蓝牙E0加密算法安全分析

郭 锋，庄奕琪

(西安电子科技大学微电子所 西安 710071)

【摘要】蓝牙的E0加密算法是利用四个移位序列进行延迟并组合生成密流序列。利用其密流序列的相关性对算法进行攻击。攻击过程是基于给定有限的输出加密流，重新导出移位序列的初始值。基本攻击和优化攻击的时间复杂度分别为$O(2^{83})$和$O(2^{78})$。最后给出了该攻击手段的E0算法的改进方案和实验数据。

关 键 词 蓝牙； 流加密； E0算法； 安全性； 攻击

中图分类号 TN92 文献标识码 A

Analysis of the E0 Encryption System in Bluetooth

GUO Feng，ZHUANG Yi-qi

(Institute of Microelectronics, Xidian University Xi'an 710071)

Abstract The encryption system E0 in Bluetooth is generated from four LFSRs (Linear Feedback Shift Registers) by delay and combination. A new algorithm is introduced to attack E0 by using the correlation of its sequence. The average time complexities of the basic and the advance attacks respectively are $O(2^{83})$ and $O(2^{78})$. Base on the way of attacking means described in the paper, an improvement on E0 is made. In the end, some theory analysis and sample data are provided.

Key words bluetooth; encryption; E0; security; attack

关于蓝牙，最能引起众人的关注和争论的莫过于它的安全机制了。不少人认为蓝牙的安全体系是产生问题的重灾区，会被任何稍有能力的投机者攻破。相反，另一些人则认为蓝牙的安全性已经足够好了。这其实取决于你想用蓝牙来做什么。对于普通用户而言，大部分信息都不值得花比信息本身更高的代价去破解。但如果要将蓝牙用于商业、金融业、军事业等来传输极具价值的信息，那么就有必要了解蓝牙的安全能力。本文将具体分析蓝牙链路层所采用的加密算法 E0 的安全性能并给出算法的改进方案和实验数据。

1 E0算法的基本内容

E0 算法是蓝牙链路层的加密算法，属于流加密方式，即将数据流与密钥比特流进行异或运算。对每一分组的有效载荷的加密是单独进行的，它发生在循环冗余校验之后，前向纠错编码之前。主要原理是利用线性反馈移位寄存器产生伪随机序列，从而形成可用于加密的密钥流，然后将密钥流与要加密的数据流进行异或，实现加密。解密时把密文与同样的密钥流再异或一次就可得到明文。

关于 E0 算法如图 1 所示。E0 算法主要有：线性反馈移位寄存器组(Linear Feedback Shift Register，LFSR)，(LFSR1～4)、组合逻辑和复合器(Blend)3 部分组成，其中 Blend 中 T_1 和 T_2 为线性变换网络，Z^{-1} 为延迟网络。LFSR*s* 的长度分别为 25、31、33、39。采用多个 LFSR 是为了增加生成的伪随机序列的长度和随机性。当产生加密流时，LFSR*s* 需要赋予初值(种子)。四个 LFSR 再加上各是两位的 C_t 和 C_{t+1} 共计 132 位，由主设备地址 ADR(48 位)、时钟 CL(26 位)和链路层加密私钥 K_c (最多 128 位)提供，K_c 由 E3 算法产生的。种子进入 LFSR*s* 的安排由图 2 给出，图中的 K_c' 是由 K_c 变换得来。当 LFSR*s* 开始进行工作时，先产生的 200 位数据的后 128 位再次作为 LFSR*s* 的种子，而 C_t 和 C_{t+1} 的值被保留，这时产生的伪随机序列就是加密所用的密钥比特流。之所以采用这样的两级加密是为了增加安全性，即使破解出第二级加密，也还必须破解第一级加

收稿日期：2003－09－23

作者简介：郭 锋(1973－)，男，博士生，讲师，主要从事IC设计、系统方案设计、嵌入式开发等方面的研究.

密才能知道加密私钥 K_c。

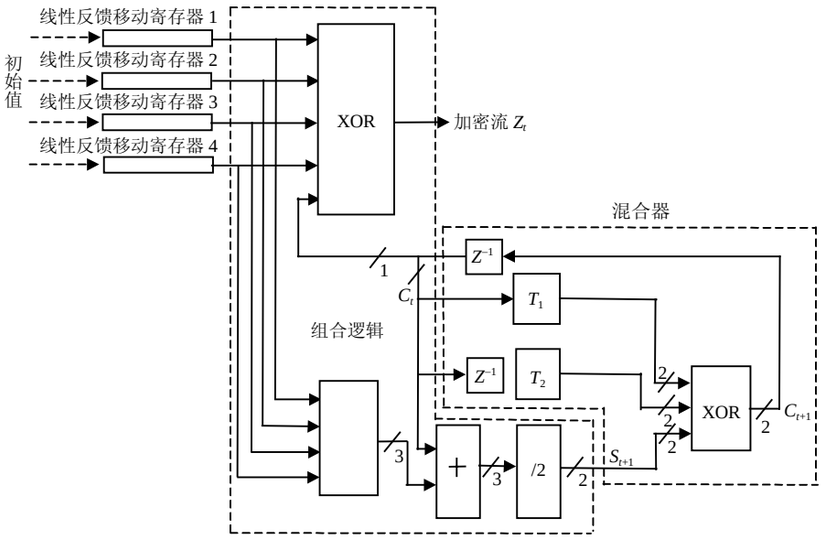

图 1　用于加密的 E0 算法的实现框图

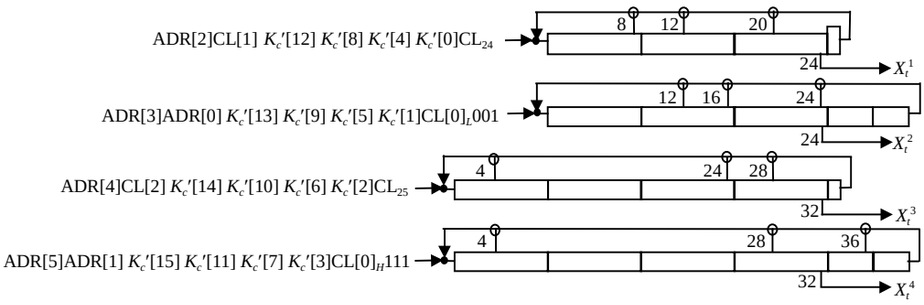

图 2　输入参数进入 LFSRs 的安排

2　对E0加密流产生器的基本攻击

这种攻击是基于给定有限的(132位左右)输出加密流，重新导出LFSRs的初始值。输出的加密流可以通过某种方式获得的明文和密文按位异或得到。这种攻击对两级加密流的产生器都是有效的。攻击时，假定已知Blend、LFSR1和LFSR2内容的初始设置，当已知输出的加密流时，虽不能输出LFSR3和LFSR4的确切值，但也能推导出LFSR3和LFSR4的异或值。由图1中得知在t时刻输出密流Z_t为LFSRs的输出(即 $x_t^1 \sim x_t^4$)与 C_t^0 (C_t的低位)的异或结果。x_t^3 和 x_t^4 的异或值也可视作 x_t^3 和 x_t^4 的约束条件，把多位加密流得到的约束条件形成约束集，称为L。首先，把L初始化为空。然后进行如下第一搜索，攻击算法的基本步骤为：

(1) 设当前所测状态为t(开始时t=0)。计算 x_t^1、 x_t^1、 C_t^0 和Z_t的异或值，输出应和 x_t^3 与 x_t^4 的异或值一致。

(2) 如果异或值为零，那么在L中加入约束条件 x_t^3 和 x_t^4 都为0或都为1。

(3) 如果异或值为1，那么在L中加入约束条件 $x_t^3 \neq x_t^4$。

(4) 如果t≥33，那么在L中的约束条件含有LFSR3的反馈链。如果t≥39，在L中的约束条件含有LFSR4的反馈链。在这两种情况下，如果新加入的约束条件与L中已有的约束相矛盾，这说明事先所做的关于Blend、LFSR1和LFSR2的假设不对，此时必须考虑假设其他情况。

(5) 如果约束条件不矛盾，则计算Blend的次态。次态取决于现态和LFSRs输出1的个数。

(6) 如果把t≥132，那么有很高的概率可以发现密流产生器的初始设置。如果不能，则继续搜索状态t+1。

该算法中有两点值得注意：先是Blend的次态取决于现态和LFSRs输出1的个数。因此，本文可以假定LFSR3和LFSR4不同而不需要知道哪个是0哪个是1，只要知道它们不同即可继续搜索。其次在约束条件集合

L中的约束可以被有效的检测是否矛盾。

下面分析这种攻击手段的有效性。首先，考虑假设LFSR1、LFSR2的内容和Blend的状态都是正确。在任意t时刻，x_t^3 和 x_t^4 的和(称为S)有两种情况：(1) 当 x_t^3 和 x_t^4 的异或值为1，S=1。Blend的次态C_{t+1}就已经决定了，因为次态只取决于现态和LFSRs输出1的个数。此时可直接进行Z_{t+1}的分析。(2) 当 x_t^3 和 x_t^4 的异或值为0时，$S\in\{0，2\}$。Blend的次态C_{t+1}要分别考虑S=0和S=2两种情况，此时需要分支考虑Z_{t+1}。如果把对Z_t的分析看作结构树的根节点，以后的Z的位的分析，则可看作对结构树的分支。这个结构树的深度为33+39=72(即LFSR3和LFSR4的长度和)。由于对Z的每位，有一半的概率要分支，平均来看，对Z的每位平均分支0.5次，同时平均得到1.5个约束条件(无分支时有一个，分支时有两个)，所以结构树的分支数为$2^{72/3}=2^{24}$枝，这数值也就是进行搜索的工作量。而最初假设的位数为60位(LFSR1和LFSR2共56位，Blend的现态和次态共4位)，要得到正确的假定平均需要试2^{59}次，因此总的时间复杂度平均为$O(2^{59+24})=O(2^{83})$。这是基本的攻击方法，还可以利用一些特殊条件对攻击进行进一步的优化。

3 对E0密流生成器的优化攻击

为了优化攻击第二层密流生成器，如果LFSR3和LFSR4的异或输出有很高的汉明码重，那么攻击会更有效。为了利用这一点，本文通过假设扩展攻击，假设在一个密流的特殊点，LFSR3和LFSR4的异或为N个连续的1(N<33+39)。由于LFSR的输出在这个长度上随机且相互独立，在N+k个输出长度上产生这样一个序列的可能性为$k\cdot 2^{-N}$(因为k<<2^N)。如果有的话，整个工作量将小于$O(N\cdot 2^{(72-N)/3})$，同时明文的需要量不小于2^N+132–N。因为当LFSR3和LFSR4的异或值为1时是不需要对结构树进行分支的。部分理论值由表1给出，同时给出了全部搜索所需要的次数。

表1 不同的N时，明文需求量与搜索时间的关系

N	基本搜索次数	平均明文需求量/bit	平均搜索次数
5	$2^{24.7}$	159	$2^{83.7}$
10	$2^{23.9}$	1 146	$2^{82.9}$
15	$2^{22.9}$	33×2^{10}	$2^{81.9}$
20	$2^{21.7}$	1×2^{20}	$2^{80.7}$
25	$2^{20.3}$	32×10^{20}	$2^{79.3}$
30	$2^{19.0}$	1×10^{30}	$2^{78.0}$

形式上，算法如下：

(1) 在已知密流中选择132个连续的已知位；

(2) 循环4位的Blender FSM、25位的LFSR1和最后的30–n位的LFSR2的状态；

(3) 计算开始的LFSR2状态的n+1位，使得LFSR3和LFSR4的异或输出为n个1；

(4) 在这一设置上运行基本攻击，如果发现恒定的初始值则停止。

以上算法将运行2^{59-n}次基本攻击，对一个单个的位置成功的可能性为2^{-n}。应当注意，即使是一个单个的数据包，其净荷长度最大为2 745位，如果可以得到多个包的明文，就可以得到超过2 745位的密流。所有需要的下一步攻击是如何知道对任何一个包(Packet)来说，第二层密流产生器的初始设置。如果可能得到多个包，逐个去试它们，就能成功地找到任何一个包的初始设置。

4 对蓝牙E0算法的改进

根据以上的分析以及可能存在的攻击可以看出，E0算法的主要弱点在于图1中的y_t信号是由LFSRs的输出位 x_t^1、x_t^2、x_t^3、x_t^4 简单的求和而得，当得知任何它们的异或结果很容易推出复合器的次态，以上的攻击手段都是在利用这一点进行的。因此可以针对这一点进行如下的改进，如图3所示，把简单的求和变成如图所示的算法。改进后的算法先对输出位 x_t^1、x_t^2、x_t^3、x_t^4 计数再求和，这时用以上所述的攻击手段不能奏效，因为求和的结果y_t不仅与输出位 x_t^1、x_t^2、x_t^3、x_t^4 的现态，也与它们的前态有关。改进后的算法具有以下优

点：

(1) 生成的加密流理论上更随机，原序列的长度最长为$2^{132}-1$，现在为最长可达$2^{144}-1$。表2中所示的即改进前后数据的对比情况。(2) 无法进行以上所述的攻击手段，如果采用穷举法进行攻击，工作量比以前要大2^{12}倍，因为系统比以前多了12个状态。(3) 对原算法只做了很少的改动。一般为了速度等原因，算法主要部分都采用硬件实现，改进后的算法不需要改动算法软件部分的内容。(4) 改动的部分和原部分很容易进行某种使能方式切换，这样可以和原算法兼容。

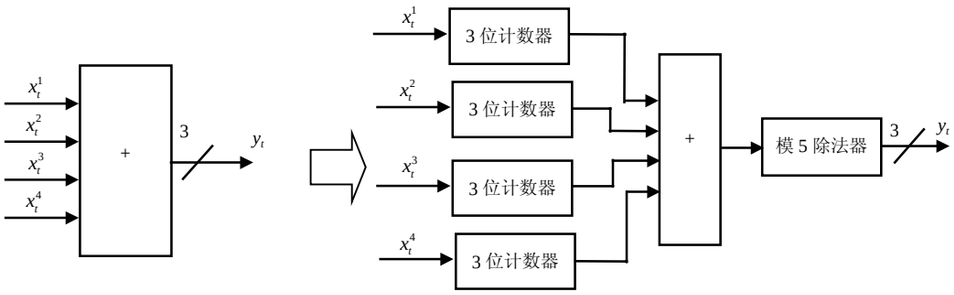

图3　对蓝牙E0算法的改进图

表2　E0算法改进前与改进后生成的加密密流数据对比

加密初始设置		生成的加密密钥流(前120位)
K_c={0x00000000000000000000000000000000}	改进前	0x46694e6193345c87711894921bb78d…
Addr={0x000000000000} Clk={0x0000000}	改进后	0x4829ee883aefbde16dcc2a02b452e3…
K_c ={0x00000000000000000000000000000000}	改进前	0x8cc31b3905d62a4c368d5ad24a4336…
Addr={0x000000000000} Clk={0x3000000}	改进后	0xa049df7c3e154e29e447d6644e08df…
K_c ={0xffffffffffffffffffffffffffffffff}	改进前	0x8bfffda98dd6f979c2bc6558531784…
Addr={0xffffffffffff} Clk={0x3ffffff}	改进后	0xe485a3c6f5183d0d3ad2d4e5c5d53a…
K_c ={0x2187f04aba9031d0780d4c53e0153a63}	改进前	0x2999f607fde02ea4cc9c1b8503a594…
Addr={0x2c7f94560f1b} Clk={0x15f1a00}	改进后	0x651502be60ce31fbac4f5251b369bd…

5　结 束 语

E0算法是蓝牙链路层加密所采用的密流算法，它的安全性直接影响到整个系统的安全性。根据本文的分析，依据所获得的密文的长度，E0算法的安全性在78~84位之间。如果不做改进，它的安全性能只能维持到2005年左右。在不改变基带的情况下，如果要提高蓝牙的安全性，只能采用公钥密码体制进行应用层的加强，例如椭圆曲线等算法。

参 考 文 献

[1] Bluetooth SIG. Specification of the bluetooth system V1.1[S], 2001.

[2] Schneier B. 应用密码学——协议、算法与C源程序[M]2版. 北京: 机械工业出版社, 2000.

[3] Jakobsson M, Wetzel S. Security weaknesses in bluetooth[A]. Proceedings of the Cryptographer's Track at the RSA Conference (CT-RSA 2001)[C]// Berlin: Springer, 2001, 176-191.

[4] Lamm G, Falauto G. Bluetooth wireless networks security features[J]. IEEE Transactions on Communications 2001, 48(4): 265-272.

[5] Marjaana Träskbäck. Security of bluetooth: An overview of bluetooth security[EB/OL]. http://whitepapers.zdnet.com/, 2001-5-10.

[6] 金　纯, 许光辰, 孙　睿. 蓝牙技术[M]. 北京: 电子工业出版社, 2001.

编　辑　刘文珍