

An application of elliptic curves to one-time pad cryptography

Justin Gieseler

Advisors: Dr. Mihai Caragiu and Dr. Ronald Johns

Department of Mathematics, Ohio Northern University



The One-Time Pad
 Gilbert Vernan (AT&T) - U.S. Patent 01310719 (1917).

The only currently known unconditionally secure cryptosystem (contingent on the good randomness properties of the key) - it adds the terms of a "random sequence" to the sequence of terms representing the plaintext.

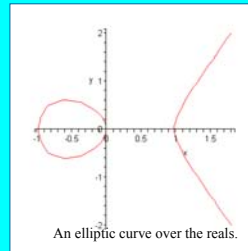
We study the possibility of using patterns obtained by projecting elliptic curves over large finite prime fields onto the x-axis in the design of the one-time pad key

$$E(a,b,p): y^2 = x^3 + ax + b \text{ - elliptic curve over } F_p$$

$$N = \text{the number of points of } E(a,b,p) \text{ over } F_p \Rightarrow |N - p| \leq 2\sqrt{p} \text{ (Hasse)}$$

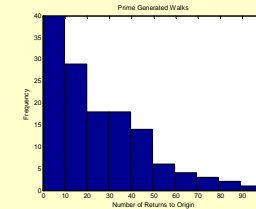
$$X(a,b,p) = \{x \in F_p \mid x^3 + ax + b \text{ is a square}\} \subseteq F_p$$

$$S(a,b,p) = \text{the characteristic function of } X(a,b,p)$$



RESULTS SUPPORTING THE RANDOM CHARACTER OF $S(a,b,p)$:

1. From the point of view of the number of returns to the origin, chi squared tests indicate that at the $\alpha=0.1$ significance level, our elliptic walks cannot be distinguished from truly random walks.



2. The grouping test: a statistical analysis of the integers represented in base 2 by groups of n consecutive bits in $S(a,b,p)$ does not find strong evidence to reject the hypothesis of randomness.

3. Nontrivial incomplete exponential sums over the subsets $X(a,b,p)$ are of the form $o(p)$. Thus the subsets $X(a,b,p)$ are quasi-random [2] according to the "EXP" criterion of Chung and Graham [3].

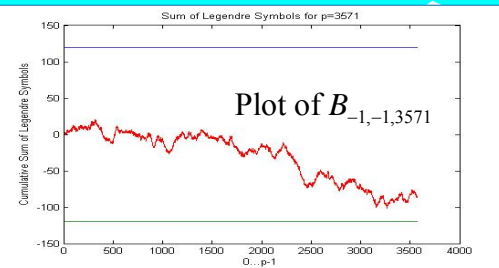
$$\sum_{x \in X(a,b,p)} e^{2\pi i m x / p} = o(p), \quad m = 1, 2, \dots, p-1$$

Important: the randomness properties of the binary sequences $S(a,b,p)$

• Statistical investigation – through associated elliptic walks

$$W_{a,b,p}(k) = \begin{cases} 1, & \text{if } k^3 + ak + b \text{ is a square in } F_p \\ -1, & \text{if } k^3 + ak + b \text{ is a non-square in } F_p \end{cases} \text{ for } k = 1, \dots, p$$

$$B_{a,b,p}(k) = \sum_{j=1}^k W_{a,b,p}(j), \quad B_{a,b,p}(0) = 0$$



• Analytic investigation – through exponential sums

RESULTS INDICATING SUBTLE DEPARTURES FROM RANDOMNESS

1. The endpoints of the complete elliptic walks are constrained to the interval $[-2\sqrt{p}, 2\sqrt{p} + 3]$ while the endpoint of a large genuine random walk of length p is in the interval $[\alpha\sqrt{p}, \beta\sqrt{p}]$ with a probability $(2\pi)^{-1/2} \int_{\alpha}^{\beta} \exp(-x^2/2) dx$

2. The Poly-Vinogradov inequality [1] forces all displacements in the walks $B_{a,b,p}$ to be bounded by a term of the form $O(\sqrt{p} \log p)$

These obstructions can be bypassed by considering smaller sub-walks of length $o(\sqrt{p})$.

CONCLUSION: We find encouraging prospects for using bit strings $S(a,b,p)$ in the design of one-time pad keys.

REFERENCES

[1] Burgess, D. A., On Dirichlet characters of polynomials, Proc. London Math. Soc. (3) 13 1963 537-548
 [2] Caragiu, M, Johns, R.A., Gieseler, J, Quasi-random Structures from Elliptic Curves, JP J. of Algebra, Number Theory and Appl. 6 (2006), 561 – 571
 [3] Chung, F. R. K. and Graham R. L., Quasi-Random Subsets of \mathbb{Z}_n , Journal of Combinatorial Theory, Series A, 61, 64-86, 1992

ACKNOWLEDGEMENTS

• We would like to thank Ohio Northern University's Getty College of Arts and Sciences for supporting the present research;
 • All computations were done using MATLAB or MAPLE.