Structured Bulletin Board with Controlled Access

Rolf Haenni

http://e-voting.bfh.ch

BFH, RISIS, E-Voting Group

June 13th, 2013

Outline

Introduction

Structured Bulletin Board

Access-Controlled Bulletin Board

Other Bulletin Board Properties

Outline

Unstructured and Uncontrolled Bulletin Board

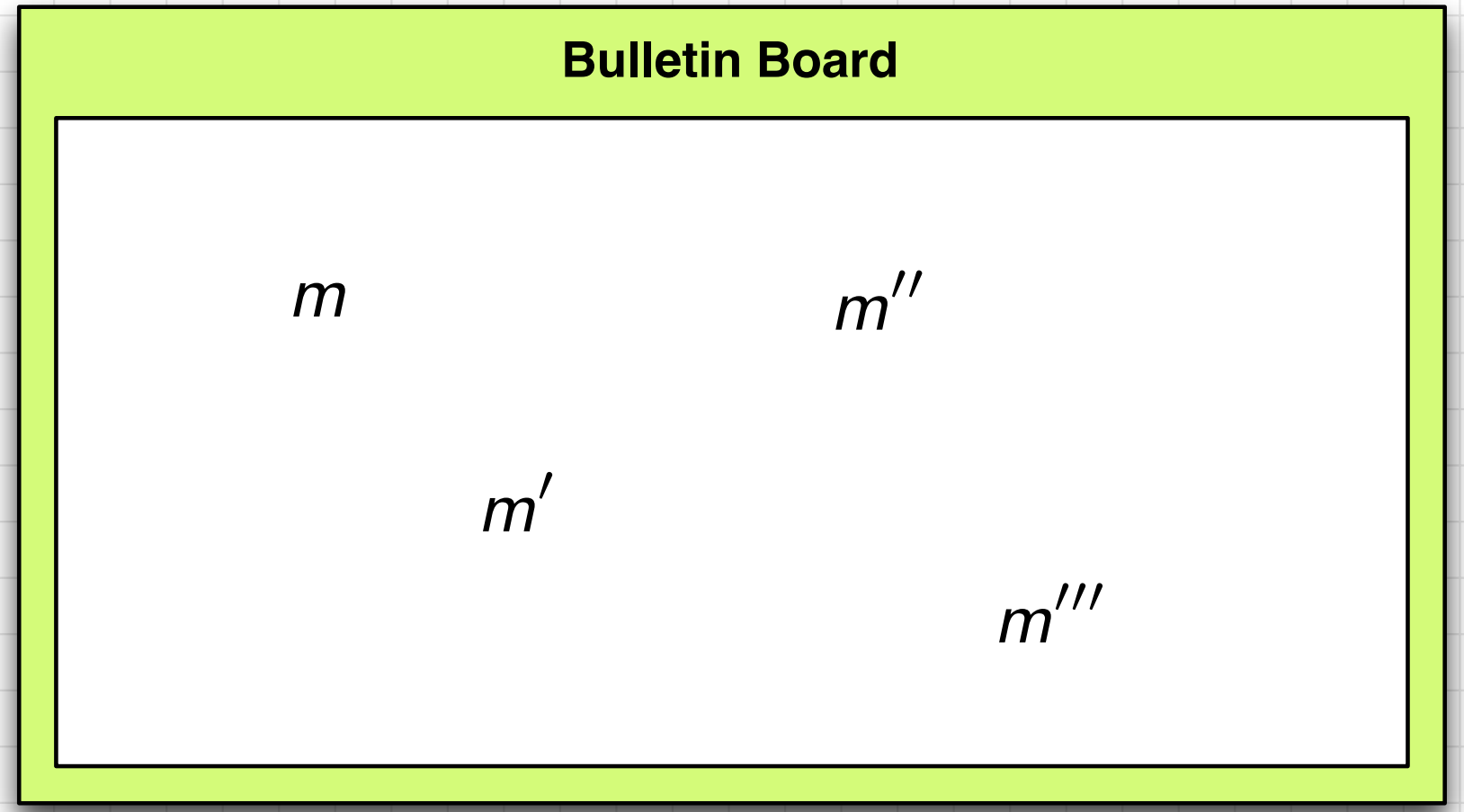
- Alphabet $\mathcal{S} = \{s_1, \ldots, s_n\}$
  - → $\mathcal{S} = \{0, 1\}$
  - → $\mathcal{S} = \{0, \ldots, 9\}$
  - → $\mathcal{S} = \{a, \ldots, z, A, \ldots, Z, 0, \ldots, 9, \_, =\}$
- Message space $\mathcal{M} \subseteq \mathcal{S}^*$
- Every message posted by

  $$Post(m)$$

  is accepted if $m \in \mathcal{M}$
- Every accepted message $m \in \mathcal{M}$ is stored in $\mathcal{BB}$
- $\mathcal{BB}$ is considered to be a multiset (the same message may be posted multiple times)

Outline

Unstructured Bulletin Board



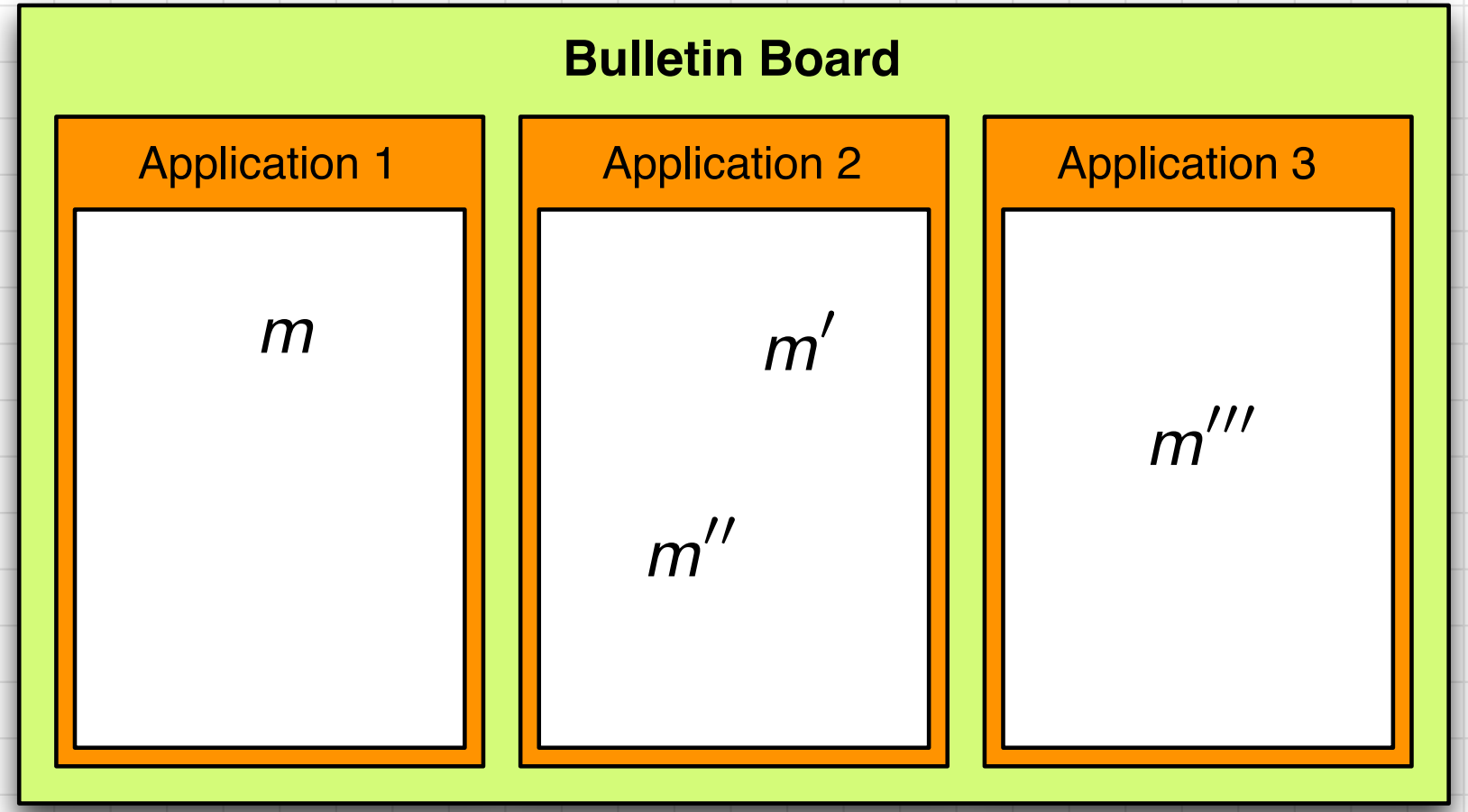
Multipurpose Bulletin Board

- Applications $A_1, \ldots, A_r$
- Every message posted by

  $$Post(i, m)$$

  is accepted, if $i \in \{1, \ldots, r\}$ and $m \in \mathcal{M}$
- Every accepted message $m \in \mathcal{M}$ is stored in $\mathcal{BB}_i$
- In addition, some applications may have different versions

Multipurpose Bulletin Board



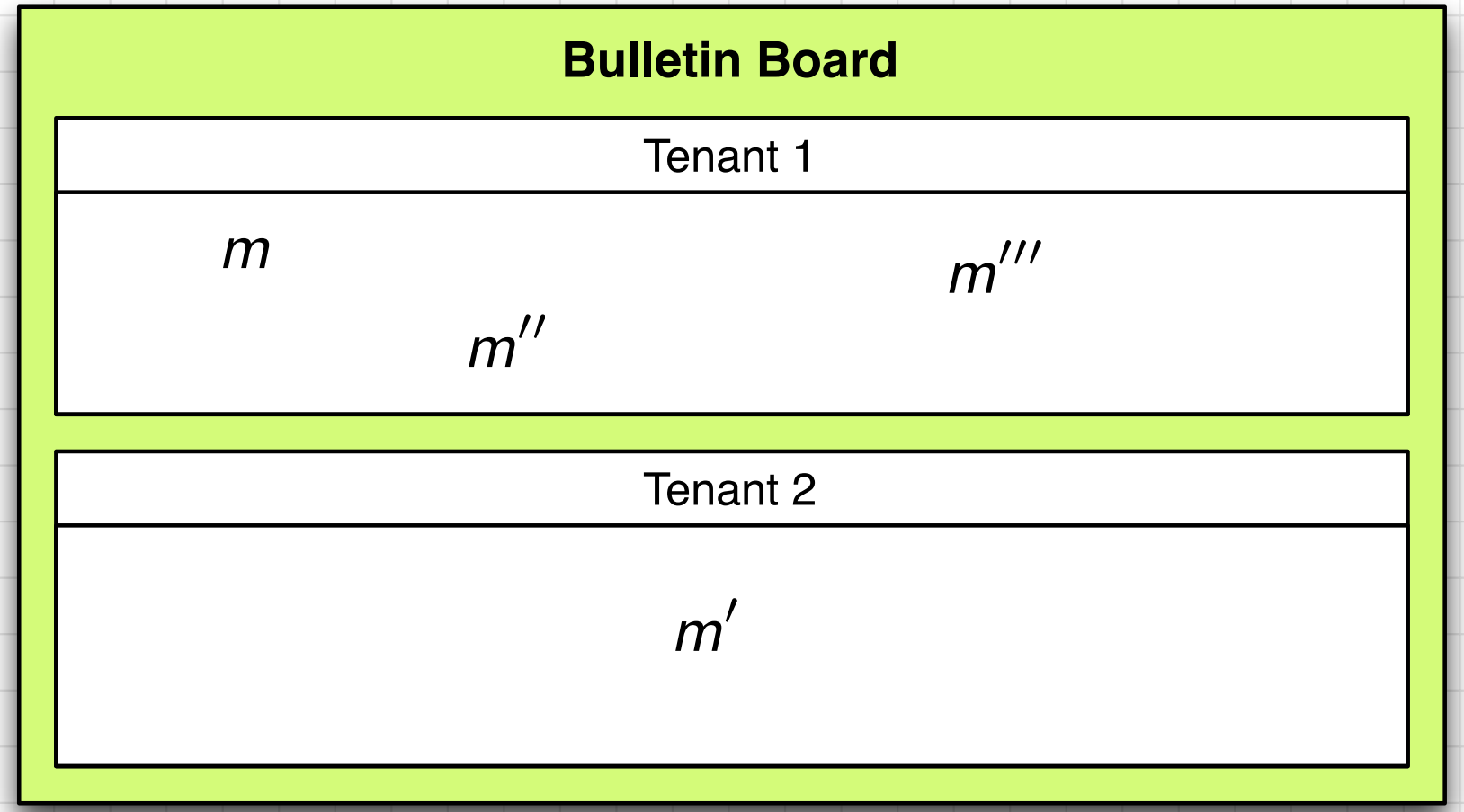
Multitenant Bulletin Board

- Tenants $E_1, \ldots, E_s$
- Every message posted by

  $$Post(j, m)$$

  is accepted, if $j \in \{1, \ldots, s\}$ and $m \in \mathcal{M}$
- Every accepted message $m \in \mathcal{M}$ is stored in $\mathcal{BB}_j$

Multitenant Bulletin Board



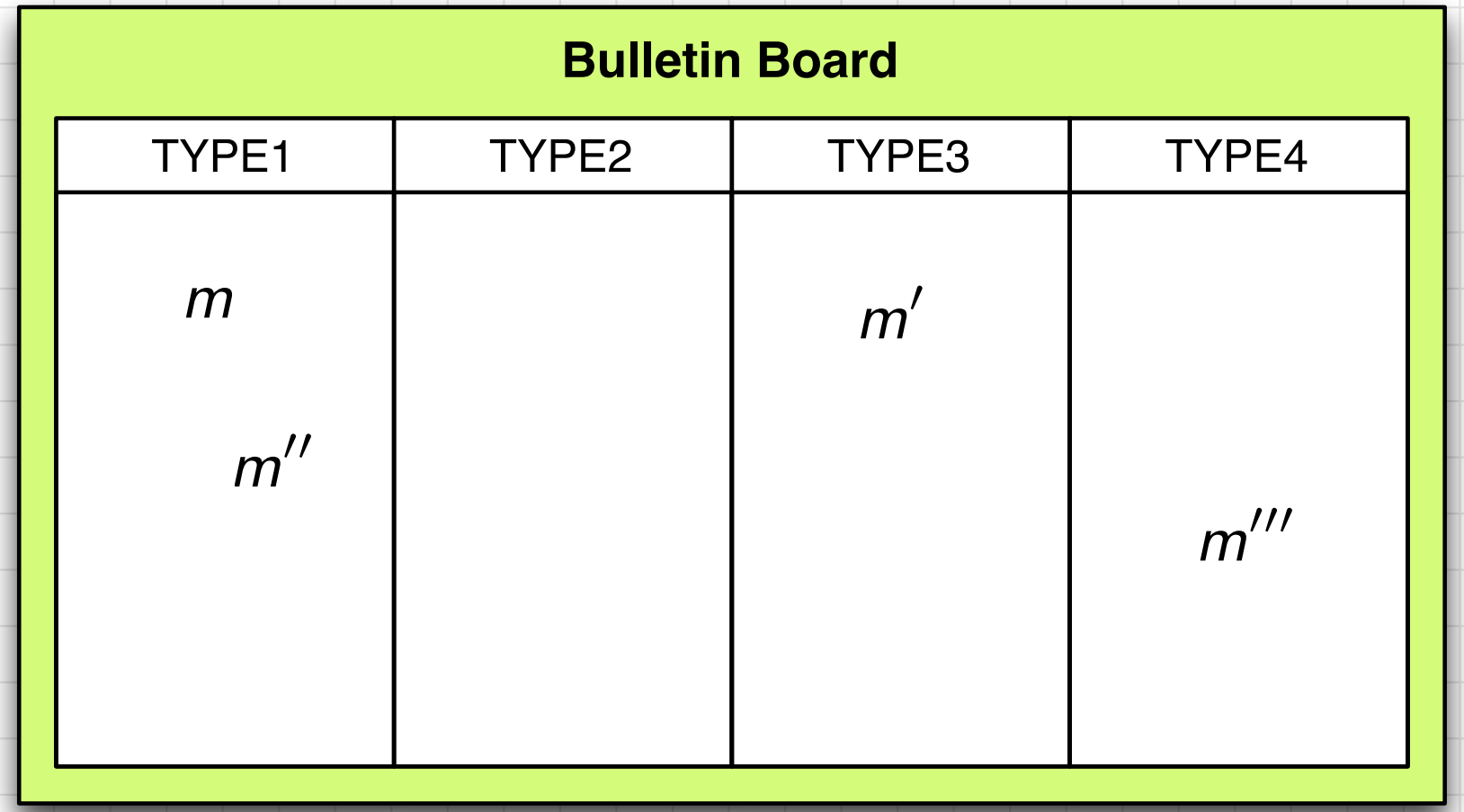
Typed Bulletin Board

- Types $T_1, \ldots, T_t \subseteq \mathcal{M}$
- A message posted by

  $$Post(k, m)$$

  is accepted, if $k \in \{1, \ldots, t\}$ and $m \in T_k$
- Every accepted message $m \in T_k$ is stored in $\mathcal{BB}_k$

Typed Bulletin Board



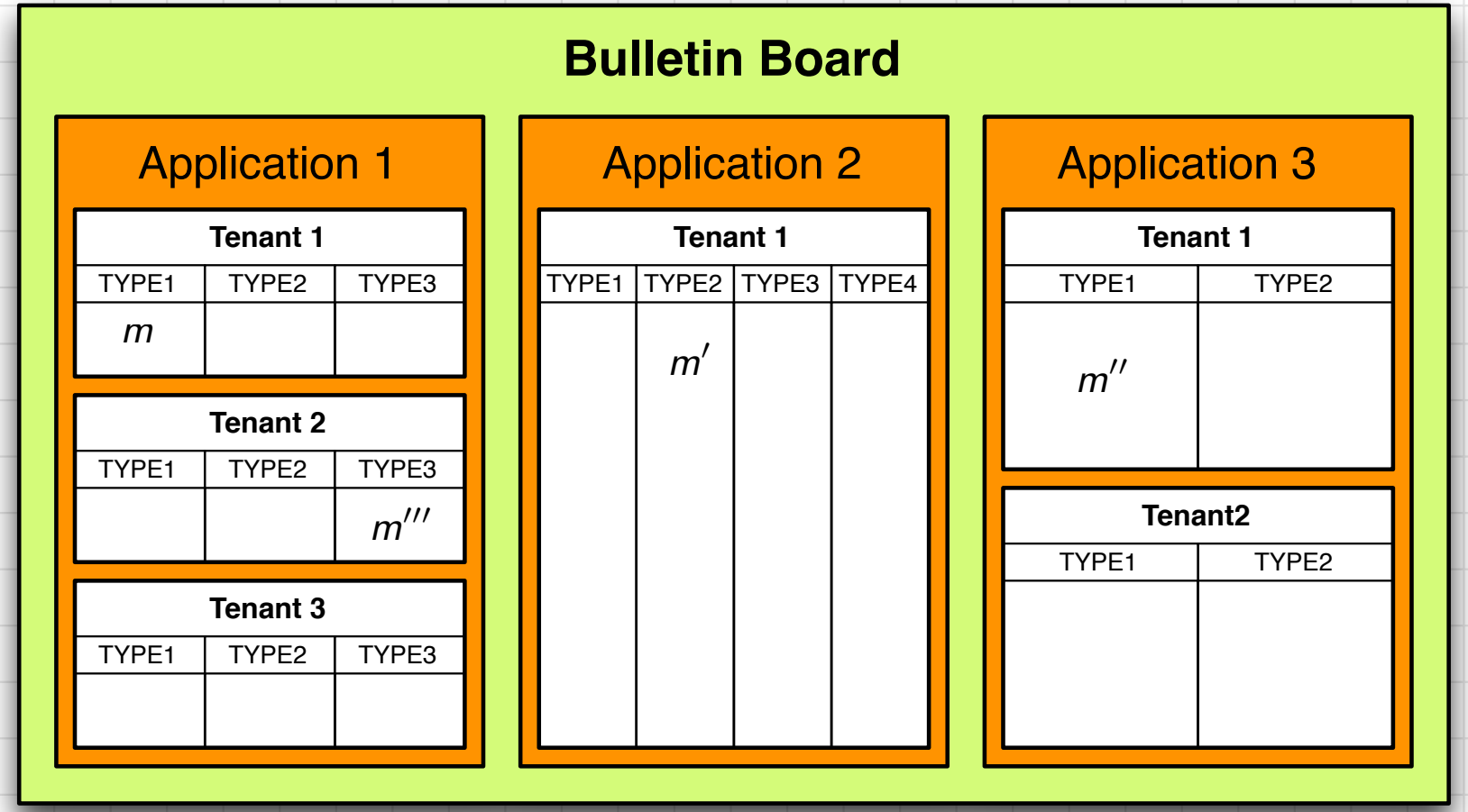
Typed Multipurpose Multitenant Bulletin B.

- Applications A_i
- Tenants E_{ij}
- Types $T_{ik} \subseteq \mathcal{M}$
- Every message posted by

  $$Post(i, j, k, m)$$

  is accepted, if $i \in \{1, \ldots, r\}$, $j \in \{1, \ldots, s_i\}$, $k \in \{1, \ldots, t_i\}$, and $m \in T_{ik}$
- Every accepted message $m \in T_{ik}$ is stored in $\mathcal{BB}_{ijk}$

Typed Multipurpose Multitenant Bulletin B.



Outline

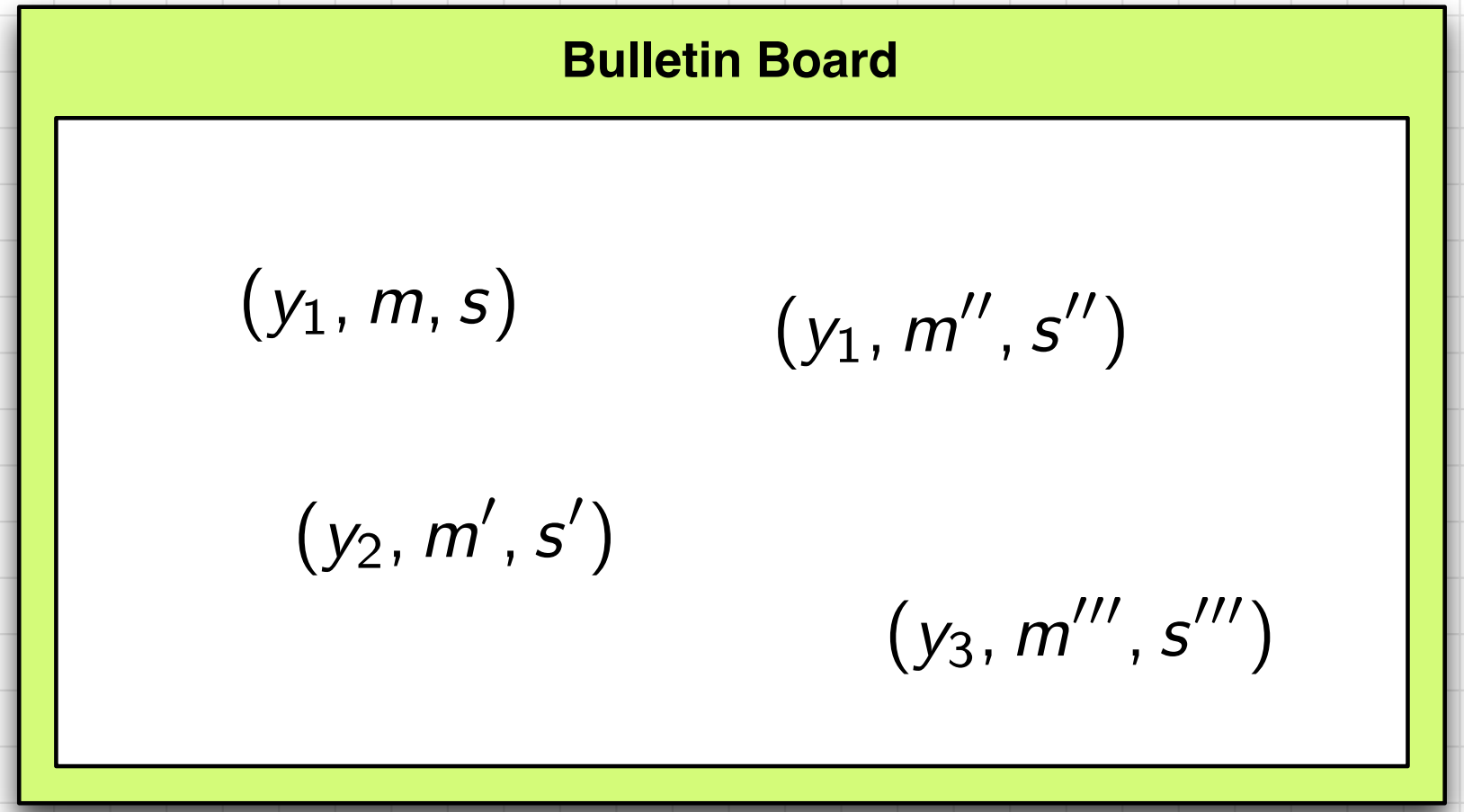
Access-Controlled Bulletin Board

- Let $\mathcal{U}$ be the set of users allowed to post messages to $\mathcal{BB}$
- Let (x_u, y_u) the key pair and C_u the certificate of user $u \in \mathcal{U}$
- Let $\mathcal{C} = \{C_u : u \in \mathcal{U}\}$ and therefore $\mathcal{Y} = \{y_u : u \in \mathcal{U}\}$ be publicly known
- Every message posted by

$$Post(y_u, m, s) = Post(y_u, m, Sign_{x_u}(m))$$

  is accepted, if $y_u \in \mathcal{Y}$, $m \in \mathcal{M}$, $Verify_{y_u}(m, s) = true$, and $(y_u, m, s) \notin \mathcal{BB}$
- Every accepted signed message (y_u, m, s) is stored in $\mathcal{BB}$
- Note that if $\mathcal{C}$ is unknown, the right to post a message is granted anonymously to the holders of the private keys x_u

Access-Controlled Bulletin Board



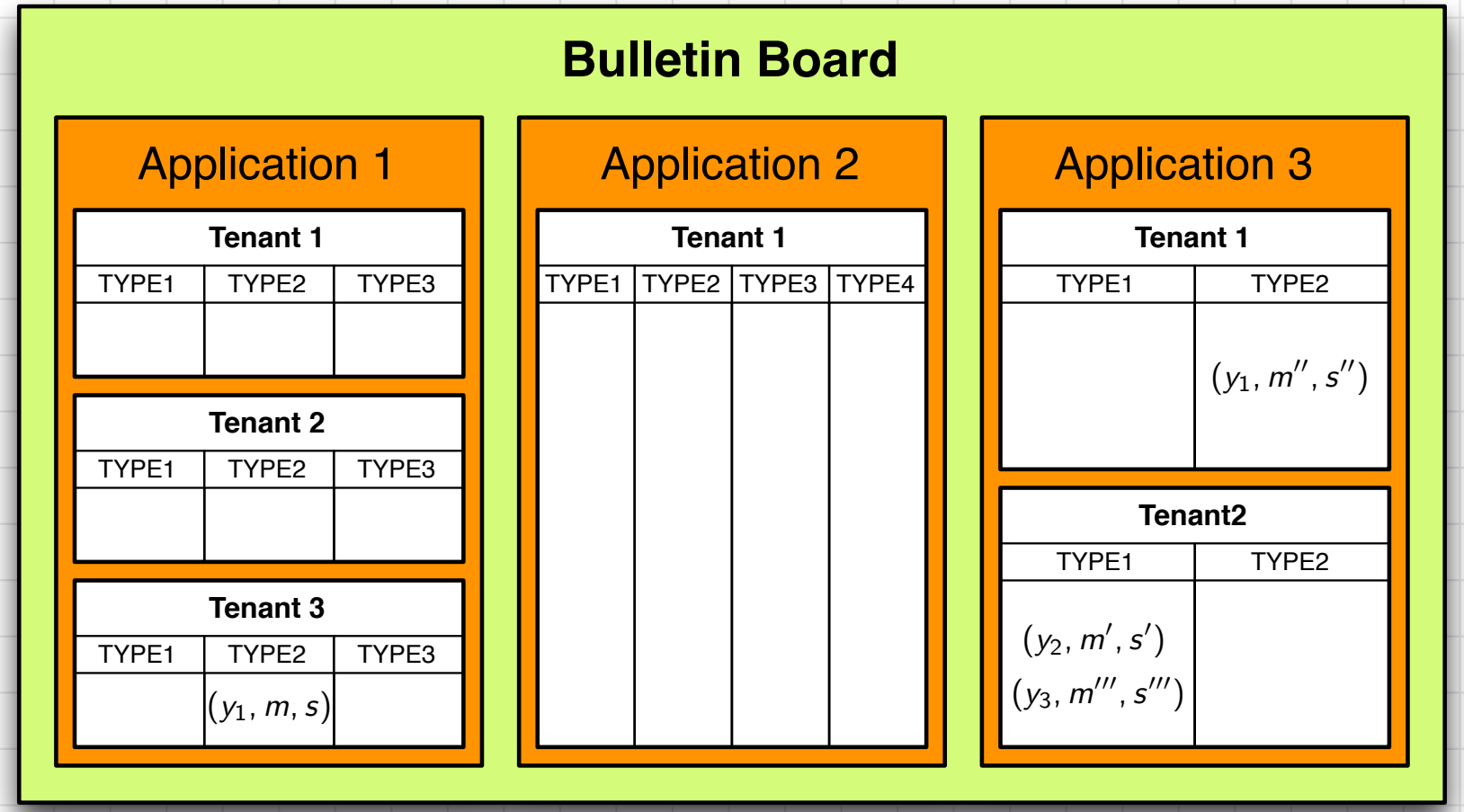
Access-Controlled Typed Multipurpose Multitenant Bulletin Board

- Applications A_i, tenants E_{ij}, types $T_{ik} \subseteq \mathcal{M}$
- Let $\mathcal{U}_{ijk}$ be the set of users allowed to post messages to $\mathcal{BB}_{ijk}$
- Let $\mathcal{C}_{ijk} = \{C_u : u \in \mathcal{U}_{ijk}\}$ and therefore $\mathcal{Y}_{ijk} = \{y_u : u \in \mathcal{U}_{ijk}\}$ be publicly known
- Every message posted by

$$Post(i, j, k, y_u, m, s) = Post(i, j, k, y_u, m, Sign_{x_u}(m))$$

  is accepted, if $i \in \{1, \ldots, r\}$, $j \in \{1, \ldots, s_i\}$, $k \in \{1, \ldots, t_i\}$, $y_u \in \mathcal{Y}_{ijk}$, $m \in T_{ik}$, $Verify_{y_u}(m, s) = true$, $(y_u, m, s) \notin \mathcal{BB}_{ijk}$
- Every accepted signed message (y_u, m, s) is stored in $\mathcal{BB}_{ijk}$

Access-Controlled Typed Multipurpose Multitenant Bulletin Board



Dynamic Access-Controlled Typed Bulletin B.

- Special user $u_0 \in \mathcal{U}$ (called *coordinator*) with certificate C_0 for key pair (x_0, y_0) is publicly known
- There is a special type $T_0 \subseteq \mathcal{M}$ for messages $m = y_u||k$, giving u the right to post messages of type $k \in \{0, 1, \ldots, t\}$
- Types $T_0, T_1, \ldots, T_t \subseteq \mathcal{M}$
- A single (unsigned) initialization message $m = y_0||0$ of type T_0 is published in $\mathcal{BB}_0$
- Afterwards, every message posted by

$$Post(k, y_u, m, s) = Post(k, y_u, m, Sign_{x_u}(m))$$

  is accepted, if $k \in \{0, \ldots, t\}$, $(*, y_u||k, *) \in \mathcal{BB}_0$, $m \in T_k$, $Verify_{y_u}(m, s) = true$, and $(y_u, m, s) \notin \mathcal{BB}_k$
- Every accepted signed message (y_u, m, s) is stored in $\mathcal{BB}_k$

Dynamic Access-Controlled Typed Bulletin B.

Bulletin Board

TYPE0	TYPE1	TYPE2	TYPE3
$(-, y_0 \|\| 0, -)$ $(y_0, y_1 \|\| 1, s_1)$ $(y_0, y_2 \|\| 3, s_2)$	(y_1, m, s)		(y_2, m', s') (y_2, m'', s'')

Access-Controlled Bulletin Board with Upper Bound

- Let $\mathcal{U}$, $\mathcal{C}$, and $\mathcal{V}$ be as before and publicly known
- Upper bound $N_u \in \mathbb{N}$, for all $u \in \mathcal{U}$
- Every message posted by

$$Post(y_u, m, s) = Post(y_u, m, Sign_{x_u}(m))$$

  is accepted, if $y_u \in \mathcal{Y}$, $m \in \mathcal{M}$, $Verify_{y_u}(m, s) = true$, $(y_u, m, s) \notin \mathcal{BB}$, and $|\{(y_u, m', s') \in \mathcal{BB}\}| < N_u$
- Every accepted signed message (y_u, m, s) is stored in $\mathcal{BB}$

Dynamic Access-Controlled Typed Bulletin Board with Upper Bound

- Let u_0, $\mathcal{U}$, $\mathcal{C}$, and $\mathcal{V}$ be as before and publicly known
- Let T_0 be set set of messages of the form $y_u||k||N$ for $y_u \in \mathcal{Y}$, $k \in \{0, 1, \ldots, t\}$, and $N \in \mathbb{N}$
- Again, a single (insigned) initialization message $m = y_0||0||\infty$ of type T_0 is published in $\mathcal{BB}_0$
- If $\mathcal{BB}_0$ contains multiple messages $y_u||k||N_i \in T_0$ for the same $y_u \in \mathcal{Y}$ and the same k, then u is allowed to post $N_u = \sum_i N_i$ messages to $\mathcal{BB}_k$
- Note a user's right to post can be revoked by allowing negative values $N \in \mathbb{Z}$

Access-Controlled Bulletin Board with Time Limit

- Let $\mathcal{U}$, $\mathcal{C}$, and $\mathcal{V}$ be as before and publicly known
- Time limit t_u, for all $u \in \mathcal{U}$
- Every message posted at time T by

$$Post(y_u, m, s) = Post(y_u, m, Sign_{x_u}(m))$$

  is accepted, if $y_u \in \mathcal{Y}$, $m \in \mathcal{M}$, $Verify_{y_u}(m, s) = true$, $(y_u, m, s) \notin \mathcal{BB}$, and $T \leq t_u$
- Every accepted signed message (y_u, m, s) is stored in $\mathcal{BB}$
- Optionally, replace the time limit t_u by a time period $[t_u^1, t_u^2]$

Dynamic Access-Controlled Typed Bulletin Board with Time Limit

- Let u_0, $\mathcal{U}$, $\mathcal{C}$, and $\mathcal{V}$ be as before and publicly known
- Let T_0 be set set of messages of the form $y_u||k||t$ for $y_u \in \mathcal{Y}$, $k \in \{0, 1, \ldots, t\}$, and time limit t
- Again, a single (insigned) initialization message $m = y_0||0||\infty$ of type T_0 is published in $\mathcal{BB}_0$
- If $\mathcal{BB}_0$ contains multiple messages $y_u||k||t_i \in T_0$ for the same $y_u \in \mathcal{Y}$ and the same k, then u is allowed to post messages before $t_u = \max_i t_i$

Outline

Other Bulletin Board Properties

- Append-only
- Robustness
- Certified posting (signed, timestamped)
- Ordered posting
- Chronological posting
- Certified reading (signed, timestamped)
- Private reading (PIR)
- Archivablility
- Active notification