



**The George Washington University
Department of Computer Science
Colloquium**

**March 4, 2008, 4:00pm
Room 736 Academic Center**

**Mira Belenkiy
Brown University**

Anonymous Credentials

ABSTRACT

How do I prove I am who I say I am? If I tell you my credit card number, username and password, or even the name of my favorite pet, then in the future, you can use this information to pretend to be me! The trick is to prove I know some secret, such as my password, without revealing what it is. One approach is to prove knowledge of a solution to an NP-hard problem. This talk shows how we can confirm our identity by leveraging Groth-Sahai proofs-of-knowledge of a solution to a bilinear equation. Besides proving that we are who we say we are, we can also prove that other people have given us signed certificates. I can prove that I am over 21 and a student at Brown University without revealing who I am. I can even delegate my certificate, so my friends can prove that they know a student at Brown University over 21.

BIOGRAPHY

Mira Belenkiy is a 5th year graduate student at the Department of Computer Science at Brown University. Her work focuses on finding cryptographic solutions to problems in privacy and security. Her recent work includes anonymous credentials, electronic cash, fair exchange, secret sharing, and privacy and accountability in peer-to-peer networks.