Introduction to Galois Fields: Exploring AES Fields and Finite Field Arithmetic

WOMANIUM GLOBAL ONLINE QUANTUM MEDIA PROJECT #Quantum30
Challenge Day 5

Listen

Introduction:

Galois Fields, also known as finite fields, are essential mathematical structures used in various applications, including cryptography. In this article, we will delve into the fascinating world of Galois Fields, exploring their relevance in *AES (Advanced Encryption Standard)* — one of the most widely used block ciphers. We will begin by discussing block ciphers, and their classification into *DES (Data Encryption Standard)*, and AES. Then, we will focus on AES, its merits, demerits, and its drawbacks related to finite fields. Afterward, we will explore the fundamentals of Galois Fields, starting with algebraic structures such as **groups, rings, and fields**. Eventually, we will delve into finite fields, specifically AES Fields ($G(2^8)$), and examine **prime fields and extension fields**, their arithmetic operations, and how they relate to AES.

. . .

Block Ciphers, DES, and AES:

Block ciphers are cryptographic algorithms that operate on fixed-size blocks of data. Two popular block ciphers are DES and AES. DES, which was widely used in the past, is now considered insecure due to its small key size. AES, on the other hand, is a modern and secure block cipher that has replaced DES as the standard encryption algorithm in various applications.

A bride intro to AES:

AES (Advanced Encryption Standard) is a fundamental cryptographic algorithm that plays a pivotal role in modern technology. As technology rapidly advances and our lives become increasingly connected, the need for secure data transmission and storage becomes paramount. We will discuss AES in detail tomorrow. AES has

numerous advantages, making it the preferred choice for secure communication. Its key strengths include strong security, simplicity of implementation, and efficient performance on modern computing platforms. AES supports key sizes of 128, 192, and 256 bits, making it adaptable to different security requirements. However, its main drawback is the need for key management, as AES encryption and decryption require a secure and efficient key exchange mechanism.

AES and Finite Fields:

AES operations heavily rely on finite fields, which are algebraic structures with a finite number of elements. In AES, Galois Fields are particularly significant, with $G(2^8)$ being used extensively. To better understand Galois Fields, let's first explore the fundamental algebraic structures of groups, rings, and fields.

. . .

Algebraic Structures: Groups, Rings, and Fields

- *Groups:* A group is a set of elements with an operation that satisfies four properties: closure, associativity, identity element, and invertibility. In AES Fields, the set of elements is finite, and the operation is typically addition.
- *Rings:* A ring is a set with two operations: addition and multiplication. It satisfies properties like closure, associativity, commutativity of addition, and distributive property of multiplication over addition.
- *Fields:* A field is a ring with an additional property: every nonzero element has a multiplicative inverse. In AES Fields, the set of elements is finite, and the operations are addition and multiplication.

Finite Fields:

Finite Fields, also known as Galois Fields, are algebraic structures with a finite number of elements. They find applications in various fields, including mathematics, computer science, and cryptography. Finite Fields are characterized by their size, which is a prime power (p^n), where 'p' is a prime number and 'n' is a positive integer.

Finite Fields in AES:

AES Fields ($G(2^8)$) are finite fields of size 2^8, which means there are 2^8 elements in this field. These fields are constructed as extension fields over a prime field of size 2 (GF(2)). Finite fields are categorized into prime fields and extension fields.

- *Prime Fields:* Prime fields, denoted as GF(p), have a prime number p as their size. In AES, the prime field GF(2) is the base field.
- *Extension Fields:* Extension fields, denoted as GF(p^n), are constructed by adding an nth-degree irreducible polynomial over a prime field GF(p). AES Fields ($G(2^8)$) is an extension field, constructed by adding a degree 8 irreducible polynomial over GF(2).

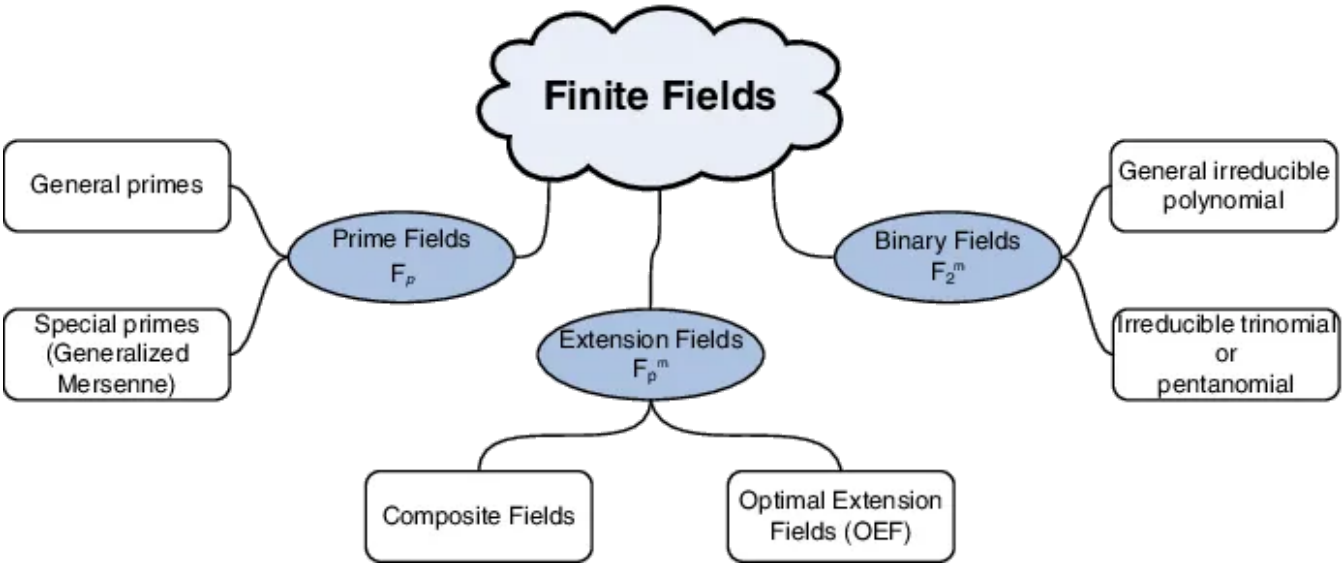


Image Source: Internet

Arithmetic Operations in Prime Fields:

In prime fields, arithmetic operations are straightforward. Addition and subtraction are performed bitwise XOR, which is identical to the operation used in stream ciphers.

Inversion in Prime Fields:

To compute the multiplicative inverse of an element in a prime field GF(p), the Extended Euclidean Algorithm is used. This algorithm finds the greatest common divisor (GCD) of two elements and computes coefficients that satisfy a linear Diophantine equation, resulting in the inverse.

Arithmetic Operations in Extension Fields:

In extension fields, arithmetic operations are performed similarly to prime fields. Addition and subtraction are carried out bitwise XOR, while multiplication is done using polynomial multiplication and modular reduction concerning the irreducible polynomial.

Multiplication in Extension Fields:

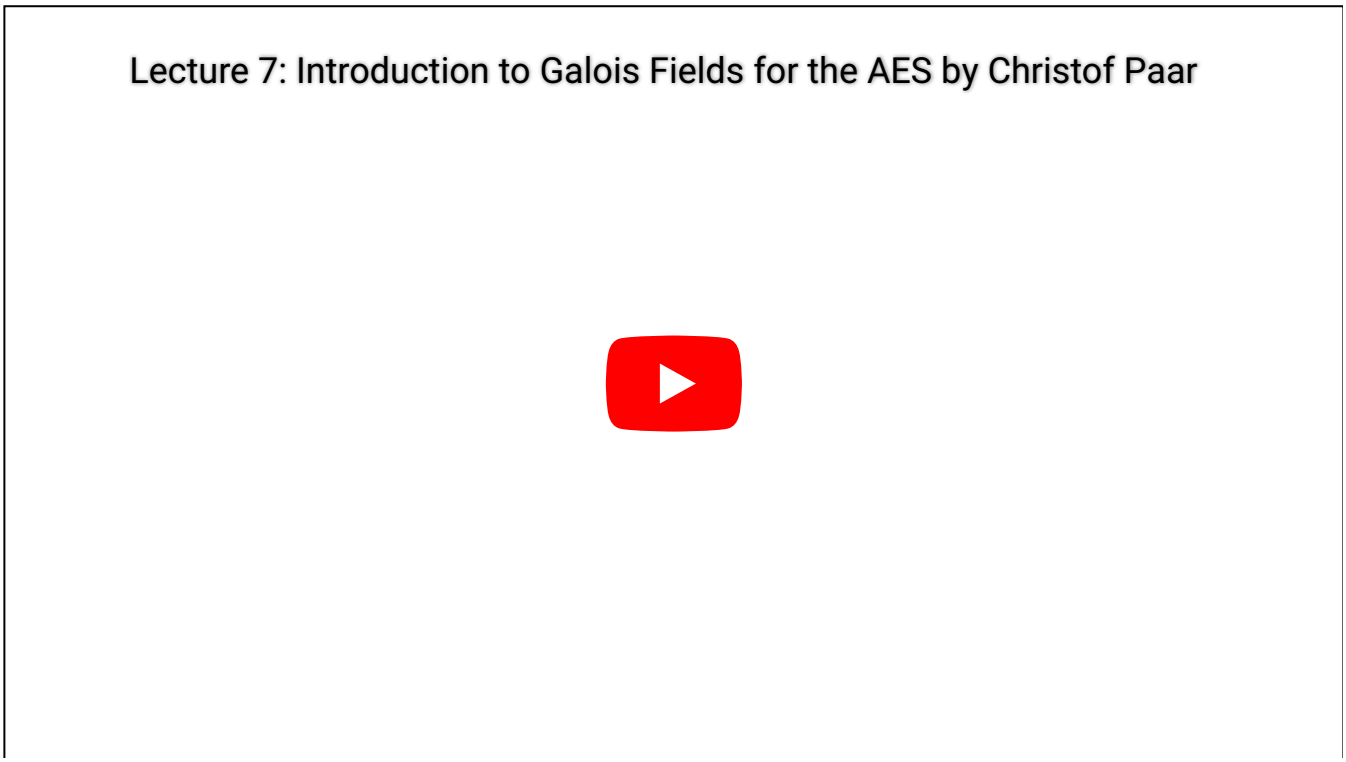
Multiplication in extension fields involves polynomial multiplication, where the product is computed modulo the irreducible polynomial to keep the result within the field's boundaries.

Conclusion:

Galois Fields, particularly AES Fields ($G(2^8)$), play a crucial role in the design and implementation of the AES block cipher. Finite field arithmetic enables secure encryption and decryption processes while taking advantage of the unique properties of these algebraic structures. Understanding Galois Fields is essential for comprehending modern encryption schemes like AES and is crucial in the field of cryptography and data security.

. . .

This article is written based on the below video lecture.



The video is provided by QuantumComputingIndia, as a part of the #Quantum30 learning challenge.

For the sake of simplicity, I try not to include all the mathematical derivation and concepts. Otherwise, this article will be long and might be boring also and other

problems like ‘Latex’ rendering. This article is written for general purposes and an overview of this field.

However, Interested people find those concepts in the video lecture if they want to deep dive into this field.

I have been exploring Cryptography since the start of this month and throughout this month I will gain in-depth knowledge of this field. Your suggestion will be really helpful for my future endeavor.

This is a part of **WOMANIUM GLOBAL ONLINE QUANTUM MEDIA PROJECT**. This project will help me to dive into the cryptographic world(From Classical to Quantum Approach). From onwards I shall share my learning log with others who are curious about this particular and promising field.

I want to take a moment to express my gratitude to **Marlou Slot** and **Dr. Manjula Gandhi** for this initiative and encouragement and sincere thanks to **Moses Sam Paul Johnraj** for providing the 30-day schedule.

#Quantum30 #QuantumComputing #QuantumJourney #QuantumEnthusiast #Womanium #Cryptography #QuantumCryptography #QuantumComputingIndia

Written by Murshed SK

Physics Undergrad | Quantum Information Science and Computation Enthusiast | Passionate about Quantum Machine Learning | <Womanium | Quantum> Scholar