

# **2025 IEEE Symposium on Low-Power and High-Speed Chips and Systems (COOL CHIPS 2025)**

**Tokyo, Japan  
16-18 April 2025**



**IEEE Catalog Number: CFP25COL-POD  
ISBN: 979-8-3315-3485-1**

**Copyright © 2025 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:    | CFP25COL-POD      |
| ISBN (Print-On-Demand): | 979-8-3315-3485-1 |
| ISBN (Online):          | 979-8-3315-3484-4 |
| ISSN:                   | 2167-9657         |

**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](mailto:curran@proceedings.com)  
Web: [www.proceedings.com](http://www.proceedings.com)

CURRAN ASSOCIATES INC.  
**proceedings**  
.com

# TABLE OF CONTENTS

|                                                                                                                                                 |    |
|-------------------------------------------------------------------------------------------------------------------------------------------------|----|
| UniCrypt: Universal Crypto Engine with Optimized Resource Sharing for Security Applications .....                                               | 1  |
| <i>Vu Trung Duong Le, Hoai Luan Pham, Tuan Hai Vu, Van Duy Tran, Yasuhiko Nakashima</i>                                                         |    |
| A High-Performance Hardware Design for Polynomial Multiplication in the CRYSTALS-Kyber<br>Algorithm .....                                       | 7  |
| <i>Hsueh Chen, Hsiu-Wei Chen, Shih-Hsu Huang, Po-Yuan Chen</i>                                                                                  |    |
| Accelerating Elliptic Curve Point Additions on Versal AI Engine for Multi-Scalar Multiplication .....                                           | 13 |
| <i>Ayumi Ohno, Kotaro Shimamura, Shinya Takamaeda-Yamazaki</i>                                                                                  |    |
| Hybrid ReRAM-NMC & SRAM-CiM Matrix Multiplication for Large Language Model.....                                                                 | 19 |
| <i>Tao Wang, Daqi Lin, Kenshin Yamauchi, Naoko Misawa, Chihiro Matsui, Ken Takeuchi</i>                                                         |    |
| A Compute-In-Memory Ascon Implementation Based on a Novel 11T SRAM Processing Macro .....                                                       | 25 |
| <i>Mark Lee, Chris Clark, Saibal Mukhopadhyay</i>                                                                                               |    |
| Proposal for Non-Volatilization of eFPGA Core .....                                                                                             | 31 |
| <i>Keizo Hiraga, Kenshu Seto, Kazuhiro Bessho, Masahiro Iida</i>                                                                                |    |
| A Power-Efficient Reconfigurable Hybrid CNN-SNN Accelerator for High Performance AI<br>Applications.....                                        | 37 |
| <i>Heuijee Yun, Daejin Park</i>                                                                                                                 |    |
| GUPA: Group-Wise Uniform Pruning Accelerator for Depthwise Separable Convolution .....                                                          | 43 |
| <i>Yi Chen, Malte Wabnitz, Jie Lou, Christian Lanius, Tobias Gemmeke</i>                                                                        |    |
| HOPE: an Efficient Accelerator with Head-Wise Overlap Processing for Sparse Attention in Vision<br>Transformer .....                            | 49 |
| <i>Jihyeon Heo, Soomin Rho, Kwangrae Kim, Ki-Seok Chung</i>                                                                                     |    |
| Exploring the Versal AI Engine for 3D Gaussian Splatting.....                                                                                   | 55 |
| <i>Kotaro Shimamura, Ayumi Ohno, Shinya Takamaeda-Yamazaki</i>                                                                                  |    |
| RustSFQ: A Domain-Specific Language for SFQ Circuit Design.....                                                                                 | 61 |
| <i>Mebuki Oishi, Sun Tanaka, Shinya Takamaeda-Yamazaki</i>                                                                                      |    |
| Evaluation of Trade-Off Between Compression Ratio and Hardware Cost for Adaptive Bandwidth<br>Compression Hardware Platform .....               | 67 |
| <i>Tomohiro Ueno, Kaito Kitazume, Masato Kiyama, Kazutomo Yoshii, Kento Sato, Norihisa Fujita, Ryohei Kobayashi, Taisuke Boku, Kentaro Sano</i> |    |
| Can the Agile-Chip Platform Carve Out a Niche Between ASICs and FPGAs? .....                                                                    | 73 |
| <i>Hideharu Amano, Atsutake Kosuge, Hirofumi Sumi, Naonobu Shimamoto, Yukinori Ochiai, Yurie Inoue, Tohru Mogami, Yoshio Mita, Makoto Ikeda</i> |    |
| TTF-GNN: Memory-Efficient GNNs Via Tensor Train Decomposition and Network Folding .....                                                         | 76 |
| <i>Hiroaki Ito, Jiale Yan, Kazushi Kawamura, Masato Motomura, Thiem Van Chu, Daichi Fujiki</i>                                                  |    |
| A Lightweight Transformer Model with Dynamic Sparse Mask for Neural Machine Translation.....                                                    | 82 |
| <i>Nastaran Asadi, Babak Golbabaee, Yirong Kan, Renyuan Zhang, Yasuhiko Nakashima</i>                                                           |    |

## Author Index