دانشگاه صنعتی امیر کبیر
(پلی تکنیک تهران)

بسم الله الرحمن الرحیم

حمله تلاقی در میان به ساختارهای فایستل

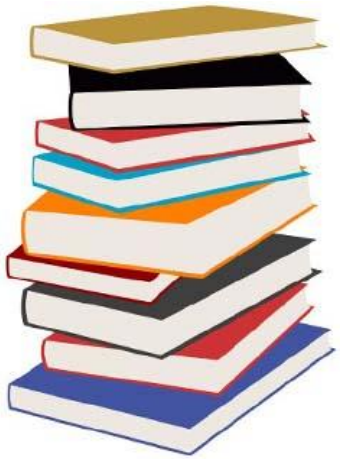
سید محمدمهدی احمدپناه
smahmadpanah@aut.ac.ir

ارائه درس معماشناسی کاربردی

دانشگاه صنعتی امیرکبیر
۲۷ بهمن ۱۳۹۴

دانشکده مهندسی کامپیوتر
و فناوری اطلاعات

فهرست



- مقدمه
- ساختارهای فایستل و حمله‌ها
- حمله تلاقی در میان
- حمله تلاقی در میان به ساختارهای فایستل و انواع آن
- جمع‌بندی
- مسائل باز
- پروژه کارشناسی ارشد

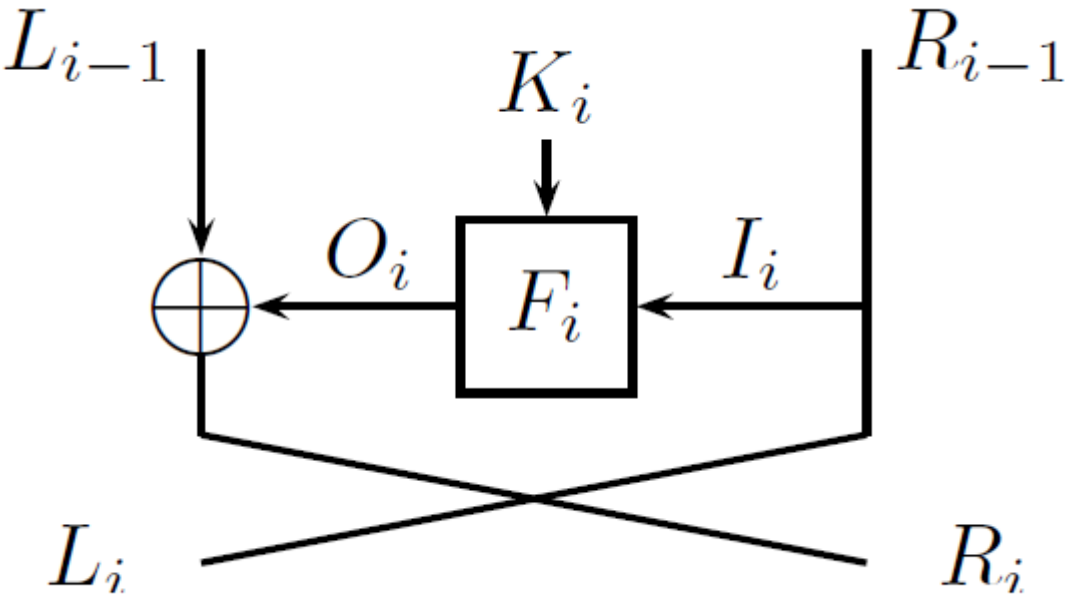
مقدمه

- اهمیت سیستم‌های رمز قطعه‌ای
- اهمیت ساختار فایستل
  - سیستم‌های رمزنگاری
    - DES، Triple-DES، Camelia، CAST، SIMON، LBlock و بسیاری از نامزدهای AES
  - توابع درهم‌ساز
    - SHA vite-3
  - طرح تصدیق اصالت LAC
    - CAESAR
- ضرورت بررسی امنیت این ساختار اولیه

مروری بر ساختار فایستل

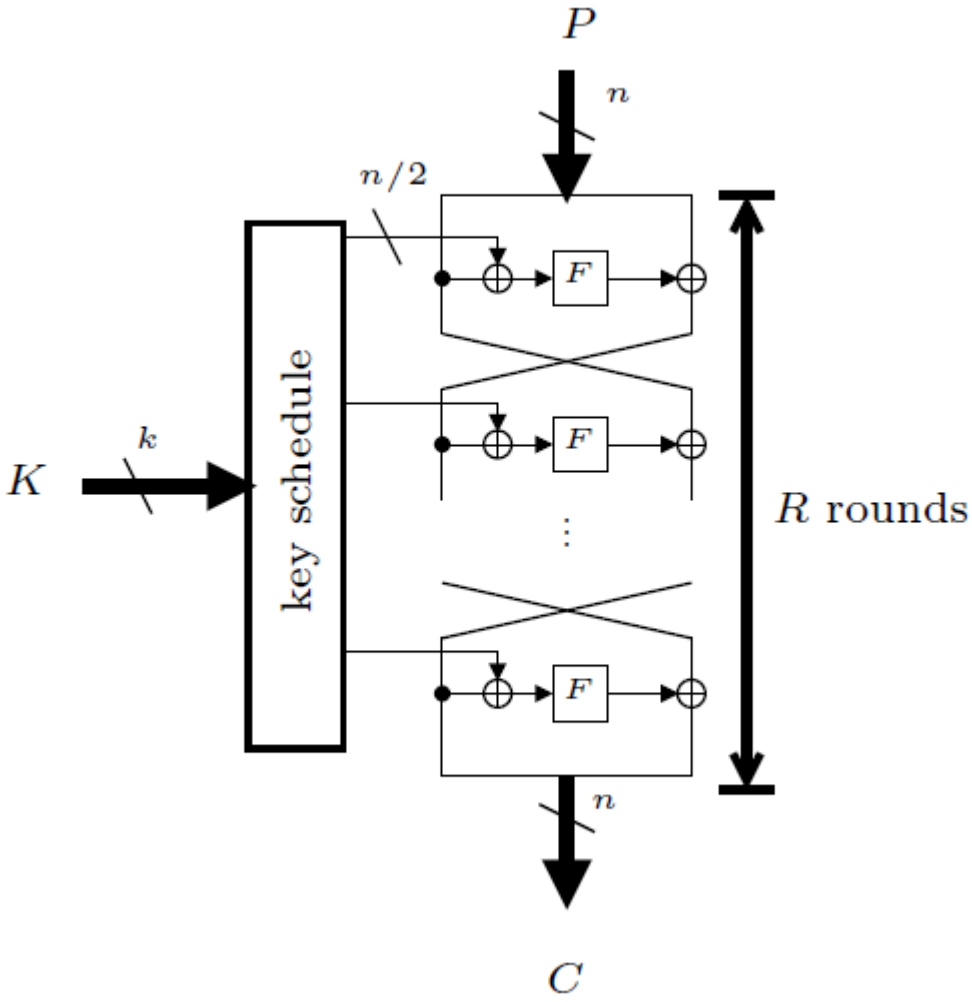
- تبدیل قطعه n-بیتی به دو قسمت مساوی (L_i, R_i)
- استفاده از زیرکلیدهای n/2-بیتی مستقل در هر l دور
- توابع دور F_i
  - $F_i(I_i , K_i) = O_i$
    - توابعی که در برابر حملات سریعتر از جستجوی جامع شکسته نشوند.

مروری بر ساختار فایستل (ادامه)



دور i-ام از یک ساختار فایستل

مروری بر ساختار فایستل (ادامه)



مروری بر ساختار فایستل (ادامه)

- $I_n = \{0,1\}^n$ is the set of the 2^n binary strings of length n.
- For $a, b \in I_n$, $[a, b]$ will be the string of length $2n$ of I_{2n} which is the concatenation of a and b.
- For $a, b \in I_n$, $a \oplus b$ stands for bit by bit exclusive or of a and b.
- $\circ$ is the composition of functions.
- The set of all functions from I_n to I_n is F_n. Thus $|F_n| = 2^{n \cdot 2^n}$.
- The set of all permutations from I_n to I_n is B_n. Thus $B_n \subset F_n$, and $|B_n| = (2^n)!$
- Let f_1 be a function of F_n. Let L, R, S and T be elements of I_n. Then by definition

$$\Psi(f_1)[L,R] = [S,T] \overset{\text{def}}{\Leftrightarrow} \begin{cases} S = R \\ \text{and} \\ T = L \oplus f_1(R) \end{cases}$$

- Let $f_1, f_2, \ldots, f_k$ be k functions of F_n. Then by definition:

$$\Psi^k(f_1, \ldots, f_k) = \Psi(f_k) \circ \cdots \circ \Psi(f_2) \circ \Psi(f_1).$$

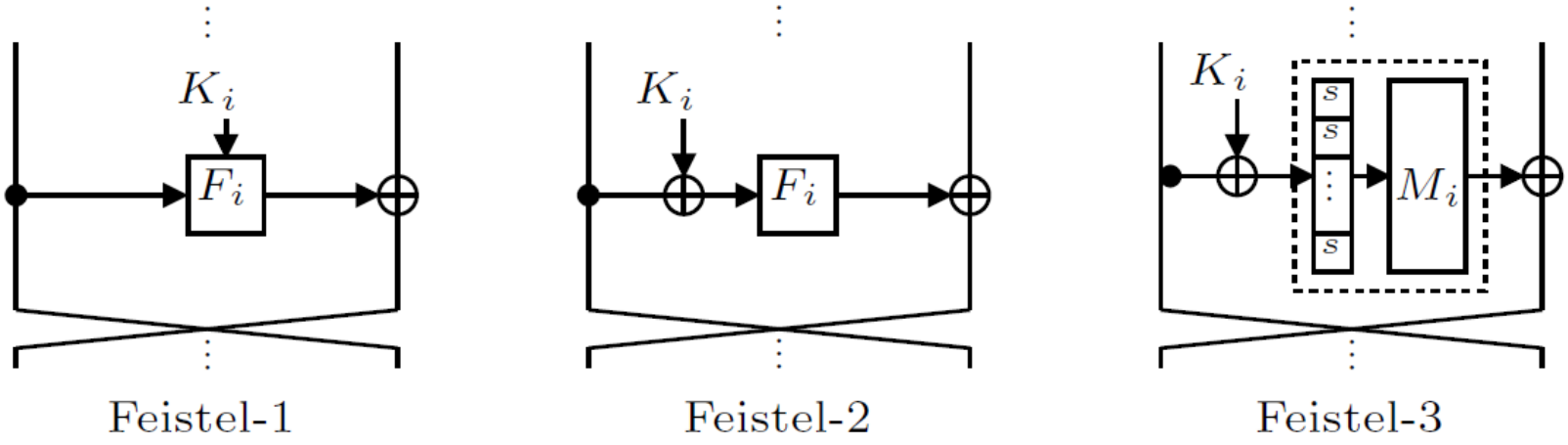
The permutation $\Psi^k(f_1, \ldots, f_k)$ is called "a Feistel scheme with k rounds" and also called Ψ^k.

ویژگی‌های ساختار فایستل

- یک به یک و پوشا بودن
  - مستقل از تابع دور
- استفاده از یک طرح برای رمز و ترجمه
- کلیدهای مستقل در هر دور
- هر دو دور متوالی معادل با یک دور در ساختار غیرفایستلی n-بیتی

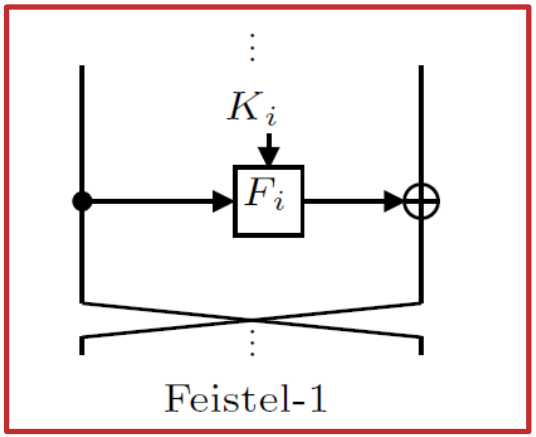
انواع ساختارهای فایستل

- متوازن و نامتوازن
  - یکسان بودن یا نبودن طول دو قسمت L و R
- انواع سه‌گانه
  - فایستل-۱، فایستل-۲، فایستل-۳

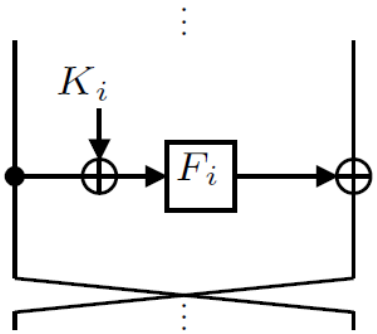


انواع ساختارهای فایستل (ادامه)

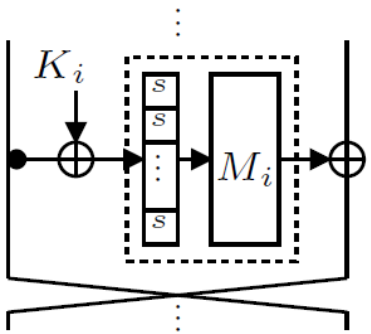
- فایستل-۱
  - توابع دور با کلید دلخواه مستقل از یکدیگر
    - توابع دور مستقل از یکدیگر



Feistel-1



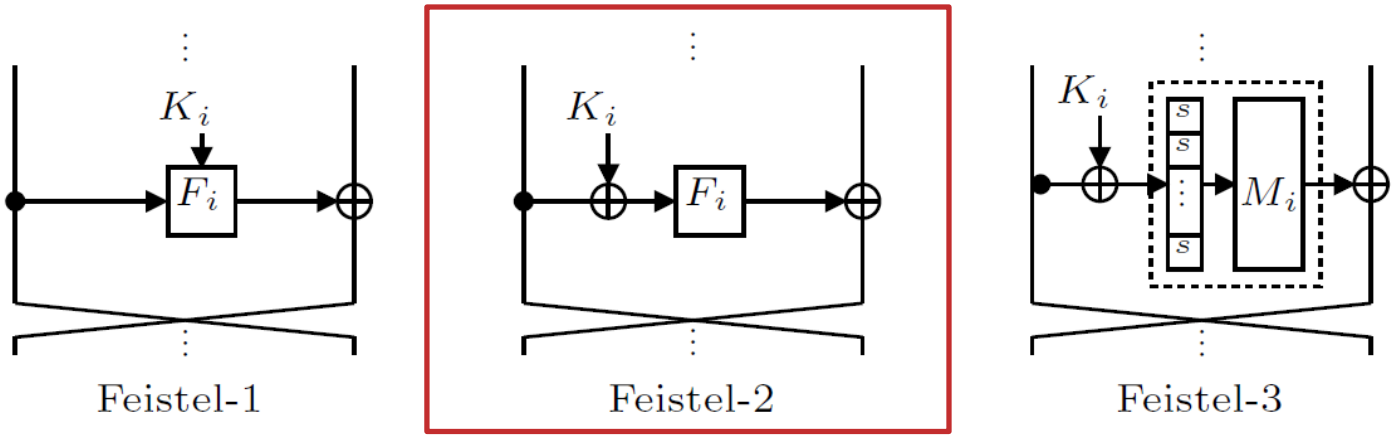
Feistel-2



Feistel-3

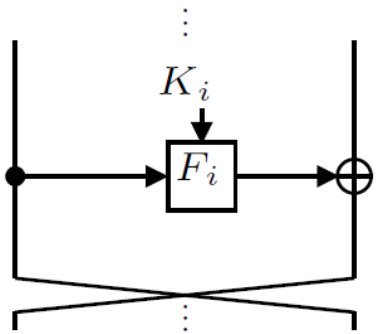
انواع ساختارهای فایستل (ادامه)

- فایستل-۲
  - در سیستم‌های رمز کاربردی
  - XOR با زیرکلید، قبل از تابع دور
  - $Y_i = F_i (X_i \text{ xor } K_i)$
    - F_i: تابع مشخص و ثابت در دور i-ام

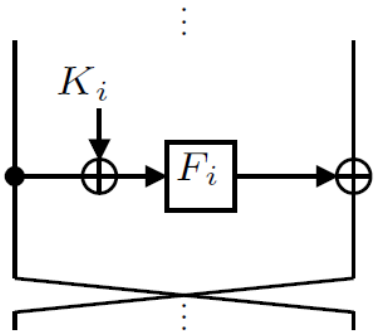


انواع ساختارهای فایستل (ادامه)

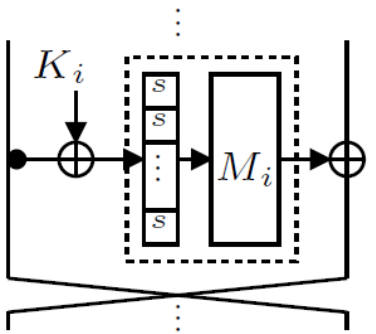
- فایستل-۳
  - فایستل-۲ای است که F_i باید از نوع SP باشد.
    - هر تابع دور شامل:
      - یک S-box دوطرفه (لایه S)
      - یک لایه پخش‌کننده خطی (لایه P)
    - XOR با زیرکلید n/2-بیتی قبل از تابع دور



Feistel-1

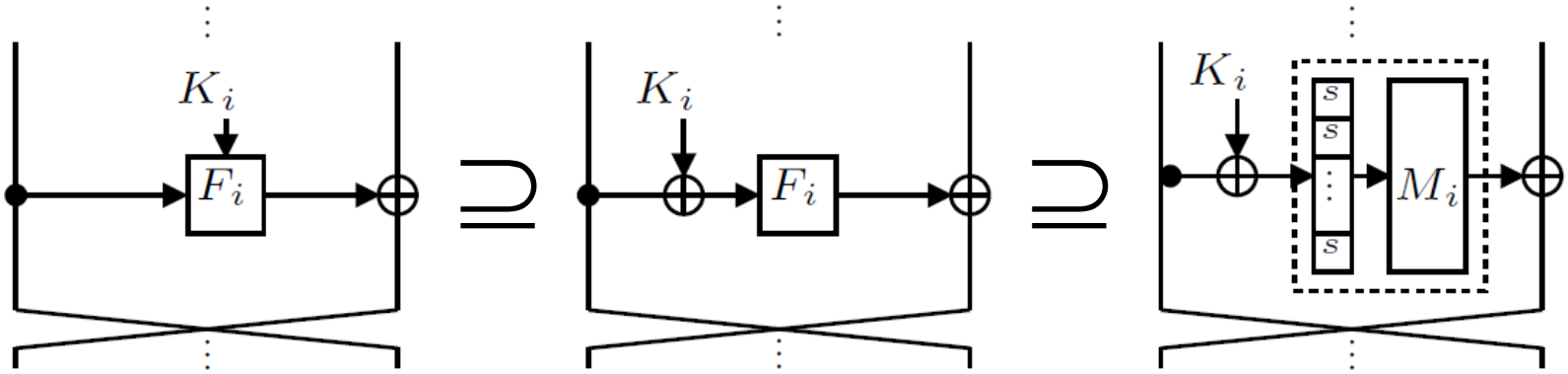


Feistel-2



Feistel-3

انواع ساختارهای فایستل (ادامه)



Feistel-1 Feistel-2 Feistel-3

حمله‌های عام به ساختار فایستل

- تعریف حمله‌های عام
  - حملاتی کارا به بیشتر طرح‌ها
  - دارای پیچیدگی ناچیز در مقایسه با جستجوی جامع
- حمله روی طرح فایستل یک دوری
  - با یک پرس‌وجو و $O(1)$
    - آیا نیمه اول خروجی برابر با نیمه دوم ورودی است؟
- حمله روی طرح فایستل دو دوری
  - به ازای ورودی‌های منتخب با پیچیدگی $O(1)$
  - به ازای ورودی‌های دلخواه با پیچیدگی $O(2^{\frac{n}{2}})$

حمله‌های عام به ساختار فایستل (ادامه)

- حمله روی طرح فایستل بیشتر از سه دور
  - نیاز به حداقل $O(2^{\frac{n}{2}})$ ورودی، حتی ورودی‌های منتخب
  - پیچیدگی $O(2^{\frac{n}{2}})$ برای سه یا چهار دور
- حمله روی طرح فایستل بیشتر از پنج دور
  - حداقل $O(2^{\frac{2n}{3}})$ پرس‌وجو، حتی با عدم محدودیت محاسباتی
  - معرفی حمله‌ای با پیچیدگی حداکثر $O(2^{\frac{3n}{2}})$ محاسبه و پیام واضح منتخب

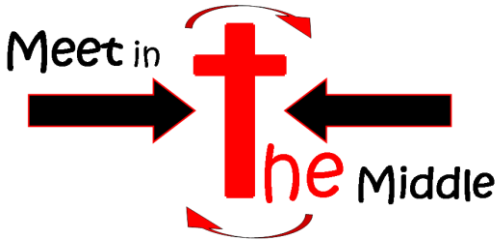
حمله‌های عام به ساختار فایستل (ادامه)

- برای افزایش سرعت الگوریتم رمز
  - تعداد دور کم
- برای افزایش امنیت الگوریتم رمز
  - تعداد دور زیاد
- سوال: حداقل تعداد دور لازم در یک طرح فایستل برای جلوگیری از همه حملات عام چیست؟
  - توصیه: **حداقل شش دور**

انواع حملات (تحلیل ها)

- جستجوی جامع
- تلاقی در میان
- خطی
- تفاضلی
- انتگرال
- تفاضلی-خطی
- تمایز
- افراز
- بومرنگ
- چرخشی
- زمانی
- کلید ضعیف
- موازنه زمان-حافظه-داده
- و...

حمله تلاقی در میان



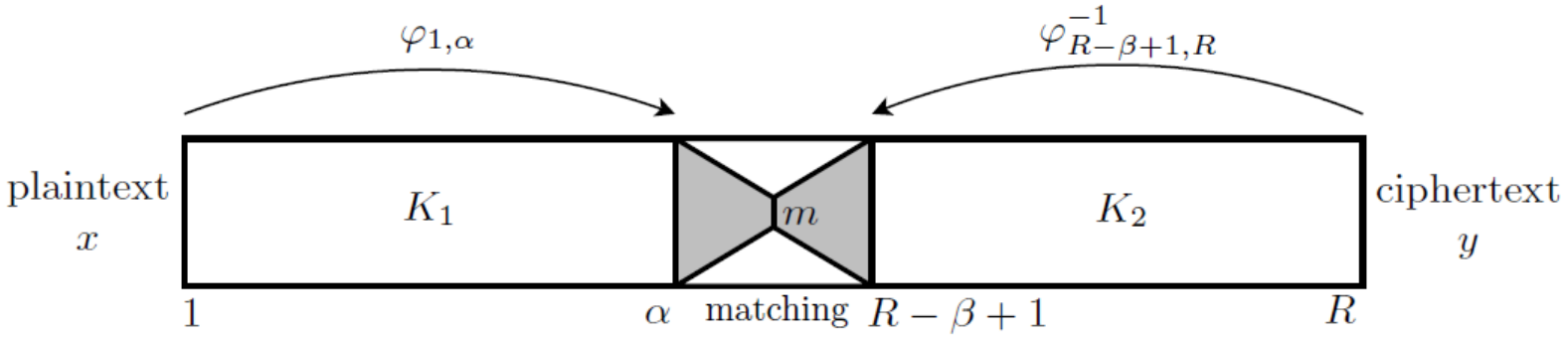
- سال ۱۹۷۷
  - معرفی توسط Diffie و Hellman
    - به عنوان روشی برای تحلیل رمز طرح‌های رمزنگاری دوگانه
- سال ۱۹۸۵
  - به کارگیری توسط Chaum و Evertse
    - در انواع مختلف DES دورکاهش‌یافته
- اکنون
  - از تکنیک‌های مهم و مطرح برای تحلیل رمز

حمله تلاقی در میان (ادامه)

- از انواع حملات کم‌داده (low-data)
  - استفاده از داده‌های کمتری نسبت به کل کتاب کد
    - نیاز به تعداد کمی متن واضح معلوم
- قابلیت اعمال روی ترکیب‌های چنددوری
- نسبت به تحلیل تفاضلی یا خطی، کمتر رایج است.

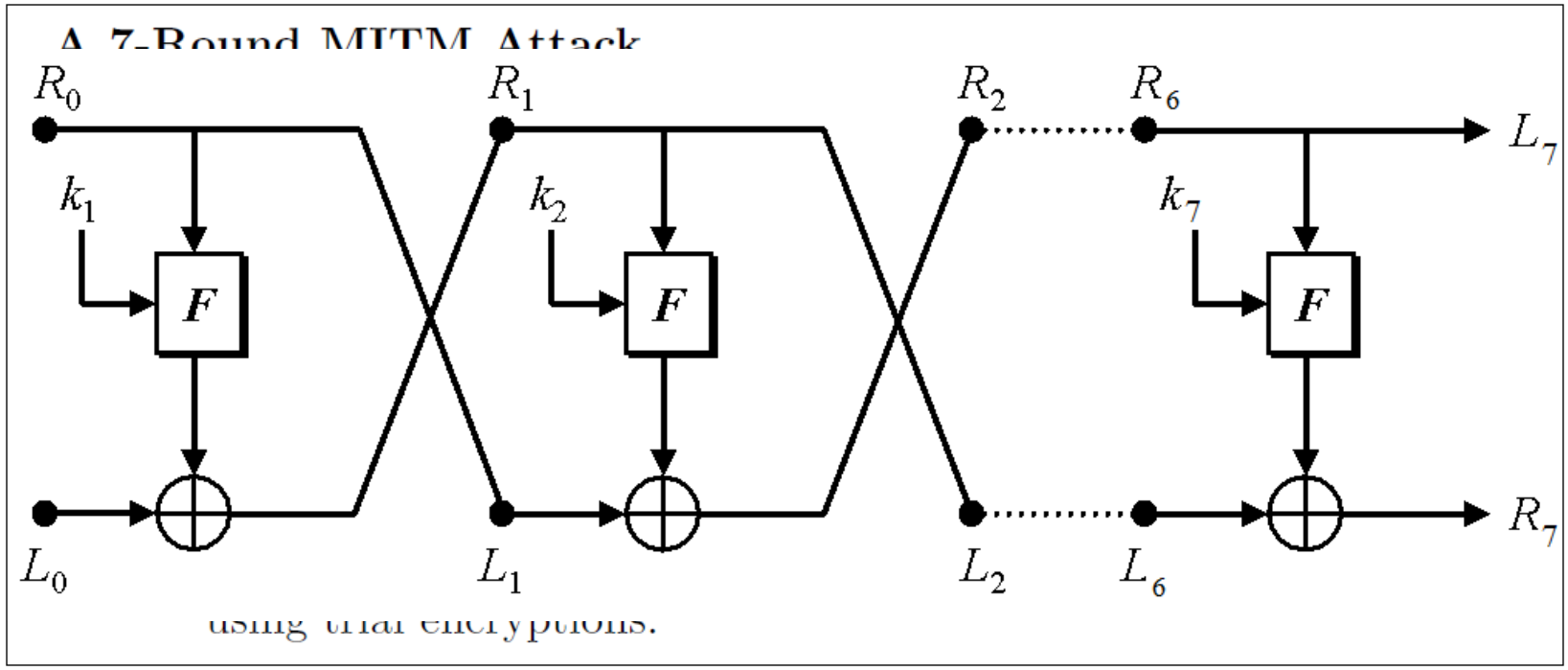
حمله تلاقی در میان (ادامه)

- $\varphi_{i,j}$: تبدیل جزئی یک سیستم رمز R-دوری، با شروع از دور i-ام و پایان در بلافاصله بعد از دور j-ام آن
- حدس برای زیرکلید بخش اول؛ محاسبه $\varphi_{1,\,\alpha}(p)$
- حدس برای زیرکلید بخش دوم؛ محاسبه $\varphi^{-1}_{\alpha+1,R}(c)$
  - کلید صحیح: $\varphi_{1,\,\alpha}(p) = \varphi^{-1}_{\alpha+1,R}(c)$



حمله تلاقی در میان (ادامه)

- حمله استاندارد تلاقی در میان به یک ساختار فایستل ۷-دوری



حمله تلاقی در میان (ادامه)

- حمله استاندارد تلاقی در میان به یک ساختار فایستل ۷-دوری
  - پیچیدگی زمانی گام دوم: $2^{1.5n}$ (معادل است با اندازه **List**)
  - پیچیدگی زمانی گام سوم:
    - برای هر طرف از عملیات رمز، $2^{1.5n}$ پیشنهاد برای کلید
    - تعداد کل پیشنهادهای کلید، پس از تطابق **2n**-بیتی در این گام:
      $$2^{1.5n+1.5n-2n} = 2^n$$
    - برای هر پیشنهاد، یک K_4 حدس زده می‌شود، که $2^{1.5n}$ کل عملیات رمز امتحان می‌شود.
    - پس پیچیدگی زمانی گام سوم، برابر با $2^{1.5n}$
  - پیچیدگی زمانی کل حمله: $2^{1.5n}$

حمله تلاقی در میان (ادامه)

- برای تعداد دور زوج 2r
  - حمله نامتوازن
    - r زیرکلید از یک طرف حمله و r-1 زیرکلید از طرف دیگر حمله!
  - اضافه کردن یک دور به ساختار فایستل
  - دوباره متوازن کردن حمله به کمک دونیم‌کردن حدس یکی از زیرکلیدهای بین دو طرف حمله

حمله تلاقی در میان (ادامه)

- برای تعداد دور زوج 2r
  - دوباره متوازن کردن حمله به کمک دونیم‌کردن حدس یکی از زیرکلیدهای بین دو طرف حمله
    - R_0 ثابت برای همه متن‌های واضح
    - $R_1 = Const \text{ xor } L_0$ (Const ثابت، وابسته به K_1)
    - تبدیل به 2r-1 دور و افزودن Const به نیمه راست متن واضح
  - استفاده از تکنیک «پیوند و برش» برای جداسازی حدس مقدار Const از طرفین حمله

انواع تکنیک‌های حمله تلاقی در میان

- تطابق جزئی (partial matching)
- تطابق احتمالاتی (probabilistic matching)
- استفاده از گراف‌های کامل دوبخشی (bicliques)
- غربال در میان (sieve-in-the-middle)
- ترکیب با حمله تشریح (dissection)

انواع تکنیک‌های حمله تلاقی در میان (ادامه)

- تطابق جزئی
  - محدودیت در فضای نگه‌داری مقادیر میانی
    - به دلیل تعداد دور زیاد الگوریتم رمز
  - تطابق تعداد کمی از بیت‌های انتخاب‌شده مقادیر میانی حمله تلاقی در میان، به جای تطابق همه بیت‌ها
  - مقاله: Cryptanalysis of A 3-Subset Meet-in-the-Middle Attack: KTANTAN the Lightweight Block Cipher

انواع تکنیک‌های حمله تلاقی در میان (ادامه)

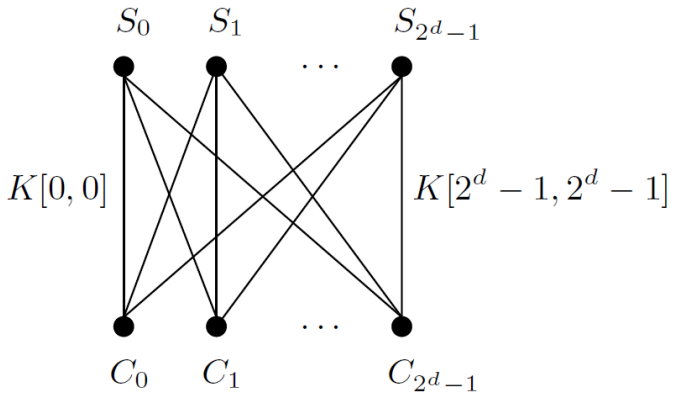
- تطابق احتمالاتی
  - محدودیت در فضای نگه‌داری مقادیر میانی
    - به دلیل تعداد دور زیاد الگوریتم رمز
  - تطابق احتمالاتی تعدادی از بیت‌های انتخاب‌شده یا همه بیت‌های مقادیر میانی حمله تلاقی در میان

انواع تکنیک‌های حمله تلاقی در میان (ادامه)

- استفاده از گراف‌های کامل دوبخشی
  - تعریف گراف کامل دوبخشی
    - گراف کاملی که بتوان مجموعه رئوس آن را به دو زیرمجموعه افراز کرد، به گونه‌ای که یک یال بین دو رأس وجود داشته باشد اگر و فقط اگر یکی از آن‌ها از مجموعه اول و دیگری از مجموعه دوم باشد.
  - گسترش تعداد دورهای ممکن حمله
  - امکان شکستن full AES و full IDEA
    - مزیت کوچکی نسبت به جستجوی جامع
  - انواع
    - Long biclique
    - Independent biclique

انواع تکنیک‌های حمله تلاقی در میان (ادامه)

- استفاده از گراف‌های کامل دوبخشی
  - تابع f: یک زیرسیستم رمز که 2^d حالت میانی $\{S_j\}$ را با 2^{2d} کلید $\{K[i,j]\}$ به 2^d متن رمزشده $\{C_i\}$ نگاشت می‌کند.
  - گراف کامل دوبخشی d-بُعدی
    - سه تایی $[\{C_i\}, \{S_j\}, \{K[i,j]\}]$
    - اگر برای هر $i,j \in \{0,\ldots,2^d - 1\}$ ، $C_i = f_{K[i,j]}(S_j)$



انواع تکنیک‌های حمله تلاقی در میان (ادامه)

- استفاده از گراف‌های کامل دوبخشی
  - گام‌های تحلیل:
    - گروه‌بندی همه کلیدهای ممکن به زیرمجموعه‌های کلید با اندازه 2^{2d}
      - کلید هر گروه در ماتریس K[i,j] با اندازه $2^d \times 2^d$
    - تقسیم سیستم رمز به f و g که E=fog و انجام حمله تلاقی در میان برای هر زیرسیستم رمز
      - K[i,0] و K[0,j] مجموعه کلید هر زیرسیستم رمز با تعداد اعضای 2^d
    - ساختن یک گراف کامل دوبخشی برای هر گروه از کلیدها
    - استفاده از decryption-oracle و دست‌یابی به متن‌های واضح P_i متناظر با متن‌های رمز شده C_i، به تعداد 2^d

انواع تکنیک‌های حمله تلاقی در میان (ادامه)

- استفاده از گراف‌های کامل دوبخشی
  - ادامه گام‌های تحلیل:
    - انتخاب یک حالت میانی S_j و متن واضح P_i متناظر با آن، و انجام حمله تلاقی در میان روی f و g
    - در صورت یافتن کلید کاندیدی که تطابق S_j با P_i صورت بگیرد، آن کلید را برای زوج دیگری از متن واضح-متن رمزشده آزمون می‌کنیم.
      - در صورتی که برای زوج دوم نیز معتبر باشد، با احتمال بالایی کلید درست خواهد بود.

انواع تکنیک‌های حمله تلاقی در میان (ادامه)

- غربال در میان
  - امکان حمله به تعداد دور بیشتر
  - جستجو برای وجود گذار معتبر بین S-box میانی
    - محاسبه تعدادی از بیت‌های ورودی و خروجی برای یک S-box میانی خاص
    - حذف کلیدهای کاندید که با گذار معتبر متناظر نیستند
  - امکان ترکیب با روش استفاده از گراف کامل دوبخشی

انواع تکنیک‌های حمله تلاقی در میان (ادامه)

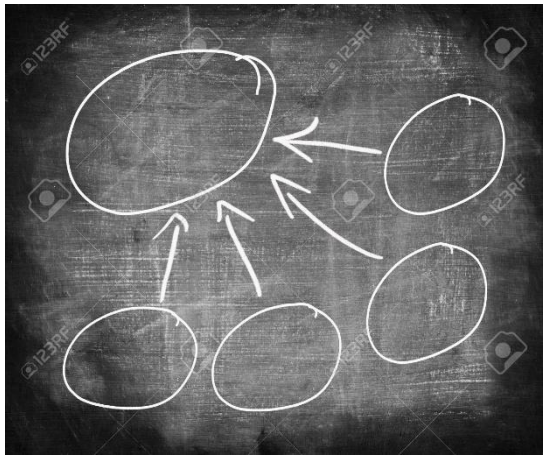
- ترکیب با حمله تشریح (dissection)
  - معرفی توسط Dinur و دیگران در ۲۰۱۲
  - بهبود چشمگیر موازنه زمان-حافظه مطرح در حملات تلاقی در میان، روی طرح‌های رمزکردن چندگانه با بیش از سه دور

انواع تکنیک‌های حمله تلاقی در میان (ادامه)

- ترکیب با حمله تشریح (dissection)
  - آغاز حمله با حدس درباره مقادیر مرتبط در میانه و سپس پیشروی به سمت دو نقطه انتهایی سیستم رمز
    - امکان شکستن مسئله تحلیل رمز به دو مسئله مستقل کوچکتر، با معلوم بودن زوج‌های متن واضح-متن رمزشده جدید در نقاط انتهایی هر یک از زیرسیستم‌ها
    - حل بازگشتی
      - امکان استفاده از روش تلاقی در میان برای حل برگ‌های درخت بازگشتی ساخته‌شده

جمع‌بندی

- ساختار فایستل، انواع و ویژگی‌های آن
- حملات عام و حمله تلاقی در میان
- تکنیک‌های مختلف حمله تلاقی در میان
  - بهبود پیچیدگی زمانی، حافظه‌ای و داده‌ای به کمک تکنیک‌ها و ترکیب آن‌ها با یکدیگر



مسائل باز

- تعداد دور بهینه برای طرح فایستل
  - امنیت
  - سرعت
- ترکیب تکنیک‌های مختلف با بهبودهای موجود در حمله تلاقی در میان
  - بهبود پیچیدگی‌های زمانی و حافظه‌ای
  - کاهش دادن مفروضات تکنیک‌ها و کلی‌سازی حمله
- اعمال حمله‌های مختلف روی سیستم‌های رمز کاربردی
  - افزایش تعداد دورها، برای حمله‌های موجود
- استفاده از حمله تلاقی در میان برای طرح‌های غیرفایستلی

پروژه کارشناسی ارشد

- حمله تلاقی در میان برای یک سیستم رمز کاربردی و بهبود پیچیدگی زمانی و حافظه‌ای
  - مطالعه انواع تکنیک‌ها و گونه‌های حمله تلاقی در میان
  - انتخاب سیستم رمز کاربردی و واقعی مناسب
    - تعیین تعداد دور برای تحلیل
  - تلفیق تکنیک‌ها و ایده‌های مختلف و جدید برای انجام حمله با رویکرد بهبود پیچیدگی زمانی و حافظه‌ای
    - با در نظر گرفتن حداقل مفروضات، برای کلی‌سازی حمله روی سیستم‌های دیگر

منابع و مراجع

[۱] I. Dinur, O. Dunkelman, N. Keller and A. Shamir, "New Attacks on Feistel Structures with Improved Memory Complexities ", Advances in Cryptology, CRYPTO 2015, 35th Annual Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2015, Proceedings, Part I, pp. 433-454.

[۲] J. Guo, J. Jean, I. Nikolic and Y. Sasaki, "Meet-in-the-Middle Attacks on Generic Feistel Constructions", Advances in Cryptology, ASIACRYPT 2014, 20th International Conference on the Theory and Application of Cryptology and Information Security, Kaoshiung, Taiwan, R.O.C., December 7-11, 2014. Proceedings, Part I, pp. 458-477.

[۳] T. Isobe and K. Shibutani, "All Subkeys Recovery Attack on Block Ciphers: Extending Meet-in-the-Middle Approach", Selected Areas in Cryptography, 19th International Conference, SAC 2012, Windsor, ON, Canada, August 15-16, 2012, Revised Selected Papers, pp. 202-221.

[۴] A. Canteaut, M.Naya-Plasencia and B. Vayssiere, "Sieve-in-the-Middle: Improved MITM Attacks," Advances in Cryptology, CRYPTO 2013, 33rd Annual Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2013. Proceedings, Part I, pp. 222-240.

[۵] J. Patarin, "Generic Attacks on Feistel Schemes", Advances in Cryptology, ASIACRYPT 2001, 7th International Conference on the Theory and Application of Cryptology and Information Security Gold Coast, Australia, December 9–13, 2001 Proceedings, pp. 222-238.

منابع و مراجع

[۶] A. Bogdanov and C. Rechberger, "A 3-Subset Meet-in-the-Middle Attack: Cryptanalysis of the Lightweight Block Cipher KTANTAN", Selected Areas in Cryptography, 17th International Workshop, SAC 2010, Waterloo, Ontario, Canada, August 12-13, 2010, Revised Selected Papers, pp. 229-240.

[۷] H. Feistel, W. A. Notz and J. L. Smith, "Some cryptographic techniques for machine-to-machine data communications", Proceedings of the IEEE , Volume:63 , Issue: 11, 1975, pp. 1545-1554.

[۸] T. Isobe and K. Shibutani, "Generic Key Recovery Attack on Feistel Scheme", Advances in Cryptology, ASIACRYPT 2013, 19th International Conference on the Theory and Application of Cryptology and Information Security, Bengaluru, India, December 1-5, 2013, Proceedings, Part I, pp. 464-485.

[۹] A. Bogodanov, D. Khovratovich and C. Rechberger, "Biclique Cryptanalysis of the Full AES", Advances in Cryptology, ASIACRYPT 2011, 17th International Conference on the Theory and Application of Cryptology and Information Security, Seoul, South Korea, December 4-8, 2011. Proceedings, pp. 344-371.

[۱۰] W. Diffie and M. E. Hellman "Special Feature Exhaustive Cryptanalysis of the NBS Data Encryption Standard", Journal Computer IEEE Computer Society Press Los Alamitos, CA, USA, Volume 10, Issue 6, June 1977, pp. 74-84.

با سپاس از توجه شما! ☺