(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 115811397 B
(45)授权公告日 2023.08.04

(21)申请号 202211455571.5
(22)申请日 2022.11.21
(65)同一申请的已公布的文献号
申请公布号 CN 115811397 A
(43)申请公布日 2023.03.17
(73)专利权人 北京神州安付科技股份有限公司
地址 102200 北京市昌平区回龙观龙域中街1号院1号楼龙域中心A座1102室
(72)发明人 张敏 胡洪金 崔焕
(74)专利代理机构 北京酷爱智慧知识产权代理有限公司 11514
专利代理师 刘志刚
(51)Int.Cl.
H04L 9/08(2006.01)
H04L 9/40(2022.01)
G06N 3/044(2023.01)

(56)对比文件
CN 110837651 A,2020.02.25
CN 110943830 A,2020.03.31
CN 111860774 A,2020.10.30
CN 113240100 A,2021.08.10
CN 114826702 A,2022.07.29
US 2003161467 A1,2003.08.28
US 2020193300 A1,2020.06.18
尹昊.《基于离散分数阶混沌系统的图像加密》.《中国优秀硕士学位论文全文数据库》.2021,全文.

审查员 谢丹

权利要求书2页 说明书5页 附图1页

(54)发明名称

一种高安全服务器密码机

(57)摘要

本发明公开了一种高安全服务器密码机,涉及密码机技术领域,通过生成数据特征均不相同的表征数据集,保障加密模块中生成的随机数均为真随机数,由于表征数据集的生成过程采用了旧数据的特征蒸馏,避免训练过程产生偏差、训练结果与旧数据重合,同时采用了以时间栈为分隔的方式,将训练过程与加解密过程分离,降低加解密过程中的数据回溯轮询时间,有效提升密码机的密钥检验效率。

CN 115811397 B

1.一种高安全服务器密码机,其特征在于,包括以下内容:

命令接口、加密模块、主控模块、加密接口,所述命令接口、加密接口均集成在所述主控模块上,所述命令接口用于获取目标设备的物理随机信号,所述加密模块与所述主控模块连接;

所述加密模块包括第一随机数发生器、第二随机数发生器、Hopfield神经网络模块、密钥库,所述第一随机数发生器基于物理随机信号生成第一随机数,所述Hopfield神经网络模块包括多个离散的Hopfield神经网络电路,其中每个离散的Hopfield神经网络电路与一位第一随机数一一对应,所述每个离散的Hopfield神经网络电路生成表征数据集,所述表征数据集用于生成接收到的一位第一随机数在当前t时刻的表征信号,所述第二随机数发生器根据表征信号生成真随机数,所述密钥库用于对随机数进行加密,得到加密随机数;

所述Hopfield神经网络模块的生成表征数据集的步骤包括:

步骤1:预设虚拟物理信号,对虚拟物理信号训练生成表征任务,并得出对应的任务样本集;

步骤2:在任务样本集可用的情况下,对每个任务数据集提取最优价值数据进行保留,得出表征数据集;

所述任务样本集可用的情况为:样本集中的样本均各不相同。

2.根据权利要求1所述的高安全服务器密码机,其特征在于,所述命令接口接收第一个随机信号到最后一个随机信号的时间间隔称为Hopfield神经网络学习的一个时间栈,所述Hopfield神经网络随着时间栈的变化修改表征数据集,在第N个时间栈中,所述Hopfield神经网络访问N号表征数据集。

3.根据权利要求2所述的高安全服务器密码机,其特征在于,所述Hopfield神经网络模块随着时间栈变化修改表征数据集的步骤包括:

步骤3:在第N-1个时间栈结束后,预设虚拟物理信号,对虚拟物理信号训练生成N号表征任务,并得出对应的N号任务样本集;在任务样本集可用的情况下,对每个任务数据集提取最优价值数据进行保留,得出N号表征数据集;

步骤4:在第N个时间栈结束后,预设虚拟物理信号,对虚拟物理信号训练生成N+1号表征任务,并得出对应的N+1号任务样本集,将N号表征任务的表征数据集加入该任务样本集中,在N+1号任务样本集可用的情况下,对每个任务数据集提取最优价值数据进行保留,得出N+1号表征数据集。

4.根据权利要求3所述的高安全服务器密码机,其特征在于,所述最优价值的数据的提取步骤包括:

步骤a:依据N号表征数据集,获取N号表征任务所对应的特征抓取器,采用特征抓取器抓取N+1号样本数据中所有样本数据的特征;

步骤b:根据所抓取的多个样本数据特征,为每一类样本数据计算特征均值,并计算多个样本数据特征与特征均值的欧几里得距离;

步骤c:保留欧几里得距离最小的样本数据特征所对应的m个样本数据。

5.根据权利要求1所述的高安全服务器密码机,其特征在于,所述第一随机数发生器和/或第二随机数发生器为热噪声随机数发生器、振荡采样随机数发生器、亚稳态随机数发生器或混沌随机数发生器中的一种或多种。

6.根据权利要求1所述的高安全服务器密码机，其特征在于，所述主控模块用于接收目标设备通过命令接口发送的任务请求，并通过加密模块将所述任务数据发送至与集线器连接的加密模块，其中，所述任务请求包含任务类型以及任务数据。

一种高安全服务器密码机

技术领域

[0001] 本发明涉及密码机技术领域,具体涉及一种高安全服务器密码机。

背景技术

[0002] 服务器密码机设备具有数据加解密、签名、验签、MAC、杂凑等功能,因此,可以为用户解决敏感信息机密性、完整性、有效性和不可抵赖等安全性问题。在使用过程中,服务器密码机设备利用管理员锁来对设备进行管理,例如管理员身份认证,或者利用管理员锁来完成设备的初始化和密钥恢复等操作。

[0003] 密码机在使用时为提高传输过程中的安全性,采用通过多路物理噪声源芯片直接产生随机数的方式,根据随机数生产密钥作为密钥因子计算数据校验密钥,虽然隔绝了操作者和操作方式的干扰,提升了破译难度,但是由于物理噪声源芯片产生的随机数受温度、时间、电压、压力、音频等环境因素影响,具有一定的重复性,且随机数的产生遵循一定的算法模拟,其结果是有规律可循的,在接收到重复的物理噪声时必定出现重复的随机数结果,所以现有的密码机会对随机数进行轮询检测,将重复的随机数进行清除,但这样的轮询过程耗时较长,密钥校验效率低下。

发明内容

[0004] 为了克服上述缺陷,本发明提供了高安全服务器密码机,以解决上述技术问题。

[0005] 一种高安全服务器密码机,包括以下内容:

[0006] 命令接口、加密模块、主控模块、加密模块,所述命令接口、加密模块均集成在所述主控模块上,所述命令接口用于获取目标设备的物理随机信号,所述加密模块与所述加密模块连接。

[0007] 作为优选地,所述加密模块包括第一随机数发生器、第二随机数发生器、Hopfield神经网络模块、密钥库,所述第一随机数发生器基于物理随机信号生成第一随机数,所述Hopfield神经网络模块包括多个离散的Hopfield神经网络电路,其中每个离散的Hopfield神经网络电路与一位第一随机数一一对应,所述每个离散的Hopfield神经网络电路生成表征数据集,所述表征数据集用于生成接收到的一位第一随机数在当前t时刻的表征信号,所述第二随机数发生器根据表征信号生成真随机数,所述密钥库用于对随机数进行加密,得到加密随机数。

[0008] 作为优选地,所述Hopfield神经网络模块的生成表征数据集的步骤包括:

[0009] 步骤1:预设虚拟物理信号,对虚拟物理信号训练生成表征任务,并得出对应的任务样本集;

[0010] 步骤2:在任务样本集可用的情况下,对每个任务数据集提取最优价值数据进行保留,得出表征数据集。

[0011] 作为优选地,所述任务样本集可用的情况为:样本集中的样本均各不相同。

[0012] 作为优选地,所述命令接口接收第一个随机信号到最后一个随机信号的时间间隔

称为Hopfield神经网络学习的一个时间栈，所述Hopfield神经网络随着时间栈的变化修改表征数据集，在第N个时间栈中，所述Hopfield神经网络访问N号表征数据集。

[0013] 作为优选地，所述Hopfield神经网络模块随着时间栈变化修改表征数据集的步骤包括：

[0014] 步骤3：在第N-1个时间栈结束后，预设虚拟物理信号，对虚拟物理信号训练生成N号表征任务，并得出对应的N号任务样本集；在任务样本集可用的情况下，对每个任务数据集提取最优价值数据进行保留，得出N号表征数据集；

[0015] 步骤4：在第N个时间栈结束后，预设虚拟物理信号，对虚拟物理信号训练生成N+1号表征任务，并得出对应的N+1号任务样本集，将N号表征任务的表征数据集加入该任务样本集中，在N+1号任务样本集可用的情况下，对每个任务数据集提取最优价值数据进行保留，得出N+1号表征数据集。

[0016] 作为优选地，所述最优价值的数据的提取步骤包括：

[0017] 步骤a：依据N号表征数据集，获取N号表征任务所对应的特征抓取器，采用特征抓取器抓取N+1号样本数据中所有样本数据的特征；

[0018] 步骤b：根据所抓取的多个样本数据特征，为每一类样本数据计算特征均值，并计算多个样本数据特征与特征均值的欧几里得距离；

[0019] 步骤c：保留欧几里得距离最小的样本数据特征所对应的m个样本数据。

[0020] 作为优选地，所述第一随机数发生器和/或第二随机数发生器为热噪声随机数发生器、振荡采样随机数发生器、亚稳态随机数发生器或混沌随机数发生器中的一种或多种。

[0021] 作为优选地，所述主控模块用于接收目标设备通过命令接口发送的任务请求，并通过加密模块将所述任务数据发送至与集线器连接的加密模块，其中，所述任务请求包含任务类型以及任务数据。

[0022] 本发明的有益效果体现在：

[0023] 本发明中通过生成数据特征均不相同的表征数据集，保障加密模块中生成的随机数均为真随机数，由于表征数据集的生成过程采用了旧数据的特征蒸馏，避免训练过程产生偏差、训练结果与旧数据重合，同时采用了以时间栈为分隔的方式，将训练过程与加解密过程分离，降低加解密过程中的数据回溯轮询时间，有效提升密码机的密钥检验效率。

附图说明

[0024] 为了更清楚地说明本发明具体实施方式或现有技术中的技术方案，下面将对具体实施方式或现有技术描述中所需要使用的附图作简单地介绍。在所有附图中，类似的元件或部分一般由类似的附图标记标识。附图中，各元件或部分并不一定按照实际的比例绘制。

[0025] 图1为本发明提供的一种高安全服务器密码机的原理图；

[0026] 图2为本发明提供的一种高安全服务器密码机生成表征数据集的步骤图。

具体实施方式

[0027] 下面将结合附图对本发明技术方案的实施例进行详细的描述。以下实施例仅用于更加清楚地说明本发明的技术方案，因此只作为示例，而不能以此来限制本发明的保护范围。

[0028] 需要注意的是,除非另有说明,本申请使用的技术术语或者科学术语应当为本发明所属领域技术人员所理解的通常意义。

[0029] 如图1所示,一种高安全服务器密码机,包括以下内容:

[0030] 命令接口、加密模块、主控模块、加密模块,所述命令接口、加密模块均集成在所述主控模块上,所述命令接口用于获取目标设备的物理随机信号,所述加密模块与所述加密模块连接。

[0031] 命令接口可以是网络接口,网络接口包括但不限于RJ-45接口,RJ-11接口,SC光纤接口,FDDI接口,AUI接口,BNC接口,Console接口;第一类接口还可以是USB接口,USB接口包括但不限于USB1.1接口,USB2.0接口,USB3.0接口;加密模块可以是网络接口,网络接口包括但不限于RJ-45接口,RJ-11接口,SC光纤接口,FDDI接口,AUI接口,BNC接口,Console接口;第一类接口还可以是USB接口,USB接口包括但不限于USB1.1接口,USB2.0接口,USB3.0接口;加密模块的数量根据实际需要进行设置,在此不做限制。

[0032] 更为具体的,所述加密模块包括第一随机数发生器、第二随机数发生器、Hopfield神经网络模块、密钥库,所述第一随机数发生器基于物理随机信号生成第一随机数,所述Hopfield神经网络模块包括多个离散的Hopfield神经网络电路,其中每个离散的Hopfield神经网络电路与一位第一随机数一一对应,所述每个离散的Hopfield神经网络电路生成表征数据集,所述表征数据集用于生成接收到的一位第一随机数在当前t时刻的表征信号,所述第二随机数发生器根据表征信号生成真随机数,所述密钥库用于对随机数进行加密,得到加密随机数。

[0033] 第一随机数发生器采用目标设备电子元件中的噪音等物理过程生成第一随机数,而第一随机数受温度、时间、电压、压力、音频等环境因素影响,在持续不变的环境下,容易在短时间内生成重复的物理噪声,产生相同的随机数,所以采用离散的Hopfield神经网络电路生成数据特征均不相同的表征数据集;

[0034] 将第一随机数与表征数据集结合,生成各不相同的表征信号,此步骤的作用在于,表征数据难以直接作为输入导入随机数发生器中得出随机数,所以采用第一随机数生成一串可能存在重复的随机数,将该随机数与各不相同的表征数据结合,得出各不相同的表征信号,再将表征信号导入第二随机数发生器中作为输入,保障第二随机数发生器中生成的随机数均为真随机数。

[0035] 如图2所示,更为具体的,所述Hopfield神经网络模块的生成表征数据集的步骤包括:

[0036] 步骤1:预设虚拟物理信号,对虚拟物理信号训练生成表征任务,并得出对应的任务样本集;

[0037] 步骤2:在任务样本集可用的情况下,对每个任务数据集提取最优价值数据进行保留,得出表征数据集。

[0038] 更为具体的,所述任务样本集可用的情况为:样本集中的样本均各不相同。

[0039] 预设虚拟物理信号的步骤,在密码机开始加解密的过程之前,将表征数据集的制作过程与加解密的过程进行隔离,降低加解密过程中的数据回溯轮询时间,有效提升密码机的密钥检验效率,表征数据集中具备有完善且数据量足够多的任务数据。

[0040] 更为具体的,所述命令接口接收第一个随机信号到最后一个随机信号的时间间隔

称为Hopfield神经网络学习的一个时间栈，所述Hopfield神经网络随着时间栈的变化修改表征数据集，在第N个时间栈中，所述Hopfield神经网络访问N号表征数据集。

[0041] 在第N个时间栈中，命令接口接收到第k个信号后开始计时，若计时时长超出设定范围后仍无下一个随机信号输入，则设第k个信号为第N个时间栈的最后一个随机信号；

[0042] 若在计时时长超出设定范围后，命令接口接收到随机信号，则以该信号作为第N+1个时间栈的第一个随机信号。

[0043] 更为具体的，所述Hopfield神经网络模块随着时间栈变化修改表征数据集的步骤包括：

[0044] 步骤3：在第N-1个时间栈结束后，预设虚拟物理信号，对虚拟物理信号训练生成N号表征任务，并得出对应的N号任务样本集；在任务样本集可用的情况下，对每个任务数据集提取最优价值数据进行保留，得出N号表征数据集；

[0045] 步骤4：在第N个时间栈结束后，预设虚拟物理信号，对虚拟物理信号训练生成N+1号表征任务，并得出对应的N+1号任务样本集，将N号表征任务的表征数据集加入该任务样本集中，在N+1号任务样本集可用的情况下，对每个任务数据集提取最优价值数据进行保留，得出N+1号表征数据集。

[0046] 在虚拟物理信号训练完成后，且新的任务样本集可用时，如果直接将表征数据集用于下一个时间栈的随机数生成，会使下一个时间栈的随机数生成结果偏向于新数据的分布，从而难以避免与前面若干时间栈产生重合。为了缓解这一现象，在生成N+1号表征任务时，旧任务N号表征任务的表征数据集将与N+1号任务样本集共同参与训练，在保留旧任务知识的同时，防止数据产生重合。

[0047] 更为具体的，所述最优价值的数据的提取步骤包括：

[0048] 步骤a：依据N号表征数据集，获取N号表征任务所对应的特征抓取器，采用特征抓取器抓取N+1号样本数据中所有样本数据的特征；

[0049] 步骤b：根据所抓取的多个样本数据特征，为每一类样本数据计算特征均值，并计算多个样本数据特征与特征均值的欧几里得距离；

[0050] 步骤c：保留欧几里得距离最小的样本数据特征所对应的m个样本数据。

[0051] 更为具体的，所述第一随机数发生器和/或第二随机数发生器为热噪声随机数发生器、振荡采样随机数发生器、亚稳态随机数发生器或混沌随机数发生器中的一种或多种。

[0052] 更为具体的，所述主控模块用于接收目标设备通过命令接口发送的任务请求，并通过加密模块将所述任务数据发送至与集线器连接的加密模块，其中，所述任务请求包含任务类型以及任务数据。

[0053] 当所述任务类型为加密业务时，所述加密模块对所述任务类型进行加密处理，得到加密信息，并将所述加密信息通过集线器以及加密模块发送给主控模块，所述主控模块接收到所述加密信息后，通过所述命令接口将所述加密信息发送给所述目标设备；

[0054] 当所述任务类型为解密业务时，所述加密芯片对所述任务数据进行解密处理，得到解密信息，并将所述解密信息通过集线器以及加密模块发送给主控模块，所述主控模块接收到所述解密信息后，通过所述命令接口将所述解密信息发送给所述目标设备。

[0055] 最后应说明的是：以上各实施例仅用以说明本发明的技术方案，而非对其限制；尽管参照前述各实施例对本发明进行了详细的说明，本领域的普通技术人员应当理解：其依

然可以对前述各实施例所记载的技术方案进行修改,或者对其中部分或者全部技术特征进行等同替换;而这些修改或者替换,并不使相应技术方案的本质脱离本发明各实施例技术方案的范围,其均应涵盖在本发明的权利要求和说明书的范围当中。

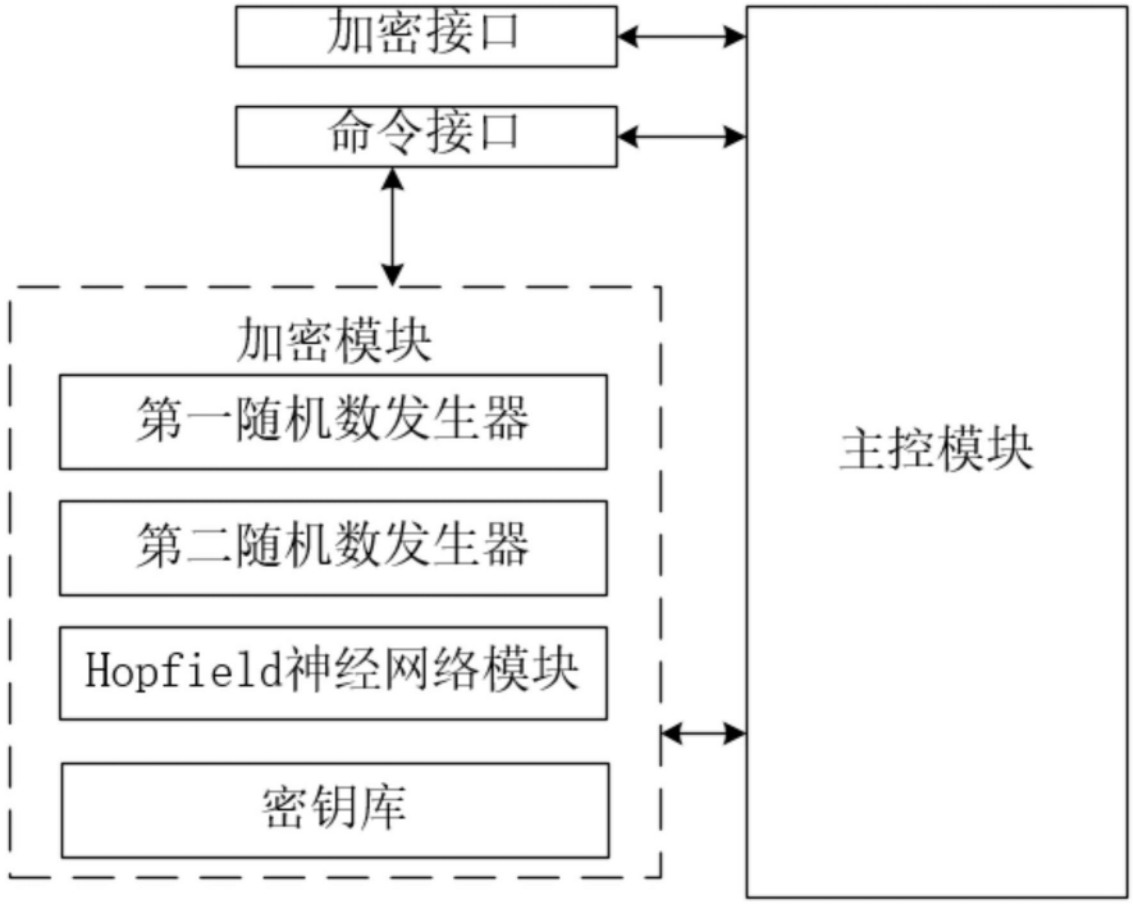
加密接口
命令接口
加密模块
第一随机数发生器
第二随机数发生器
Hopfield神经网络模块
密钥库
主控模块

图1

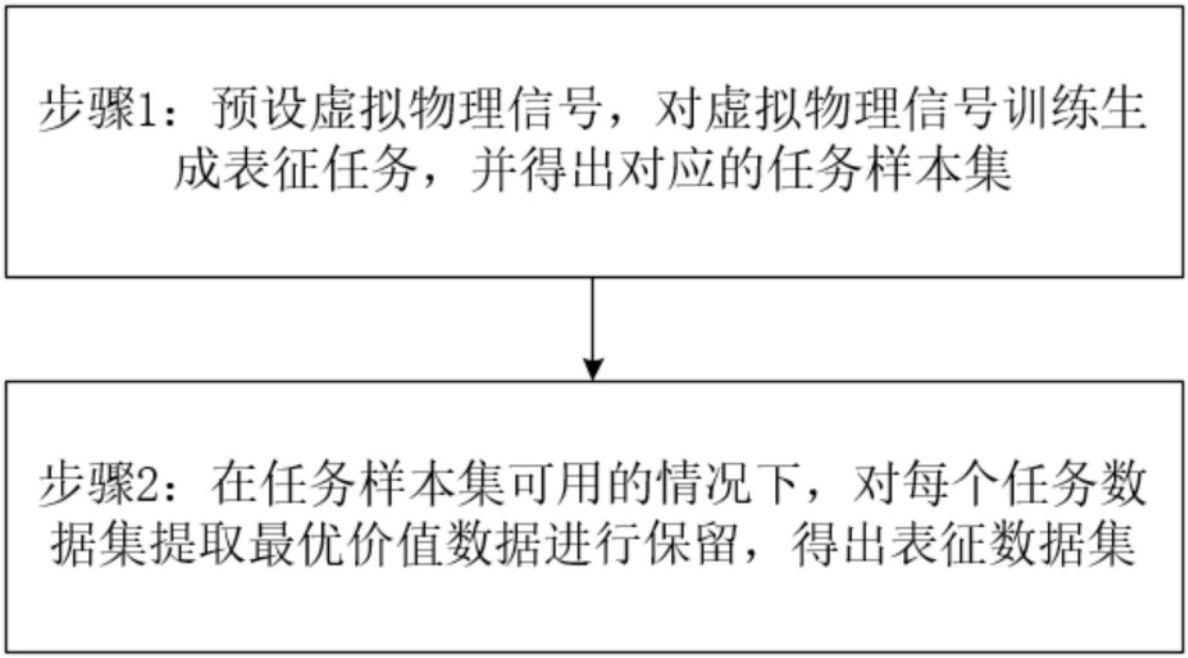
步骤1：预设虚拟物理信号，对虚拟物理信号训练生成表征任务，并得出对应的任务样本集
步骤2：在任务样本集可用的情况下，对每个任务数据集提取最优价值数据进行保留，得出表征数据集

图2