Realizing Massive-Scale Conditional Access Systems Through Attribute-Based Cryptosystems

Patrick Traynor, Kevin Butler, William Enck and Patrick McDaniel

NDSS Symposium

February 11, 2008

The Y100 Phenomenon

PENNSTATE 1855

The Y100 Phenomenon

The Coming Wave

- The number and variety of *Conditional Access* (CA) systems are increasing.
  - IPtv
  - Satellite Radio
  - "Premium" Streaming Audio
- Security in these systems is often proprietary or requires dedicated hardware.
- A solution for general purpose computing platforms is needed...

Goals

PENNSTATE 1855

- Provide an easily manageable broadcast encryption mechanism to regulate access to the expanding set of CA systems.

- Demonstrate that *Attribute-Based Cryptosystems are capable of enabling real systems*, especially those at massive scale.

Broadcast Encryption

- Allows access management without requiring two-way communication.
- Techniques such as LKH and NNL trees dominate cable television.
- Boneh et al proposed an efficient pairing-based construction that grows linearly with the number of users.

Attribute-Based Encryption

PENNSTATE 1855

- Sahai-Waters Construction (Eurocrypt'05)
  - Generalization of Identity-Based Encryption
  - Anyone with *k-out-of-n* attributes can decrypt a ciphertext
- Random Oracle Construction (CCS'06)
  - Properly tuned, can reduce the cost of encryption 98%.
  - We can use this construction to simple boolean conjunction and disjunction:

Attribute-Based Encryption

PENNSTATE 1855

- Sahai-Waters Construction (Eurocrypt'05)
  - Generalization of Identity-Based Encryption
  - Anyone with *k-out-of-n* attributes can decrypt a ciphertext
- Random Oracle Construction (CCS'06)
  - Properly tuned, can reduce the cost of encryption 98%.
  - We can use this construction to simple boolean conjunction and disjunction:

$$\text{Tall} \wedge \text{Dark} \wedge \text{Handsome}$$

Attribute-Based Encryption

PENNSTATE 1855

- Sahai-Waters Construction (Eurocrypt'05)
  - Generalization of Identity-Based Encryption
  - Anyone with *k-out-of-n* attributes can decrypt a ciphertext
- Random Oracle Construction (CCS'06)
  - Properly tuned, can reduce the cost of encryption 98%.
  - We can use this construction to simple boolean conjunction and disjunction:

$$\text{Tall} \wedge \text{Dark} \wedge \text{Handsome}$$
$$\text{Alice} \vee \text{Bob} \vee \text{Carol}$$

ABE Details

PENNSTATE 1855

- Uses bilinear maps on elements of elliptic curves:

$$e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$$

- Construction works by computing efficient bilinear map between *k-out-of-n* attributes.
  - Interpolation using Shamir's Secret Sharing.
- Accordingly, encryption is a function of *n* and decryption is a function of *k*.
  - At least on paper...

An Example

PENNSTATE 1855

An Example

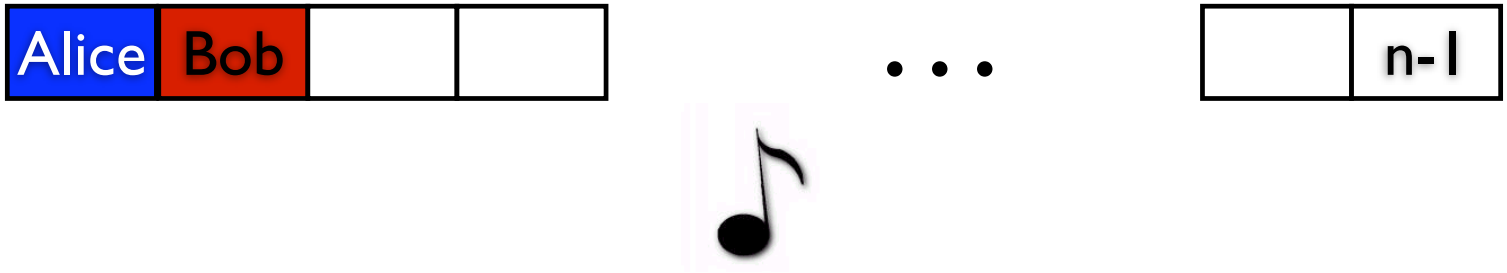
An Example

An Example

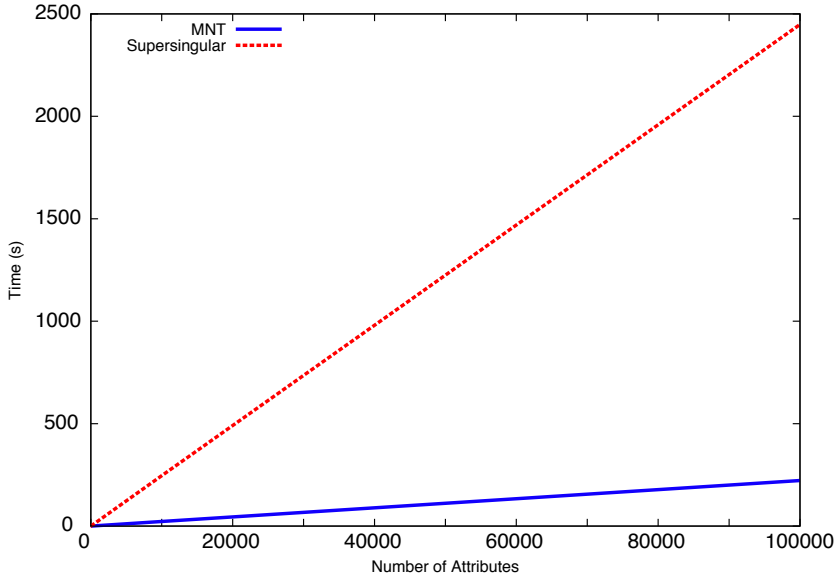
1-out-of-n

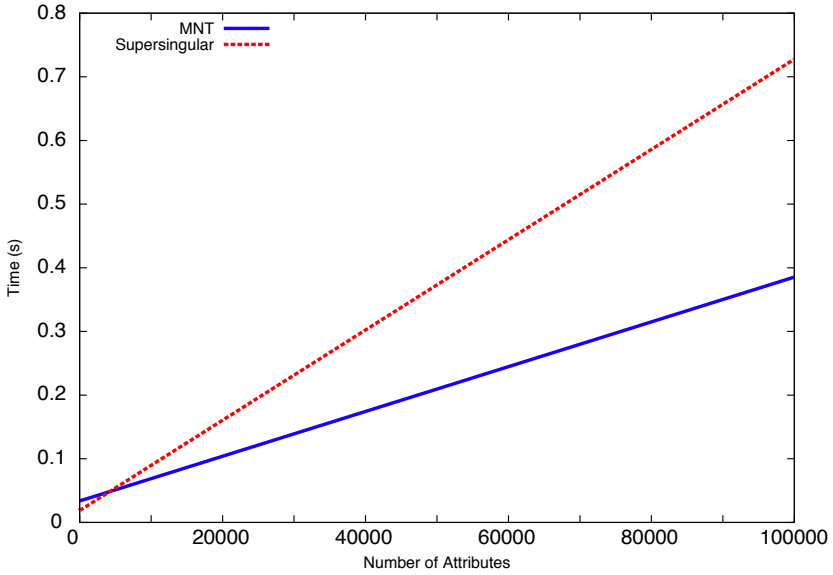
An Example

An Example



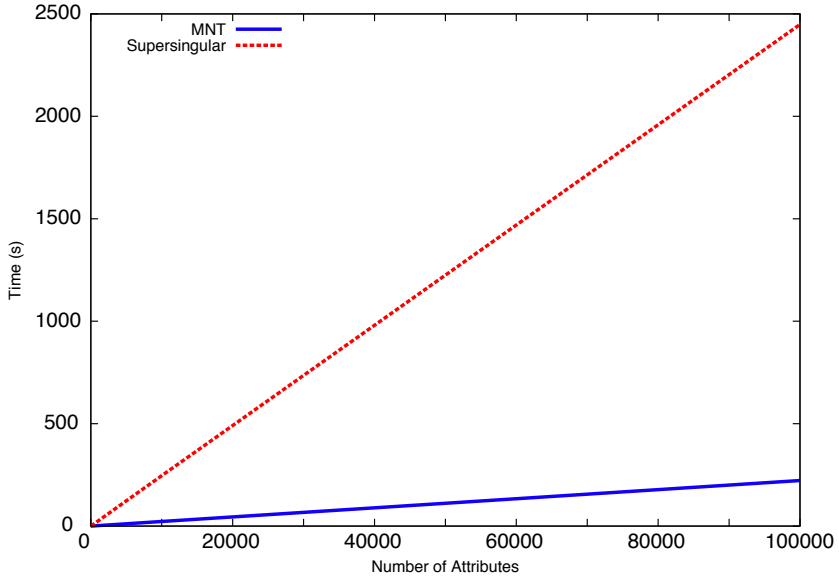
Scaling



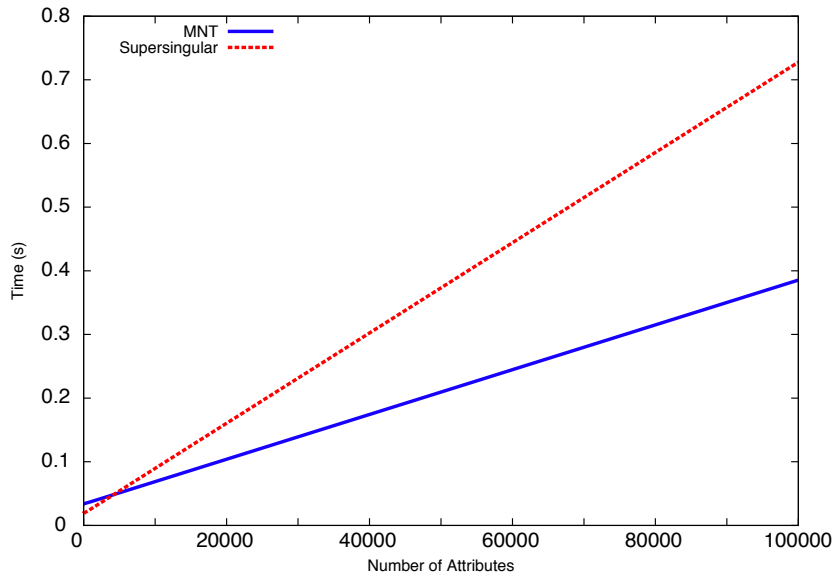


- As expected, MNT curves perform encryption faster.
- Contrary to previous work, MNT curves perform decryption faster than SS when the n > 1000.

Scaling



$$E = 2.2214 \times 10^{-3} n + 0.01804$$
$$r^2 = 0.99999997$$



$$D = 3.5159 \times 10^{-6} n + 0.033791$$
$$r^2 = 0.9999992$$

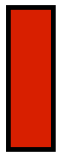
- As expected, MNT curves perform encryption faster.
- Contrary to previous work, MNT curves perform decryption faster than SS when the n > 1000.

Performance

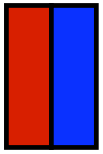
- Even with the random oracle construction, the performance of the primitives is too slow.
- Adding one new user to a group of 1,000,000 takes approximately 37 minutes.
  - This makes changing the content encryption key impossible during short programs (e.g., half-hour TV shows)
- A faster access structure is therefore necessary.

Tiered Construction

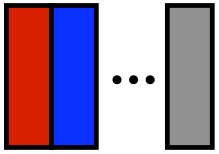
Tiered Construction



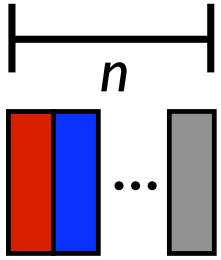
Tiered Construction



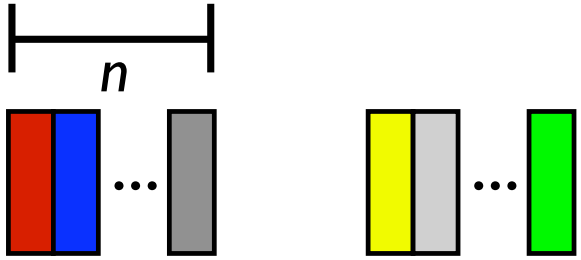
Tiered Construction



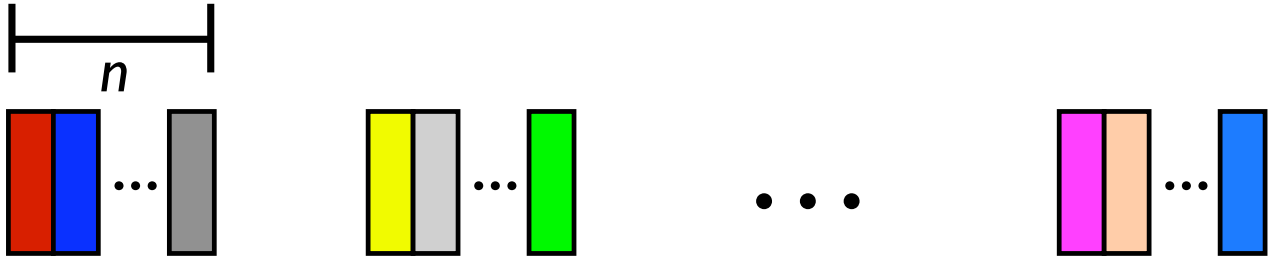
Tiered Construction



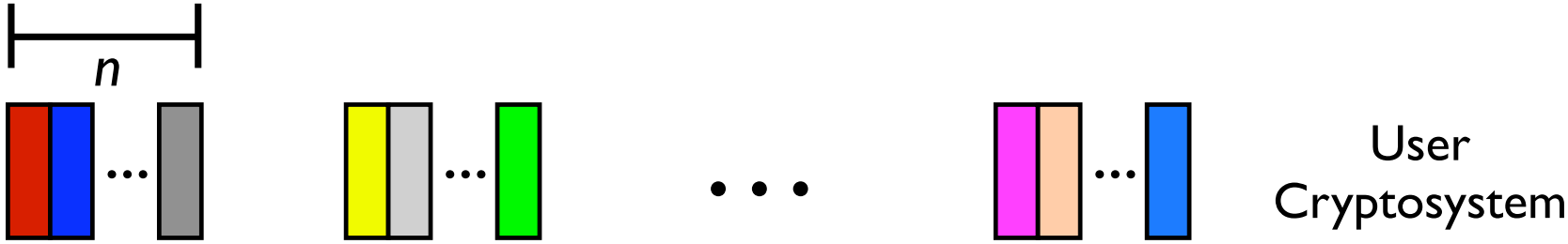
Tiered Construction



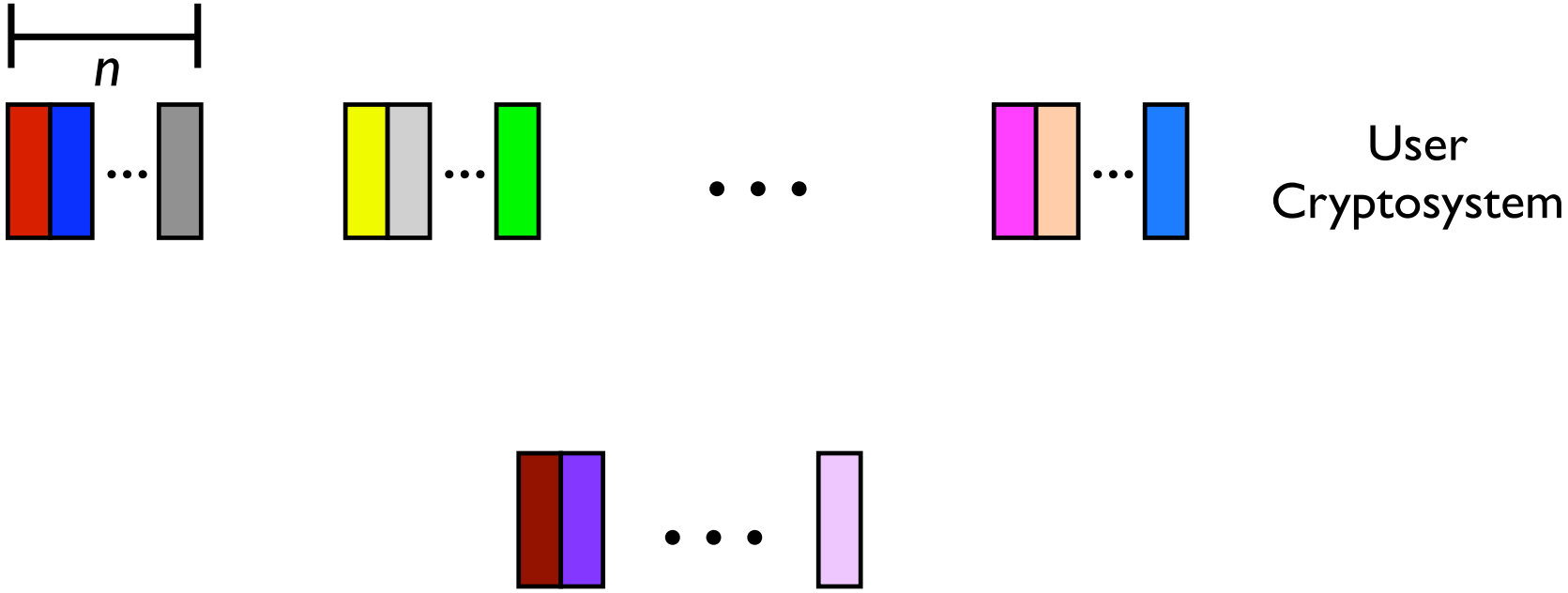
Tiered Construction



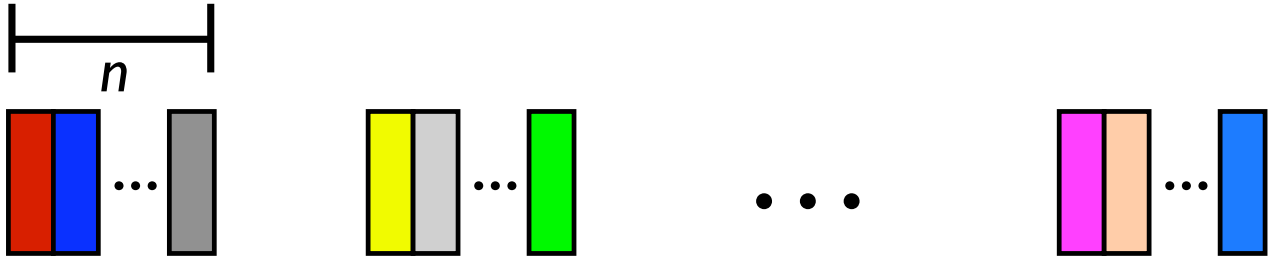
Tiered Construction



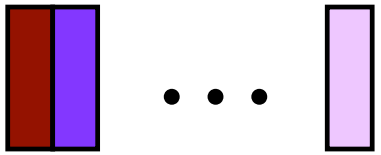
Tiered Construction



Tiered Construction

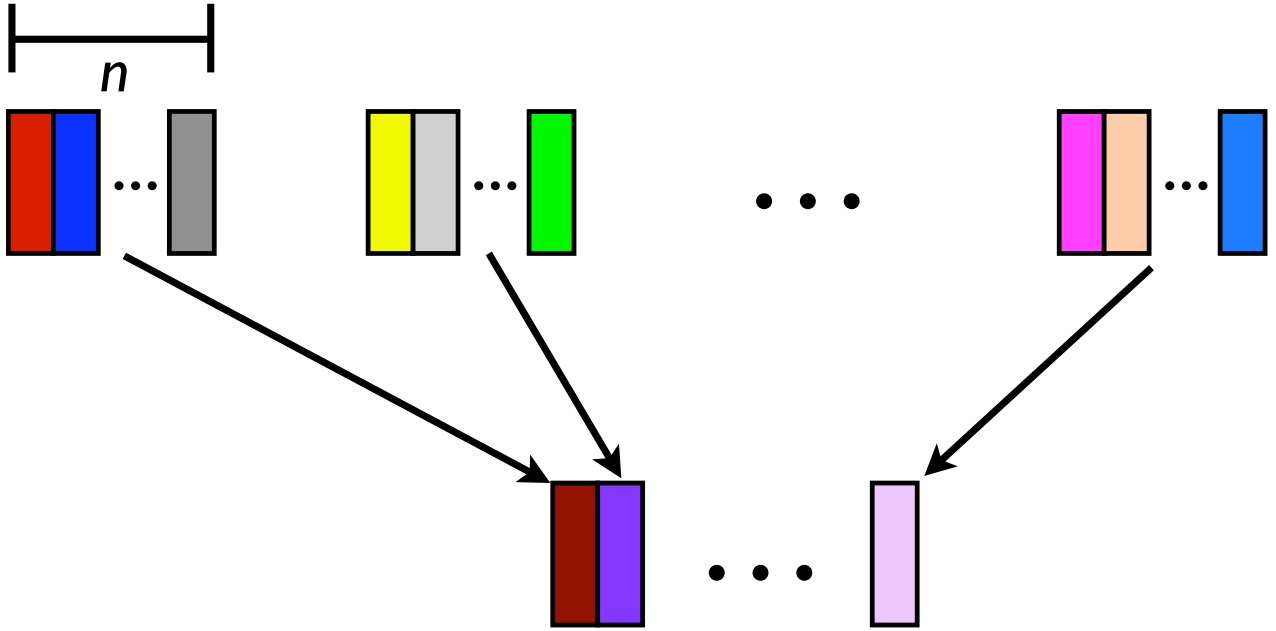


User Cryptosystem

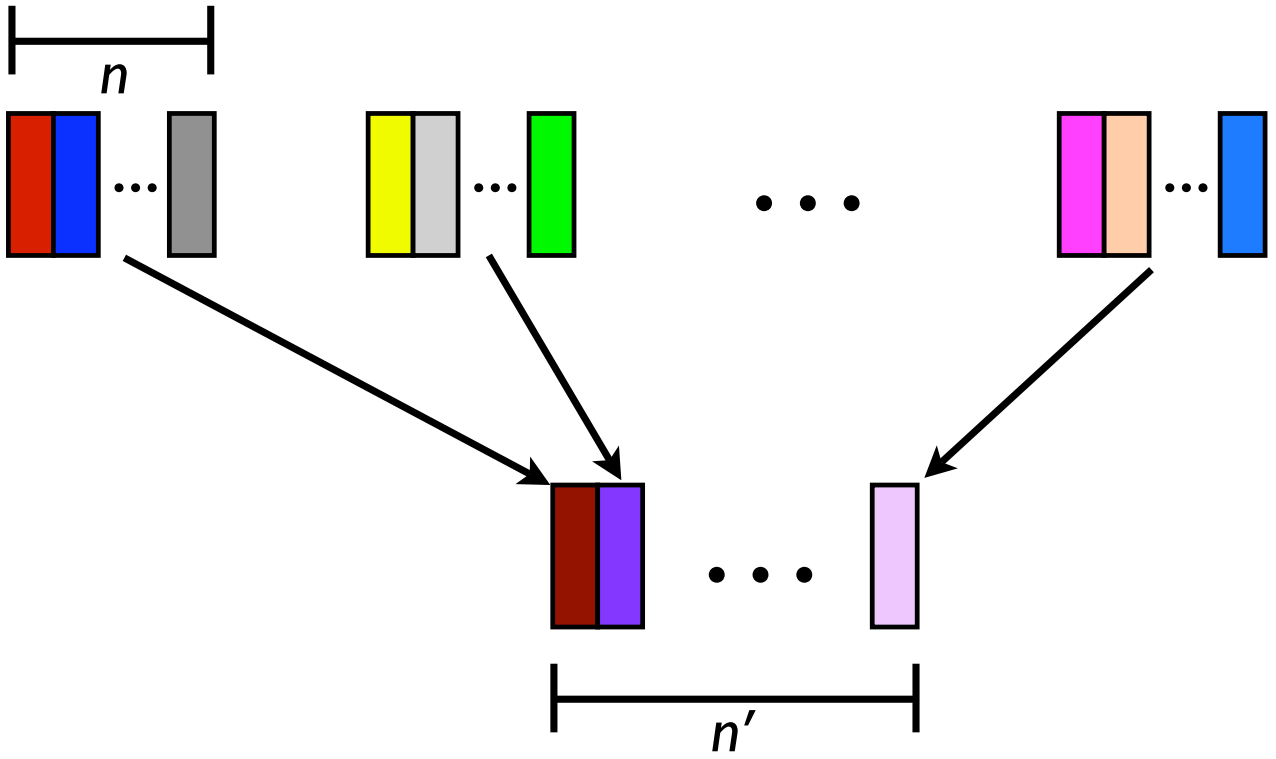


Content Cryptosystem

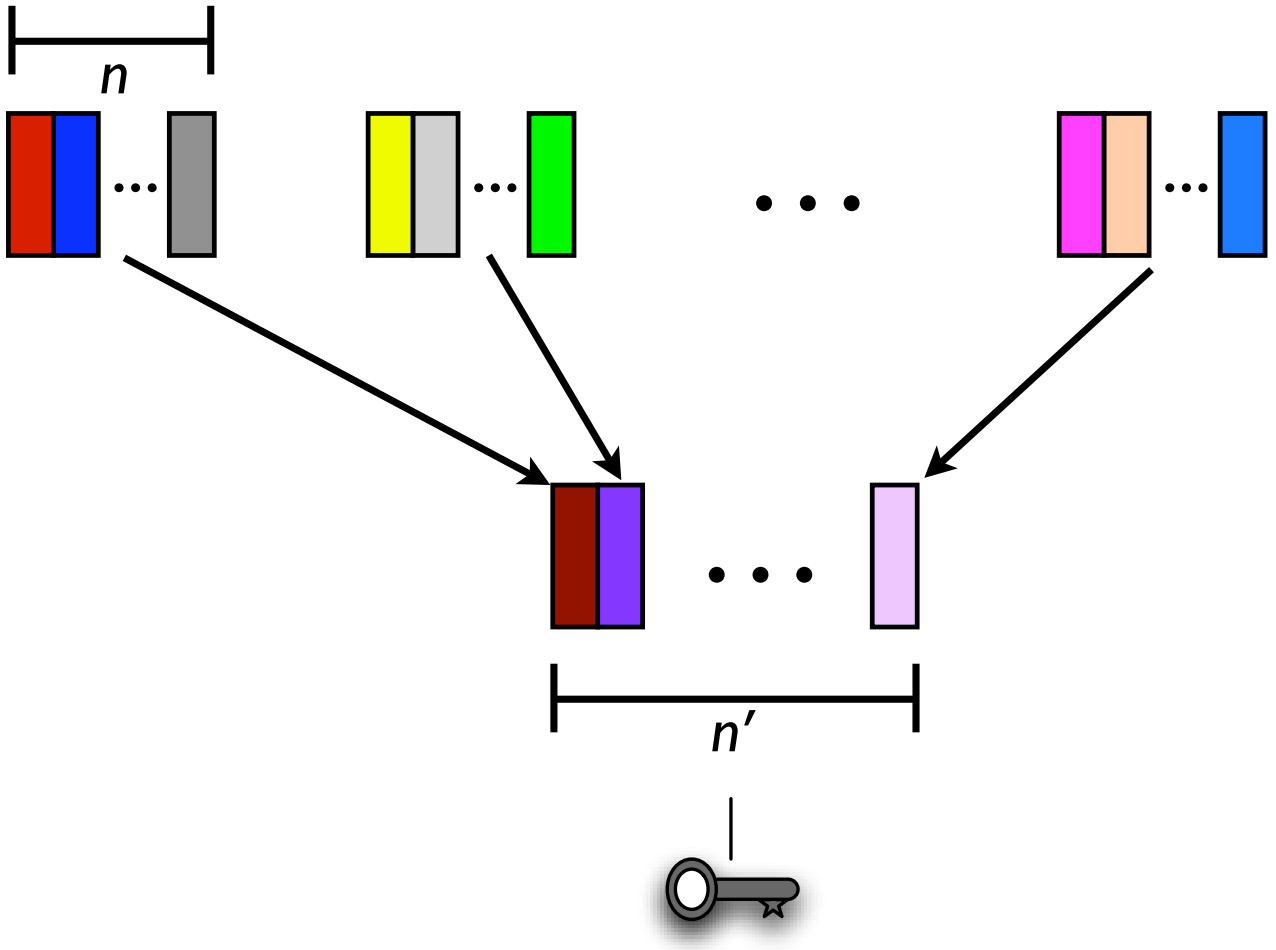
Tiered Construction



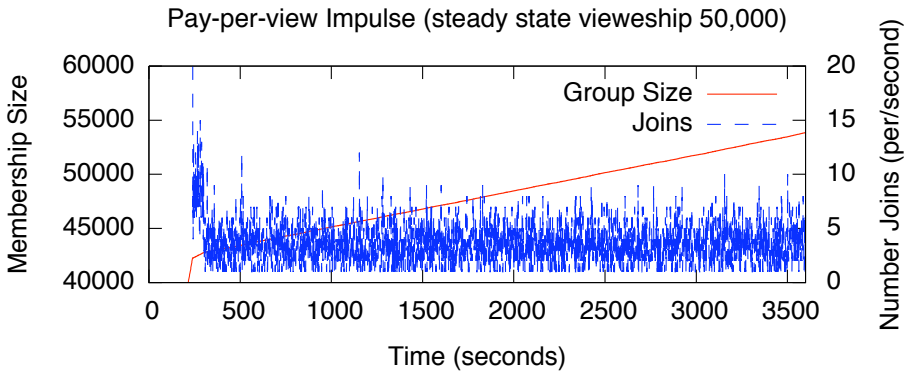
Tiered Construction

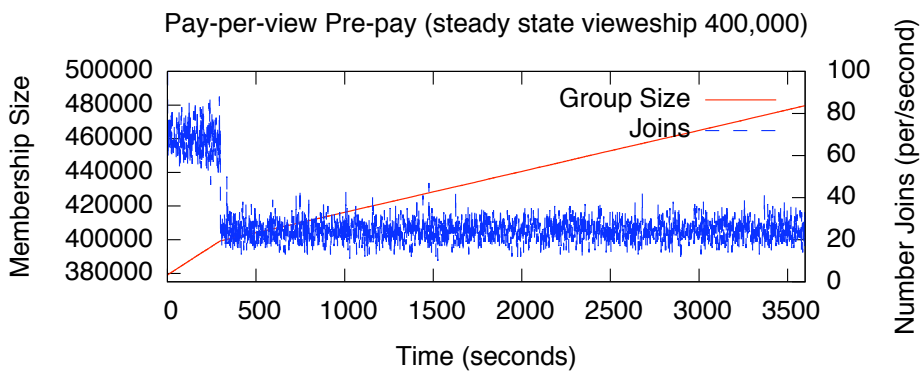


Tiered Construction



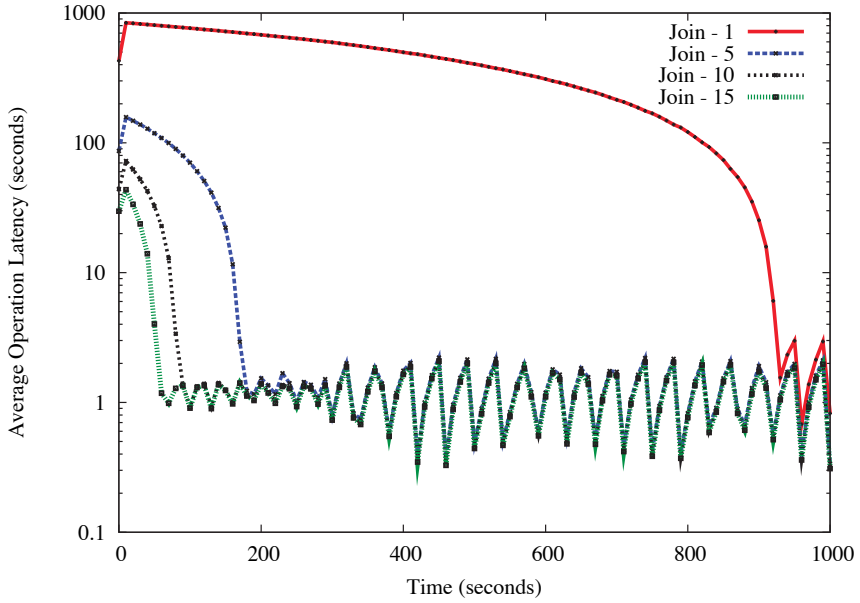
Traffic Model: PPV





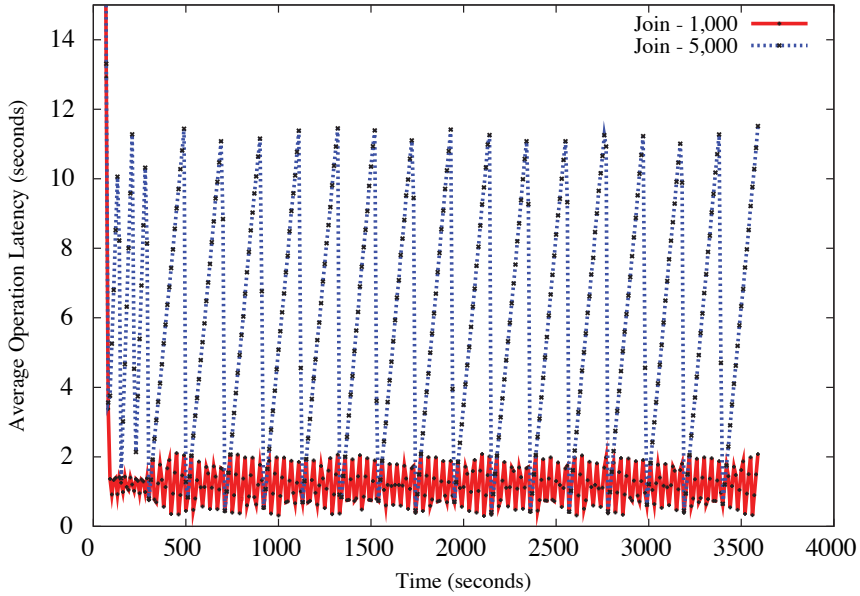
- Pay Per View (PPV) programs exhibit two types of joins: impulse and pre-pay.
  - There are no leaves - users purchase entire programs.
- We use well-known ratings to make results realistic:
  - PPV Boxing (400k) and Tyson vs Holyfield II (1.99M)

How Many Processors?



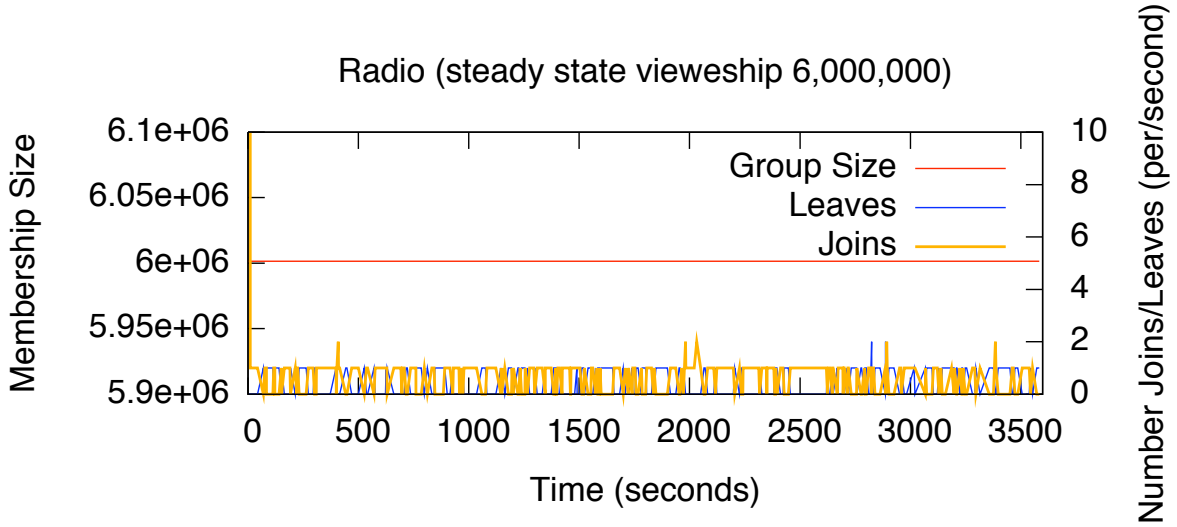
- Extra processors help the system reach quiescence faster as joins are parallelized.
- After quiescence, however, extra processors lay idle.
  - If steady state joins are less than ~400/minute, one processor is more than sufficient.

Group Size?



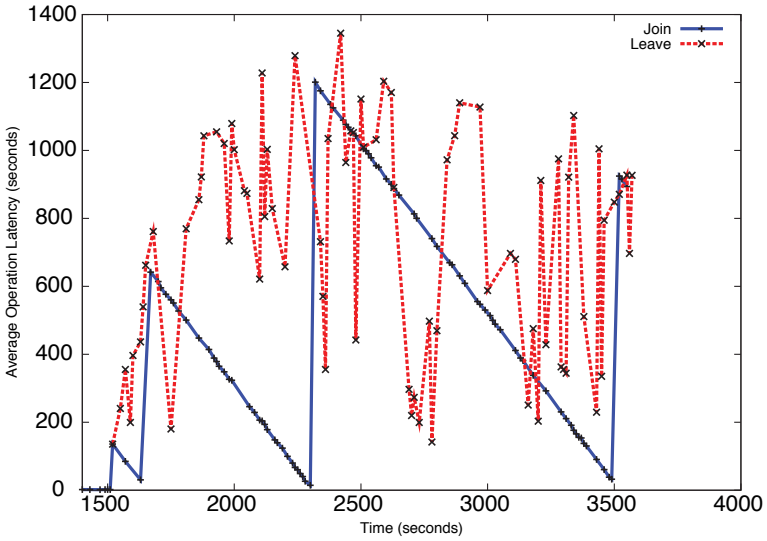
- Larger user groups yield higher latencies throughout the initial surge and quiescence.
- There is no advantage to using large user groups.

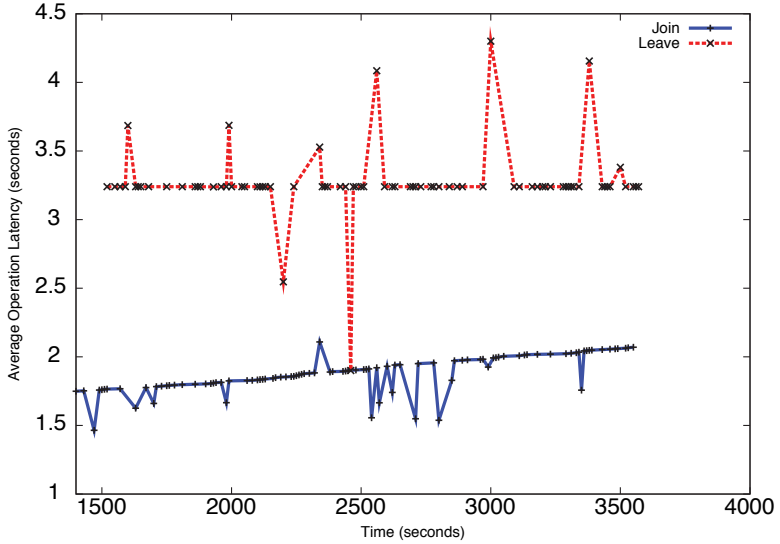
Traffic Model: Satellite Radio



- Satellite Radio users purchase subscriptions.
  - Joins and leaves happen at any time (macro-scale).
- We use Sirius Satellite Radio quarterly reports.
  - 6 million users with 2.8% join and 2% leave rates.

Improving Performance

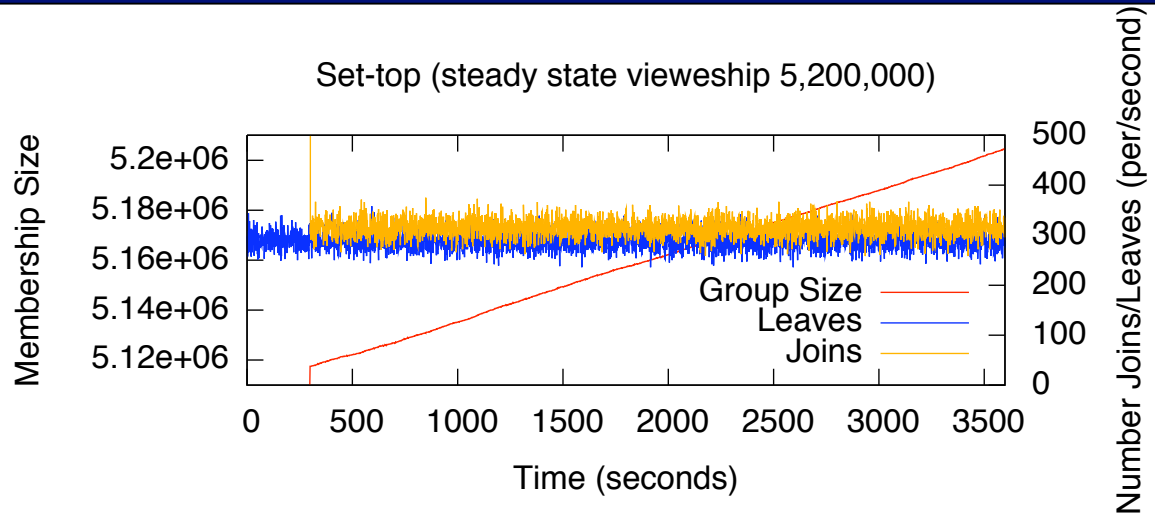




- Performance gains can be achieved both by adding processors and increasing the size of n'.

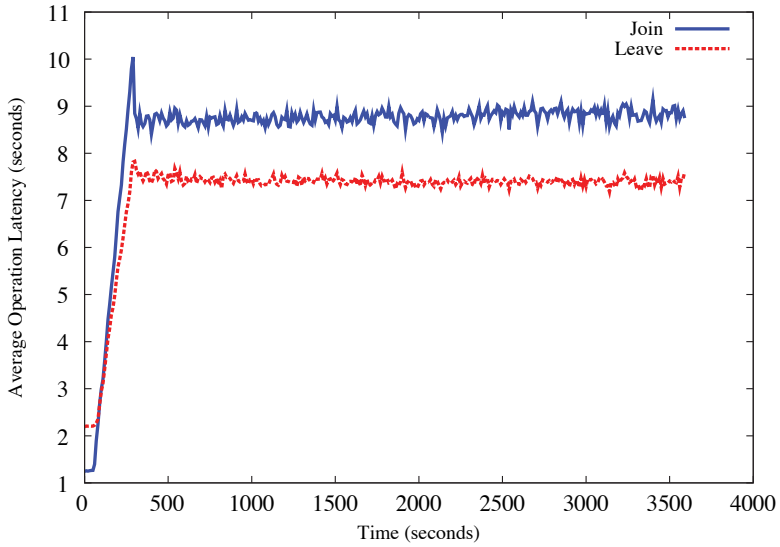
- The use of 100 processors and n'=100 makes such systems efficient.

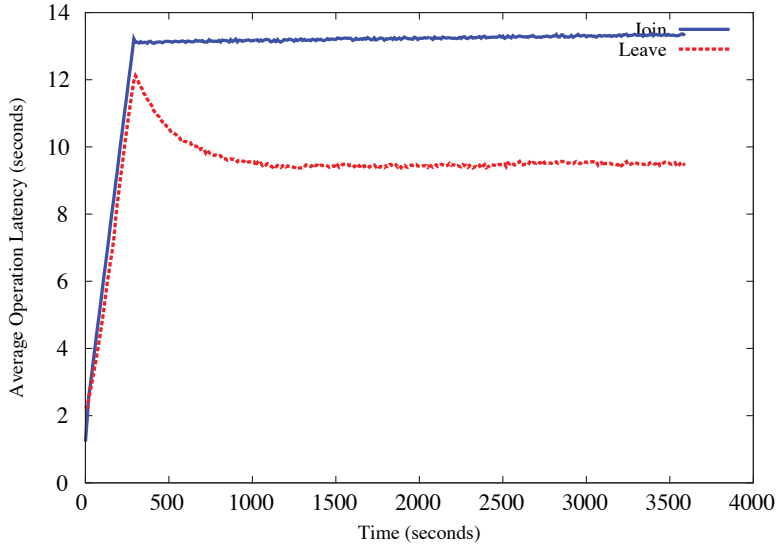
Traffic Model: IPtv



- Attempts to model a "Pay-Per-Channel" scenario.
- We use Nielsen Ratings for popular programs as the source of our data.
  - The Tonight Show: 5.22 million
  - American Idol: 26.9 million
- 2% join and leave rates throughout.

Taxing the Scheduler

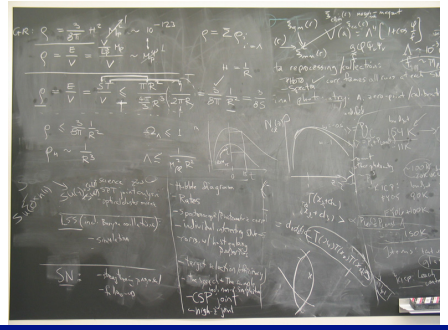




- To simplify management, we performed leaves before joins.
- Joins unfortunately became delayed by massive leaves.
- Even in this worst case scenario, performance is reasonable.

Lessons Learned

- ABE constructions can be made efficient enough to support massive-scale systems.
  - ...if you design carefully...
- Let the system do batching.
- Be aware of key exhaustion for massive systems.



Future Work

PENNSTATE 1855

- Reduce bandwidth using more compact attribute representation.
- Develop/Incorporate smart grouping strategies to lessen the cost of leaves.
- Compare delayed leave strategy to better understand hardware tradeoffs.

Y100 (redux)

Questions

PENNSTATE 1855

Patrick Traynor

traynor@cse.psu.edu

http://www.patricktraynor.org

Joins and Leaves

- A user joining the system requires a single encryption in the user cryptosystem.
- A leave/eviction requires two operations:
  - Generation of a new group attribute.
  - Encryption of that attribute in the user cryptosystem.
- Current users are not affected by joins, but must rekey on leaves.

Sizing n' For Performance

- We want the size of the content cryptosystem to be bound by the performance requirements of our system.
- We experiment with the size of the content cryptosystem under 1,000 unique groups.
- Cost of Crypto Operations:
  - Encryption: 2.24 seconds
  - Decryption: 33 ms