基于 LSSS 共享矩阵无授权策略的属性密码解密效率提高方案

刘梦君[1,2],刘树波[1,2],王 颖[1,2],王 晶[1],李永凯[1,2],曹 辉[1,2]
(1. 武汉大学计算机学院,湖北武汉 430072; 2. 武汉大学空天信息安全与可信计算教育部重点实验室(B类),湖北武汉 430072)

摘 要: 在基于 LSSS(Linear Secret-Sharing Schemes)共享矩阵的属性密码方案中,为了获得相对较高的解密效率,需要剔除授权集合中冗余参与方在解密时的计算.为达到这一目的,现有方案都需要使用授权策略进行最小参与方搜寻,而在一些应用场合下,授权策略的出现是不安全的.如果不使用授权策略,现有的解密优化方案便无法运行.本文提出一种 LSSS 共享矩阵下,无授权策略的属性密码解密效率提高方案.理论分析和实验表明,它可以在无授权策略情况下,找到最小参与方集合,从而提高了解密效率.

关键词: 属性加密; LSSS (Linear Secret-Sharing Schemes) 共享矩阵; 解密效率
中图分类号: TP309 **文献标识码:** A **文章编号:** 0372-2112 (2015) 06-1065-08
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2015.06.004

Optimizing the Decryption Efficiency in LSSS Matrix-Based Attribute-Based Encryption Without Given Policy

LIU Meng-jun[1,2], LIU Shu-bo[1,2], WANG Ying[1,2], WANG Jing[1], LI Yong-kai[1,2], CAO Hui[1,2]
(1. *School of Computer, Wuhan University, Wuhan, Hubei* 430072, *China*;
2. *Key Laboratory of Aerospace Information Security and Trusted Computing Ministry of Education, Wuhan University, Wuhan, Hubei* 430072, *China*)

Abstract: The redundant participants need to be excluded from the authorized set to achieve a high decryption efficiency in LSSS(Linear Secret-Sharing Schemes) matrix-based attribute-based encryption algorithms. The existing solutions achieve this by searching the minimum participant set in the previously given access policy. Some security threats, however, may be brought in under the previously given policy. And the absence of the access policy disables the existing searching-sound solutions. Thus, an optimizing solution is proposed. Intensive theory analysis and simulation show the proposed solution can get the minimum participant set, which improves the decryption efficiency.

Key words: attribute-based encryption; LSSS(Linear Secret-Sharing Schemes) sharing matrix; decryption efficiency

1 引言

属性密码机制[1]是一类采用字符语义属性对数据机密性进行保障的密码机制,自 Sahai 和 Waters 提出该类方案[2,3]以来,属性密码就以其安全灵活的访问控制性能,得到了广泛的研究和应用.尤其是云计算及云存储兴起后[4,5],基于属性的访问控制方案,在数据发布中应用更为广泛[6~9].

基于属性访问控制方案的核心是如何将秘密拆分成若干子秘密,并将每个子秘密映射到不同的访问控制属性集上.其理论基础来自于(n,t)门限秘密共享[10],门限秘密共享在与访问策略相结合时有两种基本形式,一种是基于拉格朗日插值法的秘密共享树[2,3];另一种是基于线性秘密共享机制的共享矩阵[11~14].基于 LSSS (Linear Secret-Sharing Schemes)的共享矩阵将访问策略和共享秘密转化到一个跟参与方属性关联的矩阵中,通过矩阵运算减少了大量秘密恢复时的计算量,比秘密共享树的解密效率高,因此得到了广泛应用[6~8].

属性加密机制虽然为数据发布提供了较高的安全性、较强的灵活性、较细的访问粒度,但由于其本质上仍然是公钥密码体系中的一种,因而其加解密耗时还是较长,尤其是解密耗时受访问策略规模的影响较大,会影

收稿日期: 2014-03-03; 修回日期: 2014-06-27; 责任编辑: 覃怀银
基金项目: 国家重点基础研究发展规划(973 计划)项目(No. 2011CB302306); 国家自然科学基金(No. 41371402); 中央高校基本科研业务费专项资金(No. 211-274230); 水利部(948)项目(No. 201044)

响系统的实时性能,如移动网络中的终端性能. 在保障安全性能的前提下,如何尽可能提高解密效率,一直是属性密码方案设计时需要考虑的重要因素.

一般而言,门限秘密共享在解密时的秘密恢复阶段面临 3 种基本情况,分别为 $k<t$、$k=t$ 和 $k>t$. $k<t$ 表明当前各方拥有子秘密数 k 小于恢复秘密的最小个数 t,意味着当前的参与方不满足授权策略; $k=t$ 表明当前各方拥有子秘密数 k 恰好等于恢复秘密的最小个数 t,意味着当前的参与方恰好满足授权策略; 而 $k>t$ 则表明,当前各方拥有子秘密数 k 大于恢复秘密的最小个数 t,意味着当前参与方集合冗余满足授权策略. 由于冗余满足部分秘密会增加额外的计算开销,因此在实际中,往往需要剔除冗余参与方部分,得到 $k'=t$ 个参与方的恰好满足授权集合. 在基于共享生成矩阵的属性密码方案中,基本的做法是采取附加授权策略,解密时使用搜寻[15]之类算法,寻找到最小参与方后,再求解参与方对应秘密恢复参数[16],然后继续计算. 但这种方式,解密时解密方需要知道授权策略,然后从中寻找一个最小参与方集合. 然而,在有些属性密码机制应用场合下,如在应用密文策略的访问控制机制中,随密文一起发布的授权策略通常会映射到某个身份的访问者,攻击者可以根据这个授权策略,在访问者获取内容时追踪到访问者的具体信息,如位置和身份等信息; 而在应用密钥策略的访问控制机制中,被授权者知晓密钥中附带的授权策略,更容易滥用密钥[17],这种情况在密文策略中也存在[18,19]. 为尽量避免以上的安全问题,具体授权策略不应被外界所知,而基于策略搜寻算法的解密优化方案[11~14]在无授权策略的应用环境下也就无法实施.

为提高无授权策略的秘密恢复效率,本文在文献[20]的基础上,提出一种有序秘密共享矩阵转化方法,并根据转化后矩阵的有序特性,设计出一个子秘密值计算参数求解方法. 该方法只需直接求解解密参数就可获得最小参与方,没必要必须知道授权策略,然后再根据授权策略搜索最小参与方,这样就节省了冗余参与方所带来消耗的大量计算时间,提高了解密效率. 理论分析和实际验证表明,本文所提方案在无授权策略时,能够提高解密效率.

2 相关研究

与本文相关的研究主要集中在寻找最少的参与方集合,达到减少解密计算开销的工作上.

作为属性密码方案研究的开创者,Sahai 和 Waters 等人在属性密码开创性工作[2,3]中也关注到了冗余参与方对解密计算带来的额外开销问题. 为了剔除冗余参与方,作者在遍历策略树、验证授权集合是否满足授权策略同时,对满足策略门限的参与方个数进行了统计,最终使用恰好满足策略门限的参与方进行解密,这种验证方式搜寻所需的时间复杂度为 $O(n\log(n))$.

Wang Cong[7]等的方案在应用文献[3]时,使用文献[15]中所述搜寻方法,将搜寻时间复杂度降低到了 $O(n)$,也即是搜寻时间随着参与方个数呈线性增长. 这个搜寻算法复杂度是目前已知最优.

随后大量基于 LSSS 共享矩阵的属性密码方案[6,12~14]提出使用矩阵来共享秘密,因为矩阵在求解共享秘密时,可以通过求解线性方程组[12]来求出秘密共享值,相比拉格朗日插值法计算秘密共享值,效率有大幅度提高. 但在求解共享秘密值时,仍然有冗余参与方参与了计算,需要使用策略搜寻算法来寻找最少参与方.

Water[11]等人最新的属性密码方案具有已知方案中最高的解密效率. 在 and/or 策略下采用文献[14]中给出的共享矩阵生成方法,将 and/or 门限授权策略转化为一个特殊矩阵,这个矩阵的最小授权集合中,关联参与方所对应的秘密值计算参数都为 1,冗余参与方秘密值计算参数都为 0,无需另寻求解秘密值计算参数. 当 $n>2$、$t\geqslant 1$,也即任意 (n,t) 门限策略时,仍然需要采取如文献[6,12~14]中方式求解秘密值计算参数. 然而,上述两种门限策略都需要事先搜寻最小参与方集合.

3 准备知识

3.1 布尔表达式到 LSSS 访问矩阵

布尔表达式在属性集密码方案中用来描述访问策略,每一个单调的布尔表达式都可以转化为一个等价的 LSSS 秘密共享方案[21]. 其中 LSSS 秘密共享矩阵有如下性质.

一个参与方集合 P 上的秘密共享方案是 Z_p 域上线性的,如果它满足下述条件:

(1) 各方共享的秘密形成一个 Z_p 域上的矩阵;

(2) 秘密共享方案存在一个共享生成矩阵 $\boldsymbol{A}$. 矩阵 $\boldsymbol{A}$ 有 l 行 m 列,对所有 $i=1,\cdots,l$,矩阵 $\boldsymbol{A}$ 的第 i 行被标识为参与方 $\rho(i)$ (ρ 是一个从 $\{1,\cdots,l\}$ 映射到 P) 的函数,同时有向量 $\boldsymbol{v}=(s,r_2,\cdots,r_m)$,其中 $s\in Z_p$ 是将要共享的秘密值,而 $r_2,\cdots,r_m\in Z_p$ 是随机数. 则向量 $\boldsymbol{A}\cdot\boldsymbol{v}$ 为秘密 s 的 l 个共享子秘密,且 $(\boldsymbol{A}\cdot\boldsymbol{v})_i$ 属于参与方 $\rho(i)$.

假定一个 LSSS 秘密共享方案的访问结构为 Λ. 令 $S\in\Lambda$ 为一个授权集合,定义 $I\subset\{1,\cdots,l\}$ 且 $I=\{i:\rho(i)\in S\}$. 存在常量值 $\{\omega_i\in Z_p\}_{i\in I}$ 使得任意合法的共享秘密 $\{\lambda_i\}_{i\in I}$,有 $\sum_{i\in I}(\omega_i\lambda_i)=\sum_{i\in I}\omega_i(\boldsymbol{M}_i\cdot\boldsymbol{v})=\boldsymbol{\varepsilon}\cdot\boldsymbol{v}=s$,其中 $\boldsymbol{\varepsilon}=(1,0,\cdots,0)$. 这些常量值 $\{\omega_i\in Z_p\}_{i\in I}$ 可以在与共享生成矩阵 $\boldsymbol{A}$ 的大小相关的多项式时间内计算出

来,而对于未授权的集合,这些常量值不存在. 而常量值的求解本质是在授权集合 S 中寻找一组与参与方对应的常量值$\{\omega_i \in Z_p\}_{i\in I}$,它通过求解线性方程组 $AX=\varepsilon$ 得到. 其中 $A_i^{\mathrm{T}}=M_i$,常量值解为 $X_i=\omega_i$. 由于矩阵 M 在有限域 Z_p 上,因此线性方程组 $AX=\varepsilon$ 求解需采用高斯消元法进行.

文献 [20] 在文献 [22] 的基础上,设计了一个将布尔表达式转换为 LSSS 共享矩阵的算法. 该算法将一个格式化的布尔表达式高效地转换为 LSSS 共享矩阵,并且可以将授权策略对应布尔表达式关联的参与方,按照格式化布尔表达式中的顺序一一对应到共享矩阵中. 其中格式化布尔表达式定义为: 令 $F_1,F_2,\cdots,F_n$ 为格式化表达式 F 的子表达式,访问策略树的根节点为一个(n,t)域门,则 $(F_1,F_2,\cdots,F_n,t)$ 为此访问策略树的格式化布尔表达式. 其中,F_i为叶子节点或者一个具有门限格式化的布尔表达式.

由于格式化布尔表达式将会决定最终生成的共享矩阵,本文将根据寻找最小化参与方的设计目标,对格式化布尔表达式做进一步处理. 布尔表达式转换为 LSSS 共享矩阵更详细的原理和细节参见文献 [20].

3.2　LSSS 共享矩阵下的解密效率

LSSS 共享矩阵在属性基密码方案解密算法中,用于快速恢复共享秘密值. 以文献 [11] 为例,在解密算法中,当求出授权集合 S 所对应的常量值 ω 存在后,算法需要执行如下计算,恢复出用于最终解密的值 $e(g,g)^{\alpha s}$.

$$\begin{aligned}&e(\hat{C},\prod_{i\in I}\underline{D_i^{\omega_i}})/e(\prod_{i\in I}R_i^{\omega_i},L)\\&=e(g^s,\prod_{i\in I}g^{\lambda\omega_i}f(S)^{r\omega_i})/e(\prod_{i\in I}g^{\lambda\omega_i},f(S)^s)\\&=e(g,g)^{\alpha s}\cdot e(g,f(S)^{s\sum_{i\in I}r\omega_i})/e(g,f(S)^{s\sum_{i\in I}r\omega_i})\\&=e(g,g)^{\alpha s}\end{aligned}$$

其中,$f(S)=\prod_{x\in S}h_x$,$\underline{D_i^{\omega_i}}=D_i\cdot\sum_{x\in S/\rho(i)}Q(i,x)=g^{\lambda_i}\cdot f(S)^{r_i}$,$L=\prod_{x\in S}f(S)^s$. 由于群 G 上的运算需要消耗大量计算时间[11],如前所述,为减少解密时间,可减少索引集合 I 的大小,恰恰索引集合 I 对应的授权集合 S 中参与方可能有冗余. 因此,若能找到最小的授权集合 S',只让最少的参与方参与上式计算,即可减少计算时间.

4　无授权策略下的解密效率提高方案

4.1　主要设计思想

由准备知识 3.1 中等式 $\sum_{i\in I}\omega_i M_i=\varepsilon$ 可以推知,$\omega_i=0$ 对应的参与方不影响最终目标向量,也即是 $\omega_i=0$ 对应的参与方为冗余,若从线性方程组 $AX=\varepsilon$ 求得使 $\omega_i=0$ 最多的一组解,余下 $\omega_i\neq 0$ 对应的参与方即为最小的授权集合. 这种方式下,只有共享生成矩阵和参与方参与计算,也就是在无授权策略的条件下,获得了最小参与方集合,并在接下来的解密过程中,减少冗余参与方带来的计算开销,从而提高解密效率.

4.2　方案设计

由 4.1 推断可知,影响参与方 $\omega_i=0$ 的个数有两个因素: 一是由布尔表达式到共享矩阵的转化,二是线性方程组求解 ω 值. 由于本文方案的目的是找到最小参与方,也就是求解参与方对应常量值 $\omega_i=0$ 个数最多的一组解. 分析 Z_p 域上线性方程组 $AX=\varepsilon$ 利用高斯消元求解过程特点. 在未知数个数大于系数矩阵 A 的秩 $R(A)$ 情况下,会有无穷多个解. 对于一个特解 ω,当 $i>R(A)$ 时 ω_i 可以全为 0,若冗余参与方对应的 ω_i 都在 $i>R(A)$ 处,则此组特解对应的恰为最优解. 而要满足上面特解的性质,就需要系数矩阵 A 中最小参与方常量解对应系数在前 $R(A)$ 列,也即在共享矩阵 M 的前 $R(A)$ 行. 满足这一性质,需要在布尔策略转化为共享矩阵时,将最小满足策略格式化布尔表达式所关联的参与方,在共享矩阵 M 中所对应的行放在矩阵的最前方,因此需要设计具有这个转换性质的转换算法. 3.1 已经说明,文献 [20] 中矩阵转化算法具有将布尔表达式按从前到后顺序一一转化到对应共享矩阵中的性质,如果将最小满足策略布尔表达式,按照策略阈值进行排序,则可以得到最小授权参与方所对应的向量处于共享矩阵最前方性质的共享矩阵.

根据以上分析过程,本文的方案划分为两个阶段,首先是格式化布尔表达式的有序化; 其次是常量值求特解处理. 这两个阶段在属性密码算法中的作用以文献 [11] 算法为例(为避免混乱,若无特别提示,本文接来下所述属性密码方案都以文献 [11] 中的方案为例),依次为: 前一个阶段是在为被授权方生成属性私钥时,提供具有上述特解性质的秘密共享矩阵; 后一个阶段则是在运行解密算法时,解得 0 尽可能多的常量值特解,以得到最少的授权参与方. 以下为各个阶段的具体方法.

4.2.1　布尔表达式的有序化

定义 1(有序格式化布尔表达式)　令 $F=(F_1,F_2,\cdots,F_n,t)$ 为文献 [1] 中所述布尔表达式,我们称 F 是有序的,如果 F 满足下述性质:

(1) F 中非叶孩子布尔表达式 F_i 的阈值 t_i 满足 $t_1\leqslant t_i\leqslant t_j\leqslant t_n$,其中 $i<j\in[1,n]$;

(2) 如果 F 中有 k 个叶子孩子,则 $(F_1,F_2,\cdots,F_k)$ 为这 k 个叶子节点;

(3) F 的非叶孩子布尔表达式 F_i 满足性质(1)、(2).

对于文献 [20] 中的格式化布尔表达式,在将其转化为 LSSS 共享矩阵之前,需要先进行预处理,使得其满足定义 1 所具有的有序化性质. 由于格式化布尔表

达式中,各个非叶孩子节点都具有门限阈值,因此可以通过门限阈值来对格式化布尔表达式进行排序调整. 算法 1 给出了格式化布尔表达式有序化的具体步骤.

算法 1 格式化布尔表达式有序化

输入: 格式化了的布尔表达式 $F=(F_1,F_2,\cdots,F_n,t)$

输出: 有序的格式化布尔表达式 $F'=(F_1',F_2',\cdots,F_n',t)$

第 1 步: 将布尔表达式 F 的 k 个叶子节点与前 k 个孩子节点进行交换,$k\in[1,n]$,并递归对所有非叶孩子节点进行相同处理;

第 2 步: 根据输入的布尔表达式 F 的非叶孩子节点的门限阈值,对布尔表达式进行的门限阈值进行比较排序,并递归对所有非叶孩子节点进行相同处理;

第 3 步: 根据步骤 2 门限阈值大小顺序,将布尔表达式 F 的非叶孩子节点位置顺序进行对应交换调整,并递归对所有非叶孩子节点进行相同处理,最终得到有序的格式化布尔表达式 $F'=(F_1',F_2',\cdots,F_n',t)$.

算法结束后,得到一个有序的格式化布尔表达式,再使用文献 [20] 中策略转换算法,便可得到一个具有最小授权参与方所对应的向量处于共享矩阵最前方性质的矩阵.

4.2.2 常量值求解

前文已经提及,常量值求解是使用高斯消元求解线性方程组的过程. 但高斯消元法在未知数个数大于系数矩阵 A 秩的情况下,会有无穷个解,而我们对高斯消元回代过程进行改造,使得求解的 X,在满足 $\sum_{i\in I}X_iM_i=\varepsilon$ 的前提下,有最多个数 0. 算法的具体过程如算法 2.

算法 2 求解常量值为 0 个数最多的常量值集合

输入: 授权集合 S,共享生成矩阵 M

输出: 有解时,得到 0 个数最多的常量值集合 $\{\omega_i\in Z_p\}_{i\in I}$,否则无解

第 1 步: 根据集合 S 在矩阵 M 所对应的行向量转置后得到一个 m 行、$|S|$ 列的线性方程组系数矩阵 A,使用高斯消元法,对增广矩阵 $B=(A|\varepsilon)$ 进行消元,得到一个下三角行阶梯矩阵 $B^{(|S|-1)}=(A^{(|S|-1)}|\varepsilon^{(|S|-1)})$,$B^{(|S|-1)}$ 表示第 $(|S|-1)$ 次消元后的矩阵,其它类推;

第 2 步: 若矩阵 A 和 B 的秩 $R(A)=R(B)$,则继续后续步骤,否则无解;

第 3 步: 使用高斯消元求解法,继续回代. 在回代求解过程中,如果矩阵 A 中 $m\geqslant|S|$,则执行步骤 4 求解,否则执行第 5 步;

第 4 步: 若矩阵 A 中 $m\geqslant|S|$,则方程组解向量 X 满足 $X_{|S|}=(\varepsilon_{|S|}^{(|S|-1)}/A_{|S|,|S|}^{(|S|-1)})$,$X_i=(\varepsilon_i^{(i-1)}-\sum_{j=i+1}^{|S|}A_{i,j}^{(i-1)}X_j)/A_{i,j}^{(i-1)}$,其中 $i=|S|-1,|S|-2,\cdots,1$;

第 5 步: 若矩阵 A 中 $m<|S|$,则方程组的解向量 X 通过如下方式得来: 对于 $i\in[m+1,|S|]$,$X_i=0$; $i=m$,$X_m=(\varepsilon_m^{(|S|-1)}/A_{m,m}^{(|S|-1)})$; $i\in[1,m-1]$,$X_i=(\varepsilon_i^{(i-1)}-\sum_{j=i+1}^{|S|}A_{i,j}^{(i-1)}X_j)/A_{i,j}^{(i-1)}$;

第 6 步: 输出 $\omega_i=X_i$.

在解密时,解密方先将使用算法 1 处理完,并使用文献 [20] 中方法生成的矩阵作为算法 2 输入,求解得所有参与方对应的常量值 ω,并根据常量值是否为 0,判断对应参与方是否为冗余及参与最终解密计算.

5 分析与讨论

5.1 正确性

5.1.1 定理及证明

在说明正确性之前先给出同级布尔表达式和最小授权布尔表达式的概念.

定义 2 本文所述同级布尔表达式是一组有着共同直接上级布尔表达式构成的布尔表达式.

定义 3 本文所述最小授权布尔表达式是指在给定参与方集合,满足授权策略条件下,拥有最少孩子数,且剔除了冗余孩子的布尔表达式.

定理 1 排序后的布尔表达式同原始输入的布尔表达式所蕴含的策略意义相同.

证明 因为同级布尔表达式的排序不会改变布尔表达式的含义,定理显然成立.

定理 2 在阈值为 t,孩子数为 n 的同级布尔表达式中,冗余孩子在格式化布尔表达式中出现的位置情况只有两种: 第一种是当前 t 个孩子都为满足授权集合孩子时,且总共有 $k\in(t,n]$ 个孩子满足授权,则后 $k-t$ 个都是冗余孩子; 第二种是当 t 个授权孩子分布在最少的前 $q\in(t,n]$ 个孩子中,则第 q 个孩子必定为授权孩子,后 $n-q$ 个孩子都为冗余,且前 q 个孩子中有 $q-t$ 个不满足授权集合的孩子.

证明 令排序后同级布尔表达式为 $F=(F_1,F_2,\cdots,F_n,t)$,对于第一种位置情况,因为前一个布尔表达式的阈值 t_i 小于后一个布尔表达式阈值 t_j. 因此,如果授权集合同时满足所有 $\{F_i\}_{i\in[1,t]}$ 布尔表达式,部分或全部满足 $\{F_i\}_{i\in[t,n]}$,在需要满足 t 个布尔表达式 F 的情况下,因为阈值 $t_1\leqslant t_2\leqslant\cdots\leqslant t_t\leqslant\cdots\leqslant t_n$,则布尔表达式 $F=(F_1,F_2,\cdots,F_t,t)$ 为一个最小授权布尔表达式,而布尔表达式 $\{F_i\}_{i\in[t+j,n],j\in[1,n-t]}$ 是冗余孩子; 对于第二种情况,首先可由第一种情况推知后 $n-q$ 个孩子都为冗余. 接下来使用反证法,首先假定第 q 个孩子不是授权孩子,则最少只需要 $q-1$ 个孩子即可满足授权要求,与最少的 q 相矛盾,假设前 q 个孩子中有 $q-t+j$,$j\in[1,n-q]$ 个满足授权集合的孩子,则最少只需要 $q-j$ 个孩子即可满足授权要求,这与最少的 q 相矛盾. 由于上述冗余与授权的位置构成了完整覆盖,因而只有上述两种冗余位置情况. 定理得证.

5.1.2 方案正确性证明

证明 首先在授权策略只有一级 (n,t) 门限策略下,排序后的格式化布尔表达式被转化共享矩阵 M:

$$\boldsymbol{M}=\begin{pmatrix}1&1&1&\cdots&1\\1&2&2^2&\cdots&2^{t-1}\\1&3&3^2&\cdots&3^{t-1}\\\vdots&\vdots&\vdots&\ddots&\vdots\\1&n&n^2&\cdots&n^{t-1}\end{pmatrix}$$

$$\boldsymbol{M}'=\begin{pmatrix}1&1&1&\cdots&1\\1&2&2^2&\cdots&2^{t-1}\\1&3&3^2&\cdots&3^{t-1}\\\vdots&\vdots&\vdots&\ddots&\vdots\\1&t&t^2&\cdots&t^{t-1}\end{pmatrix}$$

由于矩阵 $\boldsymbol{M}$ 形如范德蒙特行列式,任意行列线性无关,由此易得,矩阵 $\boldsymbol{M}^{\mathrm{T}}|\boldsymbol{\varepsilon}$ 任意行列线性无关,因此,线性方程组 $\boldsymbol{M}^{\mathrm{T}}\boldsymbol{X}=\boldsymbol{\varepsilon}$ 有解,则要求矩阵 $\boldsymbol{M}^{\mathrm{T}}$ 行数大于等于矩阵 $\boldsymbol{M}^{\mathrm{T}}|\boldsymbol{\varepsilon}$ 列数,也即是说参与方个数一定要大于 t. 在参与方个数大于阈值 t 的条件下,方程组一定有解. 在有解条件下,根据定理 2,方程组的解会出现第一种冗余情况,在算法 2 中,$X_i=0, i\in[t+1,n]$,将 0 元素回代到 $\boldsymbol{M}^{\mathrm{T}}\boldsymbol{X}=\boldsymbol{\varepsilon}$ 中,得到的系数矩阵 $\boldsymbol{M}'$. 这个方阵 $\boldsymbol{M}'$ 行列式 $|\boldsymbol{M}'|\neq 0$,且 $\boldsymbol{M}'^{\mathrm{T}}\boldsymbol{X}=\boldsymbol{\varepsilon}$ 有唯一非零解,也就是算法 2 求得的最小参与方的解.

当授权策略拥有 2 级(n,t)门限策略,根据文献[20]矩阵生成算法,2 级门限布尔表达式$((a_{1,1},\cdots,a_{1,n_1},t_1),(a_{2,1},\cdots,a_{2,n_2},t_2),\cdots,(a_{k,1},\cdots,a_{k,n_k}),t_k),t)$可以表示成如下分块矩阵:

$$\boldsymbol{M}=\begin{pmatrix}\boldsymbol{M}_{n_1,t_1}(1)&\boldsymbol{M}_{n_1,t_1}&0&\cdots&0\\\boldsymbol{M}_{n_2,t_2}(2)&0&\boldsymbol{M}_{n_2,t_2}&\cdots&0\\\vdots&\vdots&\vdots&\cdots&\vdots\\\boldsymbol{M}_{n_k,t_k}(k)&0&0&\cdots&\boldsymbol{M}_{n_1,t_k}\end{pmatrix}$$

其中,

$$\boldsymbol{M}_{n_j,t_j}(i)=\begin{pmatrix}i&i^2&\cdots&i^{t_j-1}\\i&i^2&\cdots&i^{t_j-1}\\\cdots&\cdots&\cdots&\cdots\\i&i^2&\cdots&i^{t_j-1}\end{pmatrix},$$

$$\boldsymbol{M}_{n_j,t_j}=\begin{pmatrix}1&1&\cdots&1\\1&2&\cdots&2^{t_j-1}\\\vdots&\vdots&\ddots&\vdots\\1&n&\cdots&n^{t_j-1}\end{pmatrix}.$$

使用算法 2 消元法求解 $\mathrm{sub}\ \boldsymbol{M}^{\mathrm{T}}\boldsymbol{X}=(1,0,0,\cdots,0)^{\mathrm{T}}$,$\mathrm{sub}\ \boldsymbol{M}^{\mathrm{T}}$ 为抽取 $\boldsymbol{M}^{\mathrm{T}}$ 中行形成的子矩阵线性方程组. 因为 $\boldsymbol{M}^{\mathrm{T}}$ 本为分块上三角矩阵,$\mathrm{sub}\ \boldsymbol{M}^{\mathrm{T}}$ 也为分块上三角矩阵,由于自上向下消元会优先消去排序靠后的未知变量,于是得到的解中,非零元集中靠前,而布尔表达式按照门限阈值 $t_1<t_2<\cdots<t_k$,从小到大排序,使得 $\mathrm{sub}\ \boldsymbol{M}^{\mathrm{T}}$ 所得解中非零元最少. 依此类推,当访问结构为 $d\geqslant 2$ 级门限策略时,上述结论同样成立.

综上所述,本文方案能够得到一个最小的授权参与方集合.

接下来使用一个满足定理 2 条件的布尔表达式,求解在出现定理 2 所述所有冗余情况下,得到的最终解中,冗余孩子关联参与方对应的常量值是否都为 0,来直观展示本文方案的正确性. 位置完全覆盖情况包括: 第一种位置、第二种位置和两种位置都满足的布尔表达式.

以授权策略$(A_{\mathrm{p}}\wedge((D_{\mathrm{p}},E_{\mathrm{p}},F_{\mathrm{p}},G_{\mathrm{p}},3)\vee(B_{\mathrm{p}}\wedge C_{\mathrm{p}}))$对应的格式化布尔表达式$(A_{\mathrm{p}},((D_{\mathrm{p}},E_{\mathrm{p}},F_{\mathrm{p}},G_{\mathrm{p}},3),(B_{\mathrm{p}},C_{\mathrm{p}},2),1),2)$为例,排序后为$(A_{\mathrm{p}},((B_{\mathrm{p}},C_{\mathrm{p}},2),(D_{\mathrm{p}},E_{\mathrm{p}},F_{\mathrm{p}},G_{\mathrm{p}},3),1),2)$,对于满足定理 2 所述冗余的第一种位置,所对应的两例授权集合分别为部分满足授权集合$\{A_{\mathrm{p}},B_{\mathrm{p}},C_{\mathrm{p}},D_{\mathrm{p}}\}$,孩子表达式$(B_{\mathrm{p}},C_{\mathrm{p}},2)$和 G_{p} 为冗余,关联的参与方 C_{p} 为冗余,全部满足授权集合$\{A_{\mathrm{p}},B_{\mathrm{p}},C_{\mathrm{p}},D_{\mathrm{p}},E_{\mathrm{p}},F_{\mathrm{p}}\}$,孩子表达式$(D_{\mathrm{p}},E_{\mathrm{p}},F_{\mathrm{p}},G_{\mathrm{p}},3)$为冗余,关联参与方$\{D_{\mathrm{p}},E_{\mathrm{p}},F_{\mathrm{p}}\}$为冗余; 对于第二种位置,所对应的一个授权集合为$\{A_{\mathrm{p}},B_{\mathrm{p}},D_{\mathrm{p}},E_{\mathrm{p}},F_{\mathrm{p}},G_{\mathrm{p}}\}$,孩子表达式$(B_{\mathrm{p}},C_{\mathrm{p}},2)$和 G_{p} 为冗余,关联参与方$\{B_{\mathrm{p}},G_{\mathrm{p}}\}$为冗余,注意到参与方 B_{p} 是第二种位置冗余,而参与方 G_{p} 是第一种位置冗余,授权集合$\{A_{\mathrm{p}},B_{\mathrm{p}},D_{\mathrm{p}},E_{\mathrm{p}},F_{\mathrm{p}},G_{\mathrm{p}}\}$同时满足两种位置冗余. 下面依次验证这几个授权集合下的常量值 $\boldsymbol{\omega}$ 解的结构是否如 5.1 所述.

首先根据文献[20]中算法,排序后的格式化布尔表达式$(A_{\mathrm{p}},((B_{\mathrm{p}},C_{\mathrm{p}},2),(D_{\mathrm{p}},E_{\mathrm{p}},F_{\mathrm{p}},G_{\mathrm{p}},3),1),2)$的共享矩阵为:

$$\boldsymbol{M}=\begin{pmatrix}1&1&0&0&0\\1&2&1&0&0\\1&2&2&0&0\\1&2&0&1&1\\1&2&0&2&4\\1&2&0&3&9\\1&2&0&4&16\end{pmatrix}$$

对应的参与方顺序列表 $P_L=(A_{\mathrm{p}},B_{\mathrm{p}},C_{\mathrm{p}},D_{\mathrm{p}},E_{\mathrm{p}},F_{\mathrm{p}},G_{\mathrm{p}})$.

对于授权集合$\{A_{\mathrm{p}},B_{\mathrm{p}},C_{\mathrm{p}},D_{\mathrm{p}}\}$(实际中授权集合参与方出现顺序与得到的常量值解没有关系,这里仅仅是书写上的方便),对应线性方程组求解系数矩阵 $\boldsymbol{A}$ 及化成行阶梯后的增广矩阵 $\boldsymbol{B}'$ 分别为:

$$\boldsymbol{A}=\begin{pmatrix}1&1&1&1\\1&1&1&1\\0&1&1&0\\0&0&0&1\\0&0&0&1\end{pmatrix},\boldsymbol{B}'=\begin{pmatrix}1&1&1&1&1\\0&1&1&1&-1\\0&0&1&-1&1\\0&0&0&1&0\\0&0&0&0&0\end{pmatrix}$$

按照算法 2 给出的回代方法,得到的解为: $\omega_1 = X_1 = 2, \omega_2 = X_2 = -1, \omega_3 = X_3 = 1, \omega_4 = X_4 = 0$. 得到最小授权参与方$\{A_p, B_p, C_p\}$所对应的常量值不为 0,而冗余参与方 D_p所对应的常量值为 0.

对于授权集合$\{A_p, B_p, C_p, D_p, E_p, F_p\}$,求解过程同上面,不予赘述,最终求解得到的常量值: $\omega_1 = 2, \omega_2 = -1, \omega_3 = 1, \omega_4 = \omega_5 = \omega_6 = 0$. 得到最小授权参与方$\{A_p, B_p, C_p\}$所对应的常量值不为 0,而冗余参与方$\{D_p, E_p, F_p\}$所对应的常量值为 0.

对于授权集合$\{A_p, B_p, D_p, E_p, F_p, G_p\}$,同样,最终求解得到的常量值: $\omega_1 = 2, \omega_2 = 0, \omega_3 = -3, \omega_4 = 3, \omega_5 = -1, \omega_6 = 0$. 得到最小授权参与方$\{A_p, D_p, E_p, F_p\}$所对应的常量值不为 0,而冗余参与方$\{B_p, G_p\}$所对应的常量值为 0.

由此,以上 3 种实例作为一个冗余位置的完整覆盖,验证了本文所提方案的正确性.

5.2 计算开销

由算法 2 的回代公式可知,本文方案在生成共享矩阵之前,需要对格式化布尔表达式进行排序,而这个排序过程(在生成私钥或加密时进行,这种运算一般由服务器或云端预先完成,产生的开销在服务器端或云端.)产生的开销与解密过程无关,因而无需考虑.

对于求解线性方程组的算法部分,只考虑乘除法的运算,由文献[20]转换算法可以推知,共享矩阵 M 的列数 m 为所有非叶孩子格式化布尔表达式阈值减 1 之和再加 1,与行数 $|I|$ 满足 $m \leqslant |I|$. 在线性方程组系数矩阵 A 中,共享矩阵 M 的列数 m 为系数矩阵 A 的行数,而列数为参与方的个数 $|S|$. 在求解期间计算量为:

(1) 消元期间计算量:

$$\begin{cases} \sum_{k=1}^{m-1}(m-k)(m-k+2) + (|S|-m)\sum_{k=1}^{m-1}(m-k) = m(m-1)(3|S|-m+5)/6, & |S| \geqslant m \\ \sum_{k=1}^{|S|-1}(|S|-k)(|S|-k+2) = m(m-1)(2m+5)/6, & |S| = m \\ \sum_{k=1}^{|S|-1}(|S|-k)(m-k+2) = |S|(|S|-1)(2|S|+5)/6 + |S|(|S|(m-|S|)), & |S| < m \end{cases}$$

(2) 回代计算原始高斯消元求解的计算量:

$$\begin{cases} \sum_{k=1}^{|S|-1}(|S|-k+1) = |S|(|S|+1)/2, & |S| < m \\ \sum_{k=1}^{m-1}(m-k+1) = m(m+1)/2, & |S| \geqslant m \end{cases}$$

因而总的计算开销/计算复杂度为:

$$\begin{cases} |S|(3|S|m+3|S|-1-2|S|^2)/3 = O(|S|^2 m), & |S| < m \\ m(m-1)(3|S|-m+5)/6 + m(m+1)/2 = O(|S|m^2), & |S| \geqslant m \end{cases}$$

5.3 效率分析

3.2 节中秘密恢复计算过程,从理论上已经说明减少参与方进行解密计算,可以减少解密开销. 由于在无授权策略情况下,文献[11]已无法得到最小参与方集合,冗余参与方会参与解密过程,而在文献[11]基础上应用本文方案,5.1 节已经论证,可以找到最小参与方. 为了得出实际条件下,冗余参与方对解密开销的影响,本文在此给出进一步的对比实验. 实验方案如下: 设定全局参与方个数为 100,最小参与方个数为 50,然后冗余参与方个数从 0 依次递增到 50,依次分别得出使用本文方案和未使用本文方案后的计算开销. 为此我们首先实现了文献[11]属性密码算法,然后在其上应用本文方案. 实验平台具体情况: 操作系统为 Windows 7 64 位旗舰版,CPU 为 Intel 酷睿 i7-3612qm,主频 3.0GHz,8GB RAM,代数库使用的 Java Pairing-Based Cryptography library(JPBC)[24],版本为 1.2.1. 使用基本域大小为 512bit、阶为 160bit 的 Type A 对称曲线. 解密操作重复运行 10 次.

从图 1 中可以看出,使用本文方案后,解密计算开销,不随着冗余参与方的变化而变化. 而文献[11]在没有授权策略下,只能直接求出常量值,其解密开销随着冗余参与方个数的增多而增大,当冗余参与方个数与最小参与方个数相等时,其计算开销几乎达到了本文开销的 3 倍.

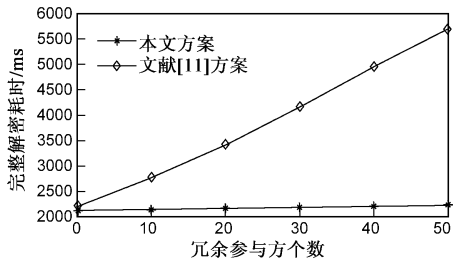

图1 冗余参与方下本文方案所带来的效率提升

从算法 2 的计算过程来看,本文中冗余参与方仍然参与了常量值计算过程. 为得出冗余参与方对于解密效率的影响,我们首先使用一个最小参与方进行分析. 由于转化后的矩阵满足最小参与方 $|S'| \leqslant m$,因此求解常量值算法复杂度为 $O(|S'|^2 m) < O(|S|^2 m)$,这说明冗余的参与方在求解常量值时会带来额外的开销. 由于线性方程组的求解是在有限域 Z_p上的,因而开销不可忽略. 为了进一步得出冗余参与方常量值求解

对最终秘密恢复的影响,设计如下实验方案: 设定全局参与方个数为 100,最小参与方个数为 50,然后冗余参与方个数从 0 依次递增到 50,依次分别得出求解常量值和完整解密操作所需时间开销. 实验平台同上,最终得到的实验结果处理后如图 2 所示.

从图 2 可以看出,常量值计算和解密时间都是随着冗余参与方个数增多而增多,其中,在线性方程组求解过程中,当$|S|\geqslant m$,也即冗余参与方个数大于 0 之后,所带来的开销确如式 $O(|S|m^2)$ 所示,随$|S|$增大呈线性增长. 而给最终解密带来的额外开销也来自于冗余参与方求解过程,可以看到即使冗余参与方个数同最小参与方个数相同,相比解密中其它计算过程,常量值求解所占开销仍然相对较小.

而对于文献[11]中方案,由于不能搜寻最小参与方,故而所有参与方都参与计算,包括常量值求解和后面的解密计算. 在这种情况下,使用高斯消元求解计算开销为 $O(|S|m^2)$,为了验证其求解效率,及对最终解密效率影响,设计如下实验方案: 设定初始全局参与方个数 50,然后参与方个数从 50 依次递增到 100,依次分别得出求解常量值和完整解密操作所需时间开销. 实验平台和环境同上,最终得到的实验结果处理后如图 3 所示.

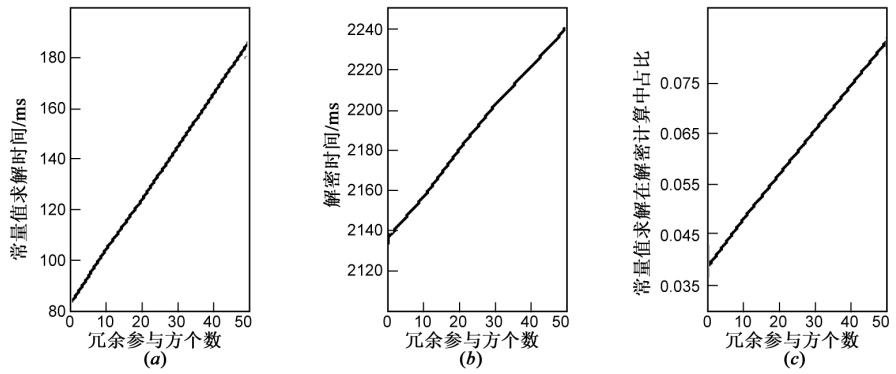

图2　冗余参与方对本文方案常量值求解及解密效率影响

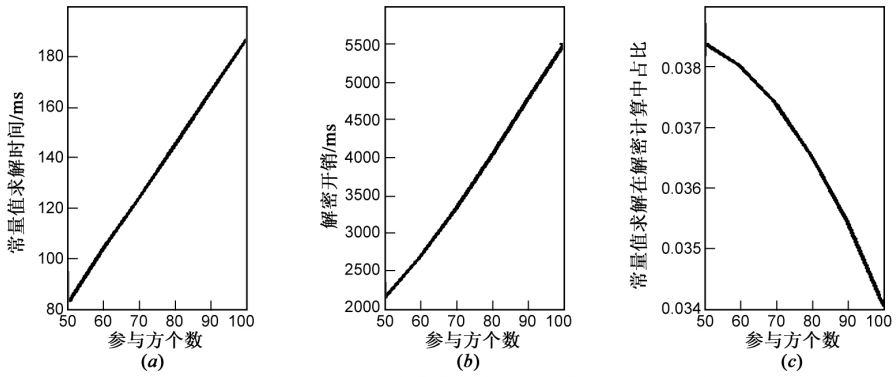

图3　文献[11]参与方个数对常量值求解及解密效率影响

从图 3 可以看出,虽然文献[11]在无法搜寻最小参与方情况下,解密过程中,常量值计算时间的占比,要比本文方案还要小,并且随着参与方增多占比以小幅度逐渐减小,但从图 3 中可以看到,其常量值计算时间仍然与本文方案是一致的,而解密计算的开销却随着参与方个数的增长而大幅增长. 因此这个占比的减少不具多少实质意义.

6　结论

在这篇文章中,针对一些基于属性密码机制的应用,无法附加授权策略导致现有解密效率提高方案不能适用的问题. 我们提出了一种无授权策略下的解密效率提高方案,它能够在无授权策略下,找到最小的参与方来进行解密计算,因而能够提高解密效率. 理论和实验结果表明,本文方案的确有效提高了这种情况下的属性密码解密效率. 考虑如何应用本文方案解决第 1 章所述应用安全性问题,是本文的下一步工作计划.

致谢　感谢匿名评审专家给本文提出的修改意见,感谢蔡朝晖和涂国庆老师给予的支持与帮助.

参考文献

[1] 苏金树,曹丹,王小峰,等. 属性基加密机制[J]. 软件学报,2011,22(6):1299－1315.
SU Jin-Shu,CAO Dan,WANG Xiao-Feng,et al. Attribute-

based encryption schemes [J]. Journal of Software, 2011, 22 (6): 1299 - 1315. (in Chinese)

[2] Sahai A, Waters B. Fuzzy identity-based encryption [A]. Aarhus: Advances in Cryptology-EUROCRYPT 2005 [C]. Berlin: Springer, 2005. 457 - 473.

[3] Bethencourt J, Sahai A, Waters B. Ciphertext-policy attribute-based encryption [A]. Procceedings of the 2007 IEEE Security and Privacy [C]. Oakland: IEEE, 2007. 321 - 334.

[4] 俞能海,郝卓,徐甲甲,等. 云安全研究进展综述 [J]. 电子学报, 2013, 41(2): 371 - 381.
YU Neng-hai, HAO Zhuo, XU Jia-jia, et al. Review of cloud computing security [J]. Acta Electronica Sinica, 2011, 41 (2): 371 - 381. (in Chinese)

[5] 吴吉义,傅建庆,平玲娣,等. 一种对等结构的云存储系统研究 [J]. 电子学报, 2011, 39(5): 1100 - 1107.
WU Ji-yi, FU Jian-qing, PING Ling-di, et al. Study on the P2P cloud storage system [J]. Acta Electronica Sinica, 2011, 39(5): 1100 - 1107. (in Chinese)

[6] Yang K, Jia X, Ren K. Attribute-based fine-grained access control with efficient revocation in cloud storage systems [A]. Proceedings of the 8th ACM SIGSAC Symposium on Information, Computer and Communications Security [C]. Berlin: ACM, 2013. 523 - 528.

[7] S Yu, C Wang, K Ren, W Lou. Achieving secure, scalable, and fine-grained data access control in cloud computing [A]. Proceedings of the 2010 IEEE INFOCOM [C]. San Diego: IEEE, 2010. 1 - 9.

[8] J Hur, D K Noh. Attribute-based access control with efficient re-vocation in data outsourcing systems [J]. IEEE Transactions on Parallel and Distributed Systems, 2011, 22 (7): 1214 - 1221.

[9] Zhou Z, Huang D. On efficient ciphertext-policy attribute based encryption and broadcast encryption [A]. Proceedings of the 17th ACM Conference on Computer and Communications Security [C]. Chicago: ACM, 2010. 753 - 755.

[10] Shamir A. How to share a secret [J]. Communications of the ACM, 1979, 22(11): 612 - 613.

[11] Hohenberger S, Waters B. Attribute-based encryption with fast decryption [A]. Public-Key Cryptography-PKC 2013 [C]. Berlin: Springer, 2013. 162 - 179.

[12] Waters B. Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization [A]. Public Key Cryptography-PKC 2011 [C]. Berlin: Springer, 2011. 53 - 70.

[13] Lewko A, Okamoto T, Sahai A, et al. Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption [A]. Advances in Cryptology-EUROCRYPT 2010 [C]. Berlin: Springer, 2010. 62 - 91.

[14] Lewko A, Waters B. Decentralizing attribute-based encryption [A]. Advances in Cryptology-EUROCRYPT 2011 [C]. Berlin: Springer, 2011. 568 - 588.

[15] Jackson P, Sheridan D. The optimality of a fast CNF conversion and its use with SAT [A]. Procceedings of the 7th International Conference on Theory and Applications of Satisfiability Testing [C]. Vancouver: Springer, 2004. 827 - 831.

[16] Golub G H, Van Loan C F. Matrix Computations [M]. Baltimore: JHU Press, 2012. 335 - 340.

[17] Yu S, Ren K, Lou W, et al. Defending against key abuse attacks in KP-ABE enabled broadcast systems [A]. Security and Privacy in Communication Networks [C]. Berlin: Springer, 2009. 311 - 329.

[18] Li J, Ren K, Kim K. Accountable attribute-based broadcast [A]. Procceedings of the 2009 IEEE Security and Privacy [C]. Oakland: IEEE, 2009. 16 - 22.

[19] Li J, Ren K, Zhu B, et al. Privacy-aware attribute-based encryption with user accountability [A]. Information Security [C]. Berlin: Springer, 2009. 347 - 362.

[20] Liu Z, Cao Z. On Efficiently Transferring the Linear Secret-Sharing Scheme Matrix in Ciphertext-policy Attribute-based Encryption [EB/OL]. http://eprint.iacr.org/2010/374.pdf, 2010-07-06/2014-02-26.

[21] Beimel A. Secure Schemes for Secret Sharing and Key Distribution [D]. Haifa, Israel: Israel Institute of Technology, Technion, 1996.

[22] Nikov V, Nikova S. New Monotone Span Programs from Old [EB/OL]. http://eprint.iacr.org/2004/282.pdf? origin=publication_detail, 2004-09-17/2014-02-26.

[23] Angelo De Caro. Benchmark of JPBC [EB/OL]. http://gas.dia.unisa.it/projects/jpbc/benchmark.html#.Uw19d_QW3vQ, 2013-12-04/2014-02-26.

作者简介

刘梦君 男,1988 年 5 月出生于湖北黄冈. 现为武汉大学计算机学院博士生. 主要研究方向为移动计算与无线网络、移动社交与分布式系统中的安全及隐私.
E-mail: lmj_whu@163.com

刘焘波(通信作者) 男,1970 年 11 月出生于黑龙江齐齐哈尔. 1993 年毕业于武汉水利电力大学应用电子专业. 现为武汉大学计算机学院教授、博士生导师,从事信息系统安全、物联网及其安全和嵌入式系统等方面的研究工作.
E-mail: liu.shubo@163.com

王 颖 女,1991 年 2 月出生于湖北武汉. 硕士生. 主要研究方向为嵌入式及信息安全.
E-mail: 543988022@qq.com