

▼ 摘要

摘要	本发明适用于各种社会现象，物理现象的数值模拟及各种信息保护领域中的密码技术，廉价且简单构成的装置，是使其发生无次序随机变数的新方法。
----	--

▼ 提供技术的内容

名称	随机变数生成方法及随机变数生成装置		
主要提供专利			
专利号	专利第 0000000		
申请号	专利申请 2005-148330 经过情报	申请日	2005/5/20
名称	随机变数生成方法及随机变数生成装置		
申请人	株式会社新泻 TLO		
专利权者	申请中		

技术领域	信息・通讯	电气・电子	
机能	控制・软件	机械・零部件的制造	其他

适用产品	用于各种信息保护领域的密码技术(安全性系统)
目的	本发明目的在于不需要对电信号档设置阈值，而是将振荡器的输出直接转换为 A-D，由于是使用数据的最末位，使物理随机变数的高速生成成为可能，并以此方法提供随机变数发生装置。
效果	本发明不使用噪音发生电路等特殊的电路，便可生成无周期性的物理随机变数。以往都是根据来自散射噪音发生电路的输出来生成随机变数的。本发明与根据阈值法产生随机变数生成法相比较时，采用的是最末位法，约为以往方法的 1800 倍左右，可大大提高随机变数的生成速度；同时，本发明所产生的随机变数的成果，已得到目前被公认的最为严密的 NIST 的 FISP140-2 表示的统计学的随机变数生成检验实验所证实，其检验通过率几乎达到 100%。
技术概要	面对快速信息化社会的今天，信息保护中主要被利用的密码方式(RSA 公开锁密码)的破译需要花费很多时间，而科学、合理的时间花费将成为防破译安全性的根据。然而，由于近几年实现了飞跃性进步的网络分散处理的发达和量子计算机的出现，使得计算量的安全性面临崩溃的危机。对此，考虑对策之一是一种更加无次序的随机变数的加密，即发生无周期性的随机变数的随机变数生成方法。本发明不使用以往的放射线和二极管的散射噪音等特殊的装置，而是根据振荡器自身的电信号的摇动而生成随机变数。由于是使用 A-D 转换器的最末位，简单明了地使以往方法中困难且无周期性的物理随机变数的高速生成的实现成为可能。对世界的情报基础设施保护方面提供了十分安全、有效的方法及装置。