# Cryptology ePrint Archive: Report 2011/067

### On the Distribution of the Subset Sum Pseudorandom Number Generator on Elliptic Curves

*Simon R. Blackburn, Alina Ostafe and Igor E. Shparlinski*

**Abstract:** Given a prime $p$, an elliptic curve $\mathcal{E}/\mathbb{F}_p$ over the finite field $\mathbb{F}_p$ of $p$ elements and a binary linear recurrence sequence $\(u(n)\)_{n =1}^\infty$ of order~$r$, we study the distribution of the sequence of points $$ \sum_{j=0}^{r-1} u(n+j)P_j, \qquad n =1,\ldots, N, $$ on average over all possible choices of $\mathbb{F}_p$-rational points $P_1,\ldots, P_r$ on $\mathcal{E}$. For a sufficiently large $N$ we improve and generalise a previous result in this direction due to E.~El~Mahassni.

**Category / Keywords:**

**Date:** received 7 Feb 2011

**Contact author:** s blackburn at rhul ac uk

**Available formats:** PDF | BibTeX Citation

**Version:** 20110208:132303 (All versions of this report)

**Discussion forum:** Show discussion | Start new discussion

[ Cryptology ePrint archive ]