1020-14-28 **Koichiro Akiyama** and **Yasuhiro Goto*** (ygoto@cc.hokkyodai.ac.jp), Dept of Mathematics, Hokkaido Univ. of Edu. at Hakodate, 1-2 Hachiman-cho, Hakodate, Hokkaido. *Rational points on curves over function fields and an application to cryptography.*

We consider an affine surface over a finite field and its trivial fibration on a line. Such a surface may be regarded as a curve over a function field. The sections of this fibration are rational points on the corresponding curve and they are usually difficult to find explicitly. In this talk, we present a cryptosystem constructed by using the difficulty of finding sections of fibered algebraic surfaces. This system is not based on the prime factorization problem or discrete logarithm problem. We explain its encryption and decryption algorithms and discuss its security. (Received August 27, 2006)