Cryptography Using Chebyshev Polynomials

Eventually, you will utterly discover a additional experience and success by spending more cash. still when? do you say yes that you require to acquire those all needs behind having significantly cash? Why don't you try to acquire something basic in the beginning? That's something that will lead you to understand even more almost the globe, experience, some places, considering history, amusement, and a lot more?

It is your agreed own get older to behave reviewing habit. among guides you could enjoy now is **cryptography using chebyshev polynomials** below.

The time frame a book is available as a free download is shown on each download page, as well as a full description of the book and sometimes a link to the author's website.

Cryptography Using Chebyshev Polynomials

We consider replacing the monomial xn with the Chebyshev polynomial T n(x) in the Diffie-Hellman and RSA cryptography algorithms. We show that we can generalize the binary powering algorithm to com-pute Chebyshev polynomials, and that the inverse problem of com-puting the degree n, the discrete log problem for T n(x) mod p, is as

Cryptography using Chebyshev polynomials

Based on Chebyshev polynomials, you can create an asymmetric cryptosystem that allows secure communication. Such a cryptosystem uses the fact that these polynomials form a semi-group due to the composition operation. This article presents new cryptosystems that use other than semi-group property dependencies. Based on these dependencies as well as modifications of Chebyshev's polynomials, two cryptosystems have been proposed.

The application of modified Chebyshev polynomials in ...

We consider replacing the monomial xn with the Chebyshev poly-

nomial Tn(x) in the Diffie-Hellman and RSA cryptography algorithms. We show that we can generalize the binary powering algorithm to com-pute Chebyshev polynomials, and that the inverse problem of com-puting the degree n, the discrete log problem for Tn(x) mod p, is as difficult as that for xn mod p. 1

CiteSeerX — B.: Cryptography using Chebyshev polynomials

Lanczos or Chebyshev iteration use Chebyshev polynomials to get O(log(1=)= p gap). I'm not going to explain this one in detail { it is a direct application of jump polynomials, where we scale and shift such that 2goes to 1 and 1goes to 1 + gap.

Chebyshev Polynomials and Approximation Theory in ...

Let n ∈ and x ∈ ; we define Chebyshev polynomial : → as T (x) = . Its semigroup property is as follows: In 2008, Zhang extended to the interval (-∞, +∞). Therefore, we have a different formula of Chebyshev polynomial as follows: where p ∈ , x ∈ and n ∈ℕ. We see that can be changed to. 2.2. The Hard Problems

Improved Chebyshev Polynomials-Based Authentication Scheme ...

When Chebyshev nodes are used, the maximum error is guaranteed to diminish with increasing polynomial order. The Remez Algorithm § The Chebyshev nodes are pretty good as far as minimising approximation error.

Practical Cryptography

New sets of orthogonal functions, which correspond to the first, second, third, and fourth kind Chebyshev polynomials with half-integer indexes, have been recently introduced. In this article, links of these new sets of irrational functions to the third and fourth kind Chebyshev polynomials are highlighted and their connections with the classical Chebyshev polynomials are shown.

The Third and Fourth Kind Pseudo-Chebyshev Polynomials of ...

Chebyshev polynomials based public key cryptosystem (CPPKC), as a kind of chaos based cryptography,,, - key of CPPKC can

guarantee the security even for small integer, so there is no need to look...

Public-Key Encryption Based on Chebyshev Polynomials ...

Clenshaw–Curtis quadrature and Fejér quadrature are methods for numerical integration, or "quadrature", that are based on an expansion of the integrand in terms of Chebyshev polynomials. In numerical analysis, Chebyshev nodes are specific real algebraic numbers, namely the roots of the Chebyshev polynomials of the first kind. One can obtain polynomials very close to the optimal one by ...

Chebyshev polynomials - hyperleap.com

The Chebyshev polynomials are two sequences of polynomials, denoted T n (x) and U n (x).They are defined as follows. By the double angle formula, $= -$ is a polynomial in cos(θ), so define T 2 (x) = 2x 2 − 1.The other T n (x) are defined similarly, using cos(nθ) = T n (cos(θ)).Similarly, define the other sequence by sin(nθ) = U n−1 (cos(θ)) sin(θ), where we have used de ...

Chebyshev polynomials - Wikipedia

The Chebyshev polynomials have the accompanying 2 issues, which are thought to be hard to handle inside polynomial time: Given 2 components and, the assignment of the DL is to find the integer, with the end goal. Given 3 components, and, the assignment of the Diffie-Hellman problem is to calculate the component. 2.3 Security notions

Chebyshev chaotic map-based ID-based cryptographic model ...

These Chebyshev polynomials form an orthogonal basis, which converge faster than expansions in other sets of polynomials , . The Chebyshev functional link artificial neural network (CFLANN) combines the benefits of the Chebyshev polynomials and the FLANN, which is a well-known improvement to solve the nonlinear system identification problem.

Time delay Chebyshev functional link artificial neural ...

Based on such polynomials, a generalization of a recently

proposed public-key encryption algorithm that uses Chebyshev polynomials over prime finite fields is presented. Since our approach uses a finite field trigonometry, it is also possible to analyze some security aspects of the mentioned algorithm in the extension field scenario.

Public-key encryption based on Chebyshev polynomials over ...

Chebyshev polynomials. I. INTRODUCTION The iteration of polynomials and rational functions over finite fields have recently become an active research topic. These dynamical systems have found applications in diverse areas, including cryptography, biology and physics. In cryptography, iterations of functions over finite fields were popularized by the

The Graph Structure of Chebyshev Polynomials over Finite ...

The authors also show that the public key cryptosystems of Kocarev and Tasev based on chaos theory and use Chebyshev polynomials defined over real numbers are insecure. Due to the finite precision...

Public-key encryption based on Chebyshev maps | Request PDF

Abstract We propose public-key encryption algorithms based on Chebyshev polynomials, which are secure, practical, and can be used for both encryption and digital signature. Software implementation and properties of the algorithms are discussed in detail.

Public-Key Encryption Based on Chebyshev Polynomials ...

Algebraic Cryptography Center at Stevens Institute of Technology Vladimir Shpil Vladimir Shpilrain (The City College of CUNY) Cryptography using Chebyshev polynomials Abstract: Chebyshev polynomials T_m(x) and T_n(x) commute for any m and n. We use this fact to contemplate using Chebyshev polynomials in public-key cryptography.

Mathematics of Post-Quantum Cryptography

In, Fu et al. proposed a digital image encryption method by using Chirikov standard map based permutation and Chebyshev polynomial based diffusion operations. In, a bit-level permutation scheme using chaotic sequence sorting has been proposed for image encryption. The operations are completed by Chebyshev polynomial and Arnold Cat map.