# Android智能手机锁屏方式及其破解

Android手机提供了几种加密方式用于锁定屏幕，分别是手势密码，PIN码密码以及复杂密码，其中最为常见的称之为手势密码。此外还有些高端型号的Android手机还提供了面部识别密码和任意图形密码，但这些密码在解密失败时都可以通过PIN码来解锁。

1. Android智能手机锁屏方式

1.1Android系统手机的手势密码

手势密码即3×3的点阵组成的图形密码（图1）。手势密码要求至少由连续的4个点组成，最多9个点。实际上这9个点是从0到8组成的9个数字，如图1中的密码即为13487。Android手势密码是将这些组成密码的数字先转换为十六进制，然后对其做SHA-1的哈希计算，最终将SHA-1的哈希值储存在手机中，存储路径通常是：data\system\gesture.key。通过计算，4~9位的手势密码一共有985 824种组合[2]。 目前对应这些密码的彩虹表已经集成在大多数的手机取证工具中。

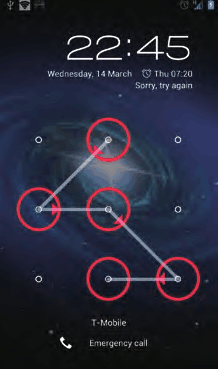
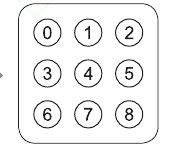


图 1

1.2Android系统手机的PIN码密码和复杂密码

PIN码密码和复杂密码非常相似，PIN码密码全部由数字组成，位数为4~16位，每一位都为任意数字；而复杂密码的组成规则要复杂的多，其组成规则为4~16位字符空间，每个字符空间有94个符号可选，包括大小写字母、数字、标点符号，但不能包括空格，如图2所示。由这些符号组成的密码连同一个随机整数一起组成密文，经过SHA-1加密后储存在password.key文件中，这个文件同样储存在data\system\路径下，文件大小为20个字节。因此PIN码密码是包含于复杂密码的，经计算，复杂密码共有3.7×1031种组合，按照不同密码长度来计算密码组合。

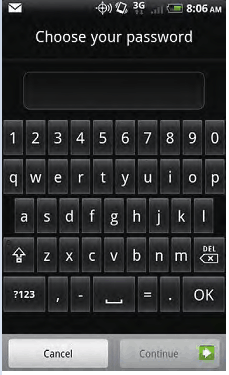
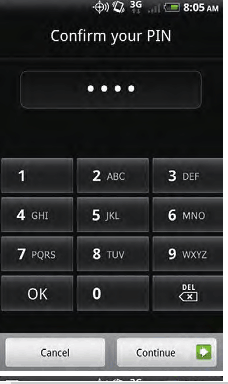


图 2

1. 相对应的破解方式：

2.1手势密码方式的破解：

2.1.1开启USB调试模式：当Android手机开启USB调试模式时，连接检材手机到检验电脑时，检验电脑系统会识别出连接到新硬件，并自动安装驱动。检验人员也可以通过手机第三方辅助工具协助判断，如91手机助手、QQ手机管家等。

检材手机在启用USB调试模式时，检验人员可以利用符合司法取证规范的检验工具来进行密码的获取，这些取证工具都是通过USB调试模式，在不打开锁屏的状态下，以ADB（Android开发调试模式） 方式推送取证工具的apk客户端到手机上，并自动安装运行，即打开了检材手机与取证工具传输数据的通道。取证工具在获取手机相关数据的同时，即可以获取密码文件并进行破解。

2.1.2未开启USB调试模式： 由于检材手机未启用USB调试模式，在手机开机状态连接到检验电脑是无法进行数据通信的。在这种情况下，较为简单的方法是利用第三方recovery分区模式（Android手机的恢复模式）启动手机，然后将整个手机自身存储或data分区备份到空白的SD存储卡中，再通过计算机提取存储卡中data镜像中的gestury.key密码文件进行破解。

2.2PIN码密码和复杂密码的破解：

由于PIN密码和复杂密码的占有空间比手势密码大很多，通过类似手势密码破解的手段获取的password.key文件，需要花费大量的时间破解，成功率很低。通过实验发现即便是合理的缩小密码空间，并且采用高性能的CPU来进行密码破解，所花费的时间也是惊人的。

通过统计，大部分手机使用者都习惯以Android默认小写字母输入键盘作为密码字符，以此为例，假设带有高性能处理器的手机检验工作站每秒破解2 500万次。

9位以下的密码破解还是可以接受的，但9位以上破解时间则难以满足案件检验的要求。如果再考虑到大写字母和数字的话，即便是5 000万次/秒的破解速度，8d也只能破解到7位密码。因此得出结论，通过暴力破解的方式进行复杂密码破解并不适用于电子证据检验工作。

使用adb命令进行复杂密码的移除方法，以三星盖世3（GT-i9300）为例，分别有开启USB调试模式和未开启USB调试模式两种情况。

2.2.1开启USB调试模式：

（1）手机启用USB调试模式，但由于使用取证工具在进行数据获取时需要在手机上进行相关授权操作，依然无法提取数据。此时可以使用一键root工具，如eRoot进行root权限获取，然后使用adbshell命令。具体步骤如下：

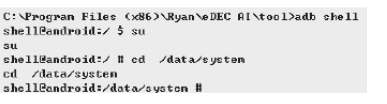
第一步：连接检材手机到检验电脑上，在CMD命令行中输入adb shell命令，使手机进入到adb调试状态（adb调试程序在eDEC狼蛛AI智能手机取证工具安装目录\tools路径中），然后输入su获取root权限，如图4所示前两行命令。

第二步：使用cd命令，可进入到/data/system路径下，如图4所示第四行。命令格式为（注意cd后的空格）：cd /data/system

第三步：使用cat命令备份已有密码文件为备份文件，即：cat password.key > password.key.bak

第四步：使用touch命令新建一个空白password.key密码文件，即：touch password.key

第五步：重启手机，输入任意密码可进入Android系统，使检材手机具备常规检验条件。



2.2.2手机未开启USB调试模式：则可以通过使用三星官方的Odin工具导入到带有root权限的第三方recovery分区，并在这种模式下，连接手机与检验电脑，使用CMD命令行进入adb shell。重置密码的方法和使用的命令与第一种情况相同。

通过上述步骤，可使检材手机恢复至正常状态在进行数据提取。

参考文献

［1］ 王桂强. 手机物证检验及其在刑事侦查中的应用［J］ . 刑

事技术，2006(1): 25-31.

［2］ http://www.oxygen-forensic.com/download/pressrelease/

PR\_FS2011\_ENG\_2011-10-31.pdf.

［3］ 丁锰，康艳荣，黄冬. 一种获取Android应用程序密码的方法［J］ .中国人民公安大学学报：自然科学版， 2014(4): 21-23.

［4］ 丁红军，范玮. 手机物证检验原则［J］ . 刑事技术，

2012(3): 48-50.

引用文献：王即墨，计超豪，裴洪卿. Android智能手机锁屏密码及破解方法研究［J］. 刑事技术，2015，40(2)：142-145