

به نام خدا



نام و نام خانوادگی: محمد اسماعیل دوست

دکتری مهندسی کامپیوتر - معماری کامپیوتر از دانشکده برق و کامپیوتر دانشگاه شهید بهشتی،
تهران

ایمیل: m_doust@guilan.ac.ir

سوابق اجرایی:

عضو هیأت علمی دانشگاه گیلان (مامور به خدمت) - ۱۴۰۳ - کنون

عضو هیأت علمی دانشگاه علوم و فنون دریایی خرمشهر ۱۳۹۱ - ۱۴۰۳

معاون پژوهشی دانشکده مهندسی دریا ۱۴۰۱ - ۱۴۰۳

مدیر امور اداری و پشتیبانی، دانشگاه علوم و فنون دریایی خرمشهر ۱۳۹۹ - ۱۴۰۱

رئیس دانشکده مهندسی دریا، دانشگاه علوم و فنون دریایی خرمشهر ۱۳۹۷ - ۱۳۹۹

مدیر فناوری اطلاعات و ارتباطات دانشگاه علوم و فنون دریایی خرمشهر ۱۳۹۱ - ۱۳۹۸

مدیر گروه الکترونیک و مخابرات دریایی، دانشگاه علوم و فنون دریایی خرمشهر ۱۳۹۱ - ۱۳۹۳

عضو کارگروه جذب دانشکده مهندسی دریا

قائم مقام منطقه ۱۰ آموزش عالی و حوزه فناوری اطلاعات وزارت علوم، تحقیقات و فناوری ۱۳۹۵ - ۱۳۹۷

سوابق تحصیلی:

دکتری مهندسی کامپیوتر - معماری کامپیوتر ۱۳۸۷ - ۱۳۹۱

دانشگاه شهید بهشتی تهران

کارشناسی ارشد مهندسی کامپیوتر - معماری کامپیوتر: ۱۳۸۵ - ۱۳۸۷

دانشگاه شهید بهشتی تهران

کارشناسی مهندسی کامپیوتر: ۱۳۸۰ - ۱۳۸۵

دانشگاه شاهد تهران

زمینه های پژوهشی:

- رمزنگاری
 - رمزنگاری منحنی بیضوی
 - **RSA**
 - **NTRU**
- اینترنت اشیاء
- امنیت شبکه
 - پروتکل های امنیتی
- حساب کامپیوتر
 - سیستم اعداد مانده ای
 - ضرب منتگومری
- **VLSI**
 - **Digital CMOS**
 - **Low power design**
 - **Carbon Nano Tube**
- سیستم های باز پیکر بندی
 - الگوریتم های اختصاص منابع (Placement)

طرح های پژوهشی انجام شده:

۱	دانشگاه علوم و فنون دریایی خرمشهر	بهبود کارایی پردازش سیگنال دیجیتال با استفاده از طراحی کارآمد سیستم اعداد مانده ای
۲	دانشگاه علوم و فنون دریایی خرمشهر	طراحی کارآمد سیستم اعداد مانده ای RSA بهبود کارایی رمزنگاری
۳	دانشگاه علوم و فنون دریایی خرمشهر	در ارتباطات دریایی RSA پیاده سازی الگوریتم رمزنگاری
۴	سازمان بنادر و دریانوردی	شناسایی ظرفیت های توسعه گردشگری بنادر منتخب خوزستان

برگزیده ای از مجلات منتشر شده:

[Efficient RNS Implementation of Elliptic Curve Point Multiplication Over](#)

[132](#)

2012

M Esmaeildoust, D Schinianakis, H Javashi, T Stouraitis, K Navi

IEEE Transactions on Very Large Scale Integration (VLSI) Systems 21 (8 ...

[How to teach residue number system to computer scientists and engineers](#) [125](#) 2010

K Navi, AS Molahosseini, M Esmaeildoust

IEEE Transactions on Education 54 (1), 156-163

[High speed reverse converter for new five-moduli set \$\{2n, 22n+1-1, 2n/2-1, 2n/2+1, 2n+1\}\$](#) [19](#) 2010

M Esmaeildoust, K Navi, MR Taheri

IEICE Electronics Express 7 (3), 118-125

[A general reverse converter architecture with low complexity and high performance](#) [18](#) 2011

K Navi, M Esmaeildoust, AS Molahosseini

IEICE TRANSACTIONS on Information and Systems 94 (2), 264-273

[Efficient RNS to binary converters for the new 4-moduli set \$\{2n, 2n+1-1, 2n-1, 2n-1-1\}\$](#) [12](#) 2012

M Esmaeildoust, K Navi, MR Taheri, AS Molahosseini, S Khodambashi

IEICE Electronics Express 9 (1), 1-7

[Efficient FPGA implementation of RNS montgomery multiplication using balanced RNS bases](#) [9](#) 2022

J Ahsan, M Esmaeildoust, A Kaabi, V Zarei

Integration 84, 72-83

[A high speed residue-to-binary converter for balanced 4-moduli set](#) [9](#) 2015

MR Taheri, N Shafiee, M Esmaeildoust, Z Amirjamshidi, ...

Journal of Computing and Security 2 (1), 43-54

[Efficient Reverse Converter Design for Five Moduli Set \$\{\$](#) [8](#) 2012

MR Taheri, E Khani, M Esmaeildoust, K Navi

Journal of Computations & Modelling 2 (1), 93-108

[Fragmentation aware placement algorithm for a reconfigurable system](#)

[8](#)

2008

M Esmaeildoust, M Fazlali, A Zakerolhosseini, M Karimi

2008 Second International Conference on Electrical Engineering, 1-5

[Efficient two-level reverse converters for the four-moduli set \$\{2^{n-1}, 2^n-1, 2^{n-1}-1, 2^{n+1}-1\}\$](#)

[5](#)

2021

M Obeidi Daghlavi, MR Noorimehr, M Esmaeildoust

Analog Integrated Circuits and Signal Processing 108 (1), 75-87

[High dynamic range RNS bases for modular multiplication](#)

[3](#)

2011

S Rezaie, M Esmaeildoust, M Gerami, K Navi, O Hashemipour

International Journal of Computer Science Issues (IJCSI) 8 (4), 69

[Four Moduli RNS Bases for Efficient Design of Modular Multiplication](#)

[3](#)

2011

M Gerami, M Esmaeildoust, S Rezaie, K Navi, O Hashemipour

Journal of Computations & Modelling 1 (2), 73-96

[High Speed Reverse Converter for the Five Moduli Set \$\{2n, 2n-1, 2n+1, 2n-3, 2n-1-1\}\$](#)

[2](#)

2014

M Esmaeildoust, A Kaabi

TJMCS

[HIGH SPEED REVERSE CONVERTER FOR HIGH DYNAMIC RANGE MODULI SET](#)

[2](#)

2012

MR Taheri, A Pirhoseinlo, M Esmaeildoust, M Esmaeildoust, K Navi

International Journal 3

- | | | |
|--|--------------------------|------|
| <u>Design of Multiple-Valued Interconnection Networks with Gate all Around Transistor for Smart Computer Networks</u> | <u>1</u> | 2023 |
| K Navi, N Ghoreishi, R Sabbaghi-Nadooshan, M Esmaeildoust | | |
| International Journal of Smart Electrical Engineering 12 (1), 11-21 | | |
| <u>On the Design of RNS Bases for Modular Multiplication.</u> | <u>1</u> | 2014 |
| M Esmaeildoust, K Navi, S Rezaei, M Gerami | | |
| Int. J. Netw. Secur. 16 (2), 118-128 | | |
| <u>Efficient Implementation of RNS Montgomery Multiplication Using Balanced RNS Bases</u> | <u>1</u> | 2014 |
| S Sharifi, M Esmaeildoust, MR Taheri, K Navi | | |
| Journal of Mathematics and Computer Science (JMCS) 12, 51-64 | | |
| <u>An efficient algorithm for online placement in a reconfigurable system</u> | <u>1</u> | 2008 |
| M Esmaeildoust, M Fazlali, A Zakeroilhosseini | | |
| 2008 11th International Conference on Optimization of Electrical and ... | | |
| <u>بررسی تاثیر فناوری‌های نوین در زمینه توسعه لجستیک و حمل و نقل یسکرانه‌ای بنادر جنوبی ایران (مطالعه موردی: بندر امام خمینی (ره))</u> | | 2025 |
| حسینی, یوسفی, همایون, اسماعیل دوست | | |
| پژوهشنامه حمل و نقل ۲۲ (۱), ۲۰۳-۲۱۸ | | |
| <u>Fast Reverse converter Design for three moduli set $\{2^n, 2^{n-1}, 2^{(n-1)-1}\}$ Using CRTF</u> | | 2022 |
| J Ahsan, M Esmaeildoust, A Kaabi, V Zarei | | |
| International Journal Of Coastal, Offshore And Environmental Engineering ... | | |
| <u>Novel Design of Multiple-Valued Interconnection networks to improve processing speed in hardware security</u> | | 2022 |
| K Navi, N Ghoreishi, NR Sabbaghi, M Esmaeildoust | | |

[Improving the performance of PRINCE cryptographic algorithm using Dynamic S-BOX and related differential attack analysis](#) 2021

E Matori, M Esmaeildoust

Journal of Marine Science and Technology

[غیر ثابت و تحلیل حمله S-BOX با استفاده از PRINCE بهبود کارایی الگوریتم رمز قالبی تفاضلی مرتبط با آن](#) 2021

مطوری, اسماعیل دوست

مجله علوم و فنون دریایی, e136677

[Performance Evaluation of Symmetric Key Cryptography Algorithms](#) 2020

M Beitabdollah, M Esmaeildoust, A Kaabi

Journal of Marine Science and Technology 19 (1), 28-38

[ارزیابی کارایی الگوریتم های رمزنگاری متقارن](#) 2020

بیت عبدالله, اسماعیل دوست, کعبی, عامر

مجله علوم و فنون دریایی ۱۹ (۱), ۲۸-۳۸

[Improved Speed of RPrime RSA Cryptography Algorithm by Using a Residue Number System](#) 2020

F Jahanbakhshi, MR Noorimehr, M Esmaeildoust

Journal of Marine Science and Technology

[با استفاده از سیستم اعداد مانده ای RPrime RSA بهبود سرعت الگوریتم رمزنگاری](#) 2020

جهانبخش, فرنوش, نوری مهر, اسماعیل دوست

مجله علوم و فنون دریایی

[تخمین ارتفاع امواج ناشی از باد با استفاده از سیستم استنتاج تطبیقی عصبی-فازی, درخت تصمیم و روش های تجربی در بندر بوشهر](#) 2018

بزرگ زاده, لیاقت, بختیاری, شهنی کرم زاده, اسماعیل دوست

علوم و مهندسی آبیاری ۴۱ (۲), ۱۵۱-۱۶۶

Year of Publication: 2015

2015

A Zalekian, M Esmaeildoust, A Kaabi

Routing Aware Placement Algorithm and Efficient Free Space Management for Reconfigurable Systems

2010

M Esmaeildoust, A Zakerolhosseini

Journal of Circuits, Systems, and Computers 19 (06), 1217-1234

Free Space Management and I/O Communication Based Placement Algorithm in Reconfigurable Systems

2010

M Esmaeildoust, M Fazlali, K Navi, A Zakerolhosseini

Proceedings of 2010 International Conference on Computational Intelligence ...

Hardware Implementation for frequent episode discovery in event sequences

2008

M Esmaeildoust, H Mousavi, M Abbaspour, A Zakerolhosseini, M Zamani

2008 3rd International Conference on Information and Communication ...

بازشناسی قلم های فارسی با استفاده از ترکیب ویژگی ها و خبره ها

زارعی وحید, اسماعیل دوست محمد, مرتضوی احسان

صنایع الکترونیک ۷ (۲), ۹۱-۹۹

Efficient Montgomery Modular Multiplication by using Residue Number System

E Khani, M Esmaeildoust, K Navi

<https://scholar.google.com/citations?hl=en&user=qBiACFMAAAAJ>

مهارت‌های تخصصی:

- Programming Skills
 - C, C++ , python (experienced)
 - Delphi, Java, Pascal (some experienced)
- HDL
 - VHDL (experienced)
 - ModelSim (experienced)
- Synthesis tools
 - Xilinx ISE (experienced)
 - Leonardo (experienced)
 - Synopsis (some experienced)
 - Xilinx Vivado (some experienced)

لینک های مرتبط:

<https://scholar.google.com/citations?user=qBiACFMAAAAJ&hl=en>

<https://orcid.org/0000-0003-2985-6390>

References

Dr. K. Navi, Professor (Supervisor in Ph.D.)
Department of Electrical and Computer Engineering
Shahid Beheshti University
Evin, Tehran
Email: navi@sbu.ac.ir

Dr. A. Zakerolhosseini, assistant professor (Supervisor in MSc)
Department of Electrical and Computer Engineering
Shahid Beheshti University
Evin, Tehran
Email: a-zaker@sbu.ac.ir

Dr. M. Eshghi, professor
Department of Electrical and Computer Engineering
Shahid Beheshti University
Evin, Tehran
Email: m-eshghi@sbu.ac.ir