رمزنگاری پیشرفته ۲۵۱۷۲۱ ۱۴ خرداد ۱۴۰۲

رمزهای جریانی، اثبات‌های ناتراوا، مباحث منتخب

مدرس: *محمود سلماسی زاده* دانشگاه صنعتی شریف

اهداف تمرین

هدف این تمرین در بخش رمزهای جریانی، آشنایی با حمله‌ی همبستگی به رمزهای جریانی است. تعاریف دو نوع این حمله‌ی همبستگی، پایه و با منطق اکثریت، و اعمال آن‌ها به دو مولد کلید بررسی می‌شود.
همچنین به مضارب چندجمله‌ای، برای استفاده از خاصیت خطی دنباله‌ی خروجی ثبات‌های انتقال با تابع فیدبک خطی (LFSR)، پرداخته می‌شود.

در بخش اثبات‌های ناتراوا [۱] به پروتکل Schnorr و بررسی ویژگی‌های یک اثبات ناتراوا، مانند: امنیت، تمامیت [۲]، صحت [۳]، ناتراوایی، پرداخته می‌شود.

در بخش مباحث منتخب در رمزنگاری نیز سوالاتی در مورد تعریف فرمال، و حمله‌ی متن اصلی منتخب پرسیده شده است.

فهرست مطالب

۱ رمزهای جریانی

سوال ۱

1- مضارب چندجمله‌ای و خواص آن را توضیح دهید.
2- حمله‌ی همبستگی با منطق اکثریت را توضیح دهید و الگوریتم آن را بنویسید.
3- برای بدست آوردن شرایط اولیه‌ی LFSR ها، به مولد رشته‌ی کلید آمده در شکل ۱ حمله‌ی همبستگی پایه و اکثریت را اعمال کنید.

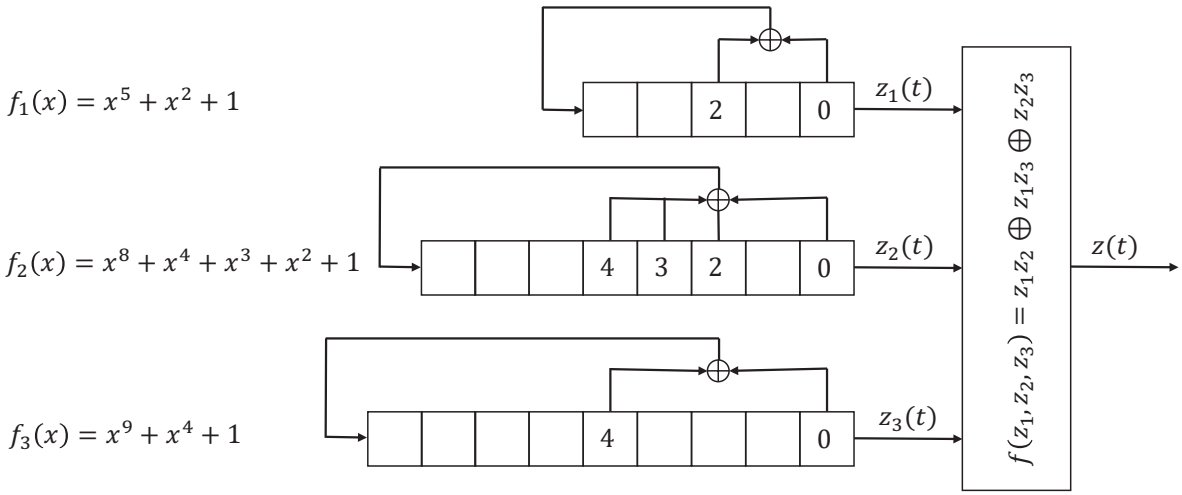
- در این حملات، مقدار احتمال همبستگی دنباله‌ی خروجی کلی با دنباله‌ی خروجی هر LFSR را با توجه به ضابطه‌ی تابع ترکیب‌کننده‌ی غیرخطی در نظر بگیرید.
- از روش مربع‌کردن برای مضارب چندجمله‌ای استفاده کنید که برای پیاده‌سازی حمله، می‌توانید

[۱] zero knowledge
[۲] completeness
[۳] soundness

از نرم‌افزار MATLAB® یا از Python استفاده نمایید.

- 256 بیت از دنباله‌ی خروجی کلی به قرار زیر است:

0110110010100001001011001111001011011101111000101101101111010001
1011001010000110001100111110000101110101000000111110011101000110
1100101000010000110001011010110111011100000011011001110100011011
0010101001001011000101001001011101110000000111101111010001101110



شکل ۱: مولد کلید با سه LFSR با تابع ترکیب‌کننده‌ی غیر خطی

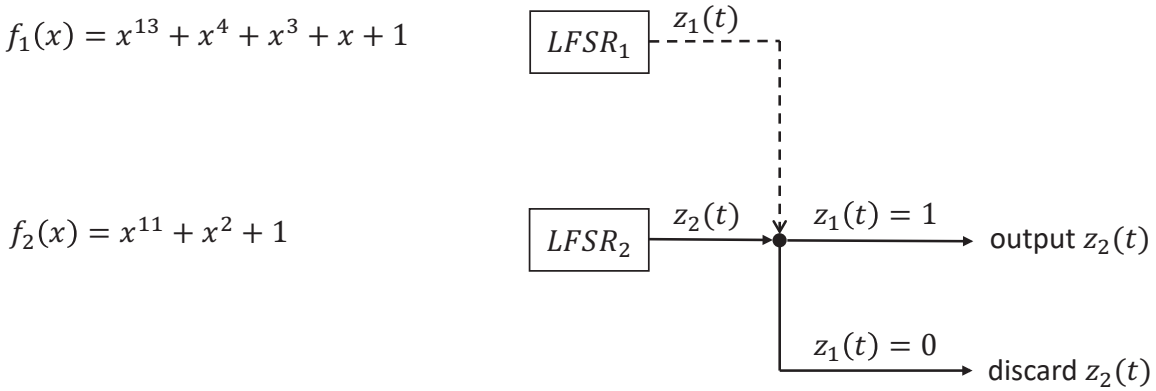
4- با توجه به توابع مولد داده شده، در مورد اثر تابع مولد، مانند درجه و وزن (تعدادجملات)، در بدست آوردن شرایط اولیه‌ی LFSR متناظرش بحث کنید.

سوال ۲

1- نحوه‌ی کار مولد جمع‌شونده را توضیح دهید.
2- مولد جمع‌شونده آمده در شکل ۲ را در نظر بگیرید.
256 بیت دنباله‌ی خروجی نهایی به صورت زیر است:

1010111001101000101000100000000000010000000101100101000000101100
0010101001000010001011100100000010101001000000000010100000000000
1000010011000000000101011000100101000000101000000000100110000000000
0010000010000000010010110100011000010001000001011000101100000010000

آیا می‌توان روشی با پیچیدگی کم‌تر از جست‌وجوی جامع برای بدست آوردن کلید رمزنگاری (شرایط اولیه‌ی LFSR ها) یافت؟



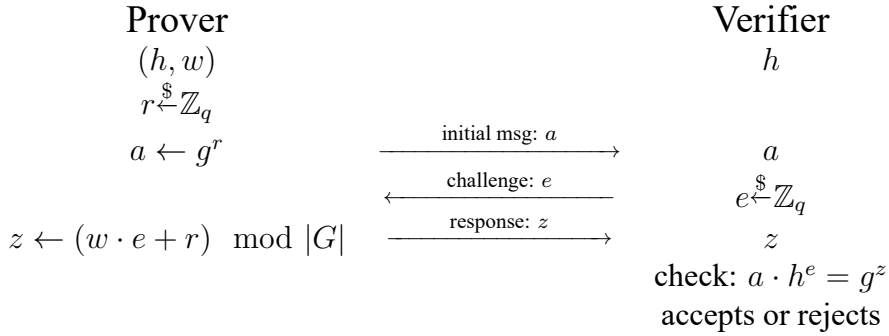
شکل ۲: مولد جمع‌شونده

۲ اثبات‌های ناتراوا

سوال ۳

در درس با مساله‌ی اثبات ناتراوای مبتنی بر مساله‌ی لگاریتم گسسته آشنا شدید. این پروتکل را غالبا با نام پروتکل Schnorr در نظر می‌گیرند. در شکل ۳ ساختار این پروتکل آورده شده است.

شکل ۳: ساختار پروتکل Schnorr



1- نشان دهید که این پروتکل با در نظر گرفتن وارسی‌کننده‌ی امین [۴] دارای ویژگی‌های تمامیت، صحت، و ناتراوایی است. برای نشان دادن ویژگی صحت، کافی است نشان دهید که احتمال متقاعد کردن وارسی‌کننده توسط یک اثبات‌کننده‌ی متقلب، ناچیز است.

2- می‌توان نشان داد که پروتکل مذکور تنها در صورت امین‌بودن وارسی‌کننده، دارای ویژگی ناتراوایی است. در صورت غیر امین‌بودن وارسی‌کننده چه راهکاری برای برقراری امنیت ساختار پیشنهاد می‌کنید؟

[۴] honest verifier

سوال ۴

با در نظر گرفتن پروتکل Schnorr، پروتکلی ناتراوا برای نشان‌دادن برابربودن دو مقدار لگاریتم گسسته‌ی زیر در مبنای متناظرشان بنویسید. ویژگی‌های تمامیت، صحت، و ناتراوایی آن را نشان دهید.

$$h = g^w, \qquad t = s^w$$

۳ مباحث منتخب در رمزنگاری

سوال ۵

از تمرینات آخر فصل اول [۱].

1- تعریفی فرمال از الگوریتم‌های Gen، Enc، و Dec برای رمز جانشینی تک‌الفبایی ارائه دهید.

2- تعریفی فرمال از الگوریتم‌های Gen، Enc، و Dec برای رمز Vigenére ارائه دهید.

سوال ۶

از تمرینات آخر فصل اول [۱]. نشان دهید رمزهای جابه‌جایی (سزار)، جانشینی، و Vigenére همه به سادگی با استفاده از یک حمله‌ی متن اصلی منتخب شکسته می‌شوند. چه مقدار متن اصلی برای بازیابی کلید هر یک از رمزها نیاز است؟

مراجع

[1] Jonathan Katz, Yehuda Lindell. "*Introduction to modern cryptography*", 3rd Edition, CRC Press, Taylor & Francis Group, A Chapman & Hall book, 2021.