

\*

概論暗号で有用な双線形写像に、楕円曲線上、または超楕円曲線上の Weil  
ペアリング、Tate  
ペアリングなどがある。楕円曲線におけるペアリング演算では、Miller  
Al-  
go-  
rithm  
や dis-  
tor-  
tion  
map  
を用いた