# 完善保密密码体制的条件和存在性证明

雷凤宇[1,2] 崔国华[1] 徐 鹏[1] 张沙沙[2] 陈 晶[3]
(华中科技大学计算机学院信息安全系 武汉 430074)[1]
(广州军区75741部队 广州 510510)[2] (武汉大学计算机学院 武汉 430079)[3]

**摘 要** 密码体制的完善保密性是衡量保密系统安全性的重要方法。通过深入分析密码体制的明文空间、密文空间、密钥空间及密钥概率之间的关系,给出并证明了两个特殊密码体制具有完善保密性的必要条件;提出了一种构造完善保密密码体制的实现方案和4个相关的条件;对一类尚未解决的特殊完善保密密码体制的存在性问题给出了相应的结论和证明;并总结了一类无法构造完善保密密码体制的明文空间、密文空间、密钥空间之间的参数关系,进一步收敛了构造完善保密密码体制的条件。

**关键词** 密码学,密码体制,完善保密,计算安全性,等价密钥
**中图法分类号** TP309 **文献标识码** A

## On the Condition and the Proof of the Existence of Perfect Secrecy Cryptosystem

LEI Feng-yu[1,2] CUI Guo-hua[1] XU Peng[1] ZHANG Sha-sha[2] CHEN Jing[3]
(College of Computer Science & Technology, Huazhong University of Science & Technology, Wuhan 430074, China)[1]
(75741 Army, Guangzhou 510510, China)[2] (Computer School, Wuhan Univ., Wuhan 430079, China)[3]

**Abstract** Perfect secrecy of cryptosystem is one of the important methods weighing the security of secrecy system. Based on the deep analysis of the relationship among plaintext size, ciphertext size, key size and the key probability of perfect secrecy of cryptosystem, two necessary conditions for special perfect secrecy cryptosystem were presented and proved. This paper suggested an approach to build perfect secrecy cryptosystem and summarized four correlated restrictions. By researching a question about the existence of a sort of special perfect secrecy cryptosystem which does not be solved, this paper gave the conclusion and correlative proof; furthermore, this paper got a group of relationship of parameter among plaintext size, ciphertext size, and key size, and proved that perfect secrecy cryptosystem can not be built in this way. The results contract the conditions to build perfect secrecy cryptosystem and develop communication theory of Shannon's secrecy system and are helpful for designing secure cryptosystem.

**Keywords** Cryptography, Cryptosystem, Perfect secrecy, Computational security, Equivalent keys

## 1 引言

一个保密系统的安全性有两种基本的衡量方法:一种是计算安全性,又称实际保密性;另一种是无条件安全性,又称完善保密性。密码系统的计算安全性指:利用已有的最好技术破译该系统所需要的努力超过了敌手的破译能力或破译该系统的难度等价于解数学上的某个已知难题。密码系统的完善保密性指:具有无限计算资源的密码分析者也无法破译该系统。因为允许计算时间无限,所以完善保密性无法用计算复杂性的观点来研究,而一般采用概率的观点进行研究。

完善保密概念由Shannon于1949年在"保密系统的通信理论"[1]一文中提出,Shannon通过信息论的观点对信息保密问题作了全面的阐述,这使信息论成为研究密码学的一个重要理论基础,宣告了科学的私钥密码学时代的到来。1988年Massey将Shannon的唯密文攻击下的完善保密性概念推广到了已知明文攻击的情况[2];1999年冯登国给出了一个完善保密密码体制的构造方法[3];2001年魏仕民等给出了一些特殊密码体制完善保密性的充分和必要条件[4];2004年亢保元等给出了完善保密性的一个充分必要条件和一个递归设计法,并提出了一类特殊完善保密密码体制的存在性问题[5];2005年Stinson等对完善保密性进行了系统分析[6]。本文通过深入分析前人的结论,给出并证明了特殊密码体制具有完善保密性的两个重要必要条件,并解决了文献[5]就一类特殊完善保密密码体制的存在性提出的一个开放性问题:对一个

到稿日期:2009-07-15 返修日期:2009-10-03 本文受国家自然科学基金(No. 60903196和60903175),湖北省自然科学基金(No. 2009CDB379)资助。

雷凤宇(1980—),女,博士生,主要研究方向为公钥密码、可证明安全性、密码学理论和实践等,E-mail:4485179@qq.com;崔国华(1947—),男,博士,教授,博士生导师,主要研究方向为信息安全、算法分析、数值分析等;徐 鹏(1981—),男,博士生,主要研究方向为公钥密码、数字签名、可证明安全性等;张沙沙(1974—),女,高级工程师,主要研究方向为信息安全、密码学;陈 晶(1981—),男,博士,主要研究方向为无线网络、网络安全。

给定的密钥概率分布，满足$|K|>|C|>|P|$的完善保密密码体制$(P,C,K,E,D)$是否一定存在？本文通过分析明文、密文之间的条件概率关系，给出了一种构造完善保密密码体制的实现方案，在此基础上证明了：满足$|K|>|C|>|P|$的完善保密密码体制$(P,C,K,E,D)$不一定存在，并进一步总结了一类无法构造完善保密密码体制的参数关系。

## 2 完善保密密码体制

### 2.1 符号说明

一个密码体制是一个5元组$(P,C,K,E,D)$，$P,C$和$K$分别表示明文空间、密文空间和密钥空间，$E$和$D$分别表示加密变换和解密变换，即对任意$k\in K$，有一个加密规则$e_k\in E$和一个解密规则$d_k\in D$。每个$e_k:P\to C$是一个单射，满足对任意明文$x\in P$，$d_k(e_k(x))=x$。记集合$\{k:d_k(y)=x\}$为$D(x,y)$，记集合$\{k:e_k(x)=y\}$为$E(x,y)$。对任意一个密钥$k\in K$，定义$C(k)=\{e_k(x):x\in P\}$，即$C(k)$表示以$k$为密钥的可能的密文集。

### 2.2 已有的结论

对任意$y\in C$，有：$p(y)=\sum_{\{k:y\in C(k)\}}p(k)p(d_k(y))$。对任意$x\in P,y\in C$，能计算出条件概率：$p(y|x)=\sum_{\{k:x=d_k(y)\}}p(k)$。

运用Bayes定理，可得：$p(x|y)=\dfrac{p(x)\sum_{\{k:x=d_k(y)\}}p(k)}{\sum_{\{k:y\in C(k)\}}p(k)p(d_k(y))}$。

**定义1** 密码体制$(P,C,K,E,D)$具有完善保密性，如果对所有$x\in P,y\in C$，有$p(x|y)=p(x)$成立。

由Bayes定理，此定义等价于：密码体制$(P,C,K,E,D)$具有完善保密性，如果对所有$x\in P,y\in C$，有$p(y)=p(y|x)$成立。

因为如果$p(y)=0$，则密文$y$永远不会出现(即可从$C$中略去)，故本文假设对所有的$y\in C,p(y)>0$。

**定理1** 密码体制$(P,C,K,E,D)$具有完善保密性，当且仅当$\sum_{k\in E(x,y)}p(k)=\sum_{u\in p}\sum_{k\in E(u,y)}p(k)p(u)$。

**定理2** 密码体制$(P,C,K,E,D)$，若对任意$x\in P,y\in C$，均有$\sum_{k\in E(x,y)}p(k)=c>0$($c$为常数)则该密码体制具有完善保密性。

**定理3** 密码体制$(P,C,K,E,D)$，若每个密钥被等概率使用，且对任意一个固定的$y\in C$及任意的$x_1,x_2\in P$，$|E(x_1,y)|=|E(x_2,y)|$成立，则此密码体制具有完善保密性。

**定理4** 密码体制$(P,C,K,E,D)$具有完善保密性的一个必要条件为$|K|\geqslant|C|\geqslant|P|$。

**定理5** 密码体制$(P,C,K,E,D)$有完善保密性的充要条件为对每一个固定的$y\in C$及任意的$x_1,x_2\in P$有$\sum_{k\in E(x_1,y)}p(k)=\sum_{k\in E(x_2,y)}p(k)$。

**定义2**[7] 在密码体制$(P,C,K,E,D)$中，如果存在密钥$k_i,k_j\in K$且$k_i\neq k_j$，对于任意$x\in P$，均有$e_{k_i}(x)=x_{k_j}(x)$，则称$k_i,k_j\in K$为等价密钥。

由于在密码体制中使用等价密钥将降低该密码体制的安全性，因此在密钥的生成和分配阶段就已经杜绝了使用等价密钥。故在本文中合理的假设任何密码体制均不存在等价密钥。

### 2.3 特殊密码体制的完善保密性

本文给出并证明了两个特殊密码体制具有完善保密性的必要条件。

**定理6** 密码体制$(P,C,K,E,D)$(且该密码体制不存在等价密钥)，则该体制具有完善保密性的一个必要条件为$|K|\leqslant P_{|C|}^{|P|}$。

证明(反证法)：假设密码体制$(P,C,K,E,D)$具有完善保密性，且满足$|K|>P_{|C|}^{|P|}$。因为明、密文空间分别为$|P|,|C|$，且每个$e_k:P\to C$是一个单射，所以$P\to C$之间的所有不同映射为$P_{|C|}^{|P|}$种。因为$|K|>P_{|C|}^{|P|}$，所以必然存在$k_i\neq k_j$($1\leqslant i,j\leqslant|K|$)，使得对任意$x\in P$，均有$e_{k_i}(x)=e_{k_j}(x)$，存在等价密钥，与前提矛盾。所以若$(P,C,K,E,D)$具有完善保密性，必然有$|K|\leqslant P_{|C|}^{|P|}$。

**定理7** 密码体制$(P,C,K,E,D)$(且该密码体制不存在等价密钥)满足$|C|=|P|$，则该体制具有完善保密性的一个必要条件为$|K|-1\neq|C|$。

证明(反证法)：假设密码体制$(P,C,K,E,D)$具有完善保密性且有$|K|-1=|C|=|P|$成立，其中$P=\{x_1,x_2,\cdots,x_{|P|}\}$，$C=\{y_1,y_2,\cdots,y_{|C|}\}$，$K=\{k_1,k_2,\cdots,k_{|K|}\}$。

因为在任何密码体制中，当$|P|=|C|$时易证$e_k:P\to C$是一个双射，所以任意固定的$y\in C$，对任意$k\in K$，存在且仅存在唯一的$x\in P$，满足$e_k(x)=y$。故由此可推出对任意固定的$y\in C$有：

$$\{k:y\in C(k)\}=\bigcup_{x\in P}\{k:e_k(x)=y\}=\bigcup_{x\in P}E(x,y)=K$$

且对任意$x_i,x_j\in P(x_i\neq x_j)$有$E(x_i,y)\cap E(x_j,y)=\varnothing$(即对任意固定的$y\in C$，$\bigcup_{x\in P}\{E(x,y)\}$构成集合$K$的一个划分)。可知对任意固定的$y\in C$，$K$细分为$|P|$块，因为$|K|-1=|P|$，所以存在且仅存在唯一的$x\in P$，满足$|E(x,y)|=2$，而对其他$|P|-1$个$x\in P$，均有$|E(x,y)|=1$。

不失一般性，令$x_1\in P,y_1\in C$，有：$e_{k_1}(x_1)=e_{k_2}(x_1)=y_1$(其中$k_1\in K,k_2\in K$)，即$|E(x_1,y_1)|=2$。

由完善保密密码体制的定义得：

$$p(y_1)=p(y_1|x_1)=\sum_{\{k:x_1=d_k(y_1)\}}p(k)=p(k_1)+p(k_2)\quad(1)$$

由上面的证明知对任意$x\in P-\{x_1\}$，均有$|E(x,y_1)|=1$。又因为任意$x_i,x_j\in P$，均有$E(x_i,y)\cap E(x_j,y)=\varnothing$，所以对$y_1\in C$，$\{P\}-\{x_1\}$和$\{K\}-\{k_1,k_2\}$一一对应。由完善保密性的定义得：

$$\begin{aligned}p(y_1)=p(y_1|x_2)=p(y_1|x_3)=\cdots=p(y_1|x_{|P|})\\=\sum_{\{k:x_2=d_k(y_1)\}}p(k)=\cdots=\sum_{\{k:x_{|P|}=d_k(y_1)\}}p(k)\\=p(k_3)=p(k_4)=\cdots=p(k_{|K|})\end{aligned}\quad(2)$$

由式(1)、式(2)可得：

$$p(k_1)+p(k_2)=p(k_3)=p(k_4)=\cdots=p(k_{|K|})\quad(3)$$

同理，对于任意$y_m\in C(2\leqslant m\leqslant|C|)$，根据完善保密的定义得：

$$\begin{aligned}p(y_m)=p(y_m|x_1)=p(y_m|x_2)=\cdots=p(y_m|x_{|P|})\\=\sum_{\{k:x_1=d_k(y_m)\}}p(k)=\cdots=\sum_{\{k:x_{|P|}=d_k(y_m)\}}p(k)\end{aligned}$$

故可得：

$$\begin{aligned}p(k_l)+p(k_r)=p(k_1)\cdots=p(k_{l-1})=p(k_{l+1})=\cdots=\\p(k_{r-1})=p(k_{r+1})=\cdots=p(k_{|K|})\\(2\leqslant l\leqslant r\leqslant|K|)\end{aligned}\quad(4)$$

显见，同时满足式(3)、式(4)的解为$p(k_l)=p(k_1)$，$p(k_r)=p(k_2)$，即对任意$x\in P,y\in C$，均有$e_{k_1}(x)=e_{k_2}(x)=y$，由此

可以推出 $k_1 \in K, k_2 \in K$ 为等值密钥，与定理的已知条件矛盾。得证具有完善保密性的密码体制 $(P,C,K,E,D)$，如果 $|C|=|P|$，则必有 $|K|-1 \neq |C|$。

## 3 完善保密密码体制的设计和问题讨论

### 3.1 完善保密密码体制的构造

由完善保密密码体制定义知，一个密码体制 $(P,C,K,E,D)$ 具有完善保密性，如果对所有 $x \in P, y \in C$，有 $p(y|x)=p(y)=\sum_{k \in E(x,y)} p(k)$ 成立，因此设 $|P|=n, |C|=m, |K|=l$，其中 $C=\{y_1,\cdots,y_m\}, P=\{x_1,\cdots,x_n\}, P=\{k_1,\cdots,k_l\}, \sum_{i=1}^{l} k_i=1 (i=1,2,\cdots,l)$，可得出明、密文之间的条件概率关系表（其中，$x,y$ 分别为列和行标识）如表 1 所列。

表 1 明、密文之间的条件概率关系

| $p(y\|x)=p(y)$ | $x_1$ | $x_2$ | … | $x_n$ |
|---|---|---|---|---|
| $y_1$ | $\sum_{k \in E(x_1,y_1)} p(k)$ | $\sum_{k \in E(x_2,y_1)} p(k)$ | … | $\sum_{k \in E(x_n,y_1)} p(k)$ |
| $y_2$ | $\sum_{k \in E(x_1,y_2)} p(k)$ | $\sum_{k \in E(x_2,y_2)} p(k)$ | … | $\sum_{k \in E(x_n,y_2)} p(k)$ |
| $y_m$ | $\sum_{k \in E(x_1,y_m)} p(k)$ | $\sum_{k \in E(x_2,y_m)} p(k)$ | … | $\sum_{k \in E(x_n,y_m)} p(k)$ |

通过分析可知，构造完善保密密码体制，至少要满足以下 4 个条件：

(1)密码体制中，任意固定的 $x \in P$，对任意 $k \in K$，均存在 $y \in C$，使得 $e_k(x)=y$，则在每一列中 $p(k_1),\cdots,p(k_l)$ 至少各出现一次。又由密码体制的性质可知，任意固定的 $x \in P$，对任意 $y_i, y_j \in C$（在此 $y_i \neq y_j$），不存在 $k \in K$，使得 $e_k(x)=y_i=y_j$。因此每一列中 $p(k_1),\cdots,p(k_l)$ 各出现且仅出现一次，且每一列概率之和为 1。

(2)任意固定的 $y \in C(p(y)>0)$，对任意 $x_i, x_j \in P$（在此 $x_i \neq x_j$），不存在 $k \in K$，使得 $e_k(x_i)=e_k(x_j)=y$，故对每一行 $p(k_1),\cdots,p(k_l)$ 任意出现至少 $n$ 个且无重复出现。

(3)对于任意 $k_i \neq k_j$，$p(k_i), p(k_j)$ 不可能在每一列都同时出现，否则对任意 $x \in P$，都有 $e_{k_i}(x)=e_{k_j}(x)$，即存在等价密钥，此时与密码体制不存在等价密钥的假设矛盾。

(4)因为 $p(y|x_1)=p(y|x_2)=\cdots=p(y)$，所以表 1 中同一行且不同列的概率都相等。

作为例子，设计一个参数 $(|P|,|C|,|K|)$ 为 (3,4,5) 的完善保密密码体制，如表 2 所列。

表 2 完善保密密码体制

| $p(y\|x)=p(y)$ | $x_1$ | $x_2$ | $x_3$ |
|---|---|---|---|
| $y_1$ | $p(k_1)+p(k_2)$ | $p(k_3)$ | $p(k_4)$ |
| $y_2$ | $p(k_3)$ | $p(k_4)$ | $p(k_2)+p(k_5)$ |
| $y_3$ | $p(k_4)$ | $p(k_1)+p(k_5)$ | $p(k_3)$ |
| $y_4$ | $p(k_5)$ | $p(k_2)$ | $p(k_1)$ |

其中，$p(k_1)=p(k_2)=p(k_5)=\frac{1}{7}$，$p(k_3)=p(k_4)=\frac{2}{7}$。

### 3.2 问题和证明

在文献[5]的最后提出了一类特殊完善保密密码体制的存在性问题。问题如下：

对一个给定的密钥概率分布（所有密钥的概率均不大于 0.5。事实上，容易看出，当一个密钥的概率大于 0.5 时，密码体制不可能完善），满足 $|K|>|C|>|P|$ 的完善保密密码体制 $(P,C,K,E,D)$ 是否一定存在？

通过分析发现，对于任意给定的参数，难以得出存在完善保密密码体制的充要条件，但是通过证明可以得出满足 $|K|>|C|>|P|$ 的完善保密密码体制 $(P,C,K,E,D)$ 不一定存在。

所以问题等价于：满足 $|K|>|C|>|P|$ 的完善保密密码体制 $(P,C,K,E,D)$ 不一定存在。证明如下：

证明（例证法）：不存在 $(|P|,|C|,|K|)$ 为 (7,9,10) 的完善保密密码体制 $(P,C,K,E,D)$。

假设能构造出 $(|P|,|C|,|K|)$ 为 (7,9,10) 的完善保密密码体制 $(P,C,K,E,D)$，则可构造一个 9 行 7 列的明、密文之间的条件概率关系表如表 3 所列。

表 3 9 行 7 列的明、密文之间的条件概率关系

| $p(y\|x)=p(y)$ | $x_1$ | $x_2$ | … | $x_7$ |
|---|---|---|---|---|
| $y_1$ | $\sum_{k \in E(x_1,y_1)} p(k)$ | $\sum_{k \in E(x_2,y_1)} p(k)$ | … | $\sum_{k \in E(x_7,y_1)} p(k)$ |
| $y_2$ | $\sum_{k \in E(x_1,y_2)} p(k)$ | $\sum_{k \in E(x_2,y_2)} p(k)$ | … | $\sum_{k \in E(x_7,y_2)} p(k)$ |
| | | …… | | |
| $y_9$ | $\sum_{k \in E(x_1,y_9)} p(k)$ | $\sum_{k \in E(x_2,y_9)} p(k)$ | … | $\sum_{k \in E(x_7,y_9)} p(k)$ |

由 3.1 节易知，每一列中 $p(k_1),\cdots,p(k_{10})$ 各出现且仅出现一次；每一行中 $p(k_1),\cdots,p(k_{10})$ 任意出现至少 7 个且无重复出现。

令 $\{K_1,K_2\}$ 为 $K$ 的划分，且对任意 $k_i,k_j \in K$，如果存在 $x \in P, y \in C$，满足 $e_{k_i}(x)=e_{k_j}(x)=y$（即 $E(x,y)=\{k_i,k_j\}$，$|E(x,y)|=2$），则 $k_i,k_j \in K_2$，定义 $K_1=K-K_2$。

因为 $|K|-|C|=1$，所以每一行有且仅有唯一的 $|E(x,y)|=2$。可假设 $p(y_1|x_1)=p(k_1)+p(k_2)$（由 $K_2$ 定义显然有 $k_i,k_j \in K_2$），可知 $|K_2| \geqslant 3$（否则对任意 $x \in P$，均有 $e_{k_1}(x)=e_{k_2}(x)$，存在多余密钥），且对任意 $y \in C-\{y_1\}$ 均有 $|E(x_1,y)|=1$。设 $k_m \in K_2-\{k_1,k_2\}$ 且 $p(k_m)$ 为 $K_2$ 中元素最小概率，必存在 $y_j \in C-\{y_1\}$，使得 $|E(x_1,y_j)|=1$ 且 $p(y_j)=p(y_j|x_1)\cdots=p(y_j|x_7)=p(k_m)$，可知 $K$ 中至少有 7 个元素的概率均等于 $p(k_m)$，大于 $p(k_m)$ 的元素个数最多为 $10-7=3$（$|K|-|P|$）个。因为概率等于 $p(k_m)$ 的所有 $k \in K$ 在 $x_1$ 列均出现一次，设 $k_1=k_2=k_m$，则至少有 5 行对所有 $x \in P$ 均有 $|E(x,y)|=1$，所以最多有 $9-7+2=4(|C|-|P|+2)$ 行存在 $|E(x,y)|=2$。故在能出现 $|E(x,y)|=2$ 的行中，每行最多有 3 个 $|E(x,y)|=1$（在存在 $|E(x,y)|=2$ 的行中，如果 $|E(x,y)|=1$ 且 $E(x,y)=\{k\}$ 则 $p(k)$ 必然要大于 $K_2$ 中元素最小概率 $p(k_m)$）。因为在可能出现 $|E(x,y)|=2$ 的 4 行中，设大于 $p(k_m)$ 的所有元素在每行都出现，最多可出现 $4*3$ 次；又 4 行共有 $4*7$ 种不同的 $(x,y)$ 组合，且 $|E(x,y)|=2$ 出现的总次数为 $|P|$，所以必须满足不等式 $4*3 \geqslant 4*7-7((|C|-|P|+2)*(|K|-|P|) \geqslant (|C|-|P|+2)|P|-|P|)$ 才能构造出完善保密密码体制，显然不等式不成立。当等于 $p(k_i)$ 的个数大于 7 时，不等式均无法成立。因此无法构造出参数为 (7,9,10) 的完善保密密码体制。

通过参数为 (7,9,10) 的例子，证明了满足 $|K|>|C|>|P|$ 的完善保密密码体制 $(P,C,K,E,D)$ 不一定存在，证明完毕。

对特殊保密密码体制的完善保密性进行进一步的研究，得到定理 8。

**定理 8** 密码体制 $(P,C,K,E,D)$（且该密码体制不存在

等价密钥)，当$|K|=|C|+1$且$2|P|>|K|$时，无法构造出完善保密密码体制。

证明(反证法)：假设密码体制$(P,C,K,E,D)$具有完善保密性，且满足$|K|=|C|+1,2|P|>|K|$。

令$\{K_1,K_2\}$为$K$的划分，且对任意$k_i,k_j\in K$，如果存在$x\in P,y\in C$，满足$e_{k_i}(x)=e_{k_j}(x)=y$(即$E(x,y)=\{k_i,k_j\}$，$|E(x,y)|=2$)，则$k_i,k_j\in K_2$，定义$K_1=K-K_2$。

令$\{C_1,C_2\}$为$C$的划分，且对任意$y\in C$，如果存在$x\in P$，使得$|E(x,y)|=2$，则$y\in C_2$，定义$C_1=C-C_2$。

因为任意固定的$x\in P,y\in C$，都有$p(y)=p(y|x)>0$，所以任意固定的$x\in P$，对任意$y\in C$，都存在$k\in K$，使得$e_k(x)=y$。又任意固定的$x\in P$，对任意$k\in K$，均存在$y\in C$，使得$e_k(x)=y$。所以$|K|=|C|+1$时，任意固定的$x\in P$，有且仅有唯一的$y\in C$，满足$|E(x,y)|=2$，而对其余$|C|-1$个$y\in C$，均有$|E(x,y)|=1$。

设$x_1\in P,y_1\in C$，有$e_{k_1}(x_1)=e_{k_2}(x_1)=y_1(k_1,k_2\in K_2)$，即$|E(x_1,y_1)|=2$。可知$|K_2|\geqslant 3$(否则对任意$x\in P$，均有$e_{k_1}(x)=e_{k_2}(x)$，存在多余密钥)。对于$x_1\in P$，因为有且仅有唯一的$|E(x_1,y_1)|=2$，所以$K-\{k_1,k_2\}$和$C-\{y_1\}$中元素一一对应。设$k_m\in K_2-\{k_1,k_2\}$，且对任意$k\in K_2$，均有$p(k)\geqslant p(k_m)$，则必存在$y_j\in C$使得$e_{k_m}(x_1)=y_j$且有$|E(x_1,y_j)|=1$。由完善保密性的定义，$y_j\in C$有$p(y_j)=p(y_j|x_1)=\cdots=p(y_j|x_{|P|})=p(k_m)$，因为任意$k\in K_2$，均有$p(k)\geqslant p(k_m)$，所以对任意$x\in P$，均有$|E(x,y_j)|=1$，即至少有$|P|$个$k\in K$，使得$p(k)=p(k_m)$。因为对于$x_1\in P$，$K-\{k_1,k_2\}$和$C-\{y_1\}$中元素一一对应，设$p(k_1)=p(k_2)=p(k_m)$，至少有$|P|-2$个$y\in C$，使得$p(y)=p(k_m)$；且这$|P|-2$个$y\in C$，对所有的$x\in P$，均有$|E(x,y)|=1$(即$y\in C_1$)。所以最多有$|C|-(|P|-2)=|K|-|P|+1$个$y\in C$使得$|E(x,y)|=2$(即$y\in C_2$)，且最多有$|K|-|P|$个$k\in K$，使得$p(k)>p(k_m)$。可知$K$中概率大于$p(k_m)$的元素在加密规则中最多在$(|K|-|P|+1)(|K|-|P|)$组不同的$(x,y)$中出现(设概率大于$p(k_m)$的任意$k\in K$，对任意$y\in C_2$都存在$x\in P$，使得$e_k(x)=y$)。因为任意$y\in C_2$，都有$|P|$个$x\in P$，使得$p(y|x)>0$(即共$(|K|-|P|+1)|P|$个不同的$(x,y)$组合)，$|E(x,y)|=2$的个数共为$|P|$个，所以$(|K|-|P|+1)(|K|-|P|)\geqslant(|K|-|P|+1)|P|-|P|$时，才有可能构造出完善保密密码体制。解这个不等式可得：

$$(|K|-|P|+1)(|K|-|P|)\geqslant(|K|-|P|+1)|P|-|P|$$
$$\Leftrightarrow(|K|-|P|+1)(|K|-2|P|)+|P|\geqslant 0$$
$$\Leftrightarrow\left(|K|-\frac{3|P|-1}{2}\right)^2\geqslant\left(\frac{|P|-1}{2}\right)^2。$$

当$|K|-\frac{3|P|-1}{2}\geqslant 0$时，有：

$$|K|-\frac{3|P|-1}{2}\geqslant\frac{|P|-1}{2}\Leftrightarrow|K|\geqslant 2|P|。$$

当$|K|-\frac{3|P|-1}{2}\leqslant 0$时，有：

$$\frac{3|P|-1}{2}-|K|\geqslant\frac{|P|-1}{2}\Leftrightarrow|K|\leqslant|P|+1。$$

可知，$|K|\geqslant 2|P|$，$|K|\leqslant|P|+1$均与前提相悖。同时由上面的讨论可知，$K$中等于$p(k_m)$的元素个数增加时，不等式均不成立。由此可得无法构造满足$|K|=|C|+1,2|P|>|K|$的完善保密密码体制。

### 3.3 下一步研究

在本文的研究过程中，存在一个值得思考的问题：是否能建立某种模型，在这种模型下，对任意给定的参数关系，可以判断是否能构造具有完善保密性的密码体制，对于可以构造具有完善保密性密码体制的参数关系，使用该模型至少能构造一个满足完善保密性的密码体制实例。

**结束语** 本文给出了特殊密码体制具有完善保密性的两个必要条件(见定理6、定理7)；给出了一种构造完善保密密码体制的实现方案和4个相关的条件(见3.1节)，并对文献[5]中提出的问题进行了讨论，给出了结论和证明；总结了满足完善保密密码体制的必要条件$|K|\geqslant|C|\geqslant|P|$，但无法构造完善保密密码体制的明文空间、密文空间、密钥空间之间的参数关系(见定理8)。目前对完善保密密码体制的研究，主要对充分条件和充要条件的研究居多，而较少对完善保密密码体制的必要条件进行研究。本文对完善保密密码体制进行的研究，推广了前人的理论成果，约束了密码体制具有完善保密性的条件，对实用密码体制的设计具有一定的意义。

## 参 考 文 献


[1] Shannon C E. Communication theory of secrecy system[J]. Bell System Technical Journal, 1949, 28: 656-715

[2] Massey J L. An introduction to contemporary cryptology[M]. Digital Object Identifier, IEEE, 1988: 533-549

[3] 冯登国，裴定一. 密码学导引[M]. 北京：科学出版社，1999

[4] 魏仕民，陈凯，肖国镇，等. 关于密码体制的完善保密性[J]. 通信学报，2001，22(7)：44-47

[5] 亢保元，王育民. 完善保密密码体制的条件与设计[J]. 通信学报，2004，25(2)：168-173

[6] Stinson D R. Cryptography theory and practice[M]. CRC press, 2005

[7] Kelsey J, Schneier B. Key-schedule cryptanalysis of deal[C]// Sixth Annual Workshop on Selected Areas in Cryptography. Springer-Verlag, 1999: 118-134


(上接第80页)


[10] Werner-Allen G, Lorincz K, Johnson J, et al. Fidelity and yield in a volcano monitoring sensor network[C]// OSDI '06: Proceedings of the 7th USENIX Symposium on Operating Systems Design and Implementation. USA USENIX Press, 2006: 27-43

[11] 颜庭莘，孙利民. TinyOS路由协议原理及性能评估[J]. 计算机工程，2007(1)：112-114

[12] Levis P, Gay D, Hill J, et al. Ad-Hoc Routing Component Architecture[Z]. http://www.tinyos.net/tinyos-1.x/doc/ad-hoc.pdf, 2003-02

[13] Gay D, Levis P, Behren R, et al. The nesC language: A holistic approach to networked embedded systems[C]// Proceedings of the ACM SIGPLAN 2003 Conference on Programming Language Design and Implementation. New York, USA: ACM Press, 2003: 1-11

[14] Levis P, Lee N, Welsh M, et al. TOSSIM: Accurate and scalable simulation of entire tinyos applications [C] // Proc. of the 1st International Conference on Embedded Networked Sensor System. New York: ACM Press, 2003: 126-137