Surjective Encodings to (Hyper)Elliptic curves over Finite Fields

Mojtaba Fadavi, Reza Rezaeian Farashahi

Isfahan University of Technology

mfadavi88@gmail.com, farashahi@cc.iut.ac.ir

In this talk, we will propose a general method for constructing surjective encoding function to varieties with special features. Let H be a hyperelliptic curve of genus $g \geq 1$ over an odd characteristic finite field $\mathbb{F}_q$ given by the equation $y^2 = f(x)$. Let $\mathcal{J}$ be the Jacobian variety of H over $\mathbb{F}_q$. We will introduce different deterministic surjective encoding algorithms from $\{0,1\} \times \mathbb{F}_q$ to $H(\mathbb{F}_q)$, where $g = 1, 2$. In particular, if H is an elliptic curve over the finite field $\mathbb{F}_q$ and $\mathfrak{s} : \{0,1\} \times \mathbb{F}_q \to H(\mathbb{F}_q)$ is our proposed surjective encoding function. Then, the random variable $\chi : E(\mathbb{F}_q) \to \mathbb{N}$, where $\chi(P) = \#\mathfrak{s}^{-1}(P)$ for any $P \in E(\mathbb{F}_q)$, has a smaller mean and variance in comparison to the other known encoding functions. In addition, we construct a surjective encoding function from $\{0,1\}^2 \times (\mathbb{F}_q)^2$ to the Jacobian variety of genus 2 hyperelliptic curve H. The idea is extended to higher genus hyperelliptic curves to construct a surjective encoding function $\mathfrak{s} : \{0,1\}^g \times (\mathbb{F}_q)^g \to \mathcal{J}(\mathbb{F}_q)$. The rejection sampling technique may be used to provide a uniform distribution on $\{0,1\}^g \times (\mathbb{F}_q)^g$ from the uniform distribution on $J(\mathbb{F}_q)$.

Let $\psi : \mathbb{F}_q \to H(\mathbb{F}_q)$ be an encoding and consider the function $\mathfrak{f}^{\otimes s} : (\mathbb{F}_q)^s \to \mathcal{J}(\mathbb{F}_q)$ where

$$\mathfrak{f}^{\otimes s}(u_1, \ldots, u_s) = \psi(u_1) + \ldots + \psi(u_s).$$

Farashahi et al. in [1] proved that for $s \geq g+1$, the distribution defined by $\mathfrak{f}^{\otimes s}$ on $J(\mathbb{F}_q)$ is statistically indistinguishable from the uniform distribution if the encoding ψ is well-distributed. For instance, for genus 2 hyperelliptic curves $\mathfrak{f}^{\otimes 3}$ is well-distributed. They also showed that if ψ is a well-distributed encoding, then for $s > 2g$, all divisors $D \in J(\mathbb{F}_q)$ have the same number of pre-images by $\mathfrak{f}^{\otimes s}$ up to negligible deviation, so $\mathfrak{f}^{\otimes s}$ is surjective.

From the surjective encoding function $\mathfrak{s}$, we propose a function $\mathfrak{g}^{\otimes s} : \{0,1\}^g \times (\mathbb{F}_q)^s \to \mathcal{J}(\mathbb{F}_q)$ where

$$\mathfrak{g}^{\otimes s}(i, u_1, \ldots, u_s) = \mathfrak{s}(i, u_1, \ldots, u_g) + \psi(u_{g+1}) + \ldots + \psi(u_s),$$

and $s \geq g+1$. It can be shown that the distribution defined by $\mathfrak{g}^{\otimes s}$ on $J(\mathbb{F}_q)$ is statistically indistinguishable from the uniform distribution assuming ψ is well-distributed.

References

[1] Farashahi, R. R., Fouque, P.-A., Shparlinski, I., Tibouchi, T., Voloch F.: Indifferentiable deterministic hashing to elliptic and hyperelliptic curves. Mathematics of Computation, volume 82, pp. 491–512 (2013)