Encrypting the Foundation of Democracy

Ayal Pierce
Ayal.Pierce@tufts.edu
Professor Benjamin Hescott

Abstract

Elections are always a mess in the United States. From hanging chads to miscounts and recounts, there always seems to be issues with choosing our leaders. Even though America wants to move towards electronic voting, there is still a need for a paper trail, should discrepancies arise. Another problem arises with the lack of ability to verify ones vote. There is no way to know if your vote was counted, or if it was counted correctly. The answer to all these problems: homomorphic encryption, specifically pallier public key encryption. The basis of a homomorphic encryption allows each vote to be encrypted, all the encrypted votes to be counted, and the sum decrypted to yield the same result if an encryption was not performed. The ballots themselves are simple: the sides with the plaintext names can be discarded with the encrypted side scanned and posted publically for the individual to verify his direct vote was counted. This system allows efficient electronic voting, a verifiable paper trail, and minimizes the ability for human election tampering. Less is more.

Introduction

Hanging chads, coercion, miscounts, and ballot stuffing are just some of the keywords heard surrounding controversial elections. Technology is evolving but the technology of voting is struggling to keep up. There is a need for a secure voting system that has the speed of electronic voting yet the verifiability and anonymity of paper ballots.

Homomorphic encryption allows specific operations on a ciphertext, as if those same operations were being performed on the plaintext, allowing a third party to manipulate data correctly, without knowing the decrypted version of that data. Although commonly used in cloud

computing, homomorphic encryption can also be applied to voting systems, eliminating numerous vulnerabilities and attacks on currently employed election systems while maintain an easy to use, verifiable voting scheme.

1.0 To the Community: Why care about voting?

Voting is the foundation of a democracy. Whether referendums that affect the lives of thousands, or electing leaders, that affect the lives of millions, the integrity of the system that people use to vote is vital in preserving democracy. The United States' history is not new to election controversy. In the presidential election of 1876, civil war nearly broke out when Rutherford Hayes and Samuel Tilden both declared victory. One of the numerous electoral disputes surrounding the election was that Tilden had been declared the winner of three southern states, when Democratic votes were disqualified for a "misleading illustrated ballot"[1] (BBC News). A committee of 15 people[2] decided the outcome of the election with the Compromise of 1877.

Sound Familiar? History repeats itself in the 2000 presidential election when George Bush and Al Gore where the margin in Florida (the state that would decide the victor) was so small that Gore was demanding a recount by hand, rather than by machine. Ultimately, the Supreme Court declared the hand recount unconstitutional, thereby declaring George Bush as the newly elected president.

Following the 2000 election, Congress passed the Help America Vote Act (HAVA) of 2002 that, among other election reforms, "help improve state and local administration of federal

[1] To help illiterate voters, Republicans were normally portrayed as a picture of Abraham Lincoln while Democrats used a rooster. On the disqualified ballots, a picture of Abraham Lincoln was allegedly used to portray Democrats.
[2] 5 Members of the Senate, 5 Members of the House of Representatives, and 5 Supreme Court Justices.

elections and authorized funding for state and local governments to expand their use of electronic voting systems." (GAO 1). However, in the 2004 presidential election, more controversies arose; some focusing on the 22.1% of votes casted electronically (Warf 534). In a 2006 congressional election[3], thousands of votes were discounted due to malfunctioning electronic machine, and the winner won by a mere 369 votes (Lee 1).

Most frightening of cases occurred in a small town election in New Jersey. Mr. Zirkle thought he had only 9 votes in his bid for a seat on the Democrat Executive Committee until over 20 people told him they voted for him. After an election official admitted there was a programming error in the system, the court brought in an expert who discovered "key files" had been deleted the day before. A new election declared Mr. Zirkle the winner (Lee 1).

In response to numerous criticisms of electronic voting, California Secretary of State Debra Bowen issued a top-to-bottom review of all electronic voting systems in place for California. The penetration testers employed found that, "all of the voting systems studied contain serious design flaws that have led directly to specific vulnerabilities, which attackers could exploit to affect election outcomes." (Bowen 1). Without knowing the source code of the software, the testers were able to gain root access, allowing them to manipulate every setting on every device in the network (Bowen 2).

With the rapid evolution of technology comes the evolution of hacks and attacks. The current electronic voting system is extremely vulnerable, making our democracy vulnerable. Confusing ballots, hanging chads, and corrupt officials cause a distrust in paper ballots while poorly programmed and irresponsibly designed machines causes a distrust in technology. However, a homomorphic cryptosystem with pret-a-voter ballots allows efficient electronic voting, a verifiable paper trail, and minimizes the ability for human election tampering.

[3] Florida 13th District

2.0 The Ideal Voting System

Accuracy: That the person who wins, is actually the winner.

Usability: The voting system can be used by an average voter, with relative ease. Additionally, election officials should be able to administer the ballots and ensure proper elections with relative ease.

Individual Verifiability: A voter can ensure, with confidence, that his or her vote was, indeed, counted; essentially a personal receipt without compromising privacy (see below).

Universal Verifiability: Any person can verify the outcome of the election. Essentially, there should be a *paper trail*, should a recount occur.

Voter Privacy: A person's vote should be private, assuming the voter does not wish to reveal his or her vote. Additionally, the casted vote should not be able to be traced back to any specific person, ensuring coercion free voting.

Receipt-freeness, introduced by Benaloh and Tunistra [ ], goes further to ensure that any voter cannot prove his vote, even if he wanted to. Receipt-freeness ensures that a voter cannot be coerced, since he or she cannot prove their vote to the coercer, and deters votes being bought, again since there is no way to prove a specific vote for or against.

3.0 Problems with current voting systems.

Problems with Accuracy: As shown with the case of Mr. Zirkle, elections are not always accurate.

Individual Verifiability: This is considerably lacking in both paper and electronic ballots. There is no widely used system in place that allows a voter to ensure, with confidence, that their vote has been cast, let alone whether the correct vote has been cast.

Universal Verifiability: Recounts are possible with a paper trail. Simply because a paper trail exists, does not mean that an official recount will always occur, as shown in Florida in the 2000 U.S. Presidential election. Currently, universal verifiability relies on the trust of election officials. True universal verifiability eliminates the need of trusting a specific subset of society and allows any voter to verify the outcome of the election. Additionally, numerous electronic voting systems do not have a paper trail.

Voter Privacy: Current systems are quite good with voter privacy. However in order to maintain privacy, individual and universal verifiability is sacrificed.

4.0 New Proposed System

4.1 Homomorphic Encryption

Homomorphic encryption allows specific operations on a ciphertext, as if those same operations were being performed on the plaintext, allowing a third party to manipulate data correctly, without knowing the decrypted version of that data. For example:

Additive Homomorphism: $Enc_N(m_1) + Enc_N(m_2) = Enc_N(m_1 + m_2)$

Multiplicative Homomorphism: $Enc_N(m_1) \cdot Enc_N(m_2) = Enc_N(m_1 \cdot m_2)$

In the case of voting, however, since the goal is to tally the votes to determine the winner, we only an additive homomorphic encryption scheme

4.2 Pallier Cryptosystem

In 2009, Craig Gentry, in his Ph.D. thesis introduced the first fully homomorphic cryptosystem. Although full homomorphism would be very useful in cloud computing, where arbitrary operations need to be performed on encrypted data, in terms of voting, fully homomorphism is not necessary.

The widely used RSA cryptosystem is also not applicable for vote tallying because it is multiplicatively homomorphic, and when dealing with binary[4], multiplicative homomorphism does not apply. Therefore the Pallier cryptosystem, with its additive homomorphism by ciphertext multiplication, would be best for electronic vote tallying.

1. $n = p \cdot q$ Generate an integer, *n,* from multiplying two large prime numbers, p and q:
2. Calculate $\lambda = lcm(p-1, q-1)$
3. Using a random integer $g \in Z^*_{n^2}$, where g ≡ 1 mod n
4. Calculate μ = modular multiplicative inverse of n and g
5. The encryption key is (n,g) and the decryption key is (λ,μ).

Encryption of a message *m* where $m \in Z_n$

1. Select a random $r \in Z^*_n$
2. Ciphertext, c = $g^m \cdot r^n \ mod \ n^2$

Decryption of ciphertext, c

1. Let L(x) = $\frac{x-1}{n}$
2. Message = $\frac{L(C^\lambda \ mod \ n^2)}{L(g^\lambda \ mod \ n^2)} \ mod \ n$

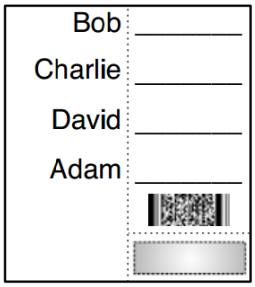
Pallier's homomorphic property is defined as: $Dec(Enc_N(m_1) \cdot Enc_N(m_2)) = m_1 + m_2$

4.3 Prêt a Voter ballot

One of the biggest downfalls in current voting schemes is the compromise of verifiability for privacy. The beauty of using encryption, though, is the ability to have both. Adida and Rivest first proposed the use of a Prêt a Voter paper ballot in *Scratch and Vote* (Adida and Rivest). The paper ballot is perforated down the middle. On the lefts is the list of candidates in a randomized order. On the right is a place to mark a choice for a candidate. Additionally on the right side of

[4] A vote for (1) or a vote against (0).

the ballot contains a barcode, with the encrypted ordering of the candidates. Once a voter casts a ballot, they will detach and discard of the left half, leaving their choice on the right side, encrypted to all.



Courtesy of Rivest et. al.

4.4 Auditing

The use of a scratch surface, similar to those used in lottery tickets, can be used to ensure the validity of ballots. The following auditing process can be performed by the voter themselves, or by an election official.

Scratching off the surface will reveal the plaintext ordering of the candidates. One can then encrypt the revealed ordering and see that it matches the encrypted version in the barcode. Any ballot with a removed scratch surface will be void, since the ordering of the candidates is no longer private.

Although the auditing process can only prove the legality of the now void ballot, the more ballots that are audited and validated, the more likely the cast ballots will also be true. It is highly improbable that all the randomly audited ballots will be secure while the used ballots will be tampered with.

4.5 The “Bulletin Board”

Since the voter has discarded of the plaintext ordering of the candidates, their encrypted vote can be publicly available on a virtual *bulletin board*. This allows the individual voter to ensure that their vote was counted, and that their vote was counted correctly. It also creates universal verifiability, as any individual can simply tally the votes and ensure the correct candidate was chosen. Having a public *bulletin board* eliminates the current system of trusting election officials to tally the votes and even trusting those same officials to perform a recount.

4.6 Proposed System vs. Ideal System

Accuracy: The winner in the system is guaranteed to win. Any votes or tallies that could potentially be altered would be caught through the individual verifiability.

Individual Verifiability: Unlike any modern voting systems, the proposed system allows individual voters to look on the bulletin board to see that their vote was counted and counted correctly. In case of an issue, the voter has the encrypted receipt to prove that the vote was not counted correctly.

Universal Verifiability: Since the bulletin board’s data is publically available, the tally is verifiable by any individual, official, or political group.

Voter Privacy: With a securely encrypted randomized candidate ordering, and with the scratch off portion of ballot discarded, a voter cannot prove who he or she voted for, even if he or she wanted to.

6.0 Considerations and limitations

6.1 Write-In Candidates

The proposed system does not account for *write in* candidates, where a voter chooses to cast a ballot for a custom candidate, rather than choose one of the named candidates on the ballot. One possible solution to the problem is to always have one of the randomized candidates be "Write In." A voter will then vote for the "Write In" candidate, like any other and cast their custom ballot separately. The only problem is the issue of privacy. Although actual choice remains private, the fact that a voter will be casting a *write in* ballot may become public knowledge.

It would not, however, open a voter up to coercion or vote-buying, since it is still receipt free. If a coercer would require a candidate choose the write in option, that voter could simply write one of the regular candidates in the choice, keeping the integrity of the vote.

6.2 Security of the Bulletin Board

There would have to be proper security measures in place so an attacker could not alter the data on the *bulletin board*. This possible vulnerability is still better than the lack of security in current electronic voting machines; ones that are insecurely stored in public places, like basements of churches, and are susceptible to attacks.

One way to mitigate attacks on the *bulletin board* is the distribution or responsibility among the citizens to verify their votes. That the *bulletin board* data is completely public, allows stratified verifiability. Citizens, after leaving the polling station, should receive an informational pamphlet on how to access the Bulletin Board and verify their vote. By allowing the bulletin board could be to group the votes as small as by municipality, more people will be inclined to

tally and universally verify the declared winner of their municipality or county. Additionally, active political groups will also be inclined to verify the election on a larger scale. By instilling a sense of social responsibility onto the population, should the data on the Bulletin Board be manipulated, it will be caught quickly.

7.0 Conclusion

An ideal voting system is accurate, verifiable, and private. The winner of an election should win, a voter should be confident that his vote was counted, and votes should be private. In an attempt to alleviate the problems of paper ballots, a move to electronic voting was attempted. However, there are rampant bugs and security flaws in current e-voting systems.

Using an additive homomorphic cryptosystem, such as the Pallier Cryptosystem, allows individual voters to verify their vote and anybody to verify the outcome of the election without compromising individual voter privacy. Through paper based Prêt a Voter ballots with a randomized candidate ordering encrypted using the Pallier Cryptosystem, elections can be accurate and verifiable without compromising voter privacy.

Prezi Presentation: tinyurl.com/homomorphic-voting

Works Cited

Adida, B., Rivest, R.L.: Scratch and Vote: Self-Contained Paper-Based Cryptographic Voting. In: WPES 2006. Proceedings of the 5th ACM workshop on Privacy in electronic society, pp.29-40. ACM Press, New York (2206).

"Flashback to 1876: History repeats itself" (http://news.bbc.co.uk/1/hi/ world/americas/1066014. stm). *BBC News*. London. December 12 2000. . Retrieved 2013-12-1.

United States. Government Accountability Office (GAO). N.p., Sept. 2005. Web. 1 Dec. 2013. <http://www.gao.gov/new.items/d05956.pdf>.

United States. State of California. Office Secretary State. *California Secretary of State*. By Debra Bowen. N.p., 25 Oct. 2007. Web. 1 Dec. 2013. <http://www.sos.ca.gov/voting-systems/oversight/ttbr/diebold-102507.pdf>.

Lee, Timothy B. "Paper Prophets: Why E-voting Is on the Decline in the United States." *Ars Technica*. N.p., 22 Oct. 2012. Web. 1 Dec. 2013. <http://arstechnica.com/features/2012/10/paper-prophets-why-e-voting-is-on-the-decline-in-the-united-states/>.

Warf, B (2006), "Voting technologies and residual ballots in the 2000 and 2004 presidential elections", *Political Geography* **25** (5): 530-556,