Increases Hardware Security and Information Processing Efficiency

This virtual architecture interface improves both security and performance for field-programmable gate arrays (FPGAs). FPGAs are integrated circuits that can be configured — and reconfigured — by a customer after manufacture. They function almost as blank slates, which the customer can customize with a bit file. This flexibility allows FGPA use in a wide variety of fields, including wearable electronics, space exploration, defense and the internet of things (IoT), which refers to the connection of devices like appliances, cars or health monitors to the internet. Available computer-aided design (CAD) tools for FPGAs fail to provide the security, performance, and programmability that these types of uses demand.

Researchers at the University of Florida have developed a full bridge LLC resonant converter that automatically dampens the amount of electromagnetic interference produced.

Application

These virtual architecture interfaces provide a range of overlay architectures to improve the performance, security, and programmability of FGPAs.

Advantages

- Improves data security, reducing risk of piracy or cloning
- Constructs overlay architecture closely matched to the requirements of an application or domain, improving programmability, flexibility, and productivity
- Reduces bitstream size, enabling easier field upgrades
- Allows for dynamic reconfiguration of FPGAs, improving working flexibility
- Increases design-space exploration speed by three orders of magnitude, allowing for faster innovation and development

Technology

Unique virtual architectures make the underlying hardware appear different on every FPGA device, despite having the same functionality, by separating true device functionality from hardware-specific resources. The architecture interface makes reverse engineering, piracy, and tampering difficult because while the actual FPGA architecture is described in documentation, and the hardware itself is identical among specific devices. The overlay architecture can be proprietary for a company or product and kept confidential. The automatically-generated architectural variants can deter large-scale piracy and reverse engineering efforts.
Inventors

**Gregory Michael Stitt, Ph.D.**, is an associate professor in the University of Florida’s Electrical and Computer Engineering Department. He earned both a bachelor’s degree and a Ph.D. in computer science from the University of California, Riverside. Dr. Stitt’s research deals with reconfigurable computing, FPGAs, synthesis/compilers/CAD, architecture, and embedded systems. He is also a recipient of the NSF CAREER Award.

**Kai Yang** is a Ph.D. candidate in the Electrical and Computer Engineering Department at the University of Florida. He received a bachelor’s degree in electrical engineering from Tianjin University and his master’s degree in electrical engineering from Beijing Institute of Technology. His current research interests include hardware security and reconfigurable hardware.

**Swarup Bhunia, Ph.D.**, is a professor in the Department of Electrical and Computer Engineering at the University of Florida. He earned his bachelor’s degree in engineering from Jadavpur University, his master’s degree from Indian Institute of Technology, and his Ph.D. in electrical and computer engineering from Purdue University in 2005. Dr. Bhunia received an IBM Faculty Award in 2013 and the National Science Foundation (NSF) Career Development Award in 2011. His research interests include low power and robust design, hardware security and trust, adaptive nanocomputing, and novel test methodologies.

**Robert A Karam, Ph.D.**, earned his bachelor’s and master’s degrees in computer engineering from Case Western Reserve University in 2012 and 2016 and his Ph.D. in electrical and computer engineering from the University of Florida in 2017. His research interests include hardware security, reconfigurable computing, and signal processing algorithm/hardware co-design for bioimplantable devices.

Contact:
Richard Croley • 352-392-8929 • rcroley@ufl.edu
UF #16477