一类细胞自动机安全性刻划与密码体制增强*

邹新瑞
(广州市白云区科学技术局, 广东 广州 510430)

摘 要: 前人采用 $r=1$ 线性细胞自动机的简单、局部与并行加密优点设计了几类高速密码体制, 但都被破译了。系统分析了 $r=1$ 细胞自动机密码体制, 证明了 $r=1$ 线性细胞自动机作为密码学的缺陷, 单纯利用线性细胞自动机加密易被线性逼近与易受差分攻击, 因而必须采用辅助信息增强密码系统安全。针对此构造了两类加密体制: A 类加密体制以非线性变换作为 $r=1$ 线性细胞自动机的非严格雪崩准则的混淆性不足的补偿, 而细胞自动机则作为扩散使用; B 类则是使用一次一密机制增强密码系统的安全性。A 类加密体制安全性依赖非线性变换, 但 A 类密码体制性能仍不如 DES 传统加密机制; 而 B 类加密体制是安全的且在性能上是高速的, 但实现复杂且只能用在通信加密中。

关键词: 细胞自动机; 布尔函数; 分组加密算法; 非线性变换; 一次一密乱码本
中图分类号: TP393.08 文献标识码: A 文章编号: 0529-6579 (2005) S2-0141-06

网格计算加速海量数据应用, 并使得细胞自动机的低成本、高速加密特性重新被提起。

数学家 Stanislaw M. Ulam 与 John von Neumann 在 50 年代提出细胞自动机以来, 细胞自动机已经在生物、工程、密码等学科进行了广泛的研究与应用。细胞自动机是一个时间、空间与状态离散的动力系统。由于细胞自动机的离散性、并行性与混沌性, 因而在密码学领域占有一席之地。

很多学者对细胞自动机密码学进行了研究。细胞自动机能够通过简单规则多次迭代产生长周期的伪随机数, 因而 S. Wolfram 1986 年提出了细胞自动机产生的伪随机数在流密码中的应用[1]。流密码是一个简单的群运算, 安全性依赖于随机数熵值。文[1]中细胞自动机变换类似于非线性反馈转换移位寄存器 (FCSR), 产生的随机数具有较大的熵值[2]。有学者证明了细胞自动机产生的伪随机数在硬件实现是有效的, 而在软件实现有效性就要弱一些。并且在同等条件下, 细胞自动机产生的伪随机数的安全性比传统的伪随机数发生器的安全性要低[2]。细胞自动机产生的随机序列的安全性是可破译的, 且产生的序列流安全强度依赖于初始种子。

由于细胞自动机产生混沌状态依赖于初始状态, 并且在一些规则中, 每个状态可能具有多个父状态, 因而从混沌状态回朔到初始状态是一个 NP 问题。细胞自动机能够被大规模并行硬件实现, 因而为了高性能加密, 很多学者将细胞自动机应用到分组密码系统中。文[3]提出了细胞自动机分组密码学, 但是不久被 Blanckburn 等[4] 破译了。文[5]提出了一个新分组加密方法, 但是由于仿射特性, 而不能达到安全特性。文[6]提出了一种新颖的方法, 四个安全等级, 主细胞自动机、次细胞自动机、CMN 与密钥混合, 其中 CMN 是非线性变换, 但是不易抵挡选择明文攻击[7,8]。这些细胞自动机密码体制都不是安全的, 本文的工作主要分为

1) $r=1$ 细胞自动机的安全性刻划。

2) A 类细胞自动机密码体制安全增强与算法评估。

3) B 类细胞自动机高速加密协议与算法评估。

1 细胞自动机基础

细胞自动机 (Cellular Automata, CA) 是时间、空间与状态都离散的动力系统。在规则网格中的细胞取有限的离散状态, 根据局部规则作同步更新。群细胞通过简单的相互作用而构成动态系统的演化。

定义 1 (细胞自动机) 细胞自动机是 $CA=(A_D, Z_q, f_i, (o, \bar{r}), B)$ 四元组, 其中

(1) 空间结构:

$$A_D=\prod_{i=0}^{D-1} Z_{N_i}=\{\bar{i}=(i_0, i_1, \cdots, i_{D-1}) \mid i_0 \in Z_{N_0}, i_1 \in Z_{N_1}, \cdots, i_{D-1} \in Z_{N_{D-1}}\}$$

是由 D 维细胞自动机单元构成的空间结构, 其中

* 收稿日期: 2005-04-02
作者简介: 邹新瑞 (1962 年生), 男, 工程师; E-mail: kjzxr@by.yov.cn

$\prod_{i=0}^{D-1} Z_{N_i} = Z_{N_0} \times Z_{N_1} \times \cdots \times Z_{N_{D-1}}$ 为集合的笛卡尔集，$Z_{N_i} = \{0, 1, \cdots, N_i - 1\}$ 为模 N_i 的整数集合，$\vec{i} = (i_0, i_1, \cdots, i_{D-1})$ 为细胞单元的 D 维空间地址索引值。

(2) 状态空间 Z_q：

细胞自动机中细胞单元 $\vec{i}$ 的状态取值范围，一般为具有 q 个元素的有限交换环 $Z_q = \{0, 1, \cdots, q-1\}$，状态赋值函数 $s^t\vec{i}$ 确定了 t 时刻细胞自动机中第 $\vec{i}$ 个细胞单元与状态空间 Z_q 之间的映射关系

$$s^t\vec{i}[\prod_{i=0}^{D-1} Z_{N_i}] \times \xrightarrow{s} Z_q, \vec{i} \in \prod_{i=0}^{D-1} Z_{N_i}, t \in \mathbf{N}$$

(3) 邻域函数规则 $f_i(o, \vec{r})$：

称由细胞自动机的领域半径 $\vec{r} = (r_0, r_1, \cdots, r_{D-1})$ 确定的第 $\vec{i}$ 单元 $\eta\vec{i}(o, \vec{r}) = \{s^{'}\vec{j}^0 \mid o \in Z_0, |j_0 - i_0| \leqslant r_0, |j_1, i_1| \leqslant r_1, \cdots, |j_{D-1} - i_{D-1}| \leqslant r_{D-1}\}$，$O$ 阶邻域状态配置与其转移状态 $S^{t+1}\vec{i}$ 之间的映射

$$S^{t+1}\vec{i} = f_i(o, \vec{r})(s^{t-0}\vec{j} \mid o \in Z_0, |j_0 - i_0 \leqslant r_0, \cdots, |j_{D-1} - i_{D-1} \leqslant r_{D-1})$$

为细胞自动机的邻域函数规则 $f_i(o, \vec{i})$。细胞自动机邻域半径由确定的邻域与由 $[\vec{r} = (r_0, r_1, \cdots, r_{D-1}) \mid \sum_{i=0}^{D-1} r_i \leqslant k]$ 确定的 J_K 邻域与由 $[\vec{r} = (r_0, r_1, \cdots, r_{D-1}) \mid r_0 \leqslant k, r_1 \leqslant k \cdots, r_{D-1} \leqslant k]$ 确定的 H_K 邻域两种。

(4) 边界条件 B：

边界条件确定了某个细胞单元 $\vec{i} = (i_0, i_1, \cdots, i_{D-1})$ 邻域半径 $\vec{r} = (r_0, r_1, r_{D-1})$ 之内的邻域单元在超出细胞自动机空间结构时的处理方法，它包括固有边界条件与循环边界条件：固定边界将超出的单元状态看成固定状态，即 $[S^{t-0}\vec{j} = k \mid o \in Z_0, s^{t-0}\vec{j} \in \eta\vec{i}(0, \vec{r}), \vec{j} \notin A_D, k \in Z_q]$；循环边界则将其在细胞空间上取模操作，即 $[S^{t-0}\vec{j} = S_j^{t-0} \bmod \prod_{i=0}^{D-1} N_i \mid o \in Z_0, S_j^{t-0} \in \eta_i^t (o, \vec{r}, j \notin A_D]$

设 d 代表空间维数，N 表示细胞空间，k 代表细胞的状态，L 表示一个所有邻域内细胞的组合。并在一个有限集合 S 中取值，r 表细胞的邻居半径。

$$A = (L, d, S, N, r)$$

$GF(2)$ 是状态集 S 只有两个元素 $\{0, 1\}$，即状态个数 $k = 2$，邻域半径 $r = 1$ 的一维细胞自动机。邻域集 N 的个数 $2r = 2$，局部映射 $f: S_3 \to S$ 可记为：

$$S_i^{t+1} = f(S_{i-1}^t, S_i^t, S_{i+1}^t)$$

其中变量有 3 个，每个变量取 2 个状态值。

例如 RULE 30：

t 10110101101

$t-1$ 010010101

对线性细胞自动机：

$$v_i[t+1] = f_i(v_{i-1}[t], v_i[t], v_{i+1}[t])$$

定义 2 (线性变换) 仿射变换 $\mathbf{R}^n$ 是 $F: \mathbf{R}^n \to \mathbf{R}^n$ 的，对所有 $p \in \mathbf{R}^n$ 映射：$F(p) = Ap + q$，A 是 $\mathbf{R}^n$ 的一个线性变换。

定义 3 (仿射细胞自动机) 一个细胞自动机称为仿射细胞自动机，满足

$$f_i(v_{i-1}[t], v_i[t], v_{i+1}[t]) = w_{i-1}v_{i-1}[t] + w_iv_i[t] + w_{i+1}v_{i+1}[t] + u_i$$

定义 4 (附加细胞自动机) 如果细胞自动机表示为：

$$f(v_1, v_2, \cdots, v_{n+k}) \sum \lambda X_{n+1} \bmod r \quad \lambda \in S$$

则称为附加细胞自动机。

2 细胞自动机安全性刻划

2.1 布尔函数安全准则刻化

定义 5 (相关免疫性) 设 f 是 n 元布尔函数，ξ 是它的序列，如果对任意的 l 有：$<\xi, l> = 0$，l 是线性函数 $\psi(x) = <\alpha, x>$ 的序列，$1 \leqslant w(\alpha) \leqslant k$，称 f 是 k 阶相关免疫的。

定义 6 (线性结构) 如果对于任意的 $\alpha \in F_2^n$，$|\triangle\alpha| = 2^n$，称 α 是 f 的线性结构。

定义 7 (扩散准则) 如果对任意的 $\alpha \in F_2^n$，$\triangle(\alpha) = 0$，称 f 满足扩散准则。

定义 8 (满足 k 次扩散准则) 如果对任意的 $\alpha \in F_2^n$，$1 \leqslant w(\alpha) \leqslant k$ 有：$\triangle(\alpha) = 0$，称 f 满足 k 次扩散准则。

定义 9 (满足严格雪崩准则) 如果对任意的 $\alpha \in F_2^n$，$w(\alpha) = 1$ 有：$\triangle(\alpha) = 0$，称 f 满足严格雪崩准则。

2.2 细胞自动机布尔函数密码性质

定义 10 n 元布尔函数 $f(x_1, x_2, \cdots, x_n)$ 称为 n 元严格雪崩准则布尔函数，当且仅当对任意的单位向量 $e_i = (0, \cdots, 1 \cdots, 0)$，$1 \leqslant i \leqslant n$ 成立

$$\tilde{\omega}(f(x + e_i) + f(x)) = 2^{n-1}$$

定义 11 RULE 30 细胞自动机为布尔函数

$$f(x_{i-1}, x_i, x_{i+1}) = (x_{i+1}x_i + x_{i+1} + x_i + x_{i-1}), 1 \leqslant i \leqslant n$$

定理 1 RULE 30 细胞自动机 F_2^n 比其它 $r = 1$ 细胞自动机更适合加密。

证明 (1) RULE 30 细胞自动机包滑的 0，1 状态的比例为 1/2。

$$\begin{cases} I = \sum_{i=0}^{I} p_i \times \log \frac{1}{p_i} \\ \sum_{i=0}^{I} p_i = 1 \end{cases}$$

$$I = p_o \times \log \frac{1}{p_o} + (1 - p_o) \times \log \frac{1}{1 - p_o},$$

将 p_o 作为自变量，使用导数法求最大值可得，当 $p_o = 1/2$ 的时候有

$$I_{\max} = \sum_{i=0}^{I} \frac{1}{2} \times \log 2$$

从而 $r=1$ 细胞自动机 RULE30 的信息量最大，产生的混沌效应最好。

(2) RULE 30 细胞自动机 F_2^n 是最适合加密 $r=1$ 线性细胞自动机的规则数量为 2^{2^3}，为 256 个规则。

首先：最大信息熵包括 RULE 15, RULE 30, RULE 45, RULE 51, RULE 54, RULE 57, …, RULE 60, RULE 62, RULE 85, …, RULE 90, RULE 102, RULE 135, RULE 150, …RULE 210 等。

其次：具高混沌效应又具有最大信息熵的规则：RULE 30, RULE 54, RULE 60, RULE 86, RULE 90, RULE 102, RULE 109, RULE！135, RULE 149, RULE 150, RULE154, RULE 165, RULE 210。

然后：附加细胞自动机是不安全的[4]，附加细胞自动机的规则有：RULE 0, RULE 60, RULE 90, RULE 102, RULE 150, RULE 170, RULE 204, RULE 240。去除这些规则，则为下列：

RULE 30, RULE 54, RULE 86, RULE 135, RULE 149, RULE 154, RULE 165, RULE 210

这些规则的循环周期比较见图 1，从图可以直观看出长周期的规则为 RULE 30, RULE 86, RULE 149。

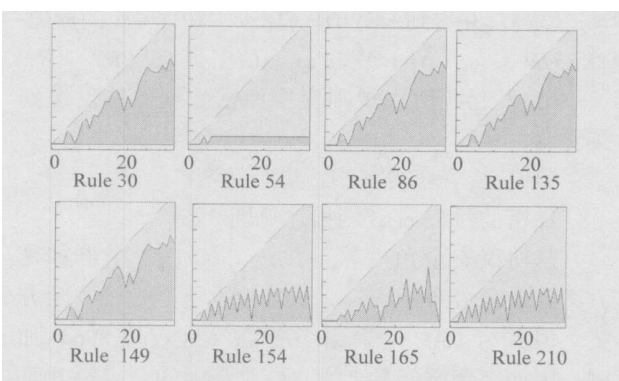

图 1　细胞自动机循环周期图

Fig. 1　Cellular automate cycle illustration

最后：剩下四个规则的计算特性，见图 2，通过比较研究发现 RULE 30, RULE 86, RULE 135, RULE 149 具有相同的信息熵与长周期循环，但 RULE 30 具有更高的复杂度。

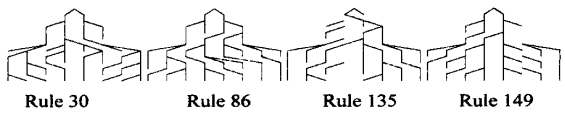

图 2　细胞自动机计算特性图

Fig. 2　Cellular automate calculate characteristic illustration

2.3　细胞自动机多输出函数的密码性质

定义 12　设细胞自动机 $S-box\ F_2^n \to F_2^m$ 是 $GF(2)^n$ 到 $GF(2)^m$ 的多输出函数，令

$$D(F) = \min\{\deg\beta \circ F) \mid \beta \neq 0, \beta \in GF(2)^m\} = \min\{\deg(\sum_{i=1}^{m} b_i f_i(x)) \mid (b_1, \cdots b_m) = \beta \neq 0, (b_1, \cdots, b_m) \in GF(2)^m\}$$

则称 $D(F)$ 为 $F(x)$ 的代数次数，这里 $f_i(x)$ $(\leqslant i \leqslant m)$ 是 n 元布尔函数，$\deg(\circ)$ 表示布尔函数的代数次数。当 $D(F)=k$ 时，称 $F(x)$ 为 k 次函数。

定义 13　设 $F_2^n \to F_2^n$，对于给定的 $\alpha \in GF(2)^n$，若 $F(x)+F(x+a)=C$，称 α 为 $F(x)$ 的线性结构。

性质 1　细胞自动机 $F(x): F_2^n \to F_2^m$ 为 α 的线性结构。

证明

$$\exists \alpha \in GF(2)^m$$

$$F(x)+F(x+\alpha) = (f_1(x)+f_1(x+\alpha), \cdots f_m(x)+f_m(x+\alpha)) = (c_1, \cdots, c_m) = C$$

因而细胞自动机 $F(x): F_2^n \to F_2^m$ 为 α 的线性结构。

性质 2　$f(x): F_2^n \to F_2$ 不满足严格雪崩准则 (Strict Avalanche Criterion, SAC)

证明

$$\forall e_i = (0, \cdots, 0, 1, 0 \cdots, 0) \in F_2^n, (1 \leqslant i \leqslant n)$$

$$f(x+e_{i-1})+f(x) = x_{i+1}x_i + x_{i+1} + x_i + (x_{i-1}+e_{i-1})x_{i+1}x_i + x_{i+1} + x_i + x_{i-1} = e_i \quad (1)$$

$$f(x+e_i)+f(x) = (x_{i+1}+e_i) + x_i + (x_{i+1}+e_i) + x_i + x_{i-1} + x_{i+}x_i + x_{i+1} + x_i + x_{i-1} = e_i x_{i+1} + e_i \quad (2)$$

$$f(x+e_{i+1})+f(x) = (x_{i+1}+e_i)x_i + (x_{i+1}+e_i) + x_i + x_{i-1} + x_{i+1}x_i + x_{i+1} + x_i + x_{i-1} = e_{i+1}x_i + e_{i+1} \quad (3)$$

由(1)式可知：$f(x+e_{i-1})+f(x)$ 为非平衡函数。

因而 $f(x)$ $:F_2^n \to F_2$ 不满足严格雪崩准则。

性质 3 细胞自动机 $F(x):F_2^n \to F_2^m$ 为非严格雪崩准则。

证明 由性质 2，易得细胞自动机 $F(x):F_2^n \to F_2^m$ 为非严格雪崩准则。

定理 2 细胞自动机不适合作 S－box。

证明 由定理 1 得：RULE 30 线性细胞自动机具有高熵值、长周期与高混沌性。

由性质 3 得：RULE30 线性细胞自动机不符合严格雪崩准则。

RULE 30 不适合作为 S－box。

3 两类加密体制

根据 RULE 30 性质 $r=1$ 细胞自动机变换不适合做 S－box，因而单纯依据 $r=1$ 细胞自动机变换的密码系统是不安全的，必须使用辅助信息增强密码系统的安全性。

3.1 A 类加密体制构造

为了能够弥补细胞自动机变换带来的安全缺陷，在连续变换过程中加入非线性变换，增强混乱效果。A 类加密函数见（4）式：

$$\Psi = (\eta_{(F_2^n \to F_2^n)^p} \to \theta_{(F_1^n \to F_2^n)^q} \oplus \kappa)^R \qquad (4)$$

其中，Ψ 代表输出结果，η 代表细胞自动机变换（包括逆变换），κ 代表密钥，$\oplus$代表密钥在有限域上的群运算，θ 代表非线性变换，$\to$代表映射关系，R 代表轮数量，p，q 代表内部变换次数。

例如可以推荐使用 RULE 30 细胞自动机逆向作为加密（正向为解密），R15 轮数，密钥 840 位，S－box 可以采用指数盒。从安全角度看，这种加密方式安全度是依赖于指数盒，而指数盒是目前仍然是安全的，被广泛应用与 SAFER，SAFER＋＋等密码体制中。细胞自动机在此密码体制中起扩散的作用。从实现的角度看，该种密码体制因为指数盒的原因，并没有体现细胞自动机易并行硬件实现的优点，反而相对复杂。从性能角度看，该种密码体制并行的特征没有体现出来，在实现过程中由于有大量访问 RAM 的操作，使性能仍然不如传统 DES 加密体制。

因而 A 类密码体制虽然增强了密码系统的安全性，却没有在性能上大幅度提高，其使用用途是有限的。

3.2 B 类密码体制构造

高速度运算、低成本实现与获得高安全级别本质上往往是冲突的。但往往在海量数据加密过程中，需要此类密码系统。B 类密码体制是解决高速度高安全运算问题，利用高速并行的细胞自动机加密特征与一次一密机制结合，增强 B 类细胞自动机的安全特性

$$\begin{cases} \Psi = (\eta_{(F_2^n \to F_2^n)^p} \oplus \kappa)^R \\ \kappa_\alpha \leftrightarrow k_\beta \end{cases} \qquad (5)$$

其中，Ψ 代表输出结果，η 代表细胞自动机变换（包括逆变换），κ 代表密钥，$\oplus$代表密钥在有限域上的群运算，θ 代表非线性变换，$\to$代表映射关系，R 代表轮数量，p 代表内部变换次数。$k_\alpha \leftrightarrow k_\beta$ 代表一次一密交换密钥协议。

例如推荐使用 Oakley 密码交换协议，η 使用 RULE 30 逆变换作为高速加密（解密为正向）算法，加密轮数为 16 轮，κ 有效位 896 位。

CAC（Cellular automata cryptosystem）高速加密协议是由 CAC 加密部件与密钥交换部件组成。CAC 加密部件是海量数据高性能对称加密部分，而 CAC 密钥交换部件则是实现一次一密机制。CAC 密钥交换部件是采用 cookie、签名等机制实现。

主要过程如下：

1) 发起者对于某个期望的远程应答者 IP 地址生成一个唯一的 Cookie（发起者为 Cookie-I，记为 CRY-I，响应者为 Cookie-R，记为 CRY-R），并选择所要求的通信组号 GRP、伪随机数 x，计算 $g^{\hat{}}x$，并同发起者所支持的 EHAO 算法列表与任意选择的随机数 Ni 发给期望应答的对，数字签名 EHAO 与数字签名。

2) 应答者校验报文的数字签名，确认发起者的身份，生成一个与之对应的 cookie，用以记录本次交换的当前状态。接着选择任意随机数 Ni 与随机数 y，计算 $g\hat{}y$，并发送给发起者。

3) 发起者检验数字签名，然后记录 $g\hat{}y$ 和 $CRY-R$。发起者都可以计算 $Z=(g\hat{}y)\hat{}x=(g\hat{}x)\hat{}y=g\hat{}(xy)$，并得到 KEYID＝CRY－I｜CRY－R 的标识

$$sKEYID = prf\{Ni \mid Nr, g\hat{}xy \mid CKY-I \mid CKY-R\}$$

4) 发起者使用规则变换加密数据，并发送到接受者；

5) 接受者获得密钥，进行解密。

加密的过程 petri 网描述见图 3。

从协议安全角度看：并行 CAC 是一个群加密方案，差分分布不均匀，从理论上不是一个安全方案。但并行 CAC 是采用 1024bit（有效位 896）加密，因而密钥空间是 2^{1024}，是非常大的，穷举几乎不可破译，即使通过差分分析之后的降次的密钥空间仍然是比较大，至少能抵挡选择密文攻击。Oakley 密钥交换协议被证明是安全的，因而本方案

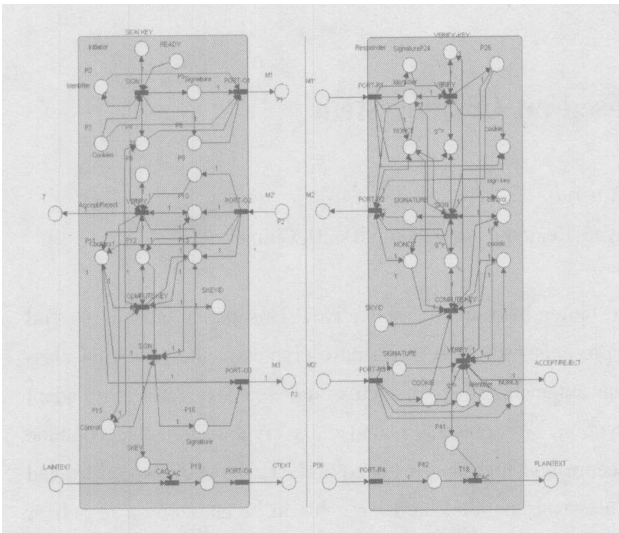

图 3　高速加密协议 petri 网模型

Fig 3　High-speed encryption perti net model illustration

是安全的。从实现角度看：密码系统的两个部分，Oakley 协议实现是相对复杂的，可使用软件程序编写代码，而并行 CAC 是非常容易硬件实现。因而整个系统是易实现的。从协议性能角度看：关键加密部件使用并行硬件实现，对 64 位使用流水设计，能在 1GHz 时钟频率下，理论加密速度达到 64Gb/s，性能大大高于当前的加密体制。但本算法用途上具有一定的局限性，只能使用在通信加密系统中。

4　结　论

细胞自动机密码学的研究已经有多年了，很多国内外文献在研究设计 $r=1$ 维线性细胞自动机应用，但公开的设计方案，都纷纷被破译。本课题的系统研究了 $r=1$ 的 256 个规则细胞自动机的密码学特性，研究结论是：

1) 从 shannon 的信息理论来看，对称密钥密码方案主要是混淆与扩散方法。单纯由 $r=1$ 细胞自动机变换构成密码方案抗差分与抗线性逼近的能力弱，方案的安全性比较弱。

2) $r=1$ 细胞自动机本身的特性使得在扩散特性上起一个很好作用。

3) 构建一个安全的细胞自动机密码体制必须具有辅助信息或者具有很大的密钥空间。如本文设计的第一类密码体制就是利用非线性 S－盒辅助信息；第二类密码体制是利用一次一密机制达到加密安全。

4) 我们用 VHDL 对两类加密体制的实例实现了 IP 核的设计与仿真（限于篇幅不描述），从加密性能上看 A 类密码体制性能不高，甚至低于传统的 DES 加密体制；B 类加密性能非常高，1G 的时钟频率下能够达到 64G 的加密性能，能使用在海量数据加密的网格计算中。

参考文献：

[1] WOLFRAM S. Random sequence generation by cellular automata[J]. Advances in Applied Mathematics, 1986, 7.

[2] WOLFRAM S. Origins of randomness in physical systems[J]. Physical Review Letters, 1985, 55: 449.

[3] NANDI S. Theory and Applications of Cellular Automata in Cryptography[J]. IEEE Transactions on Computers, 1997: 1346－1357.

[4] BLACKBURN S, MERPHY S, PATERSON K. Comments on ‘Theory and Applications of Cellular Automata in Cryptography’[J]. IEEE Transactions on Computers, 1997, 46(5): 637－638.

[5] GANGULY N, DAS A. Cellular atuomata model for cryptosystem[C] // Cellular automata Conference. Yakaham Uninversity, Japan 2000.

[6] SEN S, SHAW C. Cellular Automata Based Cryptosystem Information and Communications Security[C] // 4th International Conference, (ICICS 2002), Singapore, December 9－12, 2002.

[7] MURPHY S, PARTERSON K, WILD P. A weak cipher that generates the symmetric group[J]. Cryptology, 1994, 7: 61－64.

[8] 冯国登. 频谱理论及其在密码学中的应用. 北京：科学出版社, 2000.

Cellular Automata Based on Cryptosystem

ZOU Xin rui

(Science and Technology Bureau of Baiyun Region, Guangzhou 510430, China)

Abstract: Previous cellular automata bases cryptosystem are either insecure or ineffective. This paper proveds several theorems about cellular automata based on cryptosystem and presents two classes of secure cryptosystem. The first class cryptosystem is that increase nonlinear transform during cellular automata transform such as index S-box. In order to adopt property of cellular automata that low cost, high-speed encryption. We present second class cryptosystem that combine simple nonlinear transform and one time pad to reach both secure and high-speed encryption. Cryptosystems constructed from this scheme can be implemented in simply constructed massively parallel hardware. It can be counted on to deliver high encryption/decryption rates at low cost on data grid. At last, we implement these two schemes in VLSI and evaluate these two schemes' performance.

Key words: cellular automata; block cipher system; one time pad; affine transform; pipeline VLSI