计算机安全系统中随机序列发生器的研究

◆张传香

（南昌工学院，江西 南昌 330108）

【摘要】随着信息技术的不断发展，计算机系统的安全性日益受到关注。随机序列发生器作为计算机安全系统中的重要组成部分，对于加密、认证和安全通信等方面发挥着关键作用。本文对计算机安全系统中随机序列发生器进行了探讨，通过对随机序列发生器的概念、特点，以及其在计算机安全系统中的作用、具体应用以及加强其应用的有效策略进行了深入分析，以期能为进一步提升系统的安全性和稳定性提供一定的参考。

【关键词】计算机；安全系统；随机序列发生器；应用

1 随机序列发生器的概述

1.1 随机序列发生器的概念

随机序列发生器是一种用于生成看似无序或不可预测的数字序列的设备或算法。在计算机科学和数学领域，它们广泛应用于模拟随机事件、生成密码学密钥、进行模拟实验等各种场景。通常计算机中的随机序列发生器有两种，分别是伪随机序列发生器和真随机序列发生器，随机序列发生器原理如图1所示。伪随机序列发生器是通过确定性算法生成序列，其起始值称为“种子”，相同的种子将产生相同的序列，使其易于重现。伪随机数发生器生成的序列虽然不是真正的随机，但对于大多数应用而言，它们提供了足够的随机性。真随机序列发生器利用物理过程的不可预测性，如电子器件的噪声或大气噪声。由于这些过程的天然不确定性，真随机序列发生器生成的序列被认为是真正的随机。然而，由于硬件依赖性和相对较高的成本，它们在某些场景下可能不如伪随机序列发生器实用。选择使用哪种类型的随机序列发生器通常取决于特定应用的需求。伪随机数生成器通常用于一般应用，而真随机数生成器则在对随机性要求极高的场景中更为适用，如应用于密码学中。

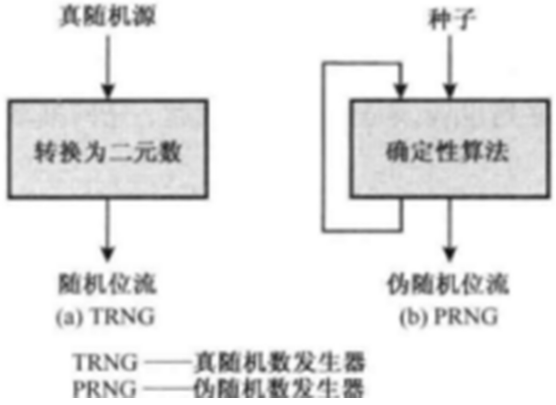

图1 随机序列发生器原理

1.2 随机序列发生器的特点

1.2.1 不可预测性

不可预测性是随机序列发生器最为关键的特点之一，这意味着生成的随机序列应该表现出一种无法被准确预测的性质。如果一个序列具有不可预测性，那么在任何给定的时刻，无法通过已经生成的部分序列来推测接下来的值。这种特性对密码学至关重要，因为密码学算法的安全性直接依赖于生成的随机数序列的无法被猜测性。在密码学中，不可预测性确保了密钥和其他关键参数的生成过程是安全的，因为攻击者无法推断出生成序列的规律或模式。如果序列是可预测的，攻击者可能会通过分析已知部分的序列来猜测未来的值，从而危及系统的安全性。这一特性要求随机序列发生器采用复杂的算法和良好的随机性源，以确保生成的序列在统计学上和计算上都是不可预测的。因此，在设计随机序列发生器时，需要综合考虑算法的复杂性、种子的选择以及输入源的质量，以确保生成的序列足够安全和不可预测。

1.2.2 均匀性

均匀性是指随机序列中的各个元素应该以相等的概率出现。如果一个序列是均匀的，那么在长期内，每个可能的值都应该在序列中出现近似相等的次数。这确保了生成的随机数在统计上是平衡的，不会有某些值频繁出现而其他值很少出现的情况。在科学模拟和统计分析中，均匀性是确保模拟实验结果或采样数据具有代表性的关键因素。例如，如果一个模拟实验中某个数值代表某个物理量，而该数值在生成的随机序列中出现的概率远高于其他数值，那么该模拟实验的结果就可能失去代表性，影响对实际系统的理解。一个好的随机序列发生器应该能够生成具有良好均匀性的随机数序列，确保在随机数应用的各个领域都能够得到可靠和准确的结果。

1.2.3 独立性

在设计和评估这样的发生器时，其中一个关键的特点是独立性。独立性是指生成的随机序列中的每个值都应该是独立的，即当前生成的值不受之前生成值的影响。这一特性在统计学和随机过程理论中占有重要地位。独立性保证

了序列中的任意两个值之间不应该存在任何关联或依赖关系。 如果一个随机序列是独立的，那么任何一个值的出现都不会提供关于序列中其他值的信息。 这意味着先前生成的值不能用来预测或影响接下来生成的值，使得序列的行为更接近真正的随机性。 在统计学中，独立性是许多推断和估计方法的基础。 当进行抽样并应用统计方法进行推断时，人们通常基于假设样本中的观测值是相互独立的。 如果这个假设不成立，统计推断的结果可能会受到影响，因为观测值之间的依赖关系可能导致对总体参数的不准确估计。对于随机序列发生器，独立性的实现通常要求使用一些数学或算法上的手段，确保生成的值不受先前生成的值的影响。这可以通过精心设计的随机数生成算法来实现，这些算法在产生序列的每一步都考虑到了先前生成的值，并且确保它们之间的关系是最小化的，以达到独立性的要求。

2 随机序列发生器在计算机安全系统中的作用

2.1 生成密码学中的密钥基础

密码学协议和算法的核心之一是使用加密密钥来对信息进行加密和解密。 为了确保密钥的安全性，随机性变得尤为关键。 随机序列发生器被用来生成高质量的随机数，这些数被作为加密密钥的基础。 如果密钥是可预测的或者具有可识别的模式，那么攻击者有可能通过分析这些模式来猜测或者破解密钥，从而威胁整个加密系统的安全性。 在一些加密算法中，特别是对称加密算法的工作模式中，使用了初始化向量，初始化向量是一个与密钥相关的固定长度的随机数，它在每次加密新的数据块时都会被使用。 随机序列发生器负责生成这些初始化向量，确保它们是随机的、不可预测的，从而增加加密系统的复杂性和安全性。 密码学的目标之一是设计能够抵御各种攻击的安全系统。 攻击者通常会尝试通过各种手段分析和破解密钥以获取敏感信息。使用随机序列发生器生成的随机数可以增加密码系统的抗攻击性。 这是因为攻击者难以预测或重现随机序列，从而使破解密钥的任务变得更加困难。 在密码学中，重放攻击是一种攻击方式，攻击者试图通过重放先前捕获的有效通信来欺骗系统。 使用随机序列发生器生成的随机数可以防止重放攻击，因为每次生成的随机数都是独一无二的，即使相同的消息被发送，由于不同的随机数参与加密，攻击者也无法获得有用的信息。

2.2 增强系统的随机性

随机序列发生器在计算机安全系统中的作用之一是增强系统的随机性。 许多安全系统依赖于访问控制来限制用户或程序对敏感资源的访问。 引入随机性可以使得访问模式不可预测，从而增加攻击者猜测正确访问模式的难度。 通过随机序列发生器生成随机的访问令牌或身份验证因子，系统可以在每次访问请求时提供不同的令牌，降低攻击者猜测访问模式的成功率。 随机性还可以通过引入随机延时来增加系统的复杂性。 在安全系统中，延时是一种有效的手段，用于防范定时攻击。 通过在系统响应中引入随机延时，攻击者将难以精确预测系统的响应时间，从而降低成功执行定时攻击的可能性。 在一些情况下，系统可能需要对特定事件做出随机响应，以增加不确定性。 例如，当检测到异常行为时，系统可以通过随机选择一种响应方式来困扰攻击者。 这可以包括随机生成错误消息、临时禁止某些功能或者引入额外的验证步骤。 这样的随机性使得攻击者更难以预测系统的反应，增加了系统的安全性。 随机性还有助于抵御重放攻击，其中攻击者试图通过重复之前的合法通信来欺骗系统。 通过在通信中引入随机序列，系统可以使得每次通信的内容都具有独特性，从而防止攻击者成功重放之前的通信。

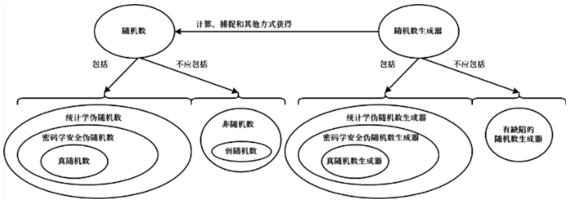

图 2 各种随机数和各类随机数生成器之间的关系

2.3 生成安全协议和通信中的安全会话密钥

安全协议和通信是计算机安全系统中至关重要的组成部分，旨在确保信息在传输和处理过程中的机密性、完整性和可用性。 在这一背景下，随机序列发生器扮演着重要的角色，在安全通信中，保护数据的机密性是首要任务之一。随机序列发生器常被用于生成随机数，这些随机数在 SSL/TLS 等协议中被用来建立安全的会话密钥。 会话密钥是在通信开始时生成的，用于加密和解密数据，其随机性使得会话密钥破解更加困难，提高了通信的安全性。 随机序列发生器还可以用于生成主密钥，该密钥用于其他密钥的生成和管理。 主密钥的随机性对于系统的整体安全至关重要，因为如果主密钥被破解，所有依赖于它的子密钥和会话密钥也将面临风险。 在通信中，为了验证消息的完整性，常常使用消息认证码。 随机序列发生器可以为生成消息认证码所需的随机数提供熵，使得攻击者难以预测和篡改通信过程中的消息。 通过引入随机性，系统可以增加密码学协议的复杂性，从而提高对密码分析和其他攻击的抵抗力。 攻击者通常依赖于预测性分析，而随机性的引入使得攻击者更难以预测和猜测密钥的生成方式，从而加强了通信的安全性。总体而言，随机序列发生器在安全协议和通信中的应用对保护敏感信息和防范潜在威胁起到了关键的作用。

3 随机序列发生器在安全系统中的具体应用

3.1 加密系统

3.1.1 数据加密

在对称加密算法中，相同的密钥用于加密和解密数据。为了增强安全性，随机序列发生器用于生成随机的密钥流，这是一系列伪随机的二进制位，这个密钥流与明文进行按位

异或，产生密文。由于密钥流是随机的，即使相同的明文被多次加密，也会生成不同的密文。这种随机性使得攻击者更难通过分析重复模式或利用统计规律来破解加密。在对称加密中，密钥的安全性至关重要。如果密钥可被预测或分析，整个系统就容易受到攻击。通过使用随机生成的密钥流，系统能够提高其强度，因为攻击者很难在事先获得的信息中找到关键的模式。这就增加了攻击者破解加密所需的时间和计算资源。

3.1.2 密钥生成

随机序列发生器用于生成加密算法所需的密钥。密钥的唯一性是指每个生成的密钥都应该是独特的，确保系统中没有两个相同的密钥。这是为了防止攻击者通过获取一个密钥然后应用于多个场景来降低系统的安全性。不可预测性则要求生成的密钥难以在生成之前被预测，这意味着即使攻击者知道了系统的其他方面，也很难推断出下一个生成的密钥是什么。密码分析是一种通过分析加密算法的结构或输出来寻找密钥的攻击方式。通过使用随机序列发生器生成密钥，系统可以更好地抵抗这些分析攻击，因为攻击者无法依赖于模式或可预测的密钥生成方法。密钥的随机性增加了密码分析的难度，提高了系统的整体安全性。

3.2 认证与访问控制

3.2.1 双因素认证

随机序列发生器在双因素认证中扮演了关键角色，增加了系统的安全性。传统的用户名和密码组合可能会被黑客截获或破解，因此引入第二个因素，即随机生成的一次性密码或令牌。这些密码或令牌只在特定的时间窗口内有效，通常是几十秒钟，用户在每次登录时都会收到一个新的随机密码，即使攻击者截获了先前的密码，由于其短暂性，再次使用的可能性很小，因此提高了身份验证的安全性。这种方法还能够抵御钓鱼攻击，因为即使用户误将密码泄露给攻击者，攻击者也只能在短时间内使用这个信息，而无法长期滥用。

3.2.2 会话密钥管理

随机序列发生器在会话密钥管理中用于生成短期的加密密钥。会话密钥是在通信会话开始时生成，用于加密和解密在该会话期间传输的数据。与长期密钥相比，会话密钥的短期性质提供了额外的安全性。由于会话密钥是短期的，即使攻击者能够获取其中一个密钥，只能在特定的通信会话期间进行潜在的攻击。这减小了密钥被滥用的风险，因为即使攻击者能够解密一次通信，无法使用相同的密钥进行未来的通信。随机生成会话密钥还允许系统动态地更新加密密钥，而无需中断整个系统。这使得即使某个密钥被泄露，系统管理员仍然可以轻松地更新密钥，而无需大规模更改整个加密基础结构。

4 加强随机序列发生器应用安全的策略

4.1 进行随机性测试和质量控制

为确保随机序列的质量和强度，需要建立严格的随机性测试和质量控制机制，包括对生成的序列进行统计测试、分析和评估。测试可以涉及检查序列的均匀性、独立性和长周期性等属性。如果随机序列存在任何可预测性或偏差，可能会成为攻击者入侵系统的弱点。因此，建立一套全面的质量控制流程，包括定期的自动化测试和手动审查，是确保随机性的关键。

4.2 物理安全和环境隔离

随机序列的安全性不仅仅取决于算法和生成过程，还与物理安全和环境隔离密切相关。保护生成器免受物理攻击、电磁攻击和其他潜在的威胁是至关重要的。将随机序列发生器部署在受到适当物理安全措施保护的环境中，例如使用专用的硬件安全模块，这将有助于减少潜在的攻击面。同时，确保生成器的环境是受到监控和审计的，以便及时检测和应对任何潜在的威胁。

4.3 建立实时监控和响应机制

建立实时监控机制，以检测潜在的攻击或随机序列生成的异常情况。实时监控涵盖对随机序列生成器性能和输出进行连续审计等方面。如果检测到任何异常情况，系统应该能够立即响应，禁用受影响的生成器、切换到备用生成器，或触发警报通知安全团队。

5 结束语

随机序列发生器作为计算机安全系统中的关键组成部分，其合理应用和有效加强对整个系统的安全性至关重要。本文深入探讨了随机序列发生器的概念、作用、具体应用以及加强策略，为提升计算机安全水平提供了有益的思路和建议。在未来的发展中，随机序列发生器的进一步创新和优化将为计算机安全领域带来更多可能性，促使安全系统在不断演进中保持高效、可靠的防护水平。

参考文献：

[1]苏桂平，吕述望.计算机安全系统中随机序列发生器的研究[J].计算机研究与发展，2003(07)：994-1000.

[2]周文彬.组合式伪随机数发生器的研究与设计[D].哈尔滨：哈尔滨工程大学，2013.

[3]孙淑琴，林君，张秉仁，等.伪随机序列发生器的研究与实现[J].吉林大学学报(信息科学版)，2004(03)：185-188.

[4]薛晖耀.基于双相采样的真随机数发生器的研究与设计[D].深圳：深圳大学，2020.

作者简介：

张传香(1994－)，女，汉族，江西九江人，硕士，研究方向：数字化教学资源的开发与利用。