Injective Encodings to Elliptic Curves

Pierre-Alain Fouque[1], Antoine Joux[2], and Mehdi Tibouchi[3]

[1] University of Rennes
pierre-alain.fouque@ens.fr
[2] CryptoExperts and Université de Versailles–Saint-Quentin
antoine.joux@m4x.org
[3] NTT Secure Platform Laboratories
tibouchi.mehdi@lab.ntt.co.jp

Abstract. For a number of elliptic curve-based cryptographic protocols, it is useful and sometimes necessary to be able to encode a message (a bit string) as a point on an elliptic curve in such a way that the message can be efficiently and uniquely recovered from the point. This is for example the case if one wants to instantiate CPA-secure ElGamal encryption directly in the group of points of an elliptic curve. More practically relevant settings include Lindell's UC commitment scheme (EUROCRYPT 2011) or structure-preserving primitives.

It turns out that constructing such an encoding function is not easy in general, especially if one wishes to encode points whose length is large relative to the size of the curve. There is a probabilistic, "folklore" method for doing so, but it only provably works for messages of length less than half the size of the curve.

In this paper, we investigate several approaches to injective encoding to elliptic curves, and in particular, we propose a new, essentially optimal geometric construction for a large class of curves, including Edwards curves; the resulting algorithm is also quite efficient, requiring only one exponentiation in the base field and simple arithmetic operations (however, the curves for which the map can be constructed have a point of order two, which may be a limiting factor for possible applications). The new approach is based on the existence of a covering curve of genus 2 for which a bijective encoding is known.

Keywords: Elliptic Curve Cryptography, Injective Encoding, Algebraic Curves.

1 Introduction

Various cryptographic protocols based on the hardness of Diffie-Hellman-like problems in a group $\mathbb{G}$, such as ElGamal encryption [7] or Lindell's recent universally-composable commitment scheme [14], assume the existence of an efficient (possibly randomized) algorithm f mapping messages $m \in \{0,1\}^\ell$ to elements of $\mathbb{G}$, in such a way that m can also be recovered efficiently from $f(m)$.

For example, ElGamal encryption is *a priori* defined on group elements, so that a message needs to be mapped to an element of $\mathbb{G}$ before encrypting it,

C. Boyd and L. Simpson (Eds.): ACISP 2013, LNCS 7959, pp. 203–218, 2013.
© Springer-Verlag Berlin Heidelberg 2013

and mapped back to a bit string upon decryption. Similarly, such a function f is an important ingredient for structure-preserving cryptography [1]: indeed, inputs and outputs of structure-preserving primitives are all group elements; this offers convenient composability properties, but to use e.g. commitments or encryption on actual bit strings, a way to map strings to the group and conversely is required.

Moreover, the size ℓ of supported bit strings should preferably be as close as possible to the bit size of $\mathbb{G}$ to optimize bandwidth. We call such an algorithm f an injective encoding.

For certain groups $\mathbb{G}$, like multiplicative groups of finite fields or some supersingular elliptic curves, it is not difficult to construct injective encodings achieving the optimal value of ℓ. On the other hand, for a general group $\mathbb{G}$, it is not obvious how to construct a function f with ℓ even super-logarithmic in the size of $\mathbb{G}$. In §2.3, we prove that this is not possible with a deterministic generic group algorithm.

When $\mathbb{G}$ is the group of points of any elliptic curve over a finite field, one can construct a probabilistic injective encoding with ℓ equal to about half of the size of $\mathbb{G}$, as we show in §2.4, but we do not know of provable constructions achieving a better ℓ in general. Works on deterministic hashing to elliptic curves, such as [17,11], typically do *not* help addressing this problem, as the functions they construct are not injective, and it is not clear how to find a convenient subset of their domain on which they become injective. Recently, however, a solution was proposed by Farashahi [8] in the special case of Hessian elliptic curves over finite fields $\mathbb{F}_q$ with $q \equiv 2 \pmod 3$.

In §3, we propose an essentially optimal construction for all ordinary elliptic curves over fields $\mathbb{F}_q$ with $q \equiv 3 \pmod 4$ with group order divisible by 4; this includes the well-known Edwards curves studied by Edwards and Bernstein–Lange [2], as well as twisted Huff curves, as studied by Joye et. al. [13]. Our construction is based on the bijective encoding from [10] to certain hyperelliptic curves of genus 2, and on the observation from [12] that those curves are quadratic covers of elliptic curves.

2 Injective Encodings

2.1 Definition

To fix ideas, and although it is not essential for our main purpose, let us first give a formal definition of what we mean by an "injective encoding".

Let us say that a *cyclic group family* $(\mathbb{G}_k)_{k\in\mathbb{N}}$ consists in the data of a sequence of integers $n_k \geq 1$ converging to infinity, a sequence of integers $s_k \geq 0$ that is at most polynomial in $\log n_k$, and for each k, an efficiently computable bijection σ_k between the cyclic group $\mathbb{Z}/n_k\mathbb{Z}$ of order n_k and a set $\mathbb{G}_k \subset \{0,1\}^{s_k}$ of bit strings of length s_k, as well as efficient algorithms:

$$\oplus_k \colon \{0,1\}^{s_k} \times \{0,1\}^{s_k} \to \{0,1\}^{s_k} \cup \{\perp\} \qquad \ominus_k \colon \{0,1\}^{s_k} \to \{0,1\}^{s_k} \cup \{\perp\}$$