



[12] 发明专利申请公开说明书

[21] 申请号 01807043.4

[43] 公开日 2003 年 5 月 21 日

[11] 公开号 CN 1419761A

[22] 申请日 2001.2.22 [21] 申请号 01807043.4

[30] 优先权

[32] 2000. 3. 23 [33] EP [31] 00106327.0

[86] 国际申请 PCT/DE01/00694 2001.2.22

[87] 国际公布 WO01/71969 德 2001.9.27

[85] 进入国家阶段日期 2002.9.23

[71] 申请人 因芬尼昂技术股份公司

地址 德国慕尼黑

[72] 发明人 N·詹森

[74] 专利代理机构 中国专利代理(香港)有限公司

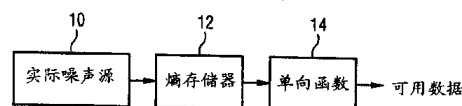
代理人 郑立柱 张志醒

权利要求书 1 页 说明书 3 页 附图 1 页

[54] 发明名称 提高噪声源可靠性和恒定性的装置
与方法

[57] 摘要

提高实际噪声源(10)操作可靠性和恒定性的装置和方法,其特征在于,一个熵存储器(12)和/或一个单向函数(14)被直接连接在噪声源(10)下游的输出上。



1. 一种提高噪声源操作可靠性和恒定性的装置,其特征是一个熵存储器(12)连接在所述噪声源(10)下游的输出上。

5 2. 根据权利要求1中所述的装置,其特征是配置一个反馈移位寄存器作为所述熵存储器(12)。

3. 根据权利要求1或2中所述的装置,其特征是一个硬布线单向函数(14)直接连接在所述熵存储器(12)的下游。

4. 根据权利要求3中所述的装置,其特征是配置一个密钥散列函数作为所述单向函数(14)。

10 5. 根据权利要求1或2中所述的装置,其特征是所述熵存储器(12)按一个低于所述噪声源性能的恒定频率进行读取。

6. 一种提高噪声源操作可靠性和恒定性的方法,其特征是对所述噪声源输出值进行缓冲。

15 7. 根据权利要求6中所述的方法,其特征是一个反馈移位寄存器被用来对所述噪声源输出值进行缓冲。

8. 根据权利要求6或7中所述的方法,其特征是缓冲后直接用一个硬体接线数学单向函数对所述噪声源输出值进行转换。

9. 根据权利要求8中所述的方法,其特征是使用一个密钥散列函数作为单向函数。

20 10. 根据权利要求6或7中所述的方法,其特征是通过一个低于所述噪声源性能的恒定时钟周期对所述噪声源的缓冲输出值进行进一步处理。

11. 根据权利要求6至10其中之一项所述的方法,其特征是所述噪声源输出值本身不得存取。

25

提高噪声源可靠性和恒定性的装置与方法

本发明论及一种能提高噪声源可靠性和恒定性的装置与方法。

- 5 在许多情况下，密钥技术都需要随机数。随机数是通过一个噪声源，例如白噪声源，输出信号的数字化而产生的。

对此类安全系统的可能的攻击可以始于实际噪声源。

如果一个实际噪声源的质量因某个攻击者的实际攻击而恶化，整个系统的安全就会受到危害。

- 10 除此之外，因制作技术的波动，已知实际噪声源会经受剧烈的性能波动。

因此，本发明的目的是：一方面能够在某一规定的时间内避免攻击者对实际噪声源的攻击；另一方面能在不降低噪声数据质量的情况下将噪声源的性能设定在一个恒定值上。

- 15 在现有技术中找不到解决此问题的办法。

本发明通过在噪声源下游输出上连接一个熵存储器或对噪声源的输出数据进行缓冲而发明性地实现了这一目的。

反馈移位寄存器尤其适合用作熵存储器。

- 20 为了使攻击噪声源更加复杂和困难，可以将一个单向函数连接在熵存储器的下游端。噪声源的输出值最好在熵存储器内缓冲后通过一个数字单向函数进行转换。

密钥散列函数尤其适合用作单向函数。

此单向函数最好是硬布线电路结构，因为只有这种方法能防止攻击者存取噪声源输出和熵存储器输出。

- 25 为了实现噪声源的恒定性能，最好以一个低于噪声源性能的恒定频率读取熵存储器。这样，熵存储器中的缓冲噪声源输出值就按照一个低于噪声源性能的恒定时钟周期进行处理。

噪声源和熵存储器的输出值禁止存取。

现在结合附图对本发明的具体实施例进行说明。

- 30 图 1：使用一个熵存储器和一个单向函数对实际噪声源进行本发明的保护。

图 2：通过使熵存储器与一理想频率同步的方法实现实际噪声源的

恒定性能。

如图 1 所示,在攻击前的一个理想噪声源上连接一个下游熵存储器 12 即可避免攻击者在规定时间内对该实际噪声源的实际攻击。

下面介绍熵存储器的功能。

- 5 熵指一定数据量如一个比特流的信息含量,它表示一个随机数发生器的输出数据。一般采用下列公式计算:

$$0 < \text{熵} \leq 1.$$

熵通常以百分比测量,因此:

$$0\% < \text{熵}[\%] < 100\%.$$

- 10 例如,某一数据量的熵值为 80%,那么,数据量可以压缩 $100\% - 80\% = 20\%$ 。由于压缩了 20%,数据不再有任何冗余并且其熵因此为 100%。尤其是,可以通过这种压缩来增大熵。无法从其中抽取数据的线性反馈移位寄存器有这种特性。因而,线性反馈移位寄存器(LFSR)即是熵存储器。

- 15 如果实际噪声源 10 的噪声质量在熵存储器 12 填充后因例如受到了攻击而不再是最佳的话,可以通过比特抽取对熵存储器进行连续清空,以使抽取的比特流的熵仅在一可调比特数后明显减小。可调比特数由熵存储器的容量确定。如图 1 所示,熵存储器 12 插在实际噪声源 10 后面,这样,熵存储器 12 的输入即是噪声源 10 的输出。反馈移位
20 寄存器可以被用作熵存储器。

为了使对噪声源输出数据做出推理成为不可能,一个数字单向函数 14 被插在熵存储器 12 后面,其输入是熵存储器 12 的输出,其输出即是可用数据。

- 25 单向函数是一种很容易进行单向计算但难以倒置的数学函数。比如,密钥散列函数就可以被用作单向函数。与散列函数相反,线性反馈移位寄存器不是单向函数,因为它们容易倒置。

- 在上述具体实施例中,原则上,插入单向函数 14 后就不能再从外部存取熵存储器 12 的输出。通过这些手段,本发明可以完全保证实际噪声源的攻击者无法收到关于实际噪声源内部情况的任何信息。鉴于
30 此原因,将单向函数作为软件来执行时不妥当的,因为这样不能排除对熵存储器 12 输出数据的存取。

不论有无外部攻击,因制作技术的波动,实际噪声源要经受剧烈的

性能波动。本发明进一步的目的是能在不降低噪声数据质量的情况下将噪声源的性能设立在一个恒定值上。连接在实际噪声源下游端的熵存储器 12 同样可以用于此目的。

5 如图 2 所示,为实现噪声源的恒定性能,熵存储器 12 受一个独立于噪声源并且其频率符合理想值的恒定时钟周期驱动。噪声源 10 的性能必须大于此理想值,以使从熵存储器 12 中抽取的比特流的熵大于或等于噪声源的熵。

当然,图 1 和图 2 中介绍的措施还可以结合起来使用,以使熵存储器 12 与一个独立于噪声源的频率同步;除此之外,一个单向函数 14
10 连接在熵存储器的下游。

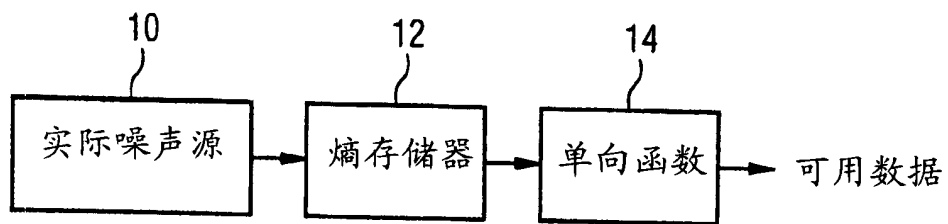


图 1

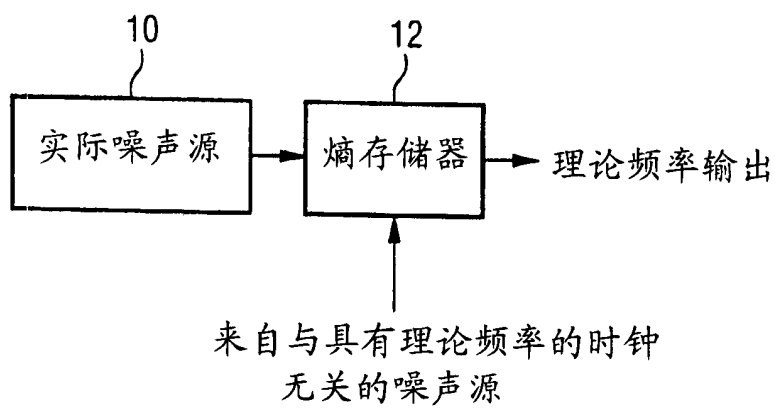


图 2