On the Privacy Provisions of Bloom Filters in Lightweight Bitcoin Clients

Arthur Gervais, Ghassan O. Karame, Damian Gruber, Srdjan Čapkun

ETH Zurich, NEC Research

ACSAC 2014
Peer-to-peer decentralized currency

Users keep Bitcoins in a wallet containing multiple addresses (@)

Unlinkability between @

Log of all transactions
Bitcoin’s scalability problems

1. Log of transactions (>25 GB)

2. Clients receive irrelevant transactions

3. Limited data traffic over 3G/4G
Bitcoin’s scalability problems

1. Log of transactions (>25 GB)

2. Clients receive irrelevant transactions

3. Limited data traffic over 3G/4G
Enable mobile Bitcoin clients

Bloom filter

0 0 0 0 0 0 0 0
Enable mobile Bitcoin clients

Insertion \{ @_1, @_2, @_3 \}

Bloom filter

\[
\begin{array}{cccccccc}
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\end{array}
\]
Enable mobile Bitcoin clients

Insertion

Bloom filter

\{ @_1, @_2, @_3 \}

0 1 0 0 1 0 0 0
Solution to scalability problems

Enable mobile Bitcoin clients

Insertion

Bloom filter

\{ @_1, @_2, @_3 \}

0 1 0 0 1 1 1 0
Enable mobile Bitcoin clients

Insertion

\[
\{ @_1, @_2, @_3 \}
\]

Bloom filter

\[
\begin{array}{cccccc}
0 & 1 & 0 & 0 & 1 & 1 & 0 \\
\end{array}
\]
Enable mobile Bitcoin clients

Insertion

Bloom filter

Membership test
Enable mobile Bitcoin clients

**Insertion**

\[
\{ @_1, @_2, @_3 \}
\]

**Bloom filter**

\[
\begin{array}{cccccc}
0 & 1 & 0 & 0 & 1 & 1 & 0 \\
\end{array}
\]

**Membership test**

\[
\{ @_1, @_4, @_5 \}
\]
Enable mobile Bitcoin clients

**Insertion**

<table>
<thead>
<tr>
<th>Bloom filter</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 1 0 0 1 1 0</td>
</tr>
</tbody>
</table>

**Membership test**

{ @1, @4, @5 }

{ @1, @2, @3 }
Enable mobile Bitcoin clients

**Insertion**

**Bloom filter**

- Insertion: \{ @1, @2, @3 \}
- Membership test: \{ @1, @4, @5 \}

- **False positive** @4

**Target False Positive Rate (FPR)**
Enable mobile Bitcoin clients

**Bloom filter**

| 0 | 1 | 0 | 0 | 1 | 1 | 0 |

**Insertion**

\{ @₁, @₂, @₃ \}

**Membership test**

\{ @₁, @₄, @₅ \}

⚠️ @₄ False positive

**target False Positive Rate (FPR)**
Enable mobile Bitcoin clients

<table>
<thead>
<tr>
<th>Insertion</th>
<th>Membership test</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bloom filter</td>
<td>{ @1, @2, @3 }</td>
</tr>
<tr>
<td>0 1 0 0 1 1 1 0</td>
<td>{ @1, @4, @5 }</td>
</tr>
</tbody>
</table>

@4 False positive

@5 True negative

target False Positive Rate (FPR)
Solution to scalability problems

**Simple Payment Verification (SPV)**

**Filter** transactions not relevant for user

SPV client

Full Bitcoin node

Full Bitcoin node
Simple Payment Verification (SPV)

Filter transactions not relevant for user

SPV client

Full Bitcoin node

Full Bitcoin node

Bloom filter
Solution to scalability problems

**Simple Payment Verification (SPV)**

**Filter** transactions not relevant for user

SPV client -> Connection -> **Bloom filter** -> Full Bitcoin node

```
@1 @2 @3
0 1 0 0 1 1 0
```

Bloom filter
Simple Payment Verification (SPV)

Filter transactions not relevant for user

SPV client

Connection

Bloom filter

Full Bitcoin node

Is transaction relevant for Bloom filter?

transactions

Full Bitcoin node
Simple Payment Verification (SPV)

Filter transactions not relevant for user

SPV client

Connection

Bloom filter

Full Bitcoin node

0 1 0 0 1 1 0

Relevant transactions

transactions

Is transaction relevant for Bloom filter?

Full Bitcoin node
Simple Payment Verification (SPV)

Filter transactions not relevant for user

SPV client

Connection

Bloom filter

0 1 0 0 1 1 0

Relevant transactions

Is transaction relevant for Bloom filter?

Full Bitcoin node

transactions

Full Bitcoin node
Solution to scalability problems

Simple Payment Verification (SPV)

Filter transactions not relevant for user

SPV client

Full Bitcoin node

Connection

Bloom filter

Relevant transactions

Is transaction relevant for Bloom filter?

Promise: 33 mio addresses in the Blockchain target FPR: 0.1%

"User addresses hidden amongst 33 000" false positives
Main contributions

1. Given **one** Bloom filter, Bitcoin addresses partially linkable
   - Addresses linkable if < 20 addresses in wallet

2. Given **multiple** Bloom filter, addresses nearly always linkable

3. Propose a lightweight and efficient **countermeasure**
   - **Significantly enhances** the privacy offered by SPV clients
   - Requires **minimum modifications** to Bitcoin
Experimental setting

Model and Privacy measure

Blockchain

SPV client

Adversary
Experimental setting

Model and Privacy measure

SPV client -> Bloom filter 1 + parameters (seed, FPR) -> Adversary
Experimental setting

Model and Privacy measure

Blockchain

All addresses of the Blockchain

SPV client

Bloom filter 1

+ parameters (seed, FPR)

Adversary
Model and Privacy measure

SPV client → Bloom filter 1 + parameters (seed, FPR) → Adversary → All addresses of the Blockchain → Blockchain

- SPV client
- Bloom filter 1
- Parameters (seed, FPR)
- Adversary
- Blockchain
- Addresses
- Positive outcomes
Experimental setting

Model and Privacy measure

![Diagram]

- SPV client
- Blockchain
- All addresses of the Blockchain
- Adversary
- Bloom filter 1
  + parameters (seed, FPR)

Positive

0 1 0 0 1 1 0
Experimental setting

Model and Privacy measure

Blockchain

All addresses of the Blockchain

Adversary

Bloom filter 2

Bloom filter 1

+ parameters (seed, FPR)

SPV client

0 1 0 0 1 1 0

0 1 0 0 1 1 0
Model and Privacy measure

SPV client

Blockchain

All addresses of the Blockchain

Total positives

Bloom filter 1

Bloom filter 2

Adversary

+ parameters (seed, FPR)

0 1 0 0 1 1 0

0 1 0 0 1 1 0

Positive

Positive

Positive

Positive
Experimental setting

Model and Privacy measure

SPV client

Blockchain

All addresses of the Blockchain

Total positives

Intersection

Bloom filter 1
0 1 0 0 1 1 0

Bloom filter 2
0 1 0 0 1 1 0

Adversary

+ parameters
(seed, FPR)
Model and Privacy measure

SPV client + \( \oplus \) Address

Bloom filter 1: 0 1 0 0 1 1 0

Bloom filter 2: 0 1 0 0 1 1 0

Blockchain

All addresses of the Blockchain

Adversary

Total positives

Intersection

True positives

Parameters: (seed, FPR)
Experimental setting

Model and Privacy measure

- SPV client
  - + @
  - Blockchain
    - All addresses of the Blockchain
    - True positives
      - Bloom filter 1
        - Parameters: seed, FPR
      - Bloom filter 2
        - + parameters
          - Total positives
            - Intersection
              - Measure privacy
                - True positives
Experimental setting

Model and Privacy measure

SPV client + @ → Blockchain

All addresses of the Blockchain

Bloom filter 2

0 1 0 0 1 1 0

Bloom filter 1

+ parameters (seed, FPR)

0 1 0 0 1 1 0

Adversary

Total positives

Intersection

Measure privacy

True positives

True positives

Total positives

Intersection

Bloom filter 2

Positive

Positive

Bloom filter 1

Positive

Positive

Adversary

True positives

Intersection

Bloom filter 2

Bloom filter 1

SPV client

Blockchain

Adversary

On the Privacy Provisions of Bloom Filters in Lightweight Bitcoin Clients - Arthur Gervais
Stair stepping

Bloom filter designed for
- N **addresses**
- **target FPR** when N addresses inserted

![Wallet icon](image) → 0100110 BF1
Stair stepping

Bloom filter designed for
- N **addresses**
- **target FPR** when N addresses inserted

![Bloom Filter Diagram]

BF1

BF2
Stair stepping

Bloom filter designed for
- N addresses
- target FPR when N addresses inserted

![Diagram showing the process of adding addresses to a Bloom filter and resizing when necessary.](image)

- BF1
- BF2
- BF3
Stair stepping

Bloom filter designed for
- N **addresses**
- target FPR when N addresses inserted

![Diagram of Bloom filter growth and resize](image)

**Rationale:** *avoid* filters with different sizes
Stair stepping

Bloom filter designed for
- N addresses
- target FPR when N addresses inserted

Create filter for N addresses, but insert less

actual FPR ≤ target FPR

Rationale: avoid filters with different sizes
Privacy influencing design choices of SPV clients

Resizing

- Hash functions adapted to fill space of new Bloom filter

- **Consequence**: New filter yields different false positives
Resizing

- Hash functions adapted to fill space of new Bloom filter

**Consequence**: New filter yields different false positives

Restarting

- Fresh seed value for hash functions of new Bloom filter

**Consequence**: New filter yields different false positives
Privacy influencing design choices of SPV clients

Resizing

- Hash functions adapted to fill space of new Bloom filter
- Consequence: New filter yields different false positives

Summary of current SPV design choices

1. Stair stepping → actual FPR ≤ target FPR
2. Resizing → different False Positive yields different False Positives
3. Restarting → different False Positive yields different False Positives

Consequence: New filter yields different false positives
Stair stepping - Actual FPR vs. Target FPR

False Positive Rate in %

Number of addresses in wallet
Stair stepping - Actual FPR vs. Target FPR

- target FPR is constant
- actual FPR << target FPR
- actual FPR = target FPR
One Bloom filter

Probability of linking all addresses

Number of addresses of SPV client

Probability of linking all addresses

Current implementation
Multiple Bloom filters

Filter 1

@1  @2  @3
Multiple Bloom filters

Filter 1

0 1 0 0 1 1 0

@1 @2 @3

Filter 2

0 1 0 0 1 1 0

@1 @4 @5
Multiple Bloom filters

Filter 1
0 1 0 0 1 1 0

Filter 2
0 1 0 0 1 1 0

... Filter n
0 1 0 0 1 1 0

@1 @2 @3

@1 @4 @5

@1 @6 @7
Multiple Bloom filters

Filter 1

Filter 2

Filter n

@1 @2 @3

@1 @4 @5

@1 @6 @7
Multiple Bloom filters

Filter 1

Filter 2

Filter n

0 1 0 0 1 1 0

0 1 0 0 1 1 0

0 1 0 0 1 1 0

False positives
## Evaluation - Multiple Bloom filters

### Experiment 1 - No resize

<table>
<thead>
<tr>
<th>Exp.</th>
<th>Client</th>
<th>Seed</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>No resize</td>
<td>Same</td>
<td>Same</td>
<td>Same</td>
</tr>
<tr>
<td>Resize</td>
<td>Same</td>
<td>Same</td>
<td>Different</td>
</tr>
<tr>
<td>Restart</td>
<td>Same</td>
<td>Different</td>
<td>Same</td>
</tr>
<tr>
<td>&gt; 2 filter</td>
<td>Same</td>
<td>Different</td>
<td>Different</td>
</tr>
</tbody>
</table>
# Evaluation - Multiple Bloom filters

## Experiment 1 - No resize

<table>
<thead>
<tr>
<th>Exp.</th>
<th>Client</th>
<th>Seed</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>No resize</td>
<td>Same</td>
<td>Same</td>
<td>Same</td>
</tr>
<tr>
<td>Resize</td>
<td>Same</td>
<td>Same</td>
<td>Different</td>
</tr>
<tr>
<td>Restart</td>
<td>Same</td>
<td>Different</td>
<td>Same</td>
</tr>
<tr>
<td>&gt; 2 filter</td>
<td>Same</td>
<td>Different</td>
<td>Different</td>
</tr>
</tbody>
</table>
Evaluation - Multiple Bloom filters

Experiment 1 - No resize

<table>
<thead>
<tr>
<th>Exp.</th>
<th>Client</th>
<th>Seed</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>No resize</td>
<td>Same</td>
<td>Same</td>
<td>Same</td>
</tr>
<tr>
<td>Resize</td>
<td>Same</td>
<td>Same</td>
<td>Different</td>
</tr>
<tr>
<td>Restart</td>
<td>Same</td>
<td>Different</td>
<td>Same</td>
</tr>
<tr>
<td>&gt; 2 filter</td>
<td>Same</td>
<td>Different</td>
<td>Different</td>
</tr>
</tbody>
</table>
### Evaluation - Multiple Bloom filters

#### Experiment 1 - No resize

<table>
<thead>
<tr>
<th>Exp.</th>
<th>Client</th>
<th>Seed</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>No resize</td>
<td>Same</td>
<td>Same</td>
<td>Same</td>
</tr>
<tr>
<td>Resize</td>
<td>Same</td>
<td>Same</td>
<td>Different</td>
</tr>
<tr>
<td>Restart</td>
<td>Same</td>
<td>Different</td>
<td>Same</td>
</tr>
<tr>
<td>&gt; 2 filter</td>
<td>Same</td>
<td>Different</td>
<td>Different</td>
</tr>
</tbody>
</table>

Results:
- $B_2$ yields additional positives compared to $B_1$
- The adversary does not learn a lot

Intersection:

- $@_1 @_2 @_3$
- $@_1 @_2 @_3 @_4$

Add addresses, No resize

> 2 filter
Evaluation - Multiple Bloom filters

Experiment 2 - Resize

B1 \[\rightarrow\] Add addresses, Resize \[\rightarrow\] B2

@1@2@3 \[\rightarrow\] Intersection \[\rightarrow\] @1@2@5@6

<table>
<thead>
<tr>
<th>Exp.</th>
<th>Client</th>
<th>Seed</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>No resize</td>
<td>Same</td>
<td>Same</td>
<td>Same</td>
</tr>
<tr>
<td>Resize</td>
<td>Same</td>
<td>Same</td>
<td>Different</td>
</tr>
<tr>
<td>Restart</td>
<td>Same</td>
<td>Different</td>
<td>Same</td>
</tr>
<tr>
<td>&gt; 2 filter</td>
<td>Same</td>
<td>Different</td>
<td>Different</td>
</tr>
</tbody>
</table>
Evaluation - Multiple Bloom filters

Experiment 2 - Resize

\[ B_1 \xrightarrow{\text{Add addresses, Resize}} B_2 \]

Intersection

@1@2@3

@1@2@5@6

Results

- Yield mostly different positives
- Can be used for intersection attack

<table>
<thead>
<tr>
<th>Exp.</th>
<th>Client</th>
<th>Seed</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>No resize</td>
<td>Same</td>
<td>Same</td>
<td>Same</td>
</tr>
<tr>
<td>Resize</td>
<td>Same</td>
<td>Same</td>
<td>Different</td>
</tr>
<tr>
<td>Restart</td>
<td>Same</td>
<td>Different</td>
<td>Same</td>
</tr>
<tr>
<td>&gt; 2 filter</td>
<td>Same</td>
<td>Different</td>
<td>Different</td>
</tr>
</tbody>
</table>
Experiment 3 - Restart

<table>
<thead>
<tr>
<th>Exp.</th>
<th>Client</th>
<th>Seed</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>No resize</td>
<td>Same</td>
<td>Same</td>
<td>Same</td>
</tr>
<tr>
<td>Resize</td>
<td>Same</td>
<td>Same</td>
<td>Different</td>
</tr>
<tr>
<td>Restart</td>
<td>Same</td>
<td>Different</td>
<td>Same</td>
</tr>
<tr>
<td>&gt; 2 filter</td>
<td>Same</td>
<td>Different</td>
<td>Different</td>
</tr>
</tbody>
</table>
Evaluation - Multiple Bloom filters

Experiment 3 - Restart

\[ \text{B}_1 \xrightarrow{\text{Restart, generate a new seed}} \text{B}_2 \]

Results

- Yield mostly different positives
- Can be used for intersection attack

<table>
<thead>
<tr>
<th>Exp.</th>
<th>Client</th>
<th>Seed</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>No resize</td>
<td>Same</td>
<td>Same</td>
<td>Same</td>
</tr>
<tr>
<td>Resize</td>
<td>Same</td>
<td>Same</td>
<td>Different</td>
</tr>
<tr>
<td>Restart</td>
<td>Same</td>
<td>Different</td>
<td>Same</td>
</tr>
<tr>
<td>&gt; 2 filter</td>
<td>Same</td>
<td>Different</td>
<td>Different</td>
</tr>
</tbody>
</table>
Evaluation - Multiple Bloom filters

Experiment 4 - More than 2 filter

<table>
<thead>
<tr>
<th>Exp.</th>
<th>Client</th>
<th>Seed</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>No resize</td>
<td>Same</td>
<td>Same</td>
<td>Same</td>
</tr>
<tr>
<td>Resize</td>
<td>Same</td>
<td>Same</td>
<td>Different</td>
</tr>
<tr>
<td>Restart</td>
<td>Same</td>
<td>Different</td>
<td>Same</td>
</tr>
<tr>
<td>&gt; 2 filter</td>
<td>Same</td>
<td>Different</td>
<td>Different</td>
</tr>
</tbody>
</table>
Evaluation - Multiple Bloom filters

Experiment 4 - More than 2 filter

Results

<table>
<thead>
<tr>
<th>Target FPR (%)</th>
<th>Probability linking all addresses with 3+ BF</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.05</td>
<td>~1</td>
</tr>
<tr>
<td>0.1</td>
<td>~1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Exp.</th>
<th>Client</th>
<th>Seed</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>No resize</td>
<td>Same</td>
<td>Same</td>
<td>Same</td>
</tr>
<tr>
<td>Resize</td>
<td>Same</td>
<td>Same</td>
<td>Different</td>
</tr>
<tr>
<td>Restart</td>
<td>Same</td>
<td>Different</td>
<td>Same</td>
</tr>
<tr>
<td>&gt; 2 filter</td>
<td>Same</td>
<td>Different</td>
<td>Different</td>
</tr>
</tbody>
</table>
Evaluation - Multiple Bloom filters

Experiment 4 - More than 2 filter

Results

<table>
<thead>
<tr>
<th>Target FPR (%)</th>
<th>Probability linking all addresses with 3+ BF</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.05</td>
<td>~1</td>
</tr>
<tr>
<td>0.1</td>
<td>~1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Exp.</th>
<th>Client</th>
<th>Seed</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>No resize</td>
<td>Same</td>
<td>Same</td>
<td>Same</td>
</tr>
<tr>
<td>Resize</td>
<td>Same</td>
<td>Same</td>
<td>Different</td>
</tr>
<tr>
<td>Restart</td>
<td>Same</td>
<td>Different</td>
<td>Same</td>
</tr>
<tr>
<td>&gt; 2 filter</td>
<td>Same</td>
<td>Different</td>
<td>Different</td>
</tr>
</tbody>
</table>

3 Bloom filter

All addresses inserted into B₁ can be linked
Observations

1. Need of constant false positive rate

2. Multiple Bloom filter with different parameters

3. SPV clients should keep state (e.g., about seed)
Countermeasures

Proposed solution

- Pre-generate Bitcoin addresses and insert into filter
- Keep state about outsourced Bloom filter
- Overhead: For 100 addresses, < 1 kb
Proposed solution

- Pre-generate Bitcoin addresses and insert into filter
- Keep state about outsourced Bloom filter

<table>
<thead>
<tr>
<th>Number of addresses of SPV client</th>
<th>Probability of linking all addresses</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>10</td>
<td>0.2</td>
</tr>
<tr>
<td>20</td>
<td>0.4</td>
</tr>
<tr>
<td>30</td>
<td>0.6</td>
</tr>
<tr>
<td>40</td>
<td>0.8</td>
</tr>
<tr>
<td>50</td>
<td>1</td>
</tr>
</tbody>
</table>

- Bloom filter 1
- Bloom filter 2

Current implementation

Countermeasure
Information leakage through Bloom Filters in SPV clients

Analytical and Empirical evaluation

- 1 Bloom filter critical if < 20 Bitcoin addresses
- 3+ Bloom filter intersection attack particularly strong
Summary

Information leakage through Bloom Filters in SPV clients

Analytical and Empirical evaluation

- 1 Bloom filter critical if < 20 Bitcoin addresses
- 3+ Bloom filter intersection attack particularly strong

Lightweight countermeasure

- **Significantly** reduces leakage
- Intersection attack **not effective**
- Requires **few** changes
Summary

Information leakage through Bloom Filters in SPV clients

Analytical and Empirical evaluation

- 1 Bloom filter critical if < 20 Bitcoin addresses
- 3+ Bloom filter intersection attack particularly strong

Lightweight countermeasure

- **Significantly** reduces leakage
- Intersection attack **not effective**
- Requires **few** changes

Conclusion

- Bloom filter for privacy is delicate
- Designed carefully we can achieve proper privacy
Summary

Information leakage through Bloom Filters in SPV clients

Analytical and Empirical evaluation

- 1 Bloom filter critical if < 20 Bitcoin addresses
- 3+ Bloom filter intersection attack particularly strong

Lightweight countermeasure

- **Significantly** reduces leakage
- Intersection attack **not effective**
- Requires **few** changes

Conclusion

- Bloom filter for privacy is delicate
- Designed carefully we can achieve proper privacy

Thank you!
Privacy metric

- Probability of correctly guessing \( j \) real addresses of a filter
- \( N \): # of addresses inserted into filter
- \( S \): # of false positives
Privacy metric

- Probability of correctly guessing $j$ **real addresses** of a filter
- $N$: # of addresses inserted into filter
- $S$: # of false positives

$$P(1) = \frac{N}{N + S}$$
Privacy metric

- Probability of correctly guessing *j* **real addresses** of a filter
- $N$: # of addresses inserted into filter
- $S$: # of false positives

\[
P(j) = \prod_{k=0}^{j-1} \frac{N - k}{N + S - k} = \frac{N}{N + S} \cdot \frac{N - 1}{N + S - 1} \cdots
\]
Privacy metric

- Probability of correctly guessing $j$ real addresses of a filter
- $N$: # of addresses inserted into filter
- $S$: # of false positives

$$P(j) = \prod_{k=0}^{j-1} \frac{N - k}{N + S - k} = \frac{N}{N + S} \cdot \frac{N - 1}{N + S - 1} \cdots$$

- Guessing all addresses correctly  \[\rightarrow\] link all addresses

$$P(N) = \prod_{k=0}^{N-1} \frac{N - k}{N + S - k} = \frac{N!S!}{(N + S)!}$$
Adversary’s model

**Goal**: Link Bitcoin addresses inserted within a Bloom filter

- Operates full Bitcoin nodes
- Parses the Blockchain for addresses
- Knows parameter for Bloom filter creation
  - Target false positive rate
- Collects multiple Bloom filters per SPV client
Solution to scalability problems

Bloom filter false positive rate

\[
FPR(m) = \left( 1 - \left( 1 - \frac{1}{n} \right)^{km} \right)^k
\]

Notation

- **n**: Size of the Bloom filter in bits
- **m**: Number of elements inserted into the Bloom filter
- **k**: Number of hash functions of the Bloom filter