امضای دیجیتال مقاوم کوانتومی بر اساس همسانی های بین خم های سوپرسینگولار

مصطفی قربانی

استاد راهنما: دکتر حسن دقیق

توجه به این نکته لازم است که تساوی زیر برقرار است :

$$(E/\langle S\rangle)/\langle\phi(R)\rangle = E/\langle R,S\rangle = (E/\langle R\rangle)/\langle\psi(S)\rangle$$

$$\begin{array}{ccc} E & \xrightarrow{\phi} & E/\langle S\rangle \\ \downarrow{\scriptstyle\psi} & & \downarrow{\scriptstyle\psi'} \\ E/\langle R\rangle & \xrightarrow{\phi'} & E/\langle R,S\rangle \end{array}$$

شکل ۱: هر فلش با همسانی و و هسته‌اش نشانه گذاری شده است