SM4 算法 S 盒输入的相关性能量攻击的研究

张 琪 吴 震 王 敏 杜之波 饶金涛
(成都信息工程学院信息安全工程学院 四川 成都 610225)

摘 要 在对 SM4 算法非线性 S 盒运算输出进行侧信道能量攻击的基础上,针对 SM4 算法中线性 S 盒输入提出相关性能量攻击分析的方法。该方法结合相关性能量攻击原理,利用汉明距离能量泄露模型进行攻击,该模型能够更准确刻画假设能量消耗与实测能量消耗之间的关系。在利用此方法获取前四轮或末四轮轮密钥的基础上,推算出 128 bit 的原始加密密钥。实际攻击结果表明,通过攻击出前四轮轮密钥后,可以成功地推出原始加密密钥。该攻击方法对 SM4 算法 S 盒输入有效可行,同时也扩展了对 SM4 算法的侧信道能量攻击方法。

关键词 相关性能量攻击 汉明距离模型 SM4 算法

中图分类号 TP3 **文献标识码** A DOI:10.3969/j.issn.1000-386x.2015.12.068

RESEARCH ON CORRELATION POWER ATTACK ON SBOX-INPUT OF SM4 ALGORITHM

Zhang Qi Wu Zhen Wang Min Du Zhibo Rao Jintao
(*School of Safety Engineering, Chengdu University of Information Technology, Chengdu 610225, Sichuan, China*)

Abstract On the basis of side channel power attack against the nonlinear sbox operation output of SM4 algorithm, in this paper we propose the method of correlation power attack analysis aiming at linear sbox input of SM4 algorithm. Combining the theory of correlation power attack, the method makes use of power leakage model of Hamming distance to conduct the attack, which can more accurately describe the relationship between the assumed power consumption and the measured power consumption. Through this attack, the round keys of the first or the last four rounds of SM4 can be obtained, and based on that the 128 bit original encryption key is derived. The results of actual attack also show that the original encryption key can be successfully calculated by attacking the keys of the first four rounds. The attack method is effective and feasible on sbox-input of SM4, and meanwhile also expands the methods of side channel power attack against SM4 algorithm.

Keywords Correlation power attacks Hamming distance model SM4 algorithm

0 引 言

密码设备在运行密码算法时会泄露包括算法的执行时间、电磁辐射及能量消耗等物理信息。能量攻击就是基于密码设备在执行加解密过程中产生的能量消耗而进行的攻击。能量攻击通过采集密码电子设备的能量消耗,并结合密码学与统计学等综合分析破译秘密信息。目前,基于能量消耗的分析技术发展迅速,包括计时攻击 TA(timing analysis)[1,2],简单能量攻击 SPA(simple power analysis)[3],差分能量攻击 DPA(Differential Power Analysis)[3-5] 和现在应用较广泛的相关性能量攻击 CPA(correlation power analysis)[6,7] 等。

SM4 算法是我国官方公布的第一个商用密码算法,也是无线局域网产品使用的算法,其安全性的研究对无线局域网产业发展和国内商用密码算法具有重要意义[8]。自 SM4 算法公布起,对其能量攻击的研究也陆续展开,文献[9-13]针对 SM4 算法结构进行了差分能量攻击和代数旁路攻击的研究,但目前还未出现对 SM4 算法相关性能量攻击的文献。

本文对 SM4 算法的结构和运算特点进行了分析,以 S 盒输入作为攻击点,基于汉明距离模型[14] 进行了 CPA 能量攻击,通过 CPA 攻击成功恢复 SM4 算法前四轮或末四轮轮密钥,从而推出原始加密密钥。

1 SM4 算法简介

SM4 算法是一个分组密码算法,分组长度为 128 比特,密钥长度为 128 比特,加密算法与密钥扩展算法都采用 32 轮非线性迭代结构。加密算法与解密算法的结构相同,只是轮密钥的使用顺序相反。下面以加密算法和密钥扩展算法为例,介绍 SM4 算法。

1.1 SM4 加密算法

SM4 加密算法的整个流程如图 1 所示。

收稿日期:2014-02-06。"十二五"国家密码发展基金资助项目(MMJJ201101022);四川省科技支撑计划项目(2011GZ0170);四川省教育厅重点科研基金资助项目(13ZA0091);成都信息工程学院科研基金项目(CRF201301)。**张琪**,硕士生,主研领域:信息安全,侧信道攻击与防御。**吴震**,副教授。**王敏**,讲师。**杜之波**,讲师。**饶金涛**,助教。

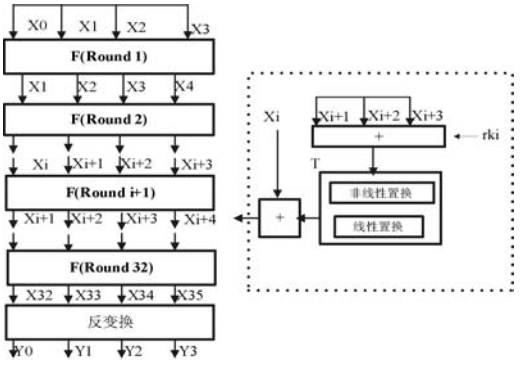

图 1　SM4 算法加/解密

在图 1 中 $X_i \in Z_2^{32}$(Z_2^e 表示 e bit 的向量集),输入明文为 $(X_0,X_1,X_2,X_3) \in (Z_2^{32})^4$,输出密文为 $(Y_0,Y_1,Y_2,Y_3) \in (Z_2^{32})^4$,轮密钥为 $rk_i \in (Z_2^{32})^4$,$i = 0,1,2,\cdots,31$,虚线部分为轮函数 F,其具体流程如图 2 所示。

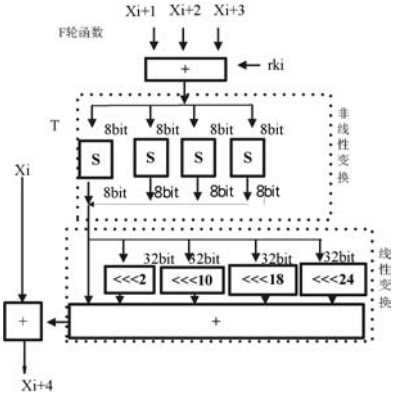

图 2　轮函数

由图 2 所示,轮函数 F 包括的运算有异或和合成置换(用 T 表示),其中 T 是由线性变换(用 L 表示)和非线性置换(用 τ 表示)组成,如式(1)所示。非线性置换 τ 是由 4 个并行的 S 盒构成,S 盒为固定的 8 bit 输入 8 bit 输出的置换,记为 $Sbox(\,)$。非线性变换 τ 的输入记为 $A \in Z_2^{32}$,输出记为 $B \in Z_2^{32}$,B 也是线性变换 L 的输入,L 的输出记为 C 线性变换如式(2)所示:

$$\begin{aligned} X_{i+4} &= F(X_i,X_{i+1},X_{i+2},X_{i+3},rk_i) \\ &= X_i \oplus T(X_{i+1} \oplus X_{i+2} \oplus X_{i+3} \oplus rk_i) \end{aligned} \tag{1}$$

$$\begin{aligned} C = L(B) &= B \oplus (B <<< 2) \oplus (B <<< 10) \oplus \\ &(B <<< 18) \oplus (B <<< 24) \end{aligned} \tag{2}$$

式(2)中的 B 可以用下式描述:

$$B = \tau(A) = sbox(A_0) \parallel sbox(A_1) \parallel sbox(A_2) \parallel sbox(A_3) \tag{3}$$

其中 $A = (A_0,A_1,A_2,A_3) \in (Z_2^{32})^4$。

1.2　密钥扩展算法

SM4 算法中加密算法的 32 轮密钥是由加密密钥通过密钥扩展算法产生的,设加密密钥为 $MK = (MK_0,MK_1,MK_2,MK_3)$,中间变量为 $K_i \in (Z_2^{32})^4$,轮密钥为 $rk_i \in (Z_2^{32})^4$,其中 $i \in \{0,1,2,\cdots,31\}$ 则轮密钥的产生方法如下:

$$\begin{aligned} (K_0,K_1,K_2,K_3) = (&MK_0 \oplus FK_0,MK_1 \oplus FK_1,MK_2 \oplus \\ &FK_2,MK_3 \oplus FK_3) \end{aligned} \tag{4}$$

$$rk_i = K_{i+4} = K_i \oplus T(K_{i+1} \oplus K_{i+2} \oplus K_{i+3} \oplus CK_i) \tag{5}$$

其中线性变换 L 为:

$$L(B) = B \oplus (B <<< 13) \oplus (B <<< 23)$$

在密钥扩展算法中,FK 为系统参数,CK 为固定参数。

2　相关性能量攻击原理

2004 年,Eric Brier 等人提出了 CPA 攻击[6,7],这种攻击技术利用了统计学中的皮尔逊相关系数 ρ 进行分析攻击,其攻击过程描述为:

1)在密码芯片系统中,将 N 组不同的明文(密文)数据和真实密钥进行加密(解密)运算,并获取密码设备的能耗即为能量迹,记为 T。

2)通过猜测密钥,产生相应的中间值,根据中间值的汉明重量或者汉明距离泄露,计算得到假设能量消耗,记为 H。

3)根据下式计算假设能量消耗与实测能量迹的线性相关系数。

$$\rho(T,H) = \frac{E(T.H) - E(T)E(H)}{\sqrt{Var(T)Var(H)}} \tag{6}$$

式(6)中 $E(\,)$ 表示求平均值,$Var(\,)$ 表示求方差。ρ 的范围在 $[-1,1]$ 之间,当 ρ 取绝对值的最大值时,即假设能量消耗与真实测量的能量迹线性相关性(即相关性系数 ρ)达到最大,则此时 H 所对应的猜测的密钥即为正确的密钥。

3　针对 SM4 算法 S 盒输入的 CPA 攻击

侧信道能量方法是否有效,其关键在于密码算法中的攻击点和相应能量模型的选择。SM4 算法在每一轮迭代中都要先将每轮的输入与每轮的轮密钥进行异或操作即 S 盒输入,在执行完这一步操作后会产生一个中间值 V 如式(7)所示:

$$V = X_{i+1} \oplus X_{i+2} \oplus X_{i+3} \oplus rk_i \tag{7}$$

由式(7)知 V 中含有明文和轮密钥的信息,故在进行 CPA 攻击时可将 V 作为攻击的中间数据,即攻击点为 S 盒输入。在能量攻击中,能量模型的选择一般是由密码算法的实现方式决定,软实现的密码算法一般选用汉明重量模型;硬实现的密码算法一般选用汉明距离模型。故在对硬实现的 SM4 算法进行 CPA 攻击时,选用汉明距离模型($HD(v1,v2)$)。汉明距离的前续状态 $v1$ 为前一轮 S 盒输入,后继状态 $v2$ 为当前轮 S 盒输入。

对 S 盒输入可以选择前四轮或末四轮进行 CPA 攻击,攻击出轮密钥后利用密钥扩展算法即可以推出原始密钥。下面以攻击前四轮的第一轮轮密钥为例,说明针对 SM4 加密算法 S 盒输入 CPA 攻击的基本思想:

1)采集能量迹,对 N 组不同的明文进行加密运算,采集能量迹,建立采样能量消耗矩阵 $M(N \times T)$:

$$M(N \times T) = \begin{bmatrix} t_{1,1}t_{1,2}\cdots t_{1,T} \\ t_{2,1}t_{2,2}\cdots t_{2,T} \\ \vdots \\ t_{m,1}\cdots t_{m,T} \\ \vdots \\ t_{N,1}t_{N,2}\cdots t_{N,T} \end{bmatrix}$$

其中,t_m 表示为第 m 个明文对应的能量迹,T 为每条能量迹中采样点个数。

2)选择 S 盒输入为攻击点,并利用其汉明距离模型进行 CPA 攻击。

对于硬件,默认寄存器的初始状态为 0,则第一轮的 S 盒输入与寄存器的初始状态的汉明距离等效为:

$$HD(v1,v2) = HW(0 \oplus X_1 \oplus X_2 \oplus X_3 \oplus rk_0) = HW(X_1 \oplus X_2 \oplus X_3 \oplus rk_0)$$

3) 猜测密钥,计算 S 盒输入的中间值确定中间值矩阵。

从理论上讲,对 rk_0 从单比特到多比特到多字节都可以攻击,由于在实现上每个 S 盒的输入为 8 bit,存在独立的 8 bit 读写,用 8 bit 攻击更容易成功,故本方法每次攻击出猜测密钥的一个字节,通过进行多次攻击从而获得对应轮的轮密钥。对第 m 组明文进行加密运算,猜测轮密钥 rk_0 的最低节 $rk_0[0]$,$rk_0[0]$ 有 256 种可能的取值,对应的中间值分别为 $V_{m,j}[0] = X_1[0] \oplus X_2[0] \oplus X_3[0] \oplus rk_{0,j}[0]$,其中 $j \in \{1,\cdots,256\}$;对 N 组不同明文输入进行加密操作时,依次计算 256 个猜测轮密钥字节 $rk_{0,j}[0]$ 对应的中间值可以确定中间值矩阵:

$$VV(N \times 256) = \begin{bmatrix} V_{1,1}[0]V_{1,2}[0]\cdots V_{1,256}[0] \\ V_{2,1}[0]V_{2,2}[0]\cdots V_{2,256}[0] \\ \vdots \\ V_{m,1}[0]V_{m,2}[0]\cdots V_{m,256}[0] \\ \vdots \\ V_{N,1}[0]V_{N,2}[0]\cdots V_{N,256}[0] \end{bmatrix}$$

4) 将中间值映射为假设能量消耗值矩阵。

由步骤 2) 将步骤 3) 中的中间值映射为假设能量消耗:$h_{m,j}[0] = HD(0,V_{m,j}[0]) = HW(V_{m,j}[0])$,即第 m 组明文第 j 个猜测密钥最低字节对应的假设能量消耗值。该 N 组明文对应的假设能量消耗矩阵为:

$$H(N \times 256) = \begin{bmatrix} h_{1,1}[0]h_{1,2}[0]\cdots h_{1,256}[0] \\ h_{2,1}[0]h_{2,2}[0]\cdots h_{2,256}[0] \\ \vdots \\ h_{m,1}[0]h_{m,2}[0]\cdots h_{m,256}[0] \\ \vdots \\ h_{N,1}[0]h_{N,2}[0]\cdots h_{N,256}[0] \end{bmatrix}$$

5) 计算假设能量消耗矩阵与能量迹矩阵的线性相关系数,得到正确的猜测密码。

对步骤 1) 的能量迹矩阵 M 和步骤 4) 的假设能量消耗矩阵 H 按列计算两者的相关系数 $\rho_{j,n}$:

$$\rho_{j,n} = \frac{\sum_{m=0}^{N}(h_{m,j} - \bar{h}_j)(t_{m,n} - \bar{t}_n)}{\sqrt{\sum_{m=0}^{N}(h_{m,j} - \bar{h}_j)^2 \sum_{m=0}^{N}(t_{m,n} - \bar{t}_n)^2}} \tag{8}$$

其中,$\rho_{j,n}$ 表示第 j 个猜测密钥对应的假设能量消耗与第 n 个时间点能量迹之间的线性相关系数。计算两个矩阵所有列列之间的相关系数,得到假设能量消耗矩阵和能量迹矩阵的相关系数矩阵为:

$$R(256 \times T) = \begin{bmatrix} \rho_{1,1}[0]\rho_{1,2}[0]\cdots\rho_{1,T}[0] \\ \rho_{2,1}[0]\rho_{2,2}[0]\cdots\rho_{2,T}[0] \\ \vdots \\ \rho_{j,1}[0]\rho_{j,2}[0]\cdots\rho_{j,T}[0] \\ \vdots \\ \rho_{256,1}[0]\rho_{256,2}[0]\cdots\rho_{256,T}[0] \end{bmatrix}$$

选取 R 矩阵中的最大值,最大值对应的猜测密钥 $rk_{0,j}[0]$ 为正确的第一轮轮密钥的最低字节。

重复步骤 1) - 步骤 5),可以分别获得第一轮轮密钥的其他 3 个字节,从而得到第一轮正确轮密钥 rk_0,对于其他三轮,使用轮密钥 rk_i 进行第 i 轮($i = 1,2,3$)加密运算,得到第 i 轮的 N 组轮输出即为下一轮(第 $i+1$ 轮)的输入,依次获得(rk_1,rk_2,rk_3)。

再根据密钥扩展算法依次利用式(5)、式(4)可以推出 K_3、K_2、K_1 和 K_0,从而得到 SM4 算法的加密密钥 MK。

4 SM4 算法 S 盒子输入相关性能量攻击实验

4.1 针对 SM4 算法前四轮 S 盒输入的 CPA 攻击

令 MK = 0x0123456789abcdeffedcba9876543210,明文随机产生,在 FPGA 上对随机产生的 10 000 组明文 (X_0,X_1,X_2,X_3) 和固定密钥 MK 进行 SM4 加密运算,并利用示波器采集加密运算中所产生的能量迹。

在实验中,所要分析的是 32 轮加密运算的能量迹的前四轮能量迹,32 轮加密运算的能量迹如图 3 所示。

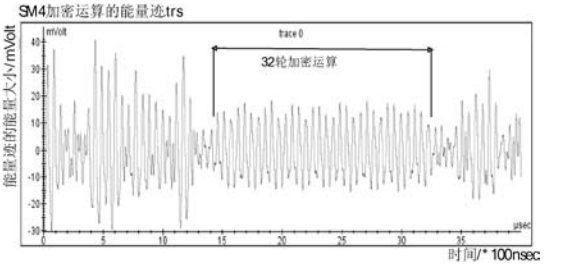

图 3 SM4 32 轮加密运算的能量迹

对图 3 中的执行 32 轮加密运算所得到的能量迹放大截取实验所需分析的 SM4 加密运算的前四轮能量迹,如图 4 所示。

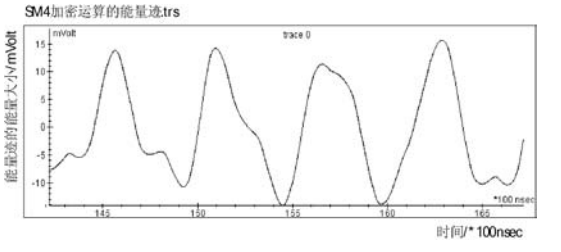

图 4 前四轮加密运算的能量迹

根据第 3 节的攻击方法对第一轮 rk_0 进行 CPA 攻击,攻击结果如表 1 所示。取相关系数绝对值最大对应的字节为攻击结果,相关系数的正负与芯片的类型有关,对于本芯片统一取正相关的相关系数,即第一轮的轮密钥 rk_0 = 0xF12186F9。

表 1 第一轮结果

轮密钥字节	序号	相关系数	猜测密钥
1	1	0.0109	241(0xF1)
	2	-0.0109	21 (0x15)
	3	0.0091	161(0xA1)
	4	-0.0091	51 (0x33)
2	1	-0.0116	52 (0x34)
	2	0.0116	33 (0x21)
	3	0.0103	226(0xE2)
	4	-0.0103	23 (0x17)
3	1	-0.0144	43 (0x2B)
	2	0.0144	134 (0x86)
	3	-0.0115	144 (0x90)
	4	0.0115	91 (0x5B)

续表 1

轮密钥字节	序号	相关系数	猜测密钥
4	1	-0.0123	159(0x9F)
	2	0.0123	249(0xF9)
	3	-0.0111	141(0x8D)
	4	0.0111	35 (0x23)

在已经获得第一轮轮密钥基础上,根据第 3 节的 CPA 攻击原理及攻击方法依次对其它三轮 S 盒输入实施 CPA 攻击,结果如表 2 - 表 4 所示。取相关系数绝对值最大对应的字节为攻击结果,依然取正相关的相关系数得第二轮的轮密钥为: rk_1 = 0x41662b61,第三轮的轮密钥为: rk_2 = 0x5A6AB19A,第四轮的轮密钥为: rk_3 = 0x7ba92077。

表 2　第二轮结果

轮密钥字节	序号	相关系数	猜测密钥
1	1	-0.0111	190(0xBE)
	2	0.0111	65 (0x41)
	3	0.0095	193(0xC1)
	4	-0.0095	62 (0x3E)
2	1	-0.0126	153 (0x99)
	2	0.0126	102 (0x66)
	3	0.0113	230(0xE6)
	4	-0.0113	25 (0x19)
3	1	-0.0134	212(0xD4)
	2	0.0134	43 (0x2B)
	3	-0.0114	148 (0x94)
	4	0.0114	107(0x6B)
4	1	-0.0143	158(0x9E)
	2	0.0143	97 (0x61)
	3	-0.0121	156(0x9C)
	4	0.0121	99 (0x63)

表 3　第三轮结果

轮密钥字节	序号	相关系数	猜测密钥
1	1	-0.0107	165(0xA5)
	2	0.0107	90 (0x5A)
	3	0.0094	229(0xE5)
	4	-0.0094	26 (0x1A)
2	1	-0.0118	149 (0x95
	2	0.0118	106(0x6A)
	3	0.0112	234(0xEA)
	4	-0.0112	21 (0x15)
3	1	0.0107	177(0xB1)
	2	-0.0107	78 (0x4E)
	3	0.0104	241 (0xF1)
	4	-0.0104	14 (0x0E)
4	1	0.0128	154(0x9A)
	2	-0.0128	101 (0x65)
	3	0.0109	152 (0x98)
	4	-0.0109	103 (0x67)

表 4　第四轮结果

轮密钥字节	序号	相关系数	猜测密钥
1	1	-0.0725	132(0x84)
	2	0.0725	123(0x7B)
	3	-0.0635	196(0xC4)
	4	0.0635	59 (0x3B)
2	1	0.0689	169(0xA9)
	2	-0.0689	86 (0x56)
	3	0.0579	233(0xE9)
	4	-0.0579	22(0x16)
3	1	-0.0662	223(0xDF)
	2	0.0662	32 (0x20)
	3	-0.0557	159(0x9F)
	4	0.0557	96 (0x60)
4	1	-0.0722	136 (0x88)
	2	0.0722	119 (0x77)
	3	-0.0612	200(0xC8)
	4	0.0612	55 (0x37)

4.2　攻击结果分析

根据 4.1 节针对 SM4 算法 S 盒输入进行 CPA 攻击分析实验,攻击出轮密钥 rk_0、rk_1、rk_2 和 rk_3。再利用密钥扩展算法依次反推出 K_3、K_2、K_1 和 K_0,最终可以推出加密密钥为 0x0123456789abcdeffedcba9876543210,与所要攻击的密钥 MK 是一致的。

4.3　攻击方法的性能分析

攻击方法所需的时间复杂度是衡量攻击方法有效性的一个标准[15]。实际的攻击实验,一次攻击出轮密钥的 8 个比特,每一轮需攻击四次得到一个 32 位的轮密钥,则完整攻击 SM4 算法所需的时间复杂度为 $2^8 \times 4 \times 4 = 2^{12}$,而直接对 32 位的轮密钥进行攻击,攻击四次,所需时间复杂度为 $2^{32} \times 4 = 2^{34}$。利用本文提出的攻击方法可以降低攻击算法的时间复杂度,从而证明了本攻击方法的有效性。

5　结　语

基于 SM4 密码算法结构和轮运算的特点,以明文与轮密钥异或输入即 S 盒输入为 CPA 攻击的攻击点,并通过建立汉明距离模型,汉明距离模型的前续状态 $v1$ 为前一轮 S 盒输入,后继状态 $v2$ 为当前轮 S 盒输入,提高了正确的猜测密钥与能量信息之间的相关性,增强了 CPA 攻击的有效性。

以 S 盒输入为攻击点进行实测 CPA 攻击,可以依次恢复出前四轮或者末四轮的轮密钥,根据密钥扩展算法,从而推算出 128 bit 的加密密钥,证明了该攻击方法的有效可行性。

参　考　文　献

[1] 王韬,赵新杰,郭世泽. 针对 AES 的 Cache 计时模板攻击研究[J]. 计算机学报,2012,35(2):325 - 341.

[2] 田军舰,寇应展,陈财森. RSA 公钥密码算法差分计时攻击研究[J]. 计算机工程,2011,37(5):146 - 148.

[3] 童莲,钱江. 椭圆曲线中抗 SPA 和 DPA 攻击标量乘算法研究[J]. 计算机工程与应用,2010,46(35):72 - 74.

(下转第 333 页)

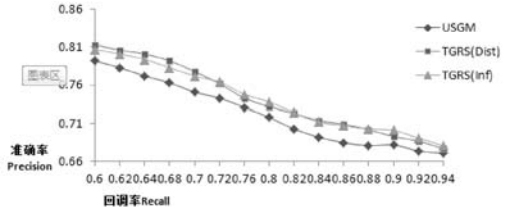

图 3　三种算法的准确率/回调率

由此可见通过加入基于社会关系的可信值,从而计算相应的用户和群体之间的相似度,具备一定可信的邻居相似度对提升算法的准确性和精确性具有推动作用。

(2) 影响力衰减因子 α 对算法 TGRS(Inf)性能的影响

这里设置邻居数 $k = 50$ 和返回的项目数 $N = 10$,实验结果如图 4 所示,随着影响力因子 α 的降低,TGRS(Inf)在准确率和回调率方面的表现。可以看在指标准确率 Precision 上的表现先为上升后为下降,而回调率 Recall 则是与其增减趋势相反。这是因为当影响力因子 α 较低时,对邻居的区分度不大,所以伴随其增加,基于影响力的社交信任因子可以较好的区分邻居的可信度;但是当其超过一定阈值,影响力因子 α 过大造成大多数的社交信任因子过低,反而造成区分度再次降低,从而准确率受到影响。

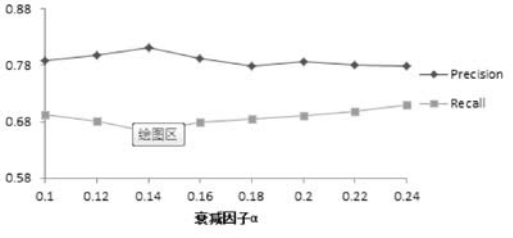

图 4　影响力衰减因子 α 对算法 TGRS(Inf)的影响

4　结　语

群体推荐在实际应用中具有重要地位,本文利用用户的社交关系上下文信息来提升算法的准确度,提出了两种不同的可信度因子计算方法,并将该因子用于寻找群体的相似邻居中,从而提升邻居质量,改善推荐的结果。基于实际数据集的仿真实验表明两种可信度因子的有效性。下一步将考虑通过对隐社交因素进行分析来改进可信度因子的计算,隐社交因素主要依赖于对用户之间交互行为的分析。

参　考　文　献

[1] Bobadilla J, Ortega F, Hernando A, et al. Recommender Systems Survey [J]. Knowledge-Based Systems, 2013, 46(1): 109 - 132.

[2] Jameson A, Smyth B. Recommendation to Groups [M]. The Adaptive Web. Heidelberg: Springer-Verlag Berlin, 2007: 596 - 627.

[3] Dwork C, Kumar R, Navor M, et al. Rank Aggragation Methods for the Web[C]//WWW, New York, 2001: 613 - 622.

[4] Young H P, Levenglick A. A Consistent Extension of Condorcet's Election Principle [J]. SIAM Journal on Applied Mathematics, 1978, 35 (2): 285 - 300.

[5] Baltrunas L, Makcinskas T, Ricci F. Group Recommendation with Rank Aggregation and Collaborative Filtering [C]//RecSys, Barcelona, 2010: 119 - 136.

[6] Salamo M, Mccarthy K, Smyth B. Generating Recommendation for Consensus Negotiation in Group Personalization Services [J]. Journal Personal and Ubiquitous Computing, 2012, 16(5): 597 - 610.

[7] Berkovsky S, Freyne J. Group-based Recipe Recommendations: Analysis of Data Aggregation and Collaborative Filtering[C]//RecSys, Barcelona, 2010: 111 - 118.

[8] Garcia I, Sebastia L, Onaindia E. On the Design of Individual and Group Recommender Systems for Tourism[J]. Expert Systems with Applications, 2011, 38(6): 7683 - 7692.

[9] Chirstensen I A, Schiaffino S. Entertainment Recommender Systems for Group of Users[J]. Expert Systems with Applications, 2011, 38: 4127 - 14135.

[10] Bobadilla J, Ortega F, Hernando A. Generalization of Recommendation Systems: collaborative Filtering Extended to Groups of Users and Restricted to Groups of Items [J]. Expert Systems with Applications, 2012, 39(1): 172 - 186.

[11] Ortega F, Bobadilla J, Hernando A, et al. Incorporating Group Recommendations to Recommender Systems: Alternatives and Performance [J]. Information Processing and Management, 2013, 49 (4): 895 - 901.

[12] Pera M S, Ng Y K. A Group Recommender for Movies based on Content Similarity and Popularity[J]. Information Processing and Management, 2013, 49(3): 673 - 687.

[13] 王立才,孟祥武,张玉洁. 上下文感知推荐系统[J]. 软件学报, 2012, 23(1): 1 - 20.

[14] 吴信东,李毅,李磊. 在线社交网络影响力分析[J]. 计算机学报, 2014, 37(4): 2 - 10.

[15] Page L, Brin S, Motwani R, et al. The PageRank Citation Ranking: Bringing Order to the Web[C]//Stanford InfoLab, 1999: 1 - 14.

[16] Ma H, Zhou D Y, Liu C, et al. Recommender Systems with Social Regularization[C]//Proceedings of the fourth ACM International Conference on Web Search and Data Mining ACM, 2011: 287 - 296.

(上接第 293 页)

[4] 李志强. 分组密码芯片差分能量攻击和安全评估技术研究[D]. 河南:解放军信息工程大学, 2012.

[5] 赵东艳,何军. 针对密码算法的高阶 DPA 攻击方法研究[J]. 电子技术与应用, 2013, 39(10): 56 - 58.

[6] Brier E, Clavier C, Olivier F. Correlation power analysis with a leakage model[C]. Cryptographic Hardware Embedded System-CHES 2004 Lecture Notes in Computer Science, 2004: 16 - 29.

[7] 段二朋,严迎建,刘凯. 针对 AES 密码芯片的 CPA 攻击点选择研究[J]. 计算机工程与应用, 2013, 49(4): 91 - 94.

[8] 石陶. 分组密码算法 SMS4 的安全性分析[D]. 山东:山东大学, 2013.

[9] 白雪飞,郭立,徐艳华. SMS4 密码算法的差分功耗分析攻击研究[J]. 微小型计算机系统, 2009, 30(3): 541 - 544.

[10] 郑秀林,沈薇,张栋. SM4 算法安全性研究[J]. 北京电子科技学院学报, 2008, 16(4): 14 - 18.

[11] 李浪,李仁发,李静. 一种 SM4 加密算法差分能量攻击[J]. 北京电子科技学院学报, 2008, 37(7): 39 - 41.

[12] 沈薇. SM4 算法的能量攻击及其防御研究[D]. 西安:西安电子科技大学, 2009.

[13] 刘会英,赵新杰,王韬. 基于汉明重的 SMS4 密码代数旁路攻击研究[J]. 计算机学报, 2013, 36(6): 1183 - 1193.

[14] 李万兴. 密码算法的能量分析研究[D]. 山东:山东大学, 2011.

[15] 李超,孙兵,李瑞林. 分组密码的攻击方法与实例分析[M]. 北京:科学出版社, 2010.