

2023 Eleventh International Symposium on Computing and Networking (CANDAR 2023)

**Matsue, Japan
28 November - 1 December 2023**



**IEEE Catalog Number: CFP2319X-POD
ISBN: 979-8-3503-0671-2**

**Copyright © 2023 by the Institute of Electrical and Electronics Engineers, Inc.
All Rights Reserved**

Copyright and Reprint Permissions: Abstracting is permitted with credit to the source. Libraries are permitted to photocopy beyond the limit of U.S. copyright law for private use of patrons those articles in this volume that carry a code at the bottom of the first page, provided the per-copy fee indicated in the code is paid through Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923.

For other copying, reprint or republication permission, write to IEEE Copyrights Manager, IEEE Service Center, 445 Hoes Lane, Piscataway, NJ 08854. All rights reserved.

****** This is a print representation of what appears in the IEEE Digital Library. Some format issues inherent in the e-media version may also appear in this print version.***

IEEE Catalog Number:	CFP2319X-POD
ISBN (Print-On-Demand):	979-8-3503-0671-2
ISBN (Online):	979-8-3503-0670-5
ISSN:	2379-1888

Additional Copies of This Publication Are Available From:

Curran Associates, Inc
57 Morehouse Lane
Red Hook, NY 12571 USA
Phone: (845) 758-0400
Fax: (845) 758-2633
E-mail: curran@proceedings.com
Web: www.proceedings.com

CURRAN ASSOCIATES INC.
proceedings
.com

2023 Eleventh International Symposium on Computing and Networking (CANDAR) **CANDAR 2023**

Table of Contents

Message from the Organizers	ix
Conference Organizers	x
Conference Committee	xii
Reviewers	xvi

11th International Symposium on Computing and Networking

Long Papers

Flexibility and Privacy: A Multi-Head Federated Continual Learning Framework for Dynamic Edge Environments	1
<i>Chunlu Chen (Kyushu University, Japan), Kevin I-Kai Wang (The University of Auckland, New Zealand), Peng Li (The University of Aizu, Japan), and Kouichi Sakurai (Kyushu University, Japan)</i>	
A New Approach to Disabling SSL/TLS: Man-in-the-Middle Attacks are Still Effective	11
<i>Keiichiro Kimura (Kobe University, Japan), Yoshiaki Shiraishi (Kobe University, Japan), and Masakatu Morii (Kobe University, Japan)</i>	
Accelerate Inference of CNN Models on CPU via Column Combining Based on Simulated Annealing	20
<i>Chien-Hung Lin (National Taiwan University, Taiwan), Ding-Yong Hong (Institute of Information Science, Academia Sinica, Taiwan), Pangfeng Liu (National Taiwan University, Taiwan), and Jan-Jan Wu (Institute of Information Science, Academia Sinica, Taiwan)</i>	
A Non-Stop Fault-Tolerant Real-Time System-on-Chip/System-in-Package	30
<i>Shota Nakabeppu (Keio University, Japan), Nobuyuki Yamasaki (Keio University, Japan), Kenta Suzuki (Sony Semiconductor Solutions Corporation, Japan), Keizo Hiraga (Sony Semiconductor Solutions Corporation, Japan), and Kazuhiro Bessho (Sony Semiconductor Solutions Corporation, Japan)</i>	
Dual Diagonal Mesh: An Optimal Memory Cube Network Under Geometric Constraints	40
<i>Masashi Oda (Kyoto University, Japan), Kai Keida (Kyoto University, Japan), and Ryota Yasudo (Kyoto University, Japan)</i>	

Efficient GPU-Accelerated Bulk Evaluation of the Boys Function for Quantum Chemistry	49
<i>Satoki Tsuji (Hiroshima University, Japan; Computing Laboratory, Fujitsu Limited, Japan), Yasuaki Ito (Hiroshima University, Japan), Koji Nakano (Hiroshima University, Japan), and Akihiko Kasagi (Computing Laboratory, Fujitsu Limited, Japan)</i>	
Solving the N-Queens Puzzle by a QUBO Model with Quadratic Size	59
<i>Shunsuke Tsukiyama (Hiroshima University, Japan), Koji Nakano (Hiroshima University, Japan), Yasuaki Ito (Hiroshima University, Japan), Takashi Yazane (NTT DATA Group Corporation, Japan), Junko Yano (NTT DATA Group Corporation, Japan), Takumi Kato (NTT DATA Group Corporation, Japan), Shiro Ozaki (NTT DATA Group Corporation, Japan), Rie Mori (NTT DATA Group Corporation, Japan), and Ryota Katsuki (NTT DATA Group Corporation, Japan)</i>	
Dimension-Extended Dragonfly: A More Flexible Interconnection Network Aimed at Reducing Hardware Cost	68
<i>Yaodong Wang (Hosei University) and Yamin Li (Hosei University)</i>	
Multi-Objective Optimization of Controller Placement in Distributed ONOS Networks	76
<i>Kang Xingyuan (Nara Institute of Science and Technology, Japan), Keichi Takahashi (Tohoku University, Japan), Chawanat Nakasan (Kasetsart University, Japan), Kohei Ichikawa (Nara Institute of Science and Technology, Japan), and Hajimu Iida (Nara Institute of Science and Technology, Japan)</i>	

Regular Papers

Accountable Ring Signatures from Symmetric-Key Primitives	86
<i>Hiroaki Anada (Aomori University, Japan), Masayuki Fukumitsu (University of Nagasaki, Japan), and Shingo Hasegawa (Tohoku University, Japan)</i>	
Issuer-Revocable Issuer-Hiding Attribute-Based Credentials using an Accumulator	93
<i>Nasima Begum (University of Asia Pacific, Bangladesh) and Toru Nakanishi (Hiroshima University, Japan)</i>	
Parallel Implementation of Vision Transformer on a Multi-FPGA Cluster	100
<i>Yasuyu Fukushima (Keio University, Japan), Kensuke Iizuka (Keio University, Japan), and Hideharu Amano (Keio University, Japan)</i>	
eSilo: Making Silo Secure with SGX	107
<i>Masahide Fukuyama (Keio University, Japan), Masahiro Tanaka (Keio University, Japan), Ryota Ogino (Keio University, Japan), and Hideyuki Kawashima (Keio University, Japan)</i>	
SMOG - An Explicitly Composable Memory Benchmark Suite for Heterogeneous Memory	113
<i>Andreas Grapentin (University of Potsdam, Germany), Felix Eberhardt (University of Potsdam, Germany), and Andreas Polze (University of Potsdam, Germany)</i>	

SEM: A Simple Yet Efficient Model-Agnostic Local Training Mechanism to Tackle Data Sparsity and Scarcity in Federated Learning	120
<i>Quang Ha Pham (Hanoi University of Science and Technology, Vietnam), Nang Hung Nguyen (Hanoi University of Science and Technology, Vietnam), Thanh Hung Nguyen (Hanoi University of Science and Technology, Vietnam), Huy Hieu Pham (VinUniversity), Phi Le Nguyen (Hanoi University of Science and Technology, Vietnam), and Truong Thao Nguyen (National Institute of Advanced Industrial Science and Technology (AIST), Japan)</i>	
Poisoning Attacks Against Network Intrusion Detection Systems using Shapley Values to Identify Trends in Poisoning Data	127
<i>Tomohiro Hasegawa (Kogakuin University, Japan) and Ryotaro Kobayashi (Kogakuin University, Japan)</i>	
Pseudo-Random Number Generation by Staggered Sampling of LFSR	134
<i>Shuichi Ichikawa (Toyohashi University of Technology, Japan)</i>	
Encryption Invalidation Attacks: Is your Wi-Fi Encryption Really Working?	141
<i>Taketo Inoue (Kobe University, Japan), Kosuke Kuriyama (Kobe University, Japan), Yoshiaki Shiraishi (Kobe University, Japan), and Masakatu Morii (Kobe University, Japan)</i>	
A Cryptanalysis Against the Cheating Detectable Secret Sharing from NISS 2019	148
<i>Kiminori Kaneko (Hosei University, Japan) and Satoshi Obana (Hosei University, Japan)</i>	
Exploiting Unlabeled RSSI Fingerprints in Multi-Building and Multi-Floor Indoor Localization Through Deep Semi-Supervised Learning Based on Mean Teacher	155
<i>Sihao Li (Xi'an Jiaotong-Liverpool University, China; University of Liverpool, U.K.), Zhe Tang (Xi'an Jiaotong-Liverpool University, China; University of Liverpool, U.K.), Kyeong Soo Kim (Xi'an Jiaotong-Liverpool University, China), and Jeremy S. Smith (University of Liverpool, U.K.)</i>	
Evaluation of Effectiveness of MAC Systems Based on LSM for Protecting IoT Devices	161
<i>Masato Miki (Okayama University, Japan), Toshihiro Yamauchi (Okayama University, Japan), and Satoru Kobayashi (Okayama University, Japan)</i>	
An Incremental Algorithm for $(2 - \epsilon)$ -Approximate Steiner Tree Requiring $O(n)$ Update Time	168
<i>Hemraj Raikwar (Indian Institute of Technology Guwahati, India) and Sushanta Karmakar (Indian Institute of Technology Guwahati, India)</i>	
Auto-Tuning Mixed-Precision Computation by Specifying Multiple Regions	175
<i>Xuanzhengbo Ren (Naogya University, Japan), Masatoshi Kawai (Nagoya University, Japan), Tetsuya Hoshino (Nagoya University, Japan), Takahiro Katagiri (Nagoya University, Japan), and Toru Nagai (Nagoya University, Japan)</i>	
Distributed MQTT Brokers Infrastructure with Network Transparent Hardware Broker	182
<i>Tokimasa Toyohara (Keio University, Japan) and Hiroaki Nishi (Keio University, Japan)</i>	

Efficient and High-Speed CGRA Accelerator for Cryptographic Applications	189
<i>Vu Trung Duong Le (Nara Institute of Science and Technology), Hoai Luan Pham (Nara Institute of Science and Technology), Thi Hong Tran (Nara Institute of Science and Technology), Thi Sang Duong (Nara Institute of Science and Technology), and Yasuhiko Nakashima (Nara Institute of Science and Technology)</i>	
Quantum Computer Architecture for Quantum Error Correction with Distributing Process to Multiple Temperature Layers	196
<i>Ryuji Ukai (R&D Group, Hitachi, Ltd., Japan), Chihiro Yoshimura (R&D Group, Hitachi, Ltd., Japan), and Hiroyuki Mizuno (R&D Group, Hitachi, Ltd., Japan)</i>	
An Accurate Positioning Geocast Protocol for Safety Message Dissemination in VANETs	203
<i>Paulo V. G. Farias (University of Brasilia, Brazil) and Jacir L. Bordim (University of Brasilia, Brazil)</i>	
Security Risk Visualization for Open-Source Software Based on Vulnerabilities, Repositories, and Dependencies	210
<i>Tomohiko Yano (SECOM CO., LTD., Japan) and Hiroki Kuzuno (Kobe University, Japan)</i>	
Zero-Knowledge Proofs of Connectivity for Labeled Directed Graphs using Bilinear-Map Accumulator	217
<i>Takuma Yoshioka (Hiroshima University, Japan), Toru Nakanishi (Hiroshima University, Japan), and Teruaki Kitasuka (Hiroshima University, Japan)</i>	
Author Index	225