Journal of Marine Science and Technology

Spring 2025, Vol. 24, No.1, pp. 86-96.

Available Online: *http://jmst.kmsu.ac.ir*

Original Article

Improved Speed of RPrime RSA Cryptography Algorithm by Using a Residue Number System

Mohammad Esmaeildoust [1*], Mohammad Reza Noorimehr [2], Farnoosh Jahanbakhshi [3]

1. Faculty of Marine Engineering, Khorramshahr University of Marine Science and Technology, Khorramshahr, Iran.
2. Department of Computer Engineering, Ahvaz Branch, Islamic Azad University, Ahvaz, Iran.
3. Department of Computer Engineering, Karoon Institute of Higher Education, Ahvaz, Iran.

[*] **Corresponding Author E-mail:** m_doust@kmsu.ac.ir

Received: 21 August 2019 **Revise Date:** 29 February 2020 **Accepted:** 2 March 2020

DOI: 10.22113/jmst.2020.198899.2305

Abstract

With the growth of technology, the need for data and information security over communication channels is necessary. One of the most critical issues is establishing information security in marine communications. The RSA encryption algorithm is one of the most popular and most asymmetric algorithms used for secure data transfer. In the RSA encryption system, due to the very long key length, the encryption and decryption step speeds decrease, so it needs to improve its speed. One of the improved ways of RSA is RPrime RSA, which includes the highest decryption speed of RSA. In this paper, the encryption and decryption speed of the RPrime RSA algorithm is improved using an efficient residual number system. The result of implementation and comparison shows that the proposed method has an average of % 22% and % 36% improvement in the encryption and decryption speed over the RPrime RSA algorithm.

Keywords: RPrime RSA cryptography system, Security, Telecommunications marine environment, Residue Number System (RNS)

1. INTRODUCTION

Encryption algorithms are divided into two categories: symmetric (Beitabdollah et al., 2016) and public key (asymmetric) (Rivest et al., 1978). The RSA encryption system is one of the public key encryption algorithms. This algorithm was designed by Rivest, Shamir, and Edelman in 1978. This encryption system has attracted the attention of researchers in recent years as one of the most prominent asymmetric encryption methods due to its capabilities, such as high security and simplicity of use. Currently, prime factors of 1024 and 2048 bits are considered for complexity with a high workload. The main security parameter in RSA encryption is the length of the key; the longer it is, the more secure the communication becomes. However, increasing the length of the key can greatly reduce the speed of the encryption and decryption processes. In order to use these algorithms in maritime environments, such as communications between ships and also communications between ships and ground stations that require secure transmission of information, it is necessary to improve this algorithm in terms of encryption and decryption speed.

2. MATERIALS AND METHODS

The RPrime RSA method was introduced by Caesar in 2003 (Paixao Filho, 2003). The idea of this method is to combine two RSA methods, namely Rebalanced RSA and MultiPrime RSA, to further improve the decryption speed. The general idea of this scheme is to use the Rebalanced RSA key generation algorithm (modified for t components) together with the MultiPrime RSA decryption algorithm.

In the proposed method, first, an efficient residue number system is presented, and an efficient reverse converter is designed for the proposed modulus set. Then, the RPrime RSA algorithm is improved using the proposed residue number system. The residue number system increases the speed of computational operations by operating on a small parallel channel.

3. RESULTS

In this section, the proposed modulo set and the designed reverse converter are evaluated and compared with the works in the literature. Then, the RNS version of the RPrime RSA algorithm is evaluated with the RPrime RSA algorithm.

The results of the ASIC implementation for n =5, 15, 25, 35 are shown in Table 1. In this table, the performance of the proposed reverse converter is compared with the reverse converters introduced in (Mohan and Premkumar, 2007; Sousa et. al., 2012; Patronik and piestrak, 2017). According to the results, the proposed converter improves the hardware delay (AT) compared to the converters in the literature. Figure 1) shows the improvement in hardware (A), delay (T), and hardware-delay (AT) metrics compared to the schemes introduced in the studies (Mohan and Premkumar, 2007; Sousa et al., 2012; Patronik and piestrak, 2017).

4. CONCLUSION

In this paper, a new architecture is proposed to improve the speed of the RPrime RSA cryptography algorithm based on the residue number system. In order to increase the efficiency of the residue number system in the RPrime RSA algorithm, a balanced and well-formed moduli set and its efficient reverse converter with a two-level structure based on the New CRT-I algorithm were designed and implemented. The implementation results show that the proposed design has improved the encryption and decryption speed compared to the original RPrime RSA algorithm.

REFERENCES

Beitabdollah, M., Esmaeildoust M. and Kaabi, A., 2016. Performance Evaluation of Symmetric Key Cryptography Algorithms. *Journal of Marine Sceince and technology, 19*(1), pp. 404-455. https://doi.org/10.22113/jmst.2016.40455.

Mohan, P.A. and Premkumar, A.B., 2007. RNS-to-Binary Converters for Two Four-Moduli Sets $\{2^{n}-1, 2^{n}, 2^{n}+ 1, 2^{{n}+ 1}-1\} $ and $\{2^{n}-1, 2^{n}, 2^{n}+ 1, 2^{{n}+ 1}+ 1\} $. *IEEE Transactions on Circuits and Systems I: Regular Papers*, *54*(6), pp.1245-1254. https://doi.org/10.1109/TCSI.2007.895515

Paixao Filho, C.A.M., 2003. DLG: An efficient variant of the RSA cryptosystem. *Eprint Archive*.

Patronik, P. and Piestrak, S.J., 2017. Design of Reverse Converters for a New Flexible RNS Five-Moduli Set {2 k, 2 n-1, 2 n+ 1, 2 n+ 1-1, 2 n-1-1}(n Even). *Circuits, Systems, and Signal Processing*, *36*(11), pp.4593-4614. https://doi.org/10.1007/s00034-017-0530-9.

Rivest, R.L., Shamir, A. and Adleman, L., 1978. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM, 21*, pp. 120-126. https://doi.org/10.1145/359340.359342.

Sousa, L., Antão, S. and Chaves, R., 2012. On the Design of RNS Reverse Converters for the Four-Moduli Set ${\bf\{2^{\mmb n}+ 1, 2^{\mmb n}-1, 2^{\mmb n}, 2^{{\mmb n}+ 1}+ 1\}} $. *IEEE transactions on very large scale integration (VLSI) systems*, *21*(10), pp.1945-1949. 10.1109/TVLSI.2012.2219564

دوره ۲۴، شماره ۱، بهار ۱۴۰۴، صفحات ۸۶ تا ۹۶

مقاله پژوهشی

Available Online: *http://jmst.kmsu.ac.ir*

بهبود سرعت الگوریتم رمزنگاری RPrime RSA با استفاده از سیستم اعداد مانده‌ای

محمد اسماعیل‌دوست * [۱]، محمدرضا نوری‌مهر [۲]، فرنوش جهانبخشی [۳]

۱. دانشکده مهندسی دریا، دانشگاه علوم و فنون دریایی خرمشهر، خرمشهر، ایران.
۲. گروه مهندسی کامپیوتر، واحد اهواز، دانشگاه آزاد اسلامی، اهواز، ایران.
۳. گروه مهندسی کامپیوتر، مؤسسه آموزش عالی کارون، اهواز، ایران.

نویسنده مسئول، پست الکترونیک: m_doust@kmsu.ac.ir

تاریخ دریافت: ۱۳۹۸/۰۵/۳۰ **تاریخ بازنگری:** ۱۳۹۸/۱۲/۱۰ **تاریخ پذیرش:** ۱۳۹۸/۱۲/۱۲

شناسه دیجیتال (DOI):10.22113/jmst.2020.198899.2305

چکیده

با گسترش فناوری، نیاز به امنیت داده‌ها و اطلاعات بر روی بستر مخابراتی ضروری می‌باشد. یکی از موارد پر اهمیت برقراری امنیت اطلاعات در ارتباطات محیط‌های دریایی می‌باشد. سیستم رمزنگاری RSA یکی از گسترده‌ترین و محبوب‌ترین الگوریتم‌های رمزنگاری نامتقارن مورد استفاده در انتقال امن اطلاعات می‌باشد. در سیستم رمزنگاری RSA به دلیل طول بسیار بزرگ کلید، سرعت مرحله‌ی رمزنگاری و رمزگشایی کاهش می‌یابد، از این‌رو نیاز به بهبود سرعت در آن می‌باشد. یکی از روش‌های بهبودیافته‌ی RSA به نام RPrime RSA می‌باشد که دارای سرعت رمزگشایی بالاتری نسبت به RSA می‌باشد. در این مقاله، سرعت رمزنگاری و رمزگشایی الگوریتم RPrime RSA با استفاده از سیستم اعداد مانده‌ای کارا بهبود داده شده است. نتایج پیاده‌سازی و مقایسات نشان می‌دهد که روش پیشنهادی به طور متوسط موجب بهبود ۲۲٪ و ۳۶٪ در سرعت رمزنگاری و رمزگشایی نسبت به الگوریتم RPrime RSA شده است.

واژگان کلیدی: الگوریتم رمزنگاری RPrime RSA، امنیت، مخابرات محیط دریایی، سیستم اعداد مانده‌ای (RNS)

۱. مقدمه

الگوریتم‌های رمزنگاری به دو دسته متقارن (Beitabdollah et al., 2016) و کلید عمومی (نامتقارن) تقسیم می‌شوند (Rivest et al., 1978). سیستم رمزنگاری RSA، بعنوان یکی از الگوریتم‌های رمزنگاری کلید عمومی در سال 1977 توسط ریوست، شامیر و ادلمن طراحی شد. این سیستم رمزنگاری به دلیل قابلیت‌هایی چون امنیت بالا و سادگی ظاهر، در سال‌های اخیر به عنوان یکی از مطرح‌ترین شیوه‌های رمزنگاری نامتقارن مورد توجه محققان قرار گرفته است. امنیت این روش مبتنی بر سختی تجزیه اعداد اول می‌باشد. در حال حاضر عامل‌های اول ۱۰۲۴ و ۲۰۴۸ بیتی برای پیچیدگی با بار کاری بالا در نظر گرفته می‌شود. پارامتر اصلی امنیتی در رمزنگاری RSA طولی از کلید است که هر چه طولانی‌تر باشد، ارتباط امن‌تر می‌شود. با این حال افزایش طول کلید می‌تواند به شدت سرعت مراحل رمزنگاری و رمزگشایی را کاهش دهد. برای آنکه بتوان از این الگوریتم‌ها در محیط‌های دریایی مانند ارتباطات مابین کشتی‌ها و همچنین ارتباط کشتی‌ها با ایستگاه‌های زمینی که نیاز به انتقال امن اطلاعات دارند، استفاده کرد، نیاز است این الگوریتم را از نظر سرعت رمزنگاری و رمزگشایی بهبود بخشید.

برای بهبود سرعت الگوریتم رمزنگاری RSA تاکنون روش‌های مختلفی ارائه شده است. در مطالعه‌ی (Quisquater and Couvreur, 1982) محاسبات رمزگشایی با استفاده از قضیه باقیمانده چینی (CRT) (Jones and Jones., 1998) بر روی پیمانه‌ها و اعداد کوچک‌تری انجام می‌شود تا سرعت رمزگشایی بهبود یابد. برای بهبود سرعت رمزگشایی در پیام رمز شده با هزینه‌ی یک رمزگشایی RSA محاسبه می‌شود (Fiat, 1997). در مطالعه‌ی (Collins et al., 1998) با انتخاب مؤلفه‌های خصوصی کوچک سرعت رمزگشایی بهبود می‌یابد. در مطالعه‌ی (Takagi, 1998) با استفاده از تغییر ساختار پیمانه، سرعت مرحله‌ی رمزگشایی بهبود می‌یابد. جهت ارتقای سرعت رمزگشایی در مطالعه‌ی Paixao Filho (2003) دو روش RSA با نام Rebalanced RSA و MultiPrime RSA ترکیب می‌شود. برای کاهش زمان اجرای مرحله‌ی رمزگشایی RSA در مطالعه‌ی Asaduzzaman et al., (2015) از معماری CUDA استفاده شده است. سرعت الگوریتم رمزنگاری RSA در پژوهش Kayode et al. (2018) با استفاده از روش ضرب و مربع بهبود می‌یابد. با توجه به اینکه زمان اجرای رمزنگاری و رمزگشایی مسئله‌ی مهمی است، در این مقاله کار انجام شده مرتبط با بهبود سرعت مرحله‌ی رمزنگاری و رمزگشایی الگوریتم RPrime RSA است.

در ادامه ساختار مقاله به این صورت است که در بخش ۲ به صورت خلاصه روش RPrime RSA و سیستم اعداد مانده‌ای بیان می‌شود و به تشریح روش پیشنهادی پرداخته می‌شود. در بخش ۳ به ارزیابی نتایج و پیاده‌سازی روش پیشنهادی پرداخته شده است و در نهایت در بخش ۴ نتیجه‌گیری کلی این مقاله بیان شده است.

۲. مواد و روش‌ها

در این بخش الگوریتم رمزنگاری RPrime RSA و سیستم اعداد مانده‌ای (RNS) شرح داده می‌شود و سپس روش پیشنهادی و پیاده‌سازی آن ارائه می‌گردد.

روش RPrime RSA توسط Caesar در سال 2003 معرفی شد (Paixao Filho, 2003). ایده‌ی این روش، ترکیب دو روش RSA یعنی Rebalanced RSA و MultiPrime RSA جهت ارتقای بیشتر سرعت رمزگشایی است. ایده کلی این طرح، استفاده از الگوریتم تولید کلید Rebalanced RSA (اصلاح شده برای اجزای t) به همراه الگوریتم رمزگشایی MultiPrime RSA است. این الگوریتم شامل سه مرحله تولید کلید، رمزنگاری و رمزگشایی است که در ادامه به شرح آن‌ها پرداخته می‌شود.

در مرحله‌ی تولید کلید، برای تولید کلید با استفاده از الگوریتم Rebalanced RSA، ابتدا t عدد اول $p_1, p_2, \dots, p_t$ را انتخاب می‌کند و $N = \prod_{i=1}^{t} p_i$ را محاسبه می‌کند. سپس به صورت تصادفی اعداد s بیتی d_{p_i} به ازای $1 \le i \le t$ انتخاب می‌شود. در نهایت مؤلفه‌ی d توسط روش CRT با استفاده از d_{p_i} به ازای $1 \le i \le t$ محاسبه می‌شود.

در مرحله رمزنگاری، رمزنگاری مانند روش RSA است، اما به دلیل اینکه مؤلفه‌ی عمومی (e) در این روش نسبت به RSA بزرگ‌تر است، در نتیجه رمزنگاری پیام (M) نسبت به RSA هزینه‌ی بالاتری دارد.

در این روش در مرحله رمزگشایی ابتدا با استفاده از الگوریتم MultiPrime RSA و توسط معادله‌ی $M_i = c^{d_{p_i}} \bmod p_i$، M_i ها به ازای $1 \le i \le t$ محاسبه می‌شود. سپس M با استفاده از قضیه‌ی باقیمانده چینی (CRT) از روی M_iها بازیابی می‌شود.

در مطالعه‌ی Omondi و Premkumar (2007)، RNS توسط یک مجموعه پیمانه مانند $\{m_1, m_2, \dots, m_n\}$ که در آن همه پیمانه‌ها اعداد صحیح مثبت و اولی هستند تعریف می‌شود، که رنج

پویایی در $[0, M)$ موجود است و M به صورت رابطه (۱) محاسبه می‌شود:

در RNS یک عدد وزنی X $(0 \le X < M)$، یک عدد منحصر به فرد است و توسط $(x_1, x_2, \ldots, x_n)$ نمایش داده می‌شود به گونه‌ای که در رابطه (۲) آورده شده است.

قضیه باقیمانده‌ی چینی جدید-۱ (New-CRT-1) توسط (Wang ،2000) متناظر عدد باینری وزنی X را می‌توان با استفاده از باقیمانده‌های $(x_1, x_2, \ldots, x_n)$ به صورت رابطه (۳) محاسبه کرد؛ که در رابطه (۳) $k_1, k_2, \ldots, k_{n-1}$ معکوس‌های ضربی هستند.

در روش پیشنهادی ابتدا یک سیستم اعداد مانده‌ای کارا با مجموعه پیمانه پیشنهادی و مبدل‌معکوس کارآمد برای آن طراحی شده است. سپس الگوریتم RPrime RSA، با استفاده از سیستم اعداد مانده‌ای پیشنهادی بهبود داده می‌شود.

رابطه (۱)
$$M = \prod_{i=1}^{n} m_i$$

رابطه (۲)
$$x_i = X \mod m_i = |X|_{m_i}$$

رابطه (۳)
$$X = x_1 + m_1 \left| k_1(x_2 - x_1) + k_2 m_2 (x_3 - x_2) + \ldots + k_{n-1} m_2 m_3 \ldots m_{n-1}(x_n - x_{n-1}) \right|_{m_2 m_3 \ldots m_n}$$

رابطه (۴)
$$\left|k_1 \times m_1\right|_{m_2 m_3 \ldots m_n} = 1, \left|k_2 \times m_1 \times m_2\right|_{m_3 \ldots m_n} = 1, \ldots, \left|k_{n-1} \times m_1 \times m_2 \times \ldots \times m_{n-1}\right|_{m_n} = 1$$

سیستم اعداد مانده‌ای سرعت عملیات محاسباتی را بواسطه موازی‌سازی آن‌ها افزایش می‌دهد. برای بهبود الگوریتم RPrime RSA با استفاده از سیستم اعداد مانده‌ای نیاز می‌باشد که سیستم اعداد مانده‌ای با کارایی بالا ارائه شود. دو مطلب مهم که در طراحی کارآمد سیستم اعداد مانده‌ای وجود دارد، انتخاب مجموعه پیمانه و الگوریتم مبدل‌معکوس است. در این مقاله یک مجموعه‌ی ۴ پیمانه‌ای جدید $\{2^n, 2^{n+1}+1, 2^{n+1}-1, 2^n-1\}$ با رنج پویایی ۴n بیتی برای nهای فرد معرفی شده است که واحد محاسباتی آن به دلیل استفاده از پیمانه‌های متوازن و مناسب کارایی بالایی دارد. سپس یک مبدل معکوس کارا با ساختار دو سطحی و براساس قضیه باقیمانده چینی جدید-۱ (New-CRT-1) برای آن طراحی شده است.

برای طراحی یک مبدل معکوس کارا برای مجموعه‌ی ۴ پیمانه‌ای $\{2^n, 2^{n+1}+1, 2^{n+1}-1, 2^n-1\}$ با توجه به باقیمانده‌های متناظر آن (x_1, x_2, x_3, x_4)، معماری دو سطحی با استفاده از الگوریتم قضیه باقیمانده چینی جدید-۱ استفاده شده است. برای برای بدست آوردن عدد باینری Y، در سطح اول یک مبدل معکوس برای زیر مجموعه‌ی $\{2^n, 2^{n+1}+1, 2^{n+1}-1\}$ براساس باقیمانده‌های نمایش داده شده (x_1, x_2, x_3) طراحی شده است. سپس برای محاسبه‌ی وزن نهایی عدد X، در سطح دوم یک مبدل معکوس برای مجموعه‌ی ۲ پیمانه‌ای $\{2^n(2^{2n+2}-1), 2^n-1\}$ براساس نتیجه سطح اول (Y) و عدد مانده‌ای (x_4) طراحی شده است.

قبل از طراحی مبدل معکوس، ما ثابت می کنیم که پیمانه‌های استفاده شده در مجموعه پیمانه‌ی $\{2^n, 2^{n+1}+1, 2^{n+1}-1, 2^n-1\}$ برای nهای فرد نسبت به هم اول هستند.

قضیه ۱: پیمانه‌های 2^n، $2^{n+1}-1$ و 2^n-1 برای n های فرد نسبت به هم اول هستند.

اثبات: در مطالعه (Mohan and Premkumar, 2007)، مجموعه پیمانه‌ی $\{2^n-1, 2^n, 2^n+1, 2^{n+1}+1\}$ معرفی شده است که پیمانه‌های 2^n-1، 2^n و $2^{n+1}+1$ برای n فرد، دو به دو نسبت به هم اول می‌باشند. همچنین در مجموعه پیمانه‌ی $\{2^{n+1}-1, 2^n, 2^n-1\}$ (Lin et al., 2008)، ثابت شده است که پیمانه‌های 2^n-1، 2^n و $2^{n+1}-1$ دو به دو نسبت به هم اول هستند. درنهایت، از آنجایی که دو عدد صحیح متوالی همیشه نسبت به هم اول هستند، پیمانه‌های $2^{n+1}-1$ و $2^{n+1}+1$ نیز نسبت به هم اول هستند.

اکنون برای طراحی مبدل معکوس سطح اول، برای زیر مجموعه‌ی $\{2^n, 2^{n+1}+1, 2^{n+1}-1\}$ روش معرفی شده در مطالعه‌ی (Lin et al., 2008) استفاده شده است. در مطالعه (

{2^{α}, $2^{\beta}-1$, $2^{\beta}+1$} مجموعه پیمانه‌ی عمومی (Molahosseini et al., 2008 که $\alpha<\beta$ است، معرفی شده است. با جایگزین کردن $\alpha=n$ و $\beta=n+1$ در مجموعه پیمانه‌ی عمومی {2^{α}, $2^{\beta}-1$, $2^{\beta}+1$}، مجموعه پیمانه‌ی {2^{n}, $2^{n+1}+1$, $2^{n+1}-1$} بدست می‌آید. بنابراین، معادله‌های مورد نیاز الگوریتم مبدل معکوس برای مجموعه پیمانه‌ی {2^{n}, $2^{n+1}+1$, $2^{n+1}-1$} را می‌توان با استفاده از روش معرفی شده در مطالعه‌ی (Molahosseini et al., 2008) به صورت رابطه (۵) نوشت. با توجه به نتایج بدست آمده از سطح اول (Y) و عدد مانده‌ای (x_4)، عدد وزنی نهایی X می‌تواند براساس قضیه باقیمانده چینی جدید-۱ و با توجه به مجموعه پیمانه‌ی {2^{n} (2^{2n+2}) $2^{n}-1$}, (-1) به شرح (۱۰) تعیین شود.

که K، معکوس ضربی $2^{n}(2^{2n+2}-1)$ به پیمانه‌ی $(2^{n}-1)$ است و به صورت (۱۱) محاسبه می‌شود:

$$Y = x_1 + 2^n L = \underbrace{L_{2n+1}\dots L_1 L_0}_{2n+2}\underbrace{x_{1,n-1}\dots x_{1,1}x_{1,0}}_{n}$$

رابطه (۵)

$$L = \left|L_1 + L_2 + L_3\right|_{2^{2n+2}-1}$$

که رابطه (۶)

$$L_1 = \underbrace{x_{2,n}\dots x_{2,0}}_{n+1}\underbrace{0\dots 0}_{n}x_{2,n+1}$$

رابطه (۷)

$$L_2 = \underbrace{\bar{x}_{1,n-1}\dots\bar{x}_{1,0}}_{n}\underbrace{\bar{x}_{2,n+1}\dots\bar{x}_{2,0}}_{n+2}$$

رابطه (۸)

$$L_3 = \underbrace{x_{3,n}\dots x_{3,0}}_{n+1}\underbrace{x_{3,n}\dots x_{3,0}}_{n+1}$$

رابطه (۹)

$$X = Y + 2^n(2^{2n+2}-1)\left|k(x_4 - y)\right|_{2^n-1}$$

رابطه (۱۰)

$$\left|k\times 2^n(2^{2n+2}-1)\right|_{2^n-1} = 1 \Rightarrow k = \sum_{i=0}^{\frac{(n-1)}{2}} 2^{2i}$$

رابطه (۱۱)

با توجه به اینکه سیستم اعداد مانده‌ای کارا با مجموعه پیمانه‌ی جدید و مبدل‌معکوس کارا برای آن پیشنهاد شد که در ادامه سرعت محاسبات پیمانه‌ای مرحله‌ی رمزنگاری و رمزگشایی الگوریتم RPrime RSA با استفاده از سیستم اعداد مانده‌ای پیشنهادی بهبود داده می‌شود.

در الگوریتم RPrime RSA، متن اصلی پیام (M) با استفاده از رابطه‌ی ($C = M^e \bmod n$) رمز می‌شود. برای کاهش پیچیدگی توان‌رسانی و بهبود سرعت عملیات در این رابطه، می‌توان (M^e) را با استفاده از سیستم اعداد مانده‌ای محاسبه نمود تا سرعت عملیات رمزنگاری بهبود یابد.

روش پیشنهادی در مرحله‌ی رمزنگاری به شرح زیر است:

- مجموعه پیمانه $\{b_1, b_2, b_3, b_4\} = \{2^n, 2^n - 1, 2^{n+1} - 1, 2^{n+1} + 1\}$ و مؤلفه‌ی عمومی (e) به عنوان ورودی دریافت می‌شود.
- متن پیام (M) در سیستم اعداد مانده‌ای، با استفاده از مجموعه پیمانه $\{b_1, b_2, b_3, b_4\} = \{2^n, 2^n - 1, 2^{n+1} - 1, 2^{n+1} + 1\}$ به نمایش RNS تبدیل می‌شود:

$$M \to (m_1, m_2, m_3, m_4)_{RNS} = (m_j)_{RNS}, 1 \le j \le 4$$

- در واحد حساب به ازای $1 \le j \le 4$، $(m_j^e \bmod b_j) = (w_j)$ محاسبه می‌شود و (w_1, w_2, w_3, w_4) حاصل می‌شود.
- با استفاده از قضیه باقیمانده چینی جدید-۱ (New CRT-1) معرفی شده، حاصل بدست آمده از مرحله‌ی قبل (w_1, w_2, w_3, w_4) از نمایش RNS خارج می‌شود.

$$(w_1, w_2, w_3, w_4)_{RNS} \to M^e$$

- در نهایت $C = M^e \ mod \ n$ محاسبه می‌شود.

برای رمزگشایی C (متن رمز شده) در الگوریتم RPrime RSA، ابتدا $(M_i = c^{d_{p_i}} \ mod \ p_i \ , 1 \le i \le t)$ محاسبه می‌شود، سپس M (متن اصلی پیام) با استفاده از الگوریتم CRT حاصل می‌شود. پیچیدگی توان‌رسانی محاسبات رمزگشایی RPrime RSA را می‌توان همانند عملیات رمزنگاری با استفاده از سیستم اعداد مانده‌ای پیشنهادی کاهش داد.

روش پیشنهادی در مرحله‌ی رمزگشایی به شرح زیر می‌باشد:

- مجموعه پیمانه $\{b_1, b_2, b_3, b_4\} = \{2^n, 2^n - 1, 2^{n+1} - 1, 2^{n+1} + 1\}$ و مؤلفه‌های خصوصی $\left(\mathrm{d}_{p_i} \ , \ 1 \le i \le t\right)$ به عنوان ورودی دریافت می‌شود.
- متن رمز شده (C) در سیستم اعداد مانده‌ای، با استفاده از مجموعه پیمانه $\{b_1, b_2, b_3, b_4\} = \{2^n, 2^n - 1, 2^{n+1} - 1, 2^{n+1} + 1\}$ به نمایش RNS تبدیل می‌شود:

$$C \ \rightarrow (c_1, c_2, c_3, c_4)_{RNS} = \left(c_j\right)_{RNS} \ , \ 1 \le j \le 4$$

- در واحد حساب به ازای $1 \le i \le t$ و $1 \le j \le 4$، $\left(c_j{}^{d_{p_i}} \ mod \ b_j\right) = \left(w_j\right)$ محاسبه می‌شود و (w_1, w_2, w_3, w_4) حاصل می‌شود.
- با استفاده از قضیه باقیمانده چینی جدید-۱ (New CRT-1) معرفی شده، حاصل بدست آمده از مرحله‌ی قبل (w_1, w_2, w_3, w_4) از نمایش RNS خارج می‌شود.

$$(w_1, w_2, w_3, w_4)_{RNS} \rightarrow c^{d_{p_i}} \ , \ 1 \le i \le t$$

- سپس $M_i = c^{d_{p_i}} \ mod \ p_i \ , 1 \le i \le t$ محاسبه می‌شود و در نهایت با استفاده از الگوریتم CRT به نمایش استاندارد M تبدیل می‌شود.

در سیستم اعداد مانده‌ای به دلیل اینکه محاسبات بر روی اعداد کوچک‌تر و به صورت موازی انجام می‌شود، از این‌رو موجب بهبود سرعت مرحله رمزنگاری و رمزگشایی الگوریتم RPrime RSA می‌شود.

۳. نتایج و بحث

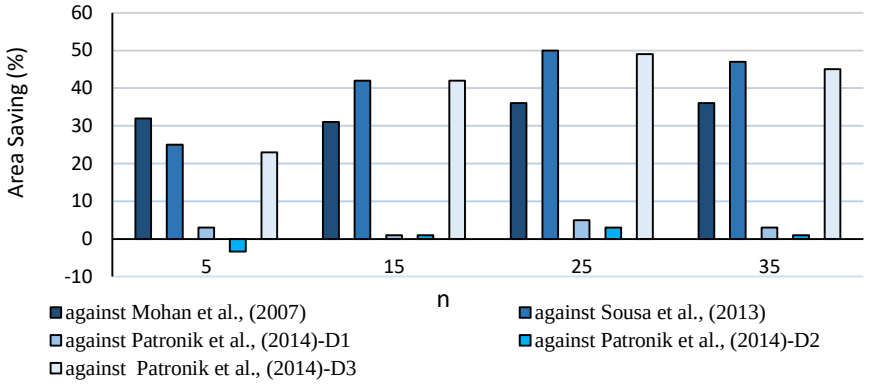
در این بخش، ابتدا به ارزیابی مجموعه پیمانه‌ی پیشنهادی $\{2^n, 2^n - 1, 2^{n+1} - 1, 2^{n+1} + 1\}$ و مبدل معکوس طراحی شده برای آن پرداخته شده است. سپس نسخه‌ی RNS الگوریتم RPrime RSA با الگوریتم RPrime RSA مورد ارزیابی قرار گرفته است.

نتایج پیاده‌سازی ASIC برای $n = 5, 15, 25, 35$ در جدول (۱) نشان داده شده است. در این جدول، کارایی مبدل‌معکوس پیشنهادی با مبدل معکوس‌های معرفی شده در مطالعات (Mohan and Premkumar, 2007; Sousa et al., 2012; Patronik and piestrak, 2017) مورد مقایسه قرار گرفته است. باتوجه به نتایج، مبدل پیشنهادی در مقایسه با مبدل کارهای مرتبط، معیار سخت‌افزار-تأخیر (AT) را بهبود می‌بخشد. شکل (۱) بهبود معیار سخت‌افزار (A)، تأخیر (T) و سخت‌افزار-تأخیر (AT) را نسبت به طرح‌های معرفی شده در مطالعات (Mohan and Premkumar, 2007; Sousa et al., 2012; Patronik and piestrak, 2017) نشان می‌دهد.

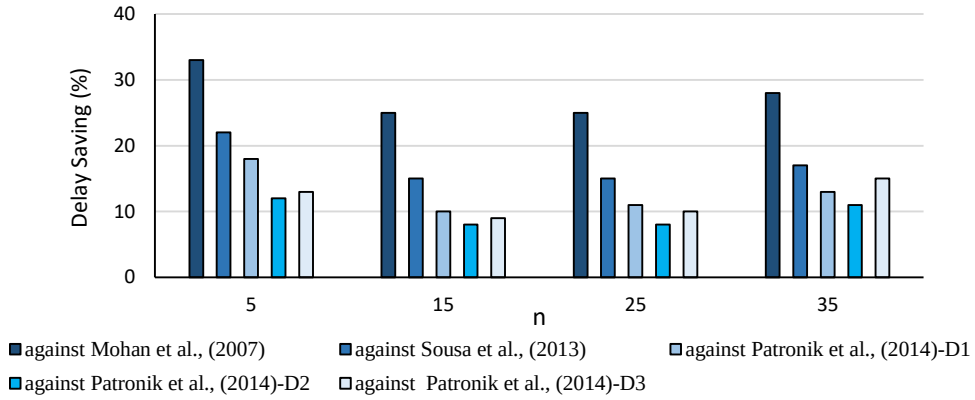
شکل ۱(الف) میزان کاهش هزینه سخت‌افزاری را نسبت به سایر مبدل‌ها نشان می‌دهد. تنها یک مبدل در مطالعه (Patronik and piestrak, 2014) ارائه شده است، که برای n=5 نیاز به سخت‌افزار کمتری دارد. شکل ۱(ب) بهبود تأخیر مبدل پیشنهادی را نسبت به سایر مبدل‌ها نشان می‌دهد. همچنین شکل ۱(ج) نشان می‌دهد که مبدل‌معکوس پیشنهادی، نسبت به مبدل‌های معرفی شده در (Mohan and Premkumar, 2007; Sousa et al., 2012; Patronik and piestrak, 2014) به طور متوسط معیار AT را به ترتیب ۵۲٪، ۵۲٪، ۱۵٪، ۱۰٪ و ۴۷٪ بهبود داده است.

در جدول (۲) نتایج زمان اجرای رمزنگاری و رمزگشایی برای طول کلیدهای ۱۰۲۴، ۲۰۴۸ و ۴۰۹۶ بیتی مورد ارزیابی قرار گرفته است. همان‌طور که جدول (۲) نشان می‌دهد، استفاده از سیستم اعداد مانده‌ای و مجموعه پیمانه‌ی متوازن $\{2^n+1, 2^n, 2^n-1, 2^{n-1}+1\}$ به ازای طول کلیدهای ۱۰۲۴، ۲۰۴۸ و ۴۰۹۶ بیتی موجب بهبود سرعت نسخه‌ی RNS الگوریتم RPrime RSA نسبت به RPrime RSA شده است.

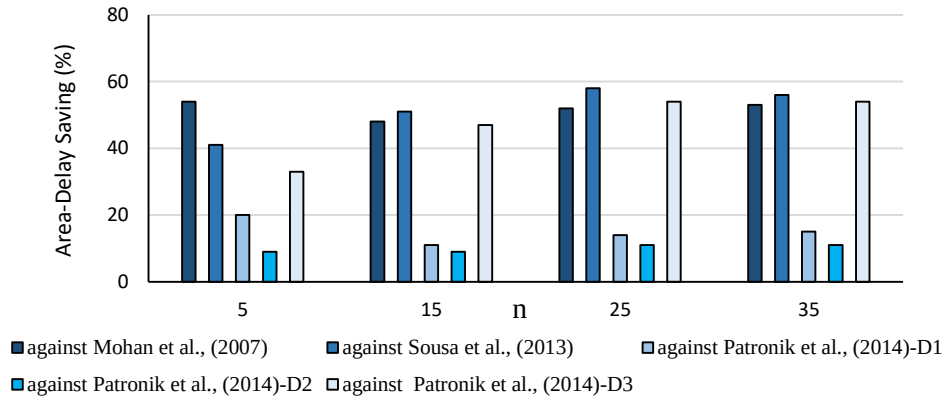
شکل (۲) سرعت رمزنگاری و رمزگشایی الگوریتم RPrime RSA با نسخه‌ی RNS الگوریتم RPrime RSA را نسبت به هم مورد ارزیابی قرار داده است. همانطور که شکل ۲ نشان می‌دهد، به ازای طول کلیدهای ۱۰۲۴، ۲۰۴۸ و ۴۰۹۶ بیتی به ترتیب موجب بهبود سرعت مرحله‌ی رمزنگاری ۲۸٪، ۱۸٪ و ۱۸٪ نسبت به RPrime RSA می‌شود. همچنین در مرحله رمزگشایی به ترتیب موجب بهبود ۳۸٪، ۳۸٪ و ۳۱٪ نسبت به RPrime RSA می‌شود.



(الف)



(ب)



(ج)

شکل ۱- مقایسه‌ی معیار سخت‌افزار (الف)، تأخیر (ب) و سخت‌افزار – تأخیر (ج) برای رنج پویایی ۵، ۱۵، ۲۵ و ۳۵

Fig. 1- Comparison with the state of the art (a) Area, (b) Delay, (g) Area-Delay for dynamic ranges 5, 15, 25, 35.

جدول ۱- نتایج پیاده‌سازی مبدل‌های مختلف

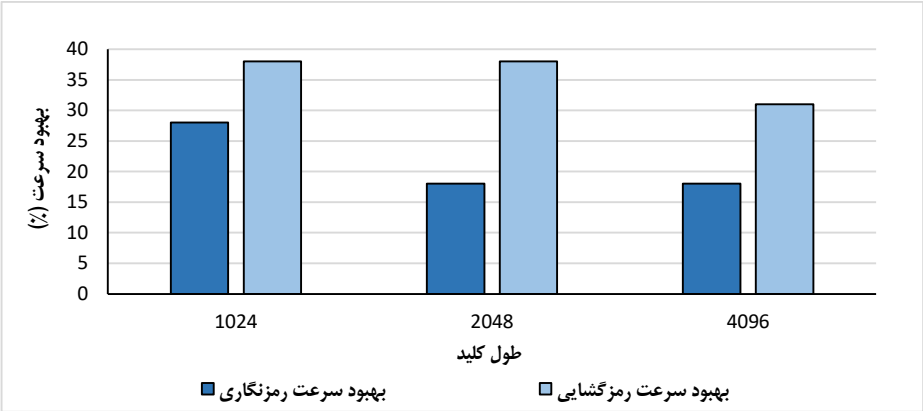
Table 1. Synthesize results of the different converters

n	Converter	A ($10\mu m^2$)	T (ns)	AT (ns×$10\mu m^2$)
5	Mohan and Premkumar (2007)	576	0.91	524
	Sousa et al., (2012)	524	0.78	408
	Patronik and piestrak (2017)-D1	407	0.74	302
	Patronik and piestrak (2017)-D2	384	0.69	264
	Patronik and piestrak (2017)-D3	512	0.70	358
	proposed	397	0.61	242
15	Mohan and Premkumar (2007)	2227	1.58	3518
	Sousa et al., (2012)	2663	1.39	3701
	Patronik and piestrak (2017)-D1	1559	1.32	2057
	Patronik and piestrak (2017)-D2	1560	1.29	2012
	Patronik and piestrak (2017)-D3	2637	1.30	3428
	Proposed	1551	1.19	1845
25	Mohan and Premkumar (2007)	4636	1.99	9225
	Sousa et al., (2012)	5978	1.76	10521
	Patronik and piestrak (2017)-D1	3138	1.67	5240
	Patronik and piestrak (2017)-D2	3098	1.63	5049
	Patronik and piestrak (2017)-D3	5897	1.65	9730
	proposed	3007	1.5	4510
35	Mohan and Premkumar (2007)	7839	2.5	19597
	Sousa et al., (2012)	9487	2.19	20776
	Patronik and piestrak (2017)-D1	5184	2.08	10783
	Patronik and piestrak (2017)-D2	5087	2.03	10326
	Patronik and piestrak (2017)-D3	9198	2.14	19683
	Proposed	5070	1.82	9227

جدول ۲- مقایسه زمان اجرای رمزنگاری و رمزگشایی

Table 2- Execution time comparison of encryption and decryption

الگوریتم رمزنگاری		RPrime RSA	RPrime RSA with RNS
زمان اجرا (ms)	n=1024	رمزنگاری	۱۶۶	۱۲۱
		رمزگشایی	۹۷	۶۱
	n=2048	رمزنگاری	۲۳۸	۱۹۷
		رمزگشایی	۱۶۷	۱۰۵
	n=4096	رمزنگاری	۳۱۷	۲۶۳
		رمزگشایی	۲۴۱	۱۶۸



شکل ۲- مقایسه سرعت رمزنگاری و رمزگشایی مدل پیشنهادی نسبت به RPrime RSA

Fig. 2- Speed comparison of encryption and decryption of the proposed model with RPrime RSA

٤. نتیجه‌گیری

در این مقاله، یک معماری جدید برای بهبود سرعت الگوریتم رمزنگاری RPrime RSA بر پایه‌ی سیستم اعداد مانده‌ای ارائه شد. به منظور افزایش کارایی سیستم اعداد مانده‌ای در الگوریتم RPrime RSA، مجموعه پیمانه‌ی بهینه $\{2^n, 2^{n+1}+1, 2^{n+1}-1, 2^n-1\}$ و مبدل‌معکوس کارا با ساختار دو سطحی و مبتنی بر الگوریتم New CRT-I برای آن طراحی شد که با هدف انجام محاسبات سریع مورد استفاده قرار گرفت. نتایج پیاده‌سازی نشان می‌دهد که روش پیشنهادی موجب بهبود سرعت رمزنگاری و رمزگشایی نسبت به الگوریتم RPrime RSA شده است.

Refrences:

Asaduzzaman, A., Gummadi, D. and Waichal, P., 2015, April. A promising parallel algorithm to manage the RSA decryption complexity. In *SoutheastCon 2015* (pp. 1-5). IEEE. DOI: 10.1109/SECON.2015.7132926

Beitabdollah, M., Esmaeildoust M. and Kaabi, A., 2016. Performance Evaluation of Symmetric Key Cryptography Algorithms. *Journal of Marine Sceince and technology*, *19*(1), pp. 404-455. https://doi.org/10.22113/jmst.2016.40455.

Collins, T., Hopkins, D., Langford, S. and Sabin, M., Tandem Computers Inc, 1998. *Public key cryptographic apparatus and method*. U.S. Patent 5,848,159.

Fiat, A. 1997. Batch RSA. *Journal of Cryptology*, *10*(2), pp.75–88. https://doi.org/10.1007/s001459900021.

Jones, G.A. and Jones, J.M., 1998. *Elementary number theory*. Springer Science & Business Media.

Kayode, S.Y. and Alagbe, G.K., 2018. RSA Cryptosystem Encryption Based on Three Moduli Set with Common Factor {2n+ 2, 2n+ 1, 2n}. *Computing and Information Systems*, *22*(3), pp.27-34.

Lin, S.H., Sheu, M.H. and Wang, C.H., 2008. Efficient VLSI design of residue-to-binary converter for the moduli set (2 n, 2 n+ 1-1, 2 n-1). *IEICE transactions on information and systems*, *91*(7), pp.2058-2060. DOI: 10.1093/ietisy/e91-d.7.2058

Mohan, P.A. and Premkumar, A.B., 2007. RNS-to-Binary Converters for Two Four-Moduli Sets $\{2^{n}-1, 2^{n}, 2^{n}+ 1, 2^{{n}+ 1}-1\} $ and $\{2^{n}-1, 2^{n}, 2^{n}+ 1, 2^{{n}+ 1}+ 1\} $. *IEEE Transactions on Circuits and Systems I: Regular Papers*, *54*(6), pp.1245-1254. DOI: 10.1109/TCSI.2007.895515

Molahosseini, A.S., Navi, K., Hashemipour, O. and Jalali, A., 2008. An efficient architecture for designing reverse converters based on a general three-moduli set. *journal of Systems Architecture*, *54*(10), pp.929-934. https://doi.org/10.1016/j.sysarc.2008.03.006

Omondi, A.R. and Premkumar, A.B., 2007. *Residue number systems: theory and implementation*

(Vol. 2). World Scientific. https://doi.org/10.1142/p523

Paixao Filho, C.A.M., 2003. DLG: An efficient variant of the RSA cryptosystem. *Eprint Archive*.

Patronik, P. and Piestrak, S.J., 2017. Design of Reverse Converters for a New Flexible RNS Five-Moduli Set {2 k, 2 n-1, 2 n+ 1, 2 n+ 1-1, 2 n-1-1}(n Even). *Circuits, Systems, and Signal Processing*, *36*(11), pp.4593-4614. https://doi.org/10.1007/s00034-017-0530-9.

Quisquater, J.J. and Couvreur, C., 1982. Fast decipherment algorithm for RSA public-key cryptosystem. *Electronics letters*, *18*(21), pp.905-907. https://doi.org/10.1049/el:19820617

Rivest, R.L., Shamir, A. and Adleman, L., 1978. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, *21*, pp. 120-126. https://doi.org/10.1145/359340.359342.

Sousa, L., Antão, S. and Chaves, R., 2012. On the Design of RNS Reverse Converters for the Four-Moduli Set ${\bf\{2^{\mmb n}+ 1, 2^{\mmb n}-1, 2^{\mmb n}, 2^{{\mmb n}+ 1}+ 1\}} $. *IEEE transactions on very large scale integration (VLSI) systems*, *21*(10), pp.1945-1949. 10.1109/TVLSI.2012.2219564

Takagi, T., 1998, August. Fast RSA-type cryptosystem modulo pkq. In *Annual International Cryptology Conference* (pp. 318-326). Berlin, Heidelberg: Springer Berlin Heidelberg.

Wang, Y., 2000. Residue-to-binary converters based on new Chinese remainder theorems. *IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing*, *47*(3), pp.197-205. http://dx.doi.org/10.1109/82.826745.