Elliptic Curves Modular Forms And Cryptography

#elliptic curves #modular forms #cryptography #elliptic curve cryptography #public key cryptography

Explore the fascinating intersection of elliptic curves, modular forms, and their vital role in modern cryptography. This deep dive covers how these advanced mathematical concepts underpin secure digital communication, including the principles behind elliptic curve cryptography and other robust public key cryptography systems, crucial for safeguarding data in today's interconnected world.

Elliptic Curves Modular Forms And Cryptography

Elliptic Curves and Modular Forms | The Proof of Fermat's Last Theorem - Elliptic Curves and Modular Forms | The Proof of Fermat's Last Theorem by Aleph 0 248,207 views 3 years ago 10 minutes, 14 seconds - Elliptic curves,, **modular forms**,, and the Taniyama-Shimura Conjecture: the three ingredients to Andrew Wiles' proof of Fermat's ...
Intro
Elliptic Curves
Modular Forms
Taniyama Shimura Conjecture
Fermat's Last Theorem
Questions for you!
Elliptic Curves - Computerphile - Elliptic Curves - Computerphile by Computerphile 523,956 views 6 years ago 8 minutes, 42 seconds - Just what are **elliptic curves**, and why use a graph shape in **cryptography**,? Dr Mike Pound explains. Mike's myriad Diffie-Hellman ...
Elliptic Curve
The Formula for an Elliptic Curve
Example of an Electric Curve
Elliptic Curve Discrete Logarithm Problem
What Curves Are Safe To Use
Elliptic Curve Cryptography Overview - Elliptic Curve Cryptography Overview by F5 DevCentral 446,087 views 8 years ago 11 minutes, 29 seconds - John Wagnon discusses the basics and benefits of **Elliptic Curve Cryptography**, (ECC) in this episode of Lightboard Lessons.
Elliptic Curve Cryptography
Public Key Cryptosystem
Trapdoor Function
Example of Elliptic Curve Cryptography

Private Key
Elliptic curves and modular forms - Elliptic curves and modular forms by mlbaker 29,501 views 8 years ago 41 minutes - Help me keep making videos: http://paypal.me/mlbakermath.
Elliptic curves - Elliptic curves by Imperial College London 128,722 views 9 years ago 58 minutes - Explore the history of counting points on **elliptic curves**,, from ancient Greece to present day. Inaugural lecture of Professor Toby ...
Pythagoras Theorem
The Congruent Number Problem
Draw the Graph of the Solutions
Why Is It a Circle
Drawing a Line through a Circle
Quadratic Formula
Fermat's Last Theorem
Example of an Elliptic Curve
Prime Numbers
The Langlands Program
When an Elliptic Curve met a Modular form - A short tale on Reciprocity Laws - When an Elliptic Curve met a Modular form - A short tale on Reciprocity Laws by Prakhar Pratyush 3,006 views 1 year ago 1 minute, 7 seconds - Reciprocity laws constitute a very general theme in modern number theory where we try to relate one kind of object to a very ...
The bridge between number theory and complex analysis - The bridge between number theory and complex analysis by Aleph 0 177,184 views 1 year ago 9 minutes, 59 seconds - (d) STRATEGY OF WILES' PROOF (how to go from **elliptic curves**, to **modular forms**,) The book "**Elliptic Curves**,, **Modular Forms**,, ...
July 5th: Introduction to modular forms and elliptic curves by Kenny Li - July 5th: Introduction to modular forms and elliptic curves by Kenny Li by Parker Glynn-Adey 2,085 views 8 months ago 56 minutes - Abstract: Abstract: A special case modularity theorem which connects **modular forms**, and **elliptic curves**, was used to prove ...
Intro
Definition of Curve
Projective space
Projective curve
Smooth curve
Elliptic function
Elliptic curve and torus
Function of lattice
Classification of elliptic curve
Moduli space
Modular form
Elliptic curve and congruent number
L functions in number theory
L function of elliptic curve
Modular elliptic curve
Significance of modularity theorem
Summary
Elliptic Curve Cryptography Tutorial - Understanding ECC through the Diffie-Hellman Key Exchange - Elliptic Curve Cryptography Tutorial - Understanding ECC through the Diffie-Hellman Key Exchange by Fullstack Academy 96,802 views 6 years ago 11 minutes, 34 seconds - Elliptic Curve Cryptography, (ECC) is a type of public key **cryptography**, that relies on the math of both **elliptic curves**, as well as ...
Intro
What is Encryption
How do you get shared keys
Multiplication and Exponents
The Problem
The Modulus Operator
Discrete Log Problem
Shared Edges
Algorithms

Elliptic curve properties
Order independence
DiffieHellman procedure
Modulus
Finite Field
Takeaway
Downsides
The math behind Fermat's Last Theorem | Modular Forms - The math behind Fermat's Last Theorem | Modular Forms by MathKiwi 36,820 views 11 months ago 14 minutes, 37 seconds - The fascinating piece of math hidden behind the proof of Fermat's last Theorem for most people. Excellent in-depth video series ...
Introduction
Lattices
Modular Forms
The Modular Group
Fourier Series
How many are there
Outro
Elliptic Curve Digital Signature Algorithm - Elliptic Curve Digital Signature Algorithm by Trustica 26,582 views 5 years ago 5 minutes, 22 seconds - Video explaining the **Elliptic Curve**, Digital Signature Algorithm in the article ...
calculates the other half of the signature by using modular arithmetic
calculating the value w from the signature number s
verify the signature
Frank Calegari: 30 years of modularity: number theory since the proof of Fermat's Last Theorem - Frank Calegari: 30 years of modularity: number theory since the proof of Fermat's Last Theorem by International Mathematical Union 17,082 views 1 year ago 43 minutes - When g is equal to one we're exactly considering the case of **elliptic curves**, of a queue hence the full hassave conjecture in this ...
Intro to Digital Signatures | ECDSA Explained - Intro to Digital Signatures | ECDSA Explained by Caleb Curry 33,344 views 4 years ago 7 minutes, 30 seconds - ~~~~~~~~~~~~~~~ CONNECT ~~~~~~~~~~~~~~~ Newsletter - https://calcur.tech/newsletter Instagram ...
Proving Fermat' s Last Theorem (almost) in just 2 minutes ! - Proving Fermat' s Last Theorem (almost) in just 2 minutes ! by MetaMaths 88,588 views 2 years ago 2 minutes - Andrew Wiles spent almost a decade proving a theorem nobody else could do before him. If you add a small extra condition to the ...
Secret Key Exchange (Diffie-Hellman) - Computerphile - Secret Key Exchange (Diffie-Hellman) - Computerphile by Computerphile 918,122 views 6 years ago 8 minutes, 40 seconds - How do we exchange a secret key in the clear? Spoiler: We don't - Dr Mike Pound shows us exactly what happens. Mathematics ...
Diffie-Hellman
Diffie-Hellman Key Exchanges
Color Mixing
Calculate a Private Key
Combine the Private Key with the Generator
Color Analogy
Elliptic Curve Cryptography |Encryption and Decryption |ECC in Cryptography & Security - Elliptic Curve Cryptography |Encryption and Decryption |ECC in Cryptography & Security by Lectures by Shreedarshan K 22,076 views 3 years ago 19 minutes - ECC - **Encryption**, and Decryption ECC in #**Cryptography**, & Security #EllipticCurveCryptography #ECC #Security ...
Introduction
Elliptical Curve Cryptography
Encryption Decryption
ECDH (Elliptic Curve Diffie Hellman) with X25519 - ECDH (Elliptic Curve Diffie Hellman) with X25519 by Bill Buchanan OBE 6,590 views 3 years ago 19 minutes - Excuse me for sometimes not saying the full wording for "2" ,"5", "5", "1", "9".
AES Explained (Advanced Encryption Standard) - Computerphile - AES Explained (Advanced Encryption Standard) - Computerphile by Computerphile 1,204,081 views 4 years ago 14 minutes, 14 seconds - Advanced **Encryption**, Standard - Dr Mike Pound explains this ubiquitous **encryption**,

technique. n.b in the matrix multiplication ...
128-Bit Symmetric Block Cipher
Mix Columns
Test Vectors
Galois Fields
Fermat's Last Theorem - Numberphile - Fermat's Last Theorem - Numberphile by Numberphile 2,314,657 views 10 years ago 9 minutes, 31 seconds - Videos by Brady Haran Patreon: http://www.patreon.com/numberphile Brady's videos subreddit: ...
Intro
Fermats Last Theorem
Secret Proof
Math Behind Bitcoin and Elliptic Curve Cryptography (Explained Simply) - Math Behind Bitcoin and Elliptic Curve Cryptography (Explained Simply) by Aimstone 71,457 views 5 years ago 11 minutes, 13 seconds - Elliptic curve cryptography, is the backbone behind bitcoin technology and other **crypto**, currencies, especially when it comes to to ...
Hey, what is up guys?
Introduction
1 private key
Public-key cryptography
Elliptic curve cryptography
Point addition
XP x is a random 256-bit integer
Private and Public keys
What is... an elliptic curve? - What is... an elliptic curve? by Alvaro Lozano-Robledo 42,411 views 3 years ago 53 minutes - In this talk, we will define **elliptic curves**, and, more importantly, we will try to motivate why they are central to modern number ...
What Is an Elliptic Curve
Why Elliptic Curves
What Is an Elliptic Curve and Why Do We Care
Pythagorean Triples
The Curved Curve
The Definition of an Elliptic Curve
Example of an Elliptic Curve
Abc Conjecture
The Congruent Number Problem
Definition of Elliptic Curve
An Equation of an Elliptic Curve
Addition of Points
Addition on Elliptic Curves
Doubling of Points
Examples of Elliptic Curves
Arc Conjecture
Major's Theorem
The Rank of the Elliptic Curve
Elliptic Curves with a High Rank
Natural Luts Theorem
Is Rank Computable
The Descent Method
The Most Difficult Math Problem You've Never Heard Of - Birch and Swinnerton-Dyer Conjecture - The Most Difficult Math Problem You've Never Heard Of - Birch and Swinnerton-Dyer Conjecture by Kinertia 152,168 views 3 years ago 20 minutes - The Birch and Swinnerton-Dyer Conjecture is a millennium prize problem, one of the famed seven placed by the Clay ...
Introduction to Elliptic Curves
Intro
What is Number Theory?
Types of Diophantine Equations
Solutions to Elliptic Curves
Clock Arithmetic
Analyzing Solutions using Modular Arithmetic

The Conjecture
What's been done?
Conclusion
Elliptic Curve Back Door - Computerphile - Elliptic Curve Back Door - Computerphile by Computerphile 501,698 views 6 years ago 12 minutes, 24 seconds - The back door that may not be a back door... The suspicion about Dual_EC_DRBG - The Dual **Elliptic Curve**, Deterministic ...
Intro
Cryptographic Random Number Generators
Random Number Generators
Dual EC
Backdoor
Curves which make Bitcoin possible. - Curves which make Bitcoin possible. by MetaMaths 9,531 views 2 years ago 7 minutes, 45 seconds - Elliptic curves, are exciting- they have beautiful mathematical properties which found very wide applications in **cryptography**,.
Intro
Adding a point to itself
Cryptography
Curves over finite fields
Bitcoin !
John Tate: The arithmetic of elliptic curves - John Tate: The arithmetic of elliptic curves by The Abel Prize 11,933 views 4 years ago 42 minutes - This lecture was held by Abel Laureate John Torrence Tate at The University of Oslo, May 26, 2010 and was part of the Abel Prize ...
Intro
What is anelliptic curve
Example
Moredell theorem
The torsion subgroup
The finite subgroup
The L function
The last theorem
Recent results
Elliptic Curve Cryptography - Session 1 - Cyber Security CSE4003 - Elliptic Curve Cryptography - Session 1 - Cyber Security CSE4003 by Satish C J 18,952 views 2 years ago 41 minutes - In this session we will learn 1. What are **Elliptic Curves**, 2. Types of **Elliptic Curves**, 3. How to construct an **Elliptic Curve**, over a ...
Elliptic Curves: Good books to get started - Elliptic Curves: Good books to get started by Daniel Rubin 13,103 views 2 years ago 32 minutes - A few books for getting started in the subject of **Elliptic Curves**,, each with a different perspective. I give detailed overviews and my ...
Intro
McKean and Moll, Elliptic Curves: Function Theory, Geometry, Arithmetic
Silverman, The Arithmetic of Elliptic Curves
Silverman and Tate, Rational Points on Elliptic Curves
Washington, **Elliptic Curves**,: Number Theory and ...
Knapp, Elliptic Curves
Iwaniec and Kowlaski, Analytic Number Theory
Martijn Grooten - Elliptic Curve Cryptography for those who are afraid of maths - Martijn Grooten - Elliptic Curve Cryptography for those who are afraid of maths by Security BSides London 48,654 views 8 years ago 28 minutes - Elliptic Curve Cryptography, (ECC) is hot. Far better scalable than traditional **encryption**,, more and more data and networks are ...
Intro
Disclaimer
Elliptic curves
Multiplication is very fast
"Division" is very slow
ECDH (Elliptic Curve Diffie Hellman)
Wireshark (client to server)
Wireshark (server to client)
What could possibly go wrong?
Random number generators using ECC

Conclusion
Search filters
Keyboard shortcuts
Playback
General
Subtitles and closed captions
Spherical videos