密码学门限签名系列

第 7 课：GG20 门限签名

lynndell 博士

新火科技 密码学专家 lynndell2010@gmail.com

目录

zk 系列

11. Groth16 证明系统

12. Plonk 证明系统

13. UltraPlonk 证明系统

14. SHA256 查找表技术

15. Halo2 证明系统

16. zkSTARK 证明系统

1. 预备知识

1.1 Paillier 同态加密

密钥生成：生成两个长度相同的大素数 p,q， $p \neq q$，满足 $\gcd\left(pq,(p-1)(q-1)\right)=1$；计算 $n \coloneqq p \cdot q$，$\lambda \coloneqq lcm(p-1,q-1)$；分式除法函数 $L(y)=(y-1)/n$；令 $g=n+1 \in Z_{n^2}^*$，使得 $\mu=\left(L(g^{\lambda} \bmod n^2)\right)^{-1} \bmod n$ 存在。公钥为 n，私钥为 p,q 或 λ。

加密：消息 $m \in Z_n$，选择随机数 $r \in Z_n^*$，计算密文 $c \coloneqq g^m \cdot r^n \bmod n^2$。

解密：输入密文 $c \in Z_{n^2}$，如下计算解密 $m \coloneqq \dfrac{L(c^{\lambda} \bmod n^2)}{L(g^{\lambda} \bmod n^2)} \bmod n$。

给定两个密文 $c_1,c_2 \in Z_{n^2}$， $c_1=Enc_{pk}(m_1),c_2=Enc_{pk}(m_2)$

密文加法同态⊕： $c_1 \oplus c_2 = c_1 c_2 \bmod n^2$，则 $c_1 \oplus c_2 = c_1 c_2 \bmod n^2 = Enc_{pk}(m_1 + m_2 \bmod n)$；

随机数与密文乘法同态⊗： $a \in Z_n, c = Enc_{pk}(m)$，则 $a \otimes c = c^a \bmod n^2 = Enc_{pk}(a \cdot m \bmod n)$。

1.2 份额转换协议 MtA

协议描述

输入：Alice 输入保密数据 a，Bob 输入保密数据 b；

输出：Alice 获得保密数据 α，Bob 获得保密数据 β；

功能：不知道对方的保密数据，且 $ab = \alpha + \beta$。

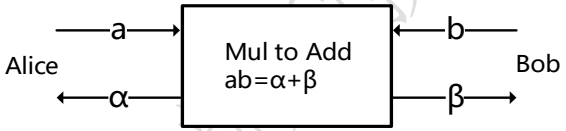

图 1. 份额转换协议

	Alice	Bob
1	Paillier 公钥为 pk，选择随机数 $a \in Z_n$，计算 $c_1 := Enc_{pk}(a)$。 **发送** c_1 与 zk-RangeProof 范围证明 $zkRangeProof\{a \mid a < q^3, c_1 = Enc_{pk}(a)\}$	
2		**接收** c_1 与范围证明 $zkRangeProof\{a \mid a < q^3, c_1 = Enc_{pk}(a)\}$ **校验**范围证明；

		选择 2 个随机数 $b,\beta' \in Z_n$ ， Paillier 同态计算 $c_2 := (b \otimes c_1) \oplus Enc_{pk}(\beta') = Enc_{pk}(ab+\beta' \bmod n), B := g^b$ 。 令加性份额为 β ，其中 $\beta = -\beta' \bmod n$ 。 发送 c_2 和 zk-RangeProof-DL 范围证明 $zkRangeProof\left\{b,\beta' \middle\| b < q^3, \beta' < q^7, c_2 = (b \otimes c_1) \oplus Enc_{pk}(\beta'), B = g^b\right\}$
3	**接收** c_2 和 zk-RangeProof-DL 范围证明 **校验** zk-RangeProof-DL； 解密 c_2 获得 α ，其中 $\alpha = ab+\beta' \bmod n$	
	分析： Alice 与 Bob 不知道对方的保密数据，但是保密数据满足关系 $\alpha+\beta = (ab+\beta')+(-\beta') = ab$	

1.3 零知识证明

1.3.1 零知识证明 1

证明：知道 Pedersen 承诺秘密。

对第 3 步的零知识证明 $ZK\left\{\sigma, l \middle| T = \sigma \cdot G + l \cdot H\right\}$ 补充。

初始化：椭圆曲线生成元为G，标量域为F_r，基域为F_q；

用户秘密为σ, l，公开输入为T, G, H，满足离散对数关系$T = \sigma \cdot G + l \cdot H$。

1：**（承诺）**选择随机数$a, b \in F_r$，计算$R := a \cdot G + b \cdot H$

2：**（挑战）**计算随机数$c := Hash(T, G, H, R) \bmod |F_r|$

3：**（响应）**计算$t := a + c \cdot \sigma \bmod |F_r|, u = b + cl \bmod |F_r|$，发送$(R, t, u)$

4：**（验证）**计算随机数$c := Hash(T, G, H, R) \bmod |F_r|$，如果等式$t \cdot G + u \cdot H == R + c \cdot T$成立，则接受，否则拒绝。

一致性原理如下：

$$t \cdot G + u \cdot H = (a + c \cdot \sigma) \cdot G + (b + cl) \cdot H = R + c \cdot T$$

1.3.2 零知识证明 2

证明：Paillier 加密秘密等于离散对数秘密

对第 5 步的零知识证明$ZK\left\{\eta \middle| \bar{R} = \eta \cdot R, E_{pk}(\eta)\right\}$补充。

证明方选择随机数$r \in \mathbb{Z}_N^*$，对随机数η进行 Paillier 加密$w = \Gamma^{\eta} r^N \bmod N^2$。

计算$y = g^{\eta}$，其中，g为群生成元。

需要证明知道秘密η，满足关系$\eta \in [-q^3, q^3], y = g^{\eta}, w = PaillierEnc_{pk}(\eta)$

承诺：证明方选择随机数$\alpha \in \mathbb{Z}_{q^3}, \beta \in \mathbb{Z}_N^*, \rho \in \mathbb{Z}_{qN}, \gamma \in \mathbb{Z}_{q^3 N}$，计算$z \coloneqq h_1^{\eta} h_2^{\rho} \bmod N, u_1 \coloneqq g^{\alpha}, u_2 \coloneqq \Gamma^{\alpha} \beta^N \bmod N^2, u_3 \coloneqq h_1^{\alpha} h_2^{\gamma} \bmod N$；

挑战：证明方计算送随机数$e \coloneqq hash(g, y, w, z, u_1, u_2, u_3)$；

响应：证明方计算$s_1 \coloneqq e\eta + \alpha, s_2 \coloneqq r^e \beta, s_3 \coloneqq e\rho + \gamma$，发送$z, u_1, u_2, u_3, e, s_1, s_2, s_3$；

校验：验证方进行以下 4 项校验

$$
\begin{aligned}
&u_1 == g^{s_1} y^{-e}, \\
&u_2 == \Gamma^{s_1} s_2^N w^{-e} \bmod N^2, \\
&u_3 == h_1^{s_1} h_2^{s_3} z^{-e} \bmod N, \\
&e == hash(g, y, w, z, u_1, u_2, u_3)
\end{aligned}
$$

一致性原理如下：

（1）sigma 协议校验变形：$g^{s_1} y^{-e} = g^{e\eta+\alpha} g^{-\eta e} = g^{\alpha} = u_1$；

（2）Paillier 加密正确性：$\Gamma^{s_1} s_2^N w^{-e} \bmod N^2 = \Gamma^{e\eta+\alpha} (r^e \beta)^N (\Gamma^{\eta} r^N)^{-e} \bmod N^2 = \Gamma^{\alpha} \beta^N \bmod N^2 = u_2$；

（3）2 个 sigma 协议并行：$h_1^{s_1} h_2^{s_3} z^{-e} \bmod N = h_1^{e\eta+\alpha} h_2^{e\rho+\gamma} (h_1^{\eta} h_2^{\rho})^{-e} \bmod N = h_1^{\alpha} h_2^{\gamma} \bmod N = u_3$；

（4）哈希校验：$e == hash(g, y, w, z, u_1, u_2, u_3)$。

1.3.3 零知识证明 3

证明：Pedersen 承诺秘密等于离散对数秘密

对第 6 步零知识证明 $ZK\left\{\sigma,l\middle|T=\sigma\cdot G+l\cdot H,S=\sigma\cdot R\right\}$ 补充

用户秘密为 σ,l，公开输入为 S,R,T,G,H，满足离散对数关系 $S=\sigma\cdot R,T=\sigma\cdot G+l\cdot H$ 。

1：**（承诺）**选择随机数 $a,b\in F_r$，计算 $A:=a\cdot R,B:=a\cdot G+b\cdot H$

2：**（挑战）**计算随机数 $c:=Hash(S,R,T,G,H,A,B)\bmod|F_r|$

3：**（响应）**计算 $t:=a+c\cdot\sigma\bmod|F_r|,u=b+cl\bmod|F_r|$，发送 (A,B,t,u)

4：**（验证）**计算随机数 $c:=Hash(S,R,T,G,H,A,B)\bmod|F_r|$，如果等式 $t\cdot R==A+c\cdot S,t\cdot G+u\cdot H==B+c\cdot T$ 成立，则接受，否则拒绝。

一致性原理如下：

$$t\cdot R=(a+c\cdot\sigma)\cdot R=A+c\cdot S,$$
$$t\cdot G+u\cdot H=(a+c\cdot\sigma)\cdot G+(b+cl)\cdot H=B+c\cdot T$$

反正，如果 $S=\sigma_1\cdot R,T=\sigma_2\cdot G+l\cdot H,\sigma_1\neq\sigma_2$，则验证等式不成立。

2 设计理念

单方 ECDSA 签名：输入任意消息 M，计算 $m:=Hash(M)$；

选择随机数 $k \in F_r$，**承诺** $R := k^{-1} \cdot G$；

挑战：取 R 横坐标为 $r := R\_x \bmod |F_r|$；

响应：$s := k(m + xr)$，则签名为 (r, s)。

校验：输入消息 M，计算 $m := Hash(M)$；校验 $r, s \in F_r$，计算 $R' := (s^{-1}m) \cdot G + (s^{-1}r) \cdot PK$，取 R' 横坐标为 $r' := R'\_x \bmod |F_r|$；**校验** $r == r'$。如果相等，则接受，否则拒绝。

注释：sigma 零知识证明由数字签名发展而来。

n 方签名核心思想：每个参与方会贡献一个随机数 k_i 和一个私钥加性份额 w_i

方法 1：每个参与方提供随机数 k 的乘性分片

$R := k^{-1} \cdot G$，其中 $k = k_1 \cdot k_2 \cdot ... \cdot k_n$

$s := k(m + xr) = km + r(kx)$，其中 $k = k_1 \cdot k_2 \cdot ... \cdot k_n$，$x = w_1 + w_2 + ... + w_t$

$R := k^{-1} \cdot G = (k_1 \cdot k_2 \cdot ... \cdot k_n)^{-1} \cdot G$

$s := k(m + xr) = km + r(kx) = (k_1 \cdot k_2 \cdot ... \cdot k_n)m + r(k_1 \cdot k_2 \cdot ... \cdot k_n)(w_1 + w_2 + ... + w_n)$

MtA 协议调用次数为 $O(2^n)$，随参与方数量 n 呈指数增加【Li18 使用这种方法，效率较低。】

$$
\begin{aligned}
&\overbrace{k_1 \cdot k_2 \cdot \ldots \cdot k_n}^{(n)elelments} \\
&= (\alpha_{1,2} + \beta_{2,1}) k_3 \cdot k_4 \cdot \ldots \cdot k_n \\
&= \overbrace{\overbrace{\alpha_{1,2} k_3 \cdot k_4 \cdot \ldots \cdot k_n}^{(n-1)-elelment} + \overbrace{\beta_{2,1} k_3 \cdot k_4 \cdot \ldots \cdot k_n}^{(n-1)-elelment}}^{2(n-1)elelments} \\
&= \overbrace{\overbrace{(\alpha_{1,2,3} + \beta_{3,2,1}) \cdot k_4 \cdot \ldots \cdot k_n}^{2(n-2)elelments} + \overbrace{(\beta_{2,1,3} + \alpha_{3,1,2}) \cdot k_4 \cdot \ldots \cdot k_n}^{2(n-2)elelments}}^{2^2(n-2)elelments} \\
&= 2^{n-1}(1)elements
\end{aligned}
$$

方法 2：每个参与方提供随机数 k 的加性分片

$R := k^{-1} \cdot G$，其中 $k = k_1 + k_2 + \ldots + k_n$

$s := k(m + xr) = km + r(kx)$，其中 $k = k_1 + k_2 + \ldots + k_n$，$x = w_1 + w_2 + \ldots + w_t$

$R := k^{-1} \cdot G = (k_1 + k_2 + \ldots + k_n)^{-1} \cdot G$

$s := k(m + xr) = km + r(kx) = (k_1 + k_2 + \ldots + k_n)m + r(k_1 + k_2 + \ldots + k_n)(w_1 + w_2 + \ldots + w_t)$

MtA 协议调用次数为 $O(n^2)$，随参与方数量 n 呈多项式增加。【GG18/20 的方法效率更高】

分析：用户 P_1, P_2 各自选择 2 个随机数 $(k_1, \gamma_1), (k_2, \gamma_2)$，计算目标为 (R, s)，如下展开

$$
\begin{aligned}
R &= k^{-1} \cdot G = (k\gamma)^{-1}\gamma \cdot G \\
&= \left((k_1 + k_2)(\gamma_1 + \gamma_2)\right)^{-1} \cdot (\gamma_1 + \gamma_2) \cdot G \\
&= \left(k_1\gamma_1 + (k_1\gamma_2) + (k_2\gamma_1) + k_2\gamma_2\right)^{-1} \cdot (\Gamma_1 + \Gamma_2) \\
&= \left(k_1\gamma_1 + (\alpha_{1,2} + \beta_{2,1}) + (\alpha_{2,1} + \beta_{1,2}) + k_2\gamma_2\right)^{-1} \cdot (\Gamma_1 + \Gamma_2) \\
&= (\delta_1 + \delta_2)^{-1} \cdot (\Gamma_1 + \Gamma_2)
\end{aligned}
$$

用户 P_1, P_2 各自广播 $(\delta_1, \Gamma_1)(\delta_2, \Gamma_2)$ 而不泄露 $(k_1, \gamma_1), (k_2, \gamma_2)$。

$$
\begin{aligned}
s &= k(m + xr) \\
&= mk + rkx \\
&= m(k_1 + k_2) + r(k_1 + k_2)(w_1 + w_2) \\
&= m(k_1 + k_2) + r\left(k_1w_1 + (k_1w_2) + (k_2w_1) + k_2w_2\right) \\
&= m(k_1 + k_2) + r\left(k_1w_1 + (u_{1,2} + v_{2,1}) + (u_{2,1} + v_{1,2}) + k_2w_2\right) \\
&= m(k_1 + k_2) + r(\sigma_1 + \sigma_2) \\
&= (mk_1 + r\sigma_1) + (mk_2 + r\sigma_2) \\
&= s_1 + s_2
\end{aligned}
$$

用户 P_1, P_2 各自广播 s_1, s_2 而不泄露 $(k_1, w_1), (k_2, w_2)$。

因此，用户 P_1, P_2 各自的**签名加性份额**为 $sig_1 = \{\delta_1, \Gamma_1, s_1\}, sig_2 = \{\delta_2, \Gamma_2, s_2\}$

3 分布式密钥生成

	P_1	P_2	P_3
1	生成 Paillier 密钥对 (N_1, p_1, q_1) 选择原始随机数 $u_1 \in [1, n-1]$ 计算椭圆曲线随机点、承诺与打开承诺 $U_1 := u_1 \cdot G$ $(KGC_1, KGD_1) = Com(U_1)$	生成 Paillier 密钥对 (N_2, p_2, q_2) 选择原始随机数 $u_2 \in [1, n-1]$ 计算椭圆曲线随机点、承诺与打开承诺 $U_2 := u_2 \cdot G$ $(KGC_2, KGD_2) = Com(U_2)$	生成 Paillier 密钥对 (N_3, p_3, q_3) 选择原始随机数 $u_3 \in [1, n-1]$ 计算椭圆曲线随机点、承诺与打开承诺 $U_3 := u_3 \cdot G$ $(KGC_3, KGD_3) = Com(U_3)$
	广播承诺 KGC_1 与 Paillier 公钥 N_1	广播承诺 KGC_2 与 Paillier 公钥 N_2	广播承诺 KGC_3 与 Paillier 公钥 N_3
2	广播打开承诺 KGD_1	广播打开承诺 KGD_2	广播打开承诺 KGD_3
3	三方均校验另外两方承诺的正确性， 然后计算公共公钥： $PK = U_1 + U_2 + U_3$		
4	选择随机数 $a_1 \in [1, n-1]$， 构造 2 阶多项式 $p_1(x) = u_1 + x \cdot a_1$ **门限为 2**	选择随机数 $a_2 \in [1, n-1]$， 构造 2 阶多项式 $p_2(x) = u_2 + x \cdot a_2$ **门限为 2**	选择随机数 $a_3 \in [1, n-1]$ 构造 2 阶多项式 $p_3(x) = u_3 + x \cdot a_3$ **门限为 2**

	构造拉格朗日冗余： 存储 $p_1(1)$，将 $p_1(2), p_1(3)$ 保密发给对应用户 P_2, P_3 计算 **Feldman 校验元组** $A_1 := a_1 \cdot G$ 广播 A_1	**构造拉格朗日冗余：**存储 $p_2(2)$，将 $p_2(1), p_2(3)$ 保密发给对应用户 P_1, P_3 计算 **Feldman 校验元组** $A_2 := a_2 \cdot G$ 广播 A_2	**构造拉格朗日冗余：**存储 $p_3(3)$，将 $p_3(1), p_3(2)$ 保密发给对应用户 P_1, P_2 计算 **Feldman 校验元组** $A_3 := a_3 \cdot G$ 广播 A_3
5	拥有保密数据为 $p_1(1) = u_1 + a_1$ $p_2(1) = u_2 + a_2$ $p_3(1) = u_3 + a_3$	拥有保密数据 $p_1(2) = u_1 + 2a_1$ $p_2(2) = u_2 + 2a_2$ $p_3(2) = u_3 + 2a_3$	拥有保密数据 $p_1(3) = u_1 + 3a_1$ $p_2(3) = u_2 + 3a_2$ $p_3(3) = u_3 + 3a_3$
6	进行 Feldman 校验 $p_1(1) \cdot G == U_1 + A_1$ $p_2(1) \cdot G == U_2 + A_2$ $p_3(1) \cdot G == U_3 + A_3$	进行 Feldman 校验 $p_1(2) \cdot G == U_1 + 2A_1$ $p_2(2) \cdot G == U_2 + 2A_2$ $p_3(2) \cdot G == U_3 + 2A_3$	进行 Feldman 校验 $p_1(3) \cdot G == U_1 + 3A_1$ $p_2(3) \cdot G == U_2 + 3A_2$ $p_3(3) \cdot G == U_3 + 3A_3$
7	计算**分片私钥** x_1	计算**分片私钥** x_2	计算**分片私钥** x_3

	$x_1 := \sum_{i=1}^{3} p_i(1) \bmod n$ $= \sum_{i=1}^{3} (u_i + a_i) \bmod n$ $= sk + \sum_{i=1}^{3} a_i \bmod n$	$x_2 := \sum_{i=1}^{3} p_i(2) \bmod n$ $= \sum_{i=1}^{3} (u_i + 2a_i) \bmod n$ $= sk + \cdot \sum_{i=1}^{3} 2a_i \bmod n$	$x_3 := \sum_{i=1}^{3} p_i(3) \bmod n$ $= \sum_{i=1}^{3} (u_i + 3a_i) \bmod n$ $= sk + \sum_{i=1}^{3} 3a_i \bmod n$
8	计算**分片公钥** $X_1 := PK + \left(\sum_{i=1}^{3} a_i \right) \cdot G$ 广播分片公钥 X_1	计算**分片公钥** $X_2 := PK + \left(\sum_{i=1}^{3} 2a_i \right) \cdot G$ 广播分片公钥 X_2	计算**分片公钥** $X_3 := PK + \left(\sum_{i=1}^{3} 3a_i \right) \cdot G$ 广播分片公钥 X_3
9	公共公钥 PK 与分片公钥 X_1, X_2, X_3 之间满足**拉格朗日插值校验**（三方均执行） $\lambda_{1,2} \cdot X_1 + \lambda_{2,1} \cdot X_2 == PK,$ $\lambda_{1,3} \cdot X_1 + \lambda_{3,1} \cdot X_3 == PK,$ $\lambda_{2,3} \cdot X_2 + \lambda_{3,2} \cdot X_3 == PK$ 一致性原理如下：		

$$\lambda_{i,j}\cdot X_i+\lambda_{j,i}\cdot X_j=\frac{j}{j-i}\cdot X_i+\frac{i}{i-j}\cdot X_j$$
$$=\frac{j}{j-i}\cdot\left(PK+\left(i\cdot\sum_{i=1}^{3}a_i\right)\cdot G\right)+\frac{-i}{j-i}\cdot\left(PK+\left(j\cdot\sum_{i=1}^{3}a_i\right)\cdot G\right)$$
$$=\frac{j-i}{j-i}\cdot PK+\left(\frac{ji}{j-i}\cdot\sum_{i=1}^{3}a_i\right)\cdot G+\left(\frac{-ji}{j-i}\cdot\sum_{i=1}^{3}a_i\right)\cdot G$$
$$=PK$$

其中，$\lambda_{i,j},\lambda_{j,i}$为任意两方对应的拉格朗日插值系数。

注释 1：三方的分片私钥为x_1,x_2,x_3，能够通过拉格朗日插值计算公共私钥sk（但是不计算），而是计算**分片签名**。

$$\lambda_{i,j}\cdot x_i+\lambda_{j,i}\cdot x_j=\frac{j}{j-i}\cdot x_i+\frac{i}{i-j}\cdot x_j$$
$$=\frac{j}{j-i}\cdot\left(sk+\left(i\cdot\sum_{i=1}^{3}a_i\right)\right)+\frac{-i}{j-i}\cdot\left(sk+\left(j\cdot\sum_{i=1}^{3}a_i\right)\right)$$
$$=\frac{j-i}{j-i}\cdot sk+\left(\frac{ji}{j-i}\cdot\sum_{i=1}^{3}a_i\right)+\left(\frac{-ji}{j-i}\cdot\sum_{i=1}^{3}a_i\right)$$
$$=sk$$

注释 2：上述过程是分布式密钥生成。可以假设存在一个**可信第三方**，**可信第三方**运行一个**公共多项式**

$$p(x)=(u_1+u_2+u_3)+(a_1+a_2+a_3)\cdot x^1+(b_1+b_2+b_3)\cdot x^2=sk+(a_1+a_2+a_3)\cdot x^1+(b_1+b_2+b_3)\cdot x^2$$

当$x=1,2,3$，则计算出**分片私钥**x_1,x_2,x_3，保密发送给各个参与方。

10	Paillier 零知识证明知道对应的私钥 p_1, q_1 Schnorr 零知识证明知道对应的分片私钥 x_1	Paillier 零知识证明知道对应的私钥 p_2, q_2 Schnorr 零知识证明知道对应的分片私钥 x_2	Paillier 零知识证明知道对应的私钥 p_3, q_3 Schnorr 零知识证明知道对应的分片私钥 x_3
11	三方均**校验**其他两方广播过来的 2 个零知识证明		
	最终结果：三方均拥有：公共公钥 PK 、3 个分片公钥 X_1, X_2, X_3、3 个 Pailler 公钥 N_1, N_2, N_3		
	拥有以下 3 项保密信息： 1. Paillier 私钥 (p_1, q_1) 2. 原始随机数 u_1 3. 分片私钥 x_1	拥有以下 3 项保密信息： 1. Paillier 私钥 (p_2, q_2) 2. 原始随机数 u_2 3. 分片私钥 x_2	拥有以下 3 项保密信息： 1. Paillier 私钥 (p_3, q_3) 2. 原始随机数 u_3 3. 分片私钥 x_3
	令 $w_1 = \lambda_1 \cdot x_1$	令 $w_2 = \lambda_2 \cdot x_2$	令 $w_3 = \lambda_3 \cdot x_3$
	注释：公共私钥 sk 不出现，满足以下**拉格朗日插值校验** $$sk = \lambda_1 \cdot x_1 + \lambda_2 \cdot x_2 + \lambda_3 \cdot x_3$$ $$= w_1 + w_2 + w_3$$ 其中 w_1, w_2, w_3 称为**分片私钥加性份额。**三个各自基于分片私钥和拉格朗日插值系数计算**分片私钥加性份额**。		

	3 个用户不重构公共私钥 sk，而是使用私钥加性份额与随机数 k，计算签名加性份额 sig_1, sig_2, sig_3，广播签名加性份额，累加后得到完整签名 $sig := sig_1 + sig_2 + sig_3$

4 方案 1：单轮在线、有匿名中断

	性质：单轮在线、允许匿名中断，不知道谁是错误方	
	P_1	P_2
	三方各自输入输入 2 份保密的原始随机数 $(k_1, k_2), (\gamma_1, \gamma_2)$	
1	选择两个随机数 $(k_1, \gamma_1) \in [1, n-1]$	选择两个随机数 $(k_2, \gamma_2) \in [1, n-1]$
	计算椭圆曲线随机点、承诺与打开承诺 $\Gamma_1 := \gamma_1 \cdot G$ $(C_1, D_1) = Com(\Gamma_1)$	计算椭圆曲线随机点、承诺与打开承诺 $\Gamma_2 := \gamma_2 \cdot G$ $(C_2, D_2) = Com(\Gamma_2)$
	广播承诺 C_1	广播承诺 C_2
	MtA 份额转换协议开始	
2	$\alpha_{1,2} \leftarrow \left\{P_1(k_1) \overset{\text{MtA}}{\rightleftarrows} P_2(\gamma_2)\right\}(k_1\gamma_2)$	$\beta_{2,1} \leftarrow \left\{P_1(k_1) \overset{\text{MtA}}{\rightleftarrows} P_2(\gamma_2)\right\}(k_1\gamma_2)$

	$\beta_{1,2} \leftarrow \left\{P_2(k_2) \overset{\text{MtA}}{\rightleftarrows} P_1(\gamma_1)\right\}(k_2\gamma_1)$	$\alpha_{2,1} \leftarrow \left\{P_2(k_2) \overset{\text{MtA}}{\rightleftarrows} P_1(\gamma_1)\right\}(k_2\gamma_1)$
	保密数据为(k_1, w_1)	保密数据为(k_2, w_2)
	$u_{1,2} \leftarrow \left\{P_1(k_1) \overset{\text{MtA}}{\rightleftarrows} P_2(w_2)\right\}(k_1w_2)$	$v_{2,1} \leftarrow \left\{P_1(k_1) \overset{\text{MtA}}{\rightleftarrows} P_2(w_2)\right\}(k_1w_2)$
	$v_{1,2} \leftarrow \left\{P_2(k_2) \overset{\text{MtA}}{\rightleftarrows} P_1(w_1)\right\}(k_2w_1)$	$u_{2,1} \leftarrow \left\{P_2(k_2) \overset{\text{MtA}}{\rightleftarrows} P_1(w_1)\right\}(k_2w_1)$
	计算 $\delta_1 := k_1\gamma_1 + \alpha_{1,2} + \beta_{1,2}$ $\sigma_1 := k_1w_1 + u_{1,2} + v_{2,1}$	计算 $\delta_2 := \beta_{2,1} + \alpha_{2,1} + k_2\gamma_2$ $\sigma_2 := k_2w_2 + u_{2,1} + v_{2,1}$
3	**为计算 R 做准备**	
	广播δ_1	广播δ_2
	计算$\delta^{-1} := (k\gamma)^{-1} = (\delta_1 + \delta_2)^{-1}$	
4	打开承诺D_1	打开承诺D_2
	校验承诺Γ_1, Γ_2	

<table>
<tr><td></td><td colspan="2">计算 ECDSA 中的$R := \delta^{-1} \cdot (\Gamma_1 + \Gamma_2)$，获得横坐标$r$

一致性原理如下：$R = \delta^{-1} \cdot \Gamma = \delta^{-1}\gamma \cdot G = (k\gamma)^{-1}\gamma \cdot G = k^{-1} \cdot G$

（CMP 图 7 将第 4 步与第 5/6 步换位置）</td></tr>
<tr><td></td><td colspan="2">**为校验δ做准备**</td></tr>
<tr><td rowspan="3">5</td><td>计算并广播$\Lambda_1 = k_1 \cdot \Gamma$

（CMP 图 7 和图 9 与此处相同）</td><td>计算并广播$\Lambda_2 = k_2 \cdot \Gamma$

（CMP 图 7 和图 9 与此处相同）</td></tr>
<tr><td>Paillier 公钥E_1对随机数k_1加密$E_1(k_1)$</td><td>Paillier 公钥E_2对随机数k_2加密$E_2(k_2)$</td></tr>
<tr><td>计算并广播零知识证明
$proof_{5,1} = ZK\{k_1 | \Lambda_1 = k_1 \cdot \Gamma, E_1(k_1)\}$</td><td>计算并广播零知识证明
$proof_{5,2} = ZK\{k_2 | \Lambda_2 = k_2 \cdot \Gamma, E_2(k_2)\}$</td></tr>
<tr><td rowspan="2">6</td><td colspan="2">**校验**零知识证明$proof_{5,1}, proof_{5,2}$

计算$\Lambda := \Lambda_1 + \Lambda_2 = (k_1 + k_2) \cdot \Gamma = k \cdot \Gamma$

校验Λ的一致性：
$\Lambda == \delta \cdot G$
一致性原理如下：$\delta \cdot G = (\delta k) \cdot R = k \cdot \Gamma$
（CMP 图 7 和图 9 与此处相同，不涉及消息 msg，记为 Pre-Signing）</td></tr>
<tr><td>计算并广播$s_1 = mk_1 + r\sigma_1$</td><td>计算并广播$s_2 = mk_2 + r\sigma_2$</td></tr>
</table>

	计算 $s = s_1 + s_2$ 校验 (r, s) 的有效性 **如果错误广播 s_i，则中断，不知道谁是错误方，所以是匿名中断。**

5 方案 2：可识别中断

	两个用户签名（完整版）	
	P_1	P_2
	椭圆曲线生成元为 G, H **MtA 份额转换协议开始（份额转换协议中包含 zk 校验）**	
1	选择两个随机数 (k_1, γ_1)	选择两个随机数 (k_2, γ_2)
	计算：$\Gamma_1 := \gamma_1 \cdot G$ $(C_1, D_1) = Com(\Gamma_1)$	计算：$\Gamma_2 := \gamma_2 \cdot G$ $(C_2, D_2) = Com(\Gamma_2)$
	广播承诺 C_1	广播承诺 C_2
2	$\alpha_{1,2} \leftarrow \left\{P_1(k_1) \overset{\text{MtA}}{\rightleftarrows} P_2(\gamma_2)\right\}(k_1\gamma_2)$	$\beta_{2,1} \leftarrow \left\{P_1(k_1) \overset{\text{MtA}}{\rightleftarrows} P_2(\gamma_2)\right\}(k_1\gamma_2)$

	$\beta_{1,2} \leftarrow \left\{P_2(k_2) \overset{\text{MtA}}{\rightleftarrows} P_1(\gamma_1)\right\}(k_2\gamma_1)$	$\alpha_{2,1} \leftarrow \left\{P_2(k_2) \overset{\text{MtA}}{\rightleftarrows} P_1(\gamma_1)\right\}(k_2\gamma_1)$
	保密数据为(k_1, w_1)	保密数据为(k_2, w_2)
	$u_{1,2} \leftarrow \left\{P_1(k_1) \overset{\text{MtA}}{\rightleftarrows} P_2(w_2)\right\}(k_1w_2)$	$v_{2,1} \leftarrow \left\{P_1(k_1) \overset{\text{MtA}}{\rightleftarrows} P_2(w_2)\right\}(k_1w_2)$
	$v_{1,2} \leftarrow \left\{P_2(k_2) \overset{\text{MtA}}{\rightleftarrows} P_1(w_1)\right\}(k_2w_1)$	$u_{2,1} \leftarrow \left\{P_2(k_2) \overset{\text{MtA}}{\rightleftarrows} P_1(w_1)\right\}(k_2w_1)$
	计算 $\delta_1 := k_1\gamma_1 + \alpha_{1,2} + \beta_{1,2}$ $\sigma_1 := k_1w_1 + u_{1,2} + v_{1,2}$	计算 $\delta_2 := \beta_{2,1} + \alpha_{2,1} + k_2\gamma_2$ $\sigma_2 := k_2w_2 + u_{2,1} + v_{2,1}$
3	**为计算 R 做准备**	
	广播δ_1	广播δ_2
	计算$\delta^{-1} := (k\gamma)^{-1} = (\delta_1 + \delta_2)^{-1}$	
	计算离散对数T_1与零知识证明 $T_1 = \sigma_1 \cdot G + l_1 \cdot H$ $proof_{3,1} = ZK\left\{\sigma_1, l_1 \middle\| T_1 = \sigma_1 \cdot G + l_1 \cdot H\right\}$	计算离散对数T_2与零知识证明 $T_2 = \sigma_2 \cdot G + l_2 \cdot H$ $proof_{3,2} = ZK\left\{\sigma_2, l_2 \middle\| T_2 = \sigma_2 \cdot G + l_2 \cdot H\right\}$

<table>
<tr><td></td><td>广播 $T_1, proof_{3,1}$</td><td>广播 $T_2, proof_{3,2}$</td></tr>
<tr><td rowspan="2">4</td><td>zk 校验 $proof_{3,1}$

打开承诺 D_1</td><td>zk 校验 $proof_{3,2}$

打开承诺 D_2</td></tr>
<tr><td colspan="2">校验打开承诺 Γ_1, Γ_2

计算 ECDSA 中的 $R := \delta^{-1} \cdot (\Gamma_1 + \Gamma_2)$，获得横坐标 r</td></tr>
<tr><td></td><td colspan="2">为校验 R 做准备</td></tr>
<tr><td rowspan="4">5</td><td>计算并广播 $\bar{R}_1 = k_1 \cdot R$</td><td>计算并广播 $\bar{R}_2 = k_2 \cdot R$</td></tr>
<tr><td>Paillier 公钥 E_1 对随机数 k_1 加密 $E_1(k_1)$</td><td>Paillier 公钥 E_2 对随机数 k_2 加密 $E_2(k_2)$</td></tr>
<tr><td>计算并广播零知识证明
$ZK\left\{k_1 \middle| \bar{R}_1 = k_1 \cdot R, E_1(k_1)\right\}$

$proof_{5,1} = ZK\left\{k_1 \middle| \bar{R}_1 = k_1 \cdot R, E_1(k_1)\right\}$</td><td>计算并广播零知识证明
$ZK\left\{k_2 \middle| \bar{R}_2 = k_2 \cdot R, E_2(k_2)\right\}$

$proof_{5,2} = ZK\left\{k_2 \middle| \bar{R}_2 = k_2 \cdot R, E_2(k_2)\right\}$</td></tr>
<tr><td colspan="2">zk 校验 $proof_{5,1}, proof_{5,2}$

校验等式 $G == \bar{R}_1 + \bar{R}_2$

一致性原理如下：</td></tr>
</table>

	$\bar{R}_1+\bar{R}_2=k_1\cdot R+k_2\cdot R=(k_1+k_2)\cdot R=k\cdot R=G$	
	为校验σ做准备	
6	计算并广播$S_1=\sigma_1\cdot R$	计算并广播$S_2=\sigma_2\cdot R$
	计算并广播零知识证明 zk-elog $proof_{6,1}=ZK\left\{\sigma_1,l_1\middle\vert\begin{matrix}T_1=\sigma_1\cdot G+l_1\cdot H,\\S_1=\sigma_1\cdot R\end{matrix}\right\}$	计算并广播零知识证明 $proof_{6,2}=ZK\left\{\sigma_2,l_2\middle\vert\begin{matrix}T_2=\sigma_2\cdot G+l_2\cdot H,\\S_2=\sigma_2\cdot R\end{matrix}\right\}$
	校验零知识证明 $proof_{6,1}, proof_{6,2}$ **校验等式** $PK==S_1+S_2$ 一致性原理如下： $S_1+S_2=\sigma_1\cdot R+\sigma_2\cdot R=(\sigma_1+\sigma_2)\cdot R=\sigma\cdot R=kx\cdot(k^{-1}G)=x\cdot G=PK$	
7	计算并广播签名份额$s_1=mk_1+r\sigma_1$	计算并广播签名份额$s_2=mk_2+r\sigma_2$
	计算$s=s_1+s_2$ 校验(r,s)的有效性	

6 识别错误方

上述协议有以下 8 个校验

- **校验①**：第 2 步的**份额转换协议**中的 zk 范围校验
- **校验②**：第 3 步的 $ZK\{\sigma, l\}$ 的 zk 校验
- **校验③**：第 4 步的**打开承诺校验**
- **校验④**：第 5 步的 $ZK\{k_1 | \bar{R}_1 = k_1 \cdot R, E_1(k_1)\}$ 的 zk 校验
- **校验⑤**：第 5 步的 $G == \bar{R}_1 + \bar{R}_2$
- **校验⑥**：第 6 步的 $ZK\{\sigma_1, l_1 | T_1 = \sigma_1 \cdot G + l_1 \cdot H, S_1 = \sigma_1 \cdot R\}$ 的 zk 校验
- **校验⑦**：第 6 步的 $PK == S_1 + S_2$
- **校验⑧**：第 7 步的 (r, s) 的校验

情况 1：校验①②③④⑥为 zk 校验和承诺校验，对应每个参与方 P_i。如果校验失败，则能够识别错误方。

情况 2：如果校验⑧失败，此时每个参与方已经广播了份额 s_i，使用份额校验 $s_i \cdot R == m \cdot \bar{R}_i + r \cdot S_i$，识别错误方。

一致性原理如下：$s_i \cdot R = (mk_i + r\sigma_i)R = m \cdot \bar{R}_i + r \cdot S_i$

情况 3：如果校验⑤⑦失败。由于⑤里面的 $\bar{R}_1, \bar{R}_2$ 包含 δ_1, δ_2，⑦里面的 S_1, S_2 包含了 σ_1, σ_2。份额转换协议校验成功，则说明参与方有正确的 δ_i, σ_i。因此，⑤⑦校验的失败，表明参与方发送了错误的 δ_i, σ_i。如果参与方广播错误的 δ_i，则导致⑤校验失败；如果参与方广播错误的 σ_i，导致⑦校验失败。因此，要添加 zk，确保参与方发送 δ_i, σ_i 的一致性。

- 第 1 个 zk：参与方 Pi 在 2 次调用份额转换协议 $k_i \cdot \gamma_j, k_i \cdot w_j$，确保这 2 个 k_i 是相等的。
- 第 2 个 zk：份额转换协议 $k_i \cdot w_j$ 中的 w_j 与公钥加性份额 $W_j = w_j \cdot G$ 中的 w_j 是相同的。
- 第 3 个 zk：份额转换协议 $k_i \cdot \gamma_j$ 中的 γ_j 与公开的离散对数点 $\Gamma_j = \gamma_j \cdot G$ 中的 γ_j 是相同的。
- 第 4 个 zk：阶段 3 公开的 δ_i 与份额转换协议结果 $\delta_i := k_i\gamma_i + \alpha_{i,j} + \beta_{i,j}$ 是相同的。
- 第 5 个 zk：阶段 6 公开的 $S_i = \sigma_i \cdot R$ 中包含的 σ_i 与份额转换协议结果 $\sigma_i := k_i w_i + u_{i,j} + v_{i,j}$ 是相同的。

情况 3.1：如果校验⑤失败： 就不执行第 8 步的广播 s_i。此时要求所有参与方都广播随机数份额 k_i, γ_i。（只要不广播 s_i，私钥加性份额 w_i 没泄露就行），那么 MtA 中的随机数加性份额 $\alpha_{i,j}, \beta_{i,j}$ 可以广播，也可以使用 k_i, γ_i 计算出来，则 $\delta_i := k_i\gamma_i + \alpha_{i,j} + \beta_{i,j}$ 也能计算出来，与第 5 步参与方广播的 δ_i 校验一致性，识别错误方。

情况 3.2：如果校验⑦校验失败： 由于 $\sigma_i := k_i w_i + u_{i,j} + v_{i,j}$ 且私钥加性份额 w_i 不能泄露。所以仅广播 $k_i, u_{i,j}$，而保密 $w_i, v_{i,j}$。分析一个方程有 2 个未知数，则不泄露私钥加性份额。

Paillier 加密算法： 给定消息 $m \in Z_n$ 和随机数 $r \in Z_n^*$，计算密文 $c := g^m \cdot r^n \bmod n^2$。

给定密文 C 和私钥 p,q，能够解密出消息 m，还能计算 $r^n := C / g^m \bmod n^2$，再计算 n 次剩余，得出随机数 r。

MtA 协议中，协议开始 Paillier 加密了 k_i，协议结束时 Paillier 密文 C1 解密获得 $u_{i,j}$。

则基于 Paillier 密文 C1 和 $g,u_{i,j},r,n$ 校验密文承诺 C1 的一致性，确保 $u_{i,j}$ 正确。**【论文 CGGMP20--zk-Paillier-Dec-q】**

确定公开的 $k_i,u_{i,j}$ 正确性后，由于**公钥加性份额** $W_i \coloneqq w_i \cdot G$ 是公开的，所以可以基于份额转换协议等式 $k_i w_j = u_{i,j} + v_{j,i}$，计算 $v_{j,i}$ 的离散对数 $v_{j,i} \cdot G = u_{i,j} \cdot G - k_i \cdot W_j$，则继续计算 $\sigma_i \cdot G \coloneqq k_i \cdot W_i + u_{i,j} \cdot G + v_{i,j} \cdot G$。要求每个参与方 pi 进行 zk 证明知道 σ_i 满足该离散对数关系且与公开的 $S_i = \sigma_i \cdot R$ 中的 σ_i 是相等的。zk 证明失败，则是错误方。

lynndell 博士 新火科技 密码学专家 lynndell2010@gmail.com