

YÅPS

*Yet Another Anonymous Publication
System:
Modified IDA for secure and
space-efficient block storage*

Christian Boesgaard

`pink@diku.dk`



Content

- Anonymous Publication Systems
- YÅPS Overview
- Censorship Resistance and Unlinkability
- Modified IDA



Anonymous Publication Systems

To speak his thoughts is every freeman's right, in peace and war, in council and in fight.

—Homer, The Iliad.



Publication Systems

A *publication system* provides users with the ability to:

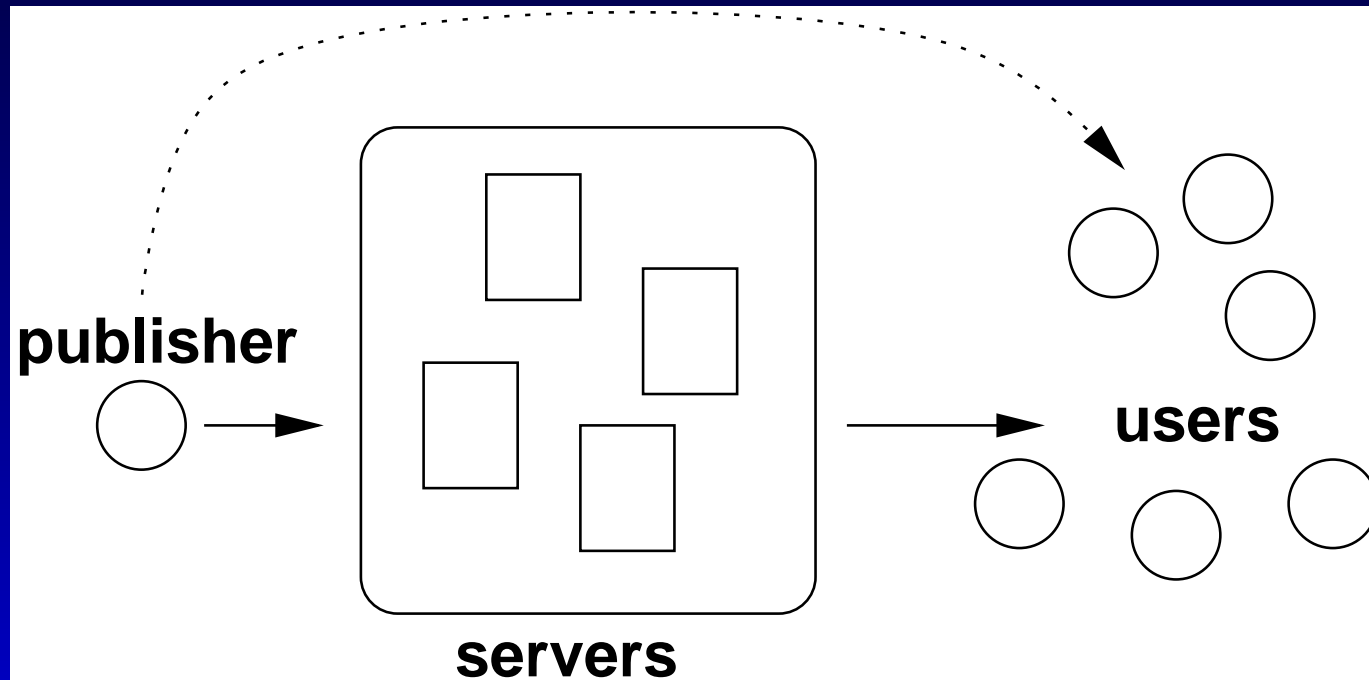
- publish documents.
- read published documents.

Examples: WWW and newspapers.



Anonymous Publication Systems

An APS is a censorship-resistant Internet-based publication system.



Examples: Freenet and Free Haven.



Goals for an APS

- Anonymity
- Censorship resistance
- Availability
- Updateable Documents



YÅPS Overview

Though this be madness, yet there is method in it. . .
—Hamlet.



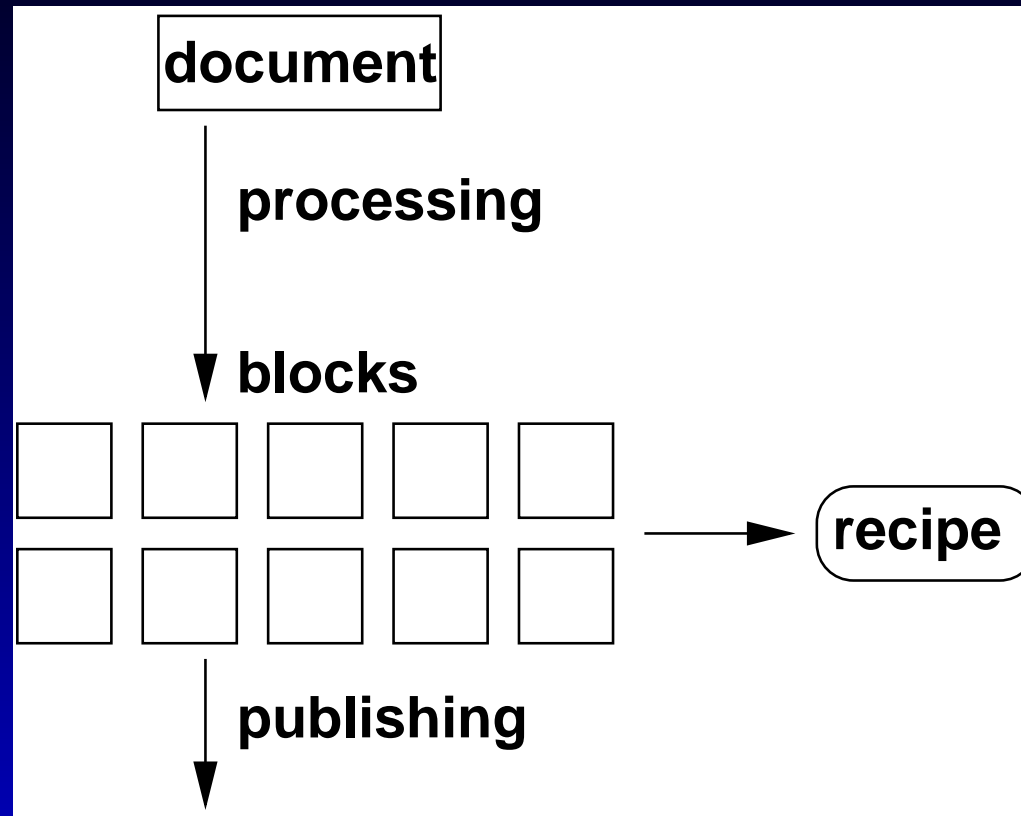
Overview

Terms:

- **Publishers publishes documents processed to blocks using storage, index, and, rerouting servers.**
- **Publishers creates recipes which users can use to retrieve published documents with.**



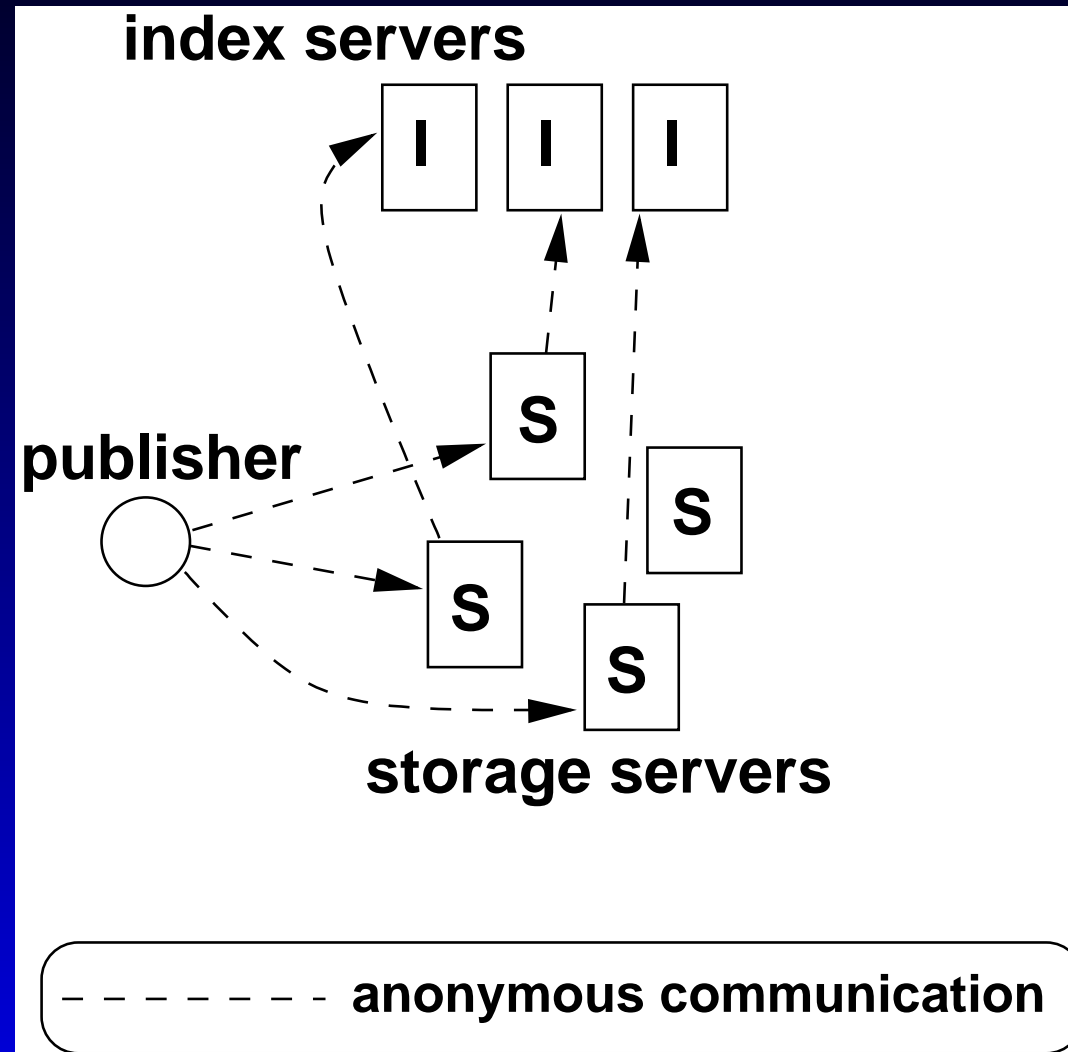
Publication



A publisher process a document to get a set of blocks.



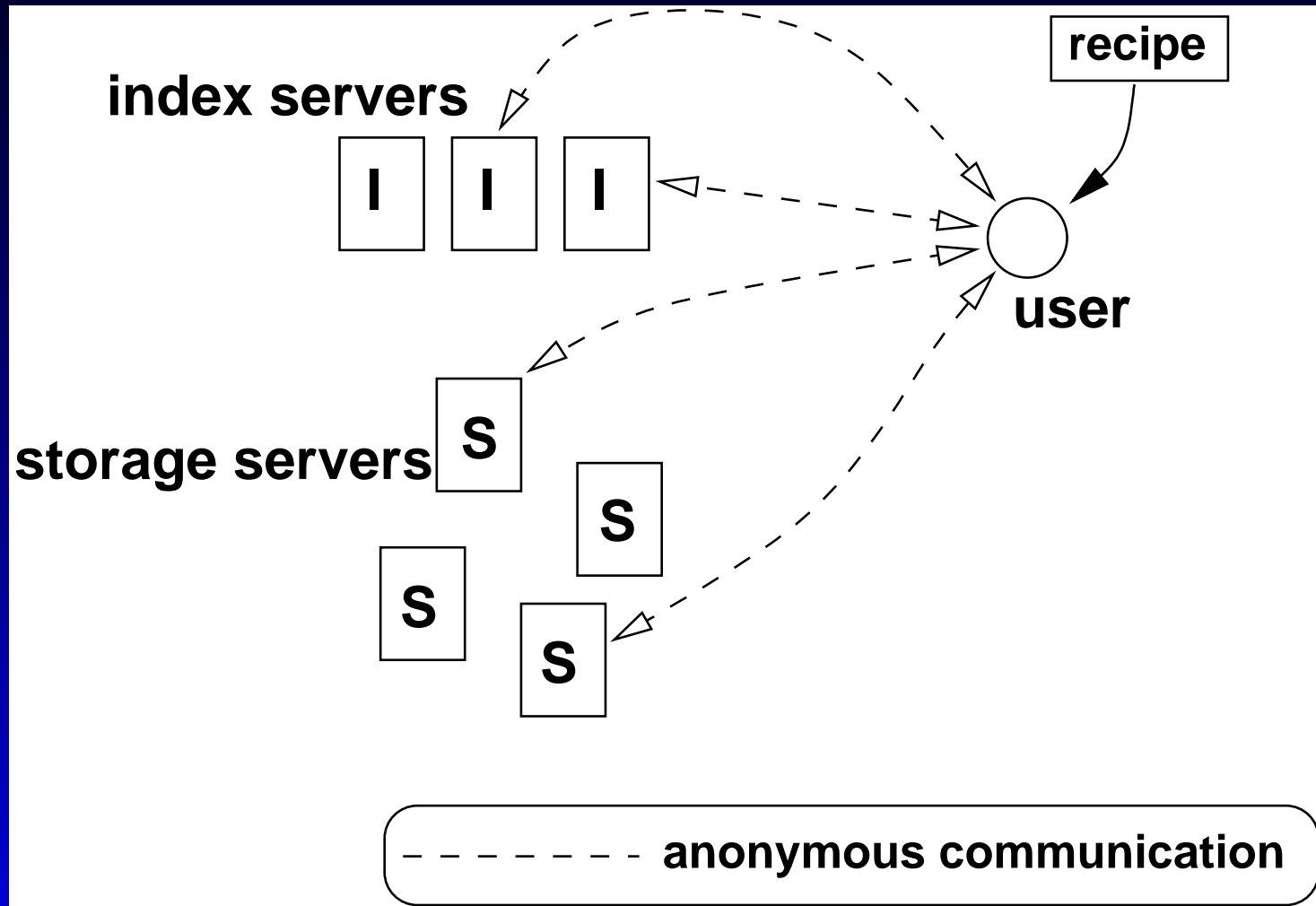
Publication



The publisher publishes the blocks.



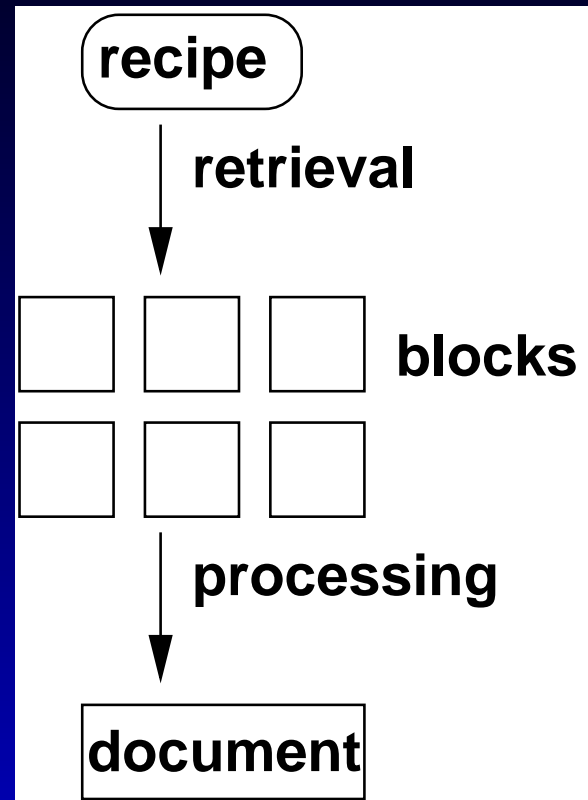
Retrieval



A user obtains a recipe and uses the index servers to locate the blocks.



Retrieval



The user recreates the document.



Some Specifications

- designed for small documents (<1MB)
- fixed blocksize (100KB)
- no search capabilities
- a recipe is a short string used to retrieve a single block with the “full recipe”
- updateable documents using updateable recipes
- location based on Chord (DHT)
- communication based on MIX (Mixminion variant with Rendez-Vous from Onion Routing)



Censorship Resistance and Unlinkability

They that can give up essential liberty to obtain a little temporary safety deserve neither liberty nor safety.

—Benjamin Franklin, Historical Review of Pennsylvania, 1759.



Censorship Resistance

Servers must be protected against censorship.

- Anonymity
- Denial (*plausible denial*)



Denial

Different grades:

- A server operator knows nothing about blocks.
- A block can be related to more than one document.
- A block can be used to recreate more than one doc (*entanglement*).
- A block can be part of any document.



Requirement

A block can be part of any document requires that:

- Given any block B and any document D , we should be able to show that B could originate from D .

Related requirements: availability, space-efficiency.



Some solutions

- IDA – not secure.
- XOR + replication – works.
- XOR + IDA – works.

Other (k, n) -threshold schemes are secure but requires more space than XOR.



Modified IDA

Out of the crooked timber of humanity, no straight thing can ever be made

—Immanuel Kant.



IDA

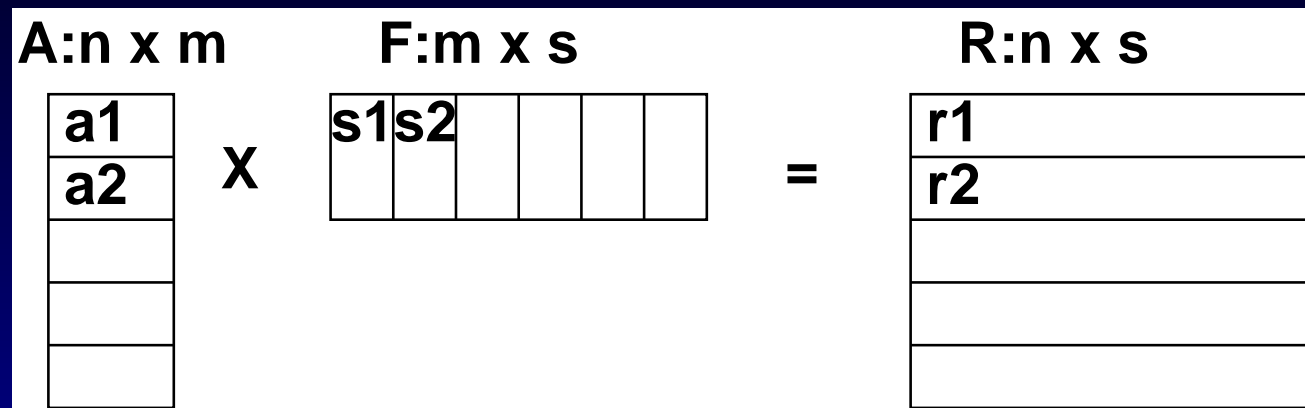
- a file F is processed into n parts of size s using a dispersal matrix A .
- F can be recreated from m parts (and rows from A).
- working on elements in \mathbb{Z}_p .

$A:n \times m$		$F:m \times s$		$R:n \times s$
a1	x	s1s2	=	r1
a2				r2

Usually the A -rows are saved with the R -rows.



Why IDA does not work



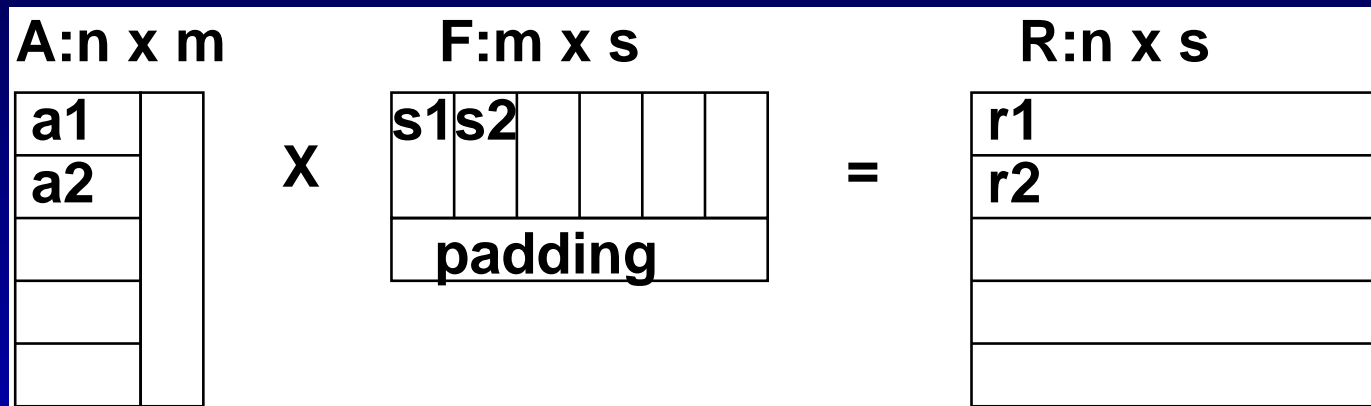
- Given any row from an R and any document F , we should be able to show that F could originate from D .

This is not possible as it requires a mapping to all combinations of s elements given only the m elements in an A row (and $m \ll s$).

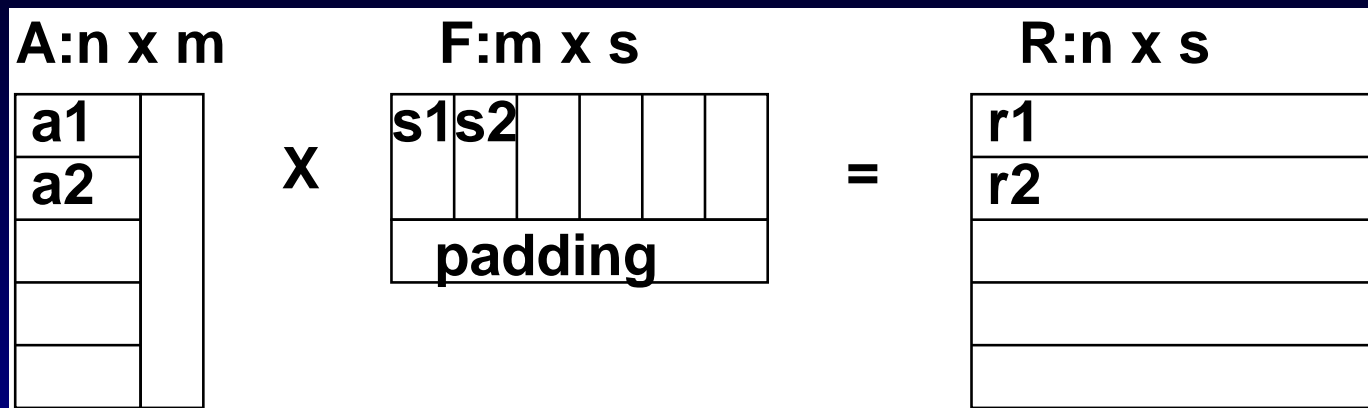


Modified IDA

- pad F with an extra row of random values.
- do not allow 0 in A .



Why Modified IDA works 1

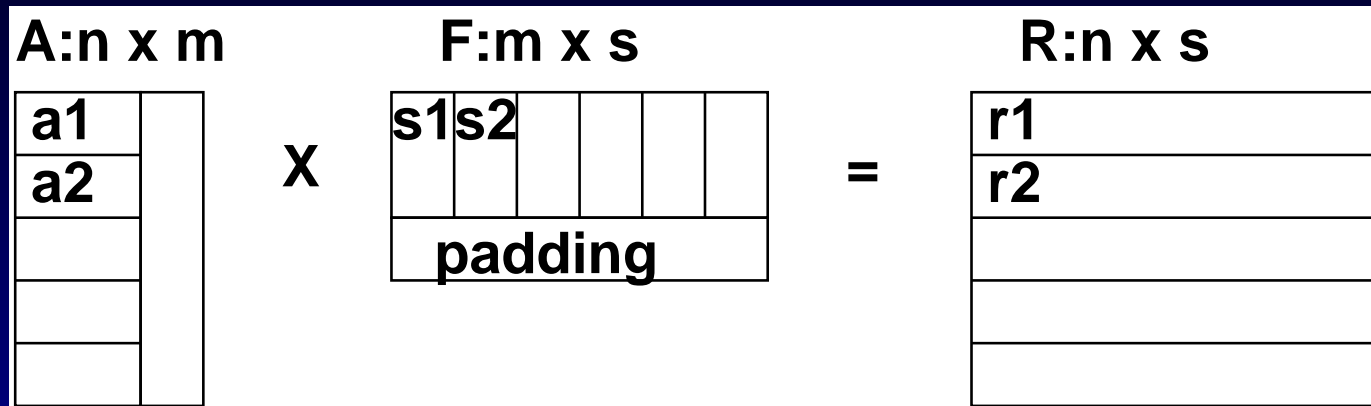


- Given any row from an R and any document F , we should be able to show that F could originate from D .

First, note as we can choose the padding, we now have a mapping from s to s elements.



Why Modified IDA works 2



Second, we can choose the sn_m in:

$$rn_1 = an_1sn_1 + \dots + an_msn_m \pmod{p}$$

and as an_m cannot be 0 we can get any rn_1 by choosing the right sn_m .



Side Effects of Modified IDA

- Requires one extra block to save the padding.
- Dispersal matrix grows with n elements.



Results

Given a fixed document size and a fixed amount of space to store the blocks, what is the availability of the document?

Systems:

- XOR+replicate 1
- XOR+replicate 2
- XOR+IDA
- Modified IDA



Results 2/8

- Document size: 2 blocks
- Space: 8 blocks

System	0.25	0.5	0.75
XOR+replicate 1	4%	32%	77%
XOR+replicate 2	22%	77%	98%
XOR+IDA	11%	64%	97%
Modified IDA	32%	86%	100%



Results 4/16

- Document size: 4 blocks
- Space: 16 blocks

System	0.25	0.5	0.75
XOR+replicate 1	0%	10%	60%
XOR+replicate 2	5%	60%	97%
XOR+IDA	3%	60%	99%
Modified IDA	37%	96%	100%



Results 16/64

- Document size: 16 blocks
- Space: 64 blocks

System	0.25	0.5	0.75
XOR+replicate 1	0%	0%	13%
XOR+replicate 2	0%	13%	88%
XOR+IDA	0%	55%	100%
Modified IDA	43%	100%	100%



Conclusion

The presented modified IDA provides the same security as XOR + replication or IDA and significantly higher availability using the same amount of space.

