E-voting and IACR elections

Yvo Desmedt Stuart Haber Shai Halevi James Hughes Antoine Joux
Jean-Jacques Quisquater

March 31, 2008

1 Background

Following some public discussion on the topic, the IACR board of directors discussed in its August-2007 meeting the possibility of using electronic voting for the IACR elections. The board formed a sub-committee (consisting of Yvo Desmedt, Stuart Haber, Shai Halevi, James Hughes, Antoine Joux, and Jean-Jacques Quisquater) in order to further investigate this topic and "produce a report to the BoD, circulated in advance of EC08 Meeting." This report is the result of our investigation into the topic.

We sent a request for input to many of the leading researchers on e-voting, and several of them responded with comments and questions. Specifically we received comments from Ben Adida, Josh Benaloh, Peter Ryan, Ron Rivest, and David Wagner, as well as three proposals of e-voting schemes that the IACR could use from Ben Adida, Aggelos Kiayias, and Kazue Sako. The report below includes a compilation of these comments, and also some earlier public comments on the subject that can be found at the URL

`http://attachments.wetpaintserv.us/$aLzn1XzS1QcPWJGu$dF5w==14551`

2 Should the IACR switch to e-voting?

The first decision that the board should make is whether or not the IACR should abandon its current system, which is based on double envelopes that are sent via the postal service, and move to an e-voting system. Below we summarize the main PROs and CONs of e-voting as they apply specifically to the IACR.

2.1 Why the IACR should switch to e-voting

Perhaps the most important reason to switch to e-voting is that it can further research in Cryptology. The IACR bylaws state that "the purposes of the IACR are to advance the theory and practice of cryptology and related fields, and to promote the interests of its members with respect thereto, and to serve the public welfare." e-voting is a relatively non-trivial and high-profile use of cryptography, and having the IACR adopt e-voting could both promote more research in this area and serve as a showcase of the capabilities of modern cryptography and the benefits that it can deliver.

Beyond this IACR-specific reason, all the usual reasons that people cite for using e-voting are also true for the IACR. One such reason is convenience: it is certainly more convenient for both members and election officials to have a web interface as opposed to dealing with double envelopes. There could be a hope that this added convenience would increase the participation in the IACR elections (which is currently at about 20%), but Ron Rivest pointed out that this hope may be unfounded:

> *Changes in voting equipment and procedures are often justified by the assertion (or hope) that they will increase voter turnout. Almost universally, voter turnout doesn't increase. [...] The best model for voters is this: there are voters who conscientiously vote every election, there are voters who don't give a damn, and there might be one or two percent who can be enticed to vote with changes in procedures or equipment.*

An important benefit of (some) e-voting solutions is verifiability. Specifically, some e-voting schemes allow open-audit, where anyone can verify that his/her vote was counted and that the result is accurate.

Another reason is reliability. Currently we rely on the postal service for actually delivering the envelopes back and forth, and we sometimes run into problems with that. At least anecdotally, we all know of people who had various problems with it. ("I was on Sabbatical and didn't get my ballot," "The mail-room at the university did not understand how to deal with the double envelopes," etc.) Also, every so often we have more serious problems (such as last year) and need to extend the voting deadline to deal with mail disruptions.

Yet another standard reason that people cite is cost. Clearly running a web-application on our server would be cheaper than stamping all these envelopes (not to mention the time of the election officials). However, it should be noted that if we want our e-voting solution to be more robust (e.g., resist denial-of-service) then we may need to move to a more expensive solution for e-voting, which would negate the cost savings.

2.2 Why the IACR should not switch to e-voting

The main reason against switching to e-voting is also an IACR-specific one. Ron Rivest expressed the following concern:

> *if the IACR moves to e-voting it "legitimizes" e-voting for others. I worry (a lot) that this would give momentum for using e-voting in situations where it should not be used "just because we can."*

It is generally agreed that the inherent drawbacks of e-voting (namely coercion and vote buying) are not a big concern for IACR, but the threat is that IACR would be seen as endorsing e-voting even for situations where these issues are a big concern. On the other hand, Josh Benaloh said:

> *I think it may be overly broad to not use verifiable Internet voting systems in places where they make sense because of fears that this will promote their use in places where they are not appropriate.*

One proposed solution (by Ron) was that the "*the IACR adopts a resolution (concurrent with supporting an Internet voting scheme for its officers) that condemns Internet voting for political elections.*"

Another argument against switching to e-voting is that it would open our elections up for cyber-attacks, possibly earning us public humiliation. Yvo Desmedt wrote:

> *An electronic vote for IACR elections is inviting the hacking community to hack it and have an headline in the New York Times about how they rigged an election of an association in information security!*

The subcommittee did not try to evaluate the actual risks posed by cyber-attacks. Different members have widely different opinions regarding these risks.

Yet another concern is that if the IACR chooses to go with some commercial solution, it would seem as an endorsement for that commercial entity by the IACR. On the other hand, using an open-source/non-commercial solution would mean that we need to provide the infrastructure for it and maintain it ourselves.

Finally, it should be noted that switching to e-voting would most likely require a change to the IACR bylaws. (The current bylaws mandate a postal-mail-based system.)

3 E-voting systems

If the board decides to switch to e-voting, then it (eventually) needs to choose a specific system to use. Below we list some possible choices, both commercial/established systems and systems which are more research prototypes or open-source projects.

The systems that are listed in Sections 3.1 and 3.2 below are using crypto-solutions for e-voting, but there are also several commercial systems available today that are not doing any crypto-based solution. One example is SBS (`http://www.gosbs.com/services/election.htm`): their web-site says that "The ballots are stored in a secure datacenter with controlled, monitored access 24 hours per day, 7 days per week," which seems to imply that the ballot are not even encrypted in any meaningful way. Another non-crypto option is "Everyone Counts" (`http://www.everyonecounts.com/`).

The advantage of using such systems is that we are outsourcing the elections, and operating/securing it becomes somebody else's problem. The disadvantage (beyond the price tag that is likely to be high) is that we lose all the advantages of e-voting (except convenience): the process will be even less verifiable than our current system, and we lose the opportunity to promote research on the topic.

If we want to use "crypto-based" e-voting systems, then we can either go with commercial/established systems or with research/open-source projects.

3.1 Commercial/established crypto-based systems

PunchScan (`www.punchscan.org`): this system by David Chaum is designed for polling-booth elections. It has several controls against coercion that cannot be used (and are not needed) in

IACR elections. Still, the system can be made usable in the IACR elections. The system is a mixed paper/electronic system and it requires some special equipment to run. (If we decide to go that way, then PunchScan may be able to help with the cost of the equipment for the first election.)

Prêt à Voter is another a mixed paper/electronic system, by Peter Ryan from Newcastle. It too was designed for a polling-booth setting but can be modified to fit the IACR election system (again, still relying on postal-mail delivery).

Others: Other commercial crypto-based systems include **VoteHere** (`http://votehere.com`) or **Scytl** (`http://www.scytl.com`). We did not try to evaluate any of them, however.

3.2 Research prototypes/open-source systems

In response to our call for input, we received three proposals for systems that can be used for the IACR elections, and we list them below. These three proposals are more research prototypes than fully complete systems (but they all are complete enough to be used by the IACR).

All three proposals sport universal-verifiability/open-audit (at least in principle), and choosing either one would likely play a significant role in promoting research on e-voting. On the negative side, they have uncertain support/maintenance, and will likely require volunteer time from IACR members to support. (We note that similar support status is currently used by the IACR for its conference registration system, the ePrint archive and the submission/review sites for conferences.) Also, these systems would need to change somewhat in order to be integrated with IACR membership system.

Digishuff-Pro from NEC, see attached file Digishuff.doc.

Type of system: based on mix-nets (EC-Elgamal with simplified proofs of correct mixing using permutation matrices).

Technology: Java applet for voting, standalone programs for administration (generating parameters, mix, decryption), web-server implementation for display of candidates, vote collection, and verification.

PROs: Relatively mature/stable: operating since 2004, used for ≈ 20 elections, fast operations.

CONs: Only Windows/IE implementations (both client and server), may need to re-write small parts to adjust to the specifics of IACR elections, most of the documentation is currently only available in Japanese.

Adder from Aggelos Kiayias at the Univ. of Connecticut (`http://cryptodrm.engr.uconn.edu/adder`), see attached email message.

Type of system: based on homomorphic encryption (ElGamal).

Technology: Java applet for voting, a standalone program for administration (generating parameters, mix, decryption), web-server implementation for display of candidates, vote collection, and verification .

PROs: Open source, fairly efficient, threshold decryption, good documentation.

CONs: Standalone admin program is very "unix-oriented" and has quite a few dependencies (built on top of QT).

Helios from Ben Adida at Harvard (`http://heliosvoting.org`), see attached file helios.pdf.

Type of system: based on mix-nets (with cut-and-choose proofs of correct mixing).

Technology: Javascript for all clients (voting, administration), Python for server functions. Verifying the proofs currently requires separate python scripts.

PROs: promised to be released as open-source, ease-of-use (due to all-Javascript implementation), simplicity, "live demo system" is available.

CONs: Very new, only initial release at this time. Currently only works on Firefox & IE7 (Safari in the works), no threshold decryption (at least yet). Currently proof verification is slow.

Another system that is promised to be released as open-source is the Cornell Civitas system (`http://www.cs.cornell.edu/projects/civitas/`).

4 What happens now

The IACR board-of-directors in its meeting on April 2008 should make an initial decision as to whether or not the IACR should replace its current postal-based system with a system based on Internet voting.

If the board decides to go ahead with this change, then perhaps a separate process should be setup to evaluate specific candidates with a goal of either recommending one system or brining 2-3 systems for the board to decide on. It seems realistic to complete this process in time for the August meeting of the board, and put these changes on the membership ballot in the fall of 2008. (This ballot is still going to be held using our current system.)

If the board rejects the change, we may still consider adding verifiability to our current paper-based system (e.g., using systems such as PunchScan or Prêt à Voter).