Tym razem się nie uda,

czyli epilog sagi kryptologicznej w odcinkach.

W tej części: o tajnych głosowaniach elektronicznych.

*Tomasz KAZANA**

* Wydział Matematyki, Informatyki i Mechaniki, Uniwersytet Warszawski

Redaktor *Delty* w latach 2016–2022.

Delta, grudzień 2003

Tajne wybory to sól demokracji.

Najwyższy rangą dokument obowiązujący w Polsce – Konstytucja RP – wspomina o nich kilkakrotnie (art. 96, 97, 127, 169), podając dość konkretne wymagania, takie jak powszechność, równość, bezpośredniość czy właśnie tajność. W tym artykule spróbujemy zastanowić się, czy w świecie cyfrowym możliwe jest uzyskanie tego ostatniego, a więc, czy realne jest przeprowadzenie tajnych wyborów elektronicznych.

Model analogowy

Zanim jednak wejdziemy w świat elektroniki, na chwilę jeszcze zostańmy na ziemi i spróbujmy rzucić okiem na klasyczne wybory li tylko od strony ich bezpieczeństwa proceduralnego. Już w tym przypadku zapewnienie tajności wymaga precyzyjnej analizy. Oczywiście jest jasne, że główna idea polega na tym, że po prostu wchodzimy do kabiny pojedynczo i tam samodzielnie, bezpiecznie głosujemy. Ale czy na pewno nie ma tam ukrytych kamer? A czy długopis nie zostawia jakiegoś identyfikującego nas śladu?

Dalsze pytania można tylko mnożyć: Czy na pewno powinniśmy pozwalać wchodzić do kabin w dwie osoby, nawet jeśli są małżeństwem? A może jedna z nich jest pod presją drugiej? Czy nie jest problemem, gdy ktoś zrobi zdjęcie swojego głosu? A może chce ten głos sprzedać i udowodnić kupującemu, jak zagłosował?

Ktoś może powiedzieć, że to brzmi paranoicznie, gdyż oczywiście niby wiadomo, że istnieją takie zagrożenia, ale skomplikowanie ich wykonania oraz niewielki wpływ pojedynczego incydentu na ostateczny wynik pozwala założyć, że wszystko na koniec dnia i tak jest w porządku. Z opiniami tego typu, dotyczącymi wyborów tradycyjnych, akurat w tym miejscu polemizować nie będziemy. Zwróćmy jednak uwagę na ważną kwestię: nawet jeśli wierzymy, że w świecie niecyfrowym pojedyncze incydenty nas nie ruszają, to musimy sobie uświadomić, że w świecie elektroniki tak to nie działa. Tutaj wszelkie podatności i niedopatrzenia da się zwykle łatwo wykorzystać – i to najczęściej stosunkowo tanio – na skalę masową. Przecież gdy raz stworzymy wirusa, który potrafi odtajnić czyjś głos, to zadziała on nie na jednym, ale na tysiącach komputerów stosujących podobne oprogramowanie, którego jakąś lukę wykorzystujemy.

Model cyfrowy

Nie ukrywamy, że drobiazgowość i plastyczność sekcji wyżej miały na celu zatrucie głowy Czytelnika jedną konkretną myślą: otóż w przypadku potencjalnych głosowań elektronicznych skrupulatność graniczącą z paranoją w podejściu do bezpieczeństwa nie jest zwyczajową manierą matematyków, ale potrzebą totalnie bezwzględną i musi być postawiona absolutnie na pierwszym miejscu.

W szczególności już na starcie powinniśmy odrzucać jakiekolwiek pomysły związane z obecnością tzw. zaufanego serwera. To znaczy każdy model, w którym istnieje jakiś jeden wyróżniony Ważny Komputer, do którego np. dostarczane są cyfrowo podpisane głosy wszystkich wyborców, następnie ten komputer zlicza wynik, po czym skutecznie usuwa informacje o głosujących (*utajnia* wybory), jest modelem kryptologicznie **nie do przyjęcia**. Zauważmy bowiem, że przy takim podejściu całe zaufanie spoczywa tak naprawdę na administratorze tego komputera. Musimy przecież uwierzyć, że ów administrator niczego sobie nie zapamięta z rzeczy, które ma usunąć, niczego nie usunie z rzeczy, które mają być policzone itp. Nie o taki system nam chodzi.

Gdy realnie myślimy o bezpiecznym tajnym głosowaniu elektronicznym, zastanawiamy się, czy da się je tak zaprojektować, aby całe bezpieczeństwo było oparte o prawa matematyki, które działają *pod spodem*, a nie o zaufanie do nawet najbardziej nieskalanego administratora, ważnego sądu czy innego podobnego organu. W kryptologii bowiem zawsze paranoicznie (a może zdroworozsądkowo) zakładamy, że w systemie są obecni (a najlepiej: przejęli pełną kontrolę nad całą infrastrukturą techniczną) złoczyńcy, którzy nieustannie sposobią się do sfałszowania wyborów bądź ich odtajnienia.

Czytelnicy *Delty* (a szczególnie Czytelnicy serii „A jednak się da” ukazującej się w latach 2018–2019) orientują się jednak, że nie takie cuda oferuje współczesna kryptologia. Jakie są więc najlepsze protokoły kryptologiczne do tajnych głosowań elektronicznych?

W 2020 roku poważni i poważani kryptolodzy wystosowali do władz USA *Joint Internet Voting Avoidance Appeal*, apel o niewprowadzanie wyborów elektronicznych.

Już tytuł tego artykułu przebił balon napięcia, więc nie będziemy udawać: świat kryptologów nie wierzy w wybory elektroniczne. I to nawet nie na zasadzie, że istnieją jakieś trudności, których do tej pory nie udało się pokonać, ale wciąż jest otwarte pytanie: czy się uda w przyszłości? Nie. Umiemy udowodnić, że nie da się lepiej, niż tak jak umiemy. A tak jak umiemy – choć i tak ma prawo zachwycać – większości fachowców nie zadowala. Dalsza część tego artykułu będzie więc próbą wyeksponowania najważniejszych cyfrowych ograniczeń tej dziedziny oraz pokazania, co jednak się da.

Warta odnotowania jest ciekawa dualność: w wyborach tradycyjnych łatwiej zapewnić tajność, bardziej podejrzane jest liczenie głosów. W wyborach elektronicznych jest na odwrót: uzyskanie poprawnego wyniku jest zadaniem znacznie łatwiejszym niż zapewnienie tajności.

Królestwo za tajność

Okazuje się, że największym wyzwaniem jest właśnie tajność (a nie np. poprawność obliczonego wyniku) wyborów. Da się bowiem – i to dość zaskakująco prostym rozumowaniem – pokazać, że jeśli całkowicie nie ufamy systemowi – nieważne jak zaawansowany matematycznie by on nie był – to po prostu nie da się jej w pełni zapewnić. Dlaczego?

W rozumowaniu o Jasiu czynimy założenie, że system wie, kto aktualnie głosuje. Zakłada się bowiem, że nie istnieje żadna realna forma bezwzględnie bezpiecznej anonimowej komunikacji z systemem do głosowania. Czytelnik Nie Dający Za Wygraną może spróbować zgłębić istniejące próby realizacji anonimowej komunikacji np. w Δ^{9}_{17} i zastanowić się nad ich wadami w kontekście głosowania elektronicznego.

Rozważmy Jasia, który o wszystkim zapomniał i teraz szuka laptopa, aby zdążyć zagłosować tuż przed końcem. Jak to z Jasiem, możliwości będą tylko dwie: albo (a) Jaś nie zdąży, (b) Jaś będzie ostatnią osobą głosującą w wyborach. Zauważmy jednak, że poprawny system będzie w stanie podać wyniki wyborów w obu przypadkach. W systemie muszą więc być zawarte wszystkie informacje, które na to pozwalają. A to oznacza, że ktoś mający ciągły dostęp do wszystkich danych systemu będzie w stanie obliczyć obie te wartości: przed i po wizycie Jasia. Ale przecież z tych dwu danych da się odtworzyć głos Jasia!

Czy więc wszystko stracone? Czy cokolwiek możemy zrobić?

Możemy, o ile nieco poluzujemy założenia. Przy czym „nieco” nie jest tu bynajmniej eufemizmem. Otóż da się zapewnić tajność, gdy zaufanie do systemu jest z naszej strony naprawdę minimalne, a w zasadzie dowolnie małe, byle niezerowe. Bardziej konkretnie: załóżmy, że system działa w modelu rozproszonym i tworzy go nie jeden, ale np. tysiąc czy nawet milion komputerów. Wówczas, jeśli tylko ufamy w uczciwość choć jednego z nich (np. obsługiwanego przez nas samych albo przez przedstawicieli naszego obozu politycznego), to już tajność naszego głosu może zostać zapewniona!

Uzyskanie „minimalnego zaufania” dla matematyka jest trudne i nadzwyczaj efektowne. Ale niestety: specjaliści i prawnicy oceniają takie założenia jako wciąż niewystarczające.

Aby nieco obniżyć pułap lotu, warto zapoznać się z niektórymi artykułami z serii „A jednak się da”; w stosownych miejscach podajemy odnośniki.

Dokładnie na takim założeniu opiera się system głosowania elektronicznego, który zaprojektowali Ronald Cramer, Matt Franklin, Berry Schoenmakers i Moti Yung. Spróbujemy naszkicować ten dość skomplikowany protokół z lotu ptaka (i to niestety raczej takiego o wysokim pułapie lotu).

Protokół Cramer–Franklin–Schoenmakers–Yung, 1996

Zanim system zostanie uruchomiony, należy wybrać pewne parametry: skupimy się na dwóch najważniejszych: N i K, które spełniają nierówności $1 \leqslant K \leqslant N$.

Warto sobie uświadomić, że wybór parametrów (N, K) jest decyzją w zasadzie polityczną. Również można się zastanawiać, czy protokół wykonywać raz globalnie, czy np. niezależnie w każdym okręgu.

System będzie składać się z N komunikujących się ze sobą komputerów (oznaczmy je jako $s_1, \ldots, s_N$), co do których zakładamy, że uczciwych jest co najmniej K spośród nich. Przypadek $K = 1$ wydaje się więc najatrakcyjniejszy, ale jest tu też druga strona medalu – aby system *zawiesić* (nie dopuścić do wiarygodnego opublikowania wyników wyborów), wystarczy zmowa bądź awaria K komputerów. Tak więc zbyt małe K ma też swoje istotne wady.

Dalej wszystko będzie dość skomplikowane, ale jednak się uda:

- Jaś, aby oddać swój głos X, musi:
  - opublikować zobowiązanie $\mathit{Commit}(X)$ do swojego głosu (zob. Δ^{11}_{18}); zauważmy, że ten pozornie podejrzany krok bynajmniej nie zdradza wartości głosu (opublikowane zobowiązanie nigdy nie zostanie otwarte) – jest natomiast potrzebny później przy weryfikacji wyników;
  - opublikować dowód poprawności $\mathit{Proof}(X)$ swojego głosu (to znaczy udowodnić protokołem zero-knowledge (zob. Δ^{1}_{19}), że jego głos jest oddany w poprawnym formacie, np. ma wartość „NIE” lub „TAK”);
  - dokonać podziału swojego głosu protokołem Shamira (zob. Δ^{2}_{11}) na kawałki $X_1, \ldots, X_N$;
  - wysłać kawałek X_i do komputera s_i.

„Opublikować” oznacza tu pewne dodatkowe założenie: musimy założyć, że istnieje zaufane publiczne cyfrowe miejsce, do którego wszyscy mają łatwy dostęp do odczytu oraz gdzie można zapisywać dane, które nie mogą być usunięte w sposób niezauważony. To założenie nie uchodzi za bardzo podejrzane, ale też jego bezpieczna realizacja stanowi pewne wyzwanie.

- gdy wszystkie głosy zostaną oddane, wówczas wszystkie komputery tworzące system do głosowania:
  - pracując razem (według protokołu MPC podobnego do opisanego w Δ^{8}_{19}), są w stanie obliczyć wynik wyborów, nie ucząc się przy tym (o ile nie więcej niż $(N-K)$ spośród nich jest nieuczciwych) niczego na temat wartości jakiegokolwiek oddanego głosu.
  - publikują nie tylko ostateczny wynik wyborów, ale i dowód (protokół jest tak zaprojektowany, że jest to możliwe), że jest on poprawny. Każdy, kto ma dostęp do tego dowodu oraz kompletu nieotwartych zobowiązań (takich jak $Commit(X)$ Jasia), jest w stanie upewnić się, czy ostateczny wynik jest poprawny. Jest to niezwykle silna cecha omawianego protokołu. Oznacza ona bowiem, że nawet gdy liczba oszustów przekracza pułap $(N-K)$, to wyniku wyborów i tak **nie da się sfałszować (!)**, a tylko wywołać zamieszanie i konsternację – wszyscy przecież i tak się zorientują, że ostateczny wynik nie jest zgodny z oddanymi głosami.

Epilog epilogu

W tym artykule chcieliśmy pokazać smak wyzwań i skalę problemów przy projektowaniu protokołów do głosowania. Jak na razie, tajność wyborów została wyeksponowana jako główny i w zasadzie dowodliwie nierozwiązywalny problem. Piszemy „w zasadzie”, bo wszystko zależy od subiektywnej opinii co do tego, na jakie założenia się godzimy. Choćby w rozważanym protokole – można dyskutować, które parametry (N, K) dają wiarygodną tajność oraz pozwalają wierzyć, że protokół wyborczy kiedykolwiek zakończy się bez zawieszenia. Wybór $K = 1$ oraz $N \simeq 30\,000\,000$ (wówczas każdy uprawniony głosujący stałby się jednym z komputerów s_i, co niewątpliwie pozwala założyć, że każdy ufa przynajmniej jednej części systemu – mianowicie, samemu sobie) może i teoretycznie daje pełną tajność, ale przecież trudno uwierzyć, że taki protokół udałoby się przeprowadzić bez zakłóceń ze strony chociaż jednego komputera.

Co więcej, okazuje się, że – oprócz powyższego – istnieją jeszcze inne, trochę pozamatematyczne, ale niestety równie fundamentalne problemy, o których tutaj ledwie wspomnimy:

Po pierwsze – gigantycznym problemem jest potencjalny handel głosami (albo zastraszanie i wymuszanie – matematycznie to podobne zagadnienia). W świecie cyfrowym wydaje się on niestety znacznie łatwiejszy niż w świecie tradycyjnym. Głosujący może przecież zainstalować sobie kamerkę w domu i pozwolić komuś z zewnątrz na bieżąco upewniać się, że głosuje on zgodnie z jego wolą. Jest to na pewno wygodniejsze i bezpieczniejsze niż wszelkie podobne działania w rzeczywistym lokalu wyborczym.

Po drugie – pamiętajmy, że w świecie cyfrowym człowiek nie wykonuje obliczeń w głowie, ale korzysta z osobistego komputera, który pamięta za niego tajne dane, dokonuje wrażliwych obliczeń itp. Ten element jest zawsze podkreślany jako potencjalne ważne źródło problemów – nikt przecież tak do końca nie wie, jakie wirusy czy programy szpiegujące ma w swoim komputerze zainstalowane lub też nawet fabrycznie wbudowane. Oznacza to w szczególności, że pułap $(N-K)$ dotyczy nie tylko świadomych oszustów, ale też nieświadomych właścicieli podejrzanego sprzętu.

Melancholijne podsumowanie

Saga „A jednak się da” miała na celu przekonanie Czytelnika, że wiele z tego, co wydaje się cyfrowo niemożliwe do zrealizowania, nauka jednak zrealizowała i stworzyła protokoły, które dla zwykłego śmiertelnika są w zasadzie nieodróżnialne od magii. Ale niestety – pychą byłoby wierzyć (może trochę jak Hilbert?), że udawać się tak będzie zawsze...

W przypadku głosowań tajnych, mimo że te najlepsze protokoły aż jeżą się od zastosowanych perełek kryptologii, po prostu w pełni nie udało się. Musimy więc albo zrezygnować z głosowania cyfrowego, albo pogodzić się z którymś ze zgniłych kompromisów dotyczących definicji bezpieczeństwa takiego głosowania.

Wir müssen nicht alles wissen.

Dodajmy tu jednak łyżkę dziegciu. Wszystkie dowody, o których tu mowa, są *niepodrabialne* przy jeszcze jednym (powszechnie uważanym za rozsądne) dodatkowym założeniu – mianowicie: wierzymy, że logarytm dyskretny jest problemem trudnym obliczeniowo. Co ciekawe i ważne, da się pokazać, że nie da się skonstruować żadnego bezpiecznego protokołu głosowania elektronicznego bez tego typu obliczeniowych założeń. Nie jest to też coś zaskakującego – podobnie sprawa ma się w przypadku chociażby podpisu elektronicznego (zob. np. Δ^{10}_{18}).

Dodatkowo część protokołów (w tym prezentowany w tym artykule) jest skonstruowana tak, że aby handlować głosami, nawet nie trzeba robić nic specjalnego (typu instalowanie kamerek) w trakcie głosowania. Nawet już po głosowaniu da się stworzyć cyfrowy dowód (w naszym przypadku – wystarczy otwarcie zobowiązania $Commit(X)$), który można po prostu pokazać, aby udowodnić kupującemu (albo zastraszającemu), że głosowało się zgodnie z jego poleceniem. Na szczęście istnieją protokoły pozbawione akurat tej wady, np. protokół Canetti-Gennaro z 1997 roku.

Niektórzy postulują, aby nie używać do głosowań własnych komputerów, tylko dedykowanych superbezpiecznych urządzeń. Oczywiście naturalne jest pytanie, kto te urządzenia by wytwarzał i jak dowodził, że faktycznie działają poprawnie.

Delta, maj 2004