

Discrete Logarithm Primitives

The diagram illustrates the relationship between a general category of cryptographic primitives and specific implementations. On the left, a gray box labeled 'Discrete Logarithm Primitives' has two dashed green lines extending from its right side. The upper line connects to a white box labeled 'Discrete Logarithm Primitives: ElGamal', and the lower line connects to a white box labeled 'Discrete Logarithm Primitives: Diffie-Hellman'. Between these two destination boxes, three header files are listed: 'elgamal.h' at the top, 'dhies.h' in the middle, and 'dlsvdp-dh.h' at the bottom. The 'elgamal.h' header is positioned between the two dashed lines, while 'dhies.h' and 'dlsvdp-dh.h' are positioned below the lower dashed line.

elgamal.h

Discrete Logarithm Primitives: ElGamal

dhies.h

dlsvdp-dh.h

Discrete Logarithm Primitives: Diffie-Hellman