



Jakub Szefer's research interests are at the intersection of computer architecture and hardware security. Jakub's recent projects focus on: security verification of processor architectures; hardware (FPGA) implementation of cryptographic algorithms, especially post-quantum cryptographic (PQC) algorithms; designs of new Physically Unclonable Functions (PUFs); and leveraging physical properties of computer hardware for new

cryptographic and security applications. Jakub's research is currently supported through National Science Foundation and industry donations. Jakub is a recipient of a 2017 NSF CAREER award. He joined Yale University in summer 2013 as an Assistant Professor of Electrical Engineering, where he started the Computer Architecture and Security Laboratory (CAS Lab). Prior to joining Yale, he received Ph.D. and M.A. degrees in Electrical Engineering from Princeton University and worked with Prof. Ruby B. Lee on secure processor architectures. He received B.S. with highest honors in Electrical and Computer Engineering from University of Illinois at Urbana-Champaign.