

Online verkiezingen in de praktijk: verbetering en toepassing van het Helios verkiezingssysteem

Pieter Maene

Thesis voorgedragen tot het behalen
van de graad van Master of Science
in de ingenieurswetenschappen:
elektrotechniek, optie Ingebedde
systemen en multimedia

Promotor:

Prof. dr. ir. B. Preneel

Assessoren:

Prof. dr. ir. V. Rijmen

Prof. dr. ir. L. Van Eycken

Begeleiders:

Dr. ir. J. Hermans

Dr. ir. F. Vercauteren

© Copyright KU Leuven

Zonder voorafgaande schriftelijke toestemming van zowel de promotor als de auteur is overnemen, kopiëren, gebruiken of realiseren van deze uitgave of gedeelten ervan verboden. Voor aanvragen tot of informatie i.v.m. het overnemen en/of gebruik en/of realisatie van gedeelten uit deze publicatie, wend u tot ESAT, Kasteelpark Arenberg 10 postbus 2440, B-3001 Heverlee, +32-16-321130 of via e-mail info@esat.kuleuven.be.

Voorafgaande schriftelijke toestemming van de promotor is eveneens vereist voor het aanwenden van de in deze masterproef beschreven (originele) methoden, producten, schakelingen en programma's voor industrieel of commercieel nut en voor de inzending van deze publicatie ter deelname aan wetenschappelijke prijzen of wedstrijden.



Voorwoord

Pieter Maene

Inhoudsopgave

Voorwoord	i
Inhoudsopgave	ii
Samenvatting	iv
Lijst van figuren en tabellen	v
Lijst van afkortingen en symbolen	vii
1 Inleiding	1
2 Literatuurstudie	3
2.1 Geschiedenis [2]	3
2.2 Vereisten	4
<i>Vertrouwen</i> 4, <i>End-to-End Verifiability</i> 4	
2.3 Systemen zonder cryptografie	5
<i>Open Counting</i> [1] 5, <i>Floating Receipts</i> [37] 6 ,	
<i>ThreeBallot</i> [35] 7 , <i>Scratch-Card</i> 10	
2.4 Systemen met cryptografie	11
<i>Secret-Ballot Receipts</i> [8] 11, <i>Scratch & Vote</i> [5] 13	
2.5 Conclusie	15
3 Helios	17
3.1 Cryptografische technieken	17
<i>ElGamal</i> [16] 17, <i>Homomorfe encryptie</i> 18, <i>Threshold</i>	
<i>encryptie</i> 19	
3.2 Stemhokje	20
3.3 Ballot Tracking Center	21
3.4 Controleapplicatie	21
4 Procedure	23
4.1 Voorbereiding	23
<i>Trustees</i> 23, <i>Vragen</i> 23, <i>Kiezers</i> 23	

4.2	Helios	24
	<i>Aanmaken van de verkiezing</i> 24, <i>Trustees</i> 25, <i>Vragen</i> 26, <i>Kiezers</i> 26, <i>Bevriezen van het stembilhet</i> 28, <i>Telling</i> 28	
5	Interface	29
5.1	Beheer	29
5.2	Trustee Dashboard	31
5.3	Controleapplicatie	32
6	Kringverkiezing	37
6.1	Aanpassingen	37
	<i>Shibboleth</i> 37, <i>Opkomst</i> 37, <i>Publicatie van het resultaat</i> 38	
6.2	Testen	38
	<i>Beheer</i> 38, <i>Stemhokje</i> 39, <i>Stresstest</i> 40	
6.3	Stemdag	41
7	Bewaren van sleutels en fingerprints	43
7.1	Sleutels	43
	<i>Disk</i> 43, <i>Web Storage</i> [18][28] 44	
7.2	Fingerprints	44
8	Web Cryptography API	45
8.1	Web Cryptography API [40]	45
8.2	NfWebCrypto	45
8.3	Benchmarks	46
	<i>Modulaire exponentiatie</i> 46, <i>RSA</i> 47	
8.4	Besluit	48
9	Besluit	51
A	English Paper	53
	Bibliografie	55



Samenvatting

Verkiezingen hebben een belangrijke rol in een democratische maatschappij. Kiezers moeten op een betrouwbare en gebruiksvriendelijke manier hun stem kunnen uitbrengen. Bij de huidige systemen moet de kiezer vertrouwen hebben in de organisatie die de verkiezingen organiseert. Een voter-verifiable stelsysteem geeft de kiezer de mogelijkheid om na te gaan of zijn eigen stem correct geregistreerd is en dat het resultaat correct is.

Het is mogelijk om een dergelijk systeem met papieren stembiljetten te implementeren, zowel met als zonder cryptografische technieken. Helios is een voter-verifiable stelsysteem voor online verkiezingen. De procedure die bij deze systemen gevolgd moet worden, is echter vaak zeer complex.

In deze thesis wordt de procedure gegeven die in Helios gevolgd moet worden om een verkiezing op te zetten. De interface van het systeem werd ook herwerkt om de beheerder beter te ondersteunen. Ook de applicatie die gebruikt wordt door de kiezers werd vereenvoudigd. Na het systeem uitgebreid getest te hebben, werd het in de praktijk gebruikt voor een reële verkiezing waarbij ongeveer 750 mensen hun stem uitbrachten.

Daarnaast wordt besproken hoe de trustees hun geheime sleutels kunnen bewaren. Er wordt ook onderzocht of de fingerprints waarvoor momenteel strings gebruikt worden niet op een betere manier weergegeven kunnen worden. Tot slot worden de prestaties van de Web Cryptography API vergeleken met deze van bestaande implementaties in JavaScript. Deze nieuwe specificatie geeft ontwikkelaars toegang tot cryptografische functies die in de browser ingebouwd zijn.

Lijst van figuren en tabellen

Lijst van figuren

2.1	Multi-Ballot[35]	7
2.2	Scratch-Card biljet[31]	10
2.3	Strookje met optische geëncrypteerde stem[8]	12
2.4	Laatste stukje ticket met beide kanten nog samen[8]	12
2.5	Scratch & Vote biljet[5]	14
2.6	Scratch & Vote encryptie[5]	14
3.1	Uitgebrachte stem	21
4.1	Aanmaken van de verkiezing	24
4.2	Trustees	25
4.3	Threshold schema	26
4.4	Vragen	27
4.5	Uploaden van kiezers	27
4.6	Admin	28
5.1	Overzicht van de verkiezing (oud)	30
5.2	Beheer van de verkiezing	30
5.3	Voortgang procedure	31
5.4	Trustee Dashboard	32
5.5	Genereren van encrypted shares (oud)	33
5.6	Genereren van encrypted shares	33
5.7	Controleapplicatie (oud)	34
5.8	Controleapplicatie	35
6.1	Laatste scherm van het stembokje	40
6.2	Bevestigen van de stem	40
6.3	Resultaat van de stemming	42
7.1	RoboHash van de fingerprint in Figuur 6.2	44

8.1	Modulaire exponentiatie	47
8.2	RSA	49

Lijst van tabellen

8.1	Modulaire exponentiatie	48
8.2	RSA	48



Lijst van afkortingen en symbolen

Lijst van symbolen

pk	Publieke sleutel
sk	Geheime sleutel
df	Decryptiefactor

Inleiding

Verkiezingen zijn een essentieel onderdeel van het democratisch proces en spelen dus een zeer belangrijke rol in onze maatschappij. In 2014 vinden in 40 landen nationale verkiezingen plaats. 42% van de wereldbevolking zal dit jaar hun stem kunnen uitbrengen.[15] Ook in België is 2014 een groot verkiezingsjaar: op 25 mei wordt tegelijk gestemd voor het Europees parlement, de Kamer van volksvertegenwoordigers en de verkiezing van de deelstaten (Vlaams of Waals parlement).

In 2012 werd tijdens de presidentiële verkiezingen in Amerika door beide kandidaten ongeveer één miljard dollar uitgegeven tijdens hun campagne.[43] In België werd tijdens de federale verkiezingen van 2010 door alle partijen samen 13,7 miljoen euro gespendeerd. Niet alleen de budgetten van de kandidaten zijn zo hoog: de kosten van de organisatie worden voor 25 mei op meer dan 10 miljoen euro geschat.[42]

Gezien het belang van de verkiezingen en de enorme bedragen die ermee gemoeid gaan, is het dus noodzakelijk dat er een betrouwbaar systeem is om het resultaat vast te leggen. Het moet bovendien eenvoudig te gebruiken zijn door de kiezers. Tijdens de Amerikaanse presidentsverkiezingen van 2000 werd in Palm Beach County, Florida een biljet gebruikt dat verwarrend zou zijn. Dit kreeg des te meer aandacht omdat de uitslag erg nipt was.[46] In België stemt bijna de helft van de kiezers elektronisch, maar ook hier kan de interface voor problemen zorgen. Tijdens de gemeenteraadsverkiezingen van 2012 kon per ongeluk een voorkeurstem gegeven worden door te lang op het scherm te duwen.[24] In veel steden werden voor 25 mei stemcomputers ter beschikking gesteld om op te oefenen.[33]

Het is dus niet eenvoudig om een gebruiksvriendelijke oplossing te ontwikkelen, noch voor papieren biljetten, noch wanneer digitaal gestemd wordt. Daarnaast heeft de kiezer vandaag geen enkele manier om na te gaan of zijn stem juist meegeteld is en dat het algemene resultaat correct is. Hij moet de instantie die de verkiezing organiseert dus volledig vertrouwen. Dit kan opgelost worden door gebruik te maken van een voter-verifiable systeem. Een groot nadeel is echter dat veel van deze systemen een complexe procedure hebben. Helios is een systeem dat het mogelijk maakt om online voter-verifiable verkiezingen te organiseren.

In [Hoofdstuk 2](#) worden papieren systemen besproken die voter-verifiable zijn. Veel van de technieken die hier gebruikt worden, zullen ook terugkomen in Helios. [Hoofdstuk 3](#) tot [Hoofdstuk 5](#) behandelen de werking van dit systeem, de procedure die gevolgd moet worden voor het opzetten van een verkiezing en de wijzigingen aan de interface. Het aangepaste systeem werd ook in de praktijk gebruikt om na te gaan hoe bruikbaar het is voor een echte verkiezing ([Hoofdstuk 6](#)).

In [Hoofdstuk 7](#) wordt kort gekeken naar methoden om de sleutels en fingerprints te bewaren. Tot slot worden de prestaties van de Web Cryptography API geëvalueerd ([Hoofdstuk 8](#)).

Literatuurstudie

Deze thesis handelt over methoden voor online verkiezingen. Een interessant verwant probleem zijn systemen die gebruik maken van papier. Eerst wordt een kort overzicht van de geschiedenis van stelsystemen gegeven (Sectie 2.1). Vervolgens worden de belangrijkste vereisten bekeken waaraan deze systemen moeten voldoen (Sectie 2.2). Belangrijk hierbij is de definitie van een voter verifiable systeem. Tot slot onderzoeken we zowel systemen die geen gebruik maken van cryptografische methoden (Sectie 2.3) als deze die daar wel op steunen (Sectie 2.4).

2.1 Geschiedenis [2]

Onze samenleving heeft een rijke geschiedenis van stemprocedures, die teruggaat tot Athene in het oude Griekenland. Hier bracht men een negatieve stem uit op een potscherf. In deze paragraaf bekijken we kort enkele die bepalend zijn geweest voor de manier waarop we vandaag werken.[51]

Sinds de uitvinding van het geheime stembiljet in 1858 in Australië is er eigenlijk niet meer zoveel veranderd. In dit systeem worden de biljetten op voorhand gedrukt door de staat en veilig bewaard tot op de stemdag. Elke stemgerechtigde krijgt op de stemdag een biljet waarna hij zijn stem uitbrengt in een stemhokje. Het grootste voordeel van deze methode ligt in het feit dat elke stem geheim is.

Deze stemmethode maakte het daarnaast ook mogelijk om mechanische (en later elektrische) machines te gebruiken. Mechanische systemen werden gebruikt in grotere gemeenschappen en waren gebaseerd op hendels en mechanische tellers. De eerste van deze machines werden in 1892 ingevoerd in New York. Rond 1960 werden de eerste elektrische machines ingevoerd. Deze maakten gebruiken van optische scans. Bij deze systemen moet de stem meestal op een specifieke manier aangegeven worden, bijvoorbeeld door het inkleuren van bolletjes.

Sinds 2000 worden Direct Recording by Electronics (DRE) machines steeds vaker gebruikt. Hierop draait speciale stemsoftware, die de keuze van de kiezer digitaal vastlegt. Deze machines maken het stemproces aanzienlijk eenvoudiger. Het grootste

probleem is dat er geen enkele bevestiging aan de kiezer gegeven wordt en dat hij deze machines dus volledig moet vertrouwen.[48]

Het gebrek aan controle door de kiezer bij DRE vormde de aanleiding voor het ontwerpen van Voter-Verified Paper Audit Trails (VVPAT) machines. Hierbij toont de machine de kiezer een afgeschermd afdruk van zijn stem, waarna hij deze kan accepteren of weigeren. Op die manier kan de kiezer verifiëren dat zijn stem correct is. In principe zouden bij een hertelling dan ook deze papieren tickets en niet de digitale data gebruikt moeten worden.[53]

2.2 Vereisten

Bij het ontwerpen van een stelsysteem zijn er twee tegenstrijdige doelen. Enerzijds moet het mogelijk zijn dat zowel de kiezer thuis kan controleren of zijn stem juist meegeteld is. Anderzijds mag diezelfde persoon niet kunnen bewijzen voor wie hij precies gestemd heeft, noch mag het mogelijk zijn dat anderen hierachter kunnen komen. Wanneer hij dit wel kan, zou hij zijn stem kunnen verkopen aan iemand die de verkiezing wil beïnvloeden, of hiertoe gedwongen worden.

Hoewel het vaak zeer moeilijk is om een grote verkiezing doorslaggevend te wijzigen, wordt stemfraude toch regelmatig geconstateerd.[2] Eén van de grote moeilijkheden is dat zowel kiezers als bijzitters corrupt kunnen zijn. Er kan dus van geen enkele deelnemer verwacht worden dat hij eerlijk is.

2.2.1 Vertrouwen

De huidige manier van stemmen vereist dat de kiezer zeer veel vertrouwen legt in het gebruikte systeem. Zoals verder besproken wordt (Sectie 2.2.2), zijn er nieuwe ontwerpen waarbij de kiezer kan controleren of zijn stem correct meegeteld is. Deze systemen steunen vaak op moeilijke cryptografische technieken, die heel wat achtergrondkennis vragen om ze te begrijpen.

Een vereiste voor om het even welk stelsysteem is dat het vertrouwd wordt door een gemiddelde kiezer, de bijzitters, de publieke opinie en media. Opdat deze mensen een dergelijk systeem zouden vertrouwen, moeten de experts die het systeem goedkeuren dit op een eenvoudige manier aan hen kunnen uitleggen.[31] Daarom zullen eenvoudige systemen die geen gebruik maken van cryptografie waarschijnlijk sneller aanvaard worden door een breed publiek.

2.2.2 End-to-End Verifiability

In een end-to-end verifiably voting systeem wordt niet nagegaan of de code van de stemmachines volledig correct is. In plaats daarvan wordt wiskundig bewezen dat het resultaat correct is. Op die manier kan de moeilijke en vaak ondoorzichtige fysieke chain-of-custody vermeden worden. Dit betekent ook dat iemand niet langer speciale

toegang moet hebben om de resultaten te controleren. Om het even wie kan nagaan of de bewijzen correct zijn.

Dergelijke end-to-end verifiable systemen kunnen zowel met als zonder cryptografische technieken gerealiseerd worden. Cryptografie kan enerzijds gebruikt worden om stemmen te encrypteren, zodat ze zeker geheim blijven. Anderzijds geven sommige systemen een zero-knowledge bewijs dat aangetoont dat de stemmen correct geteld zijn.

2.3 Systemen zonder cryptografie

In deze paragraaf worden enkele systemen besproken waarin geen gebruik gemaakt wordt van cryptografie. Open Counting ([Sectie 2.3.1](#)) is een techniek waarbij alleen de telfase aangepast wordt. Floating receipts ([Sectie 2.3.2](#)) kunnen de veiligheid van elk papieren stembiljet sterk verbeteren. ThreeBallot ([Sectie 2.3.4](#)) en Scratch-Card zijn beiden voter-verifiable systemen die gebruik maken van papieren tickets. Twin ([Sectie 2.3.2](#)) bouwt verder op respectievelijk floating receipts. Vooral ThreeBallot wordt in detail besproken omdat de belangrijkste concepten van papier-gebaseerde voter-verifiable verkiezingen hierin aan bod komen.

2.3.1 Open Counting [\[1\]](#)

Open counting vertrekt van de systemen zoals we ze vandaag kennen, maar de stemmen worden op een nieuwe manier geteld. Het stembiljet is aangepast om eenvoudig optisch geteld te worden. De stemmen worden nog steeds geteld door ambtenaren. Elke stem wordt op een scherm getoond aan verschillende telstations, elk met hun eigen hardware die het getoonde biljet filmt en analyseert. Ieder station geeft op regelmatige tijdstippen zijn huidig totaal en wanneer er onenigheid is, wordt het gedispersteerde biljet gezocht en het probleem opgelost.

Tijdens het tellen geeft ieder station ook een hash van hun opgenomen video. Hiervoor wordt een veilige hash-functie gebruikt. Deze hashes kunnen dan later gebruikt worden tijdens een geautomatiseerde audit om te controleren of er niet geknoeid is met de beelden. Dit proces is publiek en dus kan iedereen zijn eigen hardware meebrengen en de telling zelf uitvoeren. Het systeem wordt zo ontworpen dat een eenvoudige camera en computer volstaan. Ook deze waarnemers kunnen een hash van hun video publiceren om geloofwaardiger over te komen.

De verschillende telstations controleren continu elkaar en ook de waarnemers kunnen achteraf onregelmatigheden melden. Omdat het systeem snel werkt, kan de telling in het stembureau zelf gehouden worden. Op die manier kunnen alle belanghebbenden aanwezig zijn en kan het transport van de ongetelde biljetten vermeden worden. Het transparante karakter en het gebruik van eenvoudige hardware kunnen het vertrouwen van kiezers in het systeem sterk vergroten.

Open counting is een relatief eenvoudige manier om de telprocedure transparanter te maken naar de kiezers. Elke stem moet echter afzonderlijk getoond worden, waardoor dit systeem alleen gebruikt kan worden wanneer het aantal biljetten beperkt is.

2.3.2 Floating Receipts [37]

Floating receipts zijn een waardevolle toevoeging voor elk voter-verifiable papieren telsysteem. Een doos met stembiljetten wordt aan de uitgang van het stembureau geplaatst. De kiezer maakt bij het buitengaan een kopie van een stembiljet dat hij hieruit trekt, vooraleer hij zijn eigen erbij legt. Hij neemt dus een willekeurig ticket mee dat niet het zijne is, maar hij kan dit ticket toch later gebruiken om te controleren of de stemprocedure correct verlopen is. Omdat de doos initieel leeg is, krijgen de eerste T kiezers geen ticket mee naar huis. Hierbij is T een constante die veel kleiner is dan het aantal kiezers, maar voldoende groot zodat $1/T$ klein is.

Niemand weet dus met grote waarschijnlijkheid van wie hij het biljet gekopieerd heeft. Omdat de aanvaller geen betrouwbare methode heeft om alle kopieën van een ticket te bemachtigen, is het systeem bestendig tegen het vervangen van biljetten of het verkopen van een stem. Een nadeel is dat kiezer niet langer zijn eigen ticket heeft en dus misschien minder gemotiveerd is om te controleren of dit correct meegeteld is. Er wordt echter verondersteld dat een groot aantal kiezers dat toch nog steeds zal doen.

Om floating receipts te gebruiken, moeten de kiezers een extra stap volgen in de stemprocedure. De stemprocedure wordt dus complexer, maar dit kan verantwoord worden door de voordelen die deze techniek met zich meebrengt.

Short Ballot Assumption

Bij de *Short Ballot Assumption* (SBA) moet het aantal kandidaten op het biljet beperkt blijven. Wanneer er minder mogelijkheden zijn om een biljet in te vullen, wordt de kans kleiner dat iemand anders zijn biljet op identiek dezelfde manier invult. Het wordt dan voor een aanvaller moeilijker om een biljet aan een specifieke kiezer te koppelen.[9]

Twin [37]

Twin is een voter-verifiable uitbreiding van het klassieke systeem die gebruik maakt van floating receipts. Een traditioneel stembiljet wordt door elke kiezer individueel ingevuld. Onderaan het stembiljet wordt een ID geplaatst, maar dit wordt verborgen door een kraslaag. Na het invullen wordt het biljet gecontroleerd door een machine die deze laag eraf haalt en het biljet in een doos deponeert. Alle kiezers na de T^{de} krijgen een ticket van een willekeurig biljet mee naar huis. Wanneer de stemming afgelopen is, worden alle verzamelde biljetten gepubliceerd op een bulletin board.

BALLOT		BALLOT		BALLOT	
President		President		President	
Alex Jones	<input type="radio"/>	Alex Jones	<input type="radio"/>	Alex Jones	<input type="radio"/>
Bob Smith	<input type="radio"/>	Bob Smith	<input type="radio"/>	Bob Smith	<input type="radio"/>
Carol Wu	<input type="radio"/>	Carol Wu	<input type="radio"/>	Carol Wu	<input type="radio"/>
Senator		Senator		Senator	
Dave Yip	<input type="radio"/>	Dave Yip	<input type="radio"/>	Dave Yip	<input type="radio"/>
Ed Zinn	<input type="radio"/>	Ed Zinn	<input type="radio"/>	Ed Zinn	<input type="radio"/>
3147524		7523416		5530219	

FIGUUR 2.1: Multi-Ballot[35]

Twin is een heel eenvoudig systeem, zonder ingewikkelde wiskunde of specifieke regels voor het correct invullen van het stembiljet. Aangezien het ticket een kopie is van het biljet van iemand anders, kan een kiezer zijn stem niet verkopen. Daarnaast is het zowel voor de tellers als een aanvaller moeilijk om het resultaat ingrijpend te veranderen zonder gedetecteerd te worden. Er wordt immers verondersteld dat een groot aantal kiezers nagaat of zijn ticket correct op het bulletin board staan.

Het voordeel bij dit systeem is dat het gekende biljet behouden blijft. De kiezer moet dus geen nieuwe regels volgen bij het invullen ervan. Het is echter wel belangrijk dat de kiezer de procedure volgen. Dit moet duidelijk aangegeven worden door de bijzitters.

2.3.3 ThreeBallot [35]

ThreeBallot is een stelsysteem dat ontworpen werd door Ronald Rivest in 2006. Het systeem maakt gebruik van een speciaal stembiljet dat bestaat uit drie identieke delen. Er wordt gestemd door het invullen van rijen en het deponeren van kolommen. Door alle stembiljetten samen met een lijst van de kiezers op een publieke website (het bulletin-board) te plaatsen, wordt het systeem end-to-end verifiable.

Multi-Ballot

De drie delen waaruit het stembiljet bestaat, kunnen ofwel op één blad geprint worden ofwel op meerdere met perforaties ertussen. De drie delen zijn identiek, op een willekeurige identifier na. De drie IDs op een multi-ballot hebben bovendien geen enkel verband met elkaar of met deze op de andere. In [Figuur 2.1](#) wordt een voorbeeld van een multi-ballot getoond.

Bij het invullen van het multi-ballot gelden de volgende regels. Elke rij van drie bolletjes komt overeen met één kandidaat. Om voor een kandidaat te stemmen, moet de kiezer exact twee bolletjes inkleuren. Om tegen te stemmen, moet er één bolletje

aangeduid worden. In elke rij moet exact één of twee bolletjes ingevuld zijn, anders is het biljet ongeldig. Hoe de verschillende delen ingevuld zijn, maakt hierbij niet uit.

Omdat het belangrijk is voor de telling dat de kiezer deze regels juist volgt, moet hij na het invullen van het biljet dit invoeren in een controlemachine. Wanneer het biljet niet correct ingevuld is, dan geeft de machine aan waar de kiezer een fout gemaakt heeft. Indien alles wel juist is aangeduid, dan wordt een rode streep geprint op het biljet waarna hij de aparte delen indient. Deze controlemachine mag geen enkele opname maken van de ingevoerde biljetten.

Voordat hij de drie aparte biljetten afgeeft, moet de kiezer er willekeurig één uitkiezen waarvan hij een kopie meekrijgt als ticket. Het is het veiligste om dit te implementeren in de controlemachine. Door de manier waarop het biljet ingevuld is, geeft het ticket geen informatie over hoe de kiezer gestemd heeft.

Tellen van de stemmen

Wanneer de verkiezing afgelopen is, worden alle biljetten gescand en de gegevens op het bulletin board gepost. Merk op dat het eigenlijke biljet niet online gezet wordt, omdat de kiezer hier iets op zou kunnen schrijven. Ook een lijst van iedereen die deelgenomen heeft aan de stemming wordt geüpload. Een kiezer kan nu nagaan of zijn ticket ook op het bulletin board staat.

Omdat alle stemmen op het bulletin board staan, kan iedereen zelf de telling verifiëren. De stemmen kunnen zoals anders geteld worden, zij het met een kleine aanpassing. Omdat er twee bolletjes gekleurd zijn bij een voorstem en maar één bij een tegenstem, is het resultaat voor elke kandidaat vermeerderd met het aantal kiezers.

Integriteit

Door het toevoegen van een ticket en het bulletin board kan de kiezer nagaan dat zijn stembiljet gepubliceerd is en dat het totale aantal geregistreerde biljetten klopt. Deze nieuwe controles zullen ons toelaten om verschillende vormen van fraude eenvoudig te detecteren. Het is ook belangrijk te kijken of zij zelf geen nieuwe zwakheden introduceren.

Het toevoegen van nieuwe stemmen is onmogelijk zonder ook de lijst met kiezers aan te passen. Daarnaast kunnen er ook geen stemmen bijgewerkt of verwijderd worden zonder dat er mogelijk een kiezer komt klagen dat zijn stem niet correct online staat. Grootschalige fraude wordt op deze manier onmogelijk.

Bij de **Three-Pattern** aanval, vraagt de koper aan de kiezer om alle drie de delen in een bepaald patroon in te vullen. Wanneer hij dit patroon dan niet terugvindt op het bulletin board, wordt de kiezer niet betaald. Een mogelijke oplossing is het gebruik van een DRE machine. Deze print zelf de deelbiljetten in een willekeurig patroon nadat de kiezer zijn keuze gemaakt heeft op een scherm.

Bemerkt tot slot dat de controlemachine die de geldigheid van de tickets nagaat zeer goed getest moet worden. Wanneer deze aangepast zou worden, kan ze bijvoorbeeld kiezers toelaten om voor een bepaalde kandidaat drie bolletjes te kleuren en voor een andere geen. Zo zouden die stemmen veel meer gewicht krijgen dan deze die zich wel aan de regels houden. Het is bovendien onmogelijk om dergelijke ongeldige patronen achteraf terug te vinden omdat de verschillende biljetten los van elkaar worden ingediend.

Tot slot zou een aanvaller kunnen betalen voor het ticket van de kiezer. Zo kan deze de correctheid van zijn stem niet meer nagaan. De aanvaller zou dan in theorie het biljet kunnen aanpassen dat op het bulletin board geplaatst werd. De kiezers moeten dus aangemoedigd worden om hun ticket niet af te geven. Deze aanval kan eenvoudig tegengegaan worden wanneer de kiezer zonder medeweten van de aanvaller een kopie maakt van het ticket. Voor een digitaal getekend ticket (bv. met een barcode) volstaat dit namelijk ook om klacht neer te leggen.

Stemgeheim

Zoals eerder aangehaald, bevat het ticket zelf geen informatie over hoe de kiezer gestemd heeft. Het mag echter ook niet mogelijk zijn om de drie deelbiljetten aan elkaar te linken. Het ID op het ticket zou anders gebruikt kunnen worden om uit te zoeken welk tripel van een bepaalde kiezer is. Een vereiste voor het systeem is ook dat niemand vooraf weet welke drie deelbiljetten zullen samenhangen. Een mogelijke oplossing hiervoor is om de delen apart te houden en er willekeurig drie te laten trekken door de kiezer.

De kiezer mag zijn eigen multi-ballot niet kunnen reconstrueren op basis van de biljetten die op het bulletin board gepost worden. Dit kan opgelost worden door het ID te printen in de vorm van een 1D of 2D barcode, wat moeilijk te onthouden is. Het is ook verstandig om de kiezer geen vrije toegang te geven tot een kopieermachine bij het maken van het ticket. Dit is de reden dat het ticket best geprint wordt door de controlemachine.

Het moet ook onmogelijk zijn voor de kiezer om zijn stem nog te wijzigen nadat ze aanvaard is door de controlemachine. Een eerste oplossing is om hem geen fysieke toegang meer te geven tot de biljetten nadat ze gecontroleerd zijn. Een tweede is om samen met de rode streep ([Sectie 2.3.3](#)) een checksum op het biljet te printen die moeilijk veranderd kan worden door de kiezer.

Tot slot moet er opgepast worden dat een **Reconstructie** aanval niet mogelijk is. Hierbij haalt een aanvaller alle mogelijke geldige multi-ballots uit de biljetten die op het bulletin board geplaatst werden. Samen met het ticket van de kiezer zou hij dan in sommige gevallen kunnen achterhalen hoe deze gestemd heeft. Om de integriteit van de stemming te kunnen controleren, heeft de kiezer alleen het ticket van een geldig biljet nodig. Het is dus niet noodzakelijk dat hij het ticket van zijn eigen biljet mee naar huis neemt. Een mogelijke manier om dit te implementeren is door gebruik

LHC	RHC	RHC	RHC
3 – Jones			
5 – Smith			
1 – Clark			
7 – Brent			
4 – Lloyd		X	X
6 – Evans			
2 – Wain			
	722163903 (RIN)	3517462 (OCN)	722163903 (RIN)
Blank voting slip		Countable vote	Photocopied recei

FIGUUR 2.2: Scratch-Card biljet[31]

te maken van floating receipts (Sectie 2.3.2). Deze wordt niet expliciet vermeld in de paper van Rivest, maar hij bespreekt wel gelijkaardige methoden.[35]

Bruikbaarheid

Het ThreeBallot systeem is veel complexer dan de manier waarop nu gestemd wordt. De belangrijkste manier om ervoor te zorgen dat het systeem goed werkt is dan ook het opleiden van de kiezer. Het is ook moeilijker om het biljet te corrigeren wanneer er een fout gemaakt wordt: meestal is de enige optie om opnieuw te beginnen met een blanco biljet. Het gebruik van DRE machine zou het stemmen ook sterk vereenvoudigen. De kiezer moet dan wel controleren dat het geprinte biljet correct is. In Sectie 2.3.3 werd reeds aangegeven dat dit ook de ThreePattern aanval onmogelijk maakt.

Tot slot merken we nog op dat het tellen van de stemmen wel meer werk vraagt, aangezien er drie keer zoveel biljetten geteld moeten worden. ThreeBallot vergroot het vertrouwen van de kiezer in de integriteit van de verkiezing, ten koste van een moeilijker stemproces en meer werk bij het tellen.

2.3.4 Scratch-Card

Scratch-Card[31] maakt gebruik van een speciaal biljet dat makkelijk in twee gedeeld kan worden (Figuur 2.2). Belangrijk is dat de kandidaten op elk biljet in een willekeurige volgorde moeten staan. Een kiezer moet een willekeurig biljet trekken. Na het stemmen moet de kiezer het linkerdeel vernietigen. Hij kan een kopie van het rechterdeel als ticket mee naar huis nemen.

Op het rechterdeel van het biljet is onderaan een kraslaag aangebracht. Bovenop deze laag is het unieke ID (RIN) van het biljet geprint, dat de kiezer later kan gebruiken om zijn stem op het bulletin board terug te controleren. Bovendien verbergt deze laag een vooraf geprinte code die de volgorde van de kandidaten aangeeft (OCN). Bij het tellen wordt deze laag verwijderd en tegelijk verdwijnt ook het RIN van het

biljet. Het is zeer belangrijk dat de RIN en OCN volledig ongecorreleerd zijn, want anders zou achterhaald kunnen worden van wie de stem is.

Omdat het ticket een kopie is van het biljet met het kraslaagje nog intact, kan de OCN nooit meer achterhaald worden. Het is dus belangrijk goed te controleren dat de tellers niet proberen om RIN/OCN-combinaties neer te schrijven tijdens het verwijderen van het laagje.

Een nadeel aan het voorgestelde systeem is dat iedereen die een origineel rechterdeel bemachtigt, kan achterhalen op wie dat biljet gestemd heeft. Er is gelukkig wel geen rechtstreekse link tussen de RIN en de persoon die gestemd heeft. Een alternatief systeem print daarom een ID op het linker- en rechterdeel (CIN). Op het rechterdeel zit deze CIN opnieuw onder een kraslaag. In deze variant moet de kiezer na het stemmen ook zijn linkerdeel in een doos deponeren. Als ticket krijgt hij opnieuw een kopie mee van het rechterkant, waarop de kraslaag nog intact was.

Om de stemmen te tellen, wordt opnieuw de kraslaag verwijderd zodat de CIN gelezen kan worden. Vervolgens moet de linkerkant met dezelfde CIN gevonden worden om te achterhalen op wie gestemd is. Het grootste probleem is dat het zoeken naar de juiste paren heel veel werk zou vragen bij grote verkiezingen, tenzij dit geautomatiseerd zou worden.

Net zoals bij Twin ([Sectie 2.3.2](#)) is het invullen van het biljet zeer eenvoudig voor de kiezer. Ook hier is het echter belangrijk dat de kiezers de juiste procedure volgen en een kopie nemen van hun biljet voordat de kraslaag verwijderd is. Ook hier moeten de bijzitters dus toezien op het correct verloop van de verkiezing.

2.4 Systemen met cryptografie

De systemen in de vorige sectie maakten geen gebruik van ingewikkelde cryptografische technieken. Omdat het hierdoor eenvoudiger te begrijpen is, zal zo'n systeem sneller vertrouwd worden door de kiezer ([Sectie 2.2.1](#)). In deze sectie worden toch enkele systemen besproken die hier wel op steunen. Door gebruik te maken van zero-knowledge bewijzen, homomorfe cryptografie en mixnets kunnen immers veilige end-to-end verifiable systemen ontworpen worden.

Bij Secret-Ballot Receipts ([Sectie 2.4.1](#)) wordt optische cryptografie toegepast om de stem op het ticket te encrypteren. Scratch & Vote ([Sectie 2.4.2](#)) bouwt verder op de principes die geïntroduceerd werden bij Scratch-Card ([Sectie 2.3.4](#)).

2.4.1 Secret-Ballot Receipts [\[8\]](#)

Secret-Ballot Receipts werden in 2004 gepubliceerd door David Chaum. De kiezer ziet zijn stem geprint worden in het stemhokje en kan zijn ticket gebruiken om nadien te controleren of ze correct meegeteld is. Omdat zijn keuzes geëncrypteerd worden tijdens het printproces kan hij het ticket niet gebruiken om te bewijzen hoe



FIGUUR 2.3: Strookje met optische geëncrypteerde stem[8]



FIGUUR 2.4: Laatste stukje ticket met beide kanten nog samen[8]

hij gestemd heeft. Bovendien is het niet nodig om vertrouwde hardware te gebruiken aangezien de publieke code op relatief eenvoudige systemen gedraaid kan worden.

Nadat de kiezer zijn keuzes aangegeven heeft, worden deze door een speciale printer afgedrukt. De printer drukt tegelijk op beide kanten van het strookje afzonderlijke, maar uitgelijnde afbeeldingen. De kiezer wordt gevraagd om de afdruk te controleren en kan zijn stem eventueel nog aanpassen. Wanneer hij tevreden is, kan hij kiezen of hij de boven- of onderkant wil meenemen. Pas dan wordt het laatste stukje van het ticket afgedrukt en kan hij de twee delen uit de printer nemen, terwijl ze nog aan elkaar vastzitten.

Door de twee kanten van elkaar los te maken, wordt de afbeelding op het strookje schijnbaar willekeurig. Het doorgelaten licht op de plaatsen waar geen van beide kanten bedrukt is, maakte de stem zichtbaar. Geen van beide lagen bevat dus informatie over hoe gestemd is. Het laatst geprinte stukje is verschillend omdat daar wel tekst opstaat die ook na het scheiden van de twee lagen nog gelezen kan worden. Op de ene kant wordt duidelijk aangegeven dat deze bijgehouden moet worden en op de andere dat hij afgegeven moet worden. Deze laatste wordt duidelijk zichtbaar voor de kiezer vernietigd.

De computer houdt zelf een digitale versie van het volledige ticket bij en verwijdert ook de data van de andere kant. Deze data wordt na het aflopen van de stemming geüpload naar een online bulletin board. Omdat het ticket geen informatie bevat over de stem van de kiezer, kan hij dit aan iedereen tonen zonder zijn stem openbaar te maken. Door het ticket te scannen kan eenvoudig vastgesteld worden of het authentiek is. Bij een ongeldige controle is men dus zeker dat de apparatuur niet correct gewerkt heeft.

De kiezer kan na de stemming nagaan of zijn ticket juist op het bulletin board staat. Hij kan dit eenvoudig doen door te kijken of de versie die daar staat volledig overeenkomt met zijn eigen ticket. Na het afsluiten van de stemming wordt de uiteindelijke verzameling van stemmen die geteld moeten worden, online gezet. Er worden ook digitale handtekeningen van de set gepubliceerd die gebruikt kunnen

worden om de echtheid ervan te controleren. Wanneer de stemmen geteld zijn, wordt een nieuwe set online geplaatst. Deze bevat even veel biljetten, maar nu zijn afbeeldingen gedecrypteerd en is elke stem leesbaar. Om de privacy van de kiezer te bewaren, zijn de biljetten willekeurig geordend.

Er wordt gebruik gemaakt van een audit proces om te controleren of beide sets identiek dezelfde biljetten bevatten. Het telproces verloopt in verschillende stappen en na elke stap wordt een klein aantal willekeurig gekozen biljetten gedecrypteerd van de set tussen twee stappen in het telproces. Deze biljetten worden zo gekozen dat ze niet voldoende informatie bevatten zodat een kiezer geïdentificeerd kan worden, maar wel gebruikt kunnen worden om na te gaan of er geen biljetten toegevoegd, verwijderd of gewijzigd werden.

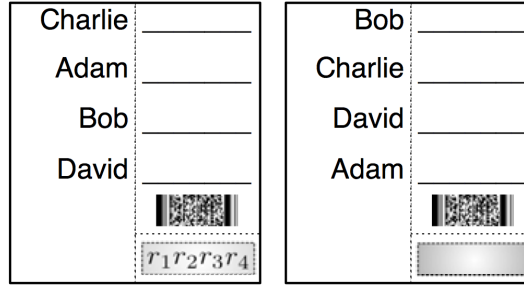
Omdat de optische encryptie neerkomt op een one-time pad, kan zelfs een aanvaller met ongelimiteerde rekenkracht de stem niet achterhalen. De gebruikte sleutels zijn dus de pixels van één van beide kanten. Deze zijn niet willekeurig, maar in de praktijk kunnen ze hiervan niet onderscheiden worden tenzij door de personen die de decryptie zullen uitvoeren.

Aangezien alles digitaal opgeslagen wordt, kan de telling ook voor grote verkiezingen efficiënt uitgevoerd worden. Een bijkomend voordeel is dat kiezers via een computer moeten stemmen, wat ze vaak reeds gewoon zijn. Hoewel de software op eenvoudige machines kan draaien, zijn er nog steeds speciale printers nodig om de tickets af te drukken.

2.4.2 Scratch & Vote [5]

Scratch & Vote werd in 2006 ontworpen door Ben Adida en Ronald L. Rivest. Het is een variatie op Scratch-Card ([Sectie 2.3.4](#)) waarbij gebruik gemaakt wordt van homomorfe cryptografie en zero-knowledge correctheidsbewijzen. Iedereen kan het uiteindelijke resultaat verifiëren en alleen de cijfertekst van de uitslag moet gedecrypteerd worden door de verantwoordelijken van de verkiezing. Het grote verschil met Scratch-Card ([Sectie 2.3.4](#)) is dat er niet langer met een RIN/CIN gewerkt moet worden, net omdat de stemmen nu geëncrypteerd worden.

Bij het aanmelden ontvangt de kiezer een biljet dat uit twee delen bestaat. Op de linkerkant staan de kandidaten in een willekeurige volgorde, die alleen door de kiezer gezien mag worden. Op de rechterkant kan de kiezer zijn stem uitbrengen. Onderaan dit deel staan verder een 2D barcode en een kraslaag. Net zoals bij Scratch-Card wordt de linkerkant na het invullen van het biljet in het stembokje afgescheurd en in een doos gedeponeerd. Een bijzitter controleert of de kraslaag op de rechterkant nog intact is en verwijdt deze daarna. Vervolgens wordt dit stukje zichtbaar voor de kiezer vernietigd. Tot slot laat de kiezer de eigenlijke stem en barcode scannen. Wanneer het stukje met de kraslaag verwijderd is van het biljet, bevat het rechterdeel geen informatie meer die gebruikt kan worden om de stem van de kiezer te achterhalen. Het gescande deel kan dus als ticket meegenomen worden.



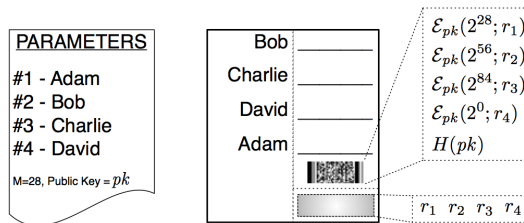
FIGUUR 2.5: Scratch & Vote biljet[5]

Door aan te melden op het bulletin board, kan de kiezer controleren of zijn biljet correct gescand werd. Omdat alle gescande biljetten online geplaatst worden, kan iedereen nagaan of de cijfertekst van de eindtelling correct is.

Voor de encryptie wordt gebruik gemaakt van het Paillier public key cryptosystem. Dit systeem heeft een additief homomorfisme door het vermenigvuldigen van de cijferteksten. Het tellen van de stemmen bij een verkiezing met meerdere kandidaten zou echter niet mogelijk zijn zonder gebruik te maken van een multi-counter. Het aantal beschikbare bits voor de leesbare tekst wordt onderverdeeld in verschillende tellers. Hierbij worden voldoende bits beschikbaar gemaakt voor elke teller zodat ze niet in elkaar kunnen overlopen.

Het systeem maakt daarnaast gebruik van zero-knowledge bewijzen. Deze worden gebruikt om aan te tonen dat een set cijferteksten c_1, c_2, \dots, c_l de encryptie is van de permutatie van m_1, m_2, \dots, m_k (ervan uitgaande dat geen twee subsets van m_i dezelfde som hebben). De verschillende m_i zijn de tellers voor de kandidaten.

Daarnaast worden ook bewijzen opgesteld die aantonen dat de biljetten zelf correct zijn. Omdat deze bewijzen te lang zijn om op de biljetten te printen, worden ze voor de start van de verkiezing geüpload naar het bulletin board. Ze worden tijdens het tellen van de stemmen gebruikt om te verzekeren dat elk biljet maar één stem uitbrengt per verkiezing. Om de kiezer te garanderen dat zijn biljet tijdens het tellen niet ongeldig verklaard zal worden, wordt ook een officiële lijst van alle geldige biljetten voorzien. De kiezer kan dan eenvoudig nagaan of zijn biljet hierop voorkomt.



FIGUUR 2.6: Scratch & Vote encryptie[5]

De 2D barcode op elk biljet encodeert de willekeurige volgorde van de cijferteksten voor de verschillende kandidaten samen met een hash van de publieke sleutel (Figuur 2.6). De startwaarde van de teller van elke kandidaat wordt samen met een willekeurige waarde geëncrypteerd. Zo heeft elk biljet een unieke cijfertekst voor elke kandidaat. Deze willekeurige waarden worden verborgen door de kraslaag. De startwaarden van de tellers vormen samen met de publieke sleutel de gepubliceerde parameters. Samen met de willekeurige waarden kunnen ze dus gebruikt worden om de volgorde van de kandidaten op het biljet te achterhalen. Daarom is het belangrijk dat dit stukje van het biljet vernietigd wordt.

Deze informatie wordt toch op de biljetten geprint omdat ze nodig zijn voor een audit. Dit wordt gedaan door de kiezer twee biljetten te laten kiezen. Door de kraslaag weg te halen, worden de willekeurige waarden zichtbaar en kan nagegaan worden of het biljet correct is. Door het verwijderen van de kraslaag wordt het biljet ongeldig, wat de reden is dat de kiezer twee biljetten moet nemen. Op deze manier wordt de helft van de biljetten getest en dus is de kans groot dat foutieve biljetten gedetecteerd worden.

Zowel naar de kiezer als de bijzitters is dit systeem zeer gebruiksvriendelijk. Het standaard stembiljet is slechts licht gewijzigd en de kiezer zou er dus vertrouwd mee moeten zijn. Ook de stemprocedure is niet radicaal gewijzigd. Aangezien de telprocedure ook geautomatiseerd is, kan deze methode ook voor grote verkiezingen gebruikt worden.

2.5 Conclusie

Bij open counting (Sectie 2.3.1) wordt een transparante manier van tellen gebruikt om het vertrouwen van de kiezer in het resultaat te vergroten. In tegenstelling tot de andere systemen kan hier door de kiezer wel niet nagegaan worden of zijn stem meegeteld is. Voter-verifiability wordt daar bekomen door gebruik te maken van een ander type biljet samen met een aangepaste stemprocedure.

Deze aanpassingen maken het stemmen voor de kiezer ingewikkelder. In tegenstelling tot bij een klassiek biljet, moeten nu verschillende regels gevolgd worden om het biljet correct in te vullen. De stemprocedures zijn vaak ook ingewikkelder dan voordien, met nieuwe regels voor zowel de kiezers als de bijzitters.

Door cryptografische technieken te gebruiken, kan de gebruiksvriendelijkheid van papieren end-to-end verifiable systemen sterk verbeterd worden. Een nadeel is hier dan weer dat de meeste mensen nog steeds zullen moeten vertrouwen op het oordeel van een expert over de correctheid van het systeem.

Papieren voter-verifiable systemen hebben dus enkele grote nadelen die hun praktisch nut sterk beperken. Ze zijn vaak zeer complex en niet bruikbaar voor grote verkiezingen. Cryptografische technieken lossen deze problemen wel deels op, maar worden dan weer moeilijker vertrouwd door de kiezer.

Helios

Het Helios verkiezingssysteem is een open-source project dat geleid wordt door Ben Adida.[3] Het laat toe om online voter-verifiable verkiezingen te organiseren. Online verkiezingen kunnen wel alleen gebruikt worden in een context waar dwang geen grote bedreiging is. Dit systeem werd vorig jaar door Robbert Coeckelbergh uitgebreid met threshold encryptie en gerangschikte verkiezingen.[10]

In dit hoofdstuk worden de belangrijkste cryptografische technieken uitgelegd die Helios gebruikt (Sectie 3.1). Daarna wordt de functionaliteit van de publieke delen van Helios besproken: het stembokje (Sectie 3.2), het ballot tracking center (Sectie 3.3) en de controleapplicatie (Sectie 3.4).

3.1 Cryptografische technieken

Op het vlak van cryptografische technieken leunt Helios het dichtste aan bij Scratch & Vote (Sectie 2.4.2). Het belangrijkste verschil is dat ElGamal gebruikt wordt in plaats van Paillier voor de homomorfe encryptie van de stemmen. Tot slot wordt de methode besproken waarop de sleutel verdeeld wordt tussen de trustees (Sectie 3.1.3).

3.1.1 ElGamal [16]

Het ElGamal cryptosystem is een asymmetrisch schema dat gebaseerd is op het Diffie-Hellman protocol. Dit betekent dat een sleutelpaar met zowel een geheime als publieke sleutel nodig is. De publieke sleutel wordt gebruikt om de klaartekst te encrypteren. De decryptie kan alleen uitgevoerd worden met de geheime sleutel.

Er wordt gewerkt in de groep \mathbb{Z}_p waar g de generator is. De geheime sleutel sk wordt willekeurig gekozen binnen \mathbb{Z}_{p-1} . De publieke sleutel is dan $pk = g^{sk} \bmod p$. De cijfertekst van een ElGamal encryptie bestaat uit twee delen: c_1 (Vergelijking 3.1) en c_2 (Vergelijking 3.2). In deze vergelijkingen is m de klaartekst en r opnieuw een willekeurig getal binnen \mathbb{Z}_{p-1} . c_1 en r hebben respectievelijk de functie van tijdelijke publieke en private sleutel.[30]

$$c_1 = g^r \mod p \quad (3.1)$$

$$c_2 = m \cdot pk^r \mod p \quad (3.2)$$

De cijfertekst kan dan gedecrypteerd worden volgens [Vergelijking 3.3](#).

$$m = \frac{c_2}{c_1^{sk}} \mod p \quad (3.3)$$

3.1.2 Homomorfe encryptie

Bij homomorfe encryptie kan een specifieke operatie met de cijfertekst uitgevoerd worden. De resulterende cijfertekst is de encryptie van een bepaalde bewerking op de klaarteksten.[\[49\]](#) Zo is het Paillier cryptosysteem dat gebruikt wordt in Scratch & Vote ([Sectie 2.4.2](#)) homomorf onder $(\times, +)$. Dit betekent dat een vermenigvuldiging van de cijferteksten resulteert in een optelling van de klaarteksten.

Het homomorfisme $(\times, +)$ kan in een verkiezingssysteem gebruikt worden om efficiënt de stemmen op te tellen. De berekening van het resultaat kan immers gebeuren aan de hand van de cijferteksten. Er moet nu alleen een decryptie gebeuren om het uiteindelijke resultaat vrij te geven.

Aan de hand van [Vergelijking 3.2](#) kan gezien worden dat ElGamal standaard homomorf is onder (\times, \times) . Zoals hiervoor besproken, is voor een verkiezingssysteem echter het homomorfisme $(\times, +)$ nodig. Dit kan gerealiseerd worden door de klaartekst ook in de exponent te plaatsen ([Vergelijking 3.4](#)).

$$c_2 = g^m \cdot pk^r \mod p \quad (3.4)$$

[Vergelijking 3.5](#) geeft het homomorfisme dat zo bekomen wordt.

$$\begin{aligned} \mathcal{E}(m_1) \cdot \mathcal{E}(m_2) &= (g^{r_1}, g^{m_1} \cdot pk^{r_1}) \cdot (g^{r_2}, g^{m_2} \cdot pk^{r_2}) \\ &= (g^{r_1+r_2}, g^{m_1+m_2} \cdot pk^{r_1+r_2}) \\ &= \mathcal{E}(m_1 + m_2) \end{aligned} \quad (3.5)$$

Omwille van het discreet logaritme probleem is het terugvinden van m echter niet meer zo vanzelfsprekend.[\[25\]](#) Dit kan alleen gedaan worden door $g^m \mod p$ te berekenen voor elke m en vervolgens te zoeken welke hetzelfde is als de klaartekst van de decryptie.

Scratch & Vote ([Sectie 2.4.2](#)) gebruikt multi-counters voor een stemming met meerdere kandidaten. Helios daarentegen encrypteert ieder mogelijk antwoord op een vraag afzonderlijk. Wanneer de optie gekozen wordt, is $m = 1$; anders wordt $m = 0$ gesteld.

3.1.3 Threshold encryptie

Oorspronkelijk kon de publieke sleutel voor de verkiezing alleen berekend worden als het product van de afzonderlijke publieke sleutels van de trustees ([Vergelijking 3.6](#)). Voor de decryptie moet iedere trustee zijn factor uit de noemer van [Vergelijking 3.7](#) berekenen. Deze factoren worden in Helios de decryptiefactoren genoemd.

$$PK = \prod_{i=1}^n pk_i \mod p \quad (3.6)$$

$$g^m = \frac{c_2}{\prod_{i=1}^n c_1^{sk_i}} = \frac{c_2}{\prod_{i=1}^n df_i} \mod p \quad (3.7)$$

Een groot probleem hierbij is dat wanneer één trustee zijn geheime sleutel verliest, het resultaat niet meer gede crypteerd kan worden. Daarom werd threshold encryptie toegevoegd door Robbert Coeckelbergh.[\[10\]](#) Er kan nu een threshold schema gedefinieerd worden zodat slechts k van de n trustees hun decryptiefactor moeten berekenen.

Secret Sharing

De methode die geïmplementeerd werd is gebaseerd op Shamir's secret sharing.[\[39\]](#) Iedere trustee genereert eerst een veelterm van graad $k - 1$. Vervolgens stuurt hij elke trustee (ook zichzelf) een zogeheten *share* van deze veelterm. Deze share is de waarde van de veelterm voor een punt x . Deze x -coördinaat moet door iedereen gekend zijn, omdat het vereist is dat de shares die een trustee ontvangt van de anderen voor dezelfde waarde werden aangemaakt. Daarom wordt hiervoor binnen Helios het database ID van de trustee gebruikt. Dit is een uniek natuurlijk getal dat wordt opgehoogd telkens een nieuwe trustee aangemaakt wordt.

Vervolgens moet de trustee de n shares die hij zo ontvangt, optellen. Zo bekomt hij de y -coördinaat die hoort bij zijn ID op een nieuwe veelterm, die de som is van de n veeltermen die door de trustees gegenereerd werden. Deze waarde kan hij nu gebruiken als zijn geheime sleutel sk . Omdat ElGamal gebruikt wordt als encryptieschema, wordt zijn publieke sleutel $pk = g^{sk} \mod p$.

Als geheime sleutel voor de verkiezing wordt nu de waarde voor $x = 0$ op de gemeenschappelijke veelterm genomen. Deze veelterm kan door Lagrange-interpolatie gereconstrueerd worden uit k punten. Hiervoor worden de eerste k trustees gebruikt (dat zijn deze met het laagste ID). Omdat alleen de publieke sleutels van de trustees beschikbaar zijn, wordt echter onmiddellijk de publieke sleutel voor de verkiezing berekend ([Vergelijking 3.11](#)).

$$\lambda_i(x) = \prod_{j=1, j \neq i}^k \frac{x - x_j}{x_i - x_j} \quad (3.8)$$

$$V(x) = \sum_{i=1}^k sk_i \lambda_i(x) \quad (3.9)$$

$$SK = V(0) = \sum_{i=1}^k sk_i \lambda_i(0) \quad (3.10)$$

$$PK = g^X = \prod_{i=1}^k pk_i^{\lambda_i(0)} \mod p \quad (3.11)$$

Om het resultaat te decrypteren moet de geheime sleutel voor de verkiezing gebruikt worden ([Vergelijking 3.10](#)). Het grote voordeel van threshold encryptie is dat het hier niet belangrijk is van welke k trustees de decryptiefactoren en bijhorende Lagrange-interpolatie gebruikt worden.

$$g^m = \frac{c_2}{\prod_{i=1}^k c_1^{sk_i \lambda_i(0)}} = \frac{c_2}{\prod_{i=1}^k df_i^{\lambda_i(0)}} \mod p \quad (3.12)$$

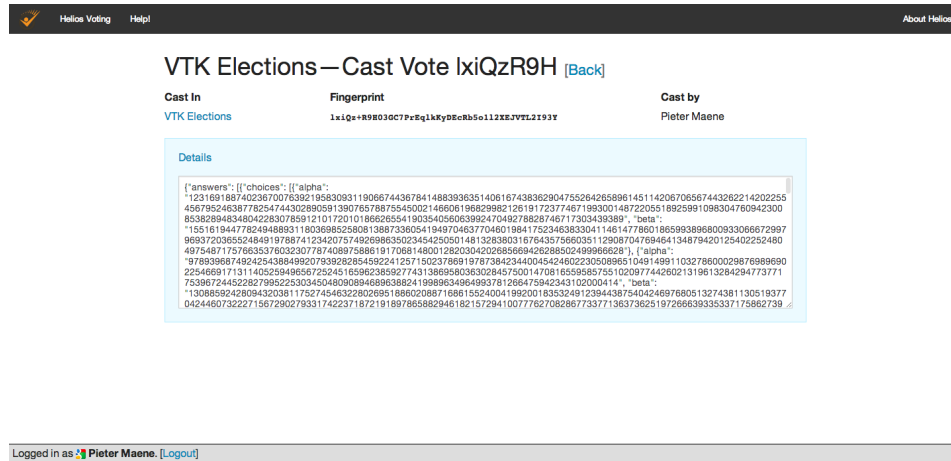
Communicatiesleutels

Voordat iedere trustee zijn gegenereerde shares doorstuurt naar de andere trustees, worden deze geëncrypteerd en getekend. Hiervoor wordt respectievelijk de publieke sleutel voor encryptie en voor tekenen van de andere trustee gebruikt. Dit geeft aanleiding tot twee nieuwe sleutelparen die de communicatiesleutels genoemd worden.

3.2 Stemhokje

Het stemhokje staat volledig los van de rest van het systeem. Het is een applicatie die de kiezer kan gebruiken om zijn stem uit te brengen. Nadat hij zijn keuze gemaakt heeft, wordt deze geëncrypteerd met de publieke sleutel voor de verkiezing. Zoals besproken in [Sectie 3.1](#), zal de cijfertekst bestaan uit twee delen ([Vergelijking 3.1](#) en [Vergelijking 3.4](#)). Wanneer threshold encryptie aanstaat, wordt de publieke sleutel zoals gedefinieerd door [Vergelijking 3.11](#) gebruikt; anders is het deze van [Vergelijking 3.6](#).

Het encryptieproces is in JavaScript geïmplementeerd en vindt dus volledig plaats in de browser van de kiezer. De stem van de kiezer zal dan nooit ongeëncrypteerd op de server toekomen. Alle informatie over de verkiezing kan eenvoudig opgevraagd worden. De kiezer zou dus ook zijn eigen software kunnen gebruiken om zijn stem te encrypteren.



FIGUUR 3.1: Uitgebrachte stem

Aan elke geëncrypteerde stem wordt een *Smart Ballot Tracker* toegekend. Dit is een fingerprint die de stem identificeert (Sectie 7.2). Aan de hand daarvan kan de kiezer zijn stem volgen doorheen het systeem en kan hij verifiëren dat zijn stem niet aangepast is.

3.3 Ballot Tracking Center

Net zoals bij Scratch & Vote (Sectie 2.4.2) worden de uitgebrachte stemmen gepubliceerd. In het ballot tracking center kan een lijst met alle kiezers teruggevonden worden. Bij een publieke verkiezing kan iedereen deze opvragen, bij een private alleen de geregistreerde kiezers. Standaard staan hier gewoon de namen van de kiezers, maar de beheerder kan ervoor kiezen om aliassen te gebruiken in de plaats.

Van zodra een kiezer zijn stem uitgebracht heeft, kan deze bekeken worden (Figuur 3.1). Dit is nodig omdat zo het resultaat van de verkiezing gecontroleerd kan worden (Sectie 3.4). Al deze informatie kan ook opgevraagd worden als JSON, zodat ze eenvoudiger verwerkt kan worden door een applicatie.

3.4 Controleapplicatie

Net zoals het stemhokje is de controleapplicatie onafhankelijk en draait ze lokaal in de browser van de gebruiker. Ze kan gebruikt worden om het resultaat van de verkiezing te controleren. Alle ruwe data wordt gedownload van de server, waarna de nodige berekeningen lokaal worden uitgevoerd.

Procedure

Dit hoofdstuk geeft de procedure die in Helios gevolgd moet worden om een verkiezing op te zetten. In [Sectie 4.1](#) wordt bekeken welke informatie gekend moet zijn voordat met het aanmaken van de verkiezing aangevat wordt. De procedure zelf wordt in [Sectie 4.2](#) beschreven.

4.1 Voorbereiding

4.1.1 Trustees

De trustees zijn de personen die verantwoordelijk zullen zijn voor het decrypteren van het resultaat. Aangezien zij een belangrijke rol spelen in het verkiezingsproces, is het belangrijk vooraf vast te leggen wie dit zal doen. Helios heeft ondersteuning voor threshold encryptie ([Sectie 3.1.3](#)). Er moet dus ook nagedacht worden over het threshold schema: hoeveel trustees nodig zullen zijn om het resultaat van de verkiezing te decrypteren. Om een trustee aan te maken, moeten zijn naam en een geldig e-mailadres opgegeven worden.

4.1.2 Vragen

Het belangrijkste van de verkiezing zijn uiteraard de vragen die de kiezers zullen moeten beantwoorden. Bij elke vraag kan in Helios aangegeven worden hoeveel antwoorden elke kiezer kan aanduiden, dus ook dit moet op voorhand bepaald worden. Het resultaat kan ofwel absoluut ofwel relatief weergegeven worden. In het eerste geval zal bij elke optie het aantal stemmen voor deze optie getoond worden, in het tweede alleen de relatieve plaatsen van de opties onderling.

4.1.3 Kiezers

Een verkiezing in Helios kan opengesteld worden voor iedereen of voor specifieke kiezers. Bij een gesloten verkiezing moet op voorhand een lijst van geldige kiezers opgesteld worden.

4. PROCEDURE

The screenshot shows the 'Create a New Election' form in the Helios Voting interface. At the top, there is a navigation bar with 'Helios Voting', 'Help', and 'About Helios' links. Below the navigation bar is a 'CREATE' button. The main heading is 'Create a New Election'. The form contains several input fields and checkboxes, each with a help icon (question mark):

- Name: Text input field.
- Short Name: Text input field.
- Election Type: Dropdown menu with 'Election' selected.
- Use Voter Aliases: Checkbox.
- Randomize Answer Order: Checkbox.
- Private: Checkbox.
- Use Threshold Encryption: Checkbox.
- Voting Starts at: Text input field.
- Voting Ends at: Text input field.
- Publish Tally at: Text input field.
- Help E-mail Address: Text input field.
- Description: Text area.

A 'Next' button is located at the bottom of the form. At the very bottom of the page, a status bar indicates 'Logged in as Pieter Maene. [Logout]'.

FIGUUR 4.1: Aanmaken van de verkiezing

Deze kiezers kunnen in Helios geïmporteerd worden door een CSV-bestand aan te maken. Helios heeft van elke kiezer de volledige naam en een uniek ID nodig. Het e-mailadres van de kiezer kan opgegeven worden, maar dit is niet vereist. Er kan ook aangegeven worden welk authenticatiesysteem (bv. Google of Shibboleth) gebruikt wordt door de kiezer. Wanneer dit laatste veld leeg is, zal een gegenereerd wachtwoord naar hem opgestuurd worden.

4.2 Helios

4.2.1 Aanmaken van de verkiezing

De eerste stap is het aanmaken van de verkiezing. Hier moet eerst de basisinformatie van de verkiezing opgegeven worden zoals de naam en het type verkiezing. Ofwel kan er een verkiezing aangemaakt worden, ofwel een referendum. Voor beide types is de procedure echter identiek.

Vervolgens kunnen een aantal belangrijke functies aan- of uitgezet worden. Wanneer aliassen gebruikt worden, dan worden de namen van de kiezers verborgen in het publieke ballot tracking center ([Sectie 3.3](#)). Het is ook mogelijk om de antwoorden in een random volgorde op het biljet te laten zetten. Een geheime verkiezing kan alleen bekeken worden door de geregistreerde kiezers. Hier moet ook aangegeven worden of threshold encryptie ([Sectie 3.1.3](#)) gebruikt zal worden.

Helios Voting Help! About Helios

CREATE ADMIN TRUSTEES

VTK Elections — Trustees [\[Back\]](#)

Trustees are responsible for decrypting the election result. Since this election uses threshold encryption, all trustees will have to go through a key ceremony. During this ceremony, each trustee receives part of the key that will be used to encrypt the ballots. When freezing the election, you will have to define the threshold scheme. This controls the number of trustees that will have to provide their secret key before the results can be decrypted.

Each trustee will be given a link to his/her personal dashboard. If a trustee lost his link, you can resend it by hitting *Send Link* below.

Helios is automatically your first trustee and will handle its key pair generation and decryption automatically. You may add additional trustees if you want, and you can even remove the Helios trustee. However, we recommend you do this only if you have a solid understanding of the trustee's role.

Next After freezing the trustee list, the threshold scheme can be defined.

[Add a Trustee +](#) [Freeze Trustee List +](#)

Public Keys

Trustee	Public Key for Signing	Public Key for Encryption
[x] [Send Login] Robin Ska	Not uploaded yet.	Not uploaded yet.
[x] [Send Login] Jeroen Van Hemelen	Not uploaded yet.	Not uploaded yet.
[x] [Send Login] Pieter Maene	Not uploaded yet.	Not uploaded yet.
[x] [Send Login] Daan Wendelen	Not uploaded yet.	Not uploaded yet.
[x] [Send Login] Daniël Slenders	Not uploaded yet.	Not uploaded yet.
[x] [Send Login] Tom Van der Voorde	Not uploaded yet.	Not uploaded yet.

Logged in as Pieter Maene. [\[Logout\]](#)

FIGUUR 4.2: Trustees

Tot slot is het mogelijk om aan te geven wanneer de verkiezing moet starten en sluiten. Wanneer het resultaat niet onmiddellijk na het aflopen van de verkiezing gepubliceerd mag worden, kan een alternatief tijdstip hiervoor opgegeven worden.

4.2.2 Trustees

Eens de nieuwe verkiezing aangemaakt is, moeten de trustees toegevoegd worden. Deze stap is eerst gezet in de procedure omdat hij veruit de meeste tijd in beslag neemt. De beheerder van de verkiezing moet eerst alle trustees aanmaken. De trustee krijgt dan ook meteen een link toegestuurd via e-mail naar zijn trustee dashboard ([Sectie 5.2](#)) waar hij al zijn acties zal moeten uitvoeren.

Verkiezing zonder threshold encryptie

Wanneer geen threshold encryptie gebruikt wordt, is dit proces eenvoudig. Van zodra een trustee aangemaakt is, kan hij het sleutelpaar genereren dat gebruikt zal worden als deel van de sleutel voor de verkiezing. Alle trustees moeten dit gedaan hebben voordat de beheerder de verkiezing kan bevriezen en openstellen voor de kiezers. Hij kan ondertussen echter wel verdergaan met de procedure.

Verkiezing met threshold encryptie

Wanneer alle trustees aangemaakt zijn, kan deze lijst bevroren worden. Op dit moment moet ook het threshold schema ingegeven worden. Wanneer dit gebeurt is,

4. PROCEDURE

Helios Voting Help About Helios

VTK Elections—Threshold Scheme [\[Back\]](#)

There are 6 trustees for the election VTK Elections. You can now specify the number of trustees that is required to decrypt the result. You can submit any number between 1 and 6.

Trustees for Decryption

[Submit](#)

Logged in as [Pieter Maene](#) [\[Logout\]](#)

FIGUUR 4.3: Threshold schema

begint voor de trustees de sleutelceremonie. Deze bestaat uit drie stappen.

1. De trustees moeten eerst de twee sleutelparen genereren die gebruikt zullen worden om hun onderlinge communicatie te beveiligen. Pas wanneer alle trustees deze stap uitgevoerd hebben, kan verdergegaan worden.
2. Elke trustee maakt vervolgens zijn shares aan en encrypteert deze voor de andere trustees. Hier moet opnieuw gewacht worden totdat alle trustees deze stap voltooid hebben.
3. De trustees kunnen nu de shares die ze van de andere gekregen hebben decrypteren en optellen. Zo bekomen ze het sleutelpaar dat later gebruikt zal kunnen worden om de encryptiesleutel van de verkiezing de reconstrueren.

Pas wanneer alle trustees de volledige sleutelceremonie doorlopen hebben, kan de verkiezing door de beheerder bevroren worden. Omdat de verschillende trustees dus vaak op elkaar moeten wachten, krijgen ze een e-mail elke keer de volgende stap uit de ceremonie aangevat kan worden. Tijdens het wachten op de trustees, kan de beheerder verdergaan met de procedure.

4.2.3 Vragen

Terwijl de trustees bezig zijn met het uitvoeren van de sleutelceremonie, kan het stembiljet wel aangemaakt worden. Alle informatie die hiervoor nodig is, werd reeds voorbereid ([Sectie 4.1.2](#)).

4.2.4 Kiezers

Ook deze stap werd reeds volledig voorbereid ([Sectie 4.1.2](#)). Hier kunnen de CSV-bestanden geüpload worden, waarna het systeem ze verwerkt en alle kiezers toevoegt aan de verkiezing.

Helios Voting Help! About Helios

CREATE > ADMIN > TRUSTEES > ADMIN > QUESTIONS

VTK Elections—Questions [\[Back\]](#)

1. Would you vote for or against the Pixel team as board candidates for VTK in the year 2014-2015? [\[x\]](#) [\[Edit\]](#)

Voters can select between 1 and 1 answers. Result Type: Absolute

- For
- Against
- Abstain

Add a Question

Voters can select between 0 and 1 answers. Result Type: Absolute

Question: Which fun team would you prefer to win?

Answer 1: Nautilus

Answer 2: Rebellion

Answer 3:

Answer 4:

Answer 5:

[Add Question](#) [Add 5 More Answers](#)

Logged in as Pieter Maene. [\[Logout\]](#)

FIGUUR 4.4: Vragen

Helios Voting Help! About Helios

CREATE > ADMIN > TRUSTEES > ADMIN > BULK UPLOAD

VTK Elections—Bulk Upload Voters [\[Back\]](#)

If you would like to specify your list of voters by name and e-mail address, you can bulk upload a list of such voters here. Please prepare a text file of comma-separated values with the fields:

```
<voter_id>|,<email>|,<full_name>|,<user_type>|
```

If the system cannot validate the second field as an e-mail address, it will assume that it specifies the user's full name instead. The user type field is optional and can be used to specify the type of user account that should be created for the voter. If left empty, a password will be generated for the voter.

For example:

```
bobsmith,bob@acme.org,Bob Smith
...
```

The easiest way to prepare such a file is to use a spreadsheet program and export as "CSV".

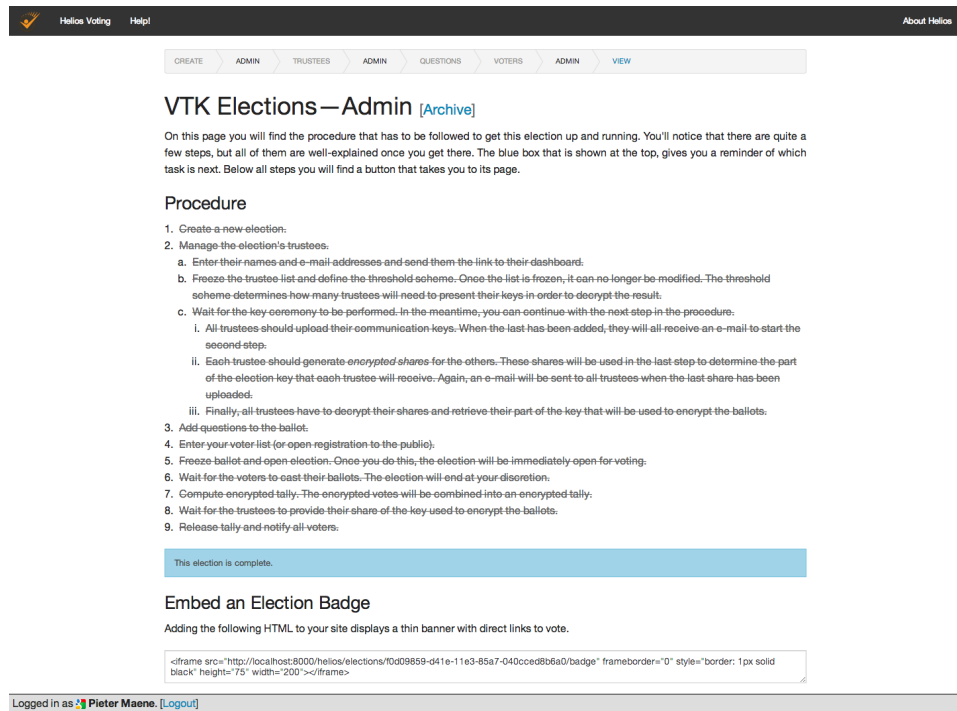
List of Voters [Choose File](#) No file chosen

[Upload](#)

Logged in as Pieter Maene. [\[Logout\]](#)

FIGUUR 4.5: Uploaden van kiezers

4. PROCEDURE



FIGUUR 4.6: Admin

4.2.5 Bevriezen van het stembilhet

Wanneer alle voorgaande informatie ingegeven is en de sleutelceremonie afgerond, kan het stembilhet bevroren worden. Wanneer er geen tijdstip gegeven is waarop de verkiezing moet starten, kunnen de kiezers onmiddellijk beginnen stemmen. Wanneer geen einddatum opgegeven is, blijft ze open totdat de beheerder ze sluit.

4.2.6 Telling

De stemming kan steeds manueel afgesloten worden door het telproces te starten. De stemmen worden dan homomorf samengeteld in een geëncrypteerd resultaat (Sectie 3.1.2). Vooraleer dit gedecrypteerd kan worden, moeten we opnieuw wachten op de trustees.

Wanneer geen threshold encryptie gebruikt wordt, moeten alle trustees nu hun decryptiefactor berekenen en uploaden. Wordt dit wel gebruikt, dan moeten slechts k van de n trustees dit doen. Zodra alle nodige decryptiefactoren beschikbaar zijn, kan de beheerder het resultaat vrijgeven. Indien geen publicatiedatum opgegeven werd, is het resultaat dan voor iedereen beschikbaar. Anders kan de beheerder het resultaat wel reeds bekijken, maar wordt het pas gepubliceerd op die datum.

Interface

Het verbeteren van de gebruiksvriendelijkheid van het Helios verkiezingssysteem was het doel van deze thesis. Er zijn op vier belangrijke plaatsen wijzigingen aangebracht. Veruit het meeste werk was nodig om de procedure van [Hoofdstuk 4](#) duidelijker te maken in het beheer ([Sectie 5.1](#)). Ook de gebruiksvriendelijkheid van het trustee dashboard werd sterk verbeterd ([Sectie 5.2](#)). Tot slot werd ook de output van de applicatie die gebruikt kan worden om het resultaat te controleren, verduidelijkt ([Sectie 5.3](#)). Hoewel in dit hoofdstuk alleen de grootste aanpassingen besproken worden, werd de layout doorheen het hele systeem aangepast.

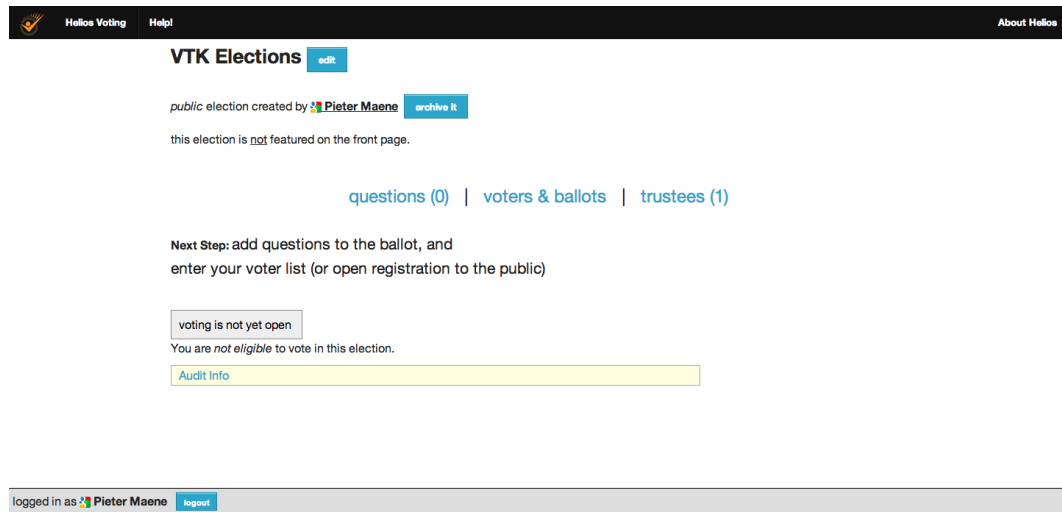
5.1 Beheer

In de oude interface zaten het beheer en het bekijken van de verkiezing op dezelfde pagina ([Figuur 5.1](#)). De gewone kiezers zagen de beheersfuncties uiteraard niet, maar dit maakte het wel verwarrend voor de beheerder. Bovendien was het niet duidelijk wat de volgende stap was of waar de beheerder juist in de procedure zat. Daarom werd besloten om deze twee functies uit elkaar te halen en een aparte pagina te voorzien voor het beheer ([Figuur 5.2](#)).

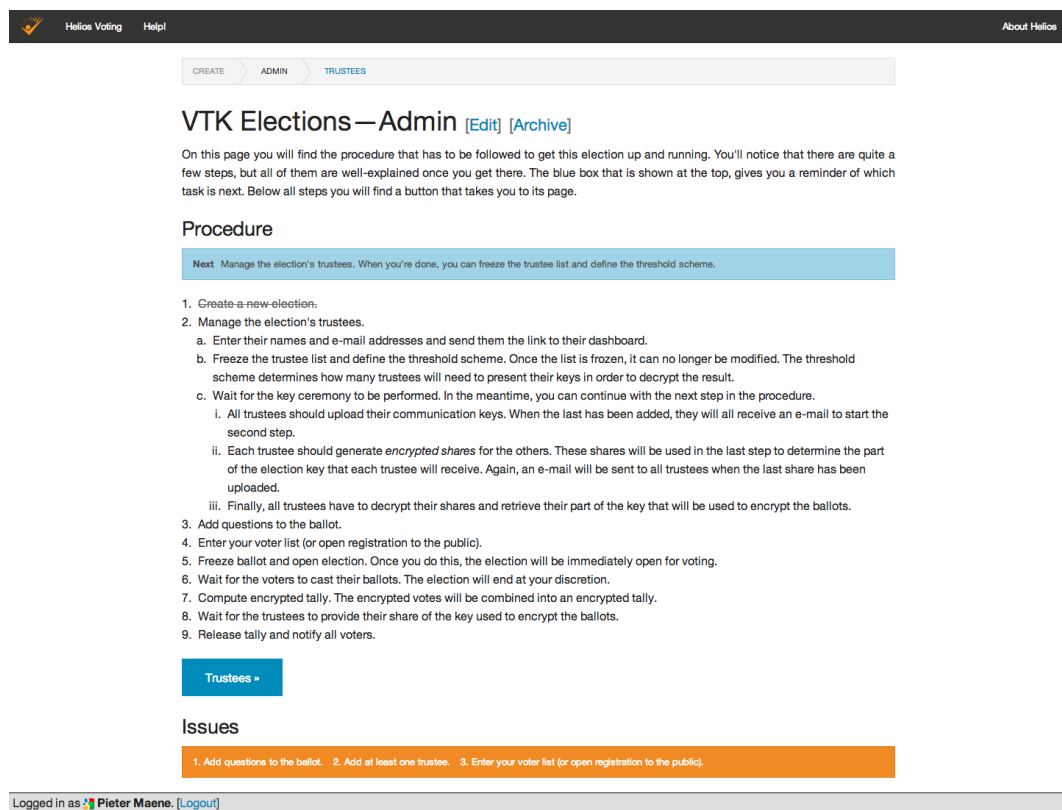
Op deze nieuwe pagina wordt de volledige procedure weergegeven. Er wordt ook aangegeven wat de volgende stap is en welke stappen reeds voltooid zijn. Tot slot staan onderaan alle problemen die nog opgelost moeten worden voordat het stembiljet bevroren kan worden. Bovendien wordt bovenaan elke pagina ook getoond waar de beheerder zit en wat de volgende stap is ([Figuur 5.3](#)). Zo kan hij dit ook volgen wanneer hij niet op de speciale beheerpagina zit.

Voor een verkiezing met threshold encryptie ([Sectie 3.1.3](#)) zijn er belangrijke veranderingen in de workflow. Robbert Coeckelbergh had een publiek bulletin board geïntroduceerd waar iedereen sleutelparen voor communicatie kon aanmaken en uploaden. De beheerder kon dan trustees toevoegen aan een verkiezing door ze te selecteren uit een lijst. Dit betekent ook dat dezelfde sleutelparen voor communicatie gebruikt werden bij elke verkiezing waar deze persoon trustee was.

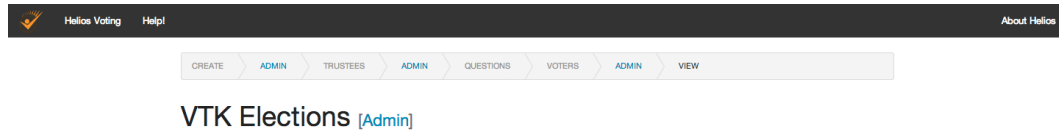
5. INTERFACE



FIGUUR 5.1: Overzicht van de verkiezing (oud)



FIGUUR 5.2: Beheer van de verkiezing



FIGUUR 5.3: Voortgang procedure

Voordat alle trustees toegevoegd konden worden aan een verkiezing, moest de beheerder dus wachten totdat iedereen zijn sleutelparen voor communicatie geüpload had. Omdat iedereen hiervoor buiten het systeem om nog eens gecontacteerd moest worden, maakte dit de sleutelceremonie nog ingewikkelder. Een bijkomend nadeel was dat om het even wie een sleutelpaar zou kunnen aanmaken, omdat het bulletin board publiek toegankelijk was. Omdat er ook geen controle was op de identiteit van de uploader, was het mogelijk om je als iemand anders voor te doen. Ervan uitgaande dat deze persoon geen toegang heeft tot de e-mailaccount van zijn slachtoffer, zou hij wel nooit de link krijgen naar het trustee dashboard ([Sectie 5.2](#)). Hij kan dus niet actief de rol van trustee spelen, maar kan het opzetten van de verkiezing wel tijdelijk blokkeren.

Daarom werd besloten om het bulletin board weg te halen. De trustees worden nu eerst toegevoegd aan de verkiezing, waarna ze een link krijgen toegestuurd naar hun trustee dashboard. De eerste stap van de sleutelceremonie die ze daar moeten uitvoeren, is nu het uploaden van de sleutelparen voor communicatie. Het proces dat een trustee doorloopt, wordt zo ook beter vergelijkbaar met dat wanneer geen threshold encryptie gebruikt wordt.

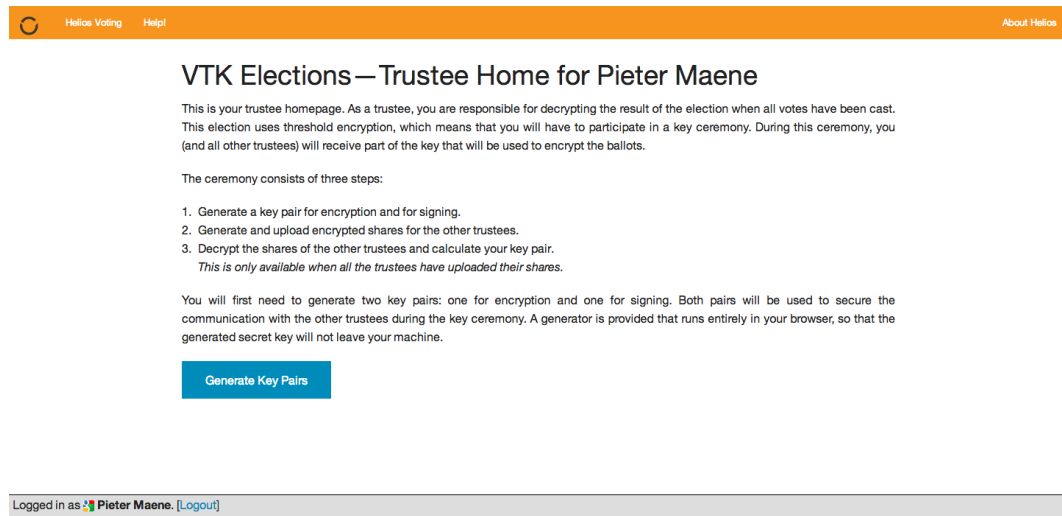
5.2 Trustee Dashboard

Iedere trustee krijgt een unieke link naar zijn trustee dashboard, dat wordt getoond in [Figuur 5.4](#). Deze link bevat naast zijn e-mailadres ook een geheime code. Dit is de plaats waar hij al de acties van de sleutelceremonie zal moeten uitvoeren. De beheerder van de verkiezing is ook vaak een trustee. De balk bovenaan werd oranje gemaakt zodat er voor hem een duidelijker verschil is tussen beide rollen.

Zoals vermeld in [Sectie 5.1](#) werd het aanmaken van de sleutelparen voor communicatie naar hier verplaatst. De volledige sleutelceremonie wordt hier op dezelfde manier getoond als de procedure voor de verkiezing op de pagina van de beheerder ([Figuur 5.2](#)). Op die manier ziet de trustee duidelijk welke stappen hij nog moet uitvoeren. Daarnaast wordt ook de rol van een trustee hier nog eens uitgelegd.

De trustee zal in totaal drie geheime sleutels genereren tijdens de sleutelceremonie ([Sectie 4.2.2](#)). Elke geheime sleutel moet lokaal bewaard worden in het JSON formaat. Oorspronkelijk moest de trustee deze zelf kopiëren naar een bestand. Om zijn sleutel te gebruiken, moest hij de inhoud daarvan opnieuw kopiëren naar een tekstvak.

5. INTERFACE



FIGUUR 5.4: Trustee Dashboard

Door gebruik te maken van de HTML5 File API kon de omgang met de sleutels veel gebruiksvriendelijker gemaakt worden.[32] Enerzijds voorziet deze API de `Blob` interface om lokaal bestanden te generen en aan te bieden als download in de browser. Anderzijds kan de `FileReader` interface gebruikt worden om objecten die voldoen aan de `Blob` of `File` interface uit te lezen. Een voorbeeld van deze laatste zijn bestanden die geselecteerd worden in een file input element.

In het trustee dashboard wordt de eerste API interface gebruikt om de geheime sleutels onmiddellijk in een JSON bestand te plaatsen dat gedownload kan worden. Zo krijgen de trustees direct een bestand en worden de cryptografische details van de sleutel voor hen verborgen. De tweede interface wordt dan weer gebruikt om de trustee deze bestanden te laten selecteren om vervolgens de geheime sleutel uit te lezen naar het tekstvak. Het verschil tussen de oude en nieuwe manier van werken kan gezien worden in [Figuur 5.5](#) en [Figuur 5.6](#) respectievelijk.

Om de communicatie te beveiligen worden twee sleutelparen gebruikt ([Sectie 3.1.3](#)). Oorspronkelijk moesten deze apart gedownload worden. Omdat het voor de gebruiker eenvoudiger is om maar met één bestand te moeten werken, werden deze samengevoegd.

5.3 Controleapplicatie

De controleapplicatie werd besproken in [Sectie 3.4](#). Het resultaat van de verificatie werd oorspronkelijk onduidelijk weergegeven ([Figuur 5.7](#)). Zoals gezien kan worden in [Figuur 5.8](#), werd er meer structuur gebracht in de output.

Helios Voting

Help!

About Helios

VTK Elections — Trustee Pieter Maene Home

Welcome, this is your trustee homepage.

As a trustee you are responsible for decrypting the result of the election when all the votes are casted.

Therefore you will have to agree on a secret with the other trustees and you will have to complete 4 steps:

First Step: Generate encrypted shares for the other trustees.

Second Step: Upload the shares.

Third Step: Decrypt the shares of the other trustees. (This is only available when all the trustees uploaded their shares)

Fourth Step: Save your secret key and upload your public key.

FIRST STEP: Generate your encrypted shares


To generate your encrypted shares enter your secret key for signatures:

*16171454362858168310348919157537769447689488454821738440009609393566161422826545340225660943261857316733095837412819970053270287734157926888923880284925734741817833808166385125411769928178256157437052613324420766068764813251264870197763776547098473637036158475394579642891388486224580689576831701469"

Generate encrypted shares

[skip to the second step](#)

(you need to have already computed your encrypted shares.)

Logged in as  **Pieter Maene.** [Logout](#)

FIGUUR 5.5: Genereren van encrypted shares (oud)

Helios Voting

Help!

About Helios

VTK Elections—Trustee Home for Pieter Maene

This is your trustee homepage. As a trustee, you are responsible for decrypting the result of the election when all votes have been cast. This election uses threshold encryption, which means that you will have to participate in a key ceremony. During this ceremony, you (and all other trustees) will receive part of the key that will be used to encrypt the ballots.

The ceremony consists of three steps:

1. Generate a key pair for encryption and for signing.
2. Generate and upload encrypted shares for the other trustees.
3. Decrypt the shares of the other trustees and calculate your key pair.

This is only available when all the trustees have uploaded their shares.


Generate Your Encrypted Shares

To generate your encrypted shares, you first have to enter your secret key for signing. If you generated your key pair with our generator, it was stored in a file called `communication_keys.json`. This file contains your private keys, which are unknown to the server. This is the reason you need it here again.

Secret Key for Signing communication_keys.json


{ "encryption": { "public_key": { "g":
"453151813875643964663339862169328223943710120431435472618409227525885020319627224726363
701529735668903577409091069810980332284525393196586705603070395613062360391093726191146
121415195311289299204727460560843415628717888690539062513769340997469477437688161936290
49261126632430965422637754104221208257819369317", "p":
"1683464927809373000890778943710564741860245155131062231020658882366753016874221778864193"

Generate Your Encrypted Shares

Logged in as  **Pieter Maene.** [Logout](#)

FIGUUR 5.6: Genereren van encrypted shares

5. INTERFACE

 Helios Voting

Election Verifier

Election URL

Start

Election

Loading election...
Loaded election: VTK Elections
Election fingerprint: GNkpQl2abBbXe73RVbi7UGFvoxbKERUm4a8vxfnx4vA
Loading list of voters...
Loaded voter list, now loading ballots for each...
Loading ballot for voter #1
FOUND a ballot for voter #1

Ballots

Voter #1
-- UUID: d8db6495-6002-4725-9e0f-7a42fa1a47f7
-- Ballot Tracking Number: lxiQz+R9H03GC7PrEqlkKyDEcRb5o1l2XEJVTl2l93Y
Question #1, Option #1 -- VERIFIED
Question #1, Option #2 -- VERIFIED
Question #1, Option #3 -- VERIFIED
Question #1 OVERALL -- VERIFIED
Question #2, Option #1 -- VERIFIED
Question #2, Option #2 -- VERIFIED
Question #2 OVERALL -- VERIFIED

Trustees

Trustee #1: pieter.maene@vtk.be
-- PK xIMrTb9m2d2pWlRzS/AwrsRbigBWgQfzVB4hcdHpN4 -- VERIFIED.


Tally

Question #1: Would you vote for or against the Pixel team as board of the student union VTK in the year 2014-2015?
Answer #1: Pro - COUNT = 1
-- Trustee pieter.maene@vtk.be: decryption factor verifies
-- VERIFIED
Question #2: Which ineligible would you prefer to win?
Answer #1: Rebellion - COUNT = 1
-- Trustee pieter.maene@vtk.be: decryption factor verifies
-- VERIFIED

FINAL RESULT

ELECTION FULLY VERIFIED -- SUCCESS!
verification took 2101 ms

FIGUUR 5.7: Controleapplicatie (oud)

 Helios Voting

Election Verifier

This tool will verify the tally of the specified election. The required data is retrieved from the server, but all calculations are done locally in your browser.

Election URL

Start

Election

Loading election...

Election Name	Election Fingerprint
VTK Elections	GNkpQ12ab5bXe73RVb17UGFv0xbkERUm4a8vxfnx4vA

✓ The election was verified.

Ballots

Loading voters...
Loading ballots...
✓ Voter #1
Verifying ballots...

Voter #1
UUID: d8db6495-6902-4725-9a0f-7a43fala47ef
Smart Ballot Tracker: lxiQz+R9H03GC7PzEqikKyDEcRb5o1l2XEJVT2I93Y

Questions

Question #1
✓ Option #1
✓ Option #2
✓ Option #3
✓ Question #1

Question #2
✓ Option #1
✓ Option #2
✓ Question #2

✓ All ballots were verified.

Trustees

Loading trustees...
Trustee #1 <pieter.maene@vtk.be>
✓ Public Key: xIMrTb9m2d2pWIRz5/AvwraRbjg9WgQfzVB4hdHpn4

Tally

Question #1
Would you vote for or against the Pixel team as board of the student union VTK in the year 2014-2015?

Tally
Pro: 1
Decryption Factors
✓ Trustee #1 <pieter.maene@vtk.be>

Contra: 0
Decryption Factors
✓ Trustee #1 <pieter.maene@vtk.be>

Abstention: 0
Decryption Factors
✓ Trustee #1 <pieter.maene@vtk.be>

Question #2
Which ineligible would you prefer to win?

Tally
Rebellion: 1
Decryption Factors
✓ Trustee #1 <pieter.maene@vtk.be>

Nautilus: 1
Decryption Factors
✓ Trustee #1 <pieter.maene@vtk.be>

✓ The tally was verified.

FIGUUR 5.8: Controleapplicatie

Kringverkiezing

Het Helios verkiezingssysteem werd in de praktijk gebruikt tijdens de kringverkiezing van de Vlaamse Technische Kring. Dit is de faculteitskring van de studenten burgerlijk ingenieur aan de KU Leuven. Om het systeem hiervoor te kunnen gebruiken, waren enkele aanpassingen nodig die overlopen worden in [Sectie 6.1](#). Gezien het cruciale karakter van een verkiezing, werd het systeem vervolgens uitgebreid getest ([Sectie 6.2](#)). Tot slot wordt het verloop van de stemdag zelf besproken in [Sectie 6.3](#).

6.1 Aanpassingen

6.1.1 Shibboleth

Shibboleth is het authenticatie mechanisme dat gebruikt wordt voor de centrale login van de KU Leuven. Iedere gebruiker kan uniek geïdentificeerd worden aan de hand van zijn studentnummer. Alle stemgerechtigde kiezers voor een kringverkiezing hebben een dergelijke account. Helios had hier echter nog geen ondersteuning voor. Gezien het modulaire ontwerp van het authenticatiesysteem, was dit relatief eenvoudig toe te voegen.

De kieslijsten zelf werden opgemaakt door LOKO, de Leuvense studentenkoepel. Deze moesten wel nog omgezet worden naar een bestand dat uitgelezen kon worden door Helios. Het studentnummer werd hierbij gebruikt als het unieke ID voor elke kiezer. Een probleem was hier wel dat de e-mailadressen van de kiezers niet mee opgenomen waren in deze lijsten. Deze kunnen wel mee doorgegeven worden met het antwoord dat de server ontvangt nadat de student zich aangemeld heeft via de centrale login.

6.1.2 Opkomst

Bij VTK vertegenwoordigt het praesidium de studenten ook op onderwijsvlak. Om dit te kunnen doen, moet er volgens het reglement van LOKO een meerderheid behaald worden bij een opkomst van minstens 10%.^[23] De berekening van dit percentage werd dan ook toegevoegd zodat dit samen met de resultaten bekend gemaakt kon worden.

6.1.3 Publicatie van het resultaat

Helios publiceert het resultaat van de verkiezing standaard van zodra het bekend is. Het is echter traditie om deze pas om middernacht bekend te maken. Het systeem moest hier dus licht voor aangepast worden.

6.2 Testen

Om er zeker van te zijn dat het systeem op de stemdag zelf goed zou functioneren, werd het na de installatie op de server getest. Hierbij werd niet alleen nagegaan of alles technisch in orde was, maar werd ook feedback gevraagd over de gebruiksvriendelijkheid.

De testen van het beheer (Sectie 6.2.1) en het stembokje (Sectie 6.2.2) werden uitgevoerd in de context van de verkiezingen bij VTK, die hier wat verder belicht wordt. Het Neutraal Comité, dat alles in goede banen leidt, wordt bij VTK aangeduid met VKK. De huidige praeses is hier steeds de voorzitter van. Hij wordt geholpen door een aantal vrijwilligers uit het praesidium die geen kandidaat zijn. Er zijn twee verschillende types kiesploegen bij VTK. Enerzijds zijn er de serieuze ploegen die opkomen als praesidium voor het volgende jaar en anderzijds de lolploegen die niet als vertegenwoordigers verkiesbaar zijn.

6.2.1 Beheer

Aangezien hier de meeste veranderingen gebeurd zijn (Sectie 5.1), moest zeker dit deel goed getest worden. Hiervoor werd een testverkiezing aangemaakt door de voorzitter van VKK, met de echte trustees en vragen. De echte kieslijsten werden vervangen door een lijst met de huidige praesidiumleden.

De trustees voor de verkiezing zijn de zes leden van VKK. Als threshold schema (Sectie 3.1.3) werd ervoor gekozen dat drie van hen nodig zijn om het resultaat te decrypteren. Tijdens deze test kwamen echter twee fouten naar boven. Ten eerste werd de Lagrange-interpolatie niet over het eindig veld berekend, maar met een rationale breuk. Wanneer slechts twee trustees gebruikt werden, was dit geen probleem omdat de noemer dan gelijk is aan één. Dit kon eenvoudig opgelost worden door de teller en noemer voor het hele product apart te berekenen (Vergelijking 6.1 en Vergelijking 6.2). Vervolgens wordt de teller vermenigvuldigd met de modulaire inverse van de noemer (Vergelijking 6.3).

$$N_i = \prod_{j=1, j \neq i}^k -x_j \mod q \quad (6.1)$$

$$D_i = \prod_{j=1, j \neq i}^k (x_i - x_j) \mod q \quad (6.2)$$

$$\lambda_i(0) = N_i * (D_i^{-1} \mod q) \mod q \quad (6.3)$$

Ten tweede werd de Helios trustee automatisch toegevoegd als trustee aan de verkiezing. Alle acties die een trustee moet uitvoeren, waren hiervoor geautomatiseerd. Na het uitvoeren van een aantal tests bleek dat de shares van deze trustee niet compatibel waren met deze van de anderen. Het grote verschil tussen beide is dat deze van Helios in Python en niet in JavaScript gegenereerd werden. Omdat er niet direct een fout gevonden kon worden, werd ervoor gekozen om Helios niet langer als trustee toe te voegen. Omdat alles hiervoor geautomatiseerd was, had deze toch niet zo'n belangrijke rol binnen het proces. Hij werd voornamelijk toegevoegd omdat dan een verkiezing zonder eigen trustees opgezet kon worden, wat leidt tot een eenvoudigere procedure.

Verder verliep deze test zeer goed. De voorzitter kon zonder hulp de volledige procedure ([Hoofdstuk 4](#)) voor het aanmaken van een verkiezing met threshold encryptie doorlopen. Er werd verder geen formele analyse van de nieuwe interface gemaakt, aangezien deze slechts door een beperkt aantal mensen gebruikt zal worden. Ook de trustees hadden weinig moeite om hun geheime sleutels te bekomen. Ondanks de e-mails die verstuurd worden telkens een actie van hen nodig is, duurde het nog steeds even voordat dit in orde was.

6.2.2 Stemhokje

Tijdens het testen kwamen geen functionele problemen naar voor met het stemhokje. Toch kwam ook hier veel feedback op van het praesidium. Veel mensen vonden het stemmen niet intuïtief. Er waren twee belangrijke bemerkingen. Ten eerste waren sommige bewoordingen te ingewikkeld. De interface is volledig in het Engels en er kwamen veel onbekende vaktermen in voor. Dit kon eenvoudig opgelost worden door eenvoudigere terminologie in de plaats te gebruiken.

Ten tweede vonden velen het proces te moeilijk. Oorspronkelijk waren er vier stappen. Gebruikers kregen eerst een korte uitleg, gevolgd door het aanduiden van hun keuzes. Hierna konden deze gecontroleerd worden, waarna de stem geëncrypteerd werd. Daarna volgde nog een scherm ([Figuur 6.1](#)) waar gekozen kon worden om een audit te doen van de stem of ze te uploaden. In het laatste geval werd het stemhokje verlaten, maar moest de gebruiker nog eens bevestigen dat hij zijn stem wilde uitbrengen. Vooral deze twee laatste stappen vonden veel mensen verwarrend.

Om dit proces te vereenvoudigen, werd de laatste stap van het stemhokje verwijderd. Na het bevestigen van zijn keuzes, wordt de kiezer onmiddellijk doorgestuurd naar het uploaden buiten het stemhokje. De audit van een stem werd verplaatst naar het scherm waar de keuzes bevestigd moet worden. Omdat de stem hiervoor reeds geëncrypteerd moet zijn, wordt dit nu gedaan na het beantwoorden van de laatste vraag. Het grootste nadeel hierbij is dat de encryptie opnieuw uitgevoerd moet worden wanneer de kiezer zijn stem wijzigt. In de huidige implementatie gaat dit echter al relatief vlot in moderne browsers. In de toekomst zal dit waarschijnlijk nog sneller kunnen door gebruik te maken van de Web Cryptography API ([Hoofdstuk 8](#)).

Helios Voting Booth [\[exit\]](#)

VTK Elections

(1) Select (2) Review (3) Submit

Your ballot is ready to be submitted

Don't forget to click "Proceed to Submission" below!

Before submitting, you can take note of your smart ballot tracker [\[print\]](#):

xOEHgJGQFRS+P7+TK9TAvy/5HAzdKWjwweJrUBpfti4

Once you click "Proceed", Helios will remember only your encrypted vote. Thus, only you know your vote.

[Proceed to Submission](#)

Election Fingerprint: 7Nmwrht9VyXGrF/L6hAX+oon1V2gdWV1Ugjk5Vch6m4 [help!](#)

FIGUUR 6.1: Laatste scherm van het stemhokje

Helios Voting [Help!](#) [About Helios](#)

VTK Elections—Confirm Your Vote

We have received, but not yet recorded, your encrypted ballot. To upload your encrypted ballot to the server, please click on the button below.

[I am Pieter Maene, submit my vote!](#)

You can cast as many ballots as you want: only the last one counts.

If you cancel now, your ballot will **not** be recorded. You can start the voting process over again, of course.

[Cancel](#)

Your Smart Ballot Tracker

1xiQz+R9H03GC7PrEq1kKyDEcRb5o112XEJVTl2I93Y

Logged in as Pieter Maene. [\[Logout\]](#)

FIGUUR 6.2: Bevestigen van de stem

Na het aanpassen van het stemhokje werd deze test herhaald om zeker te zijn dat alles nog correct werkte. Ook tijdens deze test kwamen nog vragen om enkele kleine dingen te wijzigen voor de echte verkiezing. Zo wordt er een waarschuwing gegeven wanneer de kiezer het laatste scherm sluit voordat hij zijn stem geüpload heeft.

6.2.3 Stresstest

Er is elk jaar een opkomst van ongeveer 25% bij de kringverkiezing van VTK, wat iets minder dan 1 000 kiezers zijn. Daarom werd nagegaan of Helios ook een groot

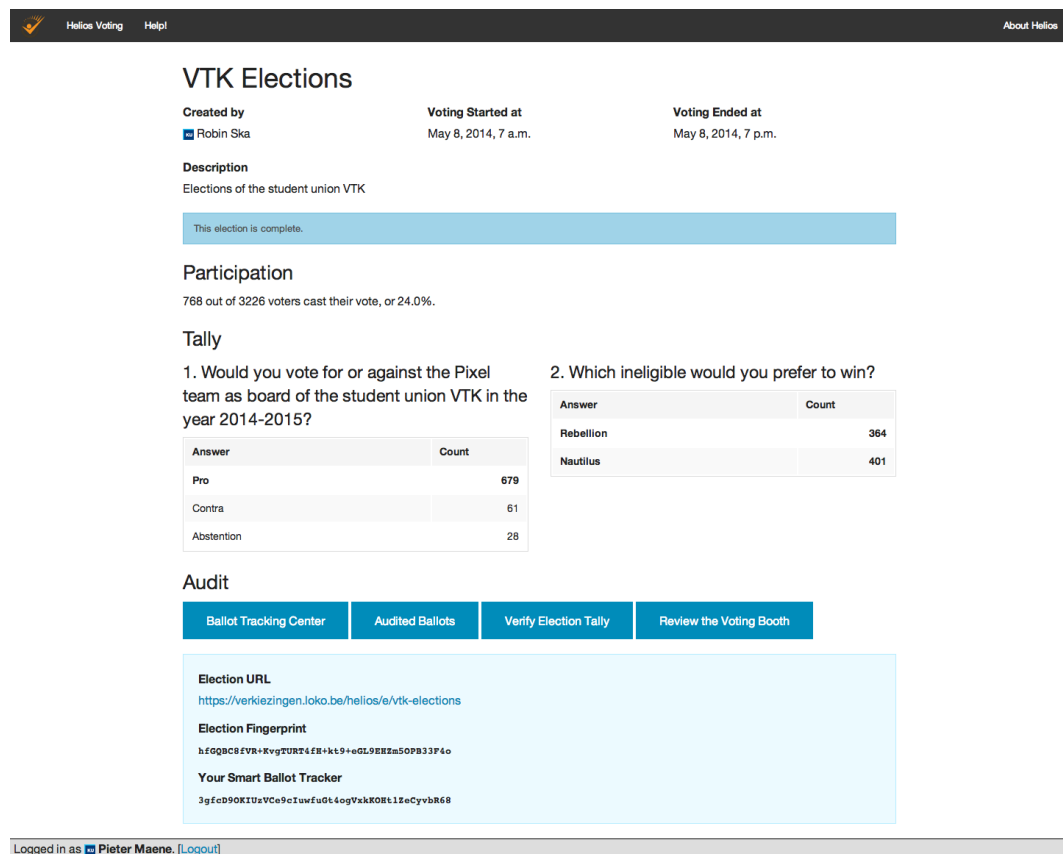
aantal stemmen nog correct kon verwerken. Hiervoor werd een aparte verkiezing aangemaakt met twee trustees en drie vragen. Vervolgens werden 1 000 stemmen uitgebracht. Het resultaat kon van de eerste keer correct gedecrypteerd worden, dus hier was geen verdere actie nodig.

Deze stemmen werden gegenereerd door een server-side actie. De kiezers stemmen normaal via het stemhokje, maar dat proces is moeilijk te automatiseren. Het grote verschil is dat de encryptie in Python in plaats van JavaScript gebeurt.

6.3 Stemdag

De stemming zelf vond plaats op donderdag 8 mei 2014. Oorspronkelijk stond ze open van 7u00 tot 19u00. Omdat de communicatie 's ochtends traag op gang gekomen was, werd dit verlengd tot 20u00, wat ondersteund wordt door Helios. De trustees en het threshold schema waren dezelfde als tijdens de test ([Sectie 6.2.1](#)). De vragen en het resultaat worden getoond in [Figuur 6.3](#). In totaal hebben 768 mensen hun stem uitgebracht, wat een sterke indicatie is dat het proces voldoende eenvoudig was. Zowel bij het stemmen als het decrypteren van het resultaat waren er geen problemen.

6. KRINGVERKIEZING



FIGUUR 6.3: Resultaat van de stemming

Bewaren van sleutels en fingerprints

Tijdens de sleutelceremonie genereren de trustees sleutelparen, waarvan de sleutels uiteraard veilig bewaard moeten kunnen worden ([Sectie 7.1](#)). Daarnaast werkt Helios op verschillende plaatsen met fingerprints. In [Sectie 7.2](#) wordt eerst hun doel besproken, waarna gekeken wordt naar alternatieve methoden om ze weer te geven.

7.1 Sleutels

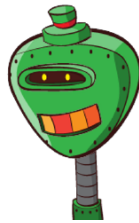
7.1.1 Disk

De trustees downloaden hun geheime sleutels als JSON bestanden ([Sectie 5.2](#)). Deze zullen dus eerst bewaard worden op de harde schijf van de computer die op dat moment gebruikt wordt. Hier zijn twee belangrijke nadelen aan. Ten eerste zou iedereen die toegang heeft tot die machine de sleutel kunnen bemachtigen. Ten tweede kan de sleutel alleen vanaf deze machine gebruikt worden.

Een eenvoudige oplossing voor het eerste probleem is de trustees vragen om hun account zeker te beveiligen met een wachtwoord. De sleutel zou ook op een beveiligde partitie geplaatst kunnen worden. Dit kan bijvoorbeeld gedaan worden door gebruik te maken van TrueCrypt.[\[44\]](#)

Wanneer de sleutel op een andere machine ingevoerd moet worden, kan deze op een USB-stick opgeslagen worden. Hier is het zeker aangeraden om de sleutel op een geëncrypteerde partitie te plaatsen. Daarnaast zou de sleutel ook geüpload kunnen worden naar een private server of een cloud opslagdienst. In dit geval moet hij zeker eerst geëncrypteerd worden.

Het zou echter veel gebruiksvriendelijker zijn om dit in de generator in te bouwen. Voordat de sleutel gedownload wordt, kan deze eerst symmetrisch geëncrypteerd worden met een wachtwoord. Hiervoor zou bijvoorbeeld AES-CTR gebruikt kunnen worden, waarbij de sleutel afgeleid wordt van het opgegeven wachtwoord.[\[21\]](#) Er zijn verschillende JavaScript libraries die hiervoor ondersteuning hebben.[\[12\]](#)[\[7\]](#) Bovendien wordt deze mode ook ondersteund door de Web Cryptography API ([Hoofdstuk 8](#)).[\[40\]](#)



FIGUUR 7.1: RoboHash van de fingerprint in [Figuur 6.2](#)

7.1.2 Web Storage [\[18\]](#)[\[28\]](#)

Door gebruik te maken van de HTML5 Web Storage specificatie, zouden de sleutels ook op een alternatieve manier bewaard kunnen worden. Deze specificatie geeft een ontwikkelaar onder andere toegang tot een persistente key/value store waar tot 5MB aan data in opgeslagen kan worden. Er wordt ook voldaan aan de same-origin policy. Dit wil zeggen dat de data alleen toegankelijk zijn van op hetzelfde domein.[\[17\]](#)

Deze functionaliteit zou toelaten om de geheime sleutels volledig te verbergen voor de trustees. In plaats van hen een bestand te laten downloaden met de sleutels, worden deze in de `localStorage` opgeslagen. Aangezien er naast de same-origin policy geen beveiligingsmechanismen ingebouwd zijn in de specificatie, is het beter om de sleutel eerst te encrypteren ([Sectie 7.1.1](#)). Een `secureStorage` binnen de browser met ingebouwde encryptie zou dit nog eenvoudiger maken voor een ontwikkelaar.[\[55\]](#) Een groot nadeel aan deze oplossing is dat de sleutel vast zit in de machine die gebruikt is om hem aan te maken.

7.2 Fingerprints

Op verschillende plaatsen binnen Helios worden fingerprints gebruikt. Dit zijn base64-geëncodeerde SHA-256 hashes van specifieke data. Zo is de *Smart Ballot Tracker* ([Figuur 6.2](#)) een fingerprint van de geëncrypteerde stem. Aan de trustee wordt ook een fingerprint van de gegenereerde publieke sleutels getoond. Dit zijn echter lange strings zijn die moeilijk te onthouden kunnen worden. Bovendien kan niet in één oogopslag gezien worden of twee fingerprints hetzelfde zijn.

Daarom kunnen hiervoor beter visuele hashes gebruikt worden. Dit zijn unieke afbeeldingen op basis van een bepaalde string. Afbeeldingen kunnen niet alleen sneller herkend worden, het is ook veel eenvoudiger om ze te bewaren. Wanneer de fingerprint een string is, moet deze neergeschreven worden of gekopieerd worden naar een bestand. Een afbeelding daarentegen kan eenvoudig gedownload worden. Voorbeelden van dergelijke visuele hashsystemen zijn RoboHash ([Figuur 7.1](#)) en Identicon.[\[38\]](#)[\[50\]](#)

Web Cryptography API

Wanneer webontwikkelaars vandaag cryptografische functies nodig hebben in hun toepassingen, moeten ze bijna JavaScript gebruiken omwille van compatibiliteit. Hoewel er de laatste jaren zeer grote vooruitgang geboekt is, zullen de meeste JavaScript engines nog steeds minder goed presteren dan native code.[\[34\]](#)[\[11\]](#)[\[41\]](#) De W3C startte in 2012 een working group op om een nieuwe browser API te definiëren: de Web Cryptography API.[\[47\]](#)

In [Sectie 8.1](#) wordt deze nieuwe API kort besproken. Daarna wordt in [Sectie 8.2](#) gekeken naar de NfWebCrypto polyfill, die de nieuwe functionaliteit implementeert in een plugin voor Google Chrome. Tot slot wordt deze implementatie in [Sectie 8.3](#) vergeleken met bestaande cryptografische libraries.

8.1 Web Cryptography API [\[40\]](#)

De Web Cryptography API definieert cryptografische operaties die gebruik maken van sleutels die beheerd worden door de browser. Al deze methodes zitten in de `SubtleCrypto` interface. Er zijn zowel methodes voor het beheren van het sleutelmateriaal als het encrypteren van data.

De API is ontworpen vanuit het idee om alleen standaardfunctionaliteit aan te bieden. Er wordt dus maar een beperkt aantal algoritmes ondersteund, die bovendien elk nog vaak hun eigen beperkingen hebben.[\[13\]](#) Naargelang de functionaliteit van het algoritme, ondersteunt ook niet elk algoritme alle methodes van de interface.

8.2 NfWebCrypto

Aangezien de standaard nog niet voltooid is, wordt deze nauwelijks ondersteund door de grote browsers.[\[19\]](#) Alleen Internet Explorer 11 heeft reeds een implementatie, maar hierin is slechts een beperkt aantal algoritmes aanwezig.[\[26\]](#) Om de vergelijking met de andere JavaScript libraries toch te kunnen uitvoeren, was dus een alternatieve implementatie nodig van deze API.

PolyCrypt is een JavaScript polyfill ontwikkeld door BBN Technologies.[29] Een polyfill implementeert een browser API die (nog) niet native ondersteund wordt. Omdat deze gebaseerd is op een oudere draft van de API, miste ook hierin functionaliteit die nodig was voor de tests. Een bijkomend nadeel aan deze implementatie is dat ze in JavaScript geschreven is, waardoor een eventueel snelheidsvoordeel ten opzichte van de andere libraries waarschijnlijk niet naar voor zou komen.

NfWebCrypto daarentegen is een C++ polyfill ontwikkeld door Netflix.[27] Intern wordt de bekende OpenSSL library gebruikt voor de cryptografische functionaliteit. Het grote voordeel is hier dus dat de cryptografische code nu native is, waardoor de prestaties vergelijkbaar zouden moeten zijn met die van een echte implementatie in de browser. Het grootste nadeel is hier wel dat het een plugin is voor Chrome. Bovendien moet deze handmatig gecompileerd worden en moet de browser op een speciale manier gestart worden, zodat het gebruik ervan niet zo vanzelfsprekend is. Hoewel dit dus gebruikt kan worden voor de tests, is dit niet direct bruikbaar voor praktische applicaties.

8.3 Benchmarks

8.3.1 Modulaire exponentiatie

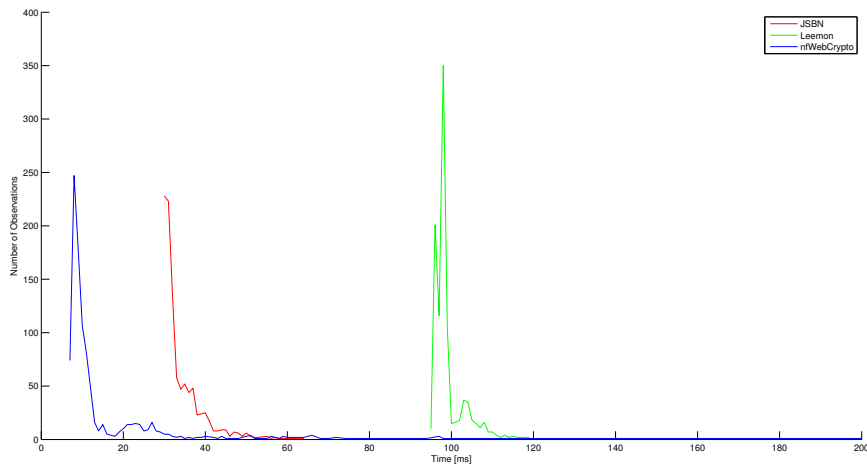
Helios maakt gebruik van ElGamal (Sectie 3.1.1) om de stemmen te encrypteren. Dit algoritme wordt echter niet ondersteund door de Web Cryptography API (Sectie 8.1). Deze kan dus niet onmiddellijk gebruikt worden om de encryptie te versnellen. De modulaire exponentiaties vragen veruit de meeste rekentijd. Een verbetering daar zou dus ook positief zijn voor de algemene prestaties.

Aangezien de enige publieke methodes van de API op hoog niveau werken, is er geen functie beschikbaar om dit te doen. Diffie-Hellman wordt echter wel ondersteund voor het genereren van een asymmetrisch sleutelpaar. De `deriveKey` methode van de API berekent de gedeelde geheime sleutel volgens Vergelijking 8.1.[14]

$$K = (g^a)^b \mod p \quad (8.1)$$

Hier is g^a de publieke sleutel van A en b de geheime sleutel van B. Om de modulaire exponentiatie $x^y \mod p$ uit te rekenen, moet het dus mogelijk zijn om de publieke sleutel g^a gelijk te stellen aan x en de geheime sleutel aan y .

Om een specifieke geheime sleutel te kunnen gebruiken in de `deriveKey` methode, moet deze eerst geïmporteerd worden in de key store. Hiervoor kan de `importKey` methode gebruikt worden. Samen met de naam van het algoritme (DH) worden als parameters de geheime sleutel, het priemgetal p en de generator g meegegeven. De standaard laat het importeren van de geheime sleutel alleen toe wanneer deze het PKCS8 formaat heeft.[22] Om de testen te vereenvoudigen, werd de NfWebCrypto



FIGUUR 8.1: Modulaire exponentiatie

plugin aangepast om het importeren van ruwe geheime sleutels toch mogelijk te maken.

Daarna kan de modulaire exponentiatie uitgerekend worden door `deriveKey` aan te roepen met x als argument voor de publieke sleutel. Na het afleiden wordt de gemeenschappelijke sleutel opnieuw opgeslagen in de key store. Ook hier waren enkele kleine aanpassingen nodig aan de code van de plugin om het berekenen van de geheime sleutel met onze eigen waarden mogelijk te maken. De `exportKey` methode kan tot slot gebruikt worden om het ruwe resultaat te exporteren.

De prestaties van NfWebCrypto worden vergeleken met deze van JSBN en Leemon, twee big number libraries die geschreven zijn in JavaScript.[54][6] Er wordt telkens een exponent van 1024 bit gebruikt, wat ook de lengte van de parameters in Helios is. De berekening werd voor elke library 1000 keer uitgevoerd om een statistisch relevant resultaat te bekomen. De resultaten worden weergegeven in **Figuur 8.1** en **Tabel 8.1**. De berekening duurt bij Leemon veruit het langste. De JSBN library is sterk geoptimaliseerd. De NfWebCrypto plugin is daarentegen gemiddeld nog eens dubbel zo snel. De variantie is hier zo groot omdat de eerste exponentiatie veel langer duurt.

Het resultaat dat bekomen wordt na de `exportKey` is wel niet correct. In de communicatie met de plugin moeten de parameters `base64` geëncodeerd worden. Vermoedelijk loopt hier nog iets mis tussen de conversie in JavaScript en C++ .

8.3.2 RSA

Een tweede vergelijking werd gemaakt tussen JSBN en NfWebCrypto voor een RSA encryptie. Dit wordt niet gebruikt in Helios, maar ook deze resultaten zijn

Library	Gemiddelde [ms]	Variantie [ms]
JSBN	33,9250	26,5019
Leemon	99,1470	15,0785
NfWebCrypto	16,0670	470,6251

TABEL 8.1: Modulaire exponentiatie

Library	Gemiddelde [ms]	Variantie [ms]
JSBN	0,6310	0,3632
NfWebCrypto	2,1360	0,4219

TABEL 8.2: RSA

zeer interessant. De berekening van de RSA cijfertekst is opnieuw een modulaire exponentiatie ([Vergelijking 8.2](#)).[\[36\]](#)

$$c = m^e \mod n \quad (8.2)$$

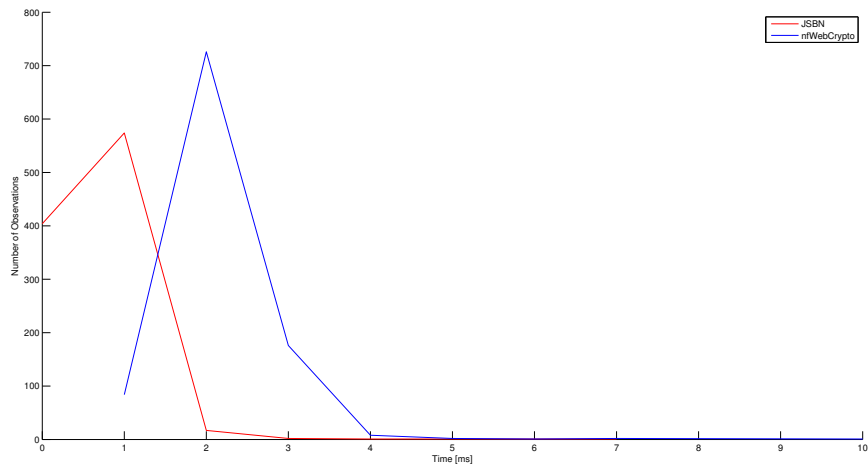
Hier is het paar (n, e) de publieke sleutel van de partij waarvoor het bericht geëncrypteerd wordt. Voor de publieke exponent e werd de standaardwaarde 65 537 genomen. Merk op dat deze heel wat korter is dan de 1 024-bit exponenten die in de tests van [Sectie 8.3.1](#) gebruikt werden. De lengte van de modulus is 1 024 bit.

De JSBN library voorziet in enkele klassen specifiek voor RSA encryptie en decryptie. Het is dus zeer eenvoudig om een bepaalde klaartekst te encrypteren met een gegeven publieke sleutel. De Web Cryptography API ondersteunt hier het `RSAPKCS1-v1_5` algoritme voor.[\[20\]](#) Hoewel het mogelijk zou moeten zijn om publieke sleutels in het SPKI-formaat te importeren, bleek het opnieuw moeilijk om de sleutel die gebruikt werd voor de JSBN encryptie om te zetten. Daarom werd besloten om voor elke encryptie een nieuwe sleutel te genereren. De tijd die hiervoor nodig is, wordt niet meegerekend in het eindresultaat.

Ook hier werd de encryptie 1 000 keer uitgevoerd. De resultaten van deze test zijn terug te vinden in [Figuur 8.2](#) en [Tabel 8.2](#). We zien dat de JavaScript implementatie voor deze veel kortere exponent sneller is dan de berekening door de NfWebCrypto plugin. De communicatie met de plugin weegt hier duidelijk zwaarder door.

8.4 Besluit

Dankzij de Web Cryptography API zal het eenvoudiger worden om cryptografie te gebruiken in de browser. Bovendien is er een merkbare snelheidswinst ten opzichte van de huidige JavaScript implementaties, wat belangrijk is voor de gebruiksvriendelijk.



FIGUUR 8.2: RSA

Dat slechts een beperkt aantal algoritmes ondersteund wordt, is een belangrijk nadeel van de API. Omdat de methodes die publiek beschikbaar zijn op een hoog niveau werken, is het zeer moeilijk om deze te gebruiken voor het versnellen van alternatieve algoritmes.

Daarnaast was het ook ingewikkeld om sleutels die buiten de plugin gegenereerd waren, correct te importeren. Dit werd echter voornamelijk veroorzaakt door de encoding van de communicatie en is dus niet noodzakelijk een inherent probleem van de API.

Besluit

Om het vertrouwen van kiezers in het resultaat te vergroten, kan een voter-verifiable verkiezingssysteem gebruikt worden. Er zijn verschillende papieren systemen beschikbaar die dit realiseren, maar deze hebben zeer complexe procedures. Hierdoor kunnen ze vaak niet op grote schaal gebruikt worden in de praktijk ([Sectie 2.5](#)). Helios is een voter-verifiable stelsysteem voor online verkiezingen. Dit betekent wel dat het alleen gebruikt kan worden wanneer dwang geen grote bedreiging vormt.

De procedure die gevolgd moet worden om een verkiezing op te zetten in Helios werd besproken in [Hoofdstuk 4](#). De interface werd ook zo aangepast dat deze procedure er veel duidelijker in terug te vinden is ([Sectie 5.1](#)). In de praktische tests bleek dat deze nieuwe interface een grote hulp was. Beheerders van de verkiezing konden zonder veel aanwijzingen een verkiezing met threshold encryptie opzetten ([Sectie 6.2.1](#)).

Om Helios te gebruiken in de kringverkiezing van VTK, werden eerst nog enkele aanpassingen doorgevoerd. Vervolgens werd alles grondig getest en op basis van de gegeven feedback nog verder gewijzigd. Vooral de procedure in het stembokje werd tijdens deze tests als te complex ervaren ([Sectie 6.2.2](#)). In [Sectie 6.3](#) werd de stemdag zelf besproken, waarbij geen grote problemen vastgesteld werden.

In [Sectie 7.1.1](#) werd gezien dat de geheime sleutels van de trustees bewaard worden in een bestand. Ook wanneer ze deze ergens anders nodig hebben, zullen deze vaak op een USB-stick geplaatst worden. Om de sleutels te beveiligen kan ofwel de partitie geëncrypteerd worden, ofwel de bestanden zelf. Als alternatief zouden deze ook in de browser zelf opgeslagen kunnen worden ([Sectie 7.1.2](#)). Visuele hashes zouden het bewaren en vergelijken van de fingerprints sterk vergemakkelijken ([Sectie 7.2](#)).

De Web Cryptography API geeft webontwikkelaars eenvoudig toegang tot cryptografische functies. Uit de vergelijkingen met bestaande JavaScript implementaties bleek dat deze ook een grote snelheidsverbetering opleveren. Er wordt wel slechts een beperkt aantal algoritmes ondersteund en de API biedt alleen high-level functies aan, waardoor het zeer moeilijk is om alternatieven te implementeren ([Sectie 8.3.1](#)).

Bijlage

A

English Paper

Online Elections in Practice: Improvement and Application of the Helios Voting System

Pieter Maene

Abstract—

- I. INTRODUCTION
- II. PROCEDURE
- III. INTERFACE
- IV. WEB CRYPTOGRAPHY API
- V. CONCLUSIONS

Bibliografie

- [1] A. Adi, W. Adi, M. Schöler, and P. Fröhlich. Demonstration of “Open Counting”: A Paper-Assisted Voting System with Public OMR-At-A-Distance Counting.
- [2] B. Adida. *Advances in Cryptographic Voting Systems*. PhD thesis, MIT, 2006.
- [3] B. Adida. Helios: Web-based Open-Audit Voting. In *Proceedings of the 17th Conference on Security Symposium*, pages 335–348, 2008.
- [4] B. Adida. Helios Documentation. <http://documentation.heliosvoting.org>, 2014. [Online; Accessed 8-May-2014].
- [5] B. Adida and R. L. Rivest. Scratch & Vote: Self-Contained Paper-Based Cryptographic Voting. In *WPES*, pages 29–40, 2006.
- [6] L. Baird. Big Integers in JavaScript. <http://leemon.com/crypto/BigInt.html>, 2009. [Online; Accessed 6-May-2014].
- [7] bitwiseshiftleft. sjcl. <https://github.com/bitwiseshiftleft/sjcl>, 2014. [Online; Accessed 19-May-2014].
- [8] D. Chaum. Secret-Ballot Receipts: True Voter-Verifiable Elections. *Security Privacy, IEEE*, 2(1):38–47, 2004.
- [9] J. Cichoń, M. Kutylowski, and B. Węglorz. Short Ballot Assumption and Three-ballot Voting Protocol. In *SOFSEM 2008: Theory and Practice of Computer Science*, volume 4910, pages 585–598. 2008.
- [10] R. Coeckelbergh. Toepassing en uitbreiding van het Helios online verkiezings-systeem, 2013.
- [11] C.A. Cois. JavaScript Performance Rundown, 2012. <http://codehenge.net/blog/2012/08/javascript-performance-rundown-2012/>, 2012. [Online; Accessed 5-May-2014].
- [12] cryodex. aes-js. <https://github.com/cryodex/aes-js>, 2014. [Online; Accessed 19-May-2014].

- [13] A. Di Federico and R. Sleevi. Algorithms and referenced documents. <http://lists.w3.org/Archives/Public/public-webcrypto-comments/2013Jun/0004.html>, 2013. [Mailing List Archive; Online; Accessed 6-May-2014].
- [14] W. Diffie and M.E. Hellman. New Directions in Cryptography. *IEEE Transactions on Information Theory*, 22(6):644–654, 1976.
- [15] The Economist. The 2014 ballot boxes. <http://www.economist.com/node/21592755>, 2014. [Online; Accessed 17-May-2014].
- [16] T. Elgamal. A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms. *IEEE Transactions on Information Theory*, 31(4):469–472, 1985.
- [17] D. Gollmann. *Computer Security (Third Edition)*. Wiley, 2011.
- [18] I. Hickson. Web Storage. W3C Recommendation 30 July 2013, W3C, 2013.
- [19] HTML5test. Web Cryptography API. <http://html5test.com/compare/feature/security-crypto.html>, 2014. [Online; Accessed 6-May-2014].
- [20] J. Jonsson and B. Kaliski. Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1. <http://www.ietf.org/rfc/rfc3447.txt>, 2003.
- [21] B. Kaliski. PKCS #5: Password-Based Cryptography Specification Version 2.0. <http://www.ietf.org/rfc/rfc2898.txt>, 2000.
- [22] B. Kaliski. Public-Key Cryptography Standards (PKCS) #8: Private-Key Information Syntax Specification Version 1.2. <http://www.ietf.org/rfc/rfc5208.txt>, 2008.
- [23] LOKO. Kiesreglement verkiezingen, 2014.
- [24] B. Maddens. Zijn de stemcomputers wel te vertrouwen? <http://www.knack.be/nieuws/belgie/zijn-de-stemcomputers-wel-te-vertrouwen/article-opinion-143099.html>, 2014. [Online; Accessed 17-May-2014].
- [25] A.J. Menezes, S.A. Vanstone, and P.C. Van Oorschot. *Handbook of Applied Cryptography*. 1996.
- [26] Microsoft. Web Cryptography. [http://msdn.microsoft.com/en-us/library/ie/dn302338\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/ie/dn302338(v=vs.85).aspx), 2014. [Online; Accessed 6-May-2014].
- [27] Netflix. Netflix WebCrypto (NfWebCrypto). <https://github.com/Netflix/NfWebCrypto>, 2014. [Online; Accessed 6-May-2014].
- [28] M. Pilgrim. Local Storage - Dive Into HTML5. <http://diveintohtml5.info/storage.html>, 2011. [Online; Accessed 19-May-2014].

-
- [29] Polycrypt. PolyCrypt: A WebCrypto Polyfill. <http://polycrypt.net>, 2014. [Online; Accessed 6-May-2014].
 - [30] B. Preneel. Cryptography and Network Security. 2013.
 - [31] B. Randell and P. Y.A. Ryan. Voting Technologies and Trust. *Security Privacy, IEEE*, 4(5):50–56, 2006.
 - [32] A. Ranganathan and J. Sicking. File API. W3C Last Call Working Draft 25 March 2014, W3C, 2014.
 - [33] De Redactie. Ga eens oefenen op een stemcomputer. <http://www.deredactie.be/cm/vrtnieuws/VK14/1.1937511>, 2014. [Online; Accessed 17-May-2014].
 - [34] J. Resig. JavaScript Performance Rundown. <http://ejohn.org/blog/javascript-performance-rundown/>, 2008. [Online; Accessed 5-May-2014].
 - [35] R. L. Rivest. The ThreeBallot Voting System. 2006.
 - [36] R. L. Rivest, A. Shamir, and L. Adleman. A Method for Obtaining Digital Signatures and Public-key Cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978.
 - [37] R. L. Rivest and W. D. Smith. Three Voting Protocols: ThreeBallot, VAV, and Twin. In *Proceedings of the USENIX Workshop on Accurate Electronic Voting Technology*, pages 16–16, 2007.
 - [38] RoboHash. RoboHash. <http://robohash.org>, 2014. [Online; Accessed 19-May-2014].
 - [39] A. Shamir. How to Share a Secret. *Communications of the ACM*, 22(11):612–613, 1979.
 - [40] R. Sleevi and M. Watson. Web Cryptography API. W3C Last Call Working Draft 12 September 2013, W3C, 2014.
 - [41] F. Smedberg. Performance Analysis of JavaScript, 2010.
 - [42] De Tijd. ‘Moeder aller verkiezingen’ kost meer dan 10 miljoen. <http://www.tijd.be/r/t/1/id/9388719>, 2013. [Online; Accessed 17-May-2014].
 - [43] The New York Times. The 2012 Money Race: Compare the Candidates. <http://elections.nytimes.com/2012/campaign-finance>, 2012. [Online; Accessed 17-May-2014].
 - [44] TrueCrypt. TrueCrypt - Free Open-Source On-The-Fly Encryption. <http://www.truecrypt.org>, 2014. [Online; Accessed 19-May-2014].
 - [45] VTK. Verkiezingsreglement VTK vzw en VTK Ondersteuning vzw, 2014.

- [46] W3C. United States presidential election in Florida, 2000. http://en.wikipedia.org/w/index.php?title=United_States_presidential_election_in_Florida,_2000&oldid=604767954, 2014. [Online; Accessed 17-May-2014].
- [47] W3C. Web Cryptography Working Group Wiki. http://www.w3.org/2012/webcrypto/wiki/index.php?title=Main_Page&oldid=483, 2014. [Online; Accessed 5-May-2014].
- [48] Wikipedia. DRE voting machine — Wikipedia. http://en.wikipedia.org/w/index.php?title=DRE_voting_machine&oldid=555933682, 2013. [Online; Accessed 11-Apr-2014].
- [49] Wikipedia. Homomorphic encryption — Wikipedia. http://en.wikipedia.org/w/index.php?title=Homomorphic_encryption&oldid=608522158, 2014. [Online; Accessed 15-May-2014].
- [50] Wikipedia. Identicon — Wikipedia. <http://en.wikipedia.org/w/index.php?title=Identicon&oldid=590908926>, 2014. [Online; Accessed 19-May-2014].
- [51] Wikipedia. Ostracon — Wikipedia. <http://en.wikipedia.org/w/index.php?title=Ostracon&oldid=603659772>, 2014. [Online; Accessed 11-Apr-2014].
- [52] Wikipedia. Pretty Good Privacy — Wikipedia. http://en.wikipedia.org/w/index.php?title=Pretty_Good_Privacy&oldid=606033746, 2014. [Online; Accessed 19-May-2014].
- [53] Wikipedia. Voter-verified paper audit trail — Wikipedia. http://en.wikipedia.org/w/index.php?title=Voter-verified_paper_audit_trail&oldid=599852086, 2014. [Online; Accessed 17-Apr-2014].
- [54] T. Wu. RSA and ECC in JavaScript. <http://www-cs-students.stanford.edu/~tjw/jsbn/>, 2009. [Online; Accessed 6-May-2014].
- [55] N.C. Zakas. SecureStore 1.0 Proposal. <http://www.nczonline.net/blog/securestore-proposal/>, 2011. [Online; Accessed 20-May-2014].

Fiche masterproef

Student: Pieter Maene

Titel: Online verkiezingen in de praktijk: verbetering en toepassing van het Helios verkiezingssysteem

Engelse titel: Online Elections in Practice: Improvement and Application of the Helios Voting System

UDC: 621.3

Korte inhoud:

Een voter-verifiable stelsysteem geeft de kiezer de mogelijkheid om na te gaan of zijn eigen stem correct geregistreerd is en dat het resultaat correct is. Het is mogelijk om een dergelijk systeem met papieren stembiljetten te implementeren, zowel met als zonder cryptografische technieken. Helios is een voter-verifiable stelsysteem voor online verkiezingen. De procedure die bij deze systemen gevolgd moet worden, is echter vaak zeer complex. In deze thesis wordt de procedure gegeven die in Helios gevolgd moet worden om een verkiezing op te zetten. De interface van het systeem werd ook herwerkt om de beheerder beter te ondersteunen. Ook de applicatie die gebruikt wordt door de kiezers werd vereenvoudigd. Na het systeem uitgebreid getest te hebben, werd het in de praktijk gebruikt voor een reële verkiezing waarbij ongeveer 750 mensen hun stem uitbrachten. Daarnaast wordt besproken hoe de trustees hun geheime sleutels kunnen bewaren. Er wordt ook onderzocht of de fingerprints waarvoor momenteel strings gebruikt worden niet op een betere manier weergegeven kunnen worden. Tot slot worden de prestaties van de Web Cryptography API vergeleken met deze van bestaande implementaties in JavaScript. Deze nieuwe specificatie geeft ontwikkelaars toegang tot cryptografische functies die in de browser ingebouwd zijn.

Thesis voorgedragen tot het behalen van de graad van Master of Science in de ingenieurswetenschappen: elektrotechniek, optie Ingebedde systemen en multimedia

Promotor: Prof. dr. ir. B. Preneel

Assessoren: Prof. dr. ir. V. Rijmen
Prof. dr. ir. L. Van Eycken

Begeleiders: Dr. ir. J. Hermans
Dr. ir. F. Vercauteren