پیچیدگی محاسباتی عملیات رمزنگاری و رمزگشایی سیستم‌های کلید همگانی McEliece و RSA

حسام محمدحسینی
بخش مهندسی برق و کامپیوتر
دانشگاه تربیت مدرس
hesam.mhosseini@gmail.com

پیام امانی
دانشکده مهندسی برق
دانشگاه صنعتیخواجه نصیرالدین طوسی
p_amani@ieee.org

احمدرضا شرافت
بخش مهندسی برق و کامپیوتر
دانشگاه تربیت مدرس
sharafat@isc.iranet.net

چکیده: در این مقاله پیچیدگی محاسباتی عملیات رمزنگاری/رمزگشایی سیستم‌های رمزنگاری کلید همگانی McEliece و RSA محاسبه و مقایسه شده‌اند. معیار محاسبه پیچیدگی، تعداد عملیات باینری لازم برای هر بار رمزنگاری/رمزگشایی یک قالب از اطلاعات در هر یک از سیستم‌ها در نظر گرفته شده است. با این معیار، مرتبه تعداد عملیات باینری لازم برای رمزنگاری/رمزگشایی در هر یک از سیستم‌های فوق به صورت تابعی از پارامترهای سیستم متناظر محاسبه شده است. نتایج محاسبات نشان می‌دهند که حجم عملیات (باینری) لازم برای هر بار رمزنگاری/ رمزگشایی یک قالب پیام در سیستم McEliece به مراتب کمتر از سیستم RSA است. با توجه به شباهت دیگر سیستم‌های رمزنگاری مبتنی بر تئوری کدینگ به سیستم McEliece، نتایج این مقاله را می‌توان به کمتر بودن حجم عملیات باینری لازم برای رمزنگاری/رمزگشایی در سیستم‌های رمزنگاری مبتنی کدینگ در مقایسه با سیستم‌های رمزنگاری مبتنی بر نظریه اعداد تعمیم داد. این ویژگی، چنین سیستم‌هایی را برای استفاده در کاربردهای نیازمند امنیت در شبکه‌ای با محدودیت توان پردازشی و یا محدودیت عمر باتری در گره‌ها، برای مثال در شبکه‌های بی‌سیم، مناسب می‌سازد؛ زیرا حمله رمزشکنی موثری به رمزنگاری مبتنی بر تئوری کدینگ موجود نیست. در پایان، نتایج بدست آمده را با نتایج مقالات موجود مقایسه و تفاوت آنها را توضیح داده‌ایم.

واژه‌های کلیدی: سیستم رمزنگاری McEliece، سیستم رمزنگاری RSA، رمزنگاری کلید همگانی، مرتبه محاسباتی.

۱- مقدمه

گسترش شبکه‌های ارتباطی منجر به پدید آمدن خواست‌ها، نیازها و چالش‌های جدید در زمینه امنیت در شبکه‌ها گردیده است. افزایش تعداد کاربران، گسترش تبادلات کاربران بر روی شبکه‌های ارتباطی عمومی، افزایش استفاده از شبکه‌های بی‌سیم و نیز تمایل به انجام انواع مبادلات، مانند انتقال اطلاعات بانکی از طریق این شبکه‌ها، از چالش‌های مبتلابه برای مسئوولین امنیتی شبکه‌ها و کشورها است.

از سیستم‌های رمزنگاری کلید عمومی با هدف ارائه راه حلی برای این چالش‌ها بوسیله تامین اعتبار یا امنیت در ارسال اطلاعات استفاده می‌شود. از طرفی، با توجه به حجم زیاد محاسبات و پردازش مورد نیاز در بیش‌تر سیستم‌های رمزنگاری کلید همگانی، استفاده از این سیستم‌ها در بیش‌تر شبکه‌ها، محدود به استفاده از آنها برای ارسال کلید به صورت امن می‌شود. در واقع، اطلاعات اصلی به کمک سیستم‌های رمز کلید خصوصی رمزنگاری می‌شوند که کلیدهای آن بوسیله یک رمزنگاری کلید همگانی، مانند RSA، در ابتدای ارتباط مبادله می‌شوند.

یکی از اولین روش‌های رمزنگاری کلید همگانی مطرح شده، سیستم رمزنگاری کلید همگانی McEliece است که در سال ۱۹۷۸ معرفی گردید[1]. امنیت بیش‌تر سیستم‌های رمزنگاری موجود، بر پیچیدگی حل مسایلی از نظریه اعداد، مانند تجزیه اعداد به عوامل اول و یا مساله لگاریتم گسسته، متکی شده است. در مقابل، امنیت سیستم McEliece، و دیگر سیستم‌های رمزنگاری ساخته شده بر اساس تئوری کدینگ، بر پیچیدگی عمل کدبرداری از یک کد خطی استوار است. در [2] نشان داده‌اند که عمل کدبرداری از یک کد خطی، بدون داشتن اطلاع خاصی در مورد ساختار کد، مانند ماتریس بررسی توازن یا ماتریس مولد آن، در حالت کلی یک مساله NP-complete است.

در مقالات و گزارش‌های متعددی ادعا شده که سیستم‌های رمزنگاری کلید همگانی مبتنی بر تئوری کدینگ از سیستم‌های رمزنگاری بر مبنای نظریه اعداد، و به طور خاص سیستم RSA، با معیار حجم و تعداد محاسبات مورد نیاز سریع‌تر هستند[5][4][3]. در این مقالات یک روش احتمالاتی برای یافتن کلمات کد با وزن کم در یک کد خطی بزرگ مطرح شده است. به علاوه جدولی از مقایسه سیستم‌های رمزنگاری RSA، McEliece، و Niederreiter [6] نیز ارائه گردیده است که نشان دهنده سریع‌تر بودن عملیات رمزنگاری و رمزگشایی سیستم McEliece و Niederreiter [6] در مقایسه با سیستم RSA است.

در این مقاله، تعداد عملیات باینری لازم برای رمزنگاری و رمزگشایی سیستم McEliece و سیستم RSA محاسبه و مقایسه می‌شوند. نتایج بدست آمده تایید می‌کنند که عملیات رمزنگاری و رمزگشایی در سیستم رمزنگاری کلید همگانی McEliece، در مقایسه با سیستم RSA، تعداد عملیات باینری به مراتب کمتری دارد. به طور تقریبی، و برای پارامترهای ذکر شده در مورد دو سیستم، عملیات رمزنگاری در حدود 17 و عملیات رمزگشایی در حدود 23.5 بار در سیستم McEliece سریعتر از سیستم RSA هستند (به جدول ۲ و ۳ نگاه کنید).

ساختار مقاله به شرح زیر است. در بخش ۲ سیستم McEliece را معرفی می‌کنیم. سپس توضیح کوتاهی در مورد کلیات سیستم رمزنگاری RSA و مرتبه تعداد محاسبات مورد نیاز آن در بخش ۳ ارائه می‌کنیم. در بخشهای ۴ و ۵ به ارائه نتایج در مورد مرتبه محاسباتی، و تعداد عملیات باینری لازم در سیستم McEliece، و مقایسه آنها در دو سیستم McEliece و RSA می‌پردازیم. بخش ۶ به مقایسه و بررسی نتایج به دست آمده در این مقاله با نتایج [3] اختصاص یافته است. در این بخش دلیل اختلاف نتایج برای سیستم‌های یکسان، و با پارامترهای مشابه، را بیان کرده‌ایم. سرانجام، بخش ۷ حاوی نتیجه‌گیری و ارائه پیشنهاد برای مطالعات بعدی است.

۲- سیستم McEliece

در این سیستم، کلید عمومی، یک ماتریس $k \times n$ به نام $\mathbf{G}'$ است. کلید خصوصی شامل ماتریسهای $\mathbf{G}_{k\times n}$، ماتریس جایگشت $\mathbf{P}_{n\times n}$ و ماتریس چگال[1] ناویژه[2] $\mathbf{S}_{k\times k}$ است. ماتریس $\mathbf{G}$ مولد یک کد گوپا با پارامترهای (n,k,t) است، که n تعداد بیت‌های ارسالی، k تعداد بیت‌های اطلاعات و t توانایی تصحیح خطای کد است. این کد خطی، یکی از زیرفضاهای k بعدی فضای n بعدی را تولید می‌کند. برای کدبرداری از این کد، الگوریتمی با مرتبه محاسباتی چندجمله‌ای، با $O(nt)$، وجود دارد[7][1]. کلید همگانی با ضرب ماتریسهای $\mathbf{G}$، $\mathbf{S}$، و $\mathbf{P}$ در هم حاصل می‌شود

$$\mathbf{G}' = \mathbf{S} \times \mathbf{G} \times \mathbf{P} \qquad (۱)$$

در ادامه، فرایند رمزنگاری و رمزگشایی در این سیستم را معرفی می‌کنیم.

- رمزنگاری

به منظور رمزنگاری، پیام را به بردارهای k بیتی $\mathbf{m}$ تقسیم می‌کنیم. متن رمزشده $\mathbf{c}$ از کدگذاری بردار $\mathbf{m}$ بوسیله G' و سپس افزودن بردار خطای تصادفی $\mathbf{e}$ با وزن همینگ t به آن حاصل می‌شود.

$$\mathbf{c}=\mathbf{m}\mathbf{G}'+\mathbf{e},\qquad \mathrm{w_h}(\mathbf{e})=t \tag{۲}$$

- رمزگشایی

رمزگشائی از بردار دریافتی $\mathbf{c}$، به ترتیب زیر انجام می‌پذیرد. ابتدا متن رمزشده از سمت راست در معکوس ماتریس جایگشت، یعنی $\mathbf{P}^{-1}$، ضرب می‌شود.

$$\mathbf{c}'=\mathbf{c}\times\mathbf{P}^{-1}=\mathbf{m}\times\mathbf{S}\times\mathbf{G}+\mathbf{e}\times\mathbf{P}^{-1}=\mathbf{m}\times\mathbf{S}\times\mathbf{G}+\mathbf{e}' \tag{۳}$$

با توجه به اینکه معکوس هر ماتریس جایگشت هم، ماتریس جایگشت است، بردار $\mathbf{e}'$ جایگشتی از $\mathbf{e}$ است، بنابراین $\mathbf{e}'$ هم بردار خطایی با وزن همینگ t است.

کد گوپا استفاده شده، قابلیت تصحیح t خطا در هر قالب n بیتی را دارد، پس با انجام عمل کدبرداری از $\mathbf{c}'$ بردار $\mathbf{c}''$ بدست می‌آید ، یعنی

$$\mathbf{c}''_{1\times k}=\mathbf{m}\times\mathbf{S} \tag{۴}$$

با توجه به (۴)، برای بدست آوردن متن اصلی باید $\mathbf{c}''_{1\times k}$ را از سمت راست در معکوس ماتریس $\mathbf{S}$ ضرب کرد. پس

$$\mathbf{m}=\mathbf{c}''_{1\times k}\times\mathbf{S}^{-1} \tag{۵}$$

۳- سیستم RSA و مرتبه محاسباتی آن

در سیستم رمزنگاری RSA ابتدا دو عدد اول بزرگ p و q انتخاب و مقدار $n=pq$ محاسبه می‌شود. برای انتخاب کلیدها، باید مقدار $\phi(n)$ محاسبه شود که در آن تابع $\phi(n)$، تابع اولر است. عدد e، یعنی کلید همگانی، را به نحوی انتخاب می‌کنیم که

$$(\phi(n),e)=1 \tag{۶}$$

پس از آن d، یعنی کلید خصوصی، به صورت معکوس e در پیمانه $\phi(n)$ محاسبه می‌شود. بنابراین

$$ed\equiv 1 \mod \phi(n) \tag{۷}$$

که n و e به‌عنوان کلیدهای همگانی و d و $\phi(n)$ به‌عنوان کلیدهای خصوصی، مخفی نگاه داشته می‌شوند[9]. می‌دانیم مرتبه محاسباتی $b^n \bmod m$ برابر $\log(n)\log^2(m)$ است [10][9].

برای رمزنگاری و رمزگشایی در سیستم RSA، به جای بردار باینری پیام (یعنی $\mathbf{m}$)، از عددی که نشان‌دهنده آن بردار باینری در مبنای ده است (یعنی m) استفاده می‌شود. برای رمزنگاری در سیستم RSA باید مقدار $c\equiv m^e \bmod n$ محاسبه شود. لذا مرتبه محاسباتی آن برابر $\log(e)\log^2(n)$ است.

برای رمزگشائی، گیرنده باید از متن رمز شده دریافتی c به ترتیب زیر متن اصلی را بدست آورد

$$c'\equiv c^d \bmod n\equiv m^{ed}\equiv m^{\phi(n)+1}\equiv m \bmod n \tag{۸}$$

بنابراین مرتبه محاسباتی آن برابر $\log(d)\log^2(m)$ است.

۴- مرتبه محاسباتی سیستم McEliece

اکنون به مرور مرتبه محاسباتی تعدادی از عملیات ماتریسی مورد استفاده در سیستم McEliece، برای ماتریسهای باینری و از مرجع [8]، می‌پردازیم. جهت ضرب ماتریس $\mathbf{A}_{n\times m}$ در ماتریس $\mathbf{B}_{m\times k}$، یعنی $\mathbf{A}_{n\times m}\times\mathbf{B}_{m\times k}$، انجام عملیات باینری از مرتبه (m جمع + m ضرب)$n\times k$ لازم است. برای محاسبه ماتریس معکوس ماتریس $\mathbf{A}_{n\times n}$، یعنی $\mathbf{A}^{-1}$، مرتبه عملیات باینری مورد نیاز برابر n^3 است، یعنی

$$O(\mathbf{A}^{-1})=n^3 \tag{۹}$$

با توجه به مطالب بخش۲ برای رمزنگاری و رابطه (۲) داریم

$$O(\text{رمزنگاری})=\ (\text{ضرب } k+\text{جمع } k)\,n+\text{جمع } n)\qquad \approx nk \tag{۱۰}$$

برای بدست آوردن مرتبه عملیات رمزگشائی باید به ترتیب مرتبه عملیات‌های (۳)، (۴) و (۵) را بدست آوریم. انجام (۳)، شامل عملیات باینری از مرتبه n^2 است. برای بدست آوردن $\mathbf{c}''$ از $\mathbf{c}'$، یعنی کدبرداری از $\mathbf{c}'$، تعداد عملیات مورد نیاز از مرتبه nt است[7][1]. همچنین مرتبه محاسباتی بدست آوردن

m از **c''** برابر k^2 است. بنابراین تعداد عملیات لازم برای رمزگشائی در حدود n^2+nt+k^2 است.

۵- مقایسه دو سیستم

نتایج حاصل از بخش ۳ و ۴ را در جدول ۱ نشان داده‌ایم. چون محاسبه d برای n های بزرگ، پیچیده است، با فرض‌های زیر، کران بالائی را برای عملیات رمزگشائی RSA محاسبه کرده‌ایم که در جدول ۱ ذکر شده است.

مرتبه محاسباتی عملیات رمزنگاری و رمزگشائی برابر است با

$$\begin{aligned}(\log(e)\log^2(n)) + \log(d)\log^2(n) &= \\ &= \log^2(n)(\log(e)+\log(d)) \\ &= \log^2(n)(\log(\phi(n)+1) \\ &< \log^3(n)\end{aligned} \qquad (۱۱)$$

بنابراین

$$\begin{aligned}O(\text{رمزگشایی}) &< \log^3(n) - \log(e)\log^2(n) \\ &< \frac{\log^3(n)}{\log(e)}\end{aligned} \qquad (۱۲)$$

جدول ۲، عملیات لازم برای رمزنگاری و رمزگشائی هر بیت ارسالی و نیز مشخصات دیگر دو سیستم را بر حسب پارامترهای آنها نشان می‌دهد. طول کلید همگانی سیستم McEliece برابر $k\times n$ بیت است. Tilborg روشی را برای کاهش اندازه آن تا $k\times(n-k)$ مطرح نمود [11]. از این نکته در سطر اول جدول ۲ استفاده شده است.

برای $(n=1024, k=524, t=50)$ در سیستم کلید همگانی McEliece، ، تعداد عملیات باینری لازم در جدول ۳ آمده است. برای سیستم RSA با مقدار e (نمای همگانی (کلید همگانی)) برابر 17، مقادیر در جدول ۳ نشان داده شده‌اند. همان‌طور که در جدول ۳ می‌بینیم، تعداد عملیات رمزنگاری و رمزگشایی در سیستم رمزنگاری کلید همگانی McEliece، در مقایسه با سیستم RSA، به مراتب کمتر است. به طور تقریبی، و برای مقادیر پارامترهای ذکر شده در مورد دو سیستم، عملیات رمزنگاری در حدود 17 بار و عملیات رمزگشایی در حدود 23.5 بار در سیستم McEliece سریعتر از سیستم RSA هستند. در بخش بعدی به مقایسه نتایج بدست آمده با مقالات موجود در این زمینه می‌پردازیم.

۶- مقایسه نتایج با مقالات پیشین

در بخش‌های قبلی این مقاله، ابتدا به صورت نظری مرتبه عملیات باینری مورد نیاز برای هر بار رمزنگاری و رمزگشایی در سیستم‌های رمزنگاری کلید همگانی McEliece و RSA را به صورت پارامتری بدست آوردیم. سپس، و برای درک بهتر میزان کارایی سیستم McEliece، مقایسه‌ای بین دو نمونه از هر یک این سیستم‌ها، ارائه شد. اکنون نتایج این مقاله را با نتایج مقاله [3]، برای مقادیر مشابه پارامترهای دو سیستم، که در محاسبه مقادیر جدول ۳ به آنها اشاره شد، مقایسه می کنیم.

با توجه به اینکه در این مقاله، تعداد عملیات مورد نیاز برای رمزنگاری و رمزگشایی برای هر بیت اطلاعات ارسالی محاسبه گردیده، انتظار داریم که در مورد سطرهای چهارم و پنجم جدول، مقادیر محاسبه شده در این مقاله، از مقادیر گزارش شده در [3] بزرگ‌تر باشد. این موضوع در مورد مرحله رمزگشایی درست نیست. در جدول ۴ مشاهده می‌شود که در مقاله [3]، تعداد ۵۱۴۰ عملیات باینری محاسبه شده است در حالی که با محاسبات مطرح شده در این مقاله، این مقدار در حدود ۲۶۲۳ عملیات باینری بدست می‌آید.

جدول ۱: مقایسه مرتبه عملیات رمزنگاری و رمزگشایی.

سیستم رمزنگاری	McEliece	RSA
رمزنگاری	$O(nk)$	$O(\log(e)\log^2(n))$
رمزگشائی	$O(n^2+nt+k^2)$	$< O(\frac{\log^3(n)}{\log(e)})$

جدول ۲: مقایسه بعضی پارامترها در دو سیستم رمزنگاری.

	McEliece	RSA
طول کلید همگانی	$n\times(n-k)$	$\log(n)+\log(e)$
نرخ ارسال	$\frac{k}{n}$	1
عملیات لازم برای رمزنگاری یک بیت	n	$\log(e)\log(n)$
عملیات لازم برای رمزگشائی یک بیت	$\frac{n^2+nt+k^2}{k}$	$< \frac{\log^2(n)}{\log(e)}$

جدول ۳: نتایج عددی حاصل به ازای مقادیر پارامترهای بیان شده برای سیستم McEliece و سیستم RSA.

	McEliece [1024,524,101] کد گوپای باینری	RSA 1024 Modulus, Public exponent = 17
اندازه کلید عمومی	64000 بایت	1024+17 بیت
تعداد بیتهای اطلاعات ارسالی در هر بار رمزنگاری	524	1024
نرخ ارسال	51.17%	100%
تعداد عملیات دودوئی لازم برای رمزنگاری به ازای هر بیت اطلاعات	1024	17408
تعداد عملیات دودوئی لازم برای رمزگشائی به ازای هر بیت اطلاعات	2623	61680

جدول ۴ : مقایسه نتایج این مقاله با نتایج [3].

	نتایج [3]	نتایج این مقاله
اندازه کلید عمومی	67072 بایت	64000 بایت
تعداد بیتهای اطلاعات ارسالی در هر بار رمزنگاری	512	524
نرخ ارسال	51.17%	51.17%
تعداد عملیات دودوئی لازم برای رمزنگاری به ازای هر بیت اطلاعات	514	1024
تعداد عملیات دودوئی لازم برای رمزگشائی به ازای هر بیت اطلاعات	5140	2623

۷- نتیجه‌گیری و زمینه‌های پژوهشی آتی

با محاسبه پیچیدگی محاسباتی عملیات رمزنگاری و رمزگشائی سیستمهای رمزنگاری کلید عمومی McEliece و RSA، و مقایسه نتایج حاصل، مشاهده گردید که سرعت سیستم McEliece با معیار تعداد محاسبات، از RSA به مراتب بیشتر است. در حالت کلی، تعداد عملیات باینری لازم برای رمزنگاری/رمزگشایی در سیستم‌های رمزنگاری مبتنی بر نظریه کدینگ، در مقایسه با سیستم‌های رمزنگاری مبتنی بر نظریه اعداد کمتر است. این مزیت، سیستم‌های رمزنگاری کلید عمومی مبتنی بر تئوری کدینگ را برای کاربردهائی که در انها توان پردازشی و/یا عمر باتری تجهیزات ارتباطی محدودیت دارد، مانند شبکه‌های بی‌سیم، مناسب ساخته است.

همچنین، به اختلاف موجود بین نتایج [3] و نتایج این مقاله اشاره نمودیم. به طور خاص برای تعداد عملیات رمزگشایی، این اختلاف قابل قبول نیست و صحت نتایج [3] مورد تردید است. گر چه مطالعه و پژوهش در زمینه سیستم McEliece، و دیگر سیستم‌های رمزنگاری کلید همگانی مبتنی بر نظریه کدینگ، با هدف افزایش امنیت سیستم در آنها در حال انجام است [13][12]، تلاش برای ارائه حملات جدید به سیستم‌های مبتنی بر نظریه کدینگ به منظور کاهش تعداد عملیات مورد نیاز برای شکستن سیستم نیز مورد توجه قرار گرفته است [15][14][13]. مطالعه برای کوچک نمودن اندازه کلیدهای عمومی و خصوصی از محورهای دیگر پژوهشی است[12].

سپاسگزاری

این پژوهش طبق قرارداد شماره ۵۰۰۷۰۹۹/ت تحت حمایت مرکز تحقیقات مخابرات ایران انجام شده است. بدین وسیله از حمایت‌های آن مرکز تقدیر و سپاسگزاری می‌شود.

۸- مراجع

[1] R. J. McEliece, “A public-key cryptosystem based on algebraic coding theory,” *Deep Space Network Progress Report 42-44,* Jet Propulsion Laboratory, California Institute of Technology, 1978, pp. 114-116.

[2] E. R. Berlekamp, J. R. McEliece and H. van Tilborg, “On the inherent intractibility of certain coding problems,” in *IEEE Trans. Info. Theory*, vol. 24, pp.384-386, May 1978.

[3] A. Canteaut and N. Sendrier, “Cryptanalysis of the original McEliece cryptosystem,” in *Advances in Cryptology – ASIACRYPT98*, LNCS 1514, pp.187-199, 1998.

[4] A. Canteaut and F. Chabaud, “A new algorithm for finding minimum-weight words in a linear code: application to McEliece’s cryptosystem and to narrow-sense BCH codes of length 511,” in *IEEE Transaction on Information Theory*, vol. 44, no. 1, pp. 367-378, January 1998.

[5] B. Schneier, *Applied Cryptography*, Wiley, 2nd ed., 1996.

[6] H. Niederreiter, "Knapsack-type cryptosystem and algebraic coding theory," *Problems of Control and Information theory*, vol. 15, no. 2, pp. 159-166, 1986.
[7] R. J. McEliece, *The Theory of Information and Coding*, Addison-Wesley, 1977. also 2nd edition, Cambridge University, 2002.
[8] T. H. Cormen, C. E. Leiserson, and R. L. Rivest, *Introduction to Algorithms*, McGraw-Hill, 1989.
[9] N. Koblitz, *A Course in Number Theory and Cryptography*, Springer-Verlag, 1987.
[10] N. Koblitz, *Algebraic Aspects of Cryptography*, Springer-Verlag, 1998.
[11] J. van Tilburg, "On the McEliece cryptosystem," in *Advances in Cryptology-CRYPTO '88 Proceedings*, Springer-Verlag, pp. 119-131,1990.
[12] T. Berger and P. Loidreau, "How to mask the structure of codes for a cryptographic use," *Designs, Codes and Cryptography*, vol.35, pp.63-79, 2005.
[13] P. Loidreau, "Strengthening McEliece public-key cryptosystem," In *Advances in Cryptology - ASIACRYPT 2000*, no.1976 in LNCS, pp. 585-598. Springer-Verlag, December 2000.
[14] K. Kobara and H. Imai, "New chosen-plaintext attack on the one-wayness of the modified McEliece PKC proposed at asiacrypt 2000," in *PKC'2002*, D. Naccache and P. Paillier (eds), LNCS2248, Springer-Verlag, pp. 237–251, 2002.
[15] T. Berger and P. Loidreau, "Designing an efficient and secure public-key cryptosystem based on reducible rank codes," *Proceedings of Indocrypt 2004*, LNCS 3348, pp. 218-229.

---

1 Dense
2 Non-Singular