بسم الله الرحمن الرحیم

سامانه های رمز کلید عمومی شبه McEliece مبتنی بر کدهای LDPC

خدیجه باقری

دانشکده ریاضی و علوم کامپیوتر– دانشگاه صنعتی امیرکبیر

kbagheri@aut.ac.ir

فهرست مطالب

دیباچه

دیباچه

- ویژگی کدهای مناسب برای سامانه های رمز کد مبنا
  - طول کوتاه کلید عمومی
  - الگوریتم کدگشایی کارا
  - بزرگ بودن اندازه ی خانواده ی کدهای هم ارز
  - نرخ زیاد انتقال

✓ استفاده از کدهای با ماتریس توازن آزمای کم چگال (LDPC) و مدل شبه دوری آن (QC-LDPC)

سامانه های رمز مبتنی بر کدهای LDPC

کدهای با ماتریس توازن آزمای کم چگال (LDPC)

- دسته ای از کدهای قالبی خطی که دارای ماتریس توازن آزمای تنک است:

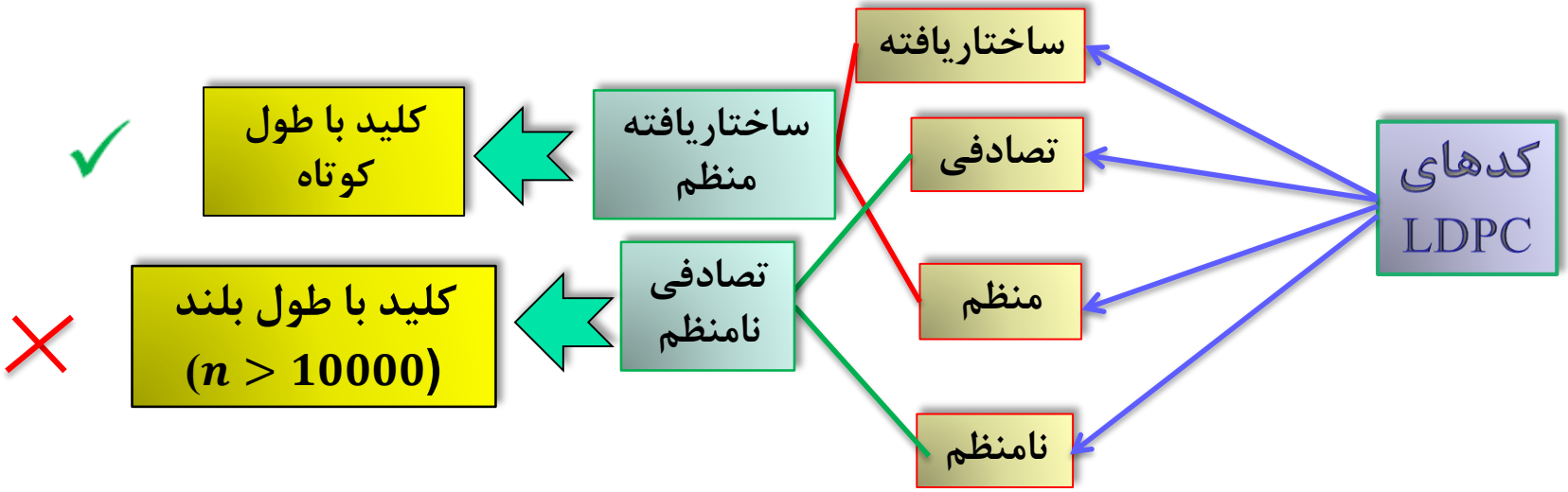
$$H=\begin{bmatrix} 1 & . & . & . & . & 1 & . \\ 1 & . & . & . & . & . & . \\ . & 1 & . & . & . & 1 & . \\ . & 1 & . & . & . & . & . \\ . & . & 1 & . & . & . & . \\ . & . & 1 & . & . & . & . \\ . & . & . & 1 & . & . & 1 \\ . & . & . & 1 & . & . & . \\ . & . & . & . & 1 & . & . \\ . & . & . & . & 1 & . & 1 \end{bmatrix}$$

- تعریف :

$$C = \{x \mid Hx^t = 0\}$$

  - قدرت تصحیح خطای زیاد
  - پیچیدگی کم کدگشایی

کدهای بررسی توازن کم چگال (LDPC)



- تفاوت عمده بین کدهای LDPC و دیگر کدهای قالبی خطی: عملکرد تصحیح خطای بسیار مناسب و نحوه کدگشایی.

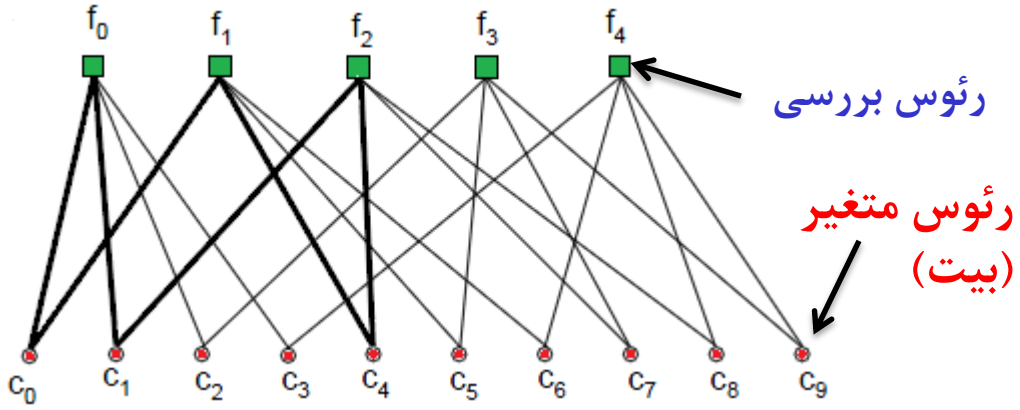
کدهای بررسی توازن کم چگال (LDPC)

گراف تنر (دوبخشی): نمایش گرافیکی ماتریس بررسی توازن کد LDPC

مثال: گراف تنر و ماتریس بررسی توازن یک کد **LDPC** منظم با $d_c = 2$ و $d_r = 4$

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

ماتریس بررسی توازن



گراف تنر (دوبخشی)

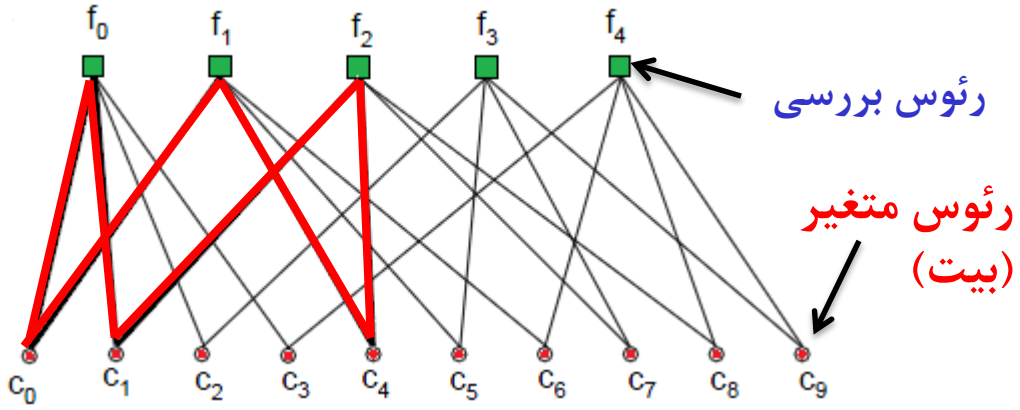
کدهای بررسی توازن کم چگال (LDPC)

گراف تنر (دوبخشی): نمایش گرافیکی ماتریس بررسی توازن کد LDPC

مثال: گراف تنر و ماتریس بررسی توازن یک کد LDPC منظم با $d_c = 2$ و $d_r = 4$

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

ماتریس بررسی توازن



گراف تنر (دوبخشی)

ویژگی مهم یک کد LDPC ← عدم وجود دورهایی به طول چهار در گراف تنر متناظر

سامانه ی رمز مبتنی بر کدهایLDPC

- ارائه در ۲۰۰۰ [MonicoRosenthalShokrollahi'00]
- تولید کلید:
  - کلید خصوصی: (H, T)
    - ✓ ماتریس $H_{(n-k)\times n}$ از مجموعه ی خانواده ی کدهای تصادفی LDPC
    - ✓ ماتریس تبدیل تصادفی T، کم چگال و معکوس پذیر $(n-k)\times(n-k)$
  - کلید عمومی: (H', S, t)
    - ✓ماتریس $S_{k\times k}$ تصادفی، کم چگال و معکوس پذیر $k \times k$
    - ✓ماتریس $H' = T \cdot H$,
    - ✓قابلیت تصحیح خطا: t

سامانه ی رمز مبتنی بر کدهای LDPC

- رمزگذاری
  - ماتریس مولد کد در فرم کاهش یافته ی پله ای
  - محاسبه $G' = S^{-1} \cdot G$

$$x = u \cdot G' + e$$

- رمزگشایی
  - الگوریتم کدگشایی LDPC و تصحیح t خطا
  - بدست اوردن $u \cdot G'$
  - بازیابی متن از K مولفه ی اول $u \cdot G'$
  - ضرب در S^{-1}

تحلیل سامانه ی رمز مبتنی بر کدهای LDPC

- شرایط
  - H و H’ هر دو معرف یک کد هستند. $H'=T\cdot H$
  - H تُنک و بدون دورهای کوچک
    - الگوریتم کدگشایی کارا و قابلیت تصحیح خطای بالا
  - T تُنک
- مزیت
  - ✓ ایجاد دورهای کوچک در H’
  - ✓ از دست دادن کارایی الگوریتم کدگشای برای مهاجم
  - ✓ کم چگال شدن ماتریس H’ و درنتیجه طول کم کلید عمومی

تحلیل سامانه ی رمز مبتنی بر کدهای LDPC

- نقص ها
  - جستجو کلمات کد با وزن کم در کد دوگان.
  - بازیابی کلید خصوصی H از روی کد عمومی.
- راهکار
  - درنظر گرفتن T چگال.
    - کلید عمومی H’ چگال.
    - از کم چگال بودن کدهای LDPC برای کاهش طول کلید استفاده نشد.

✓ استفاده از کدهای LDPC ساختاریافته (QC- LDPC) برای کاهش طول کلید.

انواع سامانه های رمز مبتنی بر کدهای QC-LDPC

کدهای شبه دوری با ماتریس توازن آزما کم چگال (QC-LDPC)

- کد های شبه دوری با ماتریس توازن آزمای تُنک (QC-LDPC) یک کلاس خاص از این کدها هستند که دارای ماتریس H ساختاریافته هستند.

$$H = \begin{bmatrix} H_{00} & H_{01} & \cdots & H_{0(n_0-1)} \\ H_{10} & H_{11} & \cdots & H_{1(n_0-1)} \\ \vdots & \vdots & \ddots & \vdots \\ H_{(r_0-1)0} & H_{(r_0-1)1} & \cdots & H_{(r_0-1)(n_0-1)} \end{bmatrix},$$

- پارامترها

$$r = r_0 p \qquad k = k_0 p \qquad n = n_0 p$$

کدهای شبه دوری با ماتریس توازن آزما کم چگال (QC-LDPC)

- هر قالب یک ماتریس چرخشی $p \times p$ دودویی با وزن سطری یا ستونی کوچک d_v

$$H_i = \begin{bmatrix} h_0 & h_1 & h_2 & \dots & h_{p-1} \\ h_{p-1} & h_0 & h_1 & \dots & h_{p-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ h_1 & h_2 & h_3 & \dots & h_0 \end{bmatrix}$$

- اگر حداقل یکی از قالب های H_i معکوس پذیر ← ماتریس H معکوس پذیر

کدهای شبه دوری با ماتریس توازن آزما کم چگال (QC-LDPC)

- در نظر گرفتن کلاس خاص

$$H = \begin{bmatrix} H_0 & H_1 & \cdots & H_{n_0-1} \end{bmatrix},$$

- وزن سطری d_v
- نرخ کد $R = n_0 - 1/n_0$
- ماتریس مولد

$$G = \begin{bmatrix} & (H_{n_0-1}^{-1} \cdot H_0)^T \\ & (H_{n_0-1}^{-1} \cdot H_1)^T \\ I & \vdots \\ & (H_{n_0-1}^{-1} \cdot H_{n_0-2})^T \end{bmatrix}$$

ویژگی های کدهای QC-LDPC

- عملیات کدگذاری در کدهای QC-LDPC نیز با پیچیدگی کم انجام می پذیرد.
- با استفاده از کدهای QC-LDPC می توان کدهایی طراحی کرد که دارای نرخ های متفاوت و حتی نزدیک به ۱ هستند.
- خانواده ی کدهای هم ارز کدهای QC-LDPC بزرگ است.

سامانه ی رمز مبتنی بر کدهای QC-LDPC

- ارائه در ۲۰۰۶

[BaldiChiaraluceGarello'06]

- تولید کلید:
  - کلید خصوصی: (H, S, P)
    - H : ماتریس توازن آزمای کم چگال با وزن کم ستونی d_v
    - S : ماتریس درهم ساز تصادفی و معکوس پذیر $k \times k$ و شبه دوری
    - P : ماتریس جایگشتی، تصادفی و شبه دوری
      - ✓ محاسبه ی ماتریس مولد G در فرم کاهش یافته ی پله ای
  - کلید عمومی: G'

$$G' = S^{-1} \cdot G \cdot P^{-1} = S^{-1} \cdot G \cdot P^{T},$$

سامانه ی رمز مبتنی بر کدهای QC-LDPC

- رمزگذاری
  - بردار خطای e با وزن t

$$x = u \cdot G' + e$$

- رمزگشایی
  - ضرب ماتریس P

$$x' = x \cdot P = u \cdot S^{-1} \cdot G + e \cdot P$$

  - الگوریتم کدگشایی LDPC و تصحیح t خطا
  - بدست آوردن $u' = u \cdot S^{-1}$
  - بازیابی متن $u = u' \cdot S$

سامانه ی رمز مبتنی بر کدهای QC-LDPC

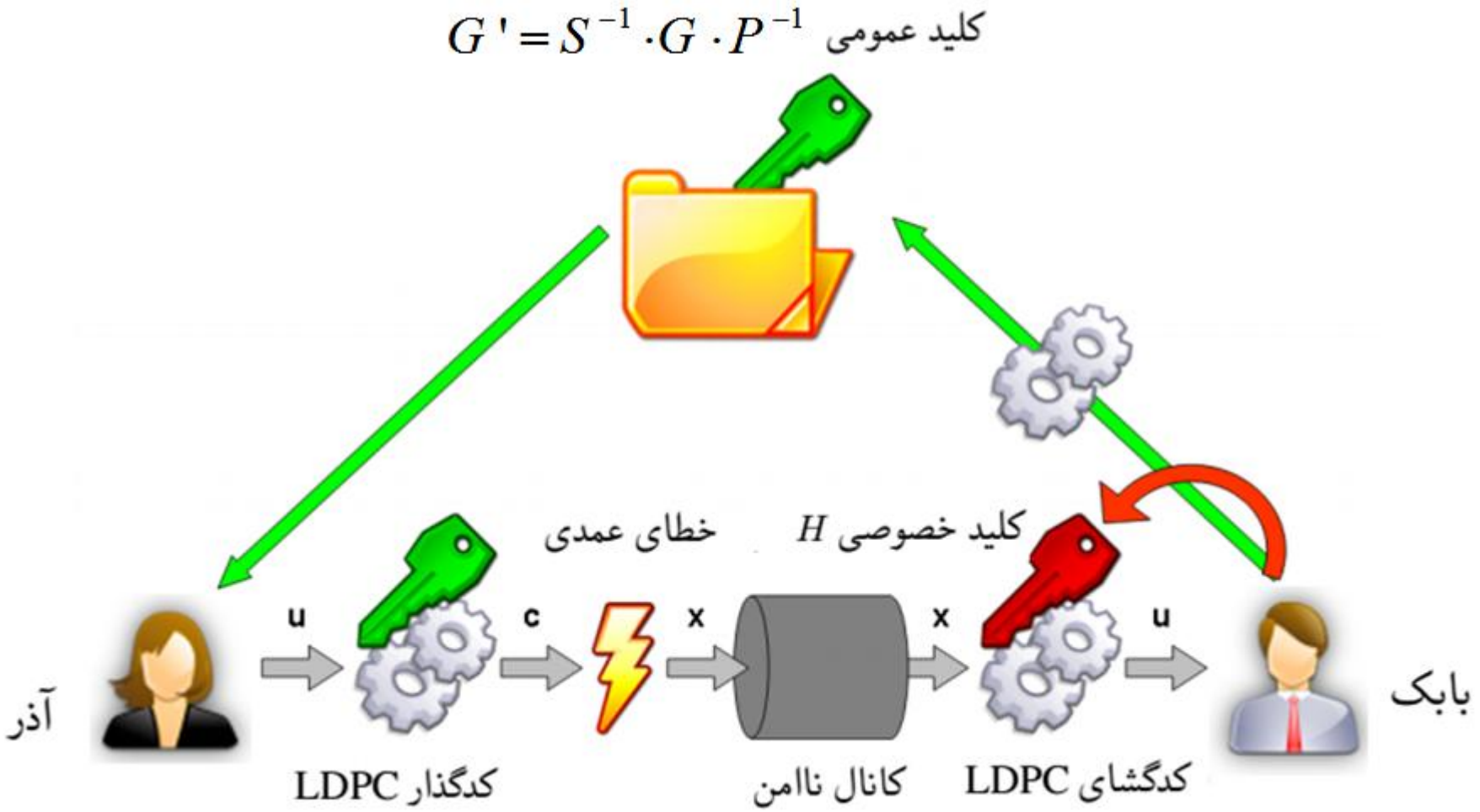


Diagram courtesy of Marco Baldi (link)

حمله به کد دوگان

- شرایط
  - ماتریس توازن آزمای کد عمومی: $H' = H \cdot P^T$
  - کدهای خصوصی و عمومی هم ارز جایگشتی.
- نقص ها
  - کلمات کد در دوگان کد عمومی (H') دارای وزن کم
    - اعمال الگوریتم یافتن کلمات کد با وزن کم.
    - قابلیت بازیابی ماتریس H از روی H’.
- راهکار
  - استفاده از ماتریس تبدیل غیر جایگشتی به جای P که وزن کلمات کد در دوگان کد عمومی را افزایش دهد.

سامانه ی رمز مبتنی بر کدهای QC-LDPC

- ارائه در ۲۰۰۷

[BaldiChiaraluce'07]

- تولید کلید:
  - کلید خصوصی: (H, S, Q)
    - H : ماتریس توازن آزما با وزن کم ستونی d_v
    - S : ماتریس معکوس پذیر و شبه دوری و کم چگال $k \times k$
    - Q : ماتریس شبه دوری و کم چگال $n \times n$ با وزن سطری و ستونی m
      - ✓ محاسبه ی ماتریس مولد G در فرم کاهش یافته ی پله ای
  - کلید عمومی: G'

$$G' = S^{-1} \cdot G \cdot Q^{-1},$$

سامانه ی رمز مبتنی بر کدهای QC-LDPC

- رمزگذاری
  - بردار خطای e با وزن $t' = {}^{t}/_{m}$

$$x = u \cdot G' + e$$

- رمزگشایی
  - ضرب ماتریس Q

$$x' = x \cdot Q = u \cdot S^{-1} \cdot G + e \cdot Q$$

  - الگوریتم کدگشایی LDPC و تصحیح خطا $t = t' \cdot m$
  - بدست اوردن $u' = u \cdot S^{-1}$
  - بازیابی متن $u = u' \cdot S$

سامانه ی رمز مبتنی بر کدهای QC-LDPC

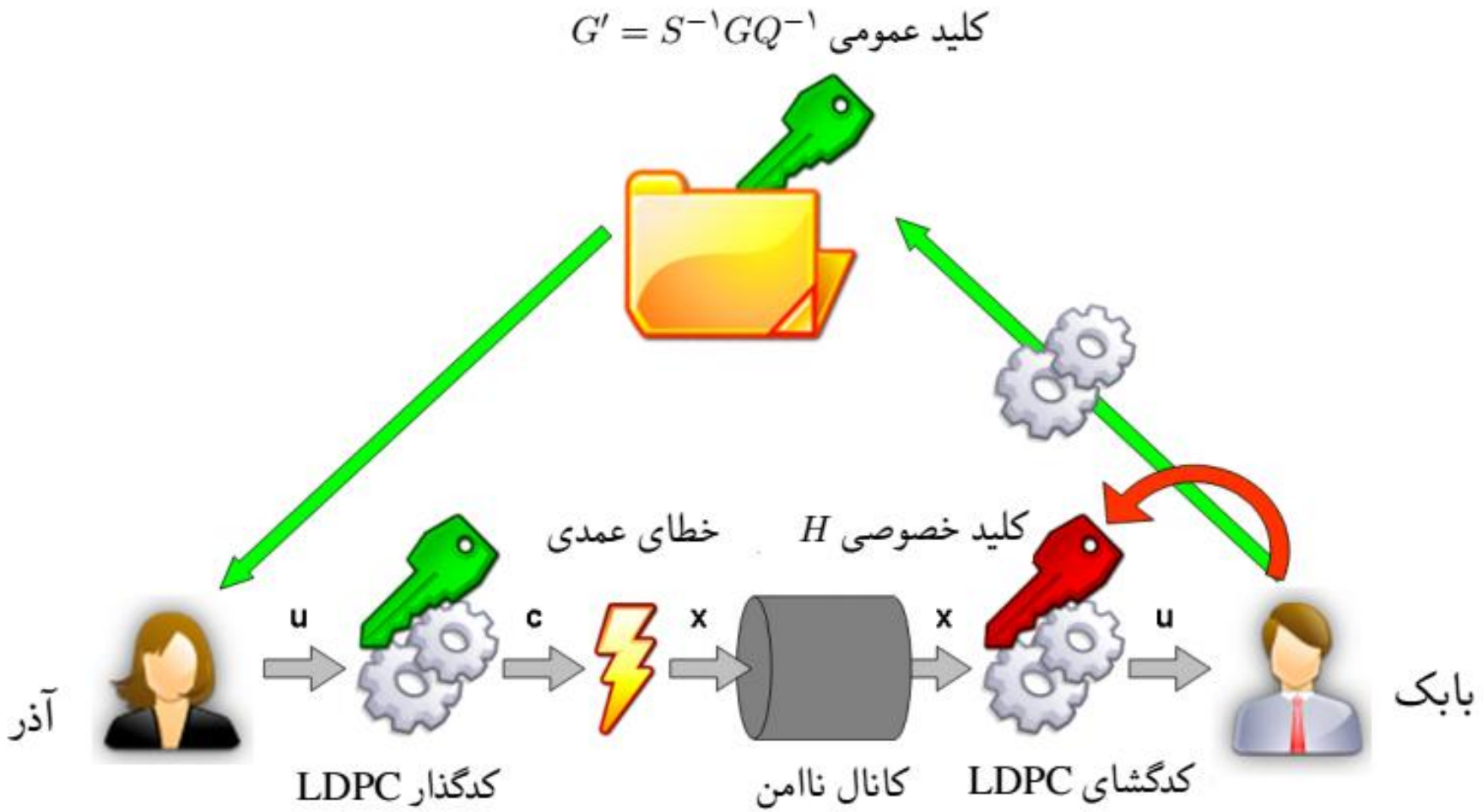


Diagram courtesy of Marco Baldi (link)

سامانه ی رمز مبتنی بر کدهای QC-LDPC

- شرایط
  - ماتریس توازن آزما کد عمومی $H' = H \cdot Q^T$
  - کدهای خصوصی و عمومی هم ارز جایگشتی نیستند
  - وزن سطری $m \cdot d_v \approx H'$
  - کلیدهای خصوصی Q و S را شبه دوری، تُنک و با وزن سطری و ستونی m (به منظور کاهش پیچیدگی رمزگذاری و رمزگشایی)
  - ماتریس Q به فرم قطری-قالبی

$$Q = \begin{bmatrix} Q_0 & 0 & 0 & 0 \\ 0 & Q_1 & 0 & 0 \\ 0 & 0 & \ddots & 0 \\ 0 & 0 & 0 & Q_{n_0-1} \end{bmatrix},$$

حمله به کد دوگان

- نقص ها
  - ماتریس H و Q هر دو تُنک
    - حمله به دوگان کد عمومی و امکان بازیابی ماتریس H
  - فرم قطری-قالبی ماتریس Q
  - تُنک بودن ماتریس S

- راهکار [BaldiBodratoChiaraluce’08]
  - انتخاب مناسب وزن سطری و ستونی (m) ماتریس Q
  - بزرگ شدن وزن کلمات کد (به اندازه‌ی کافی) در دوگان کد عمومی

حمله OTD

- طراحی حمله ی جدیدی در سال ۲۰۰۸

[OtmaniTillichDallot'08]

- انتخاب k ستون از G' توسط مهاجم

$$G'_{\leq k} = S^{-1} \cdot \begin{bmatrix} Q_0^{-1} & 0 & \cdots & 0 \\ 0 & Q_1^{-1} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & Q_{n_0-2}^{-1} \end{bmatrix},$$

- با معکوس کردن $G'_{\leq k}$ و در نظر گرفتن قالب (i,j) ام آن به $G_{i,j} = Q_i \cdot S_{i,j}$ دست پیدا می کند که معادل است با

$$g_{i,j}(x) = q_i(x) \cdot s_{i,j}(x) \mod (x^p + 1)$$

حمله OTD

- $S_{i,j}$ و Q_i ها تُنک و با وزن سطری و ستونی m

  - با احتمال زیاد $g_{i,j}(x)$ دارای دقیقا m^2 ضریب غیر صفر
  - $g_{i,j}(x)$ حداقل دارای یک شیفت از $q_i(x)$

- این نکته نقطه ی آغاز حمله ای به نام OTD است.
[OtmaniTillichDallot'08]

طرح جدید

- در سال ۲۰۰۸

[BaldiBodratoChiaraluce'08]

- با چگال درنظر گرفتن ماتریس S
  - عدم امکان بازیابی $S_{i,j}$ و Q_i از $Q_i S_{i,j}$
  - افزایش پیچیدگی رمزگشایی
    - قابل جبران با استفاده از الگوریتم های کارا برای ضرب ماتریس‌های چرخشی
- تُنک نگه داشتن ماتریس Q
  - حفظ توانایی تصحیح خطای عمدی (برای فرد مجاز)
- حذف فرض قالبی قطری بودن ماتریس Q

آخرین پیشرفت ها و نتیجه گیری

سیر تاریخی استفاده از کدهای LDPC در سامانه رمز کلید عمومی کدمبنا

- سامانه رمزنگاری بر مبنای کدهای LDPC [MonicoRosenthalShokrollahi'00]
- سامانه رمزنگاری بر مبنای کدهای QC-LDPC [BaldiChiaraluceGarello'06]
- ارائه طرح جدید مبتنی بر کدهای QC-LDPC و تحلیل رمز آن [BaldiChiaraluce'07]
  - ارائه حمله ی OTD [OtmaniTillichDallot'08]
- بهبود سامانه ی ارائه شده در ۲۰۰۷ و تحلیل آن [BaldiBodratoChiaraluce'08]
- سامانه رمز بر مبنای کدهای QC-LDPC نامنظم [ShooshtariAhmadianPayandeh'09]
- بهبود کارایی با استفاده از کدهای QC-LDPC نامنظم [BaldiBianchiMaturoChiaraluce'13]
- افزایش امنیت و کاهش اندازه ی کلید با استفاده از کدهای MDPC [MisoczkiTillichSendrierBarreto'13]

سامانه ی رمز مبتنی بر کدهای (QC)MDPC

- در سال ۲۰۱۳

[MisoczkiTillichSendrierBarreto’13]

- وجود ماتریس های Q و S لازم نیست
  - افزایش طول و وزن سطری ماتریس H به طور متوسط، کافی است.
  - در برابر تمام حملات مقاوم است.
- کدهای MDPC کدهای خطی دارای ماتریس توازن آزما با چگالی متوسط
- قدرت تصحیح خطای کمتر از کد LDPC
  - قدرت تصحیح خطای زیاد به منظور مقاومت در برابر حملات کدگشایی.
  - مجاز به استفاده از الگوریتم کدگشایی LDPC برای مقدار امن خطا.

سامانه ی رمز مبتنی بر کدهای MDPC

- تولید کلید:
  - کلید خصوصی : H
    - H : ماتریس توازن آزمای کد
  - کلید عمومی: G
    - ماتریس مولد کد در فرم کاهش یافته ی پله ای
- رمزگذاری

$$x = u \cdot G + e$$

- رمزگشایی
  - الگوریتم کدگشایی LDPC
  - بدست آوردن $u \cdot G$
  - بازیابی پیام از K مولفه ی اول $u \cdot G$

فواید سامانه ی رمز مبتنی بر کدهای (QC)MDPC

- حذف ماتریس های تبدیل
  - ✓ پیچیدگی بسیار کم عملیات رمزگذاری و رمزگشایی و تولید کلید
- افزایش وزن سطری H
  - ✓ مقاومت در برابر حمله به کد دوگان

فواید سامانه ی رمز مبتنی بر کدهای (QC)MDPC

- با توجه به ساختار ماتریس توازن آزما و مولد کد

$$H = \begin{bmatrix} H_0 & H_1 & \cdots & H_{n_0-1} \end{bmatrix},$$

$$G = \begin{bmatrix} & (H_{n_0-1}^{-1} \cdot H_0)^T \\ & (H_{n_0-1}^{-1} \cdot H_1)^T \\ I & \vdots \\ & (H_{n_0-1}^{-1} \cdot H_{n_0-2})^T \end{bmatrix}$$

- ✓ مهاجم به ماتریس توازن آزمای کم چگال دست پیدا نمی کند.
  - عدم دسترسی به الگوریتم کارای کدگشایی و پیچیدگی کم

اندازه ی کلید عمومی مبتنی بر کد QC- MDPC

اندازه ی کلید عمومی (بر حسب بیت)

اندازه کلید عمومی	t	d_v	k	n	n_0	امنیت
۴۶۰۰	۸۴	۴۵	۴۶۰۰	۹۲۰۰	۲	۸۰
۸۱۹۲	۱۱۵	۶۳	۸۱۹۲	۱۶۳۸۴	۲	۱۲۸
۶۰۰۰۰	۳۶۷	۱۸۹	۶۰۰۰۰	۱۲۰۰۰۰	۲	۲۵۶

[MisoczkiTillichSendrierBarreto’13]

- اندازه ی کلید عمومی = K

مقایسه

مقایسه سامانه های کلید عمومی کدمبنا با سامانه ی RSA

	McEliece (1024,524)	Niederreiter (1024,524)	RSA 1024-bit	McEliece like (QC-LDPC)	McEliece like (QC-LDPC)
اندازه کلید (بایت)	67072	32750	256	6144	6144
قالب اطلاعات (بیت)	524	۲۸۴	1024	12288	16384
نرخ	0.5117	0.5681	1	0.75	0.6667
تعداد عملیات باینری رمزگذاری	514	50	2402	658	776
تعداد عملیات باینری رمزگشایی	5140	7863	738112	4678	8901

[BaldiChiaraluce'07]

مقایسه

مقایسه اندازه ی کلید عمومی سامانه های مبتنی بر کدهای متفاوت

سطح امنیت	QC-MDPC	QC-LDPC	Goppa
80	4801	12096	460647
128	9857	27648	1537536
256	32771	-	7667855

[MisoczkiTillichSendrierBarreto’13]

مراجع

- C. Monico, J. Rosenthal, and A. Shokrollahi, “Using low density parity check codes in the McEliece cryptosystem,” in Proc. IEEE International Symposium on Information Theory (ISIT 2000), Sorrento, Italy, Jun. 2000, pp. 215.
- M. Baldi, F. Chiaraluce, R. Garello, and F. Mininni, “Quasi-cyclic low-density parity-check codes in the McEliece cryptosystem,” in Proc. IEEE International Conference on Communications (ICC 2007), Glasgow, Scotland, Jun. 2007, pp. 951–956.
- M. Baldi and F. Chiaraluce, “Cryptanalysis of a new instance of McEliece cryptosystem based on QC-LDPC codes,” in Proc. IEEE International Symposium on Information Theory (ISIT 2007), Nice, France, Jun. 2007, pp. 2591–2595.
- A. Otmani, J. P. Tillich, and L. Dallot, “Cryptanalysis of two McEliece cryptosystems based on quasi-cyclic codes,” in Proc. First International Conference on Symbolic Computation and Cryptography (SCC 2008), Beijing, China, Apr. 2008.
- M.K. Shooshtari, M. Ahmadian, A. Payandeh, “Improving the security of McEliece-like public key cryptosystem based on LDPC codes,’’ Advanced Communication Technology, 2009. ICACT 2009. 11th International Conference on , vol.02, pp.1050-1053, 2009.

مراجع

- M. Baldi, M. Bianchi, N. Maturo, F. Chiaraluce, “Improving the efficiency of the LDPC code-based McEliece cryptosystem through irregular codes,” In: Proceedings of IEEE symposium on computers and communications (ISCC 2013), Split, Croatia, 2013.
- R. Misoczki, J. Tillich, N. Sendrier, JP. Barreto, “MDPC-McEliece: New McEliece variants from Moderate Density Parity-Check codes,” in Proc. IEEE International Symposium on Information Theory (ISIT 2013), Istanbul, Turkey, 2013, pp. 2069–2073.
- M. Baldi, M. Bodrato, F. Chiaraluce, “A new analysis of theMcEliece cryptosystem based on QC-LDPC codes,’’ In: Security and cryptography for networks. Lecture notes in computer science, vol 5229, Springer, Berlin, 2008, pp 246–262.
- Iv. Maurich, T. Güneysu, “Lightweight code-based cryptography: QC-MDPC McEliece encryption on reconfigurable,” In Design, Automation & Test in Europe, DATE 2014 (25 March 2014).

با تشکر از توجه شما