# 基于元胞自动机的新Hash函数构想

## 作者：唐一珉 专业：电子信息 学号：201813150508

摘要：元胞自动机以其本身的简单性，信息处理的高度性等优点适用于密码学。本文意图从元胞自动机的极高的不可逆性，通过正向迭代的方式，将信息进行加密。该方法对于统计攻击，暴力攻击等常见方式有很高的安全性。

关键字：元胞自动机；密码学；不可逆算法；Hash函数

#### **正文**：

#### 0引言：

自从1985年Wolfram提出使用元胞自动机的初始状态作为密钥后，对于元胞自动机用于加密的研究就一直持续至今。但是整体的研究方向在于对可逆元胞自动机，耦合触发元胞自动机，以及反向迭代等，在1990年Damgard首次提出利用元胞自动机设计单向Hash函数后，直到1998年后就没有了新的研究。而国内对于这方面的论文也是非常的稀少。

如今即将进入5G时代，信息传播速度大幅提高，对于密码等明文的单向加密完全可以采取比sha-512都更加庞大的密文。利用Hash函数和元胞自动机可以完成加密效率高，安全可靠的加密。

#### 1 元胞自动机的基本理论：

元胞自动机（Cellular Automaton，简称CA）是一种时间和空间都离散的动力系统。它由元胞空间，状态，维数，规则构成。依照Wolfrarm可以将元胞自动机分为四大类：

⑴平稳型:自任何初始状态开始，经过一定时间运行后，元胞空间趋于一个空间平稳的构形，这里空间平稳即指每一个元胞处于固定状态。不随时间变化而变化。

⑵周期型：经过一定时间运行后，元胞空间趋于一系列简单的固定结构（Stable Patterns）或周期结构（Perlodical Patterns)。由于这些结构可看作是一种滤波器（Filter），故可应用到图像处理的研究中。

⑶混沌型：自任何初始状态开始，经过一定时间运行后，元胞自动机表现出混沌的非周期行为，所生成的结构的统计特征不再变止，通常表现为分形分维特征。

⑷复杂型：出现复杂的局部结构，或者说是局部的混沌，其中有些会不断地传播。

#### 2 本文的算法思路：

通过现有的Hash函数与元胞自动机的结合得到的新的单向加密方法，即先将明文进行一次sha-256加密转成密文后，再将密文进行分组为8组，采用一定的方式得到一个常数K。以元胞自动机的初始状态进行K轮即可得到一个Hash函数。

基于元胞自动机的极高不可逆性和局部混乱的特性，以及sha-256对于明文的敏感度，对于常见攻击的安全性很高。其次，在提高了传输速度的5G时代，对于元胞自动机的元胞分布最终会趋于守序的问题，可以对于元胞加上年龄的属性，对其存在的轮数进行记录，用以解决对于规则和初始图像的设置可能导致的局部图像完全稳定的问题。

元胞自动机的的规则可以简单的使用由Conway提出的生命游戏的规则，只需稍微改动繁殖或死亡的规则，在初始状态元胞足够多的情况下就不会出现元胞“死光”的情况。

#### 3实际应用：

对于密码的单向加密，即只需在用户和数据库各有一份随机生成的相同的元胞自动机初始图像，就可以做到比现在使用的md5,sha-256等方法更好的效果。在对于图像的混沌加密也可以起到相同作用。

#### 4 现有问题

1. 对于元胞自动机的运行规则并没有很好的方案，需要保证在足够大的运算次数后仍有一定数量的细胞。
2. 对于随机生成的元胞空间初始状态需要进行检查，防止生成弱随机的初始状态。
3. 控制由sha-256处理过的密钥生成常数，保证常数的值在一定范围内，以控制加密的效率和防止出现细胞“死光”。
4. 最大问题在于现有的Hash函数诸如MD5，sha-256等足够确保单向加密的安全度，新一代Hash函数的使用价值不明。

## 参考文献：

李佳凯 《基于DNA-记忆元胞自动机与Hash函数的图像加密算法》2016-3

平萍 《[**元胞自动机原理及其在密码学的应用研究**](http://kns.cnki.net/KCMS/detail/detail.aspx?filename=2010097951.nh&dbname=CDFD0911&dbcode=cdmd&uid=WEEvREcwSlJHSldRa1FhdXNXaEd2aGd6cFZLNGQrSmR2dk90K3BNRmZBVT0=$9A4hF_YAuvQ5obgVAqNKPCYcEjKensW4IQMovwHtwkF4VYPoHbKxJw!!&v=MTYwODZPeEdkakpycEViUElSK2ZuczR5UllhbXoxMVBIYmtxV0EwRnJDVVJMT2ZZZWRxRnlqbFZMM01WMTI2SHI=)》 2009-10

罗慧军 《基于混沌元胞自动机的图像加密算法的研究与实现》2011-6

范天恒 《元胞自动机》2014-10