# Privacy

### 20 Feb 2020

#### We are working with a different problem than standard cryptography

In the privacy world, we have to deal with multimedia (or even objects) that can be “faked” and the authenticity, ownership, origin, tracing, of the multimedia/object needs to be able to be verified. There are a couple of situations where this would be different from standard crypto:

1. Situation where we have an image that we want to find if it has been reposted on the internet. Standard cryptographic hashes are sensitive to even the slightest bit change, which would make it impossible to solve the issue of finding images, since any additional noise would cause the hash to register as a new hashed value.

2. Physical objects cannot be traditionally protected in the same way

#### We work with digital watermarking and robust hashing (fingerprinting)

#### Digital Watermarking is the active method of data hiding

In the world of privacy we care about the metadata (who what when where etc) as well as the actual media (content). Digital watermarking is the act of digital data hiding. We are embedding some data (where is a secret) into the media in order to allow us to verify its authenticity, integrity, or some sort of ownership/tracking information.

It is important to note that quality is a major factor, since the goal is not to deteriorate the quality.

In DDH, the assumption is that before distribution, some sort of active method is employed.

#### Fingerprinting is the passive method of evaluating hashes

This allows us flexibility because we’re able to determine that two images could be the same if the hamming distance of their hashes don’t differ by too much. This allows us to have a method of comparison that doesn’t rely on an active method before distribution. However, of course this would not allow us to solve the problem of ownership necessarily.