Augmented and Autonomous Vehicle Security

Kevin Gilbert, Christopher Haster, Gilberto Rodriguez III, Hao Chen, Young Chou, Joshua Bryant
University of Texas at Austin

-

Abstract

Our research project is focused on highlighting security concerns in augmented and autonomous vehicles. We have developed and built a robotics testbed and simulator on which we can measure and apply real-world data. We primarily focus on the two coupled weak points in augmented automotive cybersecurity: wireless transceiver entry points into an unsecured Controller Area Network (CAN).

Main Objectives

Our main objectives were to design and implement a testbed on which we could launch security exploits and defenses while providing a retrospective of current automotive cybersecurity. We wished to highlight the inherit dangers of an unsecured CAN bus and demonstrate the necessity of high speed, short-term encryption. Our goals were to create a secured CAN-like protocol within a FPGA coupled with hardware encryption on which we could pipe wireless packets through. We would test this device with a set of wireless transceivers at high speeds in moving vehicles and within our robotics testbed. The realworld data we generated could then be used within a simulator in which we could measure safety and implement a variety of network protocols.

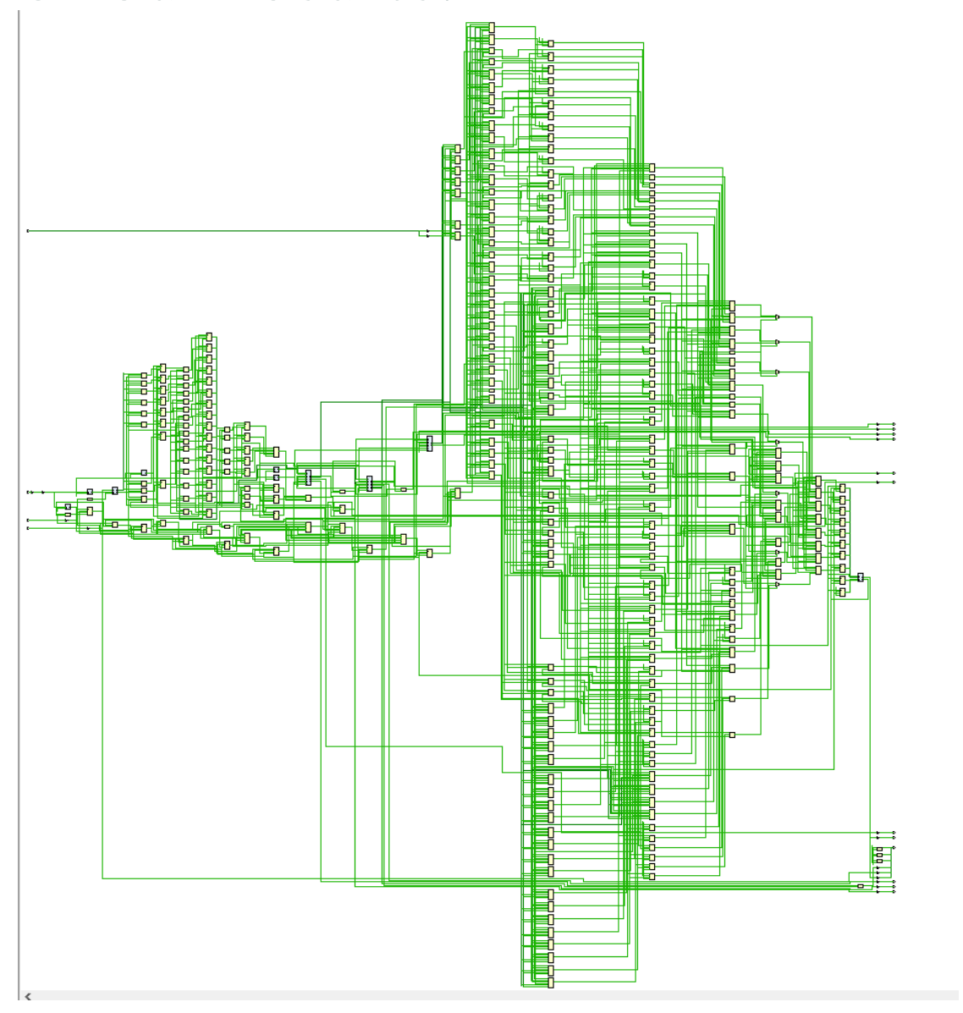
Modules

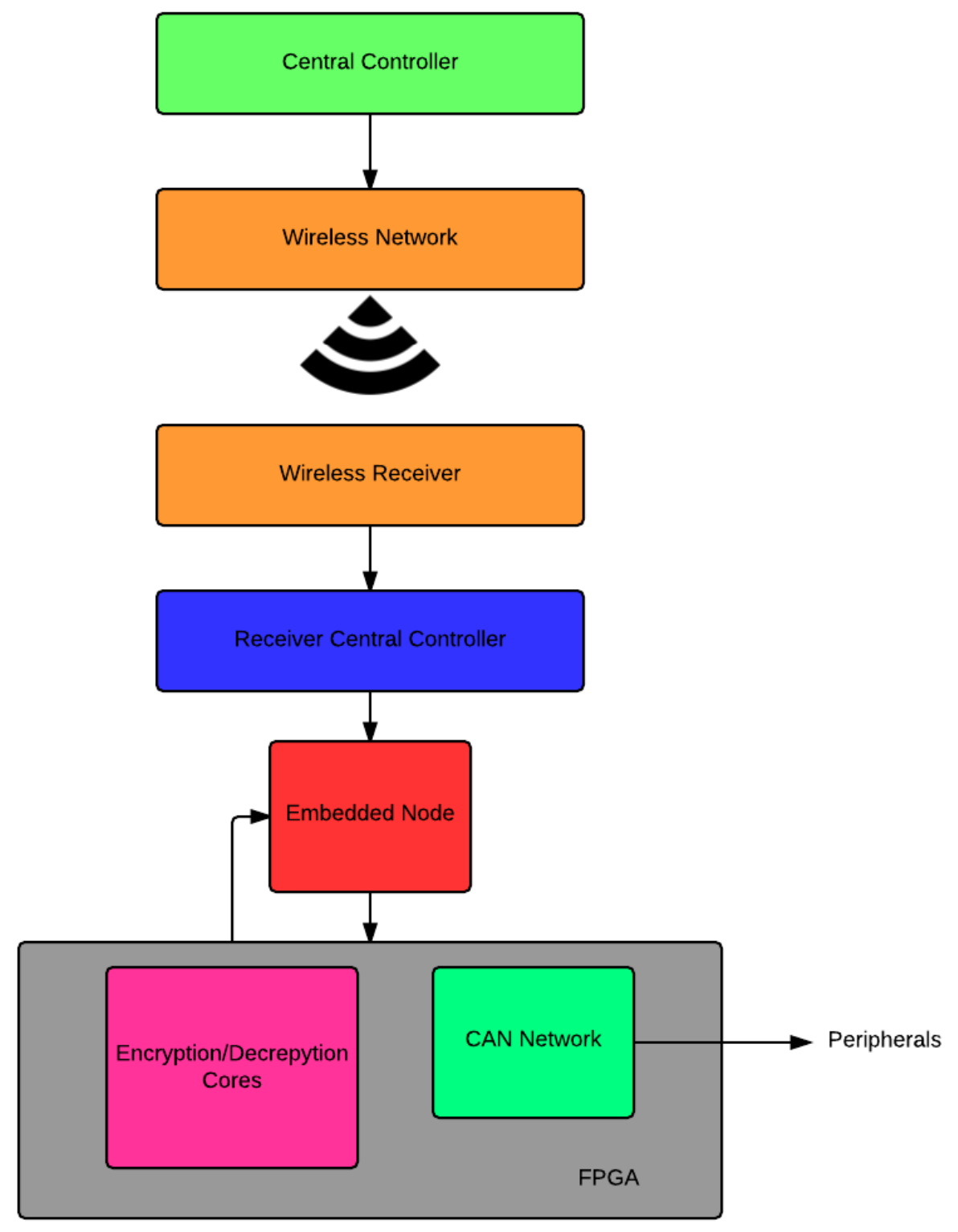
Our primary modules were broken down into:

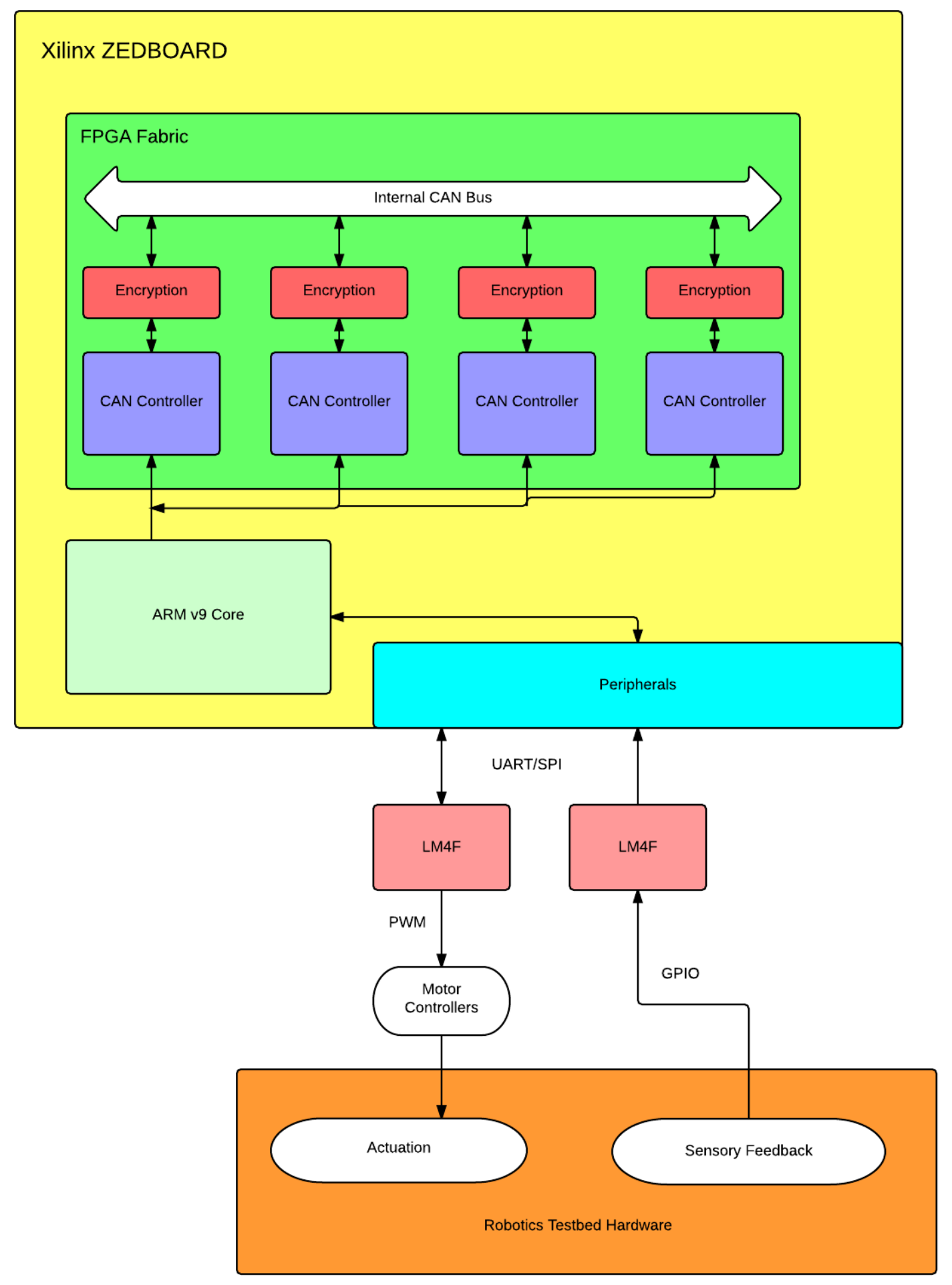
- FPGA -
  CAN Bus
  UART - CAN Packet Translation
  PWM Generation
  Hardware Encryption
- Wireless Transceivers -
  Data Transmission
  Software Encryption
- Robotics Testbed -
  Data Measurement
- Embedded -
  IMU Measurement
  Motor Control (PID)
  Laptop to CAN Bus Interface
  Sensor Interface
- Simulator -
  Network Timing Constraints

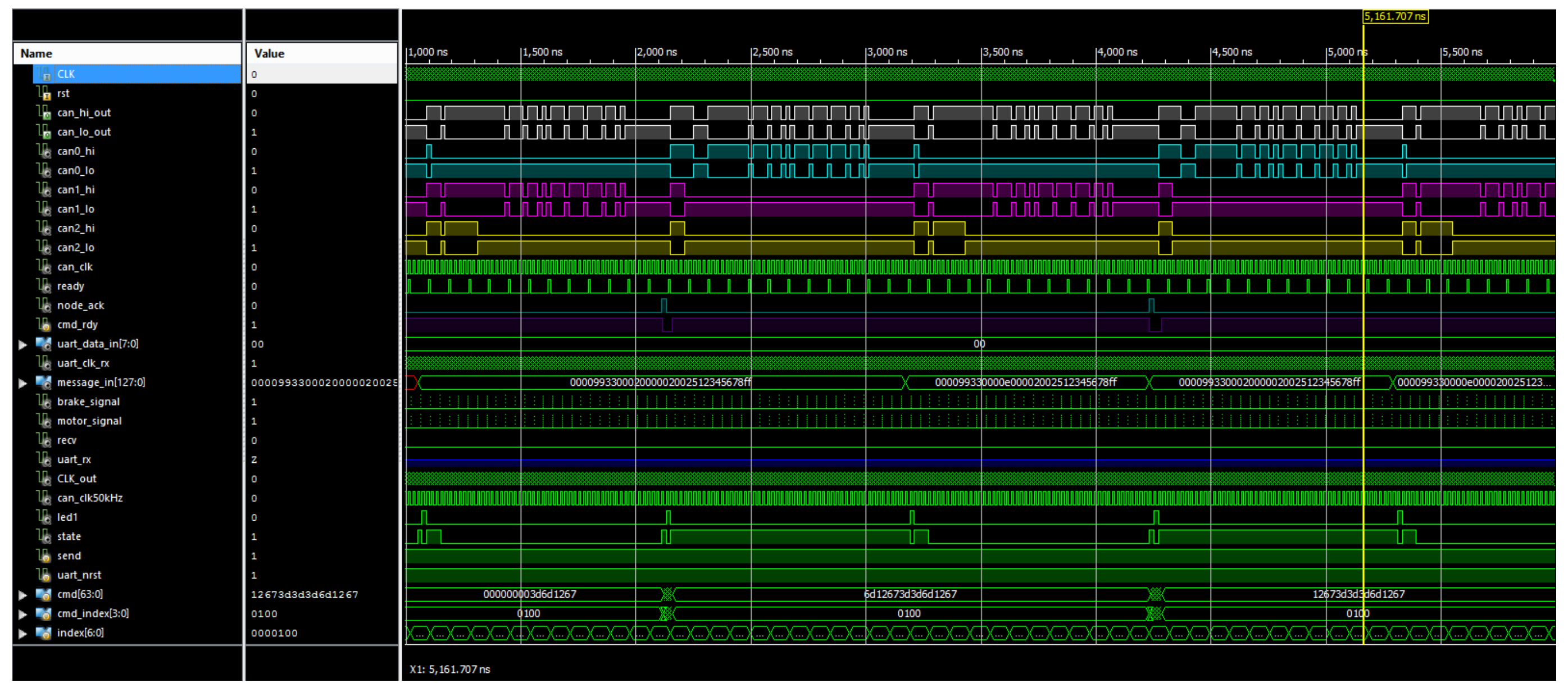
Measurements and Data

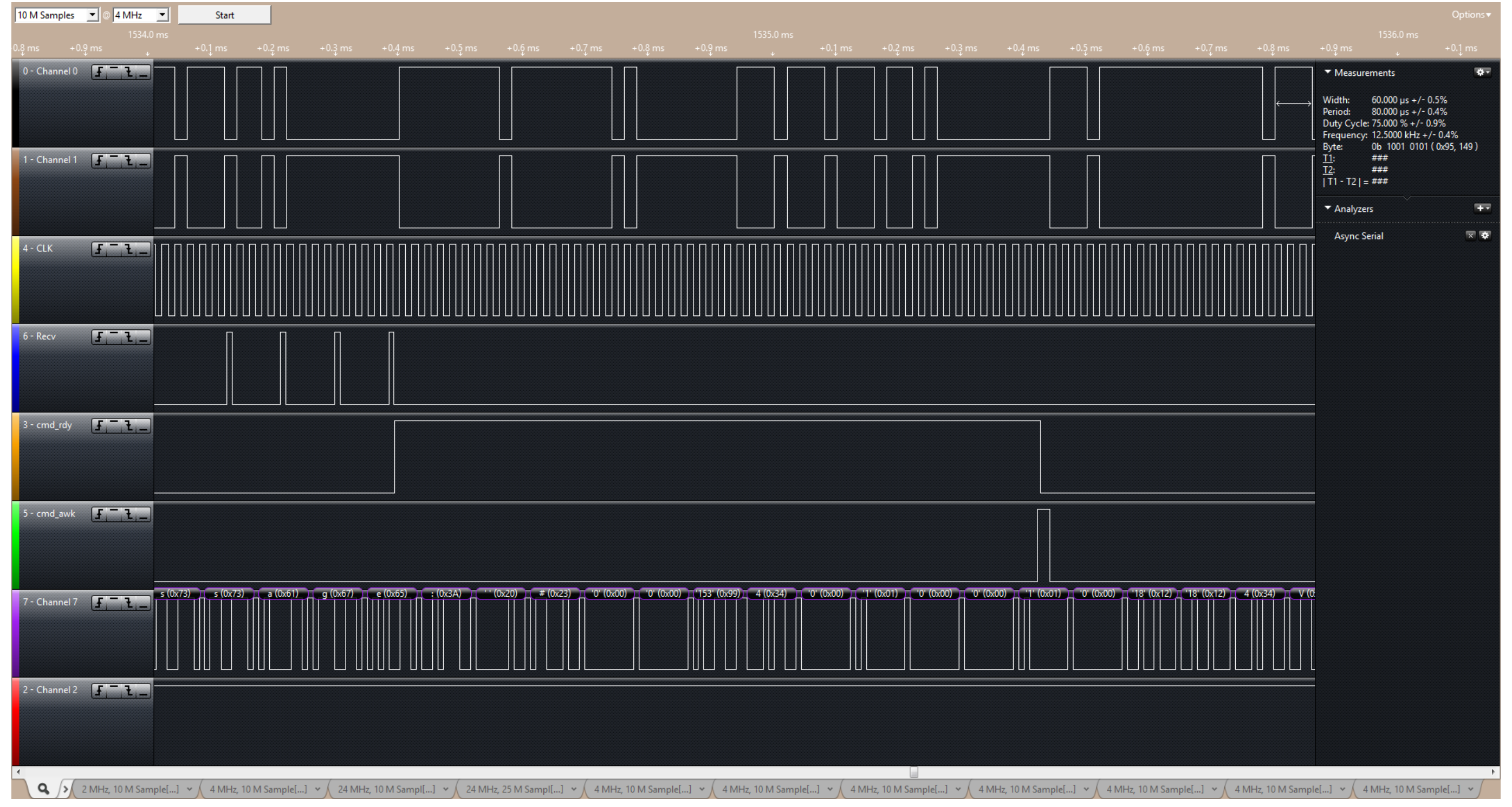
We will focus on modular specific system testing and timing constraints collected in this section. The following section will collect this data into a summary of our results.

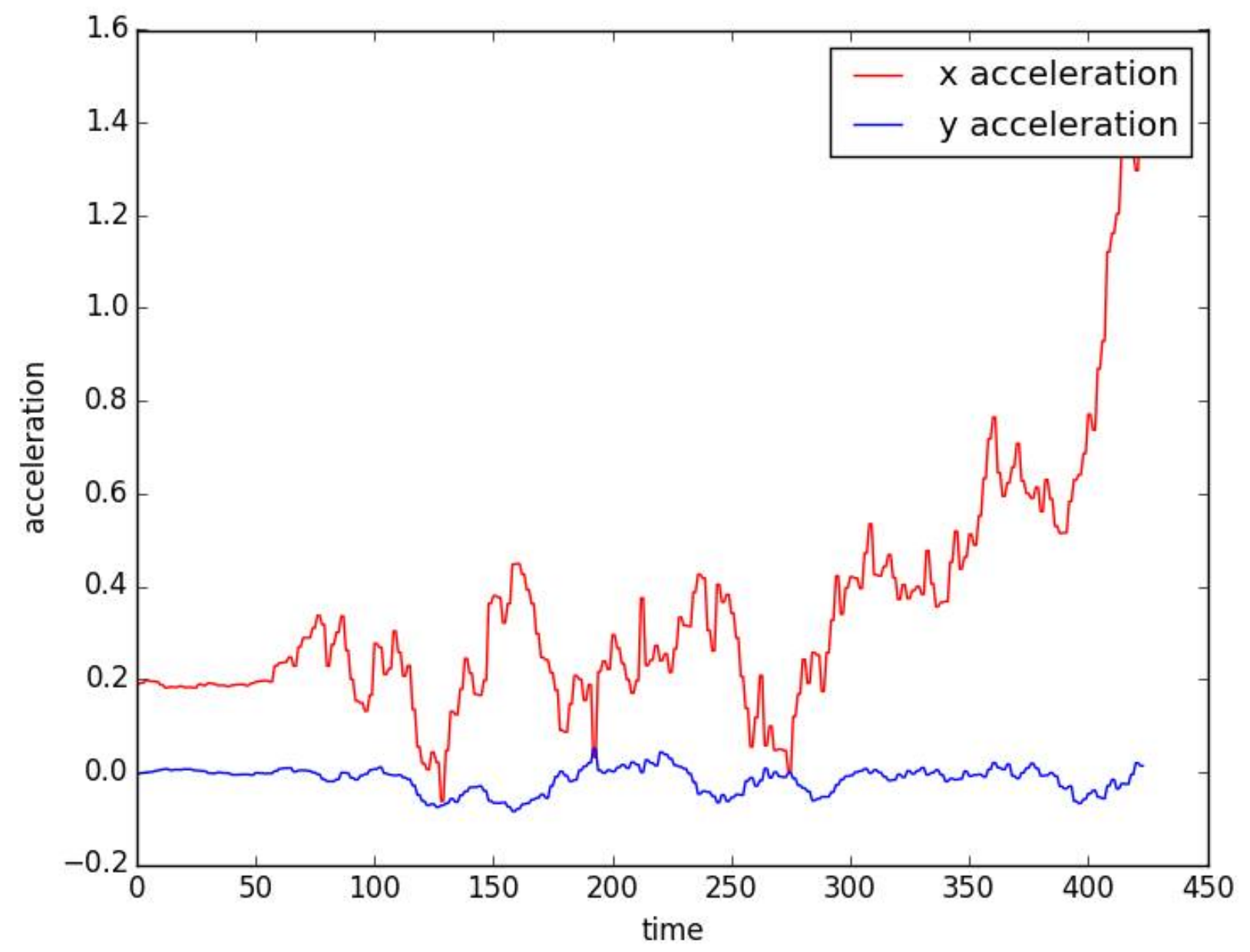


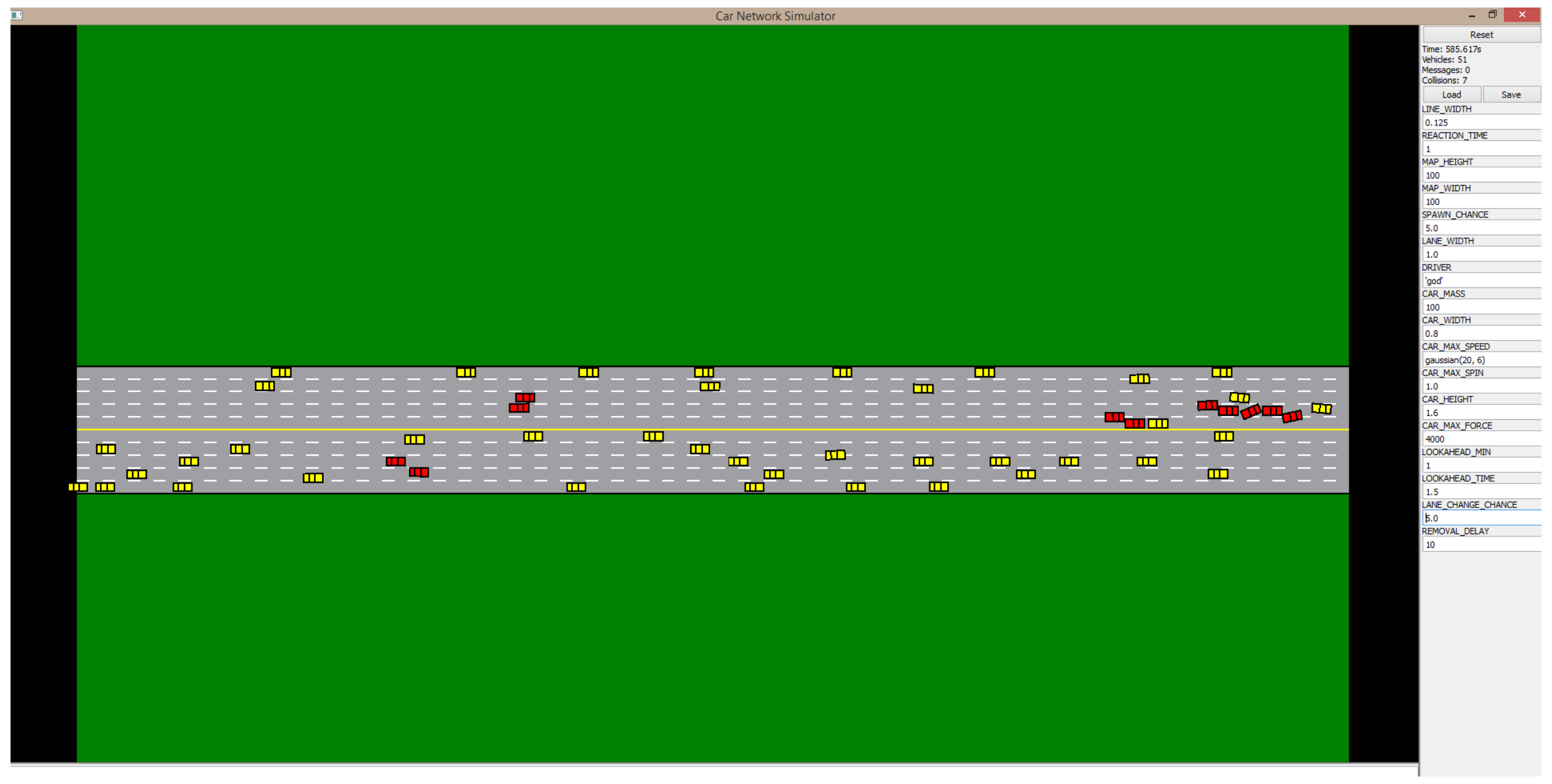












Results

Software encryption was shown to be extremely slow, taking upwards of 8.9 seconds to scramble data using a simple cipher. In addition during wireless transmission, using an ad-hoc (typically used for long term secure channels) took several seconds on average to connect. This would not be a feasible communication method at high speeds. Utilizing high frequency channels similar to DSRC would allow for rapid bursts of data, while using hardware encryption would provide ciphertext at the rate of between 20-100ns for a 128-bit block (using a tiny AES-256 core on a Xilinx Zync FPGA running at 50MHz).

Conclusions

Vivamus molestie, risus tempor vehicula mattis, libero arcu volutpat purus, sed blandit sem nibh eget turpis. Maecenas rutrum dui blandit lorem vulputate gravida. Praesent venenatis mi vel lorem tempor at varius diam sagittis. Nam eu leo id turpis interdum luctus a sed augue. Nam tellus.

Acknowledgements

Dr. Tiwari, TI, UT Austin, swiggity swaggity swoop