بسم الله الرحمن الرحیم

قطب علمی رمز

دانشگاه صنعتی شریف

انواع حمله ها به سامانه های رمز کدمبنا

معصومه کوچک شوشتری

دانشکده مهندسی برق دانشگاه صنعتی خواجه نصیر

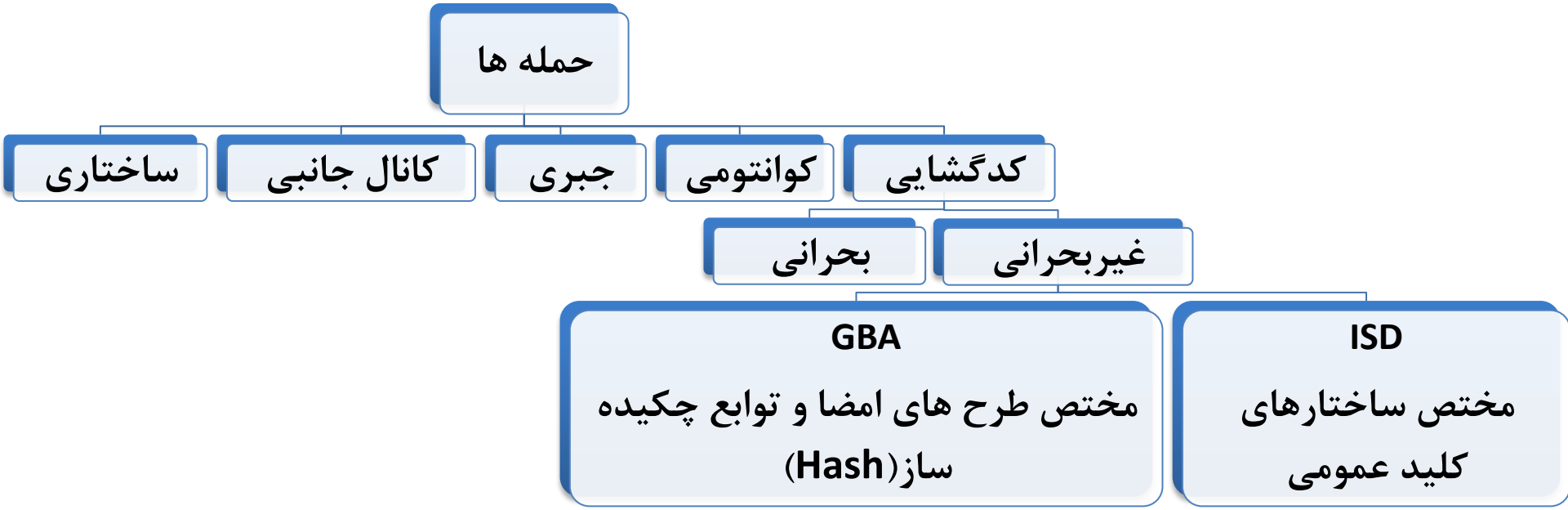
m-koochak@ee.kntu.ac.ir

فهرست مطالب

- معرفی انواع حمله های مطرح شده به سامانه های رمز کدمبنا
- مقدماتی از نظریه کدینگ و جبر خطی
- انواع حمله های کدگشایی
  - حمله های پایه
  - حمله های بهبودیافته
- مقایسه میان حمله های کدگشایی
- جمع بندی

معرفی انواع حمله های مطرح شده به سامانه های رمز کد مبنا

انواع حمله های رمزنگاری



فاکتور کار (Work Factor):

کمترین پیچیدگی محاسباتی (عملیات باینری) برای شکستن یک سامانه رمز

ISD= Information Set Decoding

GBA= Generalized Birthday attack

حمله های ساختاری (Structural Attacks)

- هدف یافتن کلید خصوصی با استفاده از کلید عمومی

1. حمله های جستجوی کامل (Brute force)

- یافتن ماتریس مولد کد $G_{k\times n}$ ← تعداد $\frac{2^{n-k}}{t}$
- یافتن ماتریس جایگشت $P_{n\times n}$ (Permutation Matrix) ← تعداد n!
- یافتن ماتریس درهم ساز $S_{k\times k}$ (Scrambling Matrix) ← تعداد 2^{k^2}
- مقاوم بودن ساختار اولیه McEliece

2. ضعف های ساختاری یا ساختار منظم

- مانند ضعف در ساختار های مبتنی بر کدهای GRS Reed Muller

حمله های کانال جانبی (Side Channel Attacks)

- **هدف** یافتن اطلاعاتی درباره کلید خصوصی و یا پیام در پیاده سازی های سخت افزاری و نرم افزاری است با فرض در اختیار بودن ابزار رمز (حمله های متن رمزشده انتخابی).

1. حمله های زمانی (Timing attacks)

- نشت اطلاعات زمانی هنگام تصحیح بردار خطا در چندجمله ای جایگاه خطا [STMOS08, SSMS09]

2. حمله های توان (Power attacks)

- تحلیل ساده توان SPA (Simple Power Analysis) ، [HMP10, MSSS11]
  - نشت اطلاعات توان از ماتریس جایگشت؛
  - توان مصرفی الگوریتم اقلیدسی تعمیم یافته در یافتن جایگاه خطا.
- تحلیل تفاضلی توان DPA (Differential Power Analysis) [CEMS15]
  - اجرا شده روی QC-MDPC McEliece ؛
  - نشت اطلاعات توان در محاسبه سندروم + محاسبات جبری برای یافتن ارتباط کلید خصوصی و عمومی.

حمله های جبری (Algebraic Attacks)

مسئله تشخیص کد گوپا Goppa Code Distinguishing (GD)

تشخیص ماتریس مولد یک کد گوپا از یک ماتریس تصادفی.

- کاربرد: امنیت اثبات پذیر کلیدعمومی و طرح های امضا.
- این حمله برای کدهای Goppa و کدهای Alternant با نرخ نزدیک به یک قابل اجراست.
- تشکیل یک دستگاه معادلات خطی برای کدبرداری هر کد خطی، با استفاده از رابطه $HG^T = 0$ (اگرچه داده هایش برای کدبرداری کم است اما می توان از آن برای تشخیص کد استفاده نمود.)

حمله های کدگشایی (Decoding Attacks)

- **هدف** یافتن پیام ارسال شده باتوجه به پیام رمزشده است.
- **بحرانی :** با افرایش پارامترهای کد نمی توان از آن ها جلوگیری کرد.
  - نیازمند اطلاعات اضافی از جمله قسمتی از پیام رمزشده و یا ارتباط دو متن رمز شده هستند.
- **غیربحرانی:** با افزایش پارامترها امنیت مورد نظر حاصل می شود.
  - کدگشایی مجموعه های اطلاعاتی (ISD)
  - تعیین کننده فاکتور کار حمله به سامانه های رمز کدمبنا است.

حمله های کوانتومی (Quantum Attacks)

- **هدف** استفاده از الگوریتم های کوانتومی در اجرای حمله ها
- حمله **Grover** (PQCrypto 2010 [Ber10]): اجرای حمله **ISD** برای یافتن پیام
  - همچنان پیچیدگی در حالت نمایی باقی می ماند.
  - برای پارامترهای سیستم **(n, k, t) = (4096, 3556, 45)** امنیت $2^{100} \rightarrow 2^{128}$
- حمله **Quantum Fourier Sampling** (CRYPTO 2011 [DMR11]):
  یافتن ماتریس کد مخفی
  - ناموفق

مقدماتی از
نظریه کدینگ و جبرخطی

کدهای باینری خطی

- زمان اجرای الگوریتم های کدبرداری : **T(n,k,d)**
- زمانی که **n→∞**، بنابر تعریف کران **Gilbert-Varshamov**، **k** و **d** باهم ارتباط پیدا می کنند. بنابراین

$$T(n,k,d) = T(n,k)$$

- الگوریتم ها را با ضریب پیچیدگی **F(k)** آن ها مقایسه می کنیم یعنی

$$T(n,k) = O(2^{F(k)n})$$

برخی نکات از جبرخطی

- تبدیل های (جبر خطی) مجاز
  - جایگشت ستون های H مسئله را تغییری نمی دهد.

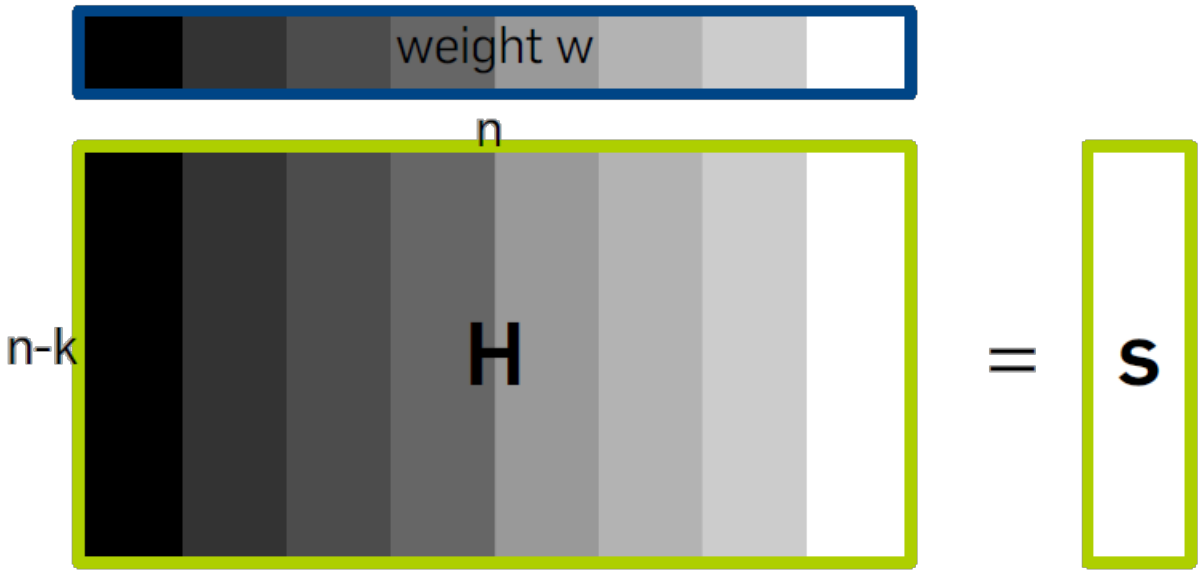


Image courtesy of Alexander Meurer (Link)

برخی نکات از جبرخطی

- تبدیل های (جبر خطی) مجاز
  - جایگشت ستون های H مسئله را تغییری نمی دهد.

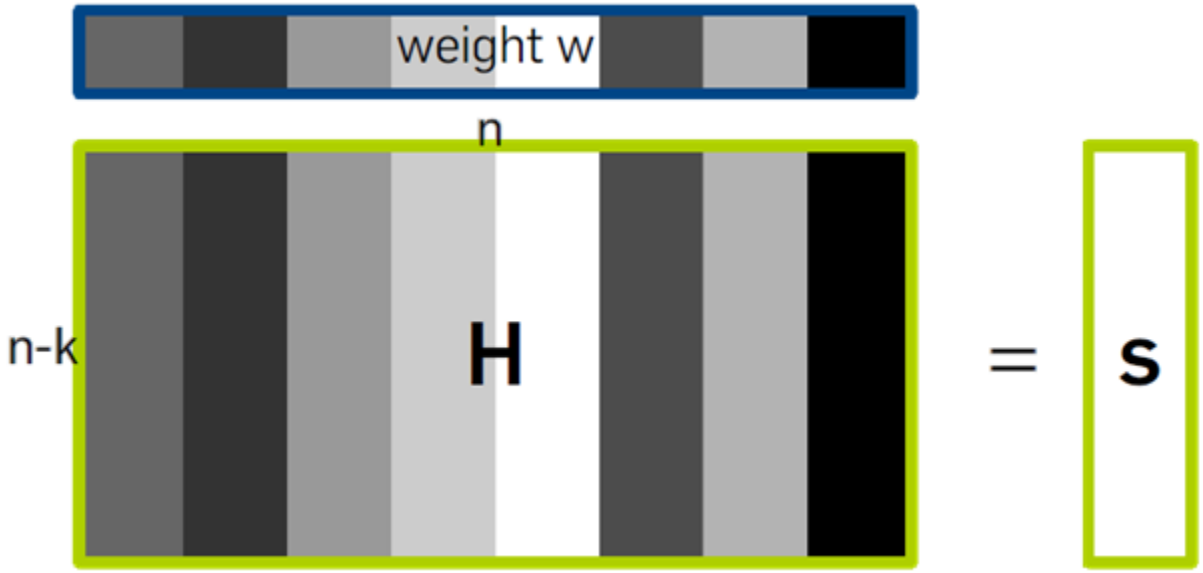


Image courtesy of Alexander Meurer (Link)

برخی نکات از جبرخطی

- تبدیل های (جبر خطی) مجاز
  - جایگشت ستون های H مسئله را تغییری نمی دهد.
  - عملیات سطری ساده روی سطرهای H مسئله را تغییری نمی دهد.

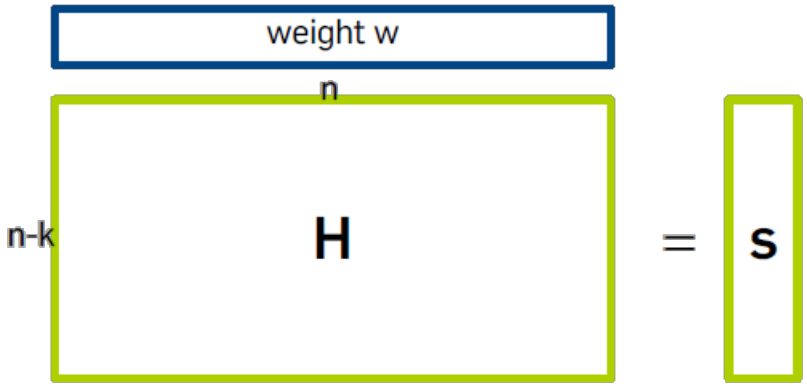


Image courtesy of Alexander Meurer (Link)

برخی نکات از جبرخطی

- تبدیل های (جبر خطی) مجاز
  - جایگشت ستون های **H** مسئله را تغییری نمی دهد.
  - عملیات سطری ساده روی سطرهای **H** مسئله را تغییری نمی دهد.

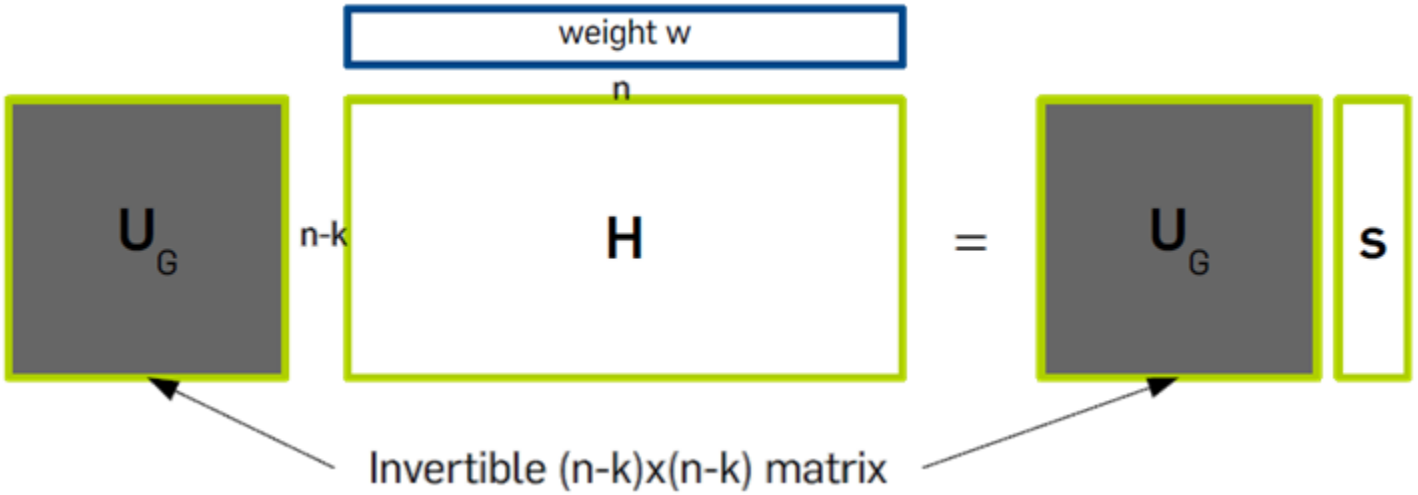
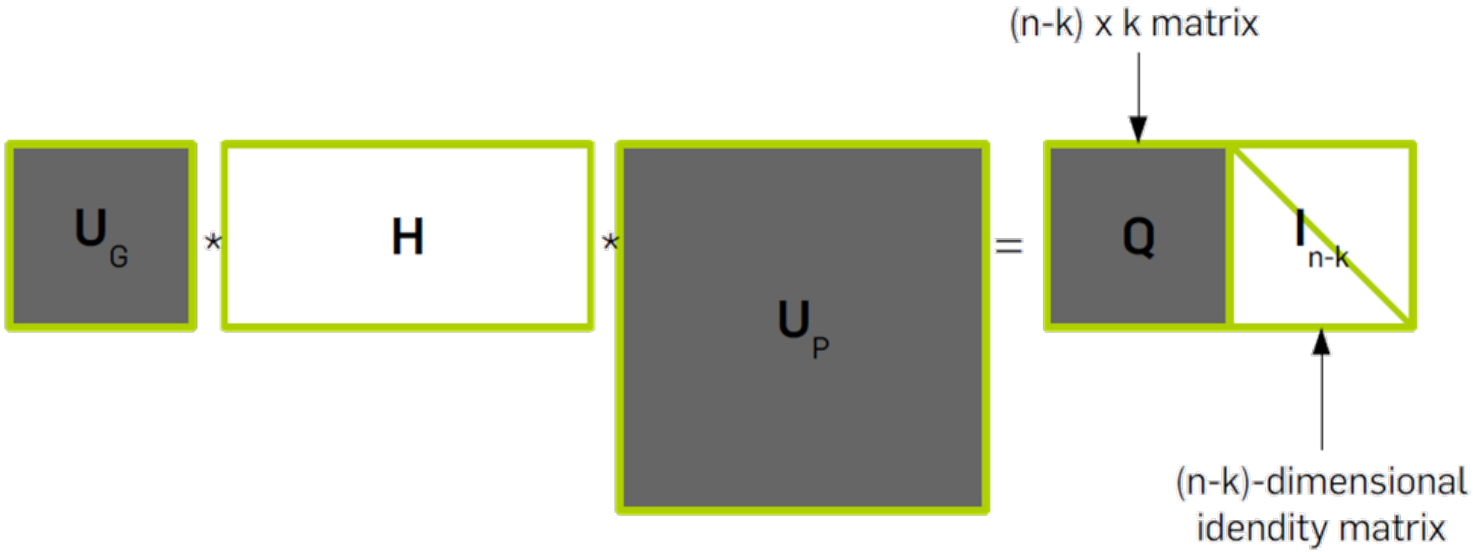


Image courtesy of Alexander Meurer (Link)

ساختار سیستماتیک تصادفی

- ما روی یک مدل تصادفی شده از H با جایگشتی روی ستون هایش که به صورت سیستماتیک در آمده است کار می کنیم:



- از این پس ما روی یک مدل سیستماتیک از H با یک جایگشت تصادفی روی ستون هایش، کار می کنیم.

Image courtesy of Alexander Meurer (Link)

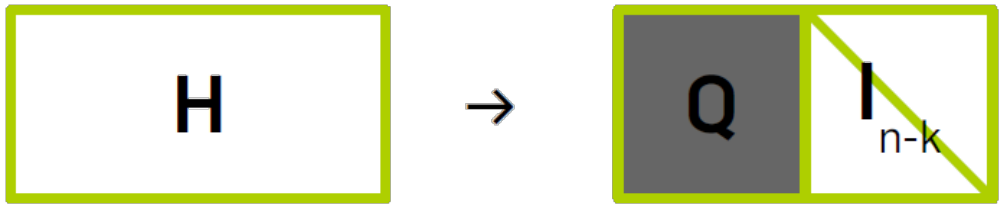
انواع حمله های کدگشایی

مجموعه اطلاعاتی (Information set)

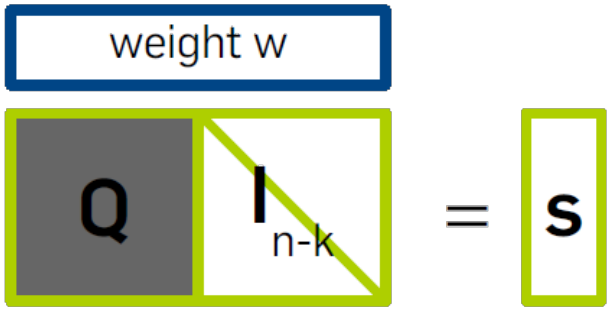
- **مجموعه اطلاعاتی A:** برای یک کد خطی با طول n و بعد k
  - یک زیرمجموعه k عضوی $A \subset \{1, \ldots, n\}$ به نحوی که
  - k ستونی از G که اندیس آن ها از A انتخاب شده است، یک زیرماتریس $k \times k$ معکوس پذیر را بسازند.
  - n-k ستون دیگر می توانند ماتریس H را به حالت سیستماتیک تبدیل کند.

مراحل کدبرداری مجموعه اطلاعاتی (ISD)

- **مرحله تصادفی سازی:** ماتریس **H** را به مدل سیستماتیک با ستون های جایگشت یافته تبدیل می کنیم.



- **مرحله جستجو:** تلاش برای یافتن e =، یعنی:

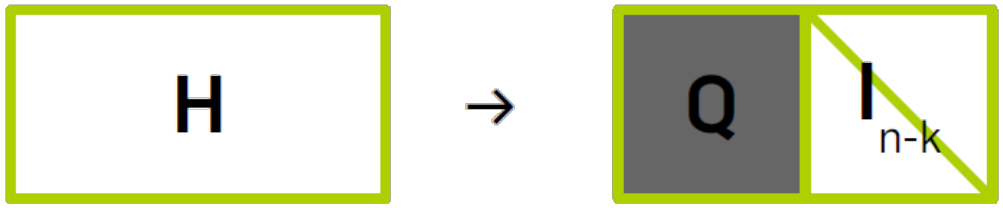


- **اگر هیچ پاسخی پیدا نشد، دوباره تصادفی سازی کنید!**

Image courtesy of Alexander Meurer (Link)

مراحل کدبرداری مجموعه اطلاعاتی (ISD)

- **مرحله تصادفی سازی:** ماتریس H را به مدل سیستماتیک با ستون های جایگشت یافته تبدیل می کنیم.



- **مرحله جستجو:** تلاش برای یافتن weight w = e، یعنی:

weight w

$$T(n,k,d) = Pr[\text{“خوب” تصادفی سازی}]^{-1} \times C\ [\text{جستجو}]$$

- اگر هیچ پاسخی پیدا نشد، دوباره تصادفی سازی کنید!

Image courtesy of Alexander Meurer (Link)

ارتباط مسئله سخت با حمله ISD

مسئله کدگشایی سندروم

- ورودی: ماتریس **H**، سندروم $\mathbf{s} = \mathbf{H}\cdot\mathbf{y} = \mathbf{H}\cdot(\mathbf{c}+\mathbf{e}) = \mathbf{H}\cdot\mathbf{e}$ و $\mathbf{w}$.
- هدف: **e** را با وزن همینگ کمتر از **w** به نحوی بیابید که $\mathbf{H}.\mathbf{e}=\mathbf{s}$

Image courtesy of Alexander Meurer (Link)

ارتباط مسئله سخت با حمله ISD

مسئله کدگشایی سندروم

- ورودی: ماتریس **H**، سندروم $\mathbf{s} = \mathbf{H}\cdot\mathbf{y} = \mathbf{H}\cdot(c+e) = H\cdot e$ و w.
- هدف: **e** را با وزن همینگ کمتر از w به نحوی بیابید که **H**.e=s

← ترکیب خطی از W ستون از **H** که جمعشان برابر با S باشد.

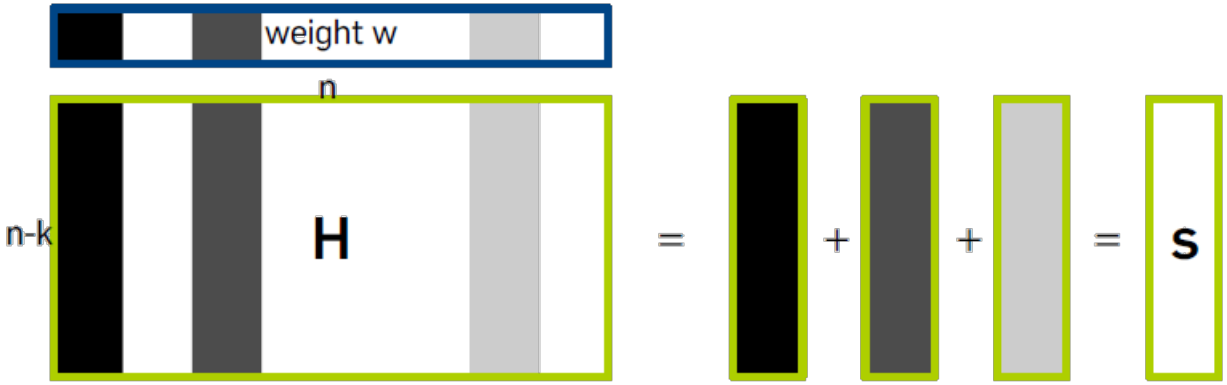


Image courtesy of Alexander Meurer (Link)

ارتباط مسئله سخت با حمله ISD

مسئله کدگشایی سندروم

- ورودی: ماتریس **H**، سندروم $\mathbf{s} = \mathbf{H}\cdot\mathbf{y} = \mathbf{H}\cdot(\mathbf{c}+\mathbf{e}) = \mathbf{H}\cdot\mathbf{e}$ و w.
- هدف: **e** را با وزن همینگ کمتر از w به نحوی بیابید که $\mathbf{H}.\mathbf{e}=\mathbf{s}$

← ترکیب خطی از W ستون از **H** که جمعشان برابر با S باشد.

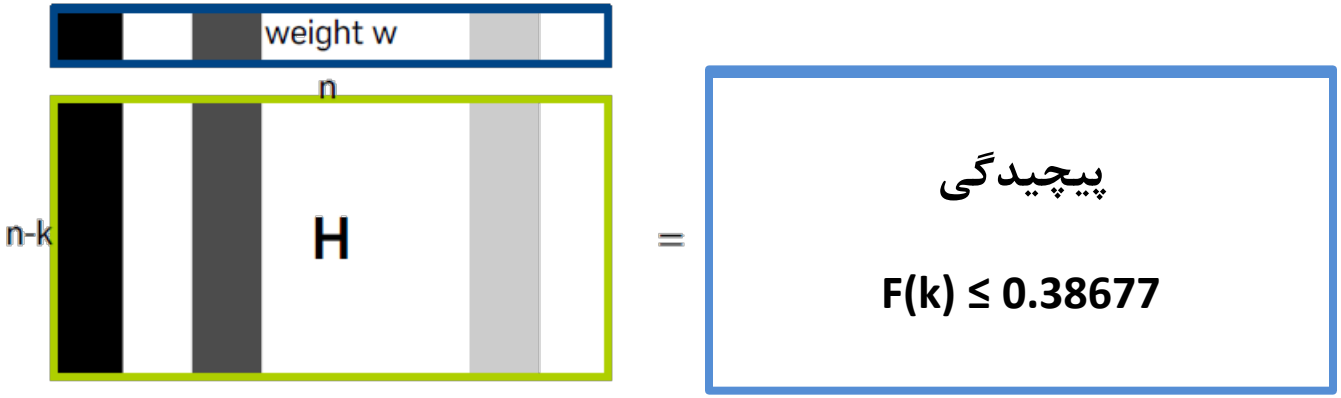


Image courtesy of Alexander Meurer (Link)

ارتباط مسئله سخت با حمله ISD

مسئله کدگشایی سندروم

- ورودی: ماتریس **H**، سندروم $\mathbf{s} = \mathbf{H}\cdot\mathbf{y} = \mathbf{H}\cdot(c+e) = H\cdot e$ و w.
- هدف: **e** را با وزن همینگ کمتر از w به نحوی بیابید که **H.e=s**

← ترکیب خطی از W ستون از **H** که جمعشان برابر با S باشد.

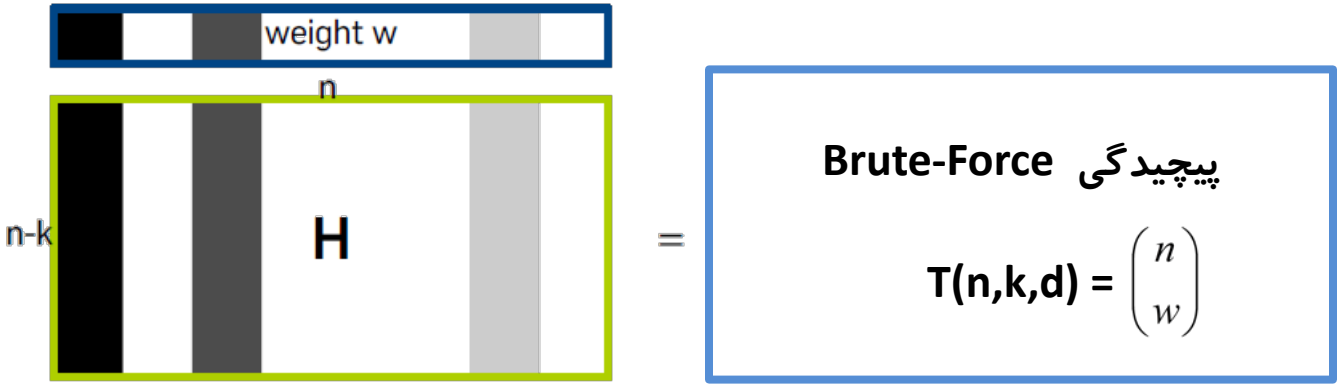
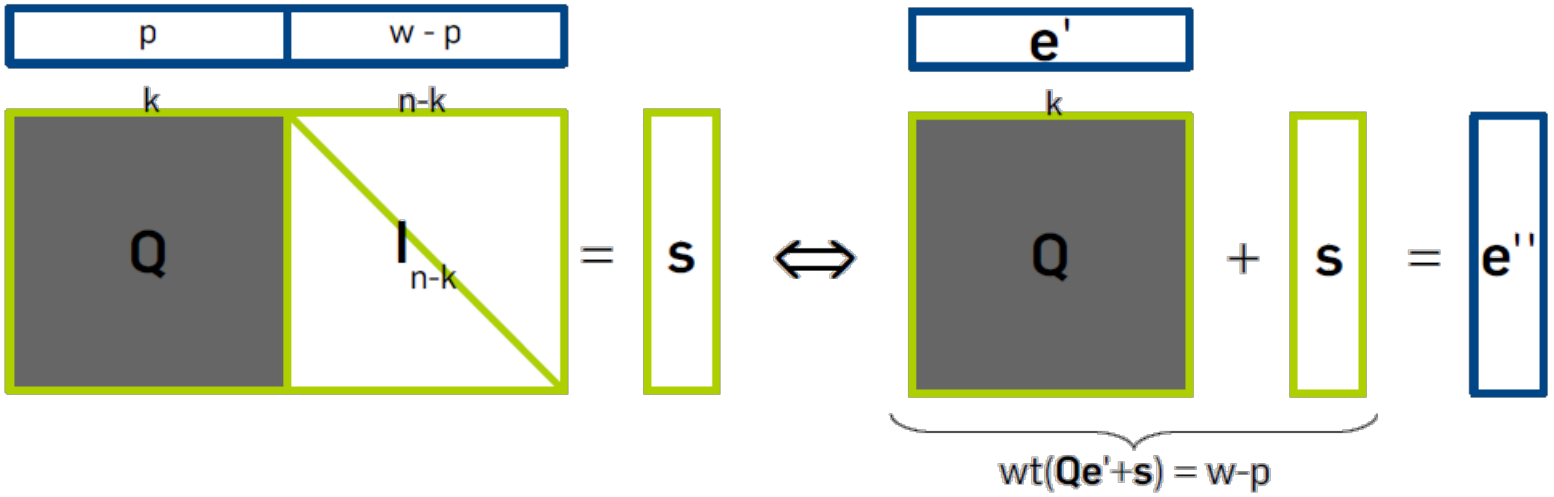


Image courtesy of Alexander Meurer (Link)

انواع الگوریتم های ISD پایه

Lee-Brickel (LB88)

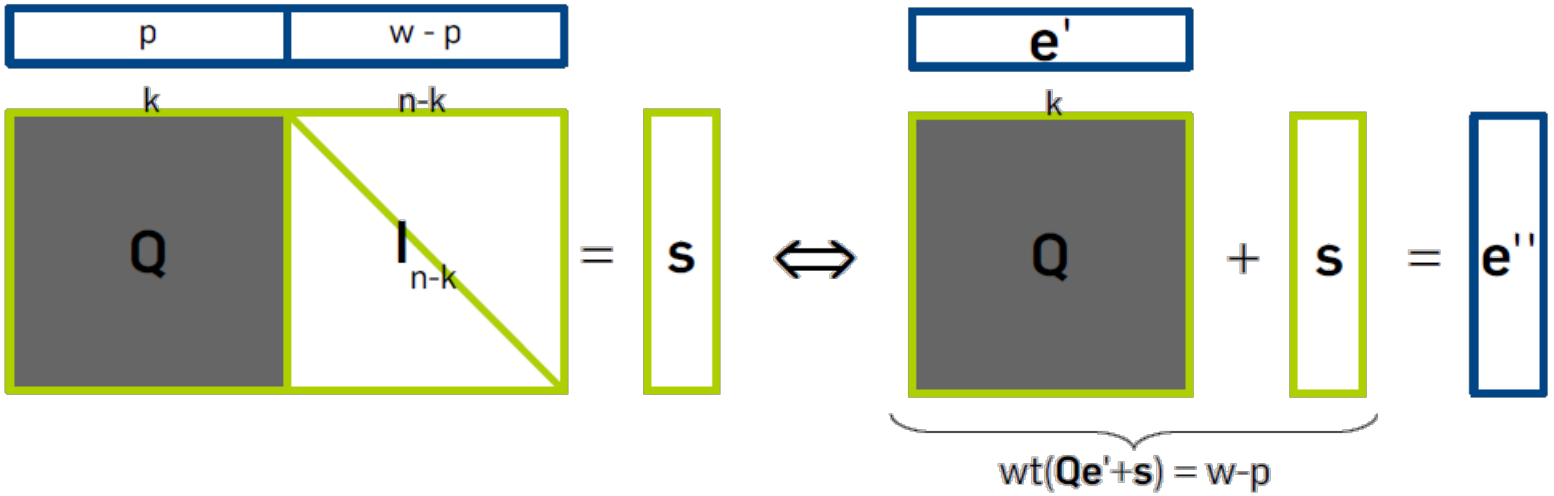


- جستجوی کامل روی Q، یعنی جستجوی $e'=$ [p] با $wt(Qe'+s) = w-p$
- در این حالت، $e''=$ [w - p] را با (w-p) ۱ باقی مانده پر کنید.

Image courtesy of Alexander Meurer (Link)

انواع الگوریتم های ISD پایه

Lee-Brickel (LB88)



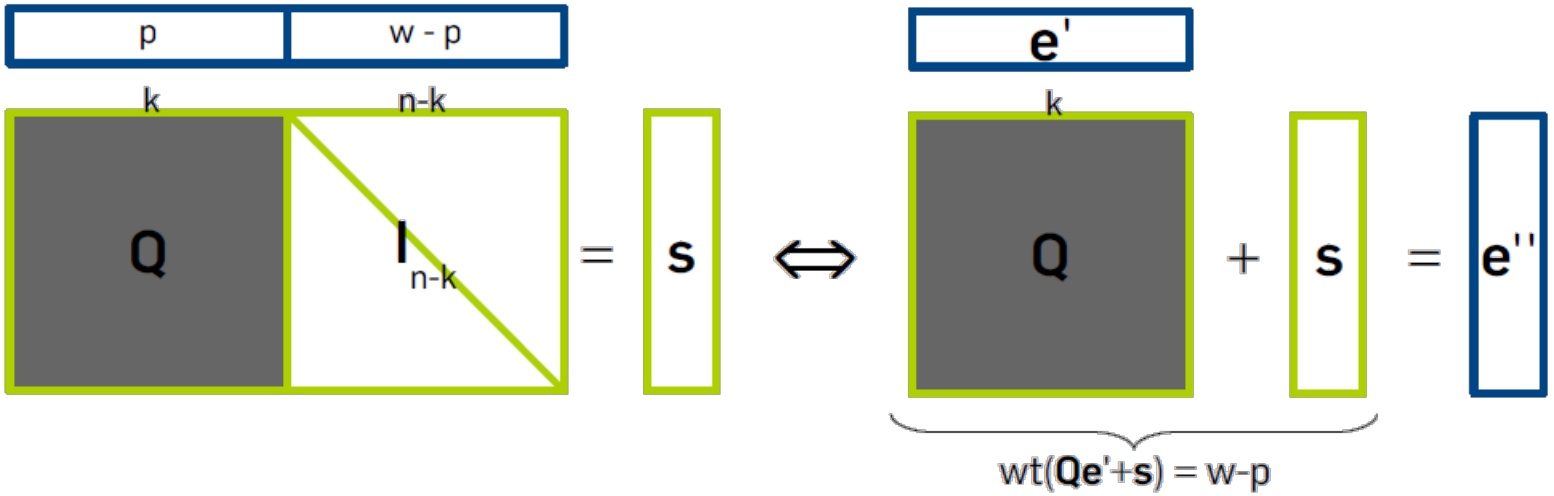
$$T(n,k,d) = Pr[\text{"خوب" تصادفی سازی}]^{-1} \times C[\text{Brute force}]$$

$$= \left(\frac{\binom{k}{p}\binom{n-k}{w-p}}{\binom{n}{w}} \right)^{-1} \times \binom{k}{p}$$

Image courtesy of Alexander Meurer (Link)

انواع الگوریتم های ISD پایه

Lee-Brickel (LB88)



پیچیدگی

$F(k) \leq 0.05751$

Image courtesy of Alexander Meurer (Link)

انواع الگوریتم های ISD پایه

- **Stern (Ste89)**

با استفاده از Birthday Paradox و Man In The Middle

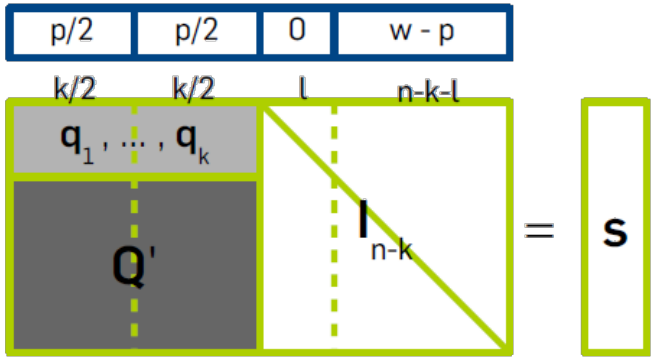
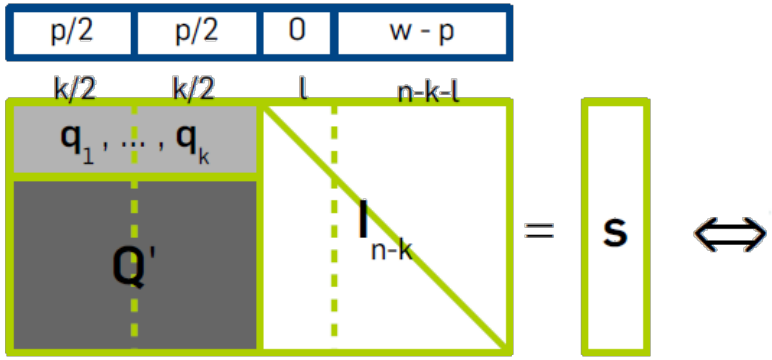
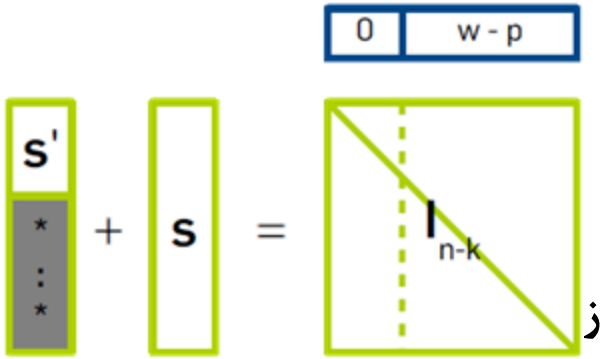


Image courtesy of Alexander Meurer (Link)

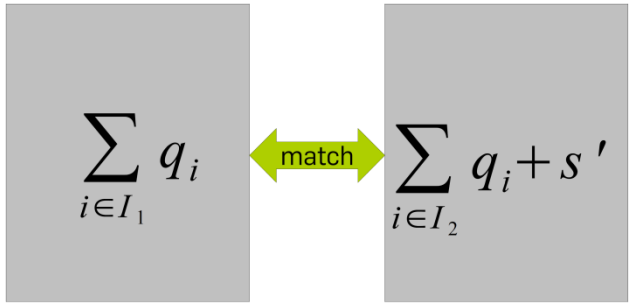
انواع الگوریتم های ISD پایه

- $e'=$ | p/2 | p/2 | را با توجه به $Qe'=s'$ روی l مولفه اول بیابید، یعنی:





- از



$$I_1 \subset [1,\ldots,\frac{k}{2}] \qquad I_2 \subset [\frac{k}{2}+1,\ldots,k]$$

Image courtesy of Alexander Meurer (Link)

انواع الگوریتم های ISD پایه

Stern (Ste89)

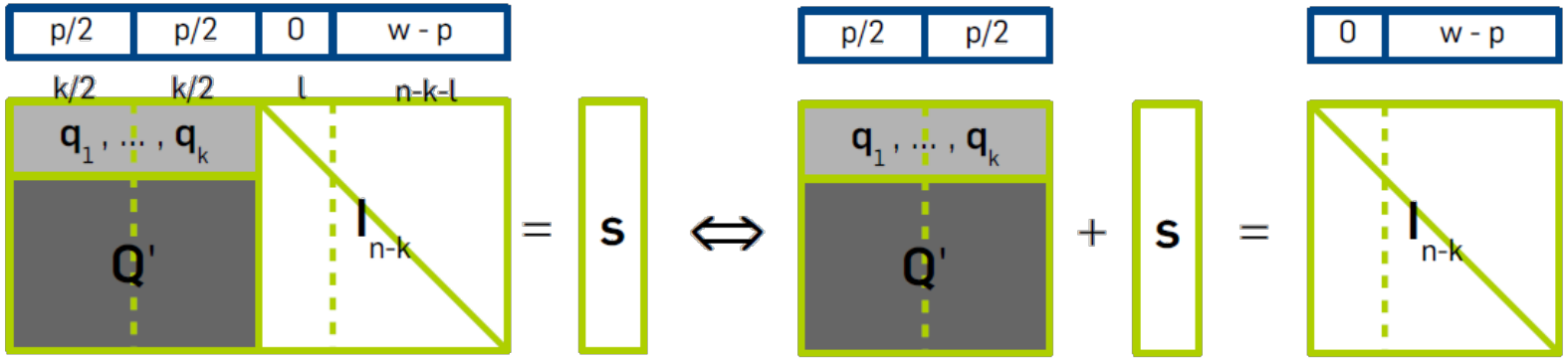


Image courtesy of Alexander Meurer (Link)

انواع الگوریتم های ISD پایه

Stern (Ste89)

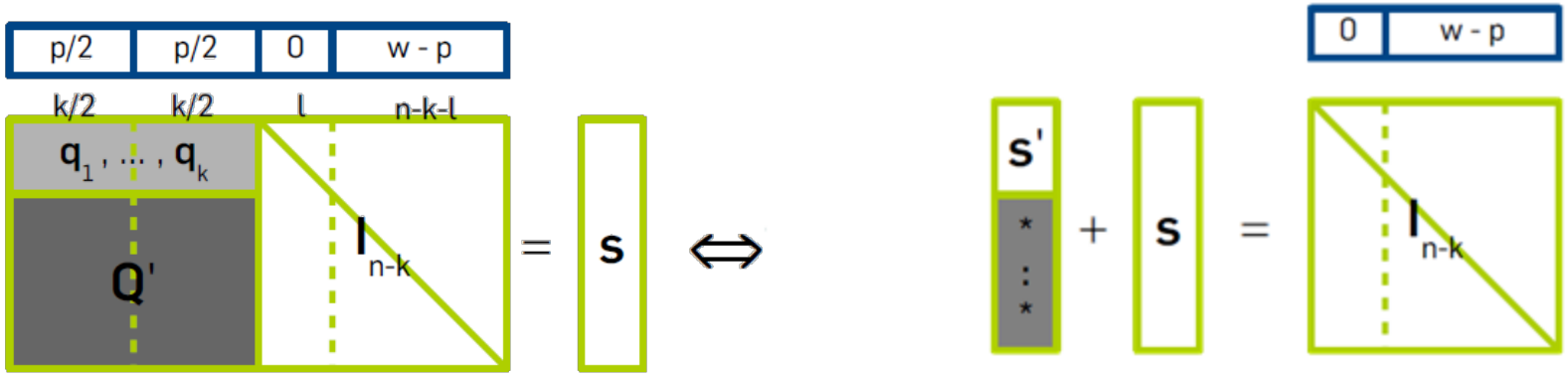


Image courtesy of Alexander Meurer (Link)

انواع الگوریتم های ISD پایه

Stern (Ste89)

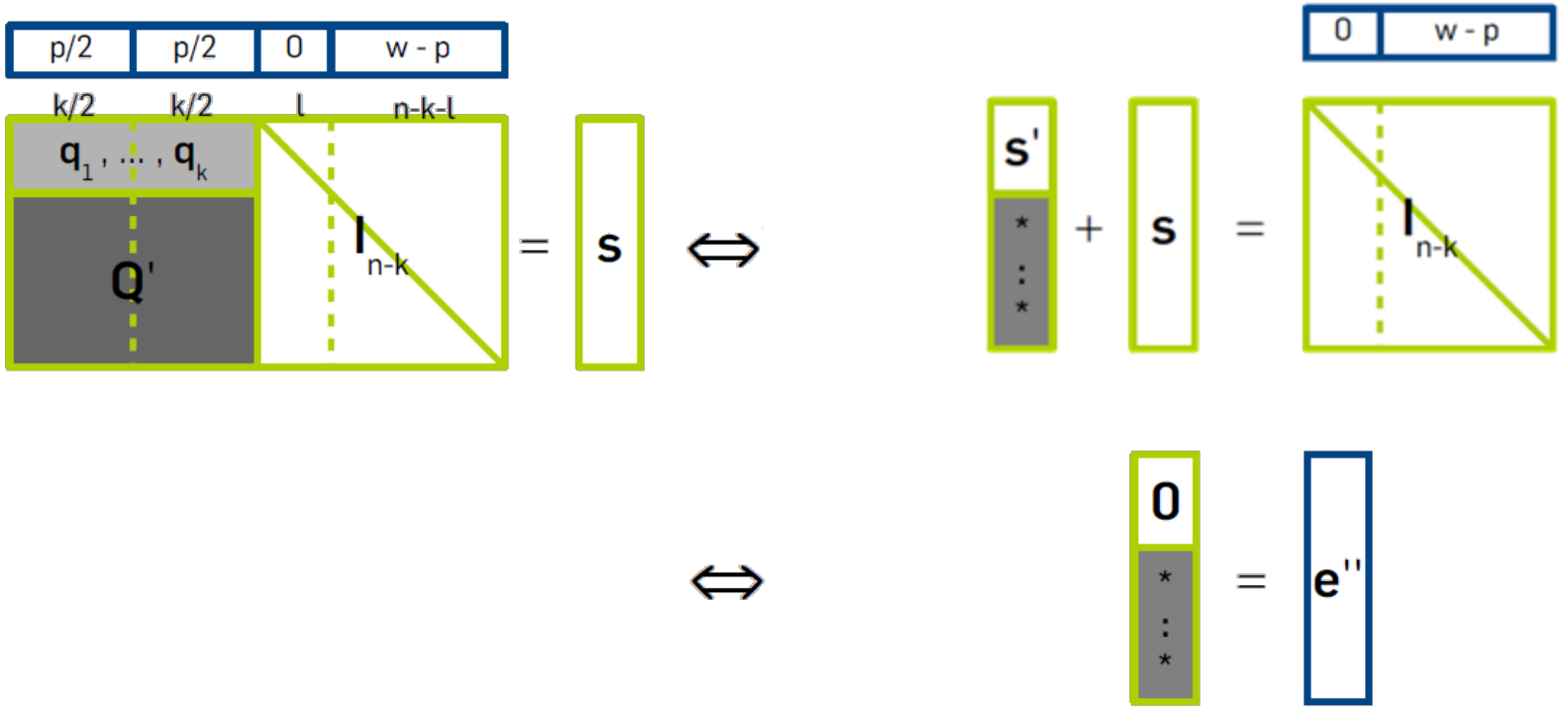
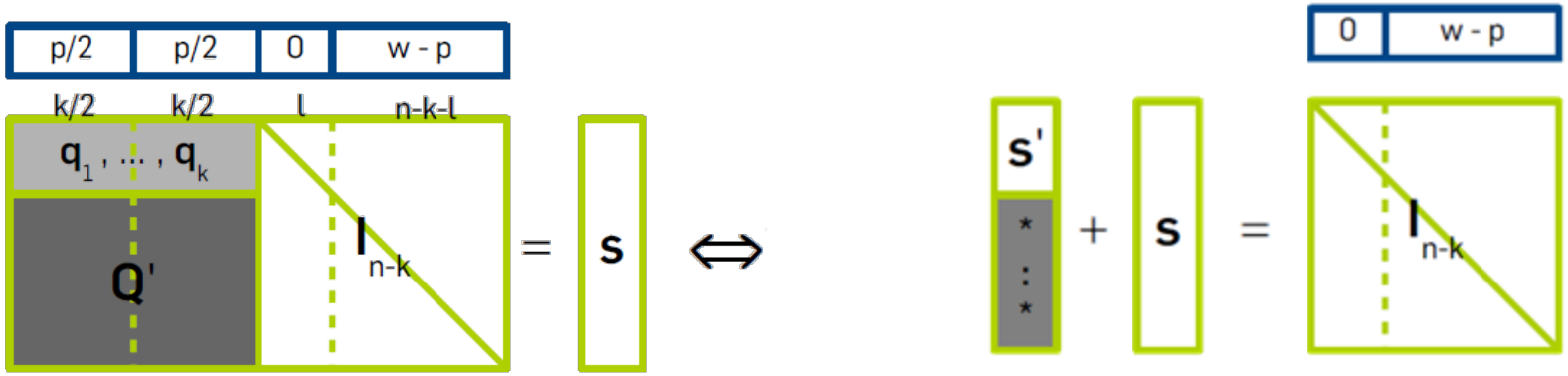


Image courtesy of Alexander Meurer (Link)

انواع الگوریتم های ISD پایه

Stern (Ste89)



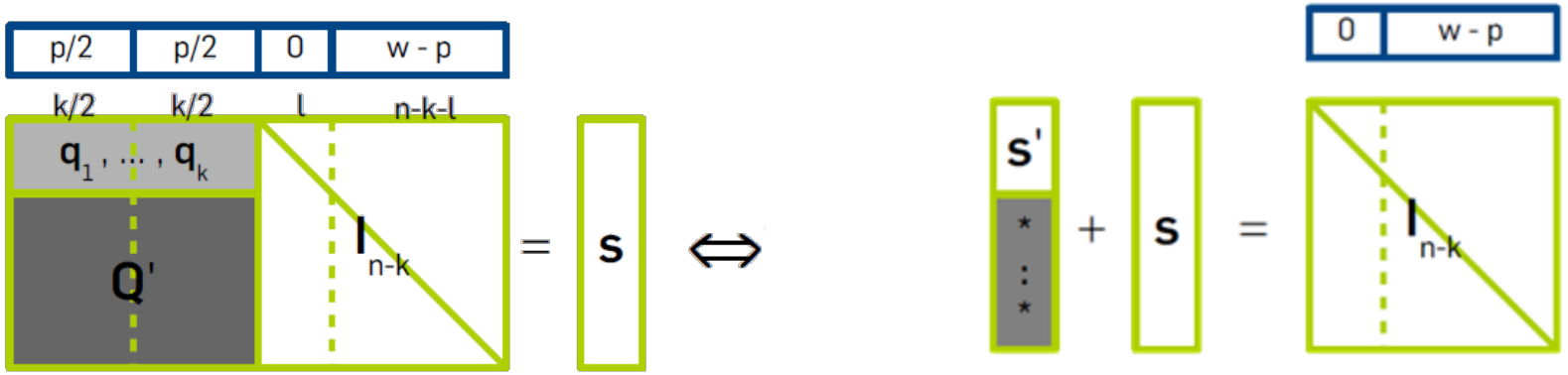
$$T(n,k,d) = \Pr[\text{“خوب” تصادفی سازی}]^{-1} \times C[\text{تصادم}]$$

$$= \left[\frac{\binom{k/2}{p/2}^2 \cdot \binom{n-k-l}{w-p}}{\binom{n}{w}}\right]^{-1} \times \binom{k/2}{p/2}$$

Image courtesy of Alexander Meurer (Link)

انواع الگوریتم های ISD پایه

Stern (Ste89)



پیچیدگی

$$F(k) \leq 0.05563$$

Image courtesy of Alexander Meurer (Link)

انواع الگوریتم های ISD پایه

- **Finiasz و Sendrier** (ASIACRYPT 2009 [FS09])
  - از آنجایی که **l** ستون اول I_{n-k} نمی تواند در الگوریتم **Stern** مورد استفاده قرار گیرد، می توان به راحتی آن ها را به سمت **Q** از **H** شیفت داد.

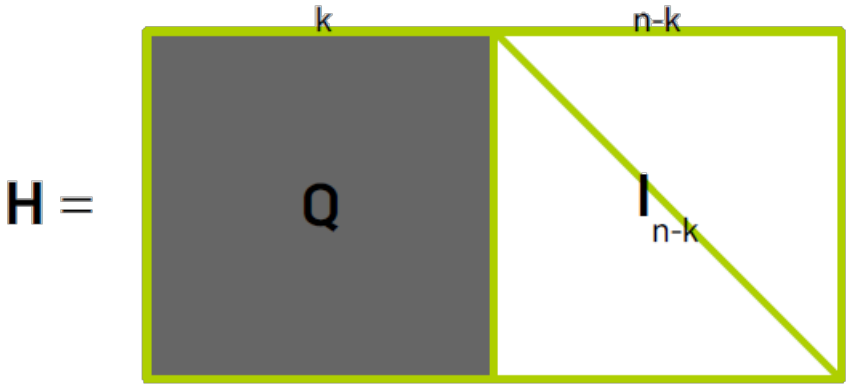


Image courtesy of Alexander Meurer (Link)

انواع الگوریتم های ISD پایه

- **Finiasz و Sendrier** (ASIACRYPT 2009 [FS09])
  - از آنجایی که **l** ستون اول I_{n-k} نمی تواند در الگوریتم **Stern** مورد استفاده قرار گیرد، می توان به راحتی آن ها را به سمت **Q** از **H** شیفت داد.

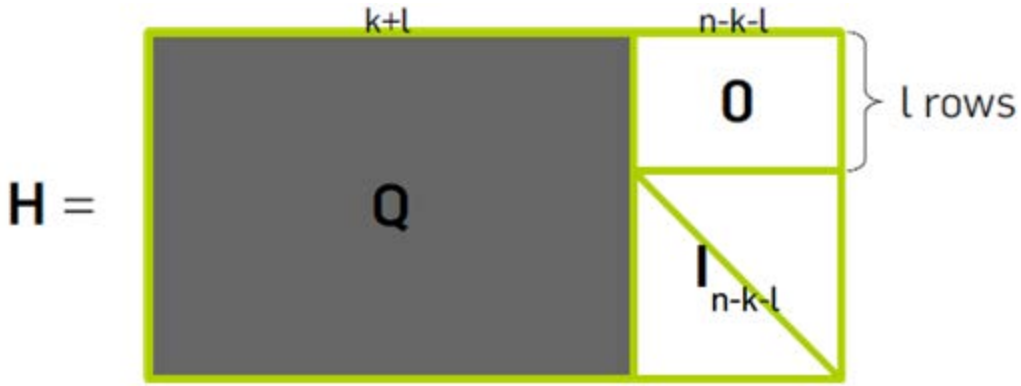


Image courtesy of Alexander Meurer (Link)

انواع الگوریتم های ISD پایه

- **Finiasz و Sendrier** (ASIACRYPT 2009 [FS09])
  - از آنجایی که **l** ستون اول I_{n-k} نمی تواند در الگوریتم **Stern** مورد استفاده قرار گیرد، می توان به راحتی آن ها را به سمت **Q** از **H** شیفت داد.
  - مانند **Stern**

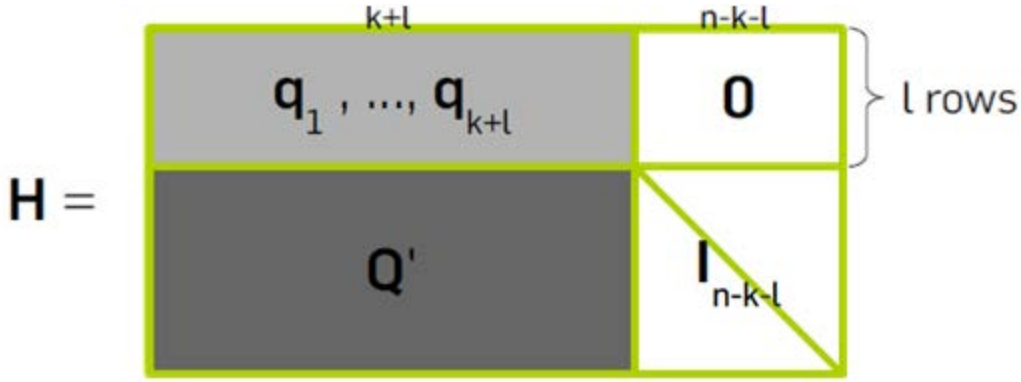


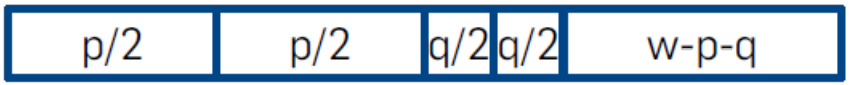
Image courtesy of Alexander Meurer (Link)

مقایسه میان انواع ISD های پایه

- روش های متفاوت جستجو برای توزیع های مختلف خطا
  - Lee-Brickel (1988)

  - Stern (1989)

- کدگشایی Ball-collision توسط Bernstein و همکاران ([BLP11] CRYPTO 2011)
  - بهبود Pr[“خوب” تصادفی سازی] با اجازه دادن به حضور q درایه ۱ دیگر درون پنجره صفر با اندازه l
  - $F(k) \leq 0.05558$



- در هر دو الگوریتم Stern و Ball-Collision، زمان اجرا با هزینه افزایش حافظه بهبود پیدا کرده است.
- ثابت شده است که Ball-collision و روش Finiasz وSendrier در حالت مجانبی، پیچیدگی یکسانی دارند.

Image courtesy of Alexander Meurer (Link)

انواع ISD بهبود یافته (MMT)

- May و همکاران ([MMT11] ASIACRYPT 2011)
- Stern مجموعه ستون های q_i را به دو مجموعه جدا از هم (disjoint) تقسیم کرد یعنی مجموعه های اندیس زیر را جستجو می کرد:

$$I_1 \subset [1,\ldots,\frac{k+l}{2}] \text{ and } I_2 \subset [\frac{k+l}{2}+1,\ldots,k+l] \text{ with } \sum_{i\in I_1} q_i + \sum_{i\in I_2} q_i = s'$$

- ایده جدید: ستون های q_i به دو مجموعه غیرجدا از هم (non-disjoint) تقسیم شوند، یعنی

$$I_1, I_2 \subset [1,\ldots,k+l] \text{ with } |I_j| = \frac{p}{2} \quad \text{and} \quad \sum_{i\in I_1} q_i + \sum_{i\in I_2} q_i = s'$$

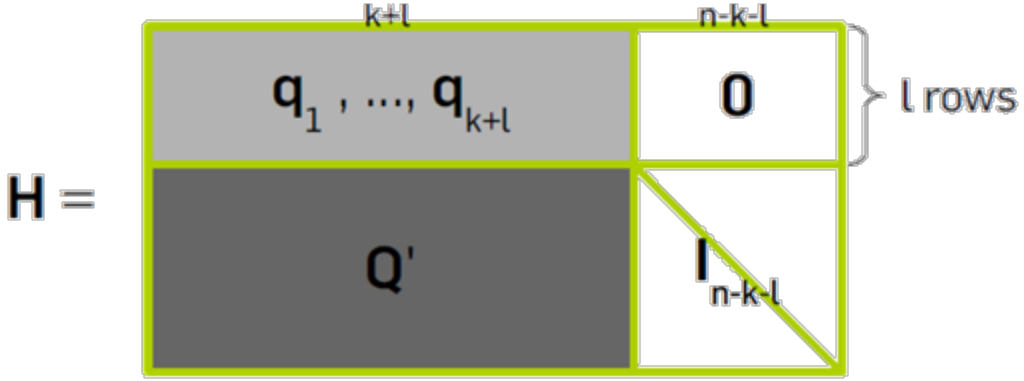
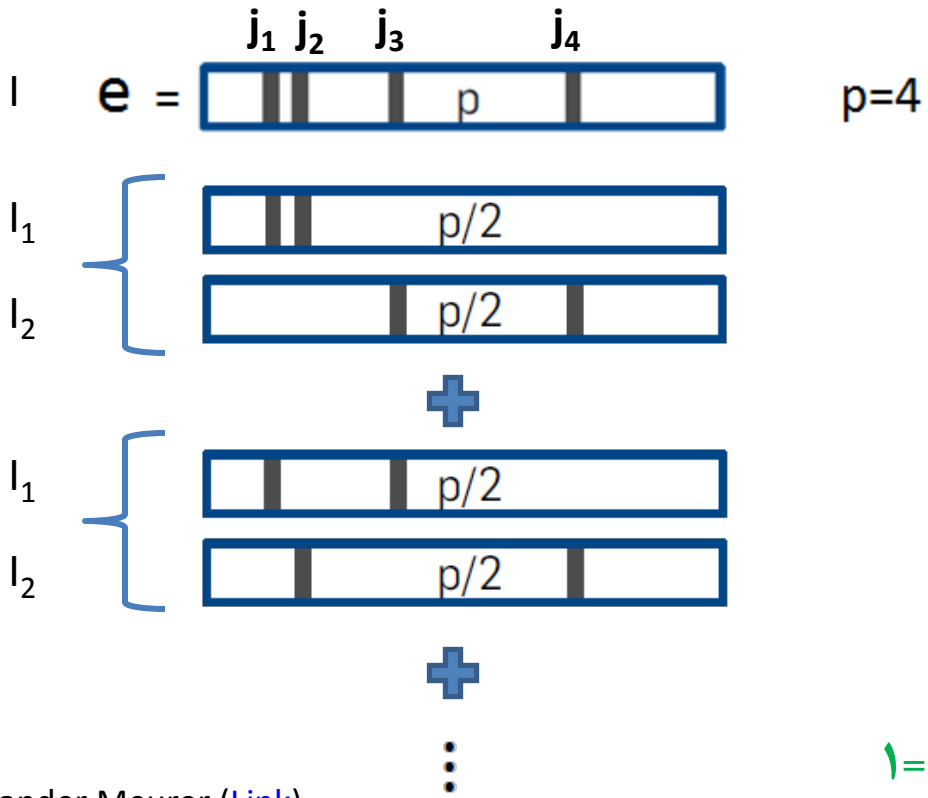


Image courtesy of Alexander Meurer (Link)

انواع ISD بهبود یافته (MMT)

- **ایده جدید:** بخش بندی مجموعه اندیس ها I_2 لاI_1= I با تکنیک نمایش (Representation)
- در این ایده $\binom{p}{p/2}$ حالت مختلف برای تجزیه و بخش بندی (Decomposition) مجموعه اندیس ها I وجود دارد.

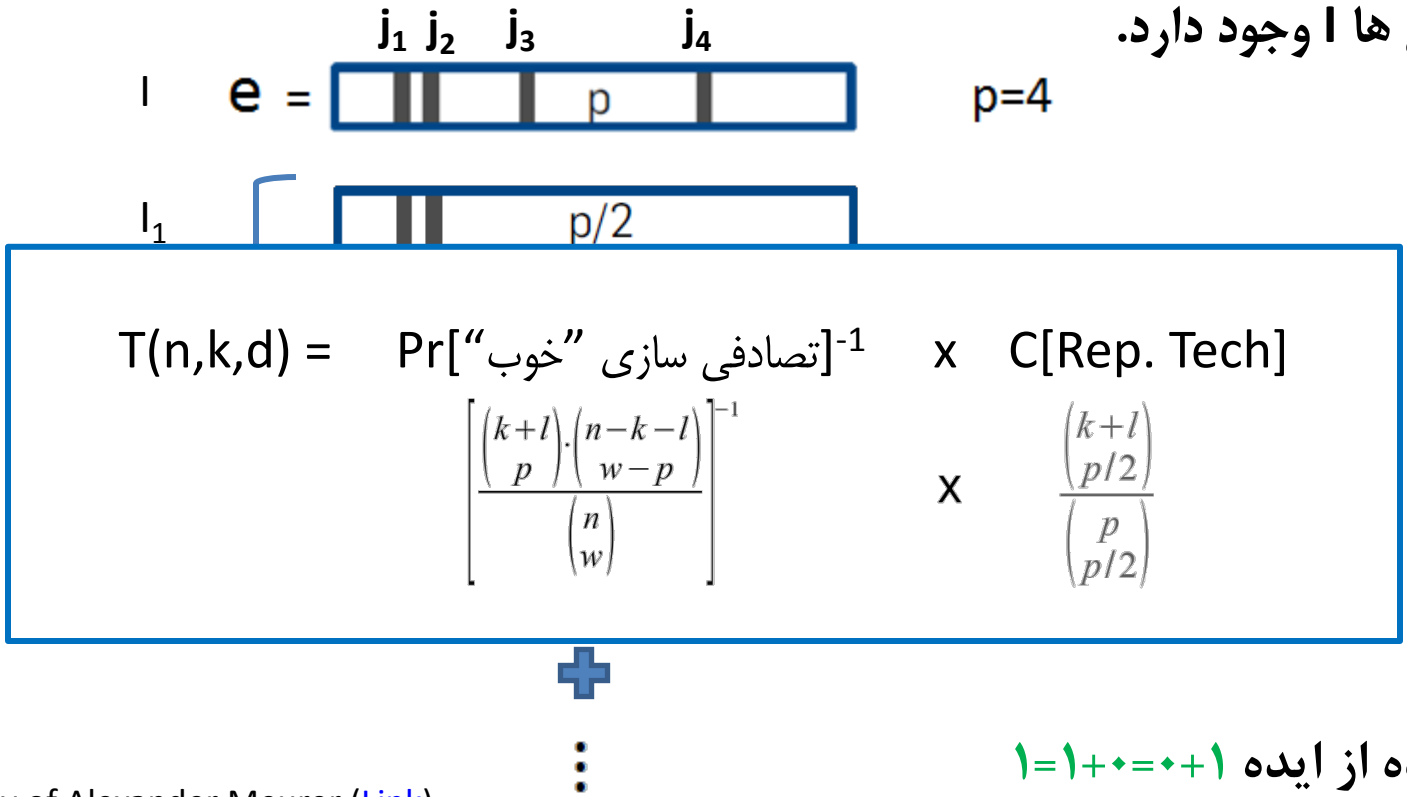


- استفاده از ایده ۱+۰=۰+۱=۱

Image courtesy of Alexander Meurer (Link)

انواع ISD بهبود یافته (MMT)

- **ایده جدید:** بخش بندی مجموعه اندیس ها I_2 لاI_1= I با تکنیک نمایش (Representation)
- در این ایده $\binom{p}{p/2}$ حالت مختلف برای تجزیه و بخش بندی (Decomposition) مجموعه اندیس ها I وجود دارد.

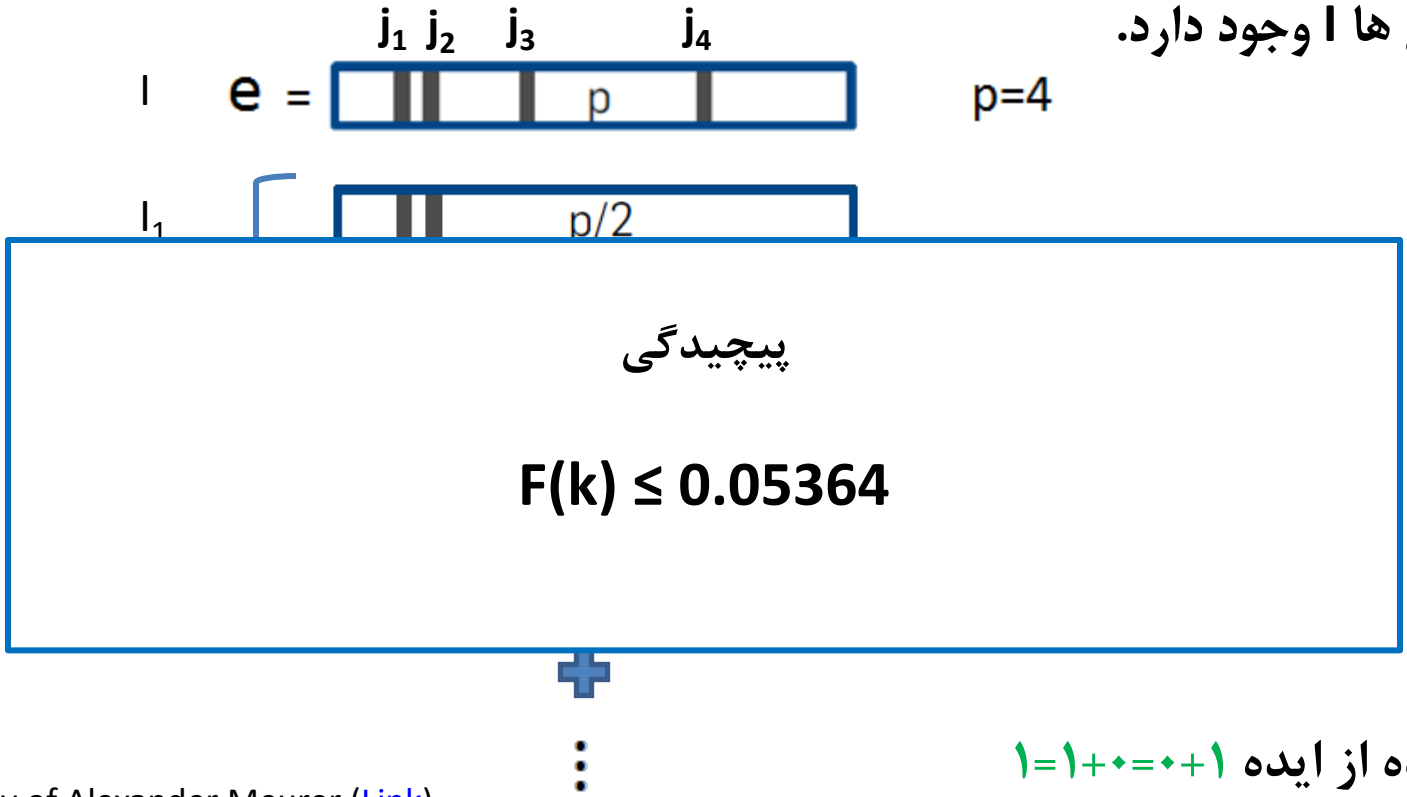


- استفاده از ایده ۱+۰=۰+۱=۱

Image courtesy of Alexander Meurer (Link)

انواع ISD بهبود یافته (MMT)

- **ایده جدید:** بخش بندی مجموعه اندیس ها I_2 لاI_1= I با تکنیک نمایش (Representation)
- در این ایده $\binom{p}{p/2}$ حالت مختلف برای تجزیه و بخش بندی (Decomposition) مجموعه اندیس ها I وجود دارد.



- استفاده از ایده ۱+۰=۰+۱=۱

Image courtesy of Alexander Meurer (Link)

انواع ISD بهبود یافته (BJMM)

- Becker و همکاران ([BJMM12] EUROCRYPT 2012)
- **ایده جدید:** تقسیم ستون های q_i به دو مجموعه دارای اشتراک (intersecting sets) و استفاده از ایده ۱+۱=۰
- مجموعه تفاضل متقارن (Symmetric difference) با پارامتر ε

$$I = I_1 \Delta I_2 := (I_1 \cup I_2) \setminus (I_1 \cap I_2) \qquad |I_1 \cap I_2| = \varepsilon$$

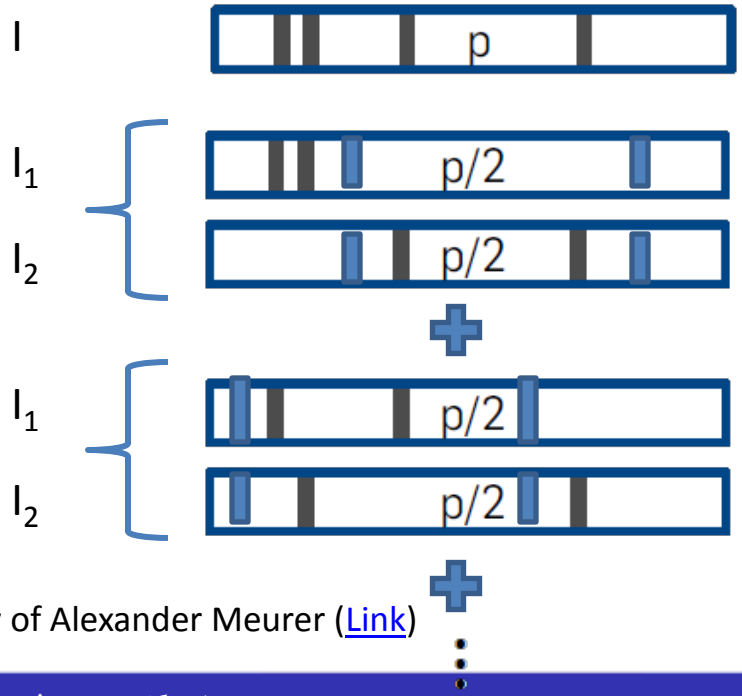


Image courtesy of Alexander Meurer (Link)

در این حالت $\binom{p}{p/2}\binom{k+l-p}{\varepsilon}$ راه برای تجزیه و بخش بندی مجموعه اندیس ها وجود دارد.

انواع ISD بهبود یافته (BJMM)

- Becker و همکاران ([BJMM12] EUROCRYPT 2012)
- **ایده جدید:** تقسیم ستون های q_i به دو مجموعه دارای اشتراک (intersecting sets) و استفاده از ایده ۱+۱=۰
- مجموعه تفاضل متقارن (Symmetric difference) با پارامتر ε

$$I = I_1 \Delta I_2 := (I_1 \cup I_2) \setminus (I_1 \cap I_2) \qquad |I_1 \cap I_2| = \varepsilon$$

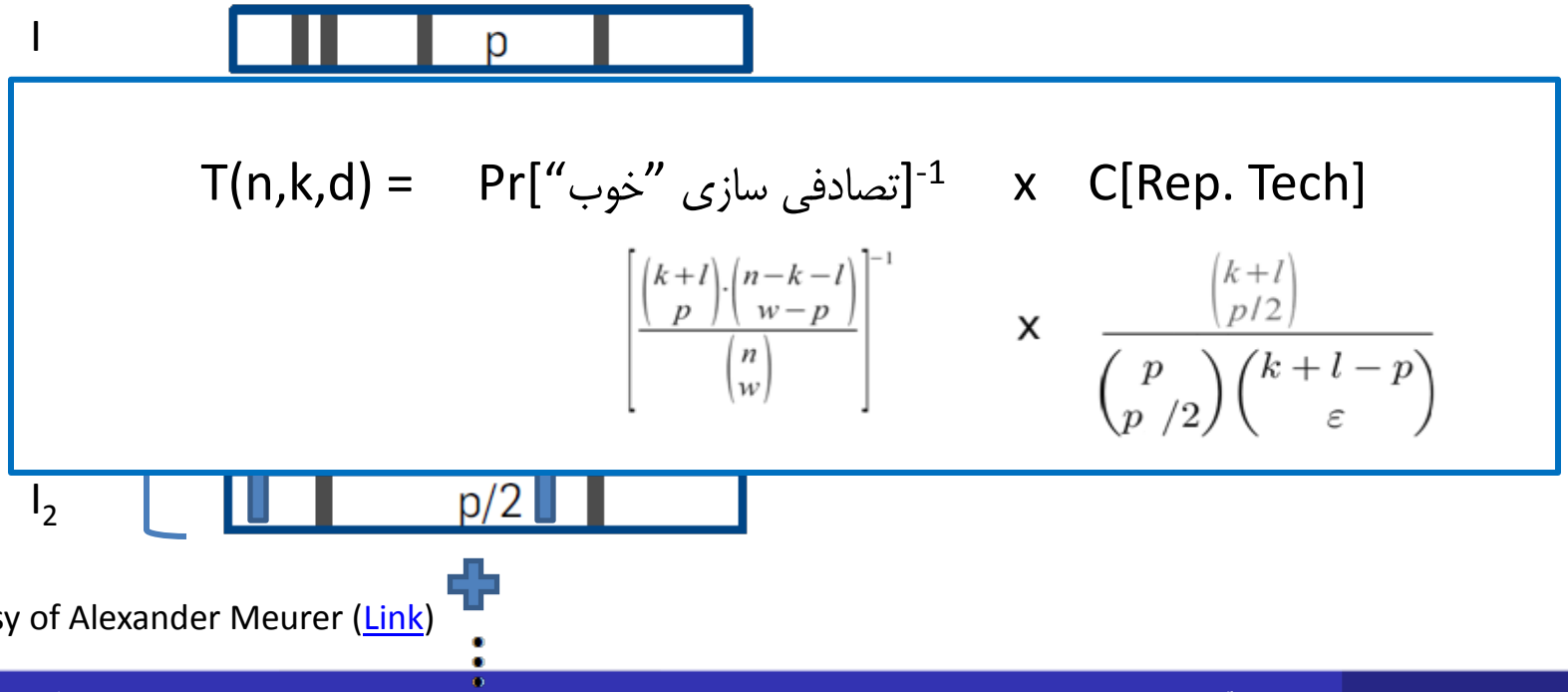


Image courtesy of Alexander Meurer (Link)

انواع ISD بهبود یافته (BJMM)

- Becker و همکاران ([BJMM12] EUROCRYPT 2012)
- **ایده جدید:** تقسیم ستون های q_i به دو مجموعه دارای اشتراک (intersecting sets) و استفاده از ایده ۰=۱+۱
- مجموعه تفاضل متقارن (Symmetric difference) با پارامتر ε

$$I = I_1 \Delta I_2 := (I_1 \cup I_2) \setminus (I_1 \cap I_2) \qquad |I_1 \cap I_2| = \varepsilon$$

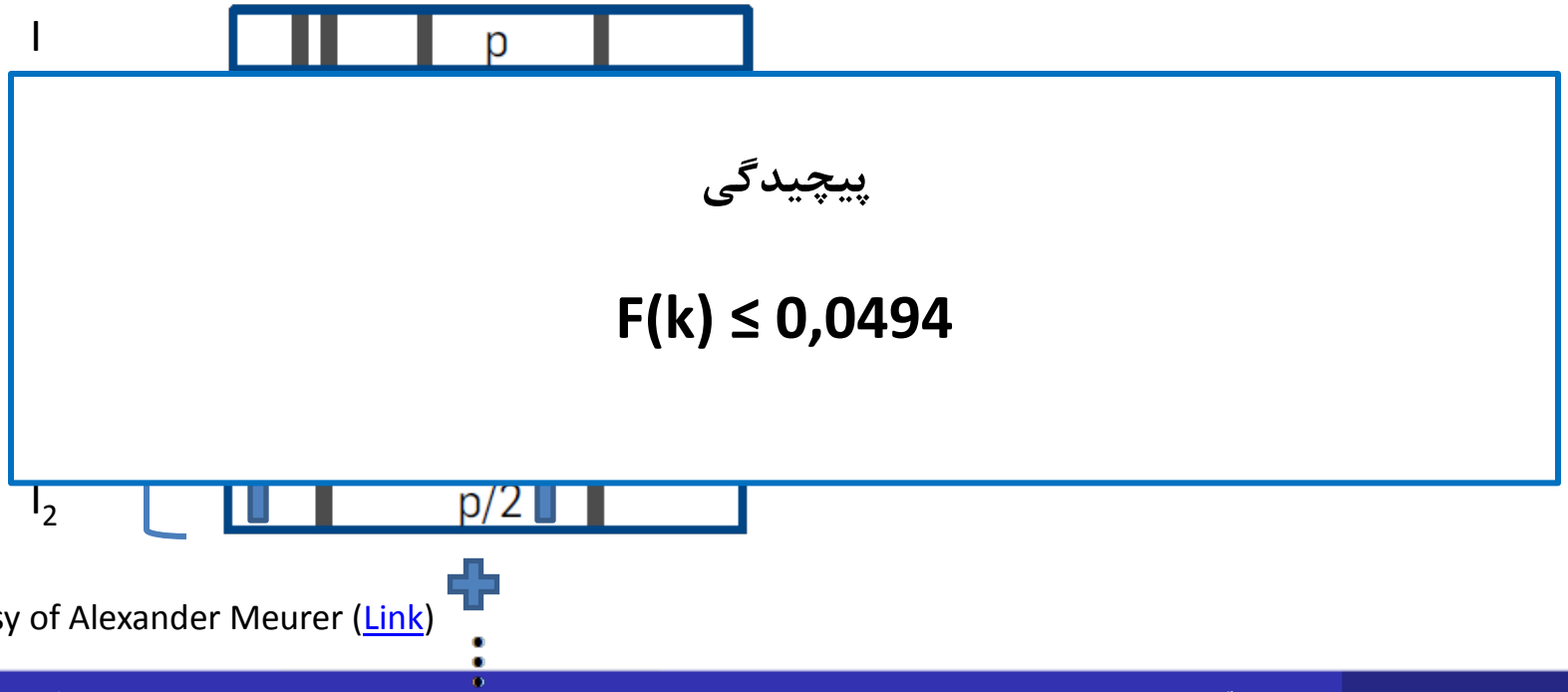


Image courtesy of Alexander Meurer (Link)

انواع ISD بهبود یافته (MO)

- May و Ozerov (EUROCRYPT 2015 [MO15])
- **ایده جدید:** به جای اینکه مانند الگوریتم Stern دقیقا به دنبال تصادم بگردیم به دنبال جفت هایی بگردیم که تقریبا با هم تصادم دارند.
- استفاده از مسئله نزدیک ترین همسایه (Nearest Neighbor) برای یافتن تصادم

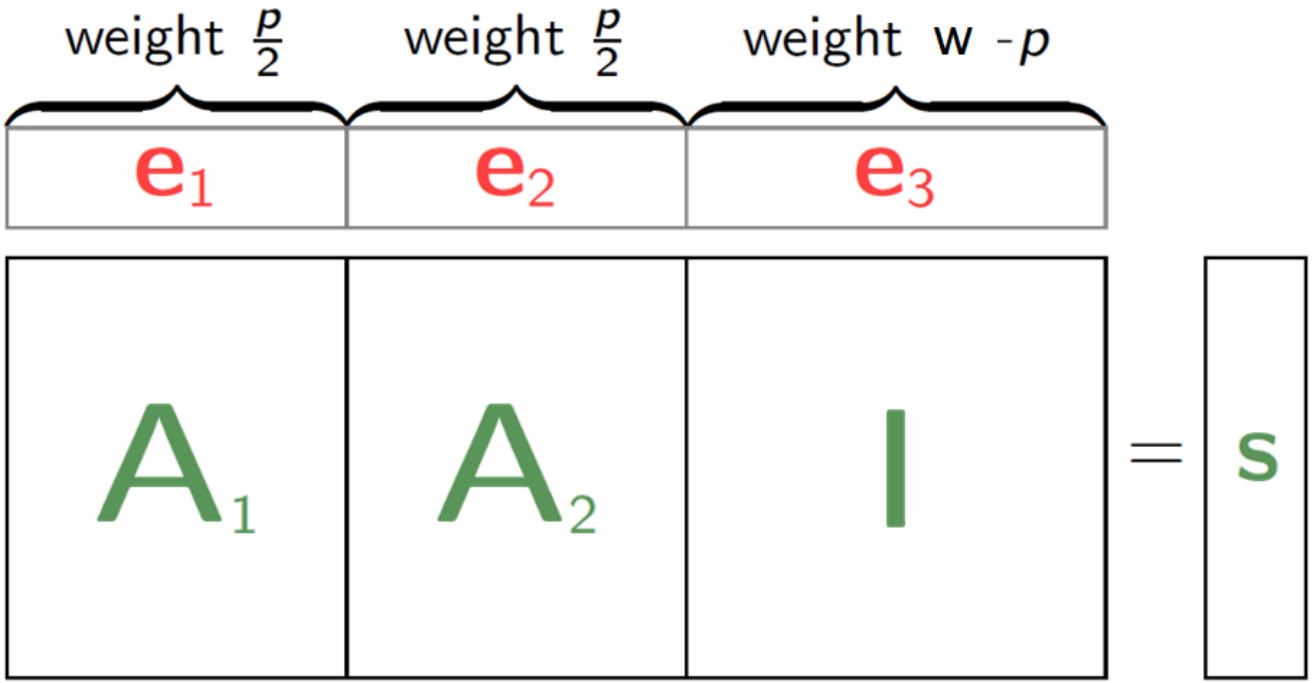


Image courtesy of Alexander May and Ilya Ozerov (Link)

انواع ISD بهبود یافته (MO)

- May و Ozerov (EUROCRYPT 2015 [MO15])
- **ایده جدید:** به جای اینکه مانند الگوریتم Stern دقیقا به دنبال تصادم بگردیم به دنبال جفت هایی بگردیم که تقریبا با هم تصادم دارند.
- استفاده از مسئله نزدیک ترین همسایه (Nearest Neighbor) برای یافتن تصادم

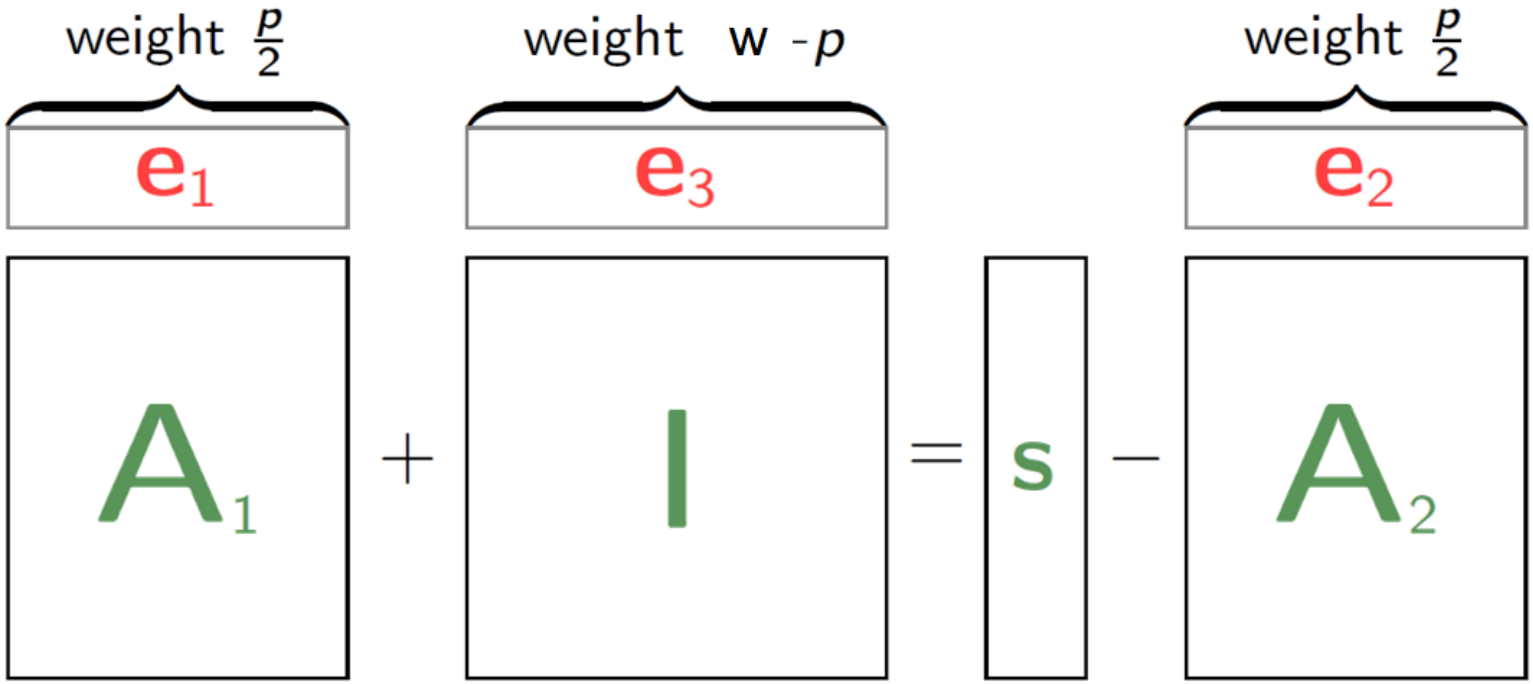


Image courtesy of Alexander May and Ilya Ozerov (Link)

انواع ISD بهبود یافته (MO)

- May و Ozerov (EUROCRYPT 2015 [MO15])
- **ایده جدید:** به جای اینکه مانند الگوریتم Stern دقیقا به دنبال تصادم بگردیم به دنبال جفت هایی بگردیم که تقریبا با هم تصادم دارند.
- استفاده از مسئله نزدیک ترین همسایه (Nearest Neighbor) برای یافتن تصادم

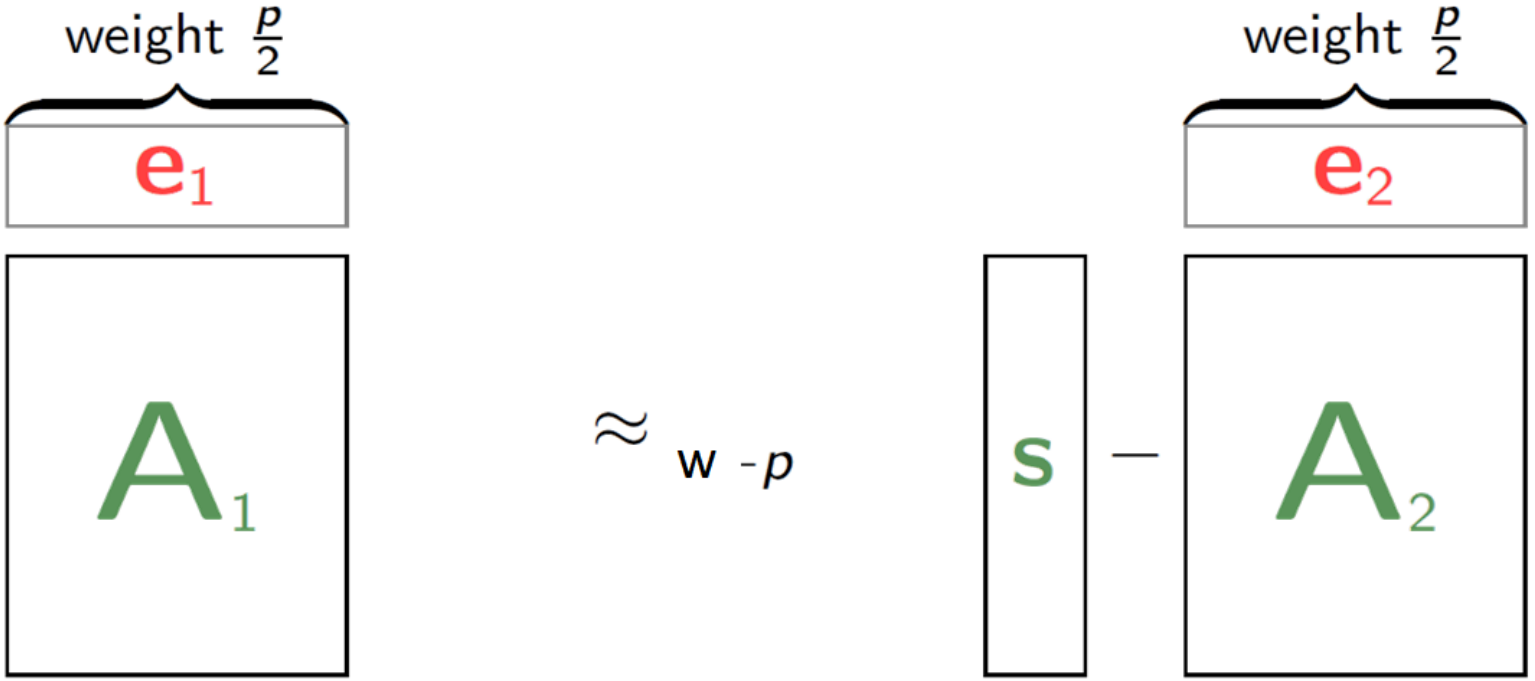


Image courtesy of Alexander May and Ilya Ozerov (Link)

انواع ISD بهبود یافته (MO)

- حل مسئله نزدیک ترین همسایه برای یافتن تصادم با $\Delta = w\text{-}p$

$$A_1 \cdot e_1 \approx s - A_2 \cdot e_2$$

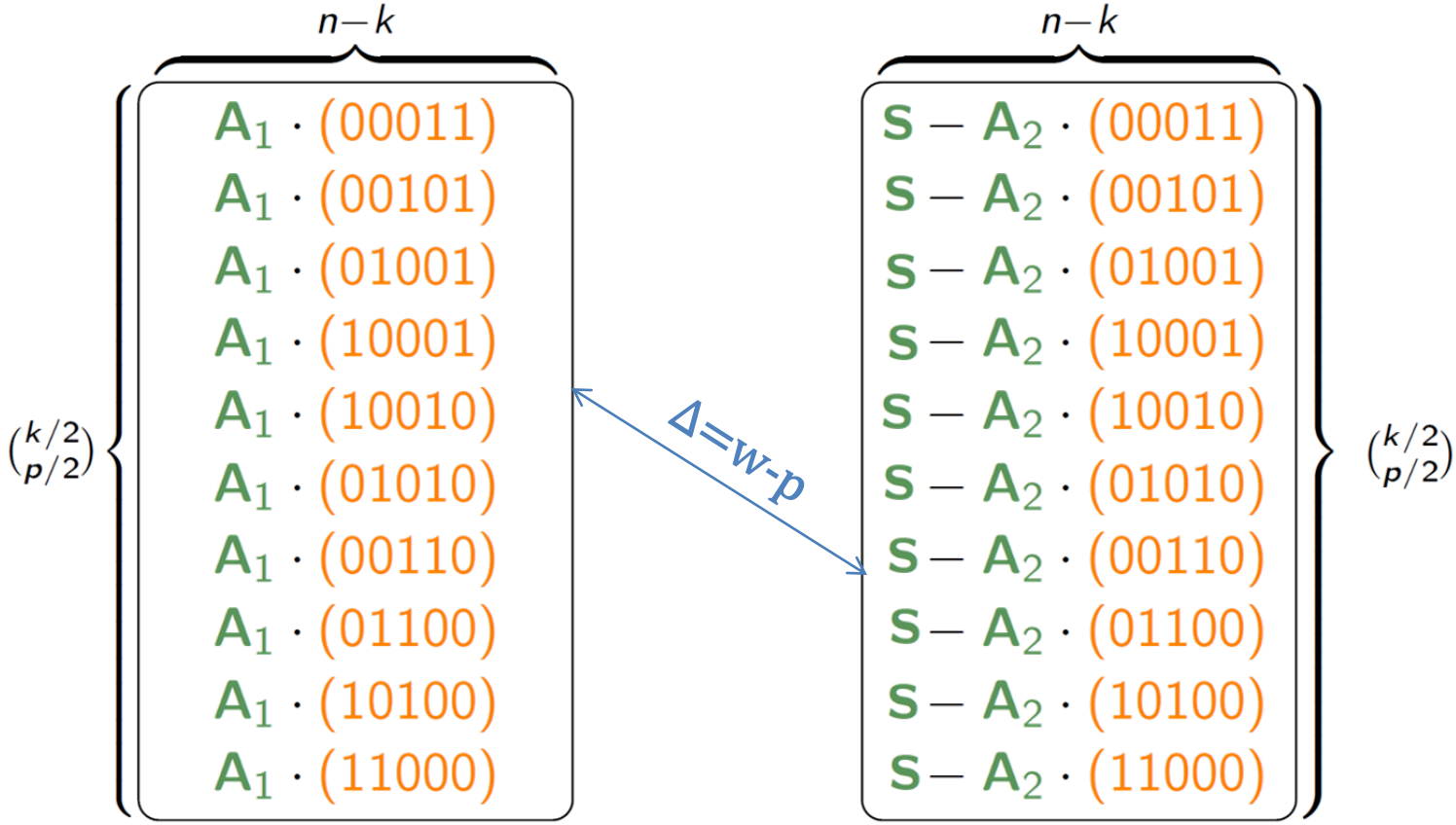
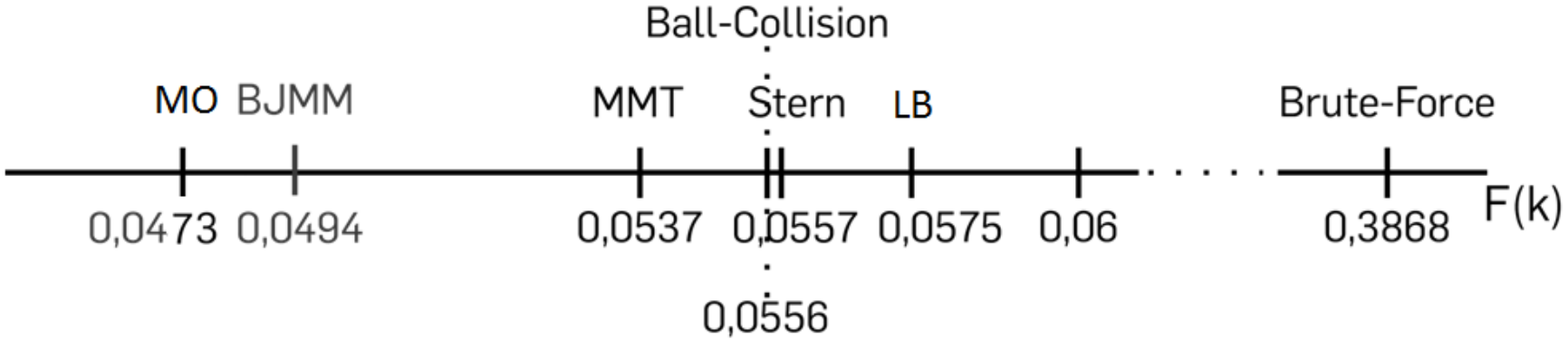


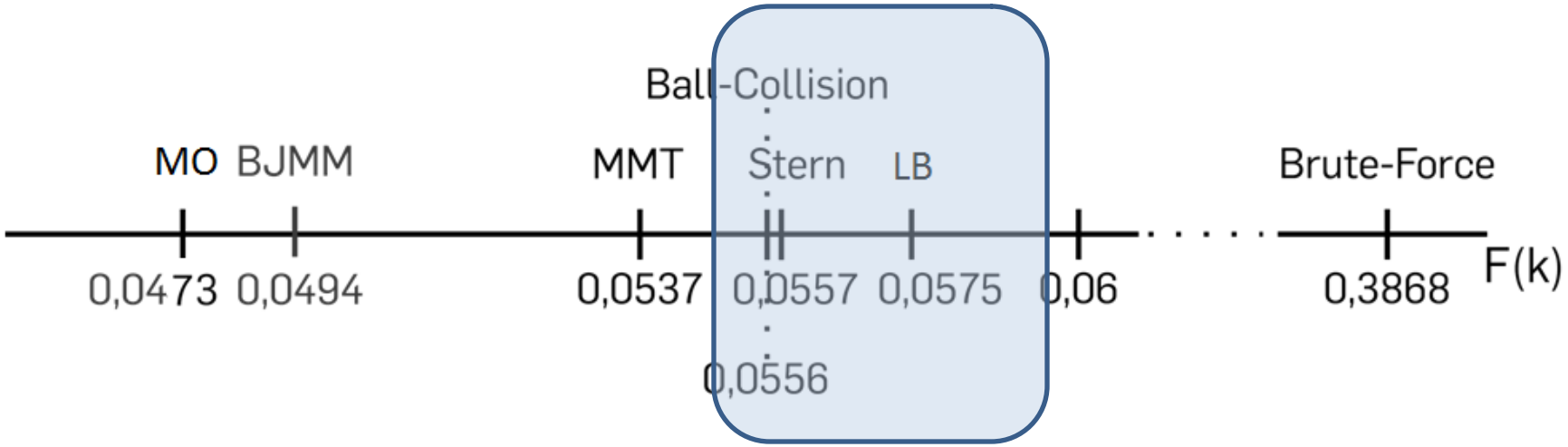
Image courtesy of Alexander May and Ilya Ozerov (Link)

مقایسه پیچیدگی ها در حالت مجانبی



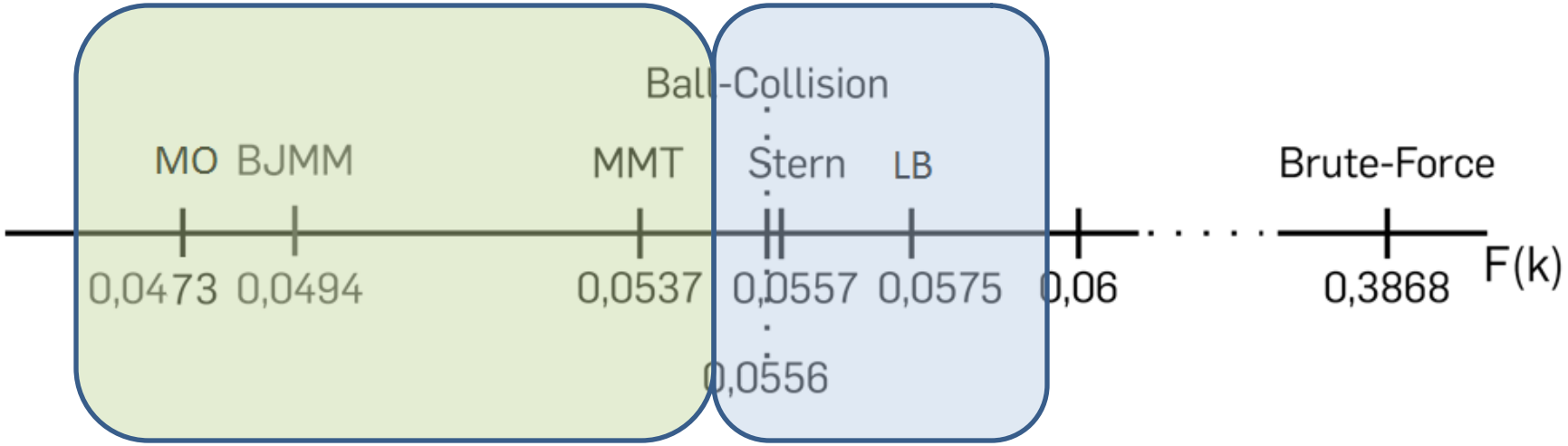
مقایسه پیچیدگی ها در حالت مجانبی

ISD های پایه



مقایسه پیچیدگی ها در حالت مجانبی

ISD های پایه **ISD های بهبودیافته**



مقایسه پیچیدگی عملیاتی حمله برای سامانه اولیه رمز کلید عمومی McEliece

McEliece (1024,524,50)

Algorithm	Year	Complexity
Lee-Brickel	1988	$2^{73.4}$
Canteaut-Sendrier	1998	$2^{64.2}$
Bernstein et al.	2008	$2^{60.55}$
Finiasz-Sendrier	2009	$2^{59.9}$
Bernstein et al. (Ballcoll)	2010	-
May et al. (MMT)	2011	-
Becker et al. (BJMM)	2012	-
May-Ozerov (MO)	2015	-

جمع بندی

- مرور کلی روی انواع حملات
  - حمله های کانال جانبی و روش های مقابله با آن ها بسیار جدید هستند.
- بسیاری از حمله ها ترکیبی هستند.
  - حمله ساختاری+ حمله ISD (حمله کد دوگان و OTD)
- حمله های ISD
  - بهینه سازی (در عملیات معکوس کردن و ضرب ماتریسی)
  - مجانبی

مراجع

[STMOS08] Strenzke, F., Tews, E., Molter, H.G., Overbeck, R., Shoufan, A.: Side channels in the McEliece PKC. In: Proceedings of International Workshop on Post-Quantum Cryptography, PQCrypto 2008, pp. 30–46 (2008)

[SSMS09] Shoufan, A., Strenzke, F., Molter, H.G., Stoettinger, M.: A timing attack against Patterson Algorithm in the McEliece PKC. In: Proceedings of the 12th International Conference on Information Security and Cryptology (ICISC'09), Lecture Notes in Computer Science (2009)

[MSSS11] H. G. Molter, M. Stöttinger, A. Shoufan · F. Strenzke, : A simple power analysis attack on a McEliece cryptoprocessor. In Journal of Cryptography Engineering. DOI 10.1007/s13389-011-0001-3

[HMP10] Heyse, S., Moradi, A., Paar, C.: Practical power analysis attacks on software implementations of McEliece. In: Post-Quantum Cryptography, pp. 108–125 (2010). doi:10.1007/978-3-642-12929-2_9

[CEMS15] C. Chen, T. Eisenbarth, I. Maurich, R. Steinwandt,: Differential Power Analysis of a McEliece Cryptosystem, accepted to publish in 13th International Conference on Applied Cryptography and Network Security proceeding, 2–5 June 2015, New York.

مراجع

[LB88] P.J. Lee and E.F. Brickell. An observation on the security of McEliece's public-key cryptosystem. In Christoph G. G¨unther, editor, EUROCRYPT '88, volume 330 of Lecture Notes in Computer Science, pages 275–280. Springer-Verlag Berlin Heidelberg, 1988.

[Ste89] J. Stern. A method for finding codewords of small weight. In G´erard D. Cohen and Jacques Wolfmann, editors, Coding theory and applications, volume 388 of Lecture Notes in Computer Science, pages 106–113. Springer-Verlag Berlin Heidelberg New York, 1989. ISBN 0387516433.

[FS09] M. Finiasz and N. Sendrier. Security bounds for the design of code-based cryptosystems. In Mitsuru Matsui, editor, ASIACRYPT 2009, volume 5912, pages 88–105. Springer-Verlag Berlin Heidelberg, 2009.

[MMT11] A. May, A. Meurer and E. Thomae, "Decoding Random Linear Codes in O(20.054n)", Advances in Cryptology - ASIACRYPT 2011, 2011.

[BJMM12] A. Becker, A. Joux, A. May and A. Meurer, "Decoding Random Binary Linear Codes in 2n/20: How 1 + 1 = 0 Improves Information Set Decoding.", Advances in Cryptology - EUROCRYPT 2012, 2012.

مراجع

[MO15] A. May, I. Ozerov, "On Computing Nearest Neighbors with Applications to Decoding of Binary Linear Codes" , In Advances in Cryptology (Eurocrypt 2015), Lecture Notes in Computer Science, Springer-Verlag, 2015.

[Pra62] E. Prange. The use of information sets in decoding cyclic codes. IRE Transactions on Information Theory, 8(5):5–9, September 1962.

[Ber10] D. Bernstein. Grover vs. mceliece. In N. Sendrier, editor, PQCrypto, volume 6061 of LNCS, pages 73–80. Springer, 2010.

[DMR11] H. Dinh, C. Moore and A. Russell, “Mceliece and niederreiter cryptosystems that resist quantum fourier sampling attacks,” In Proceedings of the 31st annual conference on Advances in Cryptology (CRYPTO 11), pp. 761–779, Springer-Verlag, Berlin, Heidelberg (2011)


باتشکر از توجه شما