Cryptographic Hardware Acceleration for Vehicular Internet of Things (IoT)

Ankush Singla
MS, Information Security
Purdue University
asingla@purdue.edu

Anand Mudgerikar
MS, Information Security
Purdue University
amudgeri@purdue.edu

Elisa Bertino
Professor
Purdue University
bertino@purdue.edu

Ioannis Papapanagiotou
Assistant Professor
Purdue University
ipapapan@purdue.edu

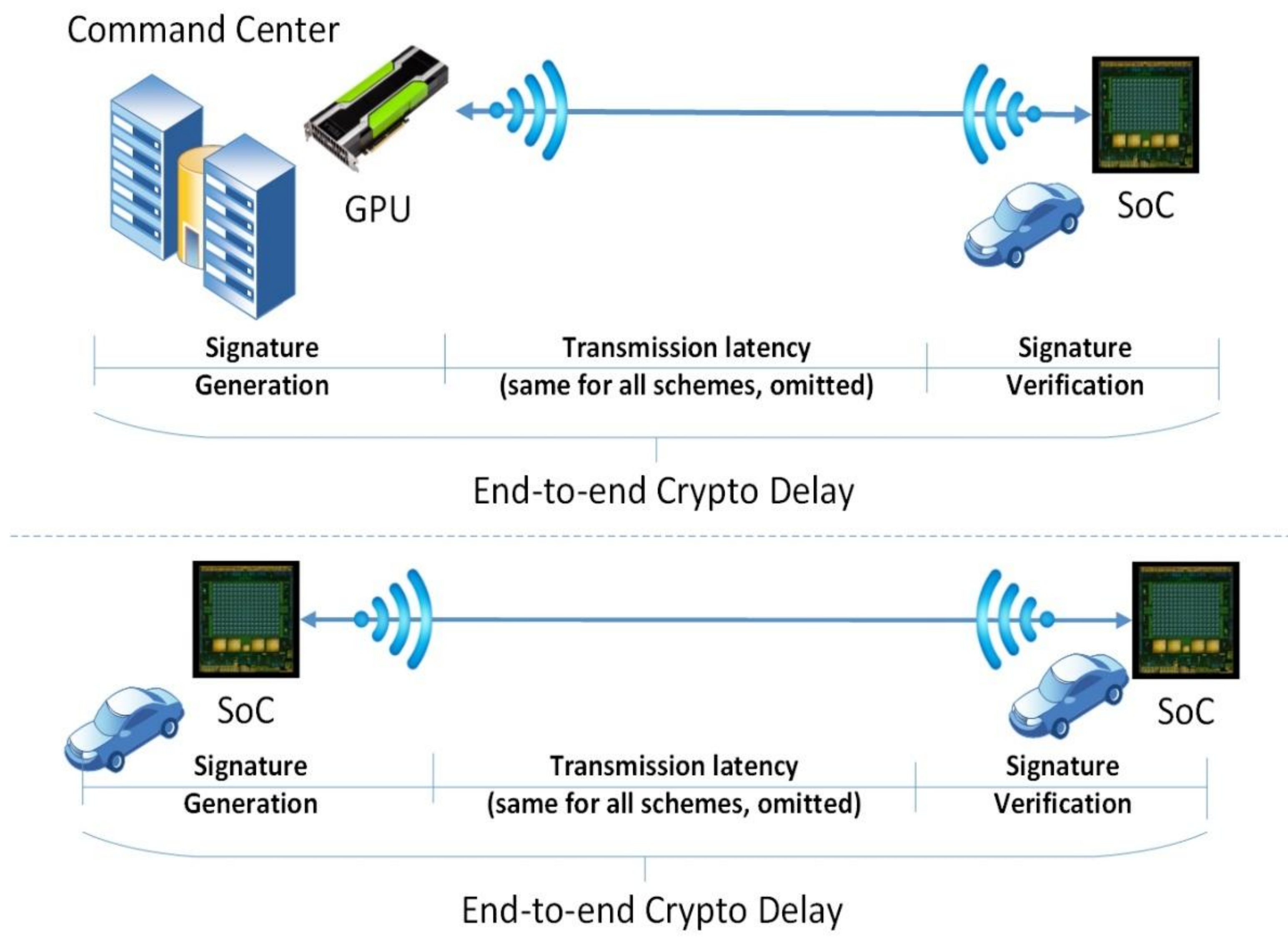
Atilla Yavuz
Assistant Professor
Oregon State University
Attila.Yavuz@oregonstate.edu

Problem Statement:

- Modern Vehicles are equipped with advanced sensing and communication technologies, which enable them to support services in Vehicular Internet of Things (IoTs) era such as autonomous driving.
- The communication in IoTs must be delay-aware, reliable, scalable and secure[1,2] to
  a) prevent an attacker from injecting/manipulating messages;
  b) minimize the impact introduced by crypto operations.
- Existing crypto mechanisms introduce significant computation and bandwidth overhead, which creates critical safety problems.

Research Objectives:

- Design new digital signatures that are ideal for delay-aware Vehicular IoTs;
- Using Mobile Multiprocessor Systems on Chip (MpSoC) integrated in vehicles;
- Evaluation via theoretical analysis, simulation, and deployment in actual vehicular networks at Purdue University airport.



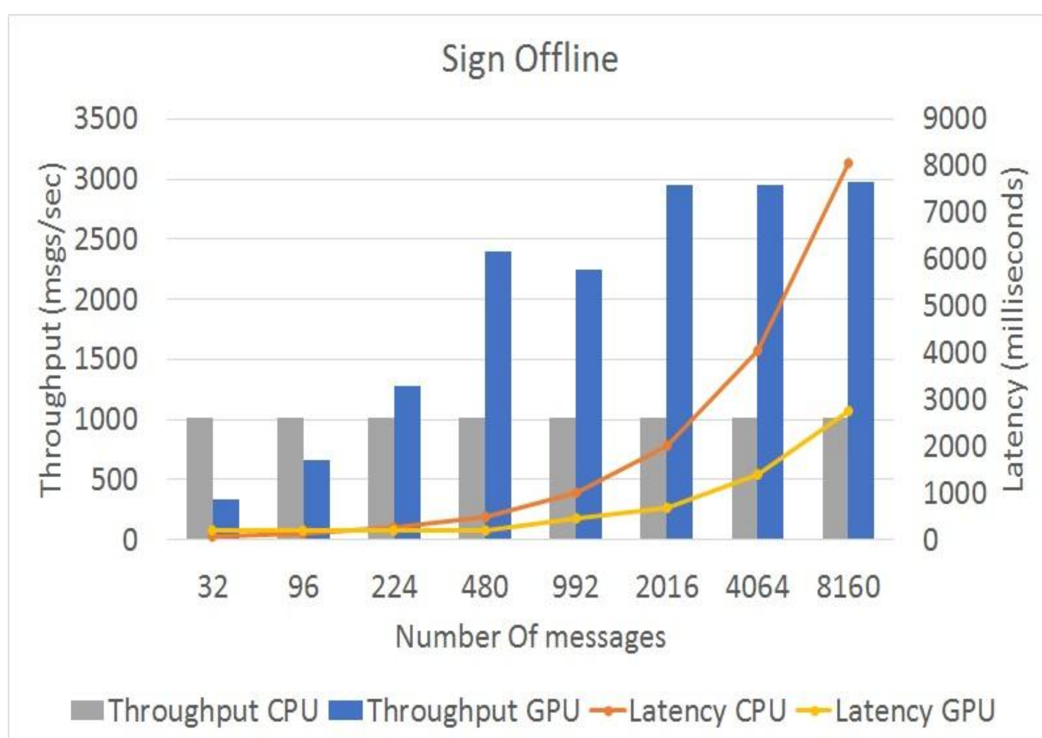
Part 1 – Design efficient Cryptographic Schemes for Vehicular IoTs

- Structure-Free and Compact Real-time Authentication: SCRA permits signing a message without assuming any pre-defined structure. It will be will be several times more efficient than existing signature schemes like RSA, ECDSA etc.
- Fast Digital Signatures via Special Offline-Online Strategies: Develop special offline-online signature strategies, which will significantly increase the computational efficiency of these schemes.

Protocol	End-End Crypto Delay (msec)
RSA – 2048	4
ECDSA – 256	1.18
RA – 2048	0.69
HAA – 2048	0.21
RA 2048 SoC	7.1
HAA – 2048 SoC	2.6

Part 2 – Multiprocessor System On Chips (MpSoCs)

- Deploy hardware optimizations in vehicular certified MpSoCs exploiting CPU/GPU co-processor architectures (Intel/ARM vs CUDA/OpenCL based GPUs).
- Develop hardware/optimization suites that exploit parallelism, and algorithmic and algebraic properties of the crypto algorithms in Vehicular IoTs.

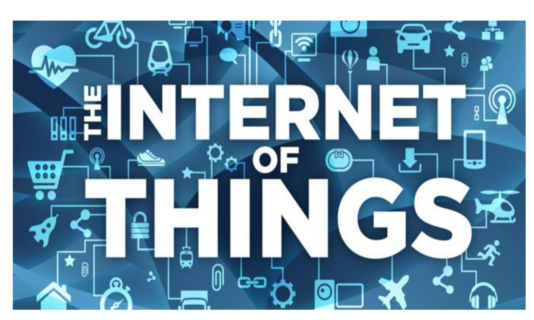


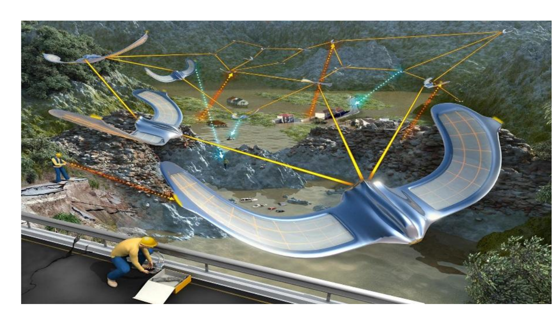
- Embedded SoCs are used by major car manufacturers (e.g., Audi, BMW, Ford, Mercedes and Tesla) for their infotainment and communication systems. They come with high-bandwidth peripherals, sensors, and network interfaces.

Part 3 – On-field deployment and Evaluation

- Perform experiments in a fleet of R/C cars equipped with MpSoCs and Arduino boards and several sensors.
- Extensively evaluate our methods on actual vehicles.
- Use Purdue Airport to perform real-time experiments in a controlled and large-scale environment.

Future possibilities





Hardware Provided By:

NVIDIA CUDA RESEARCH CENTER
intel inside
QUALCOMM

[1]*Vehicle-to-Vehicle Communications: Readiness of V2V Technology for Application*. U.S. Department of Transportation National Highway Traffic Safety
Administration (NHTSA), August 2014.
[2]*Tracking & Hacking: Security & Privacy Gaps Put American Drivers at Risk*, Ed Markey, US Senator of Massachusetts, February 2015.