College of Engineering & Applied Science
UNIVERSITY OF COLORADO BOULDER

Independent Study Agreement

Independent Study Policy & Guidelines

Introduction

Independent Study is an opportunity for students to earn academic credit for learning outside the formal class structure, under the individual direction of a faculty member. Independent Study is provided to fill an academic need of importance to the student that cannot be filled by the regular curriculum.

Students wishing to pursue an Independent Study with a College of Engineering and Applied Science faculty member (including Herbst Program faculty) must complete the following steps:

1. Meet with the proposed Sponsoring Faculty Member to discuss an Independent Study proposal and review the potential project and deliverables.

2. Complete the Independent Study Agreement form. Include a complete description of the project, procedure and deliverables, minimum of 250 words. Use of complete sentences and proper grammar is expected.

3. Upon submission of this electronic form, your proposal will be reviewed by the appropriate parties. If enrolled, it is your responsibility to discuss with your academic advisor how this Independent Study course will apply towards degree requirements.

Policies/Eligibility

1. The College allows a maximum of 6 hours of Independent Study degree credit towards the BS, but major departments may be more restrictive. A maximum of 3 hours may be taken in any one semester. ***Prior written approval, via the College's Independent Study Agreement, is required prior to any initiation of course work.***

2. For an undergraduate student to be eligible for Independent Study, a student should have completed a significant portion of his/her undergraduate studies with a very good GPA, and must have some relevant background knowledge and/or experience.

3. Independent study work cannot exceed 25% of the course work requirement for master's degree students.

4. Although the Graduate School prescribes no limit on independent study for doctoral students, major departments may be more restrictive.

5. Graduate level independent study may not be used as an avenue for allowing students to take undergraduate courses in the major department. The department may require a student to take undergraduate major courses as a means of making up deficiencies, but the student should be informed that credits generated in these courses may not be counted in the minimum number required for the degree, but are included in the cumulative GPA.

6. The student is required to complete and sign an Independent Study Agreement. The Independent Study Agreement must be approved and signed by the professor directing it, and by that professor's departmental Independent Study Coordinator. University policy states that only faculty members may sponsor Independent Study.

7. CCHE policy states that a minimum of 25 hours of work-time on the part of the student is required for each 1 semester hour of Independent Study credit.

8. Independent Study is to be enrolled for in the same timeframe as all other courses.

9. Independent Study credit will be granted upon satisfactory completion of the project requirements as defined in the Independent Study Agreement.

Restrictions

1. University rules do not normally allow Independent Study credit for internship experiences, work-study or hourly pay work done in departments, or for work also compensated by a salary.

Independent Study Policy & Guidelines (continued)

How to Enroll

The Independent Study may not be done retroactively. That is, the agreement for Independent Study is to be completed, signed, and approved by all parties prior to the initiation of the project, and no later than one week prior to the end of the registration period.

Completion of the Independent Study Agreement form does not constitute enrollment in the course.

Following the review and approval of the Independent Study Agreement by the appropriate parties, the student will be enrolled into the Independent Study course. Students are responsible for making sure registration holds and scheduling issues are resolved so enrollment in an approved Independent Study can occur successfully. Students should check MyCUInfo after 10 days of receiving the completed Independent Study Agreement signed by all parties, and if for some reason the student is still not enrolled in the course after that timeframe, the student should follow up with the Sponsoring Faculty Member's Department.

I have read and understand the Independent Study guidelines: DS AF

College of Engineering & Applied Science
UNIVERSITY OF COLORADO BOULDER

Independent Study Agreement

Name: Andrew Floyd CU Student ID #: 109943418

CU email: andrew@colorado.edu

Major: Electrical Engineering/Electrical and Computer Engineering Class standing: Senior

Cumulative GPA: 3.400 Previous number of Independent Study hours earned: 0

Sponsoring Faculty Member Full Name: Eric Wustrow

Sponsoring Faculty Member CU Email Address: ewust@colorado.edu

Year: 2023 Term: Fall

Sponsoring Faculty Member's Independent Study Course Prefix: ECEN

Sponsoring Faculty Member's Independent Study Course Number: 4840 Credit hours (1-3): 3

Description and goals of the proposed Independent Study must include:

a. A well-defined question or project must be presented in the proposed Independent Study (enter text here or attach content).

b. A statement regarding the significance of the question and/or context of the project (enter text here or attach documentation).

c. A statement of impact regarding how the information or deliverable will be utilized after the Independent Study is completed, and how the student will benefit from the experience (enter text here or attach content).

For this independent study, the student will implement the elliptic curve digital signing algorithm (ECDSA) in hardware (FPGA-based). In addition, the student will verify the performance and correctness of the implementation through a battery of simulations, unit tests, formal proofs, and other verification methods. Finally, the student will compare the performance of the hardware implementation to software implementations in terms of speed, resource and power utilization, as well as having a stretch goal of characterizing the robustness of the implementation to various side-channel attacks.

ECDSA offers a variant of the digital signing algorithm (DSA). It utilizes elliptic-curve cryptography (ECC) to provide secure, efficient signatures and signature verification. ECDSA is widely used to ensure data integrity and authentication, and it plays a critical role in digital communications and transactions. For example, ECDSA is commonly used in transport layer security (TLS), in secure shell (SSH), and even in the signing and verification of transactions for several prominent digital currency protocols. Moreover, ECDSA and cryptosystems like it are of critical importance to the security, integrity, and privacy of the digital systems that we all rely upon in the modern world.

As the student already has some exposure to cryptography, and to some of the key cryptosystems in use today (e.g. RSA, AES, ChaCha20, etc), confronting ECDSA is a natural next step in their education in this critical field. At the same time, cryptography is fraught with unique and challenging difficulties, and the number of ways to 'get it wrong' are countless. There are undoubtedly implementations of nearly every cryptosystem, existing in the wild, which contain critical vulnerabilities due solely (or in part) to their implementations. Not only will this independent study provide a safe, low-stakes environment in which to explore ECDSA, and just some of the difficulties that may arise with this cryptosystem, it will also empower the student to go out into the world and to communicate effectively about the challenges of ECDSA specifically, of cryptography generally, and about why it is often sage advice to not 'roll your own crypto.' Finally, the knowledge gained through this experience will allow the student to contribute meaningfully as a member of engineering teams implementing and verifying a wide range of computer hardware systems that make use of similar components, constructs, and calculations.

Method of conducting and evaluating the Independent Study (for example, research and reading, written reports, regular meetings and discussions, final paper or report). Indicate any specific assignments and any dates when specific elements are to be finished. Must include:

a. A complete description of methods used to investigate or evaluate the findings or test the viability of a project (enter text here or attach documentation).

b. A clearly defined mechanism for communicating the findings of the project, e.g., written report, oral presentation, demonstration, testing. Please briefly describe the content of any deliverables, e.g. product, literature review, methods, results, etc. (enter text here or attach documentation).

c. Describe how the project will be evaluated by the Sponsoring Faculty Member supervising the Independent Study. For example, describe the criteria that your professor will use to determine the grade that you earn in this project (enter text here or attach documentation)

The principal deliverable for the independent study project will be an FPGA-based implementation of the ECDSA cryptosystem. The implementation will entail the creation of several hardware modules, to include: 1) a true random number generator (TRNG), 2) a signature producing module (the "signer"), and 3) a signature verification module (the "verifier"). In addition, the student will develop firmware to allow external devices to interact with the hardware (e.g. UART or other serial interface). Meta-parameters such as the key size, elliptic curve, generator, and hash function will be decided based upon a careful review of the literature but will adhere closely to well-studied and established standards (e.g. NIST, ISO/IEC, X9, ANSI, etc). The finished product should allow a user to provide as input a key, message (or message hash), and (optionally) a signature, and it shall produce either a valid signature on the message (for a given private key) or else it shall verify that a valid signature was provided for the message by the hodler of the private key corresponding to a given public key. The computer hardware implementation shall be accompanied by a robust testbench that formally verifies the correctness of the algorithm and that further verifies the proper operation of the hardware implementation.

The project will require the student to interface with a dense literature spanning multiple knowledge domains. In particular, the student will need to grapple with the mathematical literature underpinning the ECDSA cryptosystem, along with the IEEE 1800-2017 Standard for SystemVerilog and other resources related to the formal verification of computer hardware systems (e.g first-order logic, Z3, Dafny, etc). A review of this literature will accompany a written report ("documentation") for the project, and will detail the hardware implementation, along with block diagrams, logic flowcharts, and any other information that a user of the hardware might require to enjoy full use of the product. It is anticipated that this documentation will take the form of a 5-10 page pamphlet which can be packaged with the computer hardware, testbenches, and source codes. Together, the hardware implementation, firmware, and documentation will constitute in full the student’s deliverables at the end of the project, and these materials will be evaluated by the professor to determine satisfactory completion of the independent study project.

The student and the professor will hold regular, in-person meetings to discuss the project and the student's progress. The student will also reach out to recommended faculty in the Electrical and Computer Engineering, Math/Applied Math, and Computer Science departments as recommended and/or required regarding cryptography, formal verification, or any other particular subject matter expertise.

College of Engineering & Applied Science
UNIVERSITY OF COLORADO BOULDER

Independent Study Agreement

Approvals:

Student Signature: DocuSigned by: Andrew Floyd 8CBB96D375BE4F1... Date: 9/6/2023

Faculty Member's Department: ECEN

Faculty Member Signature: DocuSigned by: Eric Mustrow 58B6F016DB754C9... Date: 9/6/2023

Additional notes from Faculty Member:

Independent Study Coordinator Signature: DocuSigned by: Mona Elhelbawy 60F504C05A2045C... Date: 9/6/2023

Additional notes from Independent Study Coordinator:

Curriculum Coordinator should enroll student in the Independent Study section associated with the sponsoring faculty member for the term and credit hours indicated. After enrolling student, Curriculum Coordinator should sign form here:

Curriculum Coordinator Signature: DocuSigned by: Dean's Office, College of Engineering 17B8863766E8403... Date: 9/7/2023

Additional notes from Curriculum Coordinator:

In lieu of ECEE Curriculum Coordinator, who is out of the office until September 20.