Research Statement

Constantin Cătălin DRĂGAN
INRIA Grand East, Nancy, France
Email: dragancc@yahoo.com

1 Electronic Voting Protocols

Voting is an important part of our democratic process, and in its electronic form has been used in an ever growing number of elections and referendums. Some of the reasons for this development include the necessity for a mechanized way of counting votes, and the comfort obtained from voting at home.

The use of electronic voting raises a number of basic questions with respect to the correctness of the voting process and the privacy of the votes. Simple question such as:

- is my vote private, and
- can I be sure my vote was counted,

while natural prove to be particular challenging to answer.

This process is made more difficult as new voting protocols and new definition of voting properties are introduced frequently. Many of these new results propose either a fix to some issue found in a previous definition or protocol, or a method to deal with a some new scenario or particular voting concern, depending on the socio-political context.

Additionally, the majority of security proofs are done by hand in a pen-and-paper style, and are error-prone and difficult to check. Nevertheless, audits of voting systems suggest that many common issues could have been prevented by using open source and formally verified implementations. However, the formal verification of voting systems down to deployed software is particularly challenging. Some of the main reasons for this ranges from the fact that defining security properties for voting systems is an active topic of investigation, to the fact that electronic voting systems are highly complex and distributed, with multiple implementations of voting clients.

2 Current and future research direction

The goal of my current research is to be able to alleviate some of these concerns. In [A2], we have started a step in this direction by refining an existing core voting construction with a high degree of abstraction and proving it satisfies privacy. More precisely, we provide privacy for a general framework that models a single voting pass protocol under standard cryptographic assumptions. The key feature of this framework is the high degree of abstraction that allows the capture of hundreds of variants of Helios, including most existing ones. The whole process is semi-automated, in the sense that we use an interactive proof assistant (EasyCrypt) to prove privacy for this framework, and then show that the analysed voting protocol can be viewed as an instance this framework. The latter is sufficient to ensure that the analysed voting protocol enjoys the same security guarantees as our framework, without having to redo the whole proof process. Furthermore, this result provides a machine-checked proofs of privacy for an electronic voting protocol in the computational model (maybe the second in literature after [B12])

Currently, I am working on a result for verifiability that follows the same methodology as the proof on privacy, and I am happy to report that we are in the final stages of finishing this result. The definition for verifiability that we have in mind is a novel version of the verifiability in [B10], where our security guarantees are provided under a slightly different standard cryptographic assumptions compared to the initial paper.

Additionally, we intend to apply this result on verifiability (and our previous result on privacy) to the voting protocol Belenios. Moreover, we will provide hundreds of variants of Belenios that satisfy both privacy and verifiability.

Another research direction that I am interested in is threshold cryptography and in particular on designing, analysing and applications of secret sharing schemes. This topic has been the focus of my PhD Thesis, and the results I obtained [A1, A7, A3, A4, A5, A8, A6] provide a necessary and sufficient characterization of the security for schemes based on the Chinese Remainder Theorem. I aim to use my knowledge about secret sharing schemes in designing a threshold model of game-based privacy, and refine the result in [B9].

3 Future research direction

For future research direction, I plan to consider further other properties such as accountability, receipt-freeness, and coercion-resistance. We believe that our previous result [A2] provides a solid step towards accountability, but would requires more work as it is necessary to first specify exactly who is responsible e.g. for the data displayed on the ballot box and the distribution of the credentials and how this is cryptographically enforced. Receipt-freeness and coercion-resistance would require an enrichment of the voting model considered in [A2], as that model is not coercion-resistant. Considering these various properties under varying trust assumptions on each of the parties would also be interesting.

Another future research direction is linked to machine-checked proofs for other voting protocols. We believe that it will be reasonable to adapt the our previous result of privacy from [A2] and our current result on verifiability to include more e-voting protocols such as sElect [B11], or Selene [B13]. The key feature of sElect is that it uses onion encryption and during a mix-net tally it removes duplicated ballots, and this aspect can not be currently handle by the simple tallying operation done in [A2]. Selene seems particularly challenging because of its core characteristic: verification is done by voters after enough time has passes since the election finished. This delay between the publication of the election result and the start of the verification process can be not handled by our model in [A2].

References

Personal

[A1] M. Barzu, F. L. Ţiplea, and C. C. Drăgan. Compact sequences of co-primes and their applications to the security of CRT-based threshold schemes. *Information Sciences*, 240:161–172, 2013.

[A2] V. Cortier, C. C. Drăgan, F. Dupressoir, B. Schmidt, P. Strub, and B. Warinschi. Machine-Checked Proofs of Privacy for Electronic Voting Protocols. In *2017 IEEE Symposium on Security and Privacy, SP 2017*, pages 993–1008. IEEE Computer Society, 2017.

[A3] C. C. Drăgan. *Security of CRT-based Secret Sharing Schemes.* PhD thesis, Alexandru Ioan Cuza University of Iaşi, Romania, Department of Computer Science, Sept. 2013.

[A4] C. C. Drăgan and F. L. Ţiplea. On the Asymptotic Idealness of the Asmuth-Bloom Threshold Secret Sharing Scheme. Information Sciences (accepted in April 2017).

[A5] C. C. Drăgan and F. L. Ţiplea. Distributive Weighted Threshold Secret Sharing Schemes. *Information Sciences*, 339:85–97, 2016.

[A6] C. C. Drăgan and F. L. Ţiplea. Key-Policy Attribute-Based Encryption for General Boolean Circuits from Secret Sharing and Multi-linear Maps. In *Second BalkanCryptSec 2015, Revised Selected Papers*, volume 9540 of *LNCS*, pages 112–133, 2015.

[A7] F. L. Ţiplea and C. C. Drăgan. A necessary and sufficient condition for the asymptotic idealness of the GRS threshold secret sharing scheme. *Inf. Process. Lett.*, 114(6):299–303, 2014.

[A8] F. L. Ţiplea and C. C. Drăgan. Key-Policy Attribute-Based Encryption for Boolean Circuits from Bilinear Maps. In *First BalkanCryptSec 2014, Revised Selected Papers*, volume 9024 of *LNCS*, pages 175–193, 2014.

Relevant

[B9] D. Bernhard, V. Cortier, D. Galindo, O. Pereira, and B. Warinschi. SoK: A Comprehensive Analysis of Game-Based Ballot Privacy Definitions. In *SP 2015: 36th IEEE Symposium on Security and Privacy*, pages 499–516. IEEE Computer Society, 2015.

[B10] V. Cortier, D. Galindo, S. Glondu, and M. Izabachène. Election Verifiability for Helios under Weaker Trust Assumptions. In M. Kutylowski and J. Vaidya, editors, *Computer Security - ESORICS 2014 - 19th European Symposium on Research in Computer Security, Wroclaw, Poland, September 7-11, 2014. Proceedings, Part II*, volume 8713 of *LNCS*, pages 327–344. Springer, 2014.

[B11] R. Küsters, J. Mueller, E. Scapin, and T. Truderung. select: A lightweight verifiable remote voting system. In *IEEE 29th Computer Security Foundations Symposium, CSF 2016, Lisbon, Portugal, June 27 - July 1, 2016*, pages 341–354. IEEE Computer Society, 2016.

[B12] R. Küsters, T. Truderung, B. Beckert, D. Bruns, M. Kirsten, and M. Mohr. A hybrid approach for proving noninterference of java programs. In C. Fournet, M. W. Hicks, and L. Viganò, editors, *IEEE 28th Computer Security Foundations Symposium, CSF 2015, Verona, Italy, 13-17 July, 2015*, pages 305–319. IEEE Computer Society, 2015.

[B13] P. Y. A. Ryan, P. B. Rønne, and V. Iovino. Selene: Voting with transparent verifiability and coercion-mitigation. In J. Clark, S. Meiklejohn, P. Y. A. Ryan, D. S. Wallach, M. Brenner, and K. Rohloff, editors, *Financial Cryptography and Data Security - FC 2016 International Workshops, BITCOIN, VOTING, and WAHC, Christ Church, Barbados, February 26, 2016, Revised Selected Papers*, volume 9604 of *Lecture Notes in Computer Science*, pages 176–192. Springer, 2016.