Privacy-Preserving SAT Solving

Ruzica Piskac
Yale University, New Haven, CT, USA

Abstract

This is an extended abstract of the invited talk presented at the joint conferences "28th International Conference on Theory and Applications of Satisfiability Testing (SAT 2025)" and "31st International Conference on Principles and Practice of Constraint Programming (CP 2025)". The talk is based on a series of three papers published previously, and it provides a unified overview of their key ideas and results.

2012 ACM Subject Classification Security and privacy → Logic and verification

Keywords and phrases SAT solving, Privacy-preserving reasoning, Zero-knowledge proofs, Propositional unsatisfiability

Digital Object Identifier 10.4230/LIPIcs.CP.2025.1

Category Invited Talk

Related Version
Full Version: `https://www.usenix.org/conference/usenixsecurity22/presentation/luo` [2]
Full Version: `https://dl.acm.org/doi/10.1145/3548606.3559373`
Full Version: `https://dl.acm.org/doi/10.1145/3576915.3616621`

Funding *Ruzica Piskac*: NSF award CNS-1562888 and CCF-2131476.

1 Extended Abstract

Formal methods offer a vast collection of techniques to analyze and ensure the correctness of software and hardware systems against a given specification. In fact, modern formal methods tools scale to industrial applications. Despite this significant success, privacy requirements are not considered in the design of these tools. For example, when using automated reasoning tools, the implicit requirement is that the formula to be proved is public. This raises an issue if the formula itself reveals information that is supposed to remain private to one party. To overcome this issue, we propose the concept of privacy-preserving automated reasoning.

We first consider the problem of privacy-preserving Boolean satisfiability [2]. In this problem, two mutually distrustful parties each provides a Boolean formula. The goal is to decide whether their conjunction is satisfiable without revealing either formula to the other party. We present an algorithm to solve this problem. Our algorithm is an oblivious variant of the classic DPLL algorithm and can be integrated with existing secure two-party computation techniques.

We next turn to the problem where one party wants to prove to another party that their program satisfies a given specification without revealing the program. We split this problem into two subproblems: (1) proving that the program can be translated into a propositional formula without revealing either the program or the formula; (2) proving that the obtained formula entails the specification. To solve the latter subproblem, we developed a zero-knowledge protocol for proving the unsatisfiability of formulas in propositional logic [1] (ZKUNSAT). Our protocol is based on a resolution proof of unsatisfiability. We encode verification of the resolution proof using polynomial equivalence checking, which enables us to use fast zero-knowledge protocols for polynomial satisfiability.

We will also outline Ou [3], the first programming framework that provides fully automated and optimal parallelization for zero-knowledge proofs. Zero-knowledge proofs are a powerful cryptographic primitive used in many decentralized or privacy-focused applications. However, the high overhead of ZKPs can restrict their practical applicability. The backend of Ou efficiently and automatically parallelizes ZKPs by formulating program parallelization as integer linear programming problems.

We will conclude by discussing future directions towards fully automated privacy-preserving program verification.

References

1 Ning Luo, Timos Antonopoulos, William R. Harris, Ruzica Piskac, Eran Tromer, and Xiao Wang. Proving UNSAT in zero knowledge. In Heng Yin, Angelos Stavrou, Cas Cremers, and Elaine Shi, editors, *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security, CCS 2022, Los Angeles, CA, USA, November 7-11, 2022*, pages 2203–2217. ACM, 2022. doi:10.1145/3548606.3559373.

2 Ning Luo, Samuel Judson, Timos Antonopoulos, Ruzica Piskac, and Xiao Wang. ppsat: Towards two-party private SAT solving. In Kevin R. B. Butler and Kurt Thomas, editors, *31st USENIX Security Symposium, USENIX Security 2022, Boston, MA, USA, August 10-12, 2022*, pages 2983–3000. USENIX Association, 2022. URL: https://www.usenix.org/conference/usenixsecurity22/presentation/luo.

3 Yuyang Sang, Ning Luo, Samuel Judson, Ben Chaimberg, Timos Antonopoulos, Xiao Wang, Ruzica Piskac, and Zhong Shao. Ou: Automating the parallelization of zero-knowledge protocols. In *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security*, CCS '23, pages 534–548, New York, NY, USA, 2023. Association for Computing Machinery. doi:10.1145/3576915.3616621.