انجمن کامپیوتر ایران
Computer Society of Iran
جزیره کیش، خلیج فارس، ایران ۱۹ الی ۲۱ اسفند ۱۳۸۶
دانشگاه صنعتی شریف
دانشکده مهندسی کامپیوتر
پوستر

مبدل مانده‌ای به دودوئی جدید

امیر صباغ ملاحسینی
گروه مهندسی کامپیوتر
دانشگاه آزاد اسلامی واحد علوم و تحقیقات، تهران، ایران
amir.sabbagh@sr.iau.ac.ir

کیوان ناوی
دانشکده مهندسی برق و کامپیوتر
دانشگاه شهید بهشتی، تهران، ایران
navi@sbu.ac.ir

چکیده: سیستم اعداد مانده‌ای یک سیستم عددی بدون انتشار رقم نقلی است که انجام محاسبات را بصورت موازی و با سرعت زیاد ممکن می سازد. انتخاب مجموعه پیمانه و تبدیل عدد مانده‌ای به معادل دودوئی آن، دو مورد از مهمترین مسائل در طراحی یک سیستم اعداد مانده‌ای هستند. در این مقاله، ما یک مبدل مانده‌ای به دودوئی کارا برای مجموعه پیمانه جدید $\{2^{n-1}, 2^{n+1}+1, 2^{n+1}-1\}$ ارائه می‌کنیم. این مجموعه پیمانه جدید شامل پیمانه‌های دوبه‌دو نسبت به هم اول و متعادل است که منجر به انجام سریع محاسبات در سیستم اعداد مانده-ای و نیز پیاده‌سازی کارای مبدل مانده‌ای به دودوئی می‌شود. ساختار سخت افزاری مبدل مانده‌ای به دودوئی پیشنهاد شده، از یک جمع کننده ذخیره رقم نقلی و یک جمع کننده پیمانه‌ای انتشار رقم نقلی تشکیل شده است. در مقایسه با دیگر مبدل‌های مانده‌ای به دودوئی برای مجموعه پیمانه‌های شبیه به مجموعه پیمانه جدید پیشنهادی، مبدل مانده‌ای به دودوئی پیشنهاد شده دارای سرعت بیشتر و هزینه سخت افزاری کمتر است.

واژه های کلیدی: مبدل مانده‌ای به دودوئی، سیستم اعداد مانده‌ای، حساب کامپیوتر، طراحی مدارهای مجتمع در مقیاس بسیار بزرگ.

۱- مقدمه

هدف از طراحی سیستم‌های VLSI، کاهش هزینه و بهبود کارائی بر حسب پیچیدگی، سرعت و توان مصرفی است. یکی از روش‌های طراحی سیستم‌های VLSI دارای توان مصرفی کم و سرعت زیاد، استفاده از سیستم اعداد مانده‌ای[i] است [1]. در سیستم اعداد مانده‌ای اعمال محاسباتی در هر پیمانه مستقل از پیمانه‌های دیگر است و در نتیجه اعمال جمع، تفریق و ضرب بدون انتشار رقم نقلی و بصورت موازی و با سرعت زیاد انجام می‌شوند [2,3].

با توجه به خاصیت عدم انتشار رقم نقلی در اعمال حسابی جمع، تفریق و ضرب، سیستم اعداد مانده‌ای در سیستم‌های محاسباتی از قبیل پردازش سیگنال‌های دیجیتال [4-6]، سیستم رمز RSA [7] و تشخیص و تصحیح خطا [8] کاربرد فراوانی دارد.

انتخاب مجموعه پیمانه اهمیت زیادی در سیستم اعداد مانده‌ای دارد زیرا محدوده دینامیکی و سرعت انجام اعمال محاسباتی در سیستم اعداد مانده‌ای بستگی به تعداد و فرم پیمانه‌های انتخاب شده دارد. همچنین انتخاب یک مجموعه پیمانه مناسب منجر به ساده شدن طراحی مبدل مانده‌ای به دودوئی[ii] می‌شود. تاکنون مجموعه پیمانه‌های مختلفی بررسی شده است. از میان آنها مجموعه پیمانه‌های سه‌تایی مورد توجه بیشتری قرار گرفته‌اند مانند مجموعه پیمانه‌های $\{2^n-1, 2^n, 2^n+1\}$ [9,10]، $\{2^{n-1}-1, 2^n-1, 2^n\}$ [11]، $\{2^n-1, 2^n, 2^{n+1}-1\}$ [12] و $\{2^n-1, 2^n+1, 2^{2n}+1\}$ [13].

علاوه بر انتخاب مجموعه پیمانه مناسب برای طراحی مبدل مانده‌ای به دودوئی، مورد مهم دیگر انتخاب الگوریتم تبدیل است. الگوریتم‌های تبدیل عدد مانده‌ای به معادل دودوئی وزنی آن عمدتا بر پایه تئوری باقیمانده چینی[iii] و تبدیل درهم مبنا[iv] است [2]. اخیرا تئوری‌های باقیمانده چینی جدید[v] پیشنهاد شده است [14] که مزایای تئوری باقیمانده چینی متداول و تبدیل درهم مبنا را باهم دارد.

در این مقاله، ما ابتدا با توجه به ویژگی‌های تئوری باقیمانده چینی جدید ۱، مجموعه پیمانه سه‌تایی جدید $\{2^{n-1}, 2^{n+1}+1, 2^{n+1}-1\}$ را پیشنهاد می‌کنیم. این مجموعه پیمانه جدید شامل پیمانه‌های دوبه‌دو نسبت به هم اول و متعادل است که منجر به انجام سریع محاسبات در سیستم اعداد مانده‌ای و نیز پیاده‌سازی کارای مبدل مانده‌ای به دودوئی می-شود. سپس، یک مبدل مانده‌ای به دودوئی کارا برای این مجموعه پیمانه با استفاده از تئوری باقیمانده چینی جدید ۱ ارائه می‌کنیم. مبدل مانده‌ای به دودوئی پیشنهاد شده دارای سرعت بیشتر و هزینه سخت افزاری کمتر نسبت به دیگر مبدل‌های مانده‌ای به دودوئی برای مجموعه پیمانه‌های شبیه به مجموعه پیمانه جدید پیشنهادی است.

در ادامه مقاله، در بخش ۲ پیش‌زمینه لازم بررسی می‌شود. مبدل مانده‌ای به دودوئی پیشنهادی در بخش ۳ ارائه می‌شود. ارزیابی کارایی مبدل برحسب تاخیر تبدیل و هزینه سخت افزاری مبدل در بخش ۴ انجام می‌شود و بخش ۵ نتیجه‌گیری است.

۲- پیش زمینه

سیستم اعداد مانده‌ای: سیستم اعداد مانده‌ای یک سیستم عددی صحیح است که بر حسب تعدادی اعداد دوبه‌دو نسبت به هم اول که مجموعه پیمانه را تشکیل می‌دهند تعریف می‌شود. در سیستم اعداد مانده‌ای با مجموعه پیمانه $\{P_1,P_2,\ldots,P_n\}$، عدد وزنی X بصورت $X=(x_1,x_2,\ldots,x_n)$ نمایش داده می‌شود که:

$$x_i = X \bmod P_i = |X|_{P_i}, 0 \le x_i < P_i \qquad (۱)$$

این نمایش مانده‌ای برای هر عدد صحیح در محدوده $[0,M-1]$ منحصر به فرد است. که $M=P_1P_2\ldots P_n$ محدوده دینامیکی سیستم نامیده می‌شود.

جمع، تفریق و ضرب بر روی باقیمانده‌ها بصورت موازی و بدون انتشار رقم نقلی مابین ارقام مانده‌ای انجام می‌شوند. از این رو، سیستم اعداد مانده‌ای با تبدیل محاسبات بر روی اعداد بزرگ به مجموعه‌ای از محاسبات موازی بر روی اعداد کوچک، به میزان قابل توجهی موجب افزایش سرعت محاسبات می‌شود.

تبدیل یک عدد صحیح وزنی دودوئی به نمایش مانده‌ای، تبدیل دودوئی به مانده‌ای[vi] و عکس آن، یعنی تبدیل از نمایش مانده‌ای به نمایش وزنی دودوئی تبدیل مانده‌ای به دودوئی نامیده می‌شود. تبدیل دودوئی به مانده‌ای عملی ساده است و توسط جمع کننده‌های پیمانه‌ای قابل پیاده‌سازی است ولی تبدیل مانده‌ای به دودوئی با پیچیدگی زیادی همراه است. الگوریتم‌های تبدیل مانده‌ای به دودوئی عمدتا برپایه تئوری باقیمانده چینی، تبدیل درهم مبنا و تئوری باقیمانده چینی جدید هستند.

تئوری باقیمانده چینی: توسط تئوری باقیمانده چینی عدد وزنی X بصورت زیر از نمایش مانده‌ای بدست می‌آید:

$$X = \left| \sum_{i=1}^{n} |x_i N_i|_{P_i} M_i \right|_M \qquad (۲)$$

که $M_i = M/P_i$ و $N_i = |M_i^{-1}|_{P_i}$ معکوس ضربی M_i در پیمانه P_i است.

تبدیل درهم مبنا: توسط تبدیل درهم مبنا عدد وزنی X بصورت زیر محاسبه می‌شود:

$$X = a_n \prod_{i=1}^{n} P_i + \ldots + a_3 P_2 P_1 + a_2 P_1 + a_1 \qquad (۳)$$

که a_i ها ضرایب درهم مبنا نامیده می‌شوند و بصورت زیر محاسبه می‌شوند:

$$a_n = \left| (((x_n - a_1)|P_1^{-1}|_{P_n} - a_2)|P_2^{-1}|_{P_n} - \cdots - a_{n-1})|P_{n-1}^{-1}|_{P_n} \right|_{P_n} \qquad (۴)$$

که $n>1$ و $a_1=x_1$ است.

تبدیل درهم مبنا یک الگوریتم ترتیبی است و مانند تئوری باقیمانده چینی موازی نیست. و از طرفی تئوری باقیمانده چینی نیاز به عملیات در پیمانه M(عددی بزرگ) دارد که هر دو برای پیاده‌سازی سخت افزاری کارا مناسب نیستند.

تئوری باقیمانده چینی جدید ۱ : توسط تئوری باقیمانده چینی جدید ۱ [14]، عدد X بصورت زیر بدست می‌آید:

$$X = x_1 + P_1 \left| \begin{matrix} k_1(x_2 - x_1) + k_2 P_2 (x_3 - x_2) + \cdots \\ + k_{n-1} P_2 P_3 \cdots P_{n-1}(x_n - x_{n-1}) \end{matrix} \right|_{P_2 P_3 \cdots P_n} \qquad (۵)$$

بطوریکه

$$|k_1 \times P_1|_{P_2 P_3 \cdots P_n} = 1$$
$$|k_2 \times P_1 \times P_2|_{P_3 \cdots P_n} = 1$$
$$\ldots\ldots$$
$$|k_{n-1} \times P_1 \times P_2 \times \cdots \times P_{n-1}|_{P_n} = 1 \qquad (۶)$$

برای مجموعه پیمانه سه‌تایی $\{P_1,P_2,P_3\}$ عدد X بصورت زیر از نمایش مانده‌ای (x_1,x_2,x_3) توسط تئوری باقیمانده چینی جدید ۱ بدست می‌آید:

$$X = x_1 + P_1 |k_1(x_2 - x_1) + k_2 P_2 (x_3 - x_2)|_{P_2 P_3} \qquad (۷)$$

که

$$|k_1 \times P_1|_{P_2 P_3} = 1 \qquad (۸)$$

$$|k_2 \times P_1 \times P_2|_{P_3} = 1 \qquad (۹)$$

۳- مبدل مانده‌ای به دودوئی

در این بخش ما با استفاده از تئوری باقیمانده چینی جدید ۱، یک الگوریتم تبدیل مانده‌ای به دودوئی کارا برای مجموعه پیمانه جدید $\{2^{n-1}, 2^{n+1}+1, 2^{n+1}-1\}$، بدست می‌آوریم. ابتدا باید ثابت کنیم که این مجموعه پیمانه شامل اعداد دوبه‌دو نسبت به هم اول است.

تئوری ۱: اعداد 2^{n-1}، $2^{n+1}+1$ و $2^{n+1}-1$ دوبه‌دو نسبت به هم اول هستند.

اثبات: با استفاده از تئوری Euclid's داریم:

$$\gcd(a, b)=\gcd(b, a \bmod b) \qquad (۱۰)$$

که $\gcd(a,b)$ بیانگر بزرگترین مقسوم علیه مشترک a و b است. بنابراین:

$$\gcd(2^{n+1}+1, 2^{n+1}-1)=\gcd(2^{n+1}-1, 2)=1 \qquad (۱۱)$$

$$\gcd(2^{n+1}+1, 2^{n-1})=\gcd(2^{n-1}, 1)=1 \qquad (۱۲)$$

$$\gcd(2^{n+1}-1, 2^{n-1})=\gcd(2^{n-1}, -1)=1 \qquad (۱۳)$$

با توجه به اینکه همه بزرگترین مقسوم علیه‌ها یک هستند، پس این سه عدد دوبه‌دو نسبت به هم اول هستند.

گزاره ۱: معکوس ضربی 2^{n-1} در پیمانه $2^{2n+2}-1$ برابر است با $k_1=2^{n+3}$.

اثبات: با جایگزینی $P_1=2^{n-1}$، $P_2=2^{n+1}+1$ و $P_3=2^{n+1}-1$ در (۸) داریم:

$$\left|k_1\times 2^{n-1}\right|_{(2^{n+1}+1)(2^{n+1}-1)}=\left|2^{n+3}\times 2^{n-1}\right|_{2^{2n+2}-1}=\left|2^{2n+2}\right|_{2^{2n+2}-1}=1 \quad (۱۴)$$

گزاره ۲: معکوس ضربی $(2^{n+1}+1)\times 2^{n-1}$ در پیمانه $2^{n+1}-1$ برابر است با $k_2=2^{n+2}$.

اثبات: با توجه به اینکه $\left|2^{n+1}+1\right|_{2^{n+1}-1}=2$ است، باجایگزینی پیمانه‌ها در (۹) داریم:

$$\left|k_2\times 2^{n-1}\times(2^{n+1}+1)\right|_{2^{n+1}-1}=\left|2^{n+2}\times 2^{n-1}\times(2^{n+1}+1)\right|_{2^{n+1}-1}=\left|2^{n+1}\times 2^{n+1}\right|_{2^{n+1}-1}=\left|1\times 1\right|_{2^{n+1}-1}=1 \quad (۱۵)$$

تئوری ۲: در سیستم اعداد مانده‌ای تعریف شده توسط مجموعه پیمانه $\{2^{n-1},\ 2^{n+1}+1,\ 2^{n+1}-1\}$، عدد وزنی X از نمایش مانده‌ای (x_1,x_2,x_3) بصورت زیر بدست می‌آید:

$$X=x_1+2^{n-1}\left|\begin{matrix}2^{n+3}(x_2-x_1)+\\2^{n+2}(2^{n+1}+1)(x_3-x_2)\end{matrix}\right|_{2^{2n+2}-1} \quad (۱۶)$$

اثبات: با جایگزینی $P_1=2^{n-1}$، $P_2=2^{n+1}+1$ ، $P_3=2^{n+1}-1$ و مقادیر معکوس‌های ضربی k_1, k_2 از گزاره‌های ۱ و ۲ در (۷)، معادله (۱۶) بدست می‌آید.

مثال: توسط مجموعه پیمانه $\{2^{n-1},\ 2^{n+1}+1,\ 2^{n+1}-1\}$ به ازای $n=4$ عدد مانده‌ای $(7,24,30)$ بصورت زیر به عدد وزنی تبدیل می‌شود با جیگزینی مقادیر باقیمانده‌ها و $n=4$ در (۱۶) داریم:

$$X=7+8\left|128(17)+64(33)(6)\right|_{1023}=4215$$

در ادامه از تئوری ۲ برای طراحی مبدل مانده‌ای به دودوئی کارا استفاده خواهیم کرد. ولی قبل از پیاده‌سازی سخت افزاری تئوری ۲، می توانیم آن را ساده کنیم تا پیچیدگی سخت افزار کاهش یابد.

نمایش دودوئی x_1، x_2 و x_3 در سطح بیتی را در نظر بگیرید:

$$x_1=(x_{1,n-2}x_{1,n-3}\cdots x_{1,1}x_{1,0}) \quad (۱۷)$$

$$x_2=(x_{2,n+1}x_{2,n}\cdots x_{2,1}x_{2,0}) \quad (۱۸)$$

$$x_3=(x_{3,n}x_{3,n-1}\cdots x_{3,1}x_{3,0}) \quad (۱۹)$$

معادله (۱۶) را می‌توان بصورت زیر بازنویسی کرد:

$$X=x_1+2^nY \quad (۲۰)$$

که

$$Y=\left|v_1+v_2+v_3\right|_{2^{2n+2}-1} \quad (۲۱)$$

$$v_1=\left|-2^{n+3}x_1\right|_{2^{2n+2}-1} \quad (۲۲)$$

$$v_2=\left|(2^{n+3}-2^{n+2}-2^{2n+3})x_2\right|_{2^{2n+2}-1} \quad (۲۳)$$

$$v_3=\left|(2^{2n+3}+2^{n+2})x_3\right|_{2^{2n+2}-1} \quad (۲۴)$$

باتوجه به گزاره‌های ۱ و ۲ داریم:

$$v_1=\left|-2^{n+3}x_1\right|_{2^{2n+2}-1}=\left|-2^{n+3}(0\underbrace{00\cdots0}_{n+3}\underbrace{11\cdots11}_{n-1}x_{1,n-2}\cdots x_{1,1}x_{1,0})\right|_{2^{2n+2}-1}$$

$$=\bar{x}_{1,n-2}\cdots\bar{x}_{1,1}\bar{x}_{1,0}\underbrace{11\cdots11}_{n-1}\underbrace{00\cdots0}_{n+3} \quad (۲۵)$$

باتوجه به این که $2^{n+3}-2^{n+2}=2^{n+2}$است، می‌توان (۲۳) را بصورت زیر بازنویسی کرد:

$$v_2=\left|(2^{n+2}-2^{2n+3})x_2\right|_{2^{2n+2}-1}=\left|v_{21}+v_{22}\right|_{2^{2n+2}-1} \quad (۲۶)$$

$$v_{21}=\left|2^{n+2}x_2\right|_{2^{2n+2}-1}=\left|2^{n+2}(0\underbrace{00\cdots0}_{n}\underbrace{11\cdots11}_{n+2}x_{2,n+1}\cdots x_{2,1}x_{2,0})\right|_{2^{2n+2}-1}$$

$$=x_{2,n+1}\cdots x_{2,1}x_{2,0}\underbrace{00\cdots0}_{n}\underbrace{11\cdots11}_{n}x_{2,n+1}x_{2,n} \quad (۲۷)$$

$$v_{22}=\left|-2^{2n+3}x_2\right|_{2^{2n+2}-1}=\left|-(0\underbrace{00\cdots0}_{n-1}\underbrace{11\cdots11}_{n+2}x_{2,n+1}\cdots x_{2,1}x_{2,0})\right|_{2^{2n+2}-1}$$

$$=1\underbrace{00\cdots0}_{n-1}\underbrace{11\cdots11}_{n+2}\bar{x}_{2,n+1}\cdots\bar{x}_{2,1}\bar{x}_{2,0}1 \quad (۲۸)$$

و در نهایت v_3 را نیز می‌توان بصورت زیر محاسبه کرد:

$$v_3=\left|(2^{2n+3}+2^{n+2})x_3\right|_{2^{2n+2}-1}=\left|2^{n+2}(2^{n+1}+1)x_3\right|_{2^{2n+2}-1}$$

$$=\left|2^{n+2}(x_{3,n}\cdots x_{3,1}x_{3,0}\underbrace{00\cdots0}_{n+1}x_{3,n}\cdots x_{3,1}x_{3,0})\right|_{2^{2n+2}-1}$$

$$=x_{3,n+1}\cdots x_{3,1}x_{3,0}\underbrace{11\cdots11}_{n}\underbrace{00\cdots0}_{n+1}x_{3,n}\cdots x_{3,1}x_{3,0}x_{3,n} \quad (۲۹)$$

$(n+3)$ بیت کم ارزش v_1 در (۲۵) و همچنین $(n-1)$ بیت با ارزش v_{22} در (۲۸) هر دو از رشته‌ای از ۱ ها تشکیل شده‌اند. در نتیجه می‌توان به جای استفاده از v_1 و v_{22} از بردارهای زیر به جای آنها استفاده کرد:

$$v_1'=\bar{x}_{1,n-2}\cdots\bar{x}_{1,1}\bar{x}_{1,0}\underbrace{11\cdots11}_{n-1}\bar{x}_{2,n+1}\cdots\bar{x}_{2,1}\bar{x}_{2,0}\underbrace{11\cdots11}_{n+2} \quad (۳۰)$$

$$v'_{22} = 1\underbrace{11\ldots1}_{n-1}3\underbrace{11\ldots1}_{n+3} \quad (۳۱)$$

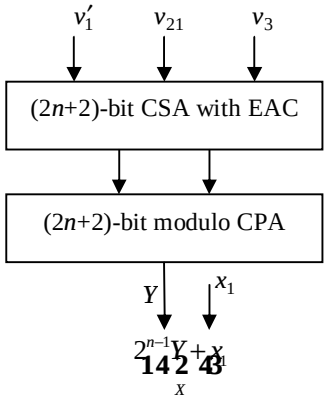
می‌دانیم که:

$$\left|v'_{22}\right|_{2^{2n+2}-1} = \left|1\underbrace{11\ldots1}_{2n+2}3\underbrace{11\ldots1}_{2^{2n+2}-1}\right| = \left|2^{2n+2}-1\right|_{2^{2n+2}-1} = 0 \quad (۳۲)$$

در نتیجه Y در (۲۱) را می‌توان از طریق معادله زیر بدست آورد:

$$Y = \left|v'_1 + v_{21} + v_3\right|_{2^{2n+2}-1} \quad (۳۳)$$

پیاده‌سازی سخت افزاری مبدل مانده‌ای به دودوئی برای مجموعه پیمانه $\{2^{n-1},\ 2^{n+1}+1,\ 2^{n+1}-1\}$ بر پایه معادلات (۲۰) و (۳۳) است. معادله (۳۳) توسط یک جمع کننده ذخیره رقم نقلی[vii] با گردش رقم نقلی انتهائی[viii] و یک جمع کننده انتشار رقم نقلی پیمانه‌ای[ix] قابل پیاده-سازی است. لازم به ذکر است که چون x_1 عددی $(n-1)$ بیتی است، محاسبه $x_1+2^{n-1}Y$ نیاز به هیچ گونه سخت افزار اضافی ندارد و فقط کافی است که x_1 را در کنار Y الحاق کنیم. ساختار سخت افزاری مبدل مانده‌ای به دودوئی پیشنهادی در شکل(۱) نشان داده شده است.



شکل (۱): ساختار سخت افزاری مبدل پیشنهادی

۴- ارزیابی کارایی

در این بخش کارایی مبدل مانده‌ای به دودوئی پیشنهادی بر حسب پیچیدگی سخت افزاری و تاخیر تبدیل ارزیابی می‌شود. محاسبه (۳۳) نیاز به یک جمع‌کننده ذخیره رقم نقلی $(2n+2)$ بیتی با گردش رقم نقلی انتهائی و یک جمع‌کننده انتشار رقم نقلی پیمانه‌ای $(2n+2)$ بیتی دارد. محاسبه (۲۷)، (۲۹) و (۳۰) نیاز به تغییر ساده سیم بندی بیت-های باقیمانده‌ها دارد. جمع‌کننده ذخیره رقم نقلی با گردش رقم نقلی انتهائی دارای یک طبقه معکوس کننده برای تمام ورودی‌هاست [3]. در نتیجه معکوس‌های بیتی که در (۳۰) نیاز است در جمع‌کننده با ذخیره رقم نقلی با گردش رقم نقلی انتهائی انجام می‌شود. با توجه به اینکه (۲۷) دارای n بیت صفر است، تعداد n تا از تمام جمع‌کننده‌های[x] جمع‌کننده ذخیره رقم نقلی به n عدد نیم جمع‌کننده[xi] کاهش می‌یابد. جمع‌کننده انتشار رقم نقلی پیمانه‌ای $(2n+2)$ بیتی که در شکل ۱ استفاده شده است همان است که در [15] پیشنهاد شده است و دارای پیچیدگی سخت افزاری $(2n+2)$ عدد تمام جمع‌کننده و تاخیر انتشار $(2n+2)t_{FA}$ است که t_{FA} نشان‌دهنده تاخیر یک تمام جمع‌کننده است. در نتیجه کل هزینه سخت افزاری مبدل پیشنهادی $n+2+2n+2=3n+4$ عدد تمام جمع‌کننده و n عدد نیم جمع‌کننده است. باتوجه به اینکه تاخیر یک جمع‌کننده ذخیره رقم نقلی به اندازه تاخیر یک تمام جمع‌کننده است، تاخیر مبدل پیشنهادی برابر با $1+2n+2=(2n+3)t_{FA}$ است.

در این مقاله یک مبدل مانده‌ای به دودوئی که اختصاص دارد به مجموعه پیمانه جدید $\{2^{n-1},\ 2^{n+1}+1,\ 2^{n+1}-1\}$ ارائه شده است. از این رو، برای بررسی میزان کارائی آن باید آن را با دیگر مبدل‌های مانده‌ای به دودوئی برای مجموعه پیمانه‌های سه‌تائی با محدوده دینامیکی شبیه به محدوده دینامیکی مجموعه پیمانه جدید پیشنهادی مقایسه کرد.

در [10] یک مبدل مانده‌ای به دودوئی برای مجموعه پیمانه کلی $\{2^k-1,\ 2^\alpha,\ 2^k+1\}$ بر اساس ترکیب روش‌های MRC و CRT پیشنهاد شده است. به ازای $k=n+1$ و $\alpha=n-1$ مبدل ارائه شده در [10] از دو جمع‌کننده ذخیره رقم نقلی $(2n+2)$ بیتی با گردش رقم نقلی انتهائی و یک جمع کننده انتشار رقم نقلی پیمانه‌ای $(2n+2)$ بیتی تشکیل شده است. دیگر مجموعه پیمانه شبیه به مجموعه پیمانه پیشنهادی، مجموعه پیمانه $\{2^n-1,\ 2^n,\ 2^{n+1}-1\}$ است و تاکنون تنها یک مبدل برای آن در [12] ارائه شده است. مبدل ارائه شده در [12] برپایه الگوریتم MRC و از چهار تفریق‌کننده تشکیل شده است. کارائی این مبدل‌ها بر حسب پیچیدگی سخت افزاری و تاخیر تبدیل در جدول ۱ نشان داده شده است.

جدول (۱): مقایسه کارائی مبدل های مانده‌ای به دودوئی

Converters	Hardware complexity	Conversion delay
[10]	$(6n+6)$ FA's	$(2n+4)t_{FA}$
[12]	$(5n+1)$ FA's	$(4n+1)t_{FA}$
Proposed	$(3n+4)$ FA's, (n) HA's	$(2n+3)t_{FA}$

با توجه به جدول ۱ کاملا مشخص است که مبدل پیشنهادی ما، سریعتر و دارای هزینه سخت افزاری کمتر نسبت به دیگر مبدل‌هاست.

۵- نتیجه گیری

در این مقاله یک مجموعه پیمانه جدید برای سیستم اعداد مانده‌ای پیشنهاد شد. این مجموعه پیمانه جدید شامل پیمانه‌های متعادل است که منجر به انجام سریع محاسبات در سیستم اعداد مانده‌ای و نیز پیاده‌سازی کارای مبدل مانده‌ای به دودوئی می‌شود. همچنین، یک مبدل مانده‌ای به دودوئی کارا برای این مجموعه پیمانه با استفاده از تئوری باقیمانده چینی جدید ۱ ارائه شد. در

مقایسه با دیگر مبدل‌ها، مبدل مانده‌ای به دودوئی پیشنهاد شده دارای سرعت بیشتر و هزینه سخت افزاری کمتر است.

مراجع

[1] T. Stouratitis and V. Paliouras, Considering the alternatives in lowpower design, *IEEE Circuits and Devices*, (2001), 23–29.

[2] M. A. Soderstrand and et al., *Residue number system arithmetic: modern applications in digital signal processing*, New York: IEEE Press, 1986.

[3] B Koren, *Computer Arithmetic Algorithms*. Englewood Cliffs, NJ: Prentice-Hall, 1993.

[4] R. Conway and J. Nelson, Improved RNS FIR Filter Architectures, *IEEE Transactions On Circuits and Systems II*, Vol. 51, No. 1, (2004), 26-28.

[5] P. G. Fernandez, et al., *A RNS-Based Matrix-Vector-Multiply FCT Architecture for DCT Computation*, Proc. of 43rd IEEE Midwest Symposium on Circuits and Systems, pp. 350-353, 2000.

[6] W. L. Freking and K. K. Parhi, *Low-power FIR digital filters using residue arithmetic*, Proc. Of 31st Asilomar Conference on Signals, Systems, and Computers, Pacific Grove, CA, USA, vol. 1, pp. 739–43, 1997.

[7] S. Yen, S. Kim, S. Lim and S. Moon, RSA Speedup with Chinese Remainder Theorem Immune against Hardware Fault Cryptanalysis, *IEEE Transactions On Computers*, (2003), 461-472.

[8] L. L. Yang, and L. Hanzo, *Redundant Residue Number System Based Error Correction Codes*, Proc. of IEEE VTC'2001, Atlantic City, USA. pp. 1472-1476, 2001.

[9] W. K. Jenkins and B. J. Leon, The use of residue number systems in the design of finite impulse response digital filters, *IEEE Trans. Circuits Syst.*, vol. CAS-24, (1977), 191–201.

[10] A. Skavantzos and T. Stouraitis, *Grouped-moduli residue number systems for fast signal processing*, IEEE ISCAS, vol. III, pp. 478–483, 1999.

[11] A. Hiasat and H. S. Abdel-Aty-Zohdy, Residue-to-binary arithmetic converter for the moduli set (2^k, 2^k-1, 2^{k-1}-1), *IEEE Trans. Circuits Syst.*, vol. 45, (1998), 204–208.

[12] J. Mathew, D. Radhakrishnan, T. Srikanthan, *Fast residue-to-binary converter architectures*, IEEE, 42nd Midwest Symposium on Circuits and Systems, pp. 1090–1093, 2000.

[13] F. Pourbigharaz and H. M. Yassine, A signed-digit architecture for residue to binary transformation, *IEEE Trans. Comput.*, vol. 46, (1997), 1146–1150.

[14] Y. Wang, *New Chinese Remainder Theorems*, Proc. 32th Asilomar Conf. Signals, Systems, Computers, vol. 1, pp. 165–171, 1998.

[15] C. Efstathiou, D. Nikolos, and J. Kalamatianos, Area-time efficient modulo 2^n-1 adder design, IEEE Trans. Circuits Syst.-II, 41, vol. 7, (1994), 463–467.

[16] A. A. Hiasat, VLSI implementation of New Arithmetic Residue to Binary decoders, *IEEE Trans. VLSI Systems*, Vol.13, (2005), 153-158.

[17] S. J. Piestrak, Design of residue generators and multioperand modular adders using carry-save adders, *IEEE Trans. Comput.*, vol. 423, no. 1, (1994), 68-77.

[18] M. Hosseinzadeh, K. Navi, S. Gorgin, *A New Moduli Set for Residue Number System: {r^n-2, r^n-1, r^n}*, Proc. IEEE International Conference on Electrical Engineering, 2007.

[19] A. Sabbagh, K. Navi, *An Improved Residue to Binary Converter for the RNS with Pairs of Conjugate Moduli*, Proc. International Conference on Electrical Engineering and Informatics, Indonesia, vol. 1, pp. 318-320, 2007.

[20] A. Hariri, K. Navi, R. Rastegar, A new high dynamic range moduli set with efficient reverse converter, *International Elsevier Journal of Computers and Mathematics with Applications*, doi:10.1016/j.camwa.2007.04.028, 2007.

زیرنویس‌ها

[i] Residue number system (RNS)
[ii] Residue to binary converter
[iii] Chinese remainder theorem (CRT)
[iv] Mixed-radix conversion (MRC)
[v] New chinese remainder theorems (New CRT's)
[vi] Binary to residue conversion
[vii] Carry save adder (CSA)
[viii] End around carry (EAC)
[ix] Modulo carry propagate adder (CPA)
[x] Full adder (FA)

[xi] Half adder (HA)