AES密码算法S盒的线性冗余研究

金晨辉,孙 莹
(解放军信息工程大学电子技术学院,河南郑州 450004)

摘 要: 本文借助有限域上的迹变换,证明了有限域 $GF(2^n)$ 上的幂双射 x^k 的坐标函数的非零线性组合都线性等价,且等价变换共有 2^n-1 个;证明了AES算法的S盒的坐标函数的非零线性组合都线性等价,且在添加0元后,本文构造的坐标函数的给定线性组合到其它线性组合的等价变换全体构成 $\{0,1\}^n$ 同构的群.本文还给出了AES算法的S盒的最低坐标函数到其它坐标函数的等价变换,它们构成了等价变换群的一组基.本文还证明了Fuller J和Millan W构造的等价变换之和都不再是坐标函数的线性组合之间的等价变换.

关键词: AES算法; S盒; 幂变换; 有限域; 线性等价
中图分类号: TN918.1 **文献标识码:** A **文章编号:** 0372-2112 (2004) 04-0639-03

Research on the Linear Redundancy in the AES S Box

JIN Chen-hui, SUN Ying
(*Institute of Electronic Technology, the PLA University of Information Engineering, Zhengzhou, Henan* 450004, *China*)

Abstract: It's proved that the nonzero linear combinations of the coordinates (NLCC for short) of a bijective monomial in a finite field of characteristic two are linearly equivalent, and the number of equivalent transformations is equal to the number of nonzero elements in the finite field. It's prove that the NLCCs of S-boxes of AES are linear equivalent, and the group formed by the zero transformation and all transformations constructed in this paper for equivalence of a given NLCC to NLCCs under the pointwise addition of transformations is isomorphic to additive group of the finite field. The equivalent transformations of the least significant coordinate to 8 coordinates are given, which is a base of this group. It's proved also that the sum of equivalent transformations of coordinates constructed by Fuller J and Millan W is not an equivalent transformation of two NLCCs of S-boxes of AES.

Key words: AES; S box; monomial; finite field; linear equivalent

1 引言

有限域 $GF(2^n)$ 上的逆变换 x^{-1} 是AES算法[1]中唯一的非线性变换,因而对该S盒的研究对于分析AES算法的强度具有重要意义.Fuller Joanne 和 Millan William[2]提出了一个检验两个Boole函数是否仿射等价,且在二者仿射等价时找出相应的等价变换的算法,并利用该算法证明了AES算法的S盒的8个坐标函数线性等价,并给出了相应的等价变换.在本文中,我们将利用有限域上的迹变换,证明有限域 $GF(2^n)$ 上的幂双射 x^k 的坐标函数的所有非零线性组合都是线性等价的,并给出相应的等价变换,分析其代数结构,从而强化了文献[2]的结果.本文的结果使我们对AES算法的密码特性有了更加深刻的认识.

2 上幂双射的坐标函数的非零线性组合的线性等价性

定义1 设 $f,g:\{0,1\}^n\to\{0,1\}$ 是两个 n 元布尔函数,如果存在 $e\in\{0,1\}$, $\boldsymbol{a}\in\{0,1\}^n$ 及 $\{0,1\}^n$ 至自身的仿射变换 ψ,使得 $f(\boldsymbol{x})=g(\psi_{f,g}(\boldsymbol{x}))\oplus\boldsymbol{a}\cdot\boldsymbol{x}\oplus e$,则称 f 与 g 仿射等价[2];又若 ψ 是线性变换且 $a=0$,则称 f 与 g 线性等价,并称 $\psi_{f,g}$ 为 f 到 g 的等价变换.其中 $\boldsymbol{a}\cdot\boldsymbol{x}$ 是向量 $\boldsymbol{a}$ 与向量 $\boldsymbol{x}$ 的内积.

命题1

设 $f(\boldsymbol{x})=g(\psi_{f,g}(\boldsymbol{x}))\oplus e$, $h(\boldsymbol{x})=g(\psi_{h,g}(\boldsymbol{x}))\oplus e'$,则 $f(\boldsymbol{x})=h(\psi_{h,g}^{-1}\psi_{f,g}(\boldsymbol{x}))\oplus e\oplus e'$,即 $\psi_{f,h}=\psi_{h,g}^{-1}\psi_{f,g}=\psi_{g,h}\psi_{f,g}$.

证明

由 $h(\boldsymbol{x})=g(\psi_{h,g}(\boldsymbol{x}))\oplus e'$,知 $g(\boldsymbol{x})=h(\psi_{h,g}^{-1}(\boldsymbol{x}))\oplus e'$,即 $\psi_{h,g}^{-1}=\psi_{g,h}$,从而

$$f(\boldsymbol{x})=g(\psi_{f,g}(\boldsymbol{x}))\oplus e=h(\psi_{h,g}^{-1}\psi_{f,g}(\boldsymbol{x}))\oplus e\oplus e'$$

因而 $\psi_{f,h}=\psi_{h,g}^{-1}\psi_{f,g}=\psi_{g,h}\psi_{f,g}$ 成立.

引理1 设 $p(\boldsymbol{x})$ 是一个 n 次不可约多项式, $(a_{n-1},a_{n-2},\cdots,a_0),(b_{n-1},b_{n-2},\cdots,b_0)\in\{0,1\}^n$,规定 $(a_{n-1},a_{n-2},\cdots,a_0)\times(b_{n-1},b_{n-2},\cdots,b_0)=(c_{n-1},c_{n-2},\cdots,c_0)$,其中

$$\sum_{i=0}^{n-1}c_i\boldsymbol{x}^i=\Big(\sum_{i=0}^{n-1}a_i\boldsymbol{x}^i\Big)\Big(\sum_{i=0}^{n-1}b_i\boldsymbol{x}^i\Big)\bmod p(\boldsymbol{x})$$

收稿日期:2002-09-25;修回日期:2003-04-03
基金项目:河南省杰出青年科学基金资助项目(No.0312001800)

则($\{0,1\}^n$,⊕,×)构成有限域.

下面首先给出二元域上向量空间$\{0,1\}^n$的点积运算$\boldsymbol{a}\cdot\boldsymbol{x}$与有限域($\{0,1\}^n$,⊕,×)上迹变换$\mathrm{Tr}(x)=\sum_{k=0}^{n-1}x^{2^k}$之间的联系. $\forall \boldsymbol{a},x\in\{0,1\}^n$,以下$\boldsymbol{a}x$恒表示$\boldsymbol{a}$与$x$在域中的乘积,$e_i$,$0\le i<n$恒表示右起第$i$分量为1且其余分量都是0的二元$n$维向量.

定理1 存在线性双射$\varphi:\{0,1\}^n\to\{0,1\}^n$,使得$\forall a\in\{0,1\}^n$,都有$\boldsymbol{a}\cdot\boldsymbol{x}=\mathrm{Tr}(\varphi(a)x)$.

证明 记Ω是线性空间$\{0,1\}^n$至$\{0,1\}$的线性变换全体,则$\Omega=\{\boldsymbol{a}\cdot\boldsymbol{x}:\boldsymbol{a}\in\{0,1\}^n\}$.但由有限域理论[3]知$\Omega=\{\mathrm{Tr}(\boldsymbol{a}x):\boldsymbol{a}\in\{0,1\}^n\}$,故存在双射$\varphi:\{0,1\}^n\to\{0,1\}^n$,使$\forall\boldsymbol{a}\in\{0,1\}^n$,都有$\boldsymbol{a}\cdot\boldsymbol{x}=\mathrm{Tr}(\varphi(\boldsymbol{a})x)$.又因$\forall\boldsymbol{a},\boldsymbol{b}\in\{0,1\}^n$,有

$$\begin{aligned}\mathrm{Tr}(\varphi(\boldsymbol{a}\oplus\boldsymbol{b})x)&=(\boldsymbol{a}\oplus\boldsymbol{b})\cdot\boldsymbol{x}=\boldsymbol{a}\cdot\boldsymbol{x}\oplus\boldsymbol{b}\cdot\boldsymbol{x}\\&=\mathrm{Tr}(\varphi(\boldsymbol{a})x)\oplus\mathrm{Tr}(\varphi(\boldsymbol{b})x)\\&=\mathrm{Tr}((\varphi(\boldsymbol{a})\oplus\varphi(\boldsymbol{b}))x)\end{aligned}$$

故由迹变换的唯一性[3]知$\varphi(\boldsymbol{a}\oplus\boldsymbol{b})=\varphi(\boldsymbol{a})\oplus\varphi(\boldsymbol{b})$,即$\varphi$是线性变换.

定理2 设$GF(2^n)$上的幂变换$f(x)=x^k$是双射,则

(1)$f(x)=x^k$的坐标函数的非零线性组合都线性等价.且$\forall\boldsymbol{a},\boldsymbol{b}\neq0$,$\boldsymbol{a}\cdot f(x)$到$\boldsymbol{b}\cdot f(x)$的等价变换$\psi_{a,b}(x)=dx$,$d$满足$d^k=\varphi(\boldsymbol{a})\varphi(\boldsymbol{b})^{-1}$,因而等价变换共有$2^n-1$;

(2)设$\boldsymbol{b}\in\{0,1\}^n$,$\boldsymbol{a}=(a_{n-1},a_{n-2},\cdots,a_0)\in\{0,1\}^n$,则有$\psi^k_{a,b}(x)=\sum_{i=0}^{n}a_i\psi^k_{e_i,b}(x)$;

(3)设$\boldsymbol{b}\in\{0,1\}^n$,则$G_b=\{\psi^k_{a,b}(x):\boldsymbol{a}\in\{0,1\}^n\}$按变换的点式加法构成与$\{0,1\}^n$同构的群.

证明 (1)设$\boldsymbol{a},\boldsymbol{b}\in\{0,1\}^n$,且$\boldsymbol{b}\neq0$,令$c=\varphi(\boldsymbol{a})\varphi(\boldsymbol{b})^{-1}$.因$f(x)=x^k$是双射,故存在唯一$d\in\{0,1\}^n$,使$d^k=c$,于是

$$\begin{aligned}\boldsymbol{a}\cdot\boldsymbol{x}^k&=\mathrm{Tr}(\varphi(\boldsymbol{a})x^k)=\mathrm{Tr}(\varphi(\boldsymbol{b})cx^k)\\&=\mathrm{Tr}(\varphi(\boldsymbol{b})(dx)^k)=\boldsymbol{b}\cdot(dx)^k\end{aligned}$$

故由$\psi_{a,b}(x)=dx$是$\{0,1\}^n$至自身的线性双射知,$\boldsymbol{a}\cdot\boldsymbol{x}^k$与$\boldsymbol{b}\cdot\boldsymbol{x}^k$线性等价且$\boldsymbol{a}\cdot\boldsymbol{x}^k$到$\boldsymbol{b}\cdot\boldsymbol{x}^k$的等价变换为$\psi_{a,b}(x)=dx$,其中$d^k=\varphi(\boldsymbol{a})\varphi(\boldsymbol{b})^{-1}$.显然当$\boldsymbol{a}\neq0$时,$d$有且只有$2^n-1$种变化,因而等价变换共有$2^n-1$.

(2)给定$\boldsymbol{b}\in\{0,1\}^n$,记$\boldsymbol{a}=(a_{n-1},a_{n-2},\cdots,a_0)$,则由$\psi^k_{a,b}(x)=d^kx=cx=\varphi(\boldsymbol{a})\varphi(\boldsymbol{b})^{-1}x$和

$$\varphi(\boldsymbol{a})=\varphi(\sum_{i=0}^{n-1}a_ie_i)=\sum_{i=0}^{n-1}a_i\varphi(e_i)$$

即$\psi^k_{a,b}(x)=\sum_{i=0}^{n-1}a_i\psi^k_{e_i,b}(x)$.

(3)由(2)即知G_b按变换的点式加法构成群,且$\boldsymbol{a}\propto\psi^k_{a,b}$是群$\{0,1\}^n$至群$G_b$的同构.

以下$\{0,1\}^n$中向量均记为行向量,并称矩阵$\boldsymbol{A}$为线性变换$\psi(x)=\boldsymbol{A}x^T$的变换矩阵.

引理2 设$\lambda(x)=\boldsymbol{A}x\oplus\boldsymbol{\delta}^T$是$\{0,1\}^n$至自身的双射,$f(x)=x^k$是$GF(2^n)$上的幂双射,这里$\boldsymbol{A}$为$n$级二元方阵,$\boldsymbol{\delta}\in\{0,1\}^n$.则$\forall\boldsymbol{a},\boldsymbol{b}\in\{0,1\}^n$,都有

$$\boldsymbol{b}\cdot\lambda(f(x))=\boldsymbol{a}\cdot\boldsymbol{\lambda}(f(\psi_{\boldsymbol{bA},\boldsymbol{aA}}(x)))\oplus(\boldsymbol{a}\oplus\boldsymbol{b})\cdot\boldsymbol{\delta}$$

证明 由定理2知,存在$\{0,1\}^n$至自身的线性双射$\psi_{\boldsymbol{bA},\boldsymbol{aA}}$,使得$(\boldsymbol{bA})\cdot f(x)=(\boldsymbol{aA})\cdot f(\psi_{\boldsymbol{bA},\boldsymbol{aA}}(x))$,故有

$$\begin{aligned}\boldsymbol{b}\cdot\lambda(f(x))&=\boldsymbol{b}(\boldsymbol{A}f(x)^T\oplus\boldsymbol{\delta}^T)=(\boldsymbol{bA})\cdot f(x)\oplus\boldsymbol{b}\cdot\boldsymbol{\delta}\\&=(\boldsymbol{aA})\cdot f(\psi_{\boldsymbol{bA},\boldsymbol{aA}}(x))\oplus\boldsymbol{b}\cdot\boldsymbol{\delta}\\&=\boldsymbol{a}\cdot\boldsymbol{\lambda}(f(\psi_{\boldsymbol{bA},\boldsymbol{aA}}(x)))\oplus(\boldsymbol{a}\oplus\boldsymbol{b})\cdot\boldsymbol{\delta}\end{aligned}$$

定理3 (1)AES算法的S盒的坐标函数的非零线性组合都线性等价,且等价变换共有2^n-1个;

(2)设$\boldsymbol{b}\in\{0,1\}^n$,$\boldsymbol{a}=(a_{n-1},a_{n-2},\cdots,a_0)\in\{0,1\}^n$,则有$\psi_{\boldsymbol{bA},\boldsymbol{aA}}(x)\sum_{i=0}^{n}a_i\psi_{\boldsymbol{bA},e_i\boldsymbol{A}}(x)$;

(3)非零$\boldsymbol{b}$组合到其它非零组合的等价变换全体在添加0元后,按变换的点式加法构成与$\{0,1\}^n$同构的群;

证明 AES算法的S盒是有限域$GF(2^8)$上的幂变换$f(x)=x^{-1}$与仿射变换$\lambda(x)=\boldsymbol{A}x^T\oplus\boldsymbol{\delta}^T$的复合,其中$\boldsymbol{\delta}=(1,1,0,0,0,1,1,0)$,矩阵$\boldsymbol{A}$的第$i$行($0\le i<n$)是(1,0,0,0,1,1,1,1)的循环右移$i$位.此时定理2中的$k=-1$,故由定理2和引理2即知(1)成立.再由$\psi^{-1}_{\boldsymbol{aA},\boldsymbol{bA}}=\psi_{\boldsymbol{bA},\boldsymbol{aA}}$,$\psi^{-1}_{e_i\boldsymbol{A},\boldsymbol{bA}}=\psi_{\boldsymbol{bA},e_i\boldsymbol{A}}$,和定理2及引理2即知(2)和(3)成立.

定理3揭示了AES算法的S盒的坐标函数的非零线性组合之间不仅线性等价,而且等价变换还具有很强的代数结构.

3 求等价变换的算法

引理3 设T_i是线性变换$\tau_i(x)=e_ix$的变换矩阵,不可约多项式为$p(x)=\sum_{i=0}^{n-1}p_ix^i$,则$T_0$是单位矩阵,$T_1$是以$p(x)$为连接多项式的移存器矩阵:

$$\boldsymbol{T}_1=\begin{pmatrix}0&0&0&0&p_0\\1&0&0&0&p_1\\0&1&0&0&p_2\\\vdots&\vdots&\vdots&\vdots&\vdots\\0&0&0&1&p_{n-1}\end{pmatrix}\tag{1}$$

且对$i=2,3,\cdots,n-1$,$T_i=T_1^i$是矩阵T_1在二元域中的i次幂矩阵.

证明 因e_0是有限域($\{0,1\}^n$,⊕,×)的幺元,故由$\tau_0(x)=x$知T_0是单位矩阵.现设$\boldsymbol{b}=(b_{n-1},b_{n-2},\cdots,b_0)\in\{0,1\}^n$,$e_1=(e_{1,n-1},e_{1,n-2},\cdots,e_{1,0})$,且$e_1\boldsymbol{b}=\boldsymbol{c}=(c_{n-1},c_{n-2},\cdots,c_0)$,则由

$$\begin{aligned}\sum_{i=0}^{n-1}c_ix^i&=(\sum_{i=0}^{n-1}e_{1,i}x^i)(\sum_{i=0}^{n-1}b_ix^i)\bmod p(x)=\sum_{i=0}^{n-1}b_ix^{i+1}\bmod p(x)\\&=\sum_{i=1}^{n-1}b_{i-1}x^i\oplus b_{n-1}x^n\bmod p(x)\\&=b_{n-1}p_0\oplus\sum_{i=1}^{n-1}(b_{i-1}\oplus b_{n-1}p_i)x^i\end{aligned}$$

即知式(1)成立.再由$e_i=e_1^i$知$\tau_i(x)=e_1^i(x)=\tau_1^i(x)$,即$T_i=T_1^i$对$i=2,3,\cdots,n-1$成立.

推论 按引理1定义的有限域上的乘法运算构成的线性

变换 $\tau(\boldsymbol{x})=d\boldsymbol{x}$ 都具有形式 $\psi=\sum_{i=0}^{n-1}d_iT_i$.

利用上述结果,就可针对有限域 $GF(2^n)$ 上的幂变换 $f(\boldsymbol{x})=\boldsymbol{x}^k$ 及 $\{0,1\}^n$ 上的仿射变换 $\lambda(\boldsymbol{x})=\boldsymbol{A}\boldsymbol{x}\oplus\boldsymbol{\delta}^T$,借助下述算法,对 $\forall\,\boldsymbol{a},\boldsymbol{b}\in\{0,1\}^n\setminus\{0\}$,求出使得 $\boldsymbol{a}\cdot\lambda(f(\boldsymbol{x}))=\boldsymbol{b}\cdot\lambda(f(\psi_{\boldsymbol{aA},\boldsymbol{bA}}(\boldsymbol{x})))\oplus e$ 成立的 $e\in\{0,1\}$ 及线性双射 $\psi_{\boldsymbol{aA},\boldsymbol{bA}}$:

预处理过程:

(1)预计算出使定理1中 $\boldsymbol{a}\cdot\boldsymbol{x}=\mathrm{Tr}(\varphi(\boldsymbol{a})\boldsymbol{x})$ 成立的线性变换 φ 的变换矩阵 $\boldsymbol{D}$;

此时,若设 $\boldsymbol{D}^{-1}=(d_{ij})_{n\times n}$,则 $\mathrm{Tr}(\boldsymbol{a}\boldsymbol{x})=\varphi^{-1}(\boldsymbol{a})\cdot\boldsymbol{x}=\boldsymbol{x}\boldsymbol{D}^{-1}\boldsymbol{a}^T$,故对 $i,j=0,1,2,\cdots,n-1$,都有

$$\mathrm{Tr}(\boldsymbol{e}_j\boldsymbol{e}_i)=\boldsymbol{e}_i\boldsymbol{D}^{-1}\boldsymbol{e}_j^T=d_{ij}$$

按照该方法可求出 $\boldsymbol{D}^{-1}$,进而可求出 $\boldsymbol{D}$.显然,$\boldsymbol{D}^{-1}$ 是对称矩阵,因而 $\boldsymbol{D}$ 也是对称矩阵.

(2)预计算出函数 $f(\boldsymbol{x})=\boldsymbol{x}^k$ 的逆变换 f^{-1} 的计算用表 S;

(3)预计算出 $GF(2^n)$ 中的逆变换 $\boldsymbol{x}^{-1}$ 的计算用表 T;

(4)利用引理3预计算出变换矩阵 $\boldsymbol{T}_0,\boldsymbol{T}_1,\cdots,\boldsymbol{T}_{n-1}$.

等价变换 $\psi_{\boldsymbol{aA},\boldsymbol{bA}}$ 的求解算法:

输入:$\boldsymbol{a},\boldsymbol{b}\in\{0,1\}^n$

Step1　利用 $e=(\boldsymbol{a}\oplus\boldsymbol{b})\cdot\boldsymbol{\delta}$ 求出 e;

Step2　计算出 $\varphi(\boldsymbol{aA})$,$\varphi(\boldsymbol{bA})$,查 T 表求出 $\varphi(\boldsymbol{bA})^{-1}$,进而求出 $\boldsymbol{c}=\varphi(\boldsymbol{aA})\varphi(\boldsymbol{bA})^{-1}$;

Step3　查 S 表求出使 $\boldsymbol{d}^k=\boldsymbol{c}$ 成立的 $\boldsymbol{d}=(d_{n-1},d_{n-2},\cdots,d_0)$;

Step4　计算出使 $\psi_{\boldsymbol{aA},\boldsymbol{bA}}(\boldsymbol{x})=\boldsymbol{d}\boldsymbol{x}$ 成立的线性变换 $\psi_{\boldsymbol{aA},\boldsymbol{bA}}$ 的变换矩阵 $\Psi=\sum_{i=0}^{n-1}d_iT_i$.

显然,当 $f(\boldsymbol{x})=\boldsymbol{x}^{-1}$ 时,利用 $\boldsymbol{d}=\varphi(\boldsymbol{bA})\varphi(\boldsymbol{aA})^{-1}$ 还可将上述算法进一步简化.

最后,我们针对AES算法,给出其S盒的右起第0(最低位)坐标函数第1至第7坐标函数的7个等价矩阵及相应的 e,这7个矩阵依次为

10011110	00010001	00001000	01011010	11110011	01111001	10111100
11010001	00011001	00001100	11110111	10001010	11000101	01100010
11101000	00001100	00000110	01111011	11000101	01100010	10110001
11101010	00010111	00001011	11100111	10010001	11001000	11100100
11101011	00011010	10001101	10101001	00111011	10011101	11001110
11110101	10001101	01000110	11010100	10011101	11001110	11100111
01111010	01000110	00100011	01101010	11001110	11100111	11110011
00111101	00100011	00010001	10110101	11100111	11110011	01111001

它们与单位矩阵一起构成等价矩阵群的一组基.这时 $(e_0,e_1,\cdots,e_7)=(0,0,1,1,1,0,0,1)$.且

$$e_1\cdot S(\boldsymbol{x})=e_i\cdot S(\psi_{1,i}(\boldsymbol{x}))\oplus e_i,[\psi_{1,i}(\boldsymbol{x})]^T=\Psi_{1,i}\boldsymbol{x}^T,$$

$$\boldsymbol{x}=(x_0,x_1,\cdots,x_7)$$

从上述结果可以看出,文中构造的等价变换不同于文献[2]给出的等价矩阵,这说明两个线性等价的布尔函数可以有不同的等价变换.借助于上述矩阵,利用定理3之(2)容易建立最低位坐标函数到坐标函数的任一线性组合的等价矩阵.然而,经验证,对所有非零的 $\boldsymbol{b}$ 及重量大于1的 $\boldsymbol{a}$,文献[2]给出的等价变换都不能使定理3之(2)成立,因而我们给出的等价变换具有更强的实用性.

4　结束语

本文证明了AES算法的坐标函数的非零线性组合都线性等价,证明了等价变换共有 2^n-1 个,并证明了给定非零线性组合到其它非零线性组合的等价变换全体在添加0元后按变换的点式加法构成一个与 $\{0,1\}^n$ 同构的群,并给出了该群的一组基.本文的研究表明AES算法的S盒具有很强的线性冗余,如何将这种线性冗余应用于AES算法的分析,还有待进一步研究.

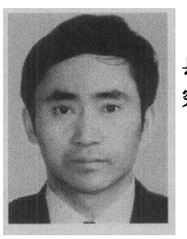
参考文献:

[1] Deamen J, Rijmen V. AES proposal: Rijndeal[DB/OL]. http://csrc.nist.gov/CryptoToolkit/aes/rijndael/ Rijndael-ammended.pdf, 1999-09-03.

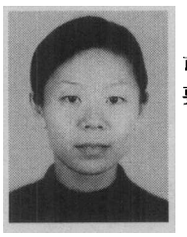
[2] Fuller J, Millan W. On the linear redundancy of AES S-box[EB/OL]. http://eprint.iacr.org, 2002.

[3] Lidl R, Niederreiter H. Finite Fields [M]. Addison-Wesley Publishing Company, 1983.1-82.

作者简介:



金晨辉　男,1965年3月出生于河南省扶沟县,信息工程大学教授,博士研究生导师,主要研究方向为密码学理论及信息安全等.



孙　莹　女,1978年8月出生于河北省唐山市,信息工程大学电子技术学院硕士研究生,主要研究方向为密码理论等.