(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 107248914 B
(45)授权公告日 2020.12.15

(21)申请号 201710693241.2

(22)申请日 2017.08.14

(65)同一申请的已公布的文献号
申请公布号 CN 107248914 A

(43)申请公布日 2017.10.13

(73)专利权人 四川长虹电器股份有限公司
地址 621000 四川省绵阳市高新区绵兴东路35号

(72)发明人 刘蛟 李伟光 马春燕 郑红

(74)专利代理机构 四川省成都市天策商标专利事务所 51213
代理人 刘兴亮 刘渝

(51)Int.Cl.
H04L 9/08(2006.01)
H04L 29/06(2006.01)

(56)对比文件
CN 101534165 A,2009.09.16
CN 106559782 A,2017.04.05
US 2006282236 A1,2006.12.14
US 2010174859 A1,2010.07.08
Martin Abadi,David G.Andersen.Learning to Protect Communications with Adversarial Neural Cryptography.《Computer Science》.2016,

审查员 李炯

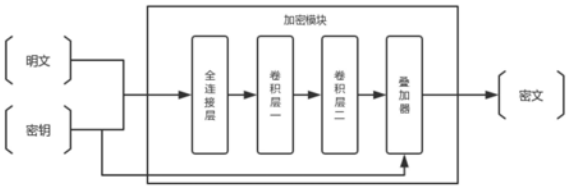
权利要求书2页 说明书5页 附图3页

(54)发明名称

一种iOS设备上新型对称加密系统及加密方法

(57)摘要

本发明公开了一种iOS设备上新型对称加密系统，包括加密模块和解密模块。本发明还提供了一种iOS设备上新型对称加密方法，包含加密流程和解密流程。本发明提出一种可应用于iOS设备上的新型的对称加密系统和加密方法，结合了神经网络来实现加解密，使其核心算法不同于传统的对称加密算法，可以加强安全性。并且神经网络的结构，使用者可以根据自己的需要进行变化，只需重新训练参数。



CN 107248914 B

1.一种iOS设备上新型对称加密方法,其特征在于:

所述的方法包含加密流程和解密流程:

加密流程包括如下步骤:

步骤一、获取需要加密的明文和加密所需要的密钥;

步骤二、对明文和密钥进行转换;

步骤三、对明文和密钥进行整合;

步骤四、检验格式是否满足要求,如果不满足要求则从步骤七结束流程,满足则继续;

步骤五、将步骤三得到的数据输入加密神经网络模块中进行加密;

步骤六、获得密文;

步骤七、流程结束;

解密流程包括如下步骤:

步骤一、输入需要解密的密文和和解密所需的密钥;

步骤二、对密钥进行转换,方法同加密过程中的步骤二;

步骤三、对密文和密钥进行整合,方法同加密过程中的步骤三;

步骤四、检验格式是否满足要求,如果不满足要求则从步骤七结束流程,满足则继续;

步骤五、将步骤三的到的数据输入解密神经网络模块中进行解密;

步骤六、获得明文;

步骤七、流程结束;

对明文和密钥进行转换,其中包括以下步骤:

1)、明文和密钥转换时,首先将明文和密钥转换成ASCII码并获取其对应的int型数值;

2)、将获取到的int型数值转换为8位的二进制数值;

3)、对每一位的二进制数值乘2减1,归一化到[-1,1]区间,形成1x8的float型向量;

获得明文流程有如下步骤:

1)、首先将输出的1x8的float型向量逐位加1除2,转换到[0,1]区间;

2)、将1x8的float型向量转换成十进制int型数据;

3)、将int型数据转换成对应的ASCII码明文;

所述加密神经网络模块:主要包含顺序连接的全连接层,两个卷积层和叠加器;

其中,全连接层:权重结构是16x16的矩阵,偏差是1x16的向量;

第一卷积层:卷积核大小是2x2,输出特征图数量是2,步长为2,激活函数为Relu;

第二卷积层:卷积核大小是2x2,输出特征图数量是1,步长为1,激活函数为Tanh;

叠加器:执行的操作是将输入向量与密钥向量的10倍相加;

所述解密神经网络模块:主要包含顺序连接的拆解器,全连接层和两个卷积层;

拆解器:执行的操作是将密文向量减去密钥向量的10倍;

全连接层:权重结构是16x16的矩阵,偏差是1x16的向量;

第一卷积层:卷积核大小是2x2,输出特征图数量是2,步长为2,激活函数为Relu;

第二卷积层:卷积核大小是2x2,输出特征图数量是1,步长为1,激活函数为Tanh。

2.根据权利要求1所述iOS设备上新型对称加密方法,其特征在于:

对明文和密钥进行整合,将密钥的1x8的float型向量拼接到明文1x8的float型向量后面,形成1x16的向量。

3.根据权利要求1所述iOS设备上新型对称加密方法,其特征在于:

加密神经网络模块中进行加密,包括如下步骤:

1)、明文和密钥首先会经过全连接层处理;

2)、过程1)的数据会经过第一卷积层和第二卷积层两次卷积处理;

3)、过程2)的数据最后经过叠加器处理。

4.根据权利要求1所述iOS设备上新型对称加密方法,其特征在于:

获得密文的格式为1x8的float型向量。

5.根据权利要求1所述iOS设备上新型对称加密方法,其特征在于:

解密神经网络模块中进行解密,包括如下步骤:

1)、将密文和密钥输入拆解器处理;

2)、将过程1)获得的数据输入全连接层处理;

3)、将过程2)获得的数据经过第一卷积层和第二卷积层两次卷积处理。

一种iOS设备上新型对称加密系统及加密方法

技术领域

[0001] 本发明涉及一种加密系统及方法，具体涉及一种iOS设备上新型对称加密系统及加密方法，属于计算机加密技术领域。

背景技术

[0002] 对称加密是一种成熟的加密方式，因其计算量小、加密速度快、加密效率高等优点而广泛应用于iOS应用的密码、文件、核心数据的加密上。现在比较流行的对称加密方法有DES、AES、Blowfish等等。

[0003] 但是对称加密的算法是公开的，且加密双方发送数据前必须保存好商定好的密钥，如果需要和多个对象完成通信，那么就会拥有数量巨大的密钥，管理如此多的密钥对双方来说都是一个很大的负担。而且只要一方的密钥泄露，那么加密信息也就不完全了。

发明内容

[0004] 本发明针对常规对称加密中存在的各种问题，实现了一种基于神经网络的iOS设备上新型对称加密系统，通过此加密系统可以使iOS设备更好的完成信息的加密、解密。

[0005] 为了实现上述目的，本发明采用如下技术方案：

[0006] 一种iOS设备上新型对称加密系统，包括加密模块和解密模块。

[0007] 更进一步的方案是：

[0008] 所述加密模块：主要包含顺序连接的全连接层，两个卷积层和叠加器；

[0009] 其中，全连接层：权重结构是16x16的矩阵，偏差是1x16的向量；

[0010] 第一卷积层：卷积核大小是2x2，输出特征图数量是2，步长为2，激活函数为Relu；

[0011] 第二卷积层：卷积核大小是2x2，输出特征图数量是1，步长为1，激活函数为Tanh；

[0012] 叠加器：执行的操作是将输入向量与密钥向量的10倍相加。

[0013] 更进一步的方案是：

[0014] 所述解密模块：主要包含顺序连接的拆解器，全连接层和两个卷积层；

[0015] 拆解器：执行的操作是将密文向量减去密钥向量的10倍；

[0016] 全连接层：权重结构是16x16的矩阵，偏差是1x16的向量；

[0017] 第一卷积层：卷积核大小是2x2，输出特征图数量是2，步长为2，激活函数为Relu；

[0018] 第二卷积层：卷积核大小是2x2，输出特征图数量是1，步长为1，激活函数为Tanh。

[0019] 本发明的另一个目的在于提供一种iOS设备上新型对称加密方法。

[0020] 一种iOS设备上新型对称加密方法，采用了本发明所述的iOS设备上新型对称加密系统，并主要包含加密流程和解密流程：

[0021] 加密流程包括如下步骤：

[0022] 步骤一、获取需要加密的明文和加密所需要的密钥；

[0023] 步骤二、对明文和密钥进行转换；

[0024] 步骤三、对明文和密钥进行整合；

[0025] 步骤四、检验格式是否满足要求，如果不满足要求则从步骤七结束流程，满足则继续；

[0026] 步骤五、将步骤三得到的数据输入神经网络模块中进行加密；

[0027] 步骤六、获得密文；

[0028] 步骤七、流程结束；

[0029] 解密流程包括如下步骤：

[0030] 步骤一、输入需要解密的密文和和解密所需的密钥；

[0031] 步骤二、对密钥进行转换，方法同加密过程中的步骤二；

[0032] 步骤三、对密文和密钥进行整合，方法同加密过程中的步骤三；

[0033] 步骤四、检验格式是否满足要求，如果不满足要求则从步骤七结束流程，满足则继续；

[0034] 步骤五、将步骤三的到的数据输入神经网络模块中进行解密；

[0035] 步骤六、获得明文；

[0036] 步骤七、流程结束。

[0037] 更进一步的方案是：

[0038] 对明文和密钥进行转换，其中包括以下步骤：

[0039] 1)、明文和密钥转换时，首先将明文和密钥转换成ASCII码并获取其对应的int型数值；

[0040] 2)、将获取到的int型数值转换为8位的二进制数值；

[0041] 3)、对每一位的二进制数值乘2减1，归一化到[-1,1]区间，形成1x8的float型向量。

[0042] 更进一步的方案是：

[0043] 对明文和密钥进行整合，方法为将密钥的1x8的float型向量拼接到明文1x8的float型向量后面，形成1x16的向量。

[0044] 更进一步的方案是：

[0045] 神经网络模块中进行加密，包括如下步骤：

[0046] 1)、明文和密钥首先会经过全连接层处理；

[0047] 2)、过程1)的数据会经过两次卷积处理，第一卷积层和第二卷积层；

[0048] 3)、过程2)的数据最后经过叠加器处理。

[0049] 更进一步的方案是：

[0050] 获得密文的格式为1x8的float型向量。

[0051] 更进一步的方案是：

[0052] 神经网络模块中进行解密，包括如下步骤：

[0053] 1)、将密文和密钥输入拆解器处理；

[0054] 2)、将过程1)获得的数据输入全连接层处理；

[0055] 3)、将过程2)获得的数据经过两次卷积处理，第一卷积层和第二卷积层。

[0056] 更进一步的方案是：

[0057] 获得明文流程有如下步骤：

[0058] 1)、首先将输出的1x8的float型向量逐位加1除2，转换到[0,1]区间；

[0059] 2)、将1x8的float型向量转换成十进制int型数据；

[0060] 3)、将int型数据转换成对应的ASCII码明文。

[0061] 本发明提出一种可应用于iOS设备上的新型的对称加密系统和加密方法，结合了神经网络来实现加解密，使其核心算法不同于传统的对称加密算法，可以加强安全性。并且神经网络的结构，使用者可以根据自己的需要进行变化，只需重新训练参数。目前，本发明的系统和方法主要用来对密码进行加密，可以对ASCII字符进行加解密，iOS上实现神经网络用到了Metal与Accelerate框架。

附图说明

[0062] 图1加密模块结构图；

[0063] 图2解密模块结构图；

[0064] 图3加密流程图；

[0065] 图4解密流程图。

具体实施方式

[0066] 为使本发明的目的、技术方案和优点更加清楚，下面结合附图对本发明做进一步地详细描述。

[0067] 如图1、2所示，本方法一共包含两个核心模块：加密模块与解密模块，两个模块都用到了神经网络结构。

[0068] 加密模块：如图1所示，该模块包含一个全连接层、两个卷积层、一个叠加器。

[0069] 1)、全连接层包含一个16x16的权重矩阵W与1x16的偏差向量b，输入X是明文与密钥整合后的1x16的向量，输出fc也是1x16的向量。计算公式如下：

[0070] $fC = X \times W + b$

[0071] 2)、第一卷积层的卷积核是2x2的conv1_weight与2x1的conv1_bias，输出特征图数量是2，步长是2，激活函数是Relu，输入是全连接层的输出fc，输出conv1是2x8的矩阵。计算公式如下：

[0072] $$conv1 = Relu(fc \otimes conv1\_weight + conv1\_bias)$$

[0073] 3)、第二卷积层的卷积核是2x2的conv2_weight与1x1的conv2_bias，输出特征图数量是1，步长是1，激活函数是Tanh，输入是第一卷积层的输出conv1，输出conv2是1x8的向量。计算公式如下：

[0074] $$conv2 = Tanh(conv1 \otimes conv2\_weight + conv2\_bias)$$

[0075] 4)、叠加器是将1x8的密钥向量key乘10加上第二卷积层的输出conv2，最后得到密文向量cryptText。计算公式如下：

[0076] $CryptText = key \cdot 10 + conv2$

[0077] 解密模块：如图2所示，该模块包含一个拆解器，一个全连接层和两个卷积层。

[0078] 1)、拆解器与叠加器相对应将密文cryptText减去1x8的密钥向量key乘10，最后得到一个1x8的向量Y。

[0079] $X = cryptText - key \cdot 10$

[0080] 2)、全连接层结构与公式和加密模块的全连接层一样，只是权重和偏差的参数不一样。输入是拆解器输出Y与密钥key整合后的1x16的向量X，输出同样是1x16的向量fc。

[0081] 3)、第一卷积层结构与公式和加密模块第一卷积层一样，只是卷积核的参数不一样。输入是全连接层的输出fc，输出是2x8的矩阵conv1。

[0082] 4)、第二卷积层结构与公式和加密模块第二卷积层一样，只是卷积核的参数不一样。输入是第一卷积层的输出conv1，输出是1x8的向量conv2。

[0083] 以上两个模块详细技术实施方案如下，主要包括两个流程：加密流程与解密流程。

[0084] 加密流程如图3所示，包含以下子步骤：首先步骤S1流程开始。接下来步骤S2，获取明文与密钥。然后在步骤S3分别将明文、密钥转换成1x8的向量。接着在步骤S4整合密钥与明文，将密钥拼接到明文后面构成一个1x16的向量。在步骤S5校验格式是否满足要求，如果不是，则直接进入步骤S8结束流程，如果满足要求，则进去步骤S6输入加密模块。最后在步骤S7获取密文，进入步骤S8流程结束。

[0085] 其中步骤S3转换明文、密钥包含以下子步骤：

[0086] a1、将明文或密钥对应的ASCII码转换成对应的int型数值。

[0087] a2、将获取到的int型数值转换为8位的二进制数值。

[0088] a3、对每一位的二进制数值乘2减1，归一化到[-1,1]区间，形成1x 8的float型向量。

[0089] 解密流程如图4所示，包含以下子步骤：首先步骤S1流程开始。接下来步骤S2，输入密文、密钥。然后在步骤S3将密钥转换成1x8的向量。接着在步骤S4，整合密钥与密文，将1x8的密钥向量拼接到1x8的密文向量后面，形成1x16的向量。在步骤S5校验格式是否满足要求，如果不是，则直接进入步骤S8结束流程，如果满足要求，则进去步骤S6输入解密模块。最后在步骤S7获取明文，进入步骤S8流程结束。

[0090] 其中步骤S3的转换流程同加密的步骤S3流程。

[0091] 步骤S7获取明文包含以下子流程：

[0092] b1、首先将输出的1x8的float型向量逐位加1除2，转换到[0,1]区间。

[0093] b2、将1x8的float型向量转换成十进制int型数据。设1x 8的float型向量为X，Xi代表第i位的数值，转换公式如下：

[0094] $$Loss_i=\begin{cases}\dfrac{1-X_i}{2^i}, X_i \geq 0.5\\ \dfrac{X_i}{2^i}, X_i < 0.5\end{cases}$$

[0095] $$f(X_i)=\begin{cases}2^i \bullet (1-Loss_i), X_i \geq 0.5\\ 2^i \bullet Loss_i, X_i < 0.5\end{cases}$$

[0096] $$Y=round(\sum_{i=0}^{7} f(X_i))$$

[0097] b3、将输出的int型数据Y转换成对应的ASCII码明文。

[0098] 尽管这里参照本发明的解释性实施例对本发明进行了描述，上述实施例仅为本发明较佳的实施方式，本发明的实施方式并不受上述实施例的限制，应该理解，本领域技术人员可以设计出很多其他的修改和实施方式，这些修改和实施方式将落在本申请公开的原则

范围和精神之内。

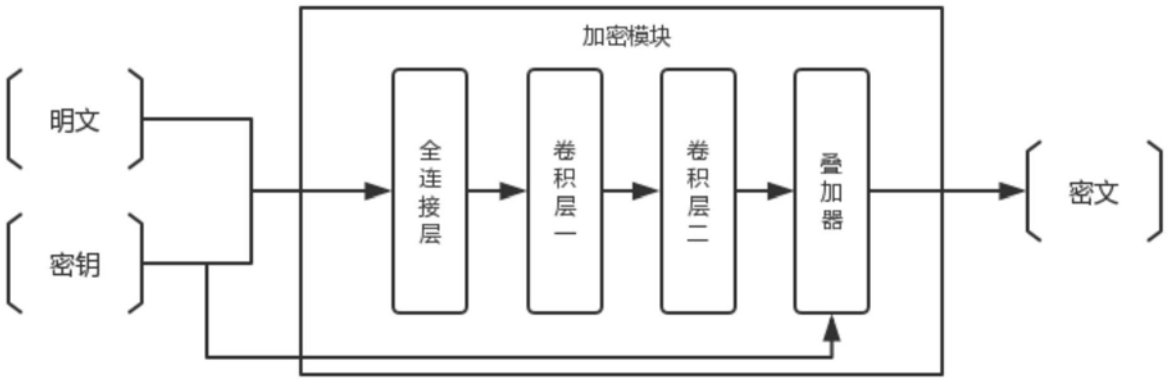

加密模块
明文
密钥
全连接层
卷积层一
卷积层二
叠加器
密文

图1

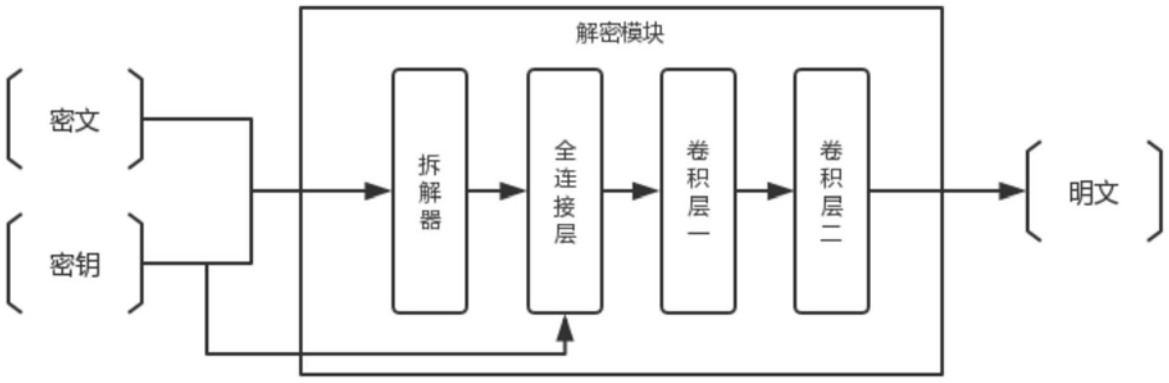

解密模块
密文
密钥
拆解器
全连接层
卷积层一
卷积层二
明文

图2

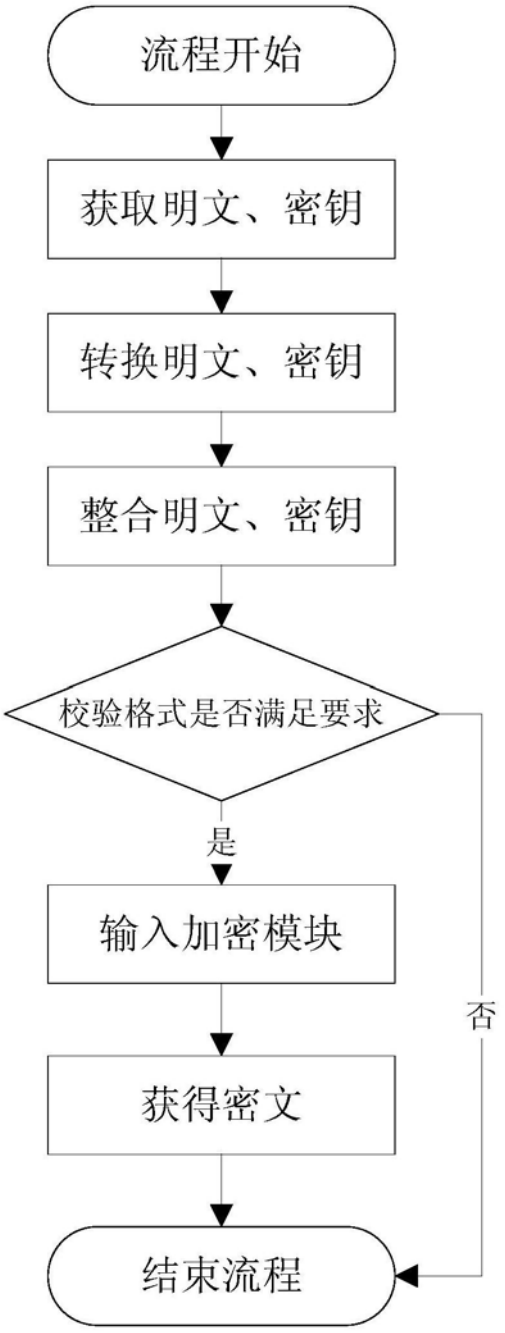


图3

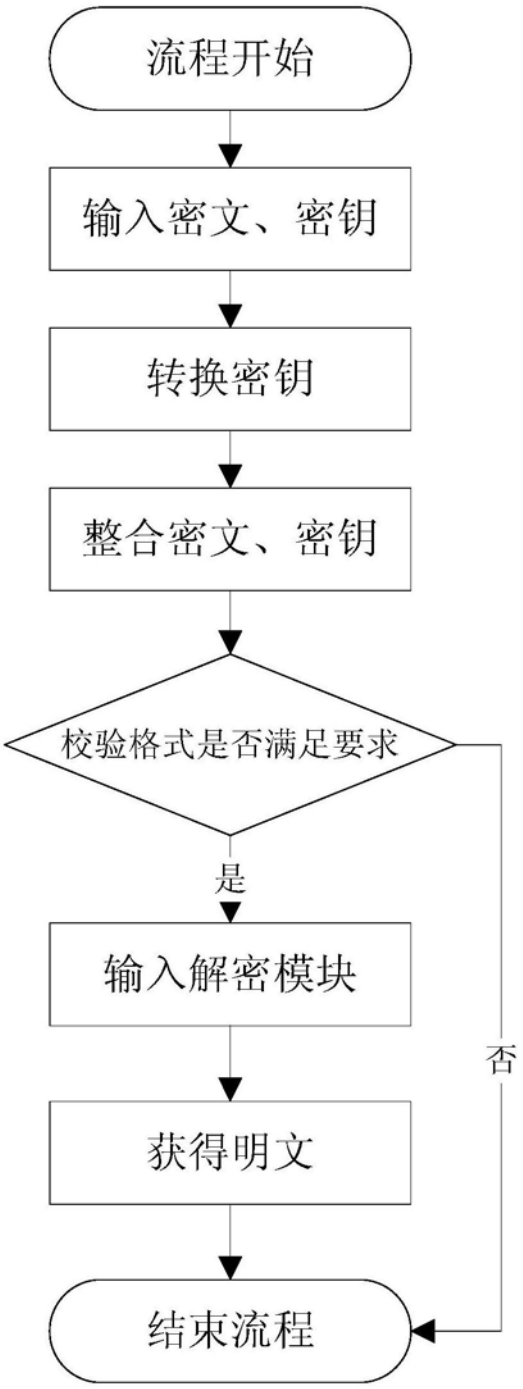


图4