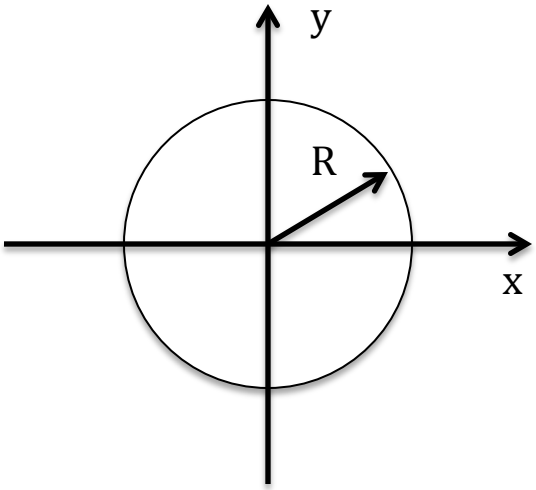
Circle is described by the following equation:

$$x^2 + y^2 = R^2$$

where R is the radius.



The circle is like an encryption algorithm, where R is the key, x is the plaintext and y is the ciphertext.

- If we know the key/radius R, then we can calculate the plaintext x from ciphertext y (or ciphertext y from plaintext x). This is similar to encryption (decryption).
- If we do not know the key/radius R, then we cannot calculate the plaintext x from ciphertext y (or the ciphertext y from plaintext x). Thus we cannot decrypt (encrypt).

The circle is only a concept: it describes the set of points that are equidistant from a Centre. Obviously, since it is only a concept, the circle does not have any physical properties (such as weight, color, etc.).

To run the encryption algorithm we need an implementation. For example, an implementation of a circle is the disk shown below.

Assume that the blacksmith can manufacture iron disks with a thickness of 5mm (this is the manufacturing technology). Thus, we know:

- The density of the material (for iron, this is 7.87 g/cm^3)
- The thickness (5mm in this case).

Side-channel attacks try to obtain additional information based on the physical properties of the implementation in order to reveal they secret key. This information is not available at the algorithm level, since the algorithm does not have any physical properties.

Side-channel attack based on weight: if we have a scale (that is, we have the financial ability to purchase a scale), then we can measure the weight of the disk (that is, the weight of the implementation). Based on weight, and since we know the density and thickness, we can easily calculate the radius.

Example: weight = 23.61 g

Volume = weight / density = 23.61 / 7.87 = 3 cm^3

Area = volume / thickness = 3 / 0.5 = 6 cm^2

Radius = $\sqrt{\frac{\text{area}}{2\,\pi}}$ = 0.96 cm

This is a successful side-channel attack based on weight. Its success is due to the fact that the weight carries information (weight is related to radius).

Possible protection against side-channel attacks based on weight: change the thickness (thus, update the implementation) in such a way that the weight of a disk no longer depends on radius (for example, increase the thickness of small radius disks, and decrease the thickness of large radius disks). Since all possible disks (that is, implementations) have the same weight, we can no longer correlate the weight with the radius. The implementation is now robust against side-channel attacks based on weight.

To summarize:

- Since the circle (that is, the algorithm) lacks physical properties, side-channel attacks are not possible against a circle (that is, against an algorithm).
- A side-channel attack can only be launched against a disk (that is, against an implementation).
- A constant weight is a very good protection against side-channel attacks based on weight (since a constant weight does not carry any information on the radius).

Whereas this example is trivial, it highlights the concepts for a non-technical audience.

Note: For the very large majority implementations of cryptosystems, the most common side-channel attacks are based on power consumption. Thus, making the power consumption constant will eliminate all (present and future) side-channel attacks based on power consumption.