有理数相等的保密判定

李顺东,杜润萌,杨颜璟,魏 琼
(陕西师范大学计算机科学学院,陕西西安 710062)

摘 要: 安全多方计算是近年来国际密码学界研究的热点.数据相等保密判定是安全多方计算的一个基本问题,在指纹匹配和关键词搜索等现实问题中有广泛的应用,因此研究数据相等保密判定有重要的理论与实际意义.本文协议 I 利用 Paillier 加密算法高效实现了两个有理数相等的保密判定,协议 II 基于椭圆曲线同态加密算法安全高效计算多个有理数相等判定问题,并且最后给出了恶意模型下的有理数相等保密判定协议.

关键词: 密码学; 安全多方计算; 数据相等; 有理数; 指纹匹配
中图分类号: TP309 **文献标识码:** A **文章编号:** 0372-2112 (2020)10-1933-05
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2020.10.009

Privately Determining Equality of Rational Numbers

LI Shun-dong, DU Run-meng, YANG Yan-jing, WEI Qiong
(*School of Computer Science, Shaanxi Normal University, Xi'an, Shaanxi* 710062, *China*)

Abstract: Secure multiparty computation (SMC) has become research focus in the international cryptographic community in recent years. Privately determining equality of data is a basic problem in SMC. It is widely applied to fingerprint matching, keyword searching and so on. Studying privately determining equality of data has important theoretical and practical significance. Protocol I which is based on the Paillier cryptosystem can privately determine equality of two rational numbers. Protocol II which is based on elliptic curve cryptosytem can privately determine equality of multiple rational numbers. Finally this paper gives the protocol for privately determining equality of rational numbers in the malicious model.

Key words: cryptography; secure multiparty computation; data equality; rational number; fingerprint matching

1 引言

安全多方计算(Secure Multiparty Computation, SMC)是由姚期智教授提出来的[1],是近年来国际密码学界的研究热点.数据相等保密判定(Privately determining equality of data, PDOED)是一个重要的安全多方计算问题,具体可以描述为保密判定多个参与者的私密数据是否相等,在指纹匹配和关键词搜索等现实问题中有广泛的应用.

数据相等保密判定问题最早是由 Liu 等人在文献[2]中提出,但 Liu 研究的是有限集合的整数比较问题,文献[3]做了一些改进,提高了效率.但文献[2,3]设计的协议都需要规定一个整数全集,且仅适用于数据范围较小的情况.文献[4]首次提出有理数相等的保密判定方案,但其方案中所涉及的思想只适用于解决两个有理数比较问题,无法解决多个有理数比较问题.

本文针对有理数分别提出两个有理数相等保密判定方案和多个有理数相等保密判定方案.本文贡献如下:

(1)解决了有理数上的数据相等保密判定问题,并对其进行了完整的理论分析.

(2)提出了按位编码的思想,以此为基础可以解决很多 SMC 问题.

2 预备知识

2.1 SMC 模型

半诚实模型[5] 本文方案的安全性均假设安全多方计算的参与者为半诚实参与者. 半诚实参与者是指参与者在协议执行过程中将按照协议忠实的执行,但他们会利用收集到的所有信息推导出其他参与者的输入.

恶意模型[6] 恶意模型下 SMC 协议应迫使参与者

收稿日期:2019-05-13;修回日期: 2019-12-24;责任编辑:李勇锋
基金项目:国家自然科学基金(No.61272435)

像半诚实参与者一样按协议要求执行协议. 但有三种恶意行为在任何协议中无法避免,即参与者拒绝参加协议,修改其原本规定的输入数据而用其他数据替代以及参与者在协议执行过程中可随时中止协议.

2.2 隐私的模拟范例

假设参与者为 $P_1,\cdots,P_m$,分别拥有秘密数据 $x_1,\cdots,x_m$.

(1)令 $X=(x_1,\cdots,x_m)$,$f(X)=(f_1(X),\cdots,f_m(X))$ 是概率多项式时间参数,π 是计算函数 f 的协议.

(2) $P_i(i=1,\cdots,m)$的信息序列记为

$$view_i^{\pi}(X)=(x_i,r_i,M_1^i,\cdots,M_t^i),$$

其中 r_i 表示 P_i 的随机数,M_j^i 表示 P_i 收到的第 j 个消息.

(3)对于部分参与者 $I=\{P_{i1},\cdots,P_{i\alpha}\}\subseteq\{P_1,P_2,\cdots,P_m\}$,记为

$$view_I^{\pi}(X)=(I,view_{i1}^{\pi}(X),\cdots,view_{i\alpha}^{\pi}(X)).$$

定义 1 假设有一个计算函数 f 的协议 π,如果对于任意的 $I=\{P_{i1},\cdots,P_{i\alpha}\}\subseteq\{P_1,P_2,\cdots,P_m\}$,都存在概率多项式时间算法 S 使得下式

$$\{S(I,\{x_{i1},\cdots,x_{i\alpha}\},f_I(X))\}\overset{c}{\equiv}\{view_I^{\pi}(X)\}\quad(1)$$

成立,则称协议 π 保密地计算 f,其中 $\overset{c}{\equiv}$ 表示计算上不可区分. 本文利用上述模拟范例方法[7]证明协议的安全性.

2.3 Paillier 密码系统

Paillier 密码系统是概率加密系统[8],具体算法是:

密钥生成 首先选取两个素数 p,q,其中 $n=p\times q$,$\lambda=\mathrm{lcm}(p-1,q-1)$是 $p-1$ 和 $q-1$ 的最小公倍数. 随机选择一个 $g\in Z_n^*$,使得 $\gcd(L(g^{\lambda}\bmod n^2),n)=1$,其中 $L(x)=\dfrac{x-1}{N}$. 公钥为(g,n),私钥为 λ.

加密 对于明文消息 m,选择一个随机数 r,$r<n$,计算

$$c=g^m r^n \bmod n^2$$

解密 对于密文 c,计算

$$m=\frac{L(c^{\lambda}\bmod n^2)}{L(g^{\lambda}\bmod n^2)}\bmod n^2$$

同态性 直接验证可得 Paillier 密码系统具有以下性质

$$\begin{aligned}E(m)^k&=(g^m r^N)^k \bmod n^2\\&=(g^{mk}r^N)\bmod n^2=E(km).\end{aligned}$$

2.4 门限椭圆曲线密码系统

门限解密在安全多方计算中是对抗合谋攻击的一个重要工具[9,10]. 本文应用椭圆曲线实现 ElGamal 密码体制并结合(m,m)门限方案构造加法同态加密算法[11,12].

密文重随机化 对于密文(c_1,c_2),选取随机正整数 r_1,计算

$$\begin{aligned}(c_1',c_2')&=(c_1+r_1K,c_2+r_1G)\\&=(M+(r+r_1)K,(r+r_1)G),\end{aligned}$$

显然(c_1',c_2')是关于 M 的一个全新的密文. 在下文中以 $R(C)$表示密文重随机化.

3 有理数相等保密判定

3.1 两个有理数相等保密判定

假设两个参与者 Alice 和 Bob 分别具有保密有理数 $x_i=a_i/b_i\neq 0$,$i=1,2$,要求两个有理数的最大公约数(Greatest common divisor,GCD)等于 1,记 $\gcd(a_i,b_i)=1$. Alice 和 Bob 希望在不泄露各自保密数据的前提下合作计算函数 $y=P(x_1,x_2)$:如果 $x_1=x_2$,$P(x_1,x_2)=1$;否则 $P(x_1,x_2)=0$.

协议 Ⅰ 两个有理数相等保密判定.

输入:Alice 和 Bob 分别具有保密有理数 $x_i=a_i/b_i$,$i=1,2$.

输出:$P(x_1,x_2)$.

预处理:Alice 和 Bob 商定一个随机数 r,分别计算 $x_i=(a_i+r)/(b_i+r)=a_i^*/b_i^*$,$i=1,2$. 选择的随机数 r 必须保证两方参与者 a_i^* 互异的质因子的数目不相等.

准备:Alice 持有私钥 λ,公钥为(n,g).

(1)Alice 选择随机数 r_1 并计算 $a_1^{*b_1^*}r_1^n \bmod n^2$,结果记作 C_1 发送给参与者 Bob.

(2)Bob 选择随机数 r_2 并计算 $C_1 a_2^{*-b_2^*}r_2^n \bmod n^2$,结果记为 C_2 发送给参与者 Alice.

(3)Alice 解密. 若 $D(C_2)=0$,输出 $P(x_1,x_2)=1$;否则输出 $P(x_1,x_2)=0$.

正确性分析 预处理中有理数 x_i 分子分母均添加随机数 r,一是为了防止双方参与者有理数的分子都是 1,而 1 的任何次方都等于 1,从而输出 $P(x_1,x_2)=1$. 二是在分子互异质因子数目和大小完全相等的前提下,也就是 $a_2=a_1^{\lambda}$,两个有理数 a_1/b_1,a_2/b_2 还满足 $a_2=a_1^{b_1/b_2}$,其中 $a_i\neq 1$. 执行协议Ⅰ:

$$\begin{aligned}&a_1^{b_1}r_1^n a_2^{-b_2}r_2^n \bmod n^2=a_1^{b_1}r_1^n(a_1^{b_1/b_2})^{-b_2}r_2^n \bmod n^2\\&=a_1^{b_1}r_1^n a_1^{-b_1}r_2^n \bmod n^2=a_1^0(r_1r_2)^n \bmod n^2\\&=g^0(r_1r_2)^n \bmod n^2.\end{aligned}$$

从而导致协议输出 $P(x_1,x_2)=1$.

证明协议Ⅰ的正确性,我们首先假设 Alice 和 Bob 的两个数据相等($a_1=a_2$,$b_1=b_2$). 根据协议Ⅰ的第 2 步,可以得到

$$\begin{aligned}&C_1 a_2^{*-b_2^*}r_2^n \bmod n^2=a_1^{*b_1^*}r_1^n a_2^{*-b_2^*}r_2^n \bmod n^2\\&=a_1^{*0}(r_1r_2)^n \bmod n^2=g^0 r^n \bmod n^2=E(0)\end{aligned}$$

Alice 计算 $D(C_2)=0$,输出 $P(x_1,x_2)=1$,与协议Ⅰ的结论保持一致. 反之,假设 Alice 和 Bob 的两个数据不相等时会导致协议无法正确解密,从而输出 $P(x_1,x_2)=0$. 值得注意的是,当 $x_1=x_2$ 时,经过模运算后得到的结果一定相同. 当 $x_1\neq x_2$ 时,经过模运算后得到相同结果的概率为 $1/n$,在概率意义下这种情况可忽略不计.

安全性分析　要证明协议Ⅰ的安全性需要构造满足式(1)的模拟器. 具体有下面结论.

定理 1　协议Ⅰ在半诚实模型下是安全的.

Alice 构造使得式(1)成立的模拟器 S,要求 $\gcd(a_i,b_i)=1,i=1,2$. 模拟过程如下:

(ⅰ)S 接受输入$(x_1,P(x_1,x_2))$,根据 $P(x_1,x_2)$ 的值构造$x_2'=a_2'/b_2'$,使得 $P(x_1,x_2')=P(x_1,x_2)$. 用 x_1,x_2'进行模拟.

(ⅱ)S 选择随机数 r'计算 $x_1=a_1^{*}{}'/b_1^{*}{}'$,$x_2'=a_2^{*}{}'/b_2^{*}{}'$,选择的随机数 r 必须保证 a_1^{*},$(a_2^{*})'$互异的质因子的数目不相等.

(ⅲ)S 选择随机数 r_1'并计算 $a_1^{*b_1^{*}}(r_1')^n \bmod n^2$,结果记作$C_1'$.

(ⅳ)S 选择随机数 r_2'并计算 $C_1'(a^{*'}_2)^{-b^{*}_2}(r_2')^n \bmod n^2$,结果记为$C_2'$.

(ⅴ)S 解密 $D(C_2')$.

在协议Ⅰ中 $view_1^{\pi}(x_1,x_2)=\{C_1,C_2,P(x_1,x_2)\}$. 令 $S(x_1,P(x_1,x_2'))=\{C_1',C_2',P(x_1,x_2')\}$. 因为 $P(x_1,x_2)=P(x_1,x_2')$,$C_1\overset{c}{\equiv}C_1'$,$C_2\overset{c}{\equiv}C_2'$. 所以下式

$$\{S(x_1,P(x_1,x_2'))\}\overset{c}{\equiv}\{view_1^{\pi}(x_1,x_2)\}$$

成立. 同理可用类似的方法构造 S_2 使得

$$\{S(x_2,P(x_1',x_2))\}\overset{c}{\equiv}\{view_2^{\pi}(x_1,x_2)\}.$$

3.2　多个有理数相等保密判定

还有一些情景,我们需要保密比较多个参与者的有理数是否相等. 如果直接将协议Ⅰ推广到多方,会出现计算错误. 基于此,我们设计了多个有理数相等保密判定协议. 假设 m 个参与者 $P_i(i=1,\cdots,m)$分别具有保密数据 $x_i=a_i/b_i=a_i^1\cdots a_i^{s_i}/b_i^1\cdots b_i^{q_i}$,其中 $\gcd(a_i,b_i)=1$,$a_i^k,b_i^l\in\{0,\cdots,9\}$,$1\leqslant k\leqslant s_i$,$1\leqslant l\leqslant q_i$,$s_i$ 表示分子的位数,q_i 表示分母的位数. m 个参与者希望在不泄露各自保密数据的前提下合作计算函数 $y=P(X)(X=x_1,\cdots,x_m)$:如果 $x_1=\cdots=x_m$,$P(X)=1$;否则 $P(X)=0$.

统一所有参与者有理数对应分子和分母的位数分别是 s,q. 位数不够的情况下可通过以下方式转换数据:

$$x_i\rightarrow\frac{0\cdots0a_i^1\cdots a_i^{s_i}}{0\cdots0b_i^1\cdots b_i^{q_i}}\rightarrow e_i^1\cdots e_i^j\cdots e_i^{s+q}.$$

其中 $1\leqslant j\leqslant s+q$.

参与者 P_1 按位编码,构造矩阵

$$\boldsymbol{U}_{(s+q)\times10}=\begin{bmatrix}u_1^1 & u_2^1 & \cdots & u_{10}^1\\ u_1^2 & u_2^2 & \cdots & u_{10}^2\\ \vdots & \vdots & & \vdots\\ u_1^{s+q} & u_2^{s+q} & \cdots & u_{10}^{s+q}\end{bmatrix},$$

对于每一行 $u^j=[u_1^j\cdots u_{10}^j]$,$1\leqslant j\leqslant s+q$ 有

$$u_k^j=\begin{cases}0, & e_1^j=k-1;\\ r_k^j, & e_1^j\neq k-1.\end{cases}\tag{2}$$

其中 $r_k^j\in Z_p^{*}$ 下不等于 0 的随机数. 这样,P_1 拥有的数据 x_1 转化为矩阵 $\boldsymbol{U}$. 参与者 P_i 公布矩阵 $\boldsymbol{U}$,其余参与者 P_i,$2\leqslant i\leqslant m$ 从 u^1 至 u^{s+q}中按位挑选对应位置的编码得到 $U_i=u^1_{(e_i^1+1)}+\cdots+u^{s+q}_{(e_i^{s+q}+1)}$ 并公布. 因此可得到以下结论.

事实 1　多个有理数相等的充要条件是:$U_2+\cdots+U_m=0$.

协议Ⅱ　多个有理数相等保密判定.

输入:m 个参与者 $P_i(i=1,\cdots,m)$分别具有保密数据 x_i.

输出:$P(X)$.

准备:m 个参与者 P_i 首先商定一条椭圆曲线 $E_p(a,b)$以及椭圆曲线上的一个生成元 G. 每个参与者 P_i 分别选择一个私钥 k_i,$2\leqslant k_i\leqslant L-1$,计算 $K_i=k_iG$,生成公钥

$$K=\sum_{i=1}^{m}K_i=\sum_{i=1}^{m}k_iG.$$

(1)参与者 P_1 操作如下:

(a)P_1 将数据 x_1 按照式(2)构造矩阵 $\boldsymbol{U}$.

(b)P_1 将矩阵 $\boldsymbol{U}$ 中 $u_k^j=0$ 的分量编码成为椭圆曲线 $E_p(a,b)$上的点 $M=u_k^jG$.

(c)P_1 用公钥 K 加密矩阵 $\boldsymbol{U}$ 得

$$E(\boldsymbol{U})=\begin{bmatrix}E(u_1^1) & E(u_2^1) & \cdots & E(u_{10}^1)\\ E(u_1^2) & E(u_2^2) & \cdots & E(u_{10}^2)\\ \vdots & \vdots & & \vdots\\ E(u_1^{s+q}) & E(u_2^{s+q}) & \cdots & E(u_{10}^{s+q})\end{bmatrix}$$

$$=\begin{bmatrix}(c_{11}^1,c_{12}^1) & (c_{21}^1,c_{22}^1) & \cdots & (c_{(10)1}^1,c_{(10)2}^1)\\ (c_{11}^2,c_{12}^2) & (c_{21}^2,c_{22}^2) & \cdots & (c_{(10)1}^2,c_{(10)2}^2)\\ \vdots & \vdots & & \vdots\\ (c_{11}^{s+q},c_{12}^{s+q}) & (c_{21}^{s+q},c_{22}^{s+q}) & \cdots & (c_{(10)1}^{s+q},c_{(10)2}^{s+q})\end{bmatrix},$$

其中 $(c^j_{(e_1^j+1)1},c^j_{(e_1^j+1)2})=E(M)$,其它 $(c^j_{(\neq e_1^j+1)1},c^j_{(\neq e_1^j+1)2})\in Z_p^{*}\times Z_p^{*}$ 为随机数对. 完成这些操作后公布密文矩阵 $E(\boldsymbol{U})$.

(2)P_2 从 $E(\boldsymbol{U})$中根据自己的数据按位依次挑选出密文 $E(u^1_{(e_2^1+1)}),\cdots,E(u^{s+q}_{(e_2^{s+q}+1)})$,计算 $E(U_2)=E(u^1_{(e_2^1+1)})+\cdots+E(u^{s+q}_{(e_2^{s+q}+1)})$. P_2 计算 $R(E(U_2))$并

公布.

(3)P_i,($3\leqslant i\leqslant m$)做与 P_2 一样的操作,依次得到 $R(E(U_i))$并公布.

(4)P_1 计算 $E(x)=R(E(U_2))+\cdots+R(E(U_m))=(c_1,c_2)$并公布.

(5)P_i,$2\leqslant i\leqslant m$ 计算 k_ic_2,结果发送给 P_1.

(6)P_1 计算 $D(x)=c_1-(k_1+\cdots+k_m)c_2$,并将 $D(x)$与 M 作比较,如果 $D(x)=M$,输出 $P(X)=1$,否则输出 $P(X)=0$.

正确性分析 协议Ⅱ的正确性可由事实 1 及本文采用的椭圆曲线编码方式得到保证.

安全性分析 要证明协议Ⅱ的安全性需要构造满足式(1)的模拟器 S. 具体有下面结论.

定理 2 协议Ⅱ在半诚实模型下是安全的,并能抵抗任意的合谋攻击.

证明 应用模拟范例严格证明定理 2. 由于各参与者地位平等,仅证明 P_1 的私密数据是安全的即可. 定义合谋者集合 $I=\{P_2,\cdots,P_m\}$. S 构造椭圆曲线公钥系统,设公钥为 K',私钥:$k'=k'_1+\cdots+k'_m$. 与定理 1 类似,S 接受输入$(I,X_I,P(X))$,随机选取 x'_1,使 $P(X)=P(X')$. 执行协议Ⅱ步骤,可得到:

$$\{view_I^{\pi}(x_1,\cdots,x_m)\}\overset{c}{\equiv}\{S(x'_1,x_2,\cdots,x_m,P(X))\}.$$

4 效率分析——复杂性分析

计算复杂性 协议Ⅰ的计算复杂性是 $6M_e$. 协议Ⅱ的计算复杂性是$((s+q+1)\log r)M_a$. 其中 M_a 表示模加运算,M_e 表示模指数运算.

通信复杂性 协议Ⅰ执行过程中需要 3 次通信. 协议Ⅱ中共需要 $3m-1$ 次通信.

5 恶意模型下数据相等保密判定

协议Ⅲ 恶意模型下的两个有理数相等保密判定.

输入:Alice,Bob 的数据 a_i^*,b_i^*.

输出:$P(x_1,x_2)$.

准备:Alice 持有私钥 λ,公钥为(n,g).

(1)Alice 计算 $C_1=a_1^{*b^*_1}r_1^n \bmod n^2$,$u=g^{\lambda}\bmod{}^2$,将 C_1,u 发送给 Bob.

(2)Bob 计算 $C_2=C_1a_2^{*-b^*_2}r_2^n \bmod n^2$,选择一个随机数 s,加密 s 得 $C=E(s)$. 将 C_2,C 发送个 Alice.

(3)Alice 计算$\bar{C}_2=C_2^{\lambda} \bmod n^2$,$\bar{C}=C^{\lambda} \bmod \bmod n^2$,$D(C)$,并发送给 Bob.

(4)如果 $D(C)=s$,Alice 向 Bob 证明 $\log_{C_2}\bar{C}_2=\log_C\bar{C}=\log_g u$,记为 P.

正确性分析 协议Ⅲ的正确性可由协议Ⅰ得到保证,为节省篇幅,这里不再赘述.

安全性分析 首先我们假设 Bob 是恶意参与者,Alice 是半诚实参与者. Bob 所能操作的恶意行为主要包括:(1) Bob 计算 $C_2=C_1a_2^{*-b^*_2}r_2^n \bmod n^2$,输入错误的 a_2^*,b_2^*,这相当于 Bob 改变自己的输入数据,该行为在任何协议中都无法避免.(2) Bob 计算 C_2 时,选择的 r_2 非随机数,但只要 Alice 选择的是随机数,就可消除 r_2 的非随机性.

现在我们假设 Alice 是恶意参与者. Alice 所能操作的恶意行为除了与 Bob 一致的恶意行为之外还包括:(3) Alice 计算 $u=g^{\lambda} \bmod n^2$ 时,选择错误的 g.(4) Alice 计算 $C_2=C_2^{\lambda} \bmod n^2$ 时或许会提供错误的解密密钥. Bob 为了防止 Alice 存在(3)(4)这两种恶意行为,第一步 Bob 加密一个随机数 s,并要求 Alice 解密. 第二步要求 Alice 发送解密证明部分[13] $u=g^{\lambda} \bmod n^2$,$\bar{C}_2=C_2^{\lambda} \bmod n^2$,$\bar{C}=C^{\lambda} \bmod n^2$ 以及向 Bob 证明 $\log_{C_2}\bar{C}_2=\log_C\bar{C}=\log_g u$,以此验证 Alice 没有作弊.

如果 Alice 和 Bob 都是恶意参与者,对此现已证明理论上无法设计出安全的协议[6]. 限于篇幅,只给出定理,证明过程省略.

定理 3 协议Ⅲ对恶意参与者是安全的.

6 结论

有理数相等保密判定问题在安全多方计算协议的构造中具有实际研究意义,除文中提到的应用场景以外,有理数相等保密判定问题的其他应用也有待发掘.

参考文献

[1] YAO A C. Protocols for secure computations[A]. Proceedings of the 23rd IEEE Symposium on Foundations of Computer Science[C]. Chicago:IEEE Press,1982. 160 – 164.

[2] 刘文,王永滨. 安全多方信息比较相等协议及其应用[J]. 电子学报,2012,40(5):871 – 876.
LIU Wen,WANG Yong-bin. Secure multi-party comparing protocol and its applications[J]. Acta Electronica Sinica,2012,40(5):871 – 876. (in Chinese)

[3] 窦家维,李顺东. 数据相等问题的安全多方计算方案研究[J]. 电子学报,2018,46(5):1107 – 1112.
DOU Jia-wei,LI Shun-dong. Secure multiparty computation for the equality problem[J]. Acta Electronica Sinica,2018,46(5):1107 – 1112. (in Chinese)

[4] GONG L M,YANG B,XUE T,et al. Secure rational numbers equivalence test based on threshold cryptosystem with rational numbers[J]. Inf Sci,2018,466:44 – 54.

[5] LI S D,WANG D S,DAI Y Q. Efficient secure multiparty computational geometry[J]. Chinese Journal of Electronics,2010,19(2):324 – 328.

[6] GOLDREICH O. Foundations of Cryptography:Volume 2,

Basic Applications [M]. London: Cambridge University Press, 2004. 599 – 764.

[7] REIMER B, FRIED R, MEHLER B, et al. Brief report: examining driving behavior in young adults with high functioning autism spectrum disorders: a pilot study using a driving simulation paradigm [J]. Journal of Autism and Developmental Disorders, 2013, 43(9): 2211 – 2217.

[8] PAILLIER P. Public-key cryptosystems based on composite degree residuosity classes [A]. Proceedings of the Advances in Cryptology [C]. Prague: EUROCRYPT, 1999. 223 – 238.

[9] DESMEDT Y, FRANKEL Y. Threshold cryptosystems [A]. Proceedings of the Workshop on Advances in Cryptology [C]. Santa Barbara: CRYPTO, 1989. 307 – 315.

[10] LONG Y, CHEN K F, MAO X P. New constructions of dynamic threshold cryptosystem [J]. Journal of Shanghai Jiaotong University (Science), 2014, 19(4): 431 – 435.

[11] 杨波. 现代密码学基础[M]. 北京:清华大学出版社, 2015. 106 – 110.
YANG B. Foundations of Modern Cryptography [M]. Beijing: Tsinghua University Press, 2015. 106 – 110. (in Chinese)

[12] LI L, EL-LATIF A A A, NIU X. Elliptic curve ElGamal based homomorphic image encryption scheme for sharing secret images [J]. Signal Processing, 2012, 92(4): 1069 – 1078.

[13] VICTOR S. Practical threshold signatures [A]. Proceedings of the Theory and Application of Cryptographic Techniques [C]. Tunisia, 2000. 207 – 220.

作者简介

李顺东　男,1963 年生于河南. 现为陕西师范大学计算机科学学院博士生导师. 主要研究方向为现代密码学与信息安全.
E-mail: shundong@ snnu. edu. cn

杜润萌　女,1994 年生于山西. 现为陕西师范大学计算机科学学院硕士研究生. 主要研究方向为现代密码学与信息安全.
E-mail: durunmeng@ snnu. edu. cn