Towards unconditionally E2E verifiable elections: the making of Demos remote e-voting system

Aggelos Kiayias, **Thomas Zacharias** & Bingsheng Zhang

Crypto.Sec Group
Department of Informatics and Telecommunications
University of Athens

4th Crypto.Sec Day
July 17, 2014

What makes a voting system reliable?

What makes a voting system reliable?

1. **Integrity:** The election result matches the vote intention of the electorate.

What makes a voting system reliable?

1. **Integrity:** The election result matches the vote intention of the electorate.
2. **Privacy:** No one can learn how the voters have voted or control their free will.

Traditional elections

1. Privacy is achieved by voting in a booth and using anonymous ballots and envelopes.

Traditional elections

1. Privacy is achieved by voting in a booth and using anonymous ballots and envelopes.
2. Integrity is **indirect** and relies on faith assumptions (conflict of interests, trust in state representatives, etc.).

Motivation for adopting Electronic voting (e-voting)

- Increasing political participation and representation among traditionally underrepresented groups.
- Cost-efficient and better administered elections.

Types of Electronic voting systems

On-site e-voting

On-site e-voting

Remote e-voting (i-voting)

Privacy in Electronic voting

- Anonymity of the votes is ensured via cryptographic primitives (mixnets, homomorphic encryption).
- At on-site e-voting systems, voters are protected from coercion as in traditional elections.

Privacy in Electronic voting

- Anonymity of the votes is ensured via cryptographic primitives (mixnets, homomorphic encryption).
- At on-site e-voting systems, voters are protected from coercion as in traditional elections. At remote e-voting systems, coercion resistance is a major challenge. Several solutions have been proposed (voting multiple times, misleading the coercer by using fake credentials or fake ballots).

Integrity in Electronic voting

The major advantage of the state-of-the-art e-voting systems is that they allow the voters to check the integrity of the elections without putting trust to any authority (impossible in traditional elections).

Integrity in Electronic voting

The major advantage of the state-of-the-art e-voting systems is that they allow the voters to check the integrity of the elections without putting trust to any authority (impossible in traditional elections).

- A single voter may check that her vote was
  - (i). Cast as intended.
  - (ii). Recorded as cast.
  - (iii). Tallied as recorded.
- Any public auditor may verify the correct execution of the elections.

Integrity in Electronic voting

The major advantage of the state-of-the-art e-voting systems is that they allow the voters to check the integrity of the elections without putting trust to any authority (impossible in traditional elections).

- A single voter may check that her vote was
  - (i). Cast as intended.
  - (ii). Recorded as cast.
  - (iii). Tallied as recorded.
- Any public auditor may verify the correct execution of the elections.

An e-voting system that satisfies these properties is called

End-to-end (E2E) Verifiable

E2E Verifiable e-voting systems

On-site E2E Verifiable e-voting systems:

- Prêt à Voter [Chaum, Ryan & Schenider - 2005].
- Scantegrity II [Chaum et al. - 2009].

E2E Verifiable e-voting systems

On-site E2E Verifiable e-voting systems:

- Prêt à Voter [Chaum, Ryan & Schenider - 2005].
- Scantegrity II [Chaum et al. - 2009].

Remote E2E Verifiable e-voting systems:

- Helios [Adida - 2008].
- Remotegrity [Zagorski et al. - 2013].
- *Demos* [Kiayias, Zacharias & Zhang - 2014].

E2E Verifiable e-voting systems

On-site E2E Verifiable e-voting systems:

- Prêt à Voter [Chaum, Ryan & Schenider - 2005].
- Scantegrity II [Chaum et al. - 2009].

Remote E2E Verifiable e-voting systems:

- Helios [Adida - 2008].
- Remotegrity [Zagorski et al. - 2013].
- *Demos* [Kiayias, Zacharias & Zhang - 2014].

Demos is the only remote e-voting proven E2E verifiable in the standard model (does not assume the existence of an external truly random source).

The making of Demos remote e-voting system

The security framework

- We consider a single Election Authority (EA) that controls the whole system (all authorities and the voter clients are potentially corrupted and colluding).
- Our aim is E2E Verifiability in the standard model in the case that EA and a constant fraction of the voters is malicious.
- We require Voter Privacy against anyone but the Election Authority.

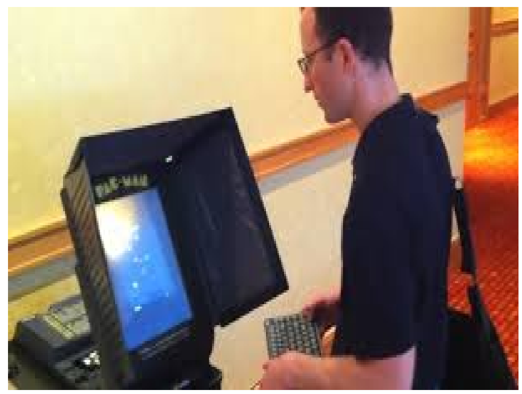
Code-voting 101

Election Authority

Candidate	Vote-code
Alice	AAAA-1111
Bob	BBBB-2222
Charlie	CCCC-3333
David	DDDD-4444

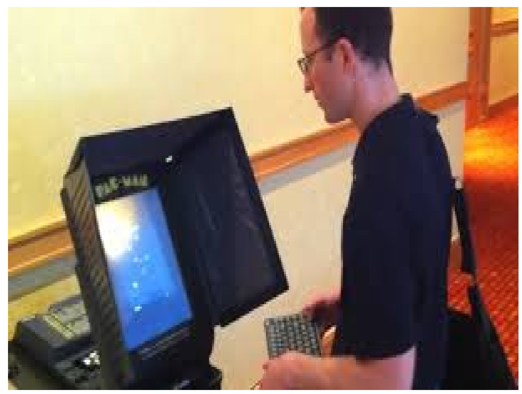
Code-voting 101

Candidate	Vote-code
Alice	AAAA-1111
Bob	BBBB-2222
Charlie	CCCC-3333
David	DDDD-4444



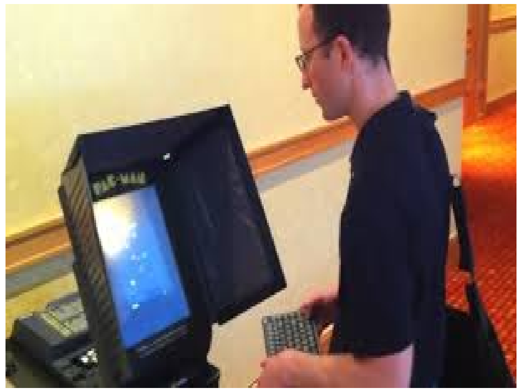
Code-voting 101

Candidate	Vote-code
Alice	AAAA-1111
Bob	BBBB-2222
Charlie	CCCC-3333
David	DDDD-4444



Code-voting 101

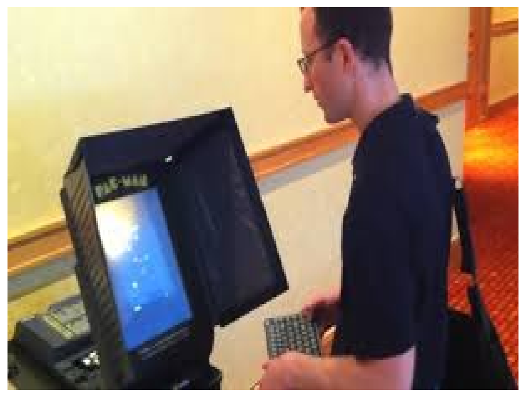
Candidate	Vote-code
Alice	AAAA-1111
Bob	BBBB-2222
Charlie	CCCC-3333
David	DDDD-4444



- The EA records the vote-codes that have been submitted by all the voters.

Code-voting 101

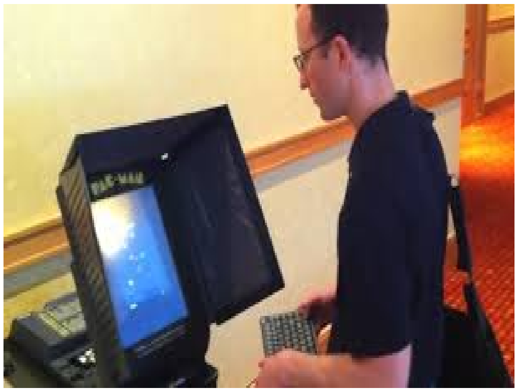
Candidate	Vote-code
Alice	AAAA-1111
Bob	BBBB-2222
Charlie	CCCC-3333
David	DDDD-4444



- The EA records the vote-codes that have been submitted by all the voters.
- The EA knows the vote-code and candidate correspondence in all ballots, so it performs tally and announces the election result.

Code-voting 101

Candidate	Vote-code
Alice	AAAA-1111
Bob	BBBB-2222
Charlie	CCCC-3333
David	DDDD-4444



- The EA records the vote-codes that have been submitted by all the voters.
- The EA knows the vote-code and candidate correspondence in all ballots, so it performs tally and announces the election result.

The described e-voting system is simple and easy. Is it reliable?

- Privacy is guaranteed against anyone that does not know the vote-code and candidate correspondence.

- Privacy is guaranteed against anyone that does not know the vote-code and candidate correspondence.
- Integrity of the system can be verified only at the minimum level.
  - The voters know that their vote was *cast-as-intended* by submitting the vote-code that corresponds to the candidates of their choice.

- Privacy is guaranteed against anyone that does not know the vote-code and candidate correspondence.
- Integrity of the system can be verified only at the minimum level.
  - The voters know that their vote was *cast-as-intended* by submitting the vote-code that corresponds to the candidates of their choice.
  - The voters cannot verify that their was *recorded-as-cast* (the vote-code could be not be accepted or altered due to system failure without any notice).
  - No audit information is published by the Election Authority, so the voters can verify that their vote was *tallied-as-recorded* or some party can verify the correct execution of the election.

Taking a step further: proving correct record of the votes

Election Authority

$\downarrow$

Candidate	Vote-code	Receipt
Alice	AAAA-1111	REC1
Bob	BBBB-2222	REC2
Charlie	CCCC-3333	REC3
David	DDDD-4444	REC4

Ballot No. 100

Taking a step further: proving correct record of the votes

Candidate	Vote-code	Receipt
Alice	AAAA-1111	REC1
Bob	BBBB-2222	REC2
Charlie	CCCC-3333	REC3
David	DDDD-4444	REC4

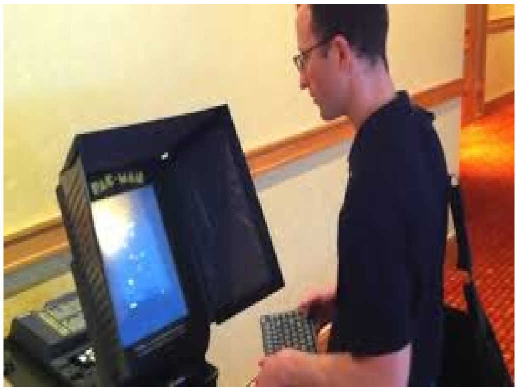
Ballot No. 100

Each vote-code is paired with a (pseudo) randomly generated receipt.

Taking a step further: proving correct record of the votes

Candidate	Vote-code	Receipt
Alice	AAAA-1111	REC1
Bob	BBBB-2222	REC2
Charlie	CCCC-3333	REC3
David	DDDD-4444	REC4

Ballot No. 100



Taking a step further: proving correct record of the votes

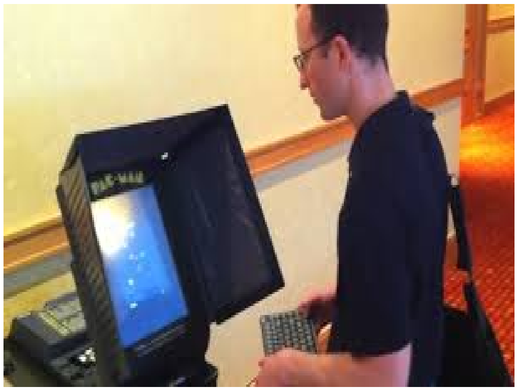
Candidate	Vote-code	Receipt
Alice	AAAA-1111	REC1
Bob	BBBB-2222	REC2
Charlie	CCCC-3333	REC3
David	DDDD-4444	REC4

Ballot No. 100

Taking a step further: proving correct record of the votes

Candidate	Vote-code	Receipt
Alice	AAAA-1111	REC1
Bob	BBBB-2222	REC2
Charlie	CCCC-3333	REC3
David	DDDD-4444	REC4

Ballot No. 100



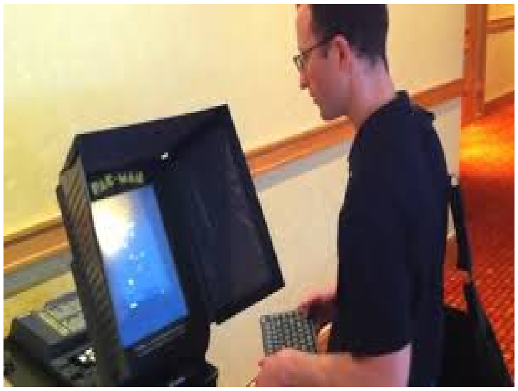
No. 100
AAAA-1111

Election Authority

Taking a step further: proving correct record of the votes

Candidate	Vote-code	Receipt
Alice	AAAA-1111	REC1
Bob	BBBB-2222	REC2
Charlie	CCCC-3333	REC3
David	DDDD-4444	REC4

Ballot No. 100

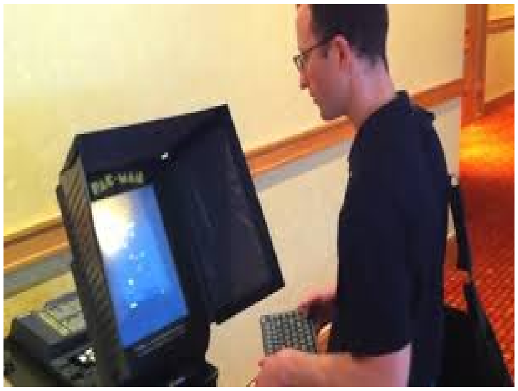


Election Authority

Taking a step further: proving correct record of the votes

Candidate	Vote-code	Receipt
Alice	AAAA-1111	REC1
Bob	BBBB-2222	REC2
Charlie	CCCC-3333	REC3
David	DDDD-4444	REC4

Ballot No. 100



REC1

Election Authority

What do we gain using receipts

- Privacy remains at the same levels since including random receipts does not leak any information about the vote-code and candidate correspondence.
- The voters can verify that their vote was cast-as-intended and that it was recorded-as-cast (the only way that the system may reply with the correct receipt is that they read the correct vote-code).
- Still, lack of further audit information does not make any further verification possible (that the recorded vote was counted-as-intended and the election was executed properly).

Enabling audit: introducing the Bulletin Board

Election Authority

Candidate	Vote-code	Receipt
Alice	AAAA-1111	REC1
Bob	BBBB-2222	REC2
Charlie	CCCC-3333	REC3
David	DDDD-4444	REC4

Ballot No.100

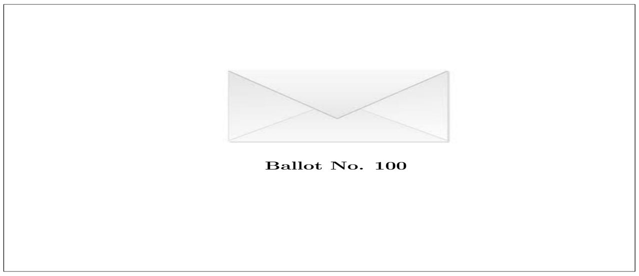
Bulletin Board

Enabling audit: introducing the Bulletin Board

Election Authority

Candidate	Vote-code	Receipt
Alice	AAAA-1111	REC1
Bob	BBBB-2222	REC2
Charlie	CCCC-3333	REC3
David	DDDD-4444	REC4

Ballot No.100



Bulletin Board

What we gain by using the Bulletin Board

- After voting ends, EA announces the result and opens the envelopes, so audit can be performed.
- The use of an electronic envelope prevents a malicious EA from posting audit information which is inconsistent.
- The electronic envelope is realised by a perfectly binding, computationally hiding and additively homomorphic **commitment scheme** $\mathrm{Com}(\cdot)$.

Exploiting the properties of a commitment scheme

The "envelope" effect:

(i). Binding: EA cannot open $\mathrm{Com}(m)$ to a message other than m, so the audit information is perfectly consistent.

(ii). Hiding: Any PPT algorithm that does not have the opening key cannot read m from $\mathrm{Com}(m)$, so sensitive information about the voters' ballots is not leaked.

Exploiting the properties of a commitment scheme

Computing the tally in a verifiable way:

(iii). Additively homomorphic:

$$\boxed{\mathrm{Com}(m_1) \cdot \mathrm{Com}(m_2) = \mathrm{Com}(m_1 + m_2)}$$

Exploiting the properties of a commitment scheme

Computing the tally in a verifiable way:

(iii). Additively homomorphic:

$$\boxed{\mathrm{Com}(m_1) \cdot \mathrm{Com}(m_2) = \mathrm{Com}(m_1 + m_2)}$$

- The EA encodes the candidates in “message” format and posts the pairs of vote-codes and encoded candidates in committed form.
- The EA opens all vote-code commitments and marks all the cast vote-codes and the commitments that are associated with them.
- The EA multiplies all the marked commitments, opens the result and posts the openings in the Bulletin Board (BB).
- Due to the binding property, anyone can verify that these computations were done correctly.

Example

- Three voters V_1, V_2 and V_3 want to vote for Alice, Alice and Bob respectively.

Example

- Three voters V_1, V_2 and V_3 want to vote for Alice, Alice and Bob respectively.
- The corresponding codes are C_1, C_2 and C_3.

Example

- Three voters V_1, V_2 and V_3 want to vote for Alice, Alice and Bob respectively.
- The corresponding codes are C_1, C_2 and C_3.
- The corresponding audit information posted on the BB is $\big(\mathrm{Com}(C_1), \mathrm{Com}(\langle \mathrm{Alice} \rangle)\big)$, $\big(\mathrm{Com}(C_2), \mathrm{Com}(\langle \mathrm{Alice} \rangle)\big)$ and $\big(\mathrm{Com}(C_3), \mathrm{Com}(\langle \mathrm{Bob} \rangle)\big)$.

Example

- Three voters V_1, V_2 and V_3 want to vote for Alice, Alice and Bob respectively.
- The corresponding codes are C_1, C_2 and C_3.
- The corresponding audit information posted on the BB is $\big(\mathrm{Com}(C_1), \mathrm{Com}(\langle \mathrm{Alice} \rangle)\big)$, $\big(\mathrm{Com}(C_2), \mathrm{Com}(\langle \mathrm{Alice} \rangle)\big)$ and $\big(\mathrm{Com}(C_3), \mathrm{Com}(\langle \mathrm{Bob} \rangle)\big)$.
- EA marks the pairs and opens $\mathrm{Com}(C_1)$, $\mathrm{Com}(C_2)$ and $\mathrm{Com}(C_3)$ to C_1, C_2 and C_3.

Example

- Three voters V_1, V_2 and V_3 want to vote for Alice, Alice and Bob respectively.
- The corresponding codes are C_1, C_2 and C_3.
- The corresponding audit information posted on the BB is $\big(\mathrm{Com}(C_1), \mathrm{Com}(\langle \mathrm{Alice} \rangle)\big)$, $\big(\mathrm{Com}(C_2), \mathrm{Com}(\langle \mathrm{Alice} \rangle)\big)$ and $\big(\mathrm{Com}(C_3), \mathrm{Com}(\langle \mathrm{Bob} \rangle)\big)$.
- EA marks the pairs and opens $\mathrm{Com}(C_1)$, $\mathrm{Com}(C_2)$ and $\mathrm{Com}(C_3)$ to C_1, C_2 and C_3.
- Any party can compute the multiplication:

$$\mathrm{Com}(\langle \mathrm{Alice} \rangle) \cdot \mathrm{Com}(\langle \mathrm{Alice} \rangle) \cdot \mathrm{Com}(\langle \mathrm{Bob} \rangle) = \\ = \mathrm{Com}(2 \cdot \langle \mathrm{Alice} \rangle + \langle \mathrm{Bob} \rangle).$$

Example

- Three voters V_1, V_2 and V_3 want to vote for Alice, Alice and Bob respectively.
- The corresponding codes are C_1, C_2 and C_3.
- The corresponding audit information posted on the BB is $\big(\mathrm{Com}(C_1), \mathrm{Com}(\langle \mathrm{Alice} \rangle)\big)$, $\big(\mathrm{Com}(C_2), \mathrm{Com}(\langle \mathrm{Alice} \rangle)\big)$ and $\big(\mathrm{Com}(C_3), \mathrm{Com}(\langle \mathrm{Bob} \rangle)\big)$.
- EA marks the pairs and opens $\mathrm{Com}(C_1)$, $\mathrm{Com}(C_2)$ and $\mathrm{Com}(C_3)$ to C_1, C_2 and C_3.
- Any party can compute the multiplication:

$$\mathrm{Com}(\langle \mathrm{Alice} \rangle) \cdot \mathrm{Com}(\langle \mathrm{Alice} \rangle) \cdot \mathrm{Com}(\langle \mathrm{Bob} \rangle) = \\ = \mathrm{Com}(2 \cdot \langle \mathrm{Alice} \rangle + \langle \mathrm{Bob} \rangle).$$

- EA posts the encoded result $2 \cdot \langle \mathrm{Alice} \rangle + \langle \mathrm{Bob} \rangle$, which is decoded as $\langle \mathrm{Alice} : 2, \mathrm{Bob} : 1, \mathrm{Charlie} : 0, \mathrm{David} : 0 \rangle$.

So, have we reached our goal?

So, have we reached our goal?

Unfortunately not yet...

So, have we reached our goal?

Unfortunately not yet...

1. The voters cannot be sure that the EA has not committed to a different vote-code and candidate correspondence at setup.

So, have we reached our goal?

Unfortunately not yet...

1. The voters cannot be sure that the EA has not committed to a different vote-code and candidate correspondence at setup.
2. The commitment scheme is hiding, so the EA could create commitments to multiple votes (e.g. $\mathrm{Com}(1000 \cdot \langle \mathrm{Alice} \rangle)$) without being detected.

So, have we reached our goal?

Unfortunately not yet...

1. The voters cannot be sure that the EA has not committed to a different vote-code and candidate correspondence at setup.
2. The commitment scheme is hiding, so the EA could create commitments to multiple votes (e.g. $\mathrm{Com}(1000 \cdot \langle \mathrm{Alice} \rangle)$) without being detected.

We have to enhance the system with verification mechanisms that prevent a malicious EA from committing inconsistently.

Fixing the first weakness...

1. The voters can verify that the EA has not committed to a different vote-code and candidate correspondence at setup.
2. The commitment scheme is hiding, so the EA could create commitments to multiple votes (e.g. $\mathrm{Com}(1000 \cdot \langle \mathrm{Alice} \rangle)$) without being detected.

Finalization of the construction of Demos: introducing the use of double ballots

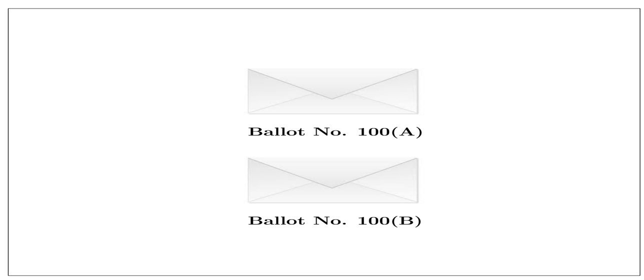
Election Authority

Candidate	Vote-code	Receipt
Alice	AAAA-1111	REC1
Bob	BBBB-2222	REC2
Charlie	CCCC-3333	REC3
David	DDDD-4444	REC4

Ballot No.100(A)

Candidate	Vote-code	Receipt
Alice	EEEE-5555	REC5
Bob	FFFF-6666	REC6
Charlie	GGGG-7777	REC7
David	HHHH-8888	REC8

Ballot No.100(B)



Bulletin Board

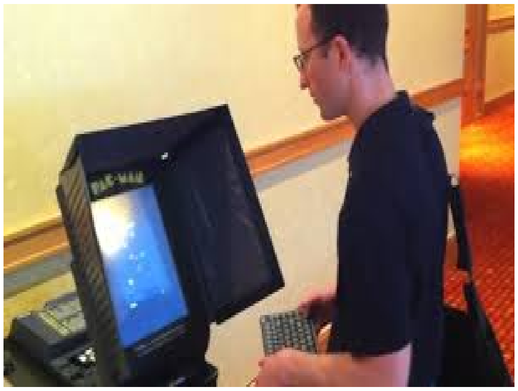
Voting with double ballots

Candidate	Vote-code	Receipt
Alice	AAAA-1111	REC1
Bob	BBBB-2222	REC2
Charlie	CCCC-3333	REC3
David	DDDD-4444	REC4

Ballot No.100(A)

Candidate	Vote-code	Receipt
Alice	EEEE-5555	REC5
Bob	FFFF-6666	REC6
Charlie	GGGG-7777	REC7
David	HHHH-8888	REC8

Ballot No.100(B)



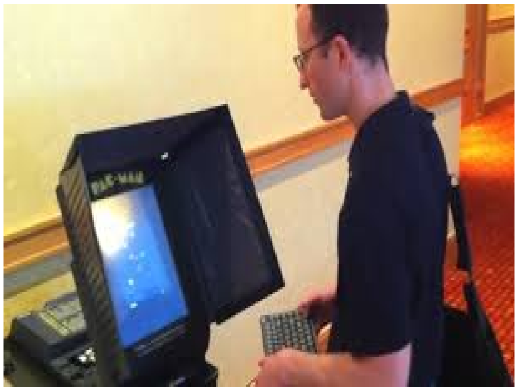
Voting with double ballots

Candidate	Vote-code	Receipt
Alice	AAAA-1111	REC1
Bob	BBBB-2222	REC2
Charlie	CCCC-3333	REC3
David	DDDD-4444	REC4

Ballot No.100(A)

Candidate	Vote-code	Receipt
Alice	EEEE-5555	REC5
Bob	FFFF-6666	REC6
Charlie	GGGG-7777	REC7
David	HHHH-8888	REC8

Ballot No.100(B)



No. 100
AAAA-1111
Open (B)

Election Authority

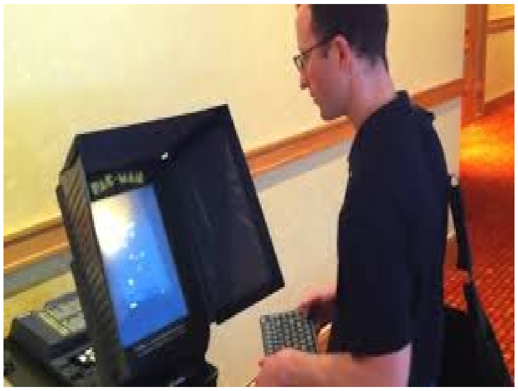
Voting with double ballots

Candidate	Vote-code	Receipt
Alice	AAAA-1111	REC1
Bob	BBBB-2222	REC2
Charlie	CCCC-3333	REC3
David	DDDD-4444	REC4

Ballot No.100(A)

Candidate	Vote-code	Receipt
Alice	EEEE-5555	REC5
Bob	FFFF-6666	REC6
Charlie	GGGG-7777	REC7
David	HHHH-8888	REC8

Ballot No.100(B)



Election Authority

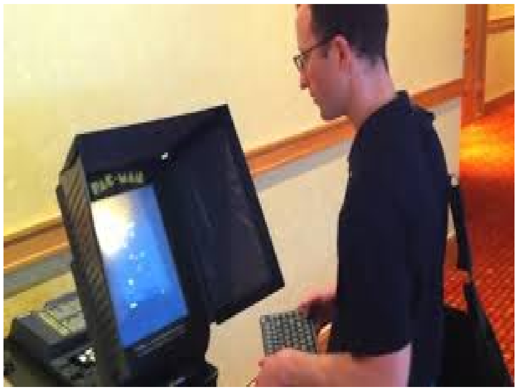
Voting with double ballots

Candidate	Vote-code	Receipt
Alice	AAAA-1111	REC1
Bob	BBBB-2222	REC2
Charlie	CCCC-3333	REC3
David	DDDD-4444	REC4

Ballot No.100(A)

Candidate	Vote-code	Receipt
Alice	EEEE-5555	REC5
Bob	FFFF-6666	REC6
Charlie	GGGG-7777	REC7
David	HHHH-8888	REC8

Ballot No.100(B)



REC1

Election Authority

What we gain by using double ballots

Privacy preservation:

- The only information that the voter keeps from the used ballot is the vote-code she submitted.
- Opening the whole information of the unused ballot does not reveal how the voter has voted.

What we gain by using double ballots

Privacy preservation:

- The only information that the voter keeps from the used ballot is the vote-code she submitted.
- Opening the whole information of the unused ballot does not reveal how the voter has voted.

Integrity:

- The EA cannot know in advance which side the voter is going to use, so any malicious behaviour will be detected with probability $1/2$ by the voter.
- If the EA attempts to alter t ballots, it will be caught with probability $1-(1/2)^t$.
- Assuming a large enough number of voters, we verify that almost all votes have been counted correctly with high probability.

Is this enough?

Is this enough?

1. The voters cannot be sure that the EA has not committed to a different vote-code and candidate correspondence at setup.
2. The commitment scheme is hiding, so the EA could create commitments to multiple votes (e.g. $\mathrm{Com}(1000 \cdot \langle \mathrm{Alice} \rangle)$) without being detected.

Is this enough?

1. The voters cannot be sure that the EA has not committed to a different vote-code and candidate correspondence at setup.
2. The commitment scheme is hiding, so the EA could create commitments to multiple votes (e.g. $\mathrm{Com}(1000 \cdot \langle \mathrm{Alice} \rangle)$) without being detected.

By injecting 1000 votes for Alice, EA could change the result significantly with 50% probability (the invalid encoding is not in the side of the ballot used for audit).

Fixing the last weakness

1. The voters can verify that the EA has not committed to a different vote-code and candidate correspondence at setup.
2. Anyone can verify that the commitments correspond to well-formed ballots, i.e. one commitment per (encoded) candidate in every side of all ballots.

Fixing the last weakness

- We construct novel **ZK proofs** for ballot correctness.

Fixing the last weakness

- We construct novel **ZK proofs** for ballot correctness.
- This is the final tool needed for E2E verifiability (no multiple vote injection, so correct counting of almost every vote implies negligible error from the actual result).

Fixing the last weakness

- We construct novel **ZK proofs** for ballot correctness.
- This is the final tool needed for E2E verifiability (no multiple vote injection, so correct counting of almost every vote implies negligible error from the actual result).
- ZK soundness requires a source of true randomness that could come from an external source (assuming a random oracle or a randomness beacon) but...

Fixing the last weakness

- We construct novel **ZK proofs** for ballot correctness.
- This is the final tool needed for E2E verifiability (no multiple vote injection, so correct counting of almost every vote implies negligible error from the actual result).
- ZK soundness requires a source of true randomness that could come from an external source (assuming a random oracle or a randomness beacon) but...
- We promised E2E verifiability in the standard model **for the first time**.

ZK soundness via human interaction

- When an honest voter chooses which side (A or B) she will use to vote, she concurrently inserts **1 bit of randomness** in the system by flipping a coin. This bit is public and cannot be altered by a malicious EA without being detected.

ZK soundness via human interaction

- When an honest voter chooses which side (A or B) she will use to vote, she concurrently inserts **1 bit of randomness** in the system by flipping a coin. This bit is public and cannot be altered by a malicious EA without being detected.
- Assuming that a small fraction of the voters are not corrupted and vote successfully, we can extract true randomness from the voters' choice and apply it to the verification of the ZK proofs.

Overview of the construction of Demos

1. We generate code-based ballots for a private and simple voting procedure from the voters' side.
2. We associate the vote-codes with receipts, so that the voters are sure that their vote was accepted by the system.
3. We introduce a public BB, that contains all necessary audit information, consistently committed by the EA.
4. We provide the voters with double ballots, so that they can choose one side of the ballot to vote and the other to audit the election without revealing their votes.
5. We use the voters' coin flips to extract true randomness for the ZK proofs, thus maintening Demos E2E verifiable in the standard model.

Activities of the FINER research team:

Implementation of Demos and the European Elections 2014 experiment

The FINER research team members

Professors:

Alex Delis (DI&T), Aggelos Kiayias (DI&T), Charalampos Koutalakis (DPS&PA), Elias Nikolakopoulos (DPS&PA), Mema Roussopoulou (DI&T), Georgios Sotirellis (DPS&PA)

Postdoctoral researchers:

Foteini Baldimtsi (DI&T), Pavlos Vasilopoulos (DPS&PA), Bingsheng Zhang (DI&T)

PhD students:

Konstadina Gavatha (DPS&PA), Lampros Paschos (DPS&PA), Thomas Zacharias (DI&T)

The FINER project is funded by the General Secretariat of Research and Technology of Greece (2013-15).

Implementation of Demos by **Bingsheng Zhang**

- The server is implemented in *Django*.
- We implement Elliptic Curve ElGamal using the fastest elliptic curve crypto library *MIRACL*.
- We support ballot distribution in three ways: via CAS, paper or email.

The European Elections 2014 experiment

The European Elections 2014 experiment

- Two groups performed parallel pilot runs of Demos into two different polling places (Ilioupoli & Chalandri).
- The goal of the experiment was (i) to get the voters familiar with Demos and (ii) test the current implementation.
- The participants (747 in total) were issued paper ballots (one side of the double ballot was printed in one side of the paper) that contained a QR code in each side.
- The QR codes were scanned by the cameras of the tablets (two for each station) and the participants were prompted in a user-friendly (web page) environment to vote.
- After voting, the participants filled in a questionnaire.

The European Elections 2014 experiment

- A paper with the analysis of the results of the experiment under the title:
  "*Pressing the Button for European Elections 2014: Public Attitudes towards Verifiable E-Voting In Greece*"
  is accepted at the upcoming EVOTE2014 conference.
- The above paper and the election result of our experiment can be found in our website:

$$http://www.demos-voting.com$$

Thank you!

Towards unconditionally E2E verifiable elections: the making of Demos remote e-voting system

Aggelos Kiayias, **Thomas Zacharias** & Bingsheng Zhang

Crypto.Sec Group
Department of Informatics and Telecommunications
University of Athens

4th Crypto.Sec Day
July 17, 2014