دانشگاه شهید بهشتی

دانشکده ریاضی و علوم کامپیوتر

پایان نامه کارشناسی ارشد علوم کامپیوتر

موضوع

طرحی جدید برای تسهیم چندین-راز بر اساس اتوماتای سلولی[1]

استاد راهنما

خانم دکتر زیبا اسلامی

استاد مشاور

آقای دکتر کورش پرند

نگارش

جمال زارع پور احمدآبادی

شهریور ۸۸

[1] در این پایان نامه از حمایتهای مادی و معنوی مرکز تحقیقات مخابرات ایران تشکر می شود.

تاریخ ....
شماره ....
پیوست..................

بسمه تعالی

دانشگاه شهید بهشتی

«صورتجلسه دفاع از پایان نامه دانشجویان دوره کارشناسی ارشد علوم کامپیوتر»

تهران ۱۹۸۳۹۶۳۱۱۳ اوین
تلفن: ۲۹۹۰۱

بازگشت به مجوز دفاع شماره **۲۰۵۱/۲۰۰/د** مورخ **۱۳۸۸/۶/۲** جلسه هیأت داوران ارزیابی پایان نامه: **آقای جمال زارع پور احمدآبادی** شماره شناسنامه: **۱۵۴۷** صادره از: اردکان متولد: **۱۳۶۲** دانشجوی رشته کارشناسی ارشد **علوم کامپیوتر**

با عنوان:

طرحی جدید برای تسهیم چندین -راز بر اساس اتوماتای سلولی

به راهنمایی :

خانم دکتر زیبا اسلامی

طبق دعوت قبلی در تاریخ **۸۸/۶/۲۵** تشکیل گردید و بر اساس رأی هیأت داوری و با عنایت به ماده ۲۰ آئین نامه کارشناسی ارشد مورخ ۷۵/۱۰/۲۵ پایان نامه مزبور با نمره ۲۰ (بیست تمام) و درجه مورد تصویب قرار گرفت.

ردیف		نام استاد	مرتبه علمی	نام دانشگاه	امضاء
۱	استاد راهنما	خانم دکتر زیبا اسلامی	استادیار	شهید بهشتی	
۲	مشاور	آقای دکتر کورش پرند	استادیار	شهید بهشتی	
۳	داور	آقای دکتر حمیدرضا میمنی	دانشیار	شهید رجایی	
۴	داور	خانم دکتر لیلا شریف	استادیار	شهید بهشتی	

پیشکش به
محضر مقدس حضرت صاحب الزمان،
و چشمانی که به اشتیاق صبح ظهورش بارانی اند.

قدردانی

مَن لَم یَشکُر المخلوق، لَم یَشکُر الخالق
بر خود لازم می‌دانم از پدر و مادر سخت کوش مهربانم، شهدای گرانقدر و تمام عزیزانی که راه را برای ترفیع و تحصیل اینجانب هموار کرده‌اند خاضعانه سپاسگزاری کنم، از معلم‌های دلسوز مدرسه تا اساتید مجرب دانشگاه. در مورد این نوشتار، از زحمات و راهنماییهای استاد ارجمندم خانم دکتر اسلامی تشکر ویژه دارم همچنین از آقای دکتر پرند، آقای دکتر میمنی و خانم دکتر شریف به خاطر عنایت به این پایان نامه قدر دانی می‌کنم. همچنین از برادر عزیزم آقای شاهینی به خاطر مساعدت در نوشتن پایان نامه متشکرم و سعادت عزیزان را از خداوند عزیز خواستارم.

طرحی جدید برای تسهیم چندین راز بر اساس اتوماتای سلولی

چکیده
یک طرح تسهیم راز به روشی اطلاق می‌شود که طی آن یک یا چند راز (اطلاع مخفی) بین گروهی از افراد، سهامداران، توزیع می‌شود به گونه‌ای که تنها زیر مجموعه‌های خاصی از این افراد قادر به بازسازی راز یا رازها باشند. از ابزارهایی که برای این منظور به کار گرفته شده‌اند می‌توان به درونیابی چندجمله‌ای، قضیه باقیمانده چینی، آرایه‌های متعامد و اتوماتای سلولی اشاره کرد.

در این پایان نامه بعد از ذکر مقدمات ضروری و برخی از طرح‌های براساس چندجمله‌ای، به توضیح اتوماتای سلولی و طرح‌های براساس آن خواهیم پرداخت و سپس طرح‌هایی را جهت تسهیم چندین راز بر اساس اتوماتای سلولی و قضیه باقیمانده چینی پیشنهاد می‌دهیم. و در نهایت با استفاده از آن‌ها به حل دو مسأله باز در این زمینه می‌پردازیم.

ادامه این پایان نامه در سه فصل سازماندهی شده است. در فصل ۱، مسأله تسهیم راز معرفی و برخی مقدمات و مفاهیم اولیه در این زمینه تشریح خواهد شد. برخی طرح‌های تسهیم راز یکه و چندگانه اخیر در فصل ۲ معرفی می‌شود. و در نهایت طرح‌های ارائه شده توسط خودمان را در فصل ۳ خواهیم آورد.

واژه‌های کلیدی: رمزنگاری، تسهیم راز، اتوماتای سلولی، قضیه باقیمانده چینی، تسهیم راز تصویری

فهرست مطالب

لیست تصاویر

لیست جداول

فصل ۱

مقدمات و مفاهیم اساسی

در این بخش به بیان برخی پیش زمینه‌ها در مورد افزایش تبادل اطلاعات از طریق کانال‌های عمومی و به تبع آن افزایش عملیات خراب‌کارانه در این ارتباطات می‌پردازیم. آنگاه برخی از مفاهیم پایه از نظریه اعداد و رمزنگاری را به اختصار مرور می‌کنیم و به معرفی نمادهای استفاده شده در این پایان نامه می‌پردازیم. در ادامه شکل کلّی مسأله تسهیم راز را به عنوان راهکاری برای مقابله با جرایم کامپیوتری و فراهم کردن امنیت مطلوب معرفی می‌کنیم. این بخش را با ذکر چند طرح تسهیم راز سنتی و بیان ساختار کلّی آن به پایان می‌بریم.

ضرورت تسهیم راز و امنیت اطلاعات

در طول سه دهه گذشته شاهد فراگیر شدن استفاده از سیستم‌های کامپیوتری و پیوستن آن‌ها به هم از طریق شبکه‌ها بوده‌ایم. استفاده از اینترنت به عنوان شبکه ارتباطی عمومی (باز) گسترش خیره کننده‌ای یافته است چنان‌که فقدان آن حتی ساده‌ترین کارها را نیز با مشکل مواجه می‌کند. روز به روز بر تعداد استفاده کنندگان آن افزوده می‌شود آمارها نشان می‌دهد که تعداد کاربران اینترنت از رقم ۱۶ میلیون در سال ۱۹۹۵ و ۷۰۰ میلیون در سال ۲۰۰۴ به ۱.۴ بیلیون کاربر در سال ۲۰۰۸ افزایش یافته است.

با افزایش وابستگی زندگی ما به کامپیوتر در تمام سطوح، اطلاعات شخصی و حساس در سیستم‌های کامپیوتری ذخیره و از طریق سیستم‌های شبکه‌ای توزیع می‌شوند، گر چه این ابزارها به طرز چشمگیری زندگی ما را آسان کرده‌اند امّا استفاده از آن‌ها خطرات و تهدیدهایی را نیز به همراه داشته است. طبق برآوردی که توسط موسسه امنیت کامپیوتر [1] (CSI) روی ۵۰۰ سازمان در آمریکا انجام گرفت، مشخص شد که در حدود ٪۹۰ آن‌ها از ابزارهای امنیتی مثل آنتی ویروس، فایروال و یا سایر ابزارهای کنترل دسترسی استفاده می‌کنند [۷۳]. اما تنها ٪۲۳ از این سازمان‌ها ادعا کردند که طی ۵ سال گذشته در معرض دسترسی‌های خرابکارانه قرار نگرفته‌اند. گزارش به خوبی نشان می‌دهد که استفاده از روش‌هایی که امنیت داده‌های حساس را تضمین کند امری اجتناب ناپذیر است. گر چه نیاز به امنیت کامپیوتر همیشه وجود داشته است، اما امروزه این نیاز چنان جدی است که تکنولوژی ساخت سیستم‌ها را تحت تأثیر قرار داده است. در دوره کامپیوترهای بزرگ [2] منابع حساس و گران قیمت را از طریق محدود کردن دسترسی و سوء استفاده، محافظت می‌کردند، البته ایده‌های محدودی هم در زمینه رسیدن به امنیت بیشتر به کار می‌رفت اما محافظت از داده‌های حیاتی از طریق کنترل دسترسی فیزیکی به ماشین انجام می‌شد.

به تدریج با مطرح شدن شبکه و خصوصاً بحث محاسبات خادم/مخدوم [3]، تأمین امنیت شکل خود را از محدودیت دسترسی به ماشین به کنترل دسترسی به داده‌ها داد. در این راستا بسیاری از شرکت‌ها، داده‌های مهم خود، مثل اطلاعات کارمندان یا مالی، را در سرور خاصی ذخیره کردند که دستیابی به آن‌ها به مجوزی نیاز داشت که حق

[1] Computer Standard Institue

[2] Mainframe

[3] Client/Server

تقدم و سطح دسترسی را مشخص می‌کرد. در این هنگام، تکنیک‌هایی مانند تصدیق[۴] کاربر، رمز گذاری داده و سایر سیاست‌های امنیتی پا به عرصه وجود نهادند.

در اوایل دهه ۱۹۹۰ با ظهور شبکه عمومی اینترنت شرایط تغییر کرد، اگر چه این شبکه جهانی موجب سهولت در دسترسی و استفاده کاربران (مجاز) از منابع شد، اما راه را برای نفوذ خرابکاران و سودجویان به منابع دیگران فراهم کرد. کاربران مجاز با اطلاع از تکنیک‌های شبکه و امنیت آن از یک سو و مهاجمان خارجی از سوی دیگر جدی‌ترین خرابکاران به شمار می‌آیند. البته از عوامل تشدید کننده این قضیه اینست که ماشین‌ها و سیستم عامل‌هایی که به اینترنت متصل می‌شوند از امنیت بالایی برخوردار نیستند، و دانش و ابزارهای مربوط به کارهای امنیتی و هکری در اختیار همگان قرار دارد.

بر اساس آن‌چه به تلخیص در بالا آمد، مشخص است که در سال‌های اخیر محافظت از داده‌های حساس اهمیت ویژه‌ای یافته است. بنابراین اگر از اطلاعات مخفی کپی‌های زیادی تهیه شود، احتمال لو رفتن آن‌ها افزایش می‌یابد. از طرفی اگر تنها یک نسخه از این اطلاعات نگهداری شود، در صورت خرابی، دیگر امکان بازیابی آن‌ها کاملاً منتفی است. توجه داریم که تفاوتی ندارد که ما اطلاعات خود را رمز کنیم یا نه، زیرا در صورت رمز کردن، کلید رمزنگاری حکم داده مخفی را دارد و باز همین بحث‌ها مطرح است. فراتر از این مباحث در بسیاری از کاربردها مطلوب این است که داده‌های مخفی فقط وقتی آشکار و استفاده شوند که گروه خاصی از افراد حاضر باشند. اینجاست که تسهیم راز به عنوان یک راه حل مطرح می‌شود. ایده اصلی تسهیم راز اینست که داده مخفی (راز) به بخش‌هایی تقسیم می‌شود، طوری‌که با زیرمجموعه‌های خاصی از این بخش‌ها، بتوان راز را بازسازی کرد. با چنین ایده‌ای مهاجم برای بدست آوردن راز باید زیرمجموعه‌ای از این بخش‌ها را داشته باشد و برای این‌که راز قابل بازیابی نباشد (از بین برود) تعداد زیادتری از این بخش‌ها باید از بین برده شوند. ناگفته پیداست که راز در برابر خرابی و دزدی بارها مقاوم‌تر از روش‌های معمولی در رمزنگاری است.

مقدمه ای بر تسهیم راز

قبل از معرفی تسهیم راز، مسأله معروف زیر را از [۶۲] در نظر بگیرید: فرض کنید یازده دانشمند در حال کار روی یک پروژه سری هستند، آن‌ها اسناد پروژه را در یک صندوق قرار می‌دهند و می‌خواهند صندوق را چنان قفل کنند تا تنها در صورتی که لااقل ۶ نفر از دانشمندان حاضر باشند، بتوانند صندوق را باز کنند. در [۶۲] خواسته شده که حداقل تعداد قفل لازم، و کمترین تعداد کلیدهایی که هر دانشمند باید همراه داشته باشد، چند تاست؟ حال سعی می‌کنیم به این سؤالات جواب دهیم:

در مورد کمترین تعداد قفل‌ها، می‌دانیم که به ازای هر زیرمجموعه لااقل ۶ عضوی از دانشمندان به یک قفل مجزا احتیاج است. با کمی تساهل، کمترین تعداد زیرمجموعه‌های مجاز (تعداد قفل‌های لازم) برابر است با تعداد زیرمجموعه‌های شش عضوی از یک مجموعه یازده عضوی. یعنی:

$$\binom{11}{6} = \frac{11!}{6!\,(11-6)!} = 462.$$

از طرفی هر قفل ۶ کلید مختلف دارد و هر دانشمند باید یک کلید برای هر قفل به همراه داشته باشد (بقیه کلیدها توسط ۵ دانشمند آورده می‌شود) بنابراین کمترین تعداد کلیدهایی که یک دانشمند باید داشته باشد برابر است با تمام زیرمجموعه‌های ۵ عضوی از مجموعه ۱۰ عضوی (تعداد حالاتی که ۵ دانشمند از ۱۰ دانشمند انتخاب شوند):

$$\binom{10}{5} = \frac{10!}{5!\,(10-5)!} = 252.$$

جواب بالا درست است زیرا:

- هر دانشمند باید ۲۵۲ کلید داشته باشد، بنابراین تعداد کل کلیدها برابر است با: $11 \times 252 = 2772$.

---

[۴] Authentication

- هر قفل به ۶ کلید احتیاج دارد، پس برای ۴۶۲ قفل تعداد کل کلیدهای لازم برابر است با: $6 \times 462 = 2772$.

مسلم است که این یک مسأله واقعی و عملی نیست، اما شرایطی در دنیای واقعی وجود دارد که لازم است اطلاعات حساسی در بین گروهی از نهادها توزیع شود طوری‌که فقط زیرگروه‌های از پیش تعیین شده‌ای از آن نهادها بتوانند اطلاعات را بازیابی کنند. اینجاست که مسأله تسهیم راز به عنوان یک راه حل مناسب مطرح می‌شود.

تسهیم راز اولین بار در سال‌های ۱۹۷۹ به طور مستقل توسط شمیر[۵] [۷۷] و بلکلی[۶] [۱۰] مطرح، و راه حل‌هایی برای آن ارائه شد. روش شمیر [۷۷] که حالت خاصی از روش بلیکلی [۱۰] و اندکی کاراتر از آن است، بر اساس درونیابی چندجمله‌ای لاگرانژ و روش بلیکلی بر اساس اشتراک صفحات هندسی می‌باشد و هدف اصلی آنها، ارائه روشی برای مدیریت و محافظت از کلیدهای مخفی بود. از آن زمان به بعد طرح‌های مختلفی برای تسهیم راز پیشنهاد شده است، که هر کدام در جهت هدف خاصی توسعه یافته است، از محافظت از کلیدها در رمزنگاری و پروتکل‌های امنیتی گرفته، تا کاربردهای روزمره‌ای مثل رأی گیری الکترونیکی و پول الکترونیکی [۵۳] و حتی کاربردهایی مثل پرتاب موشک، باز کردن گاو صندق و ...، که موافقت چند نفر شرط انجام این کارهاست [۷۹].

۱.۱ مفاهیم پایه

۱.۱.۱ نظریه اعداد

در این بخش به بیان برخی مفاهیم ابتدایی از نظریه اعداد می‌پردازیم. برای جزئیات بیشتر می‌توانید به [۲۷] مراجعه کنید.

تعریف ۱. اگر $a, b \in \mathbb{Z}$ و $b \neq 0$ باشند، خارج قسمت تقسیم a بر b را با $a\ div\ b$ و باقیمانده را با $a\ \ mod\ b$ نشان می‌دهند.

اگر باقیمانده تقسیم a بر b صفر شود، یعنی $a\ \ mod\ b = 0$، گویند a بر b بخش پذیر است یا b مقسوم[۷] a است و آن‌را با $b|a$ نشان می‌دهیم (به عبارت دیگر b، a را می‌شمارد یا عاد می‌کند).

تعریف ۲. عدد صحیح $p > 1$ که غیر از خودش و 1 شمارنده دیگری ندارد را عدد اول نامند. عدد صحیح $n > 1$ که اول نباشد، مرکب خوانده می‌شود و این یعنی باید بتوان n را به صورت حاصل ضرب اعداد صحیحی مثل $n = a \times b$ بیان کرد که $1 < a, b < n$.

در حالت کلی هر عدد صحیح مثبت را می‌توان به صورت حاصل ضرب اعداد اول بیان نمود. این عمل را فاکتور کردن به عامل‌های اول گویند و بدون توجه به ترتیب عامل‌ها در حاصل ضرب، فاکتور کردن یک عدد به عوامل اول، همواره یکتاست.

تعریف ۳. بزرگترین مقسوم علیه مشترک[۸] a و b، بزرگترین عدد صحیح مثبتی است که هر دو عدد a و b را تقسیم می‌کند و آن‌را با $gcd(a, b)$ یا (a, b) نشان می‌دهند.

اگر $gcd(a, b) = 1$، اعداد a و b را نسبت به هم اول[۹] گویند. برای یافتن بزرگترین مقسوم علیه مشترک دو الگوریتم وجود دارد: براساس فاکتور کردن اعداد، و بر اساس تقسیم‌های پی در پی (الگویتم اقلیدسی). در حالت کلی اگر $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ و $a_1^2 + a_2^2 + \cdots + a_n^2 \neq 0$، آنگاه بزرگترین مقسوم علیه مشترک $a_1, a_2, \ldots, a_n$ به صورت $gcd(a_1, a_2, \ldots, a_n)$ نمایش داده می‌شود.

---

[۵] Shamir

[۶] Blakley

[۷] Divisor

[۸] Greatest common divisor

[۹] Relatively prime

تعریف ۴. کوچکترین مضرب مشترک[۱۰] اعداد صحیح $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ و $a_1 . a_2 . \ldots . a_n \neq 0$، که با $lcm(a_1, a_2, \ldots, a_n)$ نشان می‌دهیم برابر است با عددی مثل c که دو شرط داشته باشد ۱) مضرب مشترک این اعداد باشد، یعنی $a_1 \mid c, a_2 \mid c, \ldots, a_n \mid c$. ۲) کوچکترین عددی باشد که شرط ۱ را دارد.

یکی از مفاهیم پایه و بسیار پرکاربرد در نظریه اعداد بحث حساب پیمانه‌ای یا همنهشتی‌ها است.

تعریف ۵. اگر a, b و n اعداد صحیح و $n \neq 0$ باشند. گویند a همنهشت b در پیمانه n است اگر $a - b$ مضرب (مثبت یا منفی) n باشد، و آن را با

$$a \equiv b \pmod n$$

نشان می‌دهند.

به بیان دیگر $a \equiv b \pmod n$، اگر a و b به اندازه مضربی از n تفاوت داشته باشند، یعنی $a = b + kn$ که k مقداری صحیح می‌باشد (مثبت یا منفی). اغلب با اعداد صحیح در $(mod\ n)$ کار می‌کنیم، و به صورت $\mathbb{Z}_n$ نشان می‌دهیم. این مطلب را با مجموعه $\{0, 1, 2, \ldots, n-1\}$ و جمع و تفریق و ضرب، در پیمانه n بیان می‌کنیم. عدد صحیح مثل a را به صورت باقیمانده تقسیم آن بر n بیان می‌کنیم، یعنی

$$a = nq + r \quad , 0 \leq r < n.$$

بنابراین $a \equiv r \pmod n$ و هر عدد صحیح همنهشت عددی مثل r که $0 \leq r < n$ می‌باشد.
برای انجام عملیات حسابی (جمع و تفریق و ضرب) روی اعداد در $(mod\ n)$ ابتدا با آن‌ها مانند عملیات روی اعداد صحیح رفتار کرده و در نهایت اگر حاصل بزرگتر از $n-1$ بود آن‌را بر n تقسیم و باقیمانده را به عنوان حاصل قلمداد می‌کنیم.
در مورد تقسیم دقت بیشتری لازم است زیرا حاصل تقسیم اعداد گویا می‌باشد. یک قانون کلی این است که تنها در صورتی می‌توان در $(mod\ n)$ تقسیم بر a را انجام داد که $gcd(a, n) = 1$ باشد. به صورت رسمی، اگر a, b, c, n اعداد صحیح و $n \neq 0$ و $gcd(a, n) = 1$ باشد، از $ab \equiv ac \pmod n$ نتیجه می‌شود که $b \equiv c \pmod n$.
در حالت کلی برای حل $ax \equiv b$ که $gcd(a, n) = d > 1$ باشد راه حل زیر ارائه می‌شود:
۱) اگر $d \nmid b$ جواب ندارد.
۲) اگر $d \mid b$ همنهشتی زیر را در نظر بگیرید

$$(a/d)x \equiv b/d \pmod{n/d}.$$

با توجه به این که $a/d, b/d, n/d$ همگی اعداد صحیح هستند و $gcd(a/d, n/d) = 1$. همنهشتی اخیر را با روش قبل می‌توان حل نمود. اگر x_0 جواب این همنهشتی باشد جواب رابطه اصلی به صورت زیر خواهد بود:

$$x_0, x_0 + (n/d), \ldots, x_0 + (d-1)(n/d) \pmod n$$

گفتیم که $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$، حال مجموعه $\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n \mid gcd(a, n) = 1\}$ را در نظر می‌گیریم.

تعریف ۶. برای هر عضو $a \in \mathbb{Z}_n^*$، مرتبه a نسبت به پیمانه n یعنی کوچکترین عدد صحیح مثبت k طوری که $a^k \equiv 1 \pmod n$ و به صورت $ord_n(a)$ نشان داده می‌شود.
یک ریشه اولیه[۱۱] در پیمانه n، عضوی مانند $a \in \mathbb{Z}_n^*$ است طوری که $ord_n(a) = |\mathbb{Z}_n^*|$. که $|S|$ اندازه مجموعه S را مشخص می‌کند.

---
[۱۰] Least common multiple
[۱۱] Primitive root

۲.۱.۱ مسأله لگاریتم گسسته

امنیت بسیاری از سیستم‌های رمزنگاری بر مسأله‌ای به نام لگاریتم گسسته[۱۲] استوار است مسائلی مانند توافق کلید دیفی-هلمن[۱۳] و مشتقات آن، سیستم رمزنگاری الجمال، امضای دیجیتال[۱۴] الجمال و مشتقات آن و غیره از این دسته‌اند.

تعریف: فرض کنید G یک گروه دوری متناهی از مرتبه n، α یک مولد آن و $\beta \in G$، عضوی از گروه باشد. لگاریتم گسسته β در پایه α، که با $\log_\alpha \beta$ نشان داده می‌شود، عدد صحیحی مثل x که $0 \leq x \leq n-1$ است طوری که $\beta = \alpha^x$.

مثال ۱. فرض کنید $p = 97$ باشد در این صورت $\mathbb{Z}_{97}^*$ یک گروه دوری از مرتبه $n = 96$ و $\alpha = 5$ یک مولد برای آن می‌باشد، از آن‌جا که $5^{32} \equiv 35 \ (mod\ 97)$، پس $\log_5 35 = 32$ در $\mathbb{Z}_{97}^*$ می‌باشد.

اگر α مولد گروه دوری G از مرتبه n، $\beta, \gamma \in G$ و s عددی صحیح باشد، $\log_\alpha(\beta\gamma) = (\log_\alpha \beta + \log_\alpha \gamma) \ mod\ n$ و همچنین $\log_\alpha(\beta^s) = s \log_\alpha \beta \ \ mod\ n$.

مسأله لگاریتم گسسته **DLP**: اگر p عددی اول و α مولدی برای $\mathbb{Z}_p^*$ و $\beta \in \mathbb{Z}_p^*$ باشند، عدد صحیح x که $0 \leq x \leq p-2$، را بیابید طوری که $\alpha^x \equiv \beta \ (mod\ p)$.

مسأله لگاریتم گسسته تعمیم یافته **GDLP**: با گروه دوری متناهی G از مرتبه n، مولدی مثل α و عضوی مثل $\beta \in G$، عدد صحیح x که $0 \leq x \leq n-1$ را بیابید که $\alpha^x = \beta$.

سختی مسأله لگاریتم گسسته تعمیم یافته (GDLP) مستقل از مولد است. الگوریتم‌هایی برای حل مسأله GDLP پیشنهاد شده است که خواننده برای اطلاعات بیشتر می‌تواند به [۶۷] مراجعه کند.

۳.۱.۱ رمز نگاری کلید عمومی

الگوریتم‌هایی که برای رمزنگاری وجود دارد بر دو دسته کلی‌اند: رمزنگاری متقارن[۱۵] و رمزنگاری نامتقارن[۱۶]. در رمزنگاری متقارن عملیات رمزگذاری[۱۷] و رمزگشایی[۱۸] از طریق یک کلید انجام می‌شود. با توجه به این که در رمزنگاری همواره فرض می‌کنیم الگوریتم‌ها عمومی‌اند، در این روش تنها نکته مخفی کلید می‌باشد، بنابراین در رمزنگاری متقارن قبل از انجام عملیات باید به طریقی (ملاقات، ...) بر روی کلید مخفی توافق شده باشد.

اما در رمزنگاری نامتقارن، که رمزنگاری کلید عمومی[۱۹] نیز خوانده می‌شود هر موجودیتی که بخواهد داده مخفی‌ای را دریافت کند ، آلیس، به یک زوج کلید احتیاج دارد: کلید عمومی[۲۰] e و کلید خصوصی[۲۱] d. در یک سیستم امن، بدست آوردن d از روی e از نظر محاسباتی غیر ممکن است. تبدیل رمزگذاری، E_e، با استفاده از کلید عمومی تعریف می‌شود و از کلید خصوصی در تعریف تبدیل رمزگشایی، D_d، استفاده می‌شود.

هر موجودیتی، باب، که بخواهد پیام مخفی m را برای آلیس بفرستد یک کپی معتبر از کلید عمومی آلیس بدست می‌آورد و با استفاده از الگوریتم رمزگذاری، رمز شده آن پیام را بدست می‌آورد: $c = E_e(m)$، و سپس c را برای آلیس می‌فرستد. آلیس با استفاده از کلید خصوصی خود و الگوریتم رمزگشایی پیام باب را آشکار می‌کند: $m = D_d(c)$.

---

[۱۲] Discrete Logarithm Problem(DLP)

[۱۳] Diffie-Hellman key agreement

[۱۴] Dgital signature

[۱۵] Symmetric

[۱۶] Asymmetric

[۱۷] Encryption

[۱۸] Decryption

[۱۹] Public key

[۲۰] Public key

[۲۱] Private key

در این روش نیازی به توافق کلید بین طرفین نیست ولی از آنجا که همه از کلید عمومی آگاهی دارند، توجهات روی اعتبار کلید عمومی معطوف است و این که آلیس تنها فردی است که از کلید خصوصی متناظر آن اطلاع دارد. پس مسأله اصلی روش‌های کلید عمومی، خصوصی بودن و قابلیت اعتماد به آن‌ها است. مسأله دیگر این است که این روش‌ها در مقایسه با روش‌های کلید متقارن کندترند و به همین دلیل اغلب از آن‌ها برای توافق و انتقال کلید متقارن استفاده می‌شود و داده اصلی به روش متقارن منتقل می‌گردد.

در پروتکل‌های رمزنگاری هدف اصلی دشمن[۲۲] این است که پیام مخفی را بداند و اگر به این هدف برسد آن سیستم را شکسته شده، گویند. به همین دلیل الگوریتم‌های رمزنگاری برای مقاومت در برابر حملات دشمن بر اساس مسائلی که حل آن‌ها در حالت عادی غیر ممکن (سخت) است، بنا شده‌اند. در زیر به تشریح الگوریتم کلید عمومی RSA می‌پردازیم.

RSA[۲۳]، یکی از رایج‌ترین سیستم‌هایی است که برای رمزنگاری نامتقارن به کار گرفته شده است. امنیت این سیستم بر سختی فاکتور کردن اعداد صحیح استوار است و شامل مراحل زیر است:

ساخت کلید

هر موجودیت، مثلاً آلیس، باید طبق مراحل زیر برای خود یک زوج کلید بسازد:

۱. دو عدد اول بزرگ p و q را به صورت تصادفی انتخاب می‌کند، این دو عدد تقریباً هم اندازه باشند.

۲. $n = pq$ و $\varphi = (p-1)(q-1)$ را محاسبه می‌کند.

۳. عدد تصادفی e که $1 < e < \varphi$ را انتخاب می‌کند که $gcd(e,\varphi) = 1$ باشد.

۴. با استفاده از الگوریتم تعمیم یافته اقلیدس [۶۷] عدد صحیح یکتای d، که $1 < d < \varphi$ را چنان محاسبه می‌کند که $ed \equiv 1 \pmod{\varphi}$ باشد.

۵. آلیس (n,e) را به عنوان کلید عمومی اعلام و d را به عنوان کلید خصوصی نزد خود نگه می‌دارد.

رمزگذاری و رمزگشایی

باب می‌خواهد پیام m را برای آلیس بفرستد:

۱. رمزگذاری: باب باید برای رمز کردن m مراحل زیر را اجرا کند:

(ا) کلید عمومی آلیس، (n,e)، را از طریق معتبری به دست می‌آورد.

(ب) پیام m را به صورت عدد صحیحی در بازه $[0, n-1]$ بیان می‌کند.

(ج) عدد $c \equiv m^e \pmod{n}$ محاسبه می‌کند.

(د) پیام رمز شده را برای آلیس می‌فرستد.

۲. رمزگشایی: برای بدست آوردن m از c آلیس:

(ا) با استفاده از کلید خصوصی خود $m \equiv c^d \pmod{n}$ را محاسبه می‌کند.

در ادامه این فصل مسأله تسهیم راز را به طور کلی بررسی می‌کنیم. در آغاز مدل پایه تسهیم راز را تشریح می‌کنیم و آنگاه مجموعه ویژگی‌هایی که برای بسط مدل پایه لازم است، را می‌آوریم. و در نهایت برخی از کاربردهای تسهیم راز را عنوان می‌کنیم.

---

[۲۲] Adversary

[۲۳] از سرنام مخترعان آن گرفته شده است.

فرض کنید یک اطلاع مخفی، S، (مثلاً نقشه گنج یا رمز یک گاوصندوق یا ...) داریم و می‌خواهیم از آن مراقبت کنیم. اگر تنها یک نسخه از S را نگهداری کنیم هرچند که محل نگهداری و یا شخص مراقب امن باشند، باز احتمال حمله به آن محل یا سایر آسیب‌ها، وجود دارد. اگر به جای یک نسخه چندین نسخه از S را نگهداری کنیم با این کار احتمال از بین رفتن اطلاع مخفی را کاهش داده‌ایم، اما به همان نسبت تعداد نقاط خطر پذیر را افزایش داده‌ایم مضافاً این که در هر دو مورد قبلی احتمال سوءاستفاده افراد (نگهدارندگان راز) منتفی نیست و این فرض نیز باید لحاظ شود که هیچ فرضی در مورد افراد پذیرفتنی نیست. ممکن است رمز کردن S را چاره کار بدانید، اما واقعیت اینست که با این کار به جای محافظت از راز، باید از کلید رمز نگاری[۲۴] مراقبت کنیم.

۴.۱.۱ قضیه باقیمانده چینی

یکی از ابزارهایی که برای تسهیم راز استفاده شده قضیه باقیمانده چینی می‌باشد. در برخی شرایط لازم است که یک همنهشتی در پیمانه n، به سیستمی از همنهشتی‌ها در پیمانه فاکتورهای n شکسته شود. مثلاً می‌دانیم که $x \equiv 25 \pmod{42}$، حال می‌خواهیم x را در پیمانه 6 و 7 (فاکتورهای 42) بیان کنیم. این کار به سادگی و با بردن 25 به پیمانه‌های جدید انجام می‌شود:

$$x \equiv 25 \pmod{42} \Rightarrow \begin{cases} x \equiv 4 \pmod{7} \\ x \equiv 1 \pmod{6} \end{cases}$$

قضیه باقیمانده چینی نشان می‌دهد که این عملیات قابل برگشت است. یعنی این‌که تحت شرایط خاصی می‌توان سیستمی از همنهشتی‌ها را با یک همنهشتی جایگزین کرد.

قضیه ۱.۱. فرض کنید $gcd(m,n) = 1$ با داشتن اعداد صحیح a و b و همنهشتی‌های $x \equiv a \pmod{m}$ و $x \equiv b \pmod{n}$ به صورت همزمان، دقیقاً یک جواب $x \pmod{mn}$ وجود دارد.

قضیه باقیمانده چینی کاربردهای فراوانی در علوم کامپیوتر و رمزنگاری یافته است برای مطالعه بیشتر می‌توانید به [۳۱] مراجعه کنید. از جمله طرح‌های تسهیم رازی که بر اساس قضیه باقیمانده چینی پیشنهاد شده طرح میگنوت [۶۸]، طرح آسموت-بلوم [۵] می‌باشند.

نسخه‌های متعددی از قضیه باقیمانده چینی وجود دارد، در زیر شکل استاندارد این قضیه را از [۴۰] می‌آوریم:

قضیه ۲.۱. اگر $m_1, m_2, \dots, m_k$ اعداد صحیح مثبت و دو به دو نسبت به هم اول باشند ($gcd(m_i, m_j) = 1$ برای هر $i \neq j$)، همچنین $r_1, r_2, \dots, r_k$ اعداد صحیحی باشند که $r_i \in \mathbb{Z}_{m_i}$. حال دستگاه زیر دارای جواب یکتای $Y \in \mathbb{Z}_{\prod_{i=1}^{k} m_i}$ می‌باشد:

$$\begin{cases} Y \equiv r_1 \pmod{m_1} \\ Y \equiv r_2 \pmod{m_2} \\ \vdots \\ Y \equiv r_k \pmod{m_k} \end{cases}$$

در سال 1959 گارنر [۳۸] الگوریتم کارایی را برای یافتن Y ارائه داد. بعدها در سال 1963 فرانکل [۳۴] الگوریتم را برای حالت عمومی گسترش داد. در اینجا تنها به توصیف مختصر الگوریتم گارنر اکتفا می‌کنیم:

- $M = \prod_{i=1}^{i=k} m_i$.

---

[۲۴] Crptography

• ضرایب $I_1, I_2, \dots, I_k$ به صورت زیر محاسبه می‌شوند:

$$\begin{cases} I_1 \equiv (M/m_1)^{-1} \pmod{m_1} \\ I_2 \equiv (M/m_2)^{-1} \pmod{m_2} \\ \vdots \\ I_k \equiv (M/m_k)^{-1} \pmod{m_k}. \end{cases}$$

• در نهایت Y از رابطه زیر قابل محاسبه است:

$$Y \equiv \sum_{i=1}^{i=k} t_i \times M/m_i \times I_i \pmod{M}.$$

حالتی که پیمانه‌ها دو به دو نسبت به هم اول نباشند، در شکل عمومی قضیه باقیمانده چینی بررسی می‌شود:

قضیه ۳.۱. شکل عمومی قضیه باقیمانده چینی
اگر $m_1, m_2, \dots, m_k$ اعداد صحیح مثبت و $r_1, r_2, \dots, r_k$ اعداد صحیح باشند، در این صورت دستگاه معادلات

$$\begin{cases} Y \equiv r_1 \pmod{m_1} \\ Y \equiv r_2 \pmod{m_2} \\ \vdots \\ Y \equiv r_k \pmod{m_k} \end{cases}$$

در $\mathbb{Z}$ جواب دارد، اگر و تنها اگر $r_i \equiv r_j \pmod{gcd(m_i, m_j)}$ برای تمام $1 \leq i, j \leq k$. اگر دستگاه فوق در $\mathbb{Z}$ جواب داشته باشد، آنگاه جواب منحصر به فردی در $\mathbb{Z}_{lcm(m_1, m_2, \dots, m_k)}$ دارد.

۵.۱.۱ اتوماتای سلولی

در سال ۱۹۵۰ جان ون نیومن[۲۵] سعی کرد ماشین‌های خود تولید کننده[۲۶] را بسازد، یعنی می‌خواست ماشین‌هایی را بیابد که می‌توانستند کپی‌هایی از خودشان را بسازند.

نیومن شروع به کار روی معادلات دیفرانسیل نمود، تا این‌که یکی از هم دانشگاهیان او مدل متفاوتی را به او پیشنهاد داد که شبیه فضاهای شبکه‌ای بود که از آن‌ها در مطالعه کریستال‌ها استفاده می‌شد. نیومن در ابتدا از فضای دوبعدی استفاده کرد، این فضا به سلول‌هایی تقسیم می‌شود که به آن فضای سلولی [۲۷] گویند. هر یک از سلول‌ها دارای ساختار و حالت خاصی هستند که این حالت با توجه به قوانین محلی تغییر می‌کنند. نیومن ساختارهای هر سلول را اتوماتا، و کل فضا را اتوماتای سلولی نامید.

در بسیاری از کاربردها تولید دنباله‌های شبه تصادفی اهمیت فراوانی دارند، که تکنیک‌های مونت کارلو، روش‌های بهینه سازی در آمار، شبیه سازی حرکت ذرات و رمزنگاری از جمله این کاربردها هستند. یکی از ابزارهایی که برای تولید چنین رشته‌هایی پیشنهاد شده اتوماتای سلولی می‌باشد. استفاده از اتوماتای سلولی برای طراحی سیستم های رمزنگاری به اواسط دهه هشتاد برمی‌گردد، زمانی که استفان ولفرام[۲۸] کلاس نامنظمی از اتوماتای سلولی را دسته

[۲۵] John von Neumann

[۲۶] Self-replicating

[۲۷] Cellular space

[۲۸] Stephen Wolfram

بندی کرد و دسته‌ای با شماره قانون 30 را به عنوان تولید کننده بیت‌های تصادفی [۹۳] پیشنهاد داد، که استفاده از آن به عنوان جایگزینی برای LFSR، بسیار رایج است. از آن به بعد سیستم‌های رمزنگاری زیادی بر اساس اتوماتای سلولی پیشنهاد شده که برخی برای متن [۶، ۱۹، ۳۵، ۳۷، ۴۱، ۴۲، ۶۶، ۷۰، ۹۰] و برخی دیگر برای تصویر [۳، ۴۷] هستند. استفاده از اتوماتای سلولی برای تولید اعداد تصادفی مزایایی دارد از جمله این که الگوریتم ساده‌ای دارند و پیاده سازی سخت‌افزاری آن‌ها آسان است [۹۰].

اتوماتای سلولی به عنوان سیستم پویای گسسته

اتوماتای سلولی، سیستم‌های پویایی هستند که زمان و فضا گسسته هستند. در حالت کلی یک اتوماتون سلولی، شامل آرایه‌ای نامتناهی از اجزاء می‌شود که به آن‌ها سلول گویند. هر یک از سلول‌ها در هر زمان دارای یک حالت می‌باشد که از یک مجموعه محدود انتخاب می‌شود. حالت یک سلول با گذشت زمان و بر اساس قوانین محلّی تغییر می‌کند. آرایه‌ای که سلول‌ها را در بر می‌گیرد می‌تواند چند بعدی باشد، در عمل از فضای سلولی تک، دو و یا سه بعدی استفاده می‌شود و ابعاد بالاتر جنبه نظری دارند.

اتوماتای سلولی دودویی تک بعدی حالت متناهی[۲۹] (1-D CA) عبارت است از آرایه تک بعدی متناهی از N شیء یکسان که همان سلول‌ها هستند. هر یک از سلول‌ها، در هر زمان یک حالت دارند که از مجموعه $\{0,1\} \in s$، انتخاب می‌شود. سلول‌ها با اندیس شناخته می‌شوند و i-امین سلول، که $1 \leq i \leq n$، را به صورت $\langle i \rangle$ و حالت آن در زمان T را با $a_i^{(T)}$ نشان می‌دهیم. حالت سلول‌ها با گذشت زمان، به‌طور همزمان و با توجه به یک تابع انتقال محلی تغییر می‌کند. حالت بعدی سلول به متغیرهای این تابع بستگی دارد که شامل حالت خود سلول و حالت همسایگان آن سلول در زمان جاری می‌باشد. همسایگی انواعی دارد که معمولاً همسایگی متقارن را در نظر می‌گیریم. برای سلول $\langle i \rangle$، همسایگی متقارن به شعاع r به صورت زیر تعریف می‌شود:

$$\mathcal{N} = \{\langle i-r \rangle, \ldots, \langle i \rangle, \ldots, \langle i+r \rangle\} \qquad (۱.۱)$$

تابع گذار محلی[۳۰] برای اتوماتای سلولی با شعاع همسایگی r به صورت زیر می‌باشد:

$$f\colon (\mathbb{Z}_2)^{2r+1} \longrightarrow \mathbb{Z}_2$$

حالت سلول i-ام در زمان $T+1$ به صورت زیر بدست می‌آید:

$$a_i^{(T+1)} = f(a_{i-r}^{(T)}, \ldots, a_i^{(T)}, \ldots, a_{i+r}^{(T)}), \quad 0 \leq i \leq N-1 \qquad (۲.۱)$$

یا به عبارت دیگر:

$$a_i^{(T+1)} = f(\mathcal{N}_i^{(T)}), \quad 0 \leq i \leq N-1, \qquad (۳.۱)$$

که در آن $\mathcal{N}_i^{(T)} \in (\mathbb{Z}_2)^{2r+1}$ بیانگر حالات همسایه‌های $\langle i \rangle$ در زمان T می‌باشد. دیاگرام زمان-فضا برای اتوماتای سلولی تک بعدی در شکل ۱.۱ نشان داده شده است.

همچنین برای اطمینان از درستی تعریف، اگر $i \equiv j \ (mod\ N)$، فرض می‌کنیم که $a_i^{(T)} = a_j^{(T)}$. این مطلب در شکل ۲.۱ نشان داده شده است.

بردار $C^{(T)} = (a_0^{(T)}, \ldots, a_{N-1}^{(T)})$ را پیکربندی[۳۱] اتوماتای سلولی در زمان T، و $C^{(0)}$ را پیکربندی اولیه آن می‌نامند. مجموعه تمام پیکربندی‌های ممکن برای CA را به صورت $\mathcal{C}$ نشان می‌دهیم واضح است که $|\mathcal{C}| = 2^N$. دنباله $C^{(0)}, \ldots, C^{(T)}, \ldots, C^{(k)}$ را تکامل[۳۲] CA از مرتبه k گویند.

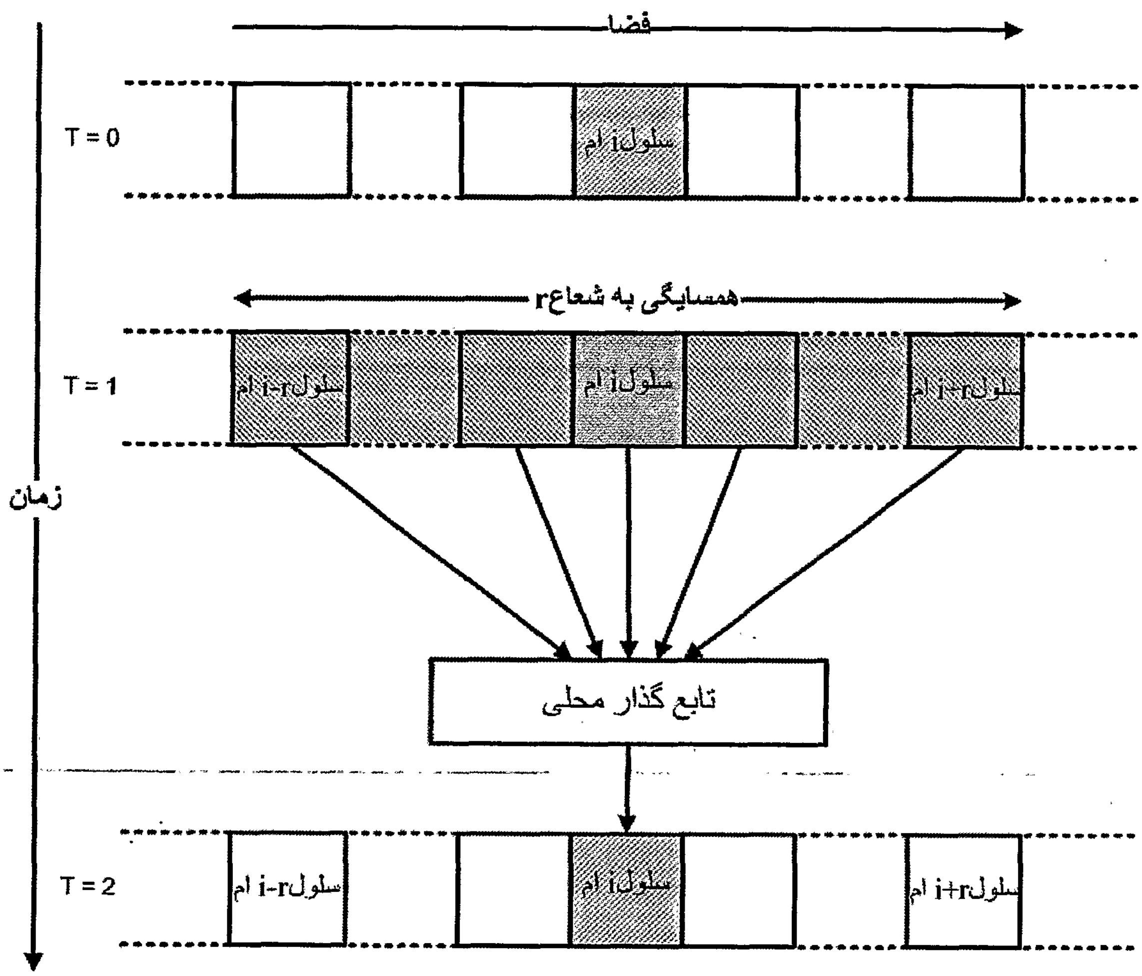
---

[۲۹] One-dimensional finite Boolean cellular automata

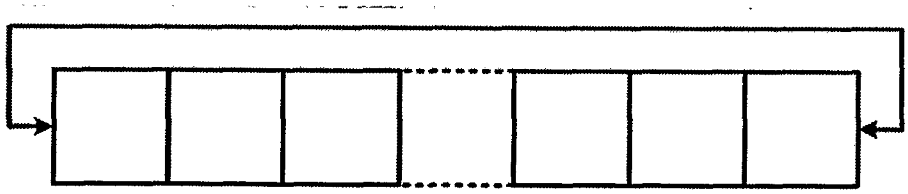
[۳۰] Local transition function

[۳۱] Configuration

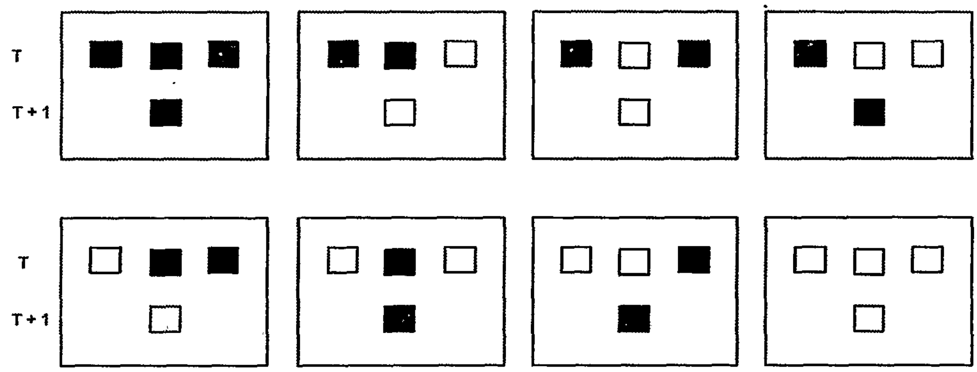
[۳۲] Evolution



شکل ۱.۱: دیاگرام زمان-فضا برای اتوماتای سلولی تک بعدی در حالت کلی



شکل ۲.۱: همسایگی در اتوماتای سلولی تک بعدی حالت متناهی



شکل ۳.۱: تمام حالات اتوماتای سلولی تک بعدی با سماره قانون ۷

تابع سراسری برای CA را به صورت تبدیل خطی $\Phi: \mathcal{C} \to \mathcal{C}$، می‌باشد که پیکربندی CA را در زمان بعدی مشخص می‌کند، یعنی $C^{(T+1)} = \Phi(C^{(T)})$. اگر برای اتوماتای سلولی CA، Φ نگاشتی دوسویی (یک به یک و پوشا) باشد، اتوماتای سلولی دیگری با تابع سراسری Φ^{-1} وجود دارد، که به آن وارون CA گویند. وقتی اتوماتای وارون برای یک CA وجود داشته باشد، آن را وارون‌پذیر گویند و تولید $C^{(T-1)}$ از روی $C^{(T)}$ ممکن است، یعنی تکامل به عقب امکان پذیر است [۸۹].

اگر تابع گذار محلی برای یک CA با شعاع همسایگی r، به صورت زیر باشد:

$$a_i^{(T+1)} = \sum_{j=-r}^{r} \alpha_j a_{i+j}^{(T)} \quad (mod\ 2), \quad 0 \le i \le N-1, \tag{۴.۱}$$

که به ازای هر j، $\alpha_j \in \mathbb{Z}_2$، به CA، اتوماتای سلولی خطی از مرتبه r، LCA، گویند. از آنجا که در همسایگی متقارن به شعاع r، تعداد $2r+1$ سلول وجود دارد و تعداد کل LCAها برابر 2^{2r+1} می‌باشد. هر یک از LCAها با عدد صحیح w، که آن را شماره قانون می‌نامند، مشخص می‌شوند، w برای LCA رابطه ۴.۱ ، از طریق زیر بدست می‌آید:

$$w = \sum_{j=-r}^{r} \alpha_j 2^{r+j}, \tag{۵.۱}$$

که $0 \le w \le 2^{2r+1} - 1$. به عنوان مثال، اتوماتای سلولی خطی با شعاع همسایگی $r = 1$ و شماره قانون 7 را در نظر می‌گیریم. تابع گذار محلی برای چنین ماشینی، را می‌توان به صورت $a_i^{(T+1)} = a_{i-1}^{(T)} \oplus a_i^{(T)} \oplus a_{i+1}^{(T)}$ نوشت. وضعیت هر سلول در زمان $T+1$ به وضعیت خود سلول، سلول سمت چپی و سلول سمت راست آن در زمان T بستگی دارد، بنابراین کلاً 8 حالت ممکن برای این سه سلول متصور است که در شکل ۳.۱ نشان داده شده است. در اینجا مربع‌های سیاه نشانه بیت صفر و مربع‌های سفید نشانه بیت یک هستند.

همچنین شکل ۴.۱ الگویی را نشان می‌دهد که با استفاده از قانون بالا تولید شده است . در این الگو در سطر اوّل با یک سلّول سیاه رنگ در وسط آرایه‌ی شروع به کار می‌کنیم. هر سطر نشان دهنده یک زمان است، چنان که مشاهده می‌شود پیشرفت فضای این ماشین در زمان از نظم خاصی پیروی می‌کند.

در CAهایی که تاکنون بحث کردیم، حالت هر سلول در زمان $T+1$ فقط به پیکربندی همسایه‌هایش در زمان T بستگی دارد، که به آن‌ها CAهای بدون حافظه[۳۳] گویند. با این وجود می‌توان حالتی را در نظر گرفت که حالت هر سلول در زمان $T+1$ علاوه بر حالت همسایه‌ها در زمان T به حالت گروه‌های مختلف از سلول‌ها و در زمان‌های $T-1, T-2, \ldots$ نیز وابسته باشد، به چنین ماشین‌هایی اتوماتای سلولی با حافظه[۳۴] (MCA) گویند [۱، ۲].

---

[۳۳] Memoryless

[۳۴] Memory cellular automata