Hacking Helios and Its Impact

Yvo DESMEDT   Saghar ESTEHGHARI
University College London, UK

August 18, 2009

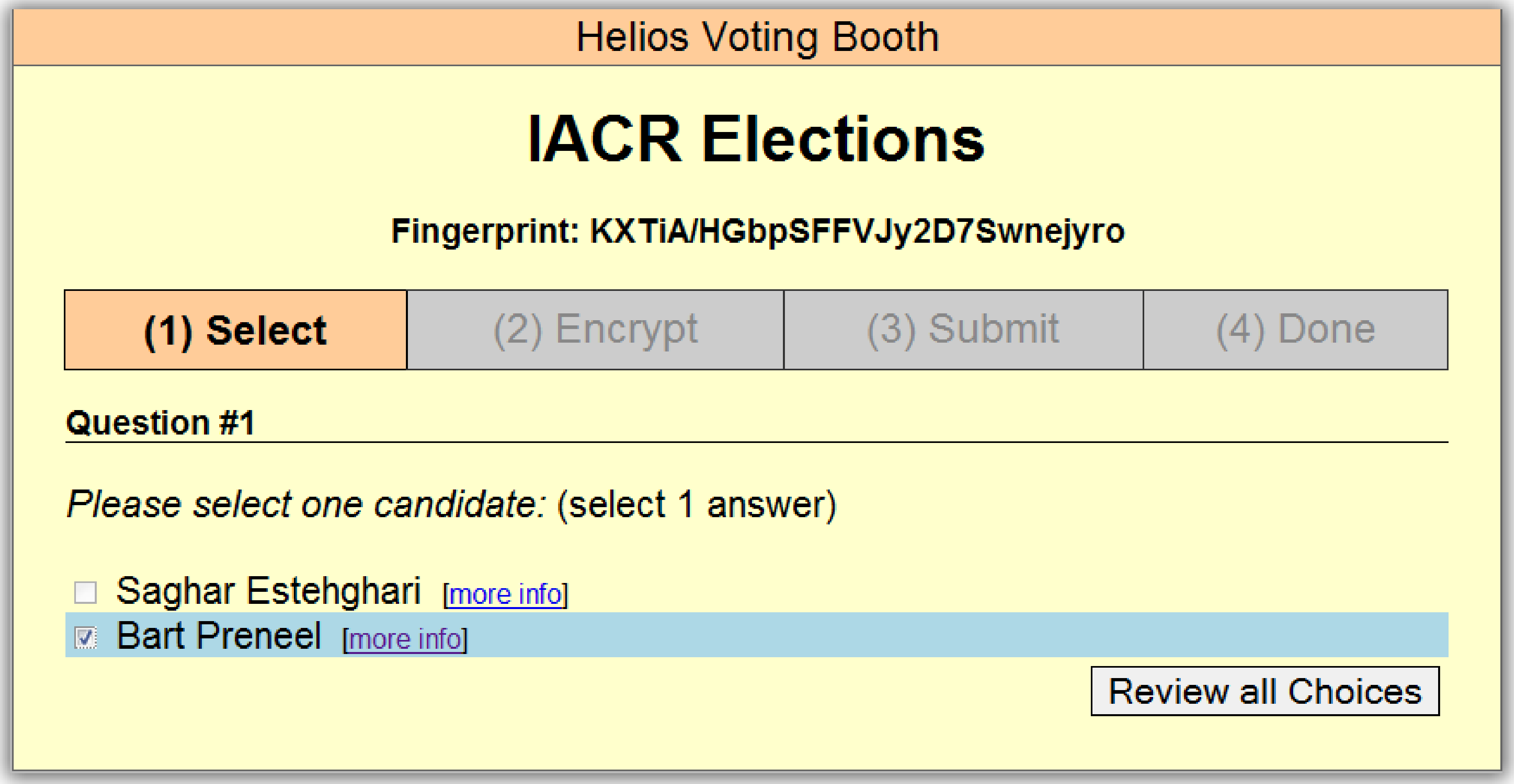
Helios Cryptographic Algorithms

- Homomorphic techniques for e-voting based on Exponential El-Gamal
- Threshold decryption with joint key generation
- Computations are done in a subgroup of $\mathbb{Z}^*_p$ with order q, p = 2048-bits and q = 256-bits

Helios Claims

From Usenix 2008:

- "... even if Helios is fully corrupt, the integrity of the election can be verified. "
- "... even a fully corrupted Helios cannot cheat the election result without a high chance of getting caught."



Helios Voting Booth

IACR Elections

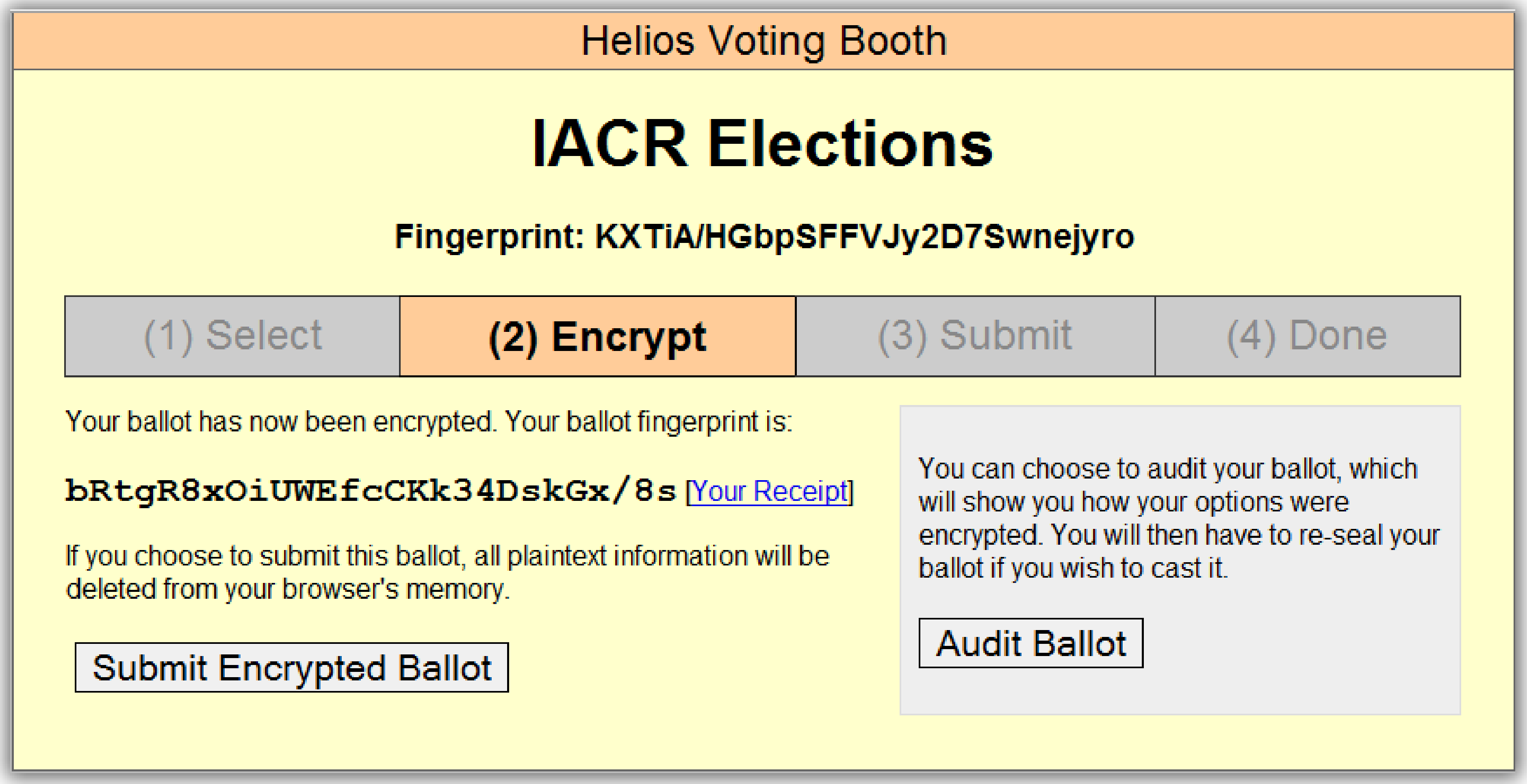
Fingerprint: KXTiA/HGbpSFFVJy2D7Swnejyro

Question #1

Please select one candidate: (select 1 answer)

☐ Saghar Estehghari [more info]

☑ Bart Preneel [more info]



Helios Voting Booth

IACR Elections

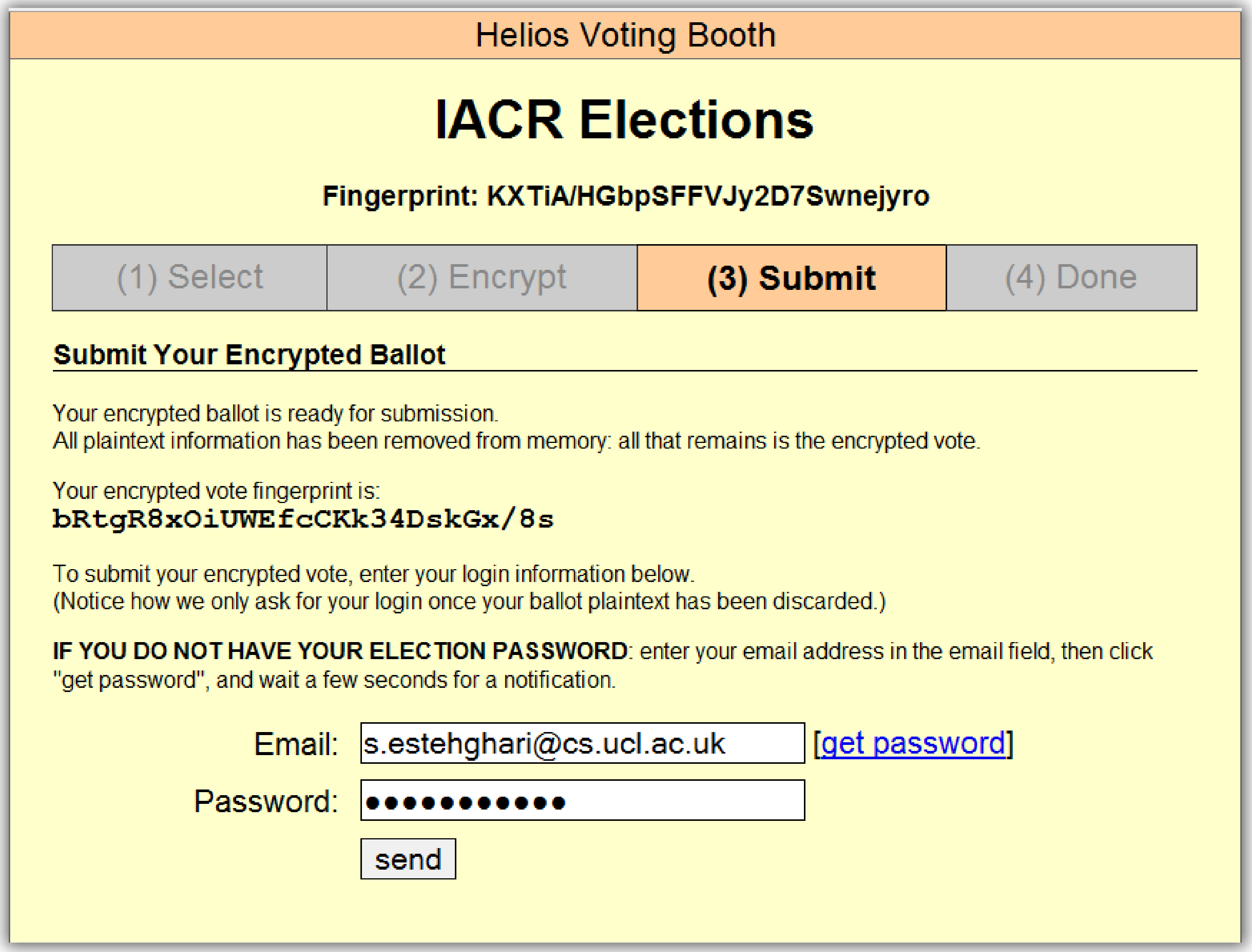
Fingerprint: KXTiA/HGbpSFFVJy2D7Swnejyro

Your ballot has now been encrypted. Your ballot fingerprint is:

bRtgR8xOiUWEfcCKk34DskGx/8s [Your Receipt]

If you choose to submit this ballot, all plaintext information will be deleted from your browser's memory.

You can choose to audit your ballot, which will show you how your options were encrypted. You will then have to re-seal your ballot if you wish to cast it.



Helios Voting Booth

IACR Elections

Fingerprint: KXTiA/HGbpSFFVJy2D7Swnejyro

(1) Select | (2) Encrypt | **(3) Submit** | (4) Done

Submit Your Encrypted Ballot

Your encrypted ballot is ready for submission.
All plaintext information has been removed from memory: all that remains is the encrypted vote.

Your encrypted vote fingerprint is:
`bRtgR8xOiUWEfcCKk34DskGx/8s`

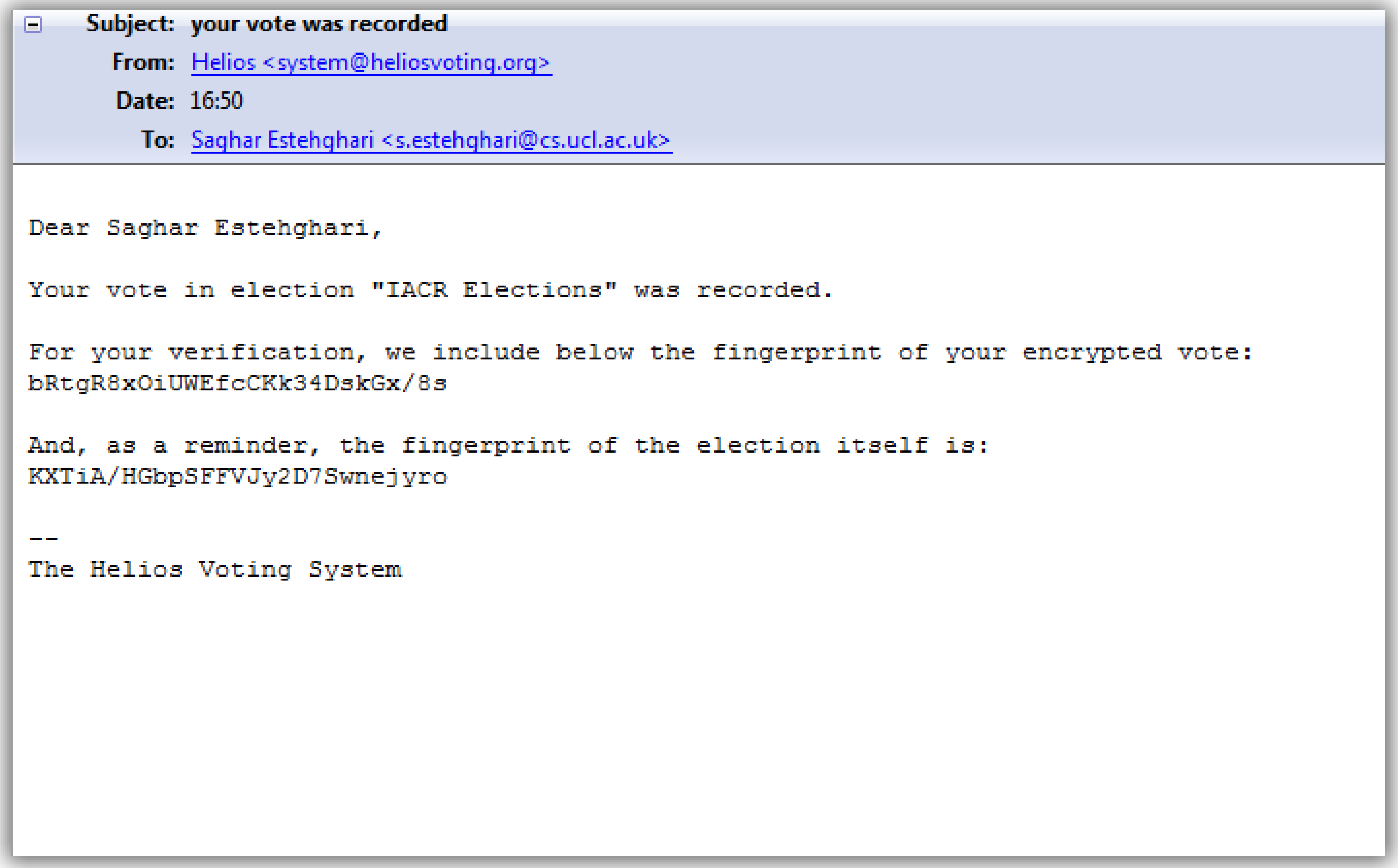
To submit your encrypted vote, enter your login information below.
(Notice how we only ask for your login once your ballot plaintext has been discarded.)

IF YOU DO NOT HAVE YOUR ELECTION PASSWORD: enter your email address in the email field, then click "get password", and wait a few seconds for a notification.

Email: s.estehghari@cs.ucl.ac.uk [get password]

Password: ●●●●●●●●●●●

send



Subject: your vote was recorded
From: Helios <system@heliosvoting.org>
Date: 16:50
To: Saghar Estehghari <s.estehghari@cs.ucl.ac.uk>

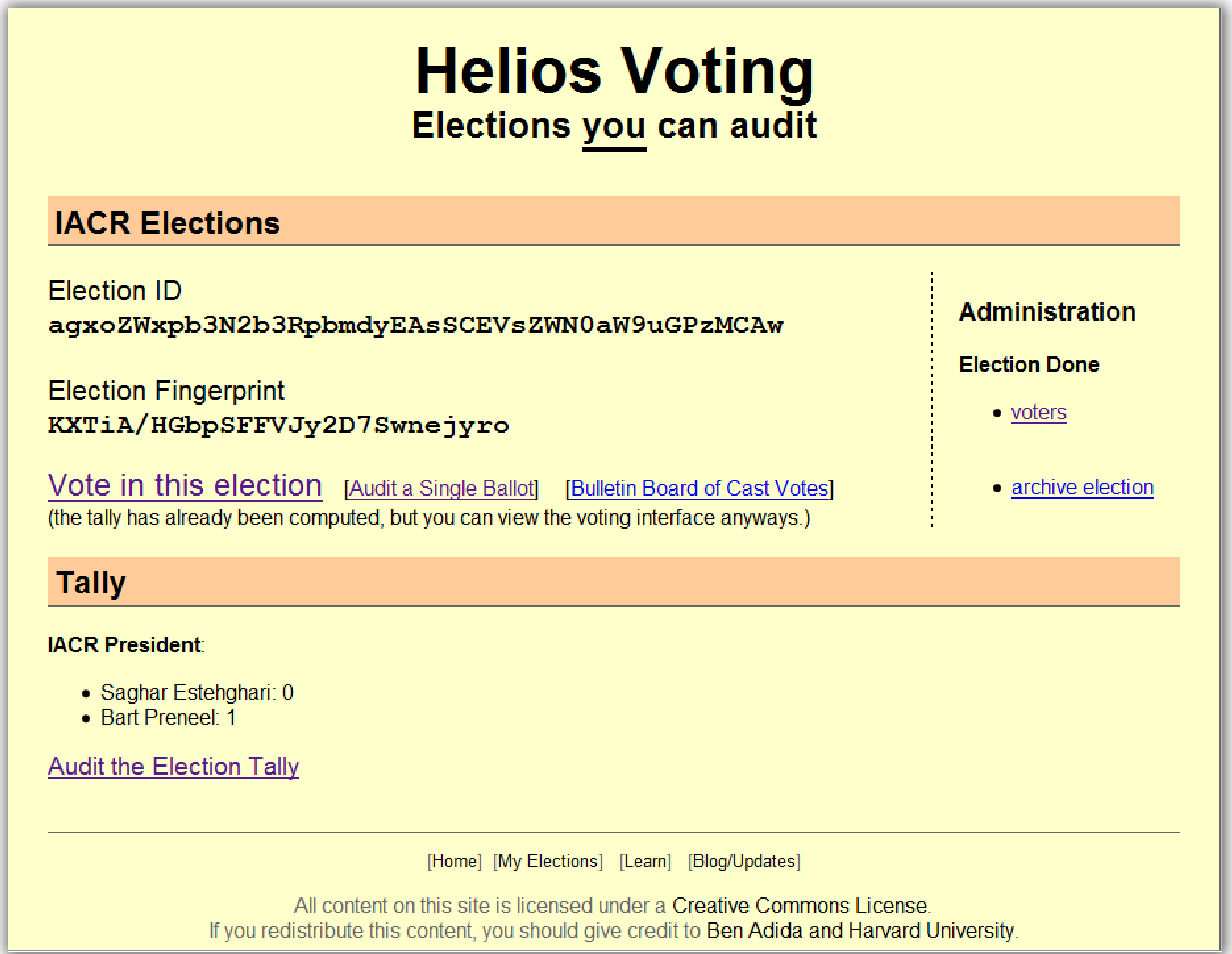
```
Dear Saghar Estehghari,

Your vote in election "IACR Elections" was recorded.

For your verification, we include below the fingerprint of your encrypted vote:
bRtgR8xOiUWEfcCKk34DskGx/8s

And, as a reminder, the fingerprint of the election itself is:
KXTiA/HGbpSFFVJy2D7Swnejyro

--
The Helios Voting System
```



Helios Voting

Elections you can audit

IACR Elections

Election ID
agxoZWxpb3N2b3RpbmdyEAsSCEVsZWN0aW9uGPzMCAw

Election Fingerprint
KXTiA/HGbpSFFVJy2D7Swnejyro

Vote in this election [Audit a Single Ballot] [Bulletin Board of Cast Votes]
(the tally has already been computed, but you can view the voting interface anyways.)

Administration

Election Done

- voters
- archive election

Tally

IACR President:

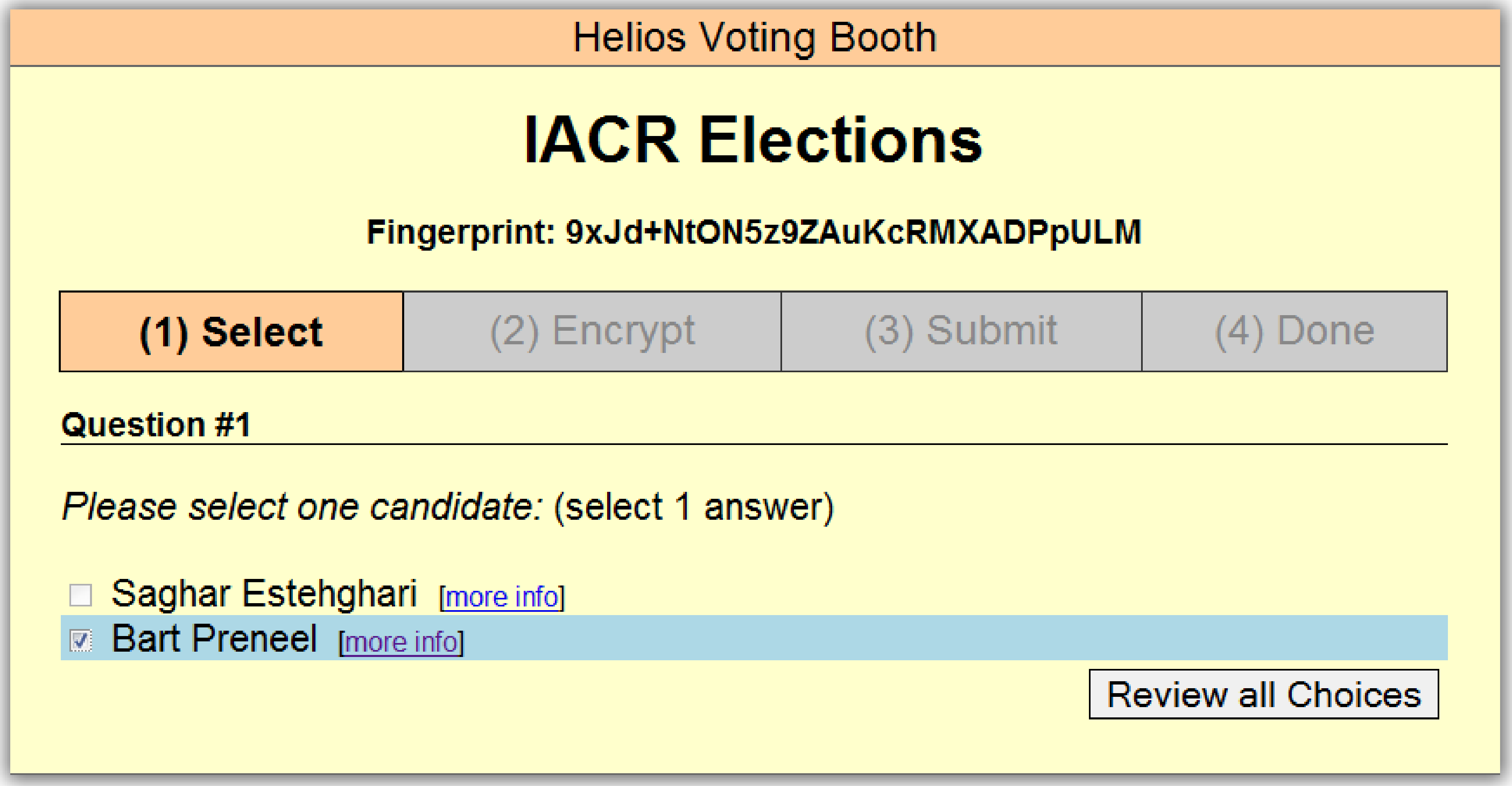
- Saghar Estehghari: 0
- Bart Preneel: 1

Audit the Election Tally

[Home] [My Elections] [Learn] [Blog/Updates]

Techniques Used

- Our malicious Firefox extension is able to break the integrity of a ballot.
- It exploits buffer overflow vulnerabilities in Adobe Acrobat/Reader to install a browser rootkit on the voter's machine.



Helios Voting Booth

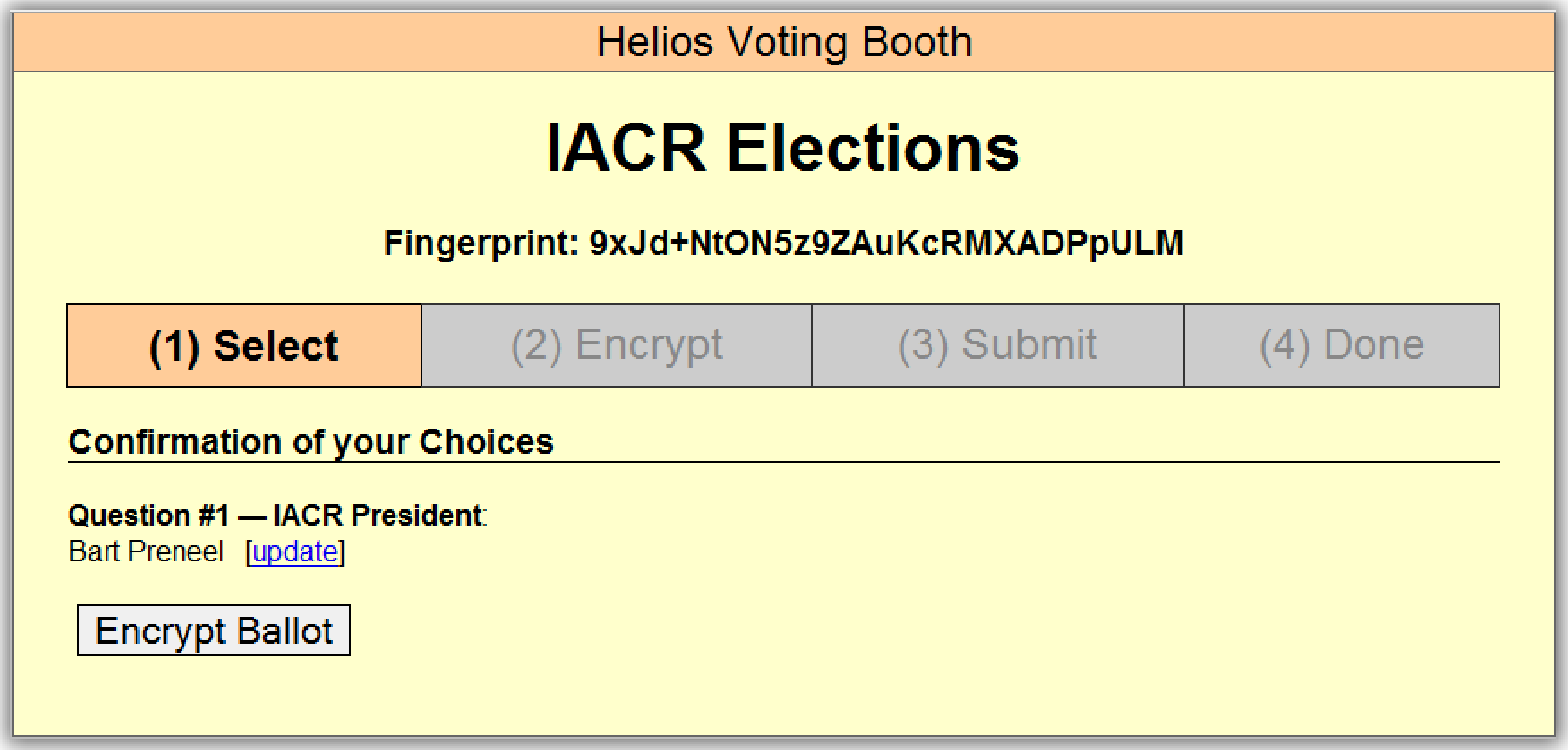
IACR Elections

Fingerprint: 9xJd+NtON5z9ZAuKcRMXADPpULM

Question #1

Please select one candidate: (select 1 answer)

□ Saghar Estehghari [more info]
☑ Bart Preneel [more info]

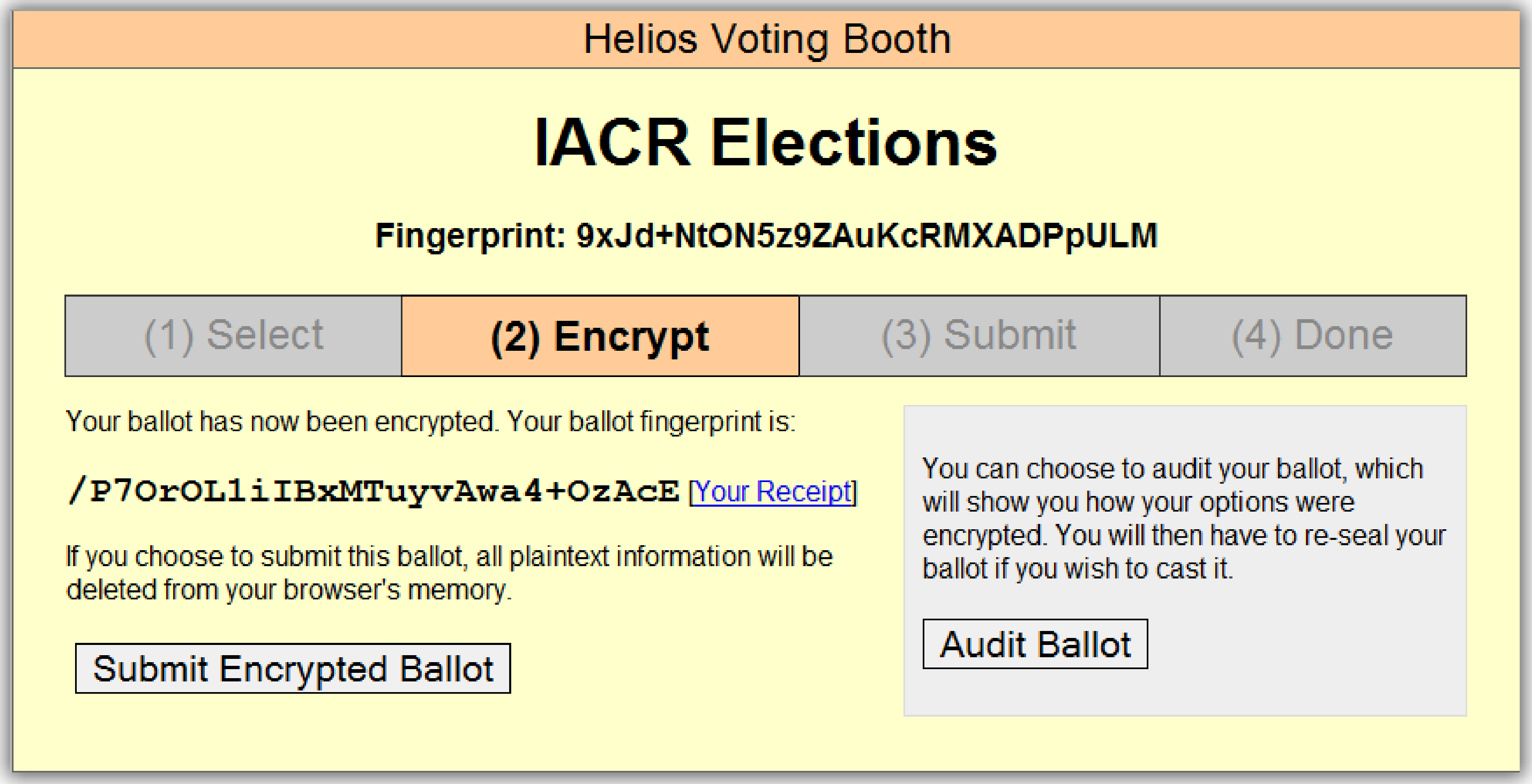


IACR Elections

Fingerprint: 9xJd+NtON5z9ZAuKcRMXADPpULM

Confirmation of your Choices

Question #1 — IACR President:
Bart Preneel [update]



IACR Elections

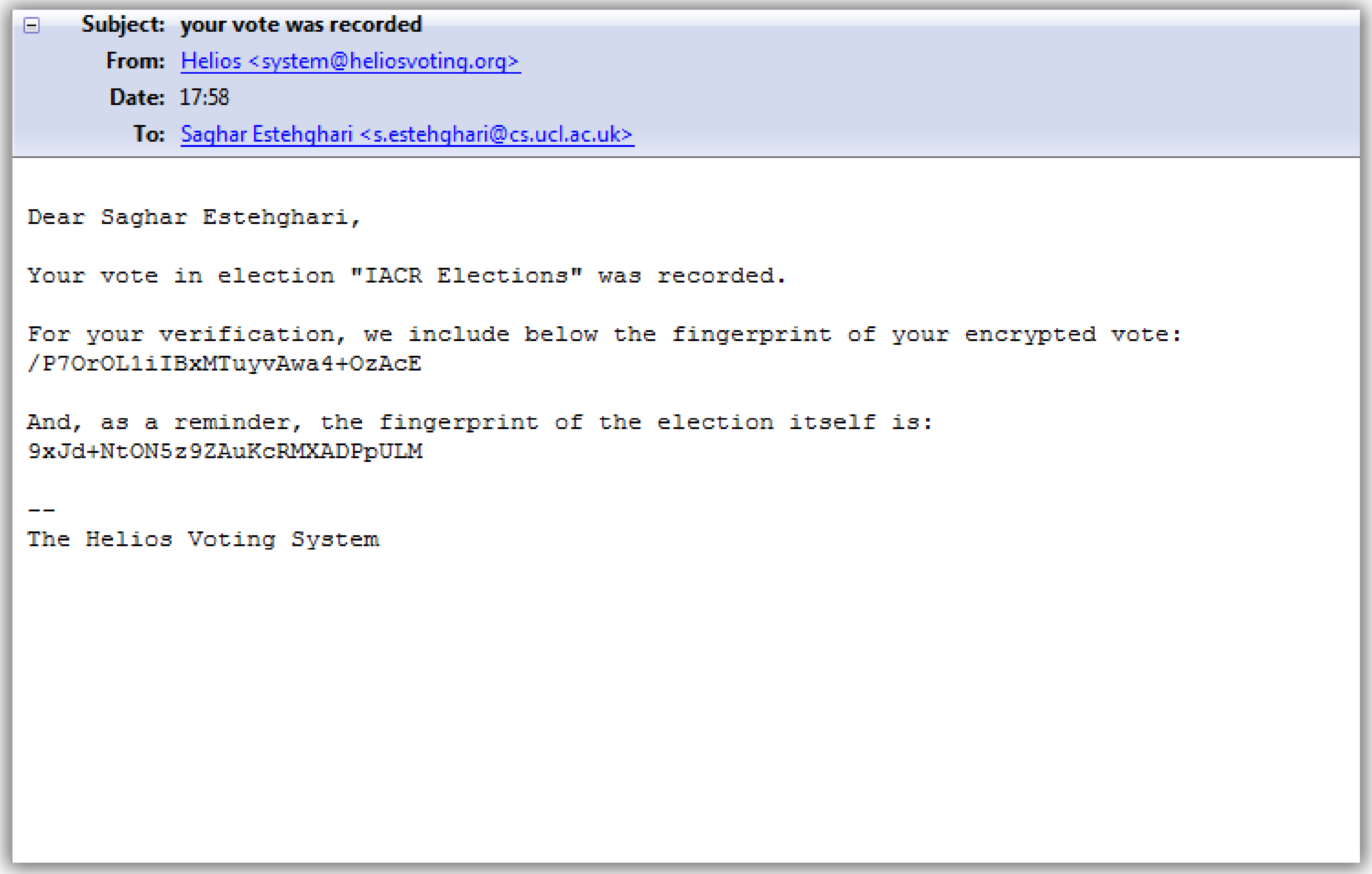
Fingerprint: 9xJd+NtON5z9ZAuKcRMXADPpULM

Your ballot has now been encrypted. Your ballot fingerprint is:

`/P7OrOL1iIBxMTuyvAwa4+OzAcE` [Your Receipt]

If you choose to submit this ballot, all plaintext information will be deleted from your browser's memory.

You can choose to audit your ballot, which will show you how your options were encrypted. You will then have to re-seal your ballot if you wish to cast it.



Subject: **your vote was recorded**
From: Helios <system@heliosvoting.org>
Date: 17:58
To: Saghar Estehghari <s.estehghari@cs.ucl.ac.uk>

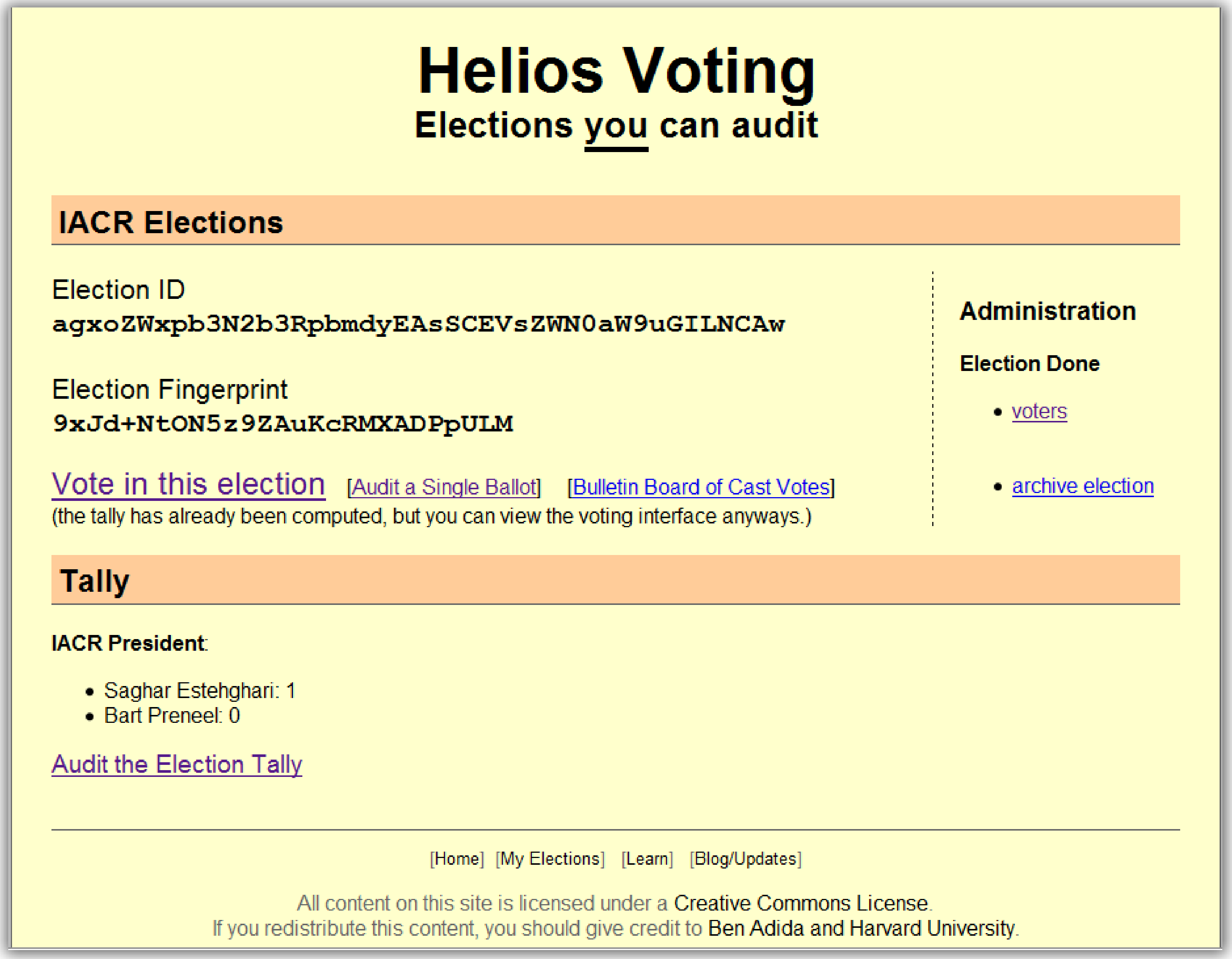
```
Dear Saghar Estehghari,

Your vote in election "IACR Elections" was recorded.

For your verification, we include below the fingerprint of your encrypted vote:
/P7OrOL1iIBxMTuyvAwa4+OzAcE

And, as a reminder, the fingerprint of the election itself is:
9xJd+NtON5z9ZAuKcRMXADPpULM


--
The Helios Voting System
```



Helios Voting

Elections you can audit

IACR Elections

Election ID
agxoZWxpb3N2b3RpbmdyEAsSCEVsZWN0aW9uGILNCAw

Election Fingerprint
9xJd+NtON5z9ZAuKcRMXADPpULM

Vote in this election [Audit a Single Ballot] [Bulletin Board of Cast Votes]
(the tally has already been computed, but you can view the voting interface anyways.)

Administration

Election Done

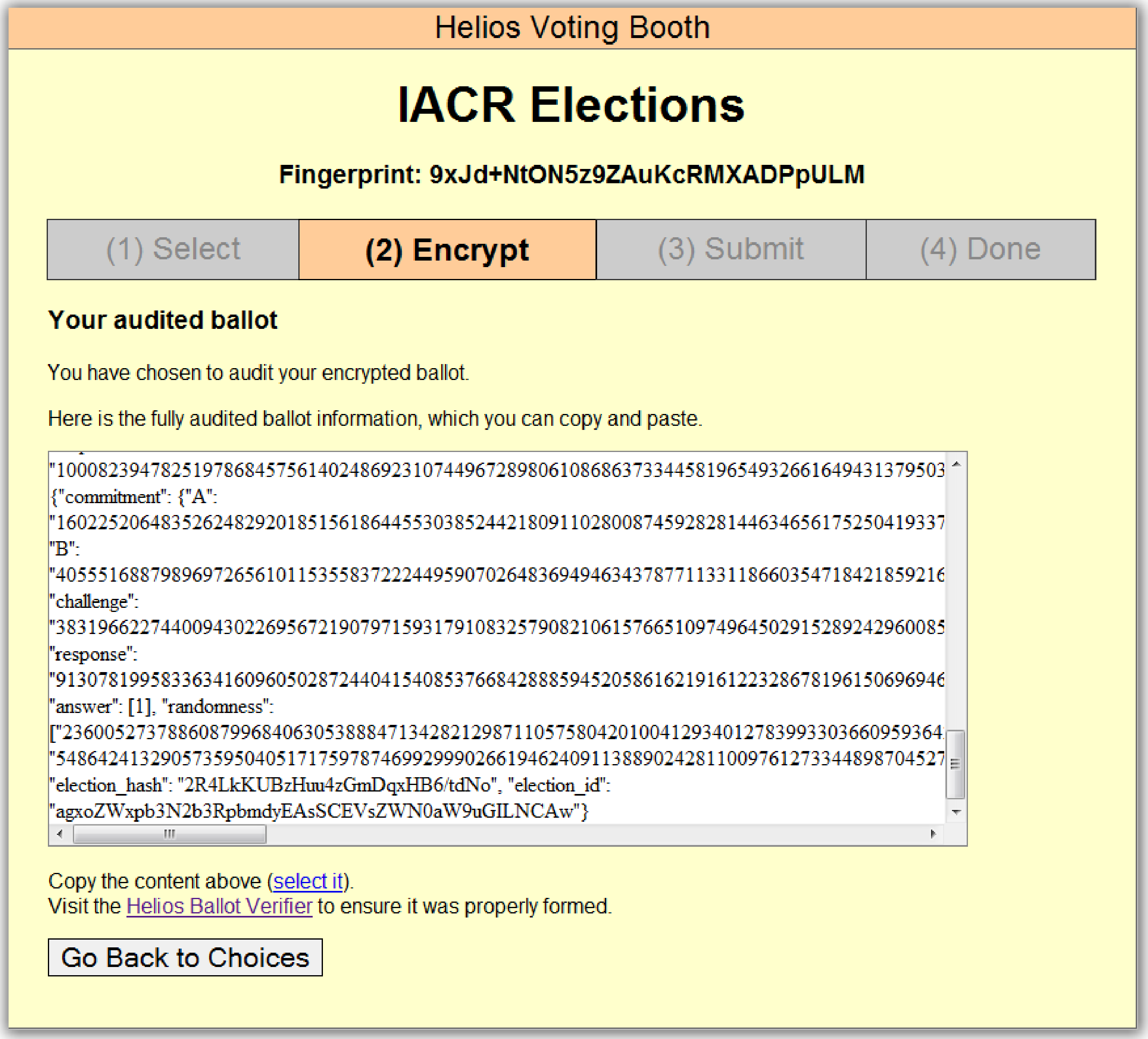
- voters
- archive election

Tally

IACR President:

- Saghar Estehghari: 1
- Bart Preneel: 0

Audit the Election Tally



Helios Voting Booth

IACR Elections

Fingerprint: 9xJd+NtON5z9ZAuKcRMXADPpULM

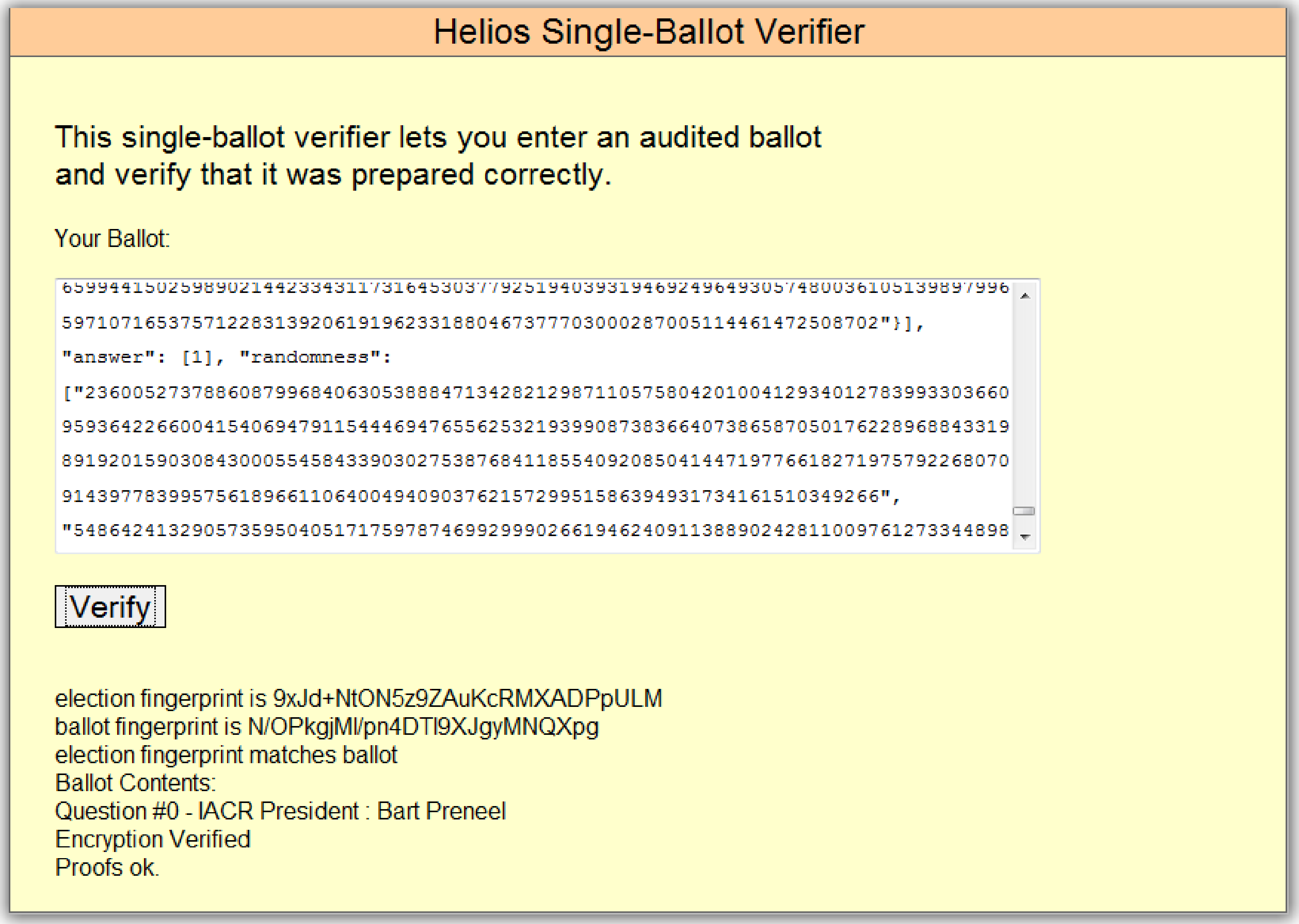
Your audited ballot

You have chosen to audit your encrypted ballot.

Here is the fully audited ballot information, which you can copy and paste.

```
"1000823947825197868457561402486923107449672898061086863733445819654932661649431379503
{"commitment": {"A":
"1602252064835262482920185156186445530385244218091102800874592828144634656175250419337
"B":
"4055516887989697265610115355837222449590702648369494634378771133118660354718421859216
"challenge":
"3831966227440094302269567219079715931791083257908210615766510974964502915289242960085
"response":
"9130781995833634160960502872440415408537668428885945205861621916122328678196150696946
"answer": [1], "randomness":
["2360052737886087996840630538884713428212987110575804201004129340127839933036609593364
"5486424132905735950405171759787469929990266194624091138890242811009761273344898704527
"election_hash": "2R4LkKUBzHuu4zGmDqxHB6/tdNo", "election_id":
"agxoZWxpb3N2b3RpbmdyEAsSCEVsZWN0aW9uGILNCAw"}
```

Copy the content above (select it).
Visit the Helios Ballot Verifier to ensure it was properly formed.



Helios Single-Ballot Verifier

This single-ballot verifier lets you enter an audited ballot and verify that it was prepared correctly.

Your Ballot:

```
65994415025989021442334311731645303779251940393194692496493057480036105139897996
597107165375712283139206191962331880467377703000287005114461472508702"}],
"answer": [1], "randomness":
["236005273788608799684063053888471342821298711057580420100412934012783993303660
959364226600415406947911544469476556253219399087383664073865870501762289688433l9
891920159030843000554584339030275387684118554092085041447197766182719757922680 70
914397783995756189661106400494090376215729951586394931734161510349266",
"5486424132905735950405171759787469929990266194624091138890242811009761273344898
```

election fingerprint is 9xJd+NtON5z9ZAuKcRMXADPpULM
ballot fingerprint is N/OPkgjMl/pn4DTl9XJgyMNQXpg
election fingerprint matches ballot
Ballot Contents:
Question #0 - IACR President : Bart Preneel
Encryption Verified
Proofs ok.

Defences & Countermeasures

- Disable the JavaScript option in Adobe Acrobat.
  - It works, but not secure against viruses, worms, and etc.
- Having a third party system which verifies the voter’s ballots.
  - One can use Adobe weakness to modify this software too.

Further Work

- The extension under development will email “Bart Preneel” who tried to vote against him.
- It is possible to launch a similar attack against voters using Internet Explorer.

Impact

Clinton in Nigeria: “In 2000 our presidential election came down to one state where the brother of one of the men running for president was governor of the state.”

Future

- Assuming Internet e-voting is used in 2012:
  - Your computer may become a target for lobbyists, extremists, etc.
  - Bush III will not need his brother!
  - Dick Cheney will know who voted against Bush III!

Conclusions

- Used to be: May the Best Candidate Win
- Today: May the Best Hacker Win

(Death of Democracy Or May the Best Hacker Win, by Christopher Bollyn)

Conclusions

Due to this successful attack on Helios, one can conclude the cryptography used is just window dressing.

Questions?

Question: Assumptions?

1. Windows XP Service Pack 0 or upper,
2. Firefox version 1.5 to 3.5.*,
3. Firefox installation folder is under Program Files,
4. The client must have write privilege for the mentioned folders,
5. Adobe Acrobat/Reader with versions 7.0.0 to 8.1.2 and 9.0.0, is installed on the client's machine.