Duffing Oscillator and Elliptic Curve Cryptography

A. V. Tsiganov

A new approach to exact discretization of the Duffing equation is presented. Integrable discrete maps are obtained by using well-studied operations from the elliptic curve cryptography.

Keywords: integrable maps, divisor arithmetic

1. Introduction

The discretization of dynamical systems in an integrability preserving way has been widely investigated in the last decades. Potentially, it has a great impact in many different areas, such as discrete mathematics, algorithm theory, numerical analysis, statistical mechanics, etc.

The aim of this paper is to discuss exact discretizations of the Duffing equation

$$\ddot{q} + 4Aq + 8Bq^3 = 0,$$  \hspace{1cm} (1.1)

where $q$ denotes the displacement of the system and $A, B$ are real system constant parameters. With the adjective exact we mean the equivalence, at all times and at all orders, of the trajectories of the discrete flow defined by the transformations and of the trajectories of the continuous flow of the model [10, 18, 19].

Duffing equations describe many kinds of nonlinear oscillatory systems in physics, mechanics and engineering [13]. Discussions of the known discretizations of the Duffing equations can be found in [1, 11, 12, 14–18]. In order to obtain new integrable discrete maps, we will make use of standard secret protocols of an elliptic curve cryptography [3, 7].

In the Hamiltonian approach we start with the Hamiltonian function

$$H = p^2 + Aq^2 + Bq^4,$$  \hspace{1cm} (1.2)

which defines the Hamiltonian equations

$$\dot{q} = \frac{\partial H}{\partial p} = 2p, \hspace{1cm} \dot{p} = -\frac{\partial H}{\partial q} = -2Aq - 4Bq^3,$$ \hspace{1cm} (1.3)

The work was supported by the Russian Science Foundation (project 18-11-00032).

Andrey V. Tsiganov
andrey.tsiganov@gmail.com
Saint-Petersburg State University
Universitetskaya nab. 7-9, St. Petersburg, 199034 Russia
associated with (1.1). The corresponding stationary Hamilton–Jacobi equation \( H = E \) at \( q(t) = x \) and \( p(t) = y \) defines an elliptic curve

\[
X: \quad y^2 + Ax^2 + Bx^4 - E = 0. \tag{1.4}
\]

Here \((x, y)\) are the abscissa and the ordinate of a point on the projective plane, which we distinguish from coordinates \((q, p)\) on the phase space. A point \(P = (x, y)\) on \(X\) corresponds to solution of the Hamiltonian equations (1.3) with fixed energy \(E\), time \(t\) and parameters \(A, B\).

In modern elliptic curve cryptography point \((x, y)\) on \(X\) plays the role of a message, which can be coded to a cryptogram \((x', y')\), which is another point, using some cryptographic protocol. It could be protocol based on a divisor arithmetic [7], post quantum protocol based on isogenies [5] and so on. In any case an encrypting operation

\[
\text{message } (x, y) \rightarrow \text{cryptogram } (x', y')
\]

defines a discrete map on the phase space

\[
\text{solution } (q, p) \rightarrow \text{solution } (q', p').
\]

We want to study the properties of such maps for the Duffing equation (1.1).

2. Arithmetic on an elliptic curve

The field of curve-based cryptography has flourished for the last quarter-century after Koblitz and Miller independently proposed the use of elliptic curves in the public-key cryptosystem in the mid-1980s. Since then, elliptic curves over finite fields have been used to implement many cryptographic systems and protocols, such as the Diffie–Hellman key agreement scheme, the elliptic curve variant of the Digital Signature Algorithm, Bitcoin block chain, etc. [3, 4, 7].

Our aim is to apply this efficient machinery in the theory of nonlinear dynamical systems and mappings. One of the main differences is that we use elliptic curves over finite fields in cryptography and elliptic curves over phase space of the given dynamical system. The second important difference is related to final aims. In cryptology we have to guarantee security and speed of computing. In nonlinear dynamical systems theory, we have to study the properties of equations that model the behavior of practical problems that arise in engineering, physics, biology and in many other applications.

We first review the most popular arithmetic formulae for a generic elliptic curve defined by the equation

\[
X: \quad y^2 = a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0.
\]

By adding two points

\[
(x_1, y_1) + (x_2, y_2) = (x_3, y_3)
\]

one gets the third point with the following abscissa and ordinate:

\[
x_3 = -x_1 - x_2 - \frac{2b_0b_2 + b_1^2 - a_2}{2b_1b_2 - a_3}, \quad \text{and} \quad y_3 = -P(x_3), \tag{2.1}
\]

where

\[
P(x) = b_2x^2 + b_1x + b_0 = \sqrt{a_4(x - x_1)(x - x_2)} + \frac{(x - x_2)y_1}{x_1 - x_2} + \frac{(x - x_1)y_2}{x_2 - x_1}.
\]
Points \((x_1, y_1), (x_2, y_2)\) and \((x_3, y_3)\) are the intersection points of the elliptic curve \(X\) and the parabola \(y = P(x)\). This allows us to calculate the second-order polynomial \(P(x)\) by using Lagrange interpolation, see the classical works \([2, 6]\) and modern discussion \([4, 7]\).

Roughly speaking, we can consider points \((x_1, y_1), (x_2, y_2)\) and \((x_3, y_3)\) as message, secret key and cryptogram, respectively. A more punctual and detailed description of various secret systems based on the arithmetic of the elliptic curve points can be found in \([3, 7, 9]\).

Doubling the point

\[
(x_2, y_2) = [2](x_1, y_1)
\]

is an example of the so-called keyless cryptographic algorithm, which gives rise to the cryptogram

\[
x_2 = -2x_1 - \frac{2b_0\sqrt{a_4} + b_1^2 - a_2}{2b_1\sqrt{a_4} - a_3}, \quad \text{and} \quad y_2 = -P(x_2)
\]

(2.2)

directly from the message \((x_1, y_1)\), i.e., without a secret key. The points \((x_1, y_1)\) and \((x_2, y_2)\) are the intersection points of the elliptic curve \(X\) and the parabola \(y = P(x)\), where

\[
P(x) = b_2x^2 + b_1x + b_0 = \sqrt{a_4}(x - x_1)^2 + \frac{(x - x_1)(4a_4x_1^3 + 3a_3x_1^2 + 2a_2x_1 + a_1)}{2y_1} + y_1
\]

is the second-order polynomial obtained now by Hermite interpolation \([4, 6]\).

Tripling the point

\[
(x_2, y_2) = [3](x_1, y_1),
\]

where

\[
x_2 = -3x_1 - \frac{a_3 - 2b_1b_2}{a_4 - b_2^2}, \quad \text{and} \quad y_2 = -P(x_2),
\]

(2.3)

is also related to the quadratic polynomial

\[
P(x) = b_2x^2 + b_1x + b_0 = -\frac{(x - x_1)^2(4a_4x_1^3 + 3a_3x_1^2 + 2a_2x_1 + a_1)^2}{8y_1^2} + \frac{(x - x_1)(x(6a_4x_1^2 + 3a_3x_1 + a_2) - 2a_4x_1^3 + a_2x_1 + a_1)}{2y_1} + y_1.
\]

In a similar manner we can consider quadrupling the point and so on \([3, 7]\).

Of course, we can extract these formulae either from the original works of Euler, Abel and Jacobi or from the classical textbooks on elliptic functions \([2, 6]\). However, it is cryptography as a computational science that has been a driving force behind the arithmetic of algebraic curves and the other parts of algebraic geometry in the past few decades. As a result, in cryptography we have formulae, algorithms and even computer programs prepared for usage \([4, 7–9]\).

2.1. Integrable maps

For the Duffing equation (1.1) the elliptic curve \(X\) (1.4) has an extended Jacobi form and we have to put

\[
a_1 = a_3 = 0, \quad a_4 = -B, \quad a_2 = -A, \quad a_0 = E
\]

into the standard expressions for addition and multiplications on an integer. Solutions \(q(t)\) of the Duffing equation (1.1) are expressed via Jacobi elliptic functions. As an example, for \(B > 0\) and \(A > -B\alpha^2\) the periodic solution of (1.1) reads as

\[
q(t) = \alpha \cn \left(2(A + 2B\alpha^2)^{1/2}t; m\right), \quad m = \frac{\alpha^2B}{A + 2\alpha^2B}.
\]
For $B > 0$ and $-B\alpha^2 < A < -2B\alpha^2$ the periodic solution is

$$q(t) = \alpha \text{dn} \left( 2B^{1/2} t ; m \right), \quad m = 2 \left( 1 + \frac{A}{2\alpha^2} \right).$$

For $B < 0$ and $A > -2B\alpha^2$ the periodic solution has the form

$$q(t) = \alpha \text{sn} \left( 2(A + B\alpha^2)^{1/2} t ; m \right), \quad m = -\frac{\alpha^2 B}{A + \alpha^2 B}.$$ 

Here $\text{cn}(z;m)$ and $\text{sn}(z;m)$ are the Jacobi elliptic functions, see [11, 14, 15].

We can get an exact integrable discretization of the Duffing equation using these explicit solutions and well-known addition theorems for Jacobi elliptic functions, for instance,

$$\text{sn}(X + Y) = \frac{\text{sn}X \text{cn}Y \text{dn}Y + \text{sn}Y \text{cn}X \text{dn}X}{1 - m^2 \text{sn}^2X \text{sn}^2Y},$$

see discussions in [18–20]. However, it is more easy and convenient to apply standard cryptographic algorithms for all the solutions simultaneously.

Let us denote $q_n = q(t_n)$ and $p_n = p(t_n)$, where $t_n$ is time for the $n$th step and $q(t), p(t)$ are solutions of the Hamiltonian equations (1.3). If we substitute coordinates in the phase space instead of coordinates on the plane

$$x_1 = q_n, \quad y_1 = p_n, \quad x_3 = q_{n+1}, \quad y_3 = p_{n+1}$$

and the key on the $n$th step of coding

$$x_2 = \lambda_n, \quad y_2 = \mu_n$$

into (2.1), we get the following discrete map:

$$q_{n+1} = \frac{q_n - \lambda_n}{B(q_n^2 - \lambda_n^2) - \sqrt{-B}(p_n - \mu_n)} \left( \frac{A + (q_n^2 + \lambda_n^2)B}{2} + \frac{\sqrt{-B} (q_n \mu_n - \lambda_n p_n)}{q_n - \lambda_n} + \frac{(p_n - \mu_n)^2}{2(q_n - \lambda_n)^2} \right),$$

$$p_{n+1} = \sqrt{-B}(q_{n+1} - q_n)(q_{n+1} - \lambda_n) + \frac{(q_{n+1} - \lambda_n) p_n}{q_n - \lambda_n} - \frac{(q_{n+1} - q_n) \mu_n}{\lambda_n - q_n},$$

(2.4)

associated with the Duffing equation.

Similarly to [10, 24] we can relate the secret key $(\lambda_n, \mu_n)$ with a discrete time interval $t_{n+1} - t_n$ on the $n$th step of discretization. Because $(\lambda_n, \mu_n)$ is an arbitrary point on the elliptic curve $X$ defined by the Hamilton–Jacobi equation $H = E$, we can consider abscissa $\lambda_n$ as an arbitrary number, but the ordinate is the function of the phase space

$$\mu_n = \sqrt{H - A\lambda_n^2 - B\lambda^4}, \quad H = p_n^2 + Aq_n^2 + Bq_n^4,$$

and this discrete map is generally two-valued. In elliptic curve cryptography over a finite field encrypting is always a single-valued operation.

**Proposition 1.** Mapping (2.4) is a canonical transformation preserving Hamiltonian (1.2)

$$H = p_n^2 + Aq_n^2 + Bq_n^4,$$  

(2.5)

i.e., it is the area-preserving integrable map.
The proof is a straightforward calculation.
For the doubling and tripling we put
\[
x_1 = q_n, \quad y_1 = p_n, \quad x_2 = q_{n+1}, \quad y_2 = p_{n+1}.
\]
In this case, doubling the point on an elliptic curve (2.2) generates a map
\[
q_{n+1} = \frac{2Bq_n^4 + Aq_n^2 + p_n^2}{2\sqrt{-B}q_np_n},
\]
\[
p_{n+1} = \frac{1}{4\sqrt{-B}} \left( 4Bq_n^2 - p_n^2 + \frac{q_n^2(4B^2q_n^4 + 4ABq_n^2 + A^2)}{p_n^2} \right),
\]
whereas tripling the point on an elliptic curve (2.3) gives rise to another map
\[
q_{n+1} = q_n - \frac{4q_np_n^2(2Bq_n^4 + Aq_n^2 + p_n^2)}{4B^2q_n^8 + 4ABq_n^6 + 8B^2q_n^4p_n^2 + A^2q_n^4 + 2Aq_n^2p_n^2 + p_n^4},
\]
\[
p_{n+1} = -p_n + \frac{(q_{n+1} - q_n)(A(q_{n+1} + q_n) + 2B(3q_{n+1} - q_n)q_n^2)}{2p_n} - \frac{2(q_{n+1} - q_n)^2(2Bq_n^3 + Aq_n)}{8p_n^3}.
\]

**Proposition 2.** Mappings (2.6) and (2.7) are canonical transformations of valence two and three, which preserve Hamiltonian (1.2)
\[
H = p_n^2 + Aq_n^2 + Bq_n^4,
\]
i.e., they are integrable maps doubling and tripling the area on a plane.

The proof goes via a direct verification.
For the Bitcoin cryptographic system \((x, y)\) is the generator point, it is publicly known and is the same for everyone, the private key \(N\) is the generator multiplier (an integer) and the public key \((x', y')\) is the point generated by the private key:
\[
(x', y') = [N](x, y).
\]
For integrable maps \((x, y) = (q, p)\) is some solution of the Hamilton–Jacobi equation, \(N\) is a valence of the canonical transformation preserving the Hamilton–Jacobi equation and \((x', y') = (q', p')\) is another solution of the same Hamilton–Jacobi equation.

There are also other secret protocols which are compositions of cryptographic algorithms and instructions. In a similar manner we can consider various combinations of the discrete maps (2.4), (2.6) and (2.7) for the Duffing equation. Any such combination preserves the Hamiltonian (1.2), which allows us to compare such discrete maps with known integrable maps also associated with the Duffing equation.

In the numerical integration of nonlinear differential equations, discretization of the nonlinear terms poses extra ambiguity in reducing the differential equation to a discrete difference equation. For instance, in the framework of the so-called standard-like discretization, the Duffing equation (1.1)
\[
\ddot{q} + 4Aq + 8Bq^3 = 0
\]
can be transformed to the difference equation
\[
\frac{q_{n+1} - 2q_n + q_{n-1}}{h^2} + 4Aq_n + 4B(q_{n+1} + q_{n-1})q_n^2 = 0,
\]
where \( h \) is a discrete time interval. Then we reduce this equation to the standard expression given by Suris [17, 18] with the mapping function \( F(q_n) \)

\[
q_{n+1} - 2q_n + q_{n-1} = F(q_n), \quad F(q_n) = \frac{-4Aq_n - 8Bq_n^3}{h^2 + 4Bq_n^2},
\]

According to [17, 18], the integrability of this second-order difference equation is a sequence of the integrability of the original Duffing equation (1.1). In [11, 12] this difference equation is transformed into a standard expression of a two-dimensional area-preserving map which is integrable, i.e., it admits a nontrivial symmetric invariant integral

\[
\tilde{H} = p_{n+1}^2 + Aq_nq_{n+1} + Bq_n^2q_{n+1}^2,
\]

which was obtained in the more general case in [17, 18].

The discrete maps (2.4), (2.6) and (2.7) preserve the nonsymmetric invariant integral (2.5). This is the main difference between the well-known standard-like discretization and the proposed exact discretizations of the Duffing equation without damping.

### 3. Conclusion

We obtain new integrable discrete maps associated with the Duffing oscillator by using addition, doubling and tripling the points of elliptic curves, which are the standard elements of modern elliptic curve cryptography.

In [21–24] we apply the same algorithms of elliptic and hyperelliptic curve cryptography to study discrete versions of the Lagrange top, Hénon–Heiles system, nonholonomic Veselova and Chaplygin systems, etc. These standard algorithms of hyperelliptic curve cryptography can be also applied to the so-called cubic-quintic Duffing oscillator

\[
\ddot{q} + 4Aq + 8Bq^3 + 12Cq^5 = 0,
\]

which can be found in the modeling of free vibrations of a restrained uniform beam with intermediate lumped mass, the nonlinear dynamics of slender elastica, the generalized Pochhammer–Chree (PC) equation, the generalized compound KdV equation in nonlinear wave systems, etc.

This system is associated with the genus two hyperelliptic curve

\[
X : \quad y^2 - E + Ax^2 + Bx^4 + Cx^6 = 0.
\]

It is the so-called bielliptic curve and, therefore, we have some additional ambiguity to construct explicit and implicit discretizations of the cubic-quintic Duffing oscillator. It can be done using a well-known computer implementation of the fast arithmetic on genus two hyperelliptic curves [8]. It will be also interesting to apply various post-quantum cryptographic algorithms to cubic and cubic-quintic Duffing oscillators.

### References


