دانشگاه زنجان

گروه برق

پایان نامه کارشناسی

گرایش :مخابرات

رمزنگاری کوانتومی

استاد راهنما

دکتر محمد مصطفوی

پژوهش و نگارش

سمانه اصانلو

زمستان ۱۳۹۲

چکیده:

امروزه حفاظت از اطلاعات رکن اساسی و مهمی در تبادلات پیام ها و اطلاعات ایفا می‌کند. روش های مختلفی از زمان های دور برای حفاظت و به هم ریختگی اطلاعات استفاده می‌شده است و در عصر مدرن هم روش های کلاسیک متعددی جهت این امر مورد استفاده قرار می‌گیرد ،اما استفاده از روش های کلاسیک مستلزم به کارگیری محاسبات پیچیده ریاضی است و در نهایت با روش‌های پیچیده ای دیگر این اطلاعات رمز شده می‌توانند شکسته شوند.اما ،جدیدترین نوع رمزنگاری پس از روش های کلاسیک ،رمزنگاری کوانتومی است که بدون استفاده از روش های پیچیده ریاضی، تبادل امن اطلاعات را نوید می‌دهد.چون این روش بر پایه قوانین مکانیک کوانتومی استوار است اگر کسی قصد شنود اطلاعات را داشته باشد، با بالا رفتن نرخ خطا در سمت گیرنده، وجود شنودگر شناسایی می‌شود و مراسله اطلاعات از طریق کانالی دیگر از سر گرفته می‌شود. این روش بر پایه ارسال و دریافت ویژگی خاصی از فوتون به نام پلاریزاسیون استوار است و اگر استراق سمع کننده سعی در اندازه گیری پلاریزاسیون داشته باشد ،پلاریزاسیون به دلیل قوانین کوانتومی، دستخوش تغییر خواهد شد. درواقع در رمزنگاری کلاسیک، بیت ها ارسال و دریافت می‌شوند اما در رمزنگاری کوانتومی، کیوبیت ،که همان پلاریزاسیون فوتون است از فرستنده به گیرنده ارسال می‌شود.

کلمات کلیدی: پلاریزاسیون، کیوبیت، فوتون، بیت، دیتا، آلیس و باب.

فهرست عناوین:

فصل اول: مقدمه ۱۵

۱-۱ - اصول ششگانه کرکهف ۱۷

۱-۲- رمزنگاری پیشرفته ۱۷

۱-۳- دلیل رمزنگاری اطلاعات در کامپیوتر ۱۷

۱- محرمانه سازی ۱۸

۲- تـمـامـیـت ۱۸

۳- اعتبار سنجی ۱۸

۱-۴- تبدیل سیگنال آنالوگ به دیجیتال ۱۹

۱-۵-الگوریتم رمزنگاری ۲۰

۱-۶-پروتکل رمزنگاری ۲۰

۱-۷- **Hash Algorithm** ۲۰

۱-۸-رمزنگاری کوانتومی ۲۲

۱-۹-فوتون ۲۳

۱-۹-۱-پلاریزاسیون ۲۴

فصل دوم : رمزنگاری کوانتومی ۲۵

۲-۱-تئوری اطلاعات کوانتوم ۱۱

۲-۱-۱- بیت های کوانتومی ۱۱

۲-۱-۲-عملگرهای خطی ۱۳

۲-۱-۳-ماتریس های پائولی ۱۴

۲-۱-٤-ضرب داخلی ۱۶

۲-۱-۵-:ضرب خارجی ۱۷

۲-۱-٦-:ضرب تنسور ۱۸
۲-۲- اندازه گیری کوانتومی ۱۹
۲-۳-:قضیه عدم کپی برداری ۲۳
۲-۴-آنتروپی شانون ۲۴
۲-۵-آنتروپی رنی ۲۶
۲-۶- توزیع کلید کوانتومی ۲۷
۲-۶-۱-ادراک فیزیکی ۲۸
۲-۷- انتقال فوتون و توان عملیاتی ۲۹
۲-۸-کانال عمومی ۳۰
۲-۸-۱-غربال کردن ۳۰
۲-۸-۲-تصدیق هویت مرحله غربال ۳۴
ارزش کل ۳۵
۲-۸-۳-اصلاح ۳۵
۲-۸-۳-۱-تخمین خطا ۳۵
۲-۸-۴-تصحیح خطا ۳۸
۲-۸-۵-تصدیق تصحیح خطا ۴۴
۲-۸-۶-تقویت محرمانگی ۴۶
۲-۹- تعدادی از پروتکل های رمزنگاری کوانتومی ۴۸
درهم تنیدگی کوانتومی ۴۸
۲-۹-۱-پروتکل **B92** ۴۹
۲-۹-۲-پروتکل **SARG04** ۵۰
پروتکلهای توزیع کلید مبتنی بر همبستگی ۵۰
۲-۹-۳-پروتکل **E91** ۵۰

۲-۹-۴-پروتکل۹۲ BB ۵۱
۲-۱۰-مقایسه انواع پروتکلها ۵۲
فصل سوم :نتیجه گیری و پیشنهادها ۵۳
فصل چهارم: فهرست مراجع ۵۳

فهرست اشکال

شکل ۱-شمایی از درهم سازی ۲۱
شکل ۲-پلاریزاسیون فوتون بعنوان کیوبیت ۲۴
شکل ۳کره بلاخ ۱۲
شکل ۴- مراحل رمزنگاری کوانتومی ۲۸
شکل ۵- شمای ارسال و دریافت کوانتومی ۳۲
شکل ۶- گین برحسب دلتا ۳۳
شکل ۷-نرخ خطا برحسب دلتا ۳۸
شکل ۸-نمونه تصحیح باینری۱ ..... ۴۲
شکل ۹-نمونه تصحیح باینری۲ ..... ۴۲
شکل ۱۰-نمونه تقویت محرمانگی ۴۸
شکل ۱۱-کدگذاری دوحالته در پروتکل **B92** ۴۹
شکل ۱۲-مدل توزیع کلید کوانتومی مبتنی بر انتنگلمنت ۵۱

فهرست جداول

جدول ۱-خلاصه ای از علامت های استاندارد مکانیک کوانتومی ۱۴
جدول ۲-نگاشت ۲۹
جدول ۳-CACcade benchmark ۴۴

فصل اول: مقدمه

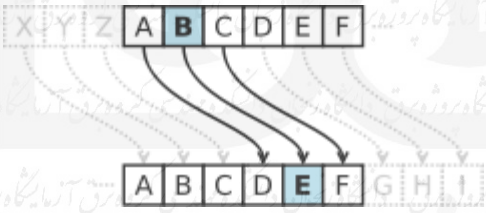
کلیات:

رمزنگاری دانشی است که به بررسی و شناختِ اصول و روش‌های انتقال یا ذخیره اطلاعات به صورت امن (حتی اگر مسیر انتقال اطلاعات و کانال‌های ارتباطی یا محل ذخیره اطلاعات ناامن باشند) می‌پردازد.رمزنگاری استفاده از تکنیکهای ریاضی، برای برقراری امنیت اطلاعات است. دراصل رمزنگاری دانش تغییر دادن متن پیام یا اطلاعات به کمک کلید رمز و با استفاده از یک الگوریتم رمز است، به صورتی که تنها شخصی که از کلید و الگوریتم مطلع است قادر به استخراج اطلاعات اصلی از اطلاعات رمز شده باشد و شخصی که از یکی یا هر دوی آن‌ها اطلاع ندارد، نتواند به اطلاعات دسترسی پیدا کند.

شروع رمزنگاری به سال ۱۹۰۰ قبل از میلاد برمیگردد، برطبق اسناد موجود ،یک مصری درآن زمان که کلمات بصورت تصویر بیان می شد ازتصاویری استفاده کرده که متداول نبوده است بنابراین شروع رمزنگاری از مصریان می‌باشد .

نمونه‌ای از روش رمز کردن موسوم به رمز سزار است که بر اساس جابجایی ساده حروف الفبا عمل می‌کند.

در بررسی نخستین استفاده‌کنندگان از تکنیک‌های رمزنگاری به سزار (امپراتور روم) و نیز الکندی که یک دانشمند مسلمان است برمی‌خوریم، که البته روش‌های خیلی ابتدایی رمزنگاری را ابداع و استفاده کرده‌اند. به عنوان مثال، با جابجا کردن حروف الفبا در تمام متن به اندازه مشخص آن را رمز می‌کردند و تنها کسی که از تعداد جابجا شدن حروف مطلع بود می‌توانست متن اصلی را استخراج کند.



یکی دیگر از شیوه‌های رمزنگاری ابتدایی، پیچیدن یک نوار کاغذی بر روی استوانه‌ای با قطر مشخص و سپس نوشتن پیام روی کاغذ پیچیده شده بوده‌است .بدیهی است بدون اطلاع از مقدار قطر استوانه، خواندن پیام کار بسیار دشواری خواهد بود و تنها کسانی که نسخه‌های یکسانی از استوانه را داشته باشند می‌توانند پیام را بخوانند.

۱–۱ – اصول ششگانه کرکهف

آگوست کرکهف در سال ۱۸۸۳ دو مقاله با عنوان «رمز نگاری نظامی» منتشر کرد. در این دو مقاله شش اصل اساسی وجود داشت که اصل دوم آن به عنوان یکی از قوانین رمز نگاری هنوز هم مورد استفاده دانشمندان در رمز نگاری پیشرفته‌است:

- سیستم رمزنگاری اگر نه به لحاظ تئوری که در عمل غیر قابل شکست باشد.
- سیستم رمز نگاری باید هیچ نکته پنهان و محرمانه‌ای نداشته باشد. بلکه تنها چیزی که سری است کلید رمز است.
- کلید رمز باید به گونه‌ای قابل انتخاب باشد که اولا بتوان به راحتی آن را عوض کرد و ثانیا بتوان آنرا به خاطر سپرد و نیازی به یاداشت کردن کلید رمز نباشد.
- متون رمز نگاری باید از طریق خطوط تلگراف قابل مخابره باشند.
- دستگاه رمز نگاری یا اسناد رمز شده باید توسط یک نفر قابل حمل و نقل باشد.
- سیستم رمزنگاری باید به سهولت قابل راه اندازی باشد.

۱–۲– رمزنگاری پیشرفته

با پدید آمدن رایانه‌ها و افزایش قدرت محاسباتی آنها، دانش رمزنگاری وارد حوزه علوم رایانه گردید و این پدیده، موجب بروز سه تغییر مهم در مسائل رمزنگاری شد:

۱. وجود قدرت محاسباتی بالا این امکان را پدید آورد که روش‌های پیچیده‌تر و مؤثرتری برای رمزنگاری به وجود آید.

۲. روش‌های رمزنگاری که تا قبل از آن اصولا برای رمز کردن پیام به کار می‌رفتند، کاربردهای جدید و متعددی پیدا کردند.

۳. تا قبل از آن، رمزنگاری عمدتاً روی اطلاعات متنی و با استفاده از حروف الفبا انجام می‌گرفت؛ اما ورود رایانه باعث شد که رمزنگاری روی انواع اطلاعات و بر مبنای بیت انجام شود.

۱–۳– دلیل رمزنگاری اطلاعات در کامپیوتر

گسترش و رشد بی سابقه اینترنت باعث ایجاد تغییرات گسترده در نحوه زندگی و فعالیت شغلی افراد ، سازمان ها و موسسات شده است. امنیت اطلاعات یکی از مسائل مشترک شخصیت های حقوقی و حقیقی است . اطمینان از عدم دستیابی افراد غیر مجاز به اطلاعات حساس از مهمترین چالش های امنیتی در رابطه با توزیع اطلاعات در

اینترنت است . اطلاعات حساس که ما تمایلی به مشاهده آنان توسط دیگران نداریم، موارد متعددی را شامل می شود.
برخی از این گونه اطلاعات به شرح زیر می باشند :

- اطلاعات کارت اعتباری
- شماره های عضویت در انجمن ها
- اطلاعات خصوصی
- جزئیات اطلاعات شخصی
- اطلاعات حساس در یک سازمان
- اطلاعات مربوط به حساب های بانکی

با استفاده از رمزنگاری سه سرویس امنیتی فراهم می شود:

۱– محرمانه سازی :

اطلاعات به هنگام ارسال یا ذخیره شدن از دید افراد غیر مجاز پنهان خواهد شد.

۲– تـــمـــامـیـــت :

تغییرات اعمال شده در اطلاعات ارسالی مشخص خواهد شد.

۳– اعتبار سنجی :

می توان منبع اطلاعات را اعتبار سنجی کرد.

عناصر مهمی که در رمزنگاری مورد استفاده قرار می‌گیرند به شرح زیر می‌باشد:

- متن آشکار

پیام و اطلاعات را در حالت اصلی و قبل از تبدیل شدن به حالت رمز، متن آشکار یا اختصاراً پیام می‌نامند.
در این حالت اطلاعات قابل فهم توسط انسان است.

- متن رمز

دانشجویان محترم:

جهت دسترسی به متن کامل پایان نامه‌ها به کتابخانه دانشکده مهندسی و یا آزمایشگاه پروژه گروه برق مراجعه فرمایید.

فصل سوم: نتیجه گیری و پیشنهادها

عده‌ای معتقدند که رمزنگاری کوانتومی، آینده رمزنگاری خواهد بود. البته به دلیل نیاز به سخت‌افزار خاص، استفاده از این روش از تعدادی نمونه محدود فراتر نرفته است.در دنیای واقع آزمایش های موفقیت آمیز زیادی در پیاده سازی توزیع کلید کوانتومی به نتیجه رسیده است.مانند آزمایش هایی که در آزمایشگاه Somervilleدر MagiQ انجام شده است. در همه این آزمایشها از فیبر نوری برای انتقال فوتونها استفاده شدهاست .برخلاف اینکه انتقال در فضای خالی اثبات شده است، فاصله توزیع کلید کوانتومی به ده ها کیلومتر محدود شده است .زیرا تقویت نوری باعث خراب شدن حالت کیوبیتها میشود .بنابراین نمیتوان از آنها برای تقویت کانال های QKD جهت گسترش فاصله استفاده کرد و تضعیف درکانالهای فیبری که تابعی از طول فیبر است باعث می شود فوتونها قابل اندازه گیری نباشند.

امروزه پیاده سازی رمزنگاری کوانتومی با مشکلات تکنیکی متفاوتی روبه رو شده است، که در بیشتر موارد مربوط به نقص در منابع تولیدکننده فوتون است .با این وجود، رمزنگاری کوانتومی با تکنولوژیهای موجود عملی است و با نرخ داده پایین امکان پذیر است .سیستمهای QKD می توانند حداکثر با نرخ چند مگابیت در ثانیه کار کنند و این وابسته به فاصله دستگاه های فرستنده و گیرنده است.

پروتکل‌های توزیع کلید کوانتومی ارائه شده میتوانند به سیستم های کلاسیک موجود اضافه شوند و وابسته به کامپیوترهای کوانتومی نیستند تنها با داشتن یک کانال کلاسیک و یک کانال کوانتومی حتی ناامن، میتوان کلید مخفی برای ارسال پیام های رمزشده به صورت کاملاً امن و بدون هیچگونه پیش فرض درباره توانایی های استراق سمع کننده، بین فرستنده و گیرنده به اشتراک گذاشت.

رمزنگاری کوانتومی به عنوان روشی مطرح شده بود که تصور می‌شد می‌تواند به‌طور صد درصد اطلاعات را در برابر حملات محافظت کند. اما یک گروه تحقیقاتی در دانشگاه Linköping سوئد، یک حفره در این فناوری پیشرفته پیدا کرده و نشان دادند که حتی رمزنگاری کوانتومی هم صد درصد امن نیست. آن‌ها نشان دادند که از نظر تئوری امکان استخراج کلید بدون جلب توجه با دستکاری همزمان بستر کوانتومی و بستر ارتباطی معمول وجود خواهد داشت. سپس با ارائه مقاله‌ای در نشریه IEEE Transactions راهکار حل این مشکل را با اعمال یک تغییر ارائه دادند. به گفته یکی از اعضای ارشد این گروه، انتظار نمی‌رفت که اشکالی در رمزنگاری کوانتومی یافت شود، اما این سیستم به واقع پیچیده است و با راهکار جایگزین آن‌ها، رمزنگاری کوانتومی می‌تواند یک فناوری امن باشد. با این حال، خطر دستیابی غیرمجاز به اطلاعاتی مانند تراکنش‌های مالی، نیاز هرچه بیشتر به فناوری‌ها و روش‌های پیشرفته‌تر رمزنگاری را ضروری می‌سازد. به گفته اندی کوردیال (Andy Cordial) مدیر شرکت Storage Origin در آینده باید بر دو فاکتوری شدن تعیین اعتبار در مقابل روش‌های تک‌فاکتوری و به عبارتی بر افزایش سطوح امنیت تأکید کرد. البته هرچقدر هم که رمزنگاری پیشرفته باشد، هرگز برای امنیت کامل کافی نخواهد بود.

فصل چهارم: فهرست مراجع

-سلطان آقایی الهه. م سلطان آقایی.۱۳۹۱. شناخت و ارزیابی پروتکل های توزیع کلید مبتنی بر رمزنگاری کوانتومی.۷ صفحه

۱- http://www.shabakeh-mag.com/

۲-http:// www.chaparel.ir

۳-http://www.itl.nist.gov

۴-http://citreseer.ist.psu.edu

۵-http://msdn2.microsoft.com

۶-http://Searchsecurity.techtarget.com

۷-http://en.wikipedia.org/wiki/Proxy_server

۸-http://www.linux.org/docs/ldp/howto/Firewall-HOWTO-11.html#ss11.4

۹-Carter, L., Wegman, M.N.: Universal classes of hash functions. J. Comput. Syst. Sci. 18(2), 143–154 (1979) 15

۱۰-Cover, T.M., Thomas, J.A.: Elements of Information Theory.Wiley-Interscience (1991). URL http://www.amazon.ca/exec/obidos/redirect?tag=citeulike09–20&path=ASIN/0471062596 19

۱۱-National Institute of Standards and Technology: FIPS PUB 186–2: Digital Signature Standard(DSS). National Institute for Standards and Technology, Gaithersburg, MD, USA(2000). URL http://www.itl.nist.gov/fipspubs/fip186–2.pdf 14

۱۲. Nielsen, M.A., Chuang, I.L.: Quantum Computation and Quantum Information. Cambridge University Press, Cambridge (2000). URL http://www.amazon.ca/exec/obidos/redirect?tag= citeulike09–20%&path=ASIN/0521635039 3, 5, 9, 10

۱۳. R´enyi, A.: On measures of information and entropy. Proceedings of the 4th Berkeley Symposium on Mathematics, Statistics and Probability, pp. 547–561 (1961) 20

۱۴. Rivest, R.L., Shamir, A., Adleman, L.M.: A method for obtaining digital signatures and publickey cryptosystems. Commun. ACM 21(2), 120–126 (1978) 14

۱۵. Shannon, C.E.: A mathematical theory of communication. The Bell System Technical Journal27, 379–423, 623–656 (1948). URL http://cm.bell-labs.com/cm/ms/what/shannonday/ shannon1948.pdf 19

۱۶ -Stinson, D.R.: Universal hashing and authentication codes. In: J. Feigenbaum (ed.) CRYPTO, Lecture Notes in Computer Science, Vol. 576, pp. 74–85. Springer, Heidelberg (1991) 15

۱۷. Wegman,M.N., Carter, L.: New hash functions and their use in authentication and set equality. J. Comput. Syst. Sci. 22(3), 265–279 (1981) 14, 15, 16, 17, 18, 19

۱۷ . Wootters,W.K., Zurek,W.H.: A single quantum cannot be cloned. Nature 299(5886), 802–803(1982). DOI 10.1038/299802a0. URL http://dx.doi.org/10.1038/299802a0 13

۱۸Ardehali, M., Chau, H.F., Lo, H.K.: Efficient quantum key distribution (1998). URL http://www.citebase.org/abstract?id=oai:arXiv.org:quant-ph/98% 03007 32

۱۹- Assche, G.V.: Quantum Cryptography and Secret-Key Distillation. Cambridge University Press, New York, USA (2006) 45

۲۰Bennett, C.H.: Quantum cryptography using any two nonorthogonal states. Phys. Rev. Lett. 68(21), 3121–3124 (1992). DOI 10.1103/PhysRevLett.68.3121 23

۲۱-Bennett, C.H., Bessette, F., Brassard, G., Salvail, L., Smolin, J.A.: Experimental quantum cryptography. J. Cryptology 5(1), 3–28 (1992) 36, 37

۲۲-Bennett, C.H., Brassard, G.: Quantum cryptography : Public key distribution and coin tossing. In: Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, pp. 175–179 (1984) 23

۲۳-Bennett, C.H., Brassard, G., Cr´epeau, C., Maurer, U.M.: Generalized privacy amplification. IEEE Trans. Inf. Theory 41(6), 1915–1923 (1995) 40, 42

۲۴-Brassard, G., Salvail, L.: Secret-key reconciliation by public discussion. In: EUROCRYPT, pp. 410–423 (1993) 34, 35, 36, 37, 38

۲۵-Bruss, D.: Optimal eavesdropping in quantum cryptography with six states. Phys. Rev. Lett81(14), 3018–3021 (1998) 23

۲۶- Carter, L., Wegman, M.N.: Universal classes of hash functions. J. Comput. Syst. Sci. 18(2), 143–154 (1979) 35

۲۷- Ekert, A.K.: Quantum cryptography based on bell's theorem. Phys. Rev. Lett. 67(6), 661–663(1991). DOI 10.1103/PhysRevLett.67.661 23

۲۸-Gilbert, G., Hamrick, M.: Practical quantum cryptography: A comprehensive analysis(part one) (2000). URL http://www.citebase.org/abstract?id=oai:arXiv.org:quant-ph/00%09027 30, 39

۲۹-Inamori, H., L¨utkenhaus, N., Mayers, D.: Unconditional security of practical quantum key distribution. Eur. Phys. J. D 41(3), 599–627 (2007) 46

۳۰-Lo, H.K., Chau, H.F., Ardehali, M.: Efficient quantum key distribution scheme and proof of its unconditional security. Journal of Cryptology 18, 133 (2005). URL http://www.citebase. org/abstract?id=oai:arXiv.org:quant-ph/0011056 26, 28, 29, 32

۳۱-L¨utkenhaus, N.: Estimates for practical quantum cryptography. Phys. Rev. A 59, 3301 (1999). URL http://www.citebase.org/abstract?id=oai:arXiv.org:quant-ph/9806008 43

۳۲-L¨utkenhaus, N.: Security against individual attacks for realistic quantum key distribution. Phys. Rev. A 61(5), 052,304 (2000). DOI 10.1103/PhysRevA.61.052304 43

۳۳-Meyer, T., Kampermann, H., Kleinmann, M., Bru, D.: Finite key analysis for symmetric attacks in quantum key distribution. Phys. Rev. A 74(4), 042,340 (2006) 46

۳۴-Nielsen, M.A., Chuang, I.L.: Quantum Computation and Quantum Information. Cambridge University Press, Cambridge (2000). URL http://www.amazon.ca/exec/obidos/redirect? tag=citeulike09-20% &path=ASIN/0521635039 24

۳۵-Renner, R.: Security of Quantum Key Distribution. Ph.D. thesis, Swiss Federal Institute of Technology 46

۳۶-Scarani, V., Acin, A., Ribordy, G., Gisin, N.: Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulses implementations. Phy. Rev. Lett. 92(5), 057,901 (2004) 23

۳۷-Scarani, V., Renner, R.: Quantum cryptography with finite resources: Unconditional security bound for discrete-variable protocols with one-way postprocessing. Phys. Rev. Lett. 100(20), 200,501 (2008) 46

۳۸-Smith, G., Renes, J.M., Smolin, J.A.: Better codes for BB84 with one-way post-processing(2006). URL http://www.citebase.org/abstract?id=oai:arXiv.org:quant-ph/0607018 32

۳۹-Tang, X., Ma, L., Mink, A., Nakassis, A., Xu, H., Hershmanand J. Bienfang, B., Su, D., Boisvert, R.F., Clark, C., Williams, C.: Quantum key distribution system operating at siftedkey

۴۰-rate over 4 Mbit/s. In: Quantum Information and Computation IV., Presented at the Society of Photo-Optical Instrumentation Engineers (SPIE) Conference, Vol. 6244 (2006). DOI 10.1117/12.664455 25

۴۱-Wegman, M.N., Carter, L.: New hash functions and their use in authentication and set equality. J. Comput. Syst. Sci. 22(3), 265–279 (1981) 44

۴۲-Xu, H., Ma, L., Mink, A., Hershman, B., Tang, X.: 1310-nm quantum key distribution system with up-conversion pump wavelength at 1550 nm. Optics Express 15, 7247–7260(2007) 26