دانشکده علوم ریاضی و آمار

مدرس: دکتر مجتبی رفیعی

نیمسال دوم ۱۴۰۰-۱۴۰۱

رمزنگاری

جلسه ۱۶: طراحی توابع چکیده‌ساز

۲۹ اردیبهشت ۱۴۰۱

فهرست مطالب

۱ طراحی توابع چکیده‌ساز

طراحی توابع چکیده‌ساز در ساختار مرکل-دمگارد و اسفنجی از مهم‌ترین روش‌های طراحی توابع چکیده‌ساز می‌باشند. در ادامه تنها به چگونگی طراحی توابع چکیده‌ساز در ساختار مرکل-دمگارد خواهیم پرداخت.

۱.۱ ساختار مرکل-دمگارد

نخستین بارمرکل و دمگارد استفاده از توابع فشرده‌ساز[1] در طراحی توابع چکیده‌ساز را مطرح نمودند. تابع فشرده‌ساز در واقع نوعی تابع چکیده‌ساز است که برای پیام‌های با طول ثابت قابل استفاده است. ایده طراحی تابع چکیده‌ساز در ساختار مرکل-دمگارد این است که با داشتن تابع فشرده‌ساز برخوردتاب $f : \{0,1\}^n \times \{0,1\}^t \to \{0,1\}^n$ می‌توان تابع چکیده‌ساز برخوردتاب $H : \{0,1\}^* \to \{0,1\}^n$ را با تکرار تابع فشرده‌ساز به صورت بازگشتی طراحی نمود.
بدین منظور ابتدا اگر طول دنباله ورودی به تابع چکیده‌ساز، مضرب صحیحی از طول قالب ورودی تابع فشرده‌ساز نباشد، به انتهای پیام ورودی، یک بیت یک و به تعداد موردنیاز بیت صفر اضافه می‌شود. و در صورتی که طول دنباله ورودی به تابع چکیده‌ساز، مضرب صحیحی از طول قالب ورودی تابع فشرده‌ساز باشد، یک بیت ۱ و $t-1$ بیت صفر به انتهای پیام ورودی اضافه می‌شود. افزودن بیت های اضافی، به این شیوه را پدینگ گوییم. ساختار تابع چکیده‌ساز در ساختار مرکل-دمگارد را در شکل ۱-۱۷ مشاهده می‌کنیم.

شکل ۱-۱۷: ساختار مرکل-دمگارد

در این ساختار h_i متغیر زنجیره‌ای[2] نامیده می‌شود و در مرحله اول برابر با یک مقدار اولیه[3] ثابت IV (مثلاً $IV = 0^n$) است. پیام ورودی m، بعد از اعمال پدینگ روی آن به b قالب t بیتی $m_1, m_2, .., m_b$ تقسیم می‌شود سپس مقدار چکیده برای پیام m به صورت زیر محاسبه می‌شود که $[\ell]_t$ نمایش دودویی طول پیام m با یک رشته t بیتی است.

- $h_0 = IV$
- $h_{i+1} = f(h_i, m_{i+1})$ for $0 \leq i < b$
- $H(m) = f(h_b, [\ell]_t)$

قضیه ۱ *اگرتابع فشرده‌ساز f برخوردتاب باشد آنگاه تابع چکیده‌ساز H نیز برخوردتاب است.*

برهان. فرض کنید تابع چکیده‌ساز H برخوردتاب نباشد بنابراین پیام‌های متمایز m و m' وجود دارند که $H(m) = H(m')$ است. نشان می‌دهیم وجود برخورد برای تابع چکیده‌ساز منجر به یافتن برخوردی برای تابع فشرده‌ساز در جایی از ساختار تکراری می‌شود. فرض کنید قالب‌های پیام‌های پد شده $m_1, \cdots, m_b$ و $m'_1, \cdots, m'_{b'}$ باشند. همچنین طول‌های پیام‌ها را با ℓ و ℓ' و متغیرهای زنجیره‌ای متناظر را $h_0, h_1, \cdots, h_b$ و $h'_0 = h_0, h'_1, \cdots, h'_{b'}$ در نظر بگیرید. بدین منظور دوحالت زیر را در نظر می‌گیریم:

- **طول پیام‌های m و m' برابر است:**

[1] compression function
[2] chaining value
[3] Initial Value

در این‌صورت $\ell = \ell'$ و $b = b'$ و بنابراین

$H(m) = f(h_b, [\ell]_t)$
$H(m') = f(h'_b, [\ell']_t)$

اگر $h'_b \neq h_b$ باشد آنگاه برخوردی برای تابع f بدست می‌آید. درغیر اینصورت یک قالب به عقب بر می‌گردیم. حال اگر $(h'_{b-1}, m'_b) \neq (h_{b-1}, m_b)$ باشد آنگاه برخوردی یافته ایم. در غیر این صورت این روند را تا یافتن برخوردی برای f ادامه می‌دهیم. با توجه به اینکه دو پیام متمایزند پس حداقل در یک قالب با هم متفاوت خواهند بود بنابراین در روند بازگشتی حتما برخوردی برای f خواهیم یافت.

- **پیام‌های m و m' طول یکسانی ندارند:**

در این صورت $\ell \neq \ell'$ و بنابراین

$H(m) = f(h_b, [\ell]_t)$
$H(m') = f(h'_{b'}, [\ell']_t)$
$H(m) = H(m') \Rightarrow f(h'_{b'}, [\ell']_t) = f(h_b, [\ell]_t)$

با توجه به اینکه $\ell \neq \ell'$ است بنابراین $f(h'_{b'}, [\ell']_t) = f(h_b, [\ell]_t)$ برخوردی برای تابع f می‌باشد.

■

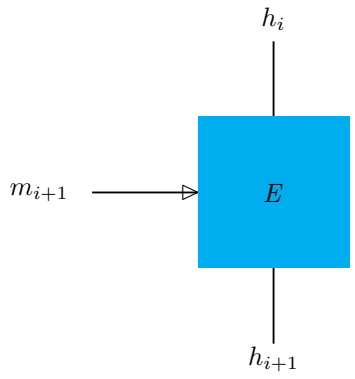
نکته ۱ *وارد کردن طول پیام در ساختار مرکل-دمگارد ضروری است. در غیر اینصورت می‌توان توابع فشرده‌ساز برخوردتابی یافت که ساختار مرکل-دمگارد متناظر (بدون قالب طول پیام) برخوردتاب نباشد (راهنمایی: فرض کنید تابع فشرده‌ساز نقطه ثابتی مانند $IV = f(IV, m)$ داشته باشد).*

نکته ۲ *عکس گزاره بالا لزومابرقرار نیست و به طورکلی نمی‌توان ضعف‌های تابع چکیده‌ساز را به تابع فشرده‌ساز تعمیم داد.*

نکته ۳ *قضیه مرکل-دمگارد نشان می دهد اگر تابع فشرده‌ساز ایده‌آل باشد به طوری که بهترین حمله برخورد برای آن دارای پیچیدگی $2^{n/2}$ باشد، بهترین حمله برخورد علیه تابع چکیده‌ساز نیز دارای همان پیچیدگی است. با این وجود ساختار مرکل-دمگارد نسبت به پیش‌تصویرتابی ایده‌ال عمل نمی‌کند؛ زیرا حملاتی با پیچیدگی بهتری از 2^n علیه آن وجود دارد.*

۲.۱ طراحی توابع فشرده‌ساز

در بخش قبل دیدیم در صورت وجود یک تابع فشرده‌ساز برخوردتاب، می‌توان تابع چکیده‌ساز برخوردتاب طراحی کرد. حال در این بخش به چگونگی طراحی تابع فشرده‌ساز مقاوم در برابر برخورد می‌پردازیم. یکی از روش های رایج در طراحی توابع فشرده‌ساز استفاده از رمزهای قالبی است. فرض کنیم $E : \{0,1\}^t \times \{0,1\}^n \to \{0,1\}^n$ یک رمزقالبی باشد.
ایده اولیه طراحی تابع فشرده‌ساز f به این صورت است که در رمزقالبی E پیام ورودی را به عنوان کلید اصلی و مقدار h_i را به عنوان متن اصلی ورودی در نظر بگیریم. ساختار تابع f را در شکل ۲-۱۷ مشاهده می‌کنیم.



شکل ۲-۱۷ .

تابع f مطابق رابطه زیر می‌باشد.

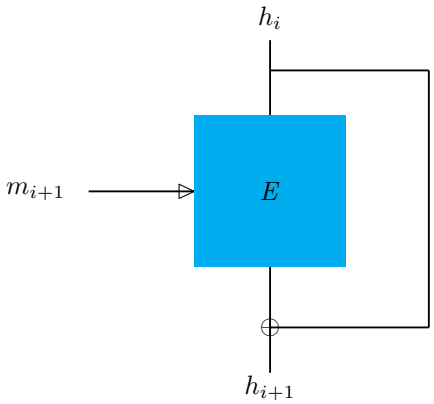
$$h_{i+1} = f(h_i, m_{i+1}) = E_{m_{i+1}}(h_i)$$

حال سوالی که مطرح می‌شود این است که آیا تابع فشرده‌ساز با ساختار معرفی شده برخوردتاب است؟ پاسخ به این پرسش منفی است. مهاجم می‌تواند به راحتی برای هر خروجی دلخواه h_{i+1} از تابع فشرده‌ساز به تعداد دلخواه پیش‌تصویر بسازد. برای این کار کلید دلخواه m_{i+1} را انتخاب می‌کند و مقدار $E^{-1}{}_{m_{i+1}}(h_{i+1})$ را محاسبه می‌کند. به وضوح $\left(m_{i+1}, E^{-1}{}_{m_{i+1}}(h_{i+1})\right)$ پیش‌تصویری برای h_{i+1} است.
برای ساختن برخورد به عنوان مثال مهاجم خروجی $h_{i+1} = 0^n$ و پیام‌های متمایز $m_{i+1} = 0^n$ و $m'_{i+1} = 1^n$ را درنظر می‌گیرد. حال با محاسبه ورودی‌های h_i و h'_i به صورت زیر برخوردی برای تابع f می‌یابد.

$$\begin{array}{l} h_i = E^{-1}_{m_{i+1}}(h_{i+1}) = E^{-1}{}_{0^n}(0^n) \\ h'_i = E^{-1}_{m'_{i+1}}(h_{i+1}) = E^{-1}{}_{1^n}(0^n) \\ f(h_i, m_{i+1}) = E_{m_{i+1}}(h_{i+1}) = 0^n \\ f(h'_i, m'_{i+1}) = E_{m'_{i+1}}(h'_{i+1}) = 0^n \end{array} \quad \Longrightarrow \quad f(h_i, m_{i+1}) = f(h'_i, m'_i)$$

در ادامه به معرفی طرح‌های دیویس-میر[۴] و ماتیاس-میر-اوسیاس[۵] می‌پردازیم که راه‌حل‌هایی برای رفع مشکل فوق می‌باشند.

۱.۲.۱ طرح Davies-Meyer



شکل ۳-۱۷: طرح دیویس-میر

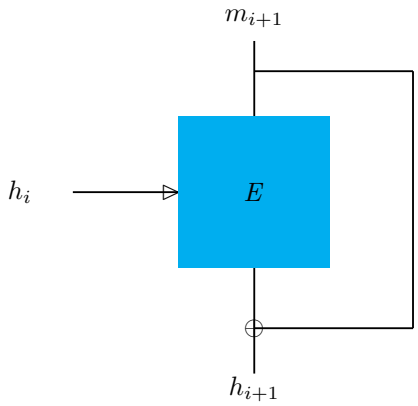
محاسبه تابع فشرده‌ساز در این طرح به صورت زیر است.

$$h_{i+1} = f(h_i, m_{i+1}) = E_{m_{i+1}}(h_i) \oplus h_i$$

- در این طرح می‌توان از هر رمز قالب دلخواه استفاده نمود.
- اگر E یک رمزقالبی ایده‌آل باشد آنگاه یافتن برخورد نیاز به محاسبه $2^{n/2}$ پیام ورودی دارد.

[4] Davies–Meyer
[5] Matyas–Meyer–Oseas

۲.۲.۱ طرح Matyas-Meyer-Oseas



شکل ۴-۱۷: طرح ماتیاس-میر-اوسیاس

برای محاسبه تابع فشرده‌ساز در این طرح از رابطه زیر استفاده می‌شود.

$$h_{i+1} = f(h_i, m_{i+1}) = E_{h_i}(m_{i+1}) \oplus m_{i+1}$$

- در این طرح از رمز قالبی استفاده شود که طول قالب ورودی و طول کلید آن یکسان باشد.
- اگر E یک رمزقالبی ایده‌آل باشد آنگاه یافتن برخورد نیاز به محاسبه $2^{n/2}$ پیام ورودی دارد.

۲ توابع چکیده‌ساز مهم

- **SHA-1:** این الگوریتم توسط NSA[۶] در ساختار مرکل-دمگارد، طراحی شده است و در سال ۱۹۹۵ توسط NIST[۷] انتشار یافت. طول خروجی این الگوریتم ۱۶۰ بیت وطول قالب آن ۵۱۲ بیت است. در سال ۲۰۰۵ نشان داده شد که با محاسبه 2^{69} مقدار ورودی می‌توان برخوردی برای این الگوریتم پیدا کرد. با وجود الگوریتم‌های اندکی بهتر هنوز برخوردی برای این تابع پیدا نشده است.

  پیش از سال ۲۰۱۰، SHA-1 کاربردهای گسترده‌ای در امضای دیجیتال DSS و پروتکل‌های SSL، TLS و PGP داشته است. در حال حاضر در بعضی از موارد SHA-1 با SHA-2 جایگزین گردیده است.
- **SHA-2:** مؤسسه NIST چهار تابع چکیده‌ساز که بر اساس طول خروجی شان نامگذاری شده بودند به نام های SHA-512، SHA-384، SHA-256 و SHA-224 معروف به خانواده SHA-2 را معرفی کرد. این خانواده از لحاظ ساختاری مشابه SHA-1 هستند. اما به طور کلی این خانواده با استقبال گسترده‌ای روبرو نشد.
- **MD5:** این الگوریتم در سال ۱۹۹۲ توسط ران ریوست[۸] در ساختار مرکل-دمگارد با طول قالب ۵۱۲ بیت وطول خروجی ۱۲۸ بیت طراحی گردید. حمله برخورد به تابع فشرده‌ساز این الگوریتم در سال ۱۹۹۶ ارایه شده است.

[6] National Security Agency
[7] National Institute of Standards and Technology
[8] Ron Rivest