Túri Éva

Doodle vs Dudle

két szavazási szolgáltatás elemzése, összehasonlítása

8. téma

Tartalomjegyzék

1 Bevezetés

A szavazás és konszenzus keresés története valószínűleg évezredekre nyúlik vissza, optimista hozzáállás szerint egyidős az emberiséggel. Ahogy azonban az alanyai fejlődtek úgy fejlődött maga a szavazás rendszere is. A kézfeltartástól a cserépdarabra való karcoláson át a papír alapú megoldásokig sok forma kipróbálásra került, amelyek a célra ugyan alkalmasak voltam ám általában valamilyen megszorítással.

Ahogy az informatika elérte azt a fejlettségi szintet, hogy szóba kerülhetett, mint a fejlődés egy újabb lépcsőfoka, úgy el is kezdték keresni a szokásos problémákra a lehetséges informatikai válaszokat. Például arra, hogy az egyes szavazók ne tudhassák a másik kire adta le voksát kezdetben ezt a legegyszerűbben elfordulással lehetett biztosítani, vagy azzal hogy mindenki egy közös edénybe helyezte szavazatait, amik csak akkor kerültek elő onnan, amikor megszámlálásra, összegzésre került sor. Ez a fajta megoldás elsőre kicsit idejétmúltnak tűnik ám az informatika esetében az alap ötlet továbbra is hasonló folyamaton nyugszik, csak elfordulás helyett kriptográfiai algoritmusok biztosítják a válaszok egymástól való elkülönítését.

A kezdeti fejlődéssel párhuzamosan a szavazás minőségének javulása is megindult egyre elterjedtebb lett az elvárás, hogy maga az eljárás ingyenes legyen, mindenki számára hozzáférhető, anonim, de mégis átlátható és ellenőrizhető. Az egymásnak látszólag ellent mondó elvárásokat azonban jól lehet matematikailag modellezni.

Az internet széles körben való elterjedésével egyidejűleg felmerült, hogy az egész folyamatot érdemes lenne az online környezetbe átültetni. A költségcsökkentésen túl, a szavazók elérése és az adatfeldolgozás folyamata is jóval egyszerűbbé válna és lévén a szavazói problémát részekre tagoltan lehet matematikai problémaként értelmezni, jogosan feltételezhető, hogy matematikai megoldás is létezik rá.

Ebben a dolgozatban ennek az elképzelésnek a gyakorlatban már megvalósult és működőképes két formáját fogom vizsgálni az általános elvek mellett külön hangsúlyt fektetve a privátszférát érintő kérdésekre.

2 Értékelési szempontok

Ahhoz, hogy a különböző rendszereket össze lehessen hasonlítani, nem csak egymással, hanem általánosságban a szavazó rendszerekkel szemben támasztott elvárásokkal, szükség van néhány szempontra, ami támpontot ad.

Az alábbi szempontok a Privacy-Enhanced Event Scheduling[2] alapján kerültek összeállításra:

- Ellenőrizhetőség: minden szavazó ellenőrizni tudja, hogy a többiek nem csaltak és az ő szavazatát számolták
- Privacy: a többi résztvevő nem láthatja a konkrét szavazatot, csak az eredményt
- Nem megbízható szerver: a közbülső résztvevőkben a lehető legkisebb bizalom
- Használhatóság: egyszerű lépések, semmilyen plusz tudás nem szükséges a használatához
- Hatékonyság: nagyszámú lehetőséget és sok részvevőt legyen képes kezelni

Ezeken a pontokon kívül rá fogok mutatni az általánosan jelen lévő biztonsági hibákra is, illetve amikor lehetséges megoldási javaslatot teszek.

3 Doodle

3.1 Eredete

A Doodle az elsők között kezdte el működését 2006-ban online időpont egyeztetetés és szavazás területen. Azóta a jelenlegi sokszereplős piacon piacvezetőnek számít, töretlen népszerűséget jól jellemzi, hogy 2011 szeptemberében elérte a 10 millió felhasználó/hónap rátát és ez a szám, azóta is növekszik [1]. Talán ennél is jobban bizonyítja azonban megbízható működését, hogy a felmérés szerint 98% mások ajánlására próbálta kezdte használni a rendszert.

Az általános, ingyenesen elérhető változat mellett van egy fizetős szolgáltatásuk is főleg vállalatok számára, ami akár az összes cégen belül szavazást (tulajdonképpen az időpont egyeztetés is szavazás) képes kezelni. Ez és a folyton jelen lévő hirdetések mutatják, hogy a vállalat szigorúan üzleti alapokon működik.

3.2 Működése

A legelső használatba vétel előtt regisztrálnia kell annak, aki szavazást szeretne kiírni. Ehhez szükséges megadnia egy választott felhasználói nevet, jelszót a későbbi azonosításhoz, illetve értesítésekhez egy email címét.

Ez nem minden esetben szerencsés, hiszen az email címre semmi szüksége nincs a szolgáltatónak addig a pontig, amíg nem kér a felhasználó folyamatos tájékoztatás az általa kiírt szavazás állapotáról. Véleményem szerint elég lenne ezen a ponton egy elérhetőséget kérni, nem pedig a regisztrációt ettől függővé tenni.

Ha ezen túljutott a felhasználó a következő lépésekben már egy varázsló végigkíséri a az időpont egyeztetés vagy szavazás kiírásának folyamatán. Ez a megoldás könnyen kezelhetővé és felhasználó baráttá teszi a programot.

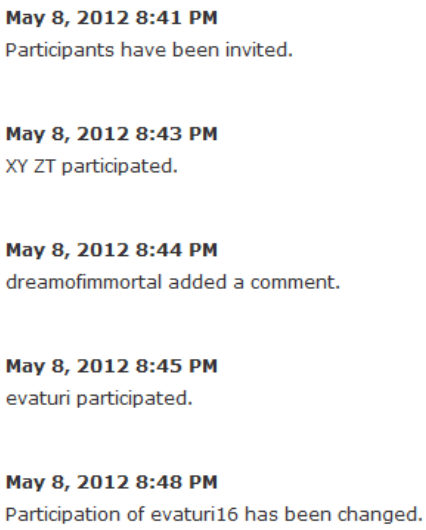
A szavazás elkészítése közben lehet beállítani, milyen típusú szavazást szeretnénk létrehozni biztonsági szempontból. Az egyik megoldás az, hogy bár meghívunk minden résztvevőt a felületre, nekik nem kell magukat előzetesen beazonosítani, elég, ha a link

birtokában vannak és az első üres sorban megadnak valamilyen becenevet, ami később az ő válaszukat azonosítja és ezzel tulajdonképpen kész is van a folyamat. Jóhiszeműen közelítve a dolgot ez egy teljesen elfogadható megoldás, könnyű megjegyezni a lépéseket és az eredmény is vizuálisan, könnyen értelmezhetően azonnal megjelenik. Azonban semmilyen védelmet nem biztosít az esetleges ártó szándék ellen.

1. ábra Doodle általános felület

A másik lehetőség, hogy a választás anonim vagy legalábbis ahhoz hasonló keretek között menjen végbe. Ehhez minden résztvevőnek regisztrációval kell rendelkeznie, ami a honlaphoz köti őket és egyértelműen azonosítja őket több szavazáson keresztül is. Továbbá lehetővé teszi a profilkészítést, ezáltal az anonimitásnak magának a tényleges hasznát kérdőjelezi meg. Egyrészt mások nem látják a szavazatot és módosítani sem tudják azt, ugyanakkor a szolgáltató felé egyre több és több adatot árul el magáról.

Ha a funkció használata mellett dönt, akkor a meghívott tagok válasza a többiek számára nem lesz nyilvános, csak az összesítésben jelenik meg. Illetve maga a szavazás időpontja sem kerül rögzítésre még a kiíró által visszanézhető log adatokban sem. Ami egyébként minden változtatást tárol, de nem feltétlenül beazonosítható módon.



2. ábra Doodle naplófájl minta

A fent látható logsorból például nem derül ki pontosan, mi történt, csak az egyes eseményeknek marad nyoma. Annak, hogy a meghívások el lettek küldve, érkezett két szavazat, egy komment és valaki megváltoztatta az egyik felhasználó válaszait. Az nem egyértelmű, milyen mértékben és konkrétan mi került módosításra, arra pedig utalás sincs, hogy ki lehetett a módosító. Jelen esetben az egyik résztvevő neve lett megváltoztatva, a válaszok megtartásával, de ha azok is módosultak volna, akkor is csak ennyi jelenne meg a naplóadatokban.

3.3 Hiányosságok, megoldandó problémák

Az első szembeszökő probléma, hogy a szavazásokat nem lehet zártkörűvé tenni. A link birtokában ugyanis bárki hozzáadhat újabb álfelhasználókat, akik nyíltan szavaznak, módosítva ezzel az eredményeket. (Ez a lehetőség akkor is adott, ha az anonim megoldást választjuk, az eltérés annyi, hogy aki nem kapott meghívót nem szavazhat anonim módon.) Ha sok felhasználó keres közös megoldást ez nem lesz annyira triviálisan nyomon követhető. Zaj kerül az adatokba, kellően nagyszámú válaszadó esetén a kimenetet is lehet ezáltal módosítani.

A másik, ennél nagyobb probléma, hogy a leadott válaszok semmilyen biztonsági védelmet nem élveznek alap esetben. Bárki bármikor törölheti, módosíthatja azokat anélkül, hogy azok visszaállítására lehetőség lenne. Arról nem is beszélve, hogy a naplózott eseményekből sem visszakövethető ki volt az elkövető, hiszen a nyilvánosra

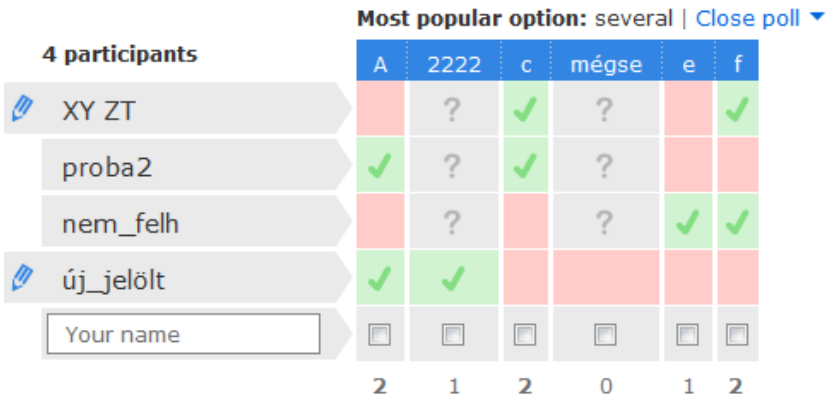
állított szavazások esetében az előzetes azonosítás csak opció nem feltétel. Ezzel a hiányossággal az egész szavazás tényleges eredményének hitelességét illetve magának a folyamatnak az értelmét kérdőjelezik meg, hiszen mi a megoldás abban az esetben, ha már X-en válaszoltak a feltett kérdésre, ám az X+1 felhasználó kitörli az egész szavazást, ugyanis erre is van lehetősége.

Előre lépést jelent, hogy az anonim opció védelmet jelent ez ellen. Mindenki csak a saját eredményeit láthatja, és azokat módosíthatja. A szavazás pontos időpillanatáról nem készül feljegyzés, hogy ezzel is növeljék az egyének biztonságát, adatainak védelmét. Azért fontos ez, mert ha valaki egy adott időpillanatban töltötte ki, akkor valószínűleg éppen ráért, ami a napi beosztásába enged egy rövid bepillantást, illetve ez és a megadott válaszok alapján akár azonosíthatóvá is válik. Például céges környezetben, ha valaki jellemzően 10 és 14 óra között ér rá, az könnyen visszakereshető a vállalat alkalmazottainak időbeosztásával egybevetve.

További probléma, hogy a szavazáshoz bárki hozzáfér, és nem anonim módon tud hozzáadni sorokat. Ezeket később természetesen figyelmen kívül lehet hagyni, ám mégis bosszantó lehet, ha nagy mennyiségben szemetelik tele az eredményt.

A létrehozó, kiíró lehetőségei is kérdéseket vetnek fel. Optimális esetben elvárás, hogy ne csak a válaszadók egymás között, de a kiíró se tudjon arról ki mikor és mit válaszolt. Erre csak részleges megoldás van jelenleg a Doodleben, biztonságos módban. Nem biztonságos módban minden további nélkül manipulálhatók a válaszok, nem csak újabb sorok hozzáadásával, de meglévők módosításával, sőt új lehetőségek hozzáadásával, régiek szerkesztésével is. Erről pedig a felhasználók nem kapnak automatikusan értesítése. Ezért ebben a beállításban csak akkor lehet érdemes tehát használni, ha egyik résztvevő félnek sem érdeke, hogy az eredményt manipulálja.

A biztonságos megoldás valamivel kifinomultabb, az anonimen szavazó résztvevők eredményei nem módosíthatók direkten, azonban maga kérdés és lehetséges válaszai igen, a kiíró által úgy, hogy a korábban válaszolók semmilyen automatikus (a létrehozótól független) értesítést nem kapnak erről, annak ellenére sem, hogy az ő email címük megvan a rendszerben, tehát a technikai lehetőség adott. Hitelességi szempontból további problémát jelent a már meglévő válaszok kezelése is.



3. ábra Doodle változáskezelése

Ezen az ábrán jól kivehető, hogy a korábban anonimen szavazó résztvevők adatait igaz nem lehet módosítani külsőleg, és a szavazás pontos idejét sem lehet ad hoc megmondani, ám ha hozzáadunk egy újabb lehetőséget (oszlopot), akkor mindenki számára egyértelmű, hiszen másképp jelölik, hogy ki szavazott a változtatás előtt és ki utána. Így bizonyos időközönként ismételve ezt az opciót, nyomon követhető a válaszadók időbeli mozgása és sorrendje. Az is biztonsági problémát jelent, hogy a kiíró látja mindenki válaszát és egyedül ő módosítani is tudja az eredményeket. Ez nagyfokú bizalmat vár el a résztvevőktől a kiíró felé.

Arra a problémára, hogy mi van olyankor, ha valaki a teljes táblázatot folyamatosan monitorozza, jelenleg nem kínálnak megoldást. Fejlesztési ötlet lehet, hogy csak bizonyos időközönként jelenjenek meg új eredmények esetleg csoportosan 2-3 új válaszonként jelenjenek meg.

Összességében könnyen és gyorsan használható a rendszer, ami majdnem az összes szavazásra meghatározott elvárásra kínál valamilyen szintű megoldást, ám tényleges használatához nagyon jóhiszemű felhasználókra és támadás mentes környezetre van szükség.

4 Dudle

4.1 Eredete

A Prime Life keretei között megvalósult szavazó és időpont egyeztető rendszer nagyban hasonlít a Doodlere, ám annak privát szférát érintő hiányosságait igyekszik kiküszöbölni. Ez a rendszer is ingyenesen használható és lévén PrimeLife keretében valósult meg, non profitként működik, ezért nincs reklám az oldalon elhelyezve.

4.2 Működése

Az indulásnál nincs szükség regisztrációra és bár nem annyira vizuálisan, mint a Doodle esetében itt is erős segítséget kap a felhasználó. A két felület nagy mértékben hasonlít egymásra a felépítéstől a színkódolásig.

A szavazás kiírására itt is két mód, út választható. Az első esetben egy teljesen nyilvános szavazást lehet létrehozni, ami mindenki számára hozzáférhető, és hasonló manipulálási lehetőségeket tartalmaz, mint a Doodle Fontos különbség azonban, hogy itt nem küldenek ki semmilyen adatot további analizálás céljából, ezáltal is védve a felhasználókat.

További előre lépés, hogy a kiírások automatikusan törlődnek, ha 3 hónapon keresztül nem érkezik rájuk lekérés. Így még az önhibából ugyanolya nevet használó felhasználók is kapnak egyfajta védelmi hálót.

A második út a pszeudo anonimitást elősegítő lehetőség, mely keretében minden résztvevőnek regisztrálnia kell egy nevet az oldalon. Azonban saját adatok megadása helyett elég egy becenevet beírni, és a rendszer automatikusan generál egy 37 karakteres kulcsot, aminek a segítségével később a felhasználó nevet lehet használni szavazásra. Ebben az esetben a kiíró csak azokat tudja anonim szavazásra meghívni, akik már szerepelnek a rendszerben. Erről ők nem kapnak értesítést, a linket külön meg kell osztani.

A névtárolás - hozzáadás folyamata valószínűleg a későbbiekben - ha a rendszer felhasználói bázisa drasztikusan megnő - problémás lesz és fejlesztésre szorul, ugyanis jelenleg a felhasználó kiválasztása egy listából történik tulajdonképpen, amit ha valakinek ez érdekében áll, végig ki lehet menteni. Ami kicsiben még nem feltétlenül okoz komoly gondot, az a növekedés után problémás lehet, hiszen egyre speciálisabb azonosító megadására lesz szükség ahhoz, hogy felhasználónevet létre lehessen hozni. Ám ha ezeket javaslatként megjelenítve bárki láthatja egy szavazás készítése során, akkor megmondható, hogy ki használja már a szolgáltatást és akár harmadik fél számára is egyértelmű lesz a szavazáson résztvevők személye. Ami, például ha egy bizalmatlansági indítványban kell dönteni, komoly problémákhoz is vezethet.

Az anonim szavazás kérdése újabb buktatónak van kitéve az összegzésnél. Ez automatikusan történik meg minden rendszerben. Akkor, ha teljesen nyilvánosak a válaszok ez egy előre mutató lehetőség, aminek reális haszna van, nem kell később visszatérni az eredmények megtekintéséért, illetve adott esetben már a csoport összességéhez képest alkalmazkodva adhatják meg a válaszaikat a felhasználók.

Azonban, ha azt a megoldást választjuk, hogy nem szeretnénk bizonyos felhasználók válaszait mások elé tárni, ez a végeredményen nem váltat. Ugyanúgy megjelennek az összesítések, mintha nyíltak lennének a válaszok és kevés résztvevő esetén, különösen, ha vegyes megoldás mellett döntünk, egyszerűen kiszámolhatóak az egyes válaszok külön is.

4. ábra Dudle eredmény problémája

Erre megoldást jelenthetne, ha titkos válaszokat is tartalmazó választások esetén a részeredményeket csak valamilyen külső kritérium teljesülése alapján lehetne látni. Például, ha már legalább hárman szavaztak ezen a módon.

Ez a probléma a Doodlenél és a többi ilyen jellegű rendszernél is fent áll. Egyéni profilokat kezelő rendszereknél, mint a Doodle megoldást jelenthet az is, hogy az eredményeket személyre szabottan jeleníti meg bejelentkezés után. Például a válaszaim megadása után csak azok a lehetőségek maradnak zölddel kiemelve, amik számomra és a többi résztvevő összességének is alkalmasak. Meg lehetne határozni külön szabályokat arra nézve, hogy 2 egyéb válasz esetén a közös eredményben megjelenik sárgán (ez a „talán” színe mind két helyen) egyébként pedig pirosan („nem” lehetőség).

A fenti problémákat leszámítva felfedeztem egy speciálisan a Dudlere szóló sebezhetőséget is. A kulcsgenerálásnál nincs meghatározva, hogy egyszerre hány új felhasználót lehet felvenni a rendszerbe. Ezzel önmagában nincs is probléma, azonban, ha valaki ártó szándékkal közeledik, megteheti azt, hogy egy tetszőleges névhez generáltat egy kulcsot, amit elment magának, majd átkattint egy másik fülre. Ekkor a fiók nem jött ugyan létre, de az adatok a regisztrációs oldalról kitörlődtek, és visszaállt a felület a kiindulási állapotba. Ha most egy másik nevet regisztrál valaki, a rendszer nem generál új kulcsot, hanem az előzőleg legenerált, megjelenített kulcsot osztja ki újra. Mivel a böngészőben vagy a felületen semmi jele nincs annak, hogy korábban valaki már elindított egy regisztrációs folyamatot, nincs, ami figyelmeztesse a felhasználót.

Megoldást jelentene, ha nem csak a cancel vagy az ok gomb lenyomása, akkor, vagy az ablak bezárásakor küldene visszajelzést az oldal a generáló algoritmusnak, hanem akkor is, ha félrekattintnak belőle. Vagy legalább a már előzőleg felfedett kulcsot ne törölje ki automatikusan.

További elméleti problémát jelenthet, hogy ezt a kulcsot nem lehet módosítani. Ez természetesen az erőssége is a rendszernek, hiszen így következetesen minden felhasználónak egy 37 karakteres egyedi jelszava lesz. Azonban egy átlagos felhasználótól nem elvárható, hogy ezt a számára hosszú és véletlennek tűnő

karaktersorozatot megjegyezze. A manuális begépelési megoldás miatt pedig a böngésző sem jegyezheti meg.

Tehát ez ugyan erősség, nem probléma, az viszont igen, hogy a mindennapi életben való használatához fog vezetni, hogy ezeket a kulcsokat valahol fizikailag is tárolni kell. Valószínűleg nem post it cetlin a monitorra ragasztva, hanem egy dokumentumba elmentve, de feltételezhetően mindenfajta titkosítást nélkülözve kerülnek majd tárolásra. Ez pedig a gyakorlati életben az anonim szavazás életképességét veszélyezteti, hiszen ha megszerezhető a kulcs, ráadásul egyszerűen, akkor onnantól a korábbi szavazásokra leadott voksokat is meg lehet nézni, módosítani lehet azokat, a nélkül, hogy ez bárkinek feltűnhetne.

A másik érdekesség, hogy ezeket a kulcsokat nem lehet újra generáltatni. Tehát, ha valakinek elveszik a kódja, akkor egy teljesen új névvel igényelhet másikat, de ez természetesen a korábbi szavazásokra nem lesz érvényes. Ráadásul nem lehet azt megtenni, hogy bármilyen nyilvános szavazásban anonim módon szavaz valaki, ehhez újra fel kell magát vetetnie a szavazást kiíróval a válaszadók listájába, és akkor tud új szavazatot leadni. Ha például módosítani szerette volna egy korábbi eredményt, erre semmilyen lehetősége nincs, és a kiíró sem törölheti ezt az eredményt, tehát valamekkora zaj marad a rendszerben. Ezt csak akkor lehet kiszűrni, ha a válaszadó felfedi, mi volt az első szavazata. Ami pedig az egész anonimitási és használhatósági funkciót megkérdőjelezi, hiszen könnyű célponttá teszi a támadók felé.

5 Összehasonlítás

Mint a rendszerismertetéseknél rámutattam, egyik változat sem hibátlan, vannak bennük bugok és komolyabb elvi hiányosságok is. Azonban a közös problémákon kívül egyediekkel is rendelkeznek, amik mégis összehasonlíthatóvá teszik őket.

A privát szféra biztonságát szem előtt tartva, a Doodle egyébkén profilépítésre is alkalmas, email címet igénylő megoldása egyértelműen nem jó. Arról nem is beszélve, hogy a folyamatos monitorozás eredményét külső félnek is kiadják elemzésre. Csak halvány részsikerként könyvelhető el, hogy a kiadásra kerülő adatokban az IP címet titkosítják[3]. Ennek a titkosításnak a részletei azonban nem nyilvánosak, illetve kutatások bizonyítják, hogy ma már nem csak és kizárólag az IP cím alapú azonosítással lehet valakit nyomon követni vagy beazonosítani online.

További különbség, hogy nyilvános szavazásokkor a Dudle automatikusan kiírja minden résztvevőhöz, hogy mikor szavazott és a megfelelő sor mellett ezt meg is jeleníti. Egy PET megoldástól ez egy érdekes lépés.

A közbülső szereplőben való megbízás és az ő manipulálási lehetőségeinek kiiktatása Doodle esetében nem jelentkezik, hiszen magában a szolgáltatóban meg kell bízni (hogy nem módosítja a kiírást, nem naplóz rosszul, stb), ez a Dudlenél annyiban módosul, hogy a rendszer teljes átláthatósága miatt könnyen nyomon követhetőek benne az ilyen jellegű változások.

	Doodle	Dudle
Könnyen kezelhető	Nagyon	Közepesen
Nyomon követhető	Igen	Nem
Privátszféra barát	Nem	Igen
Utólag módosítható	Igen	Igen
Időben követhető	Logok és egyéb módszerek	Csak a nem biztonságos változatban
Azonosítható szavazó	Regisztráltként	-
Szerverben való megbízás	Magas	Alacsony
Ellenőrizhetőség	Nem	Nem

5. ábra Doodle vs Dudle

6 Következtetés

Összességében mind a két irányban vannak előremutató fejlesztések, lehetőségek. Ha az általános, minden online szavazó rendszert érintő problémákat nem is, de a saját következetlenségeiket és támadási pontjaikat javítják, akkor életképes lehet a megoldás.

Személy szerint a Dudle megoldásától többet, stabilabb teljesítményt vártam. Az egyéni problémák száma kicsit magasnak tűnik, ahhoz képest, hogy annyival nem nyújt több lehetőséget, mint a Doodle.

Azonban a központi kulcs generálás és az, hogy a szavazat kiíró sem tudja az anonim szavazást utólag változtatni biztató előrelépés. Amennyiben a többi hibát is javítják, életképes vetélytársa lehet a Doodlenek.

7 Irodalomjegyzék

[1]: http://en.blog.doodle.com/2011/10/11/doodle-crosses-the-10-million-user-mark/ letöltve: 2012.04.30

[2]: Benjamin Kellermann and Rainer Böhme, „Privacy-Enhanced Event Scheduling" 2009

http://www.google.hu/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&ved=0CG0QFjAC&url=http%3A%2F%2Fdud.inf.tu-dresden.de%2F~ben%2Fkellermann09_privacy-enhanced_event_scheduling.pdf&ei=bCSqT_DbKOek4AS1hPjBCQ&usg=AFQjCNFm4Tl-LiLomhoNYx0o2GvkJzvwTA&sig2=avTEuQbIbJhXKr2xj2xfEA letöltve: 2012.04.30

[3]: http://doodle.com/about/policy.html letöltve: 2012.04.30

[4]:Thomas Herlea, Joris Claessens, Gregory Neven, Frank Piessens, Bart Preneel, and Bart De Decker. On securely scheduling a meeting. In M. Dupuy and P. Paradinas, editors, *Trusted Information: The New Decade Challenge, IFIP TC11 Sixteenth Annual Working Conference on Information Security (IFIP/Sec'01)*, volume 193 of *IFIP Conference Proceedings*. Kluwer Academic Publishers, pages 183-198, 2001.

[5]: Dudle – Privacy-Enhanced Event Scheduling

http://www.google.hu/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CGUQFjAA&url=http%3A%2F%2Fdud.inf.tu-dresden.de%2F~ben%2Fkellermann09_privacy-enhanced_event_scheduling.pdf&ei=oSaqT5z0Hoj04QTPqYG4AQ&usg=AFQjCNFm4Tl-LiLomhoNYx0o2GvkJzvwTA&sig2=ThYK4psX7Uo_0GV7dO5B6A letöltve: 2012.04.30