# 基于噪声的哈希密文再加密及再加密后的解密方法

## 所属领域：信息安全

## 成果简介：

**1. 成果的基本情况**

MD5 加密的主要方式是将用户的明文进行哈希加密形成密文，然后将密文存储在数据库里面，以后用户登录时，将其输入的密码转换成 MD5 码后与数据库存储的密文进行比对，判断是否一致。但是，这样的加密方式并不意味着百分之百的安全。原因在于，现在很多网络的资源可以通过使用字典方式来枚举 MD5 码的密文，从而通过这种对应的方式破解 MD5 加密之后的密文，获得用户登录密码的明文。例如：有一用户的登录密码为“mynewpassword”，经过 MD5 加密之后，其密文为“8E70383C69F7A3B7EA3F71B02F3E9731”，系统将此密文存储到数据库中，日后登录时进行比对，判断登录用户身份是否合法。但是，此密文一旦泄露，虽然无法使用数学方式反解，但我们还是可以通过之前提过的枚举手段取得其对应的明文。经过大量试验，对于并不是很复杂的用户密码的 MD5 密文，都可以通过枚举的方式对其进行解密。从这一点就可以说明，现在广泛使用的 MD5 加密手段并不是十分的可靠。虽然用户可以通过高强度和高复杂度的用户密码解决枚举的破解手段，但是这样会带来用户密码难以记忆的问题。为了解决以上问题，现有技术对用户明文进行加密，得到密文，若再次对密文进行加密，虽然可以提高密文的加密强度，但是所带来的加密解密开销会大大增加。因此，需要有一种新的加密手段对 MD5 加密后的密文再次进行加密，而且再加密开销要小，这样在降低计算量的同时，即使数据库中的密文泄露之后，也很难使用枚举方式进行破译。

**2. 主要技术指标**

本发明与现有技术相比具有以下优点：

（1）本发明的加密与解密方法简单，实现方便。

（2）本发明的加密方法采用了静态策略和动态策略相结合的加密方法，通过设置第一噪声插入位置，并采用了在第一后半哈希密文中随机找位置的方法设置第二噪声插入位置，通过在第一噪声插入位置和第二噪声插入位置插入噪声字符，能够对哈希密封进行高效、快速的再加密，在哈希密文中加入了无用的干扰字符，使得破解者无法分离出原始哈希密文，进一步加强了哈希密文的加密强度，使得哈希密文的破解难度更高，从而保证了加密解密的安全性。

（3）本发明加密解密操作通过增加少量的开销提高了加密解密的安全性，而且所带来的计算量控制在微秒级别，对于服务的影响基本上可以忽略不计。

**3. 应用范围**

数据加密。

**4. 市场需求及经济效益分析**

本发明的加密解密方法简单，易于实现，可以较高的效率对哈希密文进行再加密和再加密后的解密，能有效的提高原始哈希密文的安全性，且加密解密过程开销小，实用性强。

2. **合作方式：**专利权转让　专利权许可　技术转让　技术入股　合作开发　技术服务　双方协商　其它

**6. 联系方式**

负责人姓名：李 娜　　电　话：18740480609　　E-mail：59255974@qq.com