Can End-to-End Verifiable E-Voting be Explained Easily?

Peter Kalchgruber
Vienna University of Technology
Favoritenstr. 9–11
Vienna, Austria

Edgar R. Weippl
Secure Business Austria
Favoritenstr. 16
Vienna, Austria
weippl@securityresearch.at

ABSTRACT

E-Voting is a widely discussed topic—both in the public and in research. In the last couple of years new voting protocols have been proposed. The contribution of this paper is to explain the fundamental concepts of Ben Adida's Scratch & Vote, show an implementation we made and report on the "user" (i.e. voter) experience of a handful of technically knowledgeable voters. All voters were students and they were given an introduction to the concept and could vote which coffee the institute should buy. We explored whether they would be convinced that end-to-end auditable protocols were an improvement to "normal" voting machine typically used in the US.

Categories and Subject Descriptors

H.4 [**Information Systems Applications**]: Miscellaneous; D.2.8 [**Software Engineering**]: Metrics—*complexity measures, performance measures*

General Terms

Delphi theory

Keywords

ACM proceedings, LaTeX, text tagging

1. INTRODUCTION

Electronic Voting (E-Voting) is a recently developed technology in the most fundamental area of democracy: elections. With the first "in-vivo" runs behind us, it is appropriate to consider the advantages and disadvantages of the system. This paper explores the basics of well-known e-voting systems and their detailed working-out. The focus is on end-to-end auditable voting systems. These systems offer the voter the opportunity to prove the correct counting of the vote, and to track and verify the ballot. Furthermore the system protects confidentiality of votes and helps to avoid manipulation by coercer. In order to improve transparency in elections, end-to-end auditable voting systems can both be implemented at presence in personal and internet voting systems. The practical part includes consideration of the implementation of the end-to-end auditable election system Scratch & Vote, by Ben Adida, supplemented by a threshold decryption scheme. All knowledge necessary for the implementation of such a voting system will be provided in clearly comprehensible terms illustrated by a number of practical examples so that participants in the case study could understand how end-to-end verifiable e-voting works.

iiWAS2009 , December 14-16, 2009, Kuala Lumpur, Malaysia

2. E-VOTING

E-government encompasses many different aspects such as e-administration, e-participation, and e-justice. The European Commision [8] sees in e-government the use of information- and communication technology as the medium of communication for governmental business processes. Schubert [21] includes legal aspects in his definition

> "E-Government includes the governmental task of setting a valid legal framework for the effective use of the electronic media in a society as well as the application of these media for public procurement, services to companies and citizens and the management of the internal organization. "[22]

The goals of e-government are defined as follows [22]:

- Endowing the economy with the necessary legal framework ("making E-Business possible")
- Applying it cost-effectively for governmental tasks.

For democratic governments voting is an essential business process. When moving to "e-business" it seems obvious that e-voting should receive some attention.

> "E-Democracy is the use of information and communications technologies and strategies by 'democratic sectors' within the political processes of local communities, states/regions, nations and on the global stage." [5]

3. END-TO-END SYSTEMS

Michael Shamos published the fundamental requirements for electronic voting. [12]

1. Thou shalt keep each voter's choices an inviolable secret.

2. Thou shalt allow each eligible voter to vote only once, and only for those offices for which she is authorized to cast a vote.
3. Thou shalt not permit tampering with thy voting system, nor the exchange of gold for votes.
4. Thou shalt report all votes accurately.
5. Thy voting system shall remain operable throughout each election.
6. Thou shalt keep an audit trail to detect sins against Commandments II-IV, but thy audit trail shall not violate Commandment I

The voter should therefore be able to verify his vote on the list of results, which is one requirement of open-audit voting. "We are at the stage where we need to try many different techniques for open-audit voting, and we just don't know what's going to work better in a real-world setting" [9]. Ben Adida [11] concisely summarizes the main challenges:

1. Alice verifies her vote.
2. Everyone verifies tallying.
3. Alice cannot be coerced by Eve.

4. SCRATCH & VOTE

> "It is pretty advanced, and people believe because it's advanced, it can't be a good system, because a good voting system needs to be understandable by everybody and so on and so forth." [11]

Scratch & Vote was presented first in 2006 [2]. The major difference to other systems is that the system can be explained easily and cryptography can be used to create elections that are publicly auditable [11, 16].

> "This system is meant for pedagogical use. It is meant to explain how you can do this things in the real world. It does have certain practical weaknesses." [11]

Scratch & Vote builds on paper-based systems of David Chaum and Peter Ryan [20, 10] and combines it with multi-candidate-technology [3].

Ballot.

A ballot (Figures in Appendix C) consists of three parts that can be torn off separately. On the left side the candidates are listed in a random order. On the right side there is a field where the vote can be cast and an extra bar code that encodes a verification code. This verification code is below a sealed field; if scratched open it can be used to check for fraud using a zero-knowledge protocol.

Bulletin Board.

The Bulletin Board is a central component of Scratch & Vote. It is an information platform that is publicly accessible that shows both the names of the people who have voted and their encrypted ballot. Having the names of made public helps to detect some kinds of fraud such as dead people voting. The more people that check this board the less likely fraud becomes [14, 19].

Since all the encrypted votes are published everybody can check the tally by adding all the (encrypted) votes. Integrity of the board is important and Ben Adida [1] suggests following safeguards:

- Digital signatures of all posted data.
- Distributed byzantine agreements [15]
- Hash-Trees and cryptographic signatures on redundant servers.

4.1 Multi-Candidate

Baudron [3] describes a simple and yet effective schema to add (encrypted) votes based on a multi-candidate-approach. The basic idea is to add the votes of each candidate individually. Below are three counters that count the votes for three candidates. The length of this bit array is determined by the number of candidates and the maximum number of votes each candidate may receive.

```
0000000111110100  1010110011100011  0001010100100010
```

For the example, we assume following parameters:

b . . .Number of voters
w . . .Number of candidates

Determine a M so that: $2^M > b$
To vote for candidate j ($j \in [1, w]$) following cyphertext needs to be calculated:

$$c = Enc_{pk}(2^{(j-1)M})$$

Each counter can thus store 2^{M-1} votes. If the number of votes for a candidate exceeds this number, the votes would be counted for the wrong candidate.

4.2 Pallier-Encryption

For Scratch & Vote two encryption algorithms can be used: (1) Elgamal encryption [6] or (2) Pallier encryption [17] gewählt werden. The Pallier schema is based on residuosity problems (such as cryptosystems. Pallier states [18]:

> "The trapdoor in these schemes combines the extraction of residuosity classes over certain groups with the intractability of computing their order. Because residuosity classes are additive, such cryptosystems look like discrete-log based ones, but the trapdoor is closer in nature to those for factoring-based systems"

4.2.1 Calculation

One choses two prime numbers p, q and computes $n = pq$. Now the Euler function has to be computed φ-Funktion $\varphi(n)$. The result of this function is the number of natural numbers between 0 and n that have no common denominator with n. For example: $\varphi(6) = 2$. In $\mathbb{N}_6 = \{1, 2, 3, 4, 5, 6\}$ only the numbers 1 and 5 have no common denominator with 6.

Since prime numbers cannot be factored, φ of a prime is $\varphi(p) = p-1$. For example: $\varphi(7) = 6$. $\varphi(n)$ can be calculated as $\varphi(n) = \varphi(p) \cdot \varphi(q) = (p-1) \cdot (q-1)$. $\varphi(n)$ thus determines the cardinality of $\mathbb{Z}^*$.

Using the Carmichael function one calculates $\lambda(n)$. Since n is the product of two primes following is true: $\lambda(n) = \lambda(p) \cdot \lambda(q)$.

$\lambda(n)$ can be computed as follows: $\lambda(n) = \lambda(p) \cdot \lambda(q) = kgV(\varphi(p-1), \varphi(q-1)) = kgV(p-1, q-1)$

4.2.2 Homomorphic Properties

The entire concept of Scratch & Vote relies on the homomorphic properties of the cryptosystem. Pallier-encryption is homomorphic so that [17]

$$\forall m1, m2 \in \mathbb{Z}_n \text{ and } k \in \mathbb{N}$$
$$D(E(m_1)E(m_2) \pmod{n^2}) = m_1 + m_2 \pmod{n}$$
$$D(E(m)^k \pmod{n^2}) = km \pmod{n}$$
$$D(E(m_1)g_2^m \pmod{n^2}) = m_1 + m_2 \pmod{n}$$
$$D(E(m_1)_2^m \pmod{n^2}) = m_1 m_2 \pmod{n}$$
$$D(E(m_2)_1^m \pmod{n^2}) = m_1 m_2 \pmod{n}$$

The homomorphic properties of the addition are used to add the votes while each ballot remains encrypted.

5. CASE STUDY

The research question was: Can people with an advanced technical education understand the Scratch & Vote system easily in regard to the security benefit compared to "normal" voting machines? Students that participated had some knowledge in IT security and had recently worked on software projects that included the implementation of access control [7] and had worked on Web application security [13]. Judging from interviews conducted with students, there is obviously a lot of distrust toward e-voting systems.

While the authors see both weaknesses and strengths of e-voting, we are convinced that end-to-end verifiable e-voting is superior to voting machines used today. Paper-based ballots do not need to be replaces by e-voting; if they are, however, we strongly feel that an end-to-end verifiable protocol—not necessarily Scratch & Vote—should be used.

We used the system in two settings to observe how easy such a system is to use. In the first setting students with a lot of IT security background were given a 20-minute explanation of Scratch & Vote as described in the previous sections of this paper; they could then vote with the software depicted in the figures in Appendix C.

The second setting involved a class with 20 students who had some basic IT security knowledge. Again, they were given the same explanation and asked whether they trusted the voting process.

The main finding of this first limited assessment is that students are very critical about e-voting and the second group remained so after the first explanation. Only when they understood the complex concepts fully, they think that end-to-end auditable protocols are a good way of improving e-voting.

It seems that students are more skeptical about e-voting than the general population [4]; however, once they understood end-to-end verifiable protocols they also trusted the software implementation we provided; to be more specific: They understood that there is no need to trust any application since all results can be independently verified. The example calculation provided in the appendix proved to be an invaluable tool to explain the "magic" of homomorphic cryptosystems. Obviously, the big challenge for the adaption of such systems for general elections is to educate the public about the differences between non-verifiable systems and end-to-end verifiable solutions.

The major weakness of end-to-end verifiable e-voting for general elections is that elections require voters to trust the system. People usually trust elections only if they can understand the process. This is the beauty of paper-based election systems; an easy-to-understand 5-minute explanation suffices. This is also why people mistrust proprietary solutions such as voting machines by Premier Elections Systems (formerly Diebold). The goal of this study was to show that a lot of education is required to understand the difference between non- (or partially-) auditable systems and end-to-end verifiable e-voting.

6. REFERENCES

[1] B. Adida. *Advances in cryptographic voting systems.* PhD thesis, Massachusetts Institute of Technology, Cambridge, MA, USA, 2006. Adviser-Rivest,, Ronald L.

[2] B. Adida and R. L. Rivest. Scratch & vote: self-contained paper-based cryptographic voting. In *WPES '06: Proceedings of the 5th ACM workshop on Privacy in electronic society*, pages 29–40, New York, NY, USA, 2006. ACM.

[3] O. Baudron, P.-A. Fouque, D. Pointcheval, J. Stern, and G. Poupard. Practical multi-candidate election system. In *PODC '01: Proceedings of the twentieth annual ACM symposium on Principles of distributed computing*, pages 274–283, New York, NY, USA, 2001. ACM.

[4] T. Buchsbaum. E-voting: International developments and lessons learnt. In *Proceedings of Electronic voting in Europe - technology, law, politics and society, workshop of the ESF TED programme together with GI and OCG*, pages 31–42, 2004. `http://www.e-voting.cc/static/evoting/files/buchsbaum_p31-42.pdf`.

[5] S. Clift. E-democracy, e-governance and public net-work. In B. Lutterbeck and R. A. Gehring, editors, *Open Source Jahrbuch 2004 – Zwischen Softwareentwicklung und Gesellschaftsmodell.* Lehmanns Media, Berlin, 2004.

[6] T. Elgamal. A public key cryptosystem and a signature scheme based on discrete logarithms. *Information Theory, IEEE Transactions on*, 31(4):469–472, Jul 1985.

[7] W. Essmayr, S. Probst, and E. Weippl. Role-based access controls: Status, dissemination, and prospects for generic security mechanisms. *International Journal of Electronic Commerce Research*, 4(1):127–156, 2004.

[8] European Commission. The role of e-government in europe's future. *IWAYS*, 26(4):168–170, 2003.

[9] C. Farivar. Clean elections. *Commun. ACM*, 51(10):16–18, 2008.

[10] K. Fisher, R. Carback, and A. Sherman. Punchscan: Introduction and system definition of a high-integrity election system. In *Proceedings of the IAVoSS Workshop On Trustworthy Elections (WOTE'06), Cambridge, UK*, 2006.

[11] The Florida Senate. *Statutes & Constitution*, 2008. `http://www.flsenate.gov/statutes/`.

[12] heise.com. *Wähler-Selbstkontrolle*, May 2007. `http://www.heise.de/ct/Wenig-Vertrauen-in-Wahlmaschinen--/artikel/126221`.

[13] K.-I. Ismail, E. Weippl, W. Winiwarter, and S. Wieland. Web engineering for intranets: Rethinking software engineering. In K.-I. Ismail and S. B. W. Schwinger, editors, *Proceedings of Proceedings of the 4th International Conference on Information Integration and Web-based Applications & Services (IIWAS)*, pages 255–260, Indonesia, Sept. 2002. SCS European Publishing House.

[14] C. Karlof, N. Sastry, and D. Wagner. Cryptographic voting protocols: A systems perspective. In *USENIX Security Symposium*, pages 33–50, 2005.

[15] Y. Lindell, A. Lysyanskaya, and T. Rabin. On the composition of authenticated byzantine agreement. *J. ACM*, 53(6):881–917, 2006.

[16] MIT Computer Science and Artificial Intelligence Laboratory. *Ben Adida, Ronald Rivest, Scratch & Vote*, 2006. `http://people.csail.mit.edu/rivest/AdidaRivest-ScratchAndVote-slides.pdf`.

[17] P. Paillier. Public-key cryptosystems based on composite degree residuosity classes. In *EUROCRYPT*, pages 223–238, 1999.

[18] P. Pallier. Composite-Residuosity Based Cryptography: An Overview. *CryptoBytes*, 5(1):20–26, 2002.

[19] R. L. Rivest and W. D. Smith. Three voting protocols: Threeballot, vav, and twin. In *EVT'07: Proceedings of the USENIX Workshop on Accurate Electronic Voting Technology*, pages 16–16, Berkeley, CA, USA, 2007. USENIX Association.

[20] P. Ryan, S. Schneider, P. Ryan, and S. Schneider. Prêt à voter with re-encryption mixes. In *ESORICS*. In European Symposium on Research in Computer Security, number 4189 in Lecture Notes in Computer Science, 2006.

[21] P. Schubert. *Einführung in die E-Business-Begriffswelt*. Hanser Fachbuch, 2000.

[22] P. Schubert and U. Häusler. E-government meets e-business: A portal site for startup companies in switzerland. *Hawaii International Conference on System Sciences*, 5:5005, 2001.

APPENDIX

A. EXAMPLE OF PALLIER ENCRYPTION

$$
\begin{aligned}
p &= 13 \\
q &= 17 \\
n &= 13 \cdot 17 = 221 \\
n^2 &= 221 \cdot 221 = 48841 \\
\lambda(221) &= lcm(\lambda(13), \lambda(17)) = lcm((13-1),(17-1)) \\
&= lcm(12, 16) = 48 \\
r &= 3161 \in \mathbb{Z}^*_{48841} \\
g &= 26171 \in \mathbb{Z}^*_{48841} \\
m &= 133 \in \mathbb{Z}_{221} \text{ (=Message)} \\
c &= g^m \cdot r^n = 26171133 \cdot 3161221 = 7760 \\
&\text{(=Ciphertext)} \\
e &= \frac{L(c^\lambda \pmod{n^2})}{L(g^\lambda \pmod{n^2})} \pmod{n} = \\
e &= \frac{L(7760^{48} \pmod{48841})}{L(26171^{48} \pmod{48841})} \pmod{n} \\
&\equiv 133 \pmod{48841}
\end{aligned}
$$

B. EXAMPLE OF THRESHOLD SCHEME WITH PALLIER

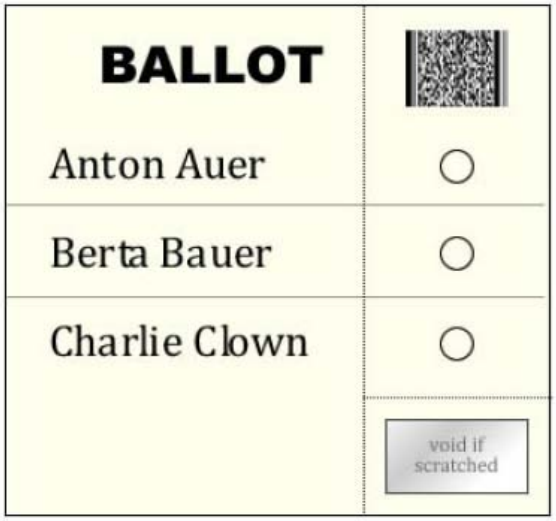
$$
\begin{aligned}
p' &= 3 \\
q' &= 5 \\
p &= (3 \cdot 2) + 1 = 7 \\
q &= (5 \cdot 2) + 1 = 11 \\
n &= p \cdot q = 7 \cdot 11 = 77 \\
n^2 &= 77^2 = 5929 \\
m &= p' \cdot q' = 7 \cdot 3 = 15 \\
\varphi &= (p-1) \cdot (q-1) = (7-1) \cdot (11-1) = 60
\end{aligned}
$$

$$
\begin{aligned}
&gcd(n, \varphi) = 1 \\
&\quad \text{define } \beta, a, b \in \mathbb{Z}^*_n \\
&gcd(n, \beta) = 1 \\
&gcd(n, a) = 1 \\
&gcd(n, b) = 1 \\
&g = (1+n)^a \cdot b^n = 155 \\
&a_0 = SK = \beta m = 60 \\
&a_1 = 3 \\
&a_2 = 5
\end{aligned}
$$

$$f(1) = s_1 = a_0 + 1 \cdot a_1 + 1^2 \cdot a_2 \pmod{n \cdot m} = 68$$
$$f(2) = s_2 = a_0 + 2 \cdot a_1 + 2^2 \cdot a_2 \pmod{n \cdot m} = 86$$
$$f(3) = s_3 = a_0 + 3 \cdot a_1 + 3^2 \cdot a_2 \pmod{n \cdot m} = 114$$
$$f(4) = s_4 = a_0 + 4 \cdot a_1 + 4^2 \cdot a_2 \pmod{n \cdot m} = 152$$
$$\theta_1 = L(g^{m \cdot \beta} \pmod{n}) = 43$$
$$\theta_2 = a \cdot m \cdot \beta \pmod{n} = 43$$

Public Key$(g, n, \theta) = (155, 77, 43)$

$$\Delta = 6$$



Ballot

$msg \ldots$ message

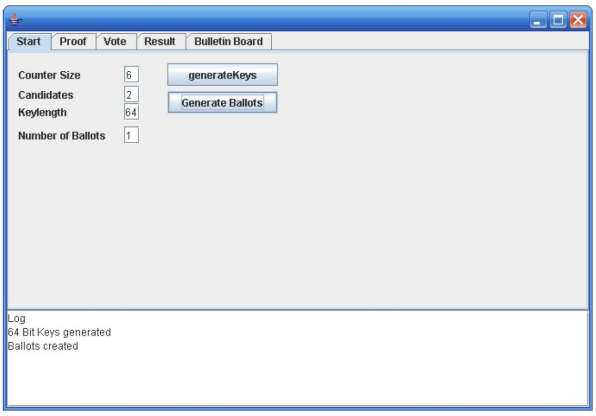
$c \ldots$ ciphertext

$msg = 8$

$$c = g^m sg \cdot x^n \pmod{n^2}$$

$c_1, c_2, c_3, c_4 \ldots$ secret shared keys

$$c_1 = c^{2 \cdot \Delta \cdot s_1} \pmod{n^2} = 3067$$
$$c_2 = c^{2 \cdot \Delta \cdot s_2} \pmod{n^2} = 2325$$
$$c_3 = c^{2 \cdot \Delta \cdot s_3} \pmod{n^2} = 267$$
$$c_4 = c^{2 \cdot \Delta \cdot s_4} \pmod{n^2} = 5615$$
$$\mu_{0,j}^S = \Delta \prod_{j' \in S \setminus \{j\}} \frac{j'}{j' - j} \in \mathbb{Z}$$



Ballot generation

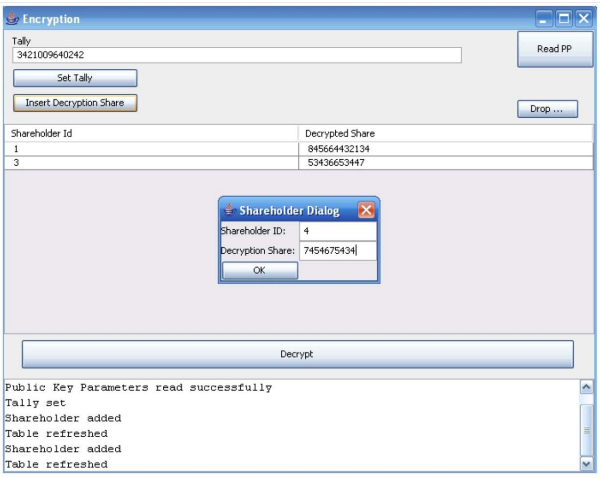
$\overset{S}{1} = 12$

$\overset{S}{2} = 12$

$\overset{S}{3} = 12$

$\overset{S}{4} = 12$

shareholder (1,3,4) used for decryption



Decryption of shares

$$M = L\left(\prod_{j \in S} c_j^{2\mu_{0,j}^S} \pmod{n^2}\right) \frac{1}{4\Delta^2\theta} \pmod{n} M$$

$$= L(1926) \cdot 65 \equiv 8 \pmod{77}$$

C. SCREEN SHOTS OF IMPLEMENTED SYSTEM