Study on the Improvement of Exponentiation for Cryptography

詹東興、顏嵩銘

E-mail: 8604571@mail.dyu.edu.tw

ABSTRACT

許多重要的公開金匙密碼系統中, 都使用到模指數運算, 然而此運算 卻極為耗時. 如何提昇指數運算之效能, 可以從兩方面來考量: 因指數運 算實際上即是一連串之乘法運算, 所以要提昇指數運算之效能, 一方面可 從加快乘法運算之速度著手; 另一方面可從減少乘法次數著手, 本文將著 重於後者之研究. 在二 元法中, 乘法運算次數 (不包括平方運算) 等於指數之二進位表示法中位 元值為?" 的個數, 平均為n/2 個, n 為指數之二進位表示法之位元數. 使用正規有號位元表示法 (Canonical signed-digit representation)平 均可將 "非 0位元" 之個數降至n/3 . 傳統之正規符號位元編碼 (Canonical recoding) 為從右到左 (from LSB to MSB)之運算模式, 而 使用有號位元之二元法指數運算法則只適用於從左到右之運算模式 (from MSB to LSB),故造成位元轉換與指數運算不能同步執行的問題. 本文將 提出一個從左到右將二進位表示法轉換為最小權值有號位元表示法之轉換 方式, 雖然其轉換後的結果不是正規有號位元表示法, 然而其權值仍然是 最小. 本文也將針對 諸多重要數位簽章系統所需之計算x^r (底數x為固定常數, 指數r 為亂 數),提出一種擬亂指數運算法則 (Pseudo random exponentiation algorithm).在此演算 法中, 指數r 為一擬亂數 (Pseudo random number),利用事先運算 (Precomputation) 技 術, 可大量降低計算x^r 所需之乘法次數.

Keywords : Exponentiation ; Binary method ; Signed-digit recoding ; Random number generator

Table of Contents