
1. Add new reference 1:


2. Renumber remaining references: 1–67 become 2–68.

3. Replace the first full paragraph on p. 12 with the following:

IBM’s Idemix project [20, 15] has independently developed a library for zero-knowledge proofs and anonymous credentials using Java; their library provides a system for obtaining, proving, and verifying anonymous credentials for use in a privacy-preserving identity systems. While Idemix and our work both provide implementations of anonymous credentials and CL signatures, our focus on efficient, repeated executions of e-cash transactions has led us to pursue our language-based strategy and develop a performance-optimized interpreter, unlike the Idemix implementation. The CACE project, independent of our efforts, has also designed a high-level language for zero-knowledge protocols; their work has focused on a compiler that can output implementation and LaTeX code from these descriptions [6, 5], and automatically check the soundness of compiled protocols using theorem proving techniques [1].

In the paper “An Analysis of Private Browsing Modes in Modern Browsers,” an author’s name is misspelled in the author listing. Replace “Burzstein” with “Bursztein.”