ID-Based Encryption for Complex Hierarchies with Applications to Forward Security and Broadcast Encryption

Danfeng Yao
Brown University

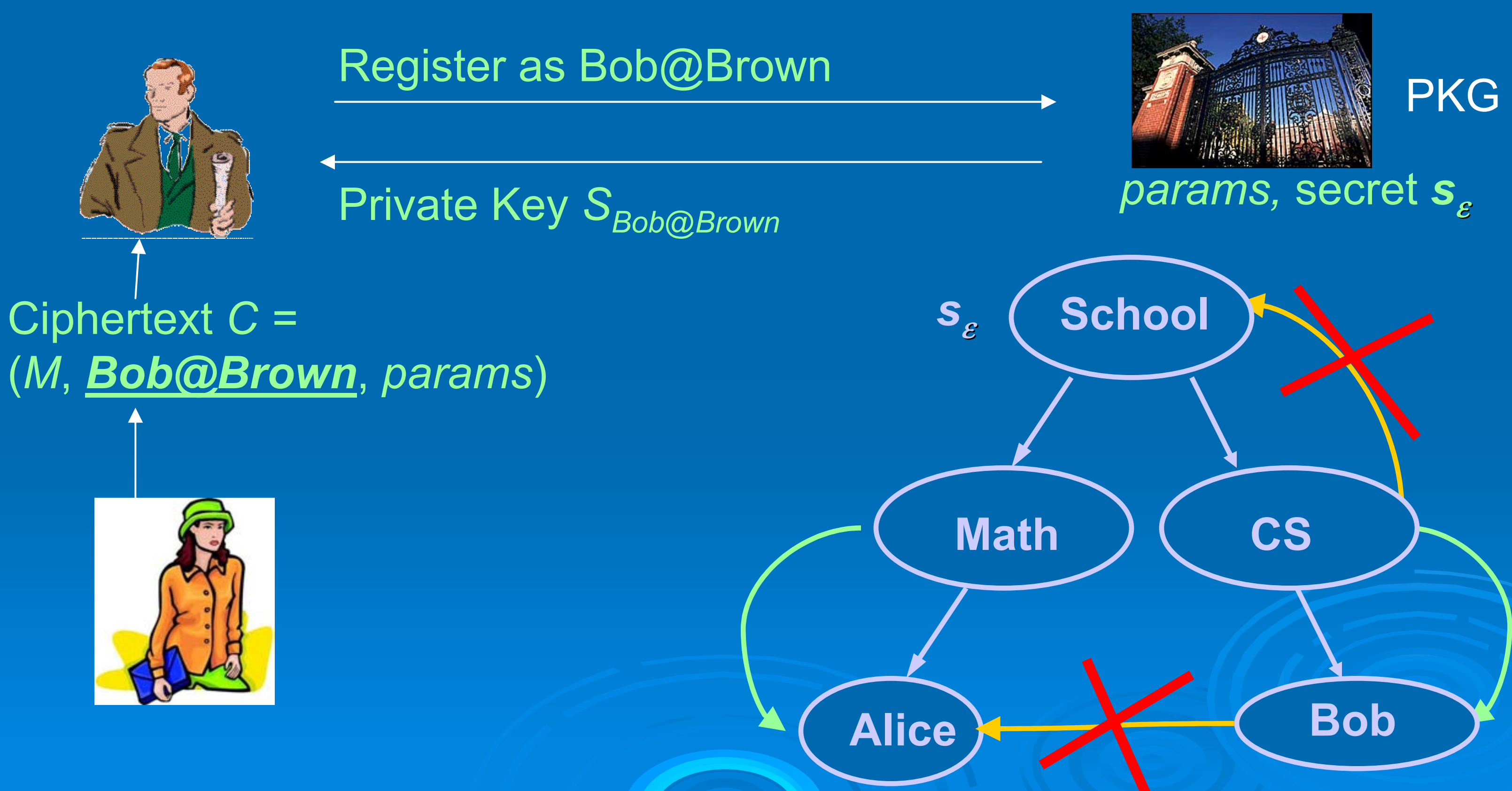
Nelly Fazio
New York University

Yevgeniy Dodis
New York University

Anna Lysyanskaya
Brown University

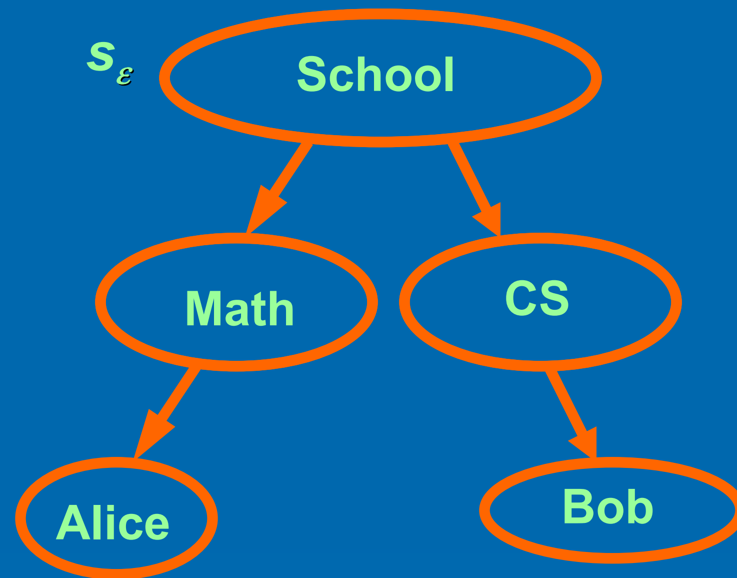
Identity-based Encryption (IBE) and Hierarchical IBE (HIBE)

- IBE [Shamir 84] [Boneh Frankline 01] [Cocks 01] [Canetti Halevi Katz 03] [Boneh Boyen 04] [Waters 04]
- HIBE [Horwitz Lynn 02] [Gentry Silverberg 02] [Boneh Boyen 04]



Why need forward-secure HIBE?

- In HIBE, exposure of parent private keys compromises children's keys
- Forward security
  - [Gunther 89] [Diffie Oorschot Wiener 92] [Anderson 97] [Bellare Miner 99] [Malkin Micciancio Miner 02] [Canetti Halevi Katz 03]
  - Secret keys are evolved with time
  - Compromising current key does NOT compromise past communications
- Forward-secure HIBE mitigates key exposure

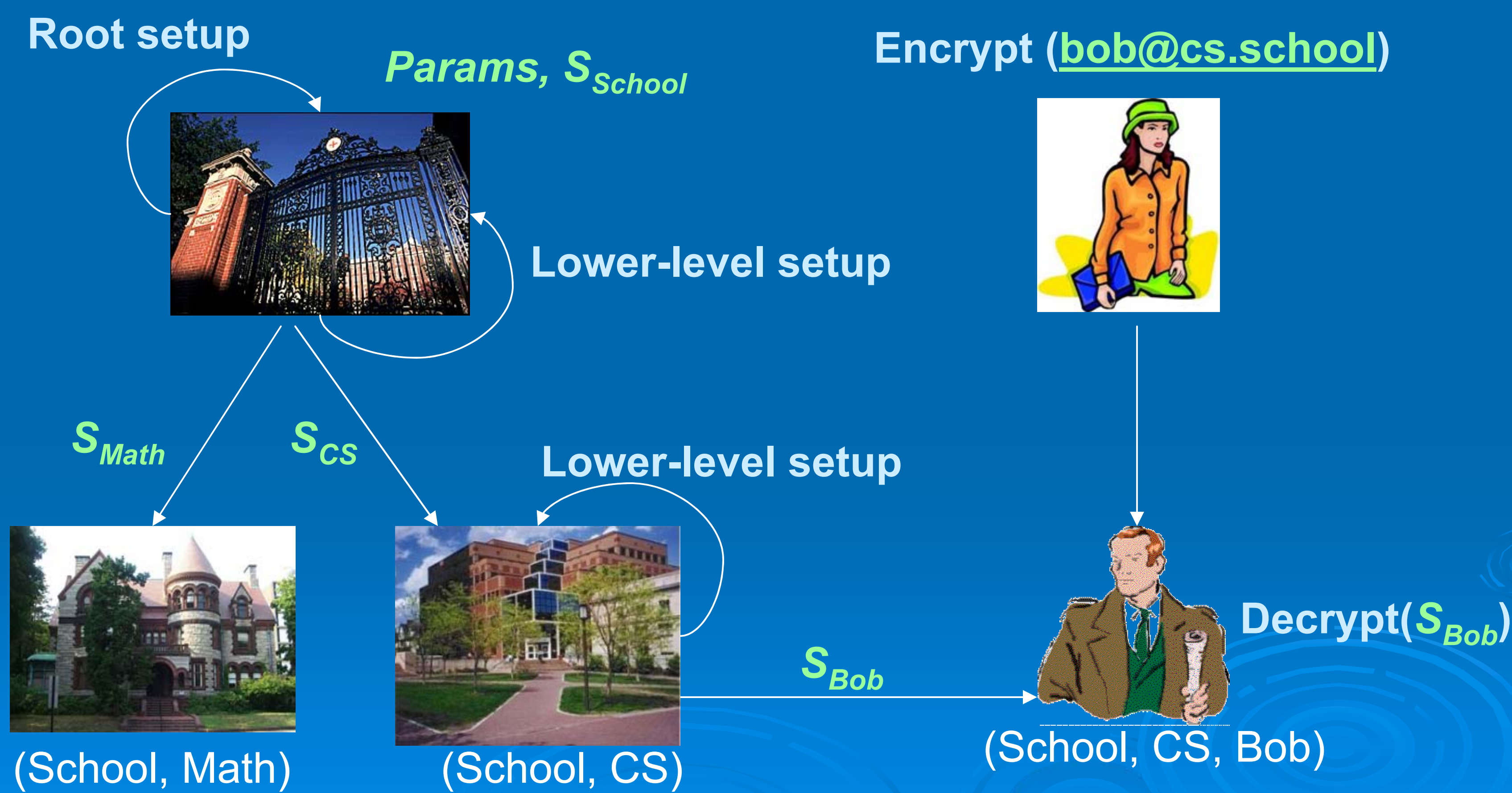


Applications of fs-HIBE

- Forward-secure public-key broadcast encryption (fs-BE)
  - BE schemes: [Fiat Naor 93] [Luby Staddon 98] [Garay Staddon Wool 00] [Naor Naor Lotspiech 01] [Halevy Shamir 02] [Kim Hwang Lee 03] [Goodrich Sun Tamassia 04] [Gentry Ramzan 04]
  - HIBE is used in public-key broadcast encryption [Dodis Fazio 02]
  - Forward security is especially important in BE
- Multiple HIBE: Encryption scheme for users with multiple roles

Hierarchical IBE

- HIBE [Horwitz Lynn 02] [Gentry Silverberg 02] [Boneh Boyen 04]

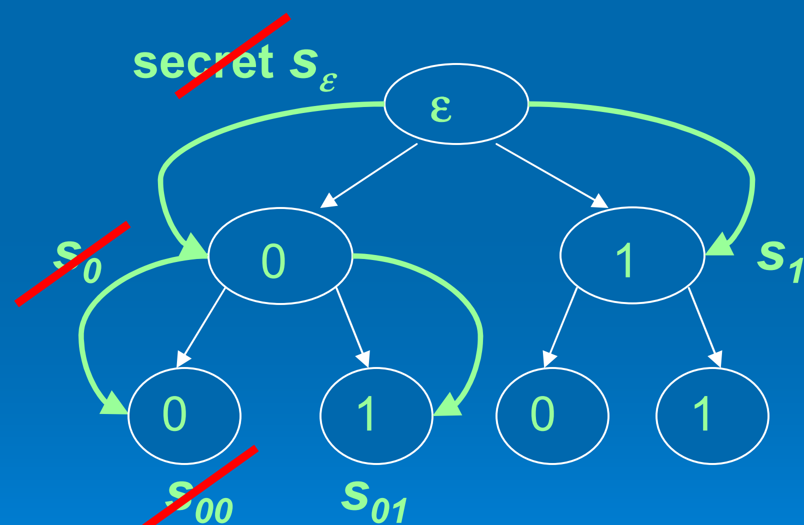


Forward-secure Public-Key Encryption

- fs-PKE (Canetti, Halevi, and Katz 2003)
  - Used to protect the private key of one user
  - Based on Gentry-Silverberg HIBE
  - A time period is a binary string
  - Private key contains decryption key and future secrets
  - Erase past secrets in algorithm **Update**

Total time periods: 4

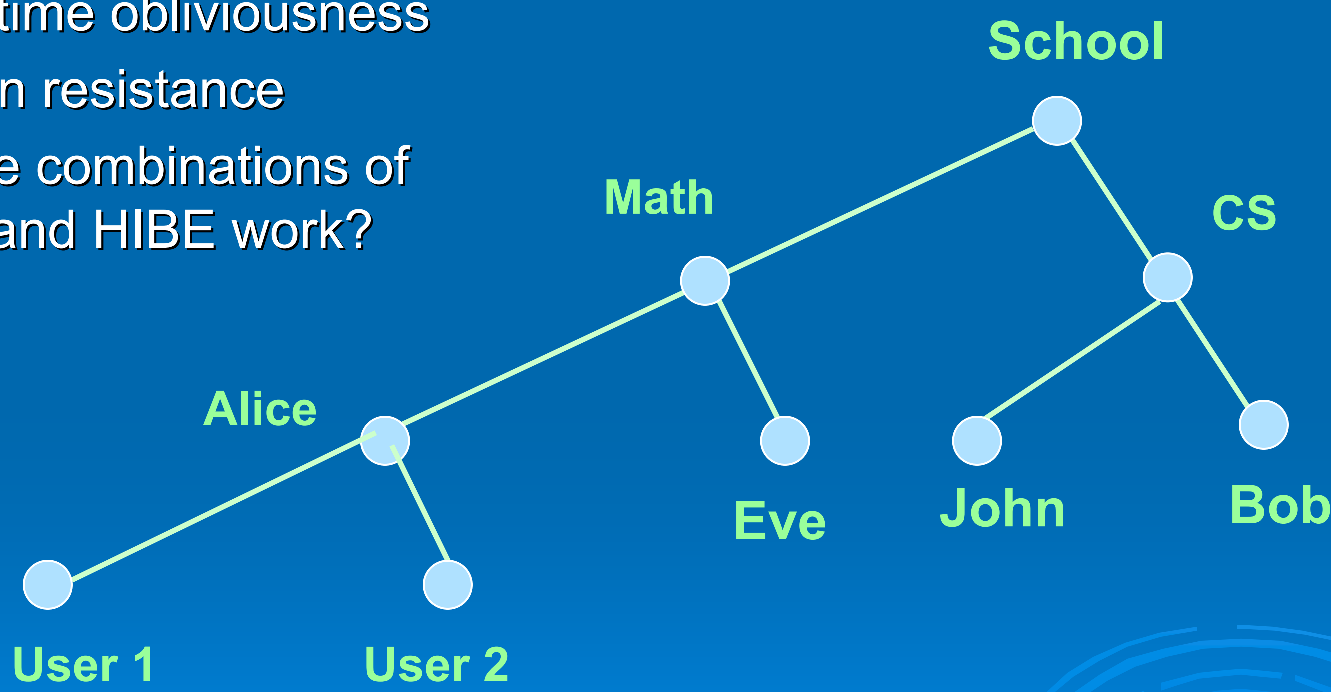
Period 1: (0 0)
Period 2: (0 1)
Period 3: (1 0)
Period 4: (1 1)



Encrypt(*params*, 0 0)

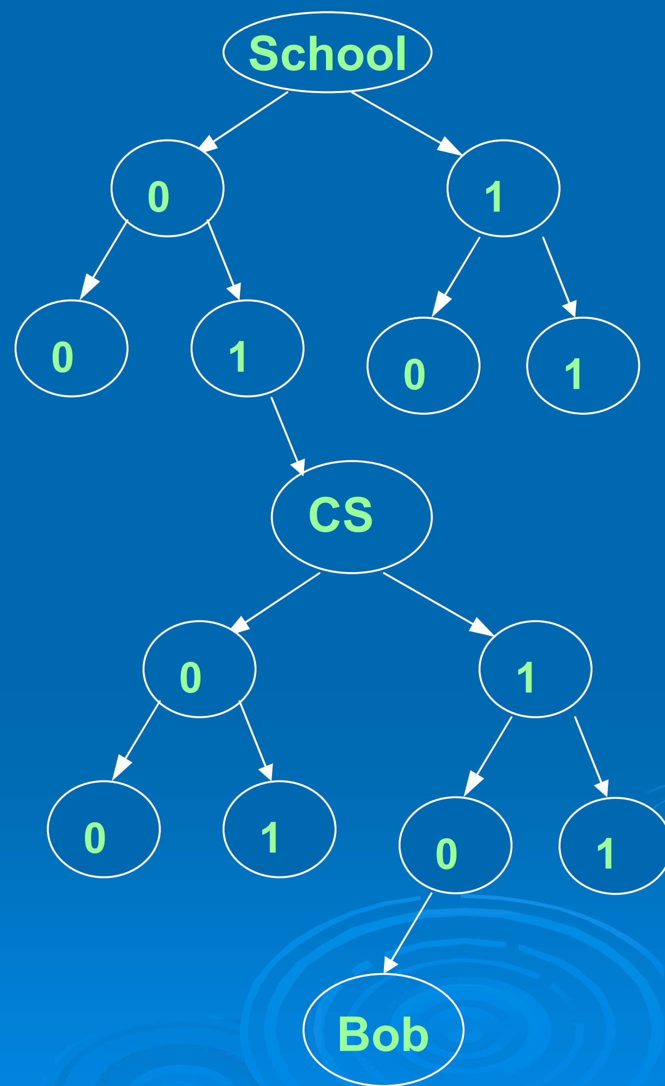
fs-HIBE requirements

- Dynamic joins
  - Users can join at any time
- Joining-time obliviousness
- Collusion resistance
- Do naïve combinations of fs-PKE and HIBE work?



An fs-HIBE attempt

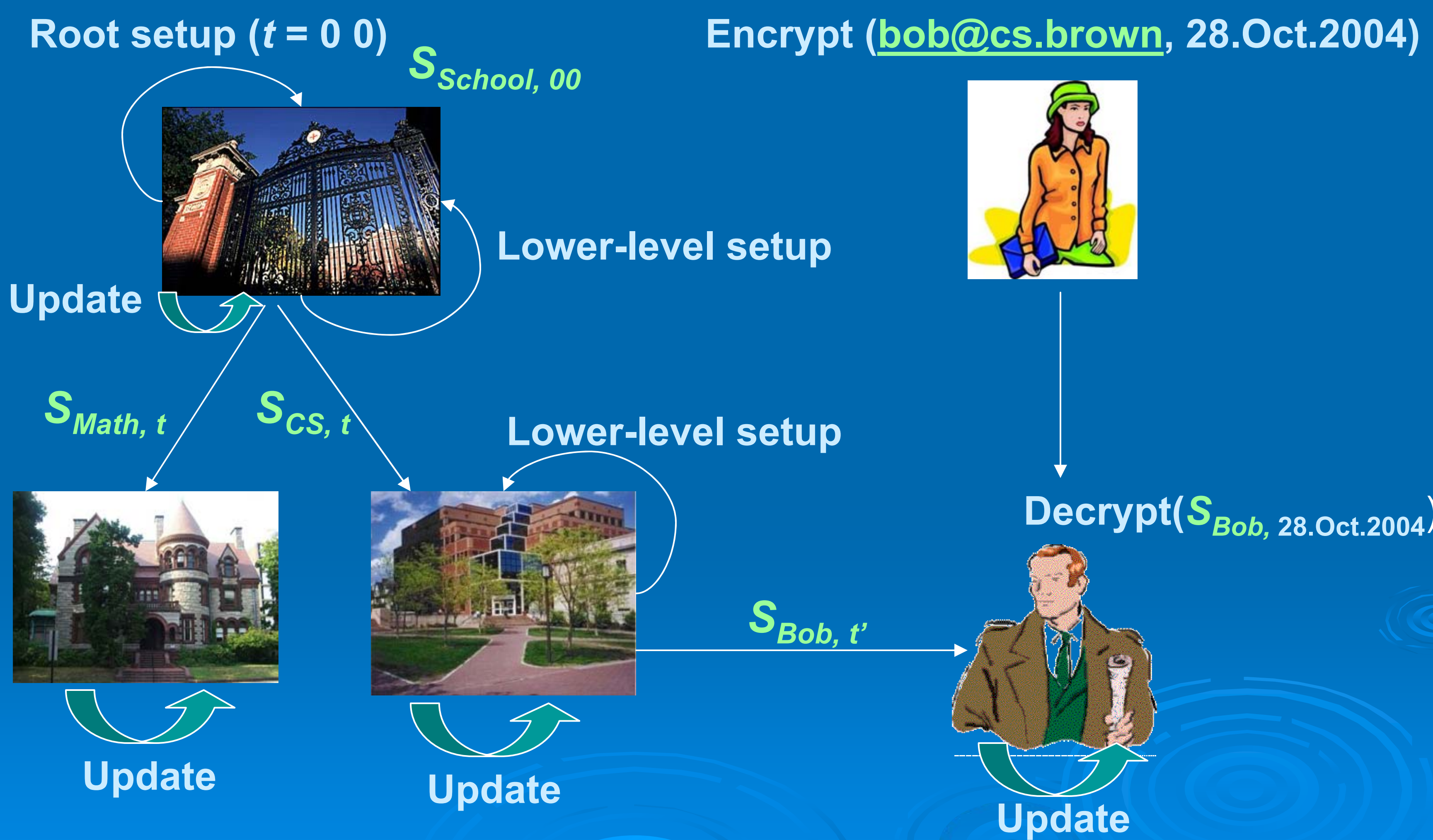
- Each entity node maintains one tree
  - For computing children's private keys
  - For the forward security of itself
- Not joining-time-oblivious
  - CS joins at (0 1) with public key (*School, 0, 1, CS*)
  - Bob joins at (1 0) with public key (*School, 0, 1, CS, 1, 0, Bob*)
  - Sender needs to know when CS and Bob joined



Overview of our fs-HIBE scheme

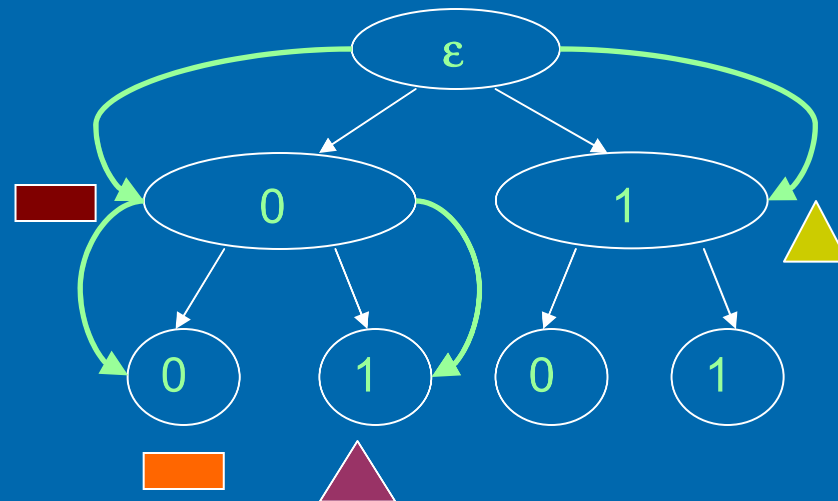
- Based on HIBE [Gentry Silverberg 02] and fs-PKE (Canetti Halevi Katz 03] schemes
- Scalable, efficient, and provable secure
  - Forward security
  - Dynamic joins
  - Joining-time obliviousness
  - Collusion resistance
- Security based on Bilinear Diffie-Hellman assumption [BF 01] and random oracle model [Bellare Rogaway 93]
  - Chosen-ciphertext secure against adaptive-chosen-(ID-tuple, time) adversary

fs-HIBE algorithm definitions



fs-HIBE Root setup

- Similar to key derivation of fs-PKE
- Private key for time (0 0) contains decryption key for (0 0), and future secrets
- Generates *params*, decryption key, and future secrets
  -  = $s_\varepsilon \times H(0 \,||\, \text{School})$
  -  = $s_\varepsilon \times H(1 \,||\, \text{School})$
  -  =  $+\ s' \times H(0\ 0 \,||\, \text{School})$
  -  =  $+\ s' \times H(0\ 1 \,||\, \text{School})$
  - Erase , s_ε and s'

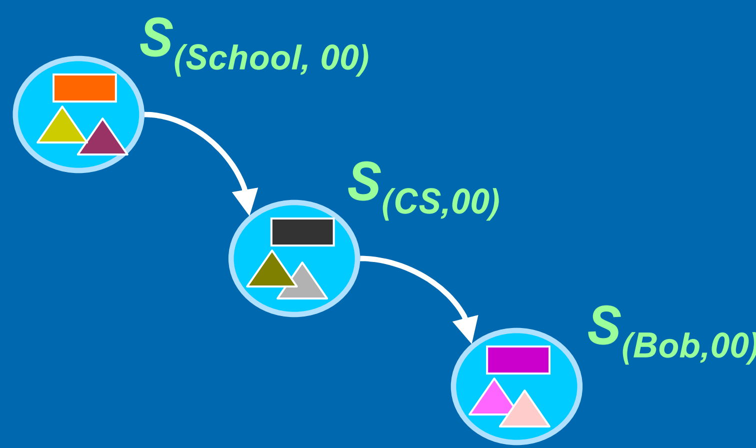


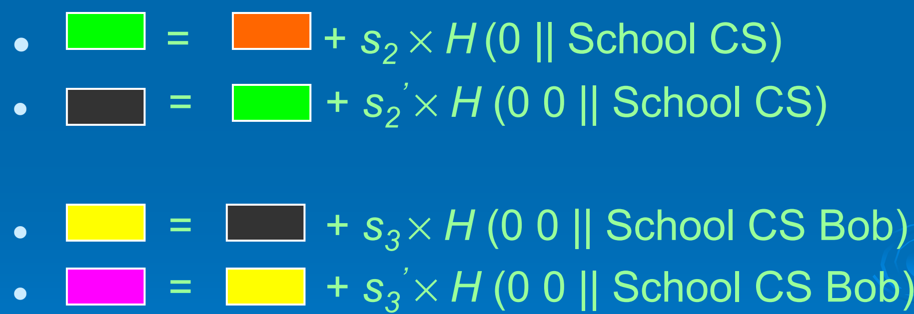
$S_{(School,00)}$

|| String concatenation
\+ Group addition operation
× Group multiplication operation

fs-HIBE algorithms cont'd

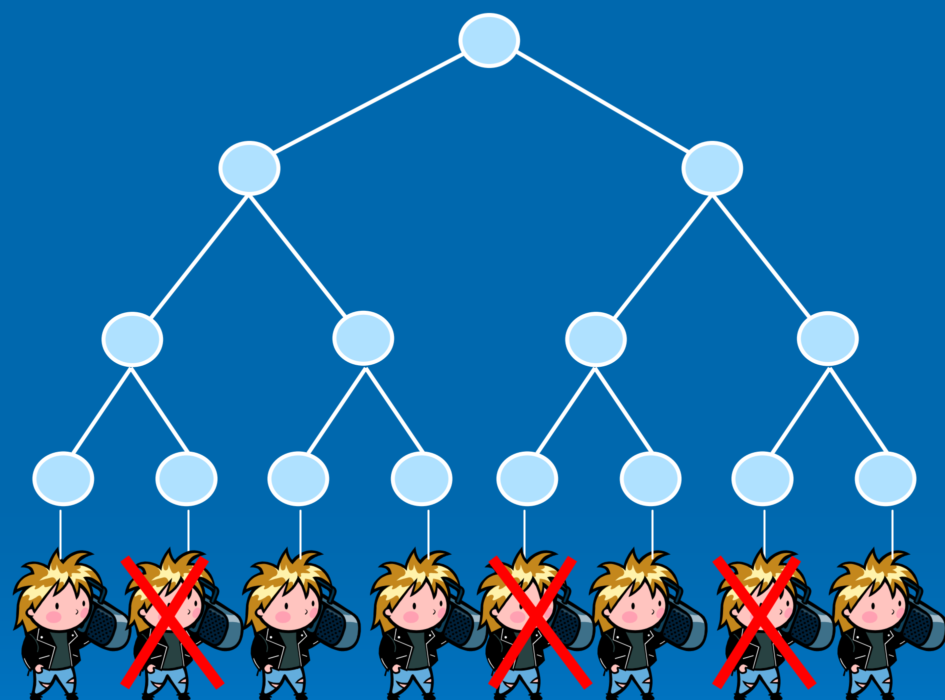
- **Lower-level setup** is used by a node at time *t* to compute keys for its children
  - Generalization of **Root setup**
  - Computes both decryption key at time *t*, and future secrets
- **Update**
  - Similar as in fs-PKE
- **Encrypt**
  - Ciphertext: $O(h \log(N))$
- **Decrypt**
  - Bob's decryption key is used





- Erase intermediate secrets

HIBE in broadcast encryption



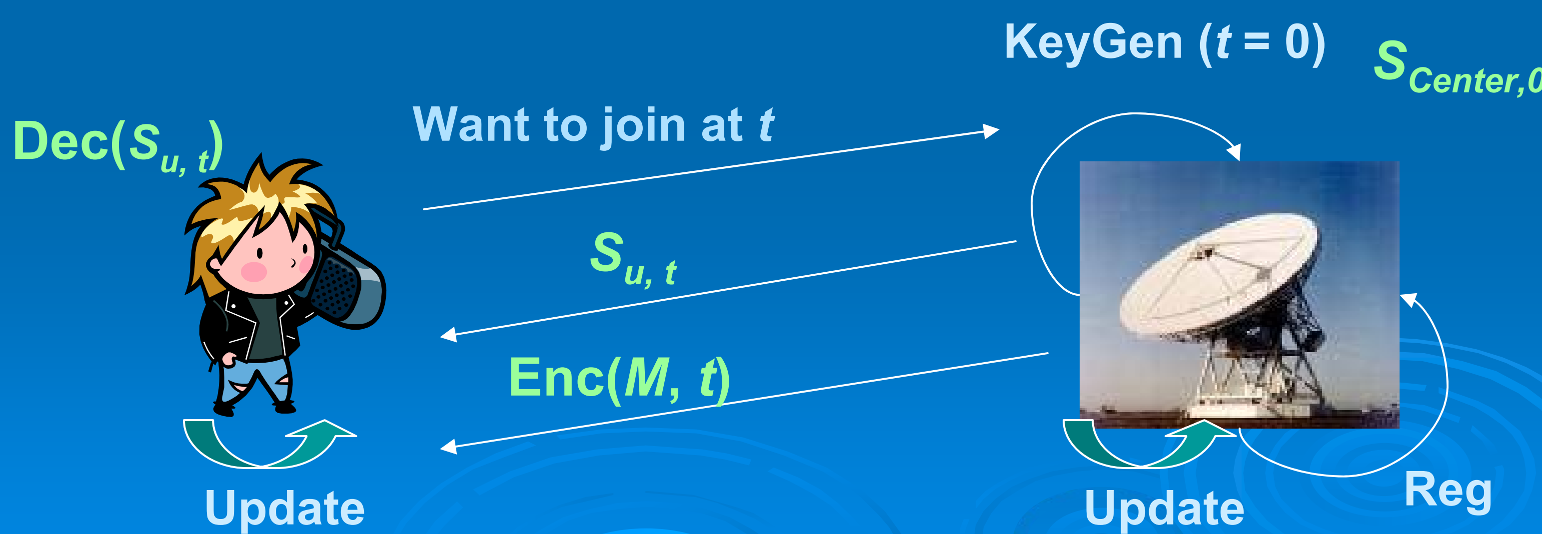
Center

Valid user

Revoked user

Forward-secure broadcast encryption

- Public-key BE by Dodis and Fazio
  - Uses HIBE to implement a subset-cover framework [Naor Naor Lotspiech 01]
- A scalable fs-BE scheme
  - Dynamic joins and joining-time obliviousness
  - Users update secret keys autonomously
- Algorithms: **KeyGen**, **Reg**, **Upd**, **Enc**, **Dec**



Security of fs-HIBE

- "Security definitions"
- Security based on hardness of BDH problem and random oracle model
- **Theorem** *Suppose there is an adaptive adversary A that has advantage ε against one-way secure fs-HIBE targeting some time and ID-tuple at level h, and that makes q_{H2} hash queries to hash function H_2 and q_E lower-level setup queries. Let N be total number of time, $l = \log_2 N$. If H_1, H_2 are random oracles, then exists an algorithm B that solves BDH problem with advantage* $\varepsilon\left(\left(\frac{h+l}{e(2lq_E+h+l)}\right)^{(h+l)/2} - \frac{1}{2^n}\right)/q_{H2}$.