

Job talk for CAISS/ Computer Science

"Tackling the Content Protection Challenge"

Nelly Fazio

Thursday, March 13, 2008

4 p.m.

NAC 8/207

ABSTRACT: Devising effective Content Protection mechanisms and building satisfactory Digital Rights Management systems have been top priorities for the Publishing and Entertainment Industries in recent years. Corporate DRM efforts have so far attempted to address this challenge with systems characterized by a tight control over the user media platform. This approach, however, brings about rigid limitations on the user experience (e.g., restrictions on the creation of back-up copies of purchased copyrighted content), ultimately resulting in an unhappy customer base.

Research advances over the last few years show that Cryptography holds promise for the development of flexible tools that could enable balanced DRM solutions. In this talk, I will provide an overview of my investigations along this direction, and I will then focus on the case of transmission of live events, where the sensitivity of the content under distribution decreases with time. For this setting, I will present a scheme in which unauthorized disclosure of access control credentials can be traced back to the leaker(s), thus discouraging piracy by the threat of detection. The proposed solution improves upon the state of the art both in communication performance and in security guarantees.

Before concluding, I will briefly discuss some of my other cryptographic research, including an on-going project that was recently funded by DARPA in the context of the "System F6" initiative.

BIOGRAPHY:

Nelly Fazio earned her M.Sc. ('03) and Ph.D. ('06) in Computer Science from New York University. During her studies, she also conducted research

at Stanford University, Ecole Normale Supérieure (France) and Aarhus University (Denmark). In 2003, she was awarded the NYU CIMS Sandra Bleistein prize, for "notable achievement by a woman in Applied Mathematics or Computer Science." Her Ph.D. thesis was nominated with honorable mention for the NYU J. Fabri prize, awarded yearly for the "most outstanding dissertation in Computer Science."

Dr. Fazio's research interests are in cryptography and information security, with a focus on digital content protection. Since July 2006, she is part of the Content Protection group at IBM Almaden Research Center, where she has been conducting research on advanced cryptographic key management, tracing technologies, and authenticated communications in dynamic federated environments. Currently, she is a visiting research scientist in the Security group at IBM T.J. Watson Research center, working on security issues of decentralized environments such as sensor networks.