(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 110069931 A
(43)申请公布日 2019.07.30

(21)申请号 201910366795.0

(22)申请日 2019.05.05

(71)申请人 济南浪潮高新科技投资发展有限公司

地址 250100 山东省济南市高新区孙村镇科航路2877号研发楼一楼

(72)发明人 于晓艳 田梦哲 刘强

(74)专利代理机构 济南信达专利事务所有限公司 37100

代理人 姜明

(51)Int.Cl.

G06F 21/57(2013.01)
G06F 21/60(2013.01)
G06F 8/65(2018.01)
H04L 9/08(2006.01)

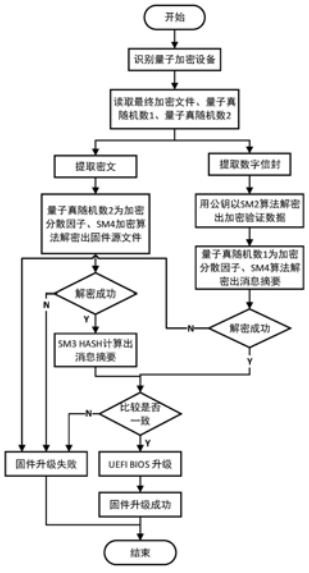
权利要求书2页 说明书4页 附图2页

(54)发明名称

一种基于量子加密的UEFI BIOS系统安全升级方法

(57)摘要

本发明特别涉及一种基于量子加密的UEFI BIOS系统安全升级方法。该基于量子加密的UEFI BIOS系统安全升级方法，包括UEFI固件源文件在量子加密设备中的加密存储和在UEFI系统主机中的解密升级两部分，结合使用量子力学固有的高随机性的量子真随机数，对消息摘要和UEFI固件源文件进行加密，文件解密后将解密出的消息摘要进行比较验证，如果验证通过则进行UEFI固件升级操作，如果验证未通过则退出升级过程升级失败。该基于量子加密的UEFI BIOS系统安全升级方法，结合使用量子力学固有的不确定性、不可预测、不可推导等特性的高随机性的量子真随机数，提高了UEFI系统固件升级的安全性。



CN 110069931 A

1.一种基于量子加密的UEFI BIOS系统安全升级方法,其特征在于:包括UEFI固件源文件在量子加密设备中的加密存储和在UEFI系统主机中的解密升级两部分,结合使用量子力学固有的高随机性的量子真随机数,对消息摘要和UEFI固件源文件进行加密,文件解密后将解密出的消息摘要进行比较验证,如果验证通过则进行UEFI固件升级操作,如果验证未通过则退出升级过程升级失败。

2.根据权利要求1所述的基于量子加密的UEFI BIOS系统安全升级方法,其特征在于:所述UEFI固件源文件在量子加密设备中的加密存储是指在量子加密设备中将消息摘要进行基于量子真随机数的加密和秘钥加密的双重加强加密过程,UEFI固件源文件也进行基于量子真随机数的加密。

3.根据权利要求1所述的基于量子加密的UEFI BIOS系统安全升级方法,其特征在于:所述在UEFI系统主机中的解密升级是指在UEFI系统主机中,增加UEFI具有识别量子加密设备和读取加密文件及加密因子,进行解密操作功能的驱动,进行文件解密和验证,如果验证通过则进行UEFI固件升级操作,如果验证未通过则退出升级过程升级失败。

4.根据权利要求2所述的基于量子加密的UEFI BIOS系统安全升级方法,其特征在于:所述量子加密设备产生两个量子真随机数,量子真随机数是利用量子力学固有的不确定性所得到的,具有不可预测和推导的特性,能够增强系统升级的安全性。

5.根据权利要求2所述的基于量子加密的UEFI BIOS系统安全升级方法,其特征在于:所述UEFI固件源文件在量子加密设备中的加密存储,包括以下步骤:

(1)增加安全信息层,使用国产哈希算法SM3HASH计算UEFI固件源文件成消息摘要;使用SM4国密算法以量子加密设备中量子真随机数发生器产生的量子真随机数1为加密分散因子,加密消息摘要为加密验证数据;相对于传统加密方法增加两层加密操作。

(2)用量子加密设备产生的安全秘钥对的私钥使用SM2算法将加密验证数据加密为数字信封;

(3)使用SM4国密算法以量子加密设备中量子真随机数发生器产生的量子真随机数2为加密分散因子,加密UEFI固件源文件为密文;

(4)组合处理加密验证数据和密文为最终加密文件。

6.根据权利要求3所述的基于量子加密的UEFI BIOS系统安全升级方法,其特征在于:所述在UEFI系统主机中的解密升级过程选择UEFI的DXE阶段为解密认证阶段,按照UEFI规范标准开发DXE驱动为具有识别量子加密设备和读取加密文件及加密因子,进行解密操作的功能。

7.根据权利要求6所述的基于量子加密的UEFI BIOS系统安全升级方法,其特征在于:所述在UEFI系统主机中的解密升级,包括以下步骤:

(1)读取量子加密设备中的最终加密文件、量子真随机数1和量子真随机数2,数据处理分别提取密文和数字信封;

(2)用量子加密设备发布的秘钥对的公钥使用SM2算法从数字信封中解密出加密验证数据,再以量子加密设备中的量子真随机数1为加密分散因子以SM4算法解密出UEFI固件源文件的消息摘要,如果解密失败则停止固件升级操作升级失败;

(3)对于密文以量子加密设备中的量子真随机数2为加密分散因子以SM4算法解密出UEFI固件源文件,如果解密失败则退出固件升级过程升级失败;

(4)使用国产哈希算法SM3HASH计算解密出的UEFI固件源文件的消息摘要,并将解密出的消息摘要与步骤(2)解密出的消息摘要比较验证,如果验证通过则进行UEFI固件升级操作,如果验证未通过则退出升级过程升级失败。

8.根据权利要求1～7任意一项所述的基于量子加密的UEFI BIOS系统安全升级方法,其特征在于,包括以下步骤:

1)量子加密设备连接UEFI系统主机,主机启动识别量子加密设备,并建立通信;

2)读取量子加密设备中的最终加密文件、量子真随机数1和量子真随机数2;

3)分别提取密文和数字信封;

4)用量子加密设备发布的秘钥对的公钥使用SM2算法从数字信封中解密出加密验证数据,再以量子加密设备中的量子真随机数1为加密分散因子以SM4算法解密出UEFI固件源文件的消息摘要;

5)以量子加密设备中的量子真随机数2为加密分散因子以SM4算法解密密文得到UEFI固件源文件;

6)使用国产哈希算法SM3HASH计算解密出的UEFI固件源文件的消息摘要。

7)步骤6)解密出的消息摘要与步骤4)解密出的消息摘要进行比较验证,如果验证通过,则进行UEFI固件升级操作;

8)升级成功,操作结束。

一种基于量子加密的UEFI BIOS系统安全升级方法

技术领域

[0001] 本发明涉及UEFI固件系统和量子加密安全技术领域,特别涉及一种基于量子加密的UEFI BIOS系统安全升级方法。

背景技术

[0002] 量子计算机(Quantum Computer)是一类遵循量子力学规律进行高速数学和逻辑运算、存储及处理量子信息的物理装置。近年来,由于量子计算的叠加、纠缠等特性带来的并行快速计算特点,以及量子的不可测量、不确定性等特性,在科学应用中都带来强大的应用价值,因而使得量子计算技术发展迅速。

[0003] 量子计算机的作用还远不止是解决一些经典计算机无法解决的问题,与经典计算机相比,量子计算机最重要的优越性体现在量子并行计算上,理论上来看已经远超目前世界上最快的超级计算机。通用量子计算机一旦实现,将对通信安全、导航、成像以及人工智能、生物制药、新材料研发等诸多领域产生颠覆性影响,带来国家安全和社会经济发展的极大变革。

[0004] 同时UEFI(Unified Extensible Firmware Interface,统一的可扩展固件接口)系统的开发效率高、可扩展性强、性能提升、启动快、以及安全性强等特点,也使UEFI发展迅速,并逐步替代传统BIOS(Basic Input/Output System,基本输入/输出系统)系统。

[0005] 基于此,本发明提出了一种基于量子加密的UEFI BIOS系统安全升级方法。

发明内容

[0006] 本发明为了弥补现有技术的缺陷,提供了一种简单高效的基于量子加密的UEFI BIOS系统安全升级方法。

[0007] 本发明是通过如下技术方案实现的:

[0008] 一种基于量子加密的UEFI BIOS系统安全升级方法,其特征在于:包括UEFI固件源文件在量子加密设备中的加密存储和在UEFI系统主机中的解密升级两部分,结合使用量子力学固有的高随机性的量子真随机数,对消息摘要和UEFI固件源文件进行加密,文件解密后将解密出的消息摘要进行比较验证,如果验证通过则进行UEFI固件升级操作,如果验证未通过则退出升级过程升级失败。

[0009] 所述UEFI固件源文件在量子加密设备中的加密存储是指在量子加密设备中将消息摘要进行基于量子真随机数的加密和秘钥加密的双重加强加密过程,UEFI固件源文件也进行基于量子真随机数的加密。

[0010] 所述在UEFI系统主机中的解密升级是指在UEFI系统主机中,增加UEFI具有识别量子加密设备和读取加密文件及加密因子,进行解密操作功能的驱动,进行文件解密和验证,如果验证通过则进行UEFI固件升级操作,如果验证未通过则退出升级过程升级失败。

[0011] 所述量子加密设备产生两个量子真随机数,量子真随机数是利用量子力学固有的不确定性所得到的,具有不可预测和推导的特性,能够增强系统升级的安全性。

[0012] 所述UEFI固件源文件在量子加密设备中的加密存储,包括以下步骤:

[0013] (5)增加安全信息层,使用国产哈希算法SM3 HASH计算UEFI固件源文件成消息摘要;使用SM4国密算法以量子加密设备中量子真随机数发生器产生的量子真随机数1为加密分散因子,加密消息摘要为加密验证数据;相对于传统加密方法增加两层加密操作。

[0014] (6)用量子加密设备产生的安全秘钥对的私钥使用SM2算法将加密验证数据加密为数字信封;

[0015] (7)使用SM4国密算法以量子加密设备中量子真随机数发生器产生的量子真随机数2为加密分散因子,加密UEFI固件源文件为密文;

[0016] (8)组合处理加密验证数据和密文为最终加密文件。

[0017] 所述在UEFI系统主机中的解密升级过程选择UEFI的DXE阶段为解密认证阶段,按照UEFI规范标准开发DXE驱动为具有识别量子加密设备和读取加密文件及加密因子,进行解密操作的功能。

[0018] 所述在UEFI系统主机中的解密升级,包括以下步骤:

[0019] (5)读取量子加密设备中的最终加密文件、量子真随机数1和量子真随机数2,数据处理分别提取密文和数字信封;

[0020] (6)用量子加密设备发布的秘钥对的公钥使用SM2算法从数字信封中解密出加密验证数据,再以量子加密设备中的量子真随机数1为加密分散因子以SM4算法解密出UEFI固件源文件的消息摘要,如果解密失败则停止固件升级操作升级失败;

[0021] (7)对于密文以量子加密设备中的量子真随机数2为加密分散因子以SM4算法解密出UEFI固件源文件,如果解密失败则退出固件升级过程升级失败;

[0022] (8)使用国产哈希算法SM3 HASH计算解密出的UEFI固件源文件的消息摘要,并将解密出的消息摘要与步骤(2)解密出的消息摘要比较验证,如果验证通过则进行UEFI固件升级操作,如果验证未通过则退出升级过程升级失败。

[0023] 该基于量子加密的UEFI BIOS系统安全升级方法,包括以下步骤:

[0024] 1)量子加密设备连接UEFI系统主机,主机启动识别量子加密设备,并建立通信;

[0025] 2)读取量子加密设备中的最终加密文件、量子真随机数1和量子真随机数2;

[0026] 3)分别提取密文和数字信封;

[0027] 4)用量子加密设备发布的秘钥对的公钥使用SM2算法从数字信封中解密出加密验证数据,再以量子加密设备中的量子真随机数1为加密分散因子以SM4算法解密出UEFI固件源文件的消息摘要;

[0028] 5)以量子加密设备中的量子真随机数2为加密分散因子以SM4算法解密密文得到UEFI固件源文件;

[0029] 6)使用国产哈希算法SM3 HASH计算解密出的UEFI固件源文件的消息摘要。

[0030] 7)步骤6)解密出的消息摘要与步骤4)解密出的消息摘要进行比较验证,如果验证通过,则进行UEFI固件升级操作;

[0031] 8)升级成功,操作结束。

[0032] 本发明的有益效果是:该基于量子加密的UEFI BIOS系统安全升级方法,结合使用量子力学固有的不确定性、不可预测、不可推导等特性的高随机性的量子真随机数,提高了UEFI系统固件升级的安全性。

附图说明

[0033] 附图1为本发明基于量子加密的UEFI BIOS系统安全升级模块示意图。

[0034] 附图2为本发明基于量子加密的UEFI BIOS系统安全升级方法示意图。

具体实施方式

[0035] 为了使本发明所要解决的技术问题、技术方案及有益效果更加清楚明白，以下结合实施例，对本发明进行详细的说明。应当说明的是，此处所描述的具体实施例仅用以解释本发明，并不用于限定本发明。

[0036] 该基于量子加密的UEFI BIOS系统安全升级方法，包括UEFI固件源文件在量子加密设备中的加密存储和在UEFI系统主机中的解密升级两部分，结合使用量子力学固有的高随机性的量子真随机数，对消息摘要和UEFI固件源文件进行加密，文件解密后将解密出的消息摘要进行比较验证，如果验证通过则进行UEFI固件升级操作，如果验证未通过则退出升级过程升级失败。

[0037] 所述UEFI固件源文件在量子加密设备中的加密存储是指在量子加密设备中将消息摘要进行基于量子真随机数的加密和秘钥加密的双重加强加密过程，UEFI固件源文件也进行基于量子真随机数的加密。

[0038] 所述在UEFI系统主机中的解密升级是指在UEFI系统主机中，增加UEFI具有识别量子加密设备和读取加密文件及加密因子，进行解密操作功能的驱动，进行文件解密和验证，如果验证通过则进行UEFI固件升级操作，如果验证未通过则退出升级过程升级失败。

[0039] 所述量子加密设备产生两个量子真随机数，量子真随机数是利用量子力学固有的不确定性所得到的，具有不可预测和推导的特性，能够增强系统升级的安全性。

[0040] 所述UEFI固件源文件在量子加密设备中的加密存储，包括以下步骤：

[0041] (9)增加安全信息层，使用国产哈希算法SM3 HASH计算UEFI固件源文件成消息摘要；使用SM4国密算法以量子加密设备中量子真随机数发生器产生的量子真随机数1为加密分散因子，加密消息摘要为加密验证数据；相对于传统加密方法增加两层加密操作。

[0042] (10)用量子加密设备产生的安全秘钥对的私钥使用SM2算法将加密验证数据加密为数字信封；

[0043] (11)使用SM4国密算法以量子加密设备中量子真随机数发生器产生的量子真随机数2为加密分散因子，加密UEFI固件源文件为密文；

[0044] (12)组合处理加密验证数据和密文为最终加密文件。

[0045] 所述在UEFI系统主机中的解密升级过程选择UEFI的DXE阶段为解密认证阶段，按照UEFI规范标准开发DXE驱动为具有识别量子加密设备和读取加密文件及加密因子，进行解密操作的功能。

[0046] 所述在UEFI系统主机中的解密升级，包括以下步骤：

[0047] (9)读取量子加密设备中的最终加密文件、量子真随机数1和量子真随机数2，数据处理分别提取密文和数字信封；

[0048] (10)用量子加密设备发布的秘钥对的公钥使用SM2算法从数字信封中解密出加密验证数据，再以量子加密设备中的量子真随机数1为加密分散因子以SM4算法解密出UEFI固件源文件的消息摘要，如果解密失败则停止固件升级操作升级失败；

[0049] (11)对于密文以量子加密设备中的量子真随机数2为加密分散因子以SM4算法解密出UEFI固件源文件,如果解密失败则退出固件升级过程升级失败;

[0050] (12)使用国产哈希算法SM3 HASH计算解密出的UEFI固件源文件的消息摘要,并将解密出的消息摘要与步骤(2)解密出的消息摘要比较验证,如果验证通过则进行UEFI固件升级操作,如果验证未通过则退出升级过程升级失败。

[0051] 该基于量子加密的UEFI BIOS系统安全升级方法,包括以下步骤:

[0052] 1)量子加密设备连接UEFI系统主机,主机启动识别量子加密设备,并建立通信;

[0053] 2)读取量子加密设备中的最终加密文件、量子真随机数1和量子真随机数2;

[0054] 3)分别提取密文和数字信封;

[0055] 4)用量子加密设备发布的秘钥对的公钥使用SM2算法从数字信封中解密出加密验证数据,再以量子加密设备中的量子真随机数1为加密分散因子以SM4算法解密出UEFI固件源文件的消息摘要;

[0056] 5)以量子加密设备中的量子真随机数2为加密分散因子以SM4算法解密密文得到UEFI固件源文件;

[0057] 6)使用国产哈希算法SM3 HASH计算解密出的UEFI固件源文件的消息摘要。

[0058] 7)步骤6)解密出的消息摘要与步骤4)解密出的消息摘要进行比较验证,如果验证通过,则进行UEFI固件升级操作;

[0059] 8)升级成功,操作结束。

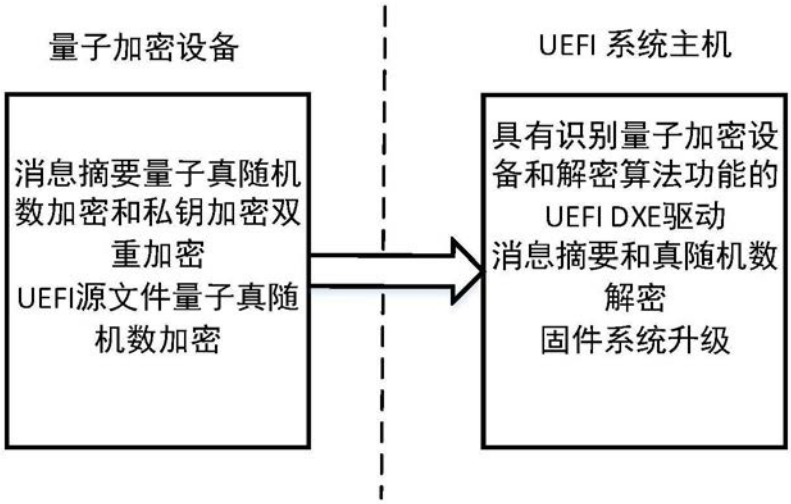

量子加密设备
UEFI 系统主机
消息摘要量子真随机数加密和私钥加密双重加密
UEFI源文件量子真随机数加密
具有识别量子加密设备和解密算法功能的UEFI DXE驱动
消息摘要和真随机数解密
固件系统升级

图1

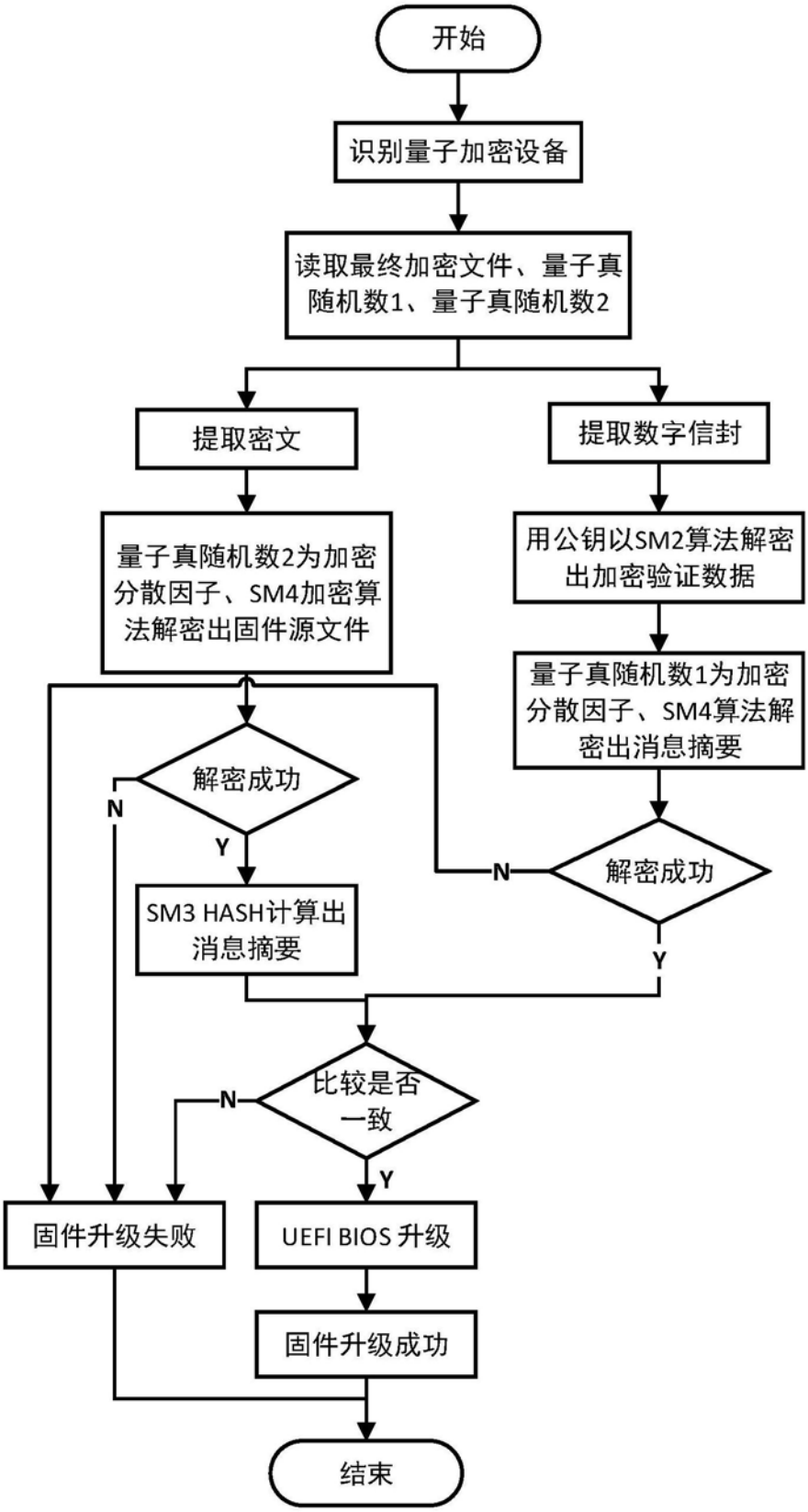

开始
识别量子加密设备
读取最终加密文件、量子真随机数1、量子真随机数2
提取密文
提取数字信封
量子真随机数2为加密分散因子、SM4加密算法解密出固件源文件
用公钥以SM2算法解密出加密验证数据
量子真随机数1为加密分散因子、SM4算法解密出消息摘要
解密成功
N
Y
SM3 HASH计算出消息摘要
N
解密成功
Y
比较是否一致
N
Y
固件升级失败
UEFI BIOS 升级
固件升级成功
结束

图2