基于矢量空间的属性基签密方案

刘 佳,王建东,庄 毅
(南京航空航天大学计算机科学与技术学院,江苏南京 210016)

摘 要: 本文提出了属性基签密方案,通过引入签密思想,将属性基加密ABE改造为属性基签密ABSC,使其可以近似一次加密运算的代价完成加密和签名,或以近似一次签名运算的代价完成双向认证;通过在矢量空间上对ABSC进行的门限构造,打破了阈值对算法执行的限制;并且基于离散对数问题进行了可验证性构造,可以发现和避免来自于协议执行方内部的欺骗.

关键词: 属性基, 矢量空间, 签密
中图分类号: TP309 **文献标识码:** A **文章编号:** 0372-2112 (2013)04-0776-05
电子学报URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2013.04.025

Attribute-Based Signcryption Scheme on Vector Space

LIU Jia, WANG Jian-dong, ZHUANG Yi
(*College of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing, Jiangsu* 210016, *China*)

Abstract: This paper proposed attribute-based signeryption (ABSC) scheme. By introducing the idea of signeryption, attribute-based eneryption (ABE) was improved to attribute-based signeryption, which can complete eneryption and signature with the cost of once encryption, or to complete the mutual authention and signature with the cost of once eneryption, or to complete the mutual authentication with the cost of once signature. Through constructing the access structure on vector space, ABSC breaks the threshold limit. And based on the discrete logarithm problem, the verification algorithm was designed so that the deceptions from the internal participants can be found.

Key words: attributed-based; vector space; signcryption

1 引言

属性基加密方案(attribute based encryption, ABE)在2005年由Sahai[1]等首次提出,随后得到了广泛的关注和快速发展,目前已设计出多种属性基加密、数字签名方案和密钥交换等安全协议[2~5],并在随机预言模型[6]或标准模型[7,8]下证明了其安全性,然而这些协议都是以拉格朗日差值多项式方法为基础进行构造的,即协议得以正确执行的前提是,参与协议的双方所具有的属性集中相同属性的个数必须大于构造时所选择的拉格朗日插值多项式的最高项次数,从而使这类协议的适用范围受到了限制.2007年,Water等人首次通过线性秘密分享的方法,在矢量空间上构造了标准模型下可证安全的CPABE(ciphertext policy ABE)方案[9],打破了目前众多方案中只能使用拉格朗日插值多项式进行构造的模式,不论在表述能力上还是安全证明上都有很大的贡献,然而该方案基于传统的"先加密后签名"的思路,无法同时提供安全高效的数据保密性、完整性和不可否认性服务.

本文将矢量空间上的属性基密码构造方法引入签密[10]之中,提出了一个矢量空间上的属性基签密方案,该方案能够以近似于一次加密运算的速度完成数据加密和数字签名.同时,定义了更为灵活的访问结构,任意满足访问结构属性组的用户均可正确进行签密和解签密运算,使得协议的执行不再受到参与双方相同属性个数的制约.最后,通过简单的运算,该方案还可实现第三方检验,有效避免了协议执行过程中的欺骗.

2 相关工作

2.1 基于矢量空间的秘密共享

设定 $A=\{A_1,A_2,\cdots,A_n\}$ 是 n 个参与者的集合,y 为要隐藏的秘密,Γ 是由 A 的子集构成的集合,并满足条件:Γ 中的元素是由能够计算出秘密 y 的参与者所构

收稿日期:2012-06-11;修回日期:2012-08-16
基金项目:国家863高技术研究发展计划(No.2008AA706103);航空科学基金(No.2010ZC13012)

成的集合,则称 Γ 为访问结构,Γ 中的元素称为授权子集,记作 B.设 $D \notin A$, $Q = GF(q)$, q 为大素数, Qw 表示 Q 上所有 w 元构成的矢量空间.如果存在函数 $\varphi: A \cup \{D\} \rightarrow Q^w$ 满足特性:

$$\varphi(D) = (1,0,\cdots,0)_w \in < \varphi(A_i) = (a_{1i}, a_{2i}, \cdots, a_{wi}) : A_i \in B > <=> B \in \Gamma$$

那么 Γ 是一个矢量空间访问结构[11].即矢量 $\varphi(D)$能表示为集合$\{\varphi(A_i) : A_i \in B\}$中向量的线性组合,当且仅当 B 是一个授权子集,可表示为 $\varphi(D) = \lambda_1\varphi(A_1) + \lambda_2\varphi(A_2) + \cdots + \lambda_p\varphi(A_p)$,这里 λ_i 是矢量空间的线性表出系数,可由 B 中成员公开计算获得[11].选择向量 $V = (y, v_2, \cdots, v_w)$,其中 $v_2, v_3, \cdots, v_w$ 为 Q 上的随机数,显然有 $y = V\varphi(D) = V\lambda_1\varphi(A_1) + V\lambda_2\varphi(A_2) + \cdots + V\lambda_p\varphi(A_p)$,若将 $V\varphi(A_i)$作为 A_i 的私钥进行分配,则可由授权子集 B 上的用户协作计算完成秘密 y 的恢复.这种秘密构造方案称为矢量空间秘密构造方案.很明显,只要令 $\varphi(A_i) = (1, a_i, a_i^2, \cdots, a_i^{w-1})$,拉格朗日插值多项式构造方法即成为矢量空间秘密共享方案中的一个特例,其中 a_i 是 Q 中的非零元素[12].

2.2　SW 属性基加密方案

属性基加密 ABE 由 Sahai[1]等于 2005 年首次提出,现已成为目前进行属性基各种相关研究的基础,以下简要介绍该方案.

设 G_1, G_2 是阶为素数 p 的乘法交换群, g 是 G_1 的生成元, $e: G_1 * G_1 \rightarrow G_2$ 是一个双线性对,满足以下三个性质:①双线性:若 $u, v \in G_1$,且 $a, b \in Zp^*$,则 $e(u^a, v^b) = e(u, v)^{ab}$;②非退化性: $e(g, g) \neq 1$;③可计算性:若 $u, v \in G_1$,则存在多项式时间算法计算 $e(u, v) \in G_2$. $\Delta_{i,s}(x) = \prod_{j \in s, j \neq i} (x - j)/(i - j)$ 是拉格朗日多项式系数,其中 $i \in Zp$, s 是 Zp 的一个子集.用户的属性由 Zp 上 n 个元素表示, v 是设定的相同属性个数.该方案由以下四个步骤组成:

(1)系统建立:系统随机选取整数 $t_1, t_2, \cdots, t_n \in Zp$ 和 $y \in Zp$,计算 $T_1 = g^{t1}$, $T_2 = g^{t2}$, $\cdots$, $T_n = g^{tn}$, $Y = e(g, g)^y$,系统公开参数为$\{T_1, T_2, \cdots, T_n, Y\}$,系统私钥 master key 为$\{t_1, t_2, \cdots, t_n, y\}$.

(2)私钥生成:系统首先随机选取一个 $v-1$ 阶多项式 $q(x)$,并使 $q(0) = y$,用户长期私钥为 $(D_i)_{i \in ID} = (g^{q(i)/ti})_{i \in ID}$.

(3)加密:设加密者 ID 为 A,解密者 ID 为 B,待加密明文记作 M,则系统随机选取 $x \in Zp$,计算密文 $E = (A, E' = MY^x, \{E_i = T_i^x\}_{i \in A})$.

(4)解密:解密者 B 的属性集合若满足 $|B \cap A| \geqslant v$,则可计算进行解密 $M = E' / \prod_{i \in s} e(D_i, E_i)^{\Delta_{i,s(0)}}$.

属性基密码算法与身份基密码算法[13,14]相比,具有更加灵活的应用环境,它不以用户的一个特征来识别用户身份,而是结合了一组可描述用户的属性集合,由该集合属性值的契合程度共同对用户身份进行认定.属性集合中元素个数可变,为该方案提供了更为灵活的应用环境;属性集合定义的方式,又使得属性集可以映射到一组有共同特征的用户,从而可以方便的实现群用户上的各种密码学应用.

2.3　Zheng 基本签密方案

签密由 Zheng 首次提出,与传统的"先签名再加密"或"先加密再签名"协议相比,签密在确保数据的完整性、机密性、不可否认性的前提下,在计算速度和效率上进行提升,使其以一次加密运算或者签名运算的代价完成加密和签名[10].Zheng 的基本签密方案由以下四个步骤组成:

(1)系统建立:选取系统参数 p:随机选取的大素数; q: $q | (p-1)$; g: Zp^* 上的随机数,且 $Ord(g) = q$; $G(\cdot)$, $H(\cdot)$:Hash 函数; $E\tau$:以 τ 为密钥的对称加密算法; $D\tau$:对应于 $E\tau$ 的解密算法.

(2)私钥生成:随机选取 $x \in Zq$,计算 $y = g^x \bmod p$, x 为用户私钥, y 为对应公钥.

(3)签密:设签密方为 A,公钥 y_A,私钥 x_A;解签密方为 B,公钥 y_B,私钥 x_B,签密运算过程为:①在 Zq 上随机选取参数 x,计算 $K = y_B^x \bmod p$;②计算 $\tau = G(K)$; $c = E\tau(m)$;③计算 $r = H(m \| y_A \| y_B \| K)$;④计算 $s = (rx_A - x) \bmod q$;⑤输出签密结果 $C = (c, r, s)$.

(4)解签密: B 对其收到的密文 $C = (c, r, s)$进行解签密计算,以恢复明文 m,同时验证 A 的签名,步骤如下:①计算 $w = y_A^r g^{-s} \bmod p$;②计算 $K = w^{x_B} \bmod p$;③计算 $\tau = G(K)$;④解密 $m = D\tau(c)$,若满足 $H(m \| y_A \| y_B \| K) = r$,则通过验证,返回消息 m;否则拒绝.

签密算法可以以一次密码运算的时间代价,同时完成加密和签名运算,从而使公钥密码算法的运算速度得到很大的提升.下文以签密算法为基础,结合属性基密码构造方法,基于矢量空间秘密分享策略进行算法构造.

3　基于矢量空间的属性基签密方案

3.1　方案描述

本文首次将矢量空间秘密共享思想引入签密之中,构造灵活的属性基签密方案.该方案使得具有一组属性 A_1 的人可针对另一组属性 A_2 进行签密运算,其签密文件可以被任一具有 A_2 属性的人进行解密,并同时可验证该文件是否真正由具有 A_1 属性的成员给出,其中 A_1, A_2 为属性集 A 的授权子集.系统的执行代价近

似于一次属性基加密解密运算.基于矢量空间的属性基签密方案由系统建立(Setup)、私钥生成(KeyGen)、属性基签密运算(AB-SC, attribute based signcryption)、属性基解签密运算(AB-USC, attribute based unsigncryption)四个算法组成,具体描述如下:

算法 1 系统建立 Setup:设 G_1, G_2 是阶为素数 p 的乘法交换群,g 是 G_1 的生成元,$e: G_1 * G_1 \rightarrow G_2$ 是一个双线性对,系统中全部属性集合 $A = \{a_1, a_2, \cdots a_n\}$.

①系统随机选取整数 $t_1, t_2, \cdots t_n \in Zp$, t_i 分别对应与某项属性 a_i,计算 $T_1 = g^{t1}, T_2 = g^{t2}, \cdots T_n = g^{tn}$;

②系统随机选取 $y \in Zp$,计算 $Y = e(g, g)^y$;

③系统公开参数为 $\{T_1, T_2, \cdots T_n, Y\}$,系统私钥 master key 为 $\{t_1, t_2, \cdots t_n, y\}$.

算法 2 私钥生成 KeyGen:对某一系统用户 p,该用户的属性集合是 A 的一个子集,记作 Ap.系统随机选取 $v_2, v_3, \cdots, v_w \in Zp$,并令 $V = (y, v_2, v_3, \cdots, v_w)$,选取函数 $\varphi: A \cup \{D\} \rightarrow Zp^w$,对 Ap 中的每一个属性 i 计算 $Di = g^{V\varphi(i)/t_i}$,用户长期私钥即为 $\{Di\}_{i \in Ap}$.

算法 3 签密运算 AB-SC:假设签密方为 P_1,其属性集合记作 A_1,其私钥为 $D = \{D_i\}_{i \in A1}$;解签密方为 P_2,其属性集合记作 A_2,其私钥为 $D = \{D_i\}_{i \in A2}$. M 为待签密的原文,$H_1(\ )$和 $H_2(\ )$为公开的哈希函数.签密过程如下:

① 在 Zp 上选取随机数 x,计算 $\sigma = \{T_i^x\}_{i \in A2}$;

② 计算 $r = H_1(\sigma \| M)$;

③ 计算 $s = \{D_i^{rx}\}_{i \in A1}$;

④ 计算 $E = M * H_2(Y^x)$;

⑤ 输出签密结果 $C = (E, \sigma, s)$.

算法 4 解签密运算 AB-USC:具有属性组 A_2 的用户集合中的任意一人 P_2 都可对此签密文件 $C = (E, \sigma, s)$进行解签密运算,还原明文 M,并同时验证文件来源是否为属性组 A_1 中成员.解签密运算过程如下:

① 计算 $\beta = \prod\limits_{i \in A_2} e(D_i, \sigma)^{\lambda i}$,其中 λ_i 为矢量空间线性表出系数,可由 P_2 公开计算获得[11];

② 计算 $M = E / H_2(\beta)$;

③ 计算 $r = H_1(\sigma \| M)$;

④ 计算 $\mu = \prod\limits_{i \in A_1} e(s, T_i)^{\lambda i}, \mu' = \beta^r$;

⑤ 若 $\mu = \mu'$,则验证通过,返回解密后的消息 M,否则拒绝.

3.2 正确性证明

定理 1 设 A_2 为属性集 A 上访问结构 Γ 中的一个授权子集,系统通过 AB-SC 进行签密运算,则所有满足 A_2 属性组的用户,都可通过 AB-USC 算法,正确计算恢复明文.

证明:由 AB-USC 算法可知 $\beta = \prod\limits_{i \in A_2} e(D_i, \sigma)^{\lambda i}$

由 AB-SC 算法可知 $\sigma = \{T_i^x\}_{i \in A2}$

由私钥生成算法 KeyGen 可知 $Di = g^{V\varphi(i)/ti}$

因此, $\beta = \prod\limits_{i \in A_2} e(D_i, \sigma)^{\lambda i} = \prod\limits_{i \in A_2} e(g^{V\varphi(i)/t_i}, g^{xt_i})^{\lambda_i}$

$= \prod\limits_{i \in A_2} e(g^{\lambda_i V\varphi(i)}, g^x) = e(g^{\sum_{i \in A_2} \lambda_i V\varphi(i)}, g^x)$

又因为 A_2 是 A 上的一个授权子集,因为由矢量空间的构造可知:

$\varphi(D) = \lambda_1 \varphi(a_1) + \lambda_2 \varphi(a_2) + \cdots + \lambda_m \varphi(a_m)$

因此,

$g^{\sum_{i \in A_2} \lambda_i V\varphi(i)} = g^{\lambda_1 V\varphi(a_1) + \lambda_2 V\varphi(a_2) + \cdots + \lambda_m V\varphi(a_m)} = g^{V\varphi(D)} = g^{(y, v_2, v_3, \ldots, v_w) \cdot (1,0,0,\ldots,0)_w} = g^y$

所以,$\beta = e(g^y, g^x) = e(g, g)^{xy} = Y^x$

由 AB-SC 第④步运算可知 $E = M * H_2(Y^x)$

因此,$M = E / H_2(Y_x) = E / H_2(\beta)$,即 AB-USC 的第①,②步运算可正确恢复出明文 M,得证.

定理 2 设 A_1, A_2 为属性集 A 上访问结构 Γ 中的授权子集,系统通过 AB-SC 进行签密运算,则所有满足 A_2 属性组的用户,都可通过 AB-USC 算法,在正确计算恢复出明文 M 的同时,还可以对信息的来源进行认证,以确保密文 C 来源于属性组 A_1 中的用户.

证明:由定理 1 可知,符合 A_2 属性组的任一用户都可以通过 AB-USC 算法计算恢复出明文 M,则可计算得 $r = H_1(\sigma \| M)$,并进一步进算得 $\mu' = \beta^r$.

由 AB-USC 的第④步运算知 $\mu = \prod\limits_{i \in A_1} e(s, T_i)^{\lambda i}$

由 AB-SC 可知 $s = \{D_i^{rx}\}_{i \in A1}$

由私钥生成算法 KeyGen 知 $Di = g^{V\varphi(i)/t_i}$

因此,

$\mu = \prod\limits_{i \in A_1} e(s, T_i)^{\lambda i} = \prod\limits_{i \in A_1} e(g^{rxV\varphi(i)/t_i}, g^{t_i})^{\lambda_i}$

$= \prod\limits_{i \in A_1} e(g^{\lambda_i V\varphi(i)}, g)^{xr} = e(g^{\sum_{i \in A_1} \lambda_i V\varphi(i)}, g)^{xr}$

又因为 A_1 是 A 上的一个授权子集,因为由矢量空间的构造可知:

$\varphi(D) = \lambda_1 \varphi(a_1) + \lambda_2 \varphi(a_2) + \cdots + \lambda_n \varphi(a_n)$

因此,

$g^{\sum_{i \in A_1} \lambda_i V\varphi(i)} = g^{\lambda_1 V\varphi(a_1) + \lambda_2 V\varphi(a_2) + \cdots + \lambda_n V\varphi(a_n)}$

$= g^{V\varphi(D)} = g^{(y, v_2, v_3, \cdots, v_w) \cdot (1,0,0,\cdots,0)_w} = g^y$

所以,$u = e(g^y, g)^{xr} = e(g, g)^{yxr} = Y^{xr} = \beta^r$

对于密文 $C = (E, \sigma, s)$,因其 s 运算的输入项包含了签密方私钥、签密方选择的随机数 x 以及待签密的明文 M 等信息,而在解签密过程中则使用了签密方属性组相对应的公钥进行运算,因此若签密方身份正确,则由上述证明可知,必然有 $u = \beta^r = \mu'$,验证成功并接

受恢复的明文 M;否则验证失败.

3.3 效率和安全性分析

基于矢量空间的属性基签密方案,可以为云计算中的各种信息交互提供灵活高效的机密性、完整性和不可否认性保障,并且通过简单运算,可以实现第三方检验.

(1)高效性:该方案的签密运算过程主要包含两次 G_1 群上的指数运算和一次 G_2 群上的指数运算,与 SW 属性基加密方案[1]中的加密运算相比,只增加了一次 G_1 群上的指数运算;在解签密运算时,较 SW 方案的解密过程,也只增加了一次双线性对运算,以较小的代价同时完成数据加密和数字签名.算法在通信量上,也只比传统的属性基加密方案增加了 G_1 群上的一个成员,非常适合于在云计算、普适计算、ad hoc 网络等要求低功耗低运算量的环境下进行应用.

(2)灵活性:在矢量空间上构造基于属性的签密方案,使得用户可以使用其具备的各种属性中的某些子集进行签密运算,运算针对对方一组属性集完成,使得符合这些属性集的用户可以对文件进行解密,并且同时验证签名.基于属性的构造方法保证了该方案应用环境的灵活性,方案的参与双方都可不是指定的某人,而是由属性集合灵活进行界定某一群体.而基于矢量空间的构造,又使得该方案与基于拉格朗日插值多项式构造的各种密码方案相比,其执行不必受限于某一固定的属性个数阈值,在应用上更具灵活性.

(3)保密性:在签密过程中输入特定属性组的公钥进行运算,使得满足该访问结构属性组的用户才可使用相应的私钥进行解签密,恢复明文;同时协议利用了系统公开参数和 master key 进行构造,使得整个签密与解签密过程不可被伪造和替代;基于文献[15]给出的证明,同理可证本文提出的矢量空间下的属性基签密运算在 DBDH 假设下是 CCA2 安全的.

(4)完整性与不可否认性:本文给出的方案在签密的过程中输入了签密方属性组的私钥进行运算,使得解签密方可以通过系统给出的公开参数对签密方属性进行验证,同时由于解签密运算还需要输入恢复出的明文项,因此,只有当签密和验证时所使用的属性公、私钥相互匹配,并且运算时输入的解密所得的明文正确,验证才能得以通过,从而保证了信息的完整性和不可否认性.

(5)第三方检验:签密方只需要提供 $E'=(s,r,k=Y^x)$给第三方,第三方则可以通过验证等式 $\prod e(s,T_i)^{\lambda i}=k^r$ 是否成立进行检验,其中 λ^i 是可以公开计算获取的线性表出系数[11].因为若 E'的确由消息所声称的来源方给出,则 $\prod e(s,T_i)^{\lambda i}=\prod e(g^{v\lambda i\varphi(i)/ti},g^{ti})^{xr}=Y^{xr}=k^r$.

4 结束语

属性基密码使得安全协议的执行者可以不再是指定的人或单位,而是满足属性集合的用户集中的任一用户,本文基于属性基密码思想,在矢量空间上构造了 CCA2 安全的可验证签密方案,该方案通过属性集授权子集的定义给出了更为灵活的访问方式,使协议的执行不再受限于某些属性组或属性的个数,并且以近似于属性基加密的代价同时完成加密和签名,高效灵活的提供了信息的保密性、完整性和不可否认性.

参考文献

[1] Sahai A, Waters B. Fuzzy ideneity-based encryption[A]. EUROCRYPT 2005, LNCS 3494[C]. Berlin: Springer-Verlag, 2005.457 – 473.

[2] Nishide T, Yoneyama K, Ohtak K. Attribute based encryption with partially hidden encryptor-specified access structure[A]. ACNS 2008, LNCS 5037[C]. Berlin: Springer-Verlag, 2008. 111 – 129.

[3] Goyal V, Jain A, Pandey O, et al. Bounded ciphertext policy attribute based encryption[A]. ICALP 2008, LNCS 5126[C]. Berlin: Springer-Verlag, 2008.579 – 591.

[4] Simak F S, Reihaeh S N. Threshold attribute based signatures and their application to anonymous credential systens[A]. AFRICACRYPT 2009, LNCS 5580[C]. Berlin: Springer-Verlag, 2009.198 – 216.

[5] Manho A, Tsang P P, Susilo Willy, et al. Dynamic universal accumulators for DDH groups and their application to attribute based anonymous credential systems[A]. CT-RSA 2009, LNCS 5473[C]. Berlin: Springer-Verlag, 2009.1042 – 1045.

[6] Wang Hao, Xu Qiu-liang, Ban Tao. A provably secure two-party attribute-based key agreement protocol[A]. The Fifth International Conference on Intelligent Information Hiding and Multimedia Signal Processing[C]. Tokey: IEEE Computer Society, 2009.1042 – 1045.

[7] Ren Yong-jun, Wang Jian-dong, Zhuang Yi, et al. Attribute-based authenticated key agreement protocol[J]. Journal of Lanzhou University (Natural Sciences), 2010, 46(2): 103 – 110.

[8] Wang Hao, Xu Qiu-liang, Fu Xiu. Revocable attribute-based key agreement protocol in the standard model[J]. Journal of Networks, 2009, 8(1): 787 – 794.

[9] Bethencourt J, Sahai A, Water B. Ciphertext-policy attribute based encryption[A]. IEEE Symposium on Security and Privacy[C]. IEEE Computer Society, 2007.321 – 334.

[10] Zheng Y. Digital signcryption or how to achieve cost (signature & encryption) < < cost (signature) + cost (encryption) [A]. Advances Cryptology-CRYPTO'97. Lecture Notes in

Computer Science [C]. Berlin: Springer, 1997. 165 – 179.
[11] Brickell E F. Some ideal secret sharing schemes[A]. Advanced in Cryptology- EUROCRYPT'89 Proceedings[C]. Berlin: Springer Verlag, 1990. 468 – 475.
[12] Liu Jia, Zhuang Yi, Wang Jian-dong. Secure distributed signcryption scheme based on vector space[J]. Journal on Communications, 2009, 30(9): 83 – 88.
[13] 张秋璞;叶顶锋. 对一个基于身份的多重签密方案的分析和改进[J]. 电子学报, 2011, 39(12): 2713 – 2720.
Zhang qiu-pu, Ye Ding-feng. Cryptanalysis and improvement of an identity-based multi-signcryption scheme[J]. Acta Electronica Sinica, 2011, 39(12): 2317 – 2720. (in Chinese)
[14] Sun Yinxia, Li Hui. ID-based signcryption KEM to multiple recipients[J]. Chinese Journal of Electronics, 2011, 20(2): 317 – 322.
[15] Pirretti M, Traynor P, Mcdaniel P, et al. Secure attribute-based systems[A]. ACM Conference on Communications Security (ACMCCS)[C]. New York: ACM, 2006. 99 – 112.

作者简介

刘 佳 女, 1980 年生, 江苏徐州人, 博士生, 南京航空航天大学计算机科学与技术学院讲师, 主要研究方向为密码学与信息安全.

王建东 男, 1945 年生, 江苏沭阳人, 南京航空航天大学计算机科学与技术学院教授, 博士生导师, 主要研究方向为人工智能与信息安全.