قطب علمی رمز

بسم الله الرحمن الرحیم

دانشگاه صنعتی شریف

سامانه رمز McEliece و سیر تحول آن

حسین خیامی

آزمایشگاه تئوری اطلاعات و مخابرات امن

دانشگاه صنعتی شریف

h_khayami@ee.sharif.edu

فهرست مطالب

- مقدماتی از نظریه کدینگ
- مسائل سخت کدگشایی
- سامانه رمز کلید عمومی McEliece
- سامانه رمز کلید عمومی Niederreiter
- ویژگی های کد مناسب برای سامانه های رمز شبه McEliece
- کدهای استفاده شده در سامانه های رمز شبه McEliece

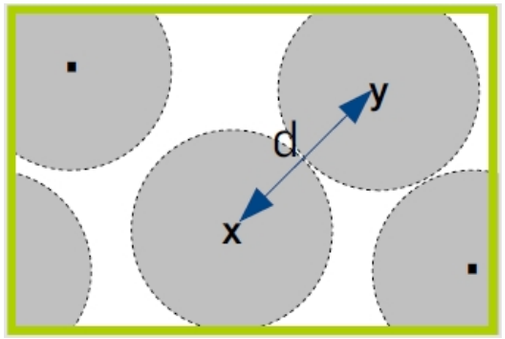
مقدماتی از نظریه کدینگ

مقدماتی از نظریه کدینگ

- یک کد باینری قالبی خطی C یک زیرفضای k بعدی از $\mathbb{F}_2^n$ است:

  - ماتریس مولد $G = \begin{bmatrix} 0/1 \end{bmatrix}_{k \times n}$ $\quad C = \{ m.G : m \in \mathbb{F}_2^k \}$

  - ماتریس توازن آزما $H = \begin{bmatrix} 0/1 \end{bmatrix}_{n-k \times n}$ $\quad C = \{ c.H^T = 0 : c \in \mathbb{F}_2^n \}$



- کمترین فاصله (Minimum distance)

  - $d = \min_{x \neq y \in C} \{ wt(x+y) \}$

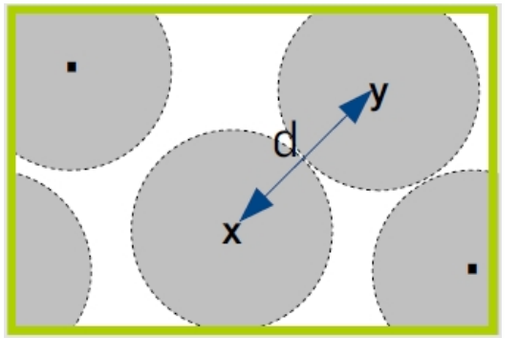
- کد $C\ (n,k,d)$ یک کد باینری قالبی خطی است.

مقدماتی از نظریه کدینگ

- یک کد باینری قالبی خطی C یک زیرفضای k بعدی از $\mathbb{F}_2{}^n$ است:

$$G.H^T = 0 \begin{cases} C = \{ m.G : m \in \mathbb{F}_2{}^k \} \\ C = \{ c.H^T = 0 : c \in \mathbb{F}_2{}^n \} \end{cases}$$

- قابلیت تصحیح خطا:



$$t = \left\lfloor \frac{d-1}{2} \right\rfloor$$

مسائل سخت کدگشایی

مسائل سخت کدگشایی

- مسئله کدگشایی عمومی
- مسئله کدگشایی با سندرم



[BerlekampMcElieceTilborg1978]

مسئله کدگشایی عام (General Decoding Problem)

- **مفروضات:** ماتریس باینری G، بردار باینری y، عدد صحیح نامنفی w
- **مسئله:** پیدا کردن بردار e با وزن همینگ w که $v = mG = y + e$
  - بردار e طول n دارد.
  - $w = wt(e) = \left\lfloor \frac{d-1}{2} \right\rfloor$
  - ماتریس G یک ماتریس $k * n$ است. (ماتریس مولد)
  - جستجو در میان 2^k راه حل ممکن

مسئله کدگشایی با سندرم (Syndrome Decoding)

- **مفروضات:** ماتریس باینری H، بردار باینری s، عدد صحیح نامنفی w
- **مسئله:** پیدا کردن بردار e با حداکثر وزن همینگ w که $e.H^T = s$
  - بردار s طول $n-k$ و بردار e طول n دارد.
  - ماتریس H یک ماتریس $(n-k) * n$ است. (ماتریس توازن آزما)

مسئله کدگشایی با سندرم (Syndrome Decoding)

- جستجو در میان 2^{n-k} راه حل ممکن

Syndrome ($n-k$ bit)	Coset leader ($v_0 = 0$)	$weight(e_i + v_i) > w$		
(00...00)	$e_0 = 0$	v_1	...	v_{2^k-1}
(00...01)	e_1	$e_1 + v_1$	...	$e_1 + v_{2^k-1}$
.	.	.	...	.
.	.	.	...	.
.	.	.	...	.
(11...11)	$e_{2^{n-k}-1}$	$e_{2^{n-k}-1} + v_1$	...	$e_{2^{n-k}-1} + v_{2^k-1}$

سامانه رمز کلید عمومی McEliece

رمزنگاری کلید عمومی McEliece

- بر اساس کدهای Goppa C (n,k,2t+1)
  - $t = 50$ $k = 524$ $n = 1024$

- دلایل استفاده از کدهای Goppa:
  - در سال ۱۹۷۸ جزو کدهای با الگوریتم سریع کدگشایی بود.
  - تعداد زیاد ماتریس های مولد متفاوت در خانواده

[McEliece1978]

رمزنگاری کلید عمومی McEliece

- **مرحله تولید کلید:**
  - **کلید خصوصی** : ماتریس های باینری S,G,P
    - $G_{k\times n}$: انتخاب تصادفی ماتریس مولد کد گوپا
    - $P_{n\times n}$:انتخاب تصادفی ماتریس جایگشت
    - $S_{k\times k}$: انتخاب تصادفی ماتریس ناویژه درهم ساز
  - **کلید عمومی:** G',t
    - $G'_{k\times n} = SGP$
    - t : قابلیت تصحیح خطای کد

[McEliece1978]

رمزنگاری کلید عمومی McEliece

❑ رمزگذاری:

$$c = mG' + e$$

- e بردار خطای عمدی به طول n و با وزن همینگ کمتر یا مساوی t

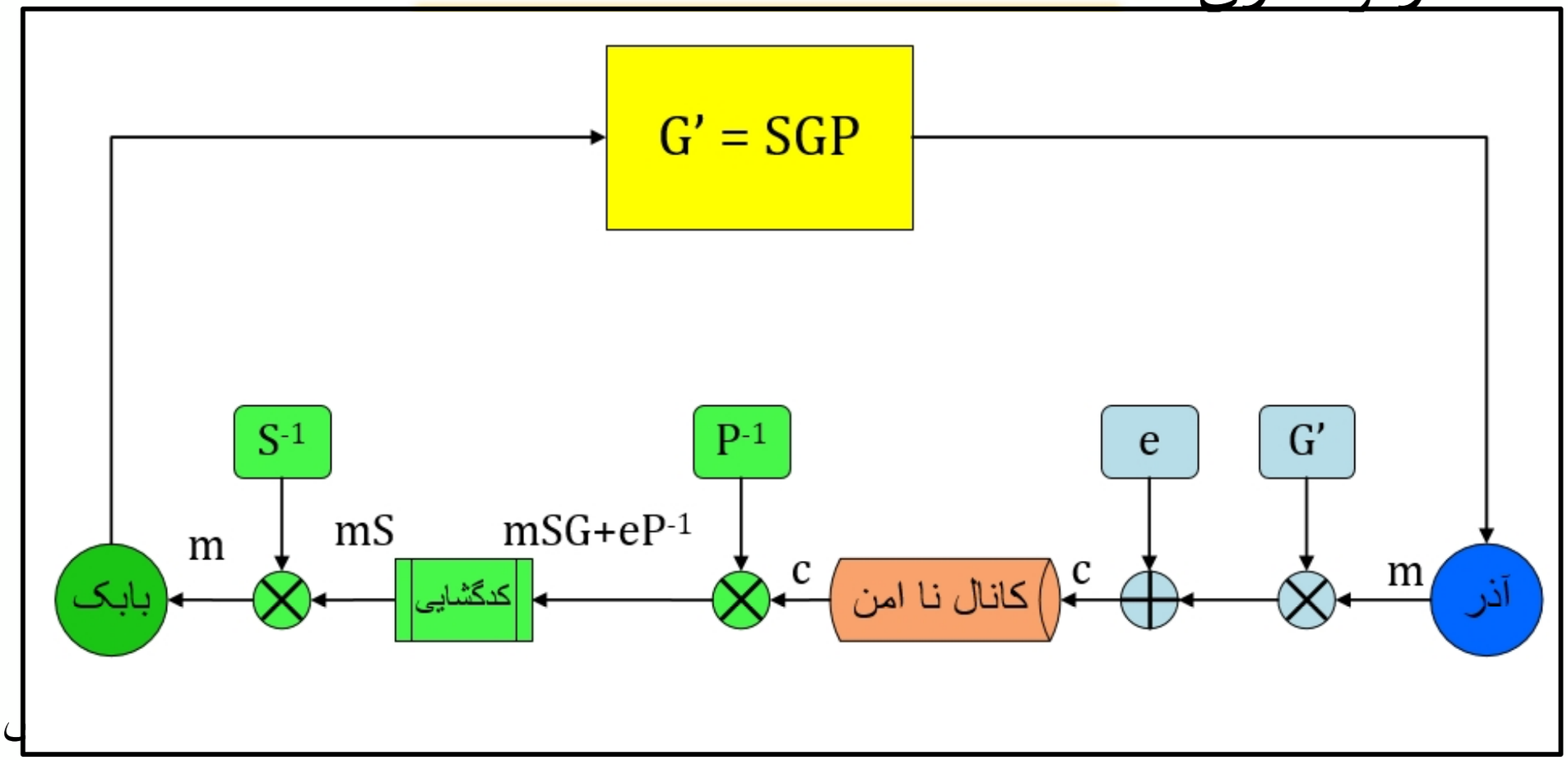
❑ رمزگشایی:

- $c' = cP^{-1} = (mG' + e)P^{-1} = (mSGP + e)P^{-1} = mSG + eP^{-1}$
- با الگوریتم کدگشایی پترسن خطا حذف و $m' = mS$ به عنوان خروجی
- $m = m'S^{-1}$

[McEliece1978]

رمزنگاری کلید عمومی McEliece

❑ رمزگذاری:



$m = m'S^{-1}$ ○

[McEliece1978]

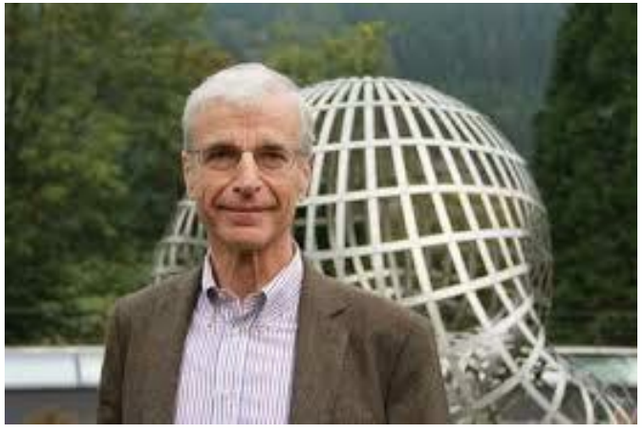
رمزنگاری کلید عمومی McEliece

- مزایا و معایب McEliece در مقایسه با RSA

پارامترها	McEliece	RSA
طول قالب اطلاعات(بیت)	۵۲۴	۱۰۲۴
طول کلید (بایت)	۶۷۰۷۲	۲۵۶
نرخ	۰.۵۱	۱
تعداد عملیات در رمزگذاری به ازای هر بیت	۵۱۴	۲۴۰۲
تعداد عملیات در رمزگشایی به ازای هر بیت	۵۱۴۰	۷۳۸۱۱۲

- RSA : شکست در برابر کامپیوتر های کوانتومی [Shor1994]
  - ✓ McEliece: مقاومت در برابر کامپیوتر های کوانتومی

سامانه رمز کلید عمومی Niederreiter



رمزنگاری کلید عمومی Niederreiter

- از نظر امنیت معادل با McEliece [Li et al.1994]
- سامانه مشابه با McEliece
- بر پایه سختی مسئله کدگشایی با استفاده از سندرم
- کد غیر باینری Reed-Solomon تعمیم یافته روی $GF(q)$

رمزنگاری کلید عمومی Niederreiter

❑ مرحله تولید کلید:

❑ کلید خصوصی : ماتریس های باینری S,H,P

- $H_{(n-k)\times n}$: انتخاب تصادفی ماتریس مولد کد گویا
- $P_{n\times n}$:انتخاب تصادفی ماتریس جایگشت
- $S_{(n-k)\times(n-k)}$: انتخاب تصادفی ماتریس ناویژه درهم ساز

❑ کلید عمومی: H',t

- $H'_{(n-k)\times n} = SHP$
- t : قابلیت تصحیح خطای کد

رمزنگاری کلید عمومی Niederreiter

❑ رمزگذاری:

- نگاشت متن اصلی به بردار های به طول n و وزن t
- $M = \varphi(m)$

$$c = MH'^T$$

❑ رمزگشایی:

- ضرب وارون ماتریس S^T از راست

$$c' = c.(S^T)^{-1} = MH'^T.(S^T)^{-1} = MP^T H^T S^T (S^T)^{-1}$$
$$= MP^T H^T$$

- کدگشایی مبتنی بر سندرم برای یافتن MP^T
- با ضرب ماتریس P از سمت راست M بدست می آید.
- عکس نگاشت: $m = \varphi^{-1}(M)$

رمزنگاری کلید عمومی Niederreiter

- طرح اولیه معرفی شده بر اساس کدهای Reed-Solomon تعمیم یافته نا امن بود.
[Wieschebrink2010][SidelnikovShestakov1992]

- بهبود: استفاده از کدهای Goppa

- در مقایسه با سامانه رمز McEliece در عملیات رمزگذاری و رمزگشایی یک نگاشت بیشتر دارد.

رمزنگاری کلید عمومی Niederreiter

- مزایا و معایب سامانه های Niederreiter و McEliece در مقایسه با RSA

پارامترها	McEliece	Niederreiter	RSA
طول قالب اطلاعات(بیت)	۵۲۴	۲۸۴	۱۰۲۴
طول کلید (بایت)	۶۷۰۷۲	۳۲۷۵۰	۲۵۶
نرخ	۰.۵۱	۰.۵۷	۱
تعداد عملیات در رمزگذاری به ازای هر بیت	۵۱۴	۵۰	۲۴۰۲
تعداد عملیات در رمزگشایی به ازای هر بیت	۵۱۴۰	۷۸۶۳	۷۳۸۱۱۲

- ✓ هر دو سامانه رمز McEliece و Niederreiter در برابر حملات کامپیوتر های کوانتومی مقاومند.

ویژگی های کد مناسب برای سامانه های رمز شبه McEliece

ویژگی های کد مناسب برای سامانه های رمز شبه McEliece

- زیاد بودن نرخ انتقال
- کلید عمومی با طول کوتاه
- دارای کدگشایی کارا
- خانواده کدهای متفاوت بزرگ

ویژگی های کد مناسب برای سامانه های رمز شبه McEliece

- زیاد بودن نرخ انتقال
  - نسبت k/n بزرگ باشد.
  - افزونگی کم ⟵ تصحیح خطای ضعیف ⟵ وزن بردار خطا کم

حمله کدگشایی

خانواده کد	نرخ
Goppa(1024,524,101)	0.51
QC-LDPC [Baldi 2013]	0.75

ویژگی های کد مناسب برای سامانه های رمز شبه McEliece

- امکان ذخیره (ارسال) کلید عمومی به صورت کارا و با طول کوتاه
  - ایده شبه چرخشی بودن ماتریس های مولد و توازن آزما
  - ماتریس شبه چرخشی متشکل از قالبهای دوری است.
  - برای ذخیره هر قالب دوری فقط یک سطر آن کافی است.

$$H = \begin{bmatrix} H_{0,0} & \cdots & H_{0,n_0-1} \\ \vdots & \ddots & \vdots \\ H_{r_0-1,0} & \cdots & H_{r_0-1,n_0-1} \end{bmatrix}_{r_0.p \times n_0.p}$$

  - قالبهای $p \times p$
  - طول کد $n = n_0.p$ و طول پیام یا بعد کد $k = k_0.p$

ویژگی های کد مناسب برای سامانه های رمز شبه McEliece

- دارای کدگشایی کارا باشد.

خانواده کد	الگوریتم کدگشایی
Goppa(1024,524,101)	Patterson
LDPC [Monico et al. 2000]	Belief Propagation

- خانواده کدهای متفاوت بزرگ داشته باشد.
  - کدهای $Goppa(1024,524)$: حدود 10^{149} کد
  - انواع خانواده های کدهای QC-LDPC
    - RDF-QC-LDPC [Baldi et al. 2013]

کدهای استفاده شده در سامانه های رمز شبه McEliece

کدهای استفاده شده در سامانه های رمز شبه McEliece

- Binary Goppa codes [McEliece78]
- Generalized Reed-Solomon [Nie86],[BCGO09]
- Binary Reed-Muller [Sidelnikov94]
- Algebraic-geometric [JanwaMoreno96]
- LDPC [Monico et al. 00]
- QC-LDPC [BCG06], [BC07], [BBC08], [BBC13]

کدهای استفاده شده در سامانه های رمز شبه McEliece

- BCH codes [Gab05]
- Quasi-Dyadic codes [MisoczkiBarreto09]
- Reed Solomon (RS) codes [BBCRS11]
- non- binary Goppa Codes(wild McEliece) [BLP11]
- Convolution Codes [LJ12]
- Rank metric [Gaborit et al.13]
- MDPC [Misoczki et al.13]

مراجع

[BMT78] Elwyn R. Berlekamp, Robert J. McEliece and Henk C. A. van Tilborg. "On the inherent intractability of certain coding problems", IEEE Transactions on Information Theory 24, pages 384-386 (1978)

[Mc78] Robert J. McEliece. "A public-key cryptosystem based on algebraic coding theory", Jet Propulsion Laboratory DSN Progress Report 42-44, pages 114-116 (1978)

[N86] Harald Niederreiter. "Knapsack-type cryptosystems and algebraic coding theory", Problems of Control and Information Theory 15, pages 159-166 (1986)

[SS92] Vladimir M. Sidel'nikov and Sergey O. Shestakov. "On insecurity of cryptosystems based on generalized Reed-Solomon codes", Discrete Mathematics and Applications 2, pages 439-444 (1992)

[S94] Vladimir M. Sidel'nikov "A public-key cryptosystem based on binary Reed-Muller codes", Discrete Mathematics and Applications 4, pages 191-207 (1994)

مراجع

[Sh94] Peter W. Shor. "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer". Proceedings of the 35th Annual Symposium on Foundations of Computer Science, Santa Fe, NM, Nov. pages 20-22, (1994)

[LDW94] Yuan Xing Li, Robert H. Deng and Xinmei Wang. "On the equivalence of McEliece's and Niederreiter's public-key cryptosystems", IEEE Transactions on Information Theory 40, pages 271-273 (1994)

[JM96] Heeralal Janwa and Oscar Moreno. "McEliece public key cryptosystems using algebraic-geometric codes", Designs, Codes and Cryptography 8, pages 293-307 (1996)

[CS98] Anne Canteaut and Nicolas Sendrier. "Cryptanalysis of the original McEliece cryptosystem", pages 187-199 in : Kazuo Ohta, Dingyi Pei (editors). Advances in cryptology-ASIACRYPT'98 (1998)

[MRS00] Monico, C.; Rosenthal, J.; Shokrollahi, A., "Using low density parity check codes in the McEliece cryptosystem," *Information Theory, 2000. Proceedings. IEEE International Symposium on* , vol., no., pp.215,, 2000

مراجع

[F04] Fossorier, M.P.C., "Quasicyclic low-density parity-check codes from circulant permutation matrices," *Information Theory, IEEE Transactions on* , vol.50, no.8, pp.1788,1793, Aug. 2004

[G05] P. Gaborit. Shorter keys for code based cryptography. In Proceedings of WCC 2005, pages 81–90, 2005.

[BCG06] Baldi, M.; Chiaraluce, F.; Garello, R., "On the Usage of Quasi-Cyclic Low-Density Parity-Check Codes in the McEliece Cryptosystem," *Communications and Electronics, 2006. ICCE '06. First International Conference on* , vol., no., pp.305,310, 10-11 Oct. 2006

[BCGM07] Baldi, M.; Chiaraluce, F.; Garello, R.; Mininni, F., "Quasi-Cyclic Low-Density Parity-Check Codes in the McEliece Cryptosystem," *Communications, 2007. ICC '07. IEEE International Conference on* , vol., no., pp.951,956, 24-28 June 2007

[BC07] M. Baldi, F. Chiaraluce, “Cryptanalysis of a new instance of McEliece cryptosystem based on QC-LDPC Codes”, Proc. IEEE International Symposium on Information Theory (ISIT 2007), pp. 2591-2595, Nice, France, 24-29 June 2007. ISBN: 978-1-4244-1397-3.

مراجع

[BBC08] M. Baldi, M. Bodrato, and F. Chiaraluce. A new analysis of the McEliece cryptosystem based on QCLDPC codes. In Security and Cryptography for Networks, volume 5229 of lecture Notes in Computer Science, pages 246–262. Springer Berlin , Heidelberg, 2008.

[BCGO09] Berger, T. P., Cayrel, P. L., Gaborit, P., & Otmani, A.. "Reducing key length of the McEliece cryptosystem."*Progress in Cryptology–AFRICACRYPT 2009*. Springer Berlin Heidelberg, 2009. 77-97.

[MB09] Misoczki, Rafael, and Paulo SLM Barreto. "Compact McEliece keys from Goppa codes." *Selected Areas in Cryptography*. Springer Berlin Heidelberg, 2009.

[W10] christian Wieschebrink. "Cryptanalysis of the Niederreiter Public Key Scheme Based on GRS Subcodes", pages 61-72 in Nicolas Sendrier (editor). Post-Quantum Cryptography, Third international workshop, PQCrypto 2010, Lecture Notes in Computer Science 6061, Springer

[BBCRS11]M. Baldi, M. Bianchi, F. Chiaraluce, J. Rosenthal, D. Schipani, “A variant of the McEliece cryptosystem with increased public key security”, Proc. 7th International Workshop on Coding and Cryptography (WCC 2011), Paris, France, 11-15 Apr. 2011.

مراجع

[BLP11] Daniel J. Bernstein, Tanja Lange, and Christiane Peters. Wild McEliece. In Alex Biryukov, Guang Gong, and Douglas Stinson, editors, Selected Areas in Cryptography, volume 6544 of Lecture Notes in Computer Science, pages 143–158. Springer-Verlag Berlin Heidelberg, 2011. ISBN 978-3-642-19573-0.

[LJ12] Löndahl, Carl, and Thomas Johansson. "A new version of McEliece PKC based on convolutional codes." Information and Communications Security. Springer Berlin Heidelberg, 2012. 461-470.

[BBMC13] Baldi, M.; Bianchi, M.; Maturo, N.; Chiaraluce, F., "Improving the efficiency of the LDPC code-based McEliece cryptosystem through irregular codes," *Computers and Communications (ISCC), 2013 IEEE Symposium on* , vol., no., pp.000197,000202, 7-10 July 2013

[GMRZ13] Gaborit, P., Murat, G., Ruatta, O., & Zémor, G. "Low rank parity check codes and their application to cryptography." International Workshop on Coding and Cryptography (WCC 2013). 2013.

[MTSB13] Misoczki, R.; Tillich, J.-P.; Sendrier, N.; Barreto, P.S.L.M., "MDPC-McEliece: New McEliece variants from Moderate Density Parity-Check codes," *Information Theory Proceedings (ISIT), 2013 IEEE International Symposium on* , vol., no., pp.2069,2073, 7-12 July 2013


با تشکر از توجه شما