动态混沌加解密及其在VoIP中的应用

石 婕[1] 仲伟波[2] 葛秀梅[2]
(苏州理工学院 镇江 212003)[1] (江苏科技大学电信学院 镇江 212003)[2]

摘 要 随着网络普及和带宽提升,网络语音传输已成为现实,但网络的开放性也给语音安全带来了巨大威胁。数据加密常被用来保证网络语音通信的安全,混沌序列的宽频谱、类随机、参数敏感等特点使其非常适合作为加解密密钥。为避免长时间使用固定混沌序列作为密钥带来的安全隐患,设计并实现了一种用于VoIP的动态混沌加解密方案,利用混沌密钥动态交换机制实现收发端混沌根密钥交换,由根密钥通过Henon映射、改进的Logistic映射及非线性置换随机生成混沌密钥,接收端根据接收到的根密钥先生成解密密钥,然后对语音密文进行解密。测试结果表明,该动态混沌加解密系统具有良好的保密效果,可用于网络语音保密通信中。

关键词 加解密,网络语音传输,混沌密钥,动态密钥
中图法分类号 TN918.91 **文献标识码** A

Dynamic Chaotic Encryption and its Application in VoIP

SHI Jie[1] ZHONG Wei-bo[2] GE Xiu-mei[2]
(Suzhou Institute of Technology, Zhenjiang 212003, China)[1]
(School of Electronics & Information, Jiangsu University of Science & Technology, Zhenjiang 212003, China)[2]

Abstract VoIP has become reality with spread of the network and its increasing bandwidthbut the speech is exposed to danger for the openness of network. Data encryption is usually used to ensure the safety of speech communication and chao-tic sequence is very suitable as the decryption cipher for its wide spectrum random ness, sensitiv to initial parameters. In order to avoid the danger come from using fixed chaos sequence as the cipher for long timea VoIP dynamic chaotic encryption scheme was designed and implemented, in which Henon mapimproved Logistic map and a nonlinear map are combined to update chaotic cipher randomlyand the receiver decrypts data using the dynamic chaotic cipher obtained through the dynamic cipher exchange system. Experiment results show that this dynamic chaotic encryption system has high security and can be used for secure speech transmission.

Keywords Encryption and decryption, VoIP, Chaotic cipher, Dynamic cipher

1 引言

语音是人们传递信息的重要方式之一,随着网络的普及和传输速率的提高,网络传输语音已经成为现实。与传统PSTN系统不同,国际电联公布的VoIP协议如H.323,SIP,H.248及MGCP中,语音数据先被封装成RTP报文,然后被进一步封装成UDP报文和IP报文进行传输。由于网络的开放性,这些语音数据包极易被截获和解析,对语音网络传输安全造成威胁,数据加密是常用来保证语音安全的重要手段之一[1]。

加解密算法可分为对称和非对称两类,其中对称加解密中加解密采用同一密钥,其特点是算法公开、运算速度快,但其安全性相对较弱,密钥管理难度大,常用算法有DES、IDEA和AES等。非对称加解密中密钥分为公开和私有密钥,公开密钥用于加密,私有密钥用于解密,公开密钥可以公开,密钥管理较为简单,但算法复杂度较大,不适合实时性要求较高的加解密中,常用算法有RSA、DSA和ECC等[2]。为减小加解密对通话质量的影响,VoIP多采用对称加解密算法。

混沌是非线性系统中出现的一种貌似无规则的类随机过程,其确定的动力学方程保证了计算可靠性,混沌轨道的遍历性满足密码设计的扩散原则,混沌参数和初值敏感性满足密码设计的混乱原则。与传统密码相比,混沌密码具有结构简单、容易实现和安全高效等特点,已被广泛用于语音、图像加密中[3-5]。但数字化中位长的限制会造成系统混沌特性退化,从而使得基于一般混沌模型的密码系统并不如人们想像的安全,通过混沌时间序列分析方法能以较高精度很快地估算出其根密钥[6,7](系统参数或初始条件)。为了提升混沌密码的安全性,众多学者使用多个混沌系统或者在混沌序列输出时进行处理以减少混沌特性的退化,提升混沌密钥流的安全和整个加解密系统的安全[8-10]。

密钥交换是语音保密通信系统的重要组成部分,为实现VoIP动态混沌加解密,本文提出并实现了一个动态密钥交换

本文受江苏高校优势学科项目和船舶工业国防科技预研项目(10J3.5.2)资助。
石 婕(1981-),女,硕士,助理研究员,主要研究方向为计算机应用,E-mail:vebo_world@sohu.com;仲伟波(1975-),男,博士,副教授,主要研究方向为信号与信息处理;葛秀梅(1989-),女,硕士,助理工程师,主要研究方向为嵌入式系统、信号采集与处理。

机制，通过它可以随机更换混沌根密钥，系统中传递的是混沌根密钥，参与加解密运算的密钥分别在通信端计算而不在信道中传输。在语音通信过程中根据保密强度要求随机设定根密钥有效期，每次使用的混沌密钥长度及其有效期都较短，窃密者很难通过分析实时得到根密钥，即使得到某次根密钥，由于混沌密钥产生模型不可预知且有效期较短，也不会造成大面积的数据失密。另外，根密钥的随机更换还能够有效避免单一根密钥和数字化带来的混沌序列特性退化，从而减小密钥被破译的可能性，提高混沌密钥和系统的安全性。实验测试结果表明，本文方法具有较好的保密效果和稳定性，可用于网络语音保密通信中。

2 混沌密钥及加解密算法

混沌序列的初值敏感、遍历性特点使得其在密码系统研究中得到广泛关注，涌现了许多混沌密钥生成算法[11]。但由于混沌序列特性的退化，对于使用与明文无关的流密钥系统，通过选择明文攻击可较易获得密钥流，从而破解保密系统[12]。为此本文先利用 Henon 映射和改进的 Logistic 映射获得初始混沌序列，然后通过非线性置换得到加密密钥，以减小通过相空间重构被逆向迭代破译的可能，最后采用国际数据加密算法(IDEA)对数据加解密，系统模型如图 1 所示。

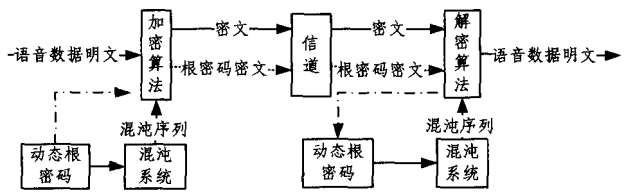


图 1 系统模型

2.1 混沌密钥的生成

系统先由 Henon 映射和改进的 Logistic 映射级联共同产生混沌序列，然后将此混沌序列进行非线性置换得到加密密钥。

系统中采用的 Henon 映射表达式为：

$$x_{n+1}=1+y_n-ax_n^2,\ y_{n+1}=bx_n \tag{1}$$

当 $a=1.4$，$b=0.3$ 时该映射所产生的序列具有典型的混沌特性，输入 x_0，y_0 两初值后进行 N(N 为大于 1000 的整数)次迭代，令 $MK_1=x_{M1}*x_N$，$MK_2=x_{M2}*x_N$，其中 $M1\neq M2$ 且小于但接近 N。

Logistic 映射的基本形式为：

$$x_{n+1}=\lambda x_n(1-x_n) \tag{2}$$

其中，$\lambda\in(0,4]$，$x_n\in[0,1]$，当 $\lambda\geqslant 3.57$ 时系统进入混沌状态，但式(2)的迭代结果存在空白窗和稳定窗，在[0,1]内不具备均匀分布的特性。针对式(2)所示的 Logistic 映射的上述问题，系统采用文献[13]给出的改进 Logistic 映射：

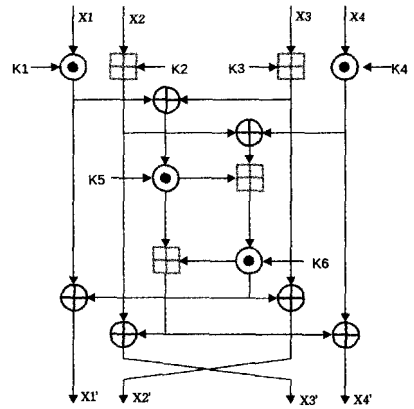
$$x_{n+2}=rx_{n+1}(1-x_{n+1})+(4-r)x_n(1-x_n) \tag{3}$$

其中，$x_n\in(0,1)$，当 $r\in[0,1.2849)\cup(3.4776,4]$时，除个别点外系统都处于混沌状态，且该映射得到的序列较基本 Logistic 映射的序列具有更好的混沌特性。

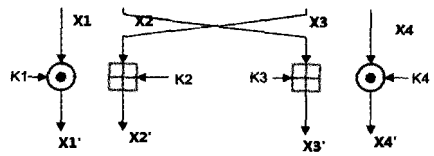
将 Henon 映射中得到的 MK_1 和 MK_2 的小数部分作为改进的 Logistic 映射的 x_0 和 x_1，经过 M 次迭代后截取所得混沌序列中最后 16 个值，通过如下非线性置换成加密密钥：将区间[0,1]平均分成 256 个子区间，每个区间用 0～255 表示。若混沌序列中某值落在第 i 个区间中，将其置换成整数 i 并标识该区间；若落入的区间 i 已标识过，则将 i 加 1 模 256，直到得到新的整数为止。如此迭代可获得一个有 16 个不重复数据的序列$\{a_0,\cdots,a_i,\cdots,a_{15}\}$，其中 $a_i\in\{0,1,\cdots,255\}$。将$\{a_0,\cdots,a_i,\cdots,a_{15}\}$中元素用二进制数表示，得到 128 位二进制密钥。

2.2 IDEA 加解密算法

James L. Massey 和来学嘉提出的 IDEA 是一种使用 128 位密钥，分组长度为 64 位的分组加密算法，具有较强的抗穷举攻击能力和抗差分密码分析攻击能力[14]。虽然若密钥含有大量 0 位则会产生弱加密等，但 IDEA 仍是目前常用的较安全的加密算法[15]。IDEA 将明文分成 4 个 16 位的子分组：X1，X2，X3 和 X4，并将其作为每轮的输入，每轮的执行步骤如图 2(a)所示，本轮的输出作为下一轮的输入。经过 8 轮运算之后，最后 4 个子分组重新连接到一起产生密文，如图2(b)所示。图中⊕表示按位异或，⊞表示模 2^{16} 加，⊙表示模 $2^{16}+1$ 乘。



(a)前 8 轮每轮的执行步骤



(b)最后一轮产生密文的步骤

图 2 IDEA 加解密过程

IDEA 加密所需的 52 个子密钥产生过程如下：首先将 128 位密钥分成 8 个 16 位子密钥，密钥向左环移 25 位后再分成 8 个子密钥，如此 6 次产生 48 个子密钥，然后密钥再次左环移 25 位，用前 64 位生成 4 个 16 位的子密钥共 52 个子密钥。IDEA 解密时也将密文分组输入，经如加密一样的 9 轮计算逐步恢复出明文，只是解密密钥与加密密钥不同，其间关系如下：第 i 轮解密的前 4 个子密钥是从第 $10-i$ 轮加密的前 4 个子密钥变化而来的，其中第 1、4 个解密子密钥为对应加密子密钥的模$2^{16}+1$乘法逆元；第 2－8 轮解密的第 2、3 个子密钥为相应的第 $10-i$ 轮加密第 3、2 个子密钥的模 2^{16} 加法逆元，而第 1 和第 9 轮解密中的第 2、3 个子密钥为第 $10-i$ 轮加密中第 2、3 个子密钥的模 2^{16} 加法逆元；前 8 轮中第 i 轮解密中最后两个解密子密钥为第 $9-i$ 轮加密子密钥的最后两个子密钥。

3 动态密钥交换机制

在对称加解密算法中，密码安全尤为重要，为了减少由于

混沌序列特性退化而引起根密钥失密的可能，语音通信双方随机约定加密密钥及其有效期。动态密钥的采用使得破译者很难通过较短的数据在有限时间内破译出混沌根密钥，即使得到某次根密钥，由于其有效期较短，对整个语音数据构成的威胁也不大。

根密钥更换频率是动态混沌加解密系统中重要的参数之一，根密钥更换频率过低则失去了动态密钥的意义，若在整个通信过程中使用相同的根密钥，系统则退化成一般的混沌加解密系统。根密钥更换频率过高不仅会占用更多的通信带宽，同时也会增加收发端由根密钥生成加解密密钥的计算代价。一般正常交谈中每个音节约占时 0.3～0.8 秒，且音节之间存在明显间隔，语音经数字化后存在大量 0 和近 0 数据。综合考虑，一般设定根密钥有效期为 1～10 秒间的随机数，当然也可以根据语音数据的重要程度缩短每次密钥的有效期。动态密钥交换机制十分重要，本文构建了如下密钥交换机制，如图 3 所示。

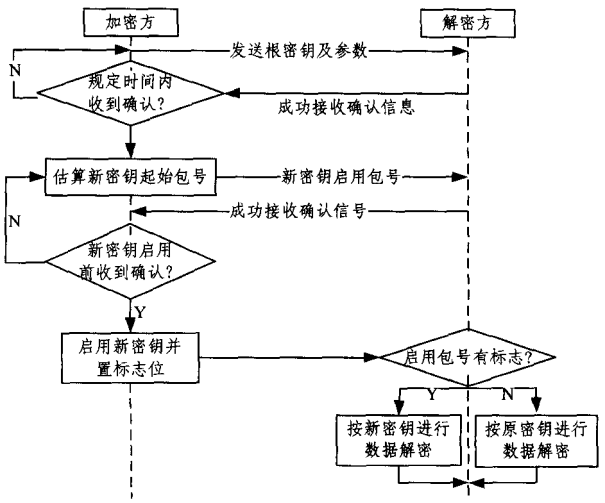


图 3　动态密钥交换机制

密钥更改时，加密方首先向解密方发送新的根密钥及相关参数，解密方收到根密钥和相关参数后向加密方发回确认信号；若加密方未在规定时间内收到解密方发回的确认信号，则说明可能由于通信等原因，解密方未接收到根密钥及参数，加密方需择机重新发送。若加密方在规定时间内接收到解密方的确认信号，则根据发送根密钥和接收确认信号之间的时间及预设规则估算出该根密钥的启用数据包号，并将该包号发送给解密方，解密方收到密钥启用包号后向加密方发回确认信号，加密方若在产生预定启用数据包前没有收到解密方发回的收到启用包号确认信号，则需重新估算启用包号并发送给解密方；若在产生预定启用数据包前收到确认信号则从启用包号开始启用新密钥，并从启用包号开始在密钥更换标志位上标记。接收方收到新密钥启用的数据包后根据密钥更换标志位判断是否启用了新密钥，如果启用了新密钥则根据新密钥进行解密，本次密钥更换成功；否则仍按旧的密钥进行解密且意味着本次密钥更换失败。

4　实验测试及分析

为验证所提方法的可行性，本文从混沌密钥产生及其特性、动态密钥交换机制及加解密对 QoS 等方面对本文所述方法进行测试和分析。

由混沌密钥产生方案可知所需的基本参数为 $(N_H, x_0, y_0, M_1, M_2, N_L, r)$，其中 N_H、N_L 分别为文中所采用的 Henon 和改进的 Logistic 映射的迭代次数。为简化，令 $N_H = N_L > 1500$，x_0、y_0 分别为 Henon 映射序列的两个初值，一般取大于 0 小于 1 的实数，M_1、M_2 分别为 Henon 序列中与最后一个元素相乘得到 MK_1，MK_2 的元素的序列号，一般为小于 N_H 但接近于 N_H 的两个不等整数，r 为 $[0, 1.2849) \cup (3.4776, 4]$ 中的实数，改进后 Logistic 映射的两个初始值 x_0，x_1 分别为 MK_1，MK_2 的小数部分。

为检验所生成的混沌密钥的随机性，首先随机生成 100 个 128 位混沌密钥，统计每个序列中‘1’出现的次数，如图 4 所示，经计算可知所产生的序列中‘1’出现频率约为 0.5012，满足伪随机序列的要求。另外根据本文给出的混沌密钥产生方法重复随机生成一个长度为 128Mb 的 0、1 序列，根据美国国家标准技术研究所(NIST)序列随机性检测标准，从单比特频度、累积和、游程、离散傅立叶变化以及近似熵 5 个方面对分别计算 p 值，根据 NIST 测试准则，当 $p \geqslant 0.01$ 时可以认为序列通过随机性测试。表 1 为用本文混沌密钥产生方法产生的混沌序列与由式(1)生成的 Henon 映射序列，以及由式(3)生成的 Logistic 映射序列的测试结果。测试结果表明，本文产生混沌密钥的方法所生成的密钥不仅具有良好的随机性，同时还能有效避免出现大量 0 位而降低 IDEA 算法安全性的可能。

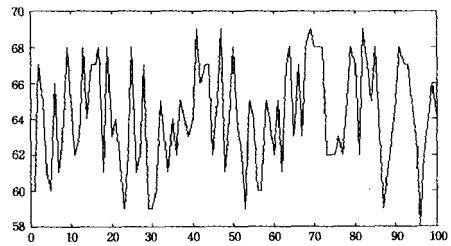
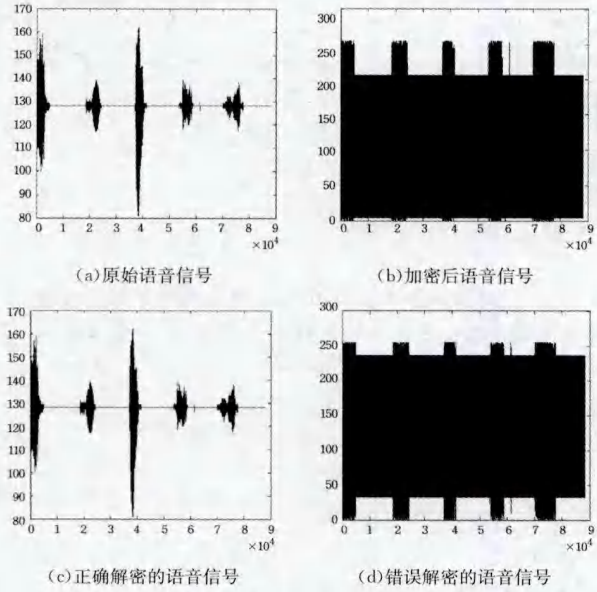


图 4　100 个 128 位序列中 1 的个数

表 1　不同混淆序列 p 值计算结果

	Henon 映射序列	基本 Logistic 映射序列	本文方法的序列
单比特频度	0.350589	0.432546	0.635781
前向累积和	0.201423	0.168723	0.258946
后向累积和	0.012658	0.021864	0.548268
游程	0.002014	0.525485	0.952438
离散傅立叶变化	0.198543	0.358942	0.458231
近似熵	0.017452	0.015637	0.369715

为验证语音加密的有效性，对采集频率为 22050Hz，量化位长为 16 位，时长为 5 秒的单声道语音数据进行加解密测试；图 5(b)为对图 5(a)语音数据进行 IDEA 加密以后的结果，实验中令 $N_H = N_L = 2000$，$x_0 = y_0 = 0$，$M_1 = 1800$，$M_2 = 1900$，$r = 0.01$；图 5(c)为对图 5(b)数据使用正确解密密钥的解密结果，经检测，解密出的结果与原明文完全相同；图 5(d)为对图 5(b)数据使用不正确解密密钥的解密结果，所用混沌密钥基本参数中令 $r = 0.001$，其他参数与加密混沌密钥参数完全相同，但解密结果与明文完全不同。实验结果表明本文所述的 VoIP 语音数据加解密方法对混沌密钥敏感，即使混沌根密钥稍微变化也无法得到正确的解密结果。除 r 变化有上述现象，实验证实 $(N_H, x_0, y_0, M_1, M_2, N_L, r)$ 中任一元素发生变化，都无法得到正确的解密结果。



(a)原始语音信号　(b)加密后语音信号

(c)正确解密的语音信号　(d)错误解密的语音信号

图5　语音数据加解密结果

为了验证动态混沌加解密的有效性，分别录制了10段时长为300秒的单声道语音数据，采集频率为22050Hz，量化位长为16位，对上述语音数据进行动态加解密效果测试，根密钥有效期为1～10中随机整数秒，解密时分别随机设置5%，10%，20%，30%，40%和50%的根密钥失密，并将解密后的语音数据播放给事先不知道明文的人听。测试结果显示，当根密钥失密率小于10%时无法得到原语音数据表达的内容，当根密钥失密率超过40%时可大致还原出原语音数据表达的内容。另外，虽然IDEA属于对称加密，由于使用动态密钥，相同的明文也有可能由于加密密钥不同而使得加密密文不同，这进一步增加了破解的难度。

本文动态密钥交换机制中动态交换的是根密钥，加解密双方根据根密钥分别生成加密密钥和解密密钥。由图3所示的动态密钥交换机制可知，在一次根密钥的交换中需要传递6个根密钥参数和1个新密钥有效起始包号，若每个参数都采用2个字节表示，供需传递14个字节，考虑到冗余，在22050Hz采样频率和16位量化长度情况下，即使每秒更改一次根密钥，根密钥交换所需的数据量仍不足数据总量的千分之一，若密钥有效期长于1秒，则所占比重更小。

对于加解密密钥计算和加解密过程的计算代价，本文以DSP5509A为核心完成语音数据的加解密，语音通过麦克风经TLV320AIC23转换由McBsp进入DSP5509A，DSP5509A对语音数据进行动态混沌加密并将其发出，接收端收到语音数据密文和混沌根密钥，先根据混沌根密钥计算出IDEA解密密钥，然后把语音密文解密成明文。测试中DSP5509A完成一次加解密密钥计算所需时间不超过2ms，完成22050个16位长语音数据的加密和解密约需10ms。若每50ms的语音数据形成一个数据包，则完成一个语音包的加解密约需1ms。每秒更换一次密钥，由数据加解密所造成的语音延时约在25ms以内，能够满足VoIP延时要求。

结束语　本文为提高VoIP的安全性，在语音通信过程中采用动态根密钥技术，通过Henon映射、改进的Logistic映射和非线性置换生成混沌加密密钥，采用IDEA算法对语音数据进行加密。接收方根据动态根密钥生成IDEA解密密钥并进行解密。

实验结果证明了动态混沌加解密方案具有较高保密性和稳定性，动态更换密钥可以加大密钥破译难度，可用于舰船间的保密通信中。当然动态密钥交换机制和密钥生成算法在通信过程中要占用一定的带宽，同时也要付出一定的计算成本，会引起网络延时与网络抖动而导致VoIP音质下降。为保证VoIP的QoS，可在语音加密前进行语音压缩技术以较少带宽获得高质量音质，也可以降低网络延时。在语音解密后采用抖动缓冲技术以提高音质和减少由于丢包带来的解密错误[16]。

参考文献

[1] Wu Shu-hua, Pu Qiong, Fei Kang. Practical authentication scheme for SIP[J]. Peer-to-Peer Netw. Appl., 2013(6): 61-74

[2] Schneier B. Applied cryptography: protocols, algorithms and source code in C[M]. New Delhi: Wiley-India, 2007: 128-131

[3] Kocarev L C. Chaos-based cryptography: a brief overview[J]. IEEE Circuits and Systems, 2001, 1(3): 6-21

[4] 朱从旭，胡玉平，孙克辉. 基于超混沌系统和密文交错扩散的图像加密新算法[J]. 电子与信息学报，2012，34(7)：1735-1743

[5] Azzaz M S, Tanougast C, Sadoudi S, et al. Robust chaotic key stream generator for real-time images encryption[J]. J Real-Time Image Proc, 2013(8): 297-306

[6] 王育民. 信息安全理论与技术的几个进展情况[J]. 中国科学基金，2003(2)：276-81

[7] Wu Xiao-gang, Hu Han-ping, Zhang Bao-liang. Parameter estimation only from the symbolic sequences generated by chaos system[J]. Chaos, Solitons and Fractals, 2004 (22): 359-366

[8] 向菲，丘水生. 基于混沌系统互扰的流密码设计[J]. 物理学报，2008，57(10)：6132-6138

[9] 尹汝明，袁坚，山秀明，等. 混沌密码系统弱密钥随机性分析[J]. 中国科学：信息科学，2011，41(7)：777-788

[10] 陈铁明，蒋融融. 混沌映射和神经网络互扰的新型复合流密码[J]. 物理学报，2013，62(4)：1-7

[11] Vlad A, Iyas A I, Luca A. Unifying running-key approach and logistic map to generate enciphering sequences[J]. Ann. Telecommun, 2013(68): 179-186

[12] 杨吉云，廖晓峰，肖迪，等. 对一种基于Logistic映射的分组加密机制的分析和改进[J]. 通信学报，2008，29(12)：86-90

[13] 万佑红，李俊刚. 一种基于Logistic的改进混沌映射及其性能分析[J]. 信息与控制，2012，41(6)：675-680

[14] Lai Xue-jia, James M. A proposal for a new block encryption standard[C]// Proceedings of Advances in Cryptology-EUROCRYPT '90. 1991: 389-404

[15] Biryukov A, Nakahara J, Preneel J B, et al. New weak-key classes of IDEA[M]// Bao F, Deng R H, Qing S. Lecture Notes in Computer Science. Springer-Verlag, 2002: 315-326

[16] Shen C, Nahum E, Schulzrinne H, et al. The Impact of TLS on SIP Server Performance: Measurement and Modeling[J]. IEEE/ACM Transactions on Networking, 2012, 20(4): 1217-1230