密码学原语如何应用？解析密文同态性的妙用

原创 李昊轩 微众银行区块链 5月27日

来自专辑

WeDPR隐私保护周三见

隐私数据在密文形式下是否依旧可以加减乘除？其背后的同态性原理具体指什么？半同态性和全同态性有什么区别？单密钥和多密钥同态加密有哪些奇妙的应用场景？

隐私保护方案设计，往往需要在密文状态下，对隐私数据进行特定的业务操作，以此保障数据的机密性。

沿用上一论的电子支付例子，客户目前拥有一张面额1000元的电子支票，电子支票以密文凭证形式存储，流转过程中不会轻易泄露金额。客户使用这张支票时，消费额可能低于1000元，需要将支票进行拆分找零。假定消费额为200元，这一支票需要被拆分成两份密文凭证，面额200元的给商户，面额800元的留给客户自己作为找零。

这个过程中，存在三个隐私保护相关的主要功能点：

- 客户不希望其他人（包括商户）获知找零的金额为800元，相当于在消费时能保护客户自身财产总额相关信息不泄露。
- 商户需要验证密文支票在本次消费前的余额不小于200元，但无需知道具体的余额。
- 签发密文支票的银行需要验证，客户和商户在交易后，没有凭空造出更多的钱，即消费额与找零额相加等于拆分前的电子支票中的余额。

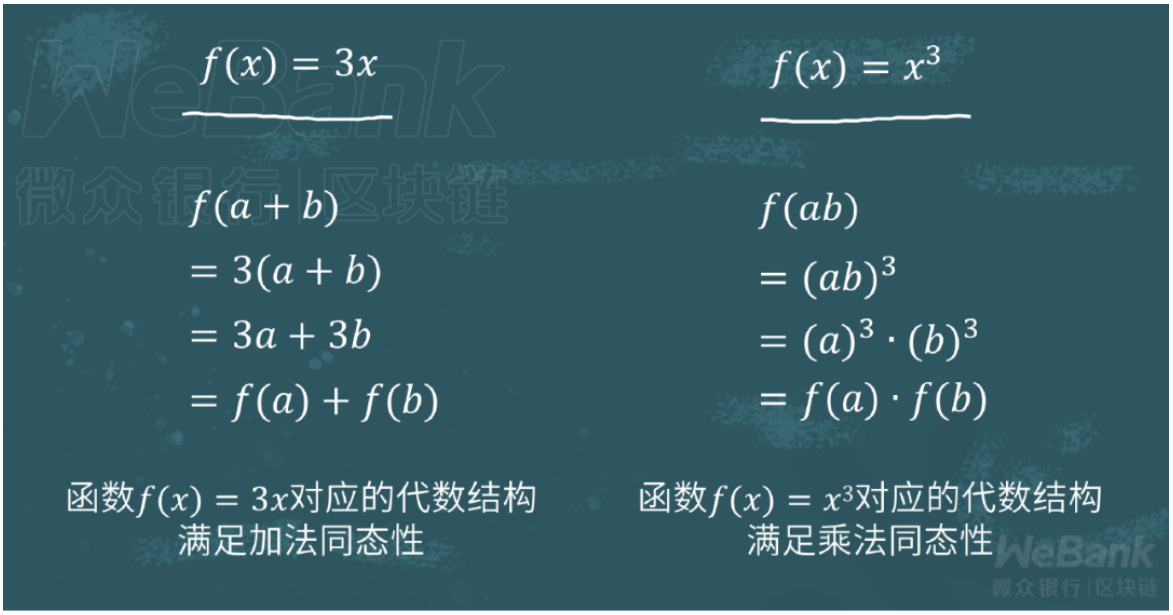
以上功能点涉及如何在不解密的限制下，对隐私数据的密文形式进行计算和验证。而解决问题的关键，就在于密文同态性的使用。

在数据业务中，密文同态性在需要隐私保护的相关场景方案中应用十分广泛，可以实现隐私数据可信跨域协作、联合数据发掘等高价值需求，在多方数据协作、机器学习、云计算等热门领域皆有用武之地。密码学同态究竟有何奇妙之处？且随本文一探究竟。

同态性

同态（Homomorphism）的概念起源于抽象代数，具体是指两个代数结构（例如群、环、向量空间等）之间保持结构不变的映射。

对应地，密码学意义中的同态，多指一类代数结构能够满足在指定运算下结构不变的性质。例如，函数f(x)=3x对应的代数结构满足加法同态性，函数f(x)=x^3对应的代数结构满足乘法同态性。



同态性在密码学中最常见的应用之一，就是用来构造**同态加密**算法。

同态加密允许在不解密的条件下，直接对密文形式下的隐私数据进行特定形式的代数运算，运算效果等同于将隐私数据明文直接计算后再加密所获的效果。

这项技术试图实现**隐私数据协同计算中的数据密文可计算，但明文不可见的效果。**

同态加密一直是密码学研究领域的一个重要课题，经典的算法有RSA、ElGamal、Paillier加密算法。2009年9月，Craig Gentry从理论上取得了重大突破，提出了全同态加密的构造方法，即可以在不解密的条件下，对隐私数据的密文形式进行任意形式的运算，并使得运算之后的结果密文满足同态性。

除了同态加密外，其他密码学原语，如上一论中提及的密码学承诺，也可能具有同态性。

同态加密与具有同态性的密码学承诺在功能上的区别在于：

- 同态加密重在计算，即对多方提供的隐私数据的密文形式进行一定计算后，对结果密文解密后得到的值，等同于对明文数据进行对应运算得到的结果。这个过程不会泄露隐私数据明文，但解密之前无法获知结果。
- 具有同态性的密码学承诺重在验证，即通过密码学承诺密文形式的同态性，对于已知的结果，构造相应的零知识证明，用以证明多个承诺满足一定的约束条件。密码学承诺难以支持计算结果未知、且需要从多方收集隐私数据的密文计算过程。

同态性在不同的密码学原语中会有不同的功能和限制，本文以同态加密算法为例，对同态性的特性和应用进行分享，其他相关密码学原语会在后续专题中展开。

0.2.

半同态vs全同态

同态加密根据支持的运算类型的限制，可分为半同态加密（SWHE，Somewhat Homomorphic Encryption或PHE，Partially Homomorphic Encryption）和全同态加密（FHE，Fully Homomorphic Encryption）。

对于一个半同态加密算法，其密文形式仅仅对部分运算方式满足同态性，有代表性的密码学算法体系如下：

- 加法运算同态性：Unpadded RSA，ElGamal，Benaloh，Paillier
- 逻辑运算同态性：Goldwasser-Micali

- Paillier加密的密文形式为$c = g^m \cdot r^n \bmod n^2$

  其中$(n、g)$为公钥，m为编码后的消息，$r \in Z_n^*$为随机数

- Paillier加密密文具有下列同态性

$$D(E(m_1)E(m_2) \bmod n^2) = m_1 + m_2 \bmod n$$

$$D(E(m_1)^k \bmod n^2) = km_1 \bmod n$$

$$D(E(m_1)g^{m2} \bmod n^2) = m_1 + m_2 \bmod n$$

$$D(E(m_1)^{m2} \bmod n^2) = m_1 m_2 \bmod n$$

$$D(E(m_2)^{m1} \bmod n^2) = m_1 m_2 \bmod n$$

半同态加密算法的优点在于构造相对简单，工程实现效率高，目前已经可以达到商用的性

能要求。

对于引言中密文支票电子支付的例子，使用一个具备加法运算同态性算法便可以构造出满足相关的隐私保护需求的密码学协议。除了支付之外，对于日常业务中的大多数场景，如投票、选举、竞拍等，半同态加密算法一般都可以满足对应的隐私保护需求。

对于一个全同态加密算法，其密文形式在理论上对任意运算方式都满足同态性。对于数据密文计算相关同态加密算法设计，这一要求通常体现为密文对应的代数结构对加法和乘法同时满足同态性。

对于任意的隐私数据x，y，全同态加密算法提供了一对加密算法E和解密算法D，满足如下关系：

$$D(\mathrm{E}(x)) + \mathrm{D}(\mathrm{E}(y)) = \mathrm{D}(\mathrm{E}(x) \oplus \mathrm{E}(y))$$

$$D(\mathrm{E}(x)) * \mathrm{D}(\mathrm{E}(y)) = \mathrm{D}(\mathrm{E}(x) \circledast \mathrm{E}(y))$$

相比半同态加密算法，全同态加密算法功能更强大、设计更复杂，整体性能远不及半同态加密算法。例如可能面临密文数据膨胀困扰。相关研究报告显示，在一次使用全同态加密开源库为敏感医疗数据构建密文线性回顾模型的尝试中，需要将隐私数据进行编码转换，映射到密文的向量空间中。

此过程，1M的明文数据编码后可能膨胀至约10G密文数据；同时，针对值域范围为512位的明文数据，单次密文乘法运算，在普通个人计算机实测耗时约5秒左右，通常一个需要全同态计算的场景涉及的密文乘法次数很多，总体耗时较高。

由此可见，全同态加密算法的愿景虽美，但目前还处于理论探索层面，离工程实用化、支持高频次和大数据量的业务需求尚有一定距离。

单密钥vs多密钥

同态加密根据数据控制方的数量，可分为单密钥同态加密（Single Key Homomorphic Encryption）和多密钥同态加密（Multi-key Homomorphic Encryption）。

早期的同态加密算法都是单密钥算法，主要应用于外包计算（Outsourced Computation）场景。数据控制方对自身的数据进行加密，然后发送到云计算服务平台，在密文的形式下完成一系列运算，最后下载结果密文，本地解密之后获得最后的计算结果。

上一节提到的ElGamal、Paillier等加密算法都是单密钥同态加密，即对于隐私数据只能使用同一对的密钥进行加解密。

单密钥同态加密优点在于构造相对简单、性能高，可用于有一定信任基础或强监管环境下的联合计算场景。

由于涉及到可信初始化和密钥选用的问题，单密钥同态加密在多方参与的协作场景中，会遇到不少挑战，例如：

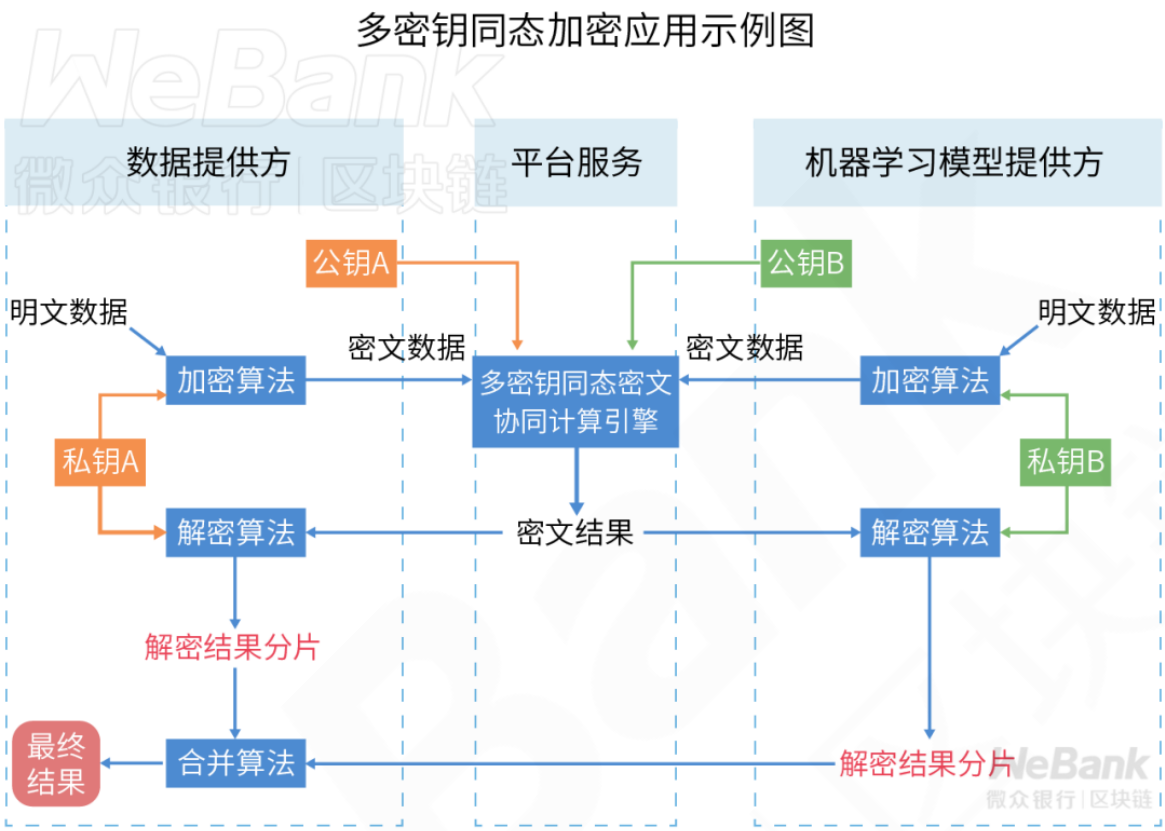
- 如何决定使用哪一方提供的密钥？数据由谁来解密？
- 如何平衡单密钥所代表的单一数据控制权？如何确保数据提供方的敏感数据输入不被解密？如何防范数据控制方恶意提前终止协议？
- 如何让所有参与方都能验证最终结果正确性？

实际业务流程中，隐私数据可以由多方提供，在可信初始化之后使用同一个公钥加密数据，并汇总密文数据进行计算，计算结束之后，需要委托可信方或者使用分布式解密协议，对最终结果进行解密。

相比单密钥同态加密算法，多密钥同态加密较好地解决了信任相关的问题。

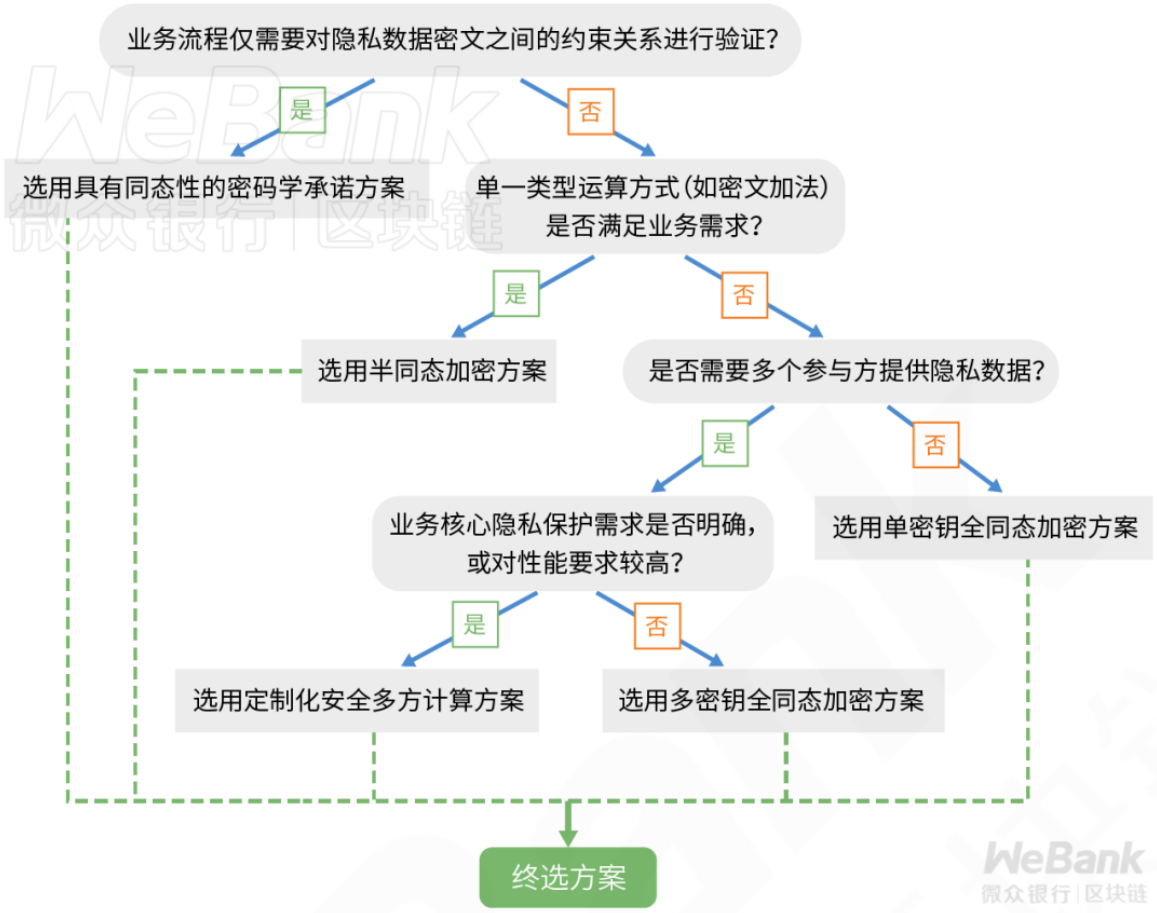
一个多密钥同态加密算法，允许不同参与方使用各自不同的密钥对加密，加密后的密文可以通过各个参与方的公钥进行密文扩展，扩展后的密文对于指定的运算方式依旧满足同态性。解密过程可以通过分布式解密协议，在不泄露各自数据私钥的前提下，对约定的结果密文进行解密。

典型的多密钥同态加密算法可以参考Clear and McGoldrick (CRYPTO 2015)、Mukherjee and Wichs (EUROCRYPT 2016)相关的论文。



目前多密钥同态加密方案，随着参与方个数的增加，系统性能会急剧降低。对于一些需求比较明确的多方协作场景，相较于多密钥同态加密方案，定制构造的安全多方计算协议或许更有效。

总体而言，密文同态性可以为业务场景中，常见的隐私数据的计算和验证需求，提供有效解决方案，根据具体的业务需求，基本技术选型可以参考下图：



正是：隐私数据密文亦无妨，计算验证同态两相宜！

具有同态性的密码学原语提供了一系列直观、便捷的密钥学协议构造利器，在保障隐私数据机密性的同时，允许多个协作方对隐私数据的密文形式进行直接运算和验证操作，以此适配多样化的隐私保护需求。

除计算和验证需求外，多方授权也是常见的业务需求之一，如对多方共有的业务数据进行授权使用，此时需要用到门限密码学相关技术，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，围绕**即时可用场景式隐私保护高效解决方案WeDPR**的核心技术点，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

第6论｜密码学技术如何选型？终探量子计算通信的安全模型

第7论｜密码密钥傻傻分不清？认识密码学中的最高机密

第8论｜密钥繁多难记难管理？认识高效密钥管理体系

上下滑动查看更多

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