# 新型的适合于VoIP传输的轻量级加密算法

王 飞，辛 阳，杨义先，钮心忻

(北京邮电大学网络与交换技术国家重点实验室 北京 海淀区 100876)

【摘要】针对现有VoIP加密算法实现相对复杂、计算量大、系统性能消耗明显的情况，提出了一种适合于重视实现成本低、速度快、最小性能消耗的商业级应用轻量级VoIP加密算法。该算法本质上仍然是对称钥体系，但由动态小算法库组成，采用有记忆的改变每次加密的算法组合的原理，并在保证一定安全性的基础上解决了传统的必须要公钥密码体制传送密钥的问题，实现简单、速度快，计算量小。

**关 键 词** 语音加密； 加密算法； HW-F算法； VoIP

**中图分类号** TP309.7 **文献标识码** A

# New Light-Weighted Encryption Algorithm for VoIP

WANG Fei, XIN Yang, YANG Yi-xian, and NIU Xin-xin

(State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications Haidian Beijing 100876)

**Abstract** The popular VoIP encryption algorithms have the disadvantages of high computational complexity and huge system capability consumption. To solve this problem, this paper proposes a new VoIP encryption algorithm suitable to civilian commercial applications with low cost, high speed, and low capability consumption. This algorithm uses the combination of encryption arithmetic operations and solves the problem that the secret key must be transmitted by public key cipher system.

**Key words** audio encryption; encrypt algorithm; HW-F algorithm; VoIP

随着宽带网络的迅猛发展以及三网合一的逐渐普及，以分组交换为基础的IP通信网络正以其强大的网络通信能力、丰富的业务种类、灵活的业务扩展、低廉的价格等优势逐渐取代传统的电信运营方式。目前，无论从功能上还是价格上，人们已不仅仅满足于传统电信业务提供的语音服务，还迫切需要功能更强大、业务更繁多、价格更优惠的新业务模式。基于IP网络的语音传输(VoIP)方案的提出正好满足了这一要求[1]。

基于IP网络的语音传输[2-4]，实际就是用户通过连接在互联网上的终端(可以连接在互联网上也可以连接在固话网上)，呼叫另一用户的通信形式。

然而基于IP网络的语音传输也有诸多的缺点。众所周知，语音数据作为IP网络内的一种特殊流量，与其他类型的数据流量并无本质区别，同样会面临IP数据网络司空见惯的病毒和攻击等安全威胁。此外，语音传输所面临的特有的安全问题还有拒绝服务(DoS)攻击、通话干扰、话费欺诈或窃听等。

本文将针对以上情况提出一种适合于商业运营的轻量级的VoIP加密算法。

## 1 算法介绍

目前，有很多机构和公司在研究VoIP的保密通信方案，提出了很多非常有效的安全措施(例如SRTP协议[5]等)，并作了很多相应的研究[6-8]。这些研究成果因其高安全性而被应用在很多对安全性要求较高的场合。但是，高安全性带来的却是高额的投资、复杂的配置部署、系统性能的大幅下降，以及语音流延迟的增加等问题。这些问题对以安全保密性为第一位的政府、军事部门是可以忍受的，而对其他很多应用场合，尤其是绝大多数的商业应用场合(如IP电话、话吧、各种软电话、语音聊天软件等)却是难以接受的。商业用户都希望以更少的投资、简易的部署、更小的性能牺牲来达到他们的目的。对于商家来讲，他们并不需要非常高的保密性，他们注重的是对语音流的传输协议(如RTP或其他私有协议)

收稿日期：2007－09－21；修回日期：2008－03－14
基金项目：国家重点基础研究发展计划(2007CB311203)
作者简介：王 飞(1980－)，男，博士，主要从事信息安全方面的研究.

以及会话建立协议(SIP、H.323或其他私有协议)进行加密[9]、对VoIP数据流特征进行特征掩盖，从而防止网络黑客或恶意用户对VoIP服务的话音偷听、话音干扰、话费欺骗等，保证自己的运营质量，而不是要使用复杂的加密方案去应对某些针对敏感数据的疯狂的、不计成本的攻击。纵观目前所有的加密方案，全部都是讨论以SRTP为主导思想的、基于分组密码、密钥协商和公钥密码体制的加密方案，然而这些复杂的加密方案因为实现困难、系统消耗大、投资大等原因并不适合商业运营。通过在现网对目前国内200多种商业VoIP案例(包括PC软件、即时通信软件、话吧等常见VoIP运营形式)的分析，几乎没有运营商采用类似SRTP的思想加密其数据流。一部分运营商采用以异或为基础的简单变换对VoIP协议部分进行加密(一旦被破解就再简单更换算法)，而大部分运营商并未对VoIP协议部分进行加密，其安全性非常差。

因此，现在的VoIP运营商迫切地需要一种适合自身的轻量级的VoIP加密方法，该方法应具有以下特征：

(1) 能适应VoIP传输中丢包比较多的环境。(2) 算法尽量简单，系统消耗尽可能小。(3) 配置、部署简单，尽量减少运营成本的增加。(4) 在满足以上要求基础上的尽可能高的安全性。

## 2 新的加密算法

本文针对现有加密方法实现复杂、资源消耗大、仅适用于特定场合的弊端，提出了一种适合于实时数据传输、易实现、安全系数较大、能在非高安全度环境下使用的轻量级的加密算法，本文称它为HW-F算法。

HW-F算法的核心思想是“一次一密”[10-11]，改变了以往的加密算法以算法复杂度提供安全性和算法固定的特点。该算法以数据包为单位，加密每个数据包时算法都变化一次，以算法的不断变化提供的“一次一密”特性来代替算法的复杂度提供的安全性，这对VoIP音频数据包的传输尤其有意义。因为根据RFC1889中关于RTP协议的介绍(RTP是基于UDP或TCP的VoIP传输的基本传输协议，目前几乎所有运营商所用的VoIP传输协议都是RTP协议或它的修改)，在每个VoIP数据包中都有协议部分，包含有重要的PT、SEQ、TimeStamp以及SSRC等关键字(在标准协议中总共是12字节，各字段的详细含义请参照文献[2-4])，加密这些数据是抵御黑客插音、干扰、重放攻击等影响VoIP运营的关键所在。

HW-F算法在每个数据包中都包含了变化算法的完整参数，且这些参数没有前后关联性，因而非常适合VoIP这种丢包率较大的应用场合(目前最好的VoIP音频编码算法甚至能容忍30%的丢包率)，而在该场合中，有些序列密码是不适用的，很多序列密码需要收发双方的严格同步。

HW-F本质上也是一种数轮迭代算法，但不同的是每轮的算法都是不固定的。该算法在每轮预置的包含$n$种小算法的算法库中临时选择一种小算法，总的算法就是每轮选择的小算法之和。根据排列组合的原理，经过$m$轮之后，所有各轮算法之和即总的算法就可能有$n^m$种。配以适当的策略，可以使这种组合的数量进一步大幅增长，并且对每一个数据包的加密都能从这些算法的组合中选择一种，从而达到近似“一次一密”的能力。另外，因为每一轮算法都仅仅是一种小算法，所以可以大大提高算法的加解密速度。

HW-F算法在上述特点的基础上，不需要密钥的协商、分配和安全传送部分，大大降低了实现的难度，简化了算法的实现复杂度，节约了实现、维护的成本，可充分满足商业实现的各项要求。

需要说明的是，算法库的大小、轮数以及具体的小算法都可以由各运营商自定义。因为目前在我国的VoIP实际运营中，都是通过专门的媒体网关实现互联互通，可以不考虑运营商之间的算法兼容性问题。算法每一轮由如下元素构成：

$$\{E_j(f_{j_1}, f_{j_2}, \cdots, f_{j_n}), P_{ji}(i=1,2,\cdots,n), D_j(1 \leqslant D_j \leqslant n)\}$$

式中 $E_j$表示算法的第 $j$ 轮的算法库；算法库的大小$n$可以按照具体的算法进行取值；$P_{jd}$表示一个指针，指针指到的算法才是该轮采用的算法；$D_j$表示指针的偏移距离，在加密一条流之前，$D_j$与该轮的密钥$K_j$(1≤$j$≤$m$，$m$表示轮数)进行有限域$n$内的加运算。总的算法结构如图1所示。

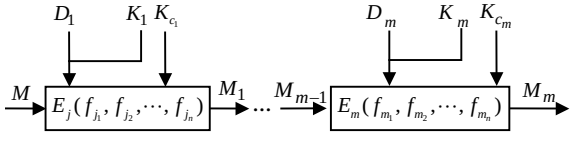


图1 算法结构示意图

图中，明文数据$M$共经历了$m$轮运算，每轮运算的计算过程为该轮的指针初始偏移距离$D_j$与该轮的密钥$K_j$在有限域$n$内相加，得出偏移距离$D'_j$，指针$P_j$根据$D'_j$指示的数值在算法库中找到算法$f_i(i=D'_i)$，然后采用该算法与明文$M$进行计算，该

轮的偏移距离$D_j$被永久地更改为$D_i'$，经过$m$轮之后，得出最后的密文$M_m$，并且所有轮的偏移距离都被更新；$K_{ci}$是一个随机数，其用途是作为次密钥，每个数据包都传递次值，每个数据包都不同。

需要指出的是，偏移距离$D$本质上就是密钥，称为密钥$D$。密钥$D$与密钥$K$相加得出某一轮要选择的算法，并用该相加值对$D$进行更新，密钥$K$在会话过程中传递而$D$不传递；密钥$D$有一个初始值，该初始值应固化在软件或硬件中，或伴随软件硬件的售出而分发，不同的客户端初始值不同，决定了对于不同的客户端，即便采用相同的密钥$K$，最终选择的算法不一样，加密结果也不一样。客户端和服务器端需要同时存储初始密钥$D$和不断被更新的密钥$D'$，一旦出现密钥$D'$不同步的情况，需要利用初始密钥$D$重置。

由上可以看出，每次用来选择算法的密钥其实是初始密钥$D$和之前所有传送过的密钥$K$在有限域$n$上的总和，因此攻击者即便截获了当前的密钥$K$，因为难以获知初始密钥$D$和之前所有传送过的密钥$K$，因而也无法解析密文，从而免去了保障密钥安全传送的考虑。

因为密钥$K$比较大，所以在每次会话中只在会话建立阶段传递一次，即在会话开始时从每个算法库中采用何种算法就已确定。为了保证在每个数据包中都采用不同的算法，还可以在每个数据包的负载中设置一个次密钥$K_c$，该密钥用来决定在已经确定的算法组合中，那一轮真正参与加密当前数据包的运算。例如在8轮的算法中，数据包包含的次密钥$K_c$如果为00101101(二进制)，则表示经过密钥$K$和$D$的选择之后，真正参与当前数据包加密的只有第3、5、6、8轮算法，从而保证了每个数据包的算法都不一致。当然，在实际应用中，轮数应该足够多，以避免选择重复的情况出现。

对算法轮数的选择要求如下：

(1) 为保证算法的随机性，轮数要足够多；

(2) 因为每8轮用一个字节表示取舍，所以轮数应是8的整数倍；

(3) 因为每个数据包都要传送属于自己的$K_c$，因此$K_c$不宜过长，以避免增加额外的带宽；

(4) $K_c$应是随机的。

最后，算法库中的算法可以是任意简单的小算法，甚至可以仅仅是与某个数异或的算法。但算法的分组长度应至少为4字节，从而能够覆盖RTP协议中4字节长度的标志位。

以下试验证明，即便是全部采用异或的小算法，算法的安全性同样很好。假设：

(1) 算法采用8轮运算，每轮算法库相同，且库中有8种算法，每种算法都与某一个数异或，算法的分组长度为4字节。

(2) 某一个数据包中4字节的明文为：

$M$=00101011 10001100 01011001 01101101

(3) 假设算法库中的共8种算法($f_1$～$f_8$表示)分别与下面的数异或(二进制)：

$f_1$=0xF00FC33C；　$f_2$=0xCC3396C3；

$f_3$=0xA66A7356；　$f_4$=0xE5762B76；

$f_5$=0xA44B07E3；　$f_6$=0xC5541766；

$f_7$=0x9456971B；　$f_8$=0x8D123717。

(4) 假设初始密钥$D$=0xA62C57；密钥$K$=0x2BD46F；数据包的次密钥$K_c$ = 76。将密钥$D$分成8个分组，每个分组3 bit，用来指示算法指针指向哪一种算法。

在本例中，根据密钥$D$每轮初始选取的算法为{$f_5, f_1, f_4, f_2, f_6, f_1, f_2, f_7$}，密钥$D$的各个分组与密钥$K$的各个分组在有限域GF($2^3$)中相加后的结果为$DK$=CDF0BE(同时$D$被永久的更改为$DK$)，从而，每轮最终选取的算法变为{$f_6, f_3, f_3, f_7, f_0, f_2, f_7, f_6$}，最后再经过密钥$K_c$的选择，最终的算法选择为{$f_3, f_3, f_7, f_2, f_7$}，因此最终的密文输出为：

$$M \wedge f_3 \wedge f_3 \wedge f_7 \wedge f_2 \wedge f_7 = \text{E7BFCFAE}$$

即便对于相同的明文、密钥$K$以及次密钥$K_c$，因为$D$值已经改变为$DK$，所以加密结果也完全不同。在上例中，每轮初始选取的算法为{$f_6, f_3, f_3, f_7, f_0, f_2, f_7, f_6$}，与密钥$K$按组在GF($2^3$)中相加后的结果为($DK$)$K$=F544E5，从而每轮最终选取的算法为{$f_7, f_5, f_2, f_4, f_2, f_3, f_4, f_5$}。经过$K_c$的选择，最终选择的算法为{$f_5, f_2, f_4, f_3, f_4$}，最终的密文为：

$$M \wedge f_5 \wedge f_2 \wedge f_4 \wedge f_3 \wedge f_4 = \text{E59EBB1B}$$

因此可以看出与上面结果完全不同。在上例中，因为每轮的算法都一样，且算法数量太少，所以最终的算法产生了相互抵消的情况，在实际操作中，应该增加每轮算法的数量、明文分组的大小和轮数。

## 3　算法性能分析

本文以采用64 bit分组、32轮的HW-F算法为例来说明其性能。假设每轮算法库中都有$2^{59}$个小算法，每个小算法都与某个数进行异或(每个数都是0～$2^{64}$数中的随机一个，且不重复，正好平均地分布在32轮算法中)。

### 3.1 算法的安全性分析

(1) 算法采用32轮，在密钥$K_c$的取舍作用下，从理论上讲，经历每$2^{32}$个包算法才能重复一次，而这么多的包需要一次通话11 930 h(G.729编码算法、1帧/包)～71 582 h (G.723.1编码算法、2帧/包) 才有可能重复，因此随机性较好。

(2) 攻击者即便知道了密钥库中的算法、密钥$K$和密钥$K_c$，因为不知道保密的密钥$D$和之前的所有密钥，因此仍然不能对明文进行解密。

(3) 因为实际使用的密钥是密钥$K$和密钥$D$的和，而密钥$D$是初始密钥和之前所有会话密钥的总和，因此仅截获当前的密钥并不能对数据进行解密，所以无需考虑密钥安全传送问题，算法安全性大大增加。

(4) 每轮$2^{59}$个小算法，一共32轮，每轮不重复，因此理论上讲64 bit的分组可以随机地与0～$2^{64}$中的任意数异或。

(5) 即便是对于同样的明文采用完全相同的密钥$K$和密钥$K_c$，算法的组合仍然不同，因此得到的密文也不相同，有利于掩盖明文的统计特性。

(6) 在RTP协议中，最长的标志字段是4字节且不变化，因此为了增加安全性，应采用64 bit以上长度的分组。

### 3.2 算法的易实现性

算法易实现体现在：

(1) HW-F中的小算法可以由用户自定义，且HW-F的结构决定了用户无须太在意算法的复杂性和数学理论，可以自由地定义简单易行的小算法(可以是异或、位移等一步完成的小算法)。

(2) 简单的小算法运算量小、速度快，相比于目前的以分组密码算法结合密钥分配或协商为基础的方法来讲，计算复杂度大幅下降，因此对它们实现加解密不必但心系统性能的下降。

(3) 因为不必担心密钥的安全传送问题，可简化系统构成，使其能够成为商业运营所能接受的VoIP加密算法。

(4) 实现加密算法，每个数据包只需增加几个字节(次密钥)，增加的字节数对带宽的额外消耗非常小。

(5) 算法的每个数据包变化一次，包与包的算法之间没有关联性，因此适用于丢包较大的VoIP的应用场合。

## 4 结 论

综合以上分析，HW-F算法是在对现网几乎所有VoIP运营模式进行分析的基础上，结合现网VoIP运营中对于算法实现成本、安全性、速度的综合要求提出的一种适合于VoIP商业运营的轻量级加密算法。该算法具有较好的安全性，实现复杂度小、成本低，系统性能消耗小、抗丢包，易于后期维护。

## 参 考 文 献

[1] 李 辉, 赵 晖. 传统PSTN与VOIP的比例研究[J]. 电子科技大学学报, 2004, 33(2): 192-195.
LI Hui，ZHAO Hui. Comparison and research of traditional PSTN and VOIP[J]. Journal of University of Electronic Science and Technology of China，2004，33(2)：192-195.

[2] SOLLAUD A. RFC 4749, RTP payload format for the G.729.1 audio codec[S]. 2006.

[3] SCHULZRINNE H, CASNER S, FREDERICK R, et al. RFC 1889, RTP: a transport protocol for real-time applications[S]. 1996.

[4] VIDAL D. Real-time technology for the internet 2000[M]. [S.l.]: Prentice Hall Inc, 1996.

[5] BAUGHER M, MCGREW D, NASLUND M, et al. RFC 3711, The secure real-time transport protocol[S]. 2004.

[6] BLOM R, CARRARA E, LINDHOLM F, et al. Conversational IP multimedia security[C]//MWCN 2002. Stockholm, Sweden: IEEE, 2002: 147-151.

[7] GUPTA P, SHMATIKOV V. Security analysis of voice-over-IP protocols[C]//CSF 2007. Italy: Venice, IEEE, 2007: 49-63.

[9] CHEN Yun, CHEN Xin. Batch private keys generation for RSA in security communication systems[J]. Journal of Electronic Science and Technology of China, 2005, 3(1): 22-26.

[9] 吴 劲, 张风荔, 何兴高. SIP安全机制研究[J]. 电子科技大学学报, 2007, 36(4): 1211-1214.
WU Jin, ZHANG Feng-li, HE Xing-gao, et al. Research of SIP security mechanism[J]. Journal of University of Electronic Science and Technology of China, 2007, 36(4): 1211-1214.

[10] 王育民, 刘建伟. 通信网的安全——理论与技术[M]. 西安: 西安电子科技大学出版社, 1999: 126-296.
WANG Yu-min, LIU Jian-wei. Security of communication network-theory and technic[M]. Xi'an: Xidian University Press, 1999.

[11] 陈鲁生, 沈世镒. 现代密码学[M]. 北京: 科学出版社, 2002: 1-168.
CHEN Lu-sheng, SHEN Shi-yi. Modern cryptogram[M]. Beijing: Science Press, 2002.

编 辑 熊思亮