METHOD OF PERFORMING ELLIPTIC POLYNOMIAL CRYPTOGRAPHY WITH ELLIPTIC POLYNOMIAL HOPPING

Inventors: Lahouari Ghoufi, Dharan (SA); Mohammad K. Ibrahim, Leicester (GB); Adnan A. Gutub, Dharan (SA)

Assignee: King Fahd University of Petroleum and Minerals, Dharan (SA)

Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 527 days.

Appl. No.: 12/656,899
Filed: Feb. 18, 2010

Prior Publication Data
US 2011/0200185 A1 Aug. 18, 2011

Int. Cl.
H04L 9/28 (2006.01)
H04L 9/30 (2006.01)
H04K 1/02 (2006.01)

U.S. Cl. .......... 380/30; 380/28; 380/43; 380/46

Field of Classification Search .......... 380/28, 380/30, 43, 46

See application file for complete search history.

References Cited
U.S. PATENT DOCUMENTS
4,668,103 A 5/1987 Wilson
4,995,082 A 2/1991 Schnorr
5,054,066 A 10/1991 Riek et al.
5,146,500 A 9/1992 Maurer
5,150,411 A 9/1992 Maurer
5,272,755 A 12/1993 Miyaji et al.

FOREIGN PATENT DOCUMENTS
EP 0892520 1/1999

OTHER PUBLICATIONS

Primary Examiner — Michael Simitoski
(74) Attorney, Agent, or Firm — Richard C. Litman

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.
METHOD OF PERFORMING ELLIPTIC POLYNOMIAL CRYPTOGRAPHY WITH ELLIPTIC POLYNOMIAL HOPPING

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates to computerized cryptographic methods for communications in a computer network or electronic communications system, and particularly to a method of performing elliptic polynomial cryptography with elliptic polynomial hopping.

2. Description of the Related Art

Encryption systems have been categorized in the art into two types, based on the characteristics of the cryptographic key: asymmetric encryption systems and symmetric encryption systems. Asymmetric encryption systems are also called dual-key systems or public-key systems. In the public-key encryption systems, there is a public key and a private key. The public key is made public, while the private key remains secret. Encryption is performed with the public key, while decryption is done with the private key. The public key and the private key are totally different, and it is difficult to derive one by inference from the other. Thus, the ability to encrypt can be separated from the ability to decrypt.

Symmetric encryption systems are also called single-key systems, private-key systems, or traditional encryption systems. Private-key systems can be categorized into stream encryption systems and block encryption systems. In a stream encryption system, plain data is encrypted on an element-by-element basis (in computer systems, one letter, character, or bit at a time). In contrast, in a block encryption system, plain data is divided into blocks with each block containing plural elements, and encryption is carried out on a block-by-block basis (in computer systems, blocks of letters, characters, or bits at a time).

Block ciphers are the most popular algorithms in use today for providing data privacy. Block ciphers with block size $n$ and key size $k$ can be viewed as a family of permutations on the set of all $n$-bit strings, indexed by $k$-bit long encryption keys and possessing certain properties. Block ciphers use fix-sized blocks. A 128-bit plaintext block will generate a 128-bit ciphertext block when encrypted. If the message is shorter than the block size, the message is padded to bring the block size up to whatever is required by the particular block cipher being used. If the message is longer than the block size, then the message will be encoded using a mode or method designed to make the encrypted message less vulnerable to attack.

From the mid-1970s through the 1990s, the Data Encryption Standard (DES) was probably the most popular and widely used block cipher cryptographic algorithm. DES had a block size of 64 bits and a key size of 56 bits, and implemented a Feistel structure built on a series of exclusive-or (XOR) operations. When the message size exceeded the block size, DES employed one of several modes. The simplest, electronic codebook (ECB), is too vulnerable to attack if the message is too long and has repeating phrases because two blocks of equivalent plaintext characters always encrypt to the same block of ciphertext. Other modes include cipher block chaining (CBC), cipher feedback (CFB), and output feedback (OFB), of which CBC is the most popular. In CBC, each plaintext block is XORed with the previous plaintext block, beginning with an initialization vector for the first block.

Once thought secure, DES has proved vulnerable to attack through increases in the speed and memory storage of computer hardware. It is now possible for an attacker to decrypt a DES encrypted message by an exhaustive key search in a comparatively short amount of time. Although DES, or variations of DES, such as 3DES or Triple DES, is still used, it is being replaced by the Advanced Encryption Standard (AES).

AES uses a 128-bit block size and may use a key size of 128 bits, 192 bits, or 256 bits. The algorithm has a Rijndael structure, which again relies upon a series of XOR operations. Nevertheless, there are concerns about the adequacy of the AES algorithm due to its simple algebraic structure. Moreover, the increase in block size may be inconvenient to implement, is not truly scalable (only three key sizes are implemented or permitted), the hardware for a 192-bit key is not completely compatible with the hardware for a 128-bit or 256-bit key, and advances in computer hardware speed and memory may eventually make AES vulnerable to an exhaustive key search in the same manner as DES.

The fundamental problem with DES, AES, and other similar block cipher algorithms is that these algorithms are essentially based upon simple XOR operations, and not upon a computationally hard or infeasible problem, such as the discrete logarithm problem or the elliptic curve (EC) analog to the discrete logarithm problem.

Elliptic curve cryptosystems are well known in the art. Elliptic curve cryptosystems rely upon the difficulty of the Elliptic Curve Discrete Logarithm Problem (ECDLP) to provide their effectiveness as a cryptosystem. Using multiplicative notation, the problem can be described as: given points $B$ and $Q$ in the group (points in a finite field satisfying a given elliptic curve equation), find a number $k$ such that $B^k = Q$, where $k$ is called the discrete logarithm of $Q$ to the base $B$. Using additive notation, the problem becomes: given two points $B$ and $Q$ in the group, find a number $k$ such that $kB = Q$.

Conventional elliptic curve arithmetic and properties, including point addition, scalar multiplication, point doubling, projective coordinates, etc., are well known in the art, and have been described in numerous texts, treatises, and cryptography handbooks, e.g., Guide to Elliptic Curve Cryptography, Hankerson et al., Springer 2004. A summary of such operations and properties appears in paragraphs [0012] through [0026] of U.S. Pat. No. 7,483,533, issued Jan. 27, 2009, which are hereby incorporated by reference.

Elliptic curve cryptography is gaining increasing acceptance in public-key applications, such as public key exchange, digital signatures, etc., because elliptic curve cryptography permits smaller key size than RSA and other such algorithms, and the difficulty of attacking or solving the EC discrete logarithm problem. However, elliptic curve cryptography is not widely used for symmetric encryption systems, block ciphers, or encryption of long messages.

The difficulty with such applications arises from the process for encrypting a plaintext message using an elliptic curve. In conventional elliptic curve cryptography, conventional bit string embedding into an elliptic curve point involves and iterative algorithm to search for an $x$-coordinate value that will lead to a quadratic residue value of the $y$-coordinate starting from an initial $x$-coordinate value specified by the bit string to be embedded. The process normally requires several iterations, and the number of iterations needed is different for different bit strings that are being embedded. This process incurs considerable overhead in time and in memory storage, since look-up tables are often used.

Also, in conventional elliptic curve cryptography, an elliptic curve polynomial defined over a finite field that needs $N$-bits for representation of its elements, only $(nx+ny+1)N−1$ bits