Abstract

The Diophantine equations define an algebraic curve or an algebraic surface and ask about lattice points on it. A Diophantine equation may either possess no non trivial solution or finite number of solutions or infinite number of solutions. Therefore, computing lattice points is difficult in general for Diophantine equations of order greater than one. This ambiguity regarding the solutions of a Diophantine equation is another source for trapdoor functions in Public key cryptography. In this paper we analyze the potentiality of Diophantine equations in the key exchange cryptosystem and propose a method for recovering a key in the key exchange cryptosystem by Diophantine equations.

References

- J. Buchmann "Introduction to cryptography", Springer-Verlag 2001
- Neal Koblitz "A course in number theory and cryptography ISBN 3-578071-8, SPIN 10893308"

Index Terms

Computer Science  
Security

Keywords

Key exchange  
Diophantine equations