網路半匿名系統安全機制之研究

A study for network report security mechanism

陳正鎔 Jonathan Jen-rong Chen 萬能科大資訊管理系所助理教授
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

許紘愷 Hung Kai Hsu 萬能科大資訊管理研究所

barsoul780528@gmail.com

摘　要

傳統報案系統係檢舉人親向治安單位舉報，之後演進至網路報案，有鑑於民間對於治安維護趨弱之隱憂，而國內報案系統隱藏著報案者擔心其身分曝光之風險，降低其報案之意願；治安單位顧慮匿名報案者藉機亂報案或誣陷他人。世界各國情治單位面臨此兩難問題，大抵束手無策。本研究結合雲端運算可突破前述技術瓶頸，以群體數位簽章(Group Signature)之資訊安全學理為基礎，結合我國特有之文化背景。本研究營造國內優質之報案系統，除可排除各國情治單位面臨該兩難問題，並可為企業資源規劃產業中之資訊安全起了一個具本土特色之優質保護檢舉人系統與服務，或可為我國治安獻上綿薄之力。

關鍵詞：企業資源規劃、網路報案，盲目數位簽章，安全機制，雲端運算。

Abstract

Traditional report system is that informant reports to security unit personally, and then it evolution to network report. Considering to the hidden worry of weaker maintenance of law and order, Domestic report system hided that reporter will cut down his intension of report, because he worried about the risk of his identity being revealed. It is almost helpless that the security units of all countries of this world faced this dilemma. The paper with cloud computing can surmount technological bottleneck mentioned above based on the theory of group signature and combined with our country’s unique cultural background. Our proposed scheme which created excellent domestic network report system, not only exclude this dilemma faced by security unit of every country, but also establish an excellent service and system with local characteristic which can protect reporter, maybe contribute a little bit of effort to social security.

Key words：ERP, Network Report, Blind Digital Signature, Mechanism, Cloud Computing..

1. 前言

傳統報案系統係檢舉人親向治安單位舉報，之後演進至網路報案，然觀諸網路報案系統(以內政部警政署刑事警察局為例)，其於網頁上有云：「如欲報案，歡迎您使用 110 或前往鄰近警察局單位報案，製作報案筆錄。依據刑事訴訟法規定，告訴、告發應以書面或言詞向檢察官或司法官為之，執行上必須確認報案人身分，因此，無法於網路上完成正式報案程序，造成您的不便，敬請見諒。」有鑑於民間對於治安維護趨弱之隱憂，而國內報案系統隱藏著報案者擔心其身分曝光之風險，降低其報案之意願；治安單位顧慮匿名報案者藉機亂報案或誣陷他人。世界各國情治單位面臨此兩難問題，大抵束手無策。

網際網路（Internet）的興起，開拓了人類的新視野；傳統注重人與人面對面的交易，隨著資訊網路安全技術的研發，而不斷受到網路跳脫時間、空間交易之挑戰。其中，網路報案【1～3、8～10、18】即是近年來學者與業界熱衷研究方向之一。有關「網路報案」之論文【2、3】，其在基層治安單位不小心洩漏檢舉人個資、檢舉內容曝光、檢舉人之保護等似乎少有著墨；Frankin and Reiter【8、9、18】於檢舉者證明自己是檢舉者者身份認定等問題有其瓶頸，且其採用機密共享理論【18】必須有（3a＋1）個以上參與秘密的監督者【8、9】以集體驗證所收到訊息的可信度。於此架構之下，如果有 a 個監督者驗證不成功；及至少（a＋1）個監督者檢驗順利，方可符合其所宣稱之競標機制。過多的參與秘密監督者，增加資訊系統之負荷，恐不易於網路上之實作。

H.Nurmi【10】則提出一個較為有趣的研究方向；網路檢舉者之間，於相互不洩露其身分的前題之下，彼此均能驗證對方之合法身分，然後接受其檢舉內容。。此一方法雖具創意，但是每一位網路檢舉者必須事先得知其網路公開金鑰(Public Key)，對參與檢舉者身份之私密性未能提供保障，且在相互驗證身分的過程中，過多的參數傳送與冗長的計算，於網路實作方面，或將有令人怯步之疑。

此外，Fan & Lei【7】應用 Chaum【6】不可追蹤電子郵件之技巧，結合因數分解【11、13、15】與赫序函數（hash function）【14】單向不易逆之特性而發展出快速盲目數位簽章策略；然其策略於簽章者計算式子（2.10）（請參閱文獻探討部份）並不能保證可以求出 t_i【16】，對其策略所宣稱之效能構成困擾。

考量雲端運算【5, 19】於資訊安全之重要性，本篇論文融合 Fan and Lei 之思維，藉由網路報案實務觀點【4】提出新的網路報案安全機制，本機制不須藉由公正第三者之協助，而檢舉者與承辦治安單位間均能於透明化之作業下，以達到檢舉者身份私密性與公正糾舉不法之訴求，且易於實作亦為本論文之優點。

2.文獻探討

Fan and Lei 【7】演算法之重點如下：

簽章者（Signer）選取二個相異大質數 p、q，該二數必需滿足下列式子

$$3 \equiv p \pmod 4 \qquad (2.1)$$

$3 \equiv q \pmod 4$ （2.2）

計算

$n = pq$ （2.3）

再選取一個單向且一對一之赫序函數（one-way、one to one hash function）H 與協議值 a，其中 n，H，a 為簽章者之公開參數，而 p、q 為其私密金匙。

假設需求者（Requester）R_i 向簽章者申請訊息 M_i 之盲目數位簽章；其過程如下：

需求者 R_i 選取二數 U_i、V_i，計算

$\alpha_i \equiv H(M_i)(U_i^2 + V_i^2) \pmod n$ （2.4）

然後將 $\{a, \alpha_i\}$ 傳送給簽章者。

簽章者選取可以解出下列式子 A_i 平方根之一數 X_i，

$A_i \equiv H(a)\left[\alpha_i(X_i^2+1)\right]^3 \pmod n$ （2.5）

然後將 $\{A_i、X_i\}$ 傳送給需求者 R_i

需求者 R_i 選取一數 b_i，計算

$\delta_i \equiv b_i^4 \pmod n$ （2.6）

$\beta_i \equiv \delta_i(U_i - V_iX_i) \pmod n$ （2.7）

然後將 β_i 傳送給簽章者，簽章者計算

$\lambda_i \equiv \beta_i^{-1} \pmod n$ （2.8）

$T_i \equiv H(a)\left[\alpha_i(X_i^2+1)\right]^3 \lambda_i^6 \pmod n$ （2.9）

$t_i^8 \equiv T_i \pmod n$ （2.10）

然後將 λ_i 與滿足式子（2.10）之一解 t_i 傳送給需求者 R_i，需求者 R_i 計算

$S_i \equiv b_i^3 t_i \pmod n$ （2.11）

$C_i \equiv (U_iX_i + V_i)\delta_i\lambda_i \pmod n$ （2.12）

然後藉由不可追蹤之電子郵件（untraceable e-mail）方式【6】傳送 $\{M_i、S_i、C_i\}$ 給簽章者，簽章者驗證

$\delta_i^8 \equiv H(a)\left[H(M_i)(C_i^2+1)\right]^3 \pmod n$ （2.13）

如果式子（2.13）成立，則接受該匿名數位簽章。

3. 網路檢舉安全機制

於此部份中，整個檢舉過程區分為公告受理階段、申請階段、分發憑證階段及半匿名檢舉階段、追蹤誣告者階段等。為便於討論，我們將基層戶政（或治安）單位稱為簽章者，參與網路辦匿名檢舉機制之使用者稱為需求者。

3.1 公告受理階段

簽章者（戶政或治安單位）於媒體刊登之廣告應包括「半匿名檢舉制度、自由參加原則」等，於安全機制方面，律定二個大的質數 p、q 所構成的合成數 n【16】，該二數 p、q 需均具有模（modulo）3 餘 2 之特徵，計算 $1 \equiv 3d \pmod{\phi(n)}$，選取安全之赫序函數 H【13】，並擬出五個時段 $D_1 \sim D_5$，其中 n，H，a，3；$D_1 \sim D_5$ 為簽章者之公開參數，而 p，q，d，ϕ（n）為其秘密參數。

3.2 申請準備階段

任一需求者（亦即未來係可能是某一半匿名案件檢舉者，假定為 R_i）R_i 透過法定之第三方(或稱公正者)取得 n，自己所擁有（或可信賴）之資訊設備，隨機(Random)選取一數 M_i，然後選取滿足下列式子之 b_i、U_i、V_i、X_i

$$b_i (U_i - V_i X_i) \equiv 0 \pmod{n} \qquad (3.1)$$

計算

$$\alpha_i \equiv H(M_i)(U_i^2 + V_i^2) \pmod{n} \qquad (3.2)$$

$$A_i \equiv a\alpha_i (X_i^2 + 1) \pmod{n} \qquad (3.3)$$

$$\beta_i \equiv b_i^3 (U_i - V_i X_i) \pmod{n} \qquad (3.4)$$

然後再將 $\{R_i、A_i、\beta_i、f_i\}$ 傳送給簽章者，簽章者計算

$$\lambda_i \equiv \beta_i^{-1} \pmod{n} \qquad (3.5)$$

$$T_i \equiv A_i \lambda_i^2 \pmod{n} \qquad (3.6)$$

$$t_i^3 \equiv T_i \pmod{n} \qquad (3.7)$$

將 $\{\lambda_i、T_i\}$ 傳送給需求者 R_i

附記：本階段之工作於 D_1 時段完成。

3.3 分發憑證階段

需求者 R_i 計算

$S_i \equiv b_i^2 t_i \ (\mathrm{mod}\ n)$ （3.8）

$C_i \equiv (U_i X_i + V_i)\, b_i^3 \lambda_i \ (\mathrm{mod}\ n)$ （3.9）

$h_i \equiv [H(M_i)]^3 \ (\mathrm{mod}\ n)$ （3.10）

然後藉由不可追蹤之電子郵件（untraceable e-mail）方式【6】傳送｛h_i、Si、Ci｝給簽章者，簽章者計算

$H(M_i) \equiv h_i^d \ (\mathrm{mod}\ n)$ （3.11）

$S_i^3 \equiv aH(M_i)(C_i^2 + 1) \ (\mathrm{mod}\ n)$ （3.12）

如果式子（3.12）成立，則接受該半匿名數位簽章，並於簽章者所律定唯其有權公告之公佈欄並將該資料加密 (亦可不公佈，其利弊得失，暫不於本論文討論)，如何加密、如何爾後與檢舉者相互網路通聯，容後續論文著墨。

附記：

（一）本階段之工作應於 D_2 時段完成，假定於公佈欄所公告（加密後） 之資料有 K 個（K≧1）。申請者 U_i 之密鑰為 M_i。

（二）前述之工作應於 D_3 時段完成，簽章者再於 D_4 時段將每一位半匿名需求者之公鑰憑證分發與申請者。

（三）簽章者應將憑證資料｛R_i、A_i、β_i、f_i、λ_i、t_i｝記錄留存，以備日後證實或否認某半匿名檢舉資料為其所發出去之依據。

3.4 半匿名檢舉階段

假定某需求者 R_i 其欲檢舉之內容為 M_0，其計算

$M_i' \equiv (M_0 M_i)^3 \ (\mathrm{mod}\ n)$ （3.13）

然後藉由不可追蹤之電子郵件（untraceable e-mail）方式【6】傳送｛M_0，M_i'｝給簽章者，有關加、解密事宜，限於篇幅，本論文暫不探討。

3.5 追蹤誣告者階段

簽章者基於某些考量，取得一定權限之長官（何謂有權限之長官，其定義如何較嚴謹，有興趣學者

可做進一步纂研）同意，計算

$M \equiv (M_0 M_i')^d \pmod n$ （3.14）

執行下列演算法

for i＝1 to K do

if H（M）≡H（M_i）（mod n）

then return（i）

end for

簽章者於 D_5 時段比對｛R_i、A_i、β_i、f_i、λ_i、t_i、M_i｝，可以追蹤出原需求者（某份檢舉資料 M_0 之提供者），簽章者計算式子（3.7）與（3.12），如果該二式子均成立，則確認某需求者 M_i，殆無疑義。

4.機制安全性之討論

於（3.2）節申請準備階段中，式子（3.2～3.4）有五個未知數，因此，簽

章者（或第三者）僅由｛A_i、β_i｝無法解出 M_i，亦即需求者密鑰之隱密性獲得保障。而式子（3.6～3.7）t_i 產生之前題是必須知曉合成數 n 因式分解之秘密

【15】，故簽章者之簽署行為他人亦將無從偽造。

（3.3）節分發憑證階段中，式子（3.9）有三個未知數，攻擊者即使結合式子（3.2～3.4），仍然面臨四個式子、五個未知數之困境。此外，需求者既然藉由不可追蹤之電子郵件方式傳送訊息，攻擊者亦無法推算出該匿名之需求者究竟是誰？由此很明顯的可以看出，唯有破解因式分解之複雜度，否則無法偽造式子

（3.12）。因此、於該階段中，需求者之身份，攻擊者無從窺探；但卻可遊說簽章者承認其為合格之需求者。簽章者於其公佈欄公佈所有需求者（前述已言之，或可不公布，此係政策決定），因之，每一位需求者於 D_2 時段（或剛完成時）均可掌握有多少位需求者參與半匿名檢舉作業之證據；但彼此之間互不知悉其他人之身份與糾舉不法之內容。

於（3.4）節半匿名檢舉階段中，共區分為二個時段；首先需求者將其糾舉內容以匿名且加密（如何加密，可後續研究）方式告知簽章者，雖然簽章者隨後公開全體需求者之匿名且加密之糾舉資料，但於本階段中，需求者之身份仍保持隱匿狀態。假設簽章者於 D_3 時段掌握全數（或部分）需求者之加密後糾舉資料，而欲勾結外人（或某些合格需求者）意圖更改糾舉內容而誤導社會大眾；然每一位需求者透過（3.2）簽章者於公佈欄所公告之資料，均可於 D_4 時段（

或剛完成時）檢驗其他需求者或簽章者之誠實性。因此，簽章者（或其他需求者）之舞弊情事應可

防堵。

（3.5）節追蹤誣告者階段中，何以斷定某份檢舉資料係哪一位需求者所提出；簽章者驗證相關式子即可判定是否為特定之需求者？下述之定理提供說明。

定理一：式子（3.12）正確

證明：$S_i^3 \equiv b_i^6 t_i^3 \pmod n$ 依據式子（3.8）

$\equiv b_i^6 T_i \pmod n$ 依據式子（3.7）

$\equiv b_i^6 A_i \lambda_i^2 \pmod n$ 依據式子（3.6）

$\equiv b_i^6 a \alpha_i (X_i^2+1)\{b_i^3 (U_i - V_i X_i)\}^{-2} \pmod n$ 依據式子（3.3～3.5）

$\equiv aH(M_i)(U_i^2+V_i^2)(X_i^2+1)\{U_i - V_i X_i\}^{-2} \pmod n$ 依據式子（3.2）

$\equiv aH(M_i)\{1+(U_i X_i+1)^2 (U_i - V_i X_i)^{-2}\} \pmod n$

$\equiv aH(M_i)(1+C_i^2) \pmod n$ 依據式子（3.9）

因此，可得證明。

Q.E.D

由定理一，吾人瞭解於不知（或無法破解）合成數 n 因式分解祕密之條件下，除非擁有｛M_i、b_i、U_i、V_i、X_i、λ_i、t_i｝之正確參數，否則將無法使式子（3.12）

成立。而式子（3.2～3.4）所產生之｛A_i、β_i｝於（3.2）節申請準備階段中，

需求者 R_i 曾告知簽章者其密鑰為（雖然簽章者當時無從得知）M_i，故簽章者於（3.5）節可追蹤誣告者，殆無疑義。

假若某一需求者 R_i 於式子（3.2～3.4）中，將所選取之密鑰 M_i 利用 Pollard and Schnorr【12】之攻擊方法而更改為 M_i'，由於式子（3.2）有赫序函數【14】保護，除非攻擊者能破解該赫序函數，否則本項攻擊亦無法得逞。

5.結論

有鑑於前瞻雲端運算【19】之著眼，為克服 Fan and Lei【7】於式子（2.10）不能保證有解 t_i【16】之缺憾，於其演算架構上，似有加上「若無解 t_i，則需求者與簽章者重新演算步驟（2.4～10）直至有解為止」敘述之必要。然如此則必增加需求者與簽章者之負擔，倘使需求者僅有少許計算能力，只能適用於智慧卡（smart card）【16】之環境中，則其方法恐有不易實作之虞。我們則運用了三次方，由

於系統建置之初，大質數 p、q 之選取即注重模 3 餘 2 之特性，因此保證式子（3.7）與（3.11）有解，相對於 Fan and Lei【7】之方法，我們的機制於實作上確實有簡易之處。

於本機制模型中，倘若簽章者與某一需求者 R_i 共謀，企圖於（3.3）節分發憑證階段與（3.4）節半匿名檢舉階段舞弊，此種顧慮；本模型排除其可能性。此乃於（3.2）申請準備階段，所有參與之需求者均將其密鑰隱匿，共謀者於無法知悉其密鑰的狀況下，於 D_2 時段猜測(Exhaustive Search) 特定需求者之密鑰時有其困難度。縱使簽章者於 D_3 時段得知所有匿名需求者之加密後之密鑰，而欲竄改 D_2 時段公佈欄所曾公告之資料亦為時已晚。顯見我們的理論模型確實達到了公平性、秘密性及投、糾舉不法過程的透明化，使得任何一位需求者均能掌握整個匿名檢舉核心過程之相關證據，以為日後若起紛爭之佐證參考。

傳統檢舉不法作業經緯萬端、氣象萬千，但其重點不外是追求整個過程的公開化與透明化【4】，而達到公平、正義之需求。本網路報案系統作業，除兼具傳統之基本功能需求外，尚應具一套安全機制以為雙方（參與需求者與承辦單位）所信賴，而得以發揮其跨越時間與空間之優越性。本論文之提出，對網路報案安全機制之理論模型或可達拋磚引玉之效果。

六、參考文獻

中文部份：

【1】線上檢舉信箱，內政部警政署刑事警察局，http://www.cib.gov.tw/mail/mail_report.aspx，2009/11/23

【2】多利用網路報案系統，善知識，http://blog.udn.com/godnews/603606，2006/12/18。

【3】廖耕億、黃景彰，「網路競標研究的現況與展望」，資訊安全通訊，第五卷第二期，民 88 年。

【4】國防部，「如何參與軍品採購問答集」，黎明文化公司，民 83 年。

英文部份：

【5】M. Armbrust, etc., Above the Clouds : A Berkeley View of Cloud Computing, http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.pdf.

【6】D. Chaum, "Untraceable electronic mail ,return addresses,& digital psendonyms," Communications of the ACM,vol.24,no.2,pp.84-88,1983.

【7】C. I. Fan and C. L .Lei, "Low-computation partially blind signatures for electronic cash," IEICE Transactions on Fundamentals,vol.E81-A,no.5,pp.818-824.

【8】Franklin, M.K. and Reiter, M.K., "The design and implementation of a secure auction service," IEEE Transactions on Software Engineering, vol.22, no.5, pp.302-312, 1996.

【9】Franklin, M.K. and Reiter, M.K. Verifiable Signature Sharing. in Advances in Cryptology-Euro CRYTO'95. pp.50-63, 1996.

【10】H. Nurmi, "Cryptographic protocols for auctions and bargaining, "Proceedings of Results and Trends in Theoretical Science,pp.317-324,1994.

【11】Y. Chen, J.- S. Chou, C. – H. Huang, “Improvements on two password-based authentication protocols,” http://eprint.iacr.org/2009/561.pdf, 2009.

【12】Pollard and C. Schnorr, "An efficient solution of the congruence $x^2+y^2\equiv m$ （mod n）,"IEEE Transactions on Information Theory,vol.33,pp.17-28,1987.

【13】M. O. Robin, "Digitalized signatures and public-key functions as intractable as factorization, "Technical Report, MIT Lab,Cambridge,Mass.,1979.

【14】R .L. Rivest, "The MD5 massage-digest algorithm, "Internet Report, RFC 1321,1992.

【15】R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public key cryptosystems ,"Communications of the ACM,vol.21, no.2,pp.120-126,1978.

【16】K. H. Rosen, Elementary number theory, Addison Wesley,U.S.A.,1993.

【17】C. P. Schnorr, "Efficient identification and signatures for smart cards, "Advances in Cryptology-CRYPTO'89,pp.235-251,1990.

【18】S. S. Vivek!, S. S. D. Selvi, S. Gopinath, C. and P. Rangan, “ Breaking and Building of Group Inside Signature,” http://eprint.iacr.org/2009/188.pdf, 2009.

【19】T. B. Winams and J. S. Brown, Cloud Computing: A Collection of Working Papers, http://www.johnhagel.com/cloudperspectives.pdf