

Understanding Monero Cryptography, Privacy -- Introduction

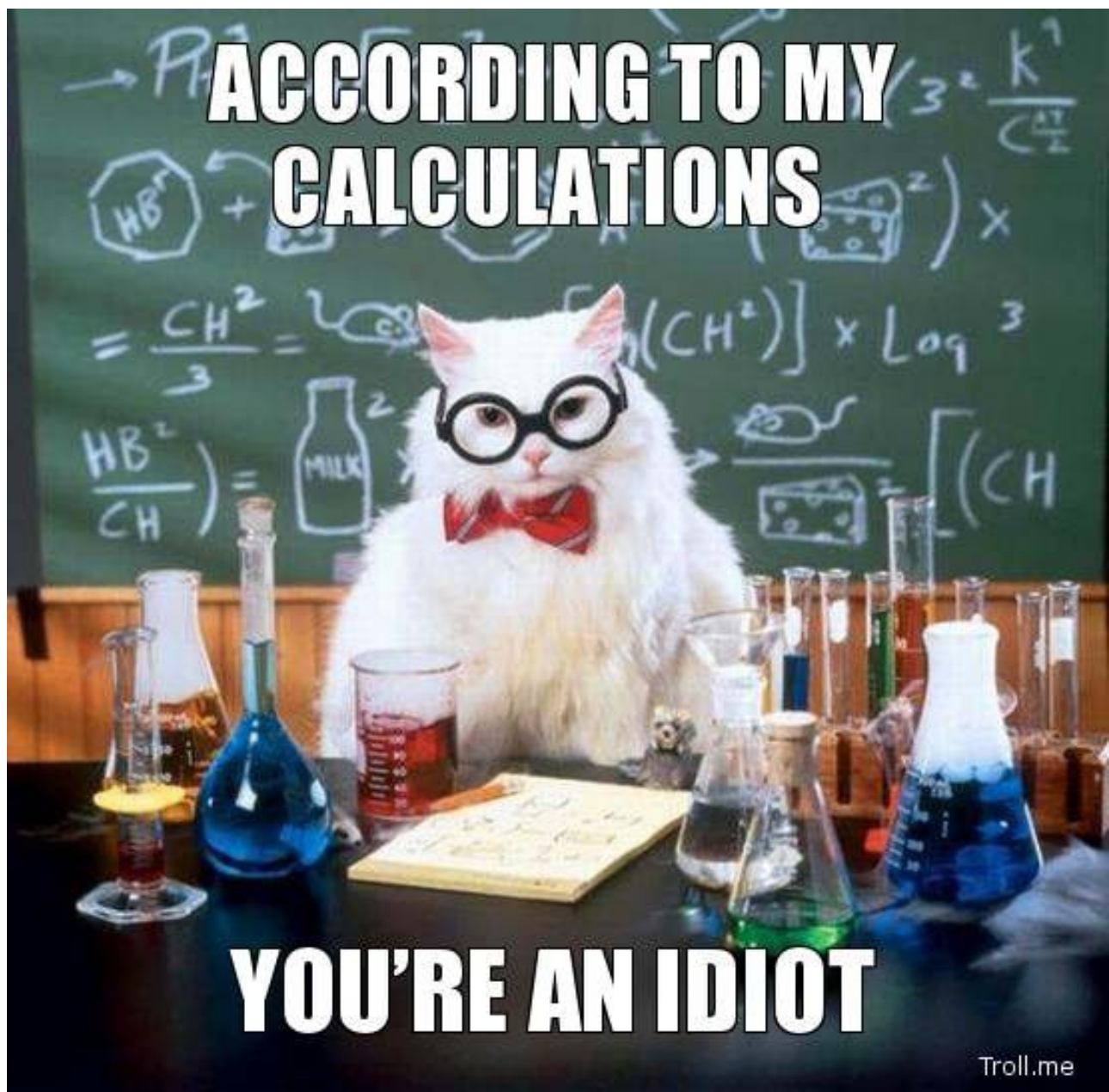
luigi1111 ⁽⁵⁵⁾ ▾ (/@luigi1111)in #monero (/trending/monero) • 6 years ago (edited)

This is part one of a series of unknown size; it'll be done when it's done.

Part one focuses on the basics: ECC, the particular curve, private and public "keys", and a bonus section on how Monero addresses are generated.

Note: Monero is based on the Cryptonote protocol -- though it has diverged and will continue to diverge -- along with numerous other coins; much of this series will apply equally well to the others with some caveats. Monero is easily the largest and most active Cryptonote-based project.

Hello! I'm an autodidact enthusiast of cryptography, particularly in relation to the crypto-currency Monero . Naturally, you should not assume everything I say is correct, and I hope any egregious errors are pointed out so I can fix them (and help my own understanding). Just calling me an idiot is fine too.



Monero's tagline is "Secure, Private, Untraceable." Secure could refer to a number of facets of a crypto-currency, but here we are only particularly interested in security relating to privacy/anonymity. These articles will be looking at how Monero achieves "privacy", that is unlinkability and untraceability, with references to security where appropriate. This article focuses on some concepts, which will hopefully make understanding the others easier. Without further ado, let's get into it!

What is Elliptic Curve Cryptography?

Alright, so what is ECC? From Wikipedia : " **Elliptic curve cryptography** (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields . "

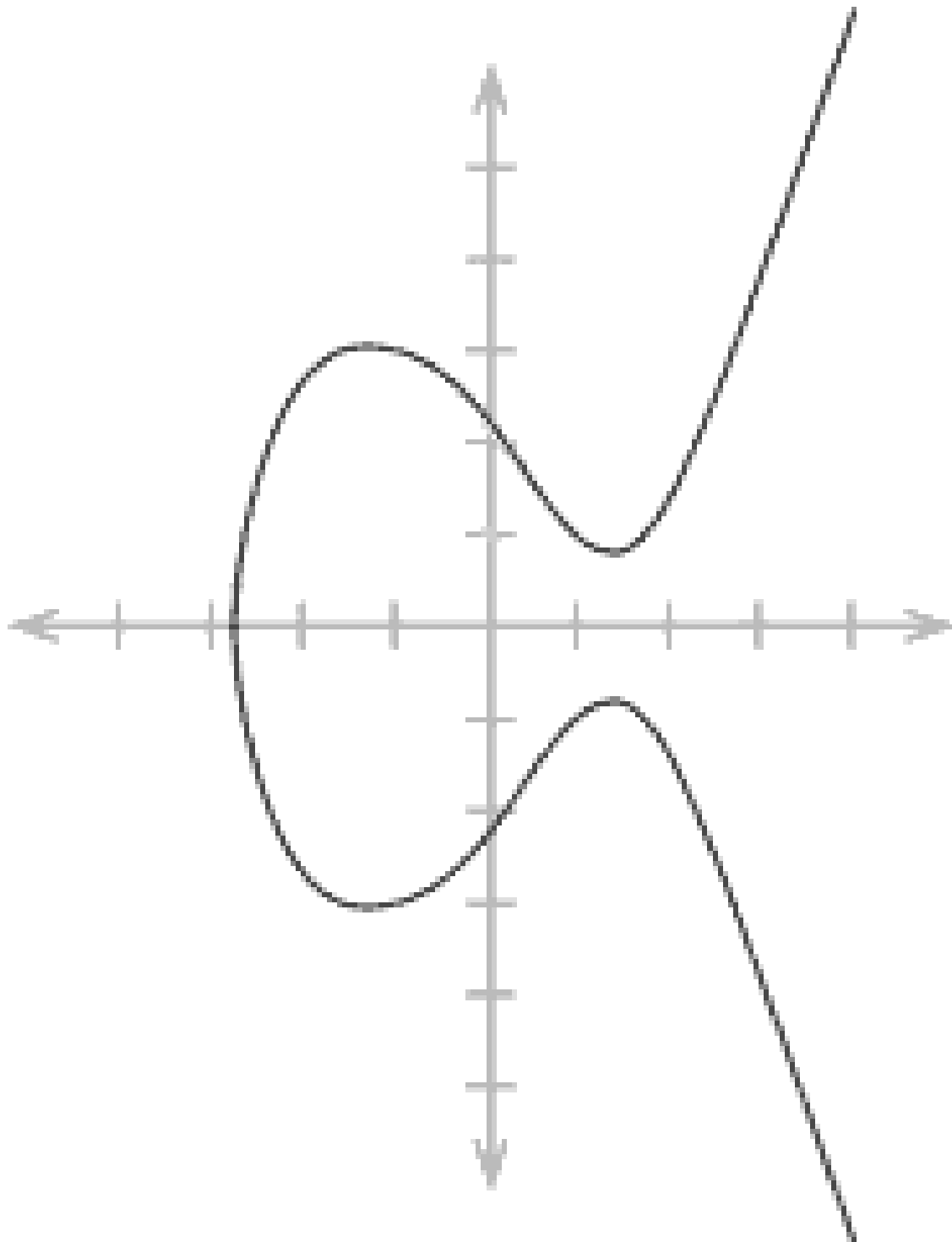
Now, what does that mean? *I have no idea.*

More seriously, let's go through it:

1. Public-Key Cryptography, or asymmetric cryptography, uses a pair of keys instead of a single private key as in symmetric cryptography (e.g., AES): a public key, to be given out to "the world"; and a private key, to be always kept secret. To be secure, it must be *hard intractable* to figure out the private key given the public key; to be usable it must be *easy* to calculate the public key given the private key. ECC relies on the ECDLP for its security. **Takeaways: public/private key pair; private->public is easy, but public->private is "impossible".**
2. "algebraic structure of elliptic curves": *What is this???* It is a plane curve satisfying

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

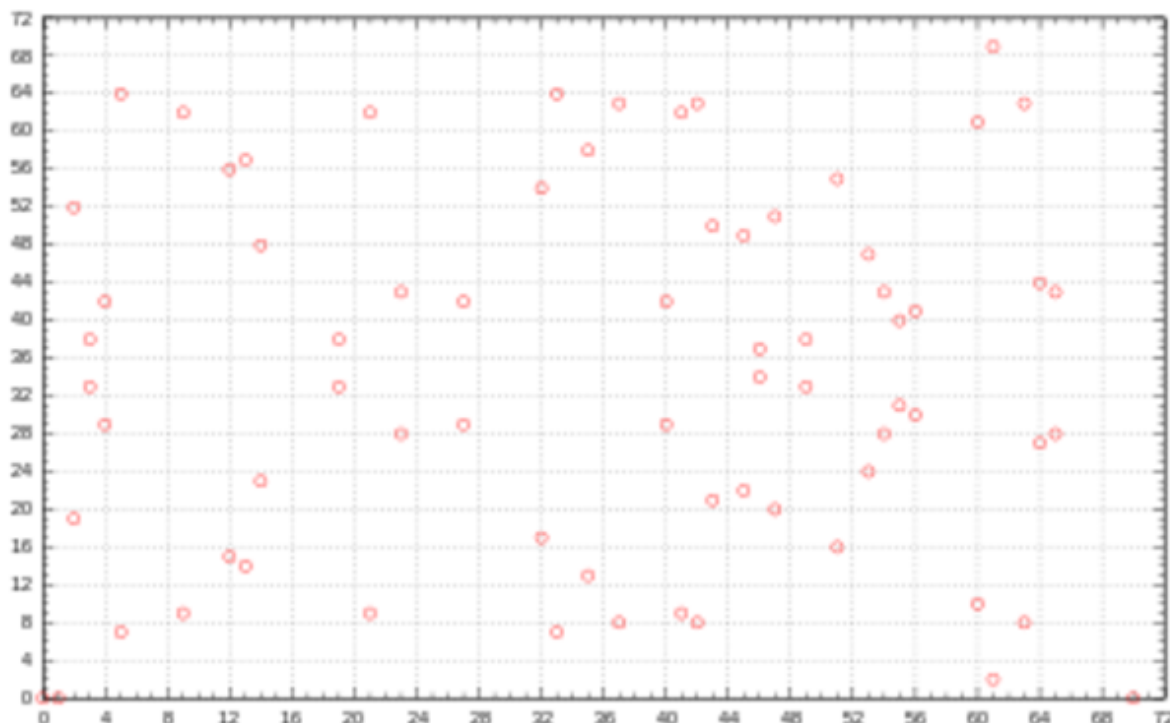
. It might look something like this:



Who cares? Right, probably no one. In case someone does, there's a wealth of articles (many related to Bitcoin) out there that explain in detail how they work, how addition is possible, etc. Some examples: A, B, C (a series itself) . Numerous videos are out there too, if you're into that. **Takeaways: none, *this funny-looking curve will not help you understand and isn't even how Monero's curve looks.***

3. "over finite fields": this just means curve points are taken modulo some (large, prime) number. Everyone is familiar with modular addition and subtraction at least (even if they've never heard the word) due to our time-keeping. *If it is 10am, what time will it be in 5 hours? **Congrats, you just did modular addition.*** An elliptic curve over a finite field

might look something like this:



Whoa, that looks odd. Yes, it does. **Takeaways: none. Actually, note how the points are "reflected" over an invisible line in the center.**

A primary benefit of using ECC vs something like RSA is that keys are much smaller for similar security levels.

I believe the only things you need to know to proceed are:

1. A point on the curve can be added to or subtracted from another point, or itself.
2. A point cannot be multiplied or divided by another point.
3. Adding a point to itself allows "scalar multiplication", **which is where the *magic* happens.**

Subtracting a point from itself isn't very useful, as it'll just return the ECC equivalent of 0. Division by integer isn't possible (the equivalent modular operation -- modular multiplicative inverse -- is, but only with knowledge of the original scalar).

Scalar multiplication is just adding a point to itself over and over; given a point A, $5A = A + A + A + A + A$. Since we use astronomically large scalars to prevent easy brute-forcing, we use techniques like *double-and-add* to allow computation in near-logarithmic time (i.e., really fast!). A quick example:

Suppose our scalar is 27, and we want to compute 27A. Using the naive method, we'd need 26 additions. Instead:

1. Add A to itself: 2A. Let's call this new point B.
2. Add B to itself: 2B = 4A = C.
3. Add C to itself: 2C = 4B = 8A = D.
4. Add D to itself: 2D = 4C = 8B = 16A = E.
5. Add D to E: 24A = F.
6. Add B to F: 26A = G.
7. Add A to G: 27A

We went from 26 additions to 7. The difference grows exponentially with larger scalars. The speed difference for an average-size scalar is something along the lines of "all the energy in the universe isn't enough" and "takes less than 1/100th of a second on an average computer", which is interesting to ponder.

That's it for general ECC stuff! If you want more in-depth technical details, please see the links above. :)

The Monero Curve and Private and Public "Keys"

Now, onto the Monero-specific stuff. *Finally.*

First some boring stuff like curve constants. From the Cryptonote whitepaper , we get:

q : a prime number; $q = 2^{255} - 19$;

d : an element of \mathbb{F}_q ; $d = -121665/121666$;

E : an elliptic curve equation; $-x^2 + y^2 = 1 + dx^2y^2$;

G : a base point; $G = (x, -4/5)$;

l : a prime order of the base point; $l = 2^{252} + 27742317777372353535851937790883648493$;

\mathcal{H}_s : a cryptographic hash function $\{0, 1\}^* \rightarrow \mathbb{F}_q$;

\mathcal{H}_p : a deterministic hash function $E(\mathbb{F}_q) \rightarrow E(\mathbb{F}_q)$.

We are dealing with the Ed25519 curve, which is a Twisted Edwards Curve . *Good, more meaningless details!*

Let's quickly go through it:

- q : this is the total number of points on this curve. It is mostly irrelevant for our purposes.
- d : an element used in the curve equation below. Not important.
- E : the equation for our Ed25519 curve. *Wow, shiny!* Not important.
- G : the base point or generator point. **This is important!** It is the base from which many operations start. It is the "A" in the above example. In hex, which all of our keys are commonly represented in, it looks like: "5866". *Great, back to useless information.*
- l : the "order" of the above base point. **This is important**, as it defines the maximum number of points we can use, and the maximum size our scalars can be. This number is like the number "12" to a clock; adding points or scalars together that would "go over" means they will "wrap around" instead. If you could add G to itself over and over and over until you reached $l-1$ number of additions, you would end up back at G .
- H_s and H_p : s means scalar, p means point. These will be discussed in a later article.

Note:

1. Scalars (private keys, really just large integers) are always represented by lowercase letters in equations.
2. Points (public keys, really an encoded coordinate on the curve) are always represented by uppercase letters.

In the "real world" (user-facing), both private and public keys in Monero are represented by 64 hex characters, similar to the above representation of G . *Time for more useless information.* Scalars are straightforwardly represented as little-endian integers (any integer between 0 and l is valid), while points are specially encoded in a way that is too complex for this article. *Or maybe I haven't cared enough about the encoding to research it.*

If we use x as our private key and P as our public key, then $P = xG$.

Some "fun" examples:

1. $x = 1$ or

"0100
00" (remember little-endian); $P =$
"5866
66" or G . ($1G = G$)

2. $x = 1 - 1$ or

[illegible]

3. The integer $(l+1)/2$,

"f7e97a2e8d31092c6bce7b51ef7c6f0a00000000000000000000000000000000
8", produces the point farthest away from G (close enough, it and the next point are tied due to I being odd),
"ac1999070321b2c6309cc8e31aa89a8b3baa75b5f8febf47855555a3e744bc
f0", similar to how 6 is farthest away from 12 on a clock. It (just like G
and every other point) has a complimentary point (in this case produced by $(I-1)/2$, with which it will sum to the identity element.

Monero Accounts and Addresses

This has gone a little long, so I'll just briefly restate the information available here for the standard deterministic derivation. The reason we have two key pairs will be discussed in a future article on stealth addresses.

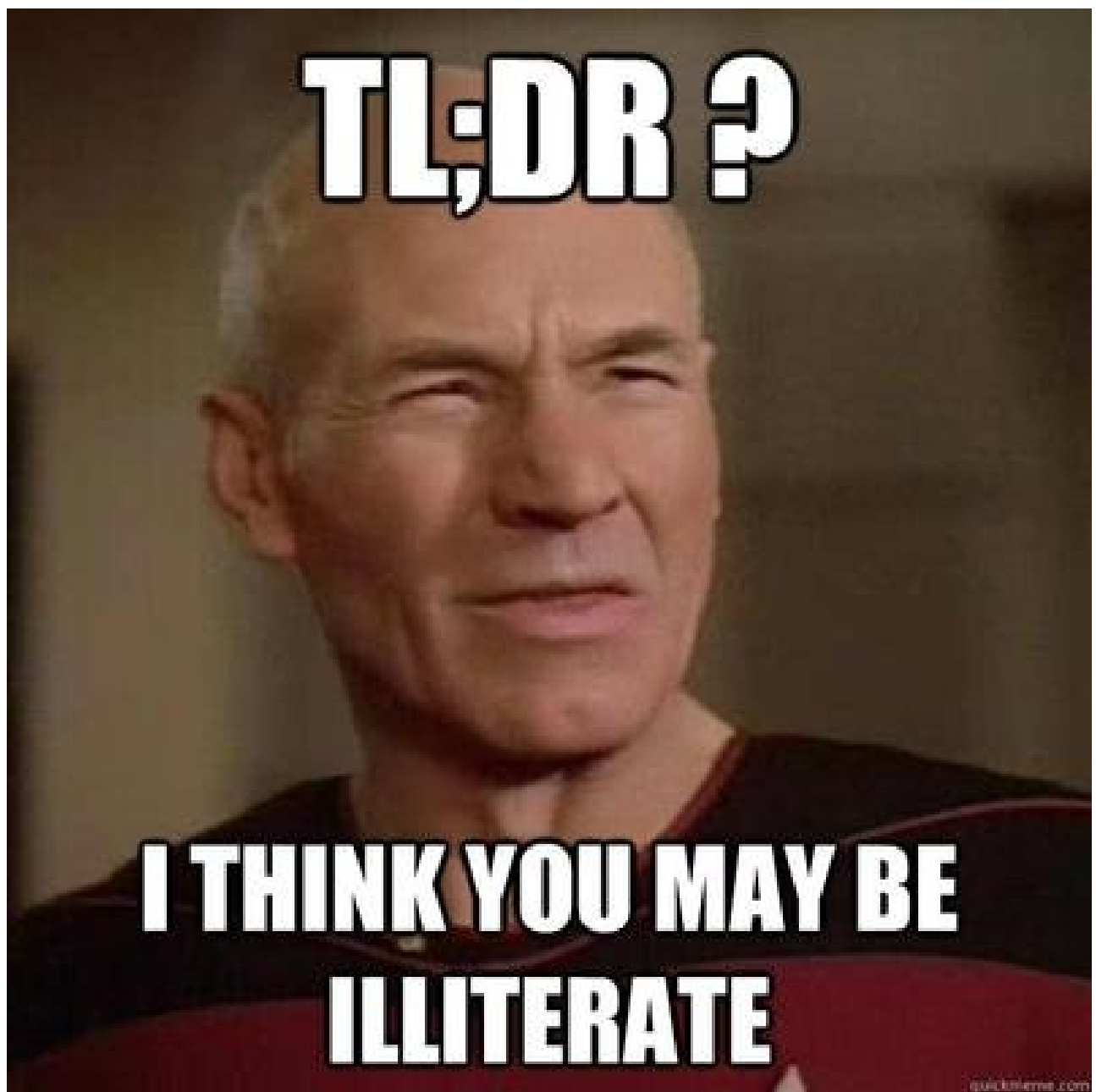
1. Choose a random private spend key, typically by creating 256 random bits then "reducing" mod I . Call this key b (to match the whitepaper -- it's confusing I know).

2. Hash b with the chosen algorithm, H (Keccak_256 in our usage). Interpret the result as an integer and reduce it mod l as before. Call this key a .

3. Calculate $B = bG$ and $A = aG$. These are your public spend and public view keys.
4. Hash (prefix (0x12 in standard Monero) + $B + A$) with H .
5. Append the first four bytes of the result to (prefix + $B + A$). This will be 69 bytes (1 + 32 + 32 + 4).
6. Convert to cnBase58. This is not as straightforward as regular base58, as it uses blocks and padding to result in fixed-length conversions. 69 bytes will always be 95 cnBase58 characters.

Integrated addresses (described here) are the same as above, but with an 8 byte Payment ID appended to A in step 4 above and a different prefix (0x13).

That does it for the introduction! Hopefully it wasn't completely incoherent rambling. Additional articles on stealth addresses and ring signatures will be coming out sometime soon. **Feedback is appreciated.**



For those of you looking for a TL;DR (or if you're just bored out of your mind), I've included a random picture (but no TL;DR).



Until next time!

[#cryptography \(/trending/cryptography\).](#) [#privacy \(/trending/privacy\).](#)

[#anonymity \(/trending/anonymity\).](#)

🕒 6 years ago in [#monero \(/trending/monero\)](#) by

[luigi1111 \(55\)](#) ▾ [./ \(@luigi1111\)](#)

👍👎 [\\$2,179.97](#) ▾ | [227 votes](#) ▾

➡ [Reply](#) | 💬 [26](#)

[./ \(monero/@luigi1111/understanding-monero-cryptography-privacy-introduction\).](#) [f](#) [t](#) [r](#) [in](#) [@](#)

Sort: [Trending](#) ▾



[xeroc \(70\)](#) ▾ [./ \(@xeroc\)](#) 6 years ago [./ \(monero/@xeroc/re-luigi1111-understanding-monero-cryptography-privacy-introduction-20160728t060310085z#@xeroc/re-luigi1111-understanding-monero-cryptography-privacy-introduction-20160728t060310085z\)](#) [\[.\]](#)

I like the way of your writing. Easy to read even for newcomers while technically correct ... GJ

👍👎 [\\$6.48](#) ▾ | [7 votes](#) ▾ | [Reply](#)



luigi1111 (55) ▾ (/@luigi1111) 6 years ago (/monero/@xeroc/re-luigi1111-understanding-monero-cryptography-privacy-introduction-20160728t060310085z#@luigi1111/re-xeroc-re-luigi1111-understanding-monero-cryptography-privacy-introduction-20160728t143427787z) [⋮]

Thanks! I had originally planned for the title to include "in plain English", but part way through I wasn't sure how "plain" it would end up being. Still, the focus is absolutely on making it as easy to understand as I can. :)

  \$0.00 | 1 vote ▾ | [Reply](#)



karenb54 (73) ▾ (/@karenb54) 6 years ago (/monero/@karenb54/re-luigi1111-understanding-monero-cryptography-privacy-introduction-20160728t010351898z#@karenb54/re-luigi1111-understanding-monero-cryptography-privacy-introduction-20160728t010351898z) [⋮]

Can I press Ctrl Alt Del and start again please

  \$0.02 ▾ | 3 votes ▾ | [Reply](#)



donutly (43) ▾ (/@donutly) 6 years ago (/monero/@donutly/re-luigi1111-understanding-monero-cryptography-privacy-introduction-20160728t011000237z#@donutly/re-luigi1111-understanding-monero-cryptography-privacy-introduction-20160728t011000237z) [⋮]

Thanks for posting this! It was so helpful, I never really understood it like this before.

  \$0.00 | 1 vote ▾ | [Reply](#)



luigi1111 (55) ▾ (/@luigi1111) 6 years ago (/monero/@donutly/re-luigi1111-understanding-monero-cryptography-privacy-introduction-20160728t011000237z#@luigi1111/re-donutly-re-luigi1111-understanding-monero-cryptography-privacy-introduction-20160728t011515519z) (edited) [⋮]

Stay tuned for more (at unknown future dates of course -- soon^tm).

  \$0.00 | 1 vote ▾ | [Reply](#)



apes (47) ▾ (/@apes) 6 years ago (/monero/@apes/re-luigi1111-understanding-monero-cryptography-privacy-introduction-20160728t074005450z#@apes/re-luigi1111-understanding-monero-cryptography-privacy-introduction-20160728t074005450z) [⋮]

you wanted to share how monero deals with privacy. Is it correct if I assume i can have many public keys and from these keys you cannot know my private key? If i now use mulitple public key my transactions can not connect to me?

  \$0.00 | 1 vote ▾ | [Reply](#)

luigi1111 (55) ▾ (/@luigi1111) 6 years ago (/monero/@apes/re-luigi1111-understanding-monero-cryptography-privacy-introduction-20160728t074005450z#@luigi1111/re-apes-re-luigi1111-understanding-monero-cryptography-privacy-introduction-20160728t142002931z) [⋮]

This is only an introduction -- prerequisites if you will -- the "meat" will come later.

  \$0.00 | [Reply](#)

maximkichev (57) ▾ (/@maximkichev) 6 years ago (/monero/@maximkichev/re-luigi1111-understanding-monero-cryptography-privacy-introduction-20160728t012735162z#@maximkichev/re-luigi1111-understanding-monero-cryptography-privacy-introduction-20160728t012735162z) [-].

It is very difficult for me ! Okay , we understand and learn what is new every day !

⬆️ ⬇️ \$0.00 | 2 votes ▾ | Reply

luigi1111 (55) ▾ (/@luigi1111) 6 years ago (/monero/@luigi1111/re-luigi1111-understanding-monero-cryptography-privacy-introduction-20160728t002846442z#@luigi1111/re-luigi1111-understanding-monero-cryptography-privacy-introduction-20160728t002846442z) (edited) [-].

Sorry folks, pics are all screwed up. Will try to fix.

Edit: fixed, I think.

⬆️ ⬇️ \$0.00 | 1 vote ▾ | Reply

monero.com

clayton-smock (53) ▾ (/@clayton-smock) 6 years ago (/monero/@luigi1111/re-luigi1111-understanding-monero-cryptography-privacy-introduction-20160728t002846442z#@clayton-smock/re-luigi1111-re-luigi1111-understanding-monero-cryptography-privacy-introduction-20160728t003311802z) [-].

They look good to me!

⬆️ ⬇️ \$0.00 | Reply

btcbtc20155 (56) ▾ (/@btcbtc20155) 6 years ago (/monero/@btcbtc20155/re-luigi1111-understanding-monero-cryptography-privacy-introduction-20160728t013003945z#@btcbtc20155/re-luigi1111-understanding-monero-cryptography-privacy-introduction-20160728t013003945z) [-].

This bring me back to my college time. Thanks.

⬆️ ⬇️ \$0.00 | Reply

cwmyao1 (54) ▾ (/@cwmyao1) 6 years ago (/monero/@cwmyao1/re-luigi1111-understanding-monero-cryptography-privacy-introduction-20160728t013039148z#@cwmyao1/re-luigi1111-understanding-monero-cryptography-privacy-introduction-20160728t013039148z) [-].

Thanks for sharing.

⬆️ ⬇️ \$0.00 | Reply

trogdor (64) ▾ (/@trogdor) 6 years ago (/monero/@trogdor/re-luigi1111-understanding-monero-cryptography-privacy-introduction-20160728t013303518z#@trogdor/re-luigi1111-understanding-monero-cryptography-privacy-introduction-20160728t013303518z) [-].



Sir, you just earned a follow.

⬆️ ⬇️ \$0.00 | Reply

serkanturan (38) ▾ (/@serkanturan) 6 years ago (/monero/@serkanturan/re-luigi1111-understanding-monero-cryptography-privacy-introduction-20160728t104705322z#@serkanturan/re- [-].



luigi1111-understanding-monero-cryptography-privacy-introduction-20160728t104705322z)

I dont understand anything you say but I respect you :)

  \$0.00 Reply



ben.zimmerman (55) ▾ (/@ben.zimmerman) 6 years ago (/monero/@ben.zimmerman/re-luigi1111-understanding-monero-cryptography-privacy-introduction-20160728t140816719z#@ben.zimmerman/re-luigi1111-understanding-monero-cryptography-privacy-introduction-20160728t140816719z) [.]

EXCELLENT POST! I am so glad that this is trending! :-)

  \$0.00 Reply

terrycraft (72) ▾ (/@terrycraft) 6 years ago (/monero/@terrycraft/re-luigi1111-understanding-monero-cryptography-privacy-introduction-20160728t143535264z#@terrycraft/re-luigi1111-understanding-monero-cryptography-privacy-introduction-20160728t143535264z) [.]

Quite clear. Thank you



  \$0.00 Reply

jimbojones (53) ▾ (/@jimbojones) 5 years ago (/monero/@jimbojones/re-luigi1111-understanding-monero-cryptography-privacy-introduction-20170821t092548290z#@jimbojones/re-luigi1111-understanding-monero-cryptography-privacy-introduction-20170821t092548290z) [.]

w00t Monero just doubled in price :)



<https://steemit.com/bitcoin/@jimbojones/exclusive-monero-just-hit-usd120>

(<https://steemit.com/bitcoin/@jimbojones/exclusive-monero-just-hit-usd120>)

  \$0.00 Reply

paupau101 (25) ▾ (/@paupau101) 5 years ago (/monero/@paupau101/re-luigi1111-understanding-monero-cryptography-privacy-introduction-20170822t090233020z#@paupau101/re-luigi1111-understanding-monero-cryptography-privacy-introduction-20170822t090233020z) [.]



i've got headache man.

  \$0.00 Reply

eoslinks (38) ▾ (/@eoslinks) 5 years ago (/monero/@eoslinks/re-luigi1111-understanding-monero-cryptography-privacy-introduction-20170824t225327481z#@eoslinks/re-luigi1111-understanding-monero-cryptography-privacy-introduction-20170824t225327481z) [.]

awesome!



atleast he's not a maximalist (part of monero core team)

  \$0.00 Reply

morlon (33) ▾ (/@morlon) 4 years ago (/monero/@morlon/re-luigi1111-understanding-monero-cryptography-privacy-introduction-20180130t012457817z#@morlon/re-luigi1111-understanding-monero-cryptography-privacy-introduction-20180130t012457817z) [.]



Great article!

When you manage to make smd laugh while reading sth about IT then you really did it right! XD

  \$0.00 Reply



samoyedfans (40) ▾ ([/@samoyedfans](#)) 4 years ago ([/monero/@samoyedfans/re-luigi1111-understanding-monero-cryptography-privacy-introduction-20180322t180104230z#@samoyedfans/re-luigi1111-understanding-monero-cryptography-privacy-introduction-20180322t180104230z](#)) [⋮]

Monero is a sneaky coin, I like it

  \$0.00 Reply



ethhawk (25) ▾ ([/@ethhawk](#)) 6 years ago ([/monero/@ethhawk/re-luigi1111-understanding-monero-cryptography-privacy-introduction-20160728t031900463z#@ethhawk/re-luigi1111-understanding-monero-cryptography-privacy-introduction-20160728t031900463z](#)) [⋮]

This is just a description of how Cryptonote coins work not Monero, every Cryptonote fork has this for years already <http://chainradar.com/>

  \$0.00 1 vote ▾ Reply



lethos3 (25) ▾ ([/@lethos3](#)) 6 years ago ([/monero/@ethhawk/re-luigi1111-understanding-monero-cryptography-privacy-introduction-20160728t031900463z#@lethos3/re-ethhawk-re-luigi1111-understanding-monero-cryptography-privacy-introduction-20160728t045558984z](#)) [⋮]

and I have them all.

  \$0.00 Reply

fluffypony (56) ▾ ([/@fluffypony](#)) 6 years ago ([/monero/@ethhawk/re-luigi1111-understanding-monero-cryptography-privacy-introduction-20160728t031900463z#@fluffypony/re-ethhawk-re-luigi1111-understanding-monero-cryptography-privacy-introduction-20160728t100742516z](#)) [⋮]

He already said that this is part one. It would be crazy for him to detail MRL-0001 , MRL-0004 , and MRL-0005 (all of which are ONLY in Monero, and fix serious problems that CryptoNote has) in the first part of this series.

  \$0.00 Reply

ethhawk (25) ▾ ([/@ethhawk](#)) 6 years ago ([/monero/@ethhawk/re-luigi1111-understanding-monero-cryptography-privacy-introduction-20160728t031900463z#@ethhawk/re-fluffypony-re-ethhawk-re-luigi1111-understanding-monero-cryptography-privacy-introduction-20160728t110532101z](#)) [⋮]



This article doesn't even mention Cryptonote once and ALL of this cryptography comes from Cryptonote not Monero and every Cryptonote coin has the same for 2 years already <http://chainradar.com/>

That is false advertising.

  \$0.00 1 vote ▾ Reply

luigi1111 (55) ▾ (@luigi1111) 6 years ago (/monero/@ethhawk/re-
luigi1111-understanding-monero-cryptography-privacy-introduction-
20160728t031900463z#@luigi1111/re-ethhawk-re-fluffypony-re-ethhawk-
re-luigi1111-understanding-monero-cryptography-privacy-introduction-
20160728t143057887z) [-].

While I have no idea what chainradar.com has to do with anything, I understand your point.
I've added a note at the top.

  \$0.00 | [Reply](#)