密码学技术如何选型？初探理论能力边界的安全模型

原创 李昊轩 微众银行区块链 3月26日

来自专辑

WeDPR隐私保护周三见

系统变更后，为何隐私数据频频泄露？密码学算法自由组合后构成的新协议是否依旧安全？当下部署的隐私保护系统，10年后是否依旧有效？密码学协议是否越安全越符合实际业务需求？

这里，我们将继续密码学技术选型的分享，从单个密码学算法扩展到由多个密码学算法构成的密码学协议的安全性，梳理相关的能力边界，以及选用不同协议对实际业务中隐私保护效果的影响。

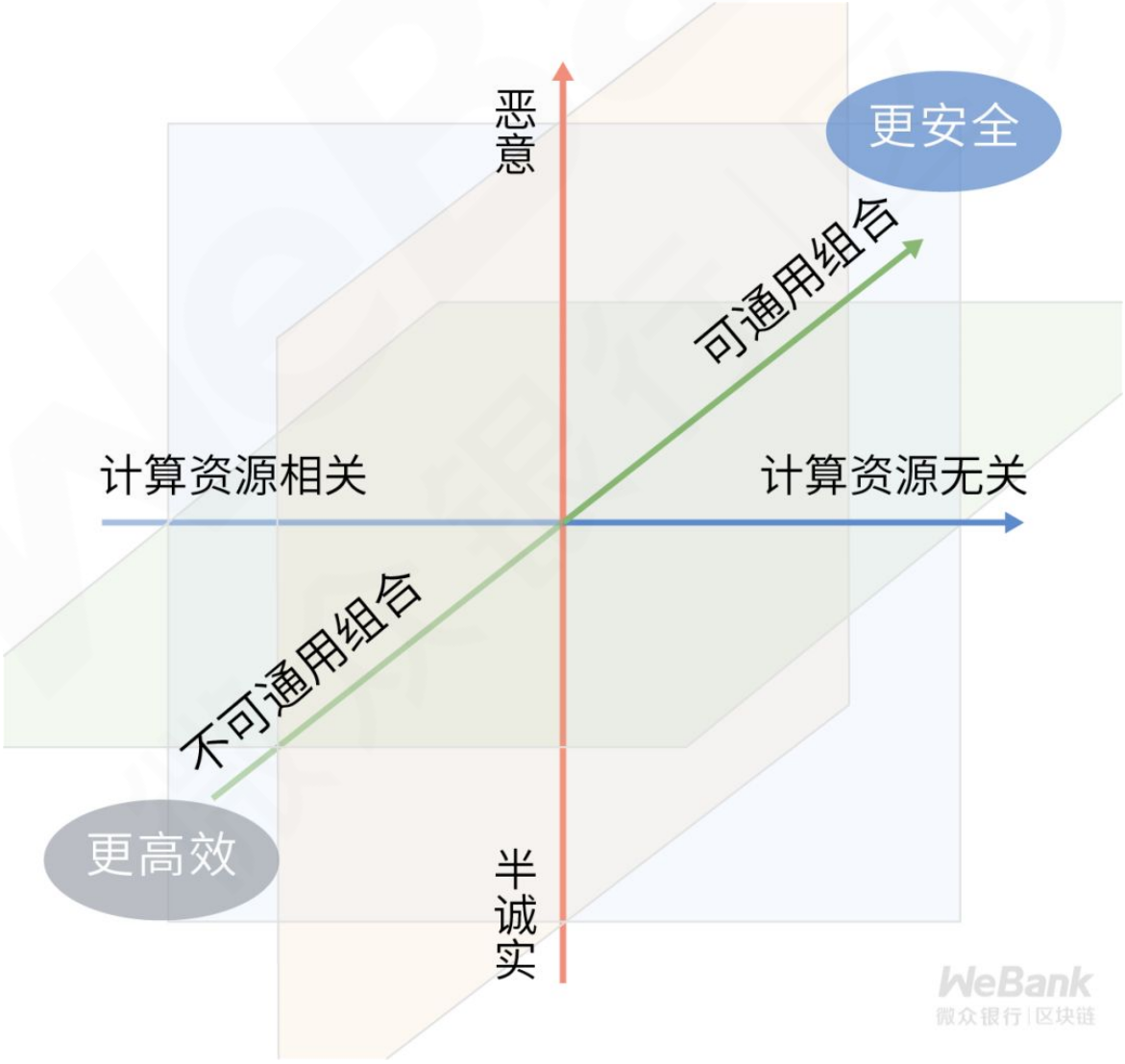
正如上一论（←点击查看）所提到的，学术界在构造密码学算法时，引入了一系列安全假设，只有当这些安全假设都成真时，对应的密码学算法才安全。类似地，由多个密码学算法构成的密码学协议，由于加入更多的交互方，需要引入更多的安全假设。

对于一个密码学协议，其所需的所有安全假设，及对应假设下的安全性要求的集合，称之为**安全模型**。

了解安全模型中引入的不同安全假设，有利于企业在进行密码学相关的隐私保护技术选型时，客观评估备选技术方案的有效性。

安全模型中不少关键安全假设是相互独立的，可以根据这些关键安全假设将安全模型进行分类，以此简化评估流程。最常见的三种分类方式如下：

- 半诚实 VS 恶意
- 可通用组合 VS 不可通用组合
- 计算资源无关 VS 计算资源相关



以上三种分类方式相互独立，相当于三维坐标轴中的三个维度。以下将以小华的故事为载体，一一阐明对应分类下，密码学协议的理论能力边界。

毕业季来临，主人公小华离开自己的家乡，来到了心仪城市就职。小华、房东美丽、房产中介之间的故事就此拉开帷幕……

半诚实 VS 恶意

小华初来驾到，眼下最迫在眉睫的事，就是找到可以让自己过夜的地方。小华通过中介获取房源列表，最终选定了一套比较满意的房源，并在中介的撮合下，与房东美丽取得了联系。

在这个过程中，中介作为参与第三方，受法律规范和社会道德所约束，一般情况下并不会对房屋合同的租金、房屋信息等内容进行篡改。但是，房屋合同中包含大量个人隐私数据，中介可轻易获取租赁双方相关行为信息，存在显著的隐私数据泄露风险。

为此，小华根据自身专业知识设计实现了一套密码学租房协议，只要中介能够正确履行该协议，交互过程中产生的隐私数据就不会泄露了。

以上租房交互协议，依赖中介能够正确执行租房交互协议的安全假设。基于这类安全假设的安全模型，在密码学中被称为半诚实模型，又称诚实且好奇模型，或被动攻击者模型。

半诚实模型

参与者一定会正确执行密码学协议，但会试图从密码学协议执行过程产生的中间结果中提取隐私数据。

当前大部分密码学协议都选用了半诚实模型，这类安全模型在效率、协议设计难度上都有显著优势。同时，大部分业务部署时，参与方都会被现实世界诸如法律法规等因素约束，不会进行极端恶意攻击。

小华期望通过上述半诚实模型下的密码学租房协议，与美丽完成房源匹配和签约流程。该技术方案将对小华和美丽的身份信息、租房明细等提供有效保护。

然而，意外还是发生了。中介并没有如约履行该协议，并在顶级黑客的协助下，篡改了部分协议流程，小华和美丽的隐私数据，最终还是泄露了。

为了应对以上隐私风险，这里需要引入密码学中更强的安全模型——恶意模型，也称主动攻击者模型。

恶意模型

参与者可以完全不遵守密码学协议，并会采取任何手段对密码学协议进行攻击从而提取隐私信息。

小华吸取了上次的教训，重新基于恶意模型设计了密码学租房协议。尽管中介和他的黑客伙伴使出了十八般武艺，但最终也没能攻破新协议。

小华和美丽的隐私数据终于得到了保护，但背后引入了高昂的代价。

在恶意模型下，构造一个安全的密码学协议，通常需要在每一个可能被攻击的环节引入零知识证明或安全多方交互。相比相同业务场景中半诚实模型下的密码学协议，其计算和通讯的代价以及协议自身的设计难度都会高很多，甚至可能会出现实际不可用的情况，影响最终的用户体验。

现实可用的密码学隐私保护方案有一定的性能要求，这里需要分析具体业务场景中攻击者的“动机”，以此来选择是否可以使用半诚实模型。如果攻击者缺乏进行恶意模型下攻击的

动机，如潜在回报小于预期收益，或者攻击只会对攻击者自身造成利益伤害，业务方案设计可以比较安全地使用半诚实模型。

在现实业务中，受益于法律规范和社会道德的约束，大多数系统面临的潜在攻击源自于半诚实模型下的威胁。

尤其是强监管行业中的业务场景和其他作恶动机低的应用场景，相比恶意模型，在半诚实模型下构建隐私保护技术方案，可以显著提升系统性能和用户体验。

可通用组合 VS 不可通用组合

小华的故事还在继续。美丽考虑到房屋未来有自住的可能，希望在密码学租房协议中提出一些支持租期灵活变动的特性。这需要对现有技术方案进行变更，添加一些新的密码算法模块。

新问题随之而来：变更之后的隐私保护技术方案是否依旧有效？

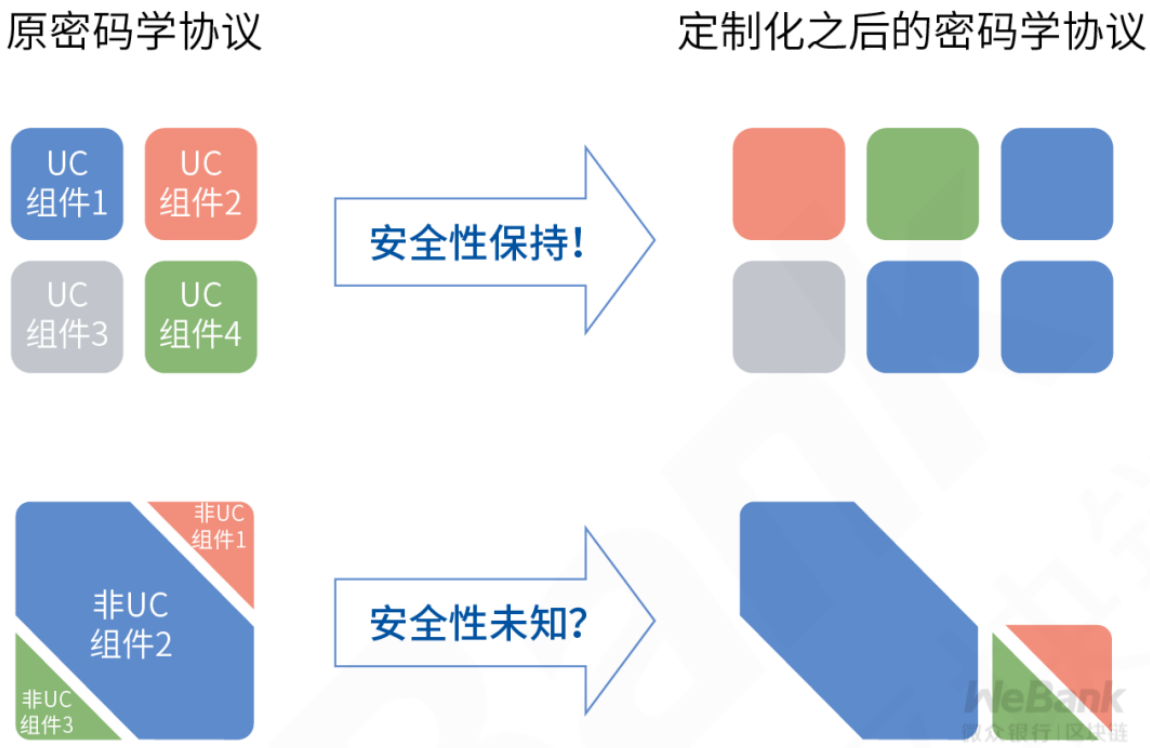
这一问题对应的两类安全模型就是可通用组合模型和不可通用组合模型，通常简称为UC模型和非UC模型。UC源自英文Universal Composable，对应的定义如下：

可通用组合模型（UC模型）

该模型下的密码学协议，其使用的密码学算法组件都满足UC的安全性要求。通过组合定理，可以将这些UC安全的密码学算法组件任意自由组合，从而构造更加复杂但依旧安全的协议。

不可通用组合模型（非UC模型）

该模型下的密码学协议，对其进行修改、重组、拆分，之后获得的新协议不一定具备原协议的安全性。



在上述小华的故事中，如果原密码学租房协议不满足UC模型的安全性要求，根据美丽的诉求更改协议之后，新协议很可能就不再安全，稍有不慎就可能泄露小华和美丽的隐私数据。

由于需要非常严谨的证明才能满足UC模型的安全性要求，UC模型下可用的密码学算法组件比较有限，目前大部分隐私保护技术方案都是非UC模型下的。

对于企业来讲，这里的警示是，务必要核实定制化过程是否破坏了隐私保护技术方案的有效性。

在业务落地过程中，难免需要对现有方案进行深度定制，而定制密码学协议的过程中，需要特别留意变更后的密码学协议是否依旧能够提供业务预期的隐私保护效果。

0.3

计算资源无关 VS 计算资源相关

再次回到小华的故事。

> 小华通过密码学租房协议，与美丽签订了一份长达5年的租房合同。在这5年内，计算机技术研究有了不少新突破，可用的计算能力上限提升了1万亿倍。之前饱受挫折的黑客卷土重来，那么，小华的密码学租房协议是否岌岌可危?

这就引入了第三类安全模型的分类方式，即是否受到计算能力发展的影响。

计算资源无关模型

即使攻击者拥有无限的计算资源，密码学协议仍然是安全的。

计算资源相关模型

密码学协议已知的最优破译方法，其所需的计算资源远远大于攻击者目前拥有的计算资源。

计算资源无关模型，通常也被称为无条件安全模型或信息论安全模型，是信息论中最严格的安全模型。即便是当下热议的可能突然出现的超高性能量子计算机，也无法破译该安全模型下的隐私保护方案。

计算资源无关模型下的可用方案极少，唯一常用的方案是基于一次一密的密码学协议，并需要额外引入关于安全地生成和传输无限长度密钥的安全假设。

绝大部分密码学协议属于后一类，即计算资源相关模型。一般通过数学规约的证明方法，证明密码学协议可以被规约到某个计算困难问题，由此保证攻击者在有限时间内难以完成计算，此时也被称为可证明安全模型。

从以上分类可以看到，小华的密码学租房协议的安全性，很大概率会受到计算能力发展的影响。

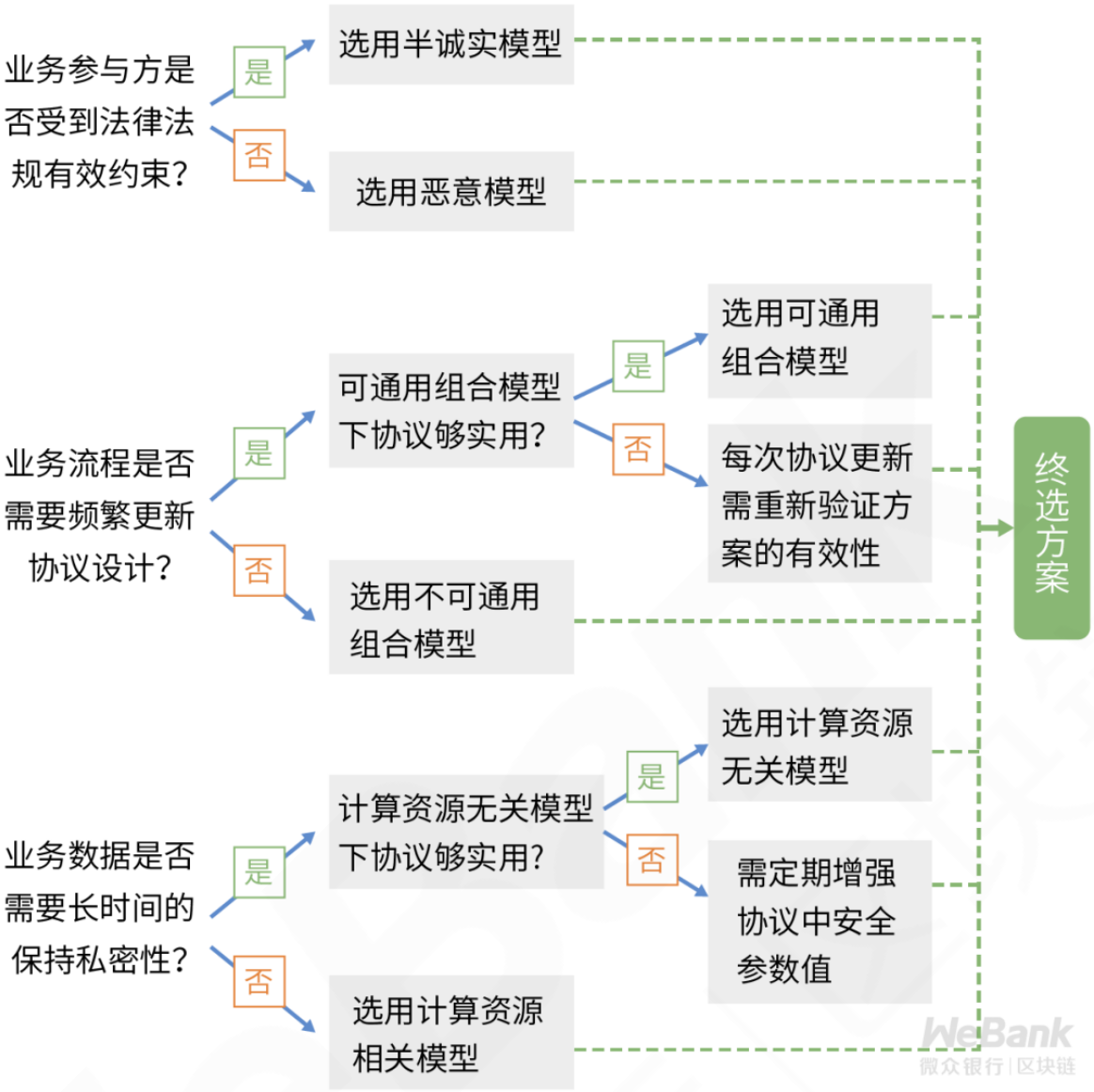
对于企业而言，评估隐私保护方案中密码协议的有效性，一定要结合隐私数据的敏感性和时效性，举例分析如下：

- 某医疗制造商需要对采购方的采购金额、身份、明细等数据进行隐私保护操作，保护的时效性可能需要5年甚至更久。因此，需要选择的技术方案需要提供较长时间的安全，才能满足计算资源相关模型的安全性要求。

- 一些业务仅仅需要在几个小时内保证数据的隐私性。这类场景下，可以选择系统效率更高，但所需破译时间相对较短的方案，也能满足计算资源相关模型的安全性要求。

平衡使用密码学协议构建隐私保护技术方案对业务商业流程的影响，实现系统效率最大化和用户体验的最优化，并不是选用的密码学协议安全性越强越好。

一般情况下，建议在满足业务需求的安全模型下，构建效率最优的密码学协议，够用就好。



正是：密码方案选型无头绪，安全模型定义知根底！

隐私保护业务落地，安全模型选型是影响隐私保护效果的重要因素之一。密码学协议安全模型多种多样，安全级别越高的安全模型往往效率越低。事实上，现实社会的法律规范和社会道德约束着很多业务场景，有利于简化密码学协议的设计。

企业需要对具体场景具体分析，选用最合适的安全模型，在此基础上定制最适合自身业务场景的隐私保护技术方案，往往比直接套用通用方案效果更佳。

除了本文分析的理论能力相关的安全模型之外，实际开发部署技术方案时，工程层面的疏漏也会不幸地导致隐私数据泄露，具体分析，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

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