

中興事件敲警鐘 商用密碼國產化

海歸棄優厚待遇回國創業 補網絡安全短板

身處互聯網時代，從銀行卡、電子支付到微信、手機解鎖，密碼可謂無處不在。然而，無論是固定密碼、手勢解鎖、指紋認證等，都普遍存在易外泄、易截獲、易破解、易攻擊的弱點，給企業和個人信息安全埋下「定時炸彈」。以孫冠樺為首的海歸青年，潛心兩年自主研發出中國首款將真實密碼、形式密碼、密碼介質三分離的「Magic Image (秘陣)」商用密碼，成功通過「國家商用密碼生產定點單位」涉密企業資質認證。孫冠樺說，「中興事件」給國人敲響了警鐘，像密碼、芯片這類底層關鍵核心技术，必須掌握在中國人自己手中。

新經濟浪潮
大公報記者宋偉遼寧報道

中國商用密碼行業現狀

- 736 家商用密碼產品生產單位
- 975 家商用密碼產品銷售許可單位
- 2200 多款商用密碼產品
- 110 款密碼芯片
- 13.2 億台商用密碼產品銷售量 (2017年)
- 239.3 億元人民幣商用密碼產品銷售額 (2017年)

數據來源：《中國信息安全》2018年第8期

秘陣科技交互體驗中心
大公報記者宋偉攝



互聯網帶來便捷的同時，也帶來不容忽視的安全隱患。據國家相關部門統計，中國一線城市人均擁有26個帳戶。秘陣科技創始人兼CEO孫冠樺直言，帳戶多、安全性低是當今密碼市場最大痛點。「無論是以銀行為代表的金融類帳戶，還是郵箱、微信這類通訊帳戶，大多使用的是大小寫字母、數字和特殊符號的固定密碼，這類密碼實際上只能稱作PIN碼 (Personal Identity Number)。」PIN碼普遍存在着記不住的問題，更有易偷窺、易外泄等致命缺陷。

帳戶多安全性低成痛點

在外企信息安全領域打拚十年，看到中國商用密碼的薄弱環節，孫冠樺與同樣具有報國之志的幾名年輕人，毅然決然放棄國外優厚待遇，回到祖國創業。「在追求便捷的同時，越來越多的網絡用戶也認識到安全是互聯網的底線。補中國網絡安全之短板，就是我們的創業初衷。」

作為人與互聯網交互認證的「防盜門」，密碼本身是個底層技術，如果密碼不安全，很容易就會被盜取身份信息，引發諸如電信詐騙等一連串不堪設想的後果。孫冠樺說，中國近年來一躍成為互聯網應用大國，儘管網絡應用層面很發達，但不容忽視的是人機交互的安全維度相對滯後。

受到滑屏解鎖和銀行動態令牌一次性密碼的啓發，「Magic Image (秘陣)」應運而生。作為中國完全自主研發的一款動態身份認證產品，其最大特點在於將高安全強度的「一次性密碼 (OTP)」與便於記憶的「圖形密碼」相結合，用「不變的圖形」對應「變化的數字」。

易記安全密碼受歡迎

孫冠樺舉例道，如果解鎖「圖形」是一個斜線，那麼用戶只需記住斜線這個圖形，解鎖時輸入當時斜線所對應的數字即可。由於隱藏圖形密碼的數字陣列表是隨機變化的，因此每次斜線對應的數字也成爲了一次性密碼，即使是大聲說出這些數字或讓別人盯着你輸入密碼，也無需擔心密碼被竊取。

不再將傳統的複雜數字和字母作爲密碼，讓用戶徹底擺脫了死記硬背固定密碼的記憶模式，在不依賴外部加密設備情況下，通過人工智能算法等技術實現了高安全性。

孫冠樺說，在提升密碼本身便捷性、安全性和易用性的同時，還可以有效應對木馬、釣魚等病毒入侵，實現全媒體、跨平台的認證互通。「而這就是秘陣決勝未來商密戰場的寶藏。」

變現慢考驗商業耐力

密碼研發成功是第一步，但如何讓用戶認可並做到合規，對孫冠樺的挑戰可能更大。「首先要改變國人觀念，讓大家知道PIN碼不等於密碼。其次，需要得到國家密碼部門的資質認證。」孫冠樺直言，這是個高風險行業，研發和認證需要漫長過程，很多初創企業都倒在路上。「兩年時間，在企業沒有正向現金流的情況下，沒有毅力是不可能堅持下去的。」

談起創業艱辛，孫冠樺笑稱「都是眼淚」，就連投資人都向他抱怨回報太慢，產品能不能先賣，有問題再改。但他卻始終堅守信念，密碼安全無小事，不能用市場去試驗產品。而在申報國密資質認證時，孫冠樺再次遇到了困難。省市密碼部門的領導好心勸他：「國密認證都是上市公司和大企業才



▲秘陣科技代表中國信息安全領域企業，登上美國納斯達克大屏

來申請，哪兒有初創企業來搞這個？到時通不過檢測，你們的錢可就都打了水漂。」前後一年時間，孫冠樺和他的團隊都在爭取申報機會。他甚至還跑到國家密碼局，硬是和門衛較勁磨泡一整天，希望諮詢自己的密碼產品是否有合規可能。

功夫不負有心人，孫冠樺和他的團隊苦熬兩年，堅持終有收穫。秘陣科技最終通過國密認證，並創下了第一家通過國密檢測的創業企業和用時最短兩項中國商用密碼史紀錄。孫冠樺堅信，「中國如果在密碼這個底層技術上有突破，那在應用維度上一定會產生重大影響。」

香港商用密碼商機大

「香港作爲世界級金融中心，應用「秘陣」的市場空間巨大。」孫冠樺說，「Magic Image」應用的第一大領域就是包括銀行、證券、保險在內的泛金融行業。在香港應用，既可使用已成爲國際專利的「國密」算法，也可應用國際通用的RSA加密算法。

他坦言，香港雖然在支付領域的便捷性沒有內地走得快，卻未曾爆出安全隱患事故。「港人同樣也在追求以安全爲前提的便捷性，這對商用密碼企業而言存在巨大商機。」

►孫冠樺直言，帳戶多、安全性低是當今密碼市場最大痛點



何爲「商用密碼」?

話你知道

商用密碼，是要對不涉及國家機密內容的信息，進行加密保護或者安全認證所使用的密碼技術和密碼產品。商用密碼的應用領域十分廣泛，主要用於對不涉及國家機密內容，但又具有敏感性的內部信息、行政事務信息、經濟信息等进行加密保護。比如：可用於企業內部的各類敏感信息的傳輸加密、存儲加密，防止非法第三方獲取信息內容，也可用於各種安全認證、網上銀行、數字簽名等。

資料來源：國家密碼管理局



▲目前內地最多互聯網企業，實際上沒有技術壁壘

初創企業唯技術稱王

創業密碼

「我們不做「科研院所」，不搞「模式創新」，定位「科技型」互聯網公司，專注互聯網+安全。」孫冠樺解釋說，密碼研究是底層技術，需要耗費大量時間、成本和資金，這本應是科研院所做的事。作爲一個初創企業，若做密碼就必須與市場接軌，明確知道用戶需要什麼，有明確的盈利模式，才能長久地生存下去。

「現在國內衆多互聯網企業實際上沒有技術壁壘。我們要做的是一家科技創新公司，而不是

商業模式創新公司。」他認爲，創新不止於模式，可以借鑒互聯網快速推廣的方法，但必須有自己的核心技术。「如果光靠燒錢把用戶堆上來，而缺乏核心技术，勢必留下隱患。」

目前，中國只有秘陣一家做純軟件商業密碼。孫冠樺直言，人機直接交互是未來科技的發展方向，像密碼這類實體介質勢必會被淘汰。除了在泛金融領域，未來秘陣還將與雲服務、物聯網進行深度結合。「初創企業一定要找準自己的定位，擁有屬於自己的核心技术，才能長久發展。」



▲服務過外國金融客戶後，秘陣科技了解到，內地普遍使用的銀行U盾，海外卻難覓蹤影



掃描微信公眾號二維碼關注新經濟故事

做出讓農民工用了叫好的密碼

不忘初心

創業初期多艱辛，一件小事卻堅定了孫冠樺的創業初心。在2016年中國國際軟件和信息服務交易會(簡稱：軟交會)期間，秘陣科技關於Magic Image密碼介紹的「易拉架」，吸引了一位正在布置展場的農民工目光。當孫冠樺要移走易拉架時，農民工一把拽住他問道：「你們這個東西挺好，賣不，多少錢？」當時孫冠樺感到很奇怪，經過交談後才知道，這位農民工兄弟的所有帳戶用的，是同一個固定密碼，他十分害怕

一個帳戶被盜後引起連鎖反應。「那你覺得我們這東西好在哪儿？」「我能看得懂！只要記個圖形，每次輸入的密碼就可以不一樣，我覺得挺安全。」回憶起當時的場景，孫冠樺感慨說，密碼安全關係社會每一個人的切身利益，沒有高低貴賤之分。「他當時特別認真在看介紹，甚至還掏出手機掃描公司二維碼想要下載。」雖然當時Magic Image還未獲得國密認證，但這件小事給了孫冠樺和他團隊滿滿的成就感和獲得感。



▲身處互聯網時代，從銀行卡、電子支付到微信、手機解鎖，密碼可謂無處不在

毋需U盾密碼未來大趨勢

市場應用

服務過外國金融客戶後，孫冠樺發現，內地普遍使用的銀行U盾，海外卻難覓蹤影。「U盾的缺點造價高，還有只能依賴PC端進行操作，無法連接手機進行大額轉帳。事實上，內地銀行業務已經開始從PC向手機端傾斜。」

由於銀行對安全系統高可用、高穩定性的要求，孫冠樺在進軍銀行安全領域前，將Magic Image進行了大規模試用。秘陣「國密」版不採用傳統U盾的明碼顯示，而是需要經過用戶的主觀判斷，才能從中提取到當次有效的一次性口令，進而從根本上杜絕了因U盾等外部加密硬件的丟失、外泄而導致安全隱患，更重要的是成本只是傳統U盾的十分之一，性價比優勢非常明顯。

「在當下BYOD (Bring Your Own Device) 的時代，毋需U盾密碼，無疑具有廣闊的市場前景。」孫冠樺說。