مروری بر سیستم‌های رمزنگاری کلید همگانی مبتنی بر تئوری کدینگ

حسام محمد حسینی و احمدرضا شرافت

بخش برق، دانشکده فنی و مهندسی، دانشگاه تربیت مدرس، صندوق پستی ۴۸۳۸-۱۴۱۵۵، تهران، ایران

{h_mhosseini@modares.ac.ir, sharafat@isc.iranet.net}

چکیده – در این مقاله به مرور کارهای انجام پذیرفته در زمینه سیستم‌های رمزنگاری کلید همگانی مبتنی بر تئوری کدینگ می‌پردازیم. با توجه به سریع‌تر بودن عملیات رمزنگاری و رمزگشایی در این سیستم‌ها، در مقایسه با دیگر انواع سیستم کلید همگانی، به نظر این سیستم‌ها جایگزین مناسبی برای استفاده به جای سیستم‌های فعلی رمزنگاری کلید همگانی هستند. به خصوص در مواردی مانند شبکه-های بی‌سیم که حجم پردازش و توان در دسترس تجهیزات کاربران محدود است، این برتری می‌تواند بسیار مفید و حیاتی باشد. در انتها مباحث و محورهایی برای مطالعه و پژوهش‌های آتی پیشنهاد می‌شود.

کلید واژه- تئوری کدینگ، رمزنگاری کلید همگانی، سیستم رمزنگاری McEliece، سیستم‌های رمزنگاری مبتنی بر تئوری کدینگ، کدهای تصدیق هویت.

۱- مقدمه

با توجه به پیشرفت سیستم‌های مخابراتی و شبکه‌های کامپیوتری در دهه‌های اخیر تقاضا برای سیستم‌های مطمئن، امن هر روز بیشتر می‌گردد. پیشرفت در فناوری‌ها و سخت‌افزار و نرم‌افزار مورد نیاز، منجر به پیدایش شبکه-های ارتباطی جدیدی گردیده است. برای مثال شبکه‌ها و تجهیزات کامپیوتری بی‌سیم، به دلیل سهولت و سادگی استفاده به همراه مزیت‌های دیگر، مورد توجه کاربران قرار گرفته اند.

در هر ارتباط مخابراتی، با توجه به عبور اطلاعات از یک کانال با نویز، نیاز به انجام عملیات تشخیص و تصحیح خطا داریم. این نیاز در شبکه‌ها با زیر ساخت سیمی و بی‌سیمی با هم متفاوت است. دلیل این موضوع احتمال خطای متفاوت دو نوع کانال است. در مورد امنیت اطلاعات ارسالی نیز تفاوت جدی بین دو حالت سیمی و بی سیم وجود دارد. در شبکه‌های سیمی تنها در صورت دسترسی دشمن به محیط انتقال اطلاعات، مراکز سوئیچ و سایر زیرساخت‌ها، امنیت سیستم مخدوش می‌گردد. در مقابل، به دلیل استفاده از کانال فضای آزاد امکان شنود اطلاعات، جعل و تکرار پیام از طرف دشمن سیستم‌های بی‌سیم در مقایسه با سیستم‌های سیمی بیش‌تر است. پس در ارتباطات بی‌سیم، به کارگیری الگوریتم‌های رمزنگاری برای تامین امنیت و اعتبار به عنوان یک نیاز پایه الزامی است. بسیاری از کاربردهای رو به گسترش و تازه، مانند بانک‌داری الکترونیکی، ارتباطات در دولت الکترونیک و مانند اینها، نیاز به ارسال امن اطلاعات دارند.

سیستم‌های موجود از بلوک‌های رمزنگاری و کدینگ کانال به طور جداگانه برای برآورده ساختن خواسته‌های مذکور استفاده می‌نمایند. در بلوک کدینگ کانال با اضافه کردن بیت‌های افزونگی[1] به اطلاعات اصلی، این امکان فراهم می‌شود تا در گیرنده بتوان به کمک این بیت‌ها عمل

تشخیص یا تصحیح خطا را انجام داد. به این بیت‌ها، بیت-های بررسی توازن[۲] نیز می‌گویند. در بلوک رمزنگاری با توجه به اینکه هر بیت از متن رمز شده می‌تواند اطلاعاتی در مورد کلید به دشمن بدهد، سعی بر این است که تا حد ممکن از گسترش اطلاعات در روند رمزنگاری جلوگیری نمود. لذا این دو بلوک در تقابل با یکدیگر عمل می‌کنند.

بخش امنیت غالبا در لایه‌های بالای پروتکل‌های انتقال اطلاعات قرار دارد، در حالی‌که کدهای تصحیح خطا در لایه‌های پایین این پروتکل‌ها به کار گرفته می‌شوند. بنابراین ممکن است اطلاعات ارسالی که در فرستنده رمز شده‌اند در عبور از واسطهای مختلف با کدهای تصحیح خطای متفاوتی، بر حسب پروتکل‌های مورد استفاده بین واسطهای میانی، مواجه شود ولی تنها در مقصد نهایی است که رمزگشایی می‌گردد.

با توجه به بار محاسباتی و زمان مورد نیاز در هر بار اجرای عملیات رمزنگاری و رمزگشایی در الگوریتم‌های رمزنگاری کلید همگانی، بحث تامین امنیت و اعتبار یک چالش جدی به نظر می‌رسد. یکی از دلایل عدم جایگزینی کامل سیستم-های کلید همگانی همین حجم زیاد پردازش و محاسبات لازم در مراحل رمزنگاری و رمزگشایی در این سیستم‌ها است. سیستم‌های رمزنگاری کلید همگانی مبتنی بر تئوری کدینگ از این لحاظ نسبت به دیگر سیستم‌های رمزنگاری کلید همگانی برتری دارند[2][1] [۳]. تولید کلیدها نیز در این سیستم در مقایسه با RSA بسیار ساده‌تر است[4].

در ادامه به ترتیب زیر به ارائه مطالب می‌پردازیم. در بخش ۲ به معرفی سیستم‌های رمزنگاری کلید همگانی متکی بر تئوری کدینگ برای تامین امنیت می‌پردازیم. بخش ۳ به تامین اعتبار و امضای دیجیتال به کمک همین سیستم‌ها اختصاص یافته است. در بخش ۴ نیز به جمع‌بندی مباحث مطرح شده و پیشنهاد برای مطالعات آتی تخصیص داده‌ایم.

۲- سیستم‌های رمزنگاری کلید همگانی مبتنی بر تئوری کدینگ برای تامین امنیت

پس از معرفی سیستم‌های رمزنگاری کلید همگانی توسط Diffie و Hellman [5] الگوریتم‌های متنوعی برای پیاده سازی این ایده مطرح گردید. برای مثال سیستم RSA، که امنیت در آن متکی به پیچیدگی تجزیه اعداد بزرگ به عوامل اولشان است، در سال ۱۹۷۸ معرفی شد. محاسبه لگاریتم گسسته، مساله کوله پشتی و محاسبه معکوس چندجمله‌ای در میدان‌های محدود، پایه‌های دیگری بودند که بر مبنای آن‌ها سیستم‌های کلید همگانی متعددی مطرح گردید. اما با پیدایش و گسترش روش‌های تجزیه و تحلیل رمز[۳] (رمزشکنی)، اکثر این روش‌ها امنیت خود را از دست دادند. تنها دو روش متکی به تجزیه به عوامل اول و لگاریتم گسسته همچنان مقاوم مانده‌اند[1][6].

درمقابل، گروهی از سیستم‌های رمزنگاری کلید همگانی بر پایه پیچیدگی عمل کدبرداری کدهای خطی،که اولین بار توسط McElliece [7] معرفی گردید، همچنان در برابر رمزشکنی مقاومت کرده‌اند. مقاومت این دسته بر مبنای پیچیدگی عمل کدبرداری یا به صورت معادل عمل یافتن کلمات کدی با حداقل وزن در کدهای خطی بزرگ، که دارای ساختار مشخصی برای دشمن نباشند، متکی است. Berlekamp، McEliece و van Tilborg [8] نشان داده‌اند که کدبرداری یک کد خطی کلی یک مساله کلاس NP[4] است.

سیستم McEliece و Niederreiter [9]، که از نظر امنیت مشابهند[10]، دو دسته مهم از این گروه هستند. همچنین به دلیل اینکه عملیات رمزنگاری و رمزگشایی این گروه در مقایسه با سیستم‌های کلید همگانی متکی بر نظریه اعداد سریع‌تر انجام می‌شود[2][1] [۳] ، نیز مورد توجه هستند. هنگامی که هیچ اطلاعی به جز کلید همگانی، در مورد ساختار کد در دست نباشد، تنها روش برای یافتن کلمات کد با وزن کم بدست آوردن تمام کلمات کد ممکن است. بدیهی است این روش زمانی که پارامترهای کد بزرگ باشند غیر ممکن[۵] می‌گردد.

در سال McEliece۱۹۷۸ سیستم رمزنگاری خود را بر پایه کدهای گوپا مطرح نمود[11]. پس از آن Niederreiter یک سیستم رمزنگاری کلید همگانی متکی بر کدهای جبری را با استفاده از کدهای عمومی شده Reed-Solomon را در

سال ۱۹۸۶ معرفی کرد[9]. آنگاه Gabidulin در سال ۱۹۹۱ یک سیستم رمزنگاری کلید همگانی متکی بر کدهای جبری با استفاده از کدهای Gabidulin را ارائه کرد. سیستم Niederreiter در سال ۱۹۹۲ توسط Sidelnikov و Shestakov شکسته شد. پس از آن Sidelnikov یک سیستم رمزنگاری کلید همگانی متکی بر کدهای جبری با استفاده از کدهای Reed-Muller را ارائه نمود[12].

سیستم McEliece از وجود یک دسته خاص از کدهای کنترل خطا، که کدهای گوپا[۶] [7][13] نامیده می‌شوند، استفاده می‌کند. ساختار کد گوپا با ضرب ماتریس مولد آن در یک ماتریس جایگشت از دشمن مخفی می‌گردد. الگوریتم سریعی برای کدبرداری کدهای گوپا موجود است[11][7]، ولی کدبرداری یک کد خطی کلی یک مساله NP است[14]. این سیستم تنها توانایی ایجاد امنیت برای اطلاعات ارسالی را دارد و به کمک آن نمی‌توان به بررسی اعتبار، و امضای دیجیتال، پرداخت. سیستم McEliece اولین سیستم کلید همگانی است که از تصادفی سازی[۷] در فرایند رمزگذاری استفاده می‌کند که این از نظر محاسباتی بسیار کارآمد است و به مقاومت سیستم در مقابل حمله‌ها می‌افزاید[15]. بعضی الگوریتم McEliece را مشابه مساله کوله‌پشتی دانسته‌اند، اما Adams و Meijer [16] نشان دادند که این برداشت صحیح نیست.

سیستم‌های رمزنگاری کلید همگانی حالتی کلی‌تر از سیستم‌های رمزنگاری کلید خصوصی هستند؛ به این معنی که می‌توان بسیاری از سیستم‌های کلید همگانی مطرح شده را فقط با همگانی نکردن کلید(ها) به سیستم کلید خصوصی تبدیل کرد. برای مطالعه نمونه‌های خاص سیستم‌های کلید خصوصی مبتنی بر تئوری کدینگ می‌توان به مقالات [17]، [18]، [19]، [20]، [21]، [22]، [23] و [24] اشاره نمود. در زمینه رمزنگاری مبتنی بر تئوری کدینگ مقالات متعددی در سال‌های اخیر انتشار یافته است. فهرست تقریبا کاملی از مقالات و پایان‌نامه‌های دکتری مرتبط در بخش مراجع آمده است. برای توضیحات بیش‌تر در مورد پیاده‌سازی عملی سیستم McEliece و روش ترکیبی مطالعه [۲۵] و برای آشنایی کلی با زمینه‌های مشترک بین کدینگ کانال و رمزنگاری مطالعه [۲۵] [26] پیشنهاد می‌گردد. به عنوان یکی از آخرین مقاله‌های چاپ شده در این زمینه باید به مقاله Berger و Loidreau [27] اشاره نمود که در آن علاوه بر افزایش مقاومت سیستم McEliece، روشی برای کاهش حجم کلید همگانی سیستم نیز ارائه نموده‌اند.

۳- سیستم‌های رمزنگاری کلید همگانی مبتنی بر تئوری کدینگ برای تامین اعتبار و امضای دیجیتال

در این بخش به مرور مقالات در زمینه تامین اعتبار و امضای دیجیتال به کمک کدهای تصحیح خطا می‌پردازیم. روش‌های تعیین اعتبار(احراز هویت) و امضای دیجیتال با این هدف، که نیازی به تامین امنیت اطلاعات ندارند، از توانایی تشخیص خطای کد برای تائید صحت اطلاعات استفاده می‌کنند.

مفهوم امضای دیجیتال توسط Diffie و Hellman در مقاله معروف‌شان در زمینه سیستم‌های رمزنگاری کلید همگانی مطرح گردید[5]. وقتی فرستنده می‌خواهد پیام $\mathbf{m}$ را امضا نموده وامضا را به گیرنده مجاز بفرستد، زوج $(\mathbf{m},\mathbf{s})$ ، که در آن $\mathbf{s} = sign(\mathbf{m})$ امضا است، را ارسال می‌کند. گیرنده مجاز می‌تواند با به کارگیری الگوریتم تایید[۸] همگانی بر روی $\mathbf{s}$ صحت امضای را بررسی و تایید نماید. برای این منظور باید رابطه $ver(\mathbf{s}) = ver(sign(\mathbf{m})) = \mathbf{m}$ برقرار باشد. این پیکربندی برای مساله اولین بار توسط Gibson، Mac Williams و Sloane در [28] ارائه گردید. آن‌ها مساله کلی را توصیف و کران بالایی برای احتمال موفقیت دشمن بر حسب تعداد عضوهای فضای کلید بدست آورده‌اند. اگر کلید بتواند یکی از K عضو موجود در فضای کلید باشد، در این صورت و با به کارگیری بهترین استراتژی توسط دشمن، احتمال آشکار نشدن جعل پیام از $K^{-\frac{1}{2}}$ بزرگ‌تر است[28]. در مواردی می‌توان پیام $\mathbf{m}$را نیز حذف نمود. در این حالت الگوریتم تایید، پیام $\mathbf{m}$را باز تولید می‌نماید. به این روش بازیابی پیام[۹] می‌گویند[29].

امضای دیجیتال با توجه به امکان جایگزین شدن آن به جای امضای عادی(تایید اعتبار)، نقش کلیدی در تجارت

الکترونیک ایفا می‌نماید. روش‌های امضای دیجیتال متعددی بر مبنای مساله تجزیه اعداد طبیعی به عوامل اول طراحی شده است. برای مثال می‌توان به الگوریتم RSA و مساله لگاریتم گسسته[10] اشاره نمود. تلاش برای طراحی روش امضای دیجیتال بر مبنای دیگر مسایل پیچیده(سخت)[11] ریاضی در حال انجام است. مساله کدبرداری از یک کد خطی کلی نیز نمونه‌ای از این مسایل پیچیده است. NP-complete بودن این مساله توسط Berlekamp، McEliece و Van Tilborg ثابت گردیده است [14]. اولین سیستم رمزنگاری کلید همگانی بر مبنای کدهای تصحیح خطای خطی توسط McEliece مطرح شده است. همان‌طور که در بخش قبل مطرح شد امنیت سیستم McEliece بر مساله کدبرداری استوار است. تاکنون هیچ حمله موثری به سیستم McEliece مطرح نشده است[29]، هر چند از نظر محاسباتی[12] حملات متعددی به آن مطرح گردیده است. برای نمونه می‌توان به [30]، [31]، [2] و[29] اشاره نمود. حملاتی به پیاده‌سازی سیستم McElice نیز، مانند [32]، [33]، [29]، مطرح شده است. پس از مقاله McEliece سیستم‌های رمزنگاری متعددی بر مبنای کدهای کنترل خطا ارائه شده است. برای مثال می‌توان از سیستم رمزنگاری کلید خصوصی Rao-Nam [18]، روش امضای دیجیتال Xinmei [34] و روش احراز هویت[13] Stern را نام برد[35]. این روش‌ها برای تامین نمودن امنیت یا فراهم کردن اعتبار[14] پیام بر حسب نیازهای مختلف استفاده می‌گردند.

برخی از سیستم‌های رمزنگاری کلید همگانی مانند RSA را می‌توان مستقیما به عنوان روشی امضای دیجیتال به کار برد. در مقابل، سیستم رمزنگاری McEliece را نمی‌توان مستقیما برای روشی امضای دیجیتال به کار برد. از آنجائیکه تابع رمزنگاری آن بردار باینری k بیتی را به n بیتی می‌نگارد، نمی‌توان معکوسی برای آن داشت[36].

در سال ۱۹۹۰ Xinmei Wang اولین روش امضای دیجیتال بر مبنای کدهای تصحیح خطا را ارائه نمود[34]. در روش Xinmei امضا به طریقی مشابه روشی که در روش Rao-Nam [18] متن اصلی رمز می‌گردد، صورت می‌پذیرد. ادعا شده که امنیت روش Xinmei بر وجود تعداد زیاد ماتریس‌های مولد یک کد تصحیح خطای خاص و پیچیدگی یافتن و بازیابی کد تصحیح خطای اصلی از نمونه‌های معادل همگانی مخلوط شده[15] استوار است[34]. در سال ۱۹۹۲ حملات متعددی به روش Xinmei مطرح گردید. به عنوان نمونه، Harn و Wang یک حمله homomorphism به این روش بدون تجزیه کردن ماتریس‌های بزرگ طرح کردند. همچنین روش بهبود یافته‌ای به نام روش Harn-Wang، که در آن از تابعی غیرخطی برای مقابله با حمله homomorphism استفاده می‌شود، ارائه کردند. همچنین Alabbadi و Wicker نشان دادند که روش Xinmei در مقابل حمله chosen plaintext با مرتبه $O(n^3)$ آسیب‌پذیر است. آن‌ها در [37] نشان دادند که روشی Harn-Wang را می‌توان با پیچیدگی‌ای از مرتبه $O(k^3)$ با حمله known plaintext شکست. سپس Van Tilburg در [38] نشان داد که در روش‌های Xinmei و Harn-Wang می‌توان مستقیما کلید خصوصی را از کلیدهای عمومی بدست آورد. در سال ۱۹۹۳ Alabbadi و Wicker امضای دیجیتال تازه‌ای بر مبنای کدهای تصحیح خطا ارائه نمودند[39]. در همین سال Van Tilburg در [40] نشان داد که با داشتن تایید n امضا، که دارای بردارهای خطای مستقل خطی از یکدیگر باشند، سیستم جدید نا امن است. در ۱۹۹۴Alabbadi و Wicker حمله universal forgery را به روش Xinmei و روش خودشان مطرح نمودند[41]. در همین سال Alabbadi و Wicker روش امضای دیجیتال دیگری متکی بر کدهای تصحیح خطا ارائه نمودند. آن‌ها ادعا نمودند که این روش در مقابل حملاتی که ثابت شده در مورد روشهای پیشین موفقیت آمیز اند، مقاوم است[42].

در سال ۱۹۹۳ Stern روش کلید همگانی برای تصدیق هویت را در کنفرانس Crypto93 ارائه نمود[35]. Courtois، Finiasz و Sendrier در سال ۲۰۰۱ روش امضای دیجیتالی، که مستقیما بر سیستم McEliece استوار است، مطرح کردند[36]. آن‌ها نشان دادند احتمال معتبر بودن یک متن امضا شده تصادفی با McEliece خیلی کم است. به بیان دیگر احتمال اینکه بتوان آن را رمزگشایی نمود در حدود $\frac{1}{t!}$ است. بنابراین، با بررسی متوالی تمام $t!$ متن رمزشده ممکن می‌توان متن معتبر مورد نظر را یافت.

یکی از جدیدترین مقاله در این زمینه مقاله Wadayama در کنفرانس ISIT ۲۰۰۵ است. او یک روش تصدیق هویت‌ی با استفاده از ماتریس کدهای LDPC[16] ارائه نموده است. همچنین به کمک برهان‌های ترکیبی[۱۷] حد بالایی برای احتمال جعل هویت و جعل پیام بدست آورده است[43].

۴- نتیجه‌گیری

در این مقاله به مرور مطالعات انجام شده در زمینه سیستم-های رمزنگاری مبتنی بر تئوری کدینگ پرداخته شد. به عنوان پیشنهاد برای مطالعات آتی می‌توان بررسی امکان تامین با استفاده از کدهای turbo و سیستم‌های رمزنگاری مبتنی بر میدان های بنا شده با خم‌های بیضوی[۱۸] اشاره نمود. مطالعه در این زمینه‌ها آغاز شده است؛ برای نمونه [44] و [45] را ببینید. از دیگر محورهای مناسب مطالعه در مورد کاهش حجم کلید همگانی این سیستم‌ها است[27]. مطالعه برای به کارگیری دسته‌های دیگری از خانواده کدهای خطی و غیرخطی نیز در حال انجام است[24].

مراجع

[1] Anne Canteaut and Florent 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,” *IEEE Transaction on Information Theory*, vol. 44, NO. 1, January 1998, pp. 367-378.

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

[۳] حسام محمد حسینی، " بررسی سیستم‌های رمزنگاری مبتنی بر تئوری کدینگ"، سمینار کارشناسی ارشد، دانشگاه تربیت مدرس، مهر ۱۳۸۴.

[4] Y. X. Li, D. X. Li and C. K. Wu, “How to Generate a Random Nonsingular Matrix in McEliece Public-Key Cryptosystem,” Singapore *ICCS/ISITA.*, 1992.

[5] W. Diffie and M. Hellman, “New directions in cryptography,” in *IEEE Transactions on Information Theory*, vol. 22, no.6, pp. 644-654, 1976.

[6] K. Kobara, and H. Imai, “Semantically Secure McEliece Pubilc-Key Cryptosystem –Conversions for McEliece PKC-,” in *PKC’2001*, K. Kim (ed.), LNCS1992, Springer-Verlag, 2001, pp. 19–35.

[7] R. J. McEliece, “A Public-Key Cryptosystem Based on Algebraic Coding Theory,” *Deep Space Network Progress Report 42-44*, California Institute of Technology, pp. 114-116, 1978.

[8] E. R. Berlekamp, J. R. McEliece and H. van Tilborg, “On the Inherent Intractability of Certain Coding Problems,” *IEEE Trans. Inform. Theory*, vol. IT-24, pp. 384-386, May 1978.

[9] H. Niederreiter, “Knapsack-type cryptosystem and algebraic coding theory,” *Problems of Control and Information theory*, vol. 15 (2), pp. 159-166, 1986.

[10] Y. X. Li, D. X. Li and C. K. Wu, “How to Generate a Random Nonsingular Matrix in McEliece Public-Key Cryptosystem,” Singapore *ICCS/ISITA.*, IEEE, 1992.

[11] R. J. McEliece, *The Theory of Information and Coding*, Addison-Wesley, 1977. also 2nd edition, Cambridge University, 2002.

[12] K. Gibson, “The Security of the Gabidulin Public Key Cryptosystem,” in *Advances in Cryptology-EUROCRYPT '96*, Springer-Verlag, pp. 212-223, 1996.

[13] E. R. Berlekamp, “Goppa Codes,” *IEEE Trans. on Inform. Theory*, Vol. IT-19, No. 5, pp. 590-592, Sep. 1973.

[14] E.R. Berlekamp, J.R. McEliece and H. van Tilborg, "On the Inherent Intractibility of Certain Coding Problems," in *IEEE Trans. Info. Theory*, Vol. IT-24, pp.384-386, May 1978.

[15] A. W. House, “On the Combination of Security and Error-Control Coding,” Available: http://www.padre.ca/house/crypt_ec.pdf

[16] C. Adams, and H. Meijer, “Security-Related Comments Regarding McEliece's Public-key Cryptosystem,” *IEEE Trans. Inform. Theory*, Vol. IT-35, pp. 454-457, March 1989.

[17] T. Hwang and T. R. N. Rao, “Secret Error-Correcting Codes (SECC),” in *Advances in Cryptology-CRYPTO ’88*, LNCS vol. 403, pp. 540–563, Springer-Verlag, 1988.

[18]T. R. N. Rao and K. Nam, “Private-Key Algebraic-Code Encryption,” in *IEEE Transactions on Info. Theory*, Vol. 35, No. 4, pp. 829-833, July 1989.

[19] Tzoneli Hwang and T. R. N. Rao, “Privet-Key algebraic Cryptosystems With High Information Rates,” in *Advances in Cryptology-EUROCRYP ’89*, pp. 657–661, Springer-Verlag, 1989.

[20] F. M. R. Alencar, A. M. R. Leo, and R. M. Campello de Souza, “Private-Key Burst Correcting Code Encryption,” in *Proc. IEEE Int. Symp. Information Theory*, pp. 227, Jan.1993.

[21] Hung-Min Sun and S. P. Shieh, “Cryptanalysis of Private-Key Encryption Schemes Based on Burst-Error-Correcting Codes,” *Third ACM Conference on Computer and Communications Security*, New Delhi, India, pp. 153-156, March 14-16, 1996.

[22] A. Kh. Al Jabri, “A Symmetric version of the McEliece Public-Key Cryptosystem,” *International Journal of Network Management*, Vol. 7, pp.316–323, 1997.

[23] Hung-Min Sun, "Private-Key Cryptosystem Based on Burst-Error-Correcting Codes," *IEE Electronics Letters*, Vol. 33, No. 24, 1997, pp. 2035-2036.
[24] T. Berger and P. Loidreau, "Designing an efficient and secure public-key cryptosystem based on reducible rank codes," in *Proceedings of INDOCRYPT 2004*, LNCS 3348, pp. 218-229.
[۲۵] حسام محمد حسینی و پیام امانی، "پیاده‌سازی ارتباط بی‌سیم بین دو کامپیوتر برای ارسال فایل متنی"، پایان نامه کارشناسی، دانشگاه صنعتی خواجه نصیرالدین طوسی، شهریور ۱۳۸۳.
[26] V. S. Pless and W. C. Huffman , *Handbook of Coding Theory*, Chapter 14, By H. C. A. van Tilborg, "Coding Theory at Work in Cryptology and Vice Versa," North-Holland, pp.1195-1227, Nov 1998.
[27] T. Berger, and P. Loidreau, "How to Mask the Structure of Codes for a Cryptographic Use," in *Designs, Codes and Cryptography*, vol.35, pp.63-79, 2005.
[28] E. Gilbert, F. J. MacWilliams, and N. J. A. Sloane, "Codes which detect deception," *Bell System Technical Journal*, 53(3), pp.405–424, March 1974.
[29] J. Doumen, "Some Applications of Coding Theory in Cryptography," Eindhoven Univ. of Tech., The Netherlands, PhD Dissertation, 6-6-2003.
[30] F. Chabaud, "On the security of some cryptosystems based on errorcorrecting codes," in *Advances in Cryptology—EUROCRYPT'94*, Springer-Verlag, 1994, pp. 131–139.
[31] T. Berson, "Failure of the McEliece Public-Key Cryptosystem Under Message-Resend and Related-Message Attack," in *Advances in Cryptology-CRYPTO '97* , Springer-Verlag, pp. 213-220, 1997.
[32] 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*, LNCS2248, Springer-Verlag, 2002, pp. 237–251.
[33] E. Verheul and J. M. Doumen and H. C. A. van Tilborg, "Sloppy Alice Attacks! Adaptive Chosen Ciphertext Attacks on the McEliece cryptosystem," in *Information, Coding and Mathematics*, Kluwer Academic Publishers, Boston, May 2002, pp. 99-119.
[34] W. Xinmei, "Digital Signature Schemes Based on Error-Correcting Codes," *Electronic letters*, Vol. 26, No. 13, June 1990.
[35] J. Stern, "A new identification scheme based on syndrome decoding," in *Advances in Cryptology-Crypto 93*, Springer-Verlag, pp. 13-21, 1993.
[36] N. Courtois, M. Finiasz and N. Sendrier, "How to achieve a McEliece_based Digital Signature Scheme," in *Advances in Cryptology-Asiacrypt 2001*, LNCS 2248, Springer-Verlag, pp. 157-174, 2001.
[37] M. Alabbadi and S. B. Wicker, "Security of XlNMEI Digital Signature Scheme," *Electronic letters*, Vol. 28, No. 9, pp.890-891 April 1992.
[38] J. v. Tilburg, "Cryptanalysis of Xinmei digital signature scheme," *Electronic Letters*, vol. 28, 1992, no. 20, pp.1935-1936.
[39] M. Alabbadi and S. B. Wicker, "Digital signature scheme based on error correcting codes," in *lEEE International Symposium on Information Theory* , San Antonio, USA, 1993, page199.
[40] J. v. Tilburg, "Cryptanalysis of the Alabbadi-Wicker digital signature scheme," *Proceedings of Fourteenth Symposium on Information Theory*, 1993, pp. 114-119.
[41] M. Alabbadi and S. B. Wicker, "Susceptibility of digital signature schemes based on error-correcting codes to universal forgery," *Error control, Cryptology, and Speech compression*, Moscow, Springer, 1994, pp. 6-12.
[42] M. Alabbadi and S. B. Wicker, "A digital signature scheme based on linear error-correcting block codes," in *Advances in cryptology-ASIACRYPT '94*, Wollongong, Springer, 1995, pp. 238-248.
[43] T. Wadayama, "An authentication scheme based on an LDPC Matrix," to be appear in *ISIT2005*.
[44] Sorin Adrian Barbulescu, "Secure Satellite Communication and Turbo-like Codes," *3rd International Symposium on Tubo Codes & Related Topics*, Brest, France, Sept 2003.
[45] Beatriz Ontiveros, Ismael Soto, and Carasco Rolando, "Turbo Code with Public Key Cryptosystem," Dec 2003.

---

[1] Redundant
[2] Parity Check Bit
[3] Cryptanalysis
[4] Nondeterministic Polynomial
[5] Infeasible
[6] Goppa Codes
[7] Randomization
[8] Verification
[9] Message Recovery Scheme
[10] Discrete Logarithm Problem
[11] Hard
[12] Computationally Intensive
[13] Identification
[14] Authenticity
[15] Scrambled
[16] Low Density Parity Check Codes
[17] Combinatorial
[18] Elliptic Curves