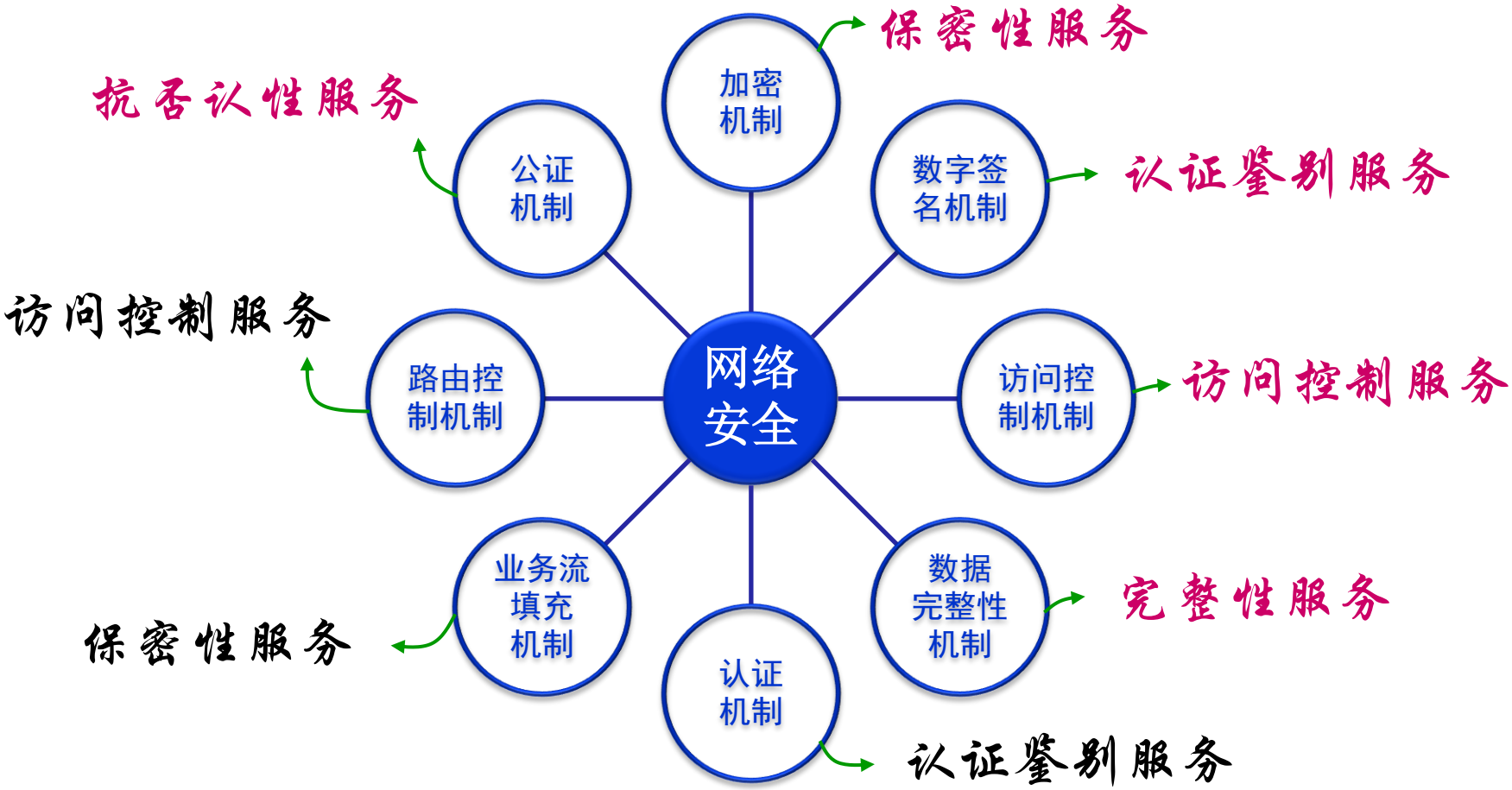
经典密码算法在隐私保护中的应用

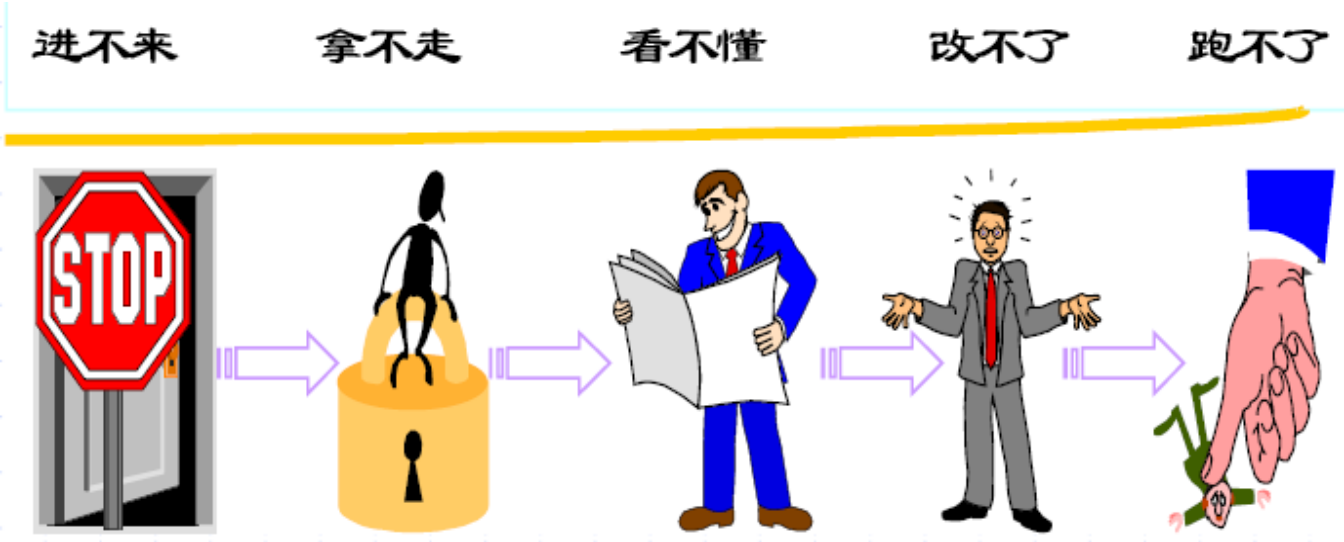
段桂华

中南大学计算机学院

duangh@csu.edu.cn

五类安全服务与八类安全机制





- 对称密码算法
- 公钥密码算法
- 数字摘要算法
- 数字签名算法

- 保密通信协议
- 密钥协商协议
- 身份鉴别协议
- 数字签名协议
- 秘密共享协议
- 安全计算协议

- …

双线性对(Weil pairing)的性质

- **双线性**:对于任意$P,Q,R\in G_1$和$a,b\in Z_q^*$,有

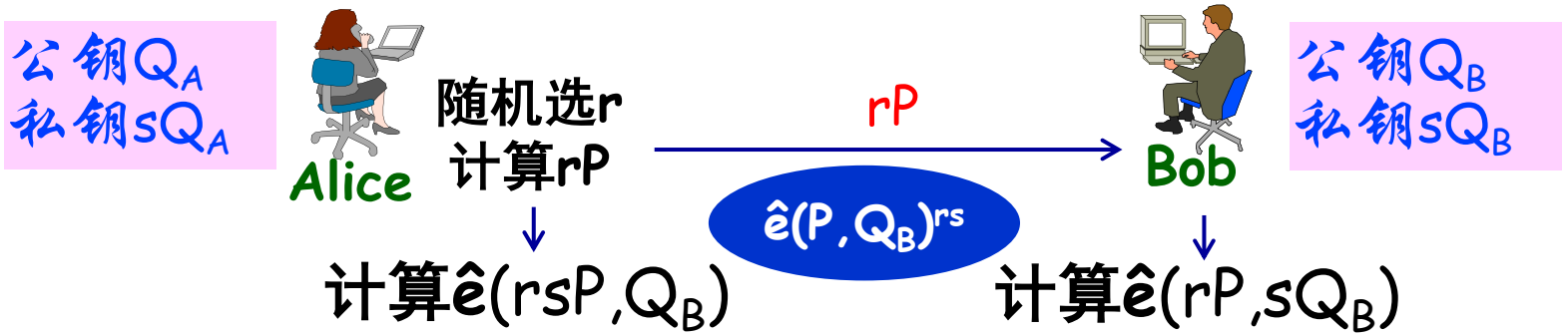
- $\hat{e}(P,P)\neq 1$
- $\hat{e}(P+Q,R)=\hat{e}(P,R)\hat{e}(Q,$
- $\hat{e}(R,P+Q)=\hat{e}(R,P)\hat{e}(R,$
- $\hat{e}(aP,bQ)=\hat{e}(abP,Q)=\hat{e}($

- $\hat{e}(P,P)\neq 1$
- $\hat{e}(PQ,R)=\hat{e}(P,R)\hat{e}(Q,R)$
- $\hat{e}(R,PQ)=\hat{e}(R,P)\hat{e}(R,Q)$
- $\hat{e}(P^a,Q^b)=\hat{e}(P^{ab},Q)=\hat{e}(P,Q^{ab})=\hat{e}(P,Q)^{ab}$

- **非退化性**:存在$P,Q\in G_1$,使得$\hat{e}(P,Q)\neq 1$.
- **对称性**:存在$P,Q\in G_1$,使得$\hat{e}(P,Q)=\hat{e}(Q,P)$.
- **可计算性**:对于任意的$P,Q\in G_1$,存在一个高效的算法计算$\hat{e}(P,Q)$.

基于双线性对的密钥协商协议

- PKG选择s,公开P,sP:



- PKG公开P:

算法	公钥y和私钥x关系	加密m	解密c
RSA	$x=y^{-1} \bmod \varphi(n)$	$c=m^y \bmod n$	$m=c^x \bmod n$
ElGamal	$y=g^x \bmod p$	$a=g^k \bmod p$ $b=m\cdot y^k \bmod p$	$b\cdot a^{-x} \bmod p$
ECC	$Y=xG$	$A=kG \quad B=m+kY$	$B-xA$

算法变又

密钥关系--私钥x,公钥 $y=g^x \bmod p$

签名过程--签名方对消息m签名得到 $s=m^x \bmod p$

验证过程-- 验证方 ① $w=s^a\cdot e^b$ → 签名方

验证方 ← ②$v=w^z \bmod p$ 签名方

选a,b

③

验证$v=m^a\cdot g^b \bmod p$

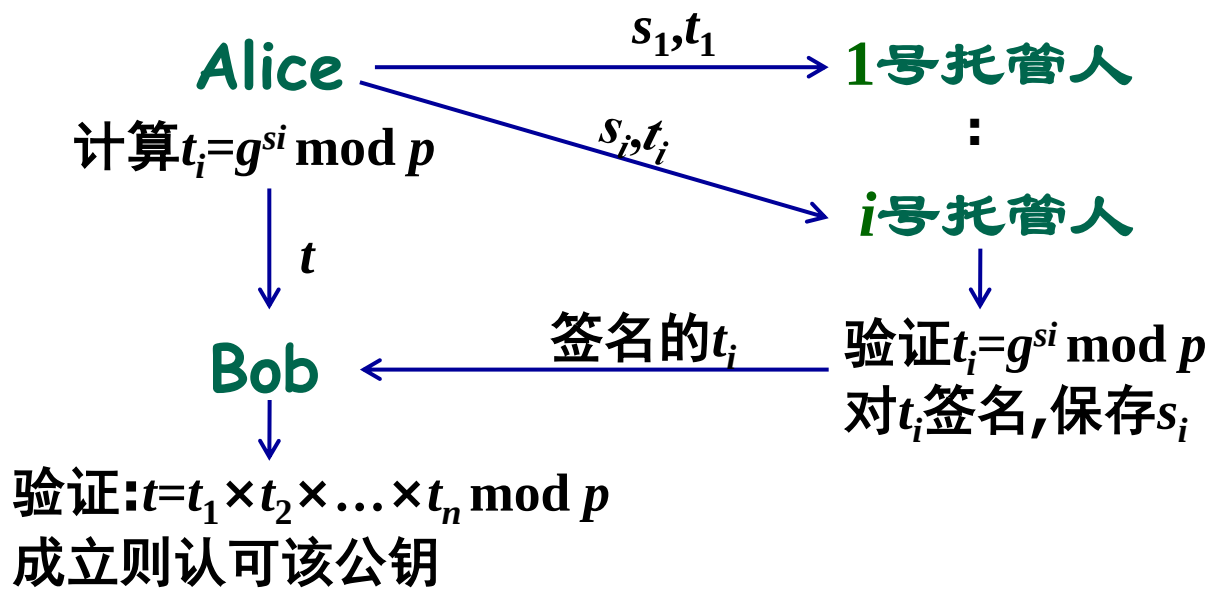
$z=x^{-1} \bmod p-1$

RSA算法的拓展

- **RSA算法**:模数$n=pq$,公钥和私钥满足$xy=1 \bmod \varphi(n)$.
  - **加密**消息m → $c=m^y \bmod n$
  - **解密**密文c → $m=c^x \bmod n$
- **算法拓展**:模数$n=pq$, $k_1 \times k_2 \times \ldots \times k_m \equiv 1 \bmod \varphi(n)$
  - **加密**消息m → 用其中若干个k_i加密
  - **解密**密文c → 用剩下的k_j解密

ElGamal算法拓展

- Alice将私钥s分割成n个：$s=(s_1+s_2+\ldots+s_n)$
- 公钥为：$t=g^s \bmod p$



Shamir门限方案

(k,n)门限方案,秘密分割成n份,≥k ($k<n$)份可恢复.

秘密分割

1. 构建k-1次多项式 $f(x)=m+a_1x+a_2x^2+\ldots+a_{k-1}x^{k-1} \bmod p$
2. 计算$D_i=f(i)$, $i=1,\ldots,n$
3. 将$D_1, D_2, \ldots, D_n$分给n个人保管

(3,5)门限方案

1. 构建2次多项式为:$13+10x+2x^2 \bmod 17$
2. 计算5个秘密份额为: $D_1=8, D_2=7, D_3=10, D_4=0, D_5=11$
3. 将D_1, D_2, D_3, D_4, D_5分给5个人保管

秘密恢复

1.获取k个秘密份额$D_{j1}, D_{j2}, \ldots, D_{jk}$

2.计算 $f(x)=\sum_{i=1}^{k}(D_{j_i}\times\prod_{s=1,s\neq i}^{k}\frac{x-j_s}{j_i-j_s}) \mod p$

3.恢复的秘密$m=f(0)$

拉格朗日插值多项式公式

(3,5)门限方案

1.获取3个秘密份额:$D_1=8, D_3=10, D_5=11$

2.根据秘密分割原理可假设 $f(x)=m+a_1x+a_2x^2 \mod 17$

则:
$$f(x)=8\frac{(x-3)(x-5)}{(1-3)(1-5)}+10\frac{(x-1)(x-5)}{(3-1)(3-5)}+11\frac{(x-1)(x-3)}{(5-1)(5-3)}$$

$$=13+10x+2x^2 \mod 17$$

3.求得到秘密$m=f(0)=13$

$8=m+a_1+a_2 \mod 17$
$10=m+3a_1+9a_2 \mod 17$
$11=m+5a_1+25a_2 \mod 17$

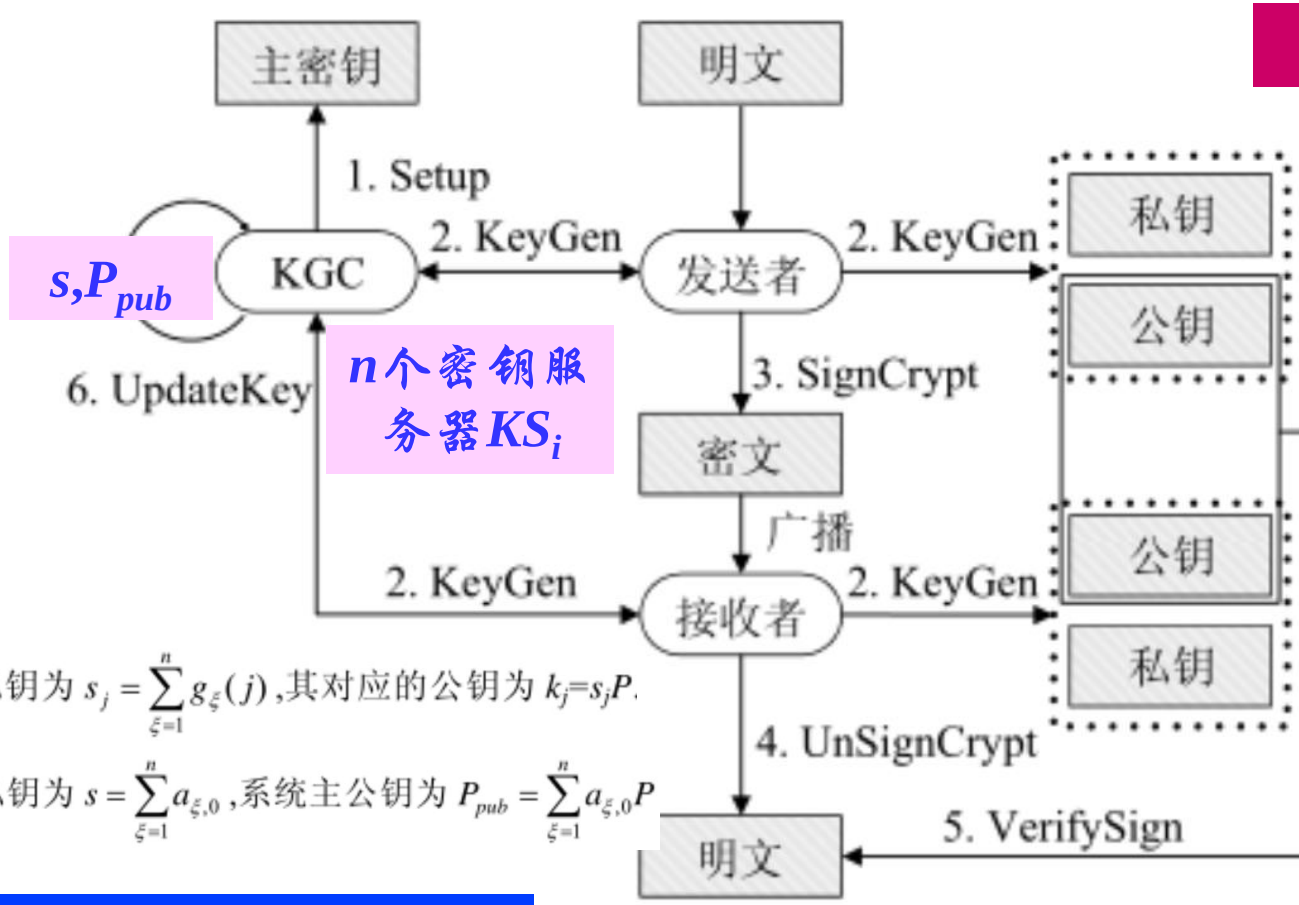
4 算法或协议应用

王利朋等.应用区块链的多接收者多消息签密方案.软件学报,2021,32(11):3606-3627

KGC私钥s 公钥$P_{pub}=sP$

Shamir门限方案

ECC密码算法



KS_i私钥s_i 公钥$k_i=s_iP$

用户私钥$s+u_{id}$ 公钥U_{id}

王利朋等.应用区块链的多接收者多消息签密方案.软件学报,2021,32(11):3606-3627

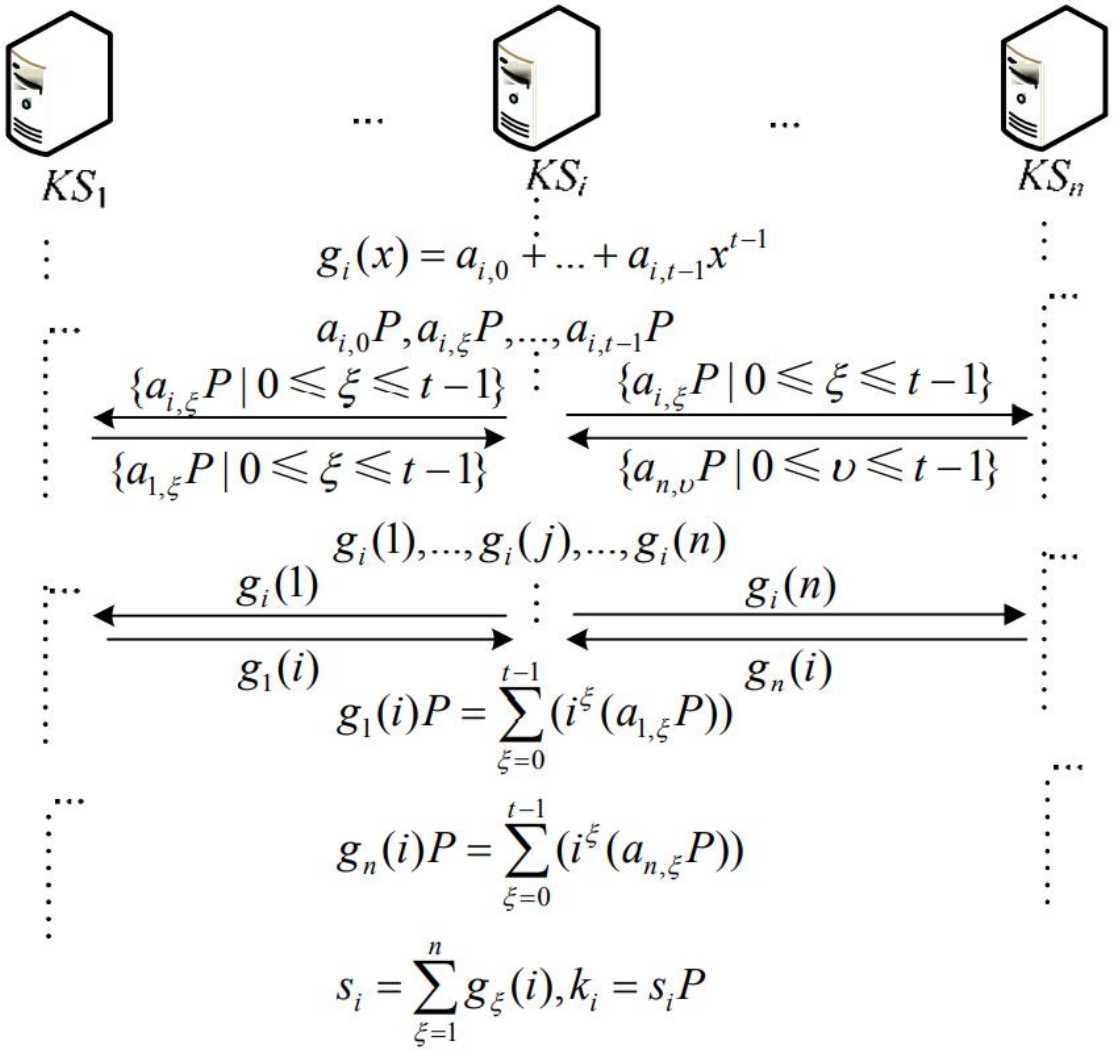


图 2　系统初始化

牛淑芬等.基于区块链的电子病历数据共享方案.自动化学报,网络首发2020-05-26

双线性映射

1.1 双线性映射

定义 1 令 G_1 和 G_2 为两个阶为素数 q 的乘法循环群, 定义一个双线性映射 $e: G_1 \times G_1 \rightarrow G_2$ 满足如下性质:

1) 双线性 (Bilinear): 对于任意 $a, b \in Z_q^*$ 和 $x, y \in G_1$, $e(x^a, y^b) = e(x, y)^{ab}$ 成立;

构造特殊多项式

为了实现联盟链上的[illegible]了一个多项式 $f(x)$, W, 系统计算 $H_1(w_1), H_1(w_2), ..., H_1(w_n)$, 并定义多项式 $f(H_1(w_i)) = 0, i \in (1, 2, ..., n)$, 即 $f(x) = (x - H_1(w_1))(x - H_1(w_2))...(x - H_1(w_n)) = 0$. 假设存在向量 $\boldsymbol{b} = [1, b_{n-1}, ..., b_0]$ 使得多项式可以表示为 $f(x) = x^n + b_{n-1}x^{n-1} + ... + b_1x + b_0$, 转换等式为 $x^n + b_{n-1}x^{n-1} + ... + b_1x = -b_0$, 其中 $x = H_1(w_i), i \in (1, 2, ..., n)$. 若设置向量 $\boldsymbol{a} = [a_n = -\frac{1}{b_0}, ..., a_1 = -\frac{b_1}{b_0}]$, 则系统可推出新多项式 $g(x) = a_nx^n + ... + a_1x$, 且 $g(H_1(w_i)) = 1, i \in (1, 2, ..., n)$. 若存在向量 $\boldsymbol{h} = \{H_1(w_1), H_1(w_2)^2, ..., H_1(w_n)^n\}$, 则有等式 $\boldsymbol{ah} = 1$. 若数据加密过程中使用的关键字属于关键字集 $W = \{w_1, w_2, ..., w_n\}$, 则等式 $\boldsymbol{ah} = 1$ 成立.

(2) 密钥生成:

患者 a 随机选择 $x_a \in Z_q^*$ 作为其私钥 sk_a, 并计算其公钥 $pk_a = g^{x_a}$. 医生 d 随机选择 $x_d \in Z_q^*$ 作为其私钥 sk_d, 并计算其公钥 $pk_d = g^{x_d}$. 数据用户 u 随机选择 $x_u \in Z_q^*$ 作为其私钥 sk_u, 并计算其公钥 $pk_u = g^{x_u}$. 通过激励机制, 选择相应的联盟链上节点作为验证者运行搜索算法和作为代理者执行代理重加密算法. 同时联盟链上的节点选择 $x_s \in Z_q^*$ 作为其私钥 sk_s, 计算公钥 $pk_s = g^{x_s}$.

ELGamal加密算法

(1) 加密:

输入病历 $m \in \{0,1\}^*$ 和关键字 $w \in \{0,1\}^*$, 医生随机选择 $r \in Z_q^*$, 计算 $B = pk_a^r$, $C = e(g^r, H_2(\beta)) \times m$, $t = e(g^r, H_3(\beta, w))$, $F = H_4(t)$.

计算向量 $\boldsymbol{X} = [X_1, X_2, ..., X_n]$, 其中 $X_1 = g^{rH_1(w)}$, $X_2 = g^{rH_1(w)^2}$, ..., $X_n = g^{rH_1(w)^n}$.

计算 $r_0 = H_5(w, B)$, $A = g^{rH_1(w) + r_0(sk_d + H_1(w))}$, $Y = h^{r_0(sk_d + H_1(w))}$.

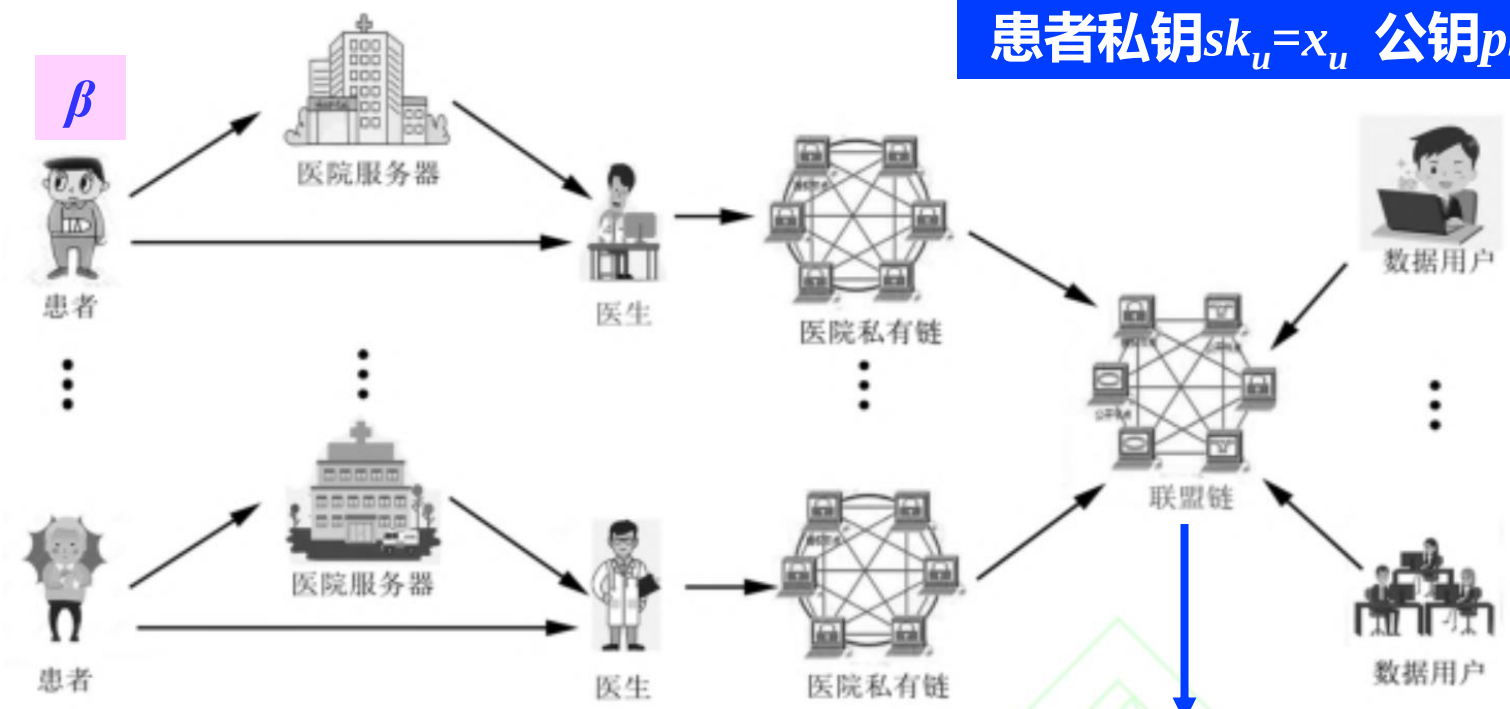
记 $C_{a_0} = (B, C)$, $C_{a_1} = (B, F)$, $C_{a_2} = (A, Y, \boldsymbol{X})$. 其中, C_{a_0} 为电子病历 m 的密文, C_{a_1} 为关键字 w 的密文, C_{a_2} 为联盟链上的一致性证明提供了依据. C_{a_0} 存储在医院 i 的服务器上, 医生将 C_{a_0} 的哈希值和由 C_{a_1}、C_{a_2} 构成的关键字索引上传至私有链

4 算法或协议应用

牛淑芬等.基于区块链的电子病历数据共享方案.自动化学报,网络首发2020-05-26

患者私钥$sk_a=x_a$ 公钥$pk_a=g^{xa}$

患者私钥$sk_u=x_u$ 公钥$pk_u=g^{xu}$



医生私钥$sk_d=x_d$ 公钥$pk_d=g^{xd}$

收到新交易后，联盟链上的验证者验证等式 $e(\prod_{i=0}^{n} X_i^{a_i}, X_2) = e(X_1, X_1)$ 和等式 $e(A, g) = e(X_1, g)Y$ 是否成立

代理重加密密钥：sk_u/sk_a

牛淑芬等.基于区块链的电子病历数据共享方案.自动化学报,网络首发2020-05-26

医生加密病历

(1) 加密:

输入病历 $m\in\{0,1\}^*$ 和关键字 $w\in\{0,1\}^*$, 医生随机选择 $r\in Z_q^*$, 计算 $B=pk_a^r$, $C=e(g^r,H_2(\beta))\times m$, $t=e(g^r,H_3(\beta,w))$,$F=H_4(t)$.

计算向量 $\boldsymbol{X}=[X_1,X_2,...,X_n]$, 其中 $X_1=g^{rH_1(w)}$, $X_2=g^{rH_1(w)^2}$,..., $X_n=g^{rH_1(w)^n}$.

计算 $r_0=H_5(w,B)$,$A=g^{rH_1(w)+r_0(sk_d+H_1(w))}$, $Y=h^{r_0(sk_d+H_1(w))}$.

$$
\begin{aligned}
e(A,g)&=e(g^{rH_1(w)+r_0(sk_d+H_1(w))},g)\\
&=e(g^{rH_1(w)},g)e(g^{r_0(sk_d+H_1(w))},g)\\
&=e(X_1,g)e(g^{r_0(sk_d+H_1(w))},g)\\
&=e(X_1,g)Y
\end{aligned}
$$

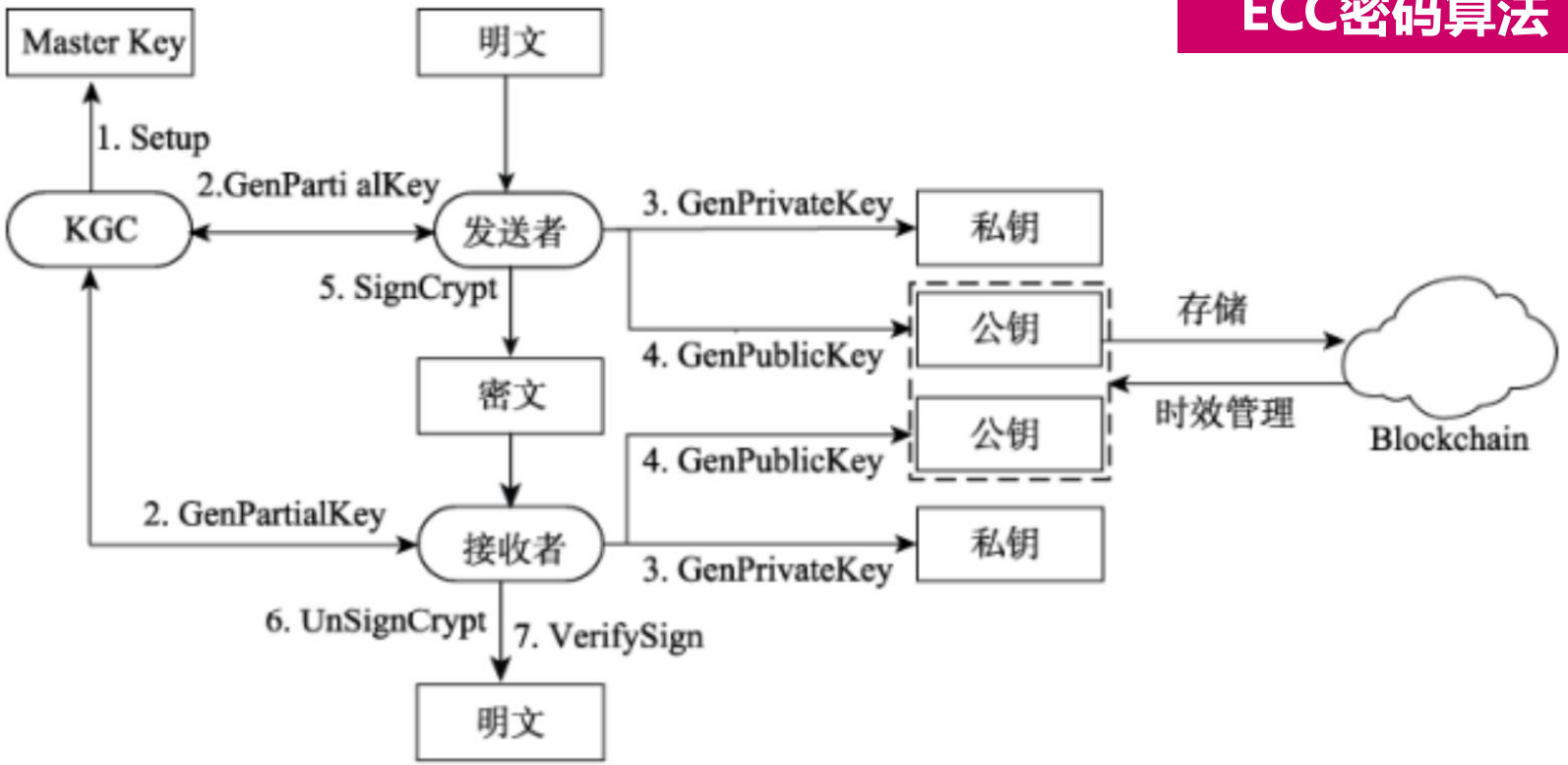
联盟链验证

$$
\begin{aligned}
&e(\prod_{i=0}^{n}X_i^{a_i},X_2)\\
&=e(\prod_{i=0}^{n}g^{ra_iH_1(w)^i},g^{rH_1(w)^2})\\
&=e(\prod_{i=0}^{n}g^{r(a_nH_1(w)^n+...+a_1H_1(w))},g^{rH_1(w)^2})\\
&=e(g^{r(\boldsymbol{ah})},g^{rH_1(w)^2})\\
&=e(g^r,g^{rH_1(w)^2})\\
&=e(g^{rH_1(w)},g^{rH_1(w)})\\
&=e(X_1,X_1)
\end{aligned}
$$

王利朋等.群智感知中基于区块链的带时效签密方案.计算机学报,2021,44(11):2217-2232

x_i和y_i　　X_i和Y_i

ECC密码算法



用户私钥选x_i计算 $X_i=x_iG$发送给KGC
KGC选r_i计算$Y_i=r_iG$(公开)和$y_i=r_i+sH_1(Id_i,X_i,Y_i)$

3 ECC算法

刘辉等.隐私保护的 VANET 警告消息发布协议.通信学报,2021,42(8):120-129

4.1 系统设置

TA 在此阶段执行以下步骤。

1) 设 F_p 是一个有限域，p 是素数，TA 定义椭圆曲线 $E: y^2=x^3+ax+b \bmod p$，其中 $a,b \in Z_q^*$。

2) TA 从 E 上选择一个阶为 q、生成元为 p 的加法循环群 G，它由椭圆曲线 E 和无穷远点 O 组成。假设 G 中的每个元素都可以用 l 位长的二进制字符串表示。TA 选择随机数 $x \in Z_q^*$ 作为系统的私钥，并计算系统公钥 $P_{\text{pub}}=xP$。

4.2 TMD 注册

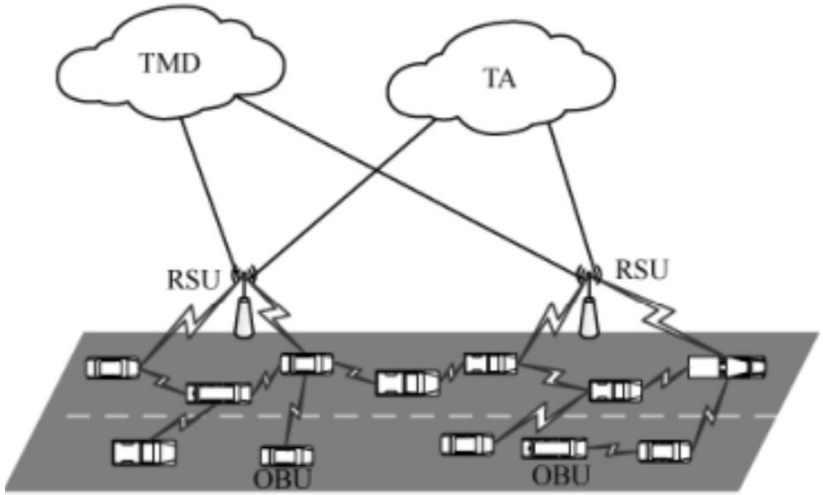
TMD 使用其真实身份 ID_{TMD} 向 TA 注册。

1) TA 生成一个随机数 $u_j \in Z_q^*$，并计算 $U_j=u_jP$，$\alpha_j=h_1(\text{ID}_{\text{TMP}} \| \text{VP}_i)$，$x_j=u_j+a_jx \bmod q$，其中 VP_i 是有效期，x_j 作为 TMD 的私钥。

2) TA 通过安全信道将 u_j 和 x_j 发送到 TMD。同时，TMD 通过 RSU 广播 U_j 和 α_j。TMD 定时生成有效期 VP_i，通过安全信道将 VP_i 发送给车辆。

ECC密码算法

TA私钥x 公钥$P_{pub}=xP$



TMD私钥x_j 公钥U_j

李继国等.标准模型下证明安全的可追踪属性基净化签名方案.计算机研究与发展,2021

双线性映射

拉格朗日插值多项式

2.1 双线性映射

假设 G 和 G_T 是 n 阶乘法循环群,其中 $n=pq$, p 和 q 是大素数.g 是 G 的生成元.一个双映射 e: $G\times G\to G_T$ 具有 3 个性质:

1) 双线性.对任意 $a,b\in Z_n$,有 $e(g^a,g^b)=e(g,g)^{ab}$.

2) 非退化性.$e(g,g)\neq 1$.

3) 可计算性.对所有 $u,v\in G$,存在多项式时间算法计算 $e(u,v)$.

2.2 拉格朗日插值

假设 p 为素数,集合 $S\subseteq Z_p$.首先定义拉格朗日系数 $\Delta_{i,S}(x)=\prod_{j\in S,j\neq i}\frac{x-j}{i-j}, i\in Z_p$.给定 Z_p 中 S,定义拉格朗日系数 $\Delta_{i,S}(x)=\prod_{j\in S,j\neq i}\frac{x-j}{i-j}$. PKG 随机选取$\alpha\in Z_n^*$,计算 $g_1=g^\alpha$,其中 g 是 G 的生成

2) 密钥生成.算法输入签名者身份 u 及其对应的属性集合 ω_u,主密钥 α 和公共参数 $params$.PKG 首先选取一个 $d-1$ 次多项式 $q(x)$,满足 $q(0)=\alpha$.然后每个用户 u 随机选取 $s\in Z_n$,计算 $D_{u,0}=g^s$, $D_{u,1}=h^s$ 对于 $i\in\omega_u$,PKG 随机选择 $r_i\in Z_n$,计算 $D_{i,0}=g_2^{q(i)}\times T(i)^{r_i}\times W(u)^s$, $D_{i,1}=g^{r_i}$.签名者私钥为 $D_{u,\omega_u}=\{s,D_{u,0},D_{u,1},D_{i,0},D_{i,1}\}$.

签名验证等式

$$\frac{e(g,\sigma_0)\,e\left(w'\prod_{j=1}^{l}w_j^{m_j},\sigma_1\right)^{-1}e(c,\sigma_1)^{-1}}{\left[\prod_{i\in\tilde{\omega}_a}e(T(i),\sigma_{ai})\right]\left[\prod_{i\in\tilde{\omega}_b}e(T(i),\sigma_{bi})\right]}=e(g_1,g_2)$$

结语 The end

谢谢！

Bruce Schneier著,吴世忠等译.应用密码学--协议,算法与C源程序.机械工业出版社