HOMOMORPHIC ENCRYPTION IN BALLOT CASTING IN THE ELECTION SYSTEMS

THE MUTUAL INFLUENCES OF TECHNOLOGY ADVANCEMENT, SOCIAL RECOGNITION, AND VOTING IN ELECTIONS

A Thesis Prospectus
In STS 4500
Presented to
The Faculty of the
School of Engineering and Applied Science
University of Virginia
In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science in Computer Science

By
Yufei Zhou

August 5, 2022

On my honor as a University student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments.

ADVISORS

Catherine D. Baritaud and Bryn Seabrook, Department of Engineering and Society

Daniel Graham, School of Engineering and Applied Science

删除了: ↵

In the Declaration of Independence, Thomas Jefferson (1776) wrote, "Governments are instituted among Men, deriving their just Powers from the Consent of the Governed." (para. 2) Ever since the United States was founded, the election system had been the essence of this country. “Elections make a fundamental contribution to democratic governance.” (The Editors of Encyclopaedia Britannica, 2020, Sec. Functions of Elections) The elections give the public right to select who becomes their representatives. The inclusiveness of the parties who are eligible to vote symbolizes the improvement in U.S. social structure and the development of equality in human nature. The concept of equality rooted in U.S. history and the fairness of the elections is an externalization of the values of U.S. citizens. Given the importance of the elections, the standards of the elections have been gradually refined, and improved along with the advancement in technology and social structure. However, nowadays, as cyber threats become more severe, widespread, and harder to detect, which in turn intensifies the distrust of the United States citizens in the result of the elections, the voting system needs to be improved to better defend against foreign attacks during elections and annihilate public’s worry on election results. It is critical to building trust bonds within the community to encourage more voters to vote. And as more voters get involved in the elections, the authority and the representativeness of the elections will be elevated. Therefore, a transparent voting process is urgently needed.

The homomorphic encryption scheme on election results is a feasible solution to address the ends described above. The technical report will elaborate on how the encryption scheme works and how such an encryption scheme can address the technological and societal problems described above. During the 16 weeks of next semester, I will be working with

删除了： is

删除了：

删除了：

删除了： governor

删除了： !?

删除了： that

删除了： punc,

删除了：

删除了： 11

Professor Daniel Graham, the Assistant Professor of Computer Science in the School of Engineering and Applied Science, to establish the code of the encryption scheme. In the tightly coupled STS research paper, I will explore the history of election systems, technological advancement, social structure evolution, and changes in voting methods of elections as a whole to discover their mutual influences and relationships based on the *technological momentum* theory suggested by Thomas P. Hughes (1994). In the article, Hughes (1994) claimed, "…technological momentum infers that social development shapes and is shaped by technology. Momentum also is time dependent." (p. 102) Under different social contexts, the "momentum" between social development and technology interacts with each other in different ways. The STS research paper, will describe and analyze several important milestones of elections throughout the U.S. democracy history: voice voting in the early 1800s; Australian Ballots in the late 1800s; voting machine ballots in the late 1900s; modern voting machine. The research paper will also be accomplished in 16 weeks next semester.

删除了： 分节符(下一页)

删除了： my

删除了： In my

删除了： I plan

删除了： to answer my research question based on

HOMOMORPHIC ENCRYPTION IN BALLOT CASTING IN THE ELECTION SYSTEMS

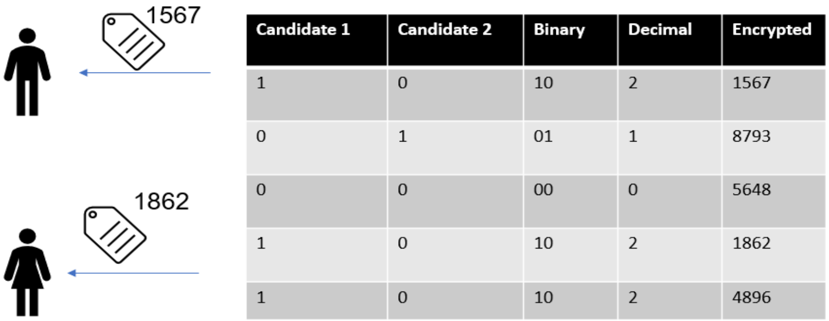
The election system is the most important and fundamental social activity throughout the history of the United States. However, due to the technological explosion in recent years, cybersecurity plays a more and more important role in society. As a result, current election systems have potential vulnerabilities of being attacked by foreign forces. During the 2020 election, two Iranian "stole voter information and engaged in intimidation and disinformation aimed at undermining confidence in the election". (Bracken, 2021) Given this, the public's

删除了： 11

trust in the elections becomes lower and lower because of the opacity of the voting procedure. I seek to provide a solution that can improve the security of the elections and meanwhile, make the voting process transparent to the public.

删除了: 分节符(下一页)

Homomorphic encryption, an encryption method that can maintain the nature of the original text, would be a feasible solution to address the transparency issue of the elections. (TechTarget Contributor, n.d.) The ballots after the encryption can be displayed to the public. And meanwhile, the encryption allows ballot counting institutions to add up the ballots, depending on the actual implementation of the encryption scheme, for the final result in a way that the entire process can be traced and kept in record for reference.



Candidate 1	Candidate 2	Binary	Decimal	Encrypted
1	0	10	2	1567
0	1	01	1	8793
0	0	00	0	5648
1	0	10	2	1862
1	0	10	2	4896

Figure1: A Possible Encryption Result. This figure provides an example of a possible matching of plaintext to cipher text. (Graham, 2022)

删除了: Example of a

删除了: p

删除了: e

删除了:

删除了: Incorrect label

To illustrate the mechanism of the encryption, Figure 1 shows a possible encryption result of ballots generated by a homomorphic encryption scheme. To address the issue that the ballots with the same selection of candidates will be encrypted into the same cipher text, randomness will be introduced.

删除了: 11

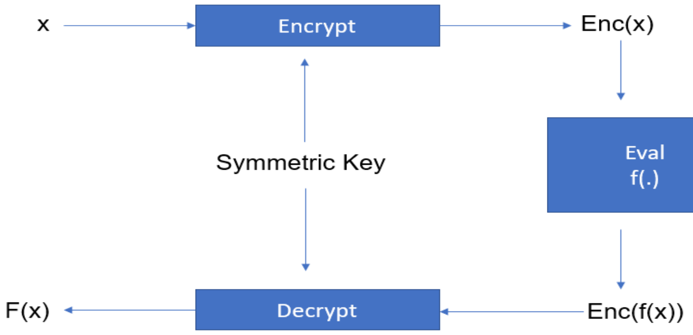


Figure 2: Mechanism of Homomorphic Encryption. This is a flow chart that explains the steps of encryption. (Graham, 2022)

As shown in Figure 2, an evaluation function will be determined. Specifically, in my encryption design, the evaluation function aims to compute the sum of the encrypted ballots. The actual implementation of the evaluation function differs by the encryption schemes. After summing the encrypted ballots, the algorithm will decrypt the cipher text to get the result of the election.

删除了: 分节符(下一页)

The design and the actual implementation of the encryption scheme will be built and tested next semester under the guidance of Daniel Graham, an associate professor of computer science in the School of Engineering and Applied Science at the University of Virginia. I will try different implementations of homomorphic encryption schemes such as RSA, El Gamal Encryption, and Paillier Encryption to search for the best and the most suitable homomorphic encryption scheme to encrypt ballots in the elections.

THE MUTUAL INFLUENCES OF TECHNOLOGY ADVANCEMENT, SOCIAL RECOGNITION, AND VOTING IN ELECTIONS

删除了: 11

Samuel Adams, an American statesman and political philosopher, noted in his essay, "Let each citizen remember at the moment he is offering his vote that he is not making a present or a compliment to please an individual - or at least that he ought not so to do; but that he is executing one of the most solemn trusts in human society for which he is accountable to God and his country." (1781) Since elections are endowed with sacred meaning in U.S. history, their authoritativeness, fairness, and inclusiveness need to be guaranteed to effectively represent the spirit of the United States. Throughout U.S. history, the forms of elections have been modified and improved several times. From voice voting to paper ballots; from paper ballots to voting machines; Every transition in voting methods is a collective consequence of technological advancement, societal structure reformation, and public recognition awakening. These factors mutually influence each other. Therefore, to better estimate the impacts on society regarding the homomorphic encryption ballot casting methods I provided in my technical report, I would analyze the relationship between the factors described above in an election-centered Actor-Network-Theory. (Cressman, 2009)

People's realization on necessary standards regarding elections first prompts the development of technology. For example, people are aware of the importance of accuracy, security, and privacy in the election process, and more voting methods are introduced to address these ends. When new technology is brought into society, the social structure would also change accordingly. As Callon states, "An actor-network is simultaneously an actor whose activity is networking heterogeneous elements and a network that is able to redefine and transform what it is made of." (1987, p.93) Therefore, an election can be deemed as an actor that integrates technology, social recognition, human rights, etc. into a network. The

删除了：????

删除了：分节符(下一页)

删除了：I assume that p

删除了：recognition

删除了：What does this mean?

删除了：In my research topic,

删除了：

删除了：the

删除了：11

actor influences all these factors. Meanwhile, it can also be recognized as a network that can redefine the components within the network. In addition, as technology improves, new technology also is included in the network.

FROM VOICE VOTING TO PAPER BALLOTS

In the early 1800s, voice voting was one of the official voting methods in the elections. Professor J. Alex Halderman (n.d.) from the University of Michigan described the voice voting process in detail:

带格式的：缩进：首行缩进： 0.74 厘米，行距：2 倍行距

删除了：↵

> The voter is going to call out the candidate he wants to vote for and those are going to be announced loudly enough for everyone standing around to hear especially for the clerks sitting in the background to hear and they're going to write down on a sheet of paper the voter’s name and his choice. [Video transcript]

It is notable that this voting method is inaccurate and lacks confidentiality. The voting process is not rigid enough to establish the authority of the elections. For example, the votes from the voters may be ignored or misheard because of the noises in the voting scene. Also, there is no record of the actual choice of the voters. If there is a dispute regarding the result, evidence can neither support the winner nor the loser. So, the process is susceptible to objective factors. Therefore, a transition from voice voting to paper ballots took place in the late 1800s.

As society realized the importance of keeping records during the voting process, paper ballots were introduced. The awakening in social recognition prompted the development of technology. As depicted in Figure 3, a ballot jar was designed to store votes from voters. The jar

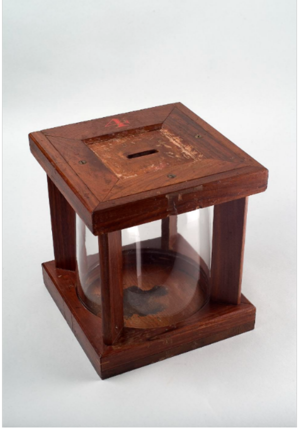
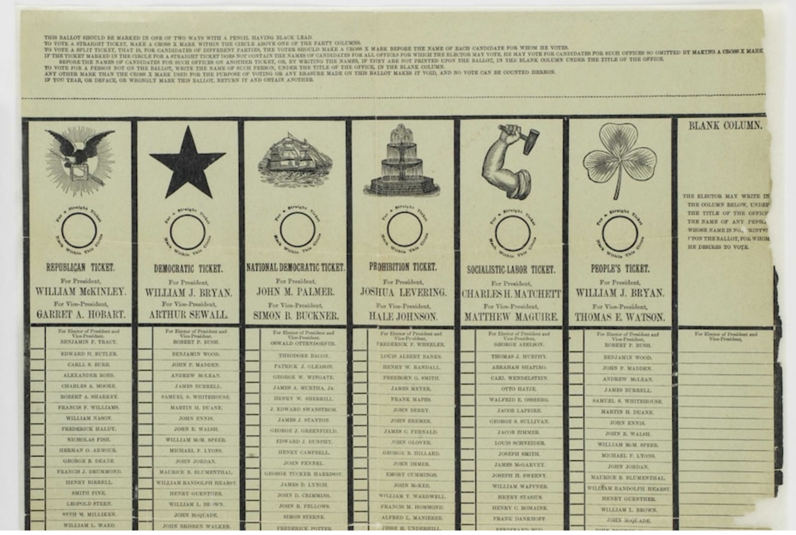


Figure 3: Glass Ballot Jar. This is a glass ballot jar with a lockable wooden housing.(National Museum of American History, n.d.)

删除了：11

was made transparent to show voters that no alteration would be made during the voting process. In ANT, the public's need for accuracy can be deemed as an actor in the network, and the paper ballots are then incorporated into the network. The paper ballots addressed the issue of inaccuracy in vote counting, but the privacy of voters still remained a problem: through the transparent jar, everyone could see others' votes. To further improve the integrity of the election process, Australian Ballots were first introduced in 1892.



THIS BALLOT SHOULD BE MARKED IN ONE OF TWO WAYS WITH A PENCIL HAVING BLACK LEAD.
TO VOTE A STRAIGHT TICKET, MAKE A CROSS X MARK WITHIN THE CIRCLE ABOVE ONE OF THE PARTY COLUMNS.
TO VOTE A SPLIT TICKET, THAT IS, FOR CANDIDATES OF DIFFERENT PARTIES, THE VOTER SHOULD MAKE A CROSS X MARK BEFORE THE NAME OF EACH CANDIDATE FOR WHOM HE VOTES.
IF THE TICKET MARKED IN THE CIRCLE FOR A STRAIGHT TICKET DOES NOT CONTAIN THE NAMES OF CANDIDATES FOR ALL OFFICES FOR WHICH THE ELECTOR MAY VOTE, HE MAY VOTE FOR CANDIDATES FOR SUCH OFFICES SO OMITTED BY MAKING A CROSS X MARK BEFORE THE NAMES OF CANDIDATES FOR SUCH OFFICES ON ANOTHER TICKET, OR, BY WRITING THE NAMES, IF THEY ARE NOT PRINTED UPON THE BALLOT, IN THE BLANK COLUMN UNDER THE TITLE OF THE OFFICE.
TO VOTE FOR A PERSON NOT ON THE BALLOT, WRITE THE NAME OF SUCH PERSON, UNDER THE TITLE OF THE OFFICE, IN THE BLANK COLUMN.
ANY OTHER MARK THAN THE CROSS X MARK USED FOR THE PURPOSE OF VOTING OR ANY ERASURE MADE ON THIS BALLOT MAKES IT VOID, AND NO VOTE CAN BE COUNTED HEREON.
IF YOU TEAR, OR DEFACE, OR WRONGLY MARK THIS BALLOT, RETURN IT AND OBTAIN ANOTHER.

						BLANK COLUMN.
For a Straight Ticket ○ Mark Within This Circle	For a Straight Ticket ○ Mark Within This Circle	For a Straight Ticket ○ Mark Within This Circle	For a Straight Ticket ○ Mark Within This Circle	For a Straight Ticket ○ Mark Within This Circle	For a Straight Ticket ○ Mark Within This Circle	THE ELECTOR MAY WRITE IN THE COLUMN BELOW, UNDER THE TITLE OF THE OFFICE THE NAME OF ANY PERSON WHOSE NAME IS NOT PRINTED UPON THE BALLOT, FOR WHOM HE DESIRES TO VOTE.
REPUBLICAN TICKET.	DEMOCRATIC TICKET.	NATIONAL DEMOCRATIC TICKET.	PROHIBITION TICKET.	SOCIALISTIC-LABOR TICKET.	PEOPLE'S TICKET.	
For President, WILLIAM McKINLEY.	For President, WILLIAM J. BRYAN.	For President, JOHN M. PALMER.	For President, JOSHUA LEVERING.	For President, CHARLES H. MATCHETT	For President, WILLIAM J. BRYAN.	
For Vice-President, GARRET A. HOBART.	For Vice-President, ARTHUR SEWALL.	For Vice-President, SIMON B. BUCKNER.	For Vice-President, HALE JOHNSON.	For Vice-President, MATTHEW MAGUIRE.	For Vice-President, THOMAS E. WATSON.	
For Elector of President and Vice-President, BENJAMIN F. TRACY.	For Elector of President and Vice-President, ROBERT P. BUSH.	For Elector of President and Vice-President, OSWALD OTTENDORFER.	For Elector of President and Vice-President, FREDERICK F. WHEELER.	For Elector of President and Vice-President, GEORGE ABELSON.	For Elector of President and Vice-President, ROBERT P. BUSH.	For Elector of President and Vice-President,
EDWARD H. BUTLER.	BENJAMIN WOOD.	THEODORE BACON.	LOUIS ALBERT BANKS.	THOMAS J. MURPHY.	BENJAMIN WOOD.	
CARLL S. BURR.	JOHN P. MADDEN.	PATRICK J. GLEASON.	HENRY W. RANDALL.	ABRAHAM SHAPIRO.	JOHN P. MADDEN.	
ALEXANDER ROSS.	ANDREW McLEAN.	GEORGE W. WINGATE.	FREEBORN G. SMITH.	CARL WENDELSTEIN.	ANDREW McLEAN.	
CHARLES A. MOORE.	JAMES BURRELL.	JAMES A. MURTHA, Jr.	JAMES MEYER.	OTTO HATJE.	JAMES BURRELL.	
ROBERT A. SHARKEY.	SAMUEL S. WHITEHOUSE.	HENRY W. SHERRILL.	FRANK MAPES.	WALFRID E. OSBERG.	SAMUEL S. WHITEHOUSE.	
FRANCIS F. WILLIAMS.	MARTIN H. DUANE.	J. EDWARD SWANSTROM.	JOHN BERRY.	JACOB LAPEIRE.	MARTIN H. DUANE.	
WILLIAM NASON.	JOHN ENNIS.	JAMES J. STANTON.	JOHN BREMER.	GEORGE S. SULLIVAN.	JOHN ENNIS.	
FREDERICK HALDY.	JOHN E. WALSH.	GEORGE J. GREENFIELD.	JAMES C. FERNALD.	JACOB ZIMMER.	JOHN E. WALSH.	
NICHOLAS FISH.	WILLIAM McM. SPEER.	EDWARD J. DUNPHY.	JOHN GLOVER.	LOUIS SCHNEIDER.	WILLIAM McM. SPEER.	
HERMAN O. ARMOUR.	MICHAEL F. LYONS.	HENRY CAMPBELL.	GEORGE B. HILLARD.	JOSEPH SMITH.	MICHAEL F. LYONS.	
GEORGE B. DEANE.	JOHN JORDAN.	JOHN FENNEL.	JOHN IHMER.	JAMES McGARVEY.	JOHN JORDAN.	
FRANCIS J. DRUMMOND.	MAURICE B. BLUMENTHAL.	GEORGE TUCKER HARRISON.	EMORY CUMMINGS.	JOSEPH H. SWEENY.	MAURICE B. BLUMENTHAL.	
HENRY BIRRELL.	WILLIAM RANDOLPH HEARST.	JAMES D. LYNCH.	JOHN McKEE.	WILLIAM WAFFNER.	WILLIAM RANDOLPH HEARST.	
SMITH PINE.	HENRY GUENTHER.	JOHN D. CRIMMINS.	WILLIAM T. WARDWELL.	HENRY STASIUS.	HENRY GUENTHER.	
LEOPOLD STERN.	WILLIAM L. BROWN.	JOHN R. FELLOWS.	FRANCIS M. HOMMOND.	HENRY C. ROMAINE.	WILLIAM L. BROWN.	
SETH M. MILLIKEN.	JOHN McQUADE.	SIMON STERNE.	ALFRED L. MANIERER.	FRANK DANKHOFF.	JOHN McQUADE.	
WILLIAM L. WARD.	JOHN BRISBEN WALKER.	FREDERICK POTTER.	JESSE H. UNDERHILL.	FERDINAND [illegible]	[illegible]	

Figure 4: Australian Ballot. This is a picture of Australian Ballot that once used in the election of 1896. (Wiggins, 2020)

"The secret ballot was designed to stop one problem made possible by these very public election days — voter intimidation. [Since] [i]t's much harder to intimidate or bribe someone if you can't see who they end up voting for." (Wiggins, 2020) As shown in Figure 4, the ballot was designed to be more detailed and hard to snoop. As a result, Australian Ballots elevated the confidentiality of the elections to a new standard since it achieved privacy for voters as well as left a reference to address possible disputes on election results.

删除了: 11

FROM PAPER BALLOTS TO VOTING MACHINES

As the world becomes digitalized, new voting methods is invented. For example, direct recording electronic (DRE) voting machines are a form of paperless voting method. The options of candidates will be displayed on the screen as depicted in Figure 5 and the voter can vote for candidates by selecting the corresponding choices. (AvanteTech, n.d.) The invention of electronic voting machines prevents physical human interference, such as destroying and altering ballots, during the elections. Also, voting machines are equipped with headphones for the disabled to cast votes much easier.

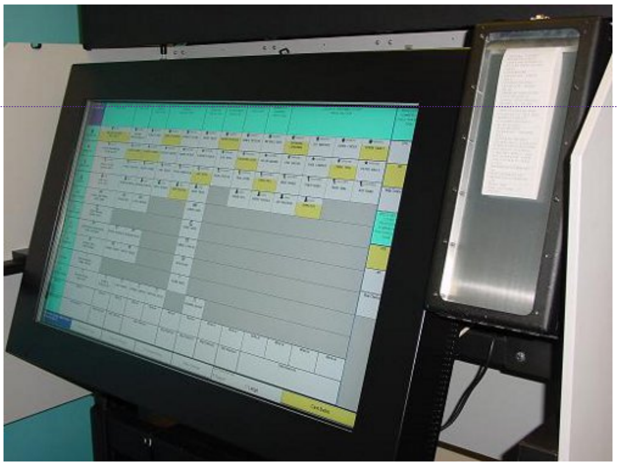


Figure 5: Direct Recording Electronics Voting Machine. This is a picture of the screen of a DRE. (AvanteTech, n.d.)

删除了： DRE

删除了： direct recording electronic

删除了： incorrect acronym use

Regarding the presence of voting machines, a chain reaction happens in ANT. First, the people’s need for a secure, reliable, and private voting process prompts the invention of voting machines. In this process, social recognition plays the role of an actor in ANT. The voting machine is subsequently incorporated into the election-centered network. Then, the accessible voting machines in turn plays the role of an actor, further motivating the disabled to involve in the voting process. This characteristic corresponds to Callon’s (1987) claim, “An actor-network is simultaneously an actor whose activity is networking heterogeneous

删除了： 11

elements and a network that is able to redefine and transform what it is made of" (p.93)

This research project will be in the form of a scholarly article discovering the relationship between technology and society. Given the analysis from past experience, I suggest that the homomorphic encryption method that will be discovered in my technical_ report will play a similar role as voting machines. Its design is motivated by the public's requirement for the transparency and confidentiality of the voting process, and its emergence will strengthen trust bonds within communities during the elections and thus will in turn appeals to more citizens to involve in the elections._

删除了: 分节符(下一页)

删除了: 11

REFERENCES

Adams, S. (1781, April 16). *Essay in the Boston Gazette.* Boston: Bos

Bracken, B. (2021, November 19). Iranians charged in cyberattacks against U.S. 2020 election. Threatpost English Global threatpostcom. Retrieved July 8, 2022, from https://threatpost.com/iranians-charged-cyberattacks-2020-election/176488/

Cressman, D. (2009). A brief overview of Actor-Network Theory: punctualization, heterogeneous engineering & translation. School of Communication, Simon Fraser University.

Avante International Technology, Inc. (2020, December 11). Direct recording electronic. https://www.avantetech.com/products/elections/dre/

Encyclopedia Britannica, inc. (n.d.). Functions of elections. Encyclopedia Britannica. https://www.britannica.com/topic/election-political-science/Functions-of-elections

Graham, D. (2022). *Homomorphic Encryption* [PowerPoint Slides]. School of Engineering and Applied Science, the University of Virginia.

Halderman, A. J. (n.d.) *The living voice - voting as a security problem*.[Video transcript] Coursera. https://www.coursera.org/lecture/digital-democracy/the-living-voice-GMEjX

The Institute for Advanced Technology in the Humanities. (n.d.). *How America Voted: By voice*. http://sociallogic.iath.virginia.edu/node/35

Hughes, T. J. (1994). *Technological Momentum.* Boston, Bos: The MIT Press.

Lange, A. (2011, May 9). Application to Cryptography. In *An Overview of Homomorphic Encryption.* https://www.cs.rit.edu/~arl9577/crypto/alange-presentation.pdf

TechTarget Contributor. (n.d.) Homomorphic Encryption. TechTarget.

设置了格式: 字体: 非倾斜

设置了格式: 字体: 非倾斜

设置了格式: 字体: 非倾斜

设置了格式: 字体: 非倾斜

设置了格式: 字体: 非倾斜

设置了格式: 字体: 非倾斜

设置了格式: 字体: 非倾斜

设置了格式: 字体: 非倾斜

域代码已更改

域代码已更改

删除了: (n.d.).

删除了: The Institute for Advanced Technology in the Humanities.

删除了:

设置了格式: 超链接, 字体: (默认) +西文正文 (DengXian), 10.5 磅

删除了: 分节符(下一页)

删除了: 11

https://www.techtarget.com/searchsecurity/definition/homomorphic-encryption#:~:text=Homomorphic%20encryption%20is%20the%20conversion,data%20without%20compromising%20the%20encryption.

Voting and electioneering, 1789–1899. (n.d.) National Museum of American History. https://americanhistory.si.edu/democracy-exhibition/machinery-democracy/voting-and-electioneering-1789%E2%80%931899

Wiggins, N. (2020, October 11). US elections were changed for better (and worse) by the secret 'Australian ballot'. ABC News. https://www.abc.net.au/news/2020-10-11/us-election-voting-changed-by-secret-australian-ballot-history/12726686

删除了: 11