失敗停止策略應用於資訊安全之研究

Fail Stop Scheme Applied to Information Security Research

陳正鎔
Jonathan Jen-Rong Chen
萬能科技大學
資訊管理系
助理教授
jonathan@mail.vnu.edu.tw

高楷璇
Kae-Shuan Kao
德明財經科技大學
財稅系
助理教授
gary@takming.edu.tw

黃永信
Huang Yung Hsin
方曙中學教務處

摘　　要

近四十年來，密碼界所設計之數位簽章大抵隱含了一個「攻擊者與被攻擊者相互擁有同樣之電腦資訊設備」之假設。就電子商務資訊安全運作之實作而言，此等迷失包含了一個危險，即攻擊者如果擁有很強大之計算功能，而被攻擊者之電腦設備顯得相對基礎時，則攻擊者以其所破解被攻擊者的密碼而冒用其身分對外行文，如此一來，整個電子商務環境恐有人人自危之憂。為免於此威脅，本論文提出一個失敗停止策略應用於資訊安全之研究，該策略之實作可適用於電子商務資通安全環境，提供使用者一個可以避免被攻擊之研究架構。

關鍵詞：數位簽章、失敗停止策略、密碼學、電子商務、資訊安全

ABSTRACT

In recent four decades, digital signature assumes “both attacker and defender share the same computer capability.” A potential risk of “the existence of a significant gap between offense and defense” goes along with this myth. It is imperative for any user to be free from the risk of being attacked by the mail from a forger in the name of a decrypted user from the point of information security view. Our FSS (fail-stop-scheme) is designed to solve this problem and provides a safer framework for e-commerce to be free from any possible attacks.

Key Word：Digital Signature, Fail-stop-scheme, Cryptography, E-commerce, Information Security

1、前言

人類使用密碼保護重要資訊已有千年的歷史，而密碼系統所隱含的文明表徵，除了智力上的較勁外，更是一種與時間賽跑的競賽。現代密碼學的應用，涵括舉凡軍事、商業、科技、生活應用等...層面廣泛，不勝枚舉。以近來應用最多的電子商務為例，其中的商務通訊、金流交換、文件傳遞或如網路銀行、線上購物、虛擬書店等商業模式，皆不難窺見密碼學的保護大傘，置身其中；而今，越來越多的網路應用，伴隨著日益猖獗的網路犯罪事件，更加深了我們對於密碼學的重視。

密碼學上援引的假定多是以該密碼演算法遭破解的時間長度來衡量其強度；假定攻擊者的運算能力與被攻擊者相當時，若破解密碼的所需的時間越長，則演算法強度越高，反之亦然。傳統之數位簽章大抵隱含了一個「攻擊者與被攻擊者相互擁有同樣之電腦資訊設備」之假設，但在電子商務環境卻是「道高一尺，魔高一丈」，倘若存在了一個擁有超強運算能力超級電腦的犯罪集團，可以於短時間內攻擊破解了密碼保護，並假冒其系統使用者身份進行金融或商業竊取，此時不但造成被假冒者的信用損害及交易端實際的財物損失，同時更牽累造成其他廣大使用者的不便，其影響及損失更是難以估算，此時，被攻擊者或被假冒者必須有能力證明自己的清白，系統業主亦必須有能力保證其系統安全性及其使用者權益不受影響，才能恢復正常的商業活動。面對上述困境，2004年德國學者Katja Schmidt-Samoa又提出了2000年的改良版本[7]，其採用植基於因式分解困難度的Fail-Stop簽章策略[1,4]，雖然能證明被偽冒者的清白，卻也同時暴露了$n = p \times q$秘密[3,17]；整個系統為了要正常繼續運作，就必須重建或更換系統參數，不但影響了整個系統的運作，也造成系統業主的信用危機。

此際值得探討的是，如何可以在不揭露$n = p \times q$秘密的同時，證明被偽冒者的清白，此外，也必須防範攻擊者惡意的否認行為。鑑此，我們提出一種嶄新的失敗停止策略，其內容綱要如下：第二部份為文獻探討；我們提出的簽章策略置於第三部份；第四部份提出本簽章演算法的安全性分析；結論及未來研究方向於篇末表述。

2、文獻探討

系統中心選取一個滿足下列式子的大質數p_1，$n \mid p_1 - 1$。其中n為二個大質數p、q之乘積，系統中心2再選取模(modulo)p_1其序(order)為p之一數g，即

$$g^{\frac{1}{2}p} \equiv -1 (\mathrm{mod}\ p_1) \quad \cdots\cdots\cdots\cdots\cdots\cdots (1)$$

系統中心之公開金匙為p_1、g、n，而秘密金匙為p、q[12,13,18]

2.1 註冊階段

使用者 A 選取二個相異數x_1、$x_2 \in z_n^*$，計算

$$y_i \equiv g^{x_i} (\mathrm{mod}\ p_1), \quad 1 \le i \le 2 \quad \cdots\cdots\cdots\cdots\cdots\cdots (2)$$

使用者 A 持$\{y_1, y_2\}$向系統中心註冊，使用者A之公開金匙為y_i，而x_i為其秘密金匙，其p　$1 \le i \le 2$。

2.2 簽章階段

假定使用者A欲將訊息m傳輸予使用者B，其數位簽章之計算為

$$m_1 \equiv m x_1 + x_2 (\mathrm{mod}\ n) \quad \cdots\cdots\cdots\cdots (3)$$

則$\{m_1\}$為訊息m之數位簽章

2.3 驗證階段

使用者 B 驗證下列式子

$g^{m_{11}} \equiv y_1^m y_2 (\bmod p_1)$ ……(4)

如果上列式子成立，則接受訊息 m，否則，拒絕接受。

2.4 爭議排除階段

使用者 B 持 $\{m_2\}$ 要求使用者 A 承認其對訊息 m 之數位簽章，使用者 A 計算

$m_1 \equiv mx_1 + x_2 (\bmod n)$ ，

$GCD(m, -m_2, n)$ ， /*Remark ： $GCD(a_1, a_2)$ 表示 a_1, a_2 二數之最大公因數*/，使用者 A 可將合成數 n 予以因數分解，因此，可澄清數位簽章 $\{m_2\}$ 並非其所簽署[2, 8, 9, 10]。流程詳見圖 1

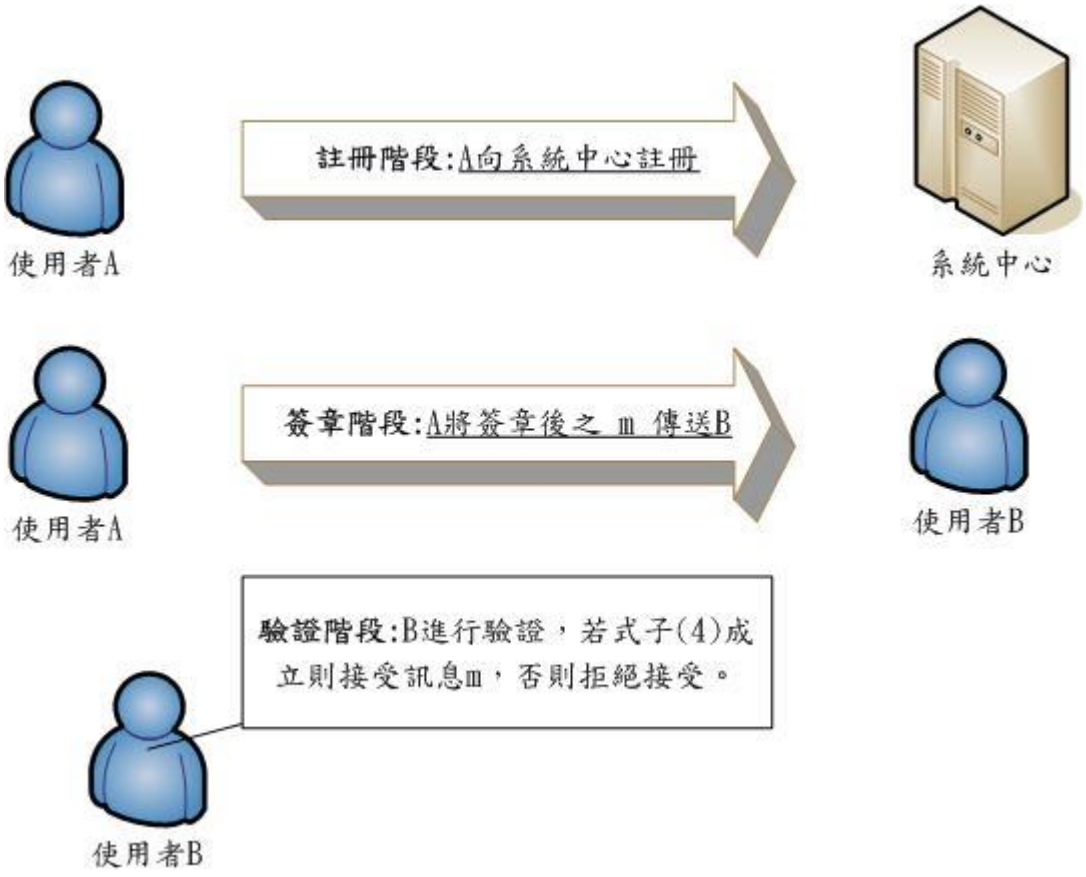

圖 1：傳統運作流程

3、我們的做法

系統中心所產生之公開與秘密金匙，均與前一節（文獻探討）所設計相同，但是我們於本節中，系統中心增加選取模（modulo） p_1 其序（order）為 n 之一數 g_1，亦為其公開金匙，即 $g_1^{\frac{n}{4}} \equiv -1 (\bmod p_1)$，所提出二個版本之註冊階段均與前一節（文獻探討）之註冊階段相同，我們省略表達。

3.1 註冊階段(同，省略)

3.2 簽章階段

假定使用者 A 欲將對訊息 m 予以數位簽章，然後傳送給使用者 B，其演算步驟如下：

（1） 計算

$a \equiv mx_1 - x_2 (\bmod n)$ ……(5)

$$s_1 \equiv g^a \pmod{p_1} \quad \cdots\cdots\cdots\cdots(6)$$

$$s_2 \equiv g_1^a \pmod{p_1} \quad \cdots\cdots\cdots\cdots(7)$$

（2） 選取相異三數 $k_i \in z_m^*$，$1 \le i \le 3$，計算

$$r_1 \equiv g^{k_1} \pmod{p_1} \quad \cdots\cdots\cdots\cdots(8)$$

$$r_2 \equiv g_1^{k_2} \pmod{p_1} \quad \cdots\cdots\cdots\cdots(9)$$

$$s_1 \equiv ar_1 - k_1 b_1 \pmod{n} \quad \cdots\cdots\cdots\cdots(10)$$

$$s_2 \equiv ar_2 - k_2 b_2 \pmod{n} \quad \cdots\cdots\cdots\cdots(11)$$

（3） 將 $\{r_i, b_i, s_j\}$ 傳送給使用者 B，$1 \le i \le 3$，$1 \le j \le 2$

3.3 驗證階段

使用者 B 收到相關訊息之後，計算

$$s_1 \equiv y_1^m / y_2 \pmod{p_1} \quad \cdots\cdots\cdots\cdots(12)$$

$$g^{s_1} \equiv s_1^{r_1} / r_1^{b_1} \pmod{p_1} \quad \cdots\cdots\cdots\cdots(13)$$

$$g_1^{s_2} \equiv s_2^{r_2} / r_2^{b_2} \pmod{p_1} \quad \cdots\cdots\cdots\cdots(14)$$

如果上述式子均成立，則接受訊息 m，否則拒絕接受。

3.4 爭議排除階段

使用者A收到使用者B所傳送被偽冒之訊息 $\{r_i', b_i', s_j'\}$，$1 \le i \le 3$，$1 \le j \le 2$。使用者 A 重複本小節簽章階段之演算步驟，然後使用者 B 重複本小節驗證階段之演算步驟，存在 $(1-q^{-1})$ 之機率，使得 $s_1 \ne s_2' \pmod{n}$，因此，可還原使用者 A 之無辜。流程詳見圖 2

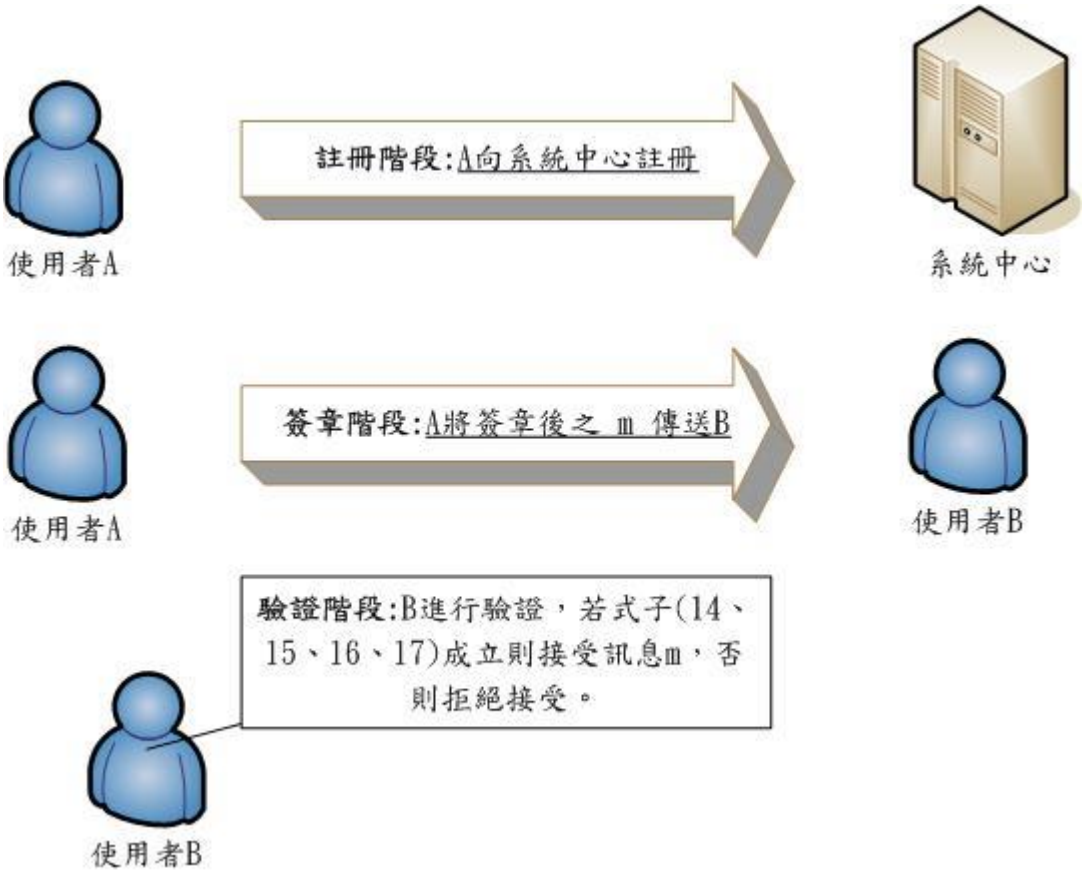

圖 2：我們的作法運作流程

4、安全性分析

引理一：假定有三數 $w_l \in z_m^*$，$1 \le l \le 3$，其中 w_i, w_j 之數已知，另一數 w_k 未知，且滿足下列條件

$$w_i \neq w_j (\mathrm{mod}\, n)$$

$$t_1 \equiv g^{w_1} (\mathrm{mod}\, p_1)$$
$$t_2 \equiv g_1^{w_2} (\mathrm{mod}\, p_1)$$
$$t_1 t_2 \equiv (g g_1)^{w_3} (\mathrm{mod}\, p_1)$$
$$=>(1)\ w_k \neq w_i (\mathrm{mod}\, n)$$

(2) $w_k \neq w_j (\mathrm{mod}\, n)$

(3) 解 w_k 之複雜度最少是求解離散對數問題之複雜度

證明：

請參考[Chen and Liu]之引理一、引理四.[11]，我們省略討論

引理二：式子(13)成立

證明：

$$g^{s_1} \equiv g^{a r_1} g^{k_1 b_1} (\mathrm{mod}\, p_1)$$ 得式子(10)取 g 為底

$$\equiv s_1^{r_1} r_1^{b_1} (\mathrm{mod}\, p_1)$$ 依據式子(6)、(8)

∴我們得到證明 Q.F.D.

式子(12)、(14)之證明如同式子(13)之證明，我們省略討論。

定理一：$s_2 \neq s_2^{'} (\mathrm{mod}\, n)$ 成立之機率為 $(1-\frac{1}{q})$

證明：參考引理一、引理二，我們知道使用者 A 於簽章階段所使用之 a 一致，而攻擊者 I 於簽章階段所使用之 $a^{'}$ 亦一致，如同[Sebrry]之論文[15]所言，我們知 $a^{'} \equiv a + lp (\mathrm{mod}\, n), 0 \le l < q-1$，亦即 $a^{'} \equiv a (\mathrm{mod}\, n)$ 之機率為 $\frac{1}{q}$，依據式子(7)，其所產生知 s_2 與 $s_2^{'}$ 相等之機率亦為 $\frac{1}{q}$，因此，我們得到證明。 .

由前所述，版本一所提演算法成立，然該版本於爭議排除階段，設若攻擊者 I 攔截使用者 A 於式子(7)之 s_2，則攻擊者 I 可計算出 a 值，如果使用者 A 於爭議排除階段後不更換其秘密金匙 x_1 或 x_2 及其所對應之公開金匙 y_1 或 y_2（參考式子(2)），則下次使用者 A 欲對訊息 m，發出數位簽章如下列部分式子

$$a_1 \equiv m_1 x_1 - x_2 (\mathrm{mod}\, n)$$
(5.1)

$$s_2^{'''} \equiv g_1^{a_1} (\mathrm{mod}\, p_1) \qquad (7.1)$$

攻擊者 I 整理上列二式以及式子(5)，可解出 x_1, x_2，攻擊者 I 再將版本一之簽章階段之第(3)步驟予以截收並扣留相關資料，然後偽造任意訊息 m_2 予任意接收者 $B^{'}$，日後，恐怕使用者 A 將無法還原其清白。

有鑑於此，使用者 A 如何於爭議排除階段，還原其清白之後，不必更換其秘密與公開金匙[5,16]，乃為本研究主要精髓所在。

5、結論與未來研究方向

我們提出了一種失敗停止策略應用於資訊安全之研究，可以在不揭露 $n = p \times q$ 秘密的同時，證明被偽冒者的清白，也防範了攻擊者的惡意否認行為。在電子商務活動日益頻繁的網路世代，如何改善現行保護機制，建立一個有保障且安全的市場秩序，一直是產官學界戮力追求的終極目標。在此，我們的簽章策略對於維持電子商務交易活動環節的秩序，提供了一定程度的支持，是本簽章最大的特色。至於未來的研究方向，我們提出以下幾點建議：

1. 推翻或強化本策略或將本策降低所需之計

算時間或參數。

2. 研擬新的可應用於資訊安全實務之失敗停止策略

參考文獻

[1] N.Bari'c and B. Pfitzmann. Collision-free accumulators and fail-stop signatures without trees.advances in Cryptology – Eurocrypt '97, Lecture Notes in Computer Science 1233, pages 480-494, 1997.

[2] Dan Boneh, Glenn Durfee, and Nick Howgrave-Graham. Factoring N = prq for large r. In Advances in Cryptology - CRYPTO 99, volume 1666 of Lecture Notes in Computer Science, pages 326–337, Berlin, 1999.

[3] W. Diffie and M. Hellman. New directions in cryptography. IEEE IT, 22:644-654, 1976.

[4] T. ELGamal, A public-key cryptosystem and a signature scheme based on discrete logarithms, IEEE Trans. On Information Theory II-31 (4), 469-472, 1985.

[5] Katja Schmidt-Samoa. Factorization-based Fail-Stop Signatures Revisited. In: Information and Communications Security (ICICS 2004), LNCS 3269, pp. 118-131. Springer-Verlag, 2004.

[6] C.-S. Laih and W.-C. kuo, New signature schemes based on factoring and discrete logarithms, IEICE Trans. Fundamentals E80-A, 46-53, 1997.

[7] A.K. Lenstra and H.W. Lenstra, Jr., editors. The Development of the Number Field Sieve, volume 1554 of Lecture Notes in Mathematics. Springer-Verlag, 1993.

[8] I. Niven, H.S. Zuckerman and H.L. Montgomery, An Introduction to the Theory of Numbers, John Wiley and Sons, 1991.

[9] J.J.R. Chen and Y. Liu , A Traceable Group Signature Scheme, Mathematical and Computer Modelling 31, 147-160, 2000.

[10] M.O. Rabin, Digitalized signatures and public-key functions as intractable as factorization, Technical Report LCS/TR 212, MIT, Cambridge, MA, 1979.

[11] R.L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. Comm. Of the ACM, 21, no. 2:120-126, 1978.

[12] D. R. Stinson. Cryptography: Theory and Practice. CRC Press, Boca Raton, New York, 1995.

[13] Willy Susilo, Rei Safavi-Naini, Marc Gysin, and Jennifer Seberry. A new and efficient fail-stop signature scheme. The Computer Journal, 43(5):430–437, 2000.

[14] Tatsuaki Okamoto and Shigenori Uchiyama. A new public-key cryptosystem as secure as factoring. In Advances in Cryptology - EUROCRYPT 98, volume 1403 of Lecture Notes in Computer Science, pages 308–317, Berlin, 1998.

[15] Torben Pryds Pedersen and Birgit Pfitzmann**,** Special digital signature schemes based on GOST R 34.10-2012. 2016 IEEE NW Russia Young Researchers in Electrical and Electronic Engineering Conference (EIConRusNW), 135-140. 2016.

Read More: http://epubs.siam.org/doi/abs/10.1137/S0097539793245577X

[16] Torben Pryds Pedersen and Birgit Pfitzmann**,** Fail-Stop Signatures for Multiple-Signers: Definitions, Constructions, and Their Extensions.

Journal of Information Processing **24**, 275-291. 2016.

[17] Tsuyoshi Takagi. A fast RSA-type public-key primitive modulo pkq using hensel lifting. IEICE Transactions, Vol.E87-A(1):94–101, 2004.