دانشگاه صنعتی شریف

بسم الله الرحمن الرحیم

قطب علمی رمز

سامانه های رمز کلید مخفی مبتنی بر کدهای LDPC

رضا هوشمند

دانشکده مهندسی برق، دانشگاه آزاد اسلامی واحد علوم و تحقیقات

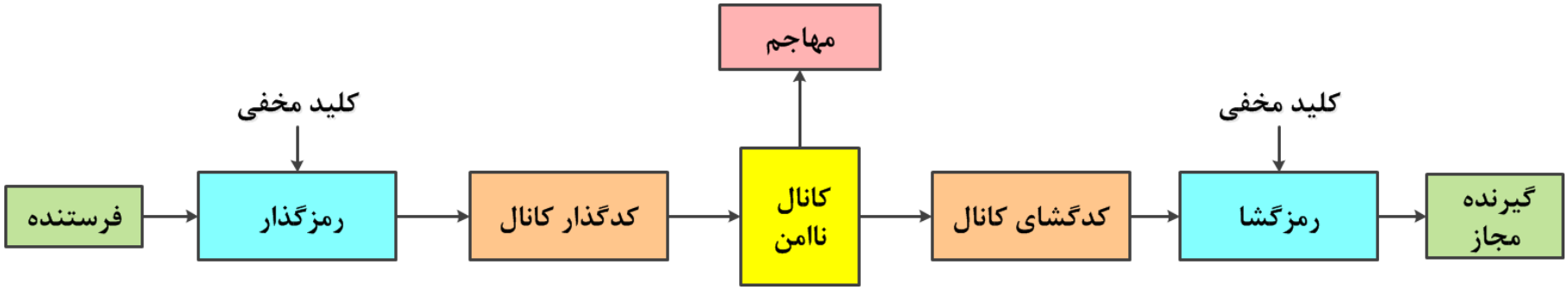
r.hooshmand@srbiau.ac.ir

فهرست مطالب

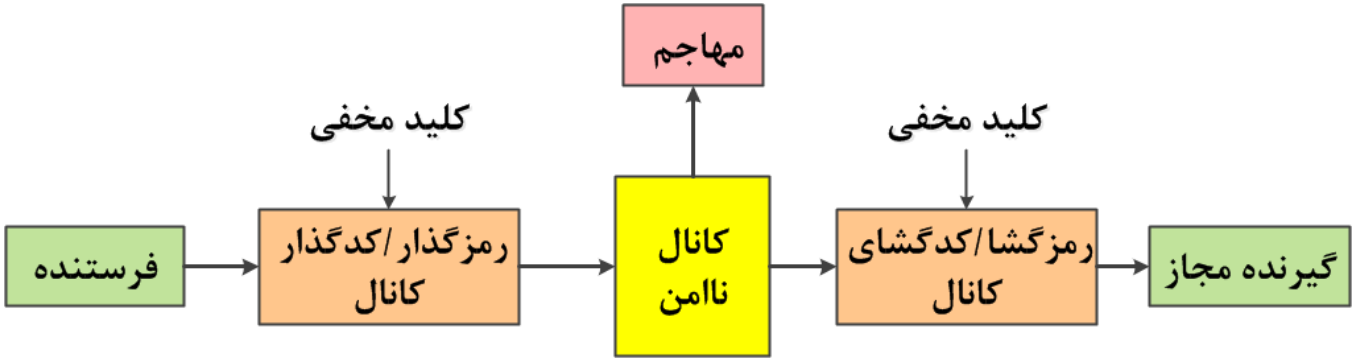
- مقدمه ای بر سامانه های رمز کلید مخفی مبتنی بر مسائل سخت کدینگ
- سامانه های رمز کلید مخفی مبتنی بر کدهای LDPC
  - سامانه توأم رمزگذاری کلید مخفی – کدگذاری کانال مبتنی بر کدهای EG-QC-LDPC
  - سامانه توأم رمزگذاری کلید مخفی – کدگذاری کانال مبتنی بر کدهای EDF-QC-LDPC

مقدمه

مقدمه



نمودار گردشی سامانه های مخابراتی متداول



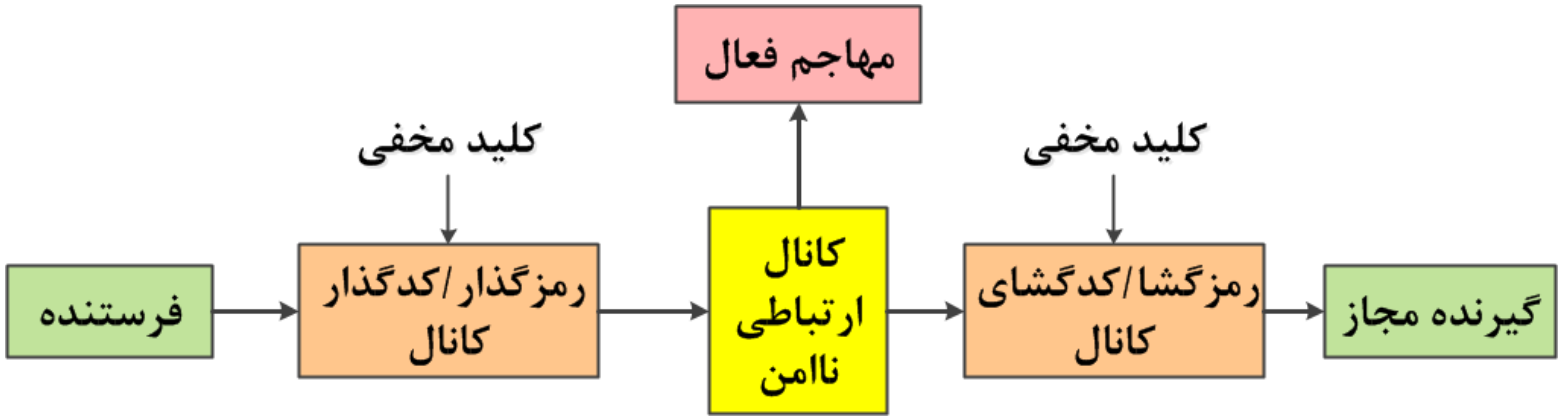
نمودار گردشی سامانه های رمز کلید مخفی مبتنی بر مسائل سخت کدینگ

مقدمه

- **مزایای سامانه های رمز کلید مخفی مبتنی بر مسائل سخت کدینگ:**
  - کاهش پیچیدگی محاسباتی و افزایش سرعت
  - افزایش بازدهی مصرف انرژی
  - مقاوم در برابر حملات رایانه های کوانتومی
  - مناسب جهت انتقال اطلاعات با حجم زیاد
- **لازمه رسیدن به این اهداف:**
  - طراحی مناسب الگوریتم های رمزگذاری/کدگذاری و رمزگشایی/کدگشایی
  - استفاده از کدهای مناسب

مقدمه

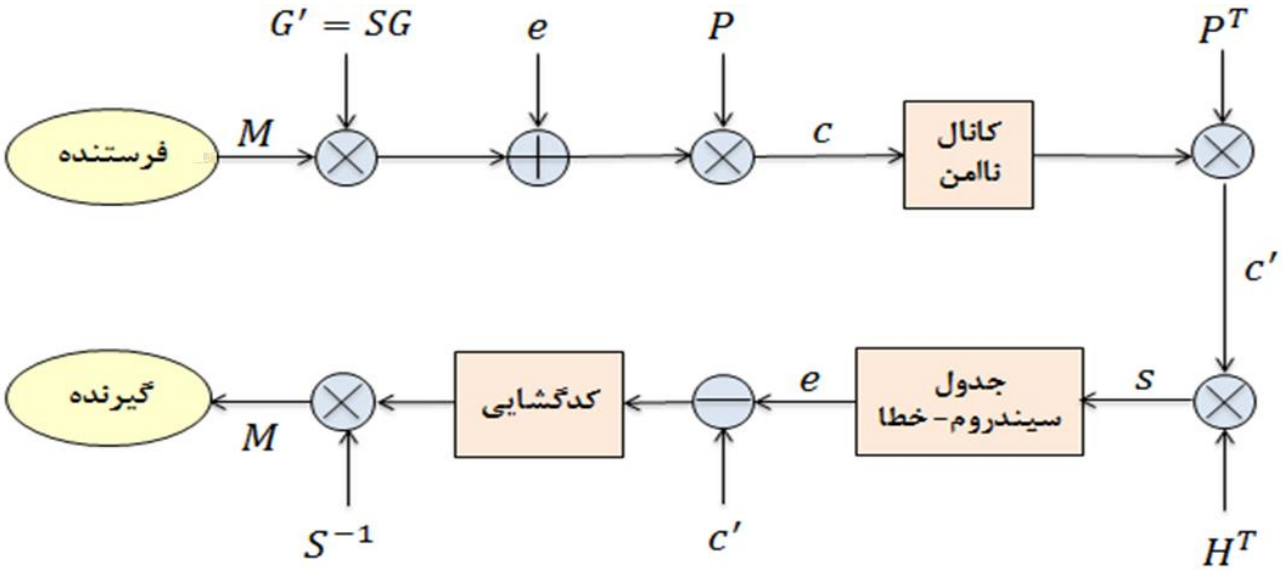
- **انواع سامانه های رمز کلید مخفی مبتنی بر مسائل سخت کدینگ:**
  - **سامانه های رمزگذاری کلید مخفی مبتنی بر کد**
  - **سامانه های توأم رمزگذاری کلید مخفی-کدگذاری کانال**



نمودار گردشی سامانه های رمزگذاری کلید مخفی مبتنی بر کد

سامانه رمز کلید مخفی Rao-Nam

- [RaoNam'89]



نمودار گردشی سامانه رمز کلید مخفی Rao-Nam

- کلید مخفی:
  - ماتریس نامنفرد S، ماتریس جایگشت P، ماتریس مولد G، جدول سندروم- خطا،

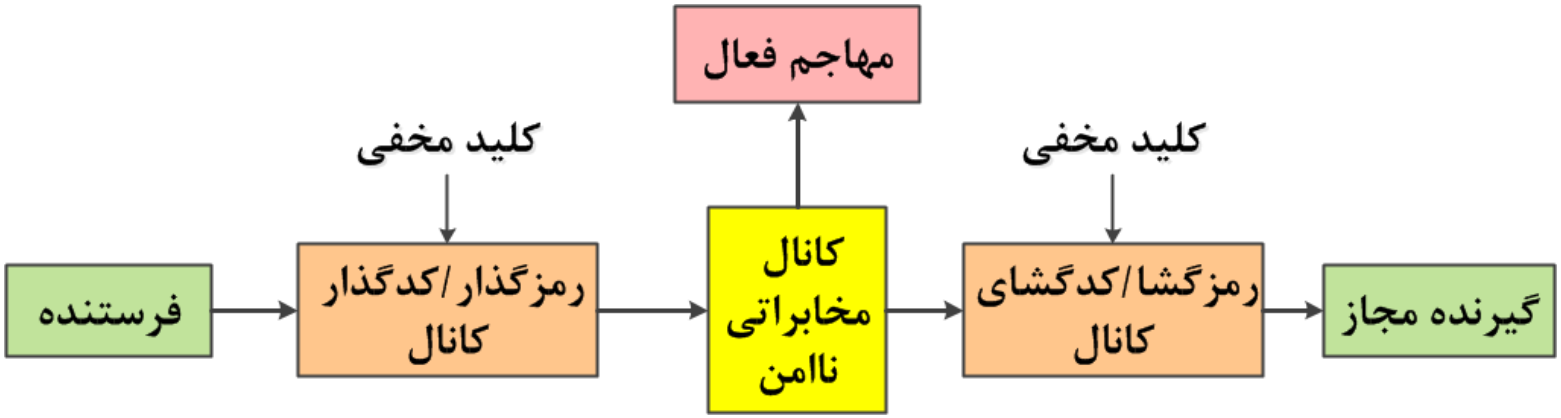
مزایا و نواقص سامانه رمز کلید مخفی Rao-Nam

- کد مورد استفاده:
  - کد همینگ به ابعاد $(72, 64)$
- مزایا:
  - پیچیدگی محاسباتی کم و سرعت زیاد
  - نرخ انتقال زیاد $(R \approx 0.89)$
- نواقص:
  - طول کلید زیاد $(18\ \text{kbits})$
  - سطح امنیت پایین در برابر حمله متن اصلی منتخب
  - تعداد کم کدهای هم ارز $(N_C = 2^8)$

سامانه های رمز کلید مخفی مبتنی بر کد

- **انواع کدهای به کار رفته:**
  - **کدهای همینگ [RaoNam’89].**
  - **کدهای غیرخطی [StruikTilburg’87].**
  - **کدهای آرایه ای [AlJabri’96].**
  - **کدهای تصحیح خطای دسته ای [Sun’97].**
  - **کدهای ضربی [SunShieh’98].**
- **نواقص سامانه های رمزگذاری کلید مخفی مبتنی بر کد:**
  - **ناامن در برابر حمله متن اصلی منتخب**
  - **استفاده از کدهای کانال ناکارآ**

سامانه های توأم رمزنگاری کلید مخفی-کدگذاری کانال



نمودار گردشی سامانه های توأم رمزگذاری کلید مخفی-کدگذاری کانال

- کدهای مورد استفاده در سامانه های توأم رمزگذاری کلید مخفی-کدگذاری کانال:
  - کدهای Turbo [PayandehAhmadianAref'06].
  - کدهای EG-QC-LDPC [SobhiAfsharEghlidosAref'09].
  - کدهای EDF-QC-LDPC [HooshmandEghlidosAref'11].

برخی از انواع خانواده های کدهای QC-LDPC

- **کدهای مبتنی بر هندسه متناهی:**
  - **کدهای توازن آزمای کم چگال شبه دوری مبتنی بر هندسه اقلیدسی (EG-QC-LDPC)**
  - **کدهای توازن آزمای کم چگال شبه دوری مبتنی بر هندسه تصویری (PG-QC-LDPC)**
- **کدهای مبتنی بر خانواده های تفاضلی:**
  - **کدهای توازن آزمای کم چگال شبه دوری مبتنی بر خانواده های تفاضلی (DF-QC-LDPC)**
  - **کدهای توازن آزمای کم چگال شبه دوری مبتنی بر خانواده های تفاضلی گسترش یافته (EDF-QC-LDPC)**

سامانه توأم مبتنی بر کدهای EG-QC-LDPC

کدهای EG-QC-LDPC

- [YuLinFossorier'01]
- $EG(m,q)$: هندسه اقلیدسی m بعدی بر میدان متناهی $GF(q)$
  - تعداد نقاط: q^m
  - تعداد خطوط: $(q^m-1)/(q-1)\,q^{(m-1)}$
  - هر خط از q نقطه می گذرد.
  - از هر نقطه $(q^m-1)/(q-1)$ خط می گذرد .
- $EG^*(m,q)$: زیرهندسه ای از $EG(m,q)$ که با حذف مبداء و تمام خطوط گذرنده از مبداء به دست می آید.
  - تعداد نقاط: $n=q^m-1$
  - تعداد خطوط: $J_0=(q^{(m-1)}-1)(q^m-1)/(q-1)$

کدهای EG-QC-LDPC

- هر عضو میدان $GF(q^m)$ را می توان به صورت یک m تایی روی $GF(q)$ نمایش داد.
  - از این رو می توان $GF(q^m)$ را با $EG(m,q)$ متناظر فرض کرد.
- اگر α عضوی اولیه از $GF(q^m)$ باشد، در این صورت $\alpha^0, \cdots, \alpha^{n-1}$ متناظر با n نقطه غیر مبدأ در $EG^*(m,q)$ است.

- بردار تلاقی یک خط L در $EG^*(m,q)$ به صورت یک n تایی $\boldsymbol{v}_L = (\boldsymbol{v}_0, \cdots, \boldsymbol{v}_{n-1})$ روی $GF(q)$ تعریف می شود که مولفه های آن متناظر با نقاط غیرمبدا $EG^*(m,q)$ هستند.
  - $\boldsymbol{v}_i = 1$ است اگر و فقط اگر α^i نقطه ای روی خط L باشد.
  - فرض کنید ${\boldsymbol{v}_L}^{(i)}$ برداری باشد که از انتقال گردشی بردار تلاقی $\boldsymbol{v}_L$ به اندازه i مولفه به سمت راست به دست آید.

کدهای EG-QC-LDPC

- به ازای $0 \le i \le n$، $\boldsymbol{v}_L^{(i)}$، بردار تلاقی خط دیگری در $EG^*(m,q)$ است .
- $\boldsymbol{v}_L$ و $n-1$ انتقال دوری آن، n بردار تلاقی متناظر در $EG^*(m,q)$ می دهد.
- بردارهای تلاقی J_0 خط موجود در $EG^*(m,q)$ را می توان به صورت دسته دوری افراز نمود. $K_0 = (q^{(m-1)}-1)\ /(q-1)$
- ماتریس توازن آزما:
  - $H_{n\times J_o} = [H_0 H_1 \dots H_{K_0}]$
    - $n = q^m - 1$
    - $J_0 = (q^{(m-1)}-1)(q^m-1)/(q-1)$

سامانه توأم مبتنی بر کدهای EG-QC-LDPC

- [SobhiAfsharEghlidosAref'09]

- کلید مخفی:
  - ماتریس توازن آزمای کد EG-QC-LDPC

$$H = [H_1 \quad H_2 \quad \cdots \quad H_{K_0}]$$

  - ماتریس جایگشت

$$P_{n\times n} = \begin{bmatrix} \pi_{l\times l} & 0 & \cdots & 0 \\ 0 & \pi_{l\times l} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \pi_{l\times l} \end{bmatrix}$$

  - بردار اولیه (IV)

سامانه توأم مبتنی بر کدهای EG-QC-LDPC

- **الگوریتم رمزگذاری:**

$$\boldsymbol{c} = (\boldsymbol{m}G + \boldsymbol{e}_P)P$$

$$\boldsymbol{e_P} = \boldsymbol{e}(\boldsymbol{s}) + h(\boldsymbol{s})$$

$$\boldsymbol{e}(\boldsymbol{s}) = \boldsymbol{s}.(H^{-1})^T$$

- **الگوریتم رمزگشایی:**

$$\boldsymbol{r} = (\boldsymbol{m}G + \boldsymbol{e}_P)\boldsymbol{P} + \boldsymbol{e}_{ch}$$

$$\boldsymbol{r'} = \boldsymbol{r}P^{-1} = \boldsymbol{m}G + \boldsymbol{e}_P + \boldsymbol{e}_{ch}P^{-1}$$

$$\boldsymbol{e_P} = \boldsymbol{e}(\boldsymbol{s}) + h(\boldsymbol{s}) = \boldsymbol{s}.\left(\boldsymbol{H^{-1}}\right)^{\boldsymbol{T}} + h(\boldsymbol{s})$$

$$\boldsymbol{r''} = \boldsymbol{r'} - \boldsymbol{e}_P = \boldsymbol{m}G + \boldsymbol{e}_{ch}P^{-1}$$

$$\boldsymbol{m} = Decode(\boldsymbol{r''})$$

سامانه توأم مبتنی بر کدهای EG-QC-LDPC

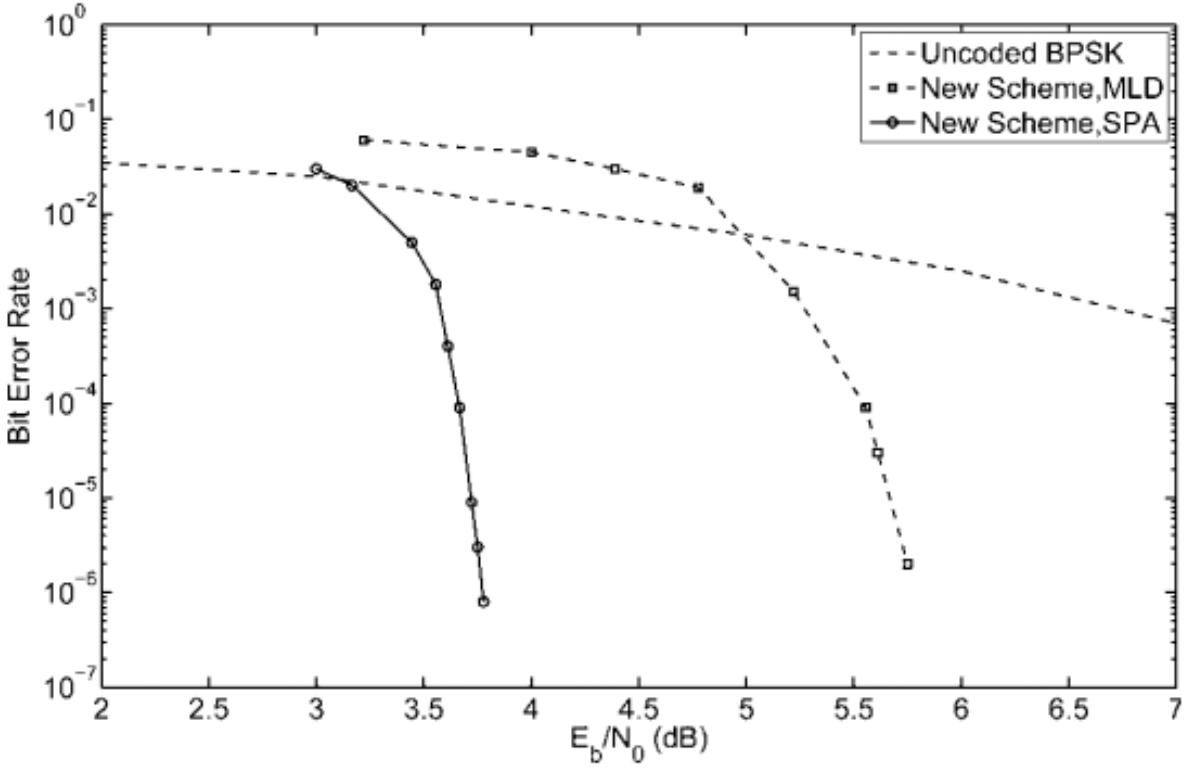
❑ مزایا:

- طول کم کلید
- استفاده از خاصیت تنک بودن ماتریس توازن آزما
  - استفاده از الگوریتم فشرده سازی

مقایسه طول کلید سامانه مبتنی بر کدهای EG-QC-LDPC [SobhiAfshar et al.'09]

سامانه	کد	طول کلید
Rao [Rao86]	$C(1024, 524)$	2 Mbits
Rao-Nam [RN89]	$C(72, 64)$	18 kbits
Struik-Tilburg [ST88]	$C(72, 64)$	18 kbits
Sun-Shieh [SS98]	$C(49, 36)$	42 kbits
Barbero-Ytrehus [BY98]	$C(1024, 524)$	4.9 kbits
سامانه مبتنی بر EG-QC-LDPC	$C(2044, 1024)$	2.5 kbits

سامانه توأم مبتنی بر کدهای EG-QC-LDPC



عملکرد تصحیح خطای کد EG-QC-LDPC به ابعاد (4088,3066) [SobhiAfshar et al.'09]

سامانه توأم مبتنی بر کدهای EG-QC-LDPC

- **مزایای دیگر:**
  - امنیت مناسب (مقاومت مناسب در برابر حملات شناخته شده)
  - قابلیت تصحیح خطای مناسب

- **حملات اعمال شده:**
  - حمله جستجوی کامل
  - حمله متن اصلی منتخب
    - حمله Rao-Nam [RaoNam’89]
    - حمله Struik-Tilburg [StruikTilburg’87]

سامانه توأم مبتنی بر کدهای EDF-QC-LDPC

کدهای EDF-QC-LDPC

- [XiaXia'05]
- خانواده تفاضلی گسترش یافته $(\mu,\ n_0)$:
  - فرض کنید $F = \{B_1, B_2, \cdots, B_{n_0}\}$ خانواده‌ای متشکل از قالب‌های پایه μ عضوی (μ عدد صحیح مخالف صفر) باشد.
  - F را یک خانواده تفاضلی گسترش‌یافته $(\mu,\ n_0)$ گویند، اگر همه فواصل درون‌مجموعه‌ای $b_{i,x} - b_{i,y}, (x, y \in \{1, \cdots, \mu\},\ x \neq y)$ مجزا باشند. بزرگترین فاصله درون‌مجموعه‌ای با d_{max} نشان می دهند.
  - برای یک خانواده تفاضلی گسترش یافته $(\mu,\ n_0)$ داریم:

$$d_{max} \geq n_0\mu(\mu - 1)/2$$

کدهای EDF-QC-LDPC

❑ ساخت کد EDF-QC-LDPC با بردار مشخصه $\overline{chr} = (m, \mu, n_0)$:

- انتخاب خانواده تفاضلی گسترش یافته (μ, n_0)
- ساخت چندجمله ای های مولد $h_i(x) = x^{b_{i,1}} + \cdots + x^{b_{i,\mu}}$، به ازای $B_i, i = 1, \cdots, n_0$
- انتخاب m به طوریکه $\mu/m \ll 1$ و ساخت ماتریس توازن آزمای

$$H_{m \times mn_0} = [H_1, H_2, \cdots, H_{n_0}]$$

- ساخت ماتریس مولد

$$G = \left[I_{m(n_0-1)} \quad | \quad \begin{matrix} (H_{n_0}^{-1} H_1)^T \\ (H_{n_0}^{-1} H_2)^T \\ \vdots \\ (H_{n_0}^{-1} H_{n_0-1})^T \end{matrix} \right]$$

سامانه توأم مبتنی بر کدهای EDF-QC-LDPC

- [HooshmandEghlidosAref'11]
- کلید مخفی:
  - ماتریس بررسی توازن $H = [H_1 \quad H_2 \quad \cdots \quad H_{n_0}]$
  - ماتریس نامنفرد $S = \begin{bmatrix} s_{1,1} & s_{1,2} & \cdots & s_{1,n_0-1} \\ s_{2,1} & s_{2,2} & \cdots & s_{2,n_0-1} \\ \vdots & \vdots & \ddots & \vdots \\ s_{n_0-1,1} & s_{n_0-1,2} & \cdots & s_{n_0-1,n_0-1} \end{bmatrix}$
  - ماتریس جایگشت $P = \begin{bmatrix} p_{1,1} & 0 & \cdots & 0 \\ 0 & p_{2,2} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & p_{n_0,n_0} \end{bmatrix}$
  - بردار اولیه (IV)

سامانه توأم مبتنی بر کدهای EDF-QC-LDPC

الگوریتم رمزگذاری:

$$\begin{aligned} \boldsymbol{c} &= \big((\boldsymbol{m}+\boldsymbol{e}')SG+\boldsymbol{e}''\big)P \\ &= \boldsymbol{m}SGP+(\boldsymbol{e}'SG+\boldsymbol{e}'')P \\ &= \boldsymbol{m}G'+\boldsymbol{e}'(s)P, \end{aligned}$$

$$\boldsymbol{e}(\boldsymbol{s}) = \boldsymbol{s}.\left(\boldsymbol{H}^{-1}\right)^{\boldsymbol{T}}$$

الگوریتم رمزگشایی:

$$\boldsymbol{r} = \boldsymbol{c} + \boldsymbol{e}_{ch} = \boldsymbol{m}SGP + (\boldsymbol{e}'SG + \boldsymbol{e}'')P + \boldsymbol{e}_{ch}$$

$$\boldsymbol{r}' = \boldsymbol{r}P^T = (\boldsymbol{m}+\boldsymbol{e}')SG + \boldsymbol{e}'' + \boldsymbol{e}_{ch}P^T$$

$$\boldsymbol{r}'' = \boldsymbol{r}' - \boldsymbol{e}'' = (\boldsymbol{m}+\boldsymbol{e}')SG + \boldsymbol{e}_{ch}P^T$$

$$\boldsymbol{r}''' = Decode(\boldsymbol{r}'') = (\boldsymbol{m}+\boldsymbol{e}')S$$

$$\boldsymbol{m}' = \boldsymbol{m}+\boldsymbol{e}' = \boldsymbol{r}'''S^{-1}$$

$$\boldsymbol{m} = \boldsymbol{m}' - \boldsymbol{e}'$$

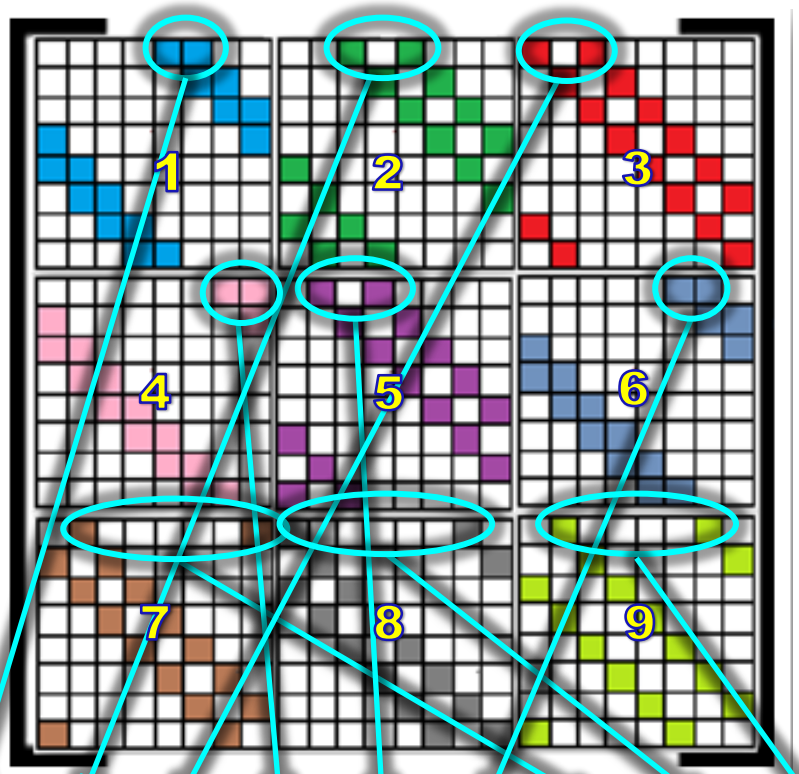
سامانه توأم مبتنی بر کدهای EDF-QC-LDPC

❑ روش فشرده سازی:

یک مثال ساده:

ماتریس قالبی دوری $A_{32\times32}$

$A=$



موقعیت های غیرصفر سطر اول هر زیرماتریس

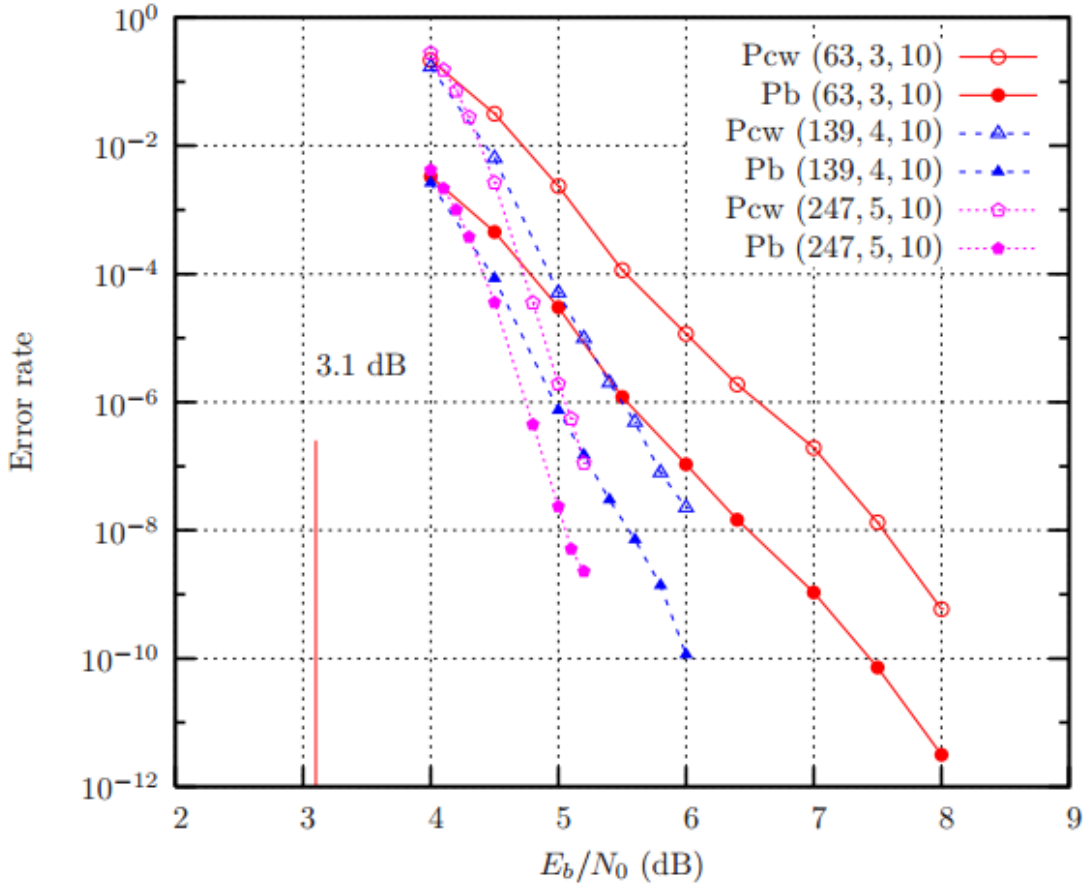
بردار فشرده شده $\overline{A_c}$

$A_c = (5, 6, 3, 5, 1, 3, 7, 8, 2, 4, 6, 7, 2, 8, 1, 7, 2, 7)$

سامانه توأم مبتنی بر کدهای EDF-QC-LDPC

- **طول کلید قبل از فشرده سازی:** $(n,k)=(2470,2223)$
  - $\mathcal{M}_H = mn_0 = 2470bit$
  - $\mathcal{M}_S = (n_0-1)\,^2m \cong 20kbit$
  - $\mathcal{M}_P = log_2^{(m!)} = log_2^{(247!)} \cong 1612bit$
  - $\mathcal{M}_{IV} = n-k = 247bit$
  - $\mathcal{M}_k = \mathcal{M}_H + \mathcal{M}_S + \mathcal{M}_P + \mathcal{M}_{IV} \cong 24.4kbit$
- **طول کلید پس از فشرده سازی:**
  - $\mathcal{M}_{\bar{H}_c} = \mu_H n_0 \le 400bit$ فشرده سازی ماتریس بررسی توازن H
  - $\mathcal{M}_{\bar{S}_c} = \mu_S(n_0-1)^2 \le 1296bit$ فشرده سازی ماتریس ناویژه S
  - $\mathcal{M}_K = \mathcal{M}_P + \mathcal{M}_{\bar{H}_c} + \mathcal{M}_{\bar{S}_c} + \mathcal{M}_{IV} \le 3.555kbit$
- **طول کلید نسبت به قبل از فشرده سازی به میزان ۸۵ درصد کوتاهتر شده است.**

سامانه توأم مبتنی بر کدهای EDF-QC-LDPC



عملکرد تصحیح خطای کد EDF-QC-LDPC به ازای سه طول متفاوت کد [XiaXia'05]

سامانه توأم مبتنی بر کدهای EDF-QC-LDPC

❑ حمله جستجوی کامل

- این حمله در صورتی امکان‌پذیر است که اندازه فضای کلید از مرتبه چندجمله‌ای باشد.
- $n = 2470,\ k = 2223,\ n_0 = 10,\ m = 247$

تعداد پارامترهای کلید مخفی سامانه مبتنی بر کدهای [Hooshmand et al.'11] EDF-QC-LDPC

تعداد کدهای هم ارز	تعداد ماتریس های نامنفرد	تعداد ماتریس های جایگشت	تعداد بردارهای خطای عمدی
$N_{EDF} = \binom{m}{\mu}^{n_0}$	$N_S > 2^{k^2-k}$	$N_P = m!$	$N_e = 2^{n-k}$
$N_{EDF} = 2^{327}$	$N_S \gg 2^{80}$	$N_P = 247! \gg 2^{80}$	$N_e = 2^{247}$

❑ با توجه به تعداد زیاد پارامترهای کلید مخفی، حمله جستجوی کامل امکان پذیر نیست.

سامانه توأم مبتنی بر کدهای EDF-QC-LDPC

❑ حمله Rao-Nam [RaoNam'89]

$$\boldsymbol{c} = \boldsymbol{m}SGP + (\boldsymbol{e}'SG + \boldsymbol{e}'')P = \boldsymbol{m}G' + \boldsymbol{e}'(s)P$$

$$\boldsymbol{m}_1 - \boldsymbol{m}_2 = (0, 0, \ldots . 0, 1, 0, \ldots . , 0)$$

i بیت i-ام، $i = 1, \ldots , k$

$$\boldsymbol{c}_1 = \boldsymbol{m}_1SGP + (\boldsymbol{e}'_1SG + \boldsymbol{e}''_1)P = \boldsymbol{m}_1G' + \boldsymbol{e}'_1(s)P$$
$$\boldsymbol{c}_2 = \boldsymbol{m}_2SGP + (\boldsymbol{e}'_2SG + \boldsymbol{e}''_2)P = \boldsymbol{m}_2G' + \boldsymbol{e}'_2(s)P$$

$$\boldsymbol{c}_1 - \boldsymbol{c}_2 = (\boldsymbol{m}_1 - \boldsymbol{m}_2)G' + \big(e'_1(s) - e'_2(s)\big)P = g'_i + \big(e'_1(s) - e'_2(s)\big)P$$

i–امین بردار سطری ماتریس G'

- به واسطه چگال بودن ماتریس مولد G کد EDF-QC-LDPC بردار $\big(e'_1(s) - e'_2(s)\big)P$ چگال است.

از این رو نمی‌توان بردار $c_1 - c_2$ را تخمین زد و حمله با شکست مواجه می‌شود.

سامانه توأم مبتنی بر کدهای EDF-QC-LDPC

❑ حمله Struik-Tilburg [StruikTilburg'87]

$$\boldsymbol{c} = \big((\boldsymbol{m}+\boldsymbol{e}')SG + \boldsymbol{e}''\big)P = \boldsymbol{m}G' + \boldsymbol{e}'(s)P$$

$$\boldsymbol{c}_1 = \big((\boldsymbol{m}+\boldsymbol{e}_1')SG + \boldsymbol{e}_1''\big)P = \boldsymbol{m}G' + \boldsymbol{e}_1'(s)P$$
$$\boldsymbol{c}_2 = \big((\boldsymbol{m}+\boldsymbol{e}_2')SG + \boldsymbol{e}_2''\big)P = \boldsymbol{m}G' + \boldsymbol{e}_2'(s)P$$
$$\vdots$$
$$\boldsymbol{c}_{\mathcal{N}_e} = \big((\boldsymbol{m}+\boldsymbol{e}_{\mathcal{N}_e}')SG + \boldsymbol{e}_{\mathcal{N}_e}''\big)P = \boldsymbol{m}G' + \boldsymbol{e}_{\mathcal{N}_e}'(s)P$$

بردارهای متن های رمز شده به ازای بردارهای خطای متفاوت

❑ به دست آوردن $\mathcal{N}_e$ متن رمز شده مجزا $\boldsymbol{c}_1, \boldsymbol{c}_2, \dots, \boldsymbol{c}_{\mathcal{N}_e}$ به ازاء هر بردار متن اصلی $\boldsymbol{m}$ به طور میانگین به $\mathcal{O}(\mathcal{N}_e log \mathcal{N}_e)$ عملیات رمزگذاری نیاز دارد.

❑ در این سامانه داریم: $\mathcal{N}_e = 2^{247}$ و $\mathcal{O}(\mathcal{N}_e log \mathcal{N}_e) = \mathcal{O}(2^{253})$

بنابراین این حمله با شکست مواجه می شود.

نتیجه گیری

نتیجه گیری

- استفاده از رمزگذاری کلید مخفی مبتنی بر مسائل سخت کدینگ یکی از راهکارهای مناسب جهت دستیابی به امنیت و کارآیی در سامانه های ارتباطی است.
- مهمترین مسئله در طراحی این نوع سامانه ها، برقراری یک بده و بستان مناسب بین امنیت و کارآیی است به طوریکه هیچ یک از پارامترهای امنیت و کارآیی، قربانی یکدیگر نشوند.
- بهره گیری از کدهای مناسب و الگوریتم های بهینه رمزگذاری و رمزگشایی، ابزارهای مناسبی جهت نیل به این هدف هستند.

مسائل باز

- استفاده از کدهای مناسب کانال در ساختار سامانه های رمز کلید مخفی مبتنی بر مسائل سخت کدینگ
  - کدهای قطبی
- طراحی الگوریتم های بهینه رمزگذاری و رمزگشایی در ساختار این نوع سامانه ها
- ارائه حملات جدید به این نوع از سامانه ها
- استفاده از مسائل سخت متفاوت جهت طراحی این نوع سامانه ها

مراجع

[Rao84] T.R.N. Rao, “Joint encryption and error correction schemes”, 11th Int. Symp. on Computer Architecture, Ann Arbor, Mich.,, pp. 240–241, 1984.

[RN89] T.R.N. Rao, K. H. Nam, “Private-Key Algebraic-Code Encryption”, IEEE Trans. Inf. Theory, Vol. 35, No. 4, pp. 829–833, 1989.

[ST87] R. Struik, J. Van Tilburg, “The Rao-Nam scheme is insecure against a chosen-plaintext attack”, CRYPTO’87, pp. 445–457, New York: Springer-Verlag, 1987.

[SS98] H. M. Sun, S. P. Shieh, “On private-key cryptosystems based on product codes”, 3rd Australian Conf. on Inf. Security and Privacy, pp. 68–79, 1998.

[BY98] A. I. Barbero, O. Ytrehus, “Modifications of the Rao-Nam Cryptosystem”, in Proc. Int. Conf. on Coding Theory, Cryptography and Related Areas, pp. 1-13, 1998.

مراجع

[YLF01] K. Yu, S. Lin, M. Fossorier, “Low density parity check codes based on finite geometries: A discovery and new results”, IEEE Trans. Inf. Theory, Vol. 47, No. 11, pp. 2711-2736, 2001.

[XiaXia05] Xia, T., Xia, B., “Quasi-cyclic codes from extended difference families”, In Proc. IEEE Wireless Commun. and Networking Conf, Vol. 2, pp. 1036-1040, Mar. 2005, New Orleans, USA.

[PAA06] A. Payandeh, M. Ahmadian, M. R. Aref, “Adaptive secure channel coding based on punctured turbo codes”, IEE Proc. Commun., Vol. 153, No. 2, pp. 313-316, 2006.

[SEA09] A. A. Sobhi Afshar, , T. Eghlidos, M. R. Aref, “Efficient secure channel coding based on quasi-cyclic low-density parity-check codes” IET Commun., Vol. 3, No. 2, pp. 279-292, 2009.

[HEA11] R. Hooshmand, T. Eghlidos, M. R. Aref, “Improving the Rao-Nam Secret Key Cryptosystem Using Regular EDF-QC-LDPC Codes”, ISeCure Journal, Vol. 4, No. 1, pp. 3-14, 2011.

با تشکر از توجه شما