

RESEARCH STATEMENT
Mira Belenkiy

Research Overview

I am interested in cryptographic solutions to problems in online privacy and security. Privacy and security are often intertwined. For example, identity theft is rampant because we have become accustomed to authentication by identification. To obtain some service, we provide enough information about our identity for an unscrupulous person to steal it (for example, we give our credit card number to Amazon.com). One of the consequences is that many people avoid e-commerce entirely due to privacy and security concerns.

The solution is to perform authentication *without* identification. In fact, I believe that *all* on-line actions should be as anonymous as possible, for this is the only way to guarantee security for the overall system. In 1986, Goldreich *et al.* introduced the concept of a zero-knowledge proof, which lets a user demonstrate knowledge of a solution to an NP-hard problem, without revealing the actual solution. Zero-knowledge proofs are naturally suited for anonymous systems. The challenge is to create efficient protocols for real-world applications. For example, if we want to use smart cards for authentication, then the protocol should take at most 10-20 exponentiations.

Finally, why a cryptographic approach? Most security flaws in today's systems are due to either (1) a flawed protocol or (2) a flawed implementation of the protocol. Cryptography ensures that, at the very least, the system's underlying protocol meets a well-defined notion of security (given that certain computational problems are hard).

Below, I describe my previous work on anonymous systems, and then outline my future plans.

Anonymous Credentials

How do you take advantage of a cross-marketing campaign without letting Orbitz compile a complete dossier on your life? Suppose Holiday Inn offers a discount for Delta customers. If Delta gives its customers a signed coupon for Holiday Inn, then a customer can simply sell the coupon on e-Bay. The trick is to tie the signed coupon to a customer's identity, without revealing the customer's identity.

In joint work with Chase, Lysyanskaya, and Kohlweiss, I constructed an anonymous credentials system [BCKL08] that solves this problem. We give the first construction where showing a credential (i.e. coupon) is efficient, non-interactive (i.e. it consists of a single message), and provably secure. If Delta and Holiday Inn combine forces, they cannot tell which of Delta's customers used the coupon. Next, our team joined with Camenisch and Shacham to construct the first practical delegatable credentials system [BCC+07], which lets users delegate their credentials to others. Thus Holiday Inn can ask several airlines / on-line portals to distribute its coupons. When a customer comes to Holiday Inn, the hotel cannot identify the delegation chain via which the customer obtained the coupon. Once again, showing a credential is efficient, non-interactive, and provably secure. The only prior work on delegatable credentials (Chase and Lysyanskaya, 2006) resulted in credentials that were super-exponential in the length of the delegation chain, while our credentials are linear in the size of the delegation chain.

Secure Electronic Payment

When you send your credit card number to someone on e-Bay, what makes you sure that the merchant will (1) send you your widget and (2) not empty your account? Electronic cash (e-cash)

is an anonymous payment system that protects your account and identity, but does not guarantee that you will receive your widget. A fair exchange protocol allows two parties to trade (digital) items, ensuring that either both parties obtain their desired item or neither. It is a well-known result that it is impossible to perform a fair exchange without the help of a trusted third party (TTP). An optimistic fair exchange protocol invokes the TTP only if one of the parties deviates from the protocol. In most fair exchange protocols, the load on both parties and on the TTP is linear in the size of the items being exchanged (in terms of both space and computation). Fair exchange of e-cash has proven elusive because e-cash is anonymous.

Together with Camenisch and Lysyanskaya [CLM07], I designed the first penalty-free fair exchange system for e-cash. The protocol proceeds in two phases: first the user gives the merchant an encrypted e-coin and then the user and merchant perform a fair exchange for the decryption key. We designed an efficient mechanism for the merchant to verify that the user entered the fair exchange with the correct decryption key. Our protocol reduces the load on the TTP to be linear in the length of the decryption key (typically 128 bits). Using secret sharing techniques, we show how to combine the decryption keys to multiple e-coins into a single master key. Therefore, the load on the TTP is the same regardless of the cost of the item the user is purchasing. Our results have implications beyond e-cash; we can use the same method to exchange any other well-structured secret. We used our fair exchange technique to create the first cryptographically secure incentives system for onion remailing. In joint work with a research team at Brown [BCE+07], I investigated using our fair exchange system in other peer-to-peer networks. I solved the problem of overloaded TTPs by developing a fair exchange protocol that reduced the load on the TTP to be poly-logarithmic in the size of the merchant's digital goods.

Secret Sharing

How do you distribute pieces of a password among your twenty best friends so that a quorum of at least three people is needed to reconstruct the password? Secret sharing is important to many cryptographic applications, from multi-party computation to threshold signatures to attribute based encryption. Shamir and Blakley independently solved this classic problem in 1979 for a narrow definition of "quorum". I addressed the much more general problem of disjoint hierarchical secret sharing [Bel07], where users are assigned to different levels of importance (e.g. clearance levels). I gave the first polynomial-time solution that allowed new users to receive shares at any time.

In joint work with Camenisch, Hohenberger, Kohlweiss and Lysyanskaya [CHK+07], I applied secret sharing techniques to protect e-cash users from faulty hardware. In a normal e-cash scheme, a user withdraws a wallet of several e-coins and spends them one at a time. It is crucial that the user maintain a counter of spent e-coins; if the user spends more e-coins than the user withdrew from the bank, then the user reveals enough information for the bank to learn the user's identity. In the case of unreliable hardware (e.g. distributed sensors), an honest but faulty user might accidentally overspend. My glitch protection scheme lets the bank detect e-coins that are spent more than once, but cryptographically prevents anyone from discovering the user's identity until the user creates too many forged e-coins within a short time interval. In this work, we also show how to use e-coins for anonymous authentication.

Future Research

The Internet is a growing factor in people's lives. Government services, medical data, and commerce are all moving on-line. Our personal data is distributed amongst many semi-trusted authorities. Merchants can offer much more personalized services when they can collect and connect data from various sources. On the other hand, if the system is too connected, a security

breach at one source can spread across the entire system. The challenge is to design cryptographic protocols that let service providers obtain only the minimum data they need to provide their service.

I am interested in solving real-world security problems that arise from distributed semi-trusted systems. In 2007, it means delving into the Orbitz cross-marketing problem: how can an on-line portal profitably offer the services that Orbitz offers today without compromising the privacy and security of its users? As the scope of on-line services increases, so will the range of relevant security problems. Yet, I suspect the solution will remain constant: to protect user privacy and limit the spread of data to the bare minimum.

Since my work is ultimately technical in nature, I end by listing a few of the technical problems I plan to address in the near future.

E-coin batch verification. Currently, merchants deposit e-coins with the bank one at a time. Thus, the bank must do as much work as all merchants combined. The problem is that the bank must verify that each e-coin is valid. There has been previous success in batch verifying digital signatures using bilinear maps. A similar approach may work for e-coins, which are really a form of digital signature.

Anonymity revocation. During the setup phase of my anonymous credentials system, it is possible to create a master revocation key that can decrypt all pseudonyms and learn the identity of all users. This concentrates too much power in one authority. Secret sharing is useful for distributing secrets. A sophisticated application can result in policies in which the central authority can authorize revoking just one user's anonymity, or even authorize revoking the anonymity of just one user at just one authority.

Weakening security assumptions. Many interesting anonymous schemes, such as e-cash, are based on very strong assumptions. My work on anonymous credentials has shown that using the Groth-Sahai proof system as a building block for cryptographic systems can eliminate some of those assumptions.

Bibliography

[BCC+07] Mira Belenkiy, Jan Camenisch, Melissa Chase, Markulf Kohlweiss, Anna Lysyanskaya, Hovav Shacham. *Delegatable Anonymous Credentials*. In submission.

[BCKL08] Mira Belenkiy, Melissa Chase, Markulf Kohlweiss, Anna Lysyanskaya. *Non-Interactive Anonymous Credentials*. To appear in Theoretical Cryptography Conference (TCC) 2008.

[BCE+] Mira Belenkiy, Melissa Chase, Chris Erway, John Jannotti, Alptekin Kupcu, Anna Lysyanskaya, Eric Rachlin. *Making P2P Accountable without Losing Privacy*. Workshop on Privacy in the Electronic Society 2007, pp-31-40.

[Bel07] Mira Belenkiy. *Disjoint Hierarchical Threshold Secret Sharing*. In submission.

[CHK+07] Jan Camenisch, Susan Hohenberger, Markulf Kohlweiss, Anna Lysyanskaya and Mira Meyerovich. *How to Win the Clone Wars: Efficient Periodic n-Times Anonymous Authentication*. ACM Computer and Communications Security (ACM CCS) 2006, pp 201-210.

[CLM07] Jan Camenisch, Anna Lysyanskaya, and Mira Meyerovich. *Endorsed E-Cash*. IEEE Security and Privacy 2007, pp 101-115.

[LM06] Anna Lysyanskaya and Mira Meyerovich. *Provably Secure Steganography with Imperfect Sampling*. Public Key Cryptography 2006, pp 123-139.