On Modular Decomposition of Integers

Billy Bob Brumley[1] and Kaisa Nyberg[1,2]

[1] Department of Information and Computer Science,
Helsinki University of Technology,
P.O. Box 5400, FI-02015 TKK, Finland
{billy.brumley,kaisa.nyberg}@tkk.fi
[2] Nokia Research Center, Finland
kaisa.nyberg@nokia.com

Abstract. At Crypto 2001, Gallant et al. showed how to exploit fast endomorphisms on some specific classes of elliptic curves to obtain fast scalar multiplication. The GLV method works by decomposing scalars into two small portions using multiplications, divisions, and rounding operations in the rationals. We present a new simple method based on the extended Euclidean algorithm that uses notably different operations than that of traditional decomposition. We obtain strict bounds on each component. Additionally, we examine the use of random decompositions, useful for key generation or cryptosystems requiring ephemeral keys. Specifically, we provide a complete description of the probability distribution of random decompositions and give bounds for each component in such a way that ensures a concrete level of entropy. This is the first analysis on distribution of random decompositions in GLV allowing the derivation of the entropy and thus an answer to the question first posed by Gallant in 1999.

Keywords: elliptic curve cryptography, GLV method, integer decompositions.

1 Introduction

Elliptic curve cryptography is a field rich with methods to obtain fast implementations. A reasonable choice when high speed ECC is needed is a curve which admits a fast endomorphism. While methods using the Frobenius endomorphism exist, for example Koblitz curves, the classes of curves for which this is useful is somewhat limited.

Gallant, Lambert, and Vanstone [1] showed a novel method of using fast endomorphisms on larger classes of curves. Given a point P of prime order n on a curve that admits a fast endomorphism ϕ, then ϕ acts as on P the multiplication map $[\lambda]$. Given a scalar $k \in \mathbb{Z}_n$, the GLV method works by computing a decomposition $k_1, k_2 \approx \sqrt{n}$ such that $k \equiv k_1 + k_2\lambda \pmod{n}$. The scalar multiplication calculation kP is then carried out as $kP = (k_1 + k_2\lambda)P = k_1P + k_2\phi(P)$ using any number of variations of the Straus-Shamir method [2,3]; the immediate effect is that half of the point doublings are eliminated.

B. Preneel (Ed.): AFRICACRYPT 2009, LNCS 5580, pp. 386–402, 2009.

For further motivation in this area, Galbraith et al. [4] recently showed how to apply the GLV method to larger classes of curves by working in quadratic extension fields to induce a similar type of endomorphism. The work of [4] has produced one of the fastest, if not the fastest known methods for scalar multiplication in software.

A method of obtaining such a scalar decomposition is outlined in [1]. It uses a number of multiplications, divisions, rounding operations, and computations in the rationals. The first contribution we present is a new method for scalar decomposition. The method is based on the extended Euclidean algorithm, and uses very different operations than those carried out in traditional decomposition. The new method is more flexible in the respect that it allows a fairly arbitrary ratio of balance between the size of the components.

Some cryptosystems require only an ephemeral key, such as Diffie-Hellman key agreement or ECDSA signature generation. In these environments as well as key generation, the natural approach is to simply start with a random decomposition. This raises concerns about the distribution of such random decompositions, as first observed by Gallant at ECC'99 [5]. This question remained unanswered.

We answer this question in our second contribution. We first state and prove a theorem which provides a complete description of the distribution of the integers $\kappa\lambda \mod n$ on the interval $[0, n]$. We then present a method for deriving bounds on each portion of the decomposition in such a way that the distribution of the resulting random decompositions can be explicitly calculated, and hence we obtain an exact formula for the achieved entropy. As far as we are aware, this is the first work on to examine this problem for GLV.

We begin in Sec. 2 with a brief overview of elliptic curves and the GLV method using curves with fast endomorphisms. In Sec. 3 we present the new method for scalar decomposition. We study the distribution of random decompositions in Sec. 4 and provide the method for deriving bounds to ensure a certain level of entropy. We conclude in Sec. 5.

2 Preliminaries

As far as speed is concerned, elliptic curves that admit fast endomorphisms allow for significantly faster scalar multiplication compared to random curves. In [1], Gallant et al. showed a novel approach to speeding up scalar multiplication on such curves; while previous methods exploited the Frobenius endomorphism, the novelty of the GLV method was the use of other fast endomorphisms to speed up the operation. We now provide a brief background on the topic.

2.1 Curves with Fast Endomorphisms

We denote E an elliptic curve and $\phi : E \to E$ an endomorphism. For some $P \in E$ we consider the main subgroup $\langle P \rangle$ of prime order n. It follows $\phi(P) \in \langle P \rangle$ and ϕ acts as the multiplication map $[\lambda]$; that is, there exists $\lambda \in \mathbb{Z}_n$ such that $\phi(Q) = \lambda Q$ for all $Q \in \langle P \rangle$. Such a λ is a root of the characteristic polynomial of ϕ modulo n. The following examples are given in [1]; such curves are standardized in [6,7].