2026 ASEE ANNUAL CONFERENCE June 21–24, 2026 | Charlotte Convention Center, NC
Host Sponsor UNC Charlotte
Paper ID #52595

Integrating Theoretical Foundations with Practical Applications in Cryptography

Dr. Bingyu Liu, Wentworth Institute of Technology

Dr. Bingyu Liu is an assistant professor in School of Computing and Data Science at Wentworth Institute of Technology. She was a postdoctoral research fellow at the Institute for Experiential AI (EAI) in Northeastern University. She received her PhD in Computer Science from Illinois Institute of Technology in 2022. Her work focuses on research and education in security and privacy, emphasizing secure computation, applied cryptography, and differential privacy, while also exploring interdisciplinary connections such as trustworthy AI, health care and theoretical foundations.

Leonidas Deligiannidis, Wentworth Institute of Technology

Integrating Theoretical Foundations with Practical Applications in Cryptography

Abstract

Learning Cryptography for undergraduate students is an incredible challenge due to its multidisciplinary complexity, as it spans multiple fields and requires a strong foundation in advanced mathematics and computer science. Students often struggle to bridge the gap between abstract theoretical proofs and practical implementations. To address this challenge, the paper presents an innovative pedagogical framework based on sustained, project-driven learning. The curriculum integrates code-based development with research, tasking students with implementing cutting-edge privacy-preserving techniques such as Homomorphic Encryption (HE), Secure Multi-Party Computation (MPC), and Differential Privacy (DP). These technologies are applied to multiple real-world domains, including healthcare and the Internet of Things (IoT), to highlight unique security and privacy guarantees. Beyond technically oriented implementation, the framework emphasizes professional competencies through oral presentations and formal reporting. Student feedback indicates that this multifaceted approach significantly enhances engagement. The paper concludes with key insights, offering a scalable model for STEM education and better preparing students for research and industry demands.

Keywords: Cryptography, Theory, Practical implementations, STEM education

Introduction

Increasing awareness of privacy in everyday life has led to heightened concerns regarding security and privacy issues. Cryptography serves as a fundamental privacy-preserving techniques in Cybersecurity by mitigating such risks and limiting the information an adversary can obtain under different threat models. It integrates advanced concepts from mathematics and computer science, requiring students to have a solid foundation in algebra, number theory, and algorithms. Many undergraduates struggle to bridge the gap between theory and practical implementations, such as cryptographic schemes, key generation, and protocols design. Moreover, with the rapid development of the field and the constant emergence of new algorithms and security techniques, it is important to keep content up to date at all times. Students with limited backgrounds in security proofs and formal reasoning have difficulty understanding complex cryptographic concepts. In most undergraduate educations, significant emphasis is placed on practical, hands-on experience, while theoretical foundations receive less attention. This imbalance creates potential barriers for learners, who may struggle to integrate theoretical knowledge with practical application. Effective instruction in Cryptography therefore demands a balance between mathematical rigor

and practical implementation, ensuring that students understand both how cryptographic systems function and why they are secure. Meanwhile, in the real world, modern Cryptography continues to develop advanced algorithms, secure protocols, and integrated system implementations that enable secure end-to-end data processing across a wide range of domains. To enhance understanding of the content, learners should be introduced to key algorithms and protocols step by step, while optional readings at different levels support deeper exploration. These challenges make Cryptography particularly demanding and call for innovative teaching methods that combine interactive problem-solving with real-world scenario. This paper presents a pedagogical framework designed to bridge the gap between theory and practice through project-based learning. The approach centers on a long-term project that combines code-based and survey-based components, enabling students to engage with Cryptography from multiple perspectives. Students are encouraged to implement algorithms, reinforcing theoretical knowledge through hands-on assignments. The projects integrate several cutting-edge cryptographic techniques, such as Homomorphic Encryption (HE)[1], Secure Multi-Party Computation (MPC)[2], and Differential Privacy (DP)[3], and apply them across domains including healthcare, smart grids, and the Internet of Things (IoT). By tackling real-world data privacy challenges, students are exposed to the unique security and privacy constraints inherent to different application areas and are encouraged to explore multiple cryptographic strategies to address these challenges. To further enhance professional development, students are also expected to prepare oral presentations and academic written reports as part of the term project outcomes. These activities reinforce conceptual understanding while building essential professional skills such as technical communication, synthesis of complex information, and academic writing, competencies critical to both research and industry contexts. Student feedback from the Applied Cryptography course demonstrates the effectiveness of this term project-based approach in enhancing learning outcomes and engagement. The paper concludes by contributing valuable insights to the broader STEM education[4] and Wentworth community.

Contributions In this paper, we present a pedagogical framework grounded in active learning and problem-based learning (PBL) to address the disconnect between theoretical foundations and practical applications in Cryptography. Central to this framework is a longitudinal, project-based structure that integrates both implementation-oriented (code-based) and analytical (survey-based) components, thereby enabling students to engage with cryptographic concepts from multiple perspectives. Specifically, we design a sequence of tasks that promote "input"-oriented learning, through which students acquire foundational knowledge and develop hands-on competencies, alongside "output"-oriented activities that serve evaluative purposes by requiring students to demonstrate their understanding through applied work. The term project further encourages self-directed learning and fosters the development of critical thinking and analytical skills[5]. Moreover, the project not only equips students with the ability to read scholarly literature, but also provides structured, step-by-step guidance to support the development of independent critical analysis and problem-solving skills. Throughout the process, students develop a range of professional competencies, including skills essential for interdisciplinary problem solving.

Theoretical Framework

This section outlines the structure and design of Cryptography course, including the class lecture and the term project. We further elaborate on the underlying rationale for the course design and its implementation.

Active Learning Compared with traditional passive learning, it greatly improves students' engagement by involving them actively in their learning through multiple structured tasks[6]. With an active-learning approach, instructors can apply proven strategies for engaging students and emphasizing key concepts used in class activities. In this work, we design multiple strategies grounded in an active learning framework to encourage students to engage deeply in the learning process through critical thinking, discussion, and collaboration, while also requiring them to master fundamental theoretical concepts.

- *Case Study:* Use a case study or running example to highlight the motivation and problem setting. For instance, introduce real-world senior such as "Any security and privacy issues in the real world?", "Why do we need Cryptography?" to show practical relevance. Present problems or questions that challenge and engage students, prompting them to apply theoretical concepts to authentic scenarios.
- *Reading materials:* Assigning reading materials is essential for theoretically rigorous disciplines like Cryptography, where strong theoretical grounding is required. Without exposure to the underlying mathematical foundations, security assumptions, and formal definitions, students may produce implementations based solely on coding skills, resulting in systems that are fundamentally insecure due to misunderstandings of key concepts such as threat models, randomness, or adversarial capabilities. Lacking this theoretical building block knowledge prevents students from fully understanding and applying the schemes.

  For example: Kerckhoff's Principle[7], Perfect Secrecy[8]

  Additionally, other type of reading could be international standards, historical background, and real-world applications, which help prepare students to communicate effectively in professional environments where precise documentation and accurate interpretation of specifications are essential. Such "input" knowledge gained through reading constitutes a critical component of fundamental Cryptography education. Students benefit substantially from these activities, particularly if they pursue advanced study or continue working in the security and privacy.
- *In-class Exercise:* In-class activities are designed to be active rather than passive. It incorporate strategies that help transform "input" knowledge into "output" knowledge. The questions used during class are open-book and open-note and are not intended for assessment. Instead, students are encouraged to review course resources (such as textbooks and online materials), engage actively, and verify their answers independently. Collaboration and discussion with peers is welcomed, allowing students to test their understanding and receive immediate feedback. Effective exercises strike a balance between being too easy and too difficult, presenting enough challenge to build problem-solving skills without causing frustration. Clear instructions, reasonable time limits, and opportunities for feedback, reflection, or discussion are essential to maintaining

student engagement and focus.

For example:

- *Q1: Based on Fermat's Little Theorem, how to compute* $3^{31} \bmod 7$?
- *Q2: Compute gcd(165,285)?*
- *Q3: RSA encryption, given p=5, q =7, then how to compute Encryption and Decryption?*

Problem-Based Learning (PBL) It enables students to collaborate in solving open problems. With thoughtful design and clear instructions, students initiate the term project by brainstorming with their teammates on given broad topics. Meanwhile researching, and practicing information literacy as they explore ways to connect course content to real-world examples. With timely feedback, students can follow guidance effectively and stay on track in the phases. Given the limited time, students also learn how to report their progress and plan the next steps. During the collaborative work, they develop project management skills as well as self-awareness and evaluation of group processes. Each student takes responsibility for working independently and engaging in self-directed learning, while critical thinking and analysis are embedded throughout the process. In Phase III, as the project concludes, students deliver presentations and written reports, allowing them to practice both oral and written communication skills. Feedback is delivered in a timely and concise manner, encompassing project progress monitoring, guidance for advancing the work, and support for the development of students' academic writing and presentation skills.

Class Design Overview

This section provides an overview of the topics covered in the Applied Cryptography course. Designed for undergraduate students, the course introduces the fundamental theory and practical applications of cryptographic techniques used in modern information security systems. Cryptography provides important tools for ensuring the privacy, authenticity, confidentiality, an integrity of data involved in modern information systems, and frames the approach used in this course. This course examines the progress from historical symmetric encryption standards and protocols to the modern public key encryption processes. Basic concepts of ciphers, blocks, hashes, MACs are discussed. Different implementation approaches are presented along with their performance impacts, along with potential attach strategies and their efficacy are discussed.

The content taught in the class is divided into a total of ten topics, covering topics ranging from an overview of security and privacy to advanced subjects (e.g., cutting-edge techniques). During each topic, students are assigned and expected to complete homework related to the material covered. In addition to the assigned homework, a set of curated laboratory exercises provides students with practical experience working with classical Cryptography algorithms in real time *(Note that the homework design is credited to Dr. Leonidas Deligiannidis, the second author of this paper)*. A term project is also assigned, in which students devise their own idea related to the course content and implement it using the Cryptography resources available to them throughout the term. Students are periodically assessed on the knowledge gained and the material covered during the course.

Course Topics:

- Topic 1 - Introduction to Cybersecuirty: Background and Overview
  (i.e., Cryptographic security notions, Security definitions, Attacks security notions)
- Topic 2 - Classical Cryptography *(i.e., Caesar Cipher, Vigenère Cipher*)
- Topic 3 - Symmetric Cryptography *(i.e., Block ciphers, Stream ciphers)*
- Topic 4 - Number theory
- Topic 5 - Public Key Cryptography
  (i.e., Diffie-Hellman key exchange, discrete log security, RSA encryption)
- Topic 6 - Cryptographic Hash Functions
- Topic 7 - Message Authentication
- Topic 8 - Digital Signatures
- Topic 9 - Advanced Topics I: Privacy-preserving state-of-the-art (SOTA) techniques, i.e., *Zero Knowledge Proofs, Homomorphic Encryption (HE), Secure Multi-Party Computation (MPC), and Differential Privacy (DP)*
- Topic 10 - Advanced Topics II: Privacy Preserving on Machine Learning.

Theoretical Framework

When considering how to improve the efficiency of students' learning of foundational inputs, it is equally important to determine the most effective methods for evaluating their corresponding outputs. Research indicates that students acquire knowledge more effectively through active engagement with their learning environment. Rather than passively receiving theories and algorithms in Cryptography, students are expected to actively utilize and review the material, applying prior knowledge and reorganizing their internal knowledge base.

The input-focused learning process helps shape critical thinking skills and encourages students to apply what they have learned to problem-solving tasks. This approach supports the development of knowledge reorganization and integration abilities, reinforcing deeper understanding and long-term retention. Within an active learning framework, students are assigned multiple tasks such as in-class exercises and group discussions. In addition, hands-on activities, rather than traditional lecture-based instruction and note-taking, it can significantly enhance learning by encouraging students to focus on problem solving using the knowledge they acquire. This process inherently supports knowledge reorganization and integration.

In our active learning approach, a term project with clear instructions guides students step-by-step through Phase I (Initialization) to Phase II and Phase III. We value student engagement and have observed that certain activities, such as discussions or basic in-class tasks, may not fully motivate

students. In contrast, the term project enables students to learn by doing: they demonstrate stronger problem-solving abilities and acquire knowledge more efficiently than through passive absorption alone. The purpose of the term project is to motivate students by allowing them to construct new understanding from their existing background knowledge. With no restrictions on project topics, students are encouraged to engage actively, driven by their own interests and curiosity. This approach promotes deeper learning and supports long-term knowledge application. Through the process of transforming "inputs" into "outputs," students actively apply in-class learning techniques and integrate these concepts into their term projects. This form of training is critically important and contributes to students' personal development, as they learn how to translate foundational inputs into meaningful solutions for real problem settings. Finally, this shift from passive learning to active application supports students' long-term growth and prepares them for future career pathways.

Term Projects

In this subsection, we examine the various aspects of the term project **design strategies**, including expected outcomes for presentations and written reports, as well as the structure of its multiple phases. It is important to note that the primary motivation behind the design is to enable students to fully explore their potential, develop critical thinking skills, and engage in step-by-step problem solving. Extra Credits would be used for encouraging, which is based on the complexity and quality of your project. Providing positive feedback can serve as a source of encouragement and motivation for students. Projects may be completed in groups of 2–3 students or individually, which encourages collaborative discussion.

Motivation The goal of this project is to encourage students to implement a cryptographic or cryptanalytic algorithm. Although students may find the list of topics and project phases somewhat daunting initially, students will also find that the stepwise approach makes project execution and completion much easier. Students' full range of skills (e.g., library research, theory development, software design and development, programming and testing, analysis, and reporting) will be enhanced by this exercise. More importantly, students will acquire an in-depth knowledge of at least one topic or topical area in cryptology, as well as an overview of the cryptologic literature.

Option I: Choose topics aligned with one's own interests. Students may submit a project proposal on any topic of students' choice. However, if students choose their own topic, it must demonstrate sufficient complexity and quality. The proposal should also align with the subject matter of this course.

Proposals Students are supposed to complete and submit a proposal beforehand. Once students have chosen a project topic, they are expected to submit proposals on Brightspace. The submission should include the project title and a brief (one-paragraph) description of the topic with references.

Option II: Survey This involves surveying a series of research papers on a particular topic. Read 4–5 papers on the subject, then write a short report summarizing the most interesting conceptual and technical content from those papers. Students do not need to cover every detail for this task,

but report should address the problem setting/motivation, main contributions/techniques, and experimental results presented in the papers.

For the survey work evaluation, students are expected to make a thoughtful effort to ensure that their reports are polished and well presented. Reports do not need to provide a comprehensive survey of the entire topic area selected. Instead, the sections included should be carefully considered, clearly presented and organized, conceptually cohesive, and easy to read.

Milestone (A reference sample)

- **Phase I – Proposal (Due: 06/16/25)**
  Each group will prepare a brief proposal document that outlines chosen topic, group members and their roles, technical approach, anticipated challenges and possible solutions, as well as preliminary references you plan to use. The purpose of this document is to encourage high-level thinking about your project.
- **Phase II – Design (Due: 06/23/25)**
  Submit a 2–3 page summary that includes:
  - a literature review
  - the basic theory you plan to use
  - a high-level software design (e.g., a block diagram)
  - expected challenges and your plans to address them, and
  - anticipated results.

  The goal is to clarify the design and begin thinking critically about potential obstacles.
- **Phase III - Implementation (Due: 07/21/25)**
  Preliminary Code and Results: Students will prepare and submit the GitHub links. This phase of project will help establish the validity of technique. It will also provide a working foundation from which to construct final report.
- **Final Submission - Reports and Presentation**
  Submit Github and Report: Students will prepare and submit a written report of project, including the following sections: Background, Previous Work, Theory, Design, Implementation, Results, Discussion (including an analysis of successes and failures), Conclusions (including suggestions for future work), and References.

Discussion and Future Directions

Many positive comments were received from students by the end of the semester. Our multi-strategy approach led to a notable increase in student engagement and significantly narrowed the gap between theory and practice. The outcomes further demonstrate that essential concepts in modern Cryptography, especially those relevant to real-world applications such as encryption, message authentication, and digital signatures, which were effectively understood. Additionally, structured feedback during the term project mitigated difficulties in selecting suitable team topics, particularly for students with limited prior background.

Meanwhile, Cryptography plays an important role in ensuring security and privacy in the real world. With the rapid development of AI, deep neural network (DNN) services have been widely deployed to provide efficient and accurate inferences across many domains. In practice, clients

may send private data (e.g., images, text, or videos) to cloud-based services to obtain inferences from proprietary DNN models, which raises significant privacy and security concerns. Cryptographic inference systems have been proposed to address these issues. For a Cryptography course, security and privacy in AI can be introduced as a relevant and timely extension. Learners should not only receive foundational knowledge, but also understand how to apply it to real-world problems. Staying informed about cutting-edge techniques is especially meaningful, as it equips students with the problem-solving skills needed for future developments.

Conclusion

In our work, we designed multiple pedagogical strategies based on active learning and problem-based learning to bridge the gap between cryptographic theory and practice. The core of our approach is a long-term, project-based framework that integrates both code-based and survey-based components, enabling students to engage with Cryptography from multiple perspectives, including theoretical foundations and practical applications. In particular, we developed and assigned tasks that support "input" learning, where students acquire foundational concepts and hands-on skills while "output" tasks provide opportunities for evaluation, allowing students to demonstrate understanding through applied activities. According to student feedback, this method greatly improved engagement and comprehension, effectively narrowing the divide between theory and practice. The course integrates instruction on core cryptographic primitives with extensive hands-on tasks. Furthermore, the success of the course highlights the need for adaptive educational frameworks that align with ongoing technological advancements and security requirements. Future work will continue to improve pedagogical strategies through the integration of AI techniques within real-world applications.

References

[1] Zvika Brakerski, Craig Gentry, and Vinod Vaikuntanathan. (leveled) fully homomorphic encryption without bootstrapping. In *Innovations in Theoretical Computer Science Conference*, pages 309–325, 2012.

[2] Andrew C. Yao. Protocols for secure computations. In *23rd IEEE Symposium on Foundations of Computer Science*, pages 160–164. IEEE, 1982.

[3] Cynthia Dwork. Differential privacy. In *Encyclopedia of Cryptography, Security and Privacy*, pages 649–652. Springer, 2025.

[4] Dina Zohrabi Alaee and Benjamin M Zwickl. A case study approach to understanding a remote undergraduate research program. In *Physics Education Research Conference 2021*, 2021.

[5] Chuanlei Zhang and Samar Swaid. Undergraduate research experience for stem students: Efforts and outcomes. *Contemporary Issues in Education Research*, 10(4):213–218, 2017.

[6] Michael J Prince and Richard M Felder. Inductive teaching and learning methods: Definitions, comparisons, and research bases. *Journal of engineering education*, 95(2):123–138, 2006.

[7] Kerckhoffs Auguste. La cryptographie militaire. *Journal des sciences militaires*, 5:161–191, 1883.

[8] Claude E Shannon. Communication theory of secrecy systems. *The Bell system technical journal*, 28(4): 656–715, 1949.