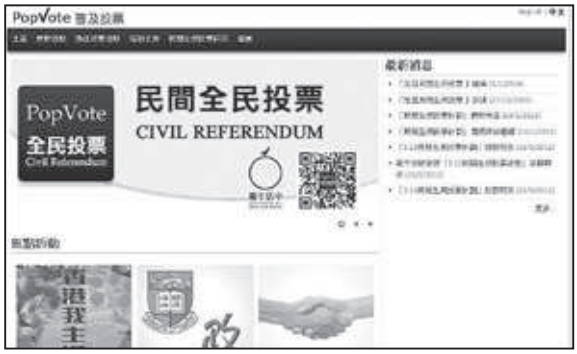
探究「民間全民投票計劃」電子投

2012 年，特首選舉前的「3.23 民間全民投票」受到襲擊，電子投票系統（系統）癱瘓令市民相繼到實體票站投票。2013 年，香港大學民意研究計劃（民研計劃）正式宣布繼續建構全民投票平台，並組成「普及投票資訊科技顧問小組」強化系統。2014 年，民研計劃受佔領中環秘書處委託，於 1 月 1 日舉行「元旦民間全民投票」。此次投票全程以電子方式進行，視為經強化後的第一次公開測試。本文重點探究系統運作原理，解釋系統研發問題，公開讓公眾參考，希望可以集思廣益。



投票渠道

投票方式分「離站投票」及「到站投票」，兩者皆是電子投票。「離站投票」是透過網站或流動應用程式投票。投票人士須根據系統畫面指示，經互聯網進行身份認證，然後投票。「到站投票」是親身到實體票站投票，工作人員配以平板電腦核實投票人士的身份證資料，然後讓投票人士於獨立投票間以平板電腦投票。

假若已透過網站進行「離站投票」，便不能重複使用流動應用程式投票，反之亦然。研發團隊了解到親身到實體票站核實身份證資料是最可靠的方式，所以若系統收到同一身份證資料於「離站」及「到站」投票，系統會自動以「到站」選票取代「離站」選票。簡單而言，同一的身份證號碼，系統只會計算一票。

系統設計

汲取受網絡攻擊令系統癱瘓的經驗，研發團隊尤其關注系統的穩定性及資訊保安問題。穩定性方面，團隊將系統存放於功能相對完善的雲端伺服器供應商，有效地運用雲端負載平衡器、伺服器自動擴展技術、記憶體緩存功能及多區伺服器部署，務求將數據盡快處理及應付突如其來的網絡流量。系統背後啟動著不同類型子系統處理數據，完善將流量分配，子系統包括驗證碼核對、應用程式介面請求處理、電子排隊、短訊接收、實體票站數據交換、選票收集、選票點算、以及系統記錄及監察。研發團隊將子系統緊密配合，動用超過 40 台伺服器。從用戶角度看，就是一個簡單數步曲的電子投票系統。

鑑於「離站投票」及「到站投票」在處理數據時皆依賴中央伺服器的正常運作，若中央伺服器出現問題便會導致「到站投票」的實體票站不能運作。有見及此，研發團隊部署票站伺服器於實體票站，寫入相同的資訊保安程序，讓實體票站能夠在離線狀態下獨立運行，儘管中央伺服器遭到網絡攻擊，亦不會影響「到站投票」運作。直到票站伺服器能成功連接中央伺服器，經散列函數處理的個人資料及加密處理的選票資料便會自動傳送上中央伺服器儲存。

認證方式

以「到站投票」方式投票，實體票站的工作人員會檢視投票人士的身份證明文件，核實身份，確保符合資格投票。至於「離站投票」，投票人士自行輸入完整身份證資料、手機號碼及確認是年滿 18 歲或以上的香港永久性居民後，必須先通過手機短訊認證方可進入投票介面。研發團隊已花盡多月的努力，唯民間沒有一種普及且完美的網上身份認證方式可應用。手機短訊認證是經權衡利弊後所作的決定，現仔細解構如下：

- 認證身份目的是要達到一人一票，而每位香港市民必定擁有兼獨一無二的就是香港身份證號碼，沒有其他。因此，收集完整的身份證號碼是必須的。

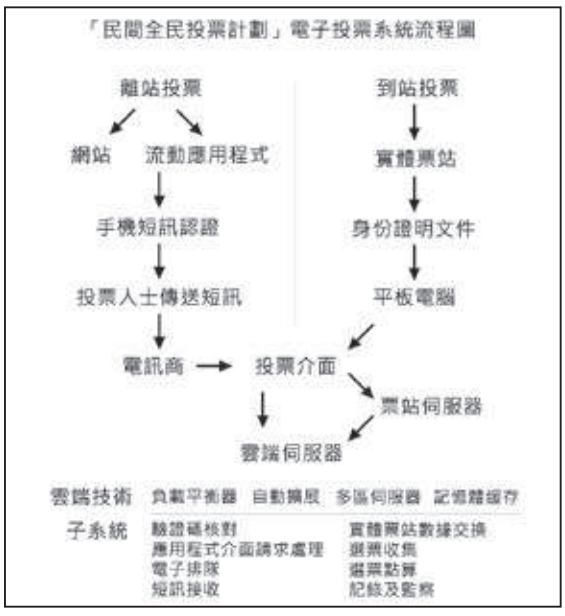
票系統

- 香港身份證號碼是由香港政府制定，完整的個人資料庫是民間不可能擁有，當中涉及的權限與私隱問題是顯而易見。唯一可以檢查一個身份證號碼的有效性是依靠完整身份證號碼括號內的資料，而這有效性檢查只能排除無效的號碼，不能核實輸入人士的身份。

- 坊間的確有工具能產生有效的身份證號碼，讓有心人胡亂填上虛假資料，輕易地逃過系統檢查。研發團隊當然不希望此舉於文明社會出現，但在一人一票的大前提下，必須加以防範。

- 要尋求一種網上身份認證方法，研發團隊想過利用電子證書，但在考慮電子證書的普及程度及流動應用程式的兼容性下，只好放棄。團隊亦想過預先進行選民登記，實體地核實市民身份，然後分配投票密碼，可是要應付香港三百多萬的登記選民，實在沒有這龐大資源設立足夠的實體登記站。第三種想法是要求投票人士上載身份證副本，讓系統自動核實身份證資料。此想法是天馬行空，因為從用戶角度看，認證步驟煩瑣，過份收集個人資料，以及沒有防偽功能。在平衡各種方法的利弊後，最終得出的結論，就是應用手機短訊方式，協助於網上進行身份認證。

- 手機短訊身份認證常見於有規模的網站，目的在防止網絡資源被濫用，務求減少一人登記多個帳戶及驗證登記者是否真實存在。故此，結合上短訊認證後，系統能大大減低非真實用戶的存取。



- 短訊可分為傳送及接收兩種，傳送的一方通常需要繳付一個短訊費用，接收的一方通常不需額外收取費用。研發團隊決定讓投票人士支付費用傳送短訊，是因為系統的經費實際上的來自民間的捐款，若要系統承擔可能出現三百多萬的香港登記選民的認證短訊，籌募的資金根本不足以應付甚至出現負債，達不到持續強化系統的目的。順帶一提，短訊費用是由電訊商收取，民研計劃亦須繳付短訊接收服務使用費。

- 或許你仍會質疑手機號碼隨處可購得，真的能防止有心人胡亂填上虛假資料嗎？答案是不能百分百防止，原因是民間不可能擁有完整的個人資料庫。研發團隊所準備的，是應用當今科技與技術，製作嚴謹性較高的系統。試想想身份證明文件或流通的貨幣，防偽特徵又是否百分百的有效？要達至理想用途，有賴文明社會裡的各方配合、互相信任。

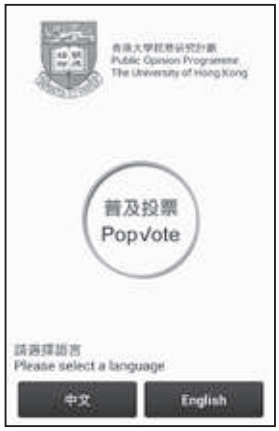
系統保安

系統存放於雲端伺服器，本已內置防火牆阻截分散式阻斷服務攻擊。研發團隊同時整合網絡保安公司的網絡監測及即時欄截設備，以及研發即時系統監測平台，讓工作人員可透過平台實時監測網絡流量變化。若遇上不尋常的流量，便可即時作出反應。

而我們關注的攻擊主要有兩種，一是令網絡癱瘓的攻擊，二是盜取或更改資料。

為減輕受網絡癱瘓的攻擊的影響，團隊不單靠防護，而且強化了系統能處理流量的能力，正正是上述提及採用雲端技術和各種子系統的流量分配，減低癱瘓風險。在應用層面上，所有「離站投票」必須輸入圖片顯示的驗證碼，目的是防止系統被機械式的重覆存取攻擊。圖片所顯示的內容是隨機產生，較複雜的圖片會較難被破解，從而增加破壞系統的難

度。假若使用較容易辨認的圖片，保安效果亦會相對減少。



關於盜取或更改資料的攻擊，亦即資訊保安方面，團隊制定了多項的保密措施讓資料外泄及被破解的風險減低，將保安程度推至頂點。措施包括：

- 用戶與伺服器之間的數據傳送，是透過SSL加密方式進行，保障數據於傳送時沒有被盜取查閱及更改。而 SSL 證書是由授權機構發出，有效認證伺服器的真實性；

- 由於身份認證過程涉及個人資料，但在系統角度並不需要原始的數據作辨認，反而將所有個人資料經過散列函數以不能還原的形式儲存，所以系統是不會儲存原始的個人資料數據；

- 散列函數是採用標準的 SHA-512 算法為基礎，然後依數據的排列方式，混入隨機運算出來的密碼，再重覆將數據經散列函數運算，增加保密效果。若要將數據還原，須花上數以年計的時間；

- 選票資料是以加密方式儲存於系統數據庫內，只有三位被委託的非技術人員配有不同部份的解密鑰匙。若要開啟電子票箱取閱選票資料，必須同時輸入由其中兩位非技術人員持有的解密鑰匙。三選二的設計是為防止鑰匙遺失而設。

功能改善

「元旦民間全民投票」所用的系統，是研發團隊花了六個多月時間重新設計及編寫。經過元旦日的一役，研發團隊正整合各方的意見，了解到不同人士有不同的體驗，亦了解到此次的公開測試並不完美。改善系統成為研發團隊刻下的重點任務，現正積極考慮改善以下主要功能：

- 海外投票：在原設計上，基於保安理由，系統透過網絡保安公司直接與香港互聯網交換中心連繫，只容許香港境內網絡進入，任何非香港網絡將不能進入系統投票。但於投票當日，不少身處海外的香港市民向我們強烈表達希望進入系統投票。團隊會考慮為非香港網絡設立特定的伺服器，而兩組系統分別承受不同的保安風險。

- 短訊認證：有感手機短訊傳達未能與系統理想地配合，而短訊傳送速度有著不能預期的因素令其大大減慢。因此，團隊會考慮加強與電訊商的配合，選用更多、更有效率的電訊服務。同時不排除引入另一種認證方法取代短訊認證。

- 認證時限：由於短訊延誤令投票人士未能於三分鐘內完成認證，白白浪費等候時間及短訊費用。有見及此，團隊會考慮延長認證時間，同時間於程式加入認證提醒功能，當系統收到短訊後會自動提醒投票人士進入投票介面，毋須長時間留意認證介面。

- 電子排隊：系統設有電子排隊機制，自動分配可承受的名額，讓投票人士分段投票。不少市民反映當日需要等候多時才能進入系統，原因是短訊認證部份失靈，觸發系統即時啟動人流管理機制。團隊會改善短訊認證問題，從而加大系統容納人數。

投票情況

最後，總括一下投票當日的情況。系統整體上運作良好，市民利用流動程式投票的有四萬多票，透過網站投票的有一萬九千多票，到達實體票站投票的有二千多票。總計六萬二千多票之中，流動程式佔了相當大部份，可見在文明社會裡，隨著智能手機的普及，市民正需要這一個渠道，和平理性地表達意見。

關於整個「民間全民投票計劃」的資料，歡迎到香港大學民意網站查閱，網址為 http://hkupop.hku.hk。

馬晉彥
香港大學民意研究計劃科技經理