细胞自动机置换群加密技术研究*)

张传武[1] 彭启琮[1] 朱甫臣[2]

(电子科技大学通信与信息工程学院 成都610054)[1]

(国防科技保密通信重点实验室 成都810信箱23分箱 成都610041)[2]

Encryption Based on the Permutation of Cellular Automata

ZHANG Chuan-Wu[1] PENG Qi-Cong[1] ZHU Fu-Chen[2]

(ICIE, University of Electronic Science and Technology of China, Chengdu 610054)[1]

(Secure Communication Key Laboratory of Defense 810 Box, 23 Extension, Chengdu 610041)[2]

Abstract With the development of the information technology, information security, as well as the implementation of the encryption system becomes more and more complexity, and therefore new methods are explored to simplify complexity of the implementation. Cellular automata has the characters of simplicity of basic components, locality of cellular automata interactions, massive parallelism of information processing, and exhibits complex global properties, which makes it suitable for the application in cryptography. This paper presents a new method of encryption, the key of the new method consists of the permutation cellular automata, the vectors inputted, and the number of the iteration. Evidently, it has larger key space than other methods with only the cellular automata itself as the key.

Keywords Cellular automata (CA), Permutation group, Block cipher

1. 引言

信息技术的发展对信息安全提出了更高的要求，并使得作为信息安全核心的加密技术及其实现变得越来越复杂。所以，人们开始探索简化加密系统实现的新方法，以满足现代信息技术发展对全方位多层次信息安全的要求。1948年，Von Neumann 在研究具有自组织特性的系统时引入了细胞自动机的概念，后经 S. Wolfram 对其结构进行简化，从而极大地推动了细胞自动机理论及其应用的发展。细胞自动机具有组成单元的简单性、单元之间作用的局部性和信息处理的高度并行性，并表现出复杂的全局特性等特点[1,2]，细胞自动机的这些特点使得其尤其适合于密码学中的应用。

1985年美洲密码学年会上，S. Wolfram 首次提出了将细胞自动机的初始状态作为密钥，使用细胞自动机前向迭代产生的伪随机序列作为序列密码[3]，从而开创了细胞自动机在密码学中的应用研究。P. Guan 根据复杂系统的多项式方程求逆的困难性，提出了一种基于混合细胞自动机的公钥加密技术[4]。S. Nandi 等人则根据细胞自动机循环群特性提出了基于置换群基本变换的分组加密技术[5]，但由于其密钥为所有细胞单元为补规则且具有偶置换群特性的细胞自动机本身，从而使得其密钥的数量大大受限。本文将外部向量引入到具有置换群特性的细胞自动机中，并提出了具有输入的细胞自动机置换群加密技术，其密钥由细胞自动机本身、细胞自动机的状态迭代次数和细胞自动机的输入向量等三部分组成，从而使得本方法比 S. Nandi 等人的方法具有更大的密钥空间和更灵活的加解密方式。

2. 细胞自动机

细胞自动机是一种有限状态机，它是状态、空间和时间均离散的动力学系统，是由空间的一组细胞单元组成的阵列，每个细胞单元处于可能的状态中的一种，其状态根据其相应的局部函数规则和局部邻居配置进行同步更新。在细胞自动机的定义中，绝大部分定义的细胞单元为无限，所以未对其边界条件作定义，但由于其不能物理实现，因此不具有工程应用价值。我们根据工程应用的需要将细胞自动机定义为由有限个细胞单元构成，并对其边界条件进行相应的限定。

定义1 细胞自动机是一个 $CA=(A,S,f,B)$ 的四元组，其中包括：

(1)空间结构 A：$A=\prod_{i=1}^{d} N_i=\{\vec{i}=(i_1,i_2,\cdots,i_d)\mid i_1\in N_1, i_2\in N_2,\cdots,i_d\in N_d\}$ 是 d 维细胞单元构成的空间结构。其中 $\prod_{i=1}^{d} N_i=N_1\times N_2\times\cdots\times N_d$ 为集合 $N_1,N_2,\cdots,N_d$ 的笛卡尔积，$N_i=\{0,1,\cdots,N_i-1\}$ 为模 N_i 的整数集，$\vec{i}=(i_1,i_2,\cdots,i_d)$ 为一个细胞单元的索引值；

(2)状态空间 S：细胞自动机中细胞单元 $\vec{i}=(i_1,i_2,\cdots,i_d)$ 的状态取值范围。一般为具有 k 个元素的有限交换环 R_k，常取模 k 的整数集合即 $R_k=Z_k=\{0,1,\cdots,k\}$，其中最简单的是 $Z_2=\{0,1\}$。将细胞单元 $\vec{i}=(i_1,i_2,\cdots,i_d)$ 在 t 时刻的状态表示为 x_i^t，而将细胞自动机所有细胞单元 t 时刻的状态称为细胞自动机的全局状态配置 X^t。

(3)局部函数规则 f_i：它确定了细胞自动机中第 $\vec{i}=(i_1,i_2,\cdots,i_d)$ 个细胞单元的转移状态 x_i^{t+1} 与其局部作用域范围 $\vec{r}=(r_1,r_2,\cdots,r_d)$ 内的所有细胞单元的状态 $\{x_j^t\mid\mid j_1-i_1\mid\leqslant r_1, \mid j_2-i_2\mid\leqslant r_2,\cdots,\mid j_d-i_d\mid\leqslant r_d\}$ 之间的映射关系：$x_i^t=f(x_j^t\mid\mid j_1-i_1\mid\leqslant r_1,\mid j_2-i_2\mid\leqslant r_2,\cdots,\mid j_d-i_d\mid\leqslant r_d)$。其中 $\vec{r}=(r_1,r_2,\cdots,r_d)$ 为规则的局部作用半径，$\eta_i^t=\{x_j^t\mid\mid j_1-i_1\mid\leqslant r_1,\mid j_2-i_2\mid\leqslant r_2,\cdots,\mid j_d-i_d\mid\leqslant r_d\}$ 为细胞单元 $\vec{i}=(i_1,i_2,\cdots,i_d)$ 的局部状态配置。

(4)边界条件 B：边界条件包括固定边界条件和循环边界条件。其中固定边界是指在细胞自动机中，将细胞单元 $\vec{i}=(i_1,i_2,\cdots,i_d)$ 的局部配置超出细胞自动机空间 $\prod_{i=1}^{d} N_i=N_1\times N_2\times\cdots\times N_d$ 的单元的状态看为状态空间 S 上的一个固定状

*)本课题为国防科技保密通信重点实验室基金课题“新型密码体制研究(基金编号2000JS06.1.2ZS0601)”。

态；而循环边界则是指将细胞单元 $\vec{i}=(i_1,i_2,\cdots,i_d)$ 的局部配置 $\eta_{\vec{r}}^t$ 中的各个细胞单元分别进行取模操作，即 $\eta_{\vec{r}}^t=\{x_{j \bmod \prod_{i=1}^{d} N_i}^t \mid |j_1-i_1|\leqslant r_1,|j_2-i_2|\leqslant r_2,\cdots,|j_d-i_d|\leqslant r_d\}$。考虑到细胞自动机的物理实现，特别是 VLSI 实现方面，一般采取固定零边界条件。

细胞自动机的重要特性是其所有的细胞单元根据其局部函数规则同步并行作用，从而引起复杂的全局状态即配置的转移。所以，全局函数是同时在所有的细胞单元进行局部函数规定的状态更新，其全局状态转移方程为：

$$(x_{\vec{r}}^{t+1}\mid \vec{i}\in A)=F(x_{\vec{r}}^t\mid \vec{i}\in A)=(f(\eta_{\vec{r}}^t)\mid \vec{i}\in A) \qquad (1)$$

定义一个局部函数规则等于向每个 $S^{\sum_{i=1}^{d}(2r_i)+1}$ 局部状态配置赋予一个状态值 x，因此，对于 d 维空间、局部作用半径为 $\vec{r}$ 的细胞自动机，总共有 $|S|^{|S|^{\sum_{i=1}^{d}(2r_i)+1}}$ 种局部函数规则，其规则数随细胞自动机的状态空间、维数和局部作用区域半径的增加而迅速增加。如当 $d=1,|S|=3,r=2$ 时，其规则的数量超过 10^{115}。

细胞自动机中，研究和应用最为广泛的是 $d=1,|S|=2,r=1$ 的基本细胞自动机(Elementary Cellular Automata)。为方便起见，我们将细胞自动机的局部配置 $\{x_{i-1}^t,x_i^t,x_{i+1}^t\}$ 的映射 $\{f_7=f(111),f_6=f(110),\cdots,f_1=f(001),f_0=f(000)\}$ 的组合 $I_f=\sum_{i=0}^{7}f_i2^i$ 称为基本细胞自动机的规则号[6]。如 $\{f_7=1,f_6=0,f_5=0,f_4=1,f_3=0,f_2=1,f_1=1,f_0=0\}$ 对应的规则号为150，其逻辑函数表达式为 $x_i^{t+1}=x_{i-1}^t+x_i^t+x_{i+1}^t$，其中“+”表示模二加运算。以后，我们便使用基本细胞自动机的规则号来代表其对应的局部函数规则。

定义2 在一个细胞自动机中，如果所有的细胞单元使用相同的规则，那么称它为单一细胞自动机(Uniform Cellular Automata：UCA)。

定义3 在一个细胞自动机中，如果对不同的细胞单元至少有两种不同的规则使用，那么称它为混合细胞自动机(Hybrid Cellular Automata：HCA)。

定义4 在一个细胞自动机中，局部函数规则只由异或运算 EXOR 和同或运算 EXNOR 组成，那么称此细胞自动机为加性细胞自动机(Additive Cellular Automata：ACA)。

定义5 称一个局部函数规则为另一个局部函数规则的补规则(Complemented Rule)，如果它们互为取反，如规则150和105互为补规则。

定义6 一个细胞自动机称为群细胞自动机，如果其状态转移为一一映射。

有关细胞自动机更为详细的内容，请参见文[1,6～8]。

3. 细胞自动机置换群加密方法

在基本细胞自动机中，只有加性规则可以使用代数的方法进行研究，而加性局部函数规则又分为群规则和非群规则两种。在群规则中，存在一类其状态转移图中的所有圈长均等于细胞自动机的阶的特殊群规则。下面集中讨论这一类细胞自动机。

引理1[10] 对于长为 n 的规则60、102和204的基本细胞自动机均为群细胞自动机，且其阶为 $O(G)=p=2^a;a=0,1,2,\cdots;p\geqslant n>p/2$。

引理2[11] 在一个群细胞自动机中，使用对应局部函数规则的补规则替换原来的规则所得到的细胞自动机也是群细胞自动机。

根据引理1和引理2可以推出引理3如下：

引理3[4] 由规则195、153和51构成的任意 n 长的单一细胞自动机(零边界条件)均是群细胞自动机，且其阶为 $O(G)=P=2^a,a=1,2,\cdots$。

引理1、2、3证略。

由上面的引理2、3可推导出引理4如下：

引理4[4] 如果由规则195、153、51构成的 n 长的混合细胞自动机(零边界条件)为群细胞自动机，那么其状态转移图中的圈长均相等，且等于细胞自动机的阶(偶数)。

由上述引理可推广为如下的定理1：

定理1 如果规则60、102和204构成的 n 长混合细胞自动机(零边界条件)为群细胞自动机，那么在相应的位置由其对应的补规则95、153和51替换原来的规则而成的细胞自动机(至少替换一个)仍然为群细胞自动机，且其状态转移图中的圈长均等于细胞自动机的阶(偶数)。

证明：设由规则60、102和204构成的 n 长混合细胞自动机(零边界条件)为转移矩阵为 T 的群细胞自动机，且有 $T^p=I$。那么，使用部分补规则替换后的细胞自动机为转移矩阵为 $\overline{T}$ 的群细胞自动机，且有 $\overline{T}^m=I$。则对于替换后的群细胞自动机的状态转移方程可写成方程式(2)：

$$X^{t+1}=\overline{T}X^t=F+TX^t \qquad (2)$$

其中 F 为一 n 维向量，其中与原细胞自动机规则相同的对应位为0，而与原细胞自动机规则相补的对应位为1。并将上式迭代 m 次有：

$$X^{t+m}=\overline{T}^mX^t=[I+T+T^2+\cdots+T^{m-1}]F+T^mX^t=X^t \qquad (3)$$

(3)式可写为：

$$(T+I)[I+T+T^2+\cdots+T^{m-1}]X^t=[I+T+T^2+\cdots+T^{m-1}]F \qquad (4)$$

方程(4)有解的充要条件为：

$$\begin{cases} I+T+T^2+\cdots+T^{m-1}=O \ or \\ rank[T+1]=rank[T+I,F] \end{cases} \qquad (5)$$

而对于规则60、102和204构成的 n 长混合细胞自动机(零边界条件)，恒有 $rank[T+I]<n$。所以，我们可以通过选取适当的 F，使得 $rank[T+I]\neq rank[T+I,F]$。这样，方程(4)有解的充要条件便是如下方程(6)恒成立：

$$I+T+T^2+\cdots+T^{m-1}=0 \qquad (6)$$

此时，由方程(3)和方程(6)有：

$$\begin{cases} \sum_{i=0}^{m-1}T^i=0 \\ T^m=I \end{cases} \qquad (7)$$

因为细胞自动机的阶为使上式成立的最小 m，而上式对于 $m=2p$ 恒成立，而对于特殊的 T，上式可能成立，所以其阶为 $m=p$ 或 $m=2p$，其中 p 为原细胞自动机的阶。

当 $p=1$ 时，$T=I$，此时必有 $m=Min(q)$ 使 $\sum_{i=0}^{q-1}T^i=O$，所以 $m=2$；

当 $p\neq 1$ 时，$m=P=2^a,a\in N$ 或 $m=2p=2^{a+1},a\in N$。

所以，细胞自动机的阶为偶数。

下面证明其圈长的唯一性：

假设选取一定的 F 后，有一个圈的长度为 m 的因子 m_i，那么它必须满足方程组(7)，这表明 m_i 也为细胞自动机的阶即有 $m_i=m$。

所以，如果规则60、102和204构成的 n 长混合细胞自动机(零边界条件)为群细胞自动机，那么在相应的位置由其对应的补规则95、153和51替换原来的规则而成的细胞自动机(至

少替换一个)即合理选取 F 的条件下,构成的细胞自动机仍然为群细胞自动机,且其状态转移圈中的圈长均等于细胞自动机的阶(偶数)。 [证毕]

我们将具有定理1的细胞自动机称为具有置换群特性的细胞自动机。下面为关于置换群细胞自动机的计数定理。

定理2 如果规则60、102和204构成的 n 长混合细胞自动机(零边界条件)为转移矩阵为 T 的群细胞自动机,那么,在一定的位置由其对应的补规则95、153和51替换原来的规则而成的细胞自动机(至少替换一个)为圈长相等的置换群细胞自动机。且具有这种特性的细胞自动机共有 $2^{l_1}(2^{l_0}-1)$,其中 $l_1=rank(T+I)<n, l_0=n-rank(T+I)$。

证明:l_0 由两部分构成:细胞自动机中规则204、第一个单元为60的数目,和最后一个单元为102的数目为 l_{0_1},而(102,*,60)规则对的数目为 l_{0_d},且有 $l_0=l_{0_1}+l_{0_d}$。

要使细胞自动机为圈长相等的群细胞自动机,方程(5)必须成立,而对于由规则60、102和204构成的细胞自动机的矩阵 T 而言,其 $rank(T+I)<n$,因为矩阵 $(T+I)$ 对应于规则204、第一个单元为60和最后一个单元为102的行向量为0,且对于(102,*,60)这一规则对中同样产生一行0向量,而产生的这一行0向量可以是这两个单元中的任意一个。

因此,只有在 F 向量中对应于规则204、第一个单元为60、最后一个单元为102的位全为0,且(102,*,60)规则对对应的位同时为0或1时,$rank[T+I]=rnak[T+I,F]$ 才成立,此时的 F 总共有 $2^{l_1-l_{0_d}}(C^0_{l_{0_d}}+C^1_{l_{0_d}}\cdots+C^{l_{0_d}}_{l_{0_d}}=2^{l_1}$ 种。

而且,当选取 F 向量使得 $rank[T+I]\neq rnak[T+I,F]$ 成立即使得 $rank[T+I]=rank[T+I,F]$ 不成立时,方程(5)有解的充要条件是方程(6)恒成立。此时,可推出由相应的补规则替换后的细胞自动机为群细胞自动机,且齐圈长相等。

所以,总共有 $2^n-2^{l_1}=2^{l_1}(2^{l_0}-1)$ 种 F 使得 $rank[T+I]\neq rank[T+I,F]$,即其对应的细胞自动机为圈长相等的群细胞自动机。[证毕]

定理1和定理2说明:如果由规则60、102和204构成的混合细胞自动机为群细胞自动机,那么我们可以构造出一组细胞自动机,其转移状态的圈长相等,并等于原细胞自动机的阶 p 或为其2倍。如由规则(60,102,204,60)规则组成的混合细胞自动机为阶 $p=2$ 的群细胞自动机,其状态转移矩阵为:

$$T=\begin{bmatrix}1&0&0&0\\0&1&1&0\\0&0&1&0\\0&0&1&1\end{bmatrix}$$

,并有 $l_1=rnak(T+I)=1$ 和 $l_0=3$。其中 $l_{0_1}=2, l_{0_d}=1$。所以对于规则为(60,102,204,60)的细胞自动机派生出的具有置换群特性的细胞自动机总共有 $2^{l_1}\times(2^{l_0}-1)=14$ 种,其中有7种的阶为 $m=p=2$,其他7种的阶为 $m=2p=4$。

对于具有置换群特性的细胞自动机,其状态转移矩阵方程满足:

$$X^t=F+TX^{t-1} \tag{8}$$

在具有 N 个细胞单元的具有置换群特性的细胞自动机(零边界)中,输入一 N 维向量 V 与细胞自动机的状态配置进行模二加运算有:

$$X^t=F+TX^{t-1}+V^{t-1} \tag{9}$$

对(9)式进行 l 次迭代并以 X^0 为初始状态有:

$$X^l=(\sum_{i=0}^{l-1}T^i)F+T^lX^0+\sum_{i=0}^{l-1}T^{l-i-1}V^i \tag{10}$$

方程(10)两边同时左乘 T^{km-l} 为:

$$T^{km-l}X^l=T^{km-l}(\sum_{i=0}^{l-1}T^i)F+T^{km-l}T^lX^0+T^{km-l}\sum_{i=0}^{l-1}T^{l-i-1}V^i \tag{11}$$

方程(11)可写为:

$$X^0=T^{km-l}(\sum_{i=0}^{l-1}T^i)F+T^l(T^{km-2l}X^l)+\sum_{i=0}^{l-1}T^{l-i-1}(T^{km-l}V^i) \tag{12}$$

方程(10)和方程(12)可改写为:

$$\begin{cases}X=T^lX^0+((\sum_{i=0}^{l-1}T^i)F+\sum_{i=0}^{l-1}T^{l-i-1}V^i)\\ \quad=T^lX^0+K_e, l=1,2,\cdots,m-1\\ X^0=T^{km-l}X^l+((\sum_{i=0}^{l-1}T^i)(T^{km-l}F)+\sum_{i=0}^{l-1}T^{l-i-1}(T^{km-l}V^i))\\ \quad=T^{km-l}X^l+K_d, k=1,2,\cdots\end{cases} \tag{13}$$

方程组(13)是细胞自动机置换群加密方法的模型,它表明:对于具有置换群特性的细胞自动机,可以将具有 $T^m=I$ 的一组细胞自动机 $CA_i, i=0,1,2,\cdots,M-1$、细胞自动机迭代的次数 l 和输入向量 $\{V^i, i=0,1,2,\cdots,l-1\}$ 作为密钥来实现信息的加解密。该方法使用相同的细胞自动机即相同的设备来实现加解密,其中加密密钥为 $K_e=(\sum_{i=0}^{l-1}T^i)F+\sum_{i=0}^{l-1}T^{l-i-1}V^i$,而解密密钥为 $K_d=(\sum_{i=0}^{l-1}T^i)(T^{km-l}F)+\sum_{i=0}^{l-1}T^{l-i-1}(T^{km-l}V^i)$。加密时,只需将信息作为原细胞自动机初始状态 X^0 进行 l 次迭代,然后将迭代的状态与加密密钥 K_e 进行模二加运算即可。而解密只需要先将接收到的密文 X^l 作为原细胞自动机的初始状态进行 $km-l$ 次迭代,然后将其与解密密钥 K_d 进行模二加运算即可完成解密。

结束语 本文提出的基于细胞自动机置换群加密方法与文[4]的方法相比,本方法在几乎不增加系统复杂性的同时可以大大增加系统的密钥空间,并可提供灵活的加解密方法;同时如果采用细胞自动机适合的VLSI或ASIC来实现时,系统具有非常高的处理速度。如对于具有 n 个细胞单元的细胞自动机,设具有置换群阶为 p 的细胞自动机的数目为 M,其迭代的次数为 $0<l<mp$,那么,系统具有的密钥空间为 $M\sum_{i=1}^{mp-1}2^{2^i}$,可以抵抗唯密文穷举法的攻击;其加解密速度为 $\frac{n}{l}\times\frac{1}{\Delta T}(bps)$,其中 ΔT 为实现芯片的处理速度,在一般情况 $l=n$、$\Delta T=10ns$ 时,其处理速度为 $100Mbps$,这要比传统的加解密处理方法快得多。

参 考 文 献

1 Wolfram S. Theory and Application of Cellular Automata. World Scientific, Singapore, 1986
2 Wolfram S. Origins of Randomness in Physical System. Physical Review Letters, 1985, 55(5): 449～452
3 Wolfram S. Cryptography with Cellular Automata. Advances in Cryptology, 1985. 429～432
4 Guan P. Cellular Automata Public-key Cryptosystems, Complex Systems, Vol. 1, 1987
5 Nandi S, Kar B K, Chaudhuri P P. Theory and Applications of Cellular Automata in Cryptography. IEEE Trans. Compu., 1994, 43 (12)
6 Farmer D, Toffoli T, Wolfram S. Cellular Automata. Physica D, 1984, 10(1)
7 Wolfram S. Statistical Mechanics of Cellular Automata. Review Modern Phys., 1983, 55(3): 601～644
8 Wolfram S. University and Complexity in Cellular Automata. Physica D, 1984, 10(1)
9 Toffoli T, Margolus N. Invertible Cellular Automata: A Review. Physica D, 1990, 45: 229～253
10 Pries W, Thanailakis A, Howard C. Card, Group Properties of Cellular Automata and VLSI Application. IEEE Trans. Computers, 1986, C-35(12): 1013～1024
11 Das A K, Ganguly A, et al. Efficient Characterisation of Cellular Automata. IEE Proceedings, 1990, 137(1): 81～87