NSF CAREER: Integrating Cryptography with Emerging Security Applications
Alexandra (Sasha) Boldyreva, Georgia Institute of Technology
http://www.cc.gatech.edu/~aboldyre

Motivation
There are emerging security applications in various CS disciplines that require crypto solutions. But there is a gap between theory and practice.

- Research communities are often disjoint.
- Schemes designed by cryptographers guarantee strong security, but applications often have particular efficiency and functionality constraints theoreticians are not always aware of.
- Practitioners are often willing to compromise some security in order to meet these constraints, and design schemes themselves. Security, however, often lacks formal treatment, and hence is not guaranteed.
- Standard bodies still often employ protocols without provable security or with it but under not so well-understood assumptions.

Goal
Try to bridge the gap between theory of cryptographic design and emerging security applications in various areas of computer science.

Approach
- Work closely with researches in applied areas and standard bodies.
- Find schemes that (1) fit the applications and (2) are provably secure for needed levels of security (this may require defining new primitives and security notions).
- Study security of protocols in standards.

Main Results so far
- Secure deterministic and efficiently searchable encryption for outsourced database applications. (Preliminary results at DBSec 2007 and Crypto 2007.)
- Ordered multisignatures and identity-based aggregate signatures for S-BGP, secure routing and network troubleshooting applications. (Preliminary results at ACM CCS 2007.)
- Security of encryption in Kerberos. (Preliminary results at IEEE Security and Privacy 2007.)
- Towards security of RSA-OAEP encryption in the standard (random oracle devoid) model. (Preliminary results at Crypto 2005 and Asiacrypt 2006.)
- Security of PKI. (Preliminary results at PKC 2007.)