第33卷 第12期 计 算 机 工 程 2007年6月
Vol.33 No.12 Computer Engineering June 2007
·安全技术· 文章编号：1000—3428(2007)12—0134—03 文献标识码：A 中图分类号：TP393.08

基于PDA的高效真随机密钥生成系统

肖攸安，周祖德
（武汉理工大学信息工程学院，武汉 430070）

摘 要：为满足基于 PDA 的移动电子商务等应用的需求，针对现有高质量密钥生成方法的速度慢、效率低的问题，提出了一种高效随机密钥生成方法，设计了一个基于 PDA 的高效密钥生成系统。按照 FIPS 140-2 标准中的规定对由该系统产生的随机密钥的质量进行了测试和分析。说明该系统能快速产生具有高质量的、满足信息安全系统标准的高强度安全密钥，特别适用于基于 PDA 的移动电子商务、电子政务等环境，具有很好的实用价值。

关键词：定点设备；密钥；信号源；真随机密钥

Efficient Truly Random Key Generating System Based on PDA

XIAO Youan, ZHOU Zude
(School of Information Engineering, Wuhan University of Technology, Wuhan 430070)

【Abstract】 To solve the problem the known high quality key generate scheme is slow and inefficient, this paper builds an embedded truly random key generating system on the PDA devices based on a new method which is called as Xiao's random key generating scheme. It analyzes the performance, efficiency, security about the proposed schemes and tests the generated sequence according to the standard of FIPS 140-2. The new system can get a batch of high-quality key meeting the requirements for information security system. It is quick, secure and efficient.

【Key words】 Point devices; Key; Signal source; Truly random key

随着嵌入式技术的高速发展，作为嵌入式系统的典型应用之一的 PDA(personal digital assistant)得到了迅速的普及，已经成为实现移动计算、移动电子商务、无线电子政务等的重要组成部分。由于无线网络的开放性，在使用 PDA 进行移动电子商务等活动中，信息安全问题将成为关键要素。

由于密钥是访问信息系统的唯一合法凭证[1]，因此安全的密钥对于信息安全系统，特别是基于PDA的移动电子商务系统等应用系统而言是十分关键的。它不仅影响系统的安全性，而且还将涉及系统的可靠性、有效性和经济性等内容。

本文分析了 PDA 环境下对密钥生成系统的需求和现有的各种密钥生成系统及其所使用的方法，在此基础上提出并设计了一种基于 PDA 的高效真随机密钥生成系统，并进行了分析。

1 基于 PDA 移动应用环境的密钥生成

由Shannon定理可知，安全的密钥要求具有足够的大小和尽可能高的熵值[1]。在PDA移动应用环境中，为了保证系统的安全，要求所选择的密钥具有足够的长度、高度的随机性、独立性和不可预测性。

随着现代通信网络和嵌入式移动计算技术的高速发展，人们对大批量的安全密钥的需求量越来越大。为了满足这一需求，目前出现了多种密钥生成器。按其产生密钥的工作原理，可分成以下 3 类：

(1)基于纯计算机算法的密钥生成器

这类密钥生成器基于某一事先确定的伪随机数生成算法或随机数表，依赖某一随机数种子来产生密钥，是最常用的密钥产生方法。由于计算机算法的固有特征(即对于给定的输入，有确定的输出)，任何企图通过纯算法来获得真正的随机数是不可能的，所生成的密钥难逃被预测的危险，因此这类密钥产生器被称为“伪随机密钥产生器”，它只能用在对安全性要求不高的场合，不能完全满足移动电子商务环境中的安全需求。如 1999 年发现的针对电子支付协议SSL的攻击[3]就是从SSL临时会话密钥的产生算法中，确定所有可能的种子集合，分析出由其产生的所有可能密钥的组合，进而从中找出真正的密钥，达到突破电子商务支付协议的目的。

(2)基于人工方法的密钥生成

这类密钥生成器通过掷硬币、扔骰子等随机方式获得密钥，是目前被公认的最安全的密钥产生方法之一。由这类方法产生的密钥具有较高的熵值和高度的随机性，但这类生成器的使用非常繁琐，不能适应现代社会对密钥产生量的需求，除了极少数非常重要的场合，一般不用这种方法。

(3)基于随机噪声发生检测方法的密钥生成器

这类密钥生成器通过产生和测量自然界中具有高度随机性的噪声信号，以获得具有较高熵值和均匀外部特征的高质量真随机密钥。目前这类装置大多通过产生和检测放射性衰变、微弱放射线、粒子轨迹、半导体热噪声、石英振荡器等真随机噪声信号源[6]来获得较为理想的真随机密钥，需要极其昂贵的随机噪声振荡器、随机信号发生器等硬件设备。由于这些装置结构复杂、操作繁琐、价格昂贵、携带不便，产生密钥的速度较慢，而且装置本身有一定的危险性，因此这类密钥生成装置无法使用于移动电子商务环境。

综上所述，现有的 3 类密钥生成器存在着安全性不够、

基金项目：国家自然科学基金资助重大项目(50335020)；武汉市青年科技晨光计划基金资助项目(20055003059-5)
作者简介：肖攸安(1973－)，男，博士后、副教授，主研方向：网络信息安全；周祖德，教授、博导
收稿日期：2006-07-17 **E-mail：**youan@mail.whut.edu.cn

不方便、实用性不高等问题。所有这些问题导致高随机性的安全密钥的产生效率极低，密钥的管理难度加大，密钥的更换频率降低，为基于 PDA 的移动电子信息系统的安全带来了巨大的隐患。

本文针对这一问题，在分析现有的各种密钥产生方法的基础上，设计并实现了一个基于PDA的高效真随机密钥生成系统 EXRKGS(embedded Xiao's random key generate system)[7]，并已获得计算机软件著作权登记(登记号：2006SR01852)。

2 基于 PDA 环境的随机密钥的产生方法

生成高质量随机密钥生成的关键在于高速随机信号源的获取。在计算机中可以利用的真随机信号源有[9]：半导体二极管和电阻器的热噪声，CPU和风扇电压，麦克风噪声，键盘击键次数，I/O缓冲区内容的变化，网络数据包和事件的发生情况，多任务操作系统环境中进程和线程调度时刻的不确定性等。

在上述各种信号源中，热噪声和电压等信号的获取需要专门的硬件芯片支持，麦克风噪声、网络数据包、键盘击键、进程调度等信号源的产生速度较慢，不具备普遍性，均不适合 PDA 环境下的快速高质量随机密钥生成，而屏幕和触笔不仅是每台 PDA 的标准设备，且是使用频率最高的设备。故基于 PDA 触笔随机指点情况的信号源具有较好的通用性，能够较快地获取大量的随机信号源数据。

本文提出以 PDA 触笔随机指点情况作为真随机信号源，通过实时跟踪测量 PDA 触笔随机在 PDA 屏幕上的随机指点时所产生的方位、速度等各种随机参量，获得安全可靠的真随机密钥。

2.1 随机信号源的收集

在PDA的使用过程中，因为任何人在不同的时刻，都不能以同样的方位和速度来操作PDA触笔，所以操作PDA触笔指点屏幕时所产生的方位、速度等各种参量具有不确定性，是不可重复的随机信号。转币模型指出[1]，用一个低频信号f_1去采样一个高频信号f_2(其中$f_2 >> f_1$)，由于两次采样之间经历了很多高频信号周期，在这段时间内，系统的微小变动会导致输出有很大的离散性，因此在统计上符合随机的概念。依据这一思想，本文提出跟踪PDA触笔在用户高速随机指点PDA屏幕时的指点情况，用低频的计算机系统时钟对其进行离散采样，获取方位、速度参量的离散变化情况，作为随机信号源。将其加入“源数据池”(data pool)中，以备后继处理。具体方法如下：

(1)方位参量的获取

设上一次采样时，PDA触笔的触点坐标为(x_1, y_1)；而本次采样时刻，PDA触笔的触点坐标为(x_2, y_2)。则依据两次采样所得到的触点坐标之间的关系及式(1)确定PDA触笔当前的移动方位。

$$Direction = \frac{y_2 - y_1}{x_2 - x_1} \tag{1}$$

由此，得到如算法 1 所示的方位参量获取算法。

算法 1 方位参量的获取算法

```
VAR
  OldPoint, APoint: lpPoint;
  XX, YY: Integer;
BEGIN
  GetCursorPos(APoint);
  XX:= APoint.X - OldPoint.X;
  YY:= APoint.Y - OldPoint.Y;
  if (XX = 0) or (YY = 0) then Exit;
  Direction:= YY / XX;
  GetCursorPos(OldPoint);
END;
```

(2)速度参量的获取

同样，设上一次采样时刻为t_1，PDA触笔的触点坐标为(x_1, y_1)；而本次采样为t_2，PDA触笔的触点坐标为(x_2, y_2)。则可依据两次采样所得到的触点坐标和两次采样的时间间隔之间的关系，依据式(2)，确定PDA触笔当前的移动速度。

$$Velocity = \left(\frac{x_2 - x_1}{t_2 - t_1}\right)^2 + \left(\frac{y_2 - y_1}{t_2 - t_1}\right)^2 \tag{2}$$

由此，可得到如算法 2 所示的速度参量获取算法。

算法 2 速度参量的获取算法

```
VAR
  OldPoint, APoint: lpPoint;
  LastTime, XX, YY, TT: Integer;
BEGIN
  GetCursorPos(APoint);
  XX:= APoint.X - OldPoint.X;
  YY:= APoint.Y - OldPoint.Y;
  TT:= GetTickCount - LastTime;
  if (XX = 0) or (YY = 0) or (TT = 0) then Exit;
  Velocity:= (XX * XX + YY * YY) / (TT*TT);
  GetCursorPos(OldPoint);
  LastTime:= GetTickCount;
END;
```

2.2 随机密钥的生成

为了进一步加快随机密钥的输出速度，提高随机密钥的质量，当“源数据池”中的随机源数据达到一定数量时，可选用合适的编码算法对池中的随机信号数据进行组合编码。为了获得具有较高熵值和高度随机性、能满足信息系统安全需求的高强度安全密钥，组合编码函数应该能够输出足够长度的满足安全系统需求的编码结果，可供选择的组合编码算法有 CRC 算法、Hash 函数等。

为了满足输出密钥长度的要求，需要多次重复上述的随机信号源的收集和随机密钥的生成过程，直到所获得的密钥总长度满足系统的需求为止。

3 系统的设计与实现

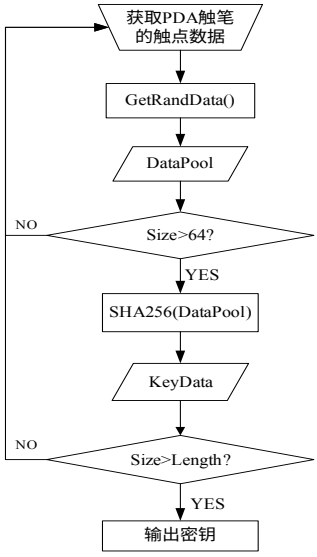

图 1 EXRKGS 随机密钥生成系统流程

基于上述方法，开发了一个基于PDA的高效真随机密钥生成系统EXRKGS，其系统流程如图 1 所示。

其中选用美国国家技术标准局NIST公布的强碰撞自由的安全散列标准算法SHA-256[10]作为组合编码算法。依据苏桂平等人的研究成果[11]，系统设定“ 源数据池 ”中所收集到的随机信号源数据长度超过 64bits时，就使用SHA-256 算法进行组合编码，获得 256bits长度的随机密钥。

EXRKGS系统使用Microsoft Visual Studio .Net 2003 进行开发，系统的运行界面如图 2 所示。通过在PDA与PC机之间建立永久连接，保持其数据同步，利用Visual Studio .Net中的远程调试工具，通过设定默认移动设备，实现跟踪查看程序运行情况，实时进行程序内部的在线调试，代码优化等工作。

图 2 EXRKGS 随机密钥生成系统运行界面

在HP公司生产的内置Microsoft PocketPC 2002 操作系统的Compaq iPAQ 3970 PDA上，当设定采样间隔为 32ms时，密钥输出速率可达 20Kb/s，并能对所产生的密钥质量进行检验。

4 随机密钥的测试

密码学意义上的随机密钥的质量检测指标包括频数检测、跟随特性检测、随机性检测，分布均匀性检测和独立性检测等多种指标。其中频数指标和跟随特性指标一般采用计数统计方法进行测试，随机性指标一般使用χ^2方法进行测试，分布均匀性指标一般使用χ^2拟合优度法进行测试，而独立性指标常用游程检验法进行测试。

在所有随机密钥质量检测方法中，以美国国家技术标准局NIST于 2001 年 5 月发布的关于密码系统的信息安全标准FIPS 140-2[12]最为著名。在FIPS 140-2 中指定了 4 种测试方式对随机密钥的质量指标进行测试，以取代常规的随机性统计检验，以合格区间的形式简化了随机密钥质量的检验过程。与同类标准相比，FIPS 140-2 的合格标准更加严格。

FIPS 140-2 标准中规定从随机序列中随机选取 20 000 位连续的位序列，进行下列 4 种测试：

(1)单比特测试(the monobit test)。通过计算连续 20 000 位随机序列中“ 1 ”的个数(X)，当 9 725<X<10 275 时，则测试通过。

(2)扑克测试(the poker test)。将连续 20 000 位随机序列按 4 位 1 组分成 5 000 组，每组(4 位)有 16 种可能的取值，统计 5 000 组中每组可能的取值数字。设 $f(i)$为取值为 i 的组数字，$i \in [0, 15]$，则按下列公式计算 X，若 2.16 < X < 46.17，则通过该项测试。

$$X = \frac{16}{5000} \times \left(\sum_{i=0}^{15} [f(i)]^2 \right) - 15$$

(3)游程测试(the runs test)。一个游程定义为连续为“ 0 ”或“ 1 ”的最大位序列，其中“ 0 ”或“ 1 ”的个数称为游程的长度。统计 20 000 位的随机位序列中各种不同长度游程的数量，显然每种长度的游程有两种情况，若所有游程长度均满足表 1，则通过该项测试。

表 1 游程测试合格标准

游程长度	1	2	3	4	5	6+
区间	2343~2 657	1135~1 365	542~708	251~373	111~201	111~201

(4)长游程测试(long runs test)。游程长度大于等于 26 的游程为长游程。若没有长游程，则测试通过。该项测试等价于分别计算“ 0 ”或“ 1 ”的所有游程长度的最大值，若该值均小于 26，则通过测试。

本文采用上述的FIPS 140-2标准对由EXRKGS系统连续生成的 500 组真随机密钥进行了测试，所有测试结果全部合格，密钥输出速率为 20Kbps。部分实验数据如表 2 所示。

表 2 FIPS140-2 测试数据

测试类型	游程长度		合法范围	测试结果 1	测试结果 2	测试结果 3	测试结果 4	测试结果 5
单比特测试			9 725~10 275	9 942	9 976	10 049	9 905	10 073
扑克测试			2.16~46.17	11.859	8.774	30.729	14.906	20.883
游程测试	0	1	2 343~2 657	2 515	2 454	2 494	2 534	2 414
	1	1	2 343~2 657	2 550	2 446	2 436	2 523	2 552
	0	2	1 135~1 365	1 252	1 246	1 250	1 225	1 257
	1	2	1 135~1 365	1 246	1 224	1 294	1 312	1 223
	0	3	542~708	634	591	647	644	615
	1	3	542~708	613	654	659	627	591
	0	4	251~373	310	328	309	328	353
	1	4	251~373	325	327	286	290	317
	0	5	111~201	158	172	135	147	169
	1	5	111~201	142	141	156	150	155
	0	≥6	111~201	156	159	159	159	169
	1	≥6	111~201	148	158	163	136	139
最大游程长度	0	<26	1~25	12	14	16	12	13
	1	<26	1~25	18	16	13	13	14

5 结论

EXRKGS 系统结合了现有各种密钥产生系统的长处，避免了使用复杂的随机噪声信号发生振荡器，以及手工操作的繁琐过程，能够快速地获得具有高质量的较高熵值和高度的随机性，满足信息安全标准的高强度安全密钥。该系统操作简单、经济实用，特别适用于基于 PDA 的移动电子商务、电子政务等环境，具有很好的实用价值。

参考文献

1 冯登国, 裴定一. 密码学引论[M]. 北京: 科学出版社, 1999.

2 刘国良, 高小鹏. Freeswan IKE 伪随机数算法效率分析及改进[J]. 计算机工程, 2005, 31(16): 83-85.

3 向剑文, 余 辰, 李 锋, 等. 电子商务的安全问题[J]. 计算机应用, 2001, 21(7): 1-4.

4 Mita M, Toshiyoshi H, Ataka M, et al. Micro Dice——An IEEE International Conference on Micro Electro Mechanical Systems. 2005-02-01: 335-338.

(下转第 147 页)