# 密码学原语如何应用？走近门限密码算法

[](https://www.zhihu.com/org/wei-zhong-yin-xing-qu-kuai-lian)

[**微众区块链**](https://www.zhihu.com/org/wei-zhong-yin-xing-qu-kuai-lian)

*作者：李昊轩 | 微众银行区块链核心开发者*

*来源：微众银行区块链微信公众号*

隐私数据密文控制权只能由单一主体掌控？代表控制权的密钥如何才能安全地交由多个互不信任的主体协同使用？如何在技术层面保障多方授权的公平公正性？任一参与协作的主体密钥丢失，如何实现安全可靠的容灾恢复？

在业务方案设计中，安全可控地让多个隐私主体参与数据协作，是隐私保护技术创造新兴商业价值的关键之一。在这一过程中，代表控制权的密钥由哪一方来掌握，是影响参与者合作意愿的重要因素。

**因为哪一方拥有了密钥，相当于哪一方就获得了控制权，未能掌控密钥的另一方，则可能在合作关系中处于弱势。这将成为实现公平对等多方协作关系的一个关键阻碍。**

以多方决策为例，上市公司的一次董事会会议中，需要多数董事对决策项进行签字才能生效。出于某些影响，会议无法面对面举行，所有董事必须使用数字签名来远程完成这一个签字过程。为了保证决议过程的机密性和公正性，每位董事不希望其他董事知晓自己的选择，同时要让股东团体对最后的决策结果，即聚合后的签名，进行验证。

这个过程中，存在三个隐私保护相关的主要功能点：

* 每位董事的签名控制权须由自己控制，而不是由中心化的可信第三方来代理行使权力。
* 代表决策结果的聚合签名只需多数董事同意，便可生成合法的声明。
* 股东团体需要对聚合后的签名进行验证，但无需知道具体哪些董事对此进行了签名。

**以上功能点涉及在多方协作过程中，如何将原本单个的密钥安全地打碎成多个密钥分片，并让每个主体独立使用自己的密钥分片，合作完成所需的密码学协议过程。**解决这一问题的关键，就在于门限密码算法的巧妙构造。

门限密码算法在多方协作的相关场景中应用十分广泛，可以实现数据联合授权、认证、密钥安全恢复、密钥安全交换等需求，在诸多分布式多方计算协议中均可见其身影。

本文主要从秘密分享、门限加密、门限签名三大应用方向，分享门限密码算法的奇妙之处。

## 1. 秘密分享

1979年，Adi Shamir和George Blakley各自独立地提出秘密分享（Secret Sharing）的概念，奠定了门限密码学体系的基础。具体而言，秘密分享是指一种安全地在多个参与者之间分享秘密的方式，其满足以下特性：

* 每个参与者都独立持有一部分关于秘密S的分片，只有将足够数目的分片组合起来，才能够重新恢复出秘密S。
* 当获得的分片数量不足时，无论采用何种组合策略，不会泄露关于秘密S的任何信息。

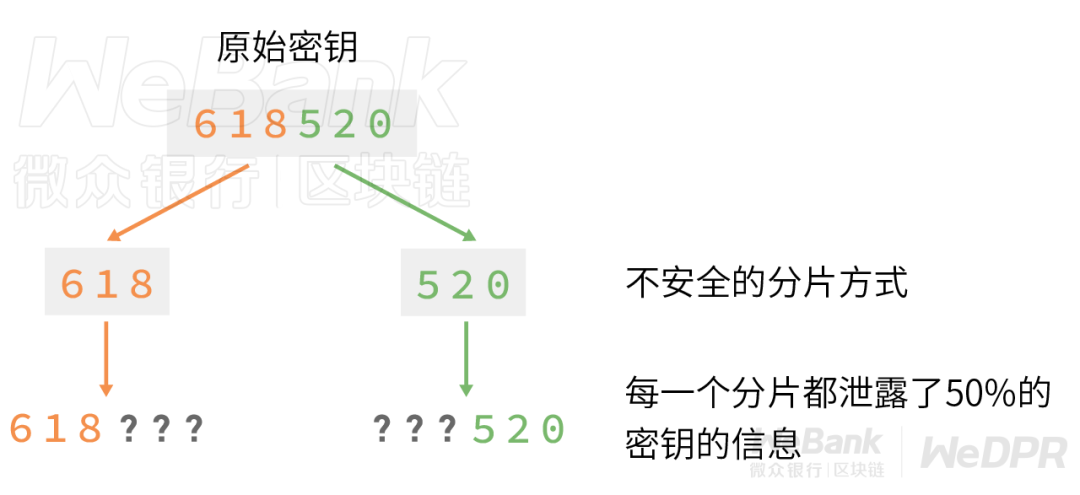
秘密分享在学术上的价值在于，提供了一种技术手段，将原本单一的密钥，以密钥分片的形式，安全地、平等地分配到多个参与者手中，除此之外，还实现了以下额外的安全特性：

* **容错高可用**：不会因为少量密钥分片损坏和丢失，而导致密钥不可用。
* **抗侧信道攻击**：原本固定的密钥，在密码学算法工程实现的执行过程中，可能会泄露一部分密钥的信息（参见[第5论](https://link.zhihu.com/?target=http%3A//mp.weixin.qq.com/s%3F__biz%3DMzU0MDY4MDMzOA%3D%3D%26mid%3D2247484389%26idx%3D1%26sn%3D62fe8b7ab31f7f36ee27bfa6e24beab3%26chksm%3Dfb34ca18cc43430efd274932216485a2308e3a3f01e779afb76c0be967a823d3bd8b77781ea8%26scene%3D21%23wechat_redirect)中的灰盒安全模型），但进行分片之后，成功实施此类攻击的难度将指数上升。

对于业务应用而言，主要使用的特性是**密钥安全平等分配**和**容错高可用**，可以用来满足价值贵重的物品或权利不能由单一主体掌控的业务需求，以此控制盗用、滥用等潜在风险。

例如，董事会的印章不能由单独的成员持有，银行保险箱的钥匙不能由单独的职员保管。在数字化的场景中，涉及多方隐私数据的业务合作，数据密钥也不能由单一主体掌管。

为了实现安全的秘密分享效果，最直接的秘密字符串分片方式并不能保障其安全性，攻击者无需收集足够的分片，便可以获得秘密的部分信息，示例如下：



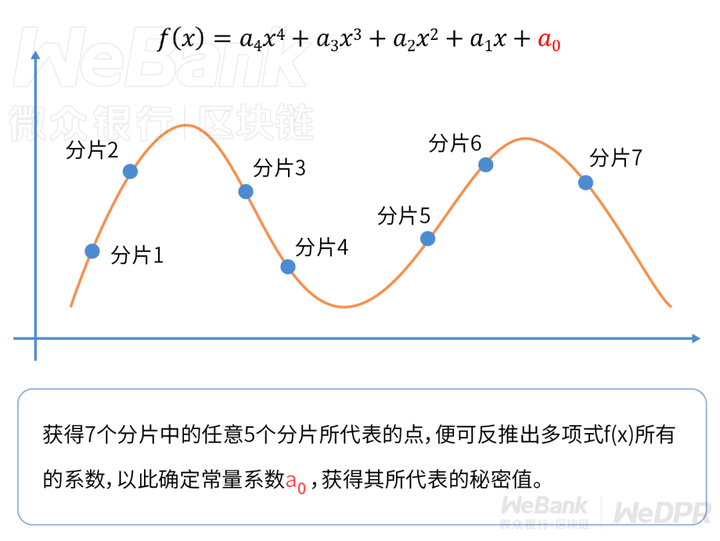
因此，我们需要引入更为精巧的分片构造方式。

最常见的构造方式利用了拉格朗日多项式插值算法。其核心思想为，t个点可以确定一个t-1阶多项式对应的曲线。每一个秘密分片都相当于多项式曲线上的一个点：

* 只要收集不同点的数目达到t个，就可以通过拉格朗日多项式插值算法求解出多项式中代表秘密的系数值。
* 如果点的数目不足t个，对应的多项式有无限多个，对应的秘密可能是任意值，对秘密的机密性保护达到了信息论安全。

具体构造方式可以参考Shamir Secret Sharing的(t, n)秘密分享方案，即，将秘密分为n份，任意t份都可以完整地恢复出拆分前的秘密。构造过程如下：

* 将秘密S作为多项式的第0阶常量系数，其余t-1个系数随机生成，由此构造出一个t-1阶的多项式，对应的曲线为C。
* 在曲线C上随机选n个不同的点，将其分发给n个参与者。
* 只要不小于t个参与者同意使用自己的点参与协同运算，便可恢复出曲线C对应的多项式，取其中第0阶常量系数，便可获得秘密S。



秘密分享在分布式密钥生成、密钥容灾恢复、数字版权管理、数据安全传输等业务领域中都有广泛应用。同时，秘密分享也是用于构造安全多方计算的重要技术之一。

基础的秘密分享方案可以进一步扩展为可验证秘密分享、多级多秘密分享、定期更新分片的主动秘密分享、可随时变更参与者的动态秘密分享、基于身份的秘密分享等方案，满足多方协作中多样化的业务需求。

**秘密分享是所有门限密码算法的基础，解决了算法设计中密钥控制权安全分发的问题，用技术手段保障了隐私数据多方协作中，权利均衡、平等互信的效果。**

## 2. 门限加密

门限加密方案是门限密码算法常见应用之一，常常体现为一类分布式加解密协议，可以实现如下功能：

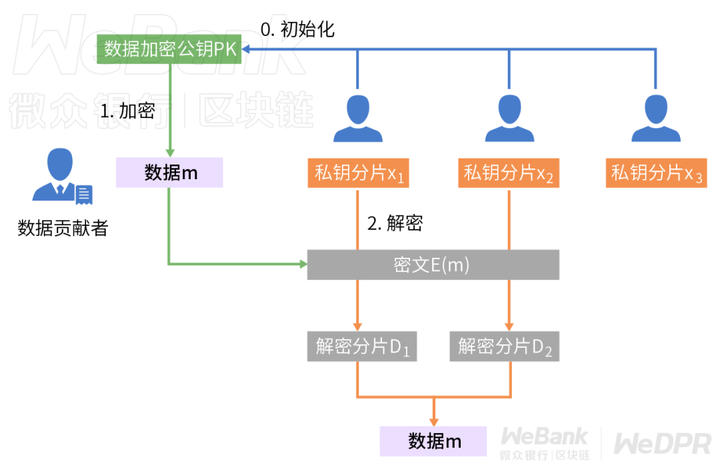
* 任意用户都可以使用公钥对数据进行加密。
* 私钥的所有权由多个指定的秘密持有者联合控制，只有满足数目的秘密持有者合作，将解密分片聚合，才能实现解密。

**门限加密方案可以有效保护需要多方授权才能使用的隐私数据。**回到之前董事会决策的示例，目前有一份敏感的业务数据需要给董事会成员汇报，由于数据的敏感性，需要确保有足够数量的董事在场，数据才能被解密。

门限加密方案可以很好地满足这一需求。传输业务数据前，使用门限加密的公钥对其进行加密，产生的密文只有当数量不少于门限值的董事授权同意之后才能进行解密。

使用门限加密方案的一般流程如下：

* **初始化**：n个参与者约定设置门限值t，并获取自己的私钥分片x，联合计算数据加密公钥PK并公开。
* **加密**：数据贡献者使用公钥PK对数据明文m进行加密，生成密文E(m)。
* **生成解密分片**：参与者分别使用自己的私钥分片x对密文E(m)进行解密，生成解密分片D\_x(m)。
* **聚合解密分片**：参与者将解密分片聚合，只有获得不小于t个不同的解密分片D\_x(m)之后，才可以完成聚合解密，获得数据明文m。



理论上，门限加密方案可以基于不同的计算困难性问题（参见[第3论](https://link.zhihu.com/?target=http%3A//mp.weixin.qq.com/s%3F__biz%3DMzU0MDY4MDMzOA%3D%3D%26mid%3D2247484310%26idx%3D1%26sn%3De780ccd6fc2eed51ec2ccc6f6b7803b9%26chksm%3Dfb34ca6bcc43437d447b0da56c68b125b01950f801362336e07184f091468537921066ccd2c8%26scene%3D21%23wechat_redirect)）构造，例如，基于离散对数的ElGamal门限密码学体系、基于Diffie-Hellman的门限密钥交换协议、基于大素数分解的RSA门限密码学体系、基于椭圆曲线离散对数问题的BLS门限密码学体系等。

工程上，门限加密方案目前已经比较成熟，以经典论文《Simple and Efficient Threshold Cryptosystem from the Gap Diffie-Hellman Group》为基础的开源参考实现为例，在个人计算机上，对单个数据块进行单次分片聚合和解密的耗时都在微秒级，**已经可以满足大部分业务的商用性能要求**。

应用上，除了之前描述的多方授权数据解密之外，门限加密方案在匿名电子投票、数据代理服务、数据外包计算等需要为**多个数据贡献者提供联合数据使用授权特性**的领域，均有广泛应用前景。

## 3. 门限签名

门限签名方案是门限密码算法最常见的应用。同样基于秘密分享的核心理念，门限签名方案通过将私钥拆分成多个秘密分片，实现了如下效果：

* 只有当不少于门限值的秘密分片持有者共同协作，才可以生成有效的签名。
* 即便部分秘密分片丢失，只要剩余秘密分片不少于门限值，依旧可以生成有效的签名。
* 联合生成的签名中，并没有透露具体哪些持有者参与了签名过程。

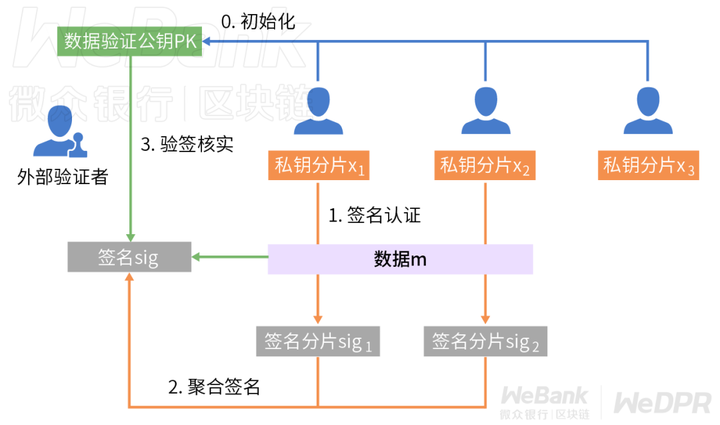
**在业务应用中，门限签名方案可以用来构造有效的多方联合签名流程。相比传统数字签名方案，整个签名过程消除了由单一主体保管密钥带来的系统性单点故障风险，以及跨机构信任问题。**

**每位秘密分片的持有者对签名私钥拥有平等的控制权，门限签名方案同时提供了私钥容灾恢复功能和外部验证匿名性。**

这类方案可以显著提高用户对数据认证的信任，并促进多方平等合作，**对于目前使用数字签名的所有应用场景都适用**，可以看作是传统数字签名方案在分布式商业环境中的全面升级。

使用门限签名方案的一般流程如下：

* **初始化**：n个参与者约定设置门限值t，并获取自己的私钥分片x，联合计算数据验签公钥PK并公开。
* **生成签名分片**：参与者使用私钥分片x对数据m生成签名分片sig\_x。
* **聚合并生成签名**：将签名分片合并，只有不少于t个签名分片才能生成完整签名sig。
* **验证签名**：验证者使用公钥PK，对关于数据m的签名sig进行验证。



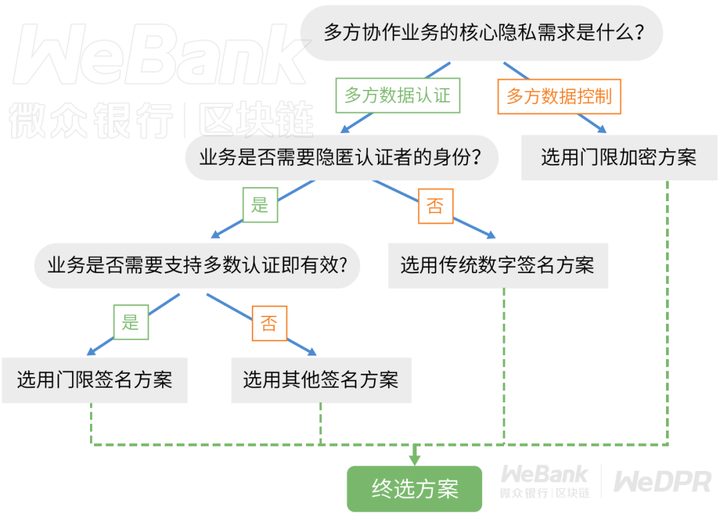
与门限加密方案类似，门限签名方案可以基于不同的计算困难性问题（参见[第3论](https://link.zhihu.com/?target=http%3A//mp.weixin.qq.com/s%3F__biz%3DMzU0MDY4MDMzOA%3D%3D%26mid%3D2247484310%26idx%3D1%26sn%3De780ccd6fc2eed51ec2ccc6f6b7803b9%26chksm%3Dfb34ca6bcc43437d447b0da56c68b125b01950f801362336e07184f091468537921066ccd2c8%26scene%3D21%23wechat_redirect)）来构造实现，例如，可以构造基于SM2国密标准算法的门限签名方案。

目前较为常见的开源实现，主要是基于BLS（Boneh–Lynn–Shacham）的签名算法。该方案验证效率尚可，但在签名聚合环节，生成签名的耗时会随参与者数量的增加而显著增加，可以达到毫秒级，比传统的数字签名方案慢几个数量级。

除此之外，目前的门限签名方案在初始化过程中，如果不依赖可信第三方，会面临交互轮数过多、构造复杂等问题。以上工程问题对需要进行高频签名操作的应用来说，可能会带来一定性能上的挑战，但对于一般应用来讲，应该不会成为性能瓶颈。

**总体而言，门限密码学方案提供了一系列高效、易用的隐私保护分布式数据协作技术**。随着其应用越来越广泛， NIST于2019年提议对门限密码学相关的密码学原语进行标准化，分别从单一主体使用和多方协作使用两个方向，对门类众多的门限密码学方案进行归类和标准化尝试。

在标准化完成之前，根据具体的业务需求，门限密码学方案的基础技术选型可以参考下图：



**正是：多方协作密钥谁掌控，门限密码分权众做主！**

门限密码学方案通过对隐私保护方案中的密钥进行分片，使得对于密钥所代表的数据控制权进行按需分配成为了可能。对于源自多方的隐私数据，门限密码学方案提供了安全、平等、高效的协同认证和计算工具，可以用来解决现代分布式商业环境中，所面临的多方数据认证、可信数据交换等核心业务挑战。

多方数据协作场景中，基于可信硬件（TEE）的解决方案也是目前行业研究的热点，其背后涉及哪些原理，欲知详情，敬请关注下文分解。

<https://zhuanlan.zhihu.com/p/150535159>