(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 104317552 B
(45)授权公告日 2018.04.13

(21)申请号 201410623403.1

(22)申请日 2014.11.06

(65)同一申请的已公布的文献号
申请公布号 CN 104317552 A

(43)申请公布日 2015.01.28

(73)专利权人 合肥濯新光电科技有限公司
地址 230001 安徽省合肥市蜀山区望江西路123号幸福里22幢2406室

(72)发明人 龚明 王茁 詹丽华 鲁礼云 李超君

(74)专利代理机构 合肥市浩智运专利代理事务所(普通合伙) 34124
代理人 方荣肖

(51)Int.Cl.
G06F 7/58(2006.01)
H04L 9/06(2006.01)

(56)对比文件
CN 103929301 A,2014.07.16,
CN 101997834 A,2011.03.30,
CN 101355422 A,2009.01.28,
CN 103929301 A,2014.07.16,
EP 2796989 A2,2014.10.29,
CN 101938351 A,2011.01.05,
CN 102158338 A,2011.08.17,
CN 102541509 A,2012.07.04,
WO 98/06175 A1,1998.02.12,

审查员 吕鑫

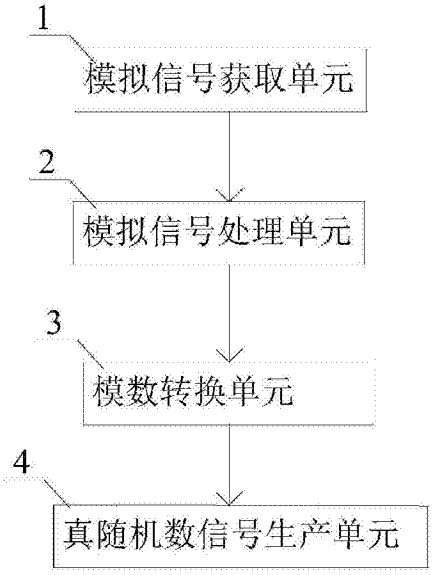
权利要求书3页 说明书7页 附图2页

(54)发明名称

真随机数发生器及方法、真随机数密钥加密系统及方法

(57)摘要

本发明公开了真随机数发生器及方法、真随机数密钥加密系统及方法。该真随机数发生器包括:模拟信号获取单元,使用一个或多个自然界中的物理现象获取模拟信号;模拟信号处理单元,对一个或多个该模拟信号进行处理,获得处理后的模拟信号;模数转换单元,对处理后的模拟信号进行放大和模数转换得到数字信号;真随机数信号生产单元,对数字信号进行处理,生成真随机数信号:计算数字信号的自相关函数,根据自相关函数计算出数字信号的功率谱,根据该功率谱计算出白化滤波器的频谱作为该真随机数信号。



CN 104317552 B

1.一种真随机数发生器,其包括:

模拟信号获取单元,使用一个或多个自然界中的物理现象获取模拟信号;

模拟信号处理单元,对一个或多个该模拟信号进行处理,获得处理后的模拟信号;

模数转换单元,对该处理后的模拟信号进行放大和模数转换,得到数字信号;

真随机数信号生产单元,对该数字信号进行处理,生成真随机数信号;

其特征在于:

该真随机数信号生产单元对该数字信号进行白化处理:计算该数字信号的自相关函数$G^{+}_{x}(\omega)$,根据该自相关函数$G^{+}_{x}(\omega)$计算出该数字信号的功率谱$H_1(s)$,将功率谱$H_1(s)$分解成在s的左半平面和后半平面,取功率谱在s的左半平面的那些值,找出零、极点,根据公式$G_x^+(\omega)=\left[\alpha\frac{(j\omega+\alpha_1)\cdots(j\omega+\alpha_k)}{(j\omega+\beta_1)\cdots(j\omega+\beta_l)}\right]$和$H_1(s)=\frac{1}{G_x^+(s)}$计算出白化滤波器的频谱作为该真随机数信号。

2.如权利要求1所述的真随机数发生器,其特征在于:该模拟信号获取单元利用电阻器件生成该模拟信号:测量该电阻器件上的自由电子的布朗运动引起的电流,作为该模拟信号;或利用晶体管生成该模拟信号:测量该晶体管的电子不规则热运动引起的电流,作为该模拟信号;或记录自然界中的声音,作为模拟信号。

3.如权利要求1所述的真随机数发生器,其特征在于:该模拟信号处理单元将该模拟信号的不同位置的信号进行相加,相乘处理,获得处理后的模拟信号;或将多个模拟信号的不同位置的信号进行相加,相乘处理,获得处理后的模拟信号。

4.一种真随机数生产方法,其包括以下步骤:

(1)使用一个或多个自然界中的物理现象获取模拟信号;

(2)对一个或多个该模拟信号进行处理,获得处理后的模拟信号;

(3)对该处理后的模拟信号进行放大和模数转换,得到数字信号;

(4)对该数字信号进行处理,生成真随机数信号;其特征在于:

在步骤(1)中,利用电阻器件生成该模拟信号:测量该电阻器件上的自由电子的布朗运动引起的电流,作为该模拟信号;或利用晶体管生成该模拟信号:测量该晶体管的电子不规则热运动引起的电流,作为该模拟信号;或记录自然界中的声音,作为模拟信号;

在步骤(2)中,将该模拟信号的不同位置的信号进行相加,相乘处理,获得处理后的模拟信号;或将多个模拟信号的不同位置的信号进行相加,相乘处理,获得处理后的模拟信号;

在步骤(4)中,对该数字信号进行白化处理:计算该数字信号的自相关函数$G^{+}_{x}(\omega)$,根据该自相关函数$G^{+}_{x}(\omega)$计算出该数字信号的功率谱$H_1(s)$,将功率谱$H_1(s)$分解成在s的左半平面和后半平面,取功率谱在s的左半平面的那些值,找出零、极点,根据公式$G_x^+(\omega)=\left[\alpha\frac{(j\omega+\alpha_1)\cdots(j\omega+\alpha_k)}{(j\omega+\beta_1)\cdots(j\omega+\beta_l)}\right]$和$H_1(s)=\frac{1}{G_x^+(s)}$计算出白化滤波器的频谱作为该真随机数信号。

5.一种真随机数发生器,其包括:

模拟信号获取单元,使用一个或多个自然界中的物理现象获取模拟信号;

模数转换单元，对该模拟信号进行放大和模数转换，得到数字信号；

数字信号处理单元，对该数字信号进行处理，获得处理后的数字信号；

真随机数信号生产单元，对该处理后的数字信号进行处理，生成真随机数信号；其特征在于：

该真随机数信号生产单元对该处理后的数字信号进行白化处理：计算该数字信号的自相关函数$G^{+}_{x}(\omega)$，根据该自相关函数$G^{+}_{x}(\omega)$计算出该数字信号的功率谱$H_1(s)$，将功率谱$H_1(s)$分解成在s的左半平面和后半平面，取功率谱在s的左半平面的那些值，找出零、极点，根据公式$G_x^+(\omega)=\left[\alpha\frac{(j\omega+\alpha_1)\cdots(j\omega+\alpha_k)}{(j\omega+\beta_1)\cdots(j\omega+\beta_l)}\right]$和$H_1(s)=\frac{1}{G_x^+(s)}$计算出白化滤波器的频谱作为该真随机数信号。

6.如权利要求5所述的真随机数发生器，其特征在于：该模拟信号获取单元利用电阻器件生成该模拟信号：测量该电阻器件上的自由电子的布朗运动引起的电流，作为该模拟信号；或利用晶体管生成该模拟信号：测量该晶体管的电子不规则热运动引起的电流，作为该模拟信号；或记录自然界中的声音，作为模拟信号。

7.如权利要求5所述的真随机数发生器，其特征在于：该数字信号处理单元将该数字信号的不同位置的信号进行相加，相乘处理，获得该处理后的数字信号；或将多个该数字信号的不同位置的信号进行相加，相乘处理，获得该处理后的数字信号。

8.一种真随机数生产方法，其包括以下步骤：

(1)使用一个或多个自然界中的物理现象获取模拟信号；

(2)对该模拟信号进行放大和模数转换，得到数字信号；

(3)对该数字信号进行处理，获得处理后的数字信号；

(4)对该处理后的数字信号进行处理，生成真随机数信号；其特征在于：

在步骤(1)中，利用电阻器件生成该模拟信号：测量该电阻器件上的自由电子的布朗运动引起的电流，作为该模拟信号；或利用晶体管生成该模拟信号：测量该晶体管的电子不规则热运动引起的电流，作为该模拟信号；或记录自然界中的声音，作为模拟信号；

在步骤(2)中，将该数字信号的不同位置的信号进行相加，相乘处理，获得该处理后的数字信号；或将多个该数字信号的不同位置的信号进行相加，相乘处理，获得该处理后的数字信号；

在步骤(4)中，对该处理后的数字信号进行白化处理：计算该数字信号的自相关函数$G^{+}_{x}(\omega)$，根据该自相关函数$G^{+}_{x}(\omega)$计算出该数字信号的功率谱$H_1(s)$，将功率谱$H_1(s)$分解成在s的左半平面和后半平面，取功率谱在s的左半平面的那些值，找出零、极点，根据公式$G_x^+(\omega)=\left[\alpha\frac{(j\omega+\alpha_1)\cdots(j\omega+\alpha_k)}{(j\omega+\beta_1)\cdots(j\omega+\beta_l)}\right]$和$H_1(s)=\frac{1}{G_x^+(s)}$计算出白化滤波器的频谱作为该真随机数信号。

9.一种真随机数密钥加密系统，其包括可分发存储介质、真随机数发生器、防火墙和专用数据加解密机构，其特征在于：该真随机数发生器为如权利要求1至3、权利要求5至7中任意一项所述的真随机数发生器，该防火墙为光纤单向数据隔离防火墙；该真随机数发生器产生真随机数信号输送至该可分发存储介质进行存储作为密钥，该专用数据加解密机构透

过该光纤单向数据隔离防火墙向该可分发存储介质获取该密钥用于加密；该可分发存储介质将该密钥以模块化方式储存：将采集到的二进制随机数存储，每一定容量为一个模块，其索引为模块序号。

10.一种真随机数密钥加密方法，其应用于如权利要求9所述的真随机数密钥加密系统中，其特征在于：该真随机数密钥加密方法包括以下步骤：

将该真随机数信号进行存储作为密钥，存储时将该密钥以模块化方式储存：将采集到的二进制随机数存储，每一定容量为一个模块，其索引为模块序号。

真随机数发生器及方法、真随机数密钥加密系统及方法

技术领域

[0001] 本发明涉及一种真随机数发生器及该真随机数发生器的真随机数生成方法、应用该真随机数发生器的真随机数密钥加密系统、该真随机数密钥加密系统的加密方法。

背景技术

[0002] 随着信息化的高速发展，人们对信息安全的需求越来越多。人员流动、市场竞争、金融危机、敌对势力等都给企事业单位的发展带来巨大风险，内部窃密、黑客攻击、无意识泄密等窃密手段成为了人与人之间、企业与企业之间、国与国之间的安全隐患。传统的人传递信息，虽然可靠性高、但时效性低，影响信息处理等的后续工作。因此加密系统的研究与发展显得尤为重要。

[0003] 在加密应用中，经常用到随机数作为密钥。因此，随机数广泛应用于密码学中。现有随机数有两种，如下介绍。

[0004] 1.伪随机数：它是由算法计算得出的，是可以预测的，也就是说当随机种子相同时，对于同一个随机函数，得出的随机数列是固定不变的。伪随机数的生成方法有：取中法，移位法和同余。

[0005] 2.真随机数：想要实现真随机数靠程序是永远无法实现的，很多情况下只能利用一些物理现象，比如布朗运动，量子效应，放射性衰变等。如以下介绍。

[0006] 2.1振荡器采样：利用热噪声放大后，影响一个由电压控制的振荡器，通过另一个高频振荡器来收集数据。

[0007] 2.2直接放大电路噪声：利用电路中各种噪声，如上述的热噪声作为随机源，对其放大，然后对一定时间内超过阈值的数据进行统计，这样就产生的随机数。

[0008] 2.3电路亚稳态：亚稳态表示触发器无法在规定时间内达到一个可确认状态，一定条件下，触发器达到两个稳态的几率为50％，所以先使电路进入亚稳态，之后根据状态转化为随机数。

[0009] 2.4混沌电路：不可预测，对初始条件的敏感的依赖性。以及混沌电路在芯片中易于实现的特点，可以产生效果不错的随机数。

[0010] 2.5利用物理信息，如宇宙射线，粒子衰变，空气噪声等作为随机源，来产生随机数。

[0011] 然而以上随机数存在如下问题。

[0012] (1)伪随机数不真正地随机，它们实际上是可以计算出来的，一旦知道生成方法和一些参数(例如随机数种子)，就可得到完全相同的伪随机数，从而进行密码破译。因此伪随机数不宜在密码学中应用。

[0013] (2)真随机数：真随机数发生器可能无法确定分布，无法保证平稳和数据间的独立性，给破译带来可能。

发明内容

[0014] 有鉴于此，本发明提供一种真随机数发生器及该真随机数发生器的真随机数生成方法、应用该真随机数发生器的真随机数密钥加密系统、该真随机数密钥加密系统的加密方法，其使用超级长度的真随机数作为数据文件的加密密钥，秘钥数据绝无任何规律可循。

[0015] 本发明是这样实现的，一种真随机数发生器，其包括：

[0016] 模拟信号获取单元，使用一个或多个自然界中的物理现象获取模拟信号；

[0017] 模拟信号处理单元，对一个或多个该模拟信号进行处理，获得处理后的模拟信号；

[0018] 模数转换单元，对该处理后的模拟信号进行放大和模数转换，得到数字信号；

[0019] 真随机数信号生产单元，对该数字信号进行处理，生成真随机数信号；

[0020] 其中，该真随机数信号生产单元对该数字信号进行白化处理：计算该数字信号的自相关函数，根据该自相关函数计算出该数字信号的功率谱，根据该功率谱计算出白化滤波器的频谱作为该真随机数信号。

[0021] 作为上述方案的进一步改进，该模拟信号获取单元利用电阻器件生成该模拟信号：测量该电阻器件上的自由电子的布朗运动引起的电流，作为该模拟信号；或利用晶体管生成该模拟信号：测量该晶体管的电子不规则热运动引起的电流，作为该模拟信号；或记录自然界中的声音，作为模拟信号。

[0022] 作为上述方案的进一步改进，该模拟信号处理单元将该模拟信号的不同位置的信号进行相加，相乘处理，获得处理后的模拟信号；或将多个模拟信号的不同位置的信号进行相加，相乘处理，获得处理后的模拟信号。

[0023] 本发明还提供一种真随机数生产方法，其包括以下步骤：

[0024] (1)使用一个或多个自然界中的物理现象获取模拟信号；

[0025] (2)对一个或多个该模拟信号进行处理，获得处理后的模拟信号；

[0026] (3)对该处理后的模拟信号进行放大和模数转换，得到数字信号；

[0027] (4)对该数字信号进行处理，生成真随机数信号；其特征在于：

[0028] 在步骤(1)中，利用电阻器件生成该模拟信号：测量该电阻器件上的自由电子的布朗运动引起的电流，作为该模拟信号；或利用晶体管生成该模拟信号：测量该晶体管的电子不规则热运动引起的电流，作为该模拟信号；或记录自然界中的声音，作为模拟信号；

[0029] 在步骤(2)中，将该模拟信号的不同位置的信号进行相加，相乘处理，获得处理后的模拟信号；或将多个模拟信号的不同位置的信号进行相加，相乘处理，获得处理后的模拟信号；

[0030] 在步骤(4)中，对该数字信号进行白化处理：计算该数字信号的自相关函数，根据该自相关函数计算出该数字信号的功率谱，根据该功率谱计算出白化滤波器的频谱作为该真随机数信号。

[0031] 本发明还提供另一种真随机数发生器，其包括：

[0032] 模拟信号获取单元，使用一个或多个自然界中的物理现象获取模拟信号；

[0033] 模数转换单元，对该模拟信号进行放大和模数转换，得到数字信号；

[0034] 数字信号处理单元，对该数字信号进行处理，获得处理后的数字信号；

[0035] 真随机数信号生产单元，对该处理后的数字信号进行处理，生成真随机数信号；其中：

[0036] 该真随机数信号生产单元对该处理后的数字信号进行白化处理：计算该处理后的

数字信号的自相关函数，根据该自相关函数计算出该处理后的数字信号的功率谱，根据该功率谱计算出白化滤波器的频谱作为该真随机数信号。

[0037] 作为上述方案的进一步改进，该模拟信号获取单元利用电阻器件生成该模拟信号：测量该电阻器件上的自由电子的布朗运动引起的电流，作为该模拟信号；或利用晶体管生成该模拟信号：测量该晶体管的电子不规则热运动引起的电流，作为该模拟信号；或记录自然界中的声音，作为模拟信号。

[0038] 作为上述方案的进一步改进，该数字信号处理单元将该数字信号的不同位置的信号进行相加，相乘处理，获得该处理后的数字信号；或将多个该数字信号的不同位置的信号进行相加，相乘处理，获得该处理后的数字信号。

[0039] 本发明还提供另一种真随机数生产方法，其包括以下步骤：

[0040] (1)使用一个或多个自然界中的物理现象获取模拟信号；

[0041] (2)对该模拟信号进行放大和模数转换，得到数字信号；

[0042] (3)对该数字信号进行处理，获得处理后的数字信号；

[0043] (4)对该处理后的数字信号进行处理，生成真随机数信号；其特征在于：

[0044] 在步骤(1)中，利用电阻器件生成该模拟信号：测量该电阻器件上的自由电子的布朗运动引起的电流，作为该模拟信号；或利用晶体管生成该模拟信号：测量该晶体管的电子不规则热运动引起的电流，作为该模拟信号；或记录自然界中的声音，作为模拟信号；

[0045] 在步骤(2)中，将该数字信号的不同位置的信号进行相加，相乘处理，获得该处理后的数字信号；或将多个该数字信号的不同位置的信号进行相加，相乘处理，获得该处理后的数字信号；

[0046] 在步骤(4)中，对该处理后的数字信号进行白化处理：计算该处理后的数字信号的自相关函数，根据该自相关函数计算出该处理后的数字信号的功率谱，根据该功率谱计算出白化滤波器的频谱作为该真随机数信号。

[0047] 本发明还提供一种真随机数密钥加密系统，其包括可分发存储介质、真随机数发生器、防火墙和专用数据加解密机构，其中，该真随机数发生器为上述任一真随机数发生器，该防火墙为光纤单向数据隔离防火墙；该真随机数发生器产生真随机数信号输送至该可分发存储介质进行存储作为密钥，该专用数据加解密机构透过该光纤单向数据隔离防火墙向该可分发存储介质获取该密钥用于加密；该可分发存储介质将该密钥以模块化方式储存：将采集到的二进制随机数存储，每一定容量为一个模块，其索引为模块序号。

[0048] 本发明还提供一种真随机数密钥加密方法，其应用于上述真随机数密钥加密系统中，该真随机数密钥加密方法包括以下步骤：将该真随机数信号进行存储作为密钥，存储时将该密钥以模块化方式储存：将采集到的二进制随机数存储，每一定容量为一个模块，其索引为模块序号。

[0049] 与现有技术相比，本发明的有益效果是使用超级长度的真随机数作为数据文件的加密密钥，秘钥数据绝无任何规律可循；使用超大容量存储介质(例如蓝光光盘)作为秘钥存储介质和分发介质，秘钥的长度足以保证在较长的使用时间内以逐字逐密的方式对大量明文数据进行加密处理；密钥以模块化方式存储，每个秘钥片段仅使用一次——每次加密和解密使用不重复的密钥片段。只要能确保用户端秘钥数据的安全就可以完全确保密文数据不可破译特性。

附图说明

[0050] 图1为本发明第一实施方式提供的真随机数发生器的模块结构示意图。

[0051] 图2为本发明第二佳实施方式提供的真随机数发生器的模块结构示意图。

具体实施方式

[0052] 为了使本发明的目的、技术方案及优点更加清楚明白，以下结合附图及实施实例，对本发明进行进一步详细说明。应当理解，此处所描述的具体实施例仅仅用以解释本发明，并不用于限定本发明。

[0053] 本发明的真随机数发生器能产生真正的真随机数，真随机数密钥加密系统利用真随机数发生器产生的真随机数作为密钥进行加密。

[0054] 实施方式1

[0055] 1、密钥产生

[0056] 如图1所示，真随机数发生器包括模拟信号获取单元1、模拟信号处理单元2、模数转换单元3、真随机数信号生产单元4。

[0057] 模拟信号获取单元1使用一个或多个自然界中的物理现象获取模拟信号。具体地，如利用电阻器件生成该模拟信号：测量该电阻器件上的自由电子的布朗运动引起的电流，作为该模拟信号；或利用晶体管生成该模拟信号：测量该晶体管的电子不规则热运动引起的电流，作为该模拟信号；或记录自然界中的声音，作为模拟信号。

[0058] 模拟信号处理单元2对一个或多个该模拟信号进行处理，获得处理后的模拟信号。具体地，对一个模拟信号进行处理时：将这个模拟信号的不同位置的信号进行相加，相乘处理，获得处理后的模拟信号；对多个模拟信号进行处理时：将多个模拟信号的不同位置的信号进行相加，相乘处理，获得处理后的模拟信号。

[0059] 模数转换单元3对该处理后的模拟信号进行放大和模数转换，得到数字信号。

[0060] 真随机数信号生产单元4对该数字信号进行处理，生成真随机数信号。具体地，计算该数字信号的自相关函数$G_x^+(\omega)$，根据自相关函数$G_x^+(\omega)$计算出该数字信号的功率谱$H_1(s)$，将功率谱$H_1(s)$分解成在s的左半平面和后半平面，取功率谱在s的左半平面的那些值，找出零、极点，根据公式$G_x^+(\omega)=\left[\alpha\frac{(j\omega+\alpha_1)\cdots(j\omega+\alpha_k)}{(j\omega+\beta_1)\cdots(j\omega+\beta_l)}\right]$和$H_1(s)=\frac{1}{G_x^+(s)}$计算出白化滤波器的频谱，其中，α为零点，β为极点。

[0061] 该真随机数发生器的真随机数生成步骤如下：

[0062] (1)使用一个或多个自然界中的物理现象获取模拟信号；

[0063] (2)对一个或多个该模拟信号进行处理，获得处理后的模拟信号；

[0064] (3)对该处理后的模拟信号进行放大和模数转换，得到数字信号；

[0065] (4)对该数字信号进行处理，生成真随机数信号。

[0066] 在步骤(1)中，利用电阻器件生成该模拟信号：测量该电阻器件上的自由电子的布朗运动引起的电流，作为该模拟信号；或利用晶体管生成该模拟信号：测量该晶体管的电子不规则热运动引起的电流，作为该模拟信号；或记录自然界中的声音，作为模拟信号；

[0067] 在步骤(2)中，将该模拟信号的不同位置的信号进行相加，相乘处理，获得处理后的模拟信号；或将多个模拟信号的不同位置的信号进行相加，相乘处理，获得处理后的模拟信号；

[0068] 在步骤(4)中，对该数字信号进行白化处理：计算该数字信号的自相关函数$G_x^+(\omega)$，根据自相关函数$G_x^+(\omega)$计算出该数字信号的功率谱$H_1(s)$，将功率谱$H_1(s)$分解成在s的左半平面和后半平面，取功率谱在s的左半平面的那些值，找出零、极点，根据公式$G_x^+(\omega)=\left[\alpha\frac{(j\omega+\alpha_1)\cdots(j\omega+\alpha_k)}{(j\omega+\beta_1)\cdots(j\omega+\beta_l)}\right]$和$H_1(s)=\frac{1}{G_x^+(s)}$计算出白化滤波器的频谱，其中，α为零点，β为极点。

[0069] 2、加密

[0070] 该真随机数密钥加密系统除了真随机数发生器还包括可分发存储介质、防火墙和专用数据加解密机构。该防火墙为光纤单向数据隔离防火墙。

[0071] 该真随机数发生器产生真随机数信号输送至该可分发存储介质进行存储作为密钥，该专用数据加解密机构透过该光纤单向数据隔离防火墙向该可分发存储介质获取该密钥用于加密。

[0072] 该可分发存储介质将该密钥以模块化方式储存：将采集到的二进制随机数存储，每一定容量为一个模块，其索引为模块序号。如利用数据库将采集到的二进制随机数存储，每10MB为一个模块，其索引为模块序号。模块序号由1为第一个模块，其后依次递增。该可分发存储介质根据存储大小可以选择硬盘或者蓝光光碟作为存储媒介。

[0073] 真随机数发生器可利用电阻器件的自然热噪声，然后通过放大器放大之后使用高速ADC采样后，之后对采集数据进行功率谱均匀化处理，然后使用专用电路在大容量存储介质即该该可分发存储介质中存储。真随机数发生器同时可以完成秘钥副本(镜像)的复制工作。可以获得某个秘钥版本的若干秘钥副本，并用于秘钥的分发。

[0074] 该真随机数密钥加密系统可采用成熟的基于PXIE构架的FPGA高速数据采集和处理模块作为基础设计。密钥分发，如在约定日期(例如每年年初)，由专业人员或者通过机密函件方式传递密钥硬盘，为通信双方分发新密钥。

[0075] 加密系统与公网的隔离——光纤单向隔离防火墙，用于加密硬件系统和外部非安全网络的数据安全隔离，用于防止外部网络对的加密硬件系统的攻击。故采用专门设计的光纤单向隔离防火墙硬件系统作为隔离防火墙。

[0076] 针对真随机数发生器可设计加密和解密硬件模块，然后结合工控处理机，将加密或解密文件路径导入，并导入下一个未用模块序号的数据库密钥，设置输出文件路径确认即可完成。

[0077] 本发明首先真随机数发生器产生数T字节的超长随机数并复制和存储于大容量存储介质中。然后定期(例如每一年)通过专用渠道分发该超长秘钥。用户使用时根据约定一次性选用与明文长度相当的秘钥，然后在专用数据加密机对明文进行逐字逐密的加密运算。加密后对数据进行交织和纠检错编码然后送入单向隔离防火墙并融入公共数据通讯网络并发送给对方用户。对方用户收到密文后做反向处理，然后使用约定的一次性秘钥进行解密运算，还原密文为明文。

[0078] 实施方式2

[0079] 实施方式1与实施方式2的区别在于，实施方式1是先进行模拟信号处理后再转换为数字信号，而实施方式2是先转换为数字信号后再进行模拟信号处理。

[0080] 1、密钥产生

[0081] 如图2所示，真随机数发生器包括模拟信号获取单元21、模数转换单元22、数字信号处理单元23、真随机数信号生产单元24。

[0082] 模拟信号获取单元21使用一个或多个自然界中的物理现象获取模拟信号。具体地，如利用电阻器件生成该模拟信号：测量该电阻器件上的自由电子的布朗运动引起的电流，作为该模拟信号；或利用晶体管生成该模拟信号：测量该晶体管的电子不规则热运动引起的电流，作为该模拟信号；或记录自然界中的声音，作为模拟信号。

[0083] 模数转换单元22对该模拟信号进行放大和模数转换，得到数字信号。

[0084] 数字信号处理单元23对该数字信号进行处理，获得处理后的数字信号。对一个数字信号进行处理，获得处理后的数字信号：将这个数字信号的不同位置的信号进行相加，相乘处理，获得处理后的数字信号；对多个数字信号进行处理，获得处理后的数字信号：将多个数字信号的不同位置的信号进行相加，相乘处理，获得处理后的数字信号。

[0085] 真随机数信号生产单元24对该处理后的数字信号进行处理，生成真随机数信号。具体地，对该数字信号进行白化处理：计算该处理后的数字信号的自相关函数$G_x^+(\omega)$，根据自相关函数$G_x^+(\omega)$计算出该处理后的数字信号的功率谱$H_1(s)$，将功率谱$H_1(s)$分解成在s的左半平面和后半平面，取功率谱在s的左半平面的那些值，找出零、极点，根据公式$G_x^+(\omega)=\left[\alpha\frac{(j\omega+\alpha_1)\cdots(j\omega+\alpha_k)}{(j\omega+\beta_1)\cdots(j\omega+\beta_l)}\right]$和$H_1(s)=\frac{1}{G_x^+(s)}$计算出白化滤波器的频谱，其中，α为零点，β为极点。

[0086] 该真随机数发生器的真随机数生成步骤如下：

[0087] (1)使用一个或多个自然界中的物理现象获取模拟信号；

[0088] (2)对该模拟信号进行放大和模数转换，得到数字信号；

[0089] (3)对该数字信号进行处理，获得处理后的数字信号；

[0090] (4)对该处理后的数字信号进行处理，生成真随机数信号。

[0091] 在步骤(1)中，利用电阻器件生成该模拟信号：测量该电阻器件上的自由电子的布朗运动引起的电流，作为该模拟信号；或利用晶体管生成该模拟信号：测量该晶体管的电子不规则热运动引起的电流，作为该模拟信号；或记录自然界中的声音，作为模拟信号；

[0092] 在步骤(2)中，将该数字信号的不同位置的信号进行相加，相乘处理，获得该处理后的数字信号；或将多个该数字信号的不同位置的信号进行相加，相乘处理，获得该处理后的数字信号；

[0093] 在步骤(4)中，对该处理后的数字信号进行白化处理：计算该处理后的数字信号的自相关函数$G_x^+(\omega)$，根据自相关函数$G_x^+(\omega)$计算出该处理后的数字信号的功率谱$H_1(s)$，将功率谱$H_1(s)$分解成在s的左半平面和后半平面，取功率谱在s的左半平面的那些值，找出

零、极点，根据公式$G_x^+(\omega)=\left[\alpha\frac{(j\omega+\alpha_1)\cdots(j\omega+\alpha_k)}{(j\omega+\beta_1)\cdots(j\omega+\beta_l)}\right]$和$H_1(s)=\frac{1}{G_x^+(s)}$计算出白化滤波器的频谱，其中，α为零点，β为极点。

[0094] 2、加密

[0095] 该真随机数密钥加密系统除了真随机数发生器还包括可分发存储介质、防火墙和专用数据加解密机构。该防火墙为光纤单向数据隔离防火墙。

[0096] 该真随机数发生器产生真随机数信号输送至该可分发存储介质进行存储作为密钥，该专用数据加解密机构透过该光纤单向数据隔离防火墙向该可分发存储介质获取该密钥用于加密。

[0097] 该可分发存储介质将该密钥以模块化方式储存：将采集到的二进制随机数存储，每一定容量为一个模块，其索引为模块序号。如利用数据库将采集到的二进制随机数存储，每10MB为一个模块，其索引为模块序号。模块序号由1为第一个模块，其后依次递增。该可分发存储介质根据存储大小可以选择硬盘或者蓝光光碟作为存储媒介。

[0098] 真随机数发生器可利用电阻器件的自然热噪声，然后通过放大器放大之后使用高速ADC采样后，之后对采集数据进行功率谱均匀化处理，然后使用专用电路在大容量存储介质即该该可分发存储介质中存储。真随机数发生器同时可以完成秘钥副本(镜像)的复制工作。可以获得某个秘钥版本的若干秘钥副本，并用于秘钥的分发。

[0099] 该真随机数密钥加密系统可采用成熟的基于PXIE构架的FPGA高速数据采集和处理模块作为基础设计。密钥分发，如在约定日期(例如每年年初)，由专业人员或者通过机密函件方式传递密钥硬盘，为通信双方分发新密钥。

[0100] 加密系统与公网的隔离——光纤单向隔离防火墙，用于加密硬件系统和外部非安全网络的数据安全隔离，用于防止外部网络对的加密硬件系统的攻击。故采用专门设计的光纤单向隔离防火墙硬件系统作为隔离防火墙。

[0101] 针对真随机数发生器可设计加密和解密硬件模块，然后结合工控处理机，将加密或解密文件路径导入，并导入下一个未用模块序号的数据库密钥，设置输出文件路径确认即可完成。

[0102] 本发明首先真随机数发生器产生数T字节的超长随机数并复制和存储于大容量存储介质中。然后定期(例如每一年)通过专用渠道分发该超长秘钥。用户使用时根据约定一次性选用与明文长度相当的秘钥，然后在专用数据加密机对明文进行逐字逐密的加密运算。加密后对数据进行交织和纠检错编码然后送入单向隔离防火墙并融入公共数据通讯网络并发送给对方用户。对方用户收到密文后做反向处理，然后使用约定的一次性秘钥进行解密运算，还原密文为明文。

[0103] 以上所述仅为本发明的较佳实施例而已，并不用以限制本发明，凡在本发明的精神和原则之内所作的任何修改、等同替换和改进等，均应包含在本发明的保护范围之内。

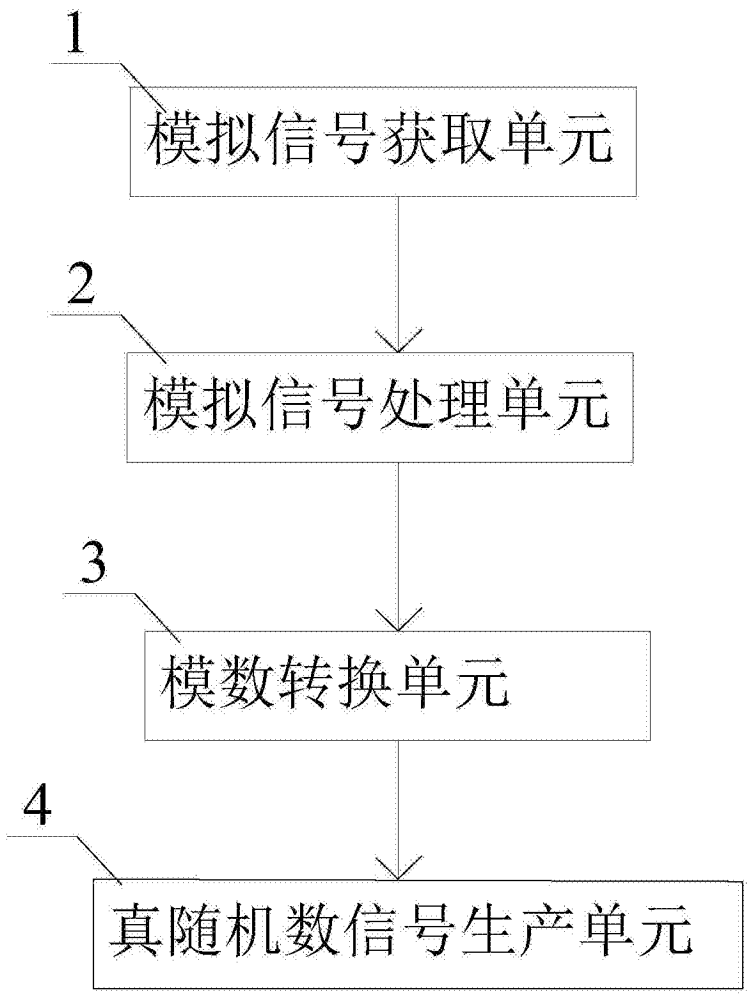


图1

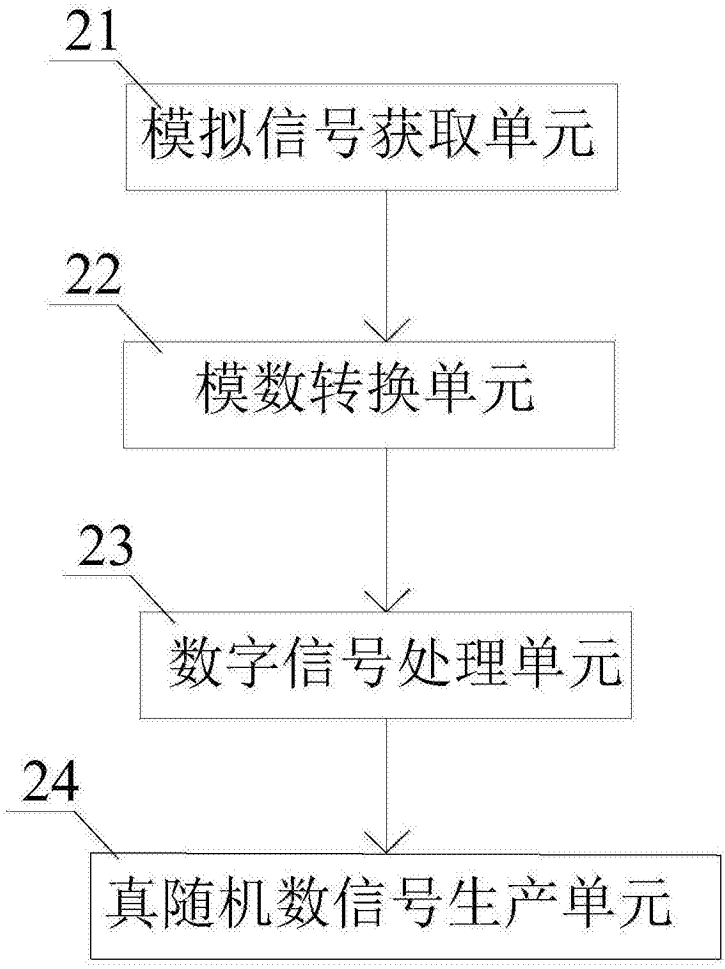


图2