網路與公開金鑰的玄奇

社團法人台灣E化資安分析管理協會理事長、中央警察大學資訊管理學系專任教授／王旭正

網路與公開金鑰的玄奇

◆ 社團法人台灣 E 化資安分析管理協會（ESAM）理事長、中央警察大學資訊管理學系專任教授 — 王旭正

網路—電腦生命力的延伸

網路，現代科技蓬勃發展的最佳助選員，催生各式科技應用如雨後春筍般，一個個接連地冒出頭。網路將固定性的個人電腦，可攜性的手機等機器串接起來，讓這些替代人類工作的機器得以快速地交換訊息。在人的思維下，我們不斷創造「不可能」的奇蹟，而數學則是人類思維的規律性整理，不斷地觀摩、探索、實驗（若邏輯錯了再修正調整，前進下一階段）。藉數學，科學之母的「愛」，讓人類天馬行空的思維得以實現，電腦的問世即是數學的實現之一。藉由機器的重複運算，把人類的想像，在機器、電腦的演算法中，逐一實現。

在網路世界裡，「個人」電腦讓每個人都得以迅速傳送訊息，也得以接收不同電腦使用者所分享的各式各樣資訊。亦可在網路平臺下載、讀取、吸取各形各色的知識訊息，提升生活、工作的品質。藉此，

網路將固定性的電腦和可攜性的手機等機器串連起來，讓這些機器得以快速地交換訊息。

現今，手機搭配網路的各種功能已和人們的日常生活密不可分。

是否可以直觀地體會到電腦搭配網路是多麼地好用，多麼地讓我們在資訊分享、新知汲取、生活需求上，以最方便、最迅速的方式成為我們資訊生活中「愛」不釋手（愛在手上、身上、永遠有一個超級無敵小的個人電腦—手機）且緊密結合生活裡食、衣、住、行、育、樂的「無所不在」。

網路—讓生命更加多彩繽紛

試想，沒有網路的連接是怎樣的情境？

- 早上起床、想要聽首 You Tube 的歌曲，可以嗎？
- 上班族準備出門前，想了解可搭乘的交通工具，（如公車站牌的到達資訊），在到達前 1 分鐘才悠然在站牌出現，可以嗎？
- 在公車到達前，自在無憂的在家、在早餐店裡，桌上一杯香磨咖啡，嘴上品嘗

漢堡美食；或在中式早餐店，品味濃郁豆漿、飽滿的傳統飯糰、古早味蛋餅，可以嗎？

- 到了上班處所，中午懶得外出，在辦公桌前點現今流行的“Uber Eats”、“Foodpanda”，呵呵，神奇地，不久後，熱騰騰、香噴噴的飯菜出現在面前，可以嗎？
- 炙熱的夏天，下班回家前，希望家裡的冷氣、3C 設備能自動啟動，在回家開門的那一瞬間，歡迎主人的歸來，可以嗎？

是的，這些都不是口號了，在網路「無所不可能」的通達裡，一切都是真的。沒了網路，科技就相形失色（或誇張地「瞬間消失」），成了「黑白」的人生，這似乎是可想而知的。網路在我們生活中的地位，以逆向的推想下，就能知道其不可或缺性。

有了網路安全，才有甜蜜可能

有了科技、有了電腦、有了網路，人們還需要什麼？我們開始進入主題。文明的發展，科技的催生，先求有再求好，沒

沒了網路，科技就相形失色，如今在食、衣、住、行等生活各面，網路運作無所不在。

有「安全」的加持，這檔事就永遠是沒有「保障」的缺憾。我們不會讓安全缺席的，安全裡的「祕密」與「真實」是自古以來人們最在乎的兩大存在價值。

1970 年代後，網路安全的必要性已被資安專家、密碼研究者看出將成為科技趨勢的基礎，建構「安全」的網路才能成就科技帶來的「便利」與習慣的「理所當然」。「安全」的基礎觀念就是「祕密」的保護與「真實」的判斷。打破傳統的思維，如何讓保障「祕密」的 “key” 不再只是「隱藏」，只讓祕密的擁有者知道？如何讓相互通訊的彼此無論認識與否，皆能自然地對通訊的「祕密」做加解密？在網路的傳遞裡，藉「安全」的機制能彼此輕鬆地分享祕密，並阻擋其他「好事者」、「竊聽者」，使之望而卻步、無計可施，達到祕密通訊的目的。

藉由「安全」機制能在網路傳遞裡彼此分享祕密，並阻擋他人竊取，達到祕密通訊的目的。

科技與神話的時空交錯

「公開金鑰」系統（public key system）即是現代「網路安全」的重要基礎。《西遊記》中其實也有著「公開金鑰」的玄機，是否記得唐三藏團隊中的孫悟空（簡稱老孫）？這老孫有著許多戲法，藉著從菩提祖師那學到的「變變變」，而能在〈摘吃仙桃〉、〈大鬧天宮〉、〈西天取經〉的故事中，從身上拔出一叢猴毛，嘴裡吹出一股氣旋，讓那叢猴毛變出千百個「小孫悟空」的小猴兒，這些小猴兒都是老孫的化身，舞刀弄劍與妖魔鬼怪廝殺，神話故事場面看得津津有味、記憶深刻。

每隻小猴都是本尊老孫的分身，傳承老孫所有功夫，得以與所有妖邪對抗。以此引申到金鑰的概念，即為當老孫本尊有一把 key，得以加解密時，老孫所變出的千百個分身小猴也都代表著老孫，所以這些小猴所持有的 key 都是來自老孫本尊，

所有 key 都能對「祕密」加密與解密。換言之，用小猴的 key 加密，也能用老孫本尊的 key 解密，如此即代表這些 key 的群體是相互有關係，能得以對「祕密」做加密與解密的處理，並自然地回復「祕密」的內涵。

藉此我們即知一個重要的概念推廣與應用，當老孫與眾分身小猴皆有 key 時，我們將傳統 key 的思維做些調整，即 key 的擁有者不再只有傳統的一把 key，而是擁有一把以上的 keys。而這些 keys 之間，是可以相互搭配來對「祕密」做處理（即加解密運算），對應到故事中，即為本尊與分身的同源性，藉由同一源體的本尊與分身的搭配即得以因應各式的需求與應用。例如以分身小猴的 key 對「祕密」做的任何加密處理，都得以本尊老孫的 key 作解密，以還原得到「祕密」。

依此脈絡下，若將分身小猴的 key 作為可公開的 key，讓所有欲與老孫祕密通訊者皆可用這些 keys 來對「祕密」做加密處理，傳送給老孫；收到的本尊老孫即可用老孫的 key 解密，如此一來即自然而然的以加密保護了「祕密」，卻也只有老孫本尊得以解密。此即科技與神話情境的時空交錯。

套用在金鏘的概念上，具有同源性的孫悟空（本尊）和以猴毛變出的小猴（分身），就是可以相互搭配來進行加解密運算的 keys。

圖 1　公開金鑰系統下牛魔王與孫悟空的安全祕密通訊

公開金鑰系統讓「網路安全」得以有最大的保障，使得「祕密」的傳遞，「真實」的判斷，得以在網路世界實現。所有的基本觀念傳承原始的傳統做法，key 還是對「祕密」進行「加」與「解」密的最關鍵元素。至於包裝祕密的各式方法，即是在公開金鑰系統理念下，如何來實現的下一個階段。

「公開金鑰」的玄機

回到網路公開金鑰系統下，我們再以《西遊記》的情境來做說明，以老孫與牛魔王這兩位人物的互動，可輕鬆揭開公開金鑰的運作。「公開」所指的是擁有 key 的主導者，為了順利在網路上達陣，將 key 分成 2 種型式，一部分來公開；另一部分仍是傳統的思維，即 key 本來是被主事者所祕密擁有，不得為任何其他人所知曉，如此才是安全保護的核心價值。

既然 key 公開了，那麼不就所有安全也都「公開」了嗎？這是一般人的誤解所在。公開系統的「公開」二字，僅限於主事者 key 的擁有與管理，為了在科技網路下依然能對「祕密」做安全保護，因此將「部分」的 key 做公開，此即「公開」二字命名來由。

依圖 1 所示說明：孫悟空與牛魔王（以下用「老牛」來稱呼）的互動裡，老牛欲

跟老孫作祕密通訊，那麼老牛會告訴老孫派個分身小猴來，小猴所持有的 key 可在網路裡公開被知，小猴亦可公開為老孫的分身。老牛看到分身小猴後，能用小猴的 key（公開的 key）將「祕密」做包裝加密，讓分身小猴將加密的包裝帶回，亦即由網路傳送給本尊的老孫。老孫輕鬆地看到加密的包裝，順手用老孫自己的 key 即可將包裝裡的「祕密」解密。因為老孫與小猴的 keys是來自同源，小猴是老孫變出來的，當然老孫的 key 可輕鬆地解密。

這套戲法，依此「祕密」的傳遞方式，網路上的牛魔王也將是如此炮製，先有一些相互有關係的 key（內容值當然是不同的），且有自己的祕密 key，並公開一部分的 key 於網路，使所有人皆知此公開的 key，若想跟老牛祕密通訊，即可用老牛的公開 key 做加密後的黑盒子包裝，而後傳送給老牛，老牛當然也輕鬆地用個人祕密持有的 key 得以將已加密的黑盒子包裝做解密。

談了公開的系統，神話故事裡的《西遊記》竟也搬上現代網路的檯面。那麼如何包裝神話故事的「古」事？如何不再只是「故事」？「前人種樹後人乘涼」，德國的高斯（Gauss）為資安的密碼技術奠下基礎；法國的費瑪（Fermat）閱讀書頁記事的神奇小定理，$a^{p-1} \bmod p=1$，其中 p 為質數，為公開金鑰系統的現代網路的安全性，揭開運用的序幕。

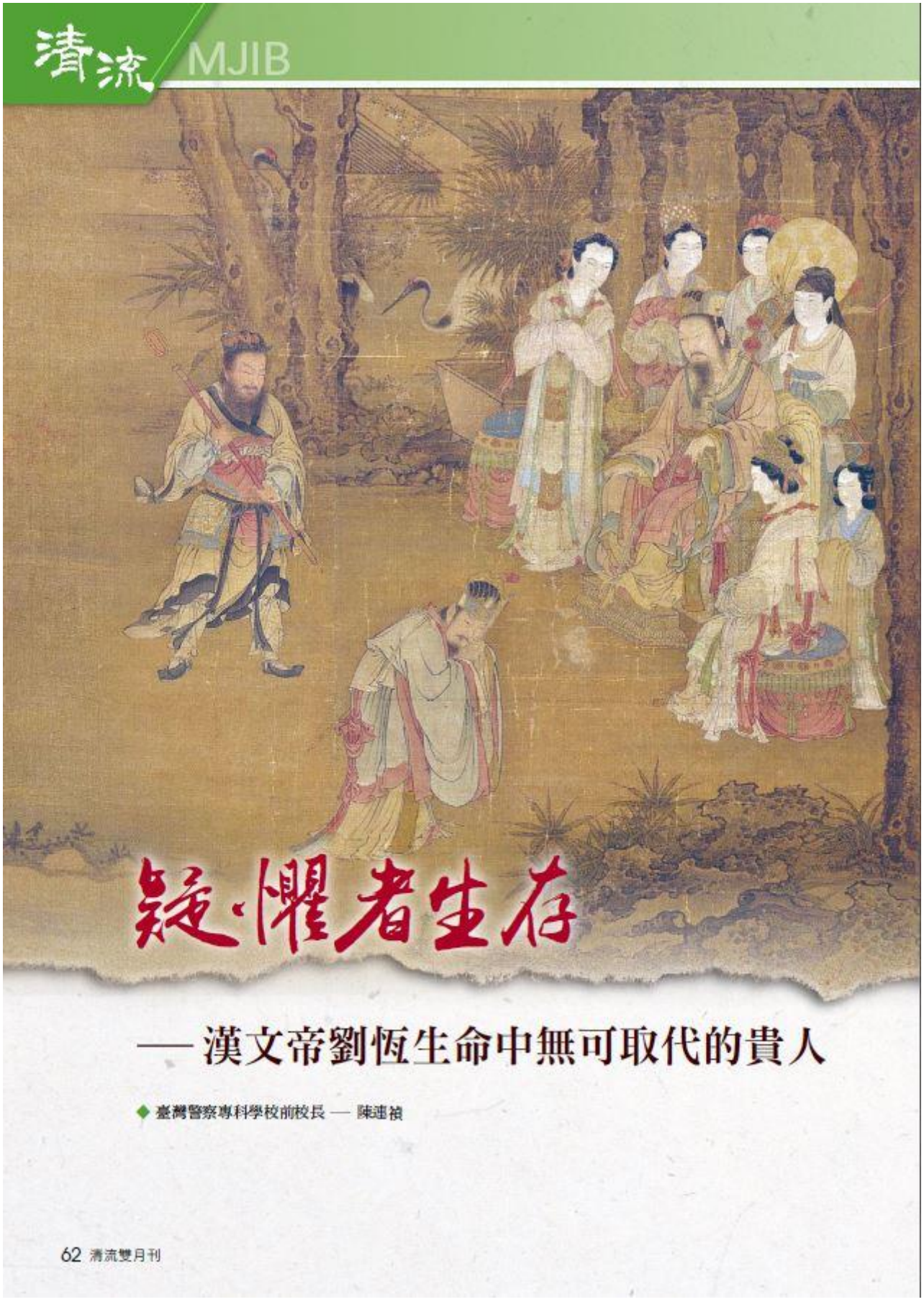
社團法人台灣 E 化資安分析管理協會（ESAM）

中央警察大學資訊密碼暨建構實驗室（ICCL）

本文摘自清流雙月刊**中華民國110年1月 號P37-P43**

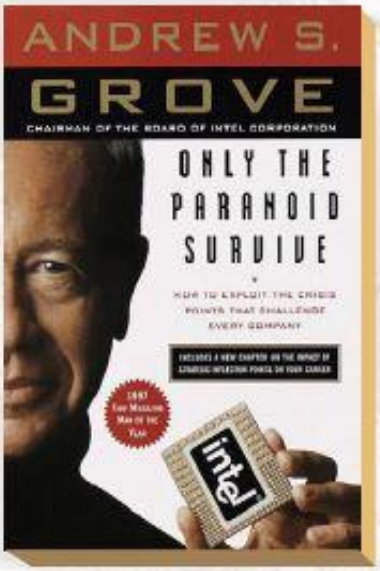
疑懼者生存－漢文帝劉恆生命中無可取代的貴人

大學臺灣警察專科學校前校長／陳連禎



只有疑懼者才能生存

1998 年台積電董事長張忠謀在交通大學開設經營管理專題課程，指定兩本必讀書，其一是英特爾前董事長葛洛夫自述經驗的《10 倍速時代》。他說這本英文書原名《Only the Paranoid Survive》，有人將「Paranoid」翻譯偏執狂，是譯錯，這字的意思應當是「疑懼」，所以書名原意就是《只有疑懼者才能生存》！書中，葛洛夫指出環境的變化快速，將以「10 倍速」狀態前進，其演變劇烈將讓人措手不及，隱喻每人都應抱持「凡是可能的，都會發生」、「愈是成功的時候，愈是危機四伏」等疑懼意識。因為，唯有敏銳觀察外在環境變化，才得以迅速調整對策，制敵於機先。



漢文帝劉恆曾遭遇過「只有疑懼者才能生存」的情境。其在代地蟄伏並遠離權力核心十數年，在當時仍有劉邦長孫劉襄準備接替帝位的情況下，劉恆突然接獲群臣擁立為帝訊息，其雖喜出望外但仍保持疑懼，才安然度過危機並順利登基。

從天而降之迎立為帝喜訊

高后八年，呂太后崩逝，大臣共謀誅呂平亂，亂事平定後，丞相陳平、太尉周勃等派人要迎立代王劉恆為帝。劉恆突然收到天上掉下來的大禮，幾乎不敢相信為真，驚懼得差點不能呼吸，預感未來發展恐危機四伏。因此，接到迎立為帝喜訊，他並沒有得意忘形，反而疑懼而思慮周密，謹慎處理。

他首先徵詢左右親近大臣，研判情資真偽。郎中令張武等人認為：漢大臣都是故高帝時的將軍，熟習兵法，常耍謀詐，其中必有詐。因為，這般大臣在京師竟敢殺盡諸呂家族，現在以迎立為名，實不可信，因而主張「稱疾毋往，以觀其變」。而中尉宋昌則認為「大臣因天下之心而欲迎立大王，大王勿疑也。」兩位親信意見分歧。劉恆疑懼不安而轉問母親薄太后，沒有得到明確答案。於是另請太常官員卜筮吉凶，得到上籤後仍不敢沾沾自喜。他先請舅舅薄昭入京面見太尉周勃，確定群臣迎立無可懷疑，才帶領重要幹部進京。

劉恆來到高陵即駐足不前，先遣中尉宋昌入長安城外的渭橋附近觀變，直至宋昌確認安全無虞後，才馳至渭橋接受諸大臣迎立。而劉恆下車後，周勃竟提出要與劉恆單獨談話，在宋昌慎思快辨後斷然拒絕，說：「所言公，公言之；所言私，王者不受私。」周勃無言以對，只得在群臣面前跪上天子璽符。

劉恆入宮後緊接一連串的連夜應變動作，充分流露文帝一貫的謹慎態度與臨深履薄的疑懼憂患，從此展開我國歷史第一個太平盛世—文景之治。文景之治，得力於文帝的憂患意識及其仁民愛物的身教奠下弘規。而文帝在位步步為營經營 23 年，奠下景、武二帝物阜民豐的盛世繁榮，實得力於母親薄太后及後來居上而扶正的竇皇后。

奠定劉恆千秋大業之幕後推手

首先，影響文帝人格成長深遠的女性，應該是他的母親薄太后。早年即有命相家斷定薄姬當生下天子，收留她的魏王豹得知，自我感覺良好而背叛漢王劉邦，魏王豹政治判斷失準，導致國亡身死，薄姬被俘而納入漢王後宮。後來經閨蜜的介紹，才得幸於漢王。臨幸前，她告訴劉邦說，昨晚夢見蒼龍盤踞腹上。薄姬的自我期許、暗示，同時鼓舞了劉邦的興致，只此一幸竟然得子，然而此後卻少見劉邦。薄姬雖不受寵於劉邦，卻也因此逃過呂太后的報復殘害，而能與兒子劉恆遠居代國。

薄姬被預言當生天子而不張揚，被幸過而不爭風吃醋。她安居邊地多年，外家又始終保持低調，薄家因此留下不揚不爭

的好印象。漢初在呂后外戚干政的經驗教訓下，大臣願意主動迎立劉恆為帝，實是託母親薄家作風極為低調之福。

陰錯陽差　麻雀變鳳凰的竇皇后

竇姬父母早逝家貧，被選為宮女，由於竇姬貌美及個性機靈，呂太后將其列入遍賜諸侯王之宮女名單。竇姬雖年輕卻是很有主見，得悉將被外派，她想回到離家近的趙國，因此超前部署，主動找上主事的宦官，請將她派遣到趙國。無奈，陰錯陽差，竇姬最終被分派到偏遠的代國；她淚如雨下，堅持不肯成行，最後，還是被強行帶走。

當時劉恆已有王后，卻對竇姬情有獨鍾，竇姬受劉恆感動，由監視變為相挺，日後為其生下 1 女 2 男。之後王后亡故，在劉恆為漢文帝後，竇姬長子劉啟被冊立為皇太子，因此，竇姬被冊立為皇后。竇皇后在未來的日子操持家務很用心思，贏得了賢內助的好形象。

劉恆低調拒惑　逃過呂后魔手

回觀劉恆，心思敏捷程度，絕不容小覷。代王早就察覺呂太后剛毅有謀，送宮女的用意絕不單純。上所賜宮女當然都精挑細選，早有縝密的政治考量，絕非毫無目的善意賞賜。呂太后透過訓練有素又信任有加的宮女，藉以攏絡諸侯王外，進而將微伺諸王動靜，其用心正如她將呂氏兒女嫁與諸王為后的手段如出一轍。因此被

挑選出來的竇姬，必然是受過調教，且賦予特殊任務。

竇姬至代國之時，劉恆王后仍健在，何以劉恆會寵幸竇姬？或可推論劉恆係對呂太后的賞賜釋出善意，表明對其順服，才能讓呂太后對他全然放心，而使劉恆安度了可怕的政治風暴。

其次，呂太后崩殂前一年，她曾徵詢劉恆是否願意高升至繁榮重地當趙王。趙國曾是竇姬之前求情想去的家鄉寶地，面對他人夢寐以求及愛人曾仰天期盼的天賜良機，劉恆卻敬謝不敏。因為劉恆與竇姬隱約得知前三任的趙王劉如意、劉友、劉恢皆以悲劇收場，故而戰戰兢兢，寧願續在偏遠的代國守邊以明志。由此可知劉恆的憂患疑懼、竇姬的自我克制與夫妻倆的警覺性之高。

劉恆生命中無可取代的貴人

由上觀之，劉恆安居代王守邊 17 年，接著經營帝位 23 年，始終如一的仁孝印記，躲過無數的風險，創造我國史家公認的第一個太平盛世，奠下日後大漢聲威的實力。而他由黑翻紅，在不安驚懼中步步為營，追根究柢影響他人格、幫助他成長的是 2 位女性：母親薄太后的樂天知命、安分守己不張揚，同時也約束外家的干預

爭權，讓劉恆的社會觀感極佳；加上很有主見的竇皇后善用心思，扮演公私兼美的賢內助，既懂得自我克制與經常地保持警覺，在在支持劉恆的疑懼憂患之行事思維。她們都是劉恆生命中無可取代的貴人。

本文摘自清流雙月刊中華民國110年1月 號P62-P66