十一、研究計畫中英文摘要：請就本計畫要點作一概述，並依本計畫性質自訂關鍵詞。

（二）計畫英文摘要。（五百字以內）

The rise of ID-based cryptography has led to extensive use of bilinear pairings such as Weil pairing and Tate pairing. Since then, the design of Pairing-based cryptosystems has been an important issue in the cryptography, such as, encryption system, key-agreement protocol, signature scheme and so on. Henceforth, applications utilizing these pairings have played an important role in modern cryptography. In many of these applications, the calculation of these pairings is one of the dominant computational tasks.

However, in the existing Pairing-based cryptosystem, the pairing computing has significant overhead. Therefore, proposing an efficient algorithm for computing bilinear pairing is an important research issue. The first efficient algorithm for computing pairings was proposed by Miller in 1986. Recently, in order to improve efficiency, most researches on pairing computation have been directed at many different aspects. In 2006, Blake et al. proposed three algorithms to improve Miller's algorithm by the *conjugate* of lines [12]. In [52], we modified the first two algorithms to reduce the computational overhead. Soon later, Wu et al. employ our new method to propose an algorithm for computing pairing over the ground field in characteristic 3 [80]. In the passed subject, we had improved [52] in a new method without segmentation algorithm.

In the first subject, we will study the feasibility for employing our new method to the BMX-3 algorithm, and implement this method for pairing computation in the ground field in characteristic 3. Further, we intend to propose an integrated algorithm, which can compute pairing in both cases. Finally, we will prove the correctness and analysis the performance for this algorithm.

In the second subject, we will evaluate the pairing computation overhead for the cryptographic application in wireless network for the devices under the restriction of computation-limited, and design an appropriate pairing computation method by the achievement of our first subject.

Key words: Elliptic curve cryptosystem, Pairing-based cryptosystem, Pairing computation, Miller algorithm, Cryptography.