链滴

比原链研究院 | 一种弱同步网络假设下的门限签名系统

作者：bytom

原文链接：https://ld246.com/article/1570843876984

来源网站：链滴

许可协议：署名-相同方式共享 4.0 国际 (CC BY-SA 4.0)

近几年门限密码学在区块链系统里开始逐渐被应用，分为门限加密和门限签名，一般见于随机预言机防审查、减少通信复杂度（HotStuff）、共识网络中防拜占庭（HoneyBadgerBFT 中用于 BA 环节的ommon coin）以及作为分布式伪随机数生成器（coin tossing）的重要原语，其优越的资产协同防特性也慢慢被新兴数字资产托管机制所重视，今天我们主要讨论公钥密码学（PKC）里的门限签名机。一种理想的门限签名系统是可以在异步的网络环境里做到容错容灾不可伪造（non-forgeability）并且拥有极度可靠安全的消息传输通道，签名份额的生成和验证是完全非交互式的，在初始密钥阶段备可以防止拜占庭行为的异步分布式密钥生成（DKG）机制。

与基础签名机制类似，门限签名机制（Threshold Signature Schemes）也分为两部分：

门限密钥生成（Thresh-Key-Gen）：基于安全参数构造一种分布式密钥生成协议 DKG，协议运行输一个共同的公钥 pk 和分属不同参与方各自所有的私钥份额 ski，聚集起满足阈值数量的私钥份额可以建出真正的私钥 sk。

门限签名（Thresh-Sig）：基于分布式通信网络，各参与方通过自己的私钥份额 ski 完成对消息 m 分布式协作签署并输出最终的可验证签名 Sig(sk, m)，这个签名跟单独用 sk 私钥签出的一模一样，以用所基于的基础签名机制里的验证函数进行本地验证，无需走通信交互验证

但是大多数情况下会通过使用一个可信的中心节点（dealer）来实现私钥份额的生成和分发。沙米尔密分享（Shamir Secret Sharing）是最简单的依赖中心 dealer 节点的门限密钥生成方法，基本原理拉格朗日插值，在 (t, n) 门限构造中，dealer 会选择一个 (t-1) 次方的随机多项式 f，令 f(0)=s，s 即要分享的秘密值，然后向每个节点分发该多项式曲线上的点 si=f(i) 作为各自的秘密份额值，简单来讲三个点确定一个二次方程曲线（Lagrange interpolation formula）。为了解决中心作恶问题，人们不断探索了基于承诺（commitment）的可验证秘密分享（VSS、PVSS），以及应用于异步网络的 VS（Cobalt BFT 在区块链系统里也尝试了结合 PoW 准入机制的 AVSS）。有许多优秀成熟的 commiment scheme 可以借鉴应用，简单来讲承诺（commitment）算法 [C(M), D(M)]=Com(pk, M, r) 中 pk 是与承诺机制有关的公钥，M 是要承诺的原始值，r 是一个随机骰子，算法输出的 C 便是 commiment，D 则是需要秘密保管的 decommitment 值，在正式公开 M 之前先公开 M 的承诺 C，即先自己要公布的消息做个上帝担保，约束自己无法更换 M，而对于 M 的受众或者接收者，它们可以通之前公布的承诺和验证算法进行验证唯一性。这里我们主要关注非交互式的 VSS 实现。

此外，在过往的研究里，签名（Sig）的生成和验证大多是交互式的，并且依赖一个同步通信网络和

播通道（broadcast channel），节点们在某种设定下接收到特定消息后便同时启动签名协议，并严遵循超时机制。而在互联网环境和区块链网络里，对网络假设的限定是有限的，所以门限系统要成功作除了需要构造真正的 DKG 协议和非交互式签名机制外，还需要具备商用级的网络系统以及被验证的成熟代码实现。这里我们（Bytom）尝试提出并构建一种弱同步网络假设下的门限签名分布式系统主要对网络模型、DKG 构建、签名机制进行一些创新结合和应用，探索在实际网络环境里最小可实的门限签名系统原型。

门限系统是一种（t, k, n）型 fault-tolerance 系统，t 代表网络最大容错，k 代表最小门限值，n 是点数，一般设定 k>=t+1，但这种对网络分区（network partition）是无能为力的，所以在一个异步占庭网络里我们依然选用经典设定 k=n-t & t<n/3 去达成系统里的一个大多数共识。

门限网络或者通信模型是实现可实用门限系统需要认真考量的一个关键点。像 HoneyBadgerBFT 所建的接近异步通信网络在现实案例中是少见的，一般会增加消息复杂度和通信轮次，异步网络模型主依赖所接收到的消息类型和数量进行判断，因为时间因子（time-based）并不能区分谁是慢节点谁恶意节点。但在这里我们更倾向采用高效的弱同步网络假设，即消息延迟和时钟偏移有上限（实际可受）但未知，延迟的渐进是合理的，保障 liveness（safety 可以采用妥协的方法处理）；能够对 cras 、network failure、byzantine 等不同情况尽量做到分开处理，比如设置规定时间内可容忍的 crash 值，对于诚实节点发生 crash 后能够从一个规定的状态恢复等；并且假设网络故障总能被修复、遭受 DoS 攻击总会停止；最后在构建通信通路上可以借助 PKI 和外部 CA 构建 TLS 链接，以及借助经典的 RBC 协议（reliable broadcast channel）。

DKG 是门限签名最为核心的环节也是第一阶段，负责完成门限密钥的生成和分发。VSS 是 DKG 的重组成部分。上面提到 VSS 的基本原理是承诺机制，一般基于 Pedersen commitment，构造形如 C=G+nH 的承诺（这里我们省去了一些对椭圆曲线群运算特征定义和假设，可以简单理解为椭圆曲线计），其中 m 来自密钥构造多项式 f(x) 系数，而 n 来自 dealer 另外构造的一个随机多项式 h(x) 的系，承诺集合 {Ci, 0<i<t} 是一种公开可获取的系数“证据”，用于证明 dealer 只承认一个合法的密钥项式。各个参与方在获得 dealer 分发给自己的密钥份额 f(i) 和秘密值份额 h(i) 后，计算 f(i)G+h(i)H 如果与对应的承诺值（多项式计算）相等，则认为合法，如果不一致，则认为 dealer 出现作恶行为开始向网络提交自己的抗议 complaint，其他人可以进行验证，如果发现事实如此，则立即停止协议如果其他人验证后发现该 complaint 不合法，则发起 complaint 的节点会被标记不可信。VSS 过程单来讲包括中心初始化密钥分发、构建承诺和重建密钥三部分内容，整个网络交互存在两轮（synchro ous）全网广播（all-to-all）达成一致，最终将密钥份额和承诺传递给每个参与节点，这里我们会定三种消息类型用于标记多轮消息序列并携带足够的信息用于计算门限密钥。

真正的 DKG 是需要去掉 VSS 里的那个中心，在分布式协作下生成秘密，避免单点泄漏风险，其原理很简单，相当于 n 个节点同时各自选择秘密值并运行自己的 VSS，每个节点收集来自其他节点的秘密额完成组装，组装后的结果便是真正私钥的份额，而各个合法节点各自分发的秘密值聚合起来便是最的构造私钥，最后在进行承诺验证。这似乎很像一个 Multi-valued Validated Byzantine Agreement (MVBA) protocol （一种被广泛研究的可以对多种提案高效率达成共识的一致性协议算法，存在多个种，比如异步公共子集 Common Subset）。

不过我们尽量避免这种复杂的实现，一般通过选举出 Leader 节点，统一协调处理这些 VSS 的完成情和最终共识，定义序列，当大多数节点（n-t）完成各自的 VSS 阶段并被其他所有诚实节点所确认后，eader 将这些已完成的 VSS 信息进行收集并重组提案，再经过两轮全网广播后，每个节点便会确定各自最终的秘密份额，因此保障 liveness 对于我们的系统是十分关键的。如果 DKG 协议里任何一方现恶意行为，协议都会立即停止，即 DKG 需要确保所有参与方的诚实行为。至此，一把公共的门限钥和分属不同参与方的门限私钥份额便构造完毕。

签名阶段简单来讲是基于上面得到的密钥份额各自完成签署自己的签名份额，最后再完成统一组装，到最终门限签名。Thresh-Sig 阶段的具体实现与所基于的数字签名算法有很大关系，例如 Schnorr 法在计算签名 s 值时所依赖的秘密值 k 在常数项，s=k-z(H(K||M))，所以可以简单的将秘密值份额相。而 ECDSA 中秘密值 k 是非线性的，即 s=(H(M)+zr)/k（其中 r 也是由 k 经过指数运算得来），存两个秘密值（k 和 z）的乘运算，所以各个节点不能仅通过拥有 k 秘密值份额来完成最终签名值的组，需要对公式进行变形，重新定义组合秘密值 kz，并分布式完成 kz 的秘密份额计算以及分发，甚至要借助安全多方计算（在不泄漏各自 k 和 z 份额的前提下，完成 kz 的结果计算并输出 kz 的秘密份

给相应参与方）、同态加密机制以及零知识证明（range proof），因此多方的 ECDSA 门限签名在现和效率上会比较复杂，现阶段以可实用的 2-2 方案研究居多。

不论是采用 ECDSA 还是 Schnorr 算法，最核心的问题依然是基于 DKG 和多方计算的原理去生成和发签名算法中需要的秘密值，每个参与方基于各自的密钥份额和秘密值份额完成自己的签名过程，最通过整体的交互组装获得最终的合法签名。同样的，如果无法达到足够门限阈值数量的合法签名方，名协议也会立即停止。根据不同的应用场景需求，我们需要认真研究用于实现门限签名机制的底层签算法，比如 ECDSA、EdDSA、Schnorr、BLS 等，不同的签名算法对应的门限机制实现复杂度和效是不同的。

此外，一个完整的门限系统可能会有成员变更的需求，原有的密钥份额随之需要新一轮变更，最直观做法是引入周期的概念，通过同步网络和共识协议发起新一轮密钥生成，产生新的主公钥和私钥份额用超时机制防止阻塞。成员变更和 DKG 是一种比较精细（或脆弱）的系统，任何一个成员 fail 或者 fault 都会引发状况外。在实现上我们用状态机复制原理构建门限（DKG）节点，基于消息输入更换自状态（例如 node_remove，leader_change，group_update）。

门限密码学随着结合应用场景的需求研究增多，不断完善自身成熟度，尤其是随着高度可靠的代码实增多，随着复杂网络环境里的系统架构成熟，有希望在价值网络里扮演“门神”的重大作用，同时会进对零知识证明、同态加密技术的进一步场景化应用，是当下区块链新技术领域为数不多值得深入研和实战的研究方向。现代密码学与价值网络相辅相成，前者给予后者“上帝保障”，后者给予前者“大战场”。

比原链研究院 刘秋杉