

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

Pieter Maene

Abstract—Helios is a voter-verifiable online voting system. Such a system allow the voter to verify whether his ballot was registered correctly and check the election result. The procedure for these systems is typically very complicated. The system's usability is determined by its interface which should support the procedure.

This paper discusses the procedure to manage an election in Helios. The system's interface was modified to better support this procedure. The modified system is deployed for a real election where the election administrator and voters used it successfully. Additionally, the Web Cryptography API adds native cryptographic functionality to user agents. A benchmark showed that its implementation is faster, which could improve the usability of web applications.

I. INTRODUCTION

Elections are an important part of our democratic society. In 2014, national elections will be held in 40 countries and 42% of the world population will be able to cast its vote.[1] It is therefore necessary to have a trustworthy voting system. In current systems, voters usually have to trust the election organiser. Voter-verifiable systems allow them to verify whether their ballot was registered correctly and check the election result. Helios is such a voter-verifiable system, that can be used for online elections. It is an open-source project developed by Ben Adida.[2] Robbert Coeckelbergh added threshold encryption to it, so that one trustee can no longer stall the election.[3] Online elections can only be used in situations where coercion is not a big threat, though.

The Web Cryptography API is a new W3C specification that will add native cryptographic functionality to user agents.[4] It could improve the usability of web applications that need user-level cryptography. The performance of this new API is compared to that of existing JavaScript cryptography libraries.

This paper will discuss the procedure that should be followed to organise an election in Helios (Section II). The interface of the system was also modified to better support this procedure and improve its usability (Section III). In Section V the performance of the new Web Cryptography API is analysed. Finally, the system was deployed in a production environment and used for a real election (Section IV).

II. ELECTION PROCEDURE IN HELIOS

This sections gives the procedure that should be followed to organise an election in the improved version of Helios (Section III). After preparing some information (Section II-A), the election administrator can start the procedure (Section II-B).

A. Preparation

The trustees will be responsible for the decryption of the result. It is therefore important to give some thought to who this role will be given. Since using threshold encryption results in a more robust decryption process, it is advisable to use this. In that case, the election administrator should also determine the threshold scheme. This determines the number of trustees that will have to present their keys in order to decrypt the result.

For each question, the election administrator can specify the number of answers that can be selected by the voter. The result for each answer is shown either as the absolute number of votes it received, or its relative position with respect to the other answers.

The election administrator can create both open and closed elections. Anybody can vote in the former, while only specific voters are allowed to cast their ballot in the latter. A closed election should therefore be used when voter lists are available.

B. Helios Setup

The first step is the creation of the election. Here, all basic information like its name should be given. It is also possible to enable options here, like threshold encryption or whether the election is private or not. The start and end date of the election can be controlled here as well.

After creating the election, the trustees have to be added. This step was placed first in the procedure because it is the longest to complete. After being added, the trustee receives an e-mail with the link to his trustee dashboard.

If threshold encryption is not being used, each trustee simply has to generate a key pair. Once all trustees have done this, the election administrator can freeze the election. If threshold encryption was enabled, the key ceremony becomes more complicated. After adding all trustees, the election administrator can define the threshold scheme. The trustees can then start the following ceremony.

- 1) The trustee generates his communication keys and uploads the public keys to the server. They will be used to encrypt and sign the communication between them.
- 2) Once this is done by all trustees, each of them generates his encrypted shares and sends them to the others.
- 3) After receiving a share from all other trustees, the trustee decrypts and adds them to obtain his share of the key that will be used to encrypt the ballots. It will serve as his private key for the election and he uploads the corresponding public key.

When all trustees have done this, the election can be frozen. Since the trustees will have to wait for the others, e-mails are

sent to all of them when action is required.

Once the election is frozen, voters will be able to cast their ballot, unless a specific starting time was entered. If no end time was given, the election will be closed at the administrator's discretion.

After the election has been closed, the homomorphic tally can be decrypted. If threshold encryption is not enabled, all trustees will have to calculate their decryption factor and submit it. Otherwise, only the number of trustees defined in the threshold scheme will have to do this.

III. USER INTERFACE IMPROVEMENTS

Most of our work on the interface to improve the usability concentrated on two big parts of Helios. First, the admin was modified to better reflect the procedure discussed in Section II. This was done by creating a separate admin page where the procedure is clearly shown to the election administrator. Second, the trustee dashboard was also simplified. Here, the HTML5 File API was used to make it easier for the trustee to manage his keys. Additionally, the layout was streamlined throughout the application.

A. Admin

The original interface integrated the administrative functions in the election view. This made it hard for the election admin to keep track of his progress in the procedure. It was therefore decided to move this functionality to a separate page. It shows the entire procedure and clearly indicates which steps have been completed. Since the actions lead away from this page, a bar was put on top of all pages where the progress is indicated as well.

The workflow for an election with threshold encryption is thoroughly changed. Originally, a public bulletin board was available where anybody could upload a pair of communication keys. The admin could only add trustees to an election from a list of people who had done this. This meant that he had to wait for all trustees to do this before he could define the threshold scheme and continue setting up the election. This required a secondary path of communication, outside of Helios. Because the bulletin board was publicly accessible, an attacker could impersonate a trustee. Unless he has access to the trustee's e-mail account, he would not receive the URL to the trustee dashboard. In that case, he would only have been able to stall the key ceremony.

The bulletin board was removed completely and trustees are immediately added to the election. They then receive an e-mail with a unique link to their trustee dashboard where they generate their communication keys.

B. Trustee Dashboard

The trustees will perform all actions of the key ceremony in the trustee dashboard. The trustee's role is explained and an overview of all steps in the ceremony is shown in the same way as the election procedure on the admin page.

The trustee will generate three key pairs during the ceremony. The private keys are stored locally in JSON files.

Originally, the JSON was simply shown to the user and he had to manually save it to a file. When the key was needed, the file's contents needed to be copied again to a text area.

The HTML5 File API offers two API interfaces that can be used to ease this process.[5] The first is the `Blob` interface that can be used to generate files in JavaScript. They can then be offered as a download in the browser. The second is the `FileReader` interface which allows a web developer to read files that conform to the `Blob` or `File` interfaces.

They are used in the trustee dashboard to offer the secret keys as a download. The details of the key are now hidden from the trustee. When his key is needed, he has to select this file in an input element. The file's contents are then read to the text area. These adjustments make it a lot easier for the trustee to manage his keys.

In addition to using this API, the two secret keys of the communication pair are now stored in a single file. Since the distinction between two was only confusing to the trustee, this simplifies the key management for him.

C. Voting Booth

The tests that were performed before using Helios for the real election will be discussed in Section IV-C. The voting booth is simplified based on feedback that was received during the test of the voting booth. The changes that were made will be detailed in that section.

IV. BOARD ELECTION

The modified Helios voting system was used in the elections for the new board of VTK, the official student organisation for engineering students at the KU Leuven. Support for some specific features was added. The system was then thoroughly tested before the election on May 8th 2014.

A. Election Requirements

A committee of at least five people from the current board watches over the election. The head of this committee is the current president of the board. He should be able to manage the election. It should be possible to appoint the other members as trustees. The decryption process cannot be blocked by one trustee.

There are two types of candidates: the first can be officially elected as the next board, the second participates for fun. Both should be separate questions on the ballot. If there is only one official team, voters have to be able to vote pro, contra or abstention. If there are two teams, at most one should be selectable. If there are more than two, voters should express their appreciation for each team. However, this last case is so rare that it's not a strong requirement for the system. In the election of the fun team, it should be possible to select all of them at most.

A list of all eligible voters can be requested from the university. These lists have the student's first name, last name and university identification number. Only these voters should be able to access the election. Therefore, an authentication system should be available. Finally, the participation percentage should be shown on the result page.

B. Specific Adjustments

Shibboleth is the single sign-on system used by the KU Leuven. Students have an account with a unique identification number. All voters in the election have such an account, so it could be used to authenticate them. Since Helios' authentication system is modular and already has support for other federated identity systems, adding Shibboleth was relatively straightforward.

The list of voters was provided by an external organisation. This included the student's identification number and name, but the e-mail address was missing. This is needed by Helios to send a confirmation message after casting a ballot. A voter's e-mail address is retrieved from the Shibboleth response and added to the account to fix this.

Helios did not yet show the election's participation percentage. This is the percentage of eligible voters that cast their vote. The system also immediately published the election result. They are traditionally announced to the public at midnight, but the election administrator does need earlier access to them. These two smaller features were therefore implemented as well.

C. Tests

After installing the system on a server, it was thoroughly tested by the current board of VTK. In addition to verifying all technical aspects, the testers were also asked for feedback on the user interfaces. The election admin and booth were tested in the context of the actual election. The real voter list was replaced by the current board of the organisation, though.

While testing the threshold encryption process, a bug was found. Real fractions were used for the calculation of the Lagrange interpolation, instead of finite modular arithmetic. After solving this, the result still couldn't be decrypted correctly. By default, Helios was added as a trustee to the election. It completed all steps in the ceremony automatically. During testing, the shares of this trustee turned out to be incompatible with these generated by the other trustees. The only difference between the two is that the former are generated in the Python application and the latter in the JavaScript trustee dashboard. Because the source of the error origin could not be found, Helios no longer could be an election trustee. Since its role in the whole process was already limited, this was not a major change. The main advantage of adding it, was that it allowed users to create an election without real trustees, which resulted in a simpler procedure.

Apart from these bugs, the test of the election admin went very well. The election administrator managed to go through the entire procedure independently. The trustees didn't have much difficulty generating their keys either.

Although its functionality worked perfectly, a lot of feedback was given on the voting booth. First, a lot of technical terms were used. This was easily solved by replacing them with more common words. Second, most testers found the voting process to be too complicated. The booth is an independent application written in JavaScript, so that only the encrypted vote is sent to the server.

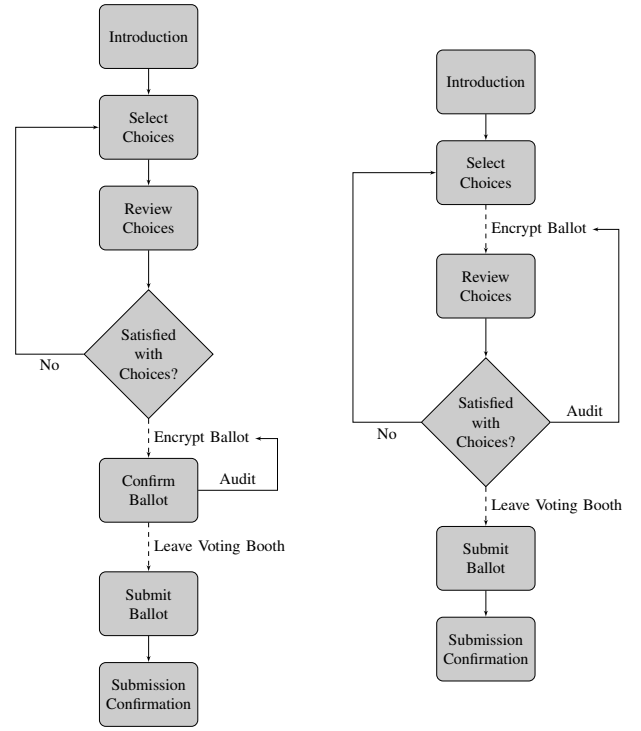


Fig. 1: Old (Left) and New (Right) Voting Booth Flows

There were two places where the user had to submit his vote originally (Fig. 1). After confirming his encrypted vote in the booth, it was sent to the server where it could finally be cast. The last screen of the voting booth was therefore removed. Since it still had to be possible to audit the encrypted vote, this also required the encryption to be moved. This is now done after the voter has made all his choices. As a result, the vote has to be encrypted again when these are changed. The current implementation is already reasonably fast and this will only improve once the Web Cryptography API is available (Section V). Finally, an alert is shown when voters try to leave the page where they have to upload their ballot to the server before doing so. The test was repeated after making these adjustments to verify their impact on both functionality and usability.

Finally, a stress test was run as well. This was done for a separate election with two trustees and three questions. 1,000 votes were inserted into the database. To do this, the encrypted votes were generated directly in Python instead of using the JavaScript voting booth. The result was decrypted successfully, indicating that the system can manage an election of that size.

D. Election Day

The election itself took place on May 8th 2014 from 7 am till 8 pm. During this time, 768 people cast a ballot which isn't significantly less than during previous years. This is a strong indication that the voting process was clear. No complaints were received from these voters either.

Since everything had been tested in advance, no problems were encountered during the voting or when decrypting the result.

V. FUTURE WORK: WEB CRYPTOGRAPHY API

Currently, web developers implement cryptographic functionality in JavaScript. Despite great improvements in recent years, it is still slower than native code.[6][7][8] In 2012 a working group was started by W3C to write the Web Cryptography API specification, which would add cryptographic functionality to user agents.[9] The specification defines the `SubtleCrypto` interface which has several high-level functions.[4] There are methods to manage the keys and to encrypt data. The API only supports a specific set of algorithms, nor does each algorithm support all functions of the interface.

Since the specification has not been completed yet, most user agents do not support it. Internet Explorer 11 is the only browser that already has an implementation, but it misses some algorithms.[10] Therefore, the `NfWebCrypto` polyfill was used for the benchmarks. This is a C++ plugin for Chrome, so its performance should be comparable to a real implementation. Since a polyfill had to be used, the API's functionality was not yet added to Helios.

A. Modular Exponentiation

Helios uses ElGamal to encrypt the ballots, which is an algorithm not supported by the API. The modular exponentiations are responsible for the majority of the calculation time. An improvement there would impact overall performance.

Since the API only offers high-level functions, this had to be implemented separately. Diffie-Hellman is one of the supported algorithms. The `deriveKey` method uses Eq. 1 to calculate the shared secret.[11]

$$K = (g^a)^b \mod p \quad (1)$$

In this equation, g^a is the public key of A and b the private key of B. If the public and private key can be specified, it can be used to calculate the modular exponentiation $x^y \mod p$. It is possible to import a specific private key into the user agent's key store. For the Diffie-Hellman algorithm, the specification only allows private keys in the PKCS8 format to be imported. To make testing easier, the `NfWebCrypto` plugin was modified to allow the import of raw keys. After calculating the shared secret, the result can be obtained with the `exportKey` function.

The performance of the `NfWebCrypto` library is compared to that of `JSBN` and `Leemon`, two JavaScript big number libraries.[12][13] A 1,024-bit exponent is used, which is the size of the keys used by Helios. The calculation is repeated 1,000 times for each library. The results are shown in Fig. 2 and Table I. The first exponentiation of the `NfWebCrypto` plugin took a lot longer, which explains the large variance. The `NfWebCrypto` plugin result was not correct. The communication with the plugin has to be `base64` encoded, which resulted in conversion issues between C++ and JavaScript.

B. RSA

RSA was used to make a second comparison between `JSBN` and `NfWebCrypto`. This cipher isn't used by Helios, but the

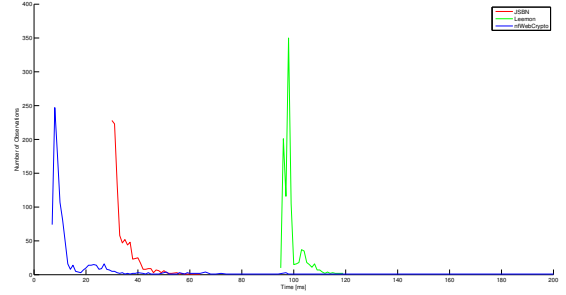


Fig. 2: Modular Exponentiation

TABLE I: Modular Exponentiation

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

results are very interesting. A standard value of 65,537 was used for the public exponent of the encryption. Notice that this is a lot shorter than the exponents used in Section V-A. The modulus is 1,024 bits large.

JSBN has specific functions for RSA encryption and decryption. The Web Cryptography API supports the `RSAPKCS1-v1_5` algorithm.[14] Although public keys in the SPKI format can be imported, this proved difficult. Therefore, a new key was generated for each encryption. The time required for this is not taken into account. The results are shown in Fig. 3 and Table II. Surprisingly, the JavaScript implementation is faster than the `NfWebCrypto` plugin. This is caused by communication overhead.

VI. CONCLUSION

Voter-verifiable systems can be used to improve voter confidence. Helios is such a system that can be used to organise online elections. Section II gave the procedure as well as some recommendations that should be followed to setup an election.

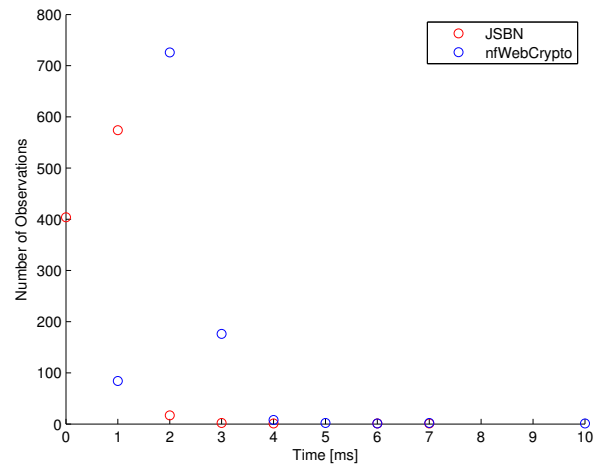


Fig. 3: RSA

TABLE II: RSA

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

The Web Cryptography API will make high-level cryptographic functions available to web developers. It also offers a considerable performance increase, compared to existing JavaScript libraries. Its biggest disadvantage is the small set of supported algorithms, which limits the possible applications. It also proved hard to import existing keys into the user agent's store.

By modifying Helios' interface to better support the procedure, its usability was greatly improved. Where the system was hard to use before, the election administrator didn't need any support in setting up the election. The trustees were also able to manage their keys without any problems. Using the simplified voting booth, a typical number of voters cast their vote in a real election.



Pieter Maene was born in Duffel in the year 1991. Because of an interest in science and technology, he started engineering studies at the KU Leuven in 2009. He enrolled in the electrical engineering master in 2011 where he took courses on signal processing, embedded systems and cryptography.

REFERENCES

- [1] The Economist, "The 2014 ballot boxes," <http://www.economist.com/node/21592755>, 2014, [Online; Accessed 17-May-2014].
- [2] B. Adida, "Helios Documentation," <http://documentation.heliosvoting.org>, 2014, [Online; Accessed 8-May-2014].
- [3] R. Coeckelbergh, "Application and extension of the Helios online voting system," 2013, Master's Thesis.
- [4] R. Sleevi and M. Watson, "Web Cryptography API," W3C, W3C Last Call Working Draft 12 September 2013, 2014. [Online]. Available: <http://www.w3.org/TR/2013/WD-FileAPI-20130912/>
- [5] A. Ranganathan and J. Sicking, "File API," <http://www.w3.org/TR/2014/WD-WebCryptoAPI-20140325/>, W3C, W3C Last Call Working Draft 25 March 2014, 2014.
- [6] J. Resig, "JavaScript Performance Rundown," <http://ejohn.org/blog/javascript-performance-rundown/>, 2008, [Online; Accessed 5-May-2014].
- [7] C. Cois, "JavaScript Performance Rundown, 2012," <http://codehenge.net/blog/2012/08/javascript-performance-rundown-2012/>, 2012, [Online; Accessed 5-May-2014].
- [8] F. Smedberg, "Performance Analysis of JavaScript," 2010, Master's Thesis.
- [9] 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].
- [10] 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].
- [11] W. Diffie and M. Hellman, "New Directions in Cryptography," *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644–654, 1976.
- [12] T. Wu, "RSA and ECC in JavaScript," <http://www-cs-students.stanford.edu/~tjw/jsbn/>, 2009, [Online; Accessed 6-May-2014].
- [13] L. Baird, "Big Integers in JavaScript," <http://leemon.com/crypto/BigInt.html>, 2009, [Online; Accessed 6-May-2014].
- [14] J. Jonsson and B. Kaliski, "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1," <http://www.ietf.org/rfc/rfc3447.txt>, Internet Engineering Task Force, 2003.