Role-Based Cascaded Delegation:

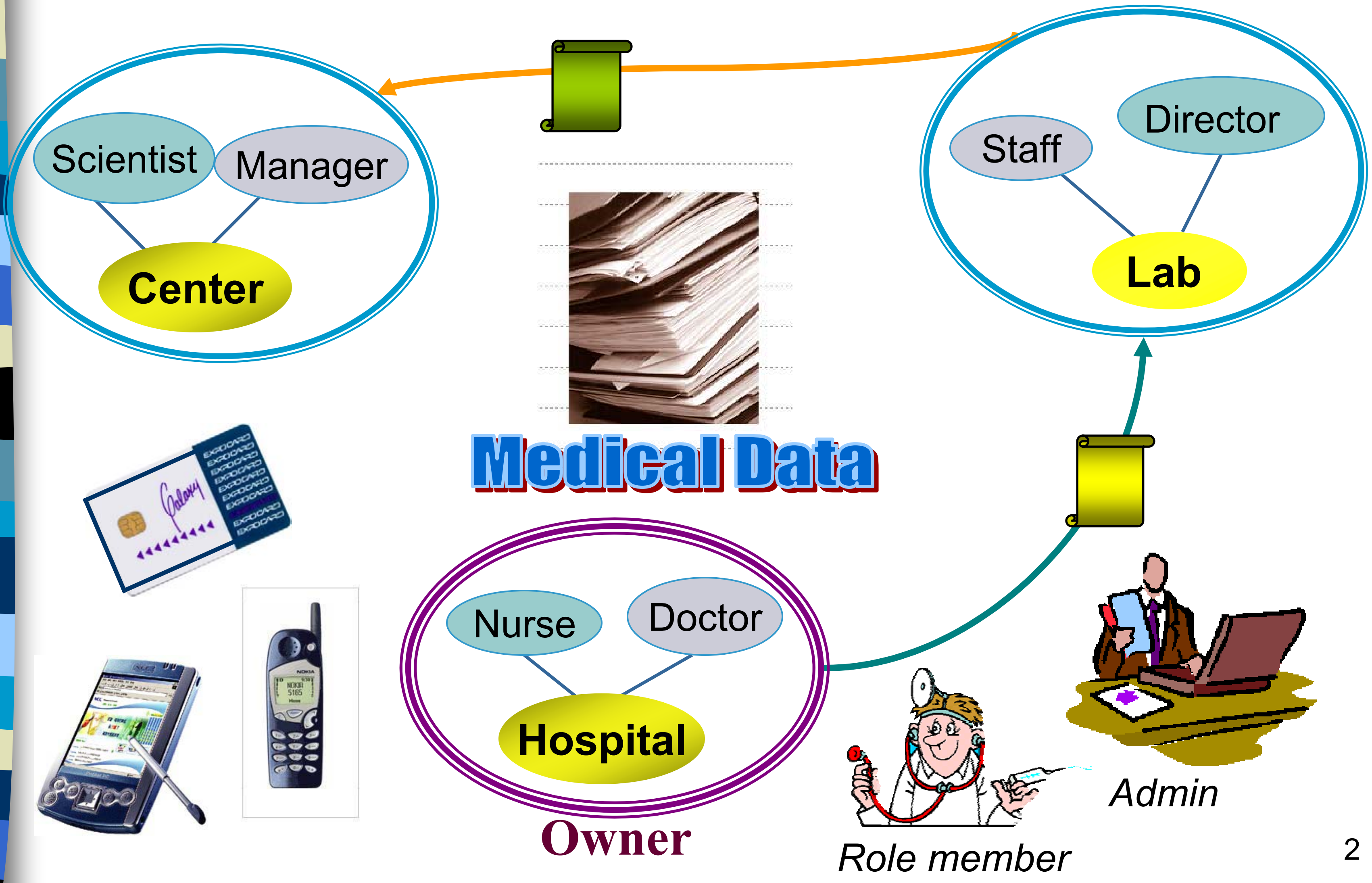
A Decentralized Delegation Model for Roles

Roberto Tamassia
Brown University

Danfeng Yao
Brown University

William H. Winsborough
George Mason University

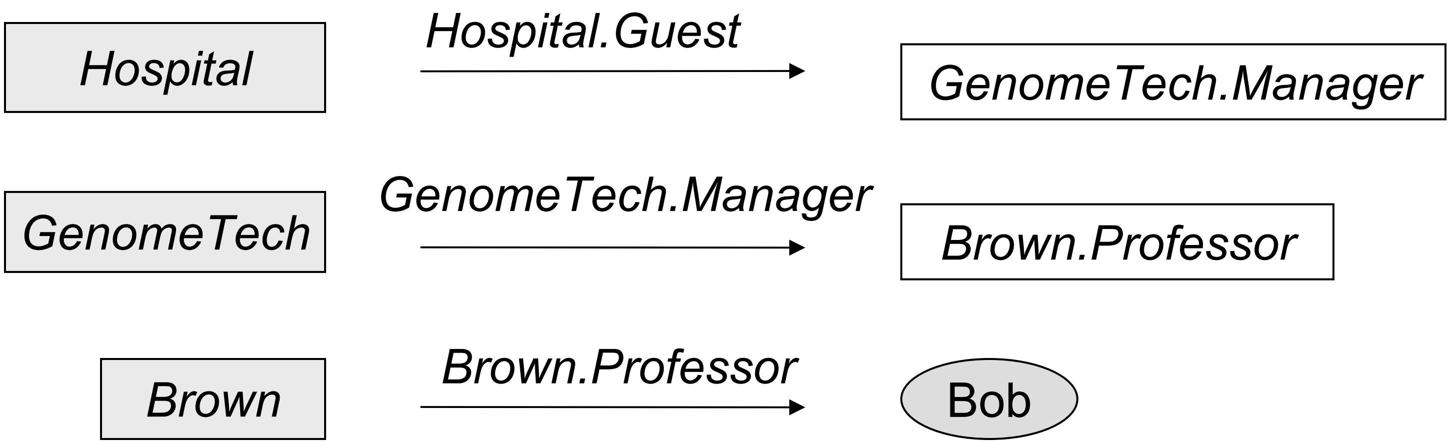
Resource Sharing and Delegation in Distributed Environment



Delegation chain

- Delegation is essential in distributed environment
  - KeyNote (Blaze Feigenbaum Ioannidis Keromytis 1998)
  - Trust Establishment (Herzberg Mass Michaeli *et al.* 2000)
  - *X*-Sec (Bertino Castano Ferrari 2001)
  - SPKI/SDSI (Clarke Elien Ellison *et al.* 2001)
  - OASIS (Bacon Moody Yao 2001)
  - *RT* framework (Li Winsborough Mitchell 2002)
  - *PBDM* (Zhang Oh Sandhu 2003)
- Delegation chain
  - Connects the resource owner to unknown ones
- Discovering and verifying delegation chains are two key issues
  - Discovery: find a delegation chain
  - Verification: authenticate the credentials on the chain

Existing role-based delegation model



Hospital —*Hospital.Guest*→ *GenomeTech.Manager*

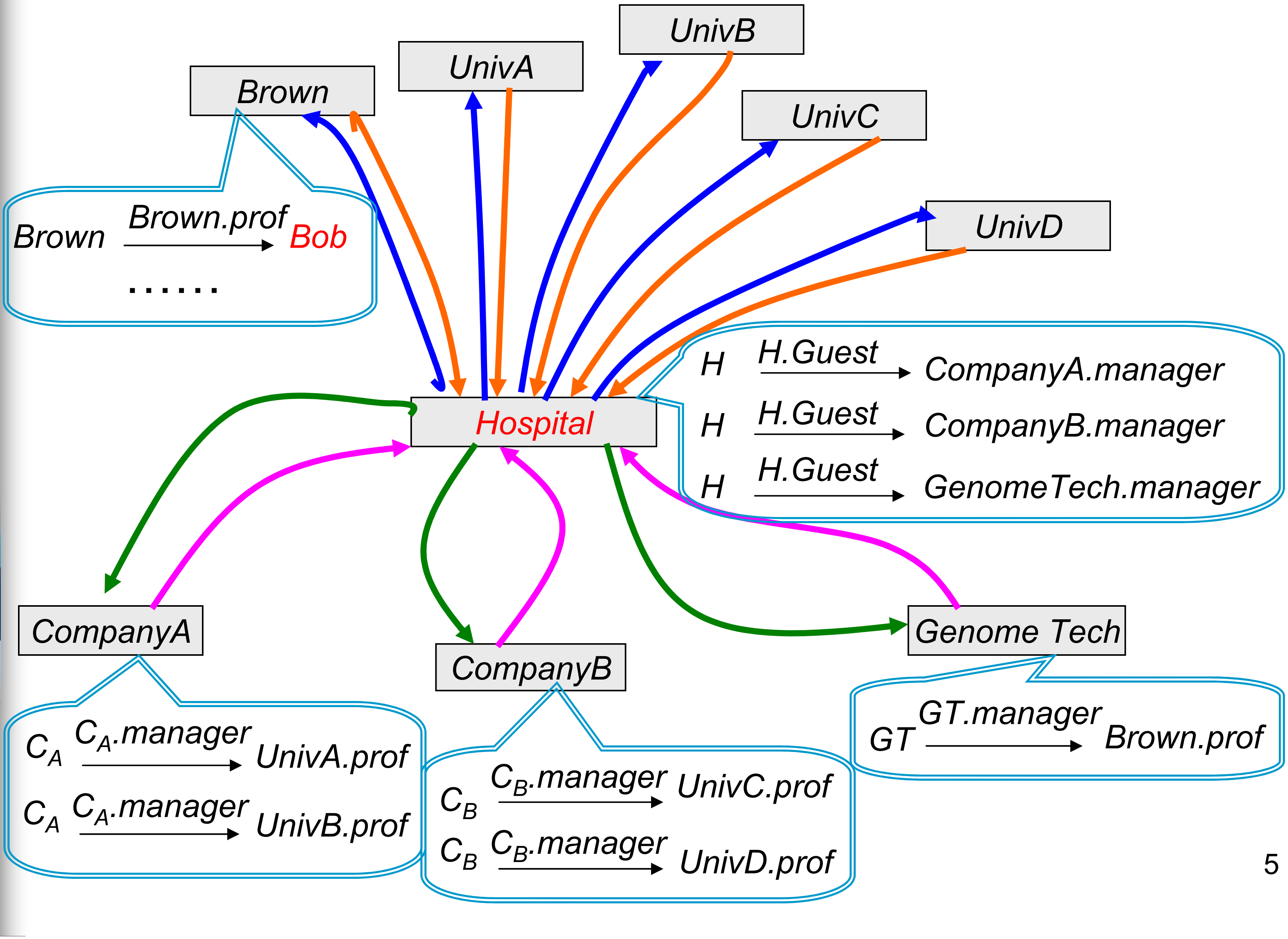
GenomeTech —*GenomeTech.Manager*→ *Brown.Professor*

Brown —*Brown.Professor*→ Bob

Bob is a member of *Hospital.Guest*

- Storage of delegation credentials
  - Distributed across the network
- Distributed delegation chain discovery algorithms (Li Winsborough Mitchell 2003)
  - Traverse the graph of delegations

Credential chain discovery example



$Brown \xrightarrow{Brown.prof} Bob$

……

$H \xrightarrow{H.Guest} CompanyA.manager$

$H \xrightarrow{H.Guest} CompanyB.manager$

$H \xrightarrow{H.Guest} GenomeTech.manager$

$C_A \xrightarrow{C_A.manager} UnivA.prof$

$C_A \xrightarrow{C_A.manager} UnivB.prof$

$C_B \xrightarrow{C_B.manager} UnivC.prof$

$C_B \xrightarrow{C_B.manager} UnivD.prof$

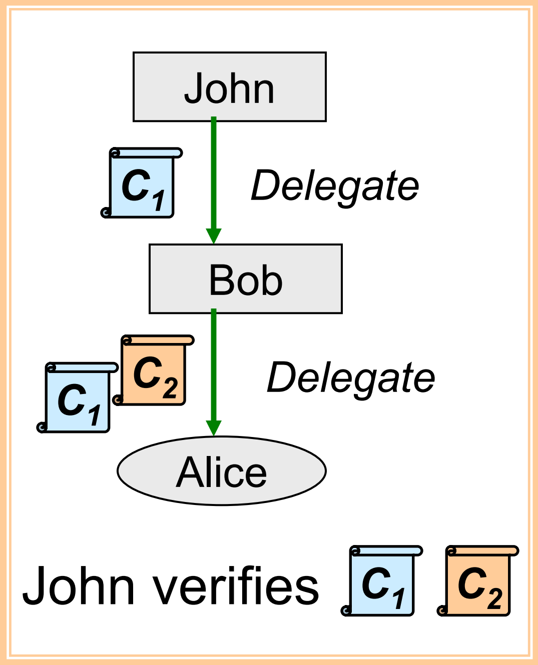
$GT \xrightarrow{GT.manager} Brown.prof$

Distributed delegation chain discovery

- Flexible role-based delegation chain discovery
  - Linking arbitrary number of delegations
  - Issuing delegations independently
- Communication among credential servers
  - Complexity increases with the size of the credential graph
- Availability of credential servers
  - Participation of servers in discovery
- Privacy considerations
  - Revealing unrelated delegations

Cascaded delegation

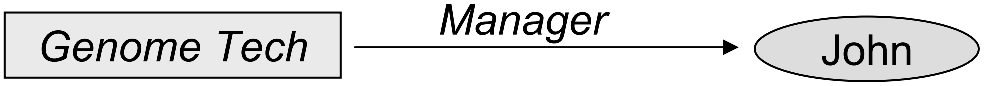
- Efficient verification of a hierarchical delegation chain (Sollins 1988)
  - Accumulates certificates at each delegation transaction
  - Avoids certificate chain discovery
- Does not support the use of roles
  - Low scalability



- **Our approach**: combine Role-Based Access Control (RBAC) with cascaded delegation
  - No need to know role members
  - Unique delegation credential
  - No administrator participation in delegation
  - Low communication costs

Our model: Role-Based Cascaded Delegation (RBCD)

- The member of a role is given a role credential by the administrator

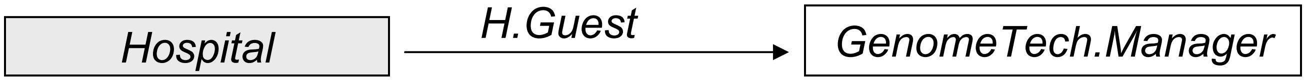

Genome Tech

Manager

John

R_J

- Delegation of privileges is initialized by the resource owner and issued to a role

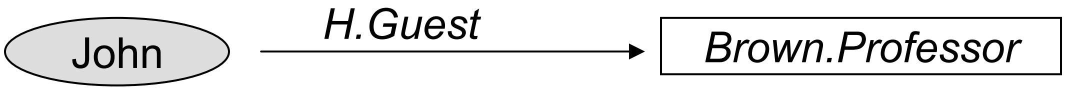

Hospital

H.Guest

GenomeTech.Manager

C_1

- Delegation may be further extended to others by any member of the role (intermediate delegator)


John

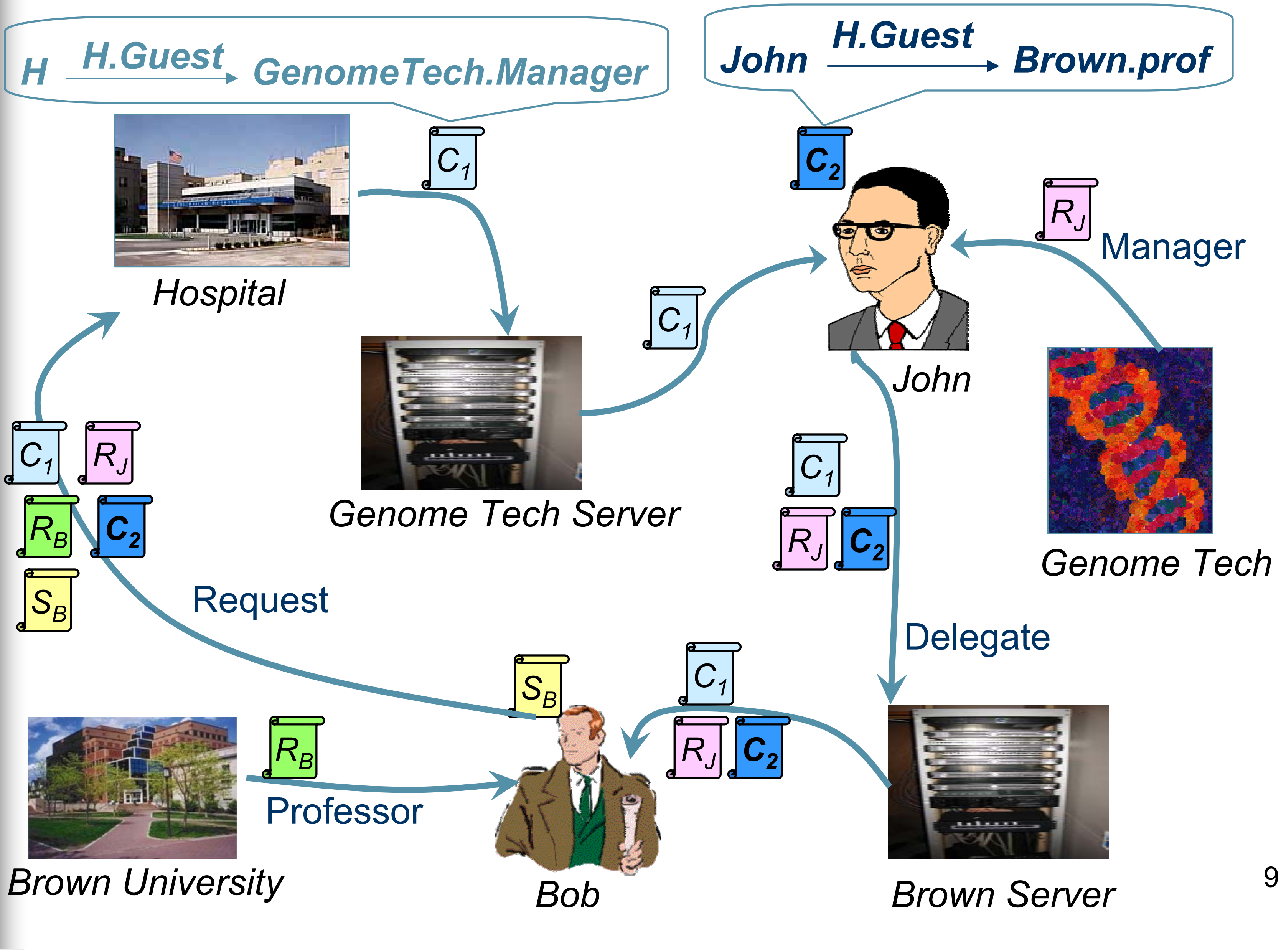
H.Guest

Brown.Professor

C_2

- Extension credential, role credential, and previous delegation credentials are issued (partial delegation credential)
  - *John* forwards C_1, R_J, and C_2 to *professor at Brown*
- Requester submits the partial delegation credential, his role credential, and his signature to the verifier
  - *Bob* submits C_1, R_J, C_2, his role credential R_B, and his signature S_B to *Hospital*

An example of RBCD



$H \xrightarrow{H.Guest} GenomeTech.Manager$

$John \xrightarrow{H.Guest} Brown.prof$

C_1

C_2

R_J

Manager

Hospital

John

Genome Tech Server

Genome Tech

C_1 R_J R_B C_2 S_B

Request

C_1 R_J C_2

Delegate

S_B

R_B

Professor

C_1 R_J C_2

Brown University

Bob

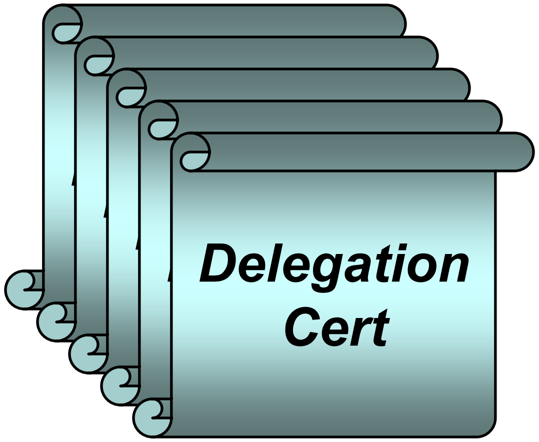
Brown Server

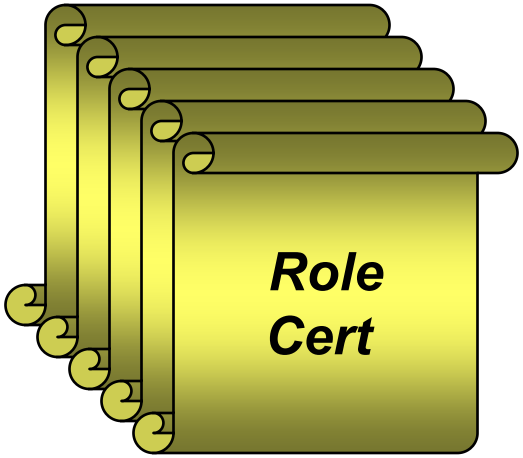
Advantages of RBCD model

- Avoidance of the distributed delegation chain discovery
  - Delegation chain is stored in the credentials
- High scalability because of the use of roles
  - Delegator does not have to know the members of a role
- Flexible and decentralized delegation
  - Delegation process does not require the participation of administrators
- Improved privacy protection
  - Unrelated credentials are not touched
- Low computation costs even if credentials are stored centrally

Implementing RBCD

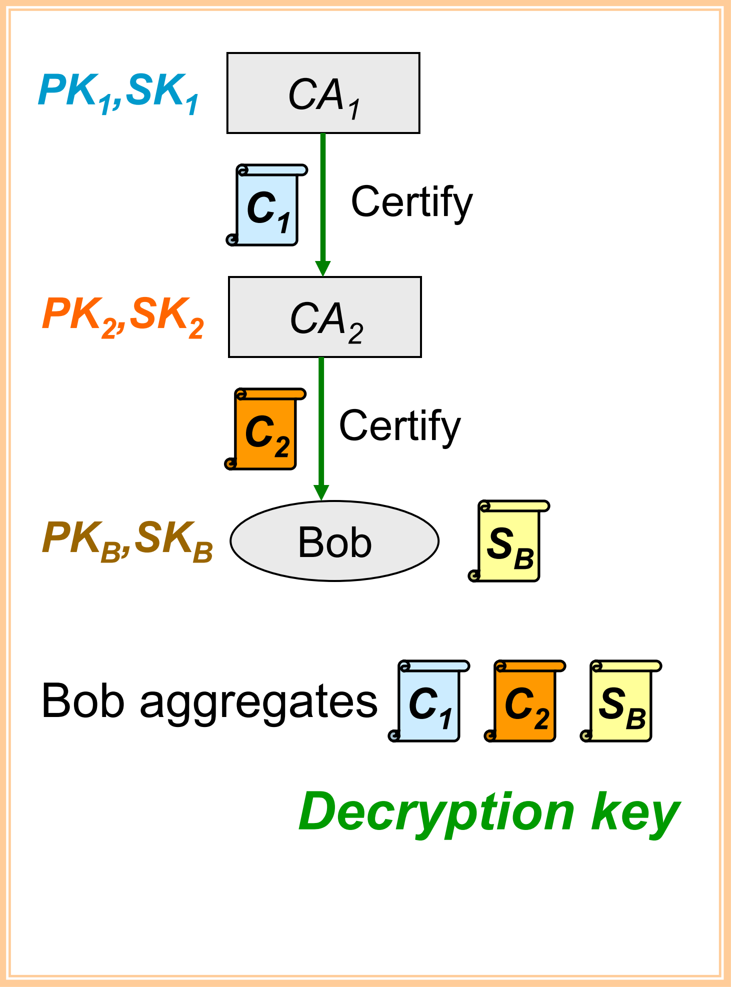
- Requirements
  - Compact credential size
  - Efficient storage and transmission
  - Security of the scheme
- **Our approach**
  - Implementing RBCD model using Hierarchical Certificate-Based Encryption



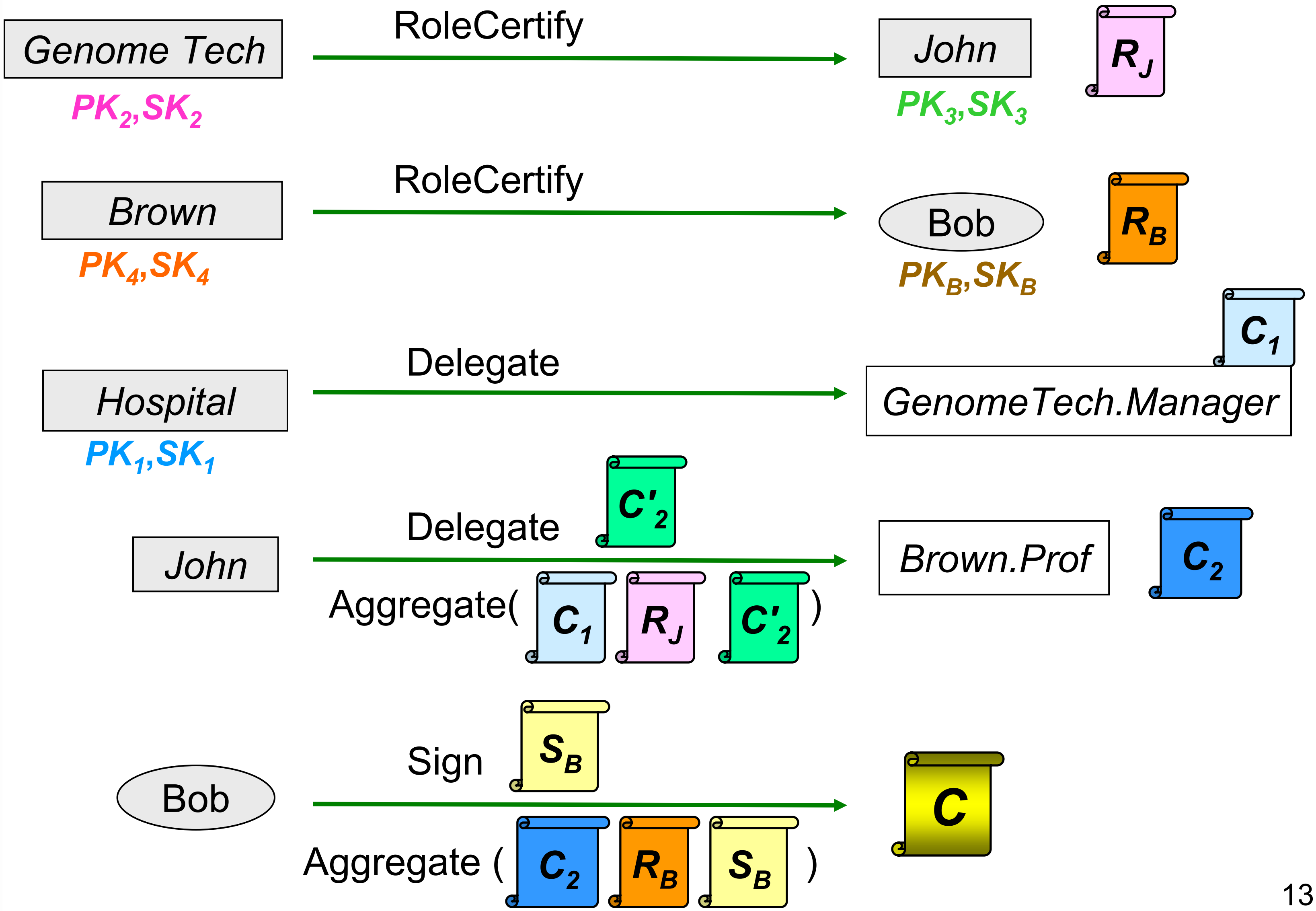


Hierarchical Certificate-Based Encryption

- HCBE scheme (Gentry 2003)
  - *Setup*, *Certify*, *Aggregate*, *Encrypt*, *Decrypt*
  - Aggregated decryption key
    - CA signatures + User signature
  - Aggregate multiple signatures into one signature (Boneh *et al.* 2003)
  - Security
- Size of signatures and public keys
  - 170 bits with security comparable to 1024 bit RSA and 320 bit DSA (Boneh *et al.* 2001)
- Response and challenge



Our approach: using HCBE to realize RBCD



Genome Tech PK_2,SK_2 — RoleCertify → *John* PK_3,SK_3 R_J

Brown PK_4,SK_4 — RoleCertify → Bob PK_B,SK_B R_B

Hospital PK_1,SK_1 — Delegate → *GenomeTech.Manager* C_1

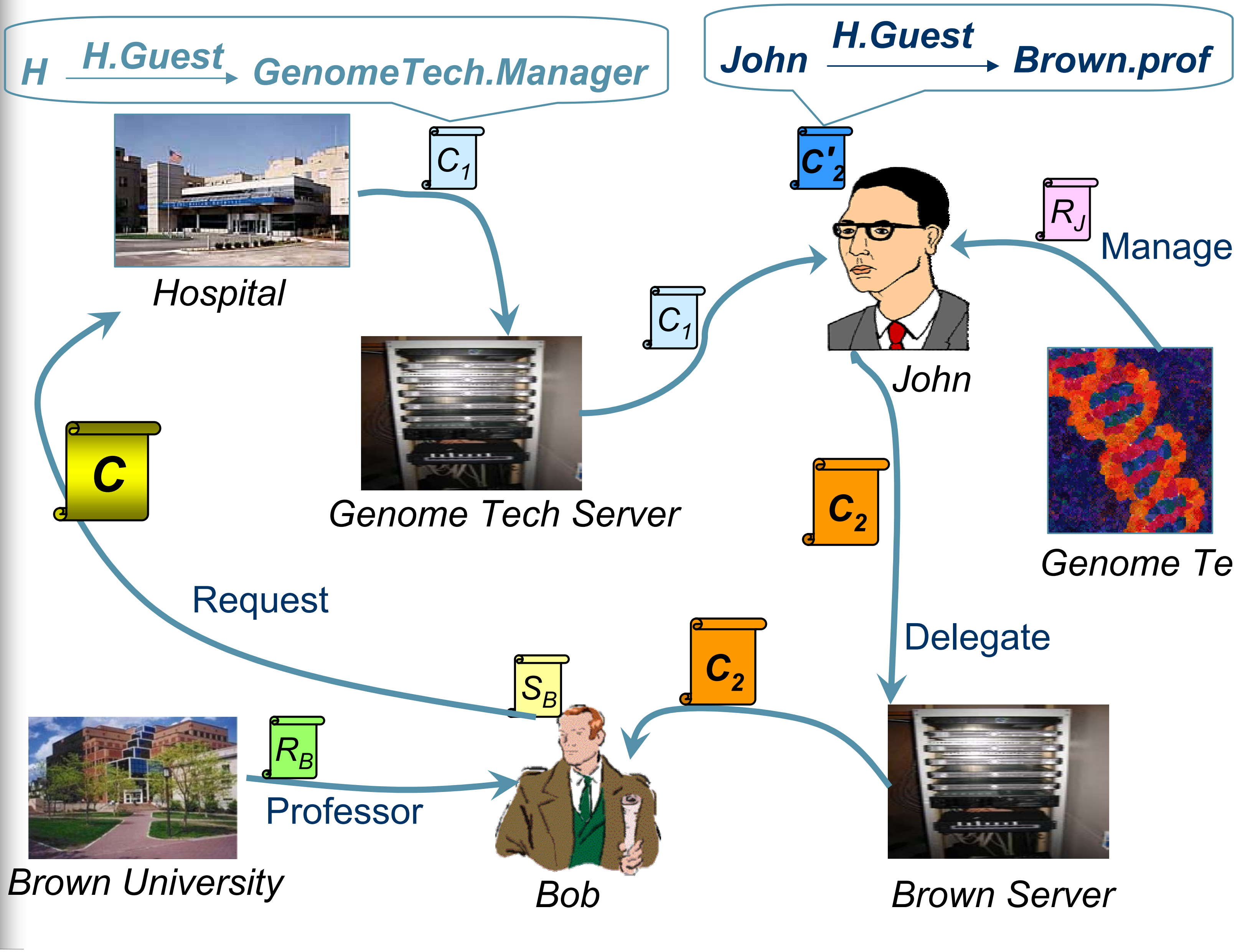
John — Delegate C'_2 → *Brown.Prof* C_2

Aggregate(C_1 R_J C'_2)

Bob — Sign S_B → C

Aggregate (C_2 R_B S_B)

Using HCBE



$H \xrightarrow{H.Guest} GenomeTech.Manager$

$John \xrightarrow{H.Guest} Brown.prof$

C_1

C'_2

R_J

Manager

Hospital

C_1

John

Genome Tech Server

C

C_2

Genome Tech

Request

Delegate

S_B

C_2

R_B

Professor

Brown University

Bob

Brown Server

Performance comparisons between the RBCD implementation using RSA and HCBE

Chain length n=20	Credential size (Kbits)	20 Kbit/s connection
RBCD using RSA	> 81	> 4s
RBCD using HCBE	< 7	< 0.35s

Scheme	Sign*	Verify*
RSA (d = 1007-bit)	7.9ms	0.4ms
HCBE	3.57ms	~ 50ms

* Performed on 1GHz Pentium III (Barreto *et al.* 2002)

- Verify(*Chain*) ~ |*Chain*|

Conclusions

- Contributions
  - Role-Based Cascaded Delegation (RBCD) model
    - Eliminating credential chain discovery
    - Supporting decentralized delegation
    - Scalable
    - Minimizing exposure of sensitive credentials
  - Implementation of RBCD using HCBE
    - Compact credentials
- Future work
  - Integration
    - Combining *RT* framework with RBCD
    - Using XACML as the policy language
  - Experimental study
    - Detailed evaluation of communication and computation costs