密码学报 ISSN 2095-7025 CN 10-1195/TN
Journal of Cryptologic Research, 2022, 9(5): 872–882

E-mail: jcr@cacrnet.org.cn
http://www.jcr.cacrnet.org.cn
Tel/Fax: +86-10-82789618

Aigis-sig 方案的门限数字签名协议研究*

赵秀凤, 付 雨

信息工程大学 密码工程学院, 郑州 450001
通信作者: 付雨, E-mail: 13663838237@163.com

摘 要: 本文利用全同态加密技术和基于多项式环的 Shamir 门限秘密分享方案, 设计了 Aigis-sig 方案的门限签名协议. Aigis-sig 等基于格的数字签名方案, 利用拒绝采样技术确保签名不泄露私钥信息, 但是拒绝采样也给设计门限签名协议带来困难, 在拒绝采样步骤完成前, 需要对加密的中间值进行运算. 因此, 本文引入全同态加密技术密态计算协议中间值. 此外, 由于 Aigis-sig 方案使用的主要代数结构为多项式环, 为适应协议构造, 本文引入了基于多项式环的 Shamir 门限秘密分享方案, 并证明了秘密分享方案在不同模约化操作下的正确性. 分析结果表明该协议满足正确性和可行性, 在两个参与者都是诚实的情况下, 生成的门限数字签名满足适应性选择消息攻击下的存在不可伪造性.

关键词: Aigis-sig 方案; 同态加密; 门限签名协议
中图分类号: TP309.7 **文献标识码:** A DOI: 10.13868/j.cnki.jcr.000554

中文引用格式: 赵秀凤, 付雨. Aigis-sig 方案的门限数字签名协议研究[J]. 密码学报, 2022, 9(5): 872–882. [DOI: 10.13868/j.cnki.jcr.000554]
英文引用格式: ZHAO X F, FU Y. A new threshold digital signature protocol for Aigis-sig[J]. Journal of Cryptologic Research, 2022, 9(5): 872–882. [DOI: 10.13868/j.cnki.jcr.000554]

A New Threshold Digital Signature Protocol for Aigis-sig

ZHAO Xiu-Feng, FU Yu

College of Cryptography Engineering, Information Engineering University, Zhenzhou 450001, China
Corresponding author: FU Yu, E-mail: 13663838237@163.com

Abstract: Threshold digital signature protocol for Aigis-sig scheme is designed by using the fully homomorphic encryption technology and Shamir secret sharing scheme based on a polynomial ring. Lattice-based digital signature protocol for Aigis-sig scheme uses rejection sampling in their design to ensure that the signature does not reveal any information about the private key, while rejection sampling brings difficulty for designing threshold signature protocol, i.e., the encrypted intermediate value needs to be calculated before rejection sampling. Therefore, a fully homomorphic encryption technique is proposed to compute the intermediate value. Because the main algebraic structure applied in the Aigis-sig is the polynomial ring, to accommodate the construction, the Shamir secret sharing scheme on the polynomial ring is introduced, and the correctness of the secret sharing scheme under different modular reduction operations is proved. The evaluation analysis demonstrates that the proposed protocol is correct and feasible. In the scenario that both parties are honest, the threshold signature is

* 基金项目: 国家自然科学基金 (61902428); 军事类研究生资助课题 (JY2019C226)
Foundation: National Natural Science Foundation of China (61902428); Military Graduate Project (JY2019C226)
收稿日期: 2021-10-20 定稿日期: 2022-03-30

unforgeable against adaptive chosen-message attack.

Key words: Aigis-sig; homomorphic encryption; threshold signing protocol

1 引言

数字签名是公钥密码体系的重要组成部分, 在电子商务、电子政务、加密货币等多个领域都发挥着重要作用. 在标准的数字签名方案中, 签名者使用私钥对消息签名, 验证者使用公钥验证签名的合法性. 近年来, 由于区块链技术的快速发展, 门限签名在该领域得到了深入研究与广泛应用. 其中一个主要原因是, 在移动互联网应用背景下, 部分移动终端的防护能力较差, 签名私钥存储的安全性很难得到有效保证. 在 (t,n)-门限签名协议中, 每个参与者拥有一个签名私钥份额, 签名过程中任何不少于 t 个参与者的集合能够利用各自私钥份额生成签名份额, 然后通过重构签名份额生成完整签名. 签名过程中单个参与者无法恢复完整的签名私钥, 既保证签名的正确性, 又保证签名私钥的安全性, 验证过程可由单个参与者利用验证公钥独立完成. 门限签名协议可以抵御单点腐化带来的安全隐患, 具有更好的鲁棒性.

目前, 国际上基于椭圆曲线数字签名算法 (elliptic curve digital signature algorithm, ECDSA) 已经设计了两方数字签名协议 [1]、门限数字签名协议 [2]. 国内有学者对基于 ECDSA 和国密算法 SM2 的两方协同生成数字签名的方法进行了研究 [3,4]. ECDSA 和 SM2 算法的安全性基于离散对数问题的困难性, 因此均不能抵抗量子计算攻击. 对于格上困难问题, 目前还没有提出有效的量子求解算法, 所以研究如何设计安全高效的基于格的数字签名方案的门限签名协议十分必要.

FSwA (Fiat-Shamir with Aborts) 框架 [5,6] 是构建基于格的数字签名方案最流行的技术之一, 目前被广泛应用于基于格的数字签名方案的设计中. 美国国家标准与技术研究所征集第三轮候选算法 CRYSTALS-Dilithium [7]、国内算法竞赛获奖算法 Aigis-sig [8]、木兰 [9] 等都采用了该框架. 使用 FSwA 框架的数字签名方案, 在签名生成过程中需要进行拒绝采样条件的验证 [6], 以确保签名值不会泄露签名私钥信息. 但是拒绝采样环节也是构造门限签名协议的主要障碍, 在协议交互过程中, 协议中间值需要保密, 即需要密态计算协议中间值, 因此本文拟引入全同态加密技术来解决此问题. Boneh 等人 [10] 基于门限全同态加密技术设计了一类通用的门限签名协议构造方法, 即先通过门限秘密分享体制生成签名私钥份额并分发给各参与者, 采用同态计算签名电路的方法生成签名份额, 再通过重构算法生成签名. 但是 Boneh 等人 [10] 只在理论上给出了门限签名协议的通用化构造方法, 并未对协议中间值的保密及协议重复运行次数等问题进行充分讨论. Damgård 等人 [11] 基于 Dilithium-G [12] 方案, 借助陷门同态承诺方案, 设计了一个两轮的 (n,n)-门限签名协议, 并证明了该协议满足适应性选择消息攻击下的存在不可伪造性. Dilithum-G 方案是 CRYSTALS-Dilithium 方案的变体, 两个方案的主要区别在于拒绝采样的实现方式不同. Dilithum-G 方案中挑战向量服从高斯分布, 其和分布仍服从高斯分布. 在上述门限签名协议中, 生成门限签名一般需要对各参与方生成的挑战向量求和, 使用 Dilihtium-G 方案可以确保生成的挑战向量和仍服从高斯分布, 因而更适用于构造门限签名协议 [11]. 在 CRYSTALS-Dilithium 方案和 Aigis-sig 方案中, 挑战向量服从均匀分布, 因此, 不同于上述方法, 本文将扩展的 Shamir 秘密分享体制用于门限签名协议设计中, 使得挑战向量的线性组合仍服从均匀分布. 此外, 由于 Aigis-sig 方案中使用的主要代数结构为多项式环 $R=\mathbb{Z}[X]/\left(X^N+1\right)$, 因此本文引入了基于多项式的 Shamir 门限秘密分享方案, 并证明了秘密分享方案在不同的模约化操作下的正确性. 本文基于 Aigis-sig 方案, 利用全同态加密技术和秘密分享体制, 设计了一个安全的 $(2,n)$-门限签名协议, 分析结果表明该协议满足正确性和可行性, 在两个参与者都是诚实的情况下, 生成的门限数字签名满足适应性选择消息攻击下的存在不可伪造性. 当对协议交互信息进行承诺和零知识证明时, 可实现恶意参与者存在时适应性选择消息攻击下的存在不可伪造性.

2 基础知识

2.1 Aigis-sig 方案

Aigis-sig 方案 [8] 安全性基于非对称模上带错误学习 (asymmetric module learning with errors, AMLWE) 问题和非对称模上小整数解 (asymmetric module small integer solutions, AMSIS) 问题的

困难性 [8]. 与格上其他同类方案相比, Aigis-sig 方案能在确保安全性不变的前提下实现更好的综合效率, 特别是拥有更短的公钥、私钥和签名长度. 综合考虑安全性、效率和构造可行性等因素, 本文选择不带公钥压缩的 Aigis-sig 方案构造安全的门限签名协议.

Aigis-sig 方案使用的代数结构为多项式环 $R=\mathbb{Z}[X]/(X^N+1)$ 及子环 $R_q=\mathbb{Z}_q[X]/(X^N+1)$. 环 R 上的加法和乘法运算定义如下:

定义 1 $\forall a,b,c\in R$, $a=\sum_{i=0}^{N-1}a_iX^i$, $b=\sum_{i=0}^{N-1}b_iX^i$, $c=\sum_{i=0}^{N-1}c_iX^i$, 若 $c=a+b$, 则 $c_i=a_i+b_i$; 若 $c=a\times b$, $c_i=\sum_{j=0}^{i}a_jb_{i-j}-\sum_{j=i+1}^{N-1}a_jb_{N+i-j}$; 当 $a,b,c\in R_q$ 时, 若 $c=a+b$, 则 $c_i=(a_i+b_i)\bmod q$; 若 $c=a\times b$, 则 $c_i=\left(\sum_{j=0}^{i}a_jb_{i-j}-\sum_{j=i+1}^{N-1}a_jb_{N+i-j}\right)\bmod q$.

对于任意的正整数 γ, 定义集合 S_γ 为环 R 中每个系数均属于 $\{-\gamma,\cdots,\gamma\}$ 的多项式组成的集合, 即 $\forall x\in S_\gamma$, $x=\sum_{i=0}^{N-1}x_iX^i$, 均满足 $x_i\in\{-\gamma,\cdots,\gamma\}$.

定义 2 [8] (模约化) $\forall r\in\mathbb{Z}$, $\alpha\in\mathbb{Z}^+$, 当 α 是偶数时定义 $r'=r\bmod^{\pm}\alpha$ 是在 $\left(-\frac{\alpha}{2},\frac{\alpha}{2}\right]\bigcap\mathbb{Z}$ 范围内中唯一元素 r' 满足 $r'=r\bmod\alpha$ 成立; 当 α 是奇数时定义 $r'=r\bmod^{\pm}\alpha$ 是在 $\left[-\frac{\alpha-1}{2},\frac{\alpha-1}{2}\right]\bigcap\mathbb{Z}$ 中唯一元素 r' 满足 $r'=r\bmod\alpha$ 成立. 定义 $r'=r\bmod^{+}\alpha$ 是在 $[0,\alpha)\bigcap\mathbb{Z}$ 中唯一元素满足 $r'=r\bmod\alpha$ 成立, 当精确的表示不重要时, 简记为 $r\bmod\alpha$.

不带公钥压缩的 Aigis-sig 方案包含 3 个算法:

密钥生成算法 Aigis-sig.KeyGen (1^κ): κ 为安全参数, 随机选择 $\rho\xleftarrow{\$}\{0,1\}^{256}$, $(\boldsymbol{s}_1,\boldsymbol{s}_2)\xleftarrow{\$}S_{\eta_1}^l\times S_{\eta_2}^k$, 通过矩阵生成算法计算 Expand () 生成矩阵 $\boldsymbol{A}=\mathrm{Expand}(\rho)\in R_q^{k\times l}$, 计算 $\boldsymbol{t}=\boldsymbol{A}\boldsymbol{s}_1+\boldsymbol{s}_2\in R_q^k$ 和 $\mathrm{tr}=\mathrm{CRH}(\rho,t)\in\{0,1\}^{384}$, CRH: $\{0,1\}^*\to\{0,1\}^{384}$ 是抗碰撞杂凑函数, 最后返回公钥 $\mathrm{pk}=(\rho,\boldsymbol{t})$ 和私钥 $\mathrm{sk}=(\rho,\mathrm{tr},\boldsymbol{s}_1,\boldsymbol{s}_2)$.

签名生成算法 Aigis-sig.Sign (sk,M): 给定私钥 $\mathrm{sk}=(\rho,\mathrm{tr},\boldsymbol{s}_1,\boldsymbol{s}_2)$ 和消息 M, 计算 $\boldsymbol{A}=\mathrm{Expand}(\rho)$, $\mu=\mathrm{CRH}(\mathrm{tr}||M)$, 并执行以下步骤:

- 随机选择 $\boldsymbol{y}\xleftarrow{\$}S_{\gamma_1-1}^l$;
- 计算 $\boldsymbol{w}=\boldsymbol{A}\boldsymbol{y}\in R_q^k$, 通过 $\mathrm{HighBits}_q(\boldsymbol{w},2\gamma_2)$ 计算 $\boldsymbol{w}$ 的高位比特向量 $\boldsymbol{w}_1$;
- 计算挑战 $c=H(\mu,\boldsymbol{w}_1)$, 其中 $H:\{0,1\}^*\to B_\tau$ 是满足密码学性质的杂凑函数, $B_\tau\subseteq R$ 表示环 R 中恰好有 τ 个系数为 ±1, 且其他系数均为 0 的元素构成的集合;
- 计算 $\boldsymbol{z}=\boldsymbol{y}+c\boldsymbol{s}_1$ 和 $\boldsymbol{u}=\boldsymbol{w}-c\boldsymbol{s}_2=\boldsymbol{A}\boldsymbol{z}-c\boldsymbol{t}$, 分别计算 $\boldsymbol{u}$ 的高位比特向量 $\boldsymbol{r}_1=\mathrm{HighBits}_q(\boldsymbol{u},2\gamma_2)$ 和低位比特向量 $\boldsymbol{r}_0=\mathrm{LowBits}_q(\boldsymbol{u},2\gamma_2)$;
- 如果 $\|\boldsymbol{z}\|_\infty\geq\gamma_1-\beta_1$ 或 $\|\boldsymbol{r}_0\|_\infty\geq\gamma_2-\beta_2$ 或 $\boldsymbol{r}_1\neq\boldsymbol{w}_1$, 重新选择随机向量 $\boldsymbol{y}$;
- 输出签名 $\sigma=(\boldsymbol{z},c)$;

签名验证算法 Aigis-sig.Verify (pk,M,σ): 给定公钥 $\mathrm{pk}=(\rho,\boldsymbol{t})$, 消息 M 和签名 $\sigma=(\boldsymbol{z},c)$, 首先计算 $\boldsymbol{A}=\mathrm{Expand}(\rho)$, $\mu=\mathrm{CRH}(\mathrm{CRH}(\mathrm{pk})||M)$, $\boldsymbol{w}_1'=\mathrm{HighBits}_q(\boldsymbol{A}\boldsymbol{z}-c\boldsymbol{t},2\gamma_2)$. 然后计算 $c'=H(\mu,\boldsymbol{w}_1')$. 如果 $\|\boldsymbol{z}\|_\infty<\gamma_1-\beta_1$ 且 $c'=c$, 接受签名, 否则拒绝签名.

算法 1 Aigis-sig 方案 Decompose 算法

```
r = r mod^+ q
r_0 = r mod^± α
if r − r_0 = q − 1 then
    r_1 = 0;
    r_0 = r_0 − 1;
end
else
    r_1 = (r − r_0)/α
end
return (r_1, r_0)
```

由算法 1 可知, 若 $(r_1,r_0)=\mathrm{Decompose}_q(r,\alpha)$, 则有 $r_1=\mathrm{HighBits}_q(r,\alpha)$, $r_0=\mathrm{LowBits}_q(r,\alpha)$. $r,z\in\mathbb{Z}$, α 为正整数, $\alpha\,|\,(q-1)$. 当上述算法被作用到多项式或多项式向量时, 其含义是对应操作被分别

独立地作用到多项式的每个系数上.

Aigis-sig 方案通过引理 1 来保证正确性:

引理 1 [7] 如果 $\|\boldsymbol{s}\|_\infty \le \beta$ 且 $\|\mathrm{LowBits}_q(\boldsymbol{r},\alpha)\|_\infty \le \frac{\alpha}{2}-\beta$, 那么有等式成立:

$$\mathrm{HighBits}_q(\boldsymbol{r},\alpha)=\mathrm{HighBits}_q(\boldsymbol{r}+\boldsymbol{s},\alpha). \tag{1}$$

2.2 同态加密方案

同态加密是一类密码学原语, 它允许用户在不解密的情况下对加密数据进行运算. Gentry 在 2009 年构造出了第一个全同态加密方案 [13], 随后又出现了各种全同态加密优化方案, 如 BFV [14]、Bra12 [15]、BGV [16]、GSW [17]、FHEW [18]、CKKS [19] 等.

一般来说, 一个全同态加密方案包含下列算法:

密钥生成算法 $\mathrm{HE.KeyGen}(\kappa, L)$: 输入安全参数 κ、层次参数 L, 运行密钥生成算法, 输出公钥 $\mathrm{pk_{HE}}$, 私钥 $\mathrm{sk_{HE}}$ 和运算密钥 $\mathrm{evk_{HE}}$.

加密算法 $\mathrm{Enc}_{\mathrm{pk_{HE}}}(m)$: 输入公钥 pk 和明文 m, 输出密文 ct.

解密算法 $\mathrm{Dec}_{\mathrm{sk_{HE}}}(\mathrm{ct})$: 输入私钥 sk 和密文 ct, 输出明文 m.

密文同态加法运算 $\mathrm{EvalAdd}_{\mathrm{evk_{HE}}}(\mathrm{ct}_1,\mathrm{ct}_2)$: 输入 m_1 和 m_2 的密文 ct_1 和 ct_2, 输出 m_1+m_2 的密文 $\mathrm{ct_{add}}$.

明密文同态乘法运算 $\mathrm{EvalMultConst}_{\mathrm{evk_{HE}}}(m_1,\mathrm{ct}_2)$: 输入 m_1, m_2 的密文 ct_2, 输出密文 $\mathrm{ct_{mult\_const}}$, 且 $\mathrm{Dec}_{\mathrm{sk_{HE}}}(\mathrm{ct_{mult\_const}})=m_1\cdot m_2$.

密文同态运算 $\mathrm{HomEval}(\mathrm{evk_{HE}}, f, \mathrm{ct}_1,\cdots,\mathrm{ct}_l)$: 使用同态运算密钥 $\mathrm{evk_{HE}}$, 对函数 f 作用的一系列密文 $\mathrm{ct}_i\,(i=1,\cdots,l)$ 进行算术运算, 输出密文 ct_f. 函数 f 表示的是包含若干个加法或乘法的运算电路.

在密态计算协议中间值时, 除了进行上述同态基本运算外, 部分中间值还需要进行同态密文比较运算. 文献 [20] 表明, 基于 CKKS 方案的同态密文比较算法实现效率较高, 因此在 $(2,n)$-门限签名的协议构造中本文采用了 CKKS 同态加密方案.

2.3 Shamir 秘密分享体制

文献 [11] 中签名私钥生成方法为直接相加, 即各参与者分别生成签名私钥份额 $(\mathbf{ss}_{1,i},\mathbf{ss}_{2,i}) \xleftarrow{\$} S_{\eta_1}^l \times S_{\eta_2}^k, i\in\{1,\cdots,t\}$, 签名私钥为 $(\sum \mathbf{ss}_{1,i}, \sum \mathbf{ss}_{2,i})$, 其私钥分布的上界由 (η_1,η_2) 变为 $(t\eta_1, t\eta_2)\,(t\ge 2)$, 私钥的上界变大将导致拒绝采样次数的期望值增加, 进而增加协议重复运行次数. 引入 Shamir 秘密分享体制可以有效地避免上述问题, 通过线性组合生成的签名私钥取值上界不变, 不会增加协议重复运行次数, 也可确保重构时签名私钥 $(\boldsymbol{s}_1,\boldsymbol{s}_2)$ 仍服从 $S_{\eta_1}^l \times S_{\eta_2}^k$ 上的均匀分布.

1979 年, Shamir 利用拉格朗日插值多项式理论设计了一个具体的 (t,n)-门限方案 [21], 该方案简单、灵活, 在门限密码学与安全多方计算中均有广泛应用. 定义拉格朗日系数为 $L_{i,S}(x)=\prod_{j=1,j\ne i}^{t}\frac{x-x_j}{x_i-x_j}$, 其中 $i\in\mathbb{Z}_p$, $S=\{x_i\}\,(1\le i\le t)$, $S\subset\mathbb{Z}_p$, p 为素数. 为适应协议的构造, 结合定义 2 中 $\mathrm{mod}^{\pm}p$ 和 $\mathrm{mod}^{+}p$ 操作的定义, 本文引入模 $\mathrm{mod}^{\pm}p$ 意义下 (t,n)-Shamir 门限方案.

命题 1 $\mathrm{mod}^{\pm}p$ 意义下 (t,n)-Shamir 门限方案满足重构正确性.

证明: 令 $P=\{P_1,P_2,\cdots,P_n\}$ 为参与者集合, t 是门限, $\mathrm{ss}\in\mathbb{Z}_p$ 为待分享的秘密, p 为素数. 可信中心 D 选择一个次数为 $t-1$ 的秘密多项式: $d(x)=\mathrm{ss}+\sum_{j=1}^{t-1}d_jx^j \bmod^{+} p$, 其中 $0\ne d_j\in\mathbb{Z}_p$, 并选择 n 个互不相同的非零元素 $x_i\in\mathbb{Z}_p$, 为每个参与者计算 $\mathrm{ss}_i=d(x_i)\in\mathbb{Z}_p$, 并将 (x_i,ss_i) 发送给参与者 P_i.

假设在 $\mathrm{mod}^{+}p$ 的意义下, (t,n) 门限方案的秘密份额为 $\{\mathrm{ss}_1,\mathrm{ss}_2,\cdots,\mathrm{ss}_n\}$, $\mathrm{ss}_i=d(x_i)\bmod^{+}p$, 任意 t 个或多于 t 个参与者可通过拉格朗日插值公式重构秘密. 不失一般性, 不妨假设前 $P_i\,(1\le i\le t)$ 个参与者利用 $\{(x_i,\mathrm{ss}_i)\}\,(1\le i\le t)$ 重构秘密, 令 $S=\{x_i\}\,(1\le i\le t)$, 则 $\mathrm{ss}=d(0)=\sum_{i=1}^{t}\mathrm{ss}_i\prod_{j=1,j\ne i}^{t}\frac{-x_j}{x_i-x_j}=\sum_{i=1}^{t}\mathrm{ss}_iL_{i,S}(0)\bmod^{+}p$.

令 $\mathrm{ss}_i'=\mathrm{ss}_i\bmod^{\pm}p$, $L_{i,S}'(0)=L_{i,S}(0)\bmod^{\pm}p$, $\mathrm{ss}'=\mathrm{ss}\bmod^{\pm}p$, $\mathrm{mod}^{\pm}p$ 与 $\mathrm{mod}^{+}p$ 操作满足如下关系: $\forall x\in\mathbb{Z}$, 令 $x'=x\bmod^{\pm}p$, $x''=x\bmod^{+}p$, 当 $x''\in\left[0,\frac{p-1}{2}\right]$ 时, $x'=x''$, 当 $x''\in\left[\frac{p+1}{2},p-1\right]$ 时, $x'=x''-p\in\left[-\frac{p-1}{2},-1\right]$.

下证 $k'=\sum_{i=1}^{t}\mathrm{ss}_i'L_{i,S}'(0)\bmod^{\pm}p$:

$$\begin{aligned}k'=k\bmod^{\pm}p&=\Big(\sum_{i=1}^{t}\mathrm{ss}_iL_{i,S}(0)\bmod^{+}p\Big)\bmod^{\pm}p\\&=\Big(\sum_{i=1}^{t}\left(\mathrm{ss}_i\bmod^{\pm}p\right)\left(L_{i,S}(0)\bmod^{\pm}p\right)\Big)\bmod^{\pm}p\\&=\sum_{i=1}^{t}\mathrm{ss}_i'L'_{i,S}(0)\bmod^{\pm}p.\end{aligned}\tag{2}$$

综上, $\bmod^{\pm}p$ 意义下 (t,n)-Shamir 门限方案是正确的. □

在 Aigis-sig 方案中, 涉及到主要的代数结构为多项式环, 因此本文引入基于多项式环的 (t,n)-Shamir 门限方案 [22] 来确保签名私钥分享协议的安全性. 可信中心选择基于多项式环 $R_p=\mathbb{Z}_p[X]/\left(X^N+1\right)$ 的秘密多项式 $d(x)=\mathrm{ss}+\sum_{j=1}^{t-1}d_jx^j\bmod^{\pm}p$, 其中 $\mathrm{ss},d_j\in R_p$, $d_j\neq 0$. 选择 $\mathbb{Z}_p$ 上 n 个不同的非零元素 x_i, 为每个参与者计算 $\mathrm{ss}_i=d(x_i)\bmod^{\pm}p\in R_p$, 并将 (x_i,ss_i) 发送给参与者 P_i.

由命题 1 及文献 [22] 中定理 2 知, 基于多项式环且系数 $\bmod^{\pm}p$ 意义下 (t,n)-Shamir 门限方案是正确的.

由基于多项式环的 (t,n)-Shamir 门限方案的机密性可知, 任何少于 t 个参与者的集合都不能得到关于秘密的任何信息, 因此敌手能得到秘密 $k\in R_p$ 的概率是可忽略的. 且有如下命题成立:

命题 2 给定系统参数, 敌手至多可以破坏 $t-1$ 个成员, 那么敌手能得到秘密 $\mathrm{ss}\in R_p$ 的概率是可忽略的.

2.4 安全性定义

数字签名方案的安全性归约实验 [8] 定义如下:

EXPERIMENT 2.4.1: $\mathrm{Expt\text{-}Sign}_{\mathcal{S},\pi}(1^{\kappa})$

(1) $(\mathrm{pk},\mathrm{sk})\leftarrow\mathrm{KeyGen}(1^{\kappa})$

(2) $(M^*,\sigma^*)\leftarrow\mathcal{S}^{\mathrm{Sign}_{\mathrm{sk}}(\cdot)}(\mathrm{pk})$, 其中签名预言机的定义为: 对询问的消息 M, 生成签名 $\sigma\leftarrow\mathrm{Sign}(\mathrm{sk},M)$, 添加 (M,σ) 到集合 Q 中, 然后返回 (M,σ) 作为回答.

(3) 该实验输出为 1 当且仅当有 $(M^*,\sigma^*)\notin Q$ 且 $\mathrm{Verify}_{\mathrm{pk}}(M^*,\sigma^*)=1$.

定义 3 如果对于任意概率多项式时间的敌手 $\mathcal{S}$ 均存在一个和 κ 有关的可忽略函数 λ, 使得下式成立:

$$\Pr\left[\mathrm{Expt\text{-}Sign}_{\mathcal{S},\pi}(1^{\kappa})=1\right]\leq\lambda(\kappa),$$

我们称数字签名方案 $\pi=(\mathrm{KeyGen},\mathrm{Sign},\mathrm{Verify})$ 满足在适应性选择消息攻击下的强存在不可伪造性 (strong existential unforgeability against adaptive chosen-message attack, SUF-CMA). 定义敌手优势为 $\mathrm{Adv}_{\pi}^{\text{SUF-CMA}}(\mathcal{S})=\Pr\left[\mathrm{Expt\text{-}Sign}_{\mathcal{S},\pi}(1^{\kappa})=1\right]$.

门限签名协议的安全性归约实验定义如下:

EXPERIMENT 2.4.2: $\mathrm{Expt\text{-}ThreSign}_{\mathcal{A},\Pi}(1^{\kappa})$

令 $\pi=(\mathrm{KeyGen},\mathrm{Sign},\mathrm{Verify})$ 为一标准数字签名方案.

(1) $(M^*,\sigma^*)\leftarrow\mathcal{A}^{\Pi(\cdot,\cdot)}(\mathrm{pk})$, 其中门限签名预言机的定义为: 对询问的消息 M, 生成门限签名 $\sigma\leftarrow\mathrm{ThreSign}(\mathrm{sk},M)$, 添加 M 到集合 Q' 中, 然后返回 σ 作为回答.

(2) 该实验的输出为 1 当且仅当有 $M^*\notin Q'$ 且 $\mathrm{Verify}_{\mathrm{pk}}(M^*,\sigma^*)=1$.

如果敌手通过多项式次适应性选择消息的 $(2,n)$-门限签名查询, 能够伪造出还没被询问消息的门限签名, 则 $\mathrm{Expt\text{-}ThreSign}_{\mathcal{A},\Pi}(1^{\kappa})=1$, 即敌手赢得了该实验. $(2,n)$-门限签名协议的安全性定义如下.

定义 4 如果对于任意的概率多项式时间的敌手 $\mathcal{A}$, 均存在一个和 κ 有关的可忽略函数 λ', 使得下式成立:

$$\Pr\left[\text{Expt-ThreSign}_{\mathcal{A},\Pi}(1^{\kappa})=1\right]\leq\lambda'(\kappa),$$

则称基于数字签名方案 π 设计的 $(2,n)$-门限签名协议 Π 满足适应性选择消息攻击下的存在不可伪造性 (existential unforgeability against adaptive chosen-message attack, EUF-CMA). 定义敌手优势为 $\text{Adv}_{\Pi}(\mathcal{A})=\Pr\left[\text{Expt-ThreSign}_{\mathcal{A},\Pi}(1^{\kappa})=1\right]$.

3 (2, n)-门限 Aigis-sig 签名协议

在本节, 我们基于 Aigis-sig 方案 [8], 借助基于多项式环的 (t,n)-Shamir 门限方案 [22] 和同态加密方案 [19], 设计了一个 $(2,n)$-门限 Aigis-sig 签名协议. 该协议包含两个子协议: 签名私钥分享协议和门限签名协议. 假设每个参与者都可以通过可信中心获得其他参与者的同态加密密钥和同态运算密钥, 则参与者 P_i 拥有的同态密钥为 $\left\{\text{pk}_{1,\text{HE}},\cdots,\text{pk}_{n,\text{HE}},\text{evk}_{1,\text{HE}},\cdots,\text{evk}_{n,\text{HE}},\text{sk}_{i,\text{HE}}\right\}$

3.1 签名私钥分享协议

可信中心 D 随机选择 $\rho\xleftarrow{\$}\{0,1\}^{256}$, 计算 $\boldsymbol{A}=\text{Expand}(\rho)\in R_q^{k\times l}$, $(\boldsymbol{s}_1,\boldsymbol{s}_2)\xleftarrow{\$}S_{\eta_1}^l\times S_{\eta_2}^k$, 计算 $\boldsymbol{t}=\boldsymbol{A}\boldsymbol{s}_1+\boldsymbol{s}_2$, 并将公钥 $(\boldsymbol{A},\boldsymbol{t})$ 通过公开信道发送给验证者. 然后中心 D 通过 $(2,n)$-门限方案产生签名私钥份额并通过保密信道分发份额.

令 $P=\{P_1,P_2,\cdots,P_n\}$ 为参与者集合, 将签名私钥 $\boldsymbol{s}_1\in S_{\eta_1}^l\subset R_p^l$, $\boldsymbol{s}_2\in S_{\eta_2}^k\subset R_p^k$ 表示为列向量的形式, 每个分量 ${\boldsymbol{s}_1}^{(i)}(1\leq i\leq l)$ 和 ${\boldsymbol{s}_2}^{(h)}(1\leq h\leq k)$ 是待分享的秘密. 中心选择 l 个多项式 $d_i(x)={\boldsymbol{s}_1}^{(i)}+d_{i,\boldsymbol{s}_1}x \bmod^{\pm}p\,(1\leq i\leq l)$, 和 k 个多项式 $d_{h+l}(x)={\boldsymbol{s}_2}^{(h)}+d_{h,\boldsymbol{s}_2}x \bmod^{\pm}p\ (1\leq h\leq k)$, 其中 $d_{i,\boldsymbol{s}_1},d_{h,\boldsymbol{s}_2}\in R_q$, $d_{i,\boldsymbol{s}_1},d_{h,\boldsymbol{s}_2}\neq 0$. 中心 D 随机选择 $\mathbb{Z}_p^*$ 上 n 个不同的元素 $\{x_1,x_2,\cdots,x_n\}$, 对 ${\boldsymbol{s}_1}^{(i)}$ 和 ${\boldsymbol{s}_2}^{(h)}$ 分别计算 $\mathbf{ss}_{1,u}^{(i)}=d_i(x_u)\bmod^{\pm}p\,(1\leq i\leq l)$, $\mathbf{ss}_{2,u}^{(h)}=d_{h+l}(x_u)\bmod^{\pm}p\ (1\leq h\leq k,1\leq u\leq n)$ 并将其分别发送给各参与者, P_u 获得关于 $(\boldsymbol{s}_1,\boldsymbol{s}_2)$ 的秘密份额为 $(\mathbf{ss}_{1,u},\mathbf{ss}_{2,u})=\left((\mathbf{ss}_{1,u}^{(1)},\mathbf{ss}_{1,u}^{(2)},\cdots,\mathbf{ss}_{1,u}^{(l)})^{\text{T}},(\mathbf{ss}_{2,u}^{(1)},\mathbf{ss}_{2,u}^{(2)},\cdots,\mathbf{ss}_{2,u}^{(k)})^{\text{T}}\right)$. 签名私钥分享协议生成 n 个秘密份额 $\{x_u,(\mathbf{ss}_{1,u},\mathbf{ss}_{2,u})\}\,(1\leq u\leq n)$.

任意两个参与者可以通过拉格朗日插值公式重构签名私钥, 不妨设两个参与者为 $\{P_1,P_2\}$. 令 $S=\{x_1,x_2\}$, 计算 ${\boldsymbol{s}_1}^{(i)}=d_i(0)=\sum_{u\in S}\mathbf{ss}_{1,u}^{(i)}L_{1,u}^{(i)}(0)\bmod^{\pm}p\,(1\leq i\leq l)$, 秘密 ${\boldsymbol{s}_2}^{(h)}\,(1\leq h\leq k)$ 也可以通过同样的方法求出. 由于拉格朗日系数只与 $\{x_1,x_2\}$ 有关, 对固定的 $u\in S$, $\forall 1\leq i\leq l$, $1\leq h\leq k$, 有 $L_{1,u}^{(i)}(0)=L_{2,u}^{(h)}(0)$ 成立, 令 $L_1=L_{1,x_1}^{(1)}(0)$, $L_2=L_{1,x_2}^{(1)}(0)$, 则生成 ${\boldsymbol{s}_1}^{(i)}\,(1\leq i\leq l)$ 和 ${\boldsymbol{s}_2}^{(h)}\,(1\leq h\leq k)$ 的拉格朗日系数为 $(L_1,L_2)\in\mathbb{Z}_p^2$, P_1 和 P_2 关于 $(\boldsymbol{s}_1,\boldsymbol{s}_2)$ 的秘密份额分别为 $(\mathbf{ss}_{1,1},\mathbf{ss}_{2,1})$ 和 $(\mathbf{ss}_{1,2},\mathbf{ss}_{2,2})$. 从而有 $\boldsymbol{s}_1=(L_1\mathbf{ss}_{1,1}+L_2\mathbf{ss}_{1,2})\bmod^{\pm}p$, $\boldsymbol{s}_2=(L_1\mathbf{ss}_{2,1}+L_2\mathbf{ss}_{2,2})\bmod^{\pm}p$. 图 1 给出了在签名私钥分享协议中，中心 D 与参与者 P_1 和 P_2 的交互过程。

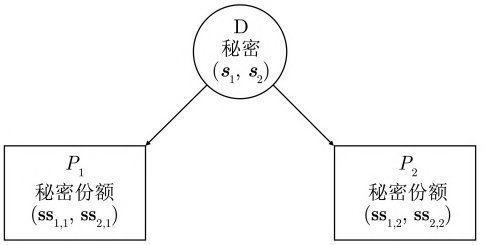


图 1 签名私钥分享协议

Figure 1 Secret sharing protocol

3.2 门限签名协议

P_1 随机选取 $\boldsymbol{y}_1\xleftarrow{\$}S_{\gamma_1-1}^l$, 计算 $\text{ct}_1=\text{Enc}_{\text{pk}_{1,\text{HE}}}(\boldsymbol{y}_1)$, 并发送给 P_2. P_2 随机选取 $\boldsymbol{y}_2\xleftarrow{\$}S_{\gamma_1-1}^l$, 计算 $\text{ct}_2=\text{EvalAddConst}_{\text{evk}_{1,\text{HE}}}\left(L_2\boldsymbol{y}_2,\text{EvalMultConst}_{\text{evk}_{1,\text{HE}}}(L_1,\text{ct}_1)\right)$,

$\mathrm{ct}_3 = \mathrm{HomEval}\left(\mathrm{evk}_{1,\mathrm{HE}}, F_{\mathrm{mod}^{\pm}p}(), \mathrm{ct}_2\right)$, 然后计算 $\mathrm{ct}_4 = \mathrm{EvalMultConst}_{\mathrm{evk}_{1,\mathrm{HE}}}(\boldsymbol{A}, \mathrm{ct}_3)$, $\mathrm{ct}_5 = \mathrm{HomEval}\left(\mathrm{evk}_{1,\mathrm{HE}}, F_{\mathrm{HighBits}_q(*,2\gamma_2)}(), \mathrm{ct}_4\right)$, 并将 ct_5 发送给 P_1.

令 $\boldsymbol{y} = (L_1\boldsymbol{y}_1 + L_2\boldsymbol{y}_2) \bmod^{\pm} p$, $\boldsymbol{w} = \boldsymbol{A}\left((L_1\boldsymbol{y}_1 + L_2\boldsymbol{y}_2) \bmod^{\pm} p\right) = \boldsymbol{A}\boldsymbol{y}$, P_1 计算 $\boldsymbol{w}_1 = \mathrm{Dec}_{\mathrm{sk}_{1,\mathrm{HE}}}(\mathrm{ct}_5) = \mathrm{HighBits}_q(\boldsymbol{w}, 2\gamma_2)$, 计算挑战 $c = H(\mu, \boldsymbol{w}_1)$ 和 $\boldsymbol{z}_1 = \boldsymbol{y}_1 + c\mathbf{ss}_{1,1}$, 并将 c, $\boldsymbol{z}_1$ 发送给 P_2.

P_2 收到 c 后计算 $\boldsymbol{z}_2 = \boldsymbol{y}_2 + c\mathbf{ss}_{1,2}$, 并将 $\boldsymbol{z}_2$ 发送给 P_1. P_2 收到 $\boldsymbol{z}_1$ 后计算 $\boldsymbol{z} = (L_1\boldsymbol{z}_1 + L_2\boldsymbol{z}_2) \bmod^{\pm} p = (L_1\boldsymbol{y}_1 + L_2\boldsymbol{y}_2 + c(L_1\mathbf{ss}_{1,1} + L_2\mathbf{ss}_{2,1})) \bmod^{\pm} p = (L_1\boldsymbol{y}_1 + L_2\boldsymbol{y}_2) \bmod^{\pm} p + c\boldsymbol{s}_1 = \boldsymbol{y} + c\boldsymbol{s}_1$, 并进行拒绝采样条件的验证:

$$\|\boldsymbol{z}\|_\infty < \gamma_1 - \beta_1, \tag{3}$$

$$\|\mathrm{LowBits}_q(\boldsymbol{A}\boldsymbol{z} - c\boldsymbol{t}, 2\gamma_2)\|_\infty < \gamma_2 - \beta_2. \tag{4}$$

P_1 收到 $\boldsymbol{z}_2$ 后计算 $\boldsymbol{z} = (L_1\boldsymbol{z}_1 + L_2\boldsymbol{z}_2) \bmod^{\pm} p = \boldsymbol{y} + c\boldsymbol{s}_1$, 并进行拒绝采样条件的验证:

$$\|\boldsymbol{z}\|_\infty < \gamma_1 - \beta_1, \tag{5}$$

$$\|\mathrm{LowBits}_q(\boldsymbol{A}\boldsymbol{z} - c\boldsymbol{t}, 2\gamma_2)\|_\infty < \gamma_2 - \beta_2. \tag{6}$$

当拒绝采样条件的验证均通过时, P_1 和 P_2 生成门限签名 $(\boldsymbol{z}, c)$, 否则重新运行门限签名协议. 图2给出了在门限签名协议中，P_1 和 P_2 的交互过程。

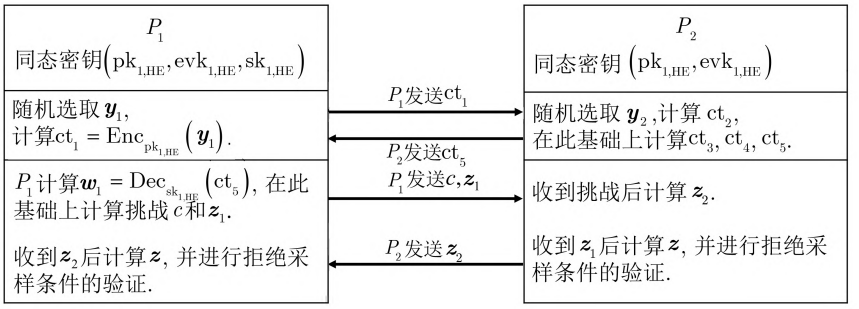


图 2 门限签名协议
Figure 2 Threshold signing protocol

4 (2, n)-门限 Aigis-sig 签名协议分析

4.1 正确性分析

4.1.1 向量 $\boldsymbol{y}$ 生成方法合理性

P_1 随机选取 $\boldsymbol{y}_1 \xleftarrow{\$} S^l_{\gamma_1-1}$, P_2 随机选取 $\boldsymbol{y}_2 \xleftarrow{\$} S^l_{\gamma_1-1}$, 令 $\boldsymbol{y} = (L_1\boldsymbol{y}_1 + L_2\boldsymbol{y}_2) \bmod^{\pm} p$, 适当选取 γ_1 使 $p = 2\gamma_1 - 1$ 是素数, 有 $S_{\gamma_1-1} \subseteq R_p$, 且 $(L_1, L_2) \in \mathbb{Z}_p^2$, 因此 $(L_1\boldsymbol{y}_1 + L_2\boldsymbol{y}_2) \bmod^{\pm} p$ 的每个分量都在集合 S_{γ_1-1} 中, 从而有 $\boldsymbol{y} \in S^l_{\gamma_1-1}$.

4.1.2 向量 $\boldsymbol{y}$ 的随机性

引理 2 设 y_1 和 y_2 是 $\mathbb{Z}_p$ 上两个相互独立的随机变量, 且均服从 $\mathbb{Z}_p$ 上均匀分布, $k_1, k_2 \in \mathbb{Z}_p^*$ 为定值, 那么 $(k_1y_1 + k_2y_2) \bmod^{\pm} p$ 服从 $\mathbb{Z}_p$ 上均匀分布.

证明: $\forall z \in \mathbb{Z}_p$, 有

$$\begin{aligned}\Pr\left[k_1y_1+k_2y_2=z \bmod^{\pm} p\right] &= \sum_{i\in\mathbb{Z}_p}\Pr\left[(k_1y_1=z-i) \bmod^{\pm} p \wedge (k_2y_2=i) \bmod^{\pm} p\right]\\ &= \sum_{i\in\mathbb{Z}_p}\Pr\left[(k_1y_1=z-i) \bmod^{\pm} p\right]\times\Pr\left[(k_2y_2=i) \bmod^{\pm} p\right]\\ &= \sum_{i\in\mathbb{Z}_p}\Pr\left[y_1=(z-i)\cdot {k_1}^{-1} \bmod^{\pm} p\right]\times\Pr\left[y_2=i\cdot k_2^{-1} \bmod^{\pm} p\right]. \end{aligned} \tag{7}$$

由 $k_1, k_2 \in \mathbb{Z}_p^*$ 且均为定值, y_2 服从 $\mathbb{Z}_p$ 上均匀分布, 有

$$\Pr\left[y_2=i\cdot k_2^{-1} \bmod^{\pm} p\right]=\Pr\left[y_2=i\cdot k_2^{-1} \bmod^{+} p\right]=\frac{1}{p},$$

因此

$$\Pr\left[k_1y_1+k_2y_2=z \bmod^{\pm} p\right]=\frac{1}{p}\sum\nolimits_{i\in\mathbb{Z}_p}\Pr\left[y_1=(z-i)\cdot {k_1}^{-1} \bmod^{\pm} p\right]=\frac{1}{p},$$

即 $(k_1y_1+k_2y_2) \bmod^{\pm} p$ 服从 $\mathbb{Z}_p$ 上均匀分布. □

推论 1 设 $\boldsymbol{y}_1$ 和 $\boldsymbol{y}_2$ 是 $S^l_{\gamma_1-1}$ 上两个相互独立的随机变量, 且均服从 $S^l_{\gamma_1-1}$ 上均匀分布, 对固定的成员 P_1 和 P_2, $L_1, L_2 \in \mathbb{Z}_p^*$ 为定值, 那么 $\boldsymbol{y}=(L_1\boldsymbol{y}_1+L_2\boldsymbol{y}_2) \bmod^{\pm} p$ 的每个分量服从 S_{γ_1-1} 上均匀分布, $\boldsymbol{y}$ 服从 $S^l_{\gamma_1-1}$ 上的均匀分布.

证明: 对 $\boldsymbol{y}_1$ 和 $\boldsymbol{y}_2$ 分量的每个系数应用引理 2 即证. □

4.2 门限签名的正确性

Aigis-sig 方案中使用拒绝采样技术 [8], 确保生成签名值不泄露签名私钥信息. 在引入 $(2,n)$-Shamir 门限方案后, 参与者在生成门限签名后进行拒绝采样条件的验证.

在公式(5)中, 如果 $\|c\boldsymbol{s}_1\|_\infty < \beta_1$ 成立, 那么当 $\|\boldsymbol{y}\|_\infty \le \gamma_1-2\beta_1-1$ 时, 总有 $\|\boldsymbol{z}\|_\infty \le \gamma_1-\beta_1-1$. 该范围的大小为 $2(\gamma_1-\beta_1)-1$. 由于 $\boldsymbol{y}$ 中的每个多项式系数都是从 $2\gamma_1-1$ 个元素中均匀取值, 因此 $\|\boldsymbol{z}\|_\infty \le \gamma_1-\beta_1-1$ 的概率为 $\left(\frac{2(\gamma_1-\beta_1)-1}{2\gamma_1-1}\right)^{Nl} \approx e^{-\frac{Nl\beta_1}{\gamma_1}}$.

在公式(6)中, $\|\boldsymbol{r}_0\|_\infty = \|\mathrm{LowBits}_q(\boldsymbol{Az}-c\boldsymbol{t}, 2\gamma_2)\|_\infty < \gamma_2-\beta_2$, 假设 $\boldsymbol{r}_0$ 中多项式的每个系数都服从在模 $2\gamma_2$ 剩余系中的均匀分布, 那么 $\|\boldsymbol{r}_0\|_\infty < \gamma_2-\beta_2$ 的概率为 $\left(\frac{2(\gamma_2-\beta_2)-1}{2\gamma_2}\right)^{Nk} \approx e^{-\frac{Nk\beta_2}{\gamma_2}}$.

因此, 运行一次协议生成门限签名的概率为: $e^{-N\left(\frac{l\beta_1}{\gamma_1}+\frac{k\beta_2}{\gamma_2}\right)}$, 当与 Aigis-sig 方案的参数设置基本一致时, 签名生成概率基本相同.

4.3 可行性分析

在签名份额的生成过程中, 引入了全同态加密方案 [19] 后, 一是可以密态实现非线性运算, 同时确保签名私钥的安全性, 二是与其他同态加密方案相比, CKKS 方案支持较快地同态密文比较运算 [20].

首先, 当 $\boldsymbol{w}=\boldsymbol{Ay}=\boldsymbol{A}\left((L_1\boldsymbol{y}_1+L_2\boldsymbol{y}_2) \bmod^{\pm} p\right)$ 时, 有 $\boldsymbol{Az}-c\boldsymbol{t}=\boldsymbol{w}-c\boldsymbol{s}_2$ 成立, 签名验证算法接受门限签名协议生成的签名. 在计算 $(L_1\boldsymbol{y}_1+L_2\boldsymbol{y}_2) \bmod^{\pm} p$ 时, 由于 (L_1, L_2) 为公开参数, 为保证敌手和 P_2 均不能在多项式时间内求解随机向量 $\boldsymbol{y}_1$, P_1 计算 $\mathrm{ct}_1=\mathrm{Enc}_{\mathrm{pk}_{1,\mathrm{HE}}}(\boldsymbol{y}_1)$, 将 ct_1 发送给 P_2, P_2 收到 ct_1 后只能密态计算 $(L_1\boldsymbol{y}_1+L_2\boldsymbol{y}_2) \bmod^{\pm} p$. 此外, 如果 P_2 不计算 ct_5 而直接将 ct_4 发送给 P_1, 虽然敌手不能在多项式时间内求解 $\boldsymbol{w}$, 但 P_1 可以使用 $\mathrm{sk}_{1,\mathrm{HE}}$ 解出 $\boldsymbol{w}$, 收到 $\boldsymbol{z}_2$ 后, 根据等式 $\boldsymbol{Az}-c\boldsymbol{t}=\boldsymbol{w}-c\boldsymbol{s}_2$ 计算签名私钥 $\boldsymbol{s}_2$. P_2 计算 ct_5 发送给 P_1, P_1 解出 $\boldsymbol{w}_1=\mathrm{Dec}_{\mathrm{sk}_{1,\mathrm{HE}}}(\mathrm{ct}_5)=\mathrm{HighBits}_q(\boldsymbol{w}, 2\gamma_2)$, P_1 此时只获得 $\boldsymbol{w}$ 的高位比特信息, P_1 不能在多项式时间内求解 $\boldsymbol{w}$, 确保了签名私钥的安全性.

其次, 门限签名协议中密文同态运算可以通过若干次 2.2 节中的同态基本运算和密文比较运算实现. 通过约 $O(lN)$ 次明密文同态乘法和 $O(lN)$ 次明密文同态加法运算可以实现 ct_2 的计算; ct_3 是 $(L_1\boldsymbol{y}_1+L_2\boldsymbol{y}_2) \bmod^{\pm} p$ 的密态运算结果, 结合 Aigis-sig 的实现代码, ct_3 的计算通过约 $O(lN)$ 次密文同

态乘法、$O(lN)$ 次密文同态加法和 $O(lN)$ 次密文比较运算可以实现. 对 ct_4 计算采用 R_q 上多项式的乘法运算, 据估计, ct_4 的计算至多通过 $O\left(N^2\right)$ 次明密文同态乘法、$O(kN)$ 次密文同态乘法、$O(kN)$ 次密文同态加法和 $O(kN)$ 次密文比较运算可以实现. ct_5 是 $\mathrm{HighBits}_q(\boldsymbol{w}, 2\gamma_2)$ 的密态运算结果, 结合算法 1 及 Aigis-sig 的实现代码, ct_5 的计算通过约 $O(kN)$ 次密文同态乘法、$O(kN)$ 次密文同态加法和 $O(kN)$ 次密文比较运算可以实现.

4.4 安全性分析

本节基于 Aigis-sig 方案的安全性, 基于多项式环的 (t,n)-Shamir 门限方案的安全性和 CKKS 同态加密方案的安全性来证明 $(2,n)$-门限签名协议的安全性.

定理 1 假设 Aigis-Sig 方案满足适应性选择消息攻击下强存在不可伪造性 [8], 基于多项式环的 (t,n)-Shamir 门限方案是可证安全的, CKKS 同态加密方案是可证明选择明文攻击安全 [19], 那么 $(2,n)$-门限签名协议满足适应性选择消息攻击下的存在不可伪造性.

证明: Aigis-sig 方案满足适应性选择消息攻击下的强存在不可伪造性, 则定义的敌手优势 $\mathrm{Adv}_{\text{Aigis-sig}}^{\text{SUF-CMA}}(\mathcal{S}) = \Pr\left[\text{Expt-Sign}_{\mathcal{S},\text{Aigis-sig}}(1^\kappa)=1\right]$ 是可以忽略的; 根据命题 2, $(2,n)$-Shamir 门限方案是安全的, 那么定义的敌手优势 $\mathrm{Adv}_{2\text{-of-}n\ \text{Threshold}}(\mathcal{B})$ 也是可以忽略的; CKKS 同态加密方案满足在选择明文攻击 (chosen-plaintext attack, CPA) 下的安全性, 则定义的敌手优势 $\mathrm{Adv}_{\text{HE}}^{\text{CPA}}(\mathcal{C})$ 也是可以忽略的.

尽管协议的两个参与者都是诚实的, 敌手 $\mathcal{A}$ 不能控制任一参与者并参与到协议的交互过程中, 但是敌手 $\mathcal{A}$ 可以拥有两个参与者交互运行的视图, 也可以获取协议运行中的公开信息, 并进行多项式次适应性选择消息的门限签名查询. 因此对于任意攻击方案 Π 的敌手 $\mathcal{A}$ 如果能在实验 $\text{Expt-ThreSign}_{\mathcal{A},\Pi}(1^\kappa)$ 中以不可忽略的概率伪造出门限签名, 则可能的情况为: 敌手在签名私钥分享协议中获取了至少两个参与者的秘密份额; 敌手解出同态密文, 并利用协议运行中的公开信息计算出签名私钥; 敌手利用多项式次适应性选择消息的门限签名查询, 并利用询问结果伪造出 Aigis-sig 方案的合法签名. 则敌手 $\mathcal{A}$ 分别以不可忽略的优势攻破 $(2,n)$-门限方案, 同态加密方案或者伪造出合法的 Aigis-sig 签名. 这与本文的给出的安全性假设矛盾, 因此, 有下述公式成立:

$$\mathrm{Adv}_{\Pi}(\mathcal{A}) \le \mathrm{Adv}_{2\text{-of-}n\ \text{Threshold}}(\mathcal{B}) + \mathrm{Adv}_{\text{HE}}^{\text{CPA}}(\mathcal{C}) + \mathrm{Adv}_{\text{Aigis-sig}}^{\text{SUF-CMA}}(\mathcal{S}). \tag{8}$$

即敌手能伪造一个新消息的门限签名概率是可忽略的. □

4.5 门限签名协议比较

表 1 给出了不同的门限签名协议在功能性、安全性等方面的比较. Boneh 等人 [10] 基于门限全同态加密技术设计了一类通用的门限签名构造方法, 利用该方法设计的门限签名协议的安全性基于带错误学习 (learning with errors, LWE) 问题的困难性. 文献 [11] 中门限签名协议是基于 Dilithium-G 方案设计的, Dilithium-G 方案是 CRYSTALS-Dilithium 的一个变体, 它使用离散高斯采样生成向量 $\boldsymbol{y}$. Dilithium-G 方案安全性基于模上带错误学习问题 (module learning with errors, MLWE) 问题和模上小整数解 (module small integer solutions, MSIS) 问题的困难性. 根据文献 [11] 中定理 1, 在陷门同态承诺方案是安全的前提下, 协议的安全性与 MLWE 和 MSIS 问题的困难性相关.

表 1 门限签名协议比较

Table 1 Comparison to threshold signature protocols

文献	签名方案	密码学工具	功能性	安全性
文献 [10]	通用构造	门限全同态加密方案	(t,n) 门限	LWE
文献 [11]	Dilithium-G	陷门同态承诺方案	(n,n) 门限	MLWE, MSIS
门限 Aigis-sig 签名协议	Aigis-sig	Shamir 门限方案, 全同态加密方案	$(2,n)$ 门限	AMLWE, AMSIS

由于上述协议均未给出参考实现结果, 因而目前无法给出详细的实现效率比较, 在下一步的研究中, 我们将尝试给出门限 Aigis-sig 协议的参考实现和详细的协议实现效率比较.

本文给出的 $(2,n)$-门限签名协议可以扩展到 (t,n)-门限签名协议 $(2\leq t<n)$. 在签名私钥分享协议中, 签名私钥被分割成 n 个秘密份额 $\{x_u,(\mathbf{ss}_{1,u},\mathbf{ss}_{2,u})\}\,(1\leq u\leq n)$, 任意 t 个参与者可以通过拉格朗日插值公式重构签名私钥:

$$\boldsymbol{s}_1=(L_1\mathbf{ss}_{1,1}+L_2\mathbf{ss}_{1,2}+\cdots+L_t\mathbf{ss}_{1,t})\bmod^{\pm}p$$
$$\boldsymbol{s}_2=(L_1\mathbf{ss}_{2,1}+L_2\mathbf{ss}_{2,2}+\cdots+L_t\mathbf{ss}_{2,t})\bmod^{\pm}p$$

在门限签名协议中, 挑战向量的计算变为 $\boldsymbol{y}=(L_1\boldsymbol{y}_1+\cdots+L_t\boldsymbol{y}_t)\bmod^{\pm}p$, 应用推论 1, 挑战向量 $\boldsymbol{y}$ 仍服从 $S^l_{\gamma_1-1}$ 上的均匀分布, $\boldsymbol{z}=(L_1\boldsymbol{z}_1+\cdots+L_t\boldsymbol{z}_t)\bmod^{\pm}p$, 通过拒绝采样判断的概率不变, 生成门限签名的概率也不会改变. 在签名验证算法中, 仍有 $\boldsymbol{Az}-c\boldsymbol{t}=\boldsymbol{w}-c\boldsymbol{s}_2$ 等式成立, 即在 t 个参与者都是诚实的情况下, 签名验证算法总是接受 (t,n)-门限签名协议生成的门限签名. 但是在 (t,n)-门限签名协议中, 由于需要使用全同态加密技术密态计算 $y=(L_1\boldsymbol{y}_1+\cdots+L_t\boldsymbol{y}_t)\bmod^{\pm}p$ 和 $\boldsymbol{w}=\boldsymbol{Ay}$, 每个参与者的计算量和通信代价会相应增大.

5 结论

本文基于 Aigis-sig 方案给出了一个后量子安全的 $(2,n)$-门限签名协议. 该协议包含签名私钥分享协议和门限签名协议, 借助 (t,n)-Shamir 门限方案和同态加密方案, 实现了分布式签名过程. 协议满足正确性和不可伪造性, 当协议交互信息进行承诺和零知识证明时, 可实现恶意参与者存在时适应性选择消息攻击下的存在不可伪造性. 本文给出的 $(2,n)$-门限签名协议具有较好的扩展性, 可以扩展到 (t,n)-门限签名协 $(2\leq t<n)$, 并且门限数字签名的签名规模和生成签名的概率与 Aigis-sig 方案基本一致. 然而由于引入全同态加密技术, 增加了协议运行过程中计算复杂度, 如何优化方案效率, 是下一步研究工作的重点.

参考文献

[1] LINDELL Y. Fast secure two-party ECDSA signing[C]. In: Advances in Cryptology—CRYPTO 2017, Part II. Springer Cham, 2017: 613–644. [DOI: 10.1007/978-3-319-63715-0_21]

[2] DOERNER J, KONDI Y, LEE E, et al. Secure two-party threshold ECDSA from ECDSA assumptions[C]. In: Proceedings of 2018 IEEE Symposium on Security and Privacy (SP). IEEE, 2018: 980–997. [DOI: 10.1109/SP.2018.00036]

[3] WANG J, WU L B, LUO M, et al. Secure and efficient two-party ECDSA signature scheme[J]. Journal on Communications, 2021, 42(2): 12–25. [DOI: 10.11959/j.issn.1000-436x.2021019]
王婧, 吴黎兵, 罗敏, 等. 安全高效的两方协同 ECDSA 签名方案 [J]. 通信学报, 2021, 42(2): 12–25. [DOI: 10.11959/j.issn.1000-436x.2021019]

[4] FENG Q, HE D B, LUO M, et al. Efficient two-party SM2 signing protocol for mobile Internet[J]. Journal of Computer Research and Development, 2020, 57(10): 2136–2146. [DOI: 10.7544/issn1000-1239.2020.20200401]
冯琦, 何德彪, 罗敏, 等. 移动互联网环境下轻量级 SM2 两方协同签名 [J]. 计算机研究与发展, 2020, 57(10): 2136–2146. [DOI: 10.7544/issn1000-1239.2020.20200401]

[5] LYUBASHEVSKY V. Fiat-Shamir with aborts: Applications to lattice and factoring-based signatures[C]. In: Advances in Cryptology—ASIACRYPT 2009. Springer Berlin Heidelberg, 2009: 598–616. [DOI: 10.1007/978-3-642-10366-7_35]

[6] LYUBASHEVSKY V. Lattice signatures without trapdoors[C]. In: Advances in Cryptology—EUROCRYPT 2012. Springer Berlin Heidelberg, 2012: 738–755. [DOI: 10.1007/978-3-642-29011-4_43]

[7] DUCAS L, KILTZ E, LEPOINT T, et al. CRYSTALS-Dilithium: A lattice-based digital signature scheme[J]. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2018, 2018(1): 238–268. [DOI: 10.13154/tches.v2018.i1.238-268]

[8] ZHANG J, YU Y, FAN S Q, et al. Tweaking the asymmetry of asymmetric-key cryptography on lattices: KEMs and signatures of smaller sizes[C]. In: Public-Key Cryptography—PKC 2020, Part II. Springer Cham, 2020: 37–65. [DOI: 10.1007/978-3-030-45388-6_2]

[9] Chinese Association for Cryptologic Research. Announcement of the selection results of the national cryptographic algorithm competitions[EB/OL]. (2020.01.02). [2021.10.07]. http://www.cacrnet. org.cn/site/cont-ent/854.html
中国密码学会. 关于全国密码算法设计竞赛算法评选结果的公示 [EB/OL]. (2020.01.02). [2021.10.07]. http://www.cacrnet.org.cn/site/cont-ent/854.html

[10] BONEH D, GENNARO R, GOLDFEDER S, et al. Threshold cryptosystems from threshold fully homomorphic encryption[C]. In: Advances in Cryptology—CRYPTO 2018, Part I. Springer Cham, 2018: 565–596. [DOI: 10.1007/978-3-319-96884-1_19]

[11] DAMGÅRD I, ORLANDI C, TAKAHASHI A, et al. Two-round n-out-of-n and multi-signatures and trapdoor commitment from lattices[C]. In: Public-Key Cryptography—PKC 2021, Part I. Springer Cham, 2021: 99–130. [DOI: 10.1007/978-3-030-75245-3_5]

[12] DUCAS L, LEPOINT T, LYUBASHEVSKY V, et al. CRYSTALS-Dilithium: Digital signatures from module lattices[EB/OL]. (2017.11.30). [2021.10.07]. https://repository.ubn.ru.nl/handle/2066/191703

[13] GENTRY C. Fully homomorphic encryption using ideal lattices[C]. In: Proceedings of the Forty-first Annual ACM Symposium on Theory of Computing. ACM, 2009: 169–178. [DOI: 10.1145/1536414.1536440]

[14] FAN J F, VERCAUTEREN F. Somewhat practical fully homomorphic encryption[J/OL]. IACR Cryptology ePrint Archive, 2012: 2012/144. https://eprint.iacr.org/2012/144.pdf

[15] BRAKERSKI Z. Fully homomorphic encryption without modulus switching from classical GapSVP[C]. In: Advances in Cryptology—CRYPTO 2012. Springer Berlin Heidelberg, 2012: 868–886. [DOI: 10.1007/978-3-642-32009-5_50]

[16] BRAKERSKI Z, GENTRY C, VAIKUNTANATHAN V. (Leveled) Fully homomorphic encryption without bootstrapping[J]. ACM Transactions on Computation Theory (TOCT), 2014, 6(3): 1–36. [DOI: 10.1145/2633600]

[17] GENTRY C, SAHAI A, WATERS B. Homomorphic encryption from learning with errors: Conceptually-simpler, asymptotically-faster, attribute-based[C]. In: Advances in Cryptology—CRYPTO 2013, Part I. Springer Berlin Heidelberg, 2013: 75–92. [DOI: 10.1007/978-3-642-40041-4_5]

[18] DUCAS L, MICCIANCIO D. FHEW: Bootstrapping homomorphic encryption in less than a second[C]. In: Advances in Cryptology—EUROCRYPT 2015, Part I. Springer Berlin Heidelberg, 2015: 617–640. [DOI: 10.1007/978-3-662-46800-5_24]

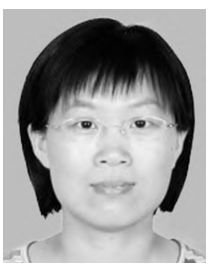
[19] CHEON J H, KIM A, KIM M, et al. Homomorphic encryption for arithmetic of approximate numbers[C]. In: Advances in Cryptology—ASIACRYPT 2017, Part I. Springer Cham, 2017: 409–437. [DOI: 10.1007/978-3-319-70694-8_15]

[20] CHEON J H, KIM D W, KIM D Y, et al. Numerical method for comparison on homomorphically encrypted numbers[C]. In: Advances in Cryptology—ASIACRYPT 2019, Part II. Springer Cham, 2019: 415–445. [DOI: 10.1007/978-3-030-34621-8_15]

[21] SHAMIR A. How to share a secret[J]. Communications of the ACM, 1979, 22(11): 612–613. [DOI: 10.1145/359168.359176]

[22] ZHU W L, YU J P, WANG T, et al. Efficient attribute-based encryption from R-LWE[J]. Chinese Journal of Electronics, 2014, 23(4): 778–782.

作者信息



赵秀凤 (1977–), 山东济宁人, 副教授. 主要研究领域为格上密码协议设计与分析、同态密码.
zhao_xiu_feng@163.com

付雨 (1997–), 河南周口人, 硕士. 主要研究领域为格上密码协议设计与分析.
13663838237@163.com