A Reconfigurable Arduino Crypto FPGA Shield

galois

Dustin Schnelle
Gomathy Venkata Krishnan
Meiqi Zhao
Ryan Bornhorst

Sponsors:
Joe Kiniry
Dan Zimmerman
Special Thanks to Flemming Andersen

Advisor:
Dr. Christof Teuscher

Project Summary

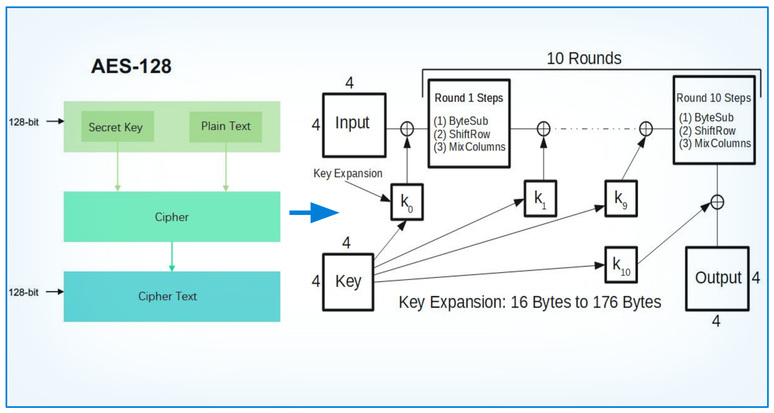
The Reconfigurable Arduino Crypto FPGA uses an FPGA shield to encrypt data. Cryptol software was used to implement a high performance, mathematically correct cryptographic algorithm. SAW software was used to generate the formally verified SystemVerilog code using SAWScript. SMT (Satisfiability Modulo Theories) and SAT solvers were used to formally verify these properties.

We verified the correctness of the AES-128 crypto-algorithm using this software. We then implemented the code into an FPGA and observed the speed it takes to encrypt the data. We compared the results and observed the trade-offs between the FPGA and other systems using the same algorithm.

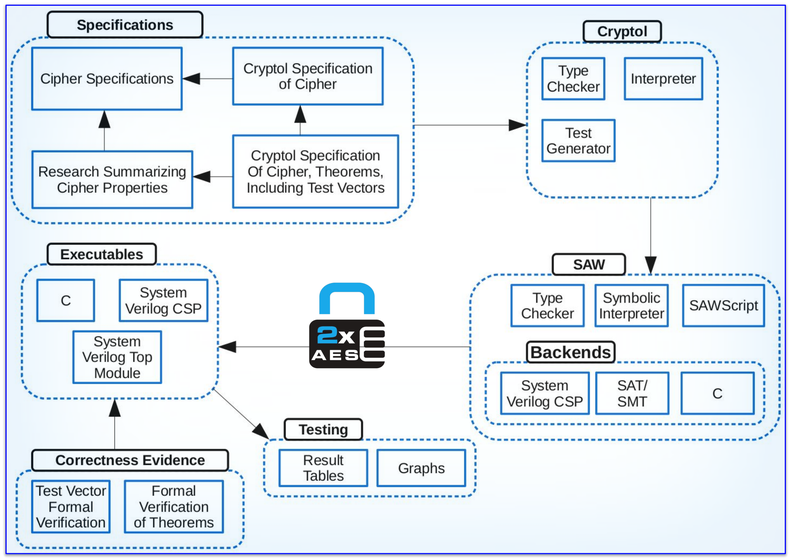
Cryptographic Algorithm: AES128

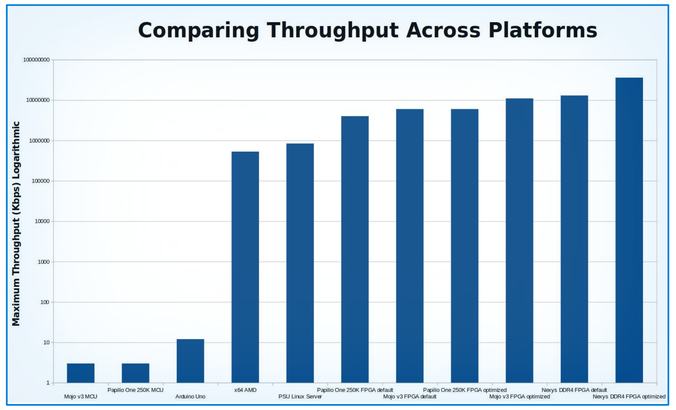
The Advanced Encryption Standard (AES) is a symmetric encryption algorithm standardized by the U. S. National Institute of Standards and Technology (NIST). AES supports multiple fixed data block sizes, and in this project we used AES with 128-bit blocks (AES-128).

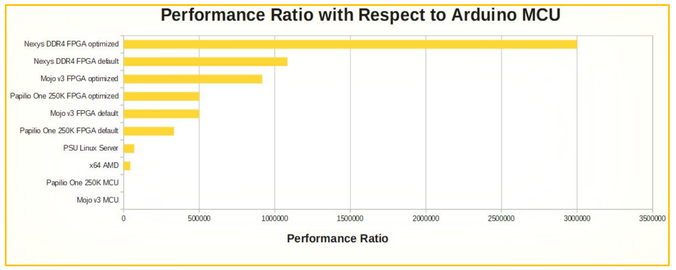
Formal assurance uses mathematical modeling to prove that a system is correct with respect to a formal specification. We used the Cryptol software to show that our hardware implementation of AES-128 is correct.



High-Assurance Crypto Toolchain







Results

Our team was able to show that AES-128 algorithm has faster speeds on an FPGA format then on a CPU or MCU. The results for both the FPGA boards (Nexys DDR4 & Mojo v3) is more than twice the speed of the CPU's running the algorithm. The results for the FPGAs are also much faster then the Arduino platform. The performance of the FPGA is the most efficient given the resources it uses and its clock frequency.

Board	System	Frequency	BRAMs	LUTs	Slices	Utilization (%)	Throughput(Gbps)
Arduino Uno	Atmega 328P	16 MHz	NA	NA	NA	NA	$12x10^{-6}$
PSU Linux Server	Intel Xeon CPU E3	3.5 GHz	NA	NA	NA	NA	$840x10^{-3}$
x64 AMD	AMD A10-5800K	3800 MHz	NA	NA	NA	NA	$530x10^{-3}$
Nexys DDR4 FPGA default	Artix-7	100 MHz	0	87	88	0.42%	13
Nexys DDR4 FPGA optimized	Artix-7	280 MHz	0	62	65	0.36%	36
Mojo v3 default	Spartan-6 XC6SLX9	50 MHz	3	1400	185	62%	6
Mojo v3 optimized	Spartan-6 XC6SLX9	88 MHz	3	1231	168	52%	11
Mojo v3 MCU	Atmega 32U4	16 MHz	NA	NA	NA	NA	$3x10^{-6}$
Papilio One 250K default	Spartan-3E 3S250E	32 MHz	4	1600	198	81%	4
Papilio One 250K optimized	Spartan-3E 3S250E	50 MHz	4	1424	187	73%	6
Papilio One 250K MCU	Atmega 32U4	16 MHz	NA	NA	NA	NA	$3x10^{-6}$

Conclusion and Future Work

While working on this project, we were able to show that the FPGA implementations of AES-128 were able to encrypt data at rates faster than other platforms considering the resources being used.

In the future, the bitstream will be generated for the Mojo v3 and the Pulserain M10 and the speed will be verified. Future work will include testing and verifying the SHA-2 and RNG (DRBG) algorithms.

A custom daughter board for the Arduino Uno will be created with the fastest FPGA which will be reconfigurable, cost effective, easy to deploy, and very secure.

Bibliography:

National Institute of Standards and Technology, "Announcing the ADVANCED ENCRYPTION STANDARD (AES)." Federal Information Processing Standards Publications, 26-Nov-2001. https://csrc.nist.gov/csrc/media/publications/fips/197/final/documents/fips-197.pdf