



(12) 发明专利申请

(10) 申请公布号 CN 101917267 A

(43) 申请公布日 2010. 12. 15

(21) 申请号 201010253577. 5

(22) 申请日 2010. 08. 13

(71) 申请人 福州星网视易信息系统有限公司

地址 350000 福建省福州市仓山区建新镇金  
山大道618号桔园洲工业园19号楼一、  
二层

(72) 发明人 郑子凤 李捷 林仁文

(74) 专利代理机构 福州市鼓楼区京华专利事  
务所（普通合伙） 35212

代理人 翁素华

(51) Int. Cl.

H04L 9/08 (2006. 01)

H04L 9/14 (2006. 01)

H04L 29/06 (2006. 01)

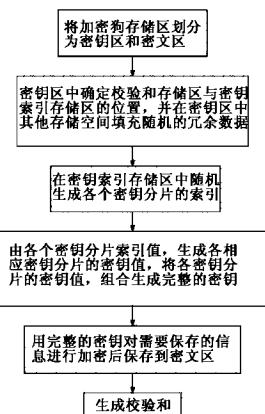
权利要求书 1 页 说明书 3 页 附图 2 页

(54) 发明名称

一种基于可存储加密狗的加密文件的随机密  
钥保存方法

(57) 摘要

本发明提供一种基于可存储加密狗的加密文  
件的随机密钥保存方法，其密钥是在加密狗内  
部生成，而且密钥是随机数，并且被拆散随机分  
布，同时添加校验机制，用来检验信息是否被篡改。  
本发明增强了加密的安全性；增强了密钥的隐蔽  
性；而且增强了加密狗的通用性。



1. 一种基于可存储加密狗的加密文件的随机密钥保存方法,其特征在于,包括以下步骤:

步骤 10、根据加密狗存储区的大小和实际的使用情况确定密钥区的大小,将加密狗存储区划分为密钥区和密文区两个部分;

步骤 20、在密钥区中确定校验和存储区与密钥索引存储区的位置,并在密钥区中,除了校验和存储区与密钥索引存储区之外的存储空间填充随机的冗余数据;

步骤 30、在密钥索引存储区中随机生成各个密钥分片的索引;

步骤 40、根据各个密钥分片的索引在密钥区中相应坐标位置获取对应密钥分片索引的值;

步骤 50、由各个密钥分片索引的值,生成各相应密钥分片的密钥值,将各密钥分片的密钥值,组合生成完整的密钥;

步骤 60、用完整的密钥对需要保存的信息进行加密后保存到密文区;

步骤 70、生成校验和;

上述步骤中所述的密钥分片的索引是指密钥所在密钥区的位置,是随机生成的,但是不能与密钥分片的索引和校验和存储区的位置重合。

2. 根据权利要求 1 所述的一种基于可存储加密狗的加密文件的随机密钥保存方法,其特征在于:所述步骤 30 中的密钥分片的索引的末尾具有一索引结束标志。

3. 根据权利要求 1 或 2 所述的一种基于可存储加密狗的加密文件的随机密钥保存方法,其特征在于:进一步包括以下解密步骤:

步骤 10、读取加密狗存储区的信息,根据校验和判断加密狗存储区信息是否被篡改,如果被篡改则直接跳出,信息无效,如果未被篡改则根据密钥索引读取各密钥分片的密钥值;

步骤 20、将读取到的密钥值组成完整的密钥;

步骤 30、根据完整的密钥对密文区的数据进行解密,得到明文信息。

4. 根据权利要求 3 所述的一种基于可存储加密狗的加密文件的随机密钥保存方法,其特征在于:所述的步骤 20 中,当密钥长度不固定时,通过密钥索引结束标志判断密钥长度。

## 一种基于可存储加密狗的加密文件的随机密钥保存方法

### 【技术领域】

[0001] 本发明涉及一种信息安全领域，尤其是基于可存储加密狗的加密文件的随机密钥保存方法。

### 【背景技术】

[0002] 目前加密狗的解密破解工作主要集中在应用程序与加密动态库之间的通讯拦截。传统的可存储加密狗的存储区可以用于存储重要的信息，这些信息一般都是经过加密的。在使用时，一般使用约定的（固定的或通过一定的算法得到的）密钥对存储区的数据进行加密或解密。这种加密方法是在加密狗外部得到密钥，然后对加密狗的存储区信息进行加密或者解密。使用在加密狗外部对加密狗存储区的信息进行加密的技术方案，由于密钥可以在通过一定的算法得到，存在一定的安全隐患，而且无法验证信息是否被篡改。

### 【发明内容】

[0003] 本发明要解决的技术问题，在于提供一种基于可存储加密狗的加密文件的随机密钥保存方法，增强了加密的安全性；增强了密钥的隐蔽性；而且解密时必须读取到加密狗存储区信息后，能从中获取到密码，增强了加密狗的通用性。

[0004] 一种基于可存储加密狗的加密文件的随机密钥保存方法，其特征在于，包括以下步骤：

[0005] 步骤 10、根据加密狗存储区的大小和实际的使用情况确定密钥区的大小，将加密狗存储区划分为密钥区和密文区两个部分；

[0006] 步骤 20、在密钥区中确定校验和存储区与密钥索引存储区的位置，并在密钥区中，除了校验和存储区与密钥索引存储区之外的存储空间填充随机的冗余数据；

[0007] 步骤 30、在密钥索引存储区中随机生成各个密钥分片的索引；

[0008] 步骤 40、根据各个密钥分片的索引在密钥区中相应坐标位置获取对应密钥分片索引的值；

[0009] 步骤 50、由各个密钥分片索引的值，生成各相应密钥分片的密钥值，将各密钥分片的密钥值，组合生成完整的密钥；

[0010] 步骤 60、用完整的密钥对需要保存的信息进行加密后保存到密文区；

[0011] 步骤 70、生成校验和；

[0012] 上述步骤中所述的密钥分片的索引是指密钥所在密钥区的位置，是随机生成的，但是不能与密钥分片的索引和校验和存储区的位置重合。

[0013] 本发明具有如下优点：一种基于可存储加密狗的加密文件的随机密钥保存方法，其密钥是在加密狗内部生成，而且密钥是随机数，并且被拆散随机分布，同时添加校验机制，用来检验信息是否被篡改，这样可以大大提高加密的安全性。

**【附图说明】**

- [0014] 下面参照附图结合实施例对本发明作进一步的说明。
- [0015] 图 1 为本发明方法结构示意图。
- [0016] 图 2 为密钥索引的分解图。
- [0017] 图 3 为对加密狗进行加密的流程示意图。

**【具体实施方式】**

[0018] 本发明的一种基于可存储加密狗的加密文件的随机密钥保存方法，首先在加密狗的存储区中开辟一定的空间用于保存随机密钥，我们称之为密钥区，其余的空间用于保存密文，称之为密文区。

[0019] 如图 1 所示，密钥区包含校验和存储区、密钥索引存储区（密钥索引存储区是指密钥所在密钥区的位置）、密钥分片（密钥 1- 密钥 n）和冗余数据组成。其中校验和存储区、密钥索引存储区和密钥分片不能重叠，校验和存储区必须在密钥索引存储区和密钥分片之前，这样才能对密钥和密文进行校验；由于密钥长度是不固定的，所以密钥索引有一结束标志；由各个密钥分片组成的密钥索引是指对应密钥分片所在的位置。图 2 为密钥索引的分解图，其中的各个密钥分片的索引是在密钥索引中生产的，各个密钥分片的索引又组成了对应的密钥索引。以下结合图 3 将对加密狗加密的过程作详细的介绍。

[0020] 加密算法实现如下：

[0021] 1、根据加密狗存储区的大小和实际的使用情况确定密钥区的大小，将存储区划分为密钥区和密文区两个部分。

[0022] 2、在密钥区中确定校验和存储区与密钥索引存储区的位置，并在密钥区中，除了校验和存储区与密钥索引存储区之外的存储空间填充随机的冗余数据。

[0023] 3、在密钥索引存储区中随机生成各个密钥分片的索引，可以根据需要在密钥分片的索引的末尾具有一索引结束标。密钥分片的索引是随机生成的，但是不能与其他的密钥分片的索引和校验和存储区的位置重合。

[0024] 4、根据各个密钥分片的索引在密钥区中相应坐标位置获取对应密钥分片索引的值。

[0025] 5、由各个密钥分片索引的值，生成各相应密钥分片的密钥值，将各密钥分片的密钥值，组合生成完整的密钥。

[0026] 6、用完整的密钥对需要保存的信息进行加密后保存到密文区。

[0027] 7、生成校验和。

[0028] 其中加密狗存储区的解密算法实现如下：

[0029] 1、读取加密狗存储区的信息，根据校验和判断加密狗存储区信息是否被篡改。如果被篡改则直接跳出，信息无效。

[0030] 2、如果未被篡改则根据密钥索引读取各密钥分片的密钥值，当密钥长度不固定时，可以通过密钥索引结束标志判断密钥长度，将读取到的密钥值组成完整的密钥。

[0031] 3、根据生成的密钥对密文区的数据进行解密，得到明文信息。

[0032] 本发明是将密钥存在加密狗内部，而且密钥是随机数，并且被拆散随机分布，同时添加校验机制，用来检验信息是否被篡改，这样可以大大提高加密的安全性。

[0033] 以上所述仅为本发明的较佳实施例，凡依本发明申请专利范围所做的均等变化与修饰，皆应属本发明的涵盖范围。

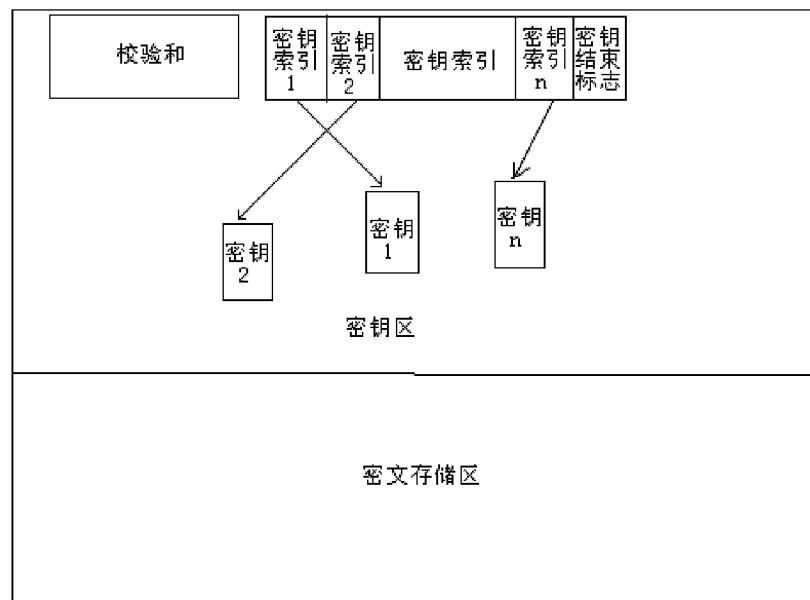


图 1

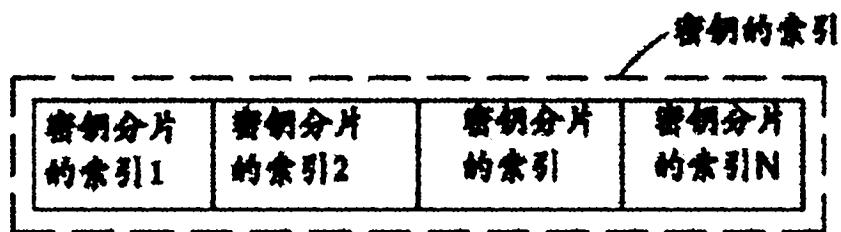


图 2

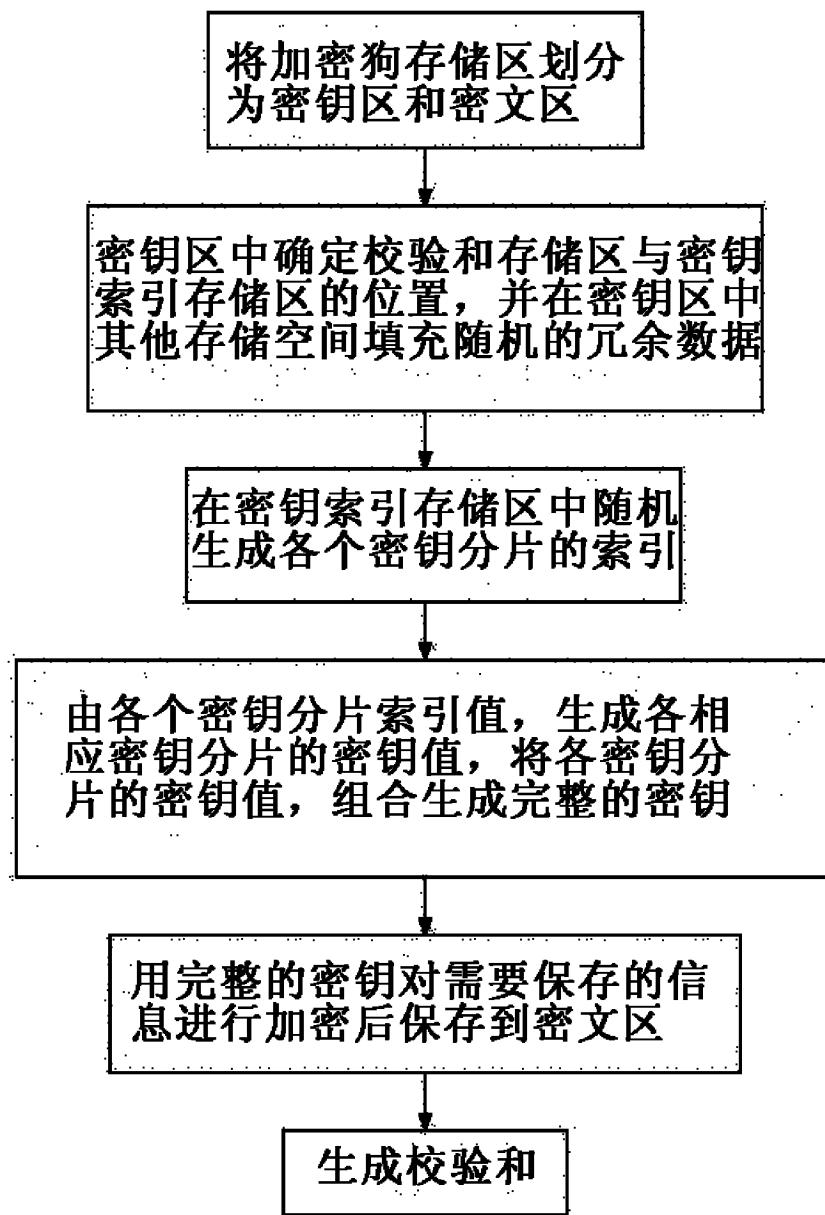


图 3