植基於 ElGamal 密碼系統之數位簽章策略

陳正鎔
國防管理學院資訊所助理教授
臺北縣中和市民安街 150 號
jonathan@mis.ndmc.edu.t

孫屏台
萬能技術學院資管系副教授兼系主任
桃園縣中壢市水尾里萬能路 1 號
kuei@a1.im.vit.edu.tw

摘要

Shao 所設計的植基於因數分解與離散對數二個複雜度的數位簽章策略，我們發現攻擊者祇要破解因數分解的難題，而不須破解離散對數難題，即可解出數位簽章者之秘密金匙。本論文架構一個簡易的雙重複雜度的數位簽章策略，所需之訊息傳輸量與訊息驗證量與原始 ElGamal scheme 均相同。

關鍵詞:密碼系統,因數分解,離散對數,秘密金匙,數位簽章策略

1.Introduction

He and Kiesler[4] 結合因數分解[7]與離散對數[2]而設計一個具有雙重複雜度的數位簽章策略，然該理論先後遭到 Harn[3]，Lee and Hwang[6]以及 Tiersma[10]採用不同角度的攻擊，Laih and Kuo[5]引用 hash function 的技巧，成功地設計一個具有雙重複雜度的數位簽章策略，但其方法要求網路上每位使用者配置過多(約 1000 把)的公開與秘密金匙，造成使用者的負擔與計算上的不靈活，誠爲其缺憾；雖然 Chen and Liu[1]彌補 He and Kiesler 方法之弱點，而達到數位簽章同時植基於因數分解與離散對數二個複雜度，不過其訊息傳輸量卻是四個，比起原始 KlGamal 的二個訊息傳輸量，對網路傳輸量的負荷而言，愈發顯得不切實際。

晚近，Shao[9]宣稱其所設計的數位簽章策略亦是結合因數分解與離散對數雙重複雜度，經過我們的研究，發現攻擊者祇要破解因數分解的難題，而不須破解離散對數難題，即可解出簽章者之秘密金匙。此外，本論文重新架構一個簡易的雙重複雜度數位簽章策略，所須之訊息傳輸量僅需二個與 ElGamal 相同，而訊息驗證量亦與 ElGamal 相同，均爲三個指數運算。

本論文寫作是如此的，第二部份介紹 Shao's scheme，攻擊 Shao's scheme 緊接著於第三部份提出，第四部分描述我們的作法，第五部分討論可能攻擊，結論與未來研究方向於最後一部份提出。

2.Shao's scheme[9]

假定 p 爲大質數，$p = 4p_1q_1 + 1$，$p_1 = 2p_2 + 1$，$q_1 = 2q_2 + 1$，其中 p_1、p_2、q_1 與 q_2 亦均爲大質數，g 模 p 之秩(order)爲 p_1q_1，使用者 A 之秘密金匙 x，公開金匙 y 之關係爲

$$y \equiv g^{x^2+x^{-2}} \pmod{p}$$，鑑於 Shao 所提出二個 scheme 相類似，且均適用於我們的攻擊，因此，我們僅介紹第一 scheme，其做法爲：

(i)任選一數 t，計算

$$r \equiv g^{t^2+t^{-2}} \pmod{p} \quad (1)$$

(ii)計算下列式子的s與k，其中k須爲奇數

$$sx + rx^{-1} \equiv mt + kt^{-1} \pmod{p_1 q_1} \quad (2)$$

$$rx + sx^{-1} \equiv kt + mt^{-1} \pmod{p_1 q_1} \quad (3)$$

則訊息m之數位簽章(k、r、s)使得下列式子成立

$$y^{(r^2+s^2)} \equiv r^{m^2+k^2} g^{4(mk-sr)} \pmod{p} \quad (4)$$

3.Attack

定理 1：假定攻擊者 B 能夠破解因數分解之複雜度，祇要收集一筆$sign(m)=(k,r,s)$而不必破解離散對數之複雜度，即可求出x。

證明：令

$$\left[(ms-kr)^2+(mr-ks)^2-(m^2-k^2)^2\right]\left[(ms-kr)(ks-mr)\right]^{-1} \pmod{p_1 q_1} \quad (5)$$

將式子(3)(4)整理成下列式子

$$t \equiv \left[(ms-kr)x+(mr-ks)x^{-1}\right]\left(m^2-k^2\right)^{-1} \pmod{p_1 q_1} \quad (6)$$

$$t^{-1} \equiv \left[(ks-mr)x+(kr-ms)x^{-1}\right]\left(k^2-m^2\right)^{-1} \pmod{p_1 q_1} \quad (7)$$

由於$1 \equiv tt^{-1} \pmod{p_1 q_1}$，因此，將式子(6)、(7)相乘並整理可以得到下列式子

$$x^2 + x^{-2} \equiv a \pmod{p_1 q_1} \quad (8)$$

攻擊者即可解出

$$x^2 \equiv \frac{a \pm \sqrt{a^2-4}}{2} \pmod{p_1 q_1} \quad (9)$$

當然，亦可解出x之值[8] #

Remark：攻擊 Shao's scheme 2，亦可得到相同結果。

4.Proposed scheme

假定p爲大質數，$p = 4p_1q_1 + 1$，$p_1 = 2p_2 + 1$，$q_1 = 2q_2 + 1$，其中p_1、p_2、q_1與q_2亦均爲大質數g模p之秩(order)爲p_1q_1，使用者 A 之秘密金匙x與公開金匙y之關係爲$y \equiv g^{x^2} \pmod{p}$，

本數位簽章之演算法如下：

(i) 任選一數t，計算

$$r \equiv g^{t^2+(h(m))^4(2t)^{-2}} \pmod{p} \quad (10)$$

(ii) 計算

$$s \equiv \left[t+(h(m))^2(2t)^{-1}\right]\left\{rx-\left[t+(h(m))^2(2t)^{-1}\right]\right\}^{-1} \pmod{p_1 q_1} \quad (11)$$

(iii) 訊息m之數位簽章$sign(m)=(r,s)$將使得下列驗證式子成立

$$y^{r^2s^2} \equiv r^{(s+1)^2} g^{(h(m))^2(s+1)^2} \pmod{p} \quad (12)$$

5.Discussion

我們討論攻擊者 B 試圖於式子(10)—(12)得到線索而進行三種可能攻擊

5.1 從式子(10)解出t

將式子(10)整理成下列式子

$$r \equiv g^{\left[t+(h(m))^2(2t)^{-1}\right]^2-(h(m))^2} \pmod{p}$$

根據 Shao's corollary[9]，要解出t等同於須同時破解因數分解與離散對數雙重困難度。

5.2 從式子(11)解出x、t或僞造任意訊息m'而求出對應的s'。

在式子(11)中，有二個未知數x與t，因此無法解出x與t，由於不知x、t，因此，亦無法由式子(11)僞造(m', s')使得式子(11)成立。

5.3 從式子(12)僞造另一份數位簽章$sign(m)=(r,s)$

(i)任選m、r，找出對應的s。

在式子(12)中，有$y^{r^2s^2}$、$r^{(s+1)^2}$、$g^{(h(m))^2(s+1)^2}$三項與s有關，因此，要解出s至少必須同時破解因數分解與離散對數的複雜度。

(ii)任選m、s，找出對應的r。

在式子(12)中，有$y^{r^2s^2}$、$r^{(s+1)^2}$二項與r有關，要解出對應的r，其難度比同時破解因數分解與離散對數還難[9]。

(iii)任選 r 、 s ，找出對應的 m 。

在式子(12)中，僅有 $g^{(h(m))^2(s+1)^2}$ 一項與 m 有關，因此，祇要同時破解因數分解、離散對數與赫序函數(hash function)，可以解出 m 。不過，縱使此種攻擊得逞，其所產生之 m 並非攻擊者 B 所能控制，如果所選取的質數 p 夠大的話，該僞造的訊息 m 將形成沒有意義的亂數的可能性是很大的。

6.Conclusion

祇要能破解因數分解之複雜度，在Known signature attack 情景下，攻擊者並不需要破解離散對數之複雜度，即可解出簽章者(亦即被攻擊者)之秘密金匙。因此，Shao's scheme 並無法到達其所宣稱的結合因數分解與離散對數雙重複雜度的數位簽章效果。

原始 ElGamel scheme，簽章者於形成數位簽章過程中，須進一個指數與一個乘法反元素運算，本方法則須一個指數與二個乘法反元素運算，僅多了一個乘法反元素運算，在簽章驗證之計算量與訊息傳輸之網路負荷量方面，本方法與 ElGamel scheme 相同，但是本方法結合因數分解與離散對數雙重複雜度，而大大提昇原始 ElGamel scheme 的安全度。(我們省略討論加法與乘法之運算)。

此外，採用 ElGamel scheme，其所選取的 k 值每次必須不同，以避免可能遭受的攻擊[2,4]，對簽章者而言，毋寧是一種負擔，我們的方法則無此顧慮，簽章者縱使於式子(10)中所選取的 t 值相同(我們建議最好還是避免)，由於訊息 m 亦混合於其中，因此，其所產生的 r 值(請參考式子(10))對攻擊者而言，仍無法判定是否出自同一個 t 值，就此點而言，我們的方法比 ElGamal 更具實用性，在未來研究方向上，我們建議以下三個思考方向：

1. 破解本方法。
2. 設計一個更安全且計算簡易的數位簽章策略。
3. 以本方法爲基礎，強化 Blind digital signature 以及 Threshold scheme 的安全度。

References

[1]J.J.-R.chen,and Y.Liu, "An Enhanced ElGamal Scheme with Respect to the Tiersma Attack, "ICS'98 Workshop on Algorithm,1998,pp.150-156.

[2] T. ElGamal, "A Public key Cryptosystem and a Signature Scheme Based on Discrete Logarithms, "IEEE Trans. on Information Theory,Vol.IT-31, No. 4, 1985,pp.637-647.

[3] L.Harn, "Enhancing the Security of ElGamal's signature Scheme," IEE Proc.-comput. Digit.Tech., Vol.142,No5,1995,p.376.

[4] J.He,and T.Kiesler, "Enhancing the Security of El Gamal's signature Scheme," IEE Proc.-Comput.Digit.Tech.,Vol.141,No.4,1994,pp.249-252.

[5] C.S.Laih,and W.C.Kuo, "New Signature Schemes Based on Factoring and Discrete Logarithms,"IEICE Trans.Fundamentals, Vol.E80-A,No.1,1997,pp.

[6] N-Y. Lee, and T. Hwang, "The Security of He and Kiesler's Signature Schemes,"

IEE Proc.-Comput.
Digit.Tech.,Vol.142,No.5,1995,pp.370-37
2.

[7] R.L.Rivest,A.Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystem," Commun ACM, Vol.21,No.2, 1978,pp. 120-126.

[8] K.H.Rosen, Elementary Number Theory and Its Applications, Addison-Wesley Publishing company,U.S.A.,1992.

[9] Z. Shao, "Signature Schemes Based on Factoring and Discrete Logarithms," IEE Proc.-Comput. Digit. Tech., Vol.145,No.1,1998,pp.33-36.

[10] H.J.Tiersma, "Enhancing the Security of ElGamal Signature Scheme : Technical Note," IEE Proc.-Comput. Digit.Tech.,Vol.144,No.1,1997,pp.47-48.