A. Bhargav-Spantzel, A. C. Squicciarini, R. Xue and E. Bertino, "Multifactor Identity Verification Using Aggregated Proof of Knowledge," in IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews), vol. 40, no. 4, pp. 372-383, July 2010.  
doi: 10.1109/TSMCC.2010.2045755

Abstract: The problem of identity theft, that is, the act of impersonating others' identities by presenting stolen identifiers or proofs of identities, has been receiving increasing attention because of its high financial and social costs. In this paper, we address the problem of verification of such identifiers and proofs of identity. Our approach is based on the concept of privacy preserving multifactor verification of such identifiers and proofs achieved by the development of a new cryptographic primitive, which uses aggregate signatures on commitments that are then used for aggregate zero-knowledge proof of knowledge (ZKPK) protocols. The resultant signatures are very short and the ZKPs are succinct and efficient. We prove the security of our scheme under the co-gap Diffie-Hellman (co-GDH) assumption for groups with bilinear maps. Our cryptographic scheme is an improvement in terms of the performance, flexibility, and storage requirements than the existing efficient ZKPK techniques that may be used to prove under zero knowledge and the knowledge of multiple secrets.  
keywords: {biometrics (access control);cryptographic protocols;data privacy;digital signatures;knowledge engineering;multifactor identity verification;privacy preservation;cryptographic primitive;aggregate zero-knowledge proof;co-gap Diffie-Hellman;bilinear map;Information security;Privacy;Cryptography;Aggregates;Collaboration;Identity management systems;Protection;Costs;Cryptographic protocols;Large-scale systems;Privacy;security},  
URL: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5447665&isnumber=5484888>