



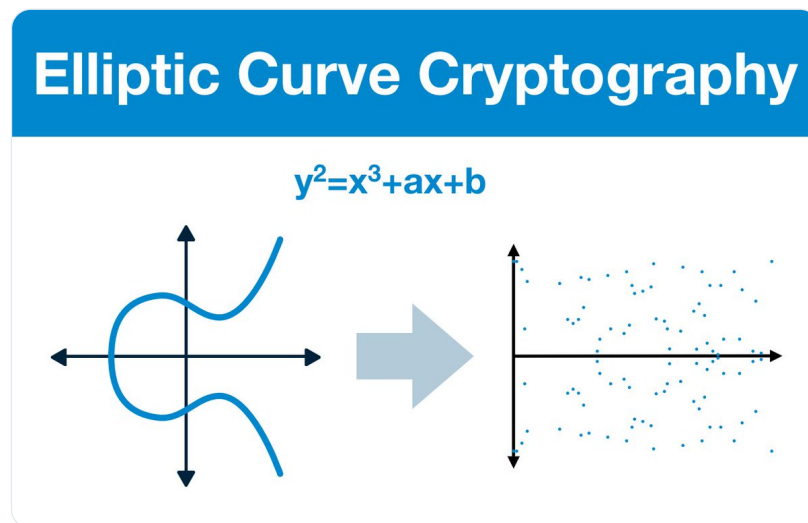
Haym @SalomonCrypto

Oct 16 · 26 tweets · [SalomonCrypto/status/1581695845023350785](#)

(1/25) Degen's Handbook: A Practical Guide to Elliptic Curve Cryptography

Elliptic Curve Cryptography is TOUGH; sometimes you need to walk away from the details and reframe on the bigger picture.


Let's start over and level set on the basics; I think this will help it all click.



(2/25) Before we begin, a quick note.

The purpose of this series is to give you a non-technical of elliptic curve cryptography and its applications for [@ethereum](#). There is some math, but you should be able to sail through with a high-school level education.



 **Haym**
@SalomonCrypto · [Follow](#)



Replying to @SalomonCrypto

(2/18) Preface:

This is part of a series on elliptic curve cryptography and its applications for [@ethereum](#). This is simplified to a MINIMAL level, aiming at ~high-school math.

[@VitalikButerin](#) [@dankrad](#) [@danboneh](#) [@chaseklvk](#), if you read this, I'm sorry for what I did to the math.

4:03 PM · Oct 15, 2022

 18  Reply  Copy link

[Read 2 replies](#)

(3/25) In [@VitalikButerin](#)'s post on elliptic curve pairings, he warns "elliptic curves themselves are very much a nontrivial topic to understand... if you do not [know how they work], I recommend this article."

Well, I read the article and (basically) transcribed it:

Haym
@SalomonCrypto · Follow

(1/25) Cryptography Fundamentals: Elliptic Curve Cryptography

Elliptic Curve Cryptography is (one of) our strongest cryptographic tools, vastly more secure than its predecessors. But... how does the moon math at the center of modern crypto work?

A layman's guide to Sci-Fi tech

Elliptic Curves

An elliptic curve is the set of points that are defined by an equation in the form:
 $y^2 = x^3 + ax + b$

Elliptic curves are horizontally symmetric; when reflected over the x-axis, both sides are the same

Pick two points on the curve

Draw a line through the points

When line intersects, flip over x-axis

Examples

Pick two points on the curve

Draw a line through the points

When line intersects, flip over x-axis

The finite field shares many of the properties of the elliptic curve

9:50 PM · Oct 13, 2022

Read the full conversation on Twitter

1.1K Reply Copy link

Read 33 replies

(4/25) Direct link

<https://blog.cloudflare.com/a-relatively-easy-to-understand-primer-on-elliptic-curve-cryptography/>

(5/25) Knowing what I know now, I see why [@grittygrease](#) wrote it the way he did. No disrespect, I still refer to it often.

But I will say, I don't think it's particularly easy to take away the important things you need to learn about elliptic curves. At least for our purposes.

(6/25) So let's review the material, but this time we are going to take a different path through the same lessons.

We are going to approach from a bit further out. Let's cover the purpose of cryptography.

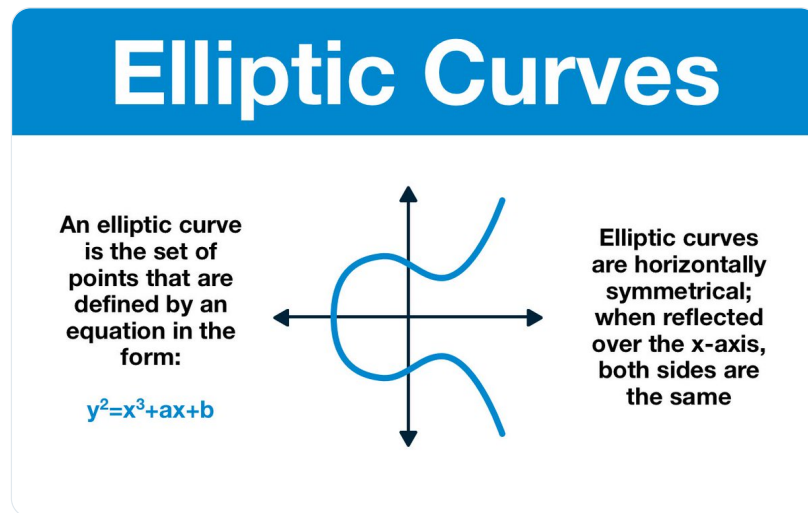
(7/25) The internet is a very public place. It basically works by blasting information at anyone listening, hoping it'll get to its intended recipient.

The goal of cryptography is to systematically alter data until it is undecipherable and undistinguishable from random data.

(8/25) Making data unreadable is easy, the trick is in altering it in a way that makes it recoverable by specific, intended recipients.

This is the problem space: how can we communicate private data through public spaces with the confidence granted by mathematical certainty?

(9/25) So, what is an elliptic curve?



(10/25) The y^2 term is particularly important. Any solution that satisfies the right side of the equation will have two y solutions: a positive and a negative.

If $y = 3$ is a solution, so is $y = -3$; both are equally correct.

Squaring y introduces ambiguity.

(11/25) Let's say there's a secret number y that we both know, but we aren't sure if the other person knows. The goal is to figure out if the other person knows without giving up the secret.

We can leverage the ambiguity in our elliptic curve equation.

(12/25) Instead of sharing y (or any info that could be used to derive y), we could agree upon an elliptic curve equation and agree to share the x value that corresponds with our y .

That x could reference y or $-y$; it is ambiguous.

(13/25) If we stopped here, we would be able to support just this 50/50 type of ambiguity. This can be useful; a lot of critical info is binary.

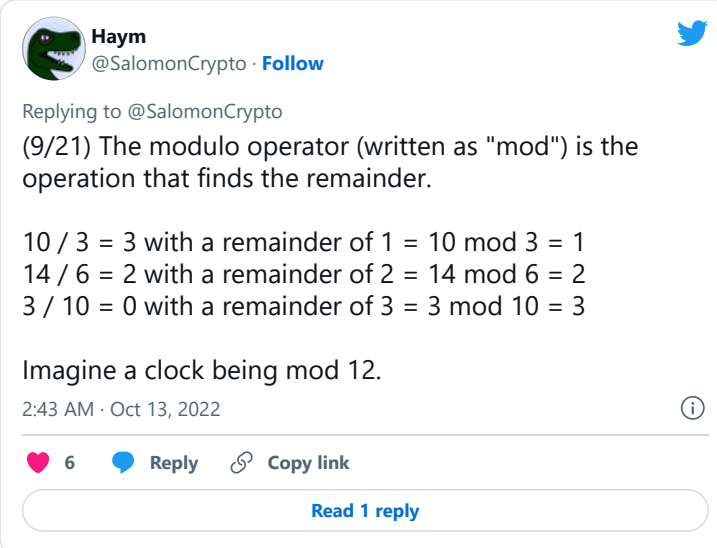
But we are not going to stop here. We are going to add more ambiguity until we can use it to obscure something substantial.

(14/25) (Pause for math)

At this point our frame shifts from normal math to discrete math. I'll give you what's important, but you'll need to know modular arithmetic.

tl;dr if you divide x by y the remainder is z, which we write as $x \bmod y = z$.

(Resume)



Haym
@SalomonCrypto · Follow

Replying to @SalomonCrypto

(9/21) The modulo operator (written as "mod") is the operation that finds the remainder.

$10 / 3 = 3$ with a remainder of $1 = 10 \bmod 3 = 1$
 $14 / 6 = 2$ with a remainder of $2 = 14 \bmod 6 = 2$
 $3 / 10 = 0$ with a remainder of $3 = 3 \bmod 10 = 3$

Imagine a clock being mod 12.


2:43 AM · Oct 13, 2022

6 ❤️ Reply Copy link

Read 1 reply

(15/25) The best place to start is always with the solutions that came before.

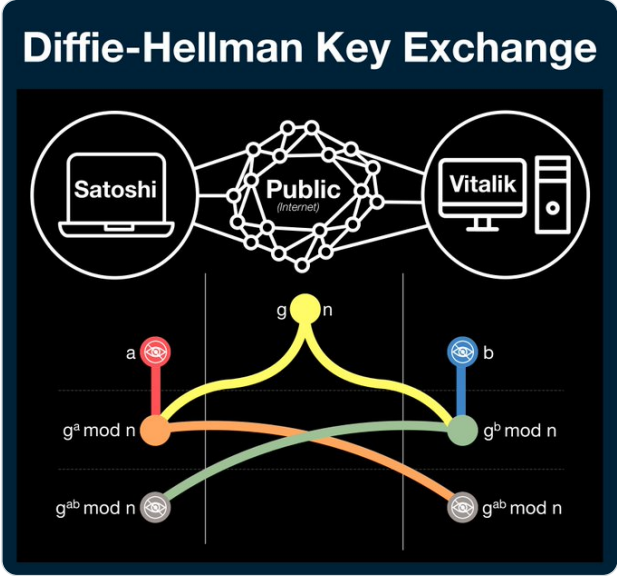
Diffie-Hellman works by generated a shared secret by passing intermediate, non-sensitive messages through public spaces.

 **Haym**
@SalomonCrypto · [Follow](#)

(1/21) Cryptography Fundamentals: Diffie-Hellman Key Exchange


How do you share private information over public networks? How can we create mathematically secure secrets? What actually is an encryption key?




A public guide for private communication.



The diagram illustrates the Diffie-Hellman Key Exchange process. At the top, two nodes labeled 'Satoshi' (with a laptop icon) and 'Vitalik' (with a computer icon) are connected to a central 'Public (Internet)' network represented by a mesh of nodes. Below this, the mathematical steps are shown: 1. A common base g and modulus n are established. 2. Satoshi chooses a private key a and calculates $g^a \text{ mod } n$. 3. Vitalik chooses a private key b and calculates $g^b \text{ mod } n$. 4. Both parties exchange their intermediate values over the public channel. 5. Each party then uses their own private key and the other's intermediate value to calculate the shared secret $g^{ab} \text{ mod } n$.

2:43 AM · Oct 13, 2022

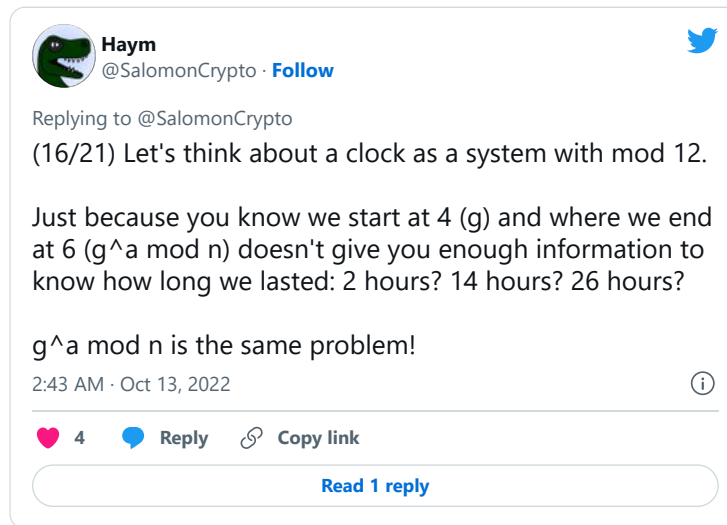
 [Read the full conversation on Twitter](#)

 451  Reply  Copy link

[Read 29 replies](#)

(16/25) These intermediate messages contain sensitive data, but they protect the value by looping through modular arithmetic.

You can see the final result, but you have no idea how many times the result passed through the mod operator before it got there.



(17/25) Our first goal is going to be to move this dynamic to elliptic curves. In order to do so, two things need to be possible:

- we can conduct the mathematical operations needed to move between points
- these operations still work when we apply modular arithmetic

(18/25) This is one of those moments where I think the previous telling was not particularly useful. I just defined this bizarre operation, and called it a dot operation and then kinda just... moved on...

Here's what you actually need to know about dot operations: they exist.

Haym
@SalomonCrypto · Follow

Replying to @SalomonCrypto

(12/25) We will define the dot operation to take advantage of the curve's unique shape and horizontal symmetry.

Shape: a line drawn through 2 points will intersect with the curve once (and only once) more

Symmetry: the curve always exists in the same place opposite the x-axis.

Dot Operation

Pick two points on the curve

Draw a line through the points

When line intersects, flip over x-axis

Examples

$A \text{ dot } C = D$

$A \text{ dot } D = E$

$A \text{ dot } E = F$

9:50 PM · Oct 13, 2022

6 ❤️ Reply Copy link

Read 1 reply

(19/25) What's practically useful is understanding that the dot operation is the elliptic curve-version of addition. You can dot/add two separate points to get a third, it's just the visualization that's weird.

We can dot/add two points and we can dot/add a point to itself.

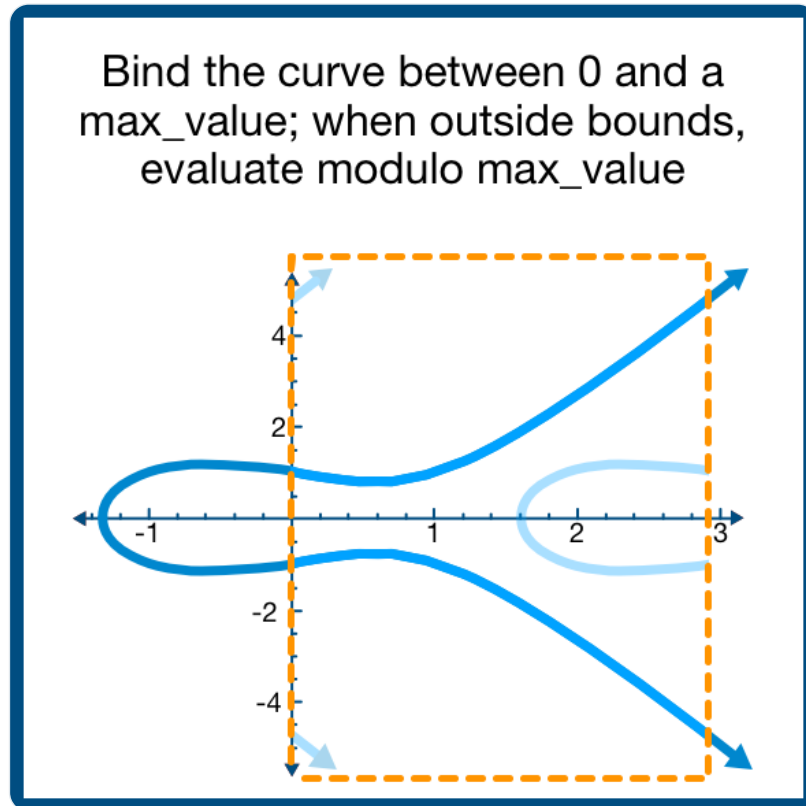
(20/25) From this primitive, we can build all the tools needed to execute the math needed to create the ambiguity of Diffie-Hellman.

And for the sake of time (and sanity) I'll just cut to the chase: everything works just as well in modular arithmetic too.

(21/25) So then the question becomes "how do we apply modular arithmetic to a curve?" It's not too bad, you just wrap the graph back within a boundary.

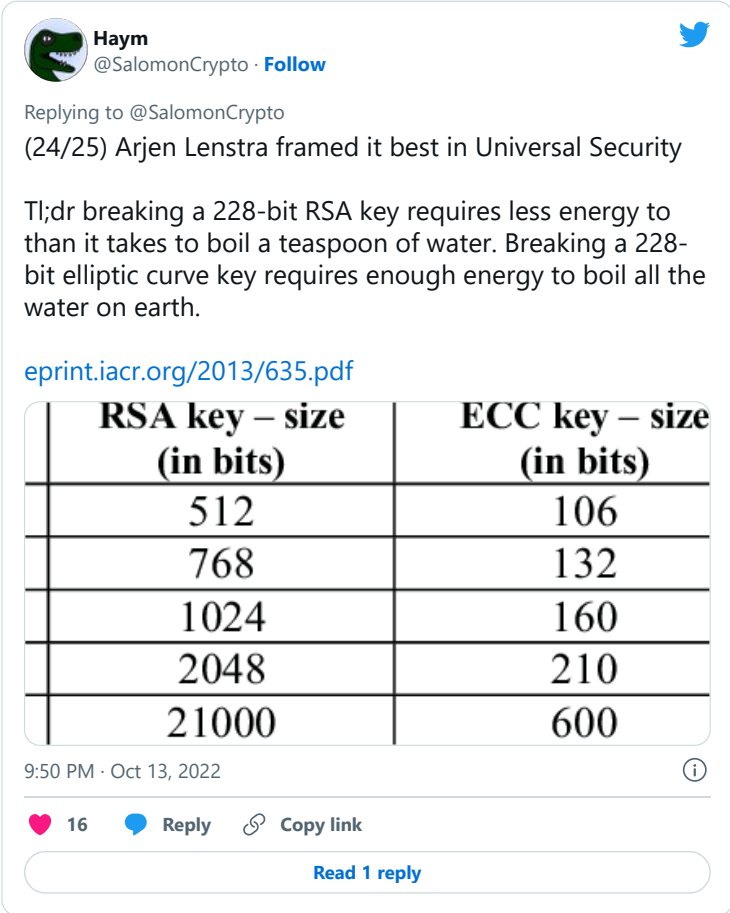
Once you're done, you have two layers of ambiguity:

- 1) y^2
- 2) $\text{mod } \text{max_value}$



(22/25) We have reached the impenetrable foundation of elliptic curve cartography: the elliptic curve discrete logarithm problem.

The discrete logarithm problem (factoring modular numbers) is provably difficult, the extra layer of ambiguity makes it SIGNIFICANTLY more difficult.



Haym
@SalomonCrypto · Follow

Replying to @SalomonCrypto
(24/25) Arjen Lenstra framed it best in Universal Security

Tl;dr breaking a 228-bit RSA key requires less energy to than it takes to boil a teaspoon of water. Breaking a 228-bit elliptic curve key requires enough energy to boil all the water on earth.

eprint.iacr.org/2013/635.pdf

RSA key – size (in bits)	ECC key – size (in bits)
512	106
768	132
1024	160
2048	210
21000	600

9:50 PM · Oct 13, 2022

16 Reply Copy link

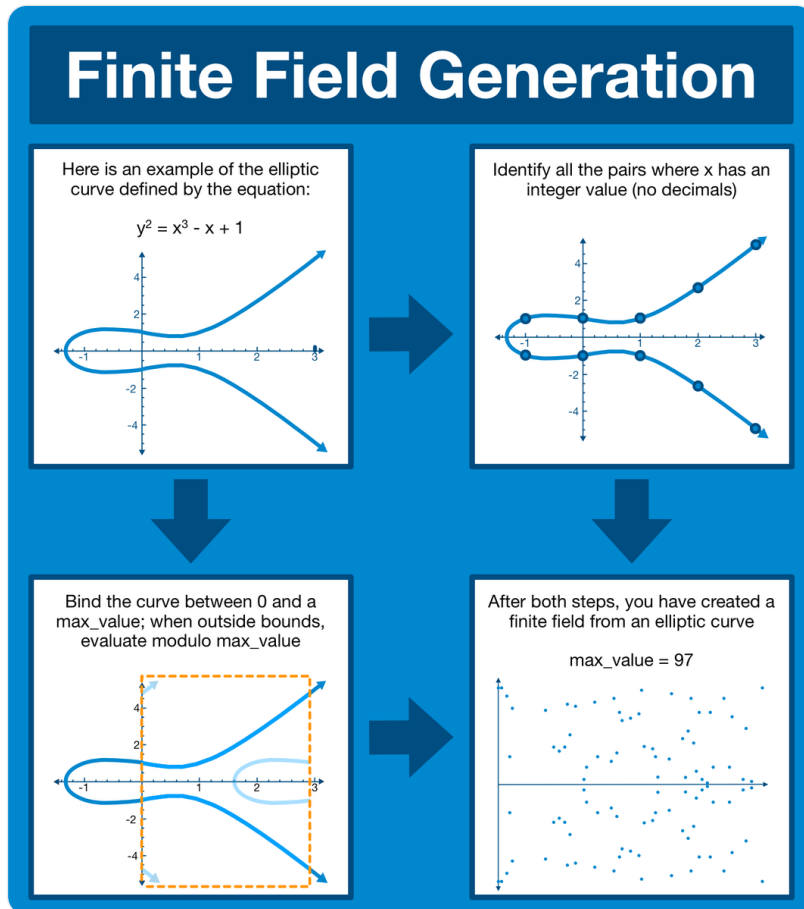
Read 1 reply

(23/25) At this stage we are done! We now have all the fundamentals we need to continue on our journey to understanding how [@ethereum](#) leverages elliptic curve cryptography.

But, for the sake of completeness (and to save time later), let's include the finite field generation.

(24/25) At this point it's very simple: we just take our elliptic curve in modular space and throw out all the values where x is not a whole number.

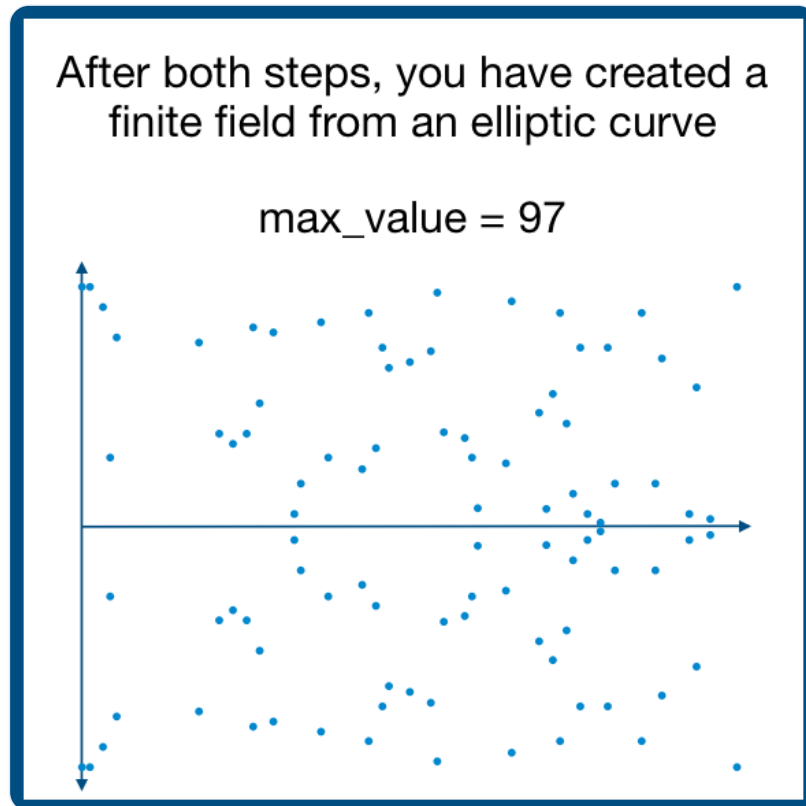
This constrains the elliptic curve to only apply to x-value integers, which will become useful a little bit down the line.



(25/25) And so here's where we will part, with a finite field generated from an elliptic curve.



When you look at it on it's own, it really seems to look like a random jumble of numbers, especially if you weren't around when we built it...

I wonder how that could come in handy?



Like what you read? Help me spread the word by retweeting the thread (linked below).

Follow me for more explainers and as much alpha as I can possibly serve.

 **Haym**
@SalomonCrypto · [Follow](#) 

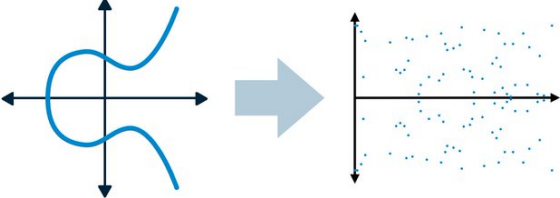
(1/25) Degen's Handbook: A Practical Guide to Elliptic Curve Cryptography


Elliptic Curve Cryptography is TOUGH; sometimes you need to walk away from the details and reframe on the bigger picture.


Let's start over and level set on the basics; I think this will help it all click.




Elliptic Curve Cryptography

$y^2=x^3+ax+b$



5:17 PM · Oct 16, 2022 

 [Read the full conversation on Twitter](#)

 453  Reply  Copy link

[Read 12 replies](#)

...