

COMPRESSED ECDSA SIGNATURES

ABSTRACT

An improved compression scheme for compressing an ECDSA signature is provided. The scheme substitutes the integer s in a signature (r, s) by a smaller value c . The value c is derived from s and another value d , d being small enough such that c is smaller than s . The compressed signature (r, c) is verified by computing a value using r and e , e being a hash of a message m , and using this value with a value R recovered from r to derive the value d . The value s can then be recovered and the full signature then recovered and verified.

Figure 1