VoteXX: A Solution to Improper Influence in Voter-Verifiable Elections (extended abstract)

David Chaum[1], Richard T. Carback[1], Jeremy Clark[2], Chao Liu[3], Mahdi Nejadgholi[2], Bart Preneel[4], Alan T. Sherman[3], Mario Yaksetig[1], Zeyuan Yin[6], Filip Zagórski[5], and Bingsheng Zhang[6]

[1] xx.network, USA
[2] Concordia University, Canada
[3] Cyber Defense Lab, University of Maryland, Baltimore County (UMBC), USA
[4] COSIC, KU Leuven and imec, Belgium
[5] Wroclaw University of Technology, Department of Computer Science, Poland
[6] Zhejiang University, Hangzhou, China

Abstract. We solve a long-standing challenge to the integrity of votes cast without the supervision of a voting booth: "*improper influence*," which we define as any combination of vote buying and voter coercion. Our approach allows each voter, or their trusted agent(s), to cancel their vote in a way that is unstoppable, irrevocable, and forever unattributable to the voter. In particular, our approach enhances security of online, remote, public-sector elections, for which there is a growing need and the threat of improper influence is most acute. In this extended abstract, we introduce the new approach, compare it with previous methods, and concisely summarize the protocols. In our full paper, we give detailed cryptographic protocols, show how they can be applied to several voting settings, describe our implementation in a full voting system called *VoteXX*, and provide UC proofs. Our system protects against the strongest adversary considered in prior related work and is suitable for widespread use in public elections.

1 Introduction

For over 150 years, the voting booth helped prevent voters from being bribed and coerced. For example, a controlling spouse might coerce their partner by observing them vote, if the partner votes online from home or by mail. The booth, however, is becoming untenable as information technology provides the means for people to vote more frequently and conveniently without booths, including using combinations of mailed paper forms and online interactions. Moreover, growing use of technology facilitates vote buying and voter coercion with electronic payments, live video streaming from voter phones, and online threats.

We present a solution to the problem of *improper influence* in voting without booths that enables any voter to *"nullify"* (effectively cancel) their vote in a way that is unstoppable, irrevocable, and forever unattributable to that voter. Our approach allows each voter to recruit one or more trusted agents, which we call "*hedgehogs*." The voter, or their hedgehog(s), can nullify the vote by proving knowledge of the voter's secret key using a zero-knowledge proof. Hedgehogs can be recruited before or during the election, from the voter's acquaintances or

using a service selected on reputation. Our approach can be applied to a variety of voting settings, including unscheduled elections.

Contributions. Our primary contributions are: (1) We introduce the new notions of nullification and hedgehogs, and present a new solution to improper influence based on them. (2) We give cryptographic protocols realizing nullification, and show how it can be applied to several voting settings, including vote-by-mail and online. (3) We present a new fully-decentralized scalable voting system, VoteXX, including registration, voting, nullification, and tallying. (4) We describe our implementation of VoteXX, which uses an *anonymous communication system (ACS)* for registration, vote casting, and other communication. While other systems complicate registration and vote casting, our approach allows simple registration and vote casting by keeping nullification separate.

Previous Work. As shown in Table 1, our approach differs from previous approaches—e.g., revoting, fake credentials, panic passwords, secure hardware, and decoy ballots—by leveraging the realistic assumption of an unknowable and untappable channel between the voter and their hedgehog(s). Our system does not have to make any of the following strong assumptions, which can be readily violated by realistic adversaries: an untappable registration channel, a final time when the voter can vote securely, or that voters are willing to help discourage vote buying by selling decoy ballots. We protect against what we believe to be the strongest possible adversarial model (apart from coercers blocking registration or voting), in which adversaries can learn all voter secrets and observe all voter interactions with the system (excluding interactions with the hedgehogs).

Informally, a voting system is *coercion resistant* means voters cannot prove how they voted (beyond what is inferable from the tally). Formally defining coercion resistance remains an open research problem. For example, Smyth [8]

Table 1. Assumptions and properties of related work for resisting improper influence in online *end-to-end (E2E)* verifiable elections. Properties are fully present (●), partially present (◐), or not present (○). Decoy ballots act indirectly against influence (◉).

Assumptions: System resists coercion when the influencer: (0) acts before/during registration; (1) colludes with the EA; (2) colludes with hardware manufactures; (3) acts at any time; (4) learns all information stored by the voter, including all keys required by the protocol; (5) learns every action taken by the vote. **Properties:** (6) voter can undo coercion undetectably; (7) system is inexpensive; (8) system has low cognitive burden; (9) system has security proof (none/game-based/UC).

		0	1	2	3	4	5	6	7	8	9
Type	**Example**	**Assumption**						**Property**			
Baseline (coercible)	Helios (2008) [1]	○	○	○	○	○	○	○	●	●	◐
Fake credentials	JCJ (2005) [6]	○	◐	●	○	○	○	●	●	●	◐
Masked ballots	WeBu09 (2009) [9]	○	●	●	○	○	○	○	●	○	●
Panic passwords	Selections (2011) [5]	○	●	●	○	○	○	●	●	◐	◐
Decoy ballots	RS-Voting (2012) [3]	●	◐	●	◉	◉	○	○	●	◐	●
Secure hardware	AOZZ (2015) [2]	●	◐	○	○	●	○	●	○	●	●
Re-voting (E2E)	VoteAgain (2020) [7]	●	●	●	○	●	○	●	●	●	◐
Hedgehogs	VoteXX (2022)	●	●	●	●	●	○	○	●	●	●

argues that some proposed definitions are too strong, and others are too weak. Meaningful comparisons among prior coercion-resistance mechanisms require a careful consideration of the associated definitions, assumptions, and properties.

2 Protocol

The VoteXX protocol comprises seven phases:

(1) **Registration Protocol.** Registration is an in-person ceremony between the voter, using a *voting client* device, and an officer for the EA. The voter registers two public keys to be used to vote YES and NO, respectively (one key for each ballot question). The keys are for a digital signature. They are based on a passphrase that can be regenerated from any voting client. The *election authority (EA)* does not learn the passphrase but has high assurance through the protocol that the human voter knows the passphrase. At completion, the *bulletin board (BB)* contains a list of eligible voters, a list of YES public keys, and a list of NO public keys. Only the voter knows the association between their identity and the associated keys.

(2) **Recruiting Protocol.** Each voter concerned with possible coercion can, at any time before nullification ends, recruit one or more hedgehog(s). The voter sends the private key associated with the voter's intention (*i.e.,* to vote YES or NO) to the hedgehog over an untappable channel. In addition, the voter and hedgehog arrange the conditions under which the hedgehog will act.

(3) **Voting Protocol.** Voting is an online procedure in which each voter posts their ballot on the BB over an ACS. The ballot consists of a signature using either the YES or NO key to indicate the voter's selection. The signature is encrypted by the voter under the EA's threshold-shared public key to prevent observers from determining a running tally for the election. At completion, the BB contains a list of encrypted ballots.

(4) **Pre-Tallying Protocol.** After the voting period ends, the trustees of the EA decrypt all submitted ballots in the order they were received. At completion, the BB contains this pre-tally without any nullification actions.

(5) **Activating Protocol.** At any time after a voter recruits a hedgehog and before nullification ends, the voter can activate the hedgehog, consistently with their prior arrangement. For example, the voter might activate the hedgehog by sending an active signal (*e.g.,* moving a potted plant or posting a specific photo to social media), using a "dead person switch" that is the absence of a signal, or relying on the hedgehog to inspect the contents of the BB (*e.g.,* activate if and only if a YES vote has been cast by the voter after the pre-tally protocol).

(6) **Nullification Protocol.** The goal of nullification is to allow voters to flag their cast ballots, particularly in the case of coercion, for "nullification." Each election has a policy defining what nullification means—for example ballots are canceled, flipped, or some other option. The default policy is to flip. The hedgehog (or voter) submits a nullification request under the EA's encryption key that flags a specific ballot. Also, they prove, under zero-knowledge, that they know the appropriate key that authorizes them to nullify the voter's ballot. At completion, the BB contains a set of encrypted nullification requests.

(7) **Tallying Protocol.** After the nullification period ends, the trustees of the EA process the nullification requests under encryption. If a voted ballot is nullified more than once, the EA applies an XOR logical operation to the set of flags to determine if the nullification will be effected. The EA then sums the number of nullifications. Next, the EA decrypts two numbers: the number of nullified YES votes and the number of nullified NO votes. The pre-tally is adjusted using these numbers to produce the final tally. Throughout pre-tallying, nullification, and tallying, the protocols do not reveal any information about how any individual voter voted beyond what can be learned from the final tally itself.

3 Discussion

Leveraging hedgehogs, an ACS, BBs, and user-generated passphrases, VoteXX provides a versatile solution to improper influence in elections against strong adversaries who learn the voter's voting keys. Our full paper [4] includes more details and a formal statement and UC proof of VoteXX's ballot secrecy, coercion resistance, and tally integrity. Future work includes piloting VoteXX in real elections to assess its usability and voter acceptance.

Currently, election systems without voting booths are vulnerable to potential improper influence attacks. Having demonstrated that coercion resistance is possible, even in Internet voting, democratic societies should insist that, as a matter of due diligence, all voting systems should provide coercion resistance. Our work protects voting beyond the booth, and such voting is an essential enabler for the advance of democracy.

Acknowledgments. This project was supported in part by xx network. Clark was supported in part by NSERC and Raymond Chabot Grant Thornton; Sherman by the National Science Foundation and the U.S. Department of Defense.

References

1. Adida, B.: Helios: Web-Based open-audit voting. In: USENIX Security Symposium. pp. 335–348 (2008)
2. Alwen, J., Ostrovsky, R., Zhou, H.S., Zikas, V.: Incoercible multi-party computation and universally composable receipt-free voting. In: Annual Cryptology Conference. pp. 763–780. Springer (2015)
3. Chaum, D.: Random-Sample Voting (2012), online
4. Chaum, D., Carback, R.T., Clark, J., Liu, C., Nejadgholi, M., Preneel, B., Sherman, A.T., Yaksetig, M., Zagórski, F., Zhang, B.: VoteXX: A solution to improper influence in voter-verifiable elections. Cryptology ePrint Archive (2022)
5. Clark, J., Hengartner, U.: Selections: Internet voting with over-the-shoulder coercion-resistance. In: Financial Cryptography (2011)
6. Juels, A., Catalano, D., Jacobsson, M.: Coercion-Resistant electronic elections. In: ACM WPES (2005)
7. Lueks, W., Querejeta-Azurmendi, I., Troncoso, C.: Voteagain: A scalable coercion-resistant voting system. In: USENIX Security (2020)
8. Smyth, B.: Surveying definitions of coercion resistance. Cryptology ePrint Archive, Report 2019/822 (2019)
9. Wen, R., Buckland, R.: Masked ballot voting for receipt-free online elections. In: VOTE-ID (2009)