Anonymous, Secure and Robust Multi-Recipient Communication

- PI: Nelly Fazio, Graduate Center & City College of CUNY
http://www-cs.ccny.cuny.edu/~fazio

Recipients' identities at times are as sensitive as content itself

⇩

Secure communication ought to protect more than just transmitted content!

This project proposes cryptographic tools for securing multicast communication beyond the mere secrecy of the data. Specific goals are to protect the recipients' identities and to hide the very fact that communication is taking place.

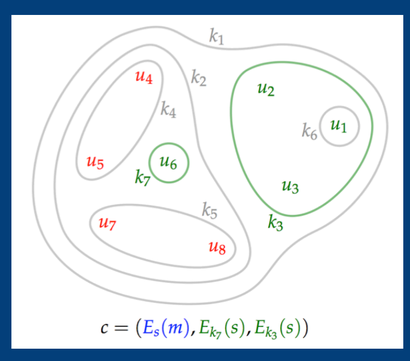
Background

- Broadcast Encryption (BS): transmit data to a dynamically changing set of recipients
  - Info about recipients is broadcast *in the clear*
- Steganography: hide the existence of the content within other, seemingly harmless communication
  - *Two* parties can communicate covertly, even in the presence of an adversary

Applications

- Networking technologies at support of military operations
  - Enable secure distribution of tactical data in missions with ad-hoc team formation while concealing identities of operatives authorized to access content
  - Enable covert distribution of tactical data for highly classified missions
- Private remote group storage
- Unlinkable secret handshake
  - Two parties can authenticate to each other as members of a group, without revealing any information to anyone who does not satisfy the group's authentication policy

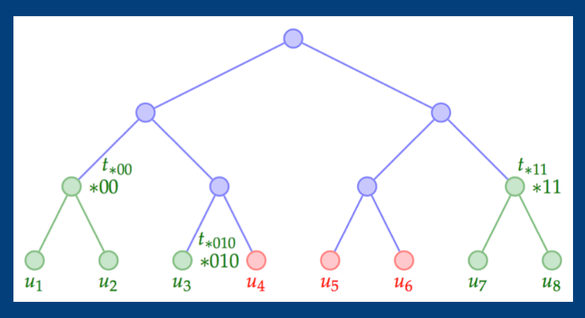
Design Methodology: Subset Cover Framework [NNL01, DF02]



To broadcast a message, first find the set of subsets covering the recipient set, and then encrypt the message under the keys of the coverset (hybrid encryption)

Enhanced Complete Subtree (CS) Method [DF02, FP12]

Idea
Anonymous (Hierarchical) Identity-Based Encryption
+
Tag system



Specific Aims

Anonymous Broadcast Encryption (AnoBE)

- Design schemes that *at once* provide transmission secrecy, recipients' anonymity, and performance comparable to standard broadcast encryption.

Robust Broadcast Encryption

- Enhance recipients' security by preventing malicious senders from crafting ambiguous ciphertexts that would appear valid to multiple decryptors.

Broadcast Steganography (BS)

- Devise primitives to transform a broadcast channel that disseminates content to a large user population (e.g., a radio station) into a medium for covert communication.

Collaborative Cloud Storage

- Design techniques to allow a *group* of users (each with their own personalized access rights) to store and accesses *shared* content in the cloud privately and **obliviously**.

Outsider Anonymous Broadcast Encryption

[PKC 12, ACITA 12, current]

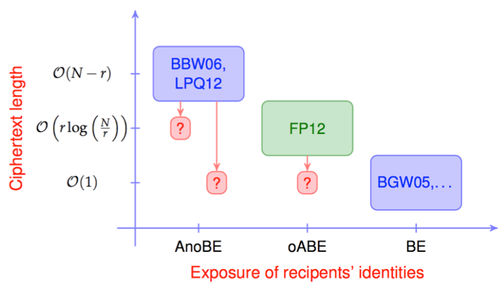
Relaxing receiver anonymity guarantees for better efficiency

- Recipients' identities hidden from outsiders…
- … but individual recipients might learn about each other
- Yield sublinear ciphertexts in the number of recipients, secure in the standard model against adaptive adversary

Efficient Constructions:

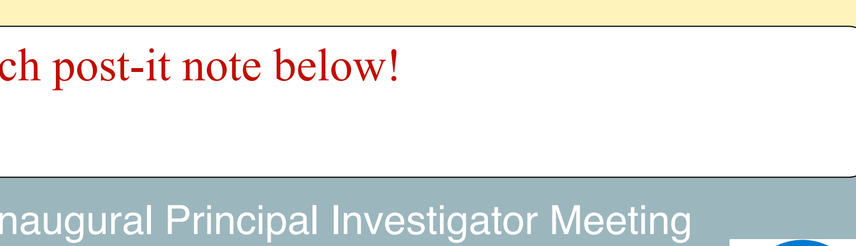
- Idea: PK-CS method + Anonymous IBE = oABE
- Generic CPA + Generic CCA + CCA w/ enhanced decryption

	Scheme	PK Length	SK Length	CT Length	Decryption Attempts
Regular	BBW06	$\mathcal{O}(N)$	$\mathcal{O}(1)$	$\mathcal{O}(N-r)$	$\mathcal{O}(N-r)$
	LPQ12	$\mathcal{O}(N)$	$\mathcal{O}(1)$	$\mathcal{O}(N-r)$	$\mathcal{O}(N-r)$
	FP12	$\mathcal{O}(1)$	$\mathcal{O}(\log N)$	$\mathcal{O}(r\log(\frac{N}{r}))$	$\mathcal{O}(r\log(\frac{N}{r})\log N)$
Enhanced	BBW06	$\mathcal{O}(N)$	$\mathcal{O}(1)$	$\mathcal{O}(N-r)$	1
	LPQ12	$\mathcal{O}(N)$	$\mathcal{O}(1)$	$\mathcal{O}(N-r)$	1
	FP12	$\mathcal{O}(N)$	$\mathcal{O}(\log N)$	$\mathcal{O}(r\log(\frac{N}{r}))$	1
	FP12	$\mathcal{O}(N^2)$	$\mathcal{O}(N)$	$\mathcal{O}(2r)$	1



Broadcast Steganography

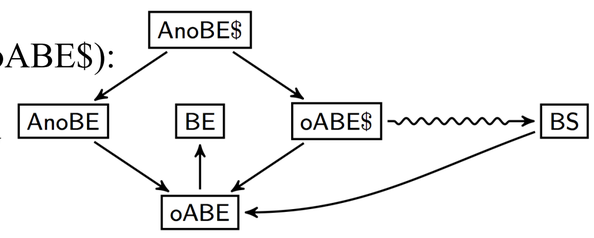
[current]



Enables a sender to communicate covertly with a dynamically designated set of receivers

- Recipients are able to recover the original content
- Unauthorized users and outsiders remain unaware of the covert communication
- Attain first BS scheme with sublinear ciphertexts secure in the standard model against adaptive adversaries

Outsider Anonymous BE with **pseudorandom ciphertexts** (oABE$): ciphertexts are required to be indistinguishable from truly random bit-strings



Interested in meeting the PIs? Attach post-it note below!

NSF Secure and Trustworthy Cyberspace Inaugural Principal Investigator Meeting
Nov. 27 -29th 2012
National Harbor, MD

National Science Foundation
WHERE DISCOVERIES BEGIN

CAISS