Journal of Computing and Security

January 2018, Volume 5, Number 1 (pp. 52--52)

http://www.jcomsec.org

یک طرح با امنیت اثبات‌پذیر از ETRU بر اساس مشبکه‌های ایده‌آل توسعه‌یافته روی حاصل‌ضرب مستقیم حوزه‌های Dedekind

رضا ابراهیمی آتانی [آ,*]، شهاب الدین ابراهیمی آتانی [ب]، امیر حسنی کرباسی [ب]،

[آ] گروه مهندسی کامپیوتر دانشگاه گیلان، رشت، ایران.
[ب] دانشکده علوم ریاضی، دانشگاه گیلان، رشت، ایران.

اطلاعات مقاله

تاریخچه مقاله:
دریافت: 02 November 2016
اصلاح: 06 July 2018
پذیرش: 01 September 2018
انتشار آنلاین: 26 December 2018

کلمات کلیدی:
رمزنگاری مشبکه ـ مبنا، ETRU، مشبکه‌های ایده‌آل، حوزه‌های Dedekind، امنیت اثبات‌پذیر.

چکیده

یارویس و نوینز، برای اولین بار ETRU را در سال ۲۰۱۳ ارائه دادند که دارای عملکرد مناسب با اندازه کلید متعادل و مقاوم در برابر کامپیوترهای کوانتومی بود. ETRU، به عنوان یک الگوریتم رمزنگاری مشبکه مبنا با ساختار مشابه NTRUEncrypt، روی حلقه‌های اعداد صحیح ایزنشتاین است که کارایی بهتر و اندازه کلیدهای کوچکتری در سطح امنیتی یکسان با NTRUEncrypt دارد. از این رو جایگزین مطلوبی برای طرح‌های کلید عمومی با امنیت مبتنی بر تجزیه اعداد صحیح یا مسئله لگاریتم گسسته است. با این حال، به دلیل ساختار آن، شک و تردید در خصوص امنیت آن رخ داده است. در این مقاله پیشنهاد می‌دهیم که چگونه ETRU را تغییر دهیم که براساس فرضیات سختی کوانتومی مسائل استاندارد مشبکه‌ها در بدترین حالت و محدود به مشبکه‌های ایده آل توسعه یافته در ارتباط با گسترشی از ساختار میدان‌های دایره بر، امنیت آن را به طور اثبات پذیر تحلیل کنیم. ما ساختار تمام حلقه‌های خارج قسمتی چند جمله ای تولید شده را بروی حاصلضرب مستقیم حوزه‌های ددکیند Z و $Z[\zeta_3]$ ارائه می‌دهیم، بطوری که ζ_3 ریشه سوم واحد است. نشان می‌دهیم که اگر چندجمله ای کلید خصوصی ETRU از حاصلضرب مستقیم بعضی از حوزه‌های ددکیند انتخاب شده با استفاده از توزیع گوسی گسسته باشد، در این صورت کلید عمومی تمییزناگذیر آماری خواهد بود. در نهایت امنیت طرح را از سختی‌های پیش فرض R-SIS و R-LWE و گسترش آن‌ها ثابت می‌کنیم.

* نویسنده مسئول.
آدرس‌های رایانامه: rebrahimi@guilan.ac.ir (ر. ا. آتانی)،
ebrahimi@guilan.ac.ir (ش. ا. آتانی)،
karbasi@phd.guilan.ac.ir (ا. ح. کرباسی)

ISSN: 2322-4460