SaTC: CORE: Small: Trustworthy System-on-Chip Design using Secure On-Chip Communication Architecture

Prabhat Mishra, University of Florida
https://www.cise.ufl.edu/research/cad/NoC.html

Overview and Motivation

➢ Network-on-Chip (NoC) is the communication fabric of modern System-on-Chip (SoC) designs.

➢ NoC connects SoC components using diverse topologies with network interfaces and routers.

➢ NoC can use different technologies such as electrical, wireless, and optical communication.
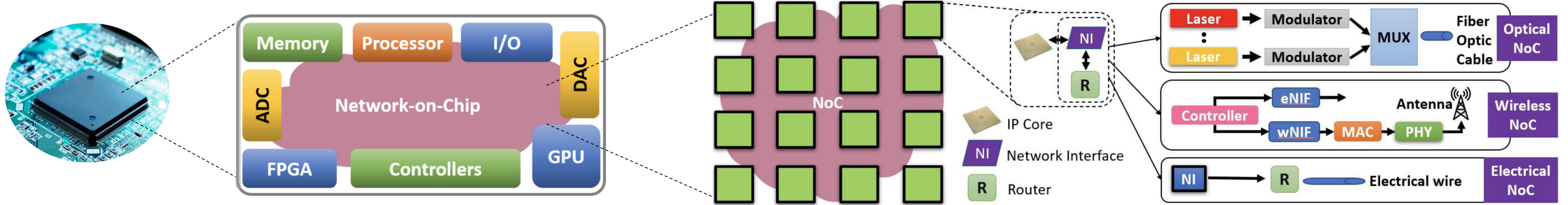
Research Challenges

➢ NoC is a primary target for security attacks since it handles information of different IPs.

➢ Traditional networking security solutions are not applicable on resource-constrained NoCs.

➢ Complexity of SoC designs have made exhaustive security validation infeasible.

➢ Security solutions need to address diverse technologies & communication architectures.

➢ Securing NoC is vital to design trustworthy computing with NoC-based SoCs.

Scientific Impact

➢ Provides lightweight solutions for securing communication in resource-constrained SoCs

➢ Presents security solution applicable on diverse technologies covering electrical, wireless, optical and hybrid communications.

➢ Covers diverse security challenges including lightweight authentication, encryption, routing anonymity, availability, real-time attack detection, and fast localization.

➢ Adaptively learns and defends new attacks.

Proposed Solutions

Developed a lightweight and secure NoC architecture for secure communication between diverse IPs addressing the following challenges:

o Reconfigurable NoC Architecture [TODAES'20]

o Lightweight encryption [HOST'21, ISVLSI'20]

o Anonymous routing [DATE 2020]

o Trust-aware routing [ISVLSI 2020]

o Real-time attack detection [DATE'19, TCAD'20]

o Digital watermarking [TVLSI 2022]

o Malware detection [DATE 2021]
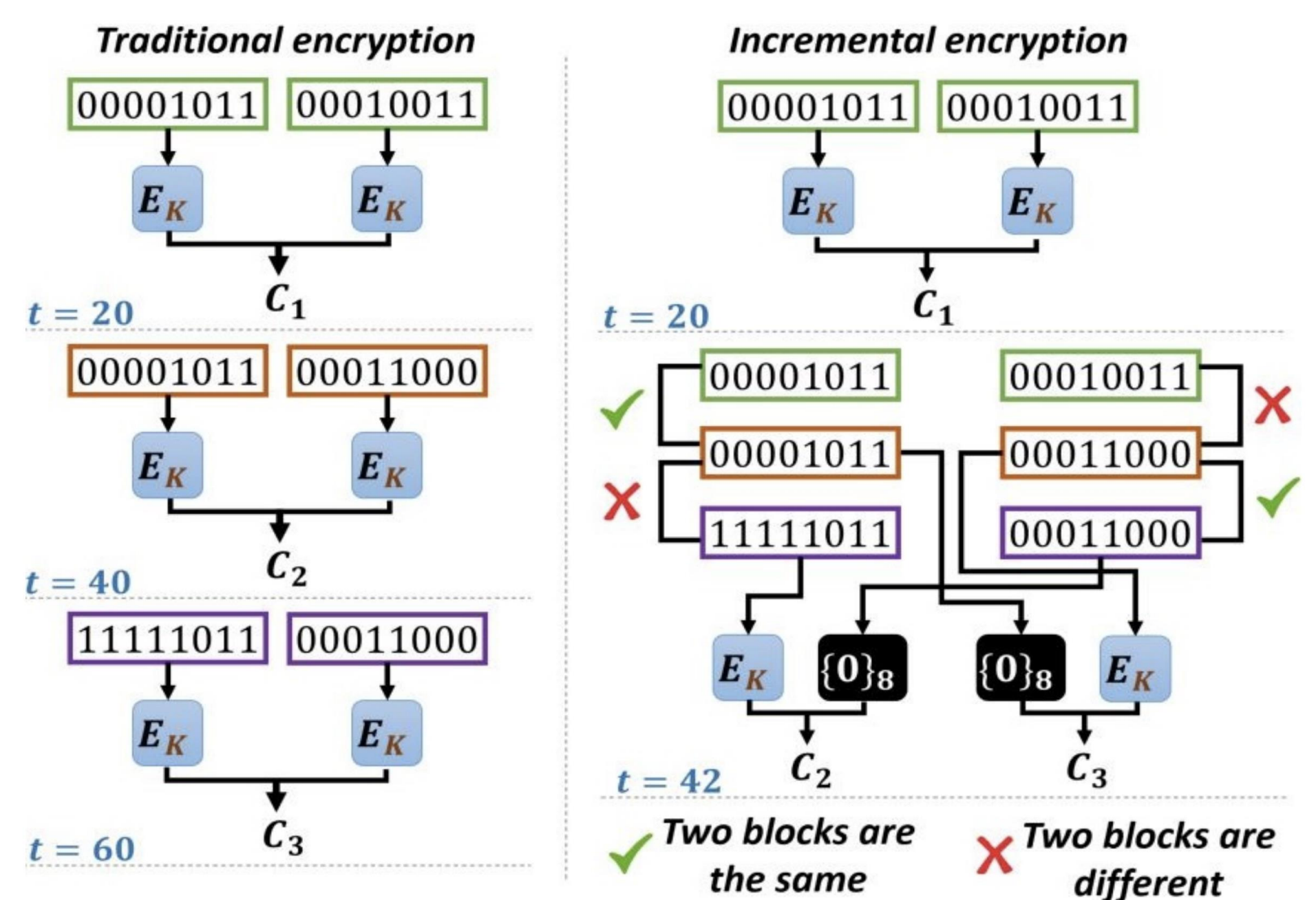
Impact on Society

➢ Secure NoC architecture would enable trusted SoC design with untrusted IPs.

➢ Improves life of people by ensuring their security and privacy in the digital world.

➢ Mitigate financial and other losses to stakeholders due to security attacks.

Education and Outreach

➢ Survey on NoC security [CSUR'21]

➢ Book on NoC security [Springer'21]

➢ Ten book chapters, six journal articles, nine conference papers, and seven (pending) patents.

➢ Panel [NoCArc'21] on ML with NoC

➢ Special session [DATE'21]

➢ Integrated as a lecture module.

Broader Participation

➢ Trained 3 PhD students (one became a faculty at Univ. of Moratuwa).

➢ Eight REU researchers including three women (two women joined PhD).

➢ Led to joint publications with researchers in several countries.