Daejun Park

Formal Verification Lead
Runtime Verification, Inc.
102 E. Main St. #500, Urbana, IL 61801

Email : daejunpark@gmail.com
Web : https://daejunpark.github.io/

Research Interests

- **Formal Methods**: *formal verification* of real-world safety-critical systems, from compilers to smart contracts to cryptographic primitives.
- **Security**: application of *verifiable computing* and *homomorphic encryption* in machine learning and blockchain.

Education

Ph.D., Computer Science, University of Illinois at Urbana-Champaign 2019
M.S., Computer Science and Engineering, Seoul National University, South Korea 2008
B.S., Computer Science and Engineering, Seoul National University, South Korea 2006

Professional Experience

Formal Verification Lead, Runtime Verification, Inc., IL 2019 – Present

- *Formally verifying* high-profile, safety-critical blockchain smart contracts and consensus protocols.

Research Intern, Microsoft Research, WA Summer 2017

- Designed a novel *verifiable computing* technique for secure deep neural network training.

Founding Member & Technical Lead, Sparrow, South Korea 2008 – 2011

- Designed and implemented *a static program analysis tool* detecting memory safety errors and security vulnerabilities in embedded systems software.

Publications

[1] **Language-Parametric Compiler Validation with Application to LLVM**.
Theodoros Kasampalis, *Daejun Park*, Zhengyao Lin, Vikram S. Adve, and Grigore Rosu. *Proceedings of the Twenty-Sixth International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS'21)*, 2021. (To appear.)

[2] **A Learning-Based Approach to Synthesizing Invariants for Incomplete Verification Engines**.
Daniel Neider, P. Madhusudan, Shambwaditya Saha, Pranav Garg, and *Daejun Park*. *Journal of Automated Reasoning*, Vol.64, No.7, Oct 2020.

[3] **End-to-End Formal Verification of Ethereum 2.0 Deposit Smart Contract**.
Daejun Park, Yi Zhang, and Grigore Rosu. *Proceedings of the 32nd International Conference on Computer-Aided Verification (CAV'20)*, 2020.

[4] **A Complete Formal Semantics of x86-64 User-Level Instruction Set Architecture**.
Sandeep Dasgupta, *Daejun Park*, Theodoros Kasampalis, Vikram S. Adve, and Grigore Rosu. *Proceedings of the 40th ACM SIGPLAN Conference on Programming Language Design and Implementation (PLDI'19)*, 2019.

[5] **Logistic Regression on Homomorphic Encrypted Data at Scale**.
Kyoohyung Han, Seungwan Hong, Jung Hee Cheon, and *Daejun Park*. *Proceedings of the Thirty-First AAAI Conference on Innovative Applications of Artificial Intelligence (IAAI'19)*, 2019.

[6] **Verifiable Computing for Approximate Computation**.
Shuo Chen, Jung Hee Cheon, Dongwoo Kim, and *Daejun Park*. *IACR Cryptology ePrint Archive, Report 2019/762*, 2019.

[7] **A Language-Independent Approach to Smart Contract Verification**.
Xiaohong Chen, *Daejun Park*, and Grigore Rosu. *Proceedings of the 8th International Symposium on Leveraging Applications of Formal Methods, Verification and Validation (ISoLA'18)*, 2018.

[8] **A Formal Verification Tool for Ethereum VM Bytecode**.
Daejun Park, Yi Zhang, Manasvi Saxena, Philip Daian, and Grigore Rosu. *Proceedings of the 2018 26th ACM SIGSOFT International Symposium on Foundations of Software Engineering (FSE'18)*, 2018.

[9] **KEVM: A Complete Formal Semantics of the Ethereum Virtual Machine**.
Everett Hildenbrandt, Manasvi Saxena, Nishant Rodrigues, Xiaoran Zhu, Philip Daian, Dwight Guth, *Daejun Park*, Yi Zhang, Brandon Moore and Grigore Rosu. *Proceedings of the 2018 IEEE Computer Security Foundations Symposium (CSF'18)*, 2018.

[10] **Invariant Synthesis for Incomplete Verification Engines**.
Daniel Neider, P. Madhusudan, Pranav Garg, Shambwaditya Saha, and *Daejun Park*. *Proceedings of the 24th International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS'18)*, 2018.

[11] **Semantics-Based Program Verifiers for All Languages**.
Andrei Stefanescu, *Daejun Park*, Shijiao Yuwen, Yilong Li, and Grigore Rosu. *Proceedings of the 2016 ACM SIGPLAN International Conference on Object-Oriented Programming, Systems, Languages, and Applications (OOPSLA'16)*, 2016. **Distinguished Paper Award**.

[12] **KJS: A Complete Formal Semantics of JavaScript**.
Daejun Park, Andrei Stefanescu, and Grigore Rosu. *Proceedings of the 36th ACM SIGPLAN Conference on Programming Language Design and Implementation (PLDI'15)*, 2015.

[13] **Global Sparse Analysis Framework**.
Hakjoo Oh, Kihong Heo, Wonchan Lee, Woosuk Lee, *Daejun Park*, Jeehoon Kang, and Kwangkeun Yi. *ACM Transactions on Programming Languages and Systems (TOPLAS)*, Vol.36, No.3, Sep 2014.

Awards

Feng Chen Memorial Award, University of Illinois at Urbana-Champaign	2017
Distinguished Paper Award at OOPSLA'16	2016

Last updated: January 11, 2021