**Motivation**

- Biometric Cryptosystems offer an effective alternative to traditional password based cryptography. However, these systems must be made efficient if they are to become widely implemented.

**Objectives and Approach**

- Implement the biometric cryptosystem designed by Hao et al. using the C programming language.
- Design specialized hardware accelerators to meet the computation demand associated in designing and implementing such systems.
- Focus on the hardware accelerator as a co-processor that offloads the work from the general purpose processor to achieve better performance and energy efficiency.
- Implementation and testing will be performed using the Xilinx Zynq®-7000 All Programmable SoC Zedboard.

**Milestones**

- Implement a software only system on the FPGA platform.
- Identify the computation intensive section(s) of code and perform hardware/software co-design.
- Develop the hardware IP and implement it on the FPGA platform.
- Evaluation of the proposed scheme.

**Contact Information**

- Chen Liu: cliu@clarkson.edu
- Charles McGuffey: mcguffcj@clarkson.edu

---

**Accomplishments**

- Software implementation of the biometric cryptosystem.
- A C project has been implemented that successfully meets the specifications of Hao et al.
- Profiling Software Implementation

![Time Taken by Percent](image)

- Program Optimization

![Runtime (ms) Biometric Cryptosystem Runtimes](image)

- One Hardware Acceleration Cycle Complete
- The count_ones function was accelerated, but due to the small size of the function there were no performance improvements.

---

**The Biometric Cryptosystem**

- 140 bit randomly generated key
- Iris biometric template

**Next Steps**

- Perform additional hardware acceleration cycles
- Combine FPGA acceleration with other acceleration techniques
- Extend acceleration techniques to additional cryptosystem algorithms
- Analyze efficiency results for hardware acceleration patterns

**References**