1135-VN-2792 **Upama Neupane*** (upama.neupane@cameron.edu), **Gokul Raj Kadel** and **Parshuram Budhathoki**. *Polynomial multiplication over binary field and its implementation.* Preliminary report.

Several cryptographic applications require efficient (time and resources wise) finite field arithmetic specifically arithmetic over binary extension field is often used. In comparison to other arithmetic multiplication contributes most to the total number of bit operations. So, the design of algorithms for binary polynomial multiplication has been of great interest to many mathematician and cryptographer. In this project, we will focus on the state-of- the- art for the polynomial multiplication and its implementation in different applications. (Received September 26, 2017)