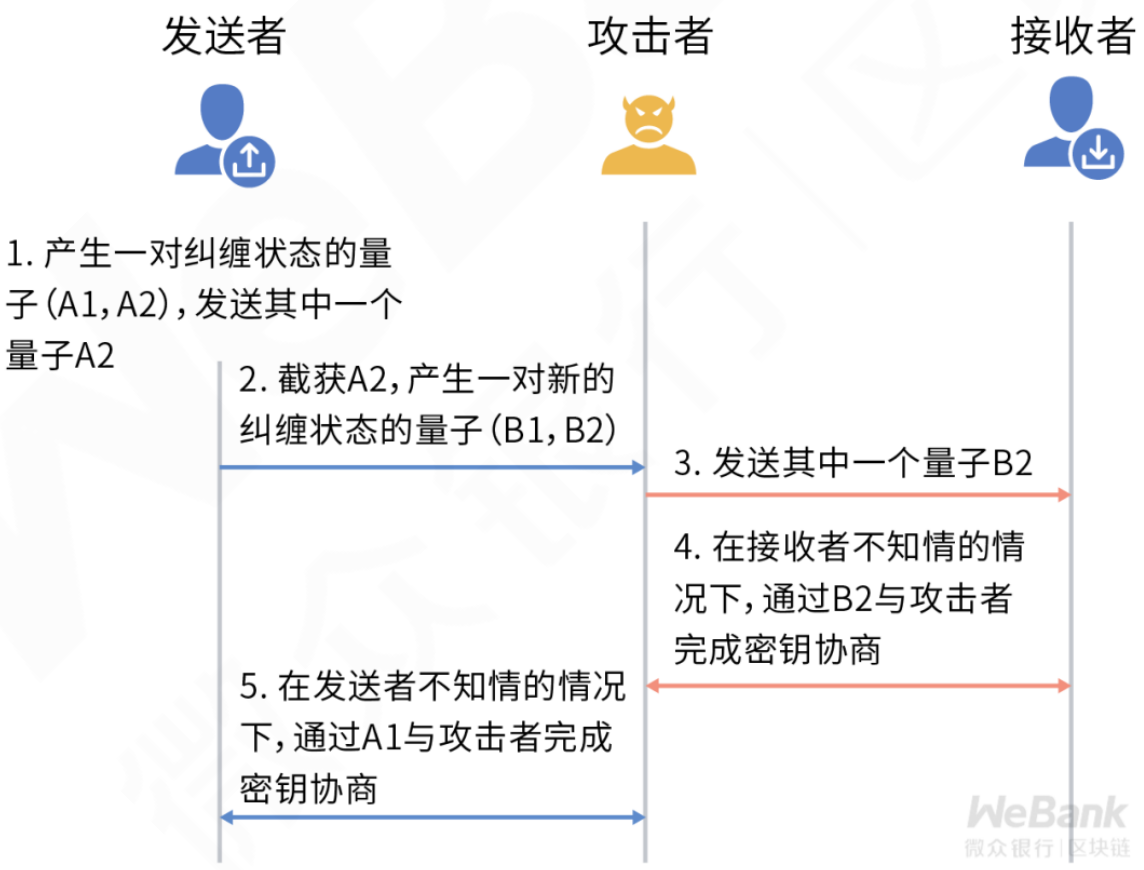
测不准原理由物理学家海森堡在1927年正式提出。作为量子力学的基本原理之一，该原理规定，对于一个量子，不可能同时知道它的位置和速度，每一次对量子的观测都会改变量子的状态。由此可以进一步推出**不可克隆原理**，即攻击者无法完美地复制一个量子的所有状态。

对于量子通信而言，即便攻击者有能力截获一个处于纠缠状态的量子，也不能完美地复制它。

攻击者无法在接受者不知情的前提下，将复制的量子转发给接受者，以此实现对于敏感数据的窃听。一旦窃听发生，必然会改变被窃听的通信双方的量子状态，由此暴露攻击者的存在。

这里需要注意的是，尽管量子密码通信协议能够有效检测出直接进行窃听的攻击者存在，但依旧可能受到其他协议层面攻击的影响。

例如，经典的中间人攻击，攻击者作为中间人在通信双方之间转发消息，对于发送方使用一对纠缠状态的量子，对于接收方使用另一对纠缠状态的量子，此时如果没有其他可信的信道连接通信双方，他们将无法感知攻击者的存在。



在工程实现方面，目前我国处于国际领先水平。2016年，墨子号量子科学实验卫星率先实现了千公里级星地双向量子纠缠密钥分发，有效带宽约为每秒千比特。

但量子通信距离民用还有相当的距离，主要受限于量子信道的不稳定性。在强干扰环境中，如日光环境、城市密集地带，长距离传输处于纠缠状态的光量子，依旧是一个巨大的挑战。

量子通信的现世，对密码学协议以及上层隐私保护方案的构造来说，无疑添加了一把利器。作为一个可信信道，量子通信可以有效简化密码学协议设计，并提高隐私保护方案的有效性，一定程度上抵抗量子计算机带来的威胁。

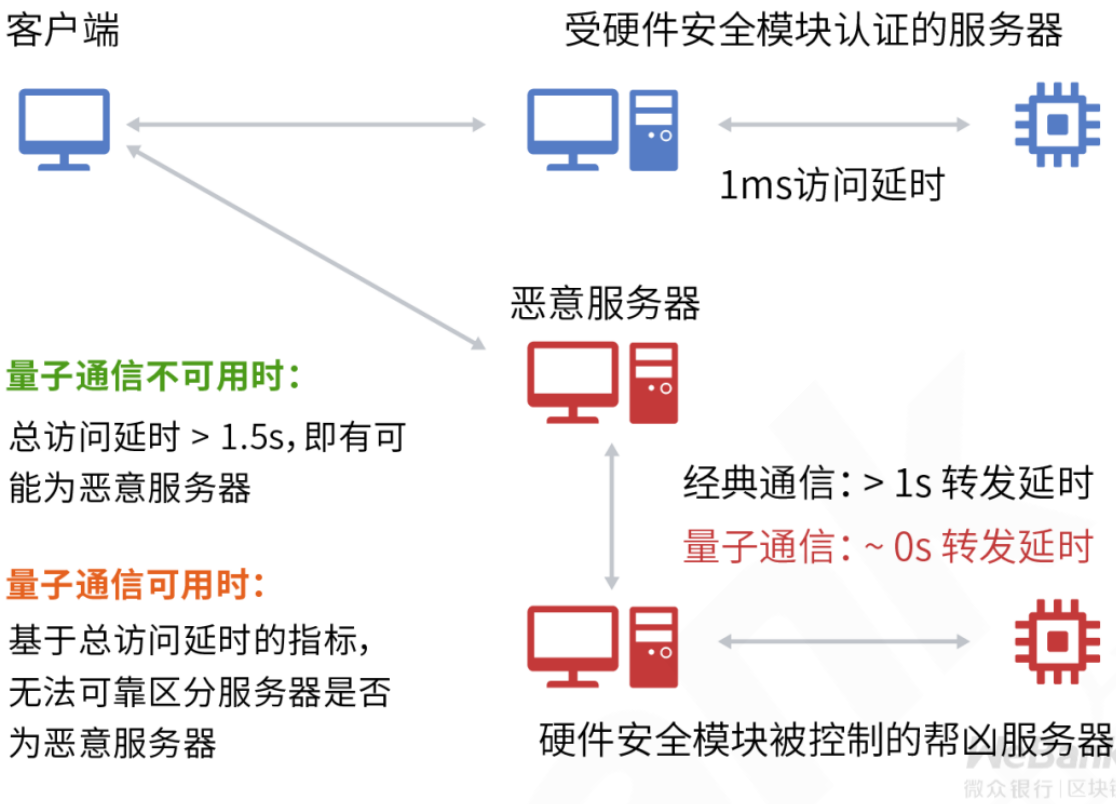
同时，对当下基于传输时间的物理限制而设计隐私保护方案来说，量子通信的出现会影响其有效性。

比较典型的例子是，结合硬件安全模块和物理距离检测的远程代码验证协议。在该协议的验证过程中，诚实的验证者会直接调用本地的硬件安全模块来完成服务器认证，只需要一次交互，有效延时能控制在较短的时间之内（如1ms）。如果攻击者试图对该协议进行攻击，必须要通过代理服务器对数据进行转发，在只考虑经典通信的前提下，额外的转发延时则需要较长的时间（如1s以上）。

因此，即便攻击者控制了另一个硬件安全模块，将远程代码验证请求转发到被控制的硬件安全模块，让其代为计算，攻击者实际消耗的总时间，也会比没有转发时，直接在本地使用未被攻克的硬件安全模块计算耗时显著地长，由此可以检测出攻击者的存在。

以上信息传递需要一定时间的安全假设，在量子通信的距离无关瞬时通信能力面前不再成立。原本攻击者使用代理服务器转发的时间，可能会由1s急剧缩小到接近0s。这一变化显著降低这类依赖信息传输时间限制而构造的远程代码验证协议的有效性，使其面临整体失效的风险。

总体而言，量子通信的出现将为信息传输过程带来了新的基本特性，基于经典通信特性设计的隐私保护方案需要适时进行再评估，核实其在量子通信安全模型下的有效性。



正是：密码经典功高无敌手，量子新秀刃利待出鞘！

量子计算和量子通信是信息技术发展过程中，一个重要的里程碑式突破，势必会对现有的技术体系产生冲击，影响现有隐私保护技术方案的有效性，但同时这些新理论和工具也将推动相关技术的革新，促使更高效、更安全的隐私保护技术方案的出现。

目前两者的工程实现距离商用还有不小的距离，加之工程技术标准化尚在逐步推动中，企业在技术选型时，应充分考虑其带来的风险，对使用经典密码学算法和硬件安全模块的系统提供可拔插设计，对不同保密级别的隐私数据提供必要的备选方案，以此控制特定量子计算通信技术突然实用化带来的冲击。

密码学技术选型相关的重点理论科普到此暂告一段落，下一论开始，我们将具体展开对密码学算法核心组件的技术剖析，欲知详情，敬请关注下文分解。

---END---

《隐私保护周三见》

“科技聚焦人性，隐私回归属主”，这是微众银行区块链团队推出《隐私保护周三见》深度栏目的愿景与初衷。每周三晚8点，专家团队将透过栏目和各位一起探寻隐私保护的发展之道。

栏目内容含括以下五大模块：关键概念、法律法规、理论基础、技术剖析和案例分享，如您有好的建议或者想学习的内容，欢迎随时提出。

栏目支持单位：零壹财经、陀螺财经、巴比特、火讯财经、火星财经、价值在线、链客社区

往期集锦

第1论 | 隐私和效用不可兼得？隐私保护开辟商业新境地

第2论 | 隐私合规风险知几何？数据合规商用需过九重关

第3论 | 密码学技术何以为信？深究背后的计算困难性理论

第4论 | 密码学技术如何选型？初探理论能力边界的安全模型

第5论 | 密码学技术如何选型？再探工程能力边界的安全模型

长按二维码关注

微众银行区块链

白皮书下载 | 订阅干货 | 进群交流 | 合作联系