X-IDEA算法在手机图文信息安全传输中应用研究

张 毅，肖四友
（浙江万里学院 智能控制研究所，浙江 宁波 315100）

摘 要：随着移动通信系统技术的发展，信息传输形式也逐渐多样化，信息传输的安全性也日显重要。针对手机的硬件性能特点，设计了基于IDEA算法改进的X-IDEA算法应用于手机图文信息安全传输，较好地解决了IDEA算法的弱密钥等问题，X-IDEA算法的加密过程也使得其混淆性与扩散性较IDEA算法更强。根据移动通信系统的特征，提出了一种基于身份的密钥管理方法，该方法可使通信双方安全地获得密钥且计算量和通信量较小。实验证明了X-IDEA算法应用于手机图文安全传输的高效性和安全性。

关键词：安全传输；IDEA算法；X-IDEA算法；密钥管理
中图分类号：TP309 **文献标识码**：A **文章编号**：1673-629X(2012)04-0250-04

Study on Mobile Communication Image-Text Security Transport Based on X-IDEA Algorithm

ZHANG Yi, XIAO Si-you
(Intelligent Control Institution of Zhejiang Wanli University, Ningbo 315100, China)

Abstract: Along with the development of mobile communication technology, information transmission form becomes diversification, the safety of information transmission is more important. According to the performance characteristics of mobile communications terminal hardware, design improved X-IDEA algorithm based on IDEA algorithm and applied to the mobile phone information security transmission, solve the key IDEA algorithm problems such as weak key and so on. Also its resistance and diffusivity of algorithmic X-IDEA encrypt process is stronger than IDEA algorithm. According to the characteristics of mobile communication system, put forward a kind of key management method based on identity, this method can make the communications get the key safely and smaller amount of computation and communication. The experiment has testified the X-IDEA algorithm high-effect and security applied to mobile communication image-text security transport.

Key words: security transport; IDEA algorithm; X-IDEA algorithm; key management

1 概 述

在第三代移动通信系统中，移动终端访问互联网的频率越来越高，涉及多媒体业务、数据业务，以及电子商务、电子贸易等多种互联网信息服务。信息能通过文本、图片和视频等多种方式传递。对于涉及商务交易的机密信息一旦泄露，危害程度巨大。所以，移动通信终端之间图文信息传输时必须采取加密措施以保证其数据通信的安全性。作为应用广泛的移动通信终端—手机，其运算能力和存储容量都相对较低，在加密方法和加密算法的选择上应充分考虑其硬件性能，既要能保证正常的通信，又有充分的资源来进行数据加密，所以加密方法应具备低运算量和高效率的特点。

对称密钥加密算法加密速度较非对称密钥加密算法快10倍以上，效率高且适合数据量较大的加密场合，软硬件实现都比较方便。针对手机的硬件性能特点，选择的加密算法应该是轻量并容易实现的。所以本系统设计基于IDEA[1]算法改进的X-IDEA算法应用于移动通信终端信息安全传输。

来学嘉博士和著名的密码专家James L. Massey于1990年提出了基于“相异代数群上的混合运算”的International Data Encryption Algorithm(IDEA)加密算法。它是对64bit大小的数据块加密的分组加密算法，密钥长度为128位，较DES[2]加密算法更容易实现，而且该算法既可用于加密，又可用于解密。

IDEA属于对称密钥的分组加密算法，对硬件要求不高且容易实现，加密速度快尤其适合需要加密大量数据的情况。加密强度上，IDEA算法的输入密钥长度为128位，如果采用穷举方式进行攻击，其密钥空

收稿日期：2011-09-06；**修回日期**：2011-12-11
基金项目：国家“核、高、基”专项项目(2009ZX01039-001-002-004)；浙江省教育科研计划项目(Y201018543)
作者简介：张 毅(1975-)，男，讲师，硕士，研究方向为智能控制、信息系统。

间为2^{128},按每秒识别100亿个密钥也需要10年的时间来完成。IDEA已被证明只需4次循环就可抵制查分密码分析。

2 基于IDEA算法改进的X-IDEA算法的设计

2.1 IDEA算法存在的问题

(1)明文统计学特性容易暴露。

IDEA算法加密前先将明文分解成64位的数据分组,再将每个数据分组分成4个16位的数据块作为加密的一次输入,加密过程通过8圈的迭代后获得4个16位的密文[3]。所以在其加密过程中各数据分组是独立进行加密的,在对格式化数据进行加密时,明文中相同的部分会被加密成相同的密文,明文的数据格式及某些统计学特性也将暴露无遗,降低了明文的保密性[4]。

(2)IDEA算法存在弱密钥问题。

对称密钥加密方法虽然加密速度快,软硬件实验容易,但在很多对称加密算法中都存在弱密钥的问题。IDEA算法也不例外。

IDEA算法中52个16位的子密钥产生过程[5]是:将128位的初始密钥份成8份,每份16位,得到第一组的8个子密钥;加密密钥循环左移25位后分成8份,得到第二组的8个子密钥;依次循环可得到6组共48个子密钥,加上最后一轮产生4个子密钥共计52组832位子密钥。

文献[6,7]阐述了IDEA算法存在弱密钥的问题,除去IDEA算法的弱密钥后其密钥空间为2^{77}而非2^{128}。

2.2 X-IDEA算法设计

针对IDEA算法存在的问题,设计基于IDEA算法改进的X-IDEA算法。主要对明文处理、子密钥生成、加密和解密过程进行了改进。其基本思路是:对于明文统计学特性容易暴露的问题,加密前对明文进行重组处理,通过重组使得明文序列更加混乱;加密过程中设计特殊的过程,使某个明文分组产生的密文与其它明文分组存在一定的关系。对于IDEA算法的弱密钥问题,改进IDEA的子密钥产生算法,并且不再强调初始密钥的长度为128位。

(1)明文重组。

在X-IDEA算法中,加密前先对明文进行重组处理,首先将明文分成等长的若干数据分组,假设明文的长度为L位,$k=\mathrm{int}(L/64)$,找到一个于10~20间的随机整数t,使$\mathrm{mod}(k,t)=0$,第一次将明文分成t组。

完成第一次明文重组后,大多数情况下重组后的明文长度不是64的整数倍,此时可在明文的后面进行补位,使其长度达到64的整数倍,补位字符为特定的特殊字符,反之则进行补位操作。进行加密前,再将已经处理好长度的明文分组依次分解成64位的数据块作为每轮加密的输入。实际上,如果要进一步增强明文的混淆性,在进行第一次明文重组时,明文分组的组合方式采用非线性的组合方式,则明文数据分组更无规则可寻。

(2)子密钥生成。

IDEA算法的52个子密钥实际上就是通过将128位的初始密钥循环左移所得到的,子密钥生成算法相对比较简单,也就不难从中分析出弱密钥。为此在X-IDEA算法中采用一种新的子密钥生成算法—X_IDEAKEY算法,其基本思想是:对于用户输入的初始密钥(长度可不为128位),通过补位使其长度与832(52组子密钥共832位)互质,再计算出密钥长度的逆元并对密钥进行移位处理,最后将移位后的密钥依次赋给子密钥。依此循环直到生成832位的子密钥。

X_IDEAKEY算法C语言描述如下:

```
X_IDEAKEY 算法:
input:初始密钥
output:52 组 * 16 位共 832 位的子密钥
char x_ideakey(char key[])
{   int le,t,i,j=0;
char subkey[];
   subkey="";
   while(strlen(subkey)<=832)
   {
     le=strlen(key);
     if (gcd(le,832)==1)      /*gcd()为自定义互质判断函数*/
      {
t=rgcd(le,832);        /*rgcd()函数为自定义质因子计算函数*/
        if( key[0]='0') key>>=t; else key<<=2;
        for(i=1;i<=le;i++)
        {
Subkey[j++]=k[i];
iff (strlen(subkey)==832) break; else continue;
}
}
else
if(le%2==0) key[++le]='0'; else key[++le]='1';
    return subkey;
}
```

X_IDEAKEY子密钥生成算法中,输入的初始密钥可为任意长度的字符串。子密钥生成过程中根据初始密钥长度的不同对初始密钥进行移位或补位操作,每轮循环中密钥的长度都会发生变化,每次移位或补位

也相应发生变化,无法通过相应的逆运算还原子密钥的生成过程。

(3)加密和解密过程。

对于重组后的长度为 64 位的所有明文分组 P_1, $P_2, P_3, \cdots, P_n$,设计加密过程如下:

①随机数发生器选取一组数据 X 作为加密的初始数据。

②IDEA 算法加密 X 得密文 C_0。

③IDEA 算法加密 $P_1, P_2, P_3, \cdots, P_{n-1}$ 得密文分组 $D_1, D_2, D_3, \cdots, D_{n-1}$。

④IDEA 算法加密 C_0 得密文 C_0'。

⑤$C_0' \oplus P_1$ 得密文 C_1, $D_1 \oplus P_2$ 得密文 $C_2, \cdots, D_{n-1} \oplus P_n$ 得密文 C_n,最后将密文 C_0 置于密文 C 头部形成总的密文 $C_0, C_1, C_2, \cdots, C_n$。

加密过程可表示如下:

$$C_1 = \mathrm{IDEA}(C_0) \oplus P_1$$

$$C_i = \mathrm{IDEA}(P_{(i-1)}) \oplus P_i (1 < i \leqslant n)$$

对于密文 $C_0, C_1, C_2, C_3, \cdots, C_n$,解密过程如下:

1、IDEA 算法加密 C 得密文 C_0'。

2、$C_0' \oplus C_1$ 得明文 P_1。

3、依次将前一步得到的明文 P_{n-1} 加密并将其与当前密文 C_n 进行异或操作得明文 P_n。

4、将解密得到的所有明文分组 $P_1, P_2, P_3, \cdots, P_n$,进行明文重组对应的逆操作,将数据进行还原。

解密过程可表示如下:

$$P_1 = \mathrm{IDEA}(C_0) \oplus C_1$$

$$P_i = \mathrm{IDEA}(P_{(i-1)}) \oplus C_i (1 < i \leqslant n)$$

3 手机图文安全传输

3.1 密钥管理

数据加密系统的可靠性一方面取决于加密算法本身的健壮性,另一方面取决于加密密钥的安全性[8]。X-IDEA 算法的加密过程相当于嵌套了 IDEA 算法,其安全性毋庸置疑,加密原理上跟 IDEA 算法一样同属于对称密钥加密方法。众所周知,对称密钥加密方式下的密钥管理和分发是相当困难的,尤其加密系统中通信用户较多时,要实现大量密钥对安全管理也非常困难。非对称加密方法的密钥管理上耗费的资源较对称加密算法小很多,分配密钥上,n 个通信者参与加密通信时,对称加密算法需分配的密钥为 n 个,非对称加密算法需要分配的密码为 n^2 个。所以,对称算法速度快,在处理大量数据时被广泛使用,其关键是保证密钥的安全[9]。

在 X-IDEA 手机图文加密传输系统中,加密算法是基于 IDEA 改进的对称加密算法。密钥管理上采用非对称加密算法的密钥管理方法来管理密钥,这样集成了对称加密算法和非对称加密算法的优点,数据加密速度快,密钥管理方便。

另外,普适环境中密钥管理方案应具备分布式、高安全性、可扩展性、低计算量和低通信量的特点[10]。

在移动通信网络中终端进行网络注册时都要进行身份验证,不同用户的身份信息肯定不同,下面来设计一种基于身份[11]的密钥分发方法,基本思路如下:

在移动基站设置一个的密钥生成中心,当移动终端开机向移动基站进行注册时,合法的用户通过基站的验证并合法注册入网后,基站密钥生成中心根据终端的身份信息(如 PUK 码、SIM 卡号、手机号等)通过秘密的算法计算出密钥,将该密钥发送给对应的终端。此密钥相当于该用户的私钥。下面来介绍一种离散对数[12]的基于身份的密钥分发方法。

Step1:基站密钥生成中心随机选取一个大素数 p 和 Zp^* 上的生成元以及一个 Z_{p-1} 上的 n 维矢量 $d = (d_1, d_2, \cdots, d_n)$,计算 $h = (h_1, h_2, \cdots, h_n)$,使得 $h_i = gd_i (\mathrm{mod}\ p)$。对所有用户公开 p、h 和一个单向函数 $f(\cdot)$,保持 g 和 d 的秘密。

Step2:终端入网注册时,向密钥中心提供其身份 ID,以二进制表示为 $(x_1, x_2, \cdots, x_k)$,密钥中心计算出其二进制扩展身份信息 $\mathrm{EID} = f(\mathrm{ID}) = (y_1, y_2, \cdots, y_n)$。根据终端的扩展身份信息进一步计算出该终端的私钥 Pkey1 并将其发送给该终端。

Step3:终端之间建立通信连接时,发送终端可以用接收终端公开的 ID 计算出接收终端的扩展 ID,得到 $\mathrm{EID}_2 = F(\mathrm{ID}) = (y_1, y_2, \cdots, y_n)$,进一步可以得到 $Z_2 = g * \mathrm{Pkey}_2 (\mathrm{modp})$。然后,发送终端通过私密密钥 Pkey_1 计算出 $K_{12} = Z_2 * \mathrm{Pkey}_1 (\mathrm{modp}) = g * \mathrm{Pkey}_1 * \mathrm{Pkey}_2 (\mathrm{modp})$。接收终端在接收到密文文件后,接收终端也可以计算出 $K_{21} = Z_1 * \mathrm{Pkey}_2 (\mathrm{mod}\ p) = g * \mathrm{Pkey}_1 * \mathrm{Pkey2}\ (\mathrm{mod}\ p)$。从运算结果可以看出,发送方和接收方得到的密码是相同的。

X-IDEA 加密算法通过 X_IDEAKEY 生成 832 位的子密钥,对初始密钥也不做 128 位的长度限制,所以上面方法生成的密钥可直接作为 X-IDEA 的初始密钥,无需进行长度处理。

该密钥管理方法最大的特点是不需要设立专门的密钥管理中心,密钥产生过程计算轻量级,通信量小,非常符合移动通信系统的特点。

3.2 手机安全传输系统

本系统验证图文安全传输所搭建的平台是利用 Android 开发的手机通讯系统,移动基站设置密钥生成中心因实验条件的限制,采用离线生成的方式。手机终端基于 Android 平台进行开发,终端中图文加密系统包含三个基本模块:通讯模块,负责终端之间建立通

讯;密钥模块,接收密钥生成中心发送的私钥并生成密钥;加解密模块,使用 X-IDEA 算法对图文文件进行加密或解密。

手机图文安全传输基本流程如下:

Step1:终端入网注册,入网终端密钥模块获得密钥中心发送的私钥。终端之间图文加密传输时,通信双方将通过该私钥与通信对方的身份信息计算出加解密密钥。前面已经证明通信双方获得的密钥是相同的。

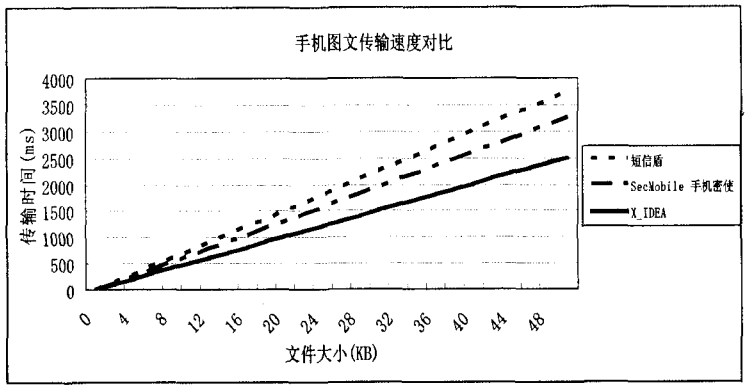

图 1 手机图文加密传输速度对比图

Step2:发送终端请求图文发送,通讯模块建立与接收端的通信连接。发送端密钥模块根据接收端的身份信息及发送端密钥计算加密密钥。

Step3:发送端加解密模块加密图文文件明文。

为使系统更具普遍性和通用性,X-IDEA 加密系以二进制的方式对图文文件进行加解密。所以,加解密过程对图文文件的类型没有特殊的限制。

对于文件长度较大的明文文件,加密前可进行压缩。根据文件的属性创建一临时文件,X-IDEA 依次将各明文分组进行加密,生成的密文分组存储在手机的外存储器中,已经加密的明文分组也同时删除。加密完成后,将手机外存储器中所有的密文分组写入临时文件中,此时明文文件已被删除,将临时文件以明文文件命名,这样保证了加密前后文件名的一致性。

Step4:通信双方的通信模块完成密文传输,发送方终端密钥模块销毁加密密钥,接收终端密钥根据发送终端身份信息及私钥计算解密密钥。

Step5:接收终端使用 X-IDEA 算法解密密文文件。

密文文件若为压缩文件则先对其进行解压缩,X-IDEA 算法先以分组的方式将所有的密文分组解密,将得到的所有密文分组,再按照加密前明文重组方式的逆过程将明文组合恢复明文文件,加密前明文重组时若有特殊字符的补位此时应将其删除。

Step6:接收终端密钥模块销毁解密密钥。通讯双方通讯模块结束通讯连接。

从上可以看出,图文信息加解密都是在终端上完成且为端到端的加密方式,所以即使移动通信提供商也无法破解终端之间传送的图文信息。

由于实验条件限制,无法在移动基站设置密钥生成中心,手机终端私钥采用计算机离线生成输入的方式,采用手机号作为终端身份标识。图 1 为 X-IDEA 算法下手机图文加密与当前几款比较流行的手机图文加密软件加密速度实验结果对比。

实验结果表明 X-IDEA 加密算法在图文加解密速度上较其他方法有明显的优势。X-IDEA 的设计过程中相当于嵌套了 IDEA 算法,算法安全性也不容置疑。

4 结束语

X-IDEA 算法是基于 IDEA 算法的改进,加密过程中当前被加密明文分组使用前一明文分组作为组密钥,所以 X-IDEA 算法的加密过程综合了分组加密和序列密码的加密特点,其安全性较 IDEA 算法有所提高;X-IDEA 算法的子密钥生成方式一方面良好地解决了弱密钥问题,对初始密钥不再严格要求为 128 位,使算法的适用性和灵活性更强;移动通信系统中应用基于身份的密钥管理方法也是安全、便捷的。

参考文献:

[1] Lai X. On the Design and Security of Block Ciphers[D]. Konstanz:Hartung-gorre Verlag,1992.

[2] National Bureau of Standards. Data Encryption Standard[S]. FIPS Pub.,1977.

[3] 张青凤,殷肖川,李长青. IDEA 算法及其编程实现[J]. 现代电子技术,2006,29(1):69-71.

[4] 吴伟彬,黄元石. IDEA 算法的改进及其应用[J]. 福州大学学报,2004,32(12):28-31.

[5] 杨维忠,李 形,都 林. IDEA 密钥空间扩展研究[J]. 计算机工程与设计,2004,25(11):1903-1904.

[6] 金茂顺. IDEA 弱密钥[J]. 密码与信息,1997,61(3):9-14.

[7] Joan D,Govaerts R,Vandewalle J. Weak keys for IDEA[M]. [s.l.]:[s.n.],1993:224-231.

[8] 徐彦彦,徐正全,任延珍. 视频会议系统安全体系设计[J]. 计算机工程与应用,2006(14):208-211.

[9] 覃如贤. 数据加密技术及其在电子商务中的应用[J]. 微计算机信息,2010(30):72-73.

[10] 霍士伟,蔡中民,罗长远. 普适环境中基于身份的组密钥管理方案[J]. 计算机应用,2011,31(4):981-983.

[11] 闫鸿滨. 密钥管理技术研究综述[J]. 南通职业大学学报,2011,25(1):79-83.

[12] 王平水,赵俊杰. 多用户环境中签名方案的安全性研究[J]. 计算机技术与发展,2009,19(1):158-160.