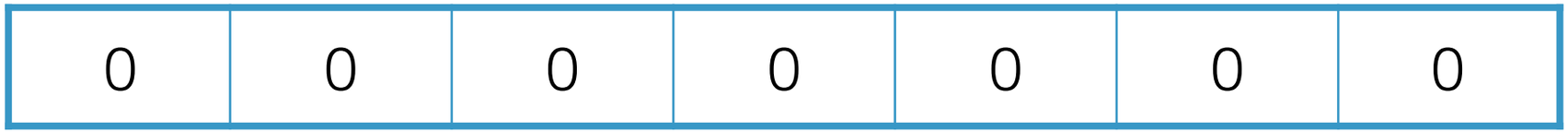
Blockchain Privacy
Bloom Filter & SPV

Enable mobile Bitcoin clients

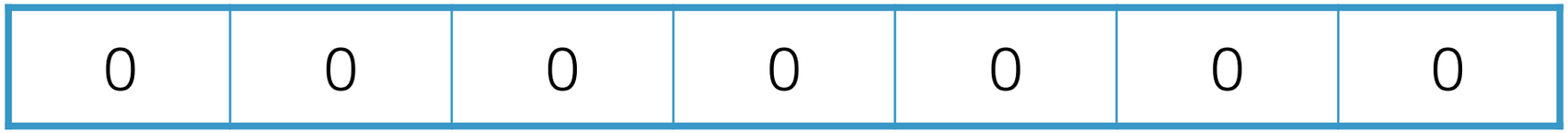
Bloom filter



Enable mobile Bitcoin clients

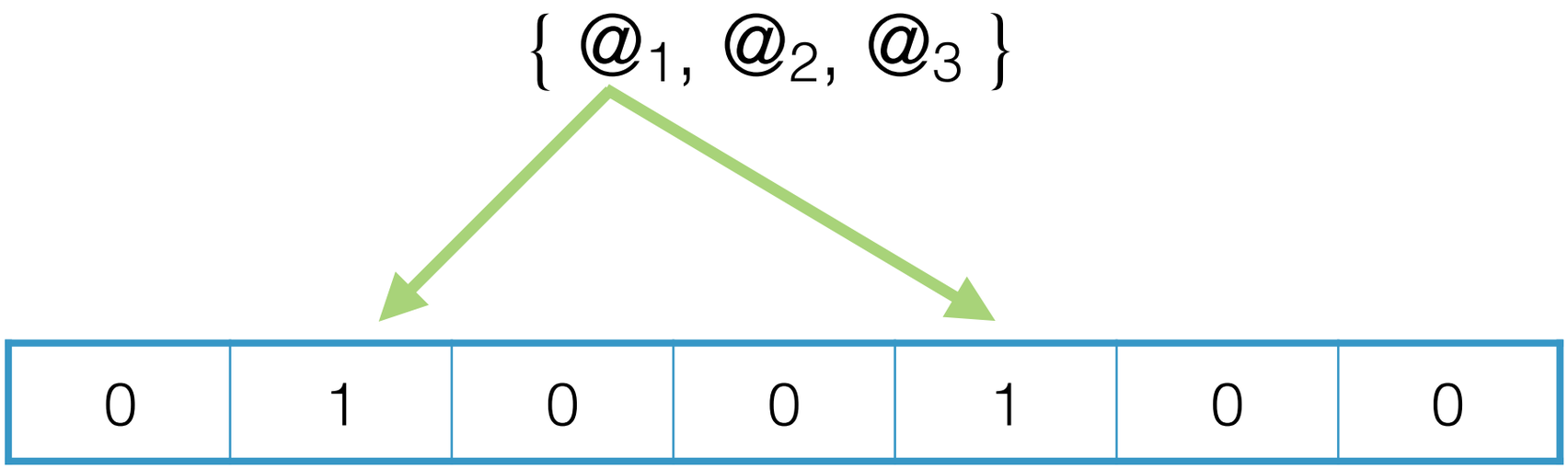
Insertion $\{ @_1, @_2, @_3 \}$

Bloom filter



Enable mobile Bitcoin clients

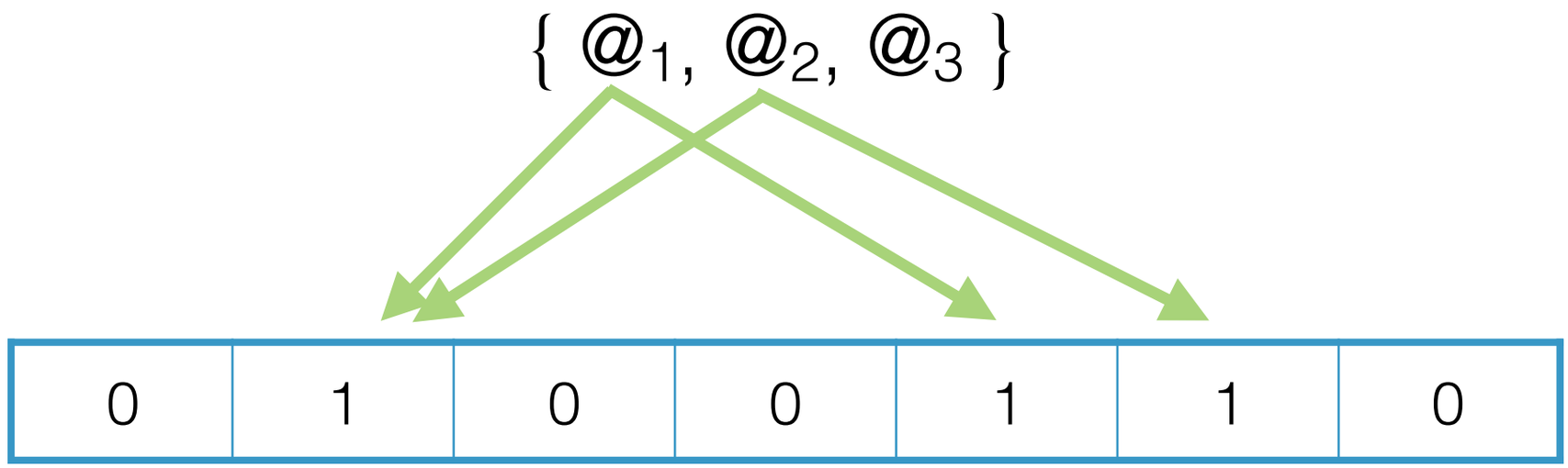
Insertion



Bloom filter

Enable mobile Bitcoin clients

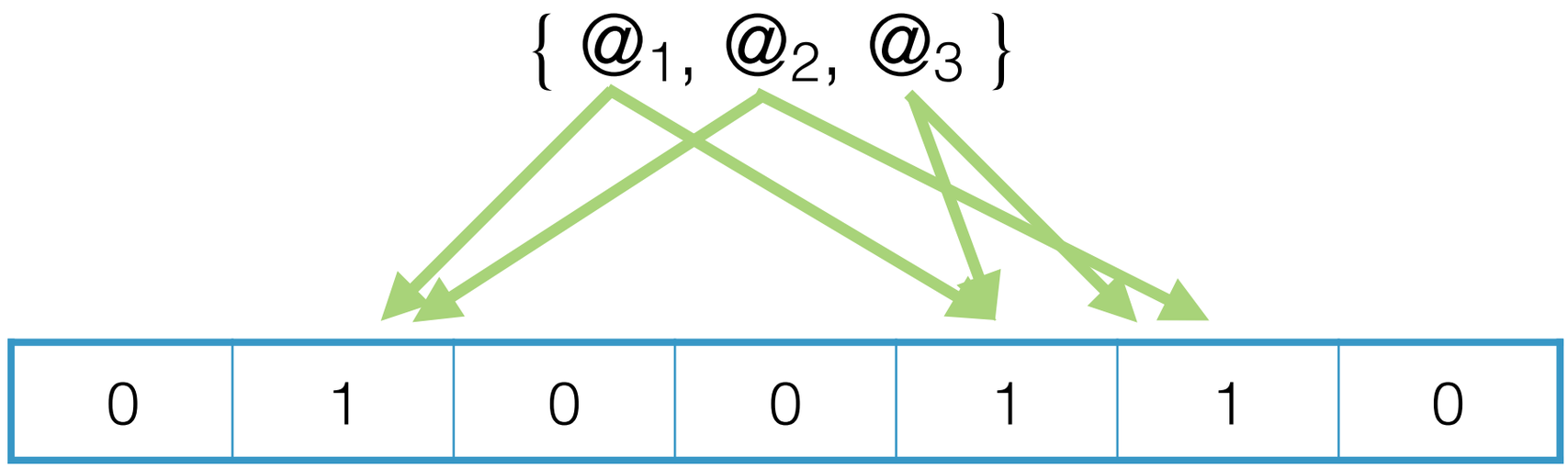
Insertion



Bloom filter

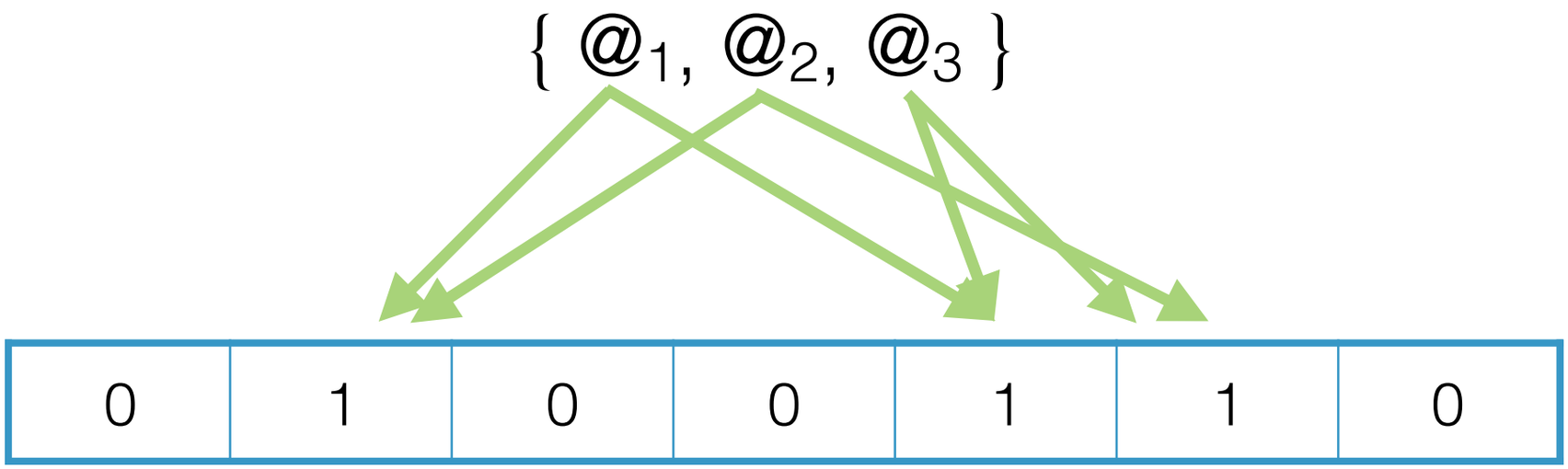
Enable mobile Bitcoin clients

Insertion



Enable mobile Bitcoin clients

Insertion

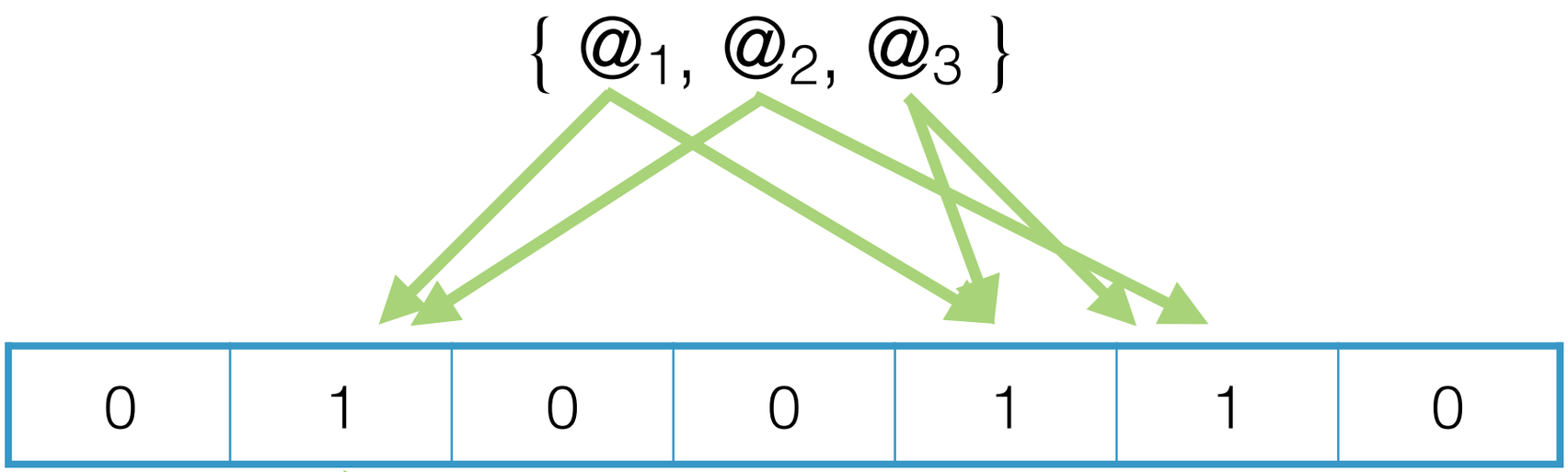


Bloom filter

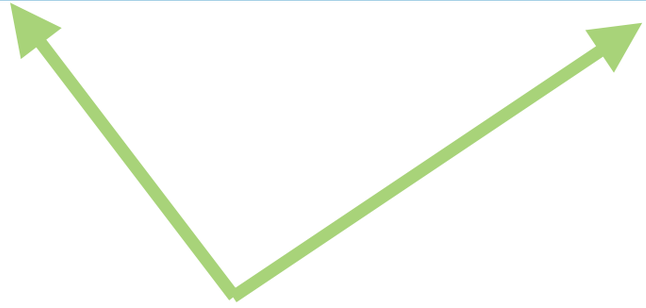
Membership test { @1, @4, @5 }

Enable mobile Bitcoin clients

Insertion

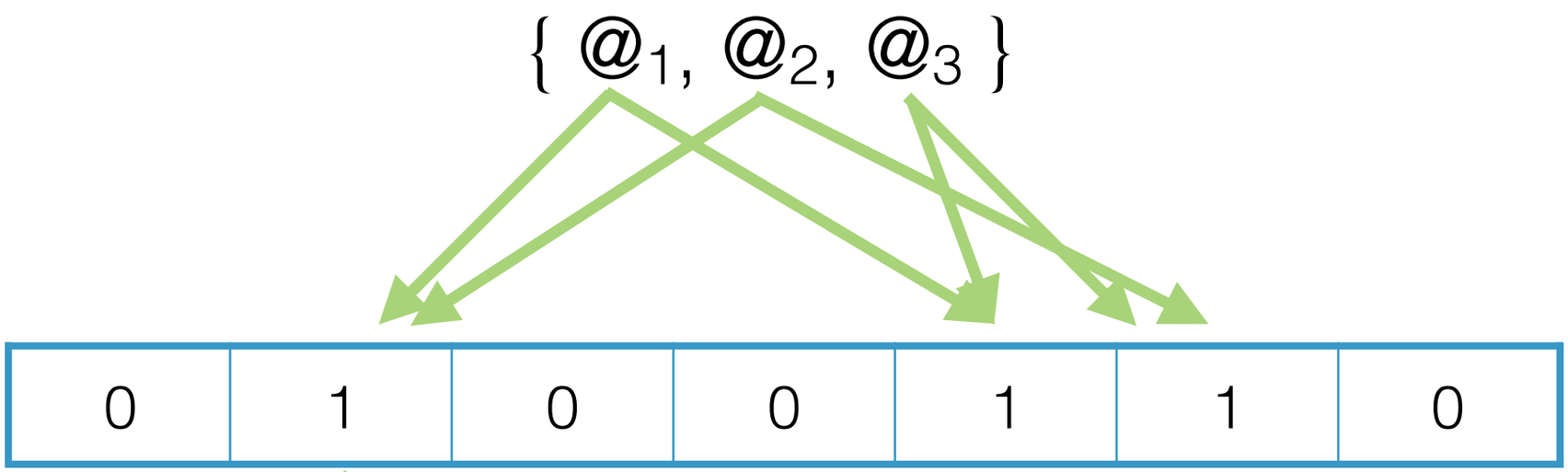


Membership test



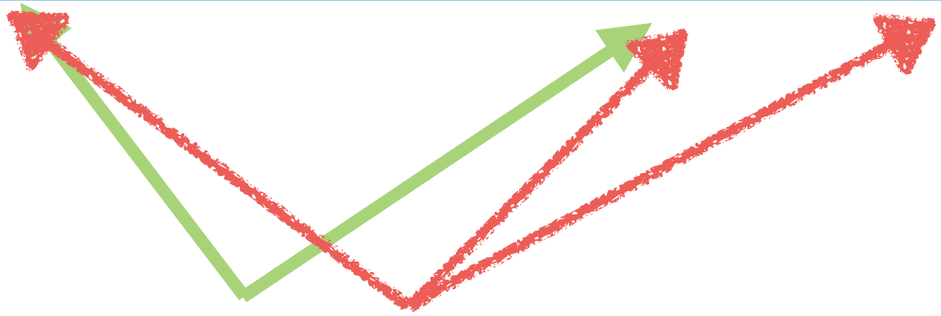
Enable mobile Bitcoin clients

Insertion



Bloom filter

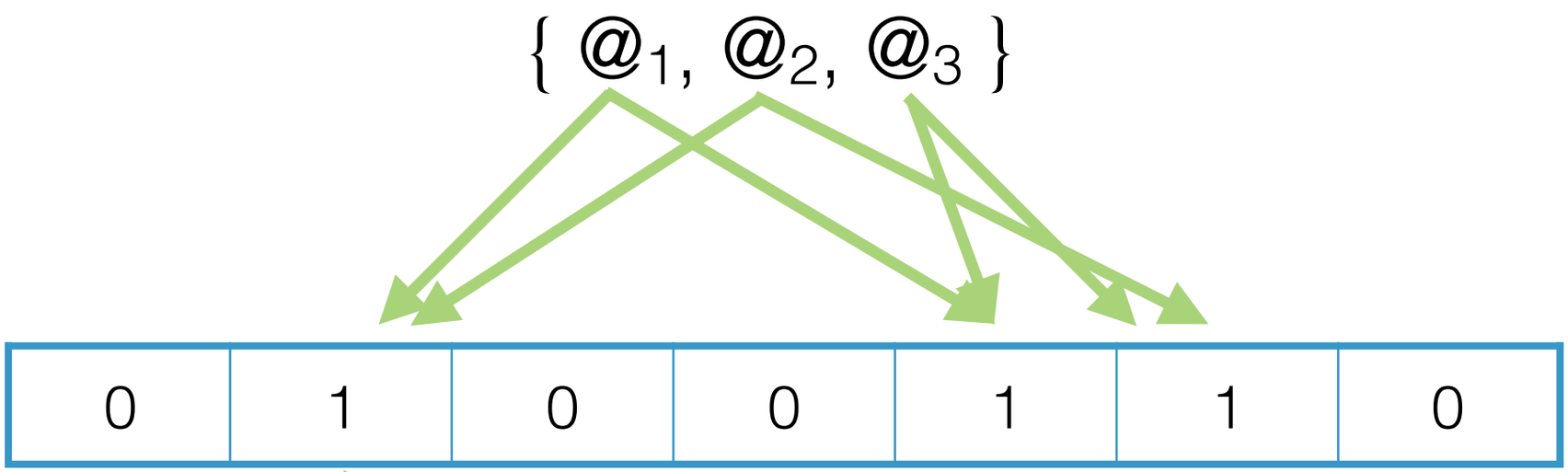
Membership test



{ @1, @4, @5 }

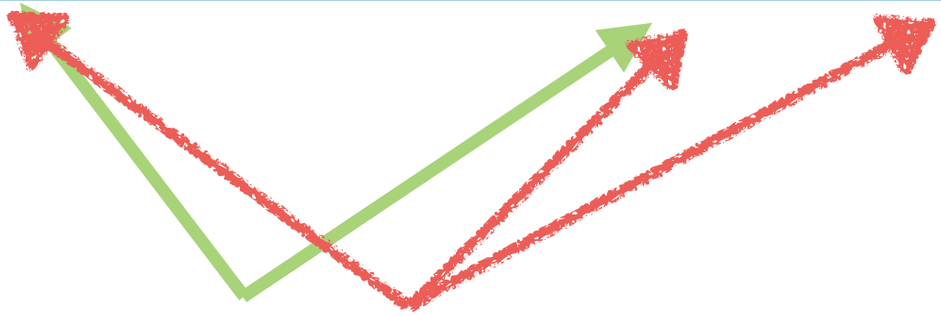
Enable mobile Bitcoin clients

Insertion



Bloom filter

Membership test

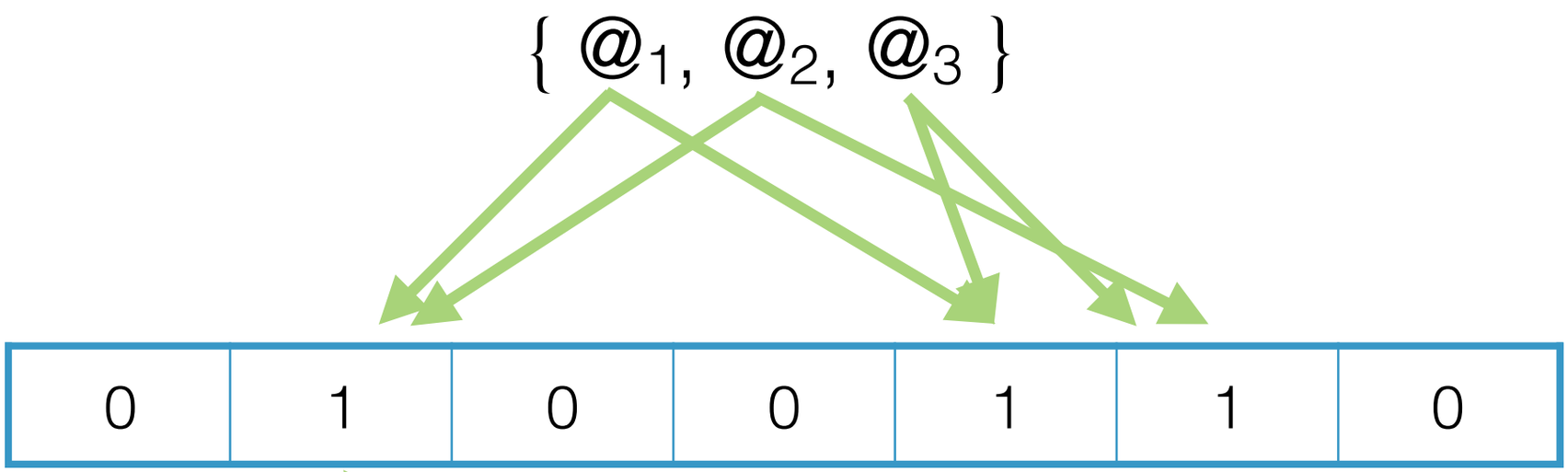


{ @1, @4, @5 }

! @4 False positive → **target False Positive Rate** (FPR)

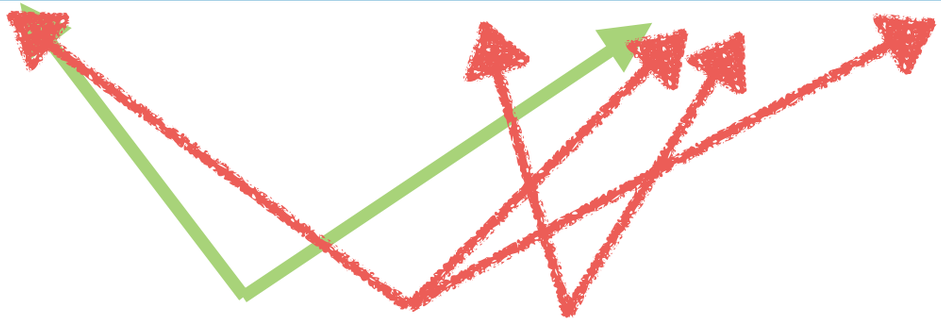
Enable mobile Bitcoin clients

Insertion



Bloom filter

Membership test

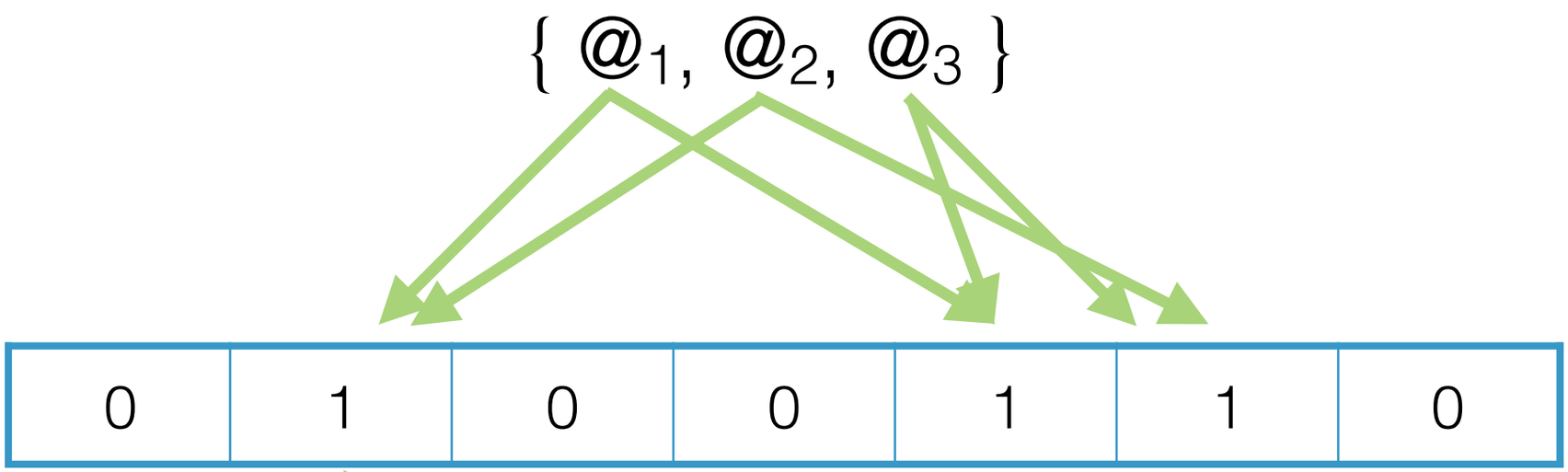


{ @1, @4, @5 }

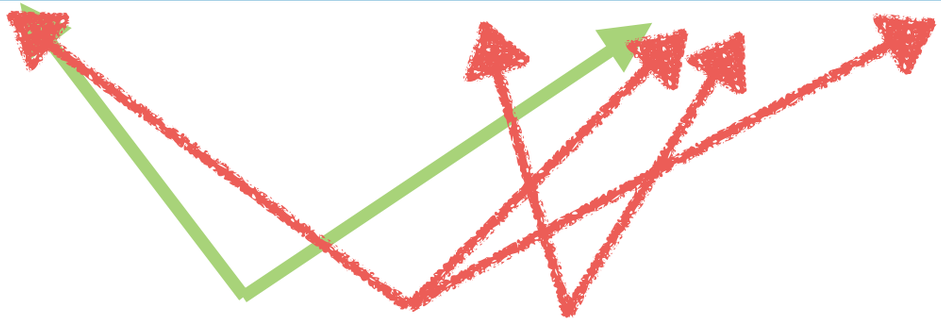
! @4 False positive → **target False Positive Rate** (FPR)

Enable mobile Bitcoin clients

Insertion



Bloom filter



Membership test

{ @1, @4, @5 }

! @4 False positive → **target False Positive Rate** (FPR)

@5 True negative

Simple Payment Verification (SPV)

Filter transactions not relevant for user

SPV client

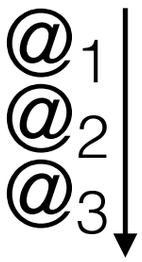
Full Bitcoin node

Full Bitcoin node

Simple Payment Verification (SPV)

Filter transactions not relevant for user

SPV client



Bloom filter

Full Bitcoin node

Full Bitcoin node

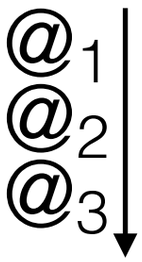
Simple Payment Verification (SPV)

Filter transactions not relevant for user

SPV client

Connection

Full Bitcoin node



Bloom filter

Full Bitcoin node

Simple Payment Verification (SPV)

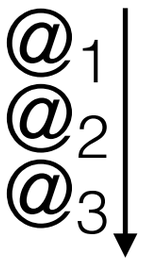
Filter transactions not relevant for user

SPV client

Connection

Bloom filter

Full Bitcoin node



Bloom filter

Full Bitcoin node

Simple Payment Verification (SPV)

Filter transactions not relevant for user

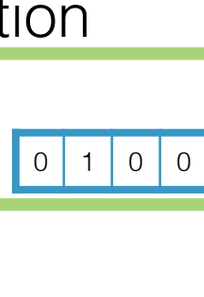
SPV client

$@_1$
$@_2$
$@_3$

Bloom filter

Connection

Bloom filter



Full Bitcoin node

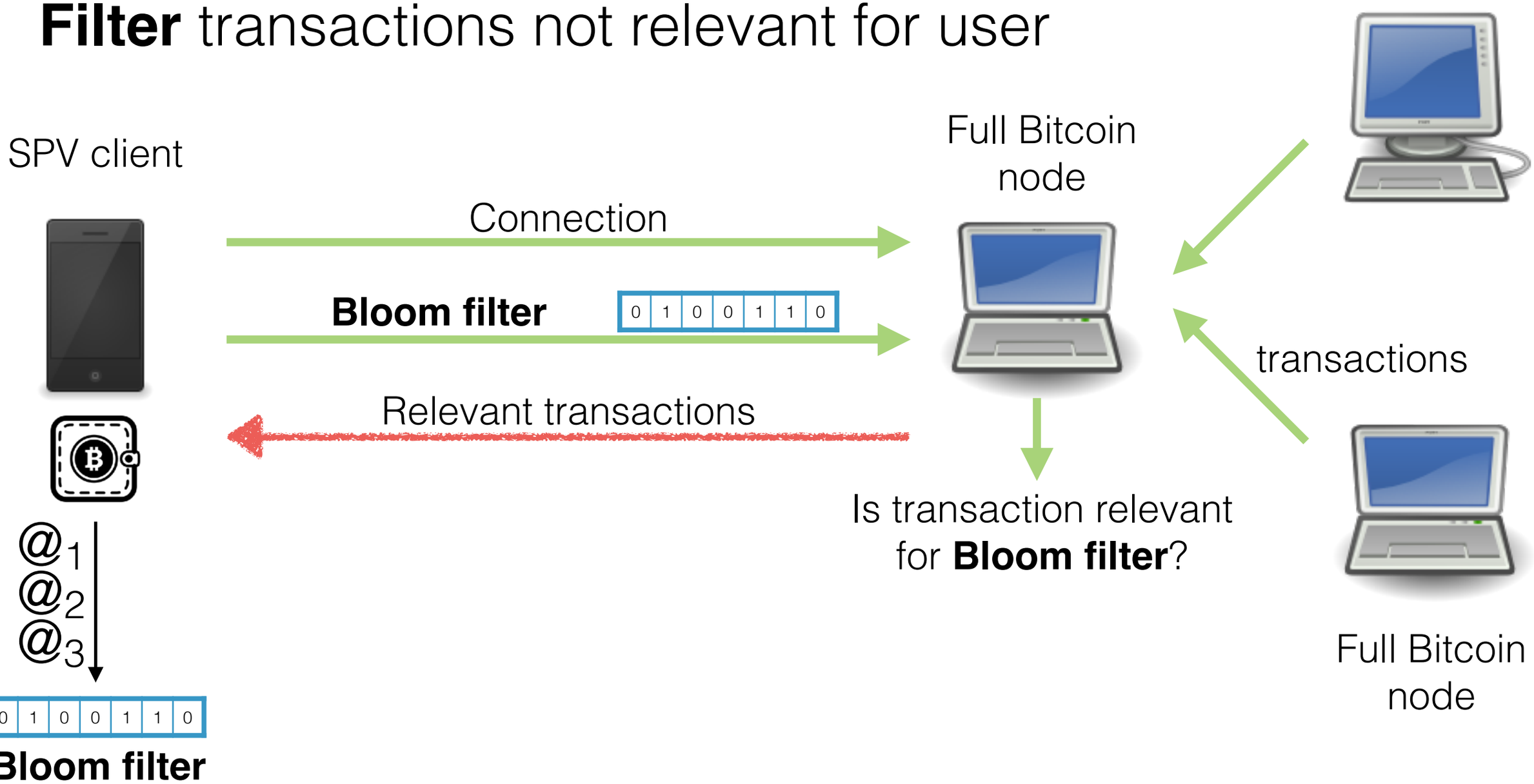
transactions

Full Bitcoin node

Is transaction relevant for **Bloom filter**?

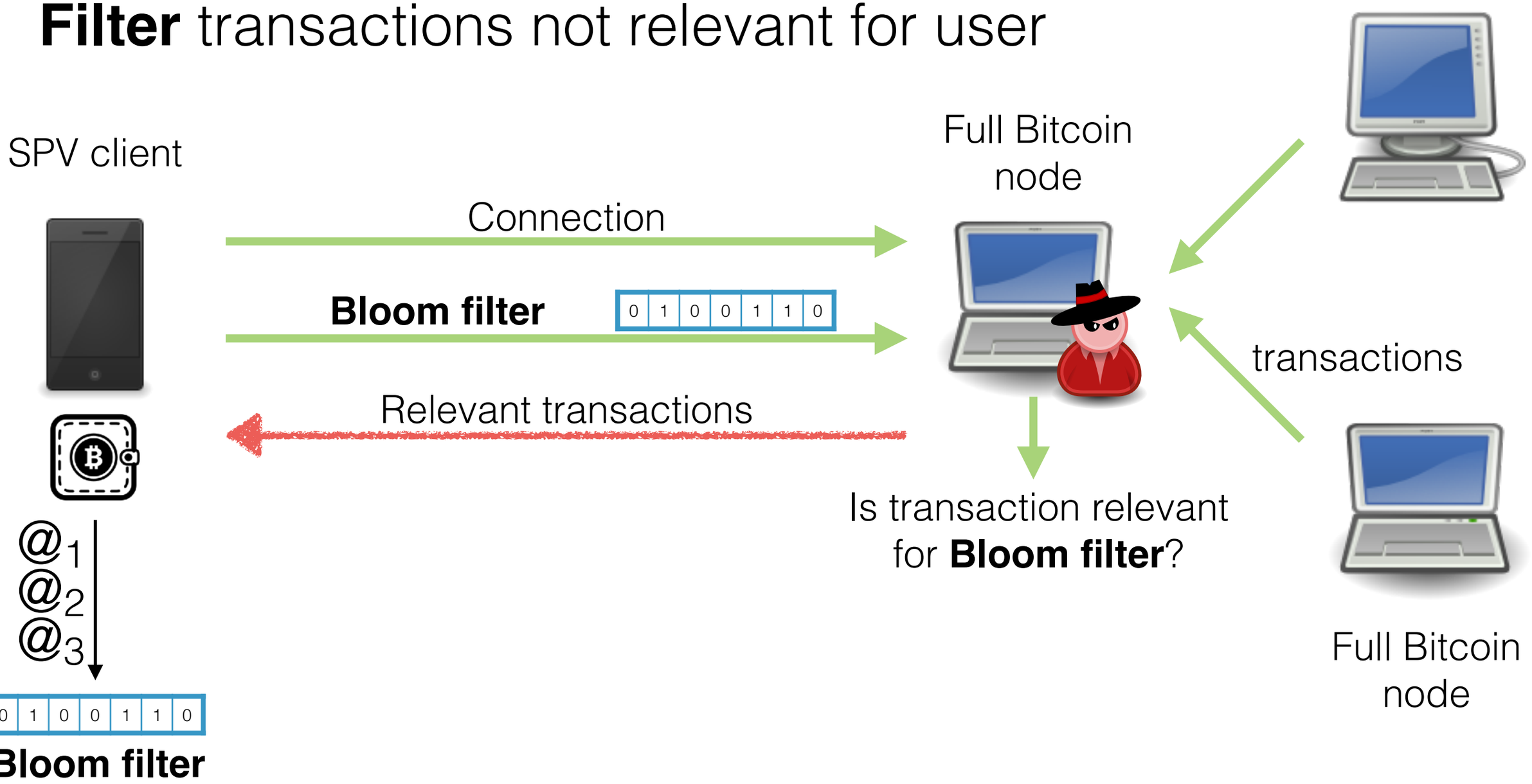
Simple Payment Verification (SPV)

Filter transactions not relevant for user



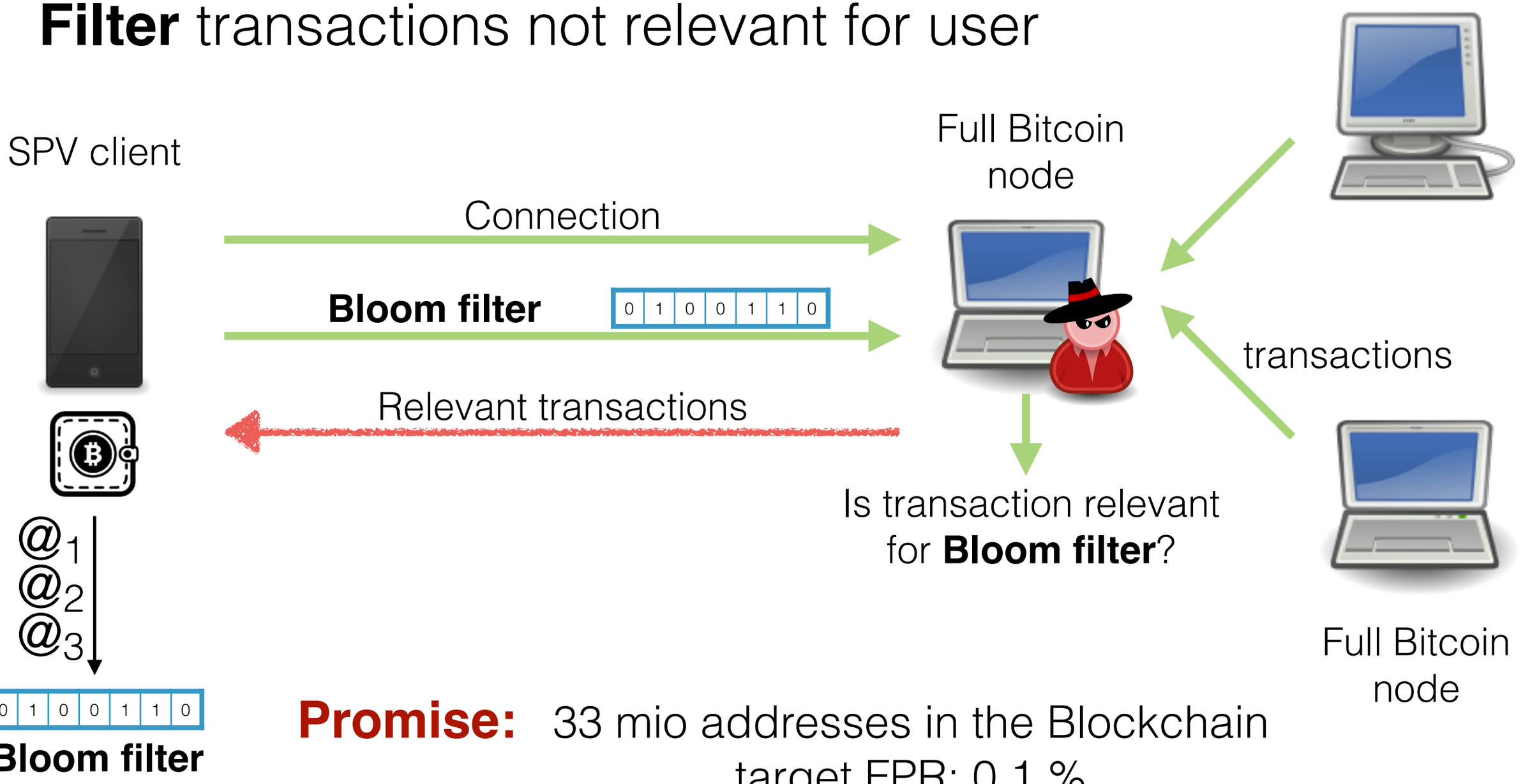
Simple Payment Verification (SPV)

Filter transactions not relevant for user



Simple Payment Verification (SPV)

Filter transactions not relevant for user



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

"User addresses hidden amongst 33 000" false positives

Model and Privacy measure

Blockchain

SPV client

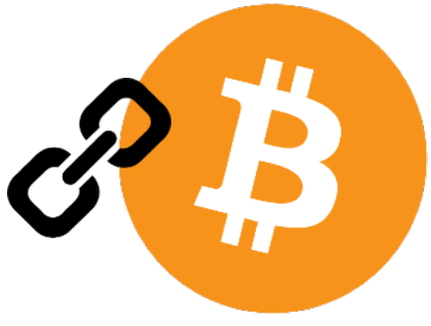
Model and Privacy measure

Blockchain

SPV client

Adversary

Model and Privacy measure



Blockchain

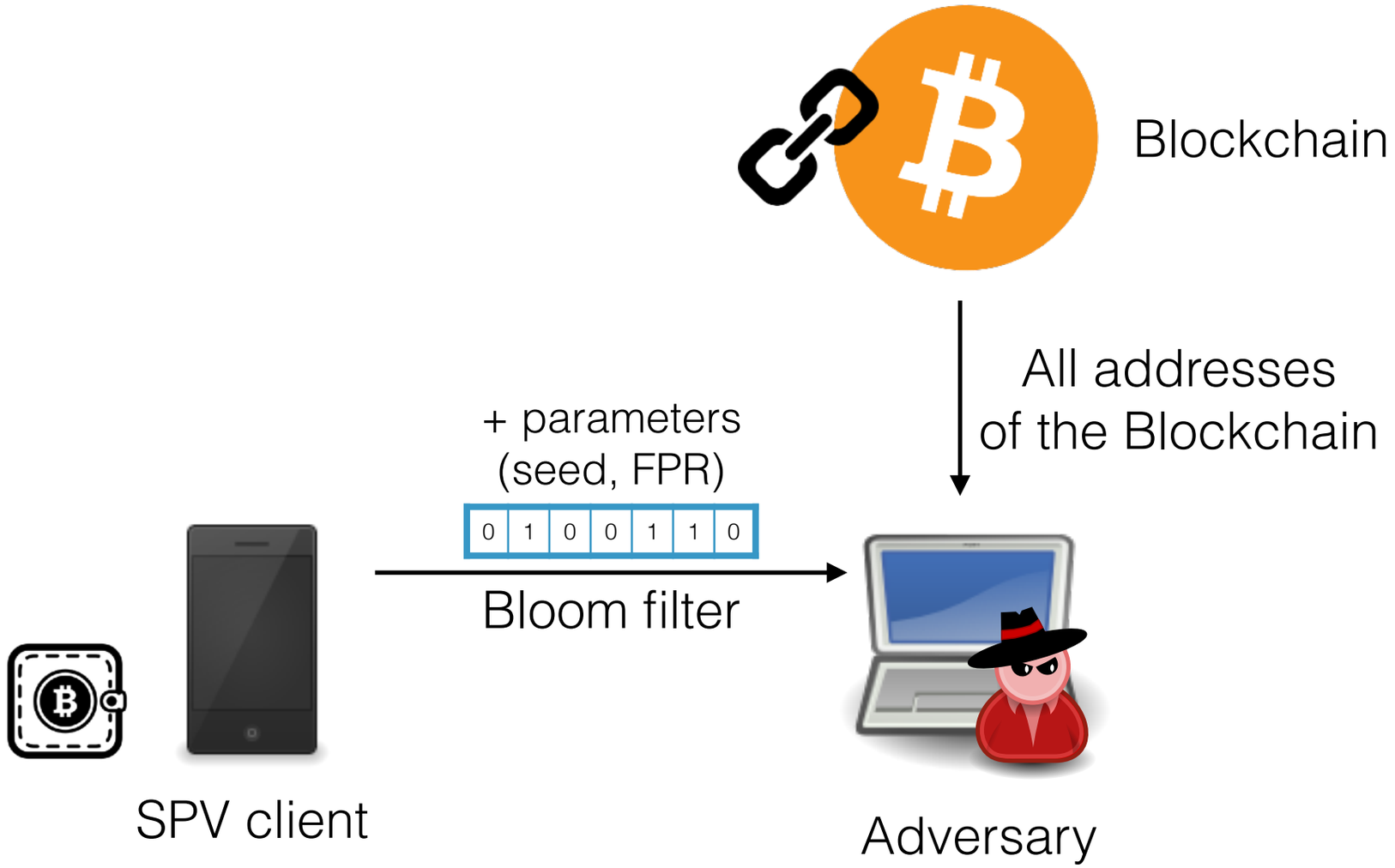
+ parameters
(seed, FPR)

SPV client

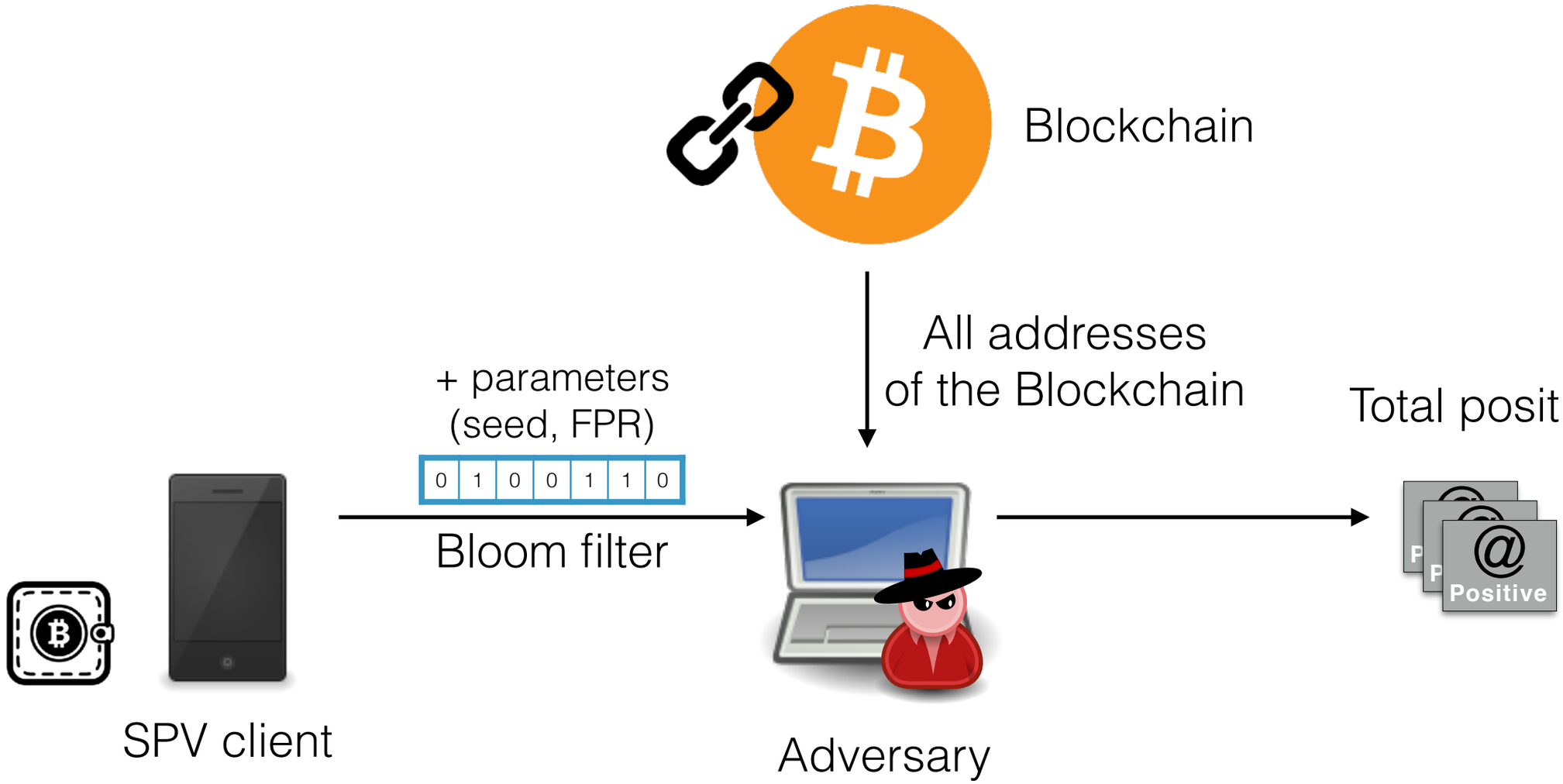
Bloom filter

Adversary

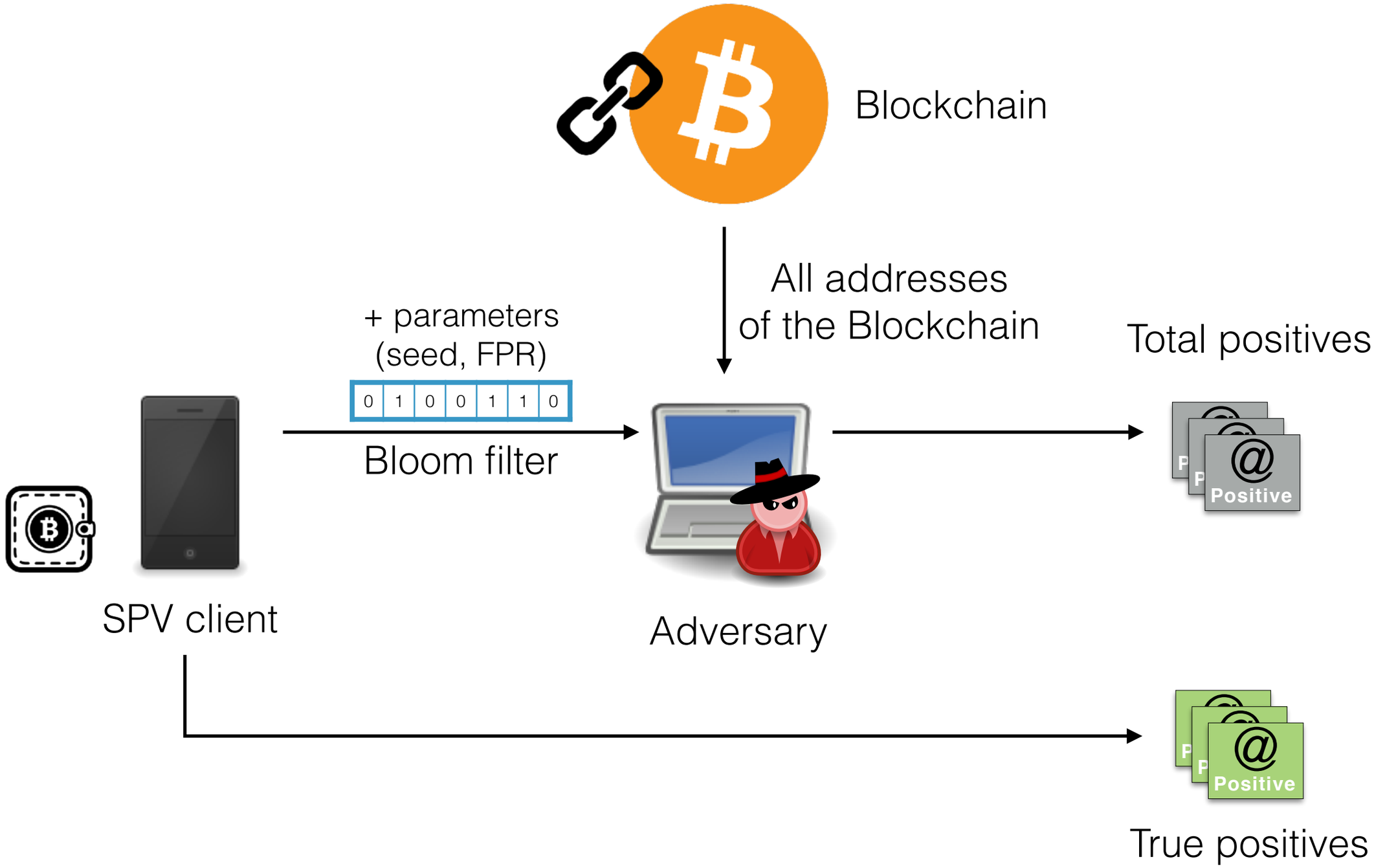
Model and Privacy measure



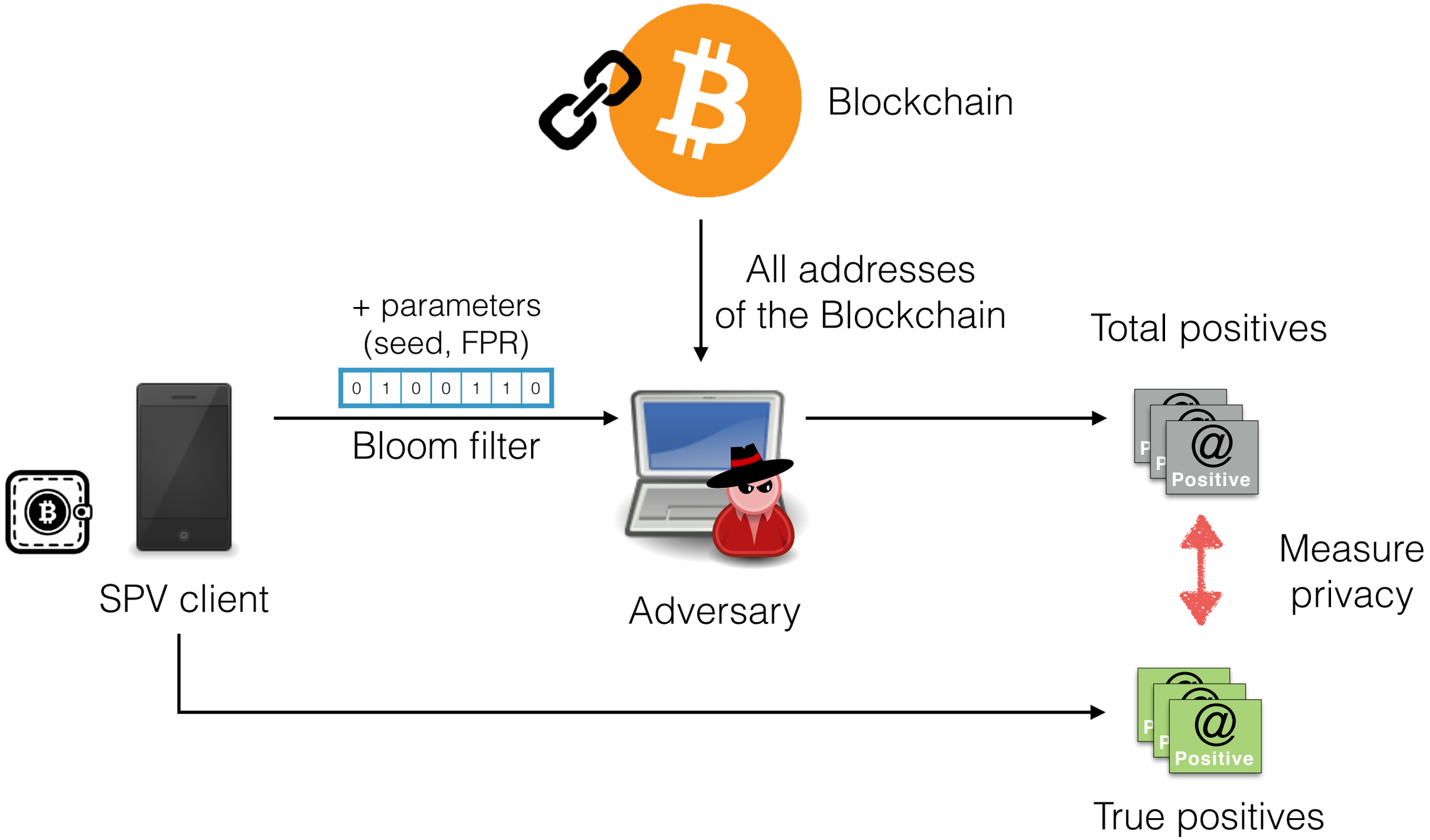
Model and Privacy measure



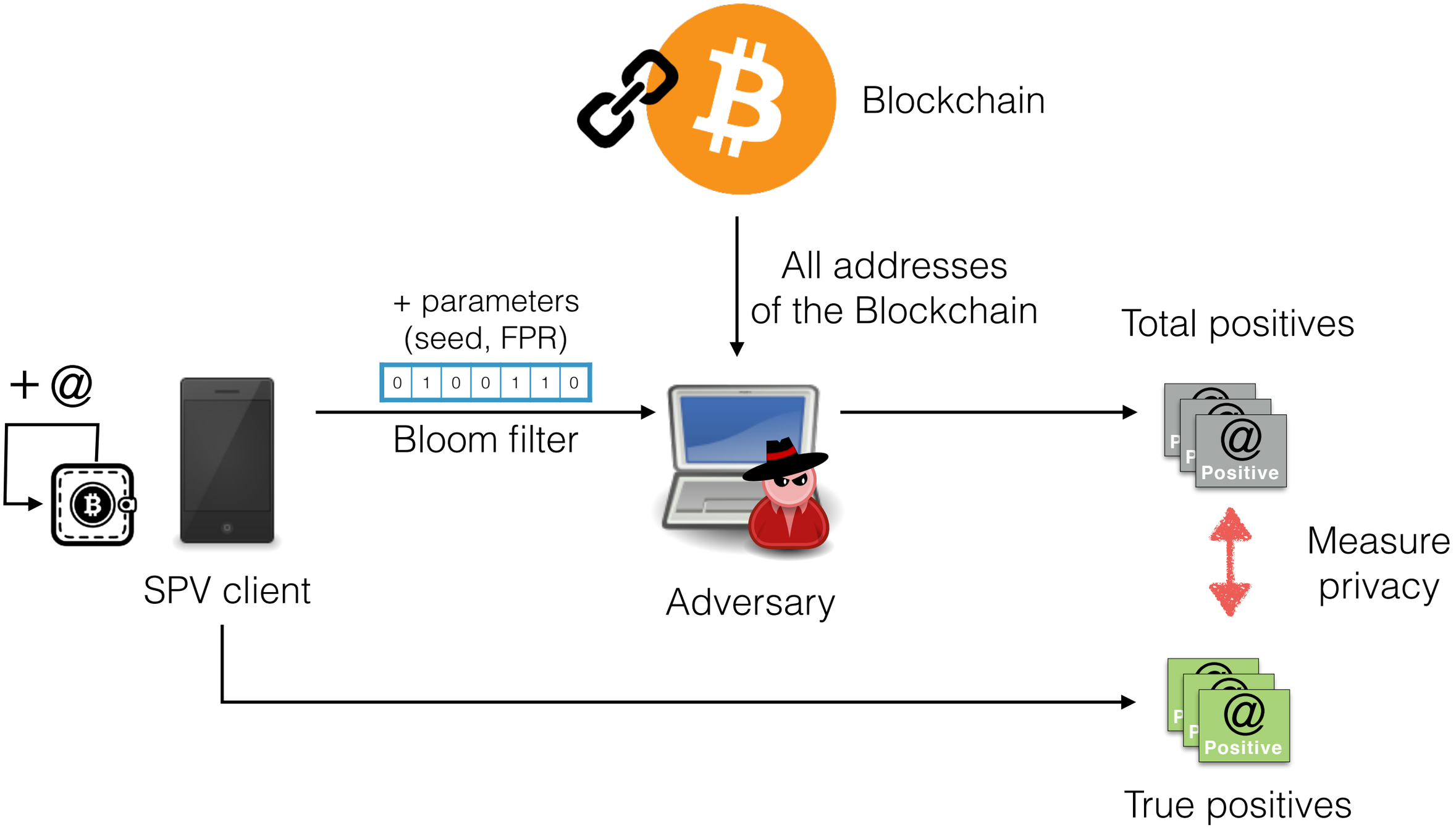
Model and Privacy measure



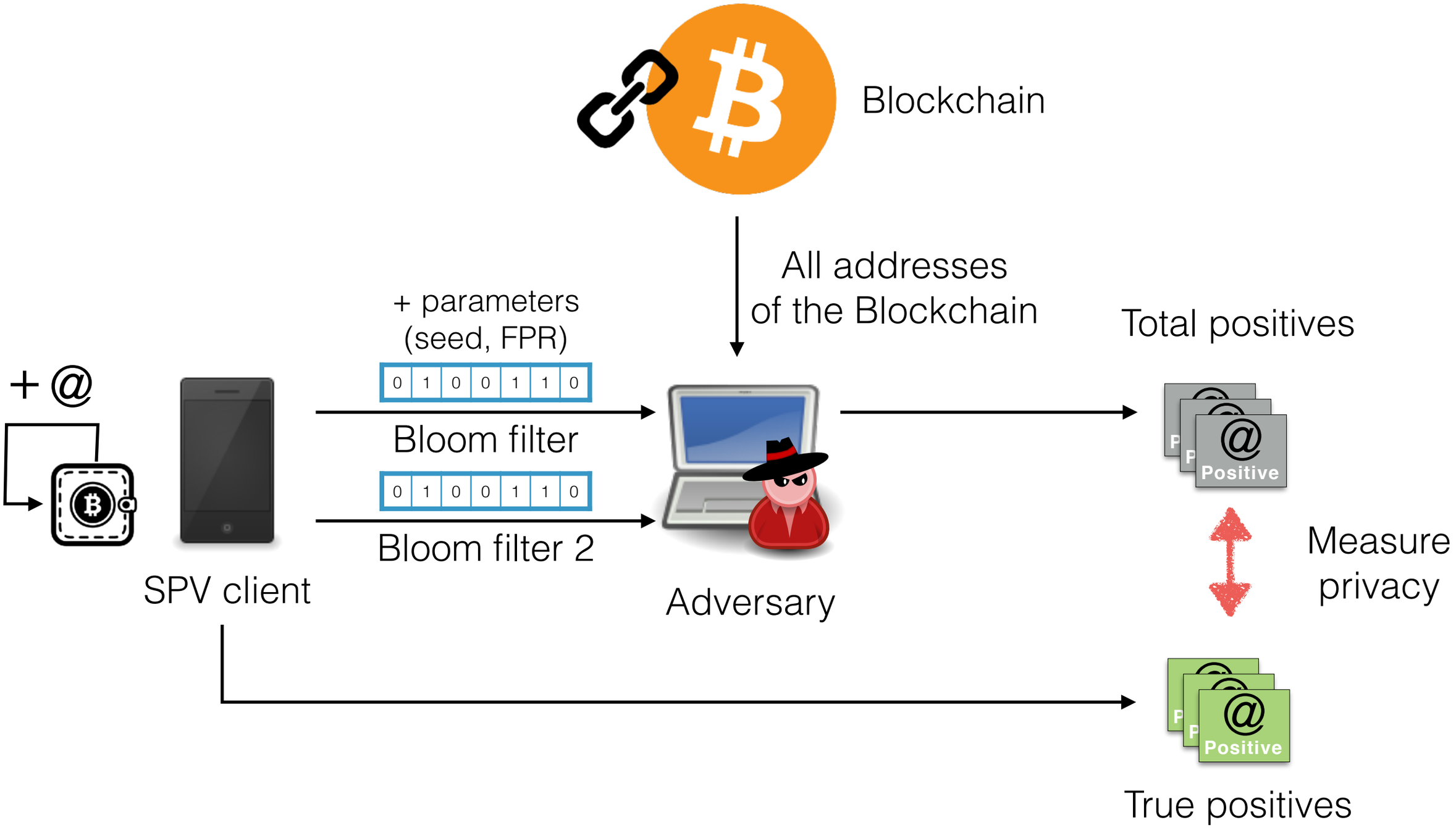
Model and Privacy measure



Model and Privacy measure

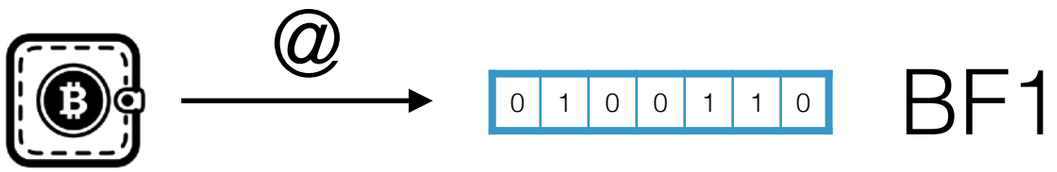


Model and Privacy measure



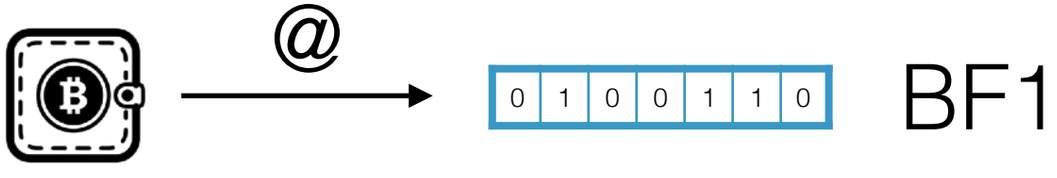
Stair stepping

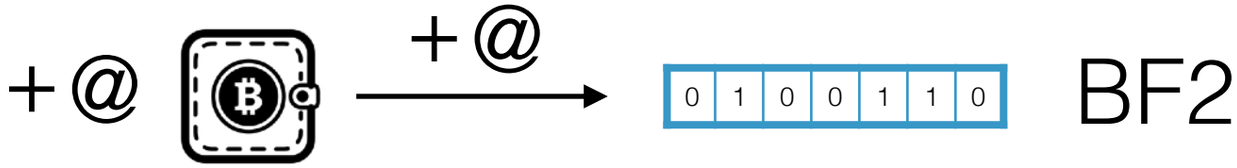
Bloom filter designed for
- max number of **addresses**
- **target FPR** when max addresses inserted



Stair stepping

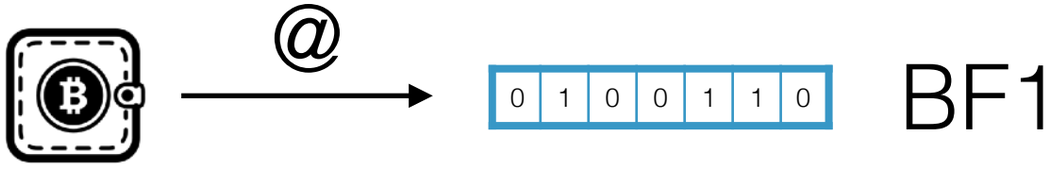
Bloom filter designed for
- max number of **addresses**
- **target FPR** when max addresses inserted

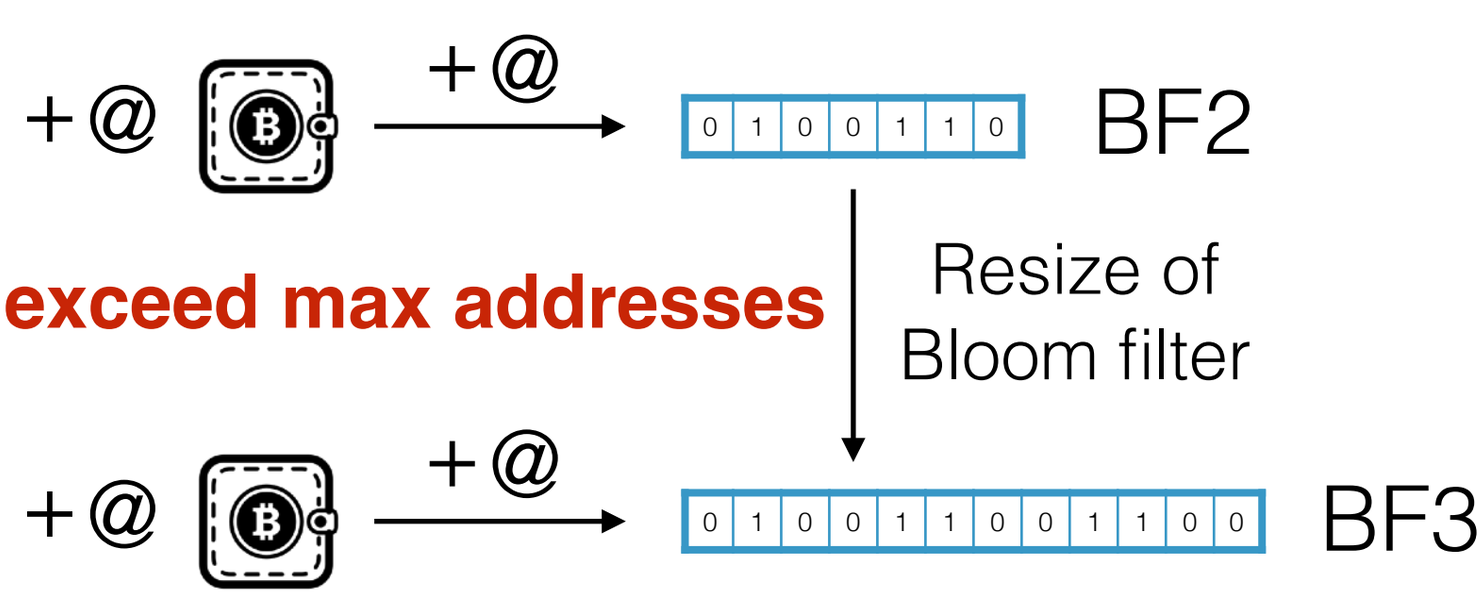




Stair stepping

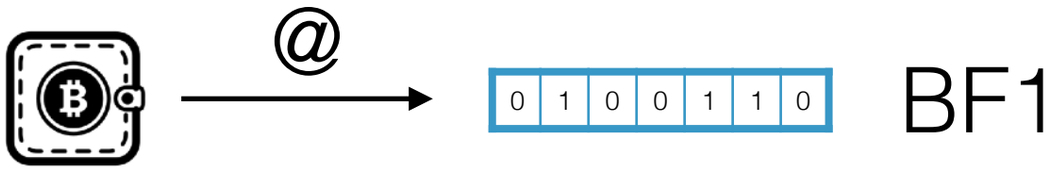
Bloom filter designed for
- max number of **addresses**
- **target FPR** when max addresses inserted

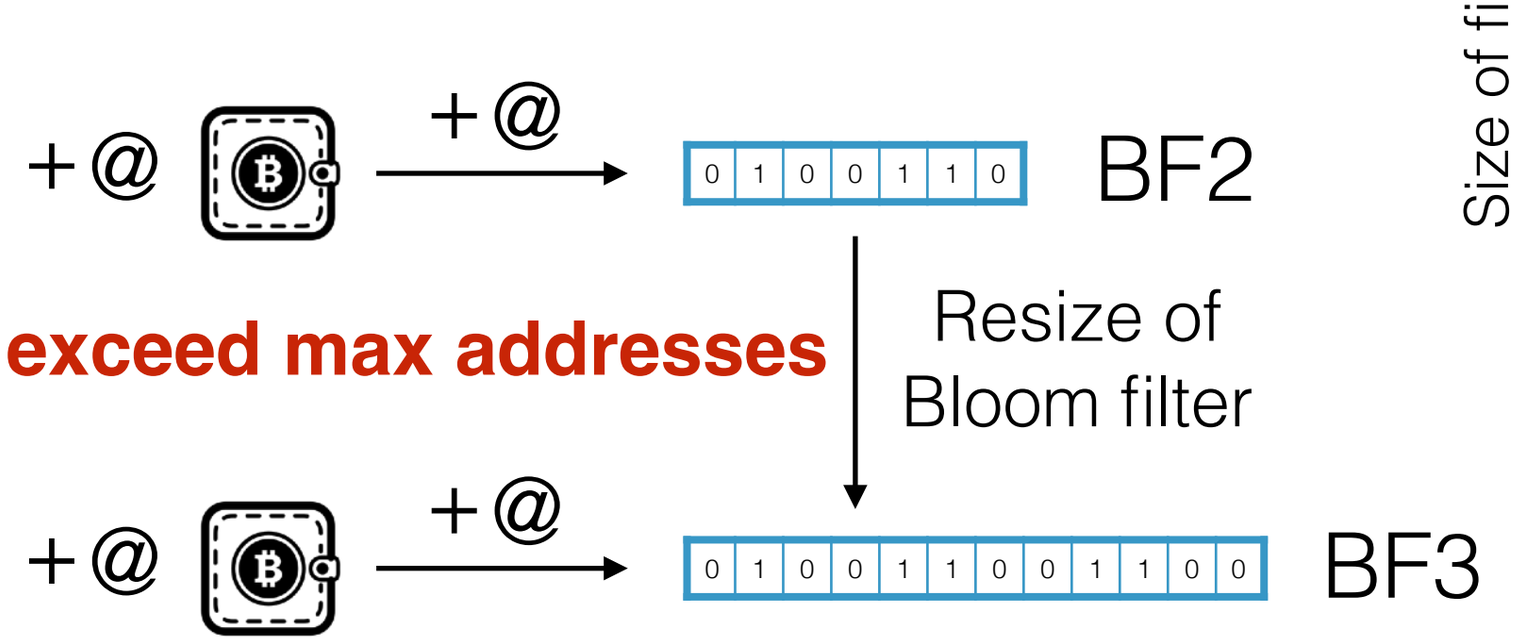


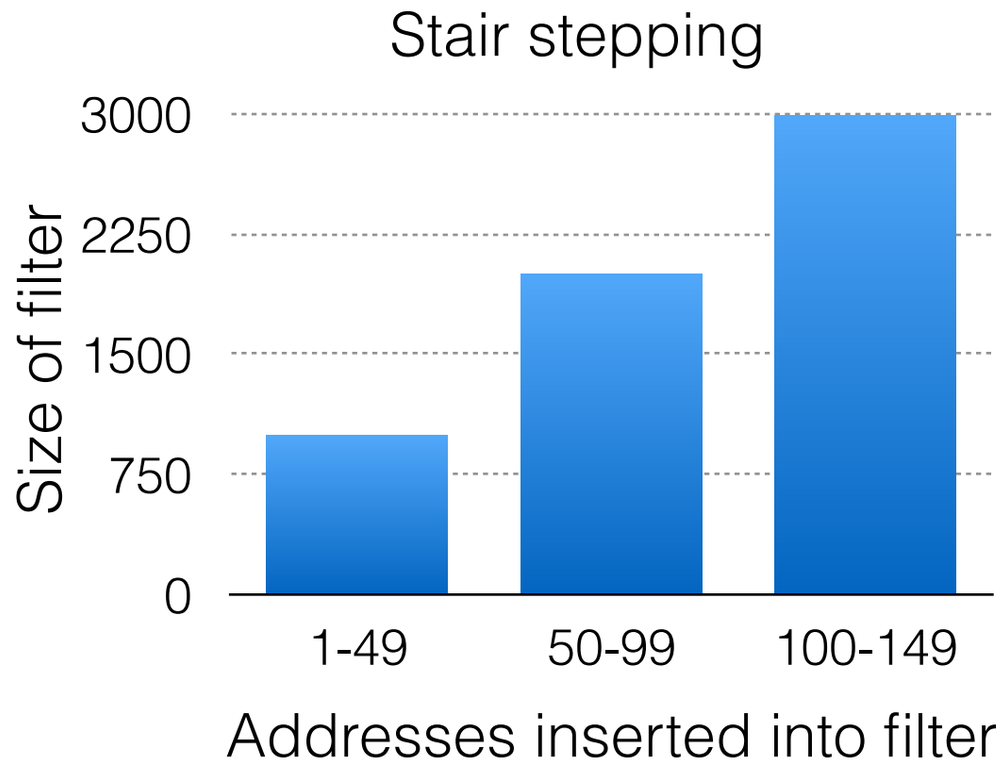


Stair stepping

Bloom filter designed for
- max number of **addresses**
- **target FPR** when max addresses inserted



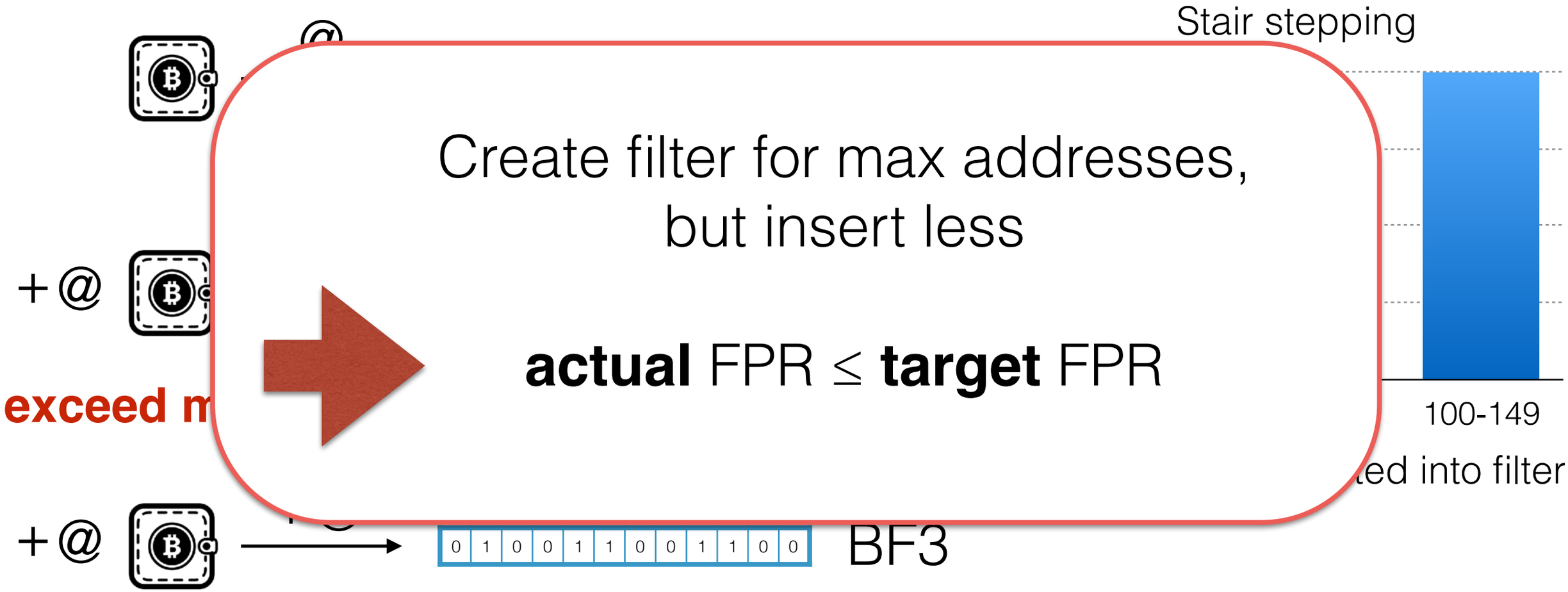




Rationale: **avoid** filters with different sizes

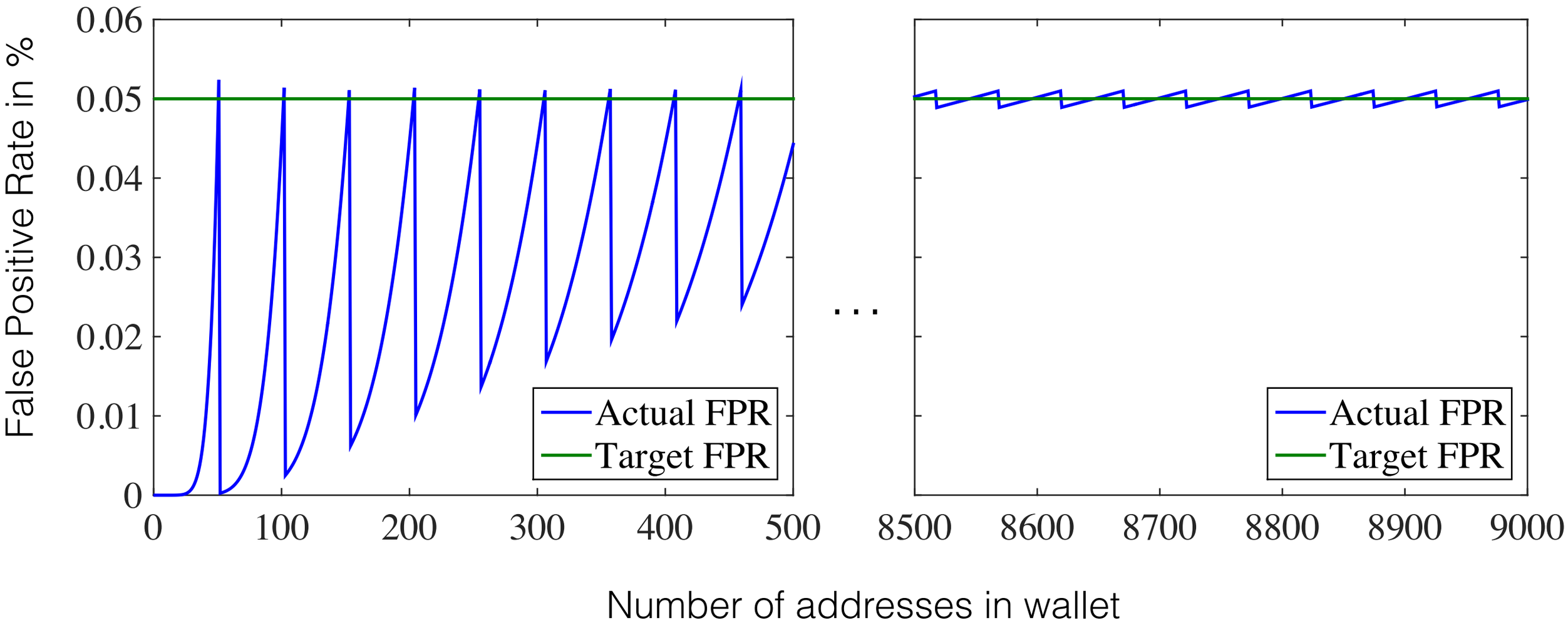
Stair stepping

Bloom filter designed for
- max number of **addresses**
- **target FPR** when max addresses inserted

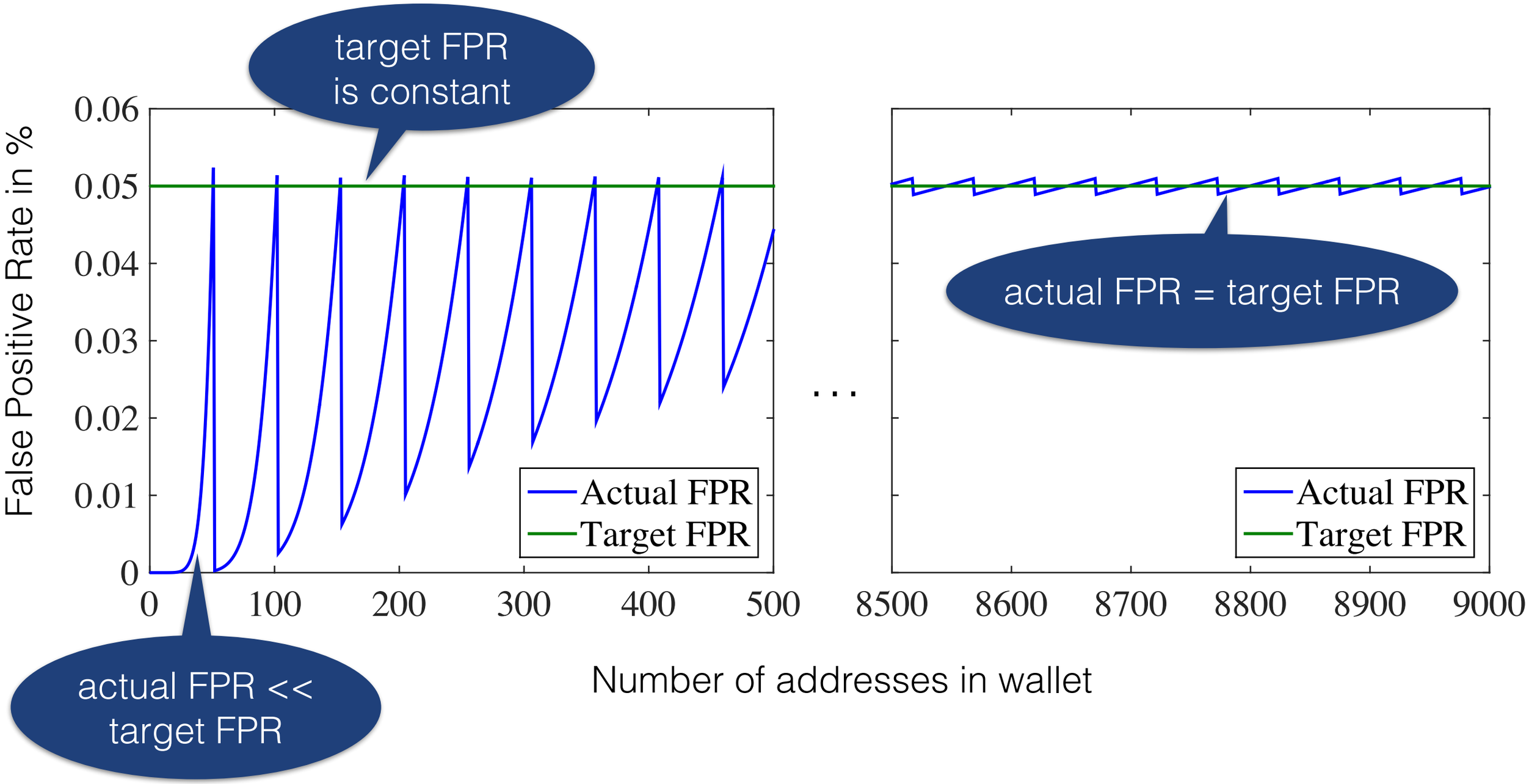


Rationale: **avoid** filters with different sizes

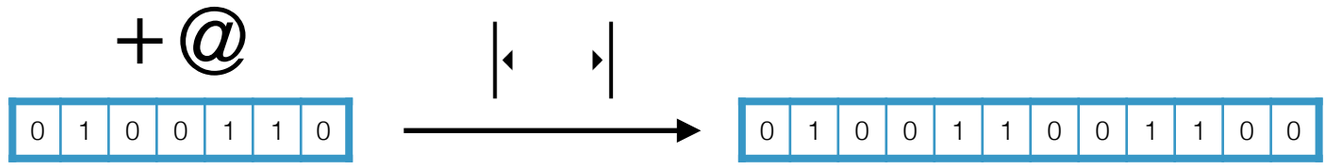
Analytical results - Actual FPR vs. Target FPR



Analytical results - Actual FPR vs. Target FPR



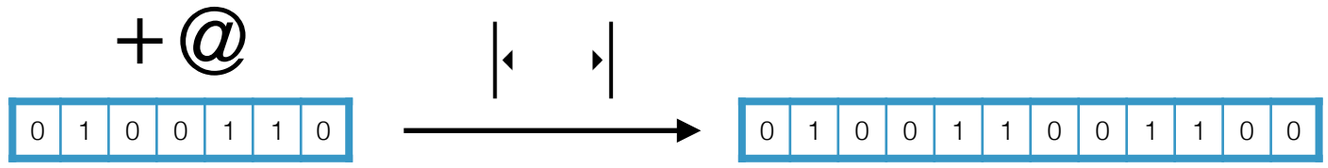
Resizing



Once max addresses inserted —> bigger filter

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

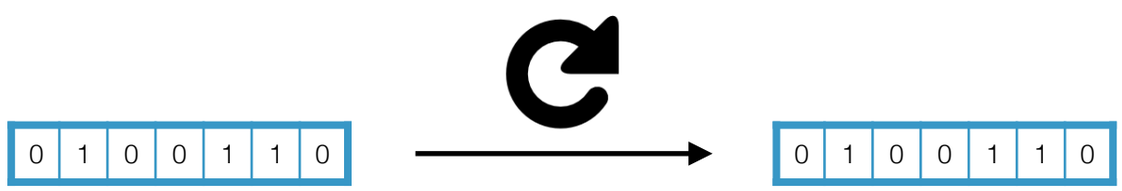
Resizing



Once max addresses inserted —> bigger filter

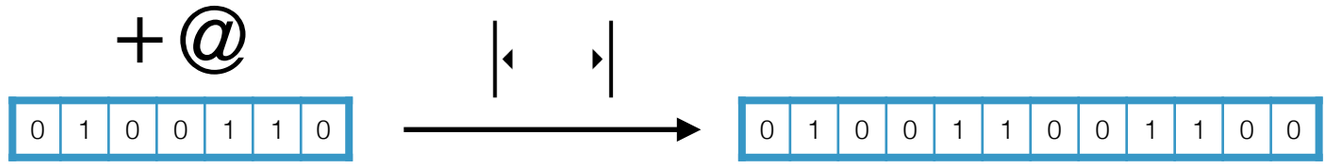
- Hash functions adapted to fill space of new filter
- **Consequence**: New filter yields **different** false positives

Restarting



- Fresh seed value for hash functions of Bloom filter
- **Consequence**: New filter yields **different** false positives

Resizing



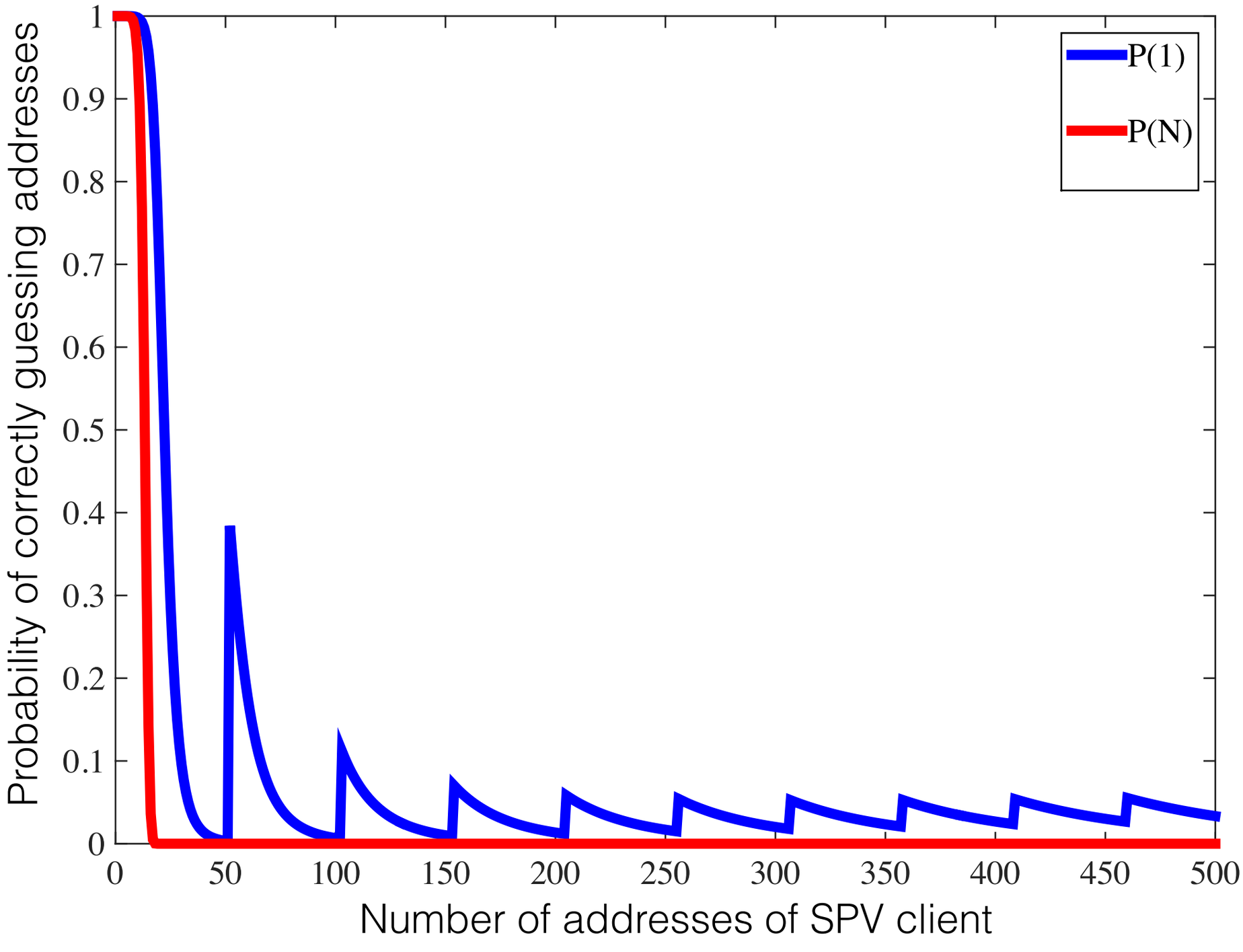
Once max addresses inserted —> bigger filter

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

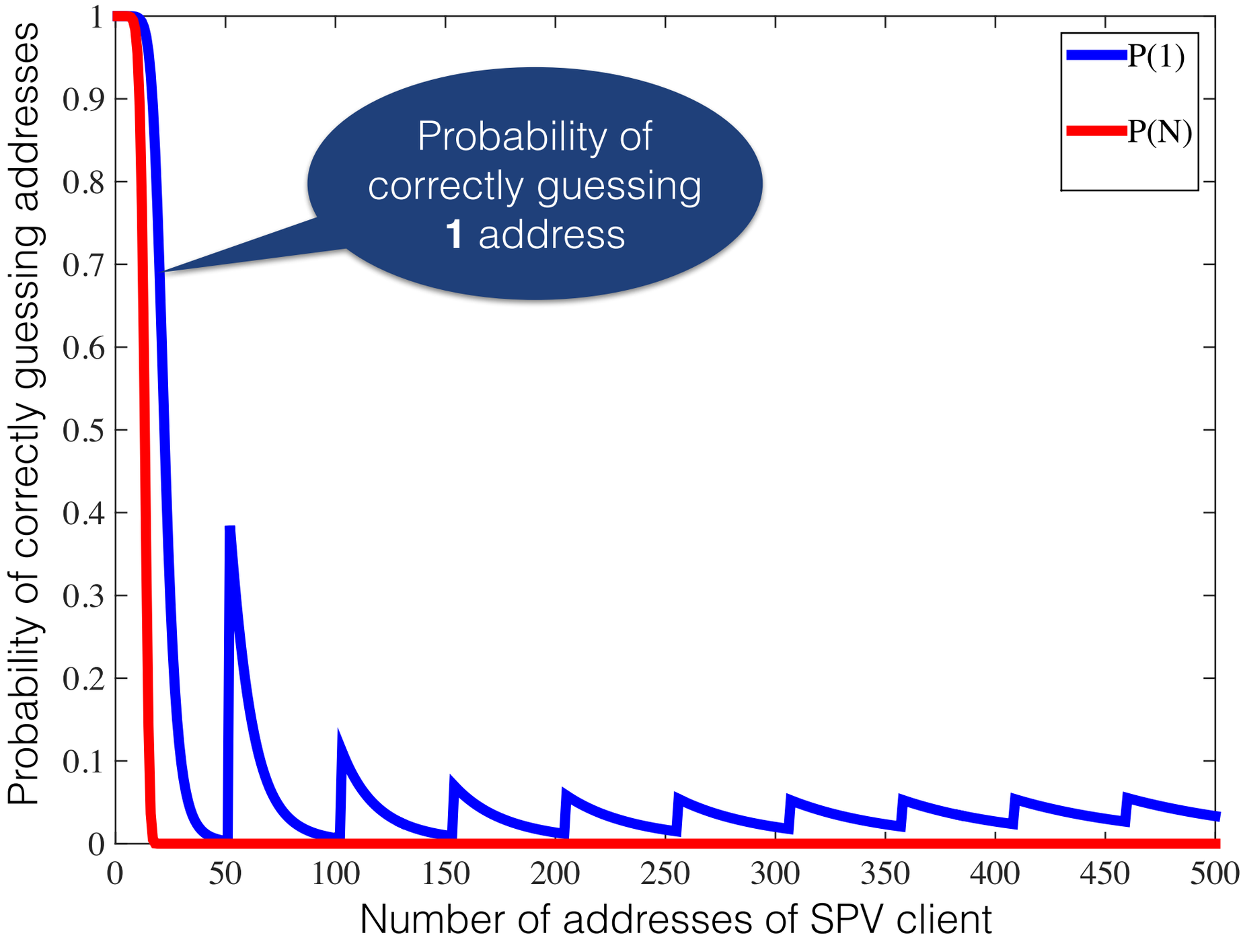
Summary of current SPV design choices

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

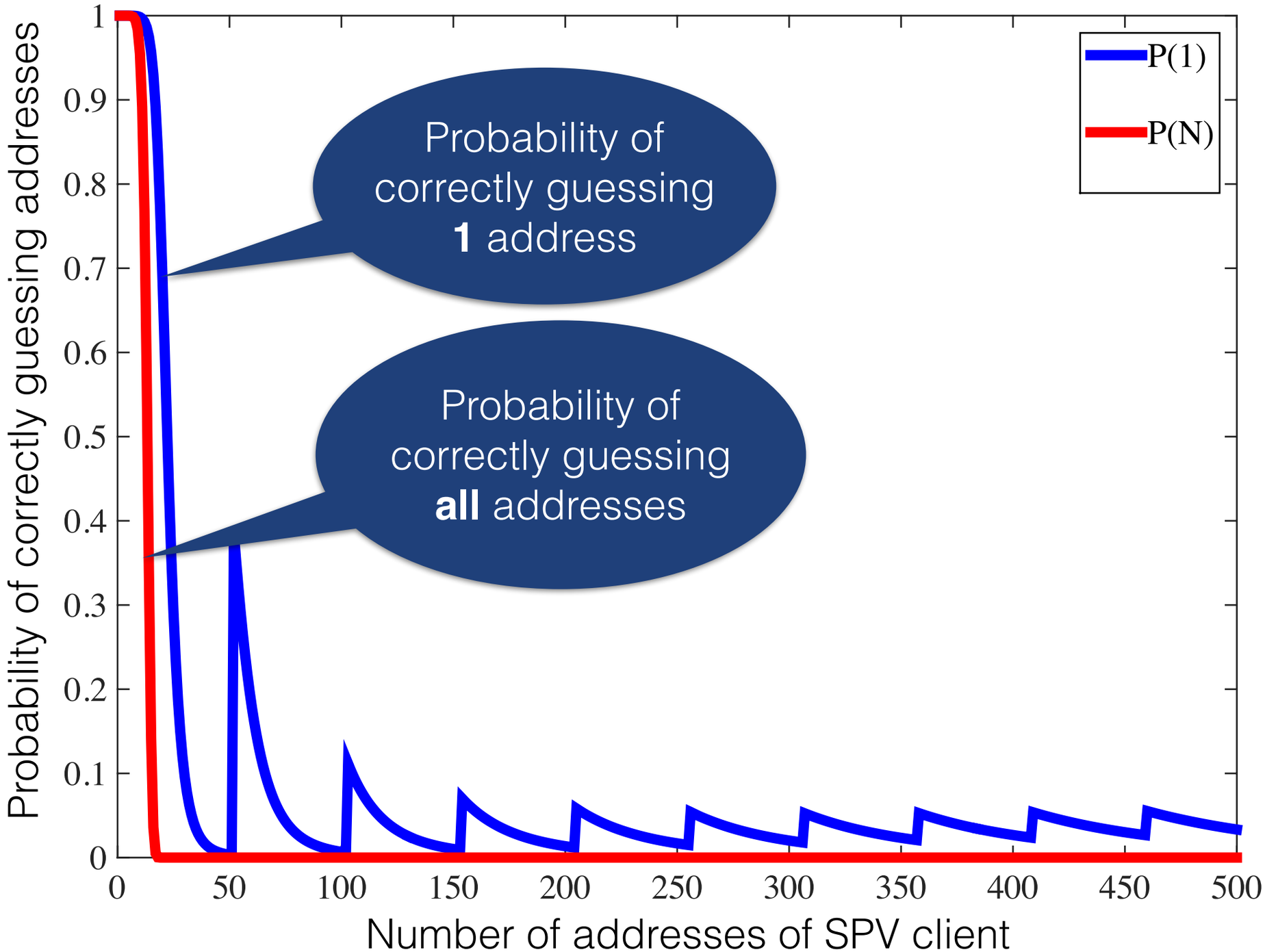
One Bloom filter



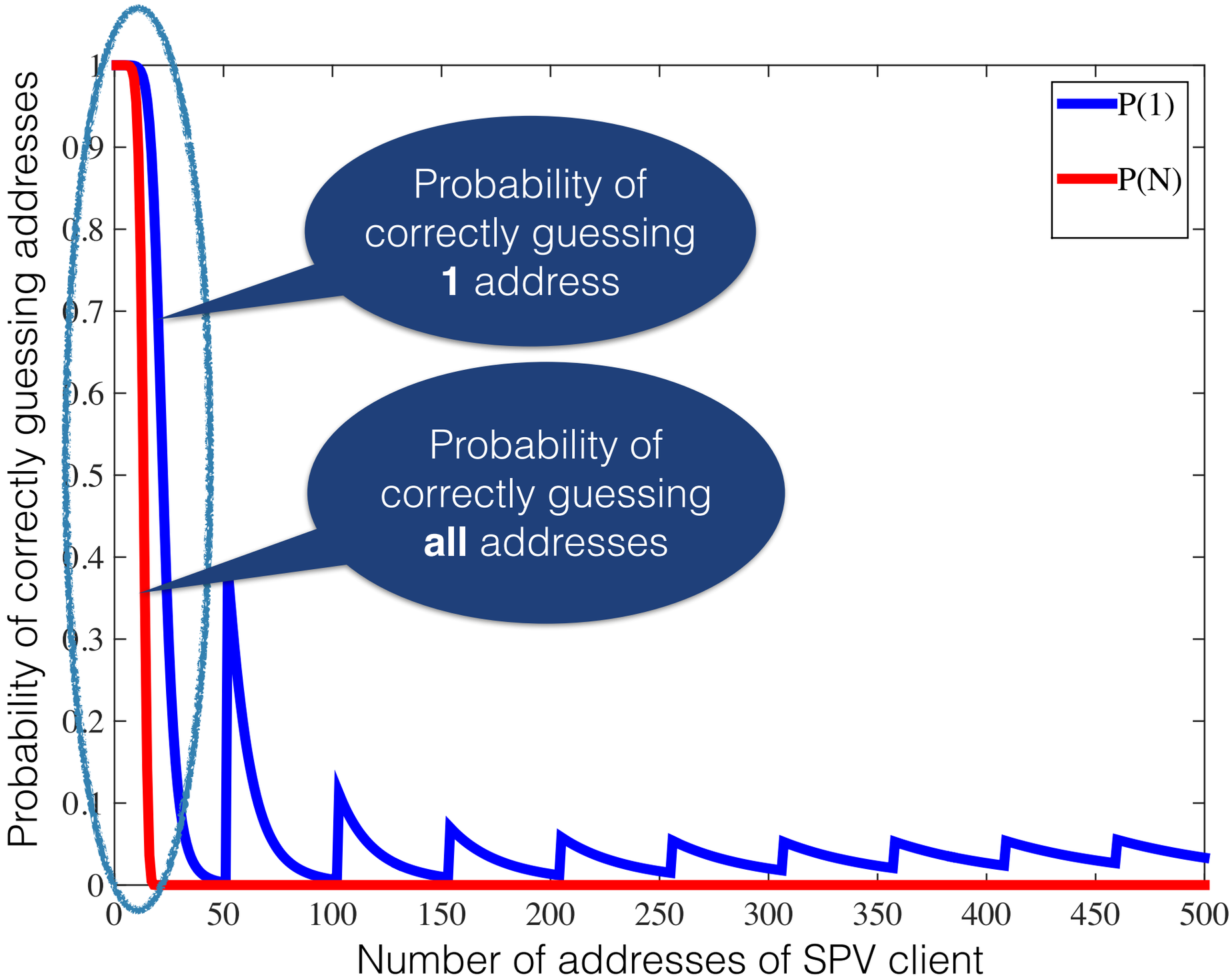
One Bloom filter



One Bloom filter

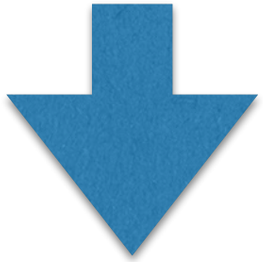


One Bloom filter



Multiple Bloom filters

Filter 1



$@_1$ $@_2$ $@_3$

Multiple Bloom filters

Filter 1

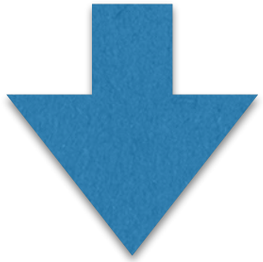
$@_1$ $@_2$ $@_3$

Filter 2

$@_1$ $@_4$ $@_5$

Multiple Bloom filters

Filter 1



$@_1$ $@_2$ $@_3$

Filter 2

$@_1$ $@_4$ $@_5$

. . .

Filter n

$@_1$ $@_6$ $@_7$

Multiple Bloom filters

Filter 1

Filter 2

. . .

Filter n

$@_1$ $@_2$ $@_3$

$@_1$ $@_4$ $@_5$

$@_1$ $@_6$ $@_7$

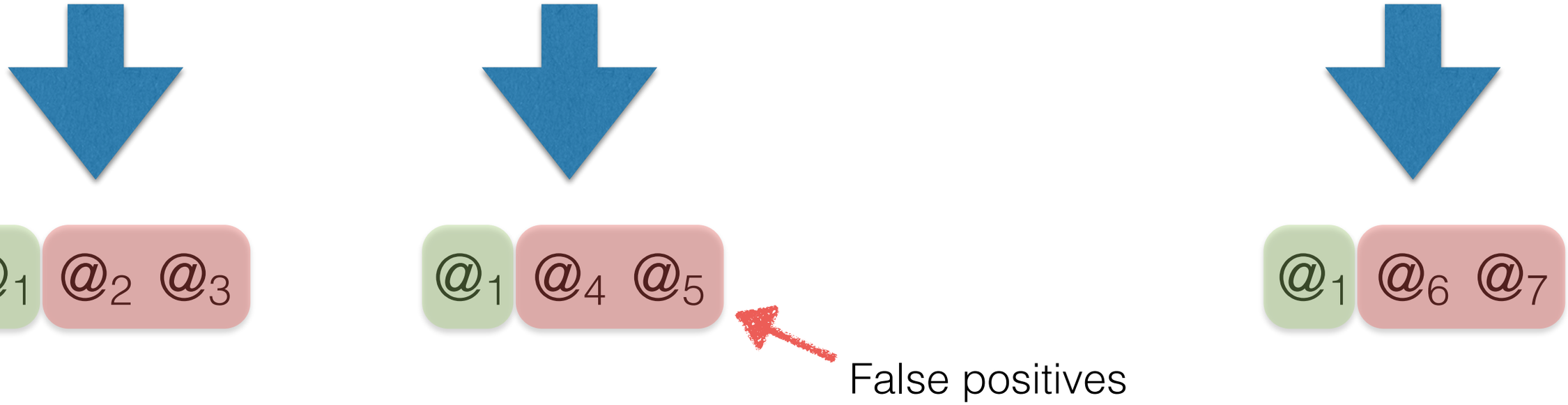
Multiple Bloom filters

Filter 1

Filter 2

. . .

Filter n



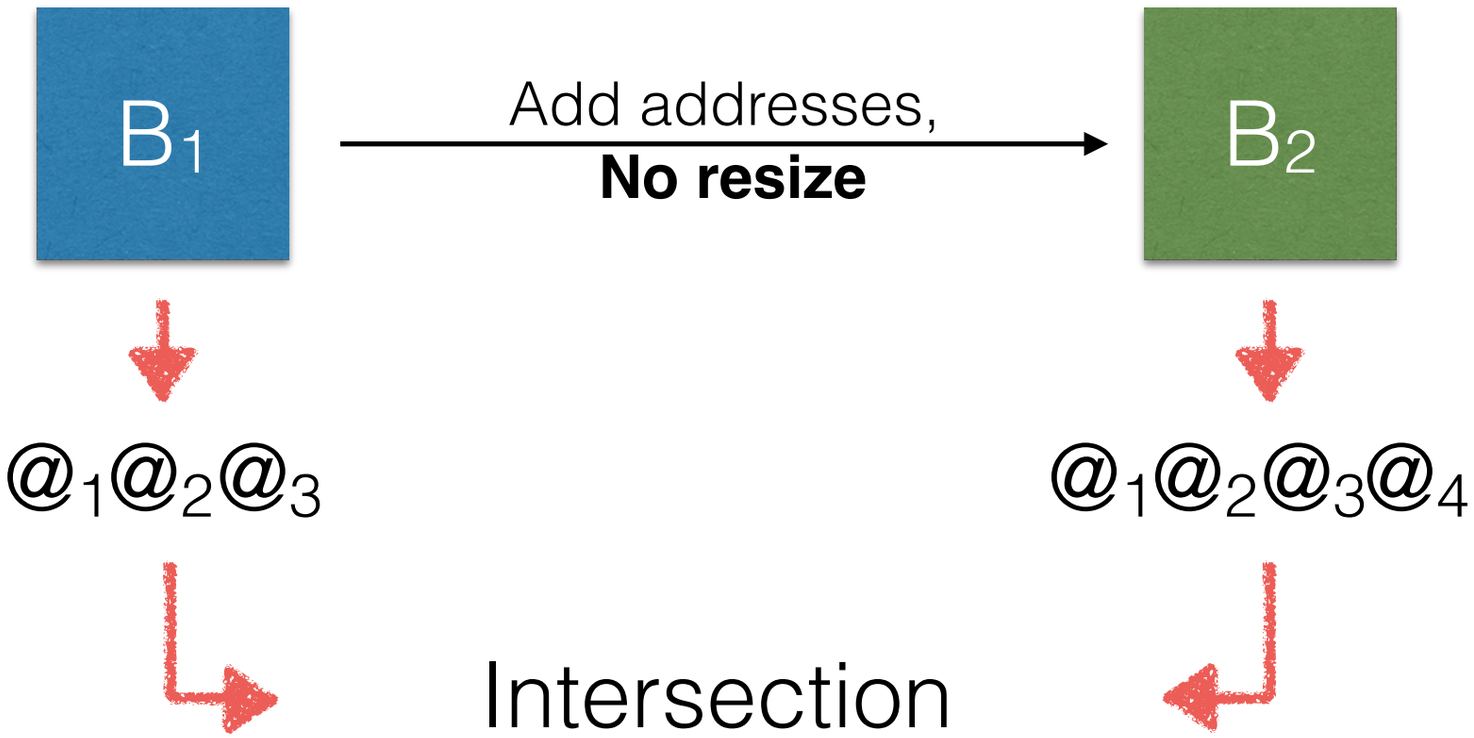
Experiment 1 - No resize

Exp.	Client	Seed	Size
No resize	**Same**	**Same**	**Same**
Resize	Same	Same	Different
Restart	Same	Different	Same
> 2 filter	Same	Different	Different

Experiment 1 - No resize

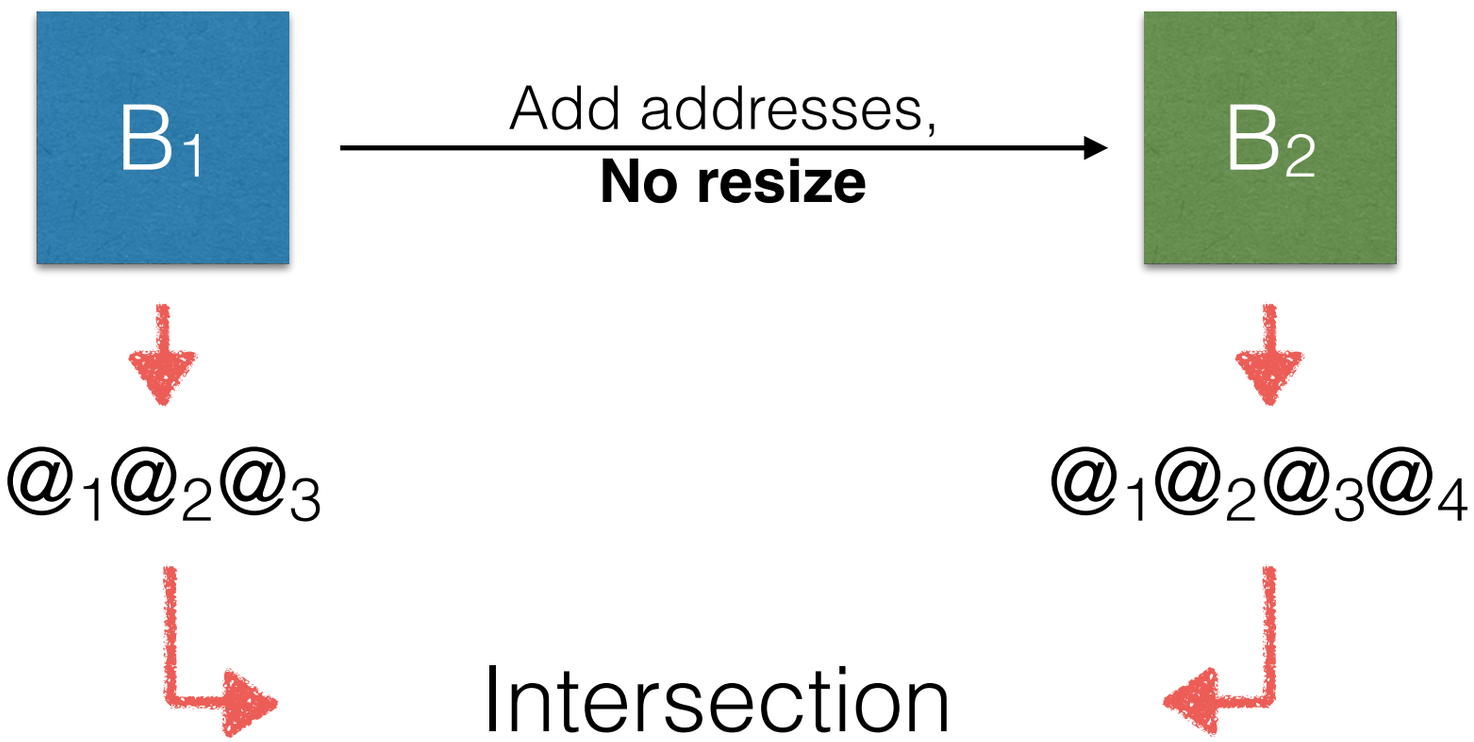
Exp.	Client	Seed	Size
No resize	**Same**	**Same**	**Same**
Resize	Same	Same	Different
Restart	Same	Different	Same
> 2 filter	Same	Different	Different

Experiment 1 - No resize



Exp.	Client	Seed	Size
No resize	**Same**	**Same**	**Same**
Resize	Same	Same	Different
Restart	Same	Different	Same
> 2 filter	Same	Different	Different

Experiment 1 - No resize

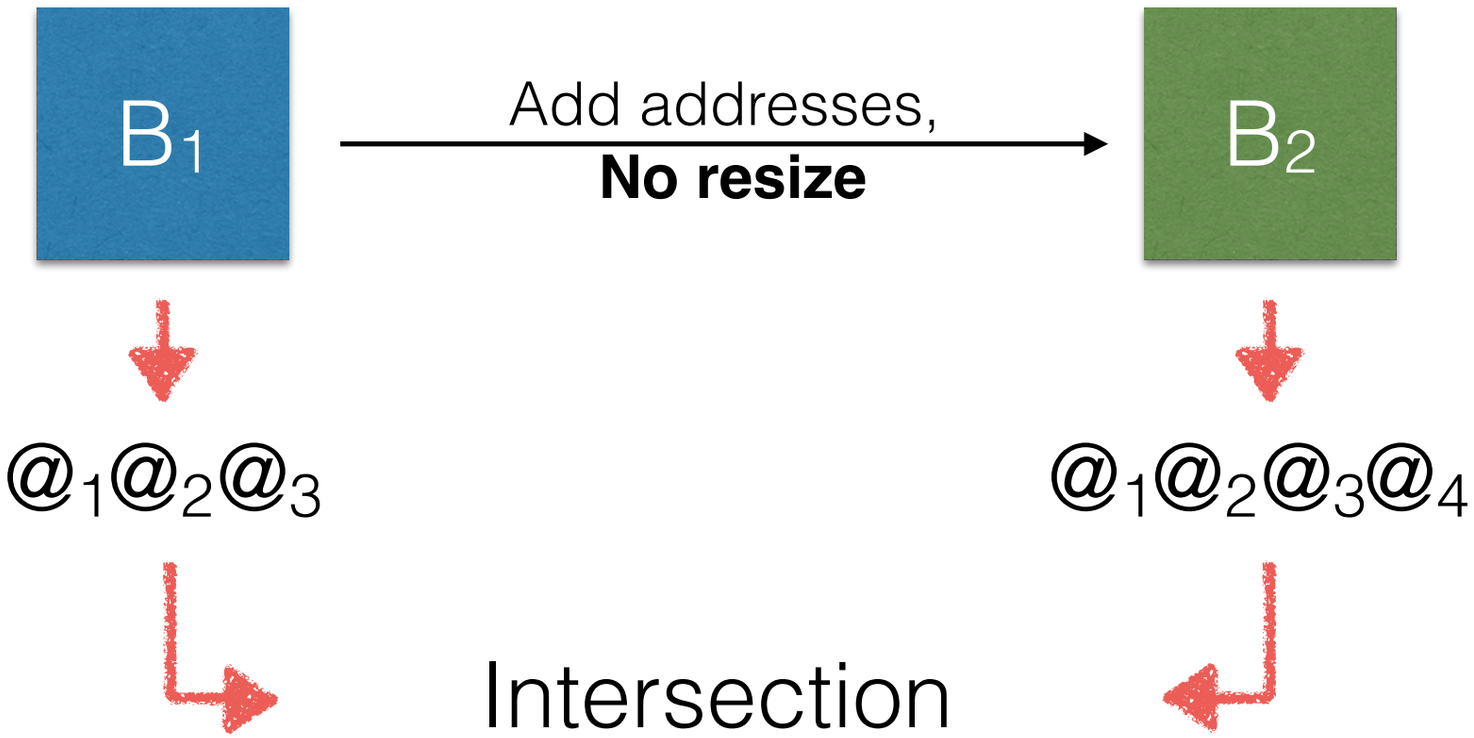


Exp.	Client	Seed	Size
No resize	**Same**	**Same**	**Same**
Resize	Same	Same	Different
Restart	Same	Different	Same
> 2 filter	Same	Different	Different

Results

Target FPR (%)	P(1) with 2 BF	P(1) with 1 BF
0.05	0.2990	0.2910
0.1	0.1020	0.1070
0.5	0.0078	0.0075

Experiment 1 - No resize

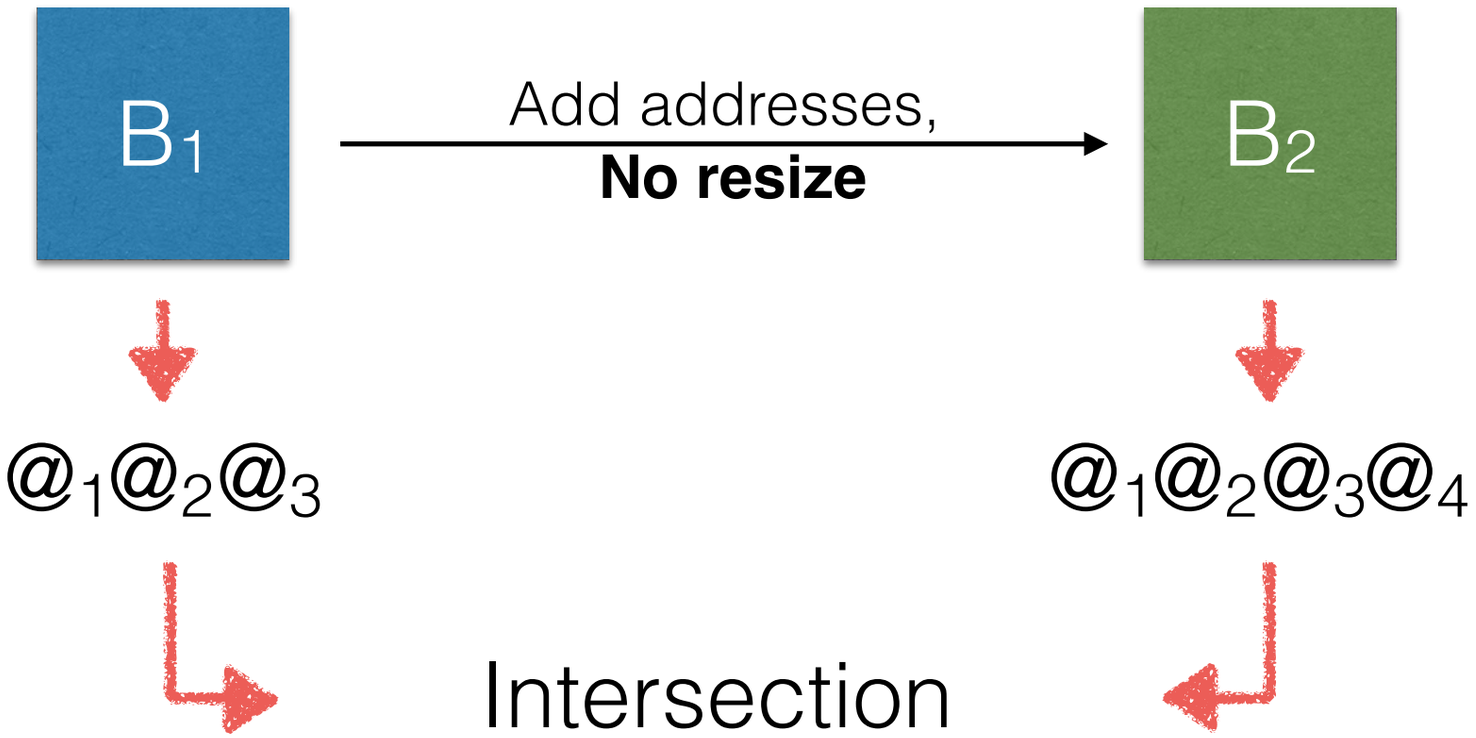


Exp.	Client	Seed	Size
No resize	**Same**	**Same**	**Same**
Resize	Same	Same	Different
Restart	Same	Different	Same
> 2 filter	Same	Different	Different

Results

Target FPR (%)	P(1) with 2 BF	P(1) with 1 BF
0.05	0.2990	0.2910
0.1	0.1020	0.1070
0.5	0.0078	0.0075

Experiment 1 - No resize

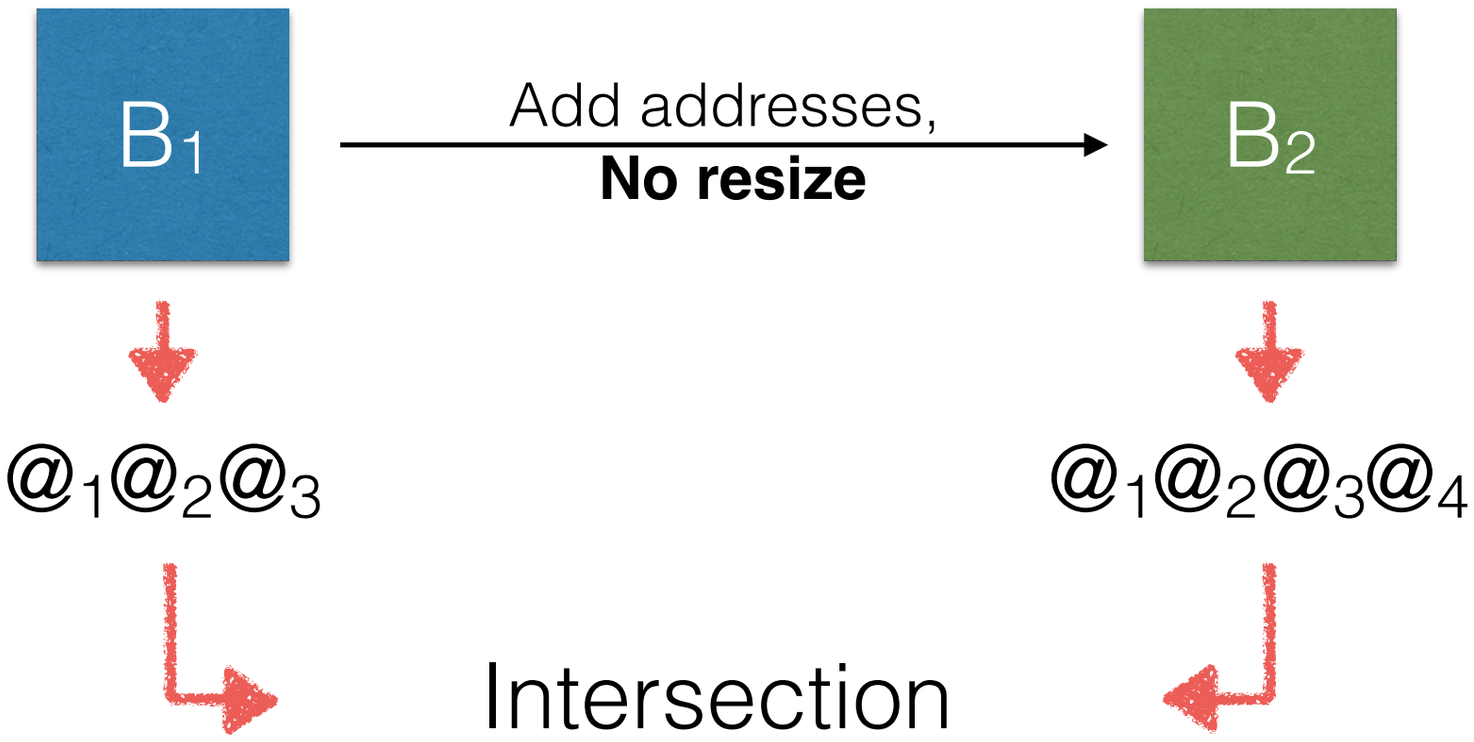


Exp.	Client	Seed	Size
No resize	**Same**	**Same**	**Same**
Resize	Same	Same	Different
Restart	Same	Different	Same
> 2 filter	Same	Different	Different

Results

Target FPR (%)	P(1) with 2 BF	P(1) with 1 BF
0.05	0.2990	0.2910
0.1	0.1020	0.1070
0.5	0.0078	0.0075

Experiment 1 - No resize



Intersection

Exp.	Client	Seed	Size
No resize	**Same**	**Same**	**Same**
Resize	Same	Same	Different
Restart	Same	Different	Same
> 2 filter	Same	Different	Different

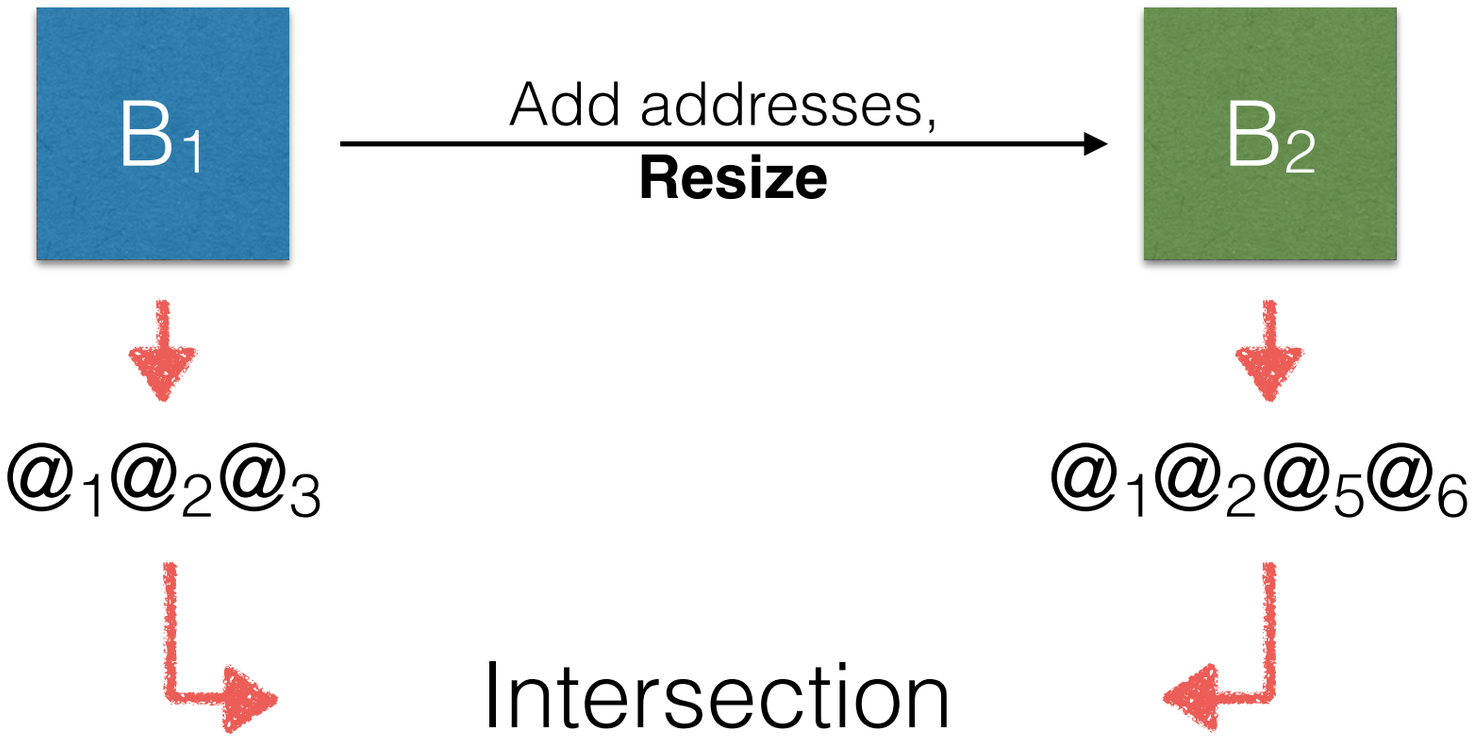
Results

Target FPR (%)	P(1) with 2 BF	P(1) with 1 BF
0.05	0.2990	0.2910
0.1	0.1020	0.1070
0.5	0.0078	0.0075

no change of privacy

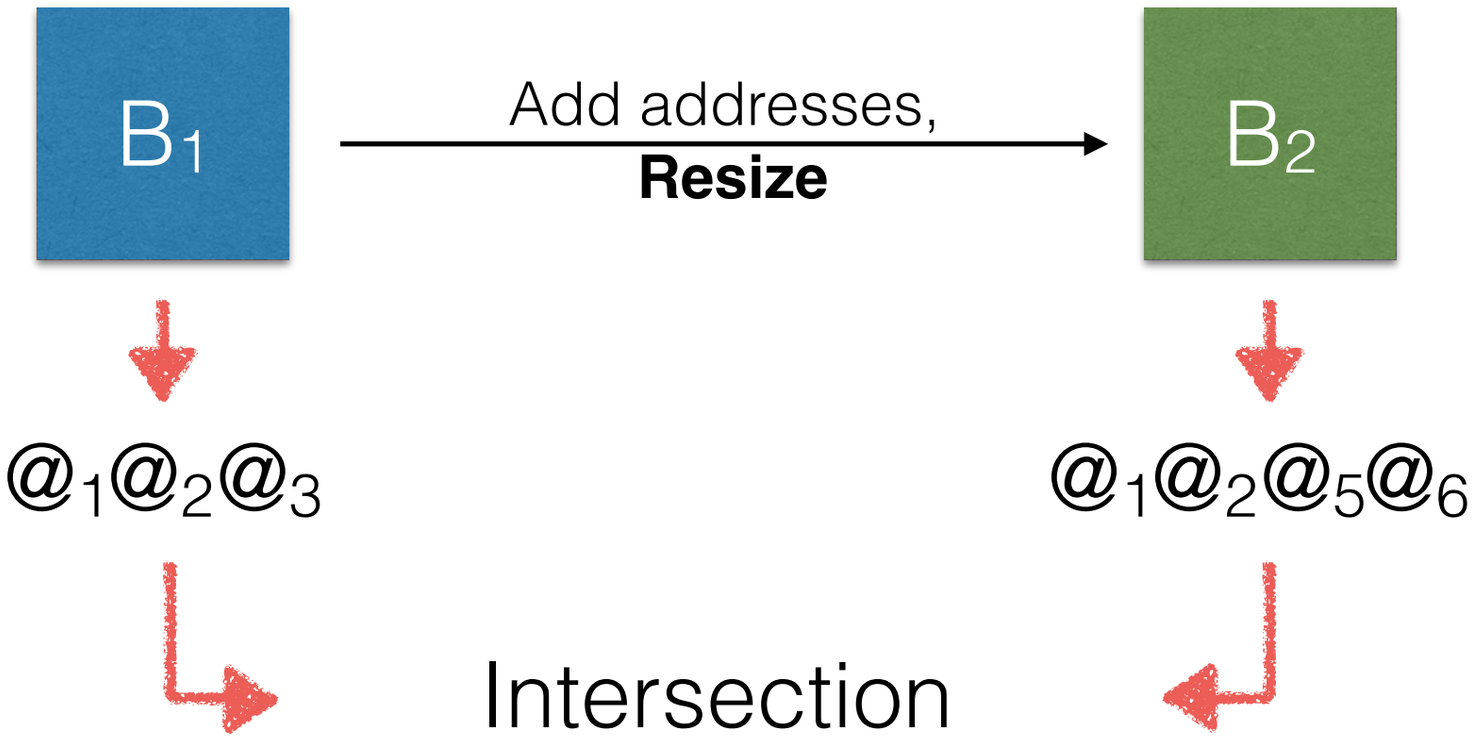
- Yield the same positives
- The adversary does not learn a lot

Experiment 2 - Resize



Exp.	Client	Seed	Size
No resize	Same	Same	Same
Resize	**Same**	**Same**	**Different**
Restart	Same	Different	Same
> 2 filter	Same	Different	Different

Experiment 2 - Resize

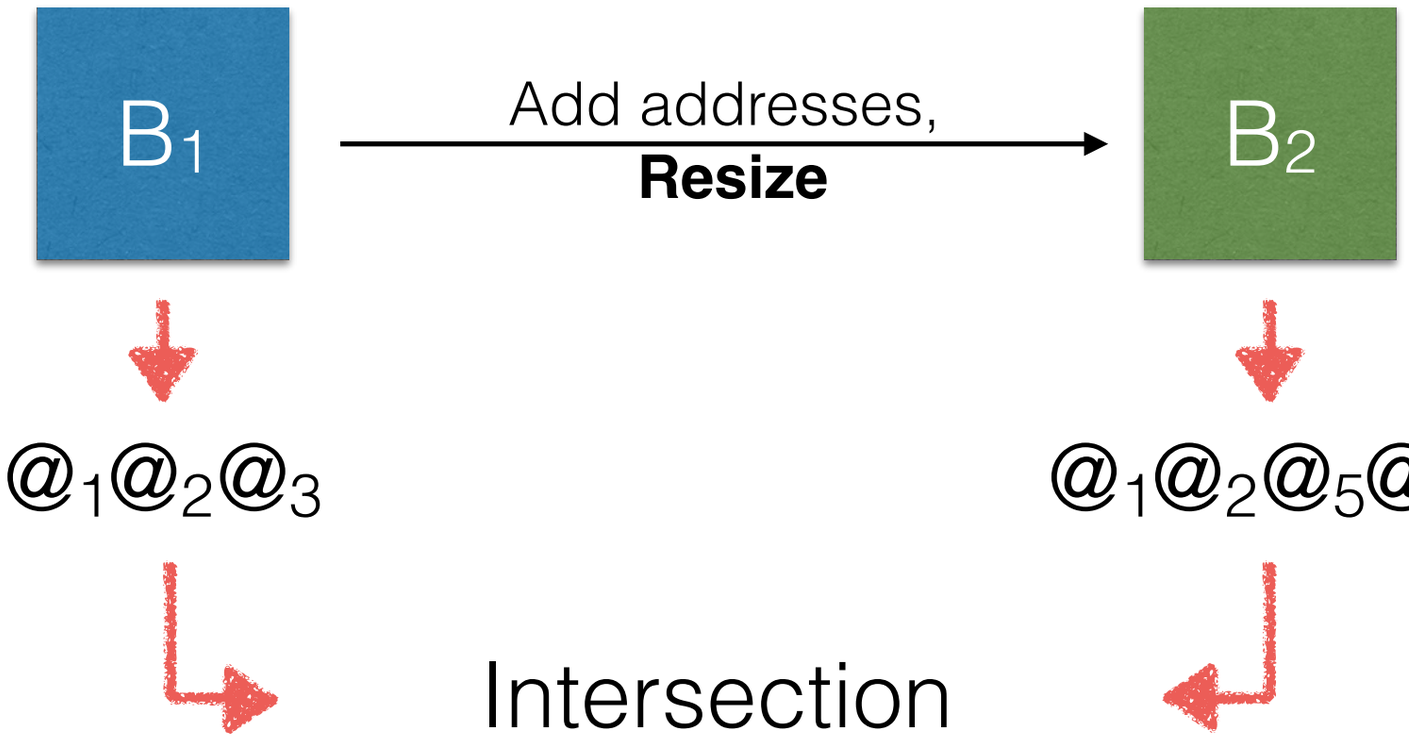


Exp.	Client	Seed	Size
No resize	Same	Same	Same
Resize	**Same**	**Same**	**Different**
Restart	Same	Different	Same
> 2 filter	Same	Different	Different

Results

Target FPR (%)	P(1) with 2 BF	P(1) with 1 BF
0.1	0.98	0.03

Experiment 2 - Resize

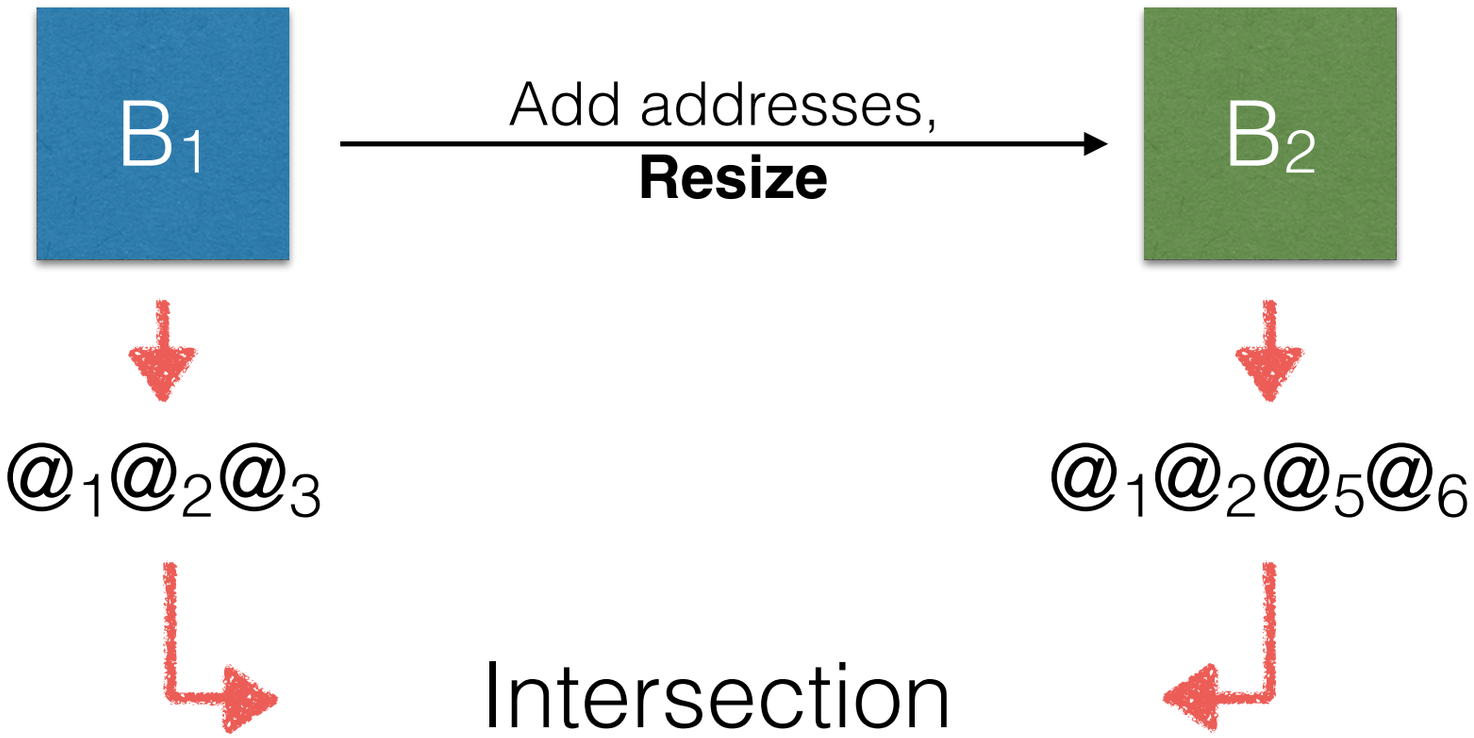


Exp.	Client	Seed	Size
No resize	Same	Same	Same
Resize	**Same**	**Same**	**Different**
Restart	Same	Different	Same
> 2 filter	Same	Different	Different

Results

Target FPR (%)	P(1) with 2 BF	P(1) with 1 BF
0.1	0.98	0.03

Experiment 2 - Resize

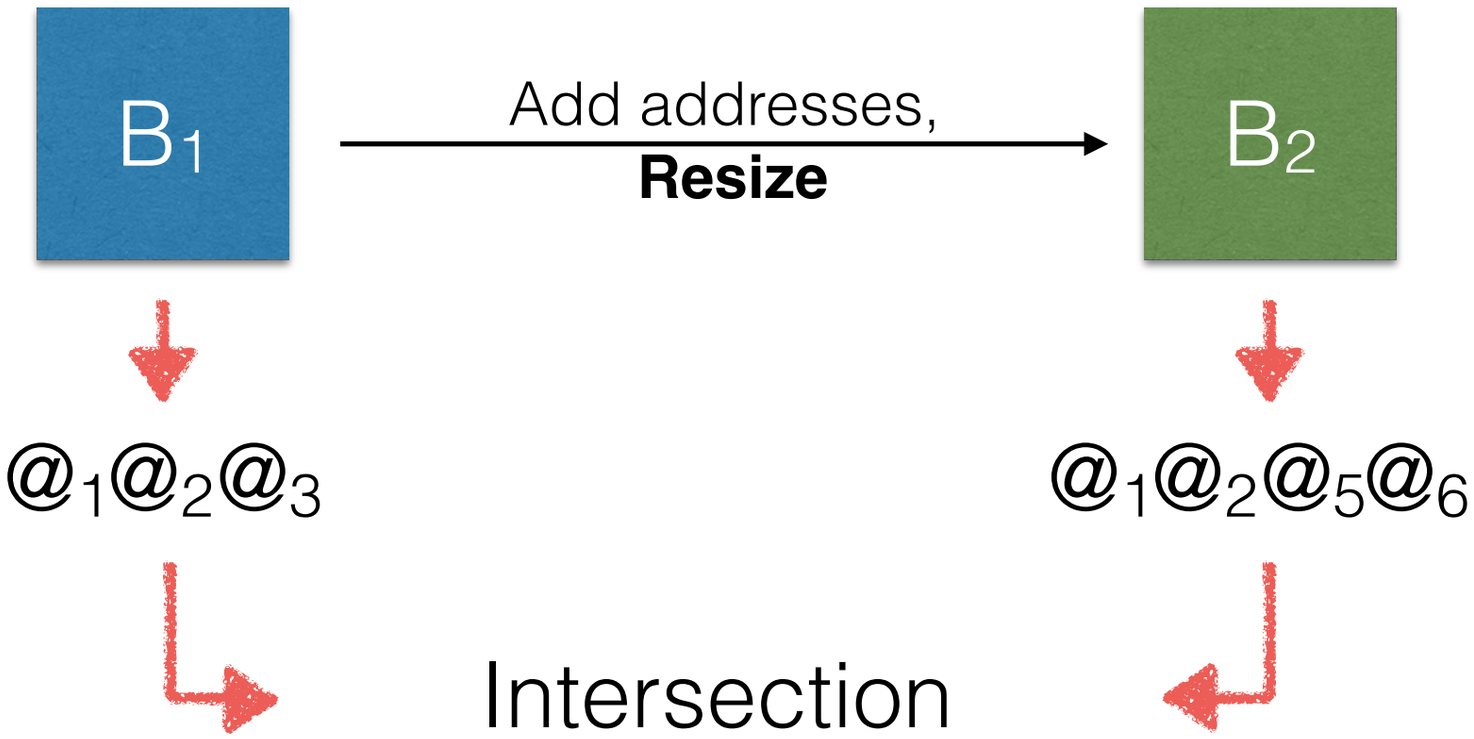


Exp.	Client	Seed	Size
No resize	Same	Same	Same
Resize	**Same**	**Same**	**Different**
Restart	Same	Different	Same
> 2 filter	Same	Different	Different

Results

Target FPR (%)	P(1) with 2 BF	P(1) with 1 BF
0.1	0.98	0.03

Experiment 2 - Resize



Results

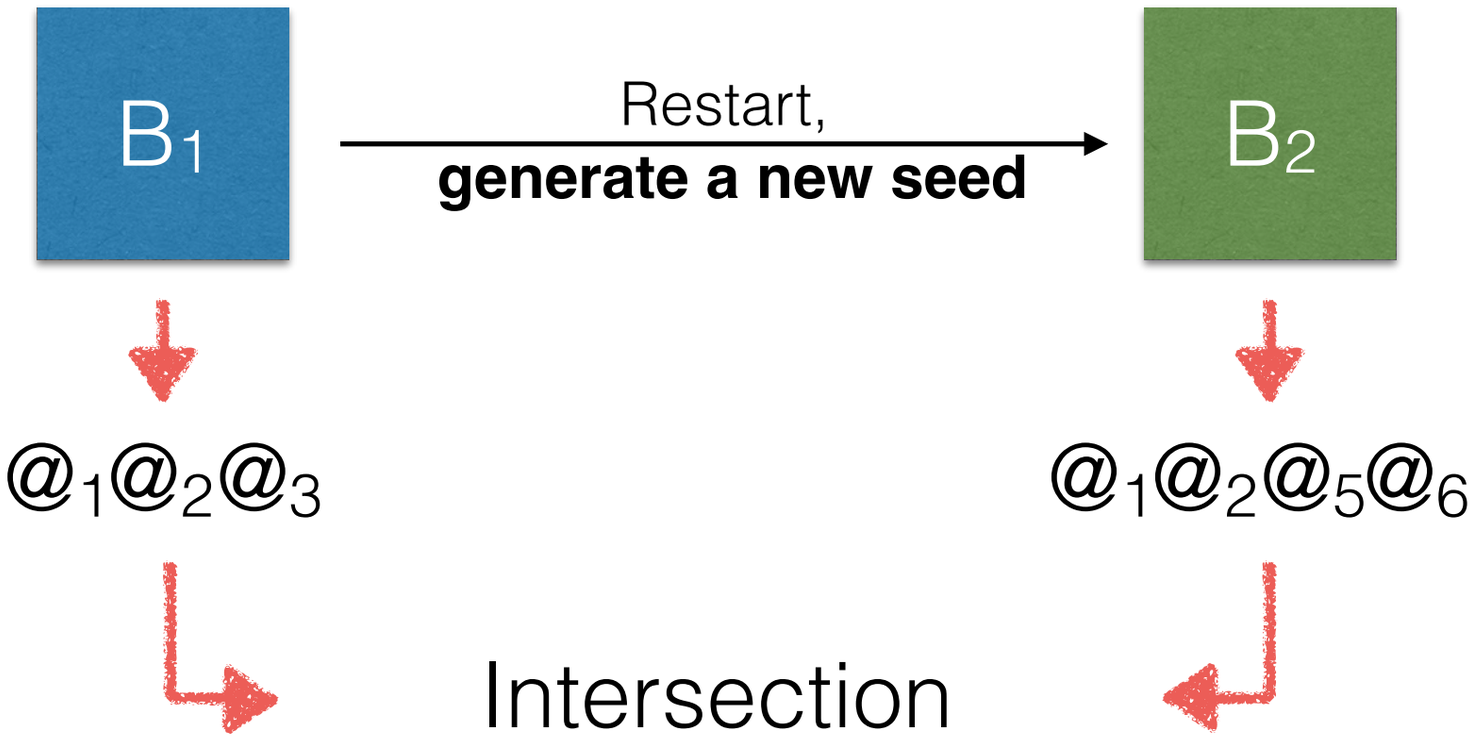
Target FPR (%)	P(1) with 2 BF	P(1) with 1 BF
0.1	0.98	0.03

significant change

Exp.	Client	Seed	Size
No resize	Same	Same	Same
Resize	**Same**	**Same**	**Different**
Restart	Same	Different	Same
> 2 filter	Same	Different	Different

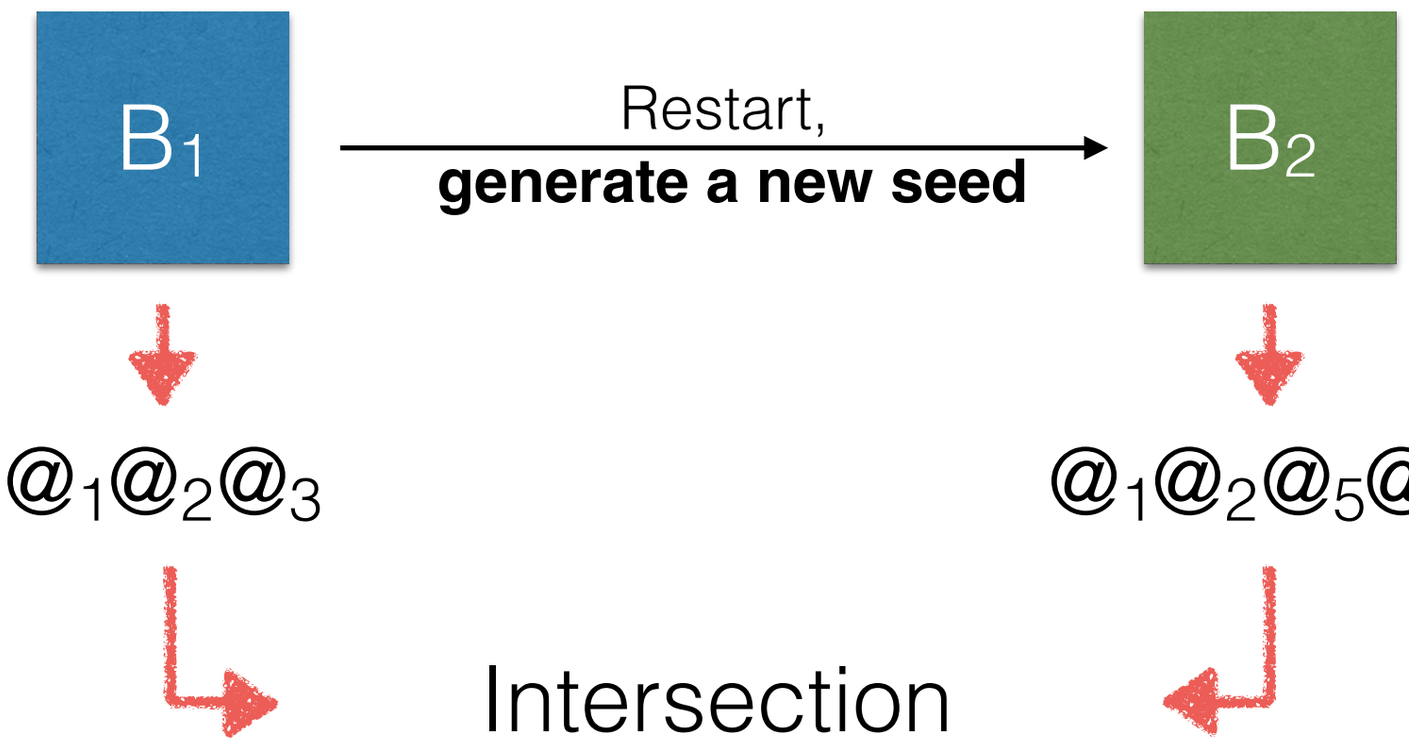
- Different BF sizes improve the attack

Experiment 3 - restart



Exp.	Client	Seed	Size
No resize	Same	Same	Same
Resize	Same	Same	Different
Restart	**Same**	**Different**	**Same**
> 2 filter	Same	Different	Different

Experiment 3 - restart

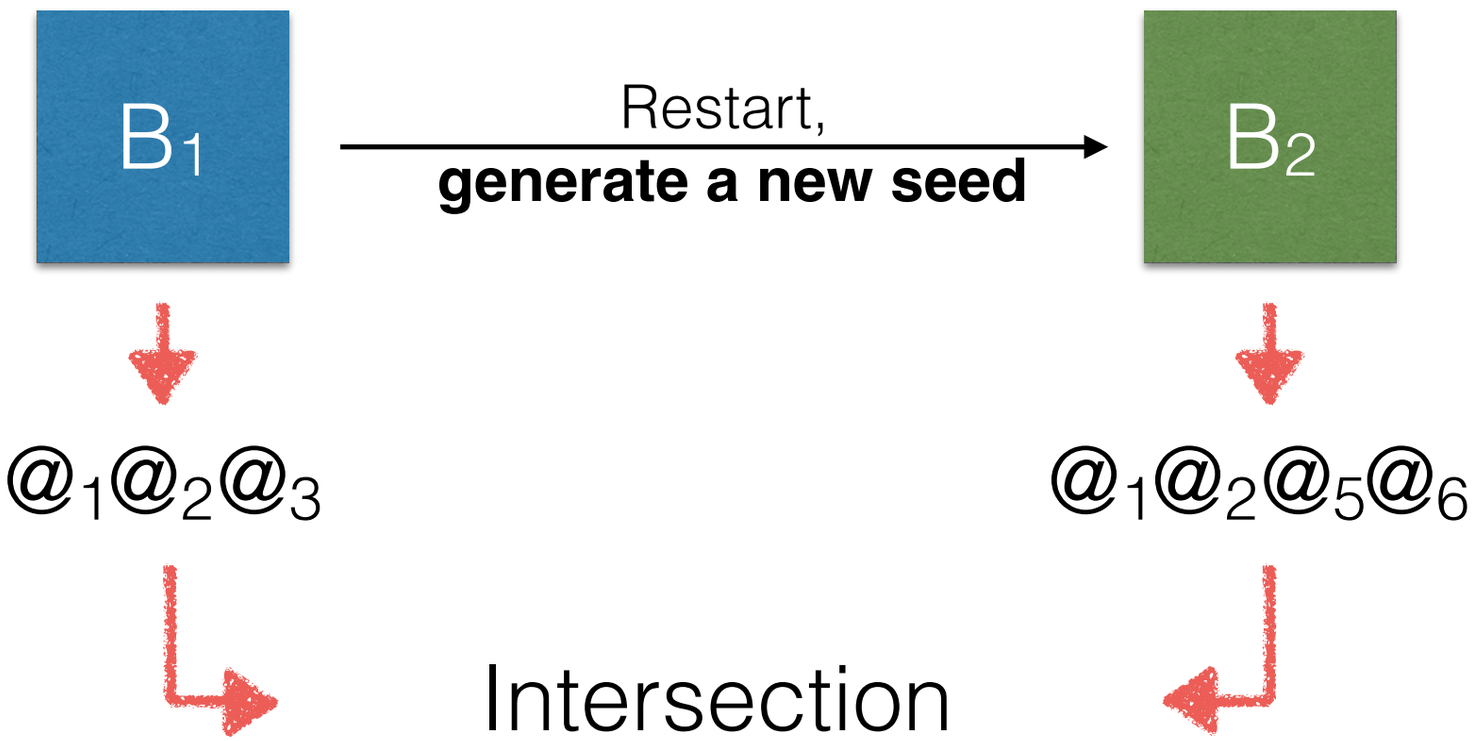


Exp.	Client	Seed	Size
No resize	Same	Same	Same
Resize	Same	Same	Different
Restart	**Same**	**Different**	**Same**
> 2 filter	Same	Different	Different

Results

Target FPR (%)	P(1) with 2 BF	P(1) with 1 BF
0.1	0.99	0.04

Experiment 3 - restart

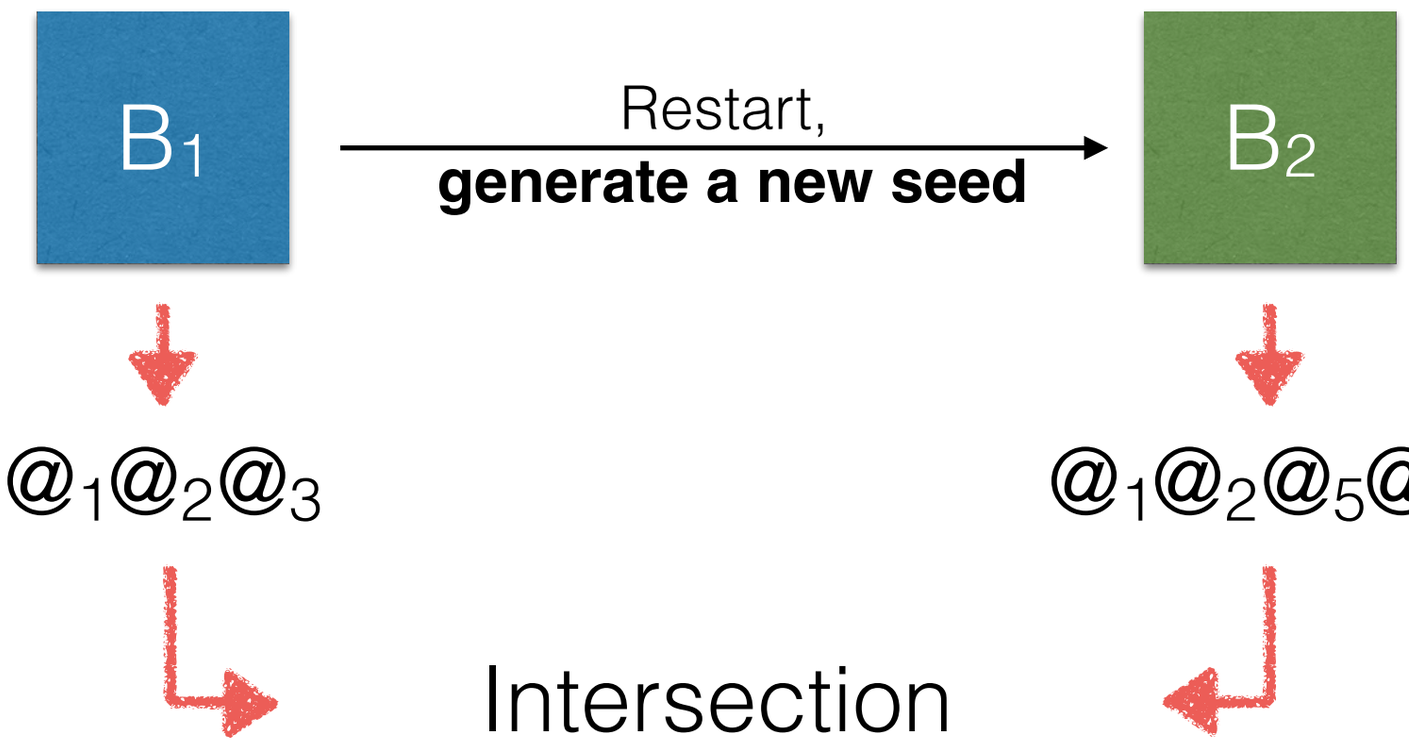


Exp.	Client	Seed	Size
No resize	Same	Same	Same
Resize	Same	Same	Different
Restart	**Same**	**Different**	**Same**
> 2 filter	Same	Different	Different

Results

Target FPR (%)	P(1) with 2 BF	P(1) with 1 BF
0.1	0.99	0.04

Experiment 3 - restart

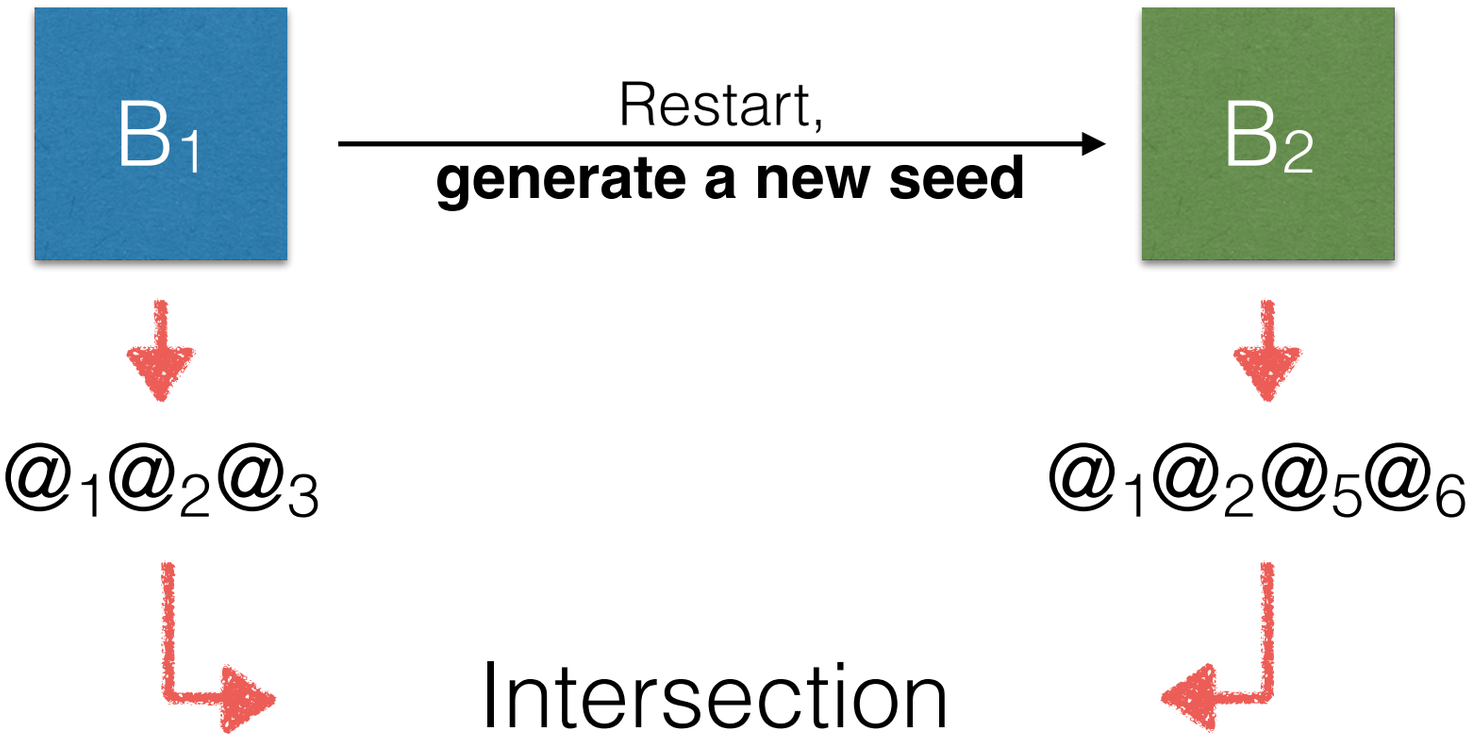


Exp.	Client	Seed	Size
No resize	Same	Same	Same
Resize	Same	Same	Different
Restart	**Same**	**Different**	**Same**
> 2 filter	Same	Different	Different

Results

Target FPR (%)	P(1) with 2 BF	P(1) with 1 BF
0.1	0.99	0.04

Experiment 3 - restart



Exp.	Client	Seed	Size
No resize	Same	Same	Same
Resize	Same	Same	Different
Restart	**Same**	**Different**	**Same**
> 2 filter	Same	Different	Different

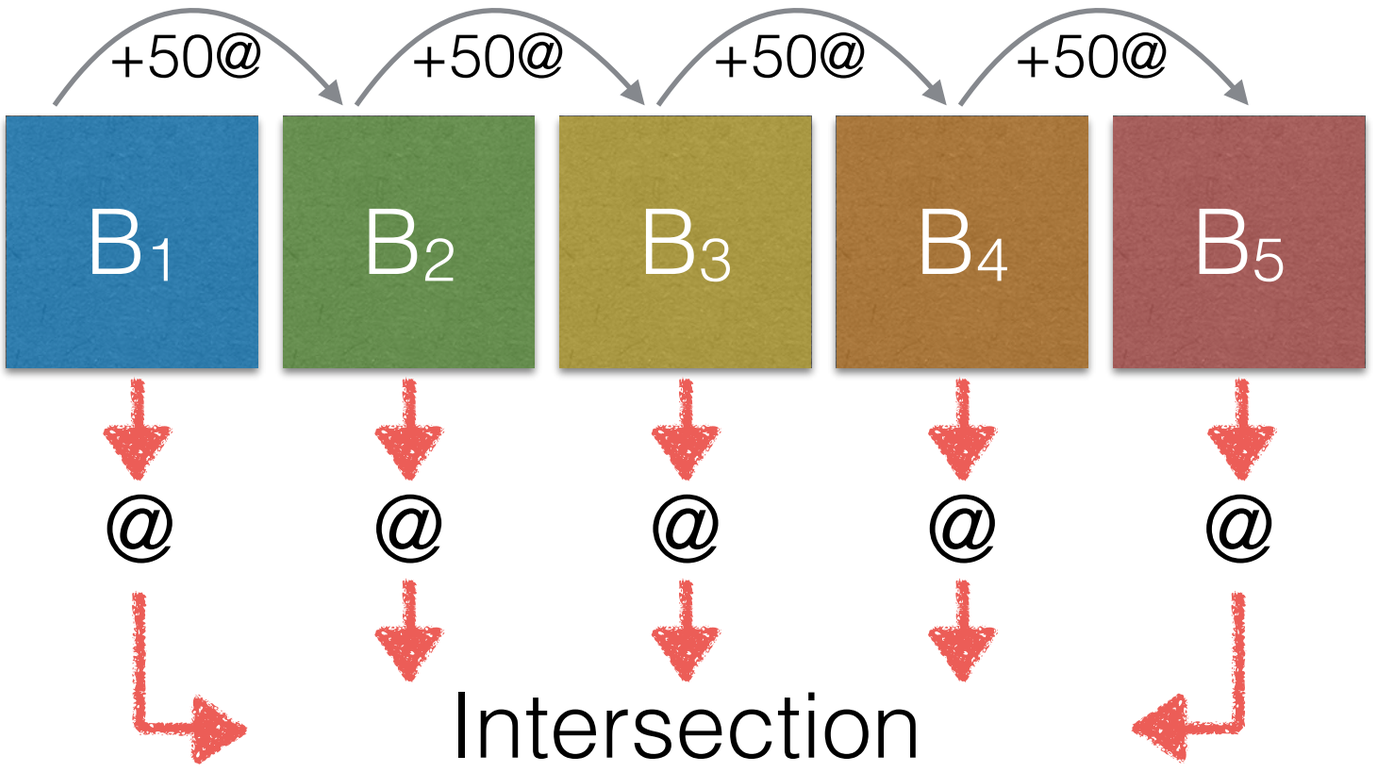
Results

Target FPR (%)	P(1) with 2 BF	P(1) with 1 BF
0.1	0.99	0.04

significant change

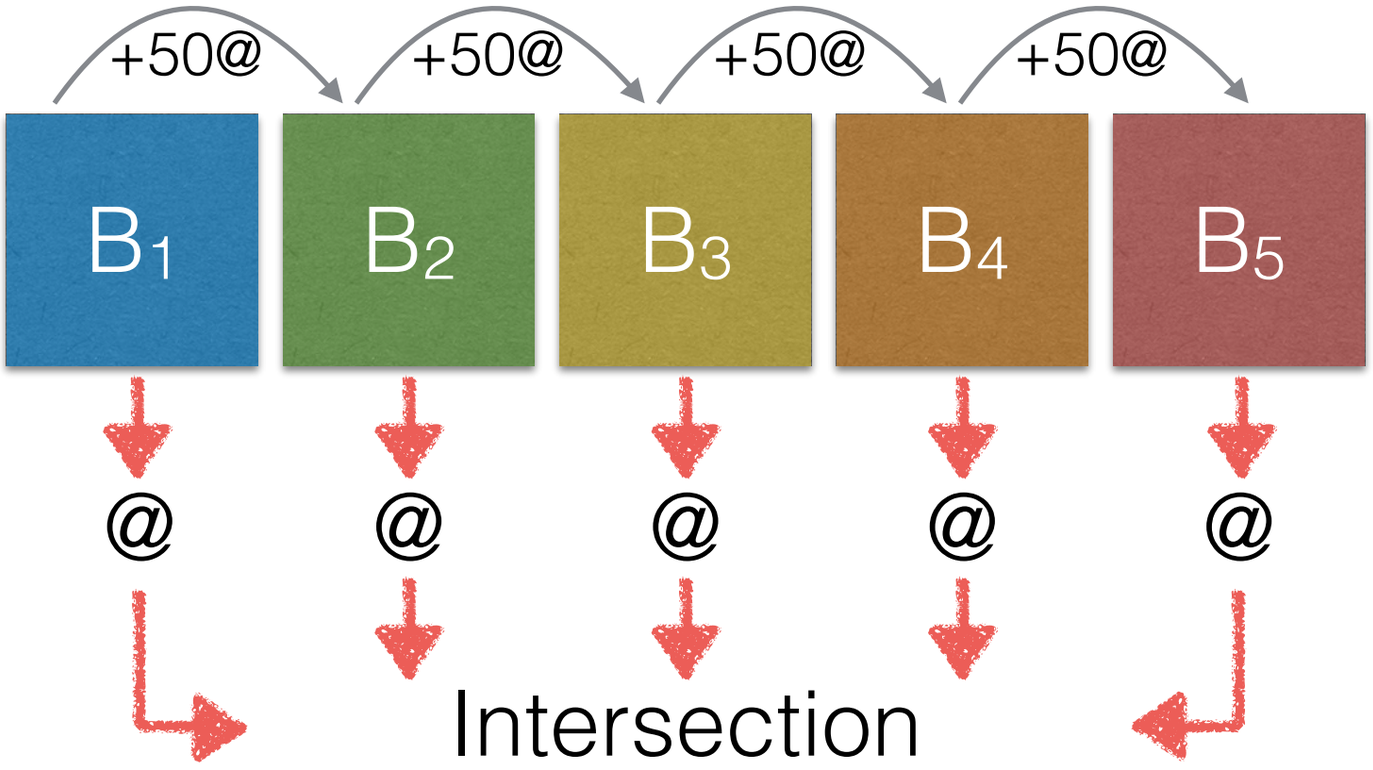
- Different BF seeds improve the attack

Experiment 4 - More than 2 filter



Exp.	Client	Seed	Size
No resize	Same	Same	Same
Resize	Same	Same	Different
Restart	Same	Different	Same
> 2 filter	**Same**	**Different**	**Different**

Experiment 4 - More than 2 filter

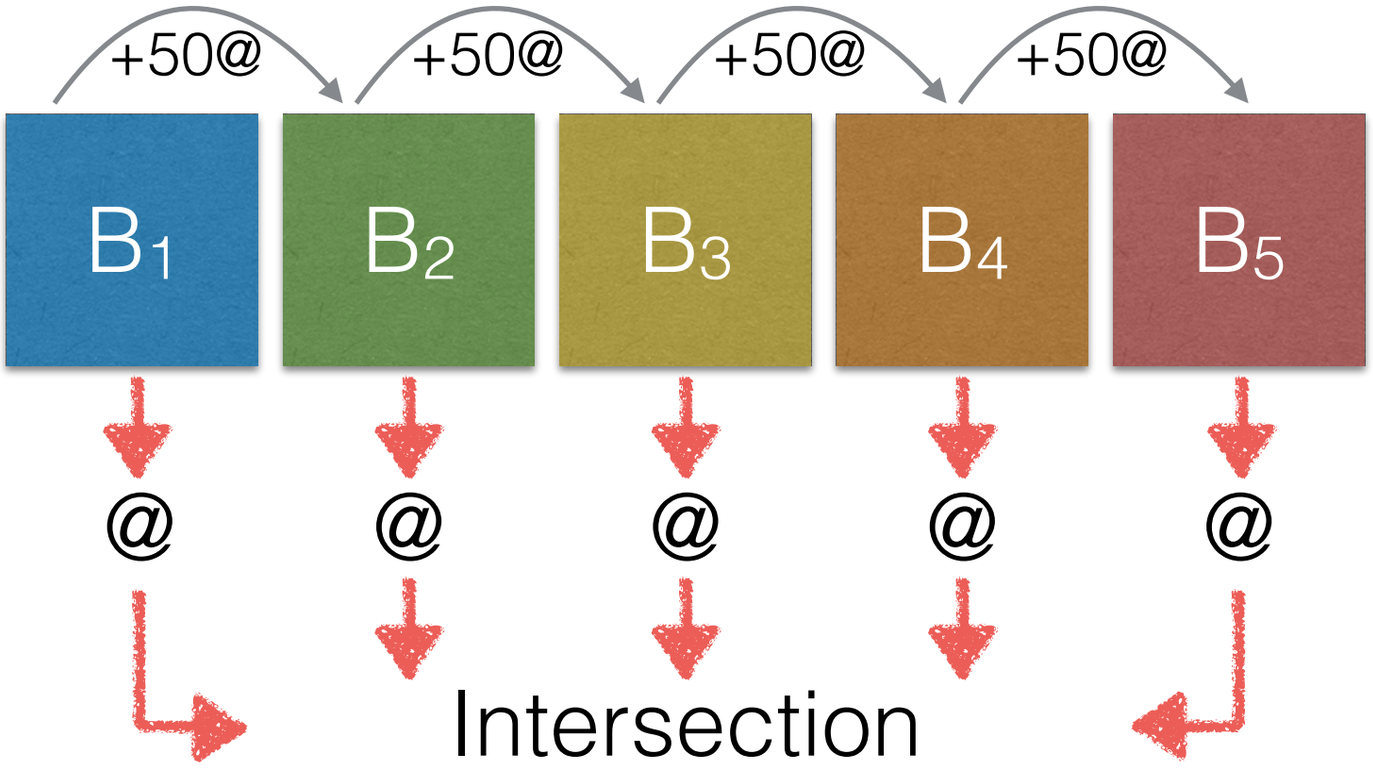


Results

Target FPR (%)	P(N) given 3 or more BF
0.05	~1
0.1	~1

Exp.	Client	Seed	Size
No resize	Same	Same	Same
Resize	Same	Same	Different
Restart	Same	Different	Same
> 2 filter	**Same**	**Different**	**Different**

Experiment 4 - More than 2 filter



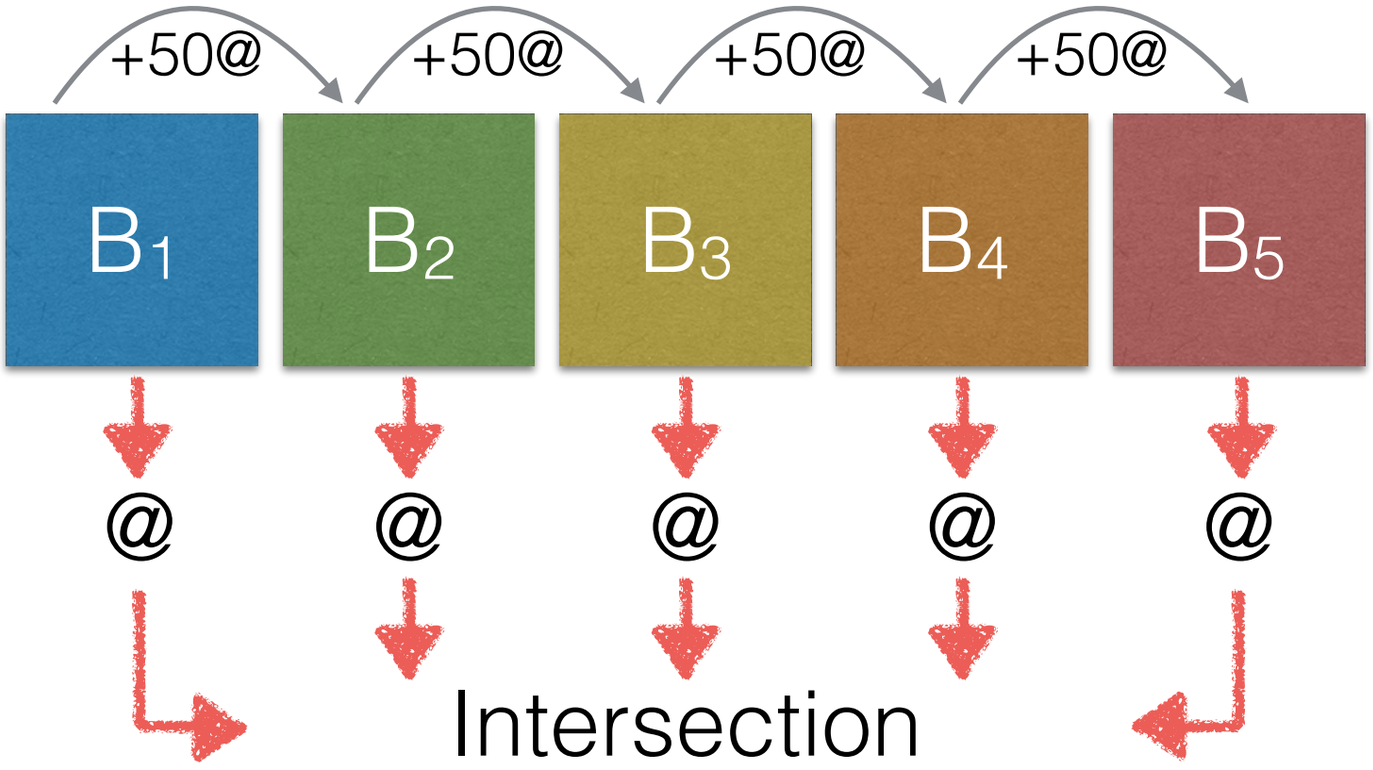
Results

Guessing all addresses

Target FPR (%)	P(N) given 3 or more BF
0.05	~1
0.1	~1

Exp.	Client	Seed	Size
No resize	Same	Same	Same
Resize	Same	Same	Different
Restart	Same	Different	Same
> 2 filter	**Same**	**Different**	**Different**

Experiment 4 - More than 2 filter



Exp.	Client	Seed	Size
No resize	Same	Same	Same
Resize	Same	Same	Different
Restart	Same	Different	Same
> 2 filter	**Same**	**Different**	**Different**

Results

Guessing all addresses

Target FPR (%)	P(N) given 3 or more BF
0.05	~1
0.1	~1

3 Bloom filter

All addresses yielded by B_1 are leaked

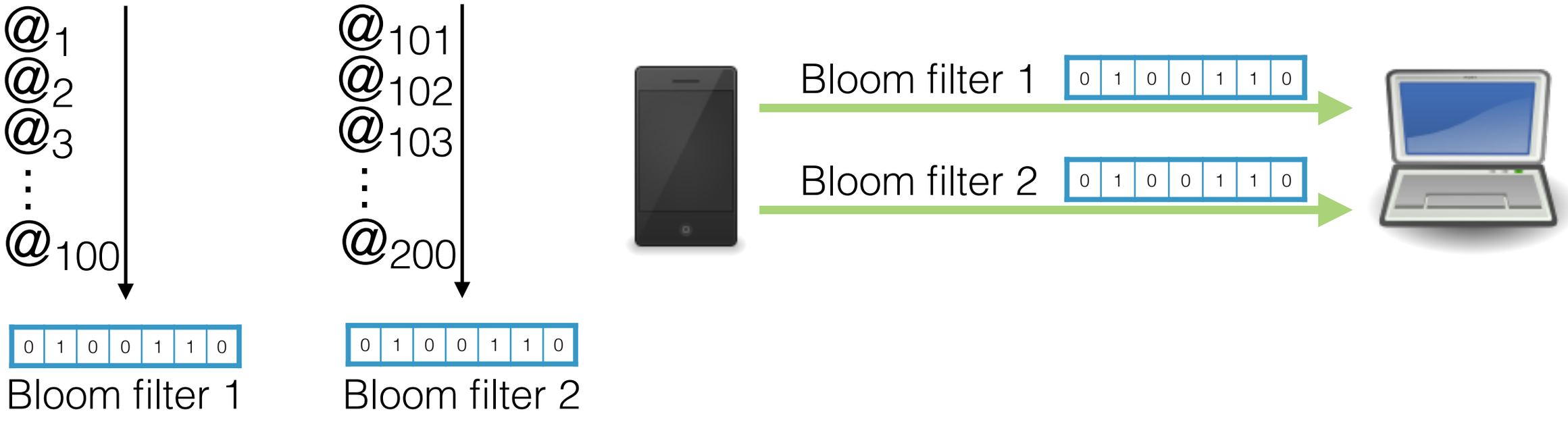
Observations

1. Need constant FPR

2. Multiple Bloom filter with different parameters 

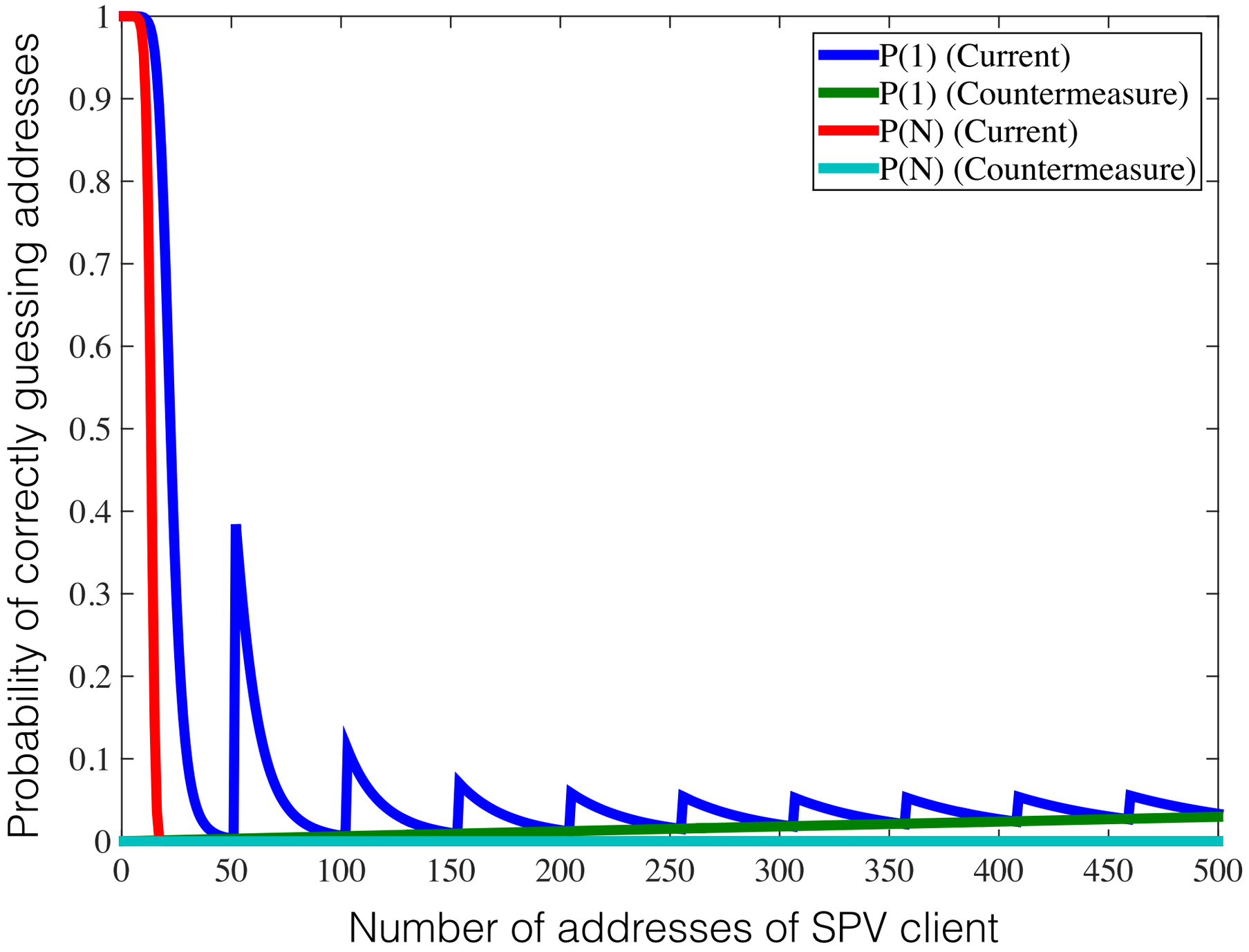
3. SPV clients should keep state (e.g., about seed) 

Proposed solution

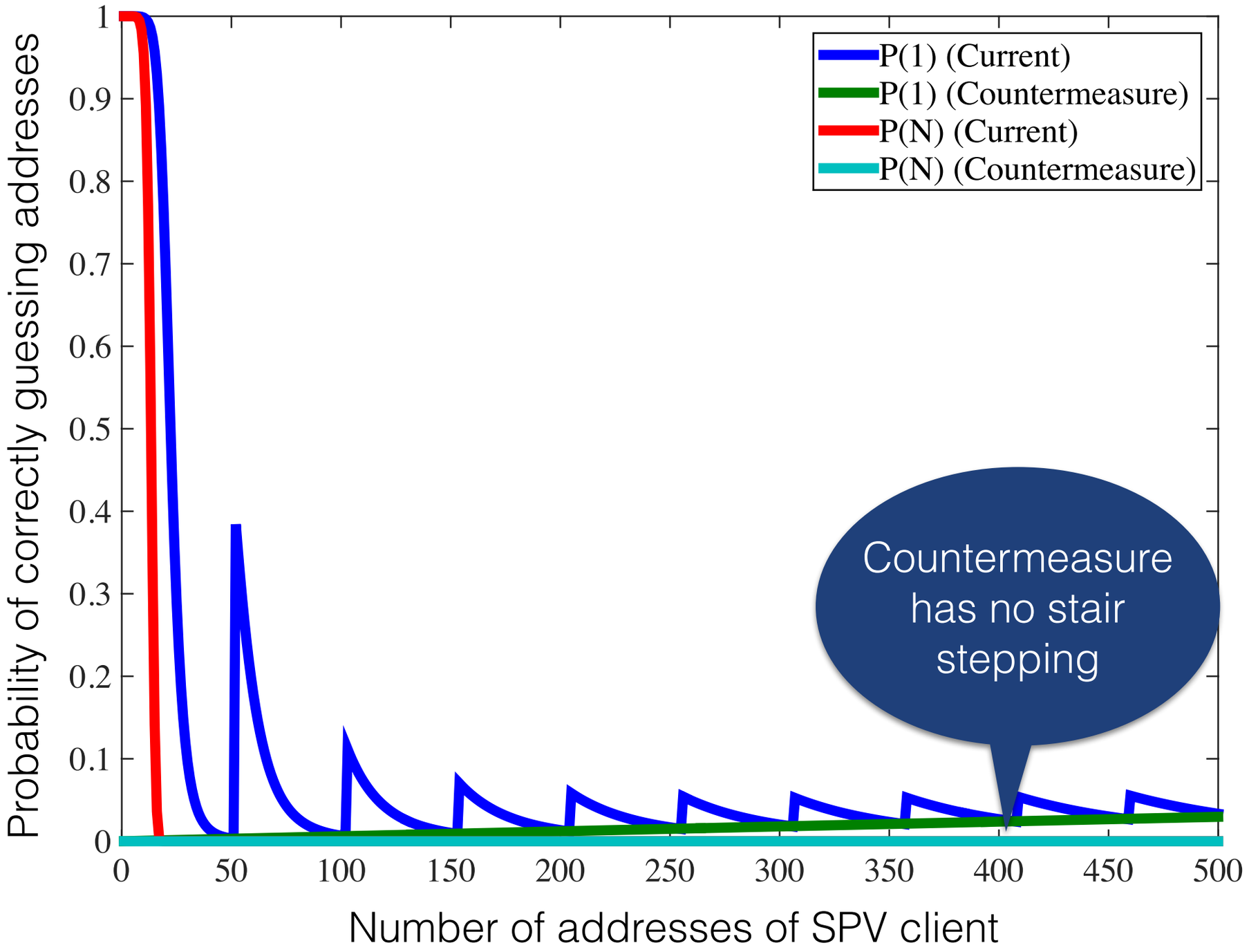


- Pre-generate Bitcoin addresses and insert into filter
- Keep state about outsourced Bloom filter
- Overhead: For 100 addresses, < 1 kb

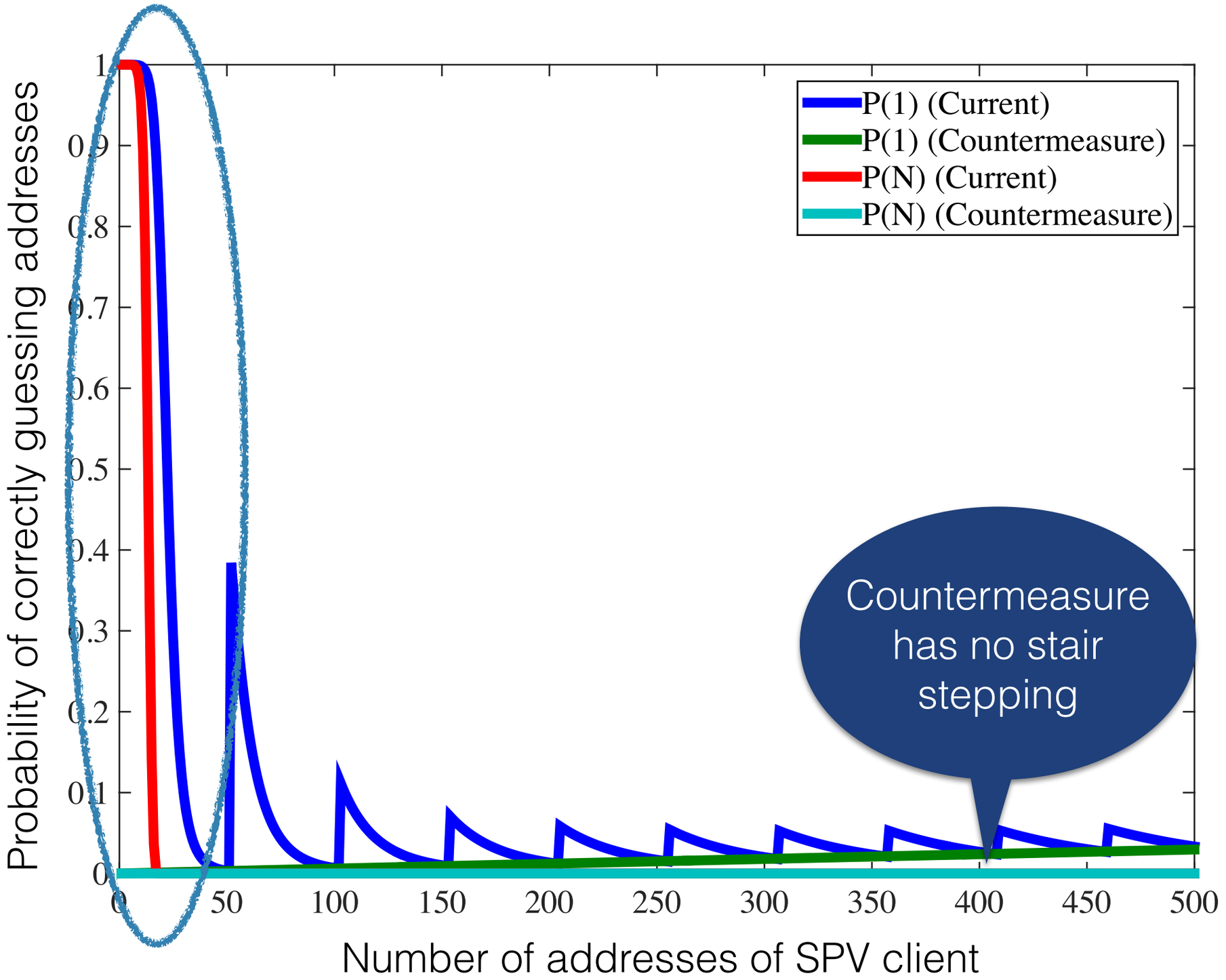
Proposed solution



Proposed solution



Proposed solution



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 

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

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

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!