

helios

State of Helios 2010: features and deployments

Ben Adida, Olivier Pereira

EVT/WOTE 2010 – August 9, 2010



Helios...

online elections
low-coercion



Helios...

online elections
low-coercion
more than **25000** votes cast



Helios...

1. New developments
2. New deployments
3. New release



Monitoring Helios elections

Helios offers a bulletin board, but . . .

- ▶ What if the Helios server is getting hacked?
Audit will see it, but are we stuck?



Monitoring Helios elections

Helios offers a bulletin board, but . . .

- ▶ What if the Helios server is getting hacked?
Audit will see it, but are we stuck?
- ▶ Audit is technical. . .
Can I share my audit results?



Monitoring Helios elections

Helios offers a bulletin board, but . . .

- ▶ What if the Helios server is getting hacked?
Audit will see it, but are we stuck?
- ▶ Audit is technical. . .
Can I share my audit results?

Observation:

The Helios server only stores public data!



Monitoring Helios elections

Helios Election Monitor (by Olivier de Marneffe)

<https://www.uclouvain.be/crypto/electionmonitor/>



Helios Election Monitor

This website monitors Helios elections: it uses the Helios API, which is also used to collect ballots at tallying time, and examines the votes that have been submitted:

- the election parameters (identifier, questions and proposed answers, ...) are extracted and recomputed,
- a new version of the bulletin board is built, with all hashes recomputed from original data,
- the bulletin board also displays the validity of the ballots (all proofs of well-formedness are valid),
- a timeline showing the evolution of vote submissions is built (all date and time displayed on this website are UTC).

You can also audit a ballot with our [ballot auditor](#).

Elections previously monitored

Election name	UUID
IACR Helios demo election	3a40d55c-1396-11df-bd14-19dba45a8649

[click on election name to view monitoring data]

Quick links: [UCL](#) | [EPL](#) | [ELEC](#) | [DICE](#) | [CRYPTO GROUP](#)

Webmaster: [Olivier de Marneffe](#)



IACR Helios demo election

[[view our bulletin board](#) | [view voting statistics](#)]

monitoring of this election is finished

Votes information

- **1542** registered voters
- **379** voters cast a vote
- **396** votes were cast (including re-votes)

Election information

- **Election Description:** The goal of this demo election is to solicit feedback from IACR members about moving to electronic elections, and also to help us evaluate the suitability of Helios for IACR elections. In addition to this goal, we would like to take this opportunity to conduct a straw poll about several issues currently under discussion by the board. The results of this demo election are **NOT** binding. The election will close on March-15 2010 at 11:59pm UTC. See More information at <http://www.iacr.org/elections/eVoting/ballot-questions.html>
- **Election UUID:** 3a40d55c-1396-11df-bd14-19dba45a8649
- **Election public key** *verified*
- **Election frozen at:** 2010-02-09 00:06:02
- **Election Fingerprint:** z1oRqXUyfvmsMH5s5VEd0gaa/wiwX5GG3t+RhzkfwGc
- **Election url:** <https://iacr-helios.appspot.com/helios/elections/3a40d55c-1396-11df-bd14-19dba45a8649/view>
- **Questions:** *election outcome audited - 2010-03-17 09:32:35 UTC*



IACR Helios demo election - Bulletin Board

[[view election information](#) | [view voting statistics](#)]

monitoring of this election is finished

1542 registered voters

Search

Look For:

In Field:

Voter ID ▾

Submit

only the first 2000 voters are displayed - hashes are recomputed - time is UTC

Voter ID	Status	Vote Fingerprint	Validity	Last Vote Cast at
V24	REVOTED	Uza64HFuZrluygHdwuEv6W3X9rK37XdUV8ycHpmPGmA	✓	Feb 22, 2010 7:00:23 PM
V240	VOTED	TFz9hZH2sY060+ks9tYn0sWZ/BEHKVxG66tio38L4x8	✓	Mar 12, 2010 2:54:10 PM
V241	NO VOTE			

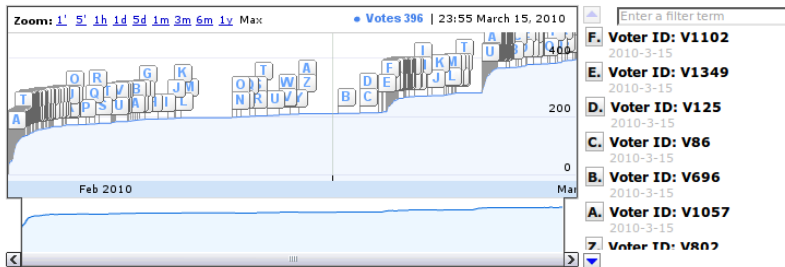


IACR Helios demo election - Voting Statistics

[[view election information](#) | [view our bulletin board](#)]

monitoring of this election is finished

379 voters cast 396 votes in this election



Audit of the tally

Should the IACR keep its current voting system, based on double envelopes sent via postal mail, or switch to electronic voting over the Internet?

[select 0 or 1 answer]

32 - *Keep current system*
344 - *Switch to electronic voting*

Is the Helios voting system, used for these demo elections, appropriate for the purpose of holding future IACR elections?

[select 0 or 1 answer]

293 - *Yes*
39 - *No*

Distributing hard copies of the Journal of Cryptology is rather costly. How do you prefer to access the journal?

[select 0 or 1 answer]

153 - *Both hard copy and web access, as is done today*
224 - *Electronic form only*

In what format would you like to obtain your copy of the proceedings when you attend an IACR conference or workshop?

[select 0 or 1 answer]

128 - *A printed book, as done today*
120 - *Only on a USB stick (cheaper than a book)*
56 - *Both a printed book and a USB stick (more expensive than just a book)*
74 - *I don't need a copy at the conference. Web access to the proceedings is sufficient*



After the UCL president election...

AGL (the UCL student association), Sep. 2009:

“Could we also have verifiable elections on the Internet?”



After the UCL president election...

AGL (the UCL student association), Sep. 2009:

“Could we also have verifiable elections on the Internet?”

- “Well, how do your elections work?”



UCL student elections

“Our ballots are a bit more complicated, here is a typical list:



Élections étudiantes 2010



Etape 1 sur 3 : Sélection des candidats

Conseil de Faculté ESPO

- BEASSE Clément *SPOL 12* [ADES]
- BORJA Andrés *SPED 21* [ADES]
- CALLENS Fanny *IAG 1 PM* [CESEC]
- COLLINGE Marie-Lucie *COMU 13* [Tous ensemble]
- DE DECKER Maité *COMU 11* [CESEC]
- DEKEYZER Sébastien *SPRI 21* [CESEC]
- DELHAYE Laurence *ECGE 12* [CESEC]
- DEMBOUR Noémie *SPRI 21* [ADES]
- DESPLANQUE Simon *SPOL 11* [Tous ensemble]
- DESSY Gaspard *INGE 13* [CESEC]
- DEWAEL Guillaume (Cubitus) *ECGE 11* [CESEC]
- DINIÉF Julien *ECMU 11* [ADES]

Vous pouvez voter pour autant de personnes que vous le désirez.
Les candidats sont présentés par ordre alphabétique.



UCL student elections

“and:

- DONNET Constantin ANTR 21 [CESEC]
- DUGAUTHIER Morgane COMU 13 [CESEC]
- EVRARD Johanne ECGE 13 [CESEC]
- FIXELLES Caroline (Josette) COMU 13 [CESEC]
- GAUTIER Stéphanie SPOL 13 [CESEC]
- GONZALES-MOHINO François (Number One) SPRI 21 [CESEC]
- HATERTE Alexandre (Penne) INGE 11 [CESEC]
- HENRY DE FRAHAN Philip INGE 11 [Tous ensemble]
- HOREMANS Mélissa COMU 12 [CESEC]
- IMPELLIZZERI Nicolas ECGE 13 [CESEC]
- JANUS Marie-Anaëlle ECGE 11 [CESEC]
- LÊ Olivier INGE 12 [ADES]
- LEMAIRE Joseph COMU 12 [ADES]
- LUTZ Fanny SPRI 21 [Tous ensemble]
- MAGNERY Marc (Marco) POLS 21 [ADES]
- MALAY Olivier SPOL 12 [Tous ensemble]
- MANSOR SAFAIAN Parham (Le Perse-Cesec) COMU 12 [CESEC]
- MARSILY Hugues ECGE 13 [CESEC]
- MENDEZ YEPEZ David Manuel ECON 21 [ADES]
- MERTENS François INGE 12 [CESEC]
- MOREAU Thomas SPRI 21 [CESEC]
- MOREAU Simon ECGE 11 [Tous ensemble]
- MOUTON Arnaud (Rouge) ECGE 11 [CESEC]
- NSANZIMANA Jérôme SPRI 21 [CESEC]



UCL student elections

“and:

- PELTIER Benjamin SPOL 21 [ADES]
- PERDAENS Alizée SPOL 13 [CESEC]
- PIERRE LOUIS Luné Roc COMU 3 D [ADES]
- POTIE Olivier ECGE 13 [CESEC]
- SCHAMPS Claire INGE 13 [ADES]
- STAS Bruno SPED 21 [ADES]
- THOMAS Vanessa ANTR 21 [Tous ensemble]
- ULUC Timur SPOL 11 [CESEC]
- VAN BINSBERGEN Laura SOCA 12 [ADES]
- VAN HIRTUM Erwin ECON 22 [Tous ensemble]
- VAN RUYCHEVELT Jérôme (Van Spring) SPRI 21 [ADES]
- VERHOEVEN Johan (Yan) SOCA 21 [ADES]
- VERMEIRE Jean-Gabriel SPRI 21 [ADES]
- WALLEMACQ Alexandre IAG 1 PM [Tous ensemble]

- Vote Blanc

Suivant

[Pages d'aide](#) | [Informations élections](#) | [Contact : e-elections@aglouvain.be](#) | [Taux de participation](#) | [Valves de l'élection électronique](#)



UCL student elections

“and:

- PELTIER Benjamin [SPOL 21](#) [ADES]
- PERDAENS Alizée [SPOL 13](#) [CESEC]
- PIERRE LOUIS Luné Roc [COMU 3 D](#) [ADES]
- POTIE Olivier [ECGE 13](#) [CESEC]
- SCHAMPS Claire [INGE 13](#) [ADES]
- STAS Bruno [SPED 21](#) [ADES]
- THOMAS Vanessa [ANTR 21](#) [Tous ensemble]
- ULUC Timur [SPOL 11](#) [CESEC]
- VAN BINSBERGEN Laura [SOCA 12](#) [ADES]
- VAN HIRTUM Erwin [ECON 22](#) [Tous ensemble]
- VAN RUYCHEVELT Jérôme (Van Spring) [SPRI 21](#) [ADES]
- VERHOEVEN Johan (Yan) [SOCA 21](#) [ADES]
- VERMEIRE Jean-Gabriel [SPRI 21](#) [ADES]
- WALLEMACQ Alexandre [IAG 1 PM](#) [Tous ensemble]

- Vote Blanc

Suivant

[Pages d'aide](#) | [Informations élections](#) | [Contact : e-elections@aglouvain.be](#) | [Taux de participation](#) | [Valves de l'élection électronique](#)

“and we typically have 3 such lists + a few smaller ones”



Helios ballot encoding

Helios ballot encoding [CGS97]: $6 \text{ modexp/candidate}$



Helios ballot encoding

Helios ballot encoding [CGS97]: 6 modexp/*candidate*

≈ 250 candidates: minutes on an old browser



We need something else...

Move to completely different crypto!

- ▶ Mixnet-based tallying
- ▶ one ciphertext per *ballot*
- ▶ use augmented cryptosystems [Wik08] to ensure ballot independence



We need something else...

Move to completely different crypto!

- ▶ Mixnet-based tallying
- ▶ one ciphertext per *ballot*
- ▶ use augmented cryptosystems [Wik08] to ensure ballot independence

$$\leq 5 \text{ modexp/ballot}$$



Deployment...



Deployment...

- ▶ New participation record!
77% of students want to keep paper and electronic polling,
22% want Internet only



Deployment...

- ▶ New participation record!
77% of students want to keep paper and electronic polling,
22% want Internet only
- ▶ Much more burden than homomorphic tallying:
 - ▶ checking ballot independence,
 - ▶ mixing,
 - ▶ decryption and counting + proof verifications

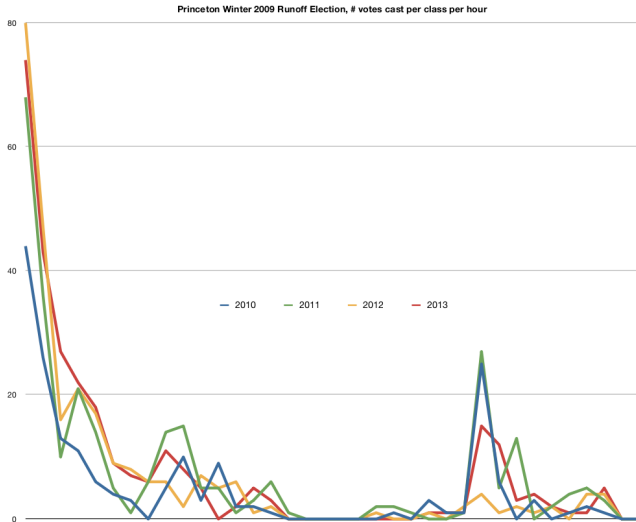


Deployment...

- ▶ New participation record!
77% of students want to keep paper and electronic polling,
22% want Internet only
- ▶ Much more burden than homomorphic tallying:
 - ▶ checking ballot independence,
 - ▶ mixing,
 - ▶ decryption and counting + proof verifications
- ▶ Still much more comfortable than paper tallying...



At Princeton



Further deployments

- ▶ Infocard Foundation
(MS, Google, Oracle, Verizon, ...)
- ▶ Université catholique de Louvain
Rector of the university
- ▶ **Top University hiring and promotion decisions**
- ▶ **Princeton Student Gov Elections**
- ▶ **IACR**



New Release

- ▶ online as of last night
<http://heliosvoting.org>
- ▶ Java no longer necessary
(but still good for increased privacy)
- ▶ streamlined UI, more social
- ▶ scalable to thousands of voters out of the box.



A Non-Profit

- ▶ Directors
 - ▶ Ben Adida
 - ▶ Lawrence Lessig
 - ▶ Jim Adler
- ▶ Tech Advisory Board
 - ▶ Josh Benaloh, Microsoft Research
 - ▶ Olivier Pereira, UCL
 - ▶ Dan Wallach, Rice University
- ▶ Code
 - ▶ Ben Adida, Olivier Pereira, Olivier de Marneffe

