رمزنگاری پیشرفته ۲۵۱۷۲۱ ۶ اسفند ۱۴۰۱

تمرین توابع چکیده‌ساز

مدرس: محمود سلماسی زاده دانشگاه صنعتی شریف

اهداف تمرین

در این تمرین با نحوه بررسی برقراری ویژگی‌های یک‌طرفه بودن،برخورد تابی ضعیف و قوی برای یک تابع چکیده‌ساز داده شده، ارتباط بین این ویژگی‌ها، نحوه کار ساختار Merkle-Damgård، مشکلات تحقق توابع چکیده‌ساز با استفاده از رمزهای بلوکی، برخی از مسائل احتمالاتی مرتبط با توابع چکیده‌ساز و حمله‌ی روز تولد پرداخته می‌شود.
در این مجموعه‌ی تمارین، به ساختار اسفنجی، توابع چکیده‌ساز SHA، مثال‌های اسباب‌بازی تابع چکیده‌ساز،درخت‌های Merkle پرداخته نشده است.

فهرست مطالب

۱ ویژگی‌های تابع چکیده‌ساز

سوال ۱

الف. تابع چکیده‌ساز زیر را در نظر بگیرید. پیام‌ها به فرم یک رشته‌ای از اعداد در $\mathbb{Z}_n$، یعنی $M = (a_1, a_2, \ldots, a_t)$ هستند. تابع چکیده‌ساز h به صورت $\sum_{i=1}^{t} a_i \ mod\ n$، برای مقدار از قبل مشخص شده‌ای از n محاسبه می‌شود.
این تابع چکیده‌ساز کدام یک از ویژگی‌های اندازه ورودی متغیر، اندازه خروجی ثابت، محاسبه پذیری کارا، پیش‌تصویر تابی (یک‌طرفه بودن)، پیش‌تصویر تابی دوم (برخوردتابی ضعیف)، برخورد تابی (برخورد تابی قوی)، شبه‌تصادفی بودن را دارد؟ پاسخ خود را توضیح دهید.

ب. بخش الف. را برای تابع چکیده‌ساز $h(M) = \left(\sum_{i=1}^{t} a_i\right)^2 \ mod\ n$ تکرار کنید.

ج. تابع چکیده‌ساز بخش ب. را برای پیام $M = (189, 632, 900, 722, 349)$ و $n = 989$ محاسبه کنید.

سوال ۲

اگر یک تابع چکیده‌ساز h را به گونه‌ای تعریف کنیم که یک رشته‌ی دودویی n بیتی را به یک رشته‌ی دودویی m بیتی تبدیل می‌کند، می‌توان به h به عنوان تابعی از $\mathbb{Z}_{2^n}$ به $\mathbb{Z}_{2^m}$ نگاه کرد. وسوسه‌انگیز خواهد بود اگر تابع h را با استفاده از عملیات صحیح به پیمانه‌ی 2^m تعریف کرد. در این تمرین نشان می‌دهیم که چنین ساختارهای ساده‌ای از این نوع، ناامن هستند و در نتیجه باید از آن‌ها پرهیز شود.

الف. فرض کنید $n = m > 1$ و $h : \mathbb{Z}_{2^m} \to \mathbb{Z}_{2^m}$ به صورت زیر تعریف شده است:

$$h(x) = x^2 + ax + b \ mod \ 2^m$$

ثابت کنید پیداکردن پیش‌تصویر دوم برای هر $x \in \mathbb{Z}_{2^m}$ معمولا کار آسانی است بدون آن که نیاز به حل معادله‌ی درجه‌ی دو باشد.
راهنمایی: نشان دهید که می‌توان تابع خطی $g(x)$ پیدا کرد به گونه‌ای که برای هر x داشته باشیم $h\Big(g(x)\Big) = h(x)$. با این کار می‌توان پیش‌تصویر دوم برای هر x را پیدا کرد که $g(x) \neq x$.

ب. فرض کنید $n > m$ و $h : \mathbb{Z}_{2^n} \to \mathbb{Z}_{2^m}$ به صورت یک چندجمله‌ای از درجه‌ی d تعریف شده باشد:

$$h(x) = \sum_{i=0}^{d} a_i x^i \ mod \ 2^m$$

که $a_i \in \mathbb{Z}$ برای $0 \leq i \leq d$. ثابت کنید که پیداکردن پیش‌تصویر دوم برای هر $x \in \mathbb{Z}_{2^n}$ آسان است بدون آن که نیاز باشد یک معادله‌ی چندجمله‌ای را حل کنیم.
راهنمایی: از این حقیقت استفاده کنید که $h(x)$ با استفاده از کاهش به پیمانه‌ی 2^m تعریف شده است اما دامنه‌ی h مجموعه‌ی $\mathbb{Z}_{2^n}$ است که $n > m$.

سوال ۳

فرض کنید تابع چکیده‌ساز $H : \{0,1\}^* \to \{0,1\}^n$ برخورد تاب باشد. کدام یک از ساختارهای زیر لزوما دارای ویژگی برخورد تابی است و در مورد آن‌ها بحث کنید.

الف. $\hat{H}(x) \coloneqq H_1\big(H_1(x)\big)$

ب. $\hat{H}(0^n 1 \| y) \coloneqq H(y)$

ج. علاوه بر برخورد تابی، یک‌طرفه بودن تابع چکیده‌ساز زیر را هم بررسی کنید. به طور دقیق‌تر، نشان دهید که پیش‌تصویر نیمی از چکیده‌ی پیام‌ها برای تابع چکیده‌ساز زیر را می‌توان پیدا کرد. با توجه به این مشاهده، آیا دارا بودن ویژگی برخورد تابی الزاما به معنی دارا بودن ویژگی یک‌طرفه بودن است؟

$$\hat{H}(x) \coloneqq \begin{cases} 0\|x & x \in \{0,1\}^n, \\ 1\|H_1(x) & \text{otherwise} \end{cases}$$

د. به نظرتان چرا در برخی منابع، دارا بودن ویژگی پیش‌تصویر تابی دوم را به معنای دارا بودن ویژگی یک‌طرفه بودن، در نظر می‌گیرند؟ به عبارت دیگر، چه فرضی را در نظر گرفته‌اند که به این نتیجه رسیده‌اند؟ (توجه شود که اگر تابع چکیده‌سازی برخورد تاب باشد، آنگاه پیش‌تصویر تاب دوم هم هست، پس طبق ادعای فوق، برخود تابی ویژگی یک‌طرفه‌بودن را نتیجه می‌دهد.) آیا با توجه به توابع چکیده‌ساز عملی موجود (نه صرفا یک مثال تئوری)، این فرض معقول است؟

سوال ۴

فرض کنید $H_1, H_2 : \{0,1\}^* \to \{0,1\}^n$ دو تابع چکیده‌ساز هستند که حداقل یکی از آن‌ها دارای ویژگی برخورد تابی است. بررسی کنید که کدام یک از ساختارهای زیر لزوما دارای ویژگی برخورد تابی است و در مورد آن‌ها بحث کنید.

الف. $\hat{H}(x) \coloneqq H_1(x) \| H_2(x)$

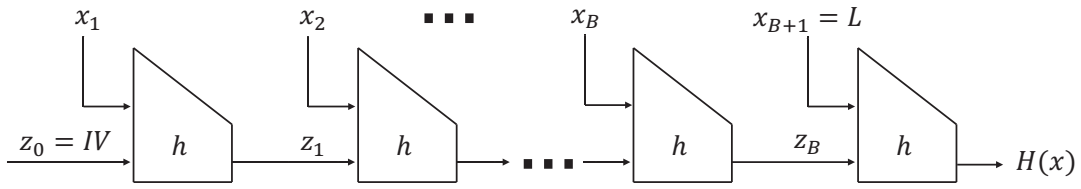
ب. $\hat{H}(x) \coloneqq H_1\big(H_2(x)\big) \| H_2\big(H_1(x)\big)$

ج. $\hat{H}(x) \coloneqq H_1\big(H_2(x) \| x\big) \| H_2\big(H_1(x) \| x\big)$

۲ تبدیل Merkle-Damgard

سوال ۵

تبدیل Merkle-Damgård را در نظر بگیرید که به تابع چکیده‌ساز h اعمال شده است و تابع چکیده‌ساز H بدست آمده است. مطابق شکل ۱.



شکل ۱: تبدیل Merkle-Damgård

الف. ساختار را به گونه‌ای تغییر دهید که طول ورودی را شامل نشود؛ یعنی، z_B را خروجی بدهد نه $z_{B+1} = h(z_B \| L)$. فرض کنید که تابع چکیده‌ساز جدید تنها برای ورودی‌هایی که طول آن‌ها مضرب صحیحی از طول بلوک است، تعریف شده است. آیا این تابع چکیده‌ساز جدید برخورد تاب است؟ اگر ورودی‌هایی را که طول آن‌ها مضرب صحیحی از طول بلوک نیست هم بپذیریم چطور؟

ب. ساختار را به گونه‌ای تغییر دهید که به جای دادن $z = h(z_B \| L)$ به عنوان خروجی، عبارت $z_B \| L$ را خروجی دهد. آیا این تابع چکیده‌ساز جدید برخورد تاب است؟

ج. به جای استفاده از یک IV، محاسبه را از x_1 شروع کند؛ یعنی، قرار دهد $z_1 := x_1$ و سپس $z_i := h(z_{i-1} \| x_i)$ را برای $i = 2, \ldots, B+1$ محاسبه کند و z_{B+1} را مانند قبل به عنوان خروجی بدهد. آیا این تابع چکیده‌ساز جدید برخورد تاب است؟

د. به جای استفاده از یک IV ثابت، قرار دهد $z_0 := L$ و سپس $z_i := h(z_{i-1} \| x_i)$ را برای $i = 1, \ldots, B$ محاسبه کند و z_B را به عنوان خروجی بدهد. آیا این تابع چکیده‌ساز جدید برخورد تاب است؟

ه. نشان دهید که تابع چکیده‌ساز h ای وجود دارد که بر خورد تاب نیست، ولی تابع چکیده‌ساز H، برخورد تاب است.

و. رد یا اثبات کنید: اگر h برخورد تاب باشد، H نیز برخورد تاب است.

ز. رد یا اثبات کنید: اگر h برخورد تاب دوم باشد، H نیز برخورد تاب دوم است.

۳ استفاده از توابع چکیده‌ساز برای ساخت رمز بلوکی و برعکس

سوال ۶

الف. آیا ممکن است بتوان با استفاده از یک تابع چکیده‌ساز، یک رمز بلوکی مشابه DES ساخت. چرا که یک تابع چکیده‌ساز، یک تابع یک‌طرفه است؛ درحالی که رمز بلوکی باید معکوس‌پذیر باشد تا رمزگشایی انجام شود. چطور این کار ممکن است؟

ب. حال، عکس حالت فوق را در نظر بگیرید: استفاده از یک الگوریتم رمزگذاری برای ساخت یک تابع چکیده‌ساز یک‌طرفه.
در این جا از یک رمزگذاری کلید عمومی در مود زنجیره‌ی بلوکی برای ساخت یک تابع چکیده‌ساز یک‌طرفه استفاده می‌کنیم. اگر کلید خصوصی را دور بیندازیم، شکستن این تابع چکیده‌ساز معادل رمزگشایی یک پیام بدون دانستن کلید خصوصی است. استفاده از RSA با یک کلید معلوم را در نظر بگیرید. سپس، یک پیام شامل یک دنباله‌ای بلوک‌ها را به صورت زیر پردازش کنید:

- اولین بلوک را رمزگذاری کنید.
- حاصل را با بلوک دوم XOR کنید و دوباره رمزگذاری کنید، و به همین ترتیب تا آخرین بلوک پیام ادامه دهید.

اگر پیام تنها یک بلوک بود، پیداکردن پیش‌تصویر معادل با حل مسئله‌ی RSA می‌بود. برخورد هم رخ نمی‌دهد زیرا تابع رمزگذاری، با یک کلید ثابت، یک تابع یک‌به‌یک است. حال، با حل مسئله‌ی زیر نشان دهید که این طرح امن نیست. دو بلوک پیام B_1 و B_2 و چکیده‌ی آن‌ها

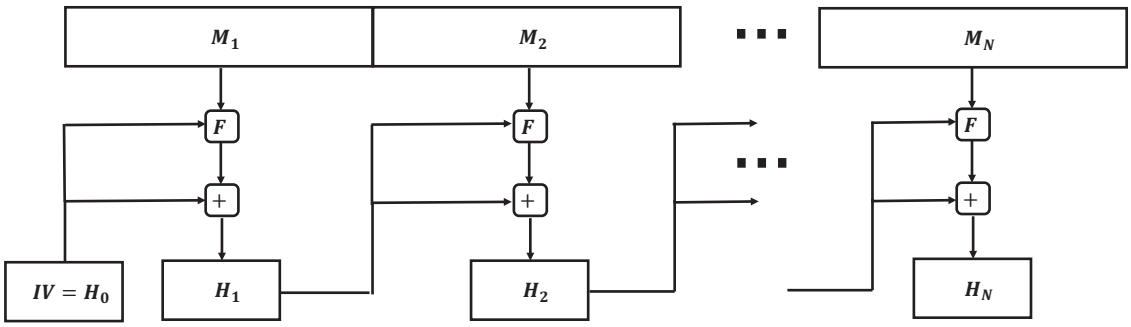
$$\mathsf{RSAH}(B_1, B_2) = \mathsf{RSA}(\mathsf{RSA}(\mathsf{B_1}) \oplus \mathsf{B_2})$$

داده شده است. با داشتن یک بلوک دلخواه C_1، بلوک C_2 را طوری انتخاب کنید که $\mathsf{RSAH}(C_1, C_2) = \mathsf{RSAH}(B_1, B_2)$. بنابراین، تابع چکیده‌ساز فوق، ویژگی برخورد تابی ضعیف را ارضا نمی‌کند.

۴ توابع چکیده‌ساز بر اساس زنجیره رمز بلوکی (CBC)

سوال ۷

از طرح‌های ارائه شده برای ساخت تابع چکیده‌ساز، می‌توان به طرح‌های مبتنی بر روش CBC [۱] اشاره کرد. در این طرح‌ها، پیام ورودی M به قالب‌هایی با طول برابر تقسیم شده و سپس با استفاده از الگوریتم رمزنگاری متقارن مانند DES، مقدار چکیده‌ی نهایی محاسبه می‌شود. دقت شود که در این حالت بر خلاف شیوه رمزنگاری CBC، کلید محرمانه وجود ندارد.



شکل ۲: ساختار چکیده‌ساز مبتنی بر CBC

الف. حال فرض کنید در ساختاری داشته باشیم $H_i = H_{i-1} \oplus F(M_i, H_{i-1})$ که در آن F تابع رمزگذاری DES با طول ورودی، خروجی و کلید 64 بیتی است. به شکل ۲ نگاه کنید.
با توجه به خاصیت مکملیت DES که اگر $Y = F(K, X)$، در این صورت: $Y' = F(K', X')$، نشان دهید که چگونه می‌توان پیام شامل قالب‌های $M_1, \ldots, M_N$ را به گونه‌ای تغییر داد که مقدار چکیده‌ی آن ثابت بماند. به عبارت دیگر، برخورد اتفاق بیفتد.

ب. نشان دهید که حمله‌ی مشابهی به طرح ارائه شده با فرمول زیر، می‌تواند موفقیت‌آمیز باشد.

$$H_i = M_i \oplus F(H_{i-1}, M_i)$$

۵ مسائل احتمالاتی و حمله‌ی روز تولد

سوال ۸

رمزگذاری یک پیام با n قالب $x = x_1 \| x_2 \ldots \| x_n$ با استفاده از روش CBC و با در نظر گرفتن تابع رمزگذاری متقارن E صورت می‌پذیرد. پیام رمز شده‌ی خروجی را به صورت $y = y_1 \| y_2 \ldots \| y_n$

[۱] cipher block chaining

نمایش می‌دهیم.

الف. نشان دهید که در صورتی که در خروجی برخوردی وجود داشته باشد؛ یعنی، برای $i \neq j$ داشته باشیم: $y_i = y_j$، می‌توان در مورد پیام ورودی اطلاعاتی کسب کرد.

ب. اگر E تابعی با قالب ورودی 64 بیتی باشد، (مثلا DES)، احتمال داشتن یک برخورد چقدر است؟

ج. حداقل اندازه‌ی ورودی که می‌توان با احتمال نزدیک به یک برای آن برخورد پیدا کرد، چقدر است؟

سوال ۹

فرض کنید که H یک تابع چکیده‌ساز امن است. با در نظر گرفتن t پرسمان به این تابع، به موارد زیر پاسخ دهید. (منظور از t پرسمان، اطلاع از خروجی تابع چکیده‌ساز به ازای t ورودی $x_1, x_2, \ldots, x_t$ است.)

الف. اگر $y \in \{0,1\}^k$ باشد، در این صورت احتمال یافتن یک ورودی x که داشته باشیم $H(x) = y$، چقدر است؟

ب. اگر مقدار $x \in \{0,1\}^*$ داده شده باشد، در این صورت احتمال یافتن x' که $x \neq x'$ و $H(x') = H(x)$، چقدر است؟

ج. نشان دهید که احتمال یافتن یک زوج (x, x') به طوری که $x' \neq x$ و $H(x') = H(x)$، حداکثر برابر خواهد بود با $\frac{t^2}{2^k}$. (خروجی تابع چکیده‌ساز را k بیتی در نظر بگیرید.)

ه. از نتایج بند ب و ج چه نتیجه‌ای می‌گیرید؟

مراجع

[1] William Stallings, "*Crytptography and network security: principles and practice*", 8th edition, Pearson, 2023.

[2] Jonathan Katz and Yehuda Lindell, "*Introductin to modern cryptography*", 3rd edition, Chapman & Hall/CRC Cryptography and Network Security Series, 2021.

[3] Douglas R. Stinson and Maura B. Paterson, "*Cryptography: theory and practice*", 4th edition, CRC Press, 2019.