密码学技术如何选型？再探工程能力边界的安全模型

原创 李昊轩 微众银行区块链 4月1日

来自专辑

WeDPR隐私保护周三见

牢不可破的密码学算法也怕物理攻击？物理信号泄露为何会威胁到隐私保护的效果？ 隐私保护方案对部署环境有何讲究？不可信执行环境下如何设计隐私保护方案？

这里，我们将继续安全模型的分析，由隐私保护技术方案中理论层面的能力边界，扩展到实际开发部署时工程层面的能力边界，梳理工程实现中相关安全假设，以及适用的业务场景。

在上一论中，我们介绍了多种不同的安全模型，来衡量基于密码学隐私保护技术方案的理论强度。然而，一个隐私保护技术方案如果只考虑理论层面的安全，而忽视工程层面的安全，其有效性是值得质疑的。

早在1985年，Wim van Eck在论文中提出，攻击者可以通过软件运行时产生的电磁辐射信号，结合统计学分析方法，破译出电子设备正在处理的机密信息内容。这就是一种典型的侧信道攻击，是密码学工程领域不能忽视的风险。

与密码学理论领域的安全模型类似，对于密码学工程领域的安全风险，我们也可以根据其安全假设来定义对应的安全模型。最常见的三类安全模型如下：

- 黑盒安全模型
- 灰盒安全模型
- 白盒安全模型

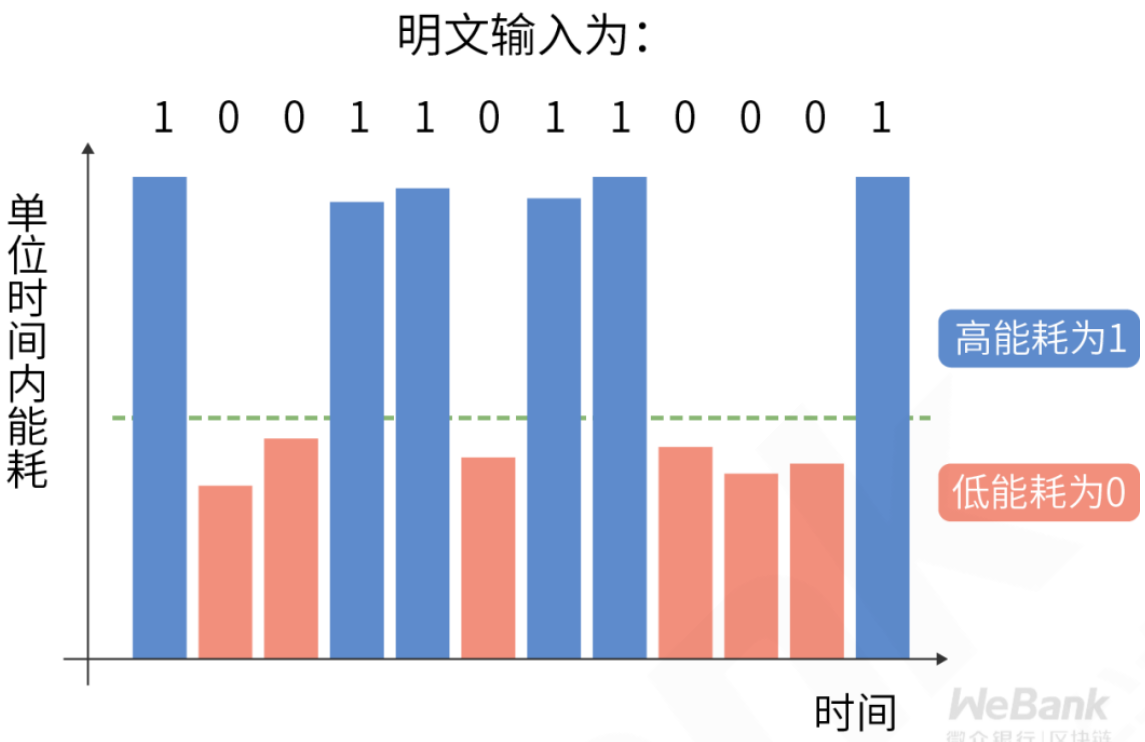
以上三类安全模型中，密码学系统对部署环境的信任要求逐步降低。本论，我们将继续叙说小华的故事，以小华向好友美丽发送私密信息时的加密过程为例，一一阐述这三类安全模型对于企业隐私保护技术选型的影响和启示。

黑盒安全模型

科班出身的小华，对于自己的技术能力相当自信，打算以加密信息的方式，给他的好友美丽一个惊喜……

小华选用了业界标准AES加密方案，将他的私密信息，用特殊的方式传达给美丽。小华使用了公用机房中的电脑，开发并运行了对应的技术方案，产生了密文信息。

不巧的是，公用机房中的电脑被攻击者植入了木马，木马通过读取代码执行时的电量消耗和其他中间状态信息，破译了小华私密信息的明文。



实际上，除了基于密码学技术构建的软件技术方案，就连基于可信硬件模块构建的硬件技术方案，也会不同程度受到以上这类隐私风险的影响。但是，我们依旧认为这些方案在常见业务环境中是安全可用的，究竟是何缘故?

这就引入了黑盒安全模型的定义，假定技术方案的执行过程对于外界是一个完全封闭的黑盒。

如果我们把整体的隐私技术保护方案抽象成关于隐私数据x的一个函数y = f(x)，对于攻击者而言，只能获得y，无法获得f(x)在运算过程中产生的任何中间状态信息。

中间状态信息包括直接敏感信息和间接敏感信息：

- 直接敏感信息：计算过程中的内部变量值、代码执行轨迹等
- 间接敏感信息：执行时间、设备能耗、内存用量、电磁辐射等

绝大多数密码学算法实现，如AES加密算法的标准实现等，都是基于黑盒安全模型的。

这意味着，即便对应的密码学算法和协议设计达到了理论能力的上限，信息论安全在黑盒安全模型要求的假设被打破的前提下，依旧可能泄露隐私数据。

反过来讲，对于受控的业务环境，可以保证没有攻击者能够进入机房，或者难以通过其他方式远程获得这些中间状态信息，而且对应软硬件模块的配置和使用都正确，那么对应的技术方案还是安全的。

考虑到隐私和效率的取舍，黑盒安全模型下的技术方案，工程实现相对复杂度低，能够提供高效的系统实现，可用于中间状态信息泄露风险低、可控部署环境中的业务场景。

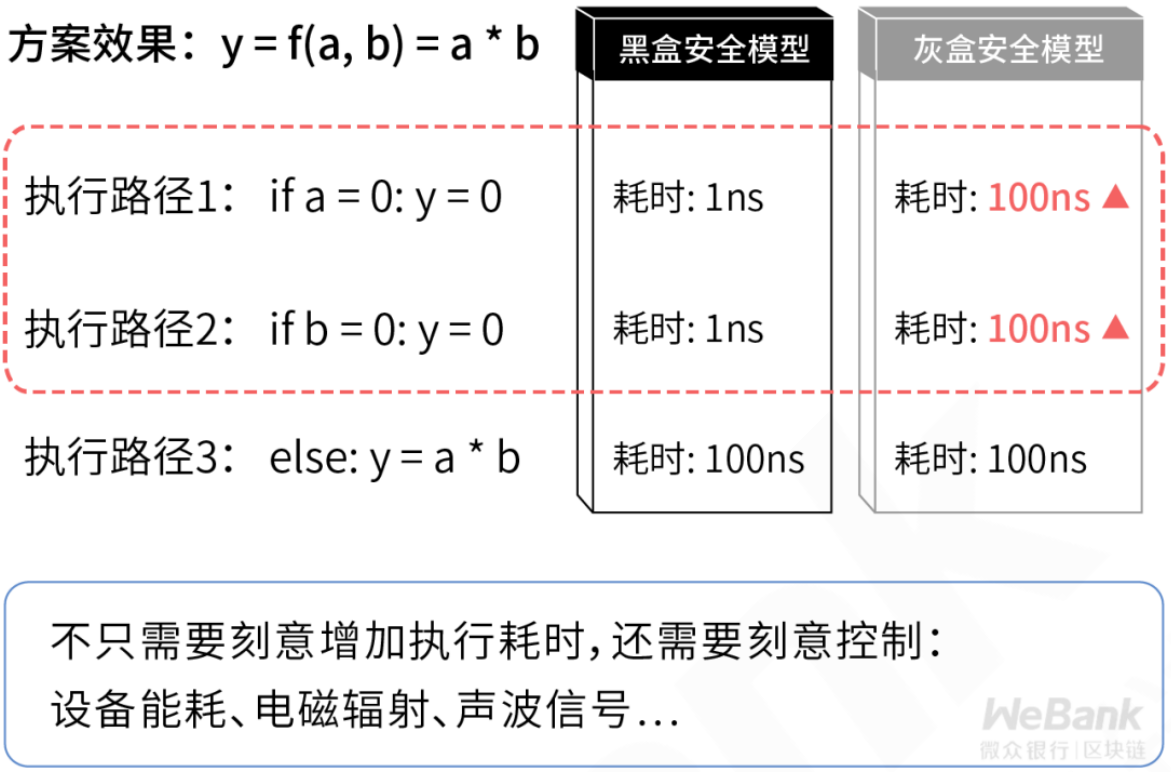
灰盒安全模型

小华吸取了上次的教训，优化了加密算法的实现，屏蔽了执行时间、设备能耗等常用中间状态信息泄露。新的方案似乎生效了，攻击者之前部署的木马无法获得有效信息来破译小华的私密信息。

小华的优化一定程度上降低了隐私保护技术方案对于部署环境的信任要求，相比之前的黑盒安全模型，这里的安全模型为灰盒安全模型，允许一定程度的中间状态信息泄露。

灰盒安全模型，要求技术方案能够防范由于常用中间状态信息而导致的隐私信息泄露。常用中间状态信息，一般指技术方案执行过程中，容易从外部观察到的各种物理信号，如执行时间、设备能耗、电磁辐射、声波信号等。这一类的攻击通常被称为侧信道攻击、旁路攻击，或统称为灰盒攻击。

为了应对这些灰盒攻击，需要在原先黑盒安全工程实现的基础上改写算法，使得在不同输入下，所需防范的物理信号表现相同。以最常见的执行时间分析攻击为例，灰盒安全模型下，对于所有的输入，技术方案的执行时间总是保持均等，以此避免由于执行时间存在差异，而泄露关于隐私数据的信息。



然而，这一类灰盒安全技术方案在系统效率上的副作用也很明显。即便某些执行路径可以更高效地执行，也需要特意降低其效率，使之与业务逻辑中效率最差的一条执行路径相匹配，以此确保执行过程使用的时间、消耗的能量等外部可观测物理信号，在任意输入下都不表现出显著差异。

由此可见，灰盒安全技术方案的执行效率总是由业务逻辑中效率最差的一条执行路径来决定，这对系统效率的优化带来了一定的挑战。

相比黑盒安全模型，灰盒安全模型对于部署环境的信任要求更接近现实情况，一定程度上考虑了内部人员风险等原本只能通过治理手段才能防范的隐私风险，具备更实用的抗攻击能力。

灰盒安全模型下，技术方案的应用主要用于防范内部人员风险，或者在不完全可信的外包环境中部署运行业务。

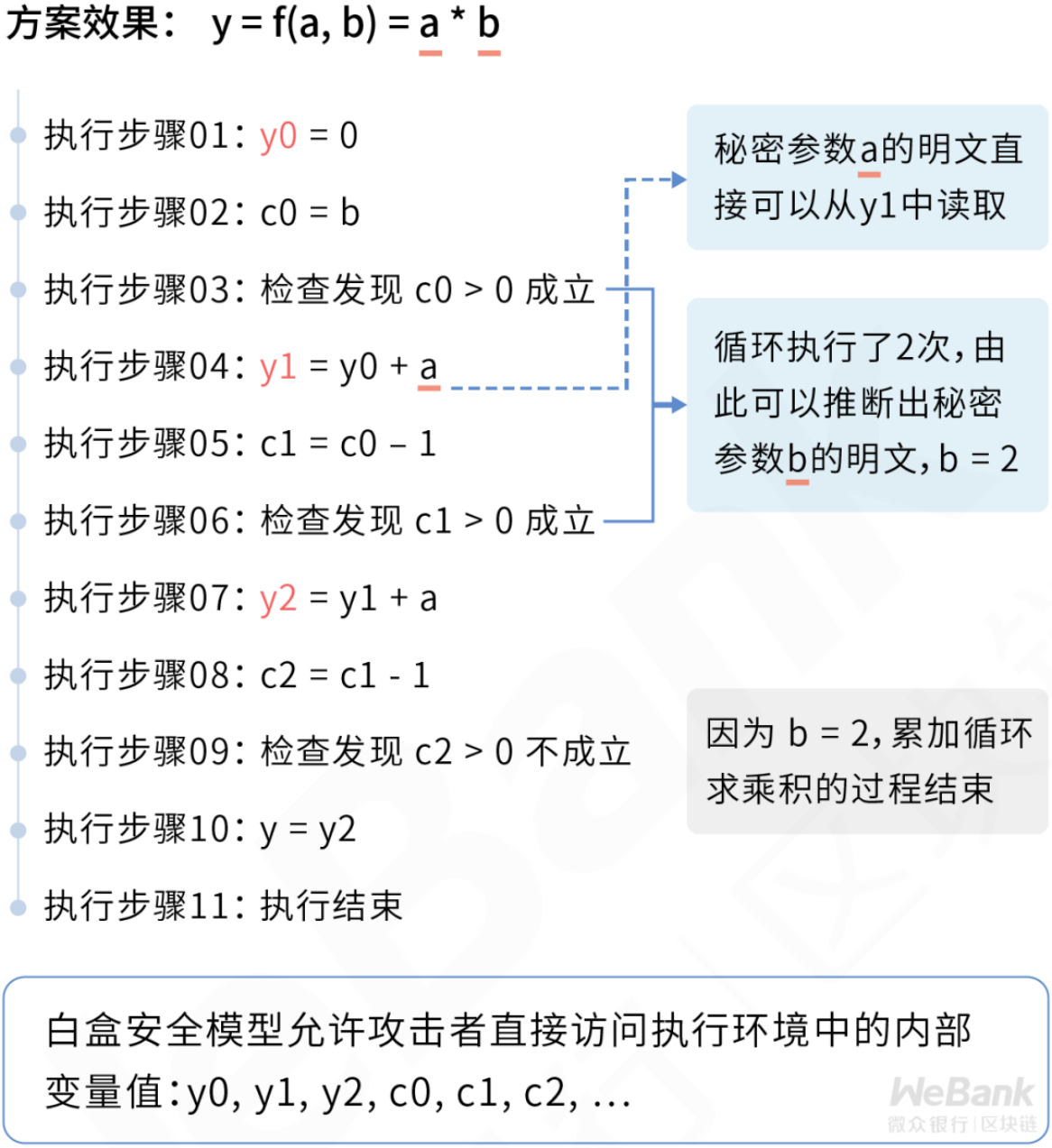
0.3

白盒安全模型

好景不长，攻击者发现之前部署的木马失效之后，升级了木马程序，小华的灰盒安全方案并不完美，攻击者获得了技术方案执行过程中的内部变量值，小华的私密信息再次遭到破译。

灰盒安全模型虽然对中间状态信息做了一定的保护，但无法保证所有的中间状态信息都能得到有效保护。如果能够实现这一点，就达到了工程层面中最强的白盒安全。

回到定义黑盒安全模型的公式，隐私技术保护方案可以抽象为关于隐私数据x的一个函数y = f(x)。在白盒安全模型下，除了x之外，攻击者可以获得y和f(x)在运算过程中产生的任何中间状态信息。

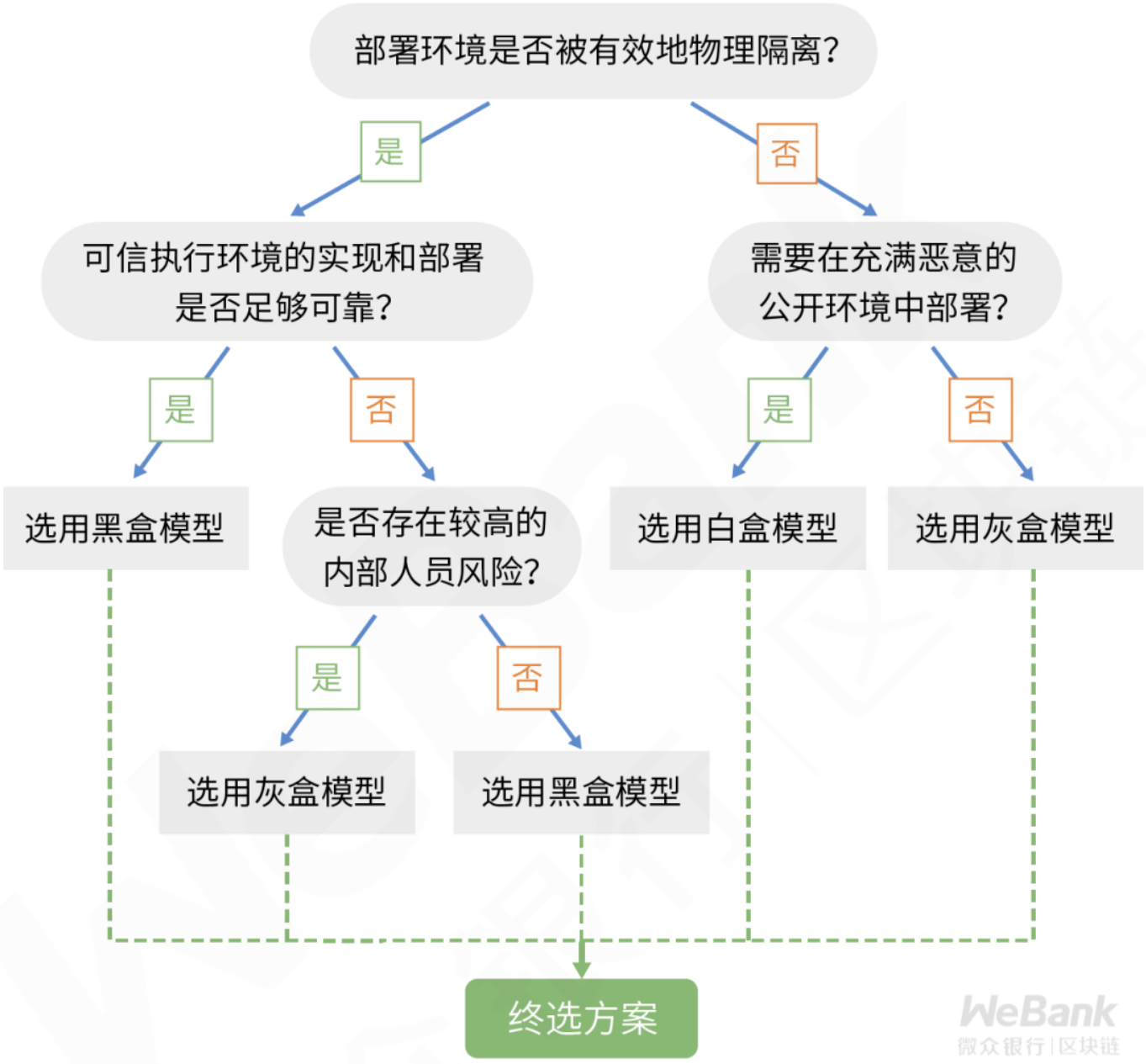


白盒安全模型假定执行环境完全对攻击者透明，听起来效果很玄幻。但密钥如何保护？明文输入不是直接就被看到了吗？面对如此强大的攻击者，如何才能保护隐私数据的安全呢？

效果确实很玄幻，目前现有研究对白盒安全模型的定义做了一定的弱化，通常会把保护目标限定为即便攻击者控制了整个执行环境，也无法轻易通过内存读取等方式提取出密钥。

为了实现白盒安全，需要在灰盒安全的基础上进一步打乱混淆密钥的存储方式并改写算法，让正确的密钥能够在执行过程中被间接使用。这一工程安全要求进一步提升工程实现的复杂度，例如，AES加密算法的白盒安全实现要比黑盒安全实现慢10倍以上。

尽管白盒安全模型下的大部分技术方案目前尚不成熟，在方案可用的前提下，对于需要在不可控的公开环境中部署的业务，如公共物联网应用，非常有必要考虑使用白盒安全技术方案，用以保护终端设备中的密钥、控制隐私数据的泄露风险。



正是：密码巧妙理论无破绽，工程精细实现需谨慎！

工程安全和理论安全是相互独立的两个维度，理论安全并不等于工程安全。再强的理论安全方案设计，也会因为不当的工程实现而导致前功尽弃。

了解密码学工程领域的安全风险，对于实际应用落地和安全运行至关重要。企业在对基于密码学技术的隐私保护技术方案选型时，需要理论联系工程，根据自身的业务场景和部署

环境的特征，选择合适的安全模型，确保隐私保护技术方案的最终有效性。

在这两论中，我们对密码学技术选型中的理论能力边界和工程能力边界进行了分析。除了算法理论和工程实现中的诸多安全假设，新兴的量子计算和量子通信也对隐私保护技术方案的有效性带来了挑战，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

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

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