

Speaking informally, a one-to-one function  $f : X \rightarrow Y$  is “one-way” if it is easy to compute  $f(x)$  for any  $x \in X$  but hard to compute  $f^{-1}(y)$  for most randomly selected  $y$  in the range of  $f$ .

N. Koblitz, A.J. Menezes. 2004. A Survey of Public-Key Cryptosystems. *SIA M Review*, **46**(4): 59–634.