Formal Verification for Correct and Secure Software

Mukesh Tiwari,
University of Cambridge,
Cambridge

UNIVERSITY OF CAMBRIDGE

CCS, USENIX

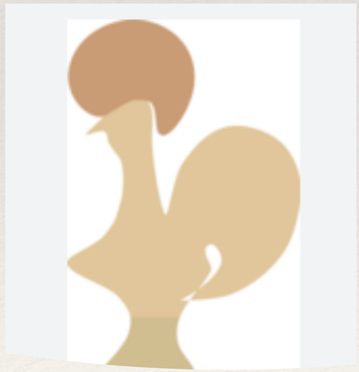
ITP, EVote, VSTTE

SIGCOMM, ICNP

Cryptography

Voting

Networking Protocols



Moscow's blockchain voting system cracked a month before election

French researcher nets $15,000 prize for finding bugs in Moscow's Ethereum-based voting system.

MOTHERBOARD
TECH BY VICE

Experts Find Serious Problems With Switzerland's Online Voting System Before Public Penetration Test Even Begins

The public penetration test doesn't begin until next week, but experts who examined leaked code for the Swiss internet voting system say it's poorly designed and makes it difficult to audit the code for security and configure it to operate securely.

KZ By Kim Zetter

Federal review says Dominion software flaws haven't been exploited in elections


By Sean Lyngaas, Evan Perez and Whitney Wild, CNN
Updated 12:18 PM EDT, Fri June 3, 2022

Flaws found in NSW iVote system yet again

Analysis of source code published at the request of the NSW Electoral Commission shows that the state's election system software was still vulnerable to attack.

I hear you: paper ballots are great

AEC ✏️
@AusElectoralCom

The Senate count is one of the most complex upper house counts in the world - it's so complex that we needed to write a program to distribute your preferences, as doing it by hand would mean we couldn't provide elected Senators in time to take their seat.

12:02 AM · Jun 14, 2022

13 Retweets **2** Quote Tweets **62** Likes

Blind advocates allege NSW's removal of online voting system is a breach of human rights

State electoral commission accused of discrimination for suspending iVoting platform as Blind Citizens Australia takes case to watchdog

Home › The Ministry and its Network › News › **2020**

A+ A–

French citizens abroad – Approval of electronic voting for consular elections (15 January 2020)

Claim

Theorem Provers can help us in implementing correct and secure software

Machine-checking Multi-Round Proofs of Shuffle: Terelius-Wikstrom and Bayer-Groth

Authors:
Thomas Haines, *Australian National University;* Rajeev Gore, *Polish Academy of Science;* Mukesh Tiwari, *University of Cambridge*

ply says "*[t]he completeness follows from the completeness of the sigma proof,*" which we have just shown not to be the case since the relationship which the sigma protocol proves may be false.

This petition was submitted during the 2010–2015 Conservative – Liberal Democrat coalition government

View other petitions from this government

Petition

Schulze method voting system

More details

Most voting systems are flawed due to their methodology (see Arrow's Impossibility Theorem for more details) but some are more 'fair' than others. The Schulze method, based on the Schwartz criterion is a voting system which is mathematically 'fairer' and will generate voting outcomes which are a better representation than most voting systems. This petition aims to start a debate into the practicalities of introducing this system into UK public voting systems.

This petition is closed

This petition ran for 6 months

3 signatures

10,000

Schulze Method

$$\prod_{k=0}^{n}\prod_{i=0}^{n}\prod_{j=0}^{n} dist[i][j] = max(dist[i][j], min(dist[i][k], dist[k][j]))$$

Schulze Method

$$\prod_{k=0}^{n}\prod_{i=0}^{n}\prod_{j=0}^{n} dist[i][j] = min(dist[i][j], dist[i][k] + dist[k][j])$$

Floyd-Warshall Algorithm

Schulze Method

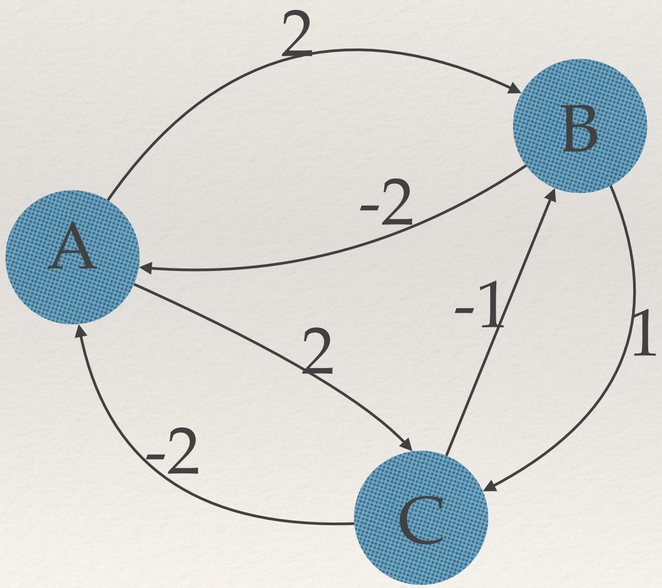
	C < B < A	C = B < A	C = B = A
A	1	1	1
B	2	2	1
C	3	2	1
	Ballot 1	Ballot 2	Ballot 3

Schulze Method

	A	B	C
A	0	1	1
B	-1	0	0
C	-1	0	0

$$C = B < A$$

Schulze Method

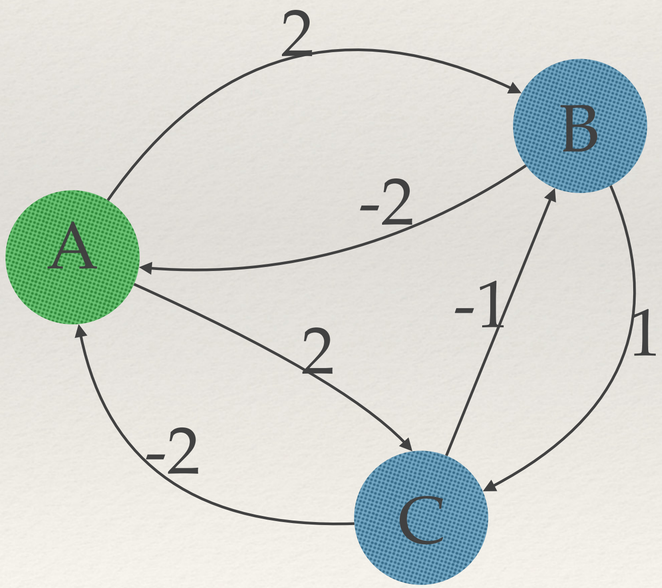


	A	B	C
A	0	2	2
B	-2	0	1
C	-2	-1	0

Margin Matrix (m)

Schulze Method

A wins



	A	B	C
A	0	2	2
B	-2	0	1
C	-2	-1	0

Generalised Margin Matrix (M)

Schulze Voting as Evidence Carrying Computation

Dirk Pattinson & Mukesh Tiwari

Conference paper

948 Accesses | 6 Citations

Part of the Lecture Notes in Computer Science book series (LNTCS,volume 10499)

No More Excuses: Automated Synthesis of Practical and Verifiable Vote-Counting Programs for Complex Voting Schemes

Lyria Bennett Moses, Rajeev Goré, Ron Levy, Dirk Pattinson & Mukesh Tiwari

Conference paper | First Online: 06 October 2017

Modular Formalisation and Verification of STV Algorithms

Milad K. Ghale, Rajeev Goré, Dirk Pattinson & Mukesh Tiwari

The Ballot Identification Problem

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
3	2	1	4	6	7	5	11	9	10	15	14	8	13	12

Verifiable Homomorphic Tallying for the Schulze Vote Counting Scheme

Thomas Haines, Dirk Pattinson & Mukesh Tiwari

Conference paper | First Online: 14 March 2020

Part of the Lecture Notes in Computer Science book series (LNPSE,volume 12031)

Encrypted Ballot

$$C < B < A$$

	A	B	C
A	E(0, r1)	E(1,r2)	E(1, r3)
B	E(-1, r4)	E(0, r5)	E(1, r6)
C	E(-1, r7)	E(-1, r8)	E(0, r9)

$$E(m, r) = (g^r, g^m \cdot h^r)$$

	A	B	C
A	E(0, r1)	E(1,r2)	E(1, r3)
B	E(-1, r4)	E(0, r5)	E(1, r6)
C	E(-1, r7)	E(-1, r8)	E(0, r9)

Ballot 1: C < B < A

	A	B	C
A	E(0, r11)	E(-1, r12)	E(-1, r13)
B	E(1, r14)	E(0, r15)	E(-1, r16)
C	E(1, r17)	E(1, r18)	E(0, r19)

Ballot 2: A < B < C

$$Enc(m_1, r_1) = (g^{r_1}, g^{m_1} \cdot h^{r_1})$$
$$Enc(m_2, r_2) = (g^{r_2}, g^{m_2} \cdot h^{r_2})$$
$$Enc(m_1, r_1) \cdot Enc(m_2, r_2) = (g^{r_1+r_2}, g^{m_1+m_2} \cdot h^{r_1+r_2})$$

Challenge

What is the ordering of candidates in this ballot?

	A	B	C
A	E(0, r1)	E(**1**, r2)	E(**1**, r3)
B	E(**1**, r4)	E(0, r5)	E(-1, r6)
C	E(**1**, r7)	E(-1, r8)	E(0, r9)

Challenge

What about this one?

	A	B	C
A	E(0, r1)	E(100, r2)	E(100, r3)
B	E(-100, r4)	E(0, r5)	E(1, r6)
C	E(-100, r7)	E(-1, r8)	E(0, r9)

Challenge

Deciding if a ballot is valid or not

For **every ballot**, the counting authority generates a **secret permutation**, but it is **publicly verifiable** that it is a valid permutation (Zero-Knowledge Proof)

[A -> C, C -> B, B -> A]

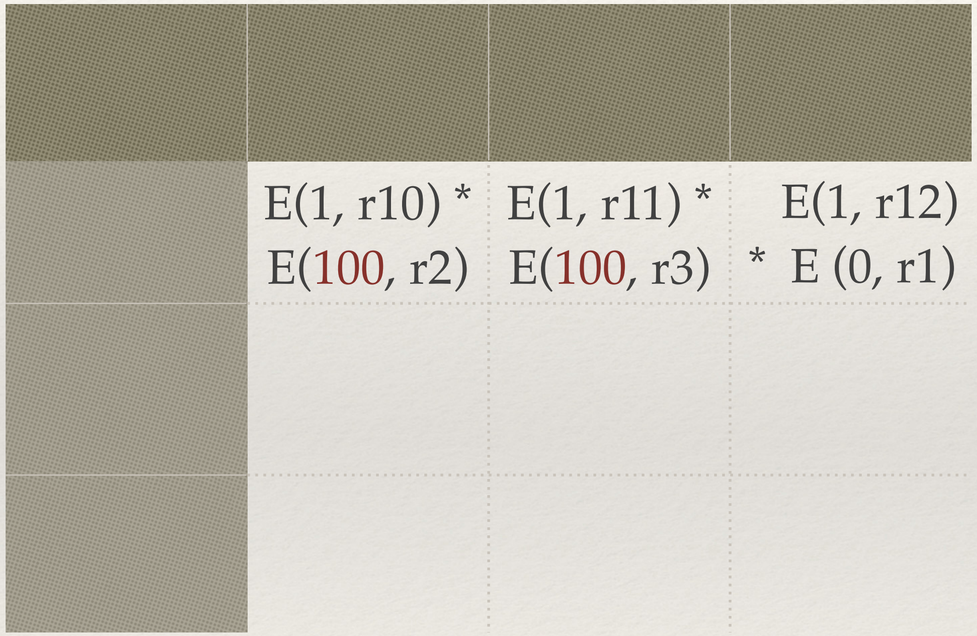
	A	B	C
A	E(0, r1)	E(100, r2)	E(100, r3)
B	E(-1, r4)	E(0, r5)	E(1, r6)
C	E(-1, r7)	E(-1, r8)	E(0, r9)

Original Ballot

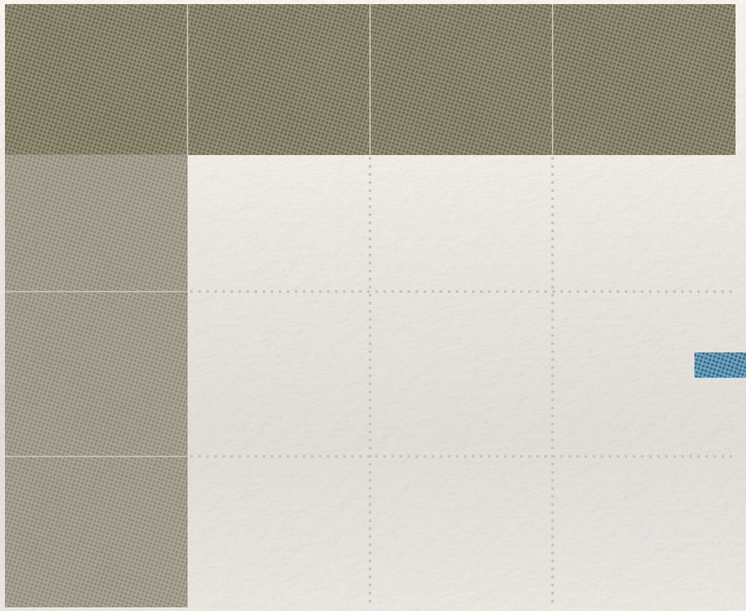
	E(1, r10) * E(100, r2)	**E(1, r11)** * E(100, r3)	**E(1, r12)** * E(0, r1)

Row-Shuffled Ballot

\+ Zero-Knowledge Proof



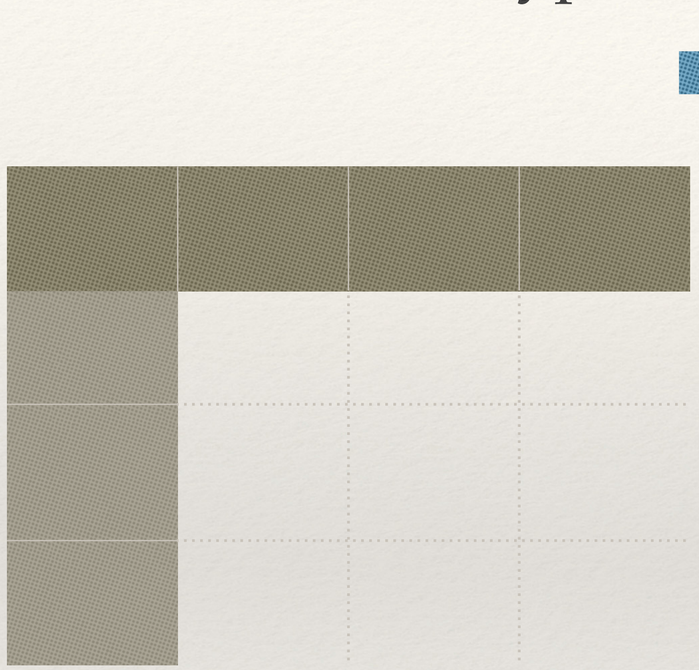
Row-Shuffled Ballot



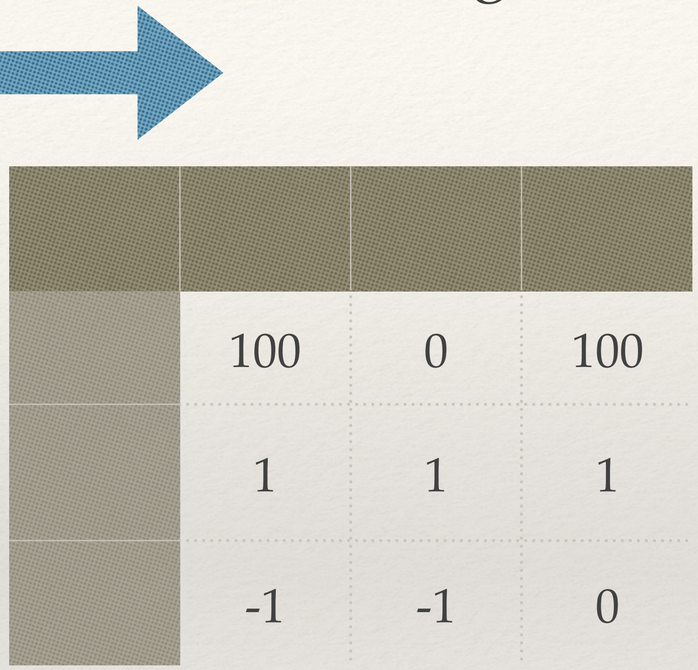
Row-Column-Shuffled Ballot

Zero-Knowledge Proof

Decryption with Zero-Knowledge Proof



Row-Column-Shuffled Ballot



Decrypted Row-Column-Shuffled Ballot

+

Zero-Knowledge Proof

Future Projects and Possible Collaborators

Exploring zk-SNARK, Blockchain, and Multiparty computation for public good

- Domain Specific Language for zk-SNARK with Prof. Neil Ghani, Dr Conor McBride, Dr Robert Atkey, and Dr Fredrik Nordvall Forsberg
- Social Choice Theory with Dr Jules Hedges

What values do I bring to Strathclyde?

Cyber security backed by Constructive Logic

Questions?