You are the attacker against the CryptoNote protocol desiring to use the "multiple equations" approach to find a private key. Suppose you have:

- A secret key x (represented as an integer in the field G(2^255-19))
- A basepoint G on the elliptic curve E, which is for example Curve25519, which is a commonly used elliptic curve in Diffie-Helman cryptography [1], and also happens to be the curve used in the CryptoNote protocol.
- A public key, $P = xG$
- A "ring-image" $I = xH_p(P)$, where $H_p(-)$ is a hash function[2] taking a point on E to another point on E (which happens to be another multiple of the basepoint G).

and your goal is to solve, using the two equations $P = xG$, and $I = xH_p(P)$ for the integer x. Note that $H_p(P) = bG$ for some integer b (you may or may not know what that integer is, but let's even assume you can control the integer b to make your job as attacker easier).

Thus you have the two equations

$$P = xG$$

and

$$I = xbG.$$

You know what the integer b is, and what the points G, P, and I are, but not what the integer x is at this point.

Now compare this to the Elliptic Curve Diffie-Helman (ECDH) shared-key exchange. The ECDH procedure is as follows[3]:

- Profesor Xavier and Bob both know a basepoint G on the curve E
- Professor Xavier selects a secret integer x and computes the point $P = xG$ on the curve E
- Bob selects a secret integer b and computes the point $B = bG$ on the curve E

[1] http://cr.yp.to/ecdh/curve25519-20060209.pdf

[2] Keccak1600 is used in CryptoNote, but the hash function doesn't matter for the sake of this document

[3] Silverman, Arithmetic of Elliptic Curves pages 375-380

- Professor Xavier and Bob exchange values of P and B over an insecure communications line.
- Bob computes $bP = bxG = I$ and Professor Xavier computes $xB = xbG$ so they both know the shared key $I = bxG$.

Now the question is, can Bob, who knows the three pieces of information b, $bxG = I$, and $xG = P$ use these pieces of information to compute x, Xavier's private key? This is the exact same problem which is given above in the supposed "CryptoNote Attack." Because in Diffie-Helman it is well-known[4] to be difficult (computationally infeasible) to solve for the other party's private key (even in the case of multiple secret key uses - see section 3 in Bernstein's paper in the footnote), and since both problems involve exactly the same equations, that implies that no such attack, as outlined above, is possible against CryptoNote protocol. - Shen.Noether

[4] http://cr.yp.to/ecdh/curve25519-20060209.pdf