Method of Performing Elliptic Polynomial Cryptography with Elliptic Polynomial Hopping

Lahouari Ghouti, Mohammad K. Ibrahim, and Adnan A. Gutub,

Abstract

The method of performing elliptic polynomial cryptography with elliptic polynomial hopping allows for the encryption of messages through elliptic polynomial cryptography, i.e. using elliptic polynomials with multi x-coordinates, and particularly with the utilization of elliptic polynomial hopping based upon both the elliptic polynomial and its twist, regardless of whether the elliptic polynomial and its twist are isomorphic with respect to one another.

Each plaintext block is encrypted by a different elliptic polynomial, and the elliptic polynomials used are selected by an initial secret key and a random number generator. The method is particularly useful for symmetric encryption systems, and provides a block cipher fundamentally based upon a computationally hard problem.

Attributes:

- Submitted to USPTO: USPTO
- Patent Number: US_8385541
- Filing Date: Feb 18, 2010
- Issue Date: Feb 26, 2013
- Title: Method of Performing Elliptic Polynomial Cryptography with Elliptic Polynomial Hopping
- Inventors: Lahouari Ghouti, Mohammad K. Ibrahim, and Adnan A. Gutub

Abstract:

The method of performing elliptic polynomial cryptography with elliptic polynomial hopping allows for the encryption of messages through elliptic polynomial cryptography, i.e. using elliptic polynomials with multiple x-coordinates, and particularly with the utilization of elliptic polynomial hopping based upon both the elliptic polynomial and its twist, regardless of whether the elliptic polynomial and its twist are isomorphic with respect to one another.

Each plaintext block is encrypted by a different elliptic polynomial, and the elliptic polynomials used are selected by an initial secret key and a random number generator. The method is particularly useful for symmetric encryption systems, and provides a block cipher fundamentally based upon a computationally hard problem.

Abstract:

The method of performing elliptic polynomial cryptography with elliptic polynomial hopping allows for the encryption of messages through elliptic polynomial cryptography, i.e. using elliptic polynomials with multiple x-coordinates, and particularly with the utilization of elliptic polynomial hopping based upon both the elliptic polynomial and its twist, regardless of whether the elliptic polynomial and its twist are isomorphic with respect to one another.

Each plaintext block is encrypted by a different elliptic polynomial, and the elliptic polynomials used are selected by an initial secret key and a random number generator. The method is particularly useful for symmetric encryption systems, and provides a block cipher fundamentally based upon a computationally hard problem.

Abstract:

The method of performing elliptic polynomial cryptography with elliptic polynomial hopping allows for the encryption of messages through elliptic polynomial cryptography, i.e. using elliptic polynomials with multiple x-coordinates, and particularly with the utilization of elliptic polynomial hopping based upon both the elliptic polynomial and its twist, regardless of whether the elliptic polynomial and its twist are isomorphic with respect to one another.

Each plaintext block is encrypted by a different elliptic polynomial, and the elliptic polynomials used are selected by an initial secret key and a random number generator. The method is particularly useful for symmetric encryption systems, and provides a block cipher fundamentally based upon a computationally hard problem.

Abstract:

The method of performing elliptic polynomial cryptography with elliptic polynomial hopping allows for the encryption of messages through elliptic polynomial cryptography, i.e. using elliptic polynomials with multiple x-coordinates, and particularly with the utilization of elliptic polynomial hopping based upon both the elliptic polynomial and its twist, regardless of whether the elliptic polynomial and its twist are isomorphic with respect to one another.

Each plaintext block is encrypted by a different elliptic polynomial, and the elliptic polynomials used are selected by an initial secret key and a random number generator. The method is particularly useful for symmetric encryption systems, and provides a block cipher fundamentally based upon a computationally hard problem.

Abstract:

The method of performing elliptic polynomial cryptography with elliptic polynomial hopping allows for the encryption of messages through elliptic polynomial cryptography, i.e. using elliptic polynomials with multiple x-coordinates, and particularly with the utilization of elliptic polynomial hopping based upon both the elliptic polynomial and its twist, regardless of whether the elliptic polynomial and its twist are isomorphic with respect to one another.

Each plaintext block is encrypted by a different elliptic polynomial, and the elliptic polynomials used are selected by an initial secret key and a random number generator. The method is particularly useful for symmetric encryption systems, and provides a block cipher fundamentally based upon a computationally hard problem.

Abstract:

The method of performing elliptic polynomial cryptography with elliptic polynomial hopping allows for the encryption of messages through elliptic polynomial cryptography, i.e. using elliptic polynomials with multiple x-coordinates, and particularly with the utilization of elliptic polynomial hopping based upon both the elliptic polynomial and its twist, regardless of whether the elliptic polynomial and its twist are isomorphic with respect to one another.

Each plaintext block is encrypted by a different elliptic polynomial, and the elliptic polynomials used are selected by an initial secret key and a random number generator. The method is particularly useful for symmetric encryption systems, and provides a block cipher fundamentally based upon a computationally hard problem.

Abstract:

The method of performing elliptic polynomial cryptography with elliptic polynomial hopping allows for the encryption of messages through elliptic polynomial cryptography, i.e. using elliptic polynomials with multiple x-coordinates, and particularly with the utilization of elliptic polynomial hopping based upon both the elliptic polynomial and its twist, regardless of whether the elliptic polynomial and its twist are isomorphic with respect to one another.

Each plaintext block is encrypted by a different elliptic polynomial, and the elliptic polynomials used are selected by an initial secret key and a random number generator. The method is particularly useful for symmetric encryption systems, and provides a block cipher fundamentally based upon a computationally hard problem.

Abstract:

The method of performing elliptic polynomial cryptography with elliptic polynomial hopping allows for the encryption of messages through elliptic polynomial cryptography, i.e. using elliptic polynomials with multiple x-coordinates, and particularly with the utilization of elliptic polynomial hopping based upon both the elliptic polynomial and its twist, regardless of whether the elliptic polynomial and its twist are isomorphic with respect to one another.

Each plaintext block is encrypted by a different elliptic polynomial, and the elliptic polynomials used are selected by an initial secret key and a random number generator. The method is particularly useful for symmetric encryption systems, and provides a block cipher fundamentally based upon a computationally hard problem.

Abstract:

The method of performing elliptic polynomial cryptography with elliptic polynomial hopping allows for the encryption of messages through elliptic polynomial cryptography, i.e. using elliptic polynomials with multiple x-coordinates, and particularly with the utilization of elliptic polynomial hopping based upon both the elliptic polynomial and its twist, regardless of whether the elliptic polynomial and its twist are isomorphic with respect to one another.

Each plaintext block is encrypted by a different elliptic polynomial, and the elliptic polynomials used are selected by an initial secret key and a random number generator. The method is particularly useful for symmetric encryption systems, and provides a block cipher fundamentally based upon a computationally hard problem.