Outsider-Anonymous Broadcast Encryption
with Sublinear Ciphertexts

Nelly Fazio[1,2] and Irippuge Milinda Perera[2]

[1] The City College of CUNY
fazio@cs.ccny.cuny.edu

[2] The Graduate Center of CUNY
{nfazio,iperera}@gc.cuny.edu

Motivation & State-of-the-Art

❖ **Crypto tools for secure multicast communications**

❖ **Broadcast Encryption (BE)**

- Transmit data to a dynamically changing set of recipients
- Info about receivers is broadcast in the clear

**Receivers' identities are often sensitive.
Secure communication ought to protect
more than just transmitted content!**

❖ **Anonymous BE (AnoBE):** also hides receiver set [BBW06]

- Ciphertext linear in number of recipients
- Security model against static adversary
- Security of enhanced construction based on the ROM
- [LPQ12] recently removed ROM + active adversary

Applications

❖ **Networking technology for military operations**

- AnoBE enables secure distribution of tactical data in missions with ad-hoc team formation while concealing identities of operatives authorized to access content

❖ **BE enables efficient encrypted file systems**

- AnoBE avoids disclosure of identities of authorized users, not only from outsiders, but also from one another

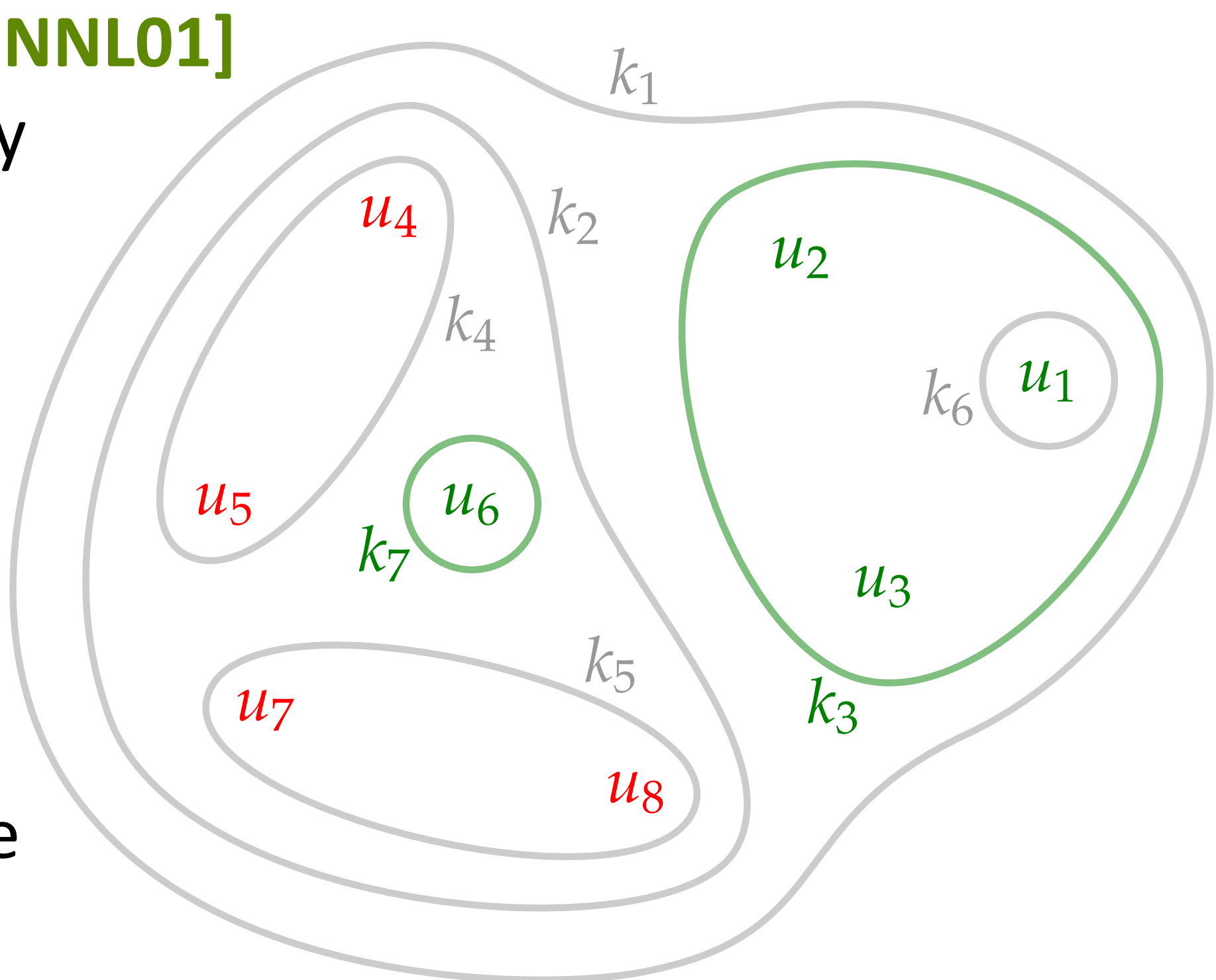
Primitives

❖ **Anonymous Identity-based Encryption (AIBE)**

- A public-key encryption scheme where the user public key is an arbitrary bit-string
- Ciphertext hides the identity under which it is encrypted

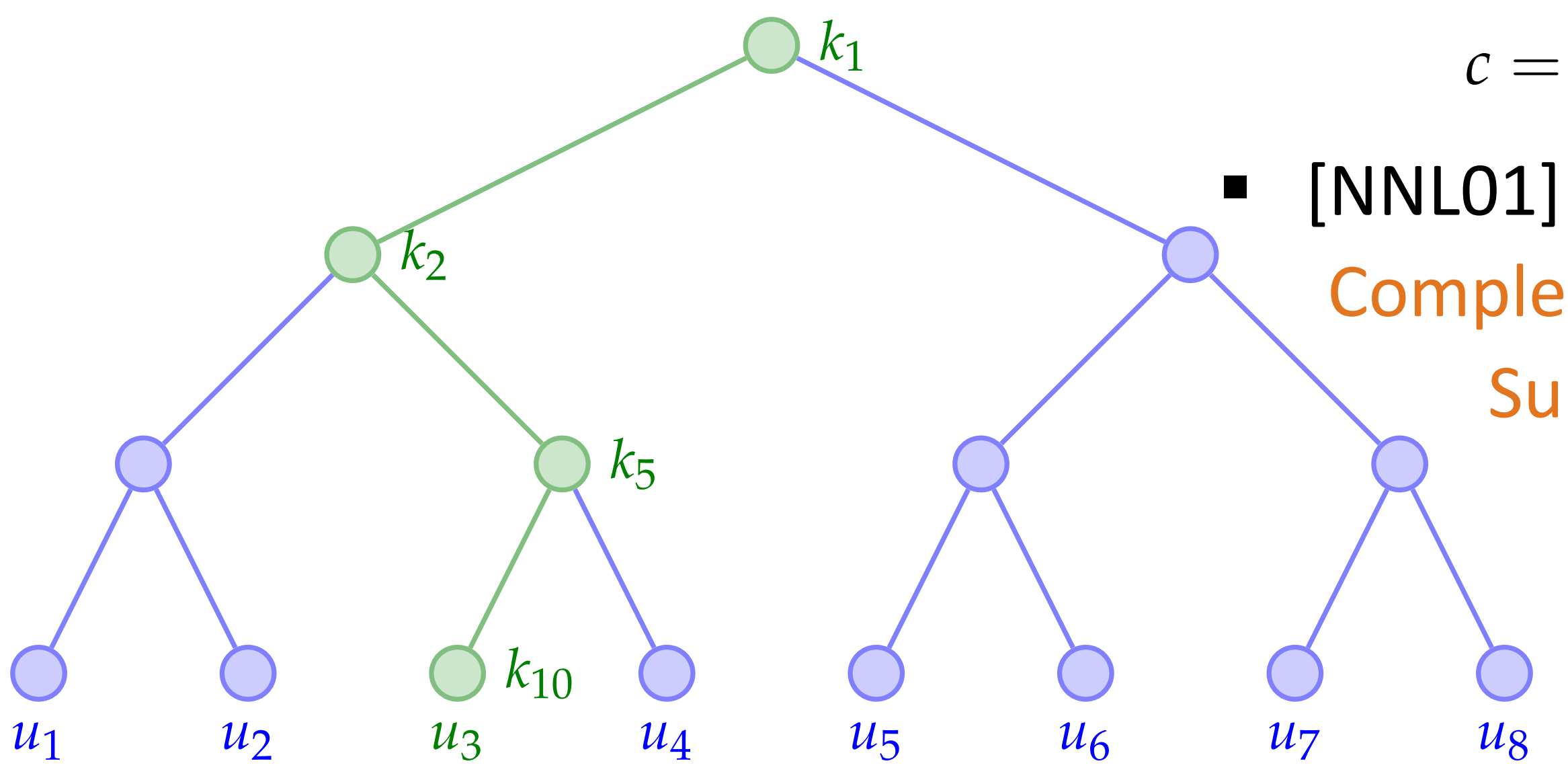
❖ **The Subset Cover (SC) Framework [NNL01]**

- **Goal:** Define and analyze security of revocation schemes in the private-key setting
- Users belong to multiple subsets with associated keys
- To broadcast a message, first find the cover set, and then hybrid-encrypt the message under the keys of the coverset



$$c = (E_s(m), E_{k_7}(s), E_{k_3}(s))$$

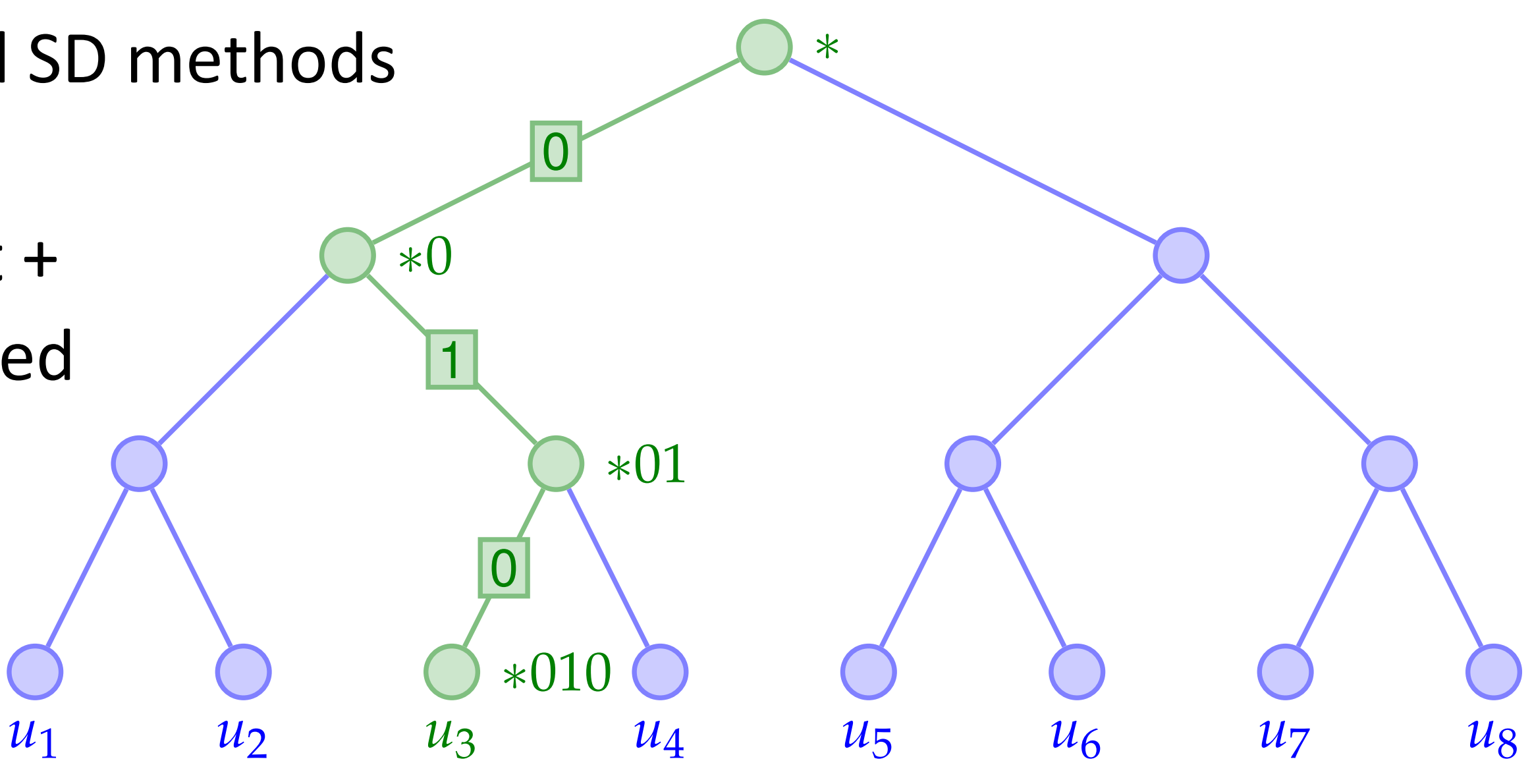
- [NNL01] presents two SC algorithms: Complete Subtree (CS) method and Subset Difference (SD) method



Private-Key Complete Subtree Method of [NNL01]

❖ **Extension of the Subset Cover Framework to Public-Key Setting [DF02]**

- [DF02] extends the CS and SD methods to the public-key setting
- **Idea:** Novel ID assignment + (Hierarchical) Identity-Based Encryption ((H)IBE)



Public-Key Complete Subtree Method of [DF02]

Our Contribution (Published at PKC'12)

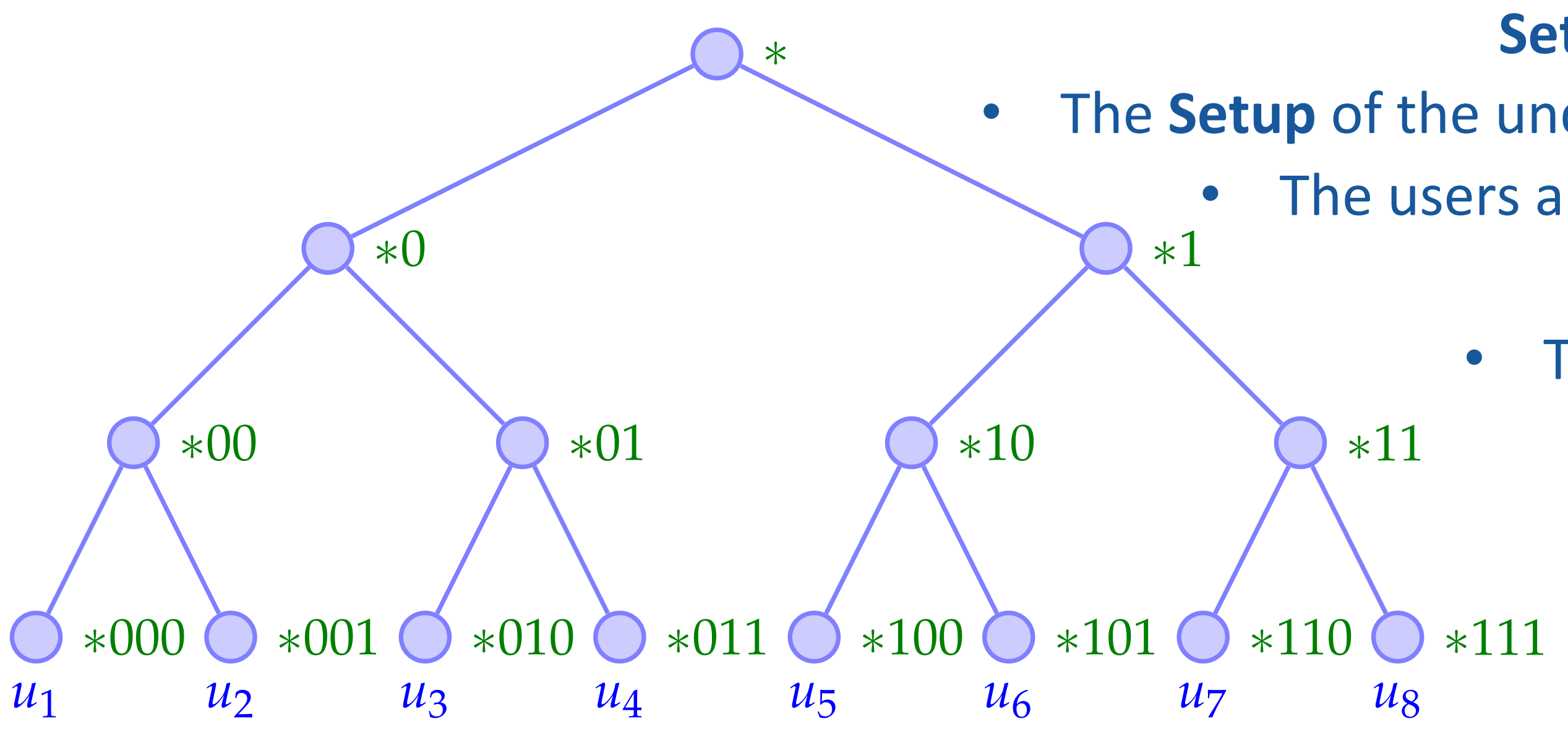
❖ **Outsider-Anonymous Broadcast Encryption (oABE)**

- Relaxing receiver anonymity guarantees for better efficiency
- Recipient's identities hidden from outsiders…
- … but individual recipients might learn about each other
- Attain sub-linear ciphertexts in the number of recipients (in the standard model), and security against active adversary

Our Constructions

❖ **Idea:** PK-CS method + Anonymous IBE = oABE

❖ Generic CPA, Generic CCA, CCA with enhanced decryption

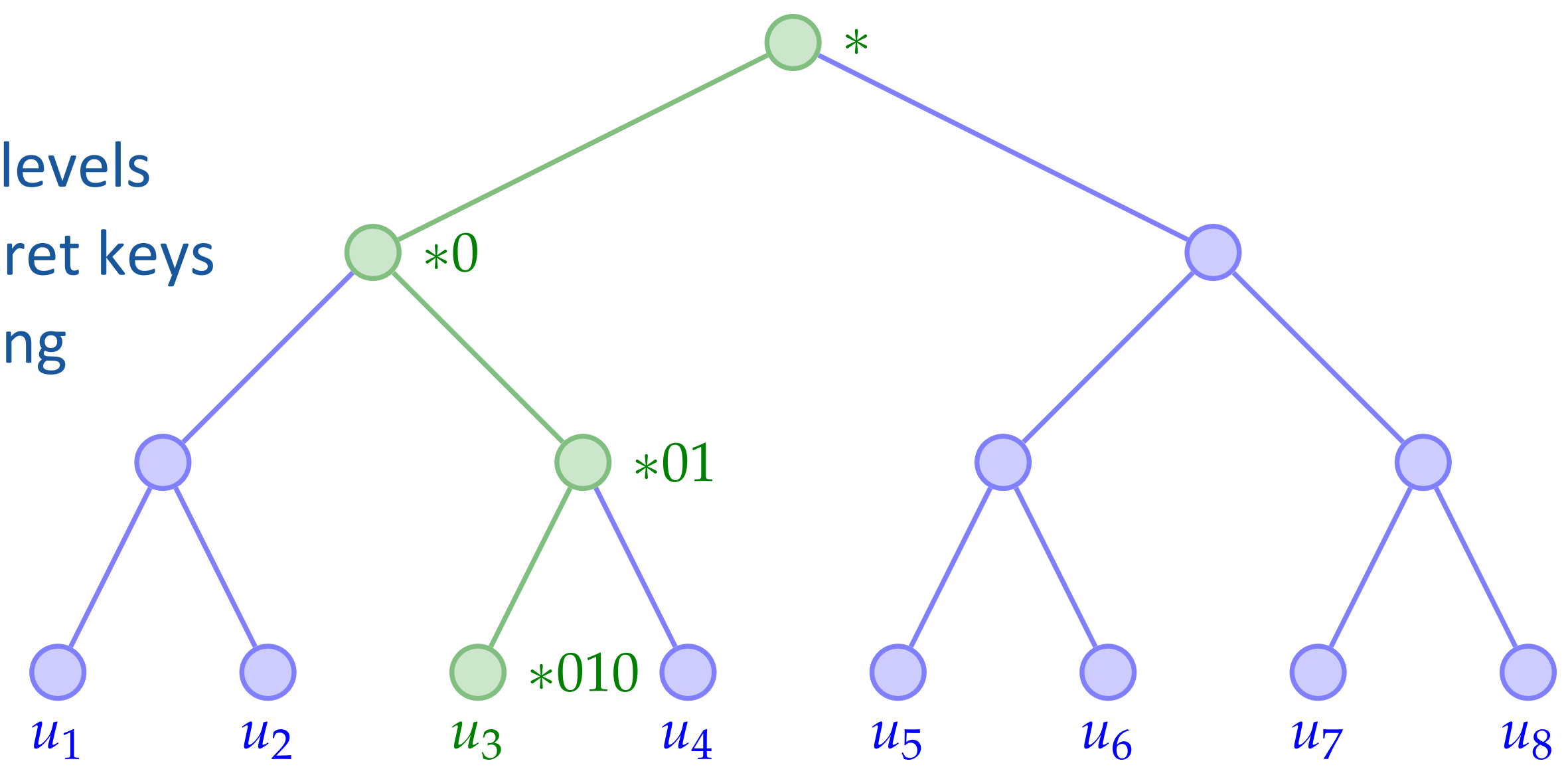


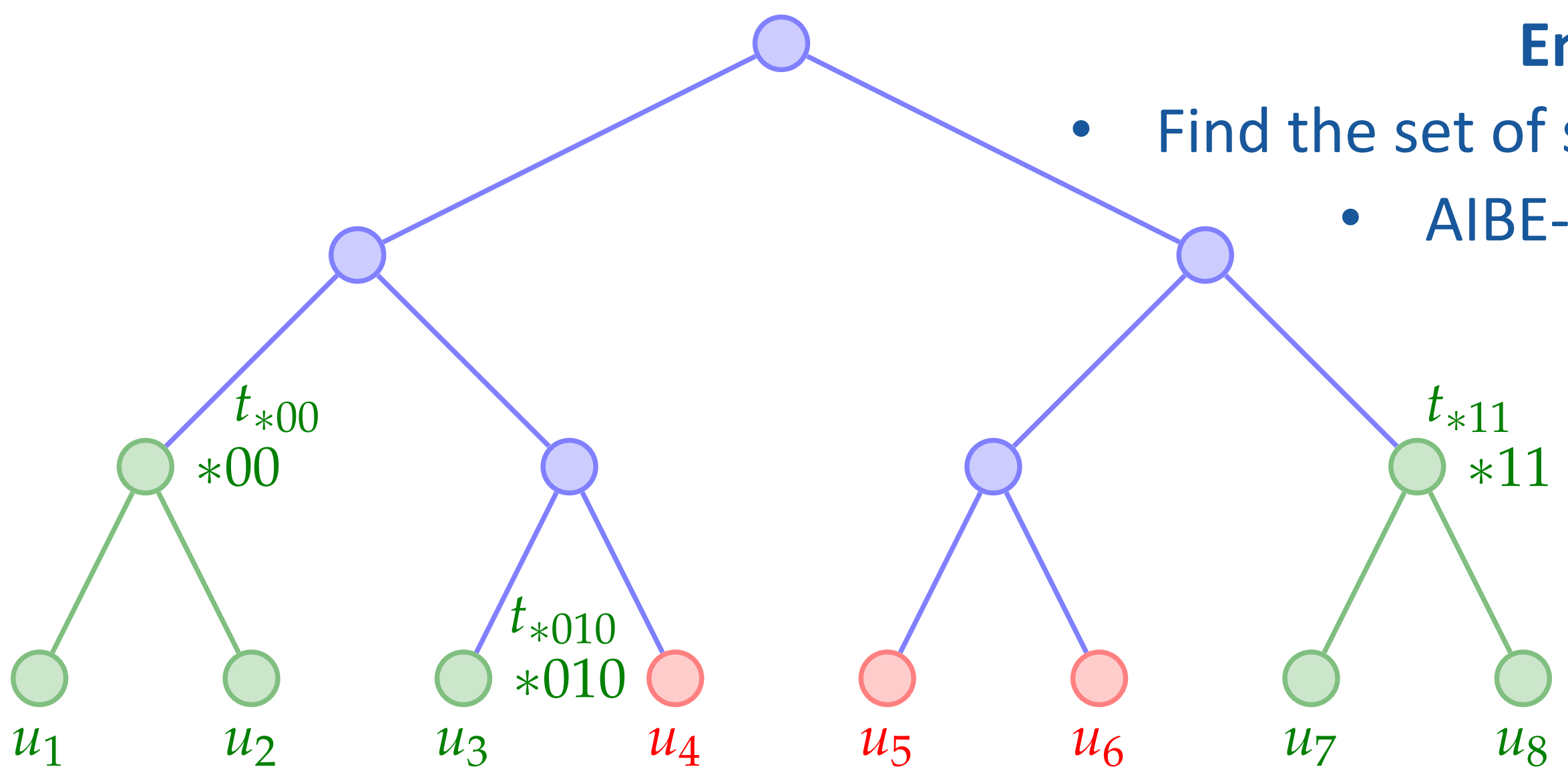
Setup

- The **Setup** of the underlying AIBE scheme is run
- The users are denoted by the leaves of a perfect binary tree
- The subtrees of this tree are the possible subsets

KeyGen

- Each u_i belongs to $log(N)+1$ levels
- u_i is given $log(N)+1$ AIBE secret keys of the identities corresponding to the ancestor nodes in those levels





Encrypt/Decrypt

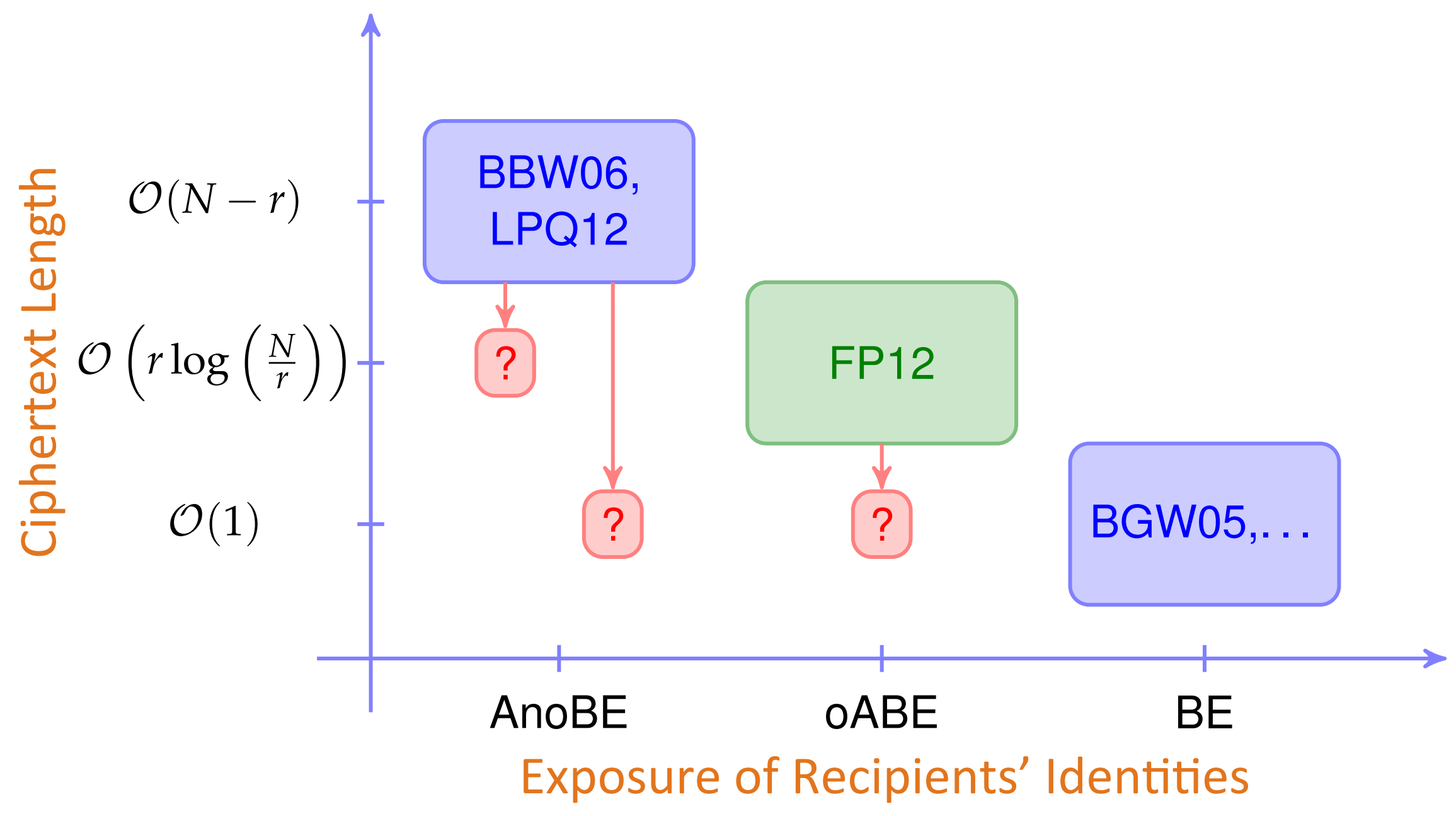
- Find the set of subtrees covering the recipients
- AIBE-Encrypt the message under the identities corresponding to the root nodes of those subtrees
- Also attach a "tag" to each ciphertext to allow efficient decryption at the receivers

Comparisons

	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	$\mathcal{O}(N)$	$\mathcal{O}(1)$	$\mathcal{O}(N-r)$	$\mathcal{O}(N-r)$
	FP12a	$\mathcal{O}(1)$	$\mathcal{O}(\log N)$	$\mathcal{O}\left(r\log\left(\frac{N}{r}\right)\right)$	$\mathcal{O}\left(r\log\left(\frac{N}{r}\right)\log N\right)$
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
	FP12a	$\mathcal{O}(N)$	$\mathcal{O}(\log N)$	$\mathcal{O}\left(r\log\left(\frac{N}{r}\right)\right)$	1
	FP12b	$\mathcal{O}(N^2)$	$\mathcal{O}(N)$	$\mathcal{O}(r)$	1

N: total number of users. r: number of revoked users.

Future Work



The 1st Computer Science Student Workshop
The Graduate Center of CUNY
May 3, 2013