Exploring Extensions of a New Paradigm in Anonymous Credentials

Jacob White (PhD), *Christina Garman* (PI) June 28, 2024

Project Proposal. Privacy-preserving identity verification is an apparent contradiction in terms: it seems impossible for one to simultaneously identify themselves and remain private. And yet, this is increasingly necessary on the Internet today, with recent legislation and policies requiring users to attest that they are, for example, not a robot, old enough to access age restricted media, or a member of a particular group before accessing online services.

A rich body of cryptographic literature has explored *anonymous credentials systems* as a privacy-preserving solution for identity verification, allowing users to selectively disclose necessary attributes and even construct proofs about complex identity properties for service providers to verify, without excessively revealing or linking together attributes when issuing or showing credentials. However, while many theoretical extensions of anonymous credentials such as delegation [1] have been proposed in the cryptographic literature, even minor changes to the scheme's feature set often require extensive cryptographic protocol re-designs and re-deployments, which makes them unwieldy to use or build upon. Furthermore, many real world applications such as Privacy Pass[1] and Signal Private Groups[2] do not support complex zero-knowledge proofs or modular protocols for issuing and presenting credentials.

Our recent work [2] serves as the technical foundation for how to design anonymous credentials in a more modular and extensible manner, providing a unified paradigm under which researchers and developers alike can easily extend a core anonymous credentials scheme with useful features for various applications. While it seems intuitively clear that our scheme is both general and expressive enough to capture the vast majority of extensions and applications currently considered in the literature, it remains non-trivial to prove that our proposed paradigm gives feature parity with existing schemes, while still remaining competitive with (or even improving upon!) their overall efficiency.

The first thrust of the proposed project focuses on enhancing the modularity and extensibility of anonymous credentials. For most schemes, the feature set is primarily determined by the underlying signature scheme by which issuers and service providers can verify the authenticity of anonymous credentials and their attributes. Relying on complex PKI and an associated chain of trust to validate the issuers' public keys, however, introduces a single and significant point of failure. By leveraging zkSNARKs – which can prove about and verify any NP statement – to instead replace PKI for authenticating credentials, we propose to extend our prior work [2] to explore solutions for efficiently delegating the issuance of credentials. And indeed, many zkSNARK "gadgets" such as recursive proof composition already exist which would allow us to support efficient proofs validating the delegation chain. Directly supporting complex delegation policies that span the gap between public and private delegation remains an enticing and open area of future work.

The second thrust of this project focuses on maintaining the strict efficiency guarantees necessary for real-world deployments of anonymous credentials. For example, CAPTCHA and other "attestations of personhood" must contend with very low bandwidth and verification time in networked environments, in part to prevent a flood of bots or even genuine user traffic from causing denials of service. Fortunately, the constant proof size and ability to batch verifications of zkSNARKs serves as an excellent alternative to other optimized but constrained zero-knowledge proof techniques currently used in applications of anonymous credentials such as Privacy Pass. We hope to demonstrate how (1) anonymous credentials built within our unified paradigm can function just as effectively at scale as bespoke schemes, and; (2) how building anonymous credentials schemes will allow for more direct and principled analysis of the security and efficiency tradeoffs that exist when choosing between variants of anonymous credential schemes.

Student Qualifications. Jacob White is one of the co-authors of the work that serves as the foundation for this proposed project. He has extensive expertise in anonymous credentials and zero-knowledge proofs. He also has experience in project management, helping mentor two undergraduates on related projects over the last semester.

References

[1] Johannes Blömer and Jan Bobolz. "Delegatable Attribute-Based Anonymous Credentials from Dynamically Malleable Signatures". In: *Applied Cryptography and Network Security*. June 2018, pp. 221–239.

[2] Michael Rosenberg, Jacob White, Christina Garman, and Ian Miers. "`zk-creds`: *Flexible Anonymous Credentials from zkSNARKs and Existing Identity Infrastructure*". In: *2023 IEEE Symposium on Security and Privacy (SP)*. May 2023, pp. 790–808.

[1] https://blog.cloudflare.com/privacy-pass-standard
[2] https://signal.org/blog/signal-private-group-system/