Ashwin Machanavajjhala et al. presents two attacks on *k*-anonymity, homogeneity attack and background information. An attacker can discover sensitive attributes when the data is not diverse enough. A homogeneity attack leaks information due to the lack of diversity in the sensitive attribute. An attacker may have background knowledge, which can be used to infer knowledge. Ashwin Machanavajjhala et al. proposes Bayes-Optimal and *l*-diversity. Bayes optimal is an algorithm that works under the assumption that the data publisher and adversary know the complete distribution set of sensitive and non-sensitive attributes. *L*-diversity provides privacy without the data publisher knowing how much background information an adversary may have. Although Bayes optimal covers a wider scope, it is not practical in use. It is unlikely that the adversary and data publisher have complete knowledge of all sets of sensitive and non-sensitive attributes.

Each block of quasi-identifier groups, q-blocks, should have the same frequency of sensitive attributes. The frequency of sensitive attributes can protect against knowledge an attacker may know. Ashwin Machanavajjhala et al. proposes 2 versions of *l­­*-diversity, entropy and recursive diversity. Entropy diversity ensures that q-block has well represented groups of sensitive attributes. The more uniform a q-block is, the higher the entropy. Recursive diversity is another algorithm that checks if a sensitive attribute occurs too frequently. Ashwin Machanavajjhala et al. proposes other algorithms to handle non-sensitive attributes, which involve variations of entropy and recursive diversity.