
بسم الله الرحمن الرحیم

باسمه تعالی

تعهد نامه اصالت اثر

اینجانب خلیل علامی مهماندوستی متعهد می شوم که مطالب مندرج در این پایان نامه حاصل کار پژوهشی اینجانب است و دستاوردهای پژوهشی دیگران که در این پژوهش از آن ها استفاده شده است، مطابق مقررات، ارجاع و در فهرست منابع و مآخذ ذکر گردیده است. این پایان نامه قبلا برای احراز هیچ مدرک هم سطح یا بالاتر ارایه نشده است. در صورت اثبات تخلف (در هر زمان) مدرک تحصیلی صادر شده توسط دانشگاه از اعتبار ساقط خواهد شد.

خلیل علامی مهماندوستی

امضاء

دانشکده علوم پایه

اصلاح توابع بولی برای تضمین ماکزیمم امنیت جبری

نگارش:
خلیل علامی مهماندوستی

اساتید راهنما: **دکتر فرح بخش کمالی**
و
دکتر حمیدرضا میمنی

استاد مشاور: **دکتر عبدالرضا اسکویی**

پایان نامه برای دریافت درجه کارشناسی ارشد
در رشته ریاضی محض

بهمن ماه ۱۳۹۲

تقدیم

تقدیم به آنان که قلبشان برای زیستن در جهانی پر از صلح و عدالت و مهربانی می‌تپد و برای رسیدن به این جهان از هیچ کوششی مضایقه نمی‌کنند.

تقدیر و قدردانی

قبل از هر چیز سپاسگزار راهنمایی و زحمات اساتید عزیزم آقای دکتر حمید رضا میمنی و خانم دکتر فرح‌بخش کمالی هستم. همچنین بر خود لازم میبینم از استاد مشاورم آقای اسکویی و خانم امینی‌فر و خانم نجفی و آقای دکتر سعادت که در مراحل مختلف انجام پایان‌نامه ، نهایت اهتمام و تلاش را مبذول داشتند کمال تشکر و قدردانی را به عمل آورم. در پایان از خانواده‌ی عزیزم نیز کمال تشکر را دارم.

چکیده

در این پایان‌نامه با معرفی سیستم‌های رمزنگاری و یکی از انواع مهم آن به نام رمزهای جریان به سراغ توابع بولی رفته و با تعریف تابع بولی و مفاهیم مرتبط با آن از جمله درجه‌ی جبری، غیر خطی بودن، صفر کنندگی و امنیت جبری و... آشنا می‌شویم. سپس حملات جبری به سیستم‌های رمزنگاری را شرح خواهیم داد و ارتباط امنیت جبری با مقاومت یک سیستم رمزنگاری در مقابل حملات جبری را بیان خواهیم کرد. در ادامه قضایایی خواهیم دید که با اصلاح مناسب توابع بولی، توابع جدیدی به دست می‌دهند که دارای ماکزیمم امنیت جبری خواهند بود ، ودر پایان الگوریتم‌هایی مناسب را برای تضمین به‌دست آوردن توابع با ماکزیمم امنیت جبری بیان می‌کنیم.

کلید واژه‌ها: سیستم‌های رمزنگاری،توابع دودویی،ماکزیمم امنیت جبری،صفر کنندگی،حملات جبری.

فهرست مطالب

فصل ۱

مفاهیم مقدماتی

۱.۱ مقدمه

توابع بولی تشکیل ساختارهای دفاعی مهمی برای سیستم‌های رمز نگاری چه به صورت جعبه‌های جایگزینی [۱] در رمزهای بلوکی [۲] یا به صورت توابع فیلتر در رمزهای جریان می‌دهند.

امنیت این سیستم‌ها اساسا وابسته به خواص مشخص و مهم توابع می‌باشد. با دقت بیشتر، توابع بولی رمزی نیاز به ویژگی‌های خاص همچون نامتعادل بودن یا غیر خطی بودن بالا در جهت تضمین مقاومت در مقابل حملات جبری دارد.

در میان حملات، حمله‌ی جبری در سالهای اخیر بیشتر مورد توجه قرار گرفته است که از ساختار اساسی توابع برای ساخت یک سیستم معادلات چند متغیره غیر خطی بهره‌برداری می‌کند که اجازه می‌دهد تا کلید رمز را مشخص کنیم[۱۱].

در مقابل حملات جبری، بحث امنیت جبری مطرح می‌شود که می‌گوید نباید تابع g از درجه‌ی پایین با این ویژگی وجود داشته باشد که $f*g=0$ یا $(f+1)*g=0$ بشود. اگر چنانچه تابع g از درجه‌ی پایین وجود داشته باشد، آنگاه یک حمله‌ی جبری بسیار راحت قابل اجرا خواهد بود.

در فصل یک به تعریف رمزنگاری و توابع بولی ومفاهیم مرتبط به آن ها پرداخته‌ایم. سپس در فصل دو مفاهیم عمومی استراتژی اصلاح توابع بولی را بیان کرده‌ایم که با این اصلاحات جزئی توابع بولی، توابع جدیدی بدست می‌آیند که دارای امنیت جبری ماکزیمم می‌شوند. در فصل سه با تفکیک مقدار متغیر n به فرد و زوج با ارائه‌ی قضایا و گزاره‌هایی در پی اصلاح توابع بولی هستیم تا توابعی با امنیت جبری ماکزیمم بدست‌آوریم و یک الگوریتم برای بدست آوردن این توابع ارائه می‌کنیم ودر فصل چهارم ساختارهای بیشتری از توابع با امنیت جبری ماکزیمم را ارائه می‌کنیم و در ادامه الگوریتم دوم برای بدست آوردن این توابع را ارائه می‌کنیم.مقالات مطالعه شده دراین پایان نامه به شرح زیراست:

---

[۱] S-boxes

[۲] Block cipher

[1] Konstantinos Limniotis,Nicholas Kolokotronis and Nicholas Kalouptsidis "Modifying Boolean Functions To Ensure Maximum Algebraic Immunity " Presented at the IEEE International symposium on information theory,San Petersburg, Russia, july 31-August 6,2011.

[2] P.Rizomiliotis ,"On The Resistance Of Boolean Functions Against Algebraic Attacks Using Univariate Polynomial Representation" IEEE Trance Information Theory , vol.56. pp .4014-4024,2010.

[3] X.Zeng , C. Carlet , J.Shan and L.Hu, "More Balanced Boolean Functions With Optimal Algebraic Immunity And Good Nonlinearity And Resistance To Fast Algebraic Attack " IEEE Trance . Information Theory , vol. 57,pp. 6310-6320.2011 .

در این فصل به تعریف سیستم‌های رمز نگاری [۱] و توابع بولی [۲] و مفاهیم مرتبط با آن می‌پردازیم. سپس چند نماد از مرجع [۲۱] و [۲۵] معرفی می‌کنیم.

۲.۱ سیستم‌های رمزنگاری

تعریف ۱.۲.۱ رمزنگاری[۳]: علم و مطالعه‌ی روشهای مختلف نوشتن سری و مبادله‌ی اطلاعات امن.

تعریف ۲.۲.۱ روش سری نوشتن.

تعریف ۳.۲.۱ متن اصلی [۴]: پیام یا متنی که می‌بایستی پس از رمز شدن برای گیرنده‌ی خاصی ارسال شود.

تعریف ۴.۲.۱ متن رمز شده[۵]: متن رمز شده که توسط کانال نا امن ارسال می‌گردد. فرآیند تبدیل متن اصلی به متن رمز شده را رمزگذاری می‌نامند.

تعریف ۵.۲.۱ الگوریتم[۶]:روشی را که رمز کننده برای رمز کردن متن اصلی به‌کار می‌برد، الگوریتم نامیده می‌شود.

---

[۳] Cryptography

[۴] Main text

[۵] Cipher text

[۶] Algorithm

تعریف ۶.۲.۱ کلید[۷]: الگوریتم عموما متکی به یک کلید است که می‌بایستی برای دریافت کننده‌ی متن رمز شده معلوم باشد و سایرین از آن اطلاعی نداشته باشند. گیرنده با استفاده از کلید، متن اصلی را از متن رمز شده استخراج می‌کند.

عمل استخراج متن اصلی از متن رمز شده را رمزگشایی [۸] گویند.

تعریف ۷.۲.۱ دشمن[۹]: کسی که حق فهمیدن پیام را ندارد اما در جستجوی آن است.

تعریف ۸.۲.۱ شکستن رمز[۱۰]: دانش و مطالعه‌ی روشهای مختلف بدست آوردن پیام توسط دشمن.

تعریف ۹.۲.۱ یک سیستم رمز نگاری ، عبارت است از یک پنج تایی $(P, C, K, \varepsilon, D)$ که دارای شرایط زیر باشد:

۱) P مجموعه‌ی متناهی از متن‌های ممکن است.

۲) C مجموعه‌ی متناهی از متن‌های رمز شده ممکن است.

۳) K فضای کلید، یک مجموعه از کلیدهای ممکن است.

۴) برای هر $k \in K$، یک $e_k \in \varepsilon$ وجود دارد که به عنوان رمز کننده می‌باشد و متناظر آن یک $d_k \in D$ وجود دارد که نقش رمز گشا را بازی می‌کند.

$$e_k : P \to C$$

و

$$d_k : C \to P$$

توابعی هستند که

$$\forall x \in P \quad d_k(e_k(x)) = x$$

شرط 4، شرط اصلی می‌باشد که بیان می‌کند اگر متنی مانند x با استفاده از e_k رمز شود و به صورت یک متن رمز شده Y در آید، دوباره با استفاده از d_k رمز گشایی شود و در نهایت همان متن اصلی x به دست گیرنده خواهد رسید.

---

[۷] Key

[۸] Deciphering

[۹] Cryptanalyst

[۱۰] Cryptanalysis

باب وآلیس به دنبال استفاده از یک سیستم رمز نگاری برای برقراری ارتباط هستند. ابتدا آن ها به تصادف یک کلید $k \in K$ را انتخاب می‌کنند. این قسمت در جایی است که آلیس و باب هستند ولی اسکار یا هیچ کس دیگر قابلیت رؤیت آنها را ندارد.فرض کنید آلیس می‌خواهد با یک پیام با باب در یک شبکه نا امن (مثل اینترنت) ارتباط برقرار کند.

فرض کنیم پیام یک رشته‌ی $x = x_1x_2...x_n$ برای عدد صحیح $n \geq 1$ باشد که

$$x_i \in P \quad 1 \leq i \leq n.$$

هر x_i توسط e_k با استفاده از کلید پیش فرض رمز می‌شود در نتیجه آلیس،

$$y_i = e_k(x_i)\ 1 \leq i \leq n$$

را محاسبه می‌کند و در نتیجه متن رمز شده‌ی $y = y_1y_2...y_n$ توسط شبکه فرستاده می‌شود.

وقتی باب متن رمز شده‌ی $y = y_1y_2...y_n$ را با استفاده از تابع رمز گشایی d_k ،رمز گشایی می‌کند متن اصلی $x = x_1x_2...x_n$ را در یافت می‌کند.

تعریف ۱۰.۲.۱ فرض کنید برای $0 \leq k \leq 25$

$$P = C = K = \mathbb{Z}_{26}$$

تعریف می‌کنیم

$$e_k(x) = (x + k) \quad \textbf{(سنج۲۶)}$$

و

$$d_k(y) = (y - k) \quad \textbf{(سنج۲۶)}$$

که $x, y \in \mathbb{Z}_{26}$

تعریف بالا برای مثال زیر ارائه شده است.

مثال ۱۱.۲.۱ فرض کنید کلید برای رمز انتقال $k = 11$ باشد و متن اصلی $wewillmeetatmidnight$ باشد. ابتدا متن اصلی را تبدیل به دنباله‌ای از اعداد صحیح متناظر با آن می‌کنیم که به صورت زیر به‌دست می‌آید.

4 22 8 11 11 12 4 4 19 0 19 12 8 3 13 8 6 7 19

در ادامه با 11 به سنج 26 جمع می‌کنیم باقیمانده‌ی این جمع به سنج ۲۶ برابر است با:

15 7 19 22 22 23 15 15 4 11 4 23 19 14 24 19 17 ,18 4

در نهایت دنباله‌ای اعداد صحیح را تبدیل به کاراکترهای الفبایی تبدیل می‌کنیم که متن رمز شده‌ی زیر به دست می‌آید:

$$HPHTWWXPPELEXTOYTRSE$$

برای رمز گشایی متن رمز شده، ابتدا باید متن رمز شده را تبدیل به دنباله‌ی اعداد صحیح نماید. سپس هر مقدار را به سنج 26از 11 کم کند و نهایتا به دنباله‌ی اعداد صحیح متناظر متن اصلی شود.

حال به تعریف رمز جریان می‌پردازیم.

تعریف ۱۲.۲.۱ رمز جریان[11]: یک رمز جریان، همزمان یک چند تایی $P, C, K, L, \varepsilon, D$ با یک تابع g است چنانچه در شرایط زیر صادق باشد:

۱) P مجموعه‌ی متناهی از متن‌های ممکن است.

۲) C مجموعه‌ی متناهی از متن‌های رمز شده ممکن است.

۳) K فضای کلید، یک مجموعه‌ی متناهی از کلیدهای ممکن است.

۴) L مجموعه متناهی است، که الفبای کلید جریان نامیده می‌شود.

۵) g مولد کلید جریان می‌باشد. g یک کلید k ورودی را می‌گیرد و یک رشته نا متناهی $z_1 z_2 ...$ که کلید جریان نامیده می‌شود را تولید می‌کند که در آن

$$z_i \in L_i \geq 1$$

[11] Stream cipher

۶) برای هر $z \in L$، یک $e_z \in \varepsilon$ ومتناظر آن یک $d_z \in D$ وجود دارد به‌طوری که

$$e_z : P \to C$$

و

$$d_z : C \to P$$

توابعی هستند که

$$d_z(e_z(x)) = x$$

برای هر $x \in P$

برای شرح تعریف بالا فرض کنید $P = C = L = \mathbb{Z}_{26}$ و $K = (\mathbb{Z}_{26})^m$ و تعریف می‌کنیم:

$$e_z(x) = x + z \quad \textbf{(سنج۲۶)}$$

و

$$d_z(y) = y - z \quad \textbf{(سنج۲۶)}$$

و در نهایت رشته‌ی کلید $z_1 z_2 ...$ به صورت زیر به‌دست می‌آید:

$$z_i = \begin{cases} k_i & if \quad 1 \leq i \leq m \\ z_{i-m} & if \quad m-1 \leq i \end{cases}$$

که $K = (k_1, ..., k_m)$ لذا رشته‌ی کلید به صورت زیر تولید می‌شود:

$$k_1 k_2 k_3 ... k_m k_1 k_2 ... k_m ...$$

رمز جریان یک رمز متناوب با دوره‌ی تناوب d است اگر برای هر عدد صحیح $i \geq 1$ $Z_{i+d} = Z_i$. در مثال بالا دوره‌ی تناوب m می‌باشد.

رمز جریان معمولا با الفبای دودویی تشریح می‌شود به عبارت دیگر $P = C = L = \mathbb{Z}_2$ در این موقعیت رمز نگاری و رمز گشایی با عملگر جمع به سنج 2 انجام می‌شود.

$$e_z(x) = (x + z) \text{ (سنج۲)}$$

و

$$d_z(y) = (y + z) \text{ (سنج۲)}$$

در نتیجه کار رمزگشایی و رمز نگاری در سخت افزار می‌تواند بسیار مناسب انجام گیرد.

روشی دیگر برای تولید کلید جریان: ما روی الفبای دودویی کار خواهیم کرد. فرض کنید با m تایی $k_1, k_2, ..., k_m$ شروع کنیم و فرض کنید

$$z_i = k_i \, , 1 \leq i \leq m$$

حال کلید جریان را با استفاده از دنباله‌ی بازگشتی خطی از درجه‌ی m تولید می‌کنیم:

$$z_{i+m} = \sum_{j=0}^{m-1} c_j z_{i+j} \text{ (سنج۲)}$$

برای هر $i \geq 1$ و $c_0, c_1, ..., c_{m-1} \in \mathbb{Z}_2$.

می‌توان $c_0 = 1$ در نظر گرفت، بدون اینکه از کلیت مساله کاسته شود.

اگر $c_0, c_1, ..., c_{m-1}$ را ثابت در نظر بگیریم با انتخاب آغازین بردار $(k_1, ..., k_m)$ می‌توانیم یک کلید جریان متناوب با دوره‌ی تناوب $2^m - 1$ داشته باشیم، لذا یک کلید کوتاه می‌تواند به یک کلید جریان با دوره‌ی تناوب بالا به دست آید.

مثال ۱۳.۲.۱ فرض کنید $m = 4$ و کلید جریان توسط دنباله‌ی بازگشتی خطی زیر تولید شود.

$$z_{i+4} = (z_i + z_{i+1}) \text{ (سنج۲)}, \; i \geq 1$$

اگر کلید جریان با هر بردار بجز $(0, 0, 0, 0)$ آغاز شود، آن گاه یک کلید جریان با دوره‌ی تناوب $d = 2^m - 1$ یعنی $2^4 - 1 = 15$ به‌دست می‌آید.

به عنوان مثال با آغاز $(1, 0, 0, 0)$ کلید جریان به صورت .....100010011010111 به دست می‌آید.

یکی دیگر از جلوه‌های جذاب از این روش تولید کلید حریان ،این است که کلید جریان

در سخت افزار به صورت مناسبی با استفاده از $LFSR$ [۱۲] تولید شود. ما با استفاده از $shift\,register$، m مرحله خواهیم داشت.

بردار $(k_1, k_2, ..., k_m)$ در آغاز در $shift\,register$ استفاده شده است.

در هر واحد زمان مراحل زیر را عمل خواهیم کرد:

۱) k_1 را اولین بیت برای بیت‌های بعدی کلید جریان در نظر می‌گیریم.

۲) $k_2, ..., k_m$ در هر مرحله به سمت چپ یک‌بار انتقال می‌یابد.

۳) هر ارزش جدید از k_m ها توسط

$$\sum_{j=0}^{m-1} c_j k_{i+j}$$

محاسبه خواهد شد.

مثال قبل یک $LFSR$ است.

تعریف ۱۴.۲.۱ تابع بولی[۱۳]: فرض کنید $B = \{0, 1\}$. متغیر x را یک متغیر بولی می‌نامند، اگر مقدارش از مجموعه‌ی B به‌دست آید.

یک تابع از B^n مجموعه‌ی $\{(x_1, x_2, ..., x_n)|x_i \in B,\ 1 \leq i \leq n\}$ به B را یک تابع بولی با n متغیر می‌نامند.

$$f : \{0, 1\}^n \to \{0, 1\}$$

که فرم نرمال جبری آن به صورت زیر می باشد:

$$f(x_1, ..., x_n) = a_0 + \sum_{I \subseteq \{1,2,...,n\}} a_I \Pi_{i \in I} x_i$$

تعریف ۱۵.۲.۱ جدول ارزشی[۱۴]: جدول ارزش یک تابع بولی روی B^n ، لیست کامل از همه‌ی نقاط B^n با ارزش تابع در نقطه می‌باشد.

---

[۱۲] Linear feedback shift register

[۱۳] Boolean function

[۱۴] Truth table

مثال ۱۶.۲.۱ جدول ارزشی تابع بولی B^3 در زیر نشان داده شده است.

(x_1, x_2, x_3)	$f(x_1, x_2, x_3)$
$(0,0,0)$	1
$(0,0,1)$	1
$(0,1,0)$	0
$(0,1,1)$	1
$(1,0,0)$	0
$(1,0,1)$	1
$(1,1,0)$	0
$(1,1,1)$	1

تعریف ۱۷.۲.۱ درجه‌ی جبری [۱۵]: درجه‌ی جبری تابع بولی f که با $deg(f)$ نمایش داده می شود برابر با بیشینه تعداد متغیرهای موجود در عبارتهای سازنده ی فرم نرمال جبری آن است.

مثال ۱۸.۲.۱ تابع زیر از درجه ۳ می باشد.

$$f(x_1, ..., x_4) = x_1 + x_2 + x_3 + x_4 + x_1x_3 + x_2x_3 + x_1x_2x_3 + x_2x_3x_4$$

تعریف ۱۹.۲.۱ تابع آفین[۱۶]: یک تابع بولی f را آفین نامیم هرگاه $deg(f) \leq 1$ و مجموعه‌ی همه‌ی توابع آفین را با A_n نمایش می‌دهیم که زیر مجموعه‌ی کل توابع بولی می‌باشد.

عبارت جبری ارائه شده، فرم نرمال جبری توابع آفین می‌باشد:

$$a_0 \oplus a_1x_1 \oplus ... \oplus a_{n-1}x_{n-1} \oplus a_nx_n \quad (a_i \in \{0,1\})$$

درعبارت فوق اگر $a_0 = 0$ باشد ،آنگاه تابع را خطی می نامیم.

مثال ۲۰.۲.۱ تابع زیر از درجه ی ۱ آفین می باشد.

$$g(x_1, x_2) = x_1 + x_2$$

[۱۵] Algebraic degree

[۱۶] Affine function

تعریف ۲۱.۲.۱ مجموعه‌ی زیر را محمل f می‌نامیم.

$$Supp(f) = \{x \in F_2^n | \, f(x) = 1\}$$

تعریف ۲۲.۲.۱ وزن تابع بولی f[۱۷]: برابر است با تعداد بردارهایی که در $Supp(f)$ قرار دارند. در واقع $Wt(f) = |Supp(f)|$.

تعریف ۲۳.۲.۱ تابع بولی متعادل[۱۸]: یک تابع بولی n متغیره را متعادل گوییم اگروتنهااگر $Wt(f) = 2^{n-1}$

تعریف ۲۴.۲.۱ فاصله همینگ دو تابع [۱۹]:
برای دو تابع بولی f و g، فاصله‌ی همینگ ، $d(f,g)$ به صورت زیر تعریف می‌شود.

$$d(f,g) = Wt(f+g)$$

یا

$$d(f,g) = |\{x \in F_2^n | \, f(x) \neq g(x)\}|$$

تعریف ۲۵.۲.۱ غیر خطی بودن تابع بولی f[۲۰]: غیر خطی بودن تابع بولی f برابر است با مینیمم فاصله‌ی همینگ بین f و تمام توابع آفین. به عبارت دیگر:

$$nl(f) = min_{\, g \in A_n} d(f,g)$$

تعریف ۲۶.۲.۱ فرض کنید $f \in B_n$ داده شده باشد. گوییم $g \in B_n$ یک صفر کننده‌ی f است، اگر و فقط اگر در مجموعه‌ی زیر قرار داشته باشد.

$$AN(f) = \{g \in B_n : f * g = 0\}$$

که در آن $(*)$ ضرب نقطه‌ای است.
فرض کنید $x = (x_1, ..., x_n)$ و $w = (w_1, ..., w_n)$ متعلق به B_n باشند آنگاه

$$x * w = x_1 w_1 \oplus x_2 w_2 \oplus ... \oplus x_n w_n$$

---

[۱۷] Weight(f)

[۱۸] Balanced Boolean Function

[۱۹] Hamming Distance

[۲۰] Nonlinearity

تعریف ۲۷.۲.۱ امنیت جبری تابع بولی f [۲۱]: امنیت جبری تابع بولی n متغیره f برابر است با کمترین درجه از توابع غیر صفر g چنانکه $fg = 0$ یا $(f+1)g = 0$ شود و با $AI_n(f)$ نمایش داده می شود.

مثال ۲۸.۲.۱ فرض کنیم

$f(x_1, ..., x_4) = x_1 + x_2 + x_3 + x_4 + x_1x_3 + x_2x_3 + x_1x_2x_3 + x_2x_3x_4$ آنگاه تابع

$g(x_1, ..., x_4) = x_1x_2 + x_1x_4$

ازدرجه ی ۲ وجوددارد که $f * g = 0$.

$$f * g = (x_1 + x_2 + x_3 + x_4 + x_1x_3 + x_2x_3 + x_1x_2x_3 + x_2x_3x_4) * (x_1x_2 + x_1x_4) =$$

$$x_1x_2 + x_1x_4 + x_1x_2 + x_1x_2x_4 + x_3x_1x_2 + x_3x_1x_4 + x_4x_1x_2 + x_1x_4 + x_1x_2x_3 + x_1x_3x_4 +$$

$$x_1x_2x_3 + x_1x_2x_3x_4 + x_1x_2x_3 + x_1x_2x_3x_4 + x_1x_2x_3x_4 + x_1x_2x_3x_4 = 0.$$

رابطه‌ی بین سیستم‌های رمزنگاری و امنیت جبری:

یک حمله‌ی جبری [۱]یک روش رمز گشایی بسیار قدیمی است که کشف نوشته‌ی رمزی سیستم رمز نگاری حمله شده را به یک مساله‌ی پیدا کردن و حل کردن یک دستگاه معادلات چند جمله‌ای ساده سازی میکند. علاوه بر این مساله‌ی حل کردن یک سیستم معادلات غیر خطی روی میدان‌های متناهی نهایت کار حملات جبری است.

شانون [۲۲] نوشته است: یک رمز خوب باید به صورتی باشد که حل دستگاه معادلات همزمان آن دارای تعداد زیادی از نامعلومات پیچیده باشد.

قانون اصلی حملات جبری تبدیل ساده‌ی یک مساله از حملات سیستم رمز نگاری (برای مثال یافتن کلید مخفی یک رمز متقارن) به حل مساله معادلات چند جمله‌ای است.

لذا حمله‌ی جبری از دو مرحله تشکیل شده است.

۱) پیدا کردن دستگاه معادلات.

۲) حل دستگاه معادلات.

هر چند که یک مساله اساسی دیگر نیز از حملات جبری وجود دارد و آن این است که حل دستگاه معادلات چند جمله‌ای روی میدان‌های متناهی یک مساله تقریبا مشکل می‌باشد که در این مقاله ما با حل این معادلات کاری نداریم و فقط در واقع پیرامون امنیت جبری مسائلی را

[۲۱] Algebraic immunity

[۲۲] Claude Shannon

مطرح خواهیم کرد. در واقع امنیت جبری یک تابع باعث افزایش مقاومت تابع در برابر حملات جبری می‌باشد. در فصل 2 به بعد قضیه‌هایی را برای توابع بولی مطرح می‌کنیم که باعث به‌دست آمدن توابع با ماکزیمم امنیت جبری خواهند بود.

قضیه ۲۹.۲.۱ فرض کنید f یک تابع بولی$f : GF(2^n) \to GF(2)$باشد، آنگاه یک تابع بولی $g \neq 0$ از درجه‌ی حداکثر $\lceil \frac{n}{2} \rceil$ وجود دارد، چنانکه $f(x)g(x)$ از درجه‌ی حداکثر $\lfloor \frac{n}{2} \rfloor$ می‌باشد. به عبارت دیگر

$$Al_n(f) \leq \lceil \frac{n}{2} \rceil$$

.

اثبات. اگرA را تمام تک جمله‌ای های با درجه‌ی حداکثر $\lceil \frac{n}{2} \rceil$ قراردهیم

آنگاه $A = \{1, x_1, x_2, ..., x_1x_2, ...\}$

$|A| = \sum_{i=0}^{\lceil \frac{n}{2} \rceil} \binom{n}{i} > \frac{1}{2}2^n$

مشابها ، B را حاصلضرب f در تمام تک جمله ایهای با درجه ی حداکثر $\lceil \frac{n+1}{2} \rceil$ قرار می دهیم.

آنگاه $B = \{f(x), f(x).x_1, f(x).x_2, ..., .f(x).x_1x_2, ...\}$

$|B| = \sum_{i=0}^{\lceil \frac{n+1}{2} \rceil} \binom{n}{i} > \frac{1}{2}2^n$

قرار می دهیم $C = A \cup B$.همه ی عناصر A و B و C می توانند به صورت چندجمله ایهای چند متغیره با x_iها درنظرگرفته شوند.یعنی به صورت فرم نرمال جبری نوشته شوند.حال f را به صورت فرم نرمال جبری می نویسیم.A ،مجموعه ی چندجمله ایهای چندمتغیره ی با n متغیر است که نمی تواند بعدبیشتراز 2^n داشته باشد.اگر بعد این مجموعه بزرگتراز 2^n باشد دراین صورت وابسته های خطی وجود خواهند داشت که امکانپذیر نیست. بعد C برابر 2^n است زیرا پایه ی تمام توابع بولی ازدرجه ی حداکثر یک است.ازطرف دیگر

چون $|C| = |A| + |B| = \sum_{i=0}^{\lceil \frac{n}{2} \rceil} \binom{n}{i} + \sum_{i=0}^{\lceil \frac{n+1}{2} \rceil} \binom{n}{i} = \sum_{i=0}^{n} \binom{n}{i} + \binom{n}{\lfloor \frac{n}{2} \rfloor} > 2^n$

$|C| > 2^n$ لذا تعدادی وابسته خطی وجوددارند.علاوه براین درقسمت A هیچ وابسته ی خطی وجودندارد درنتیجه وابسته های خطی یا بایدترکیبی ازعناصرB یا A, B باشند.

واین بدین معنی است که اگر

$$g_i \in B$$