Embedding Cover-Free Families

Thaís Bardini Idalino
Departamento de Informática e Estatística
Universidade Federal de Santa Catarina

IV Workshop on Finite Fields and Applications

Joint work with Lucia Moura

2012

Undergrad

Tópicos Especiais em Computação III:
Corpos Finitos e Aplicações à Teoria
de Códigos e Criptografia

2013

Masters

Research meetings & paper

2015

PhD

Comprehensive exam committee
PhD proposal committee

Today

Collaboration with students’ research

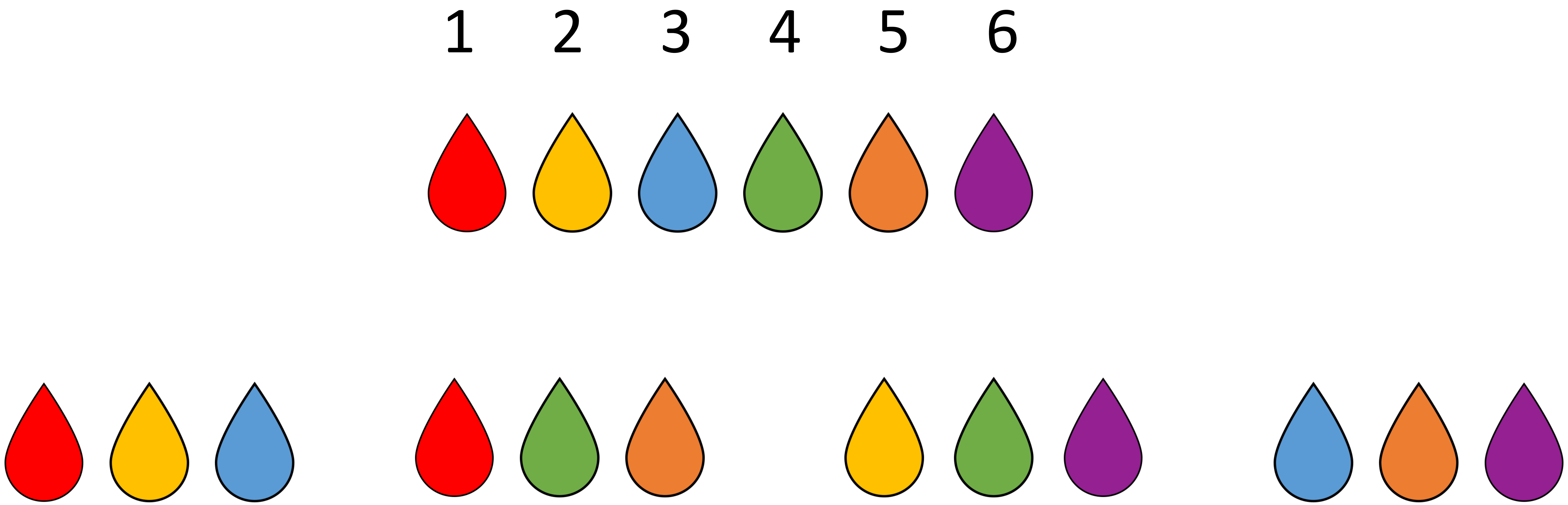
Embedding Cover-Free Families

Thaís Bardini Idalino
Departamento de Informática e Estatística
Universidade Federal de Santa Catarina

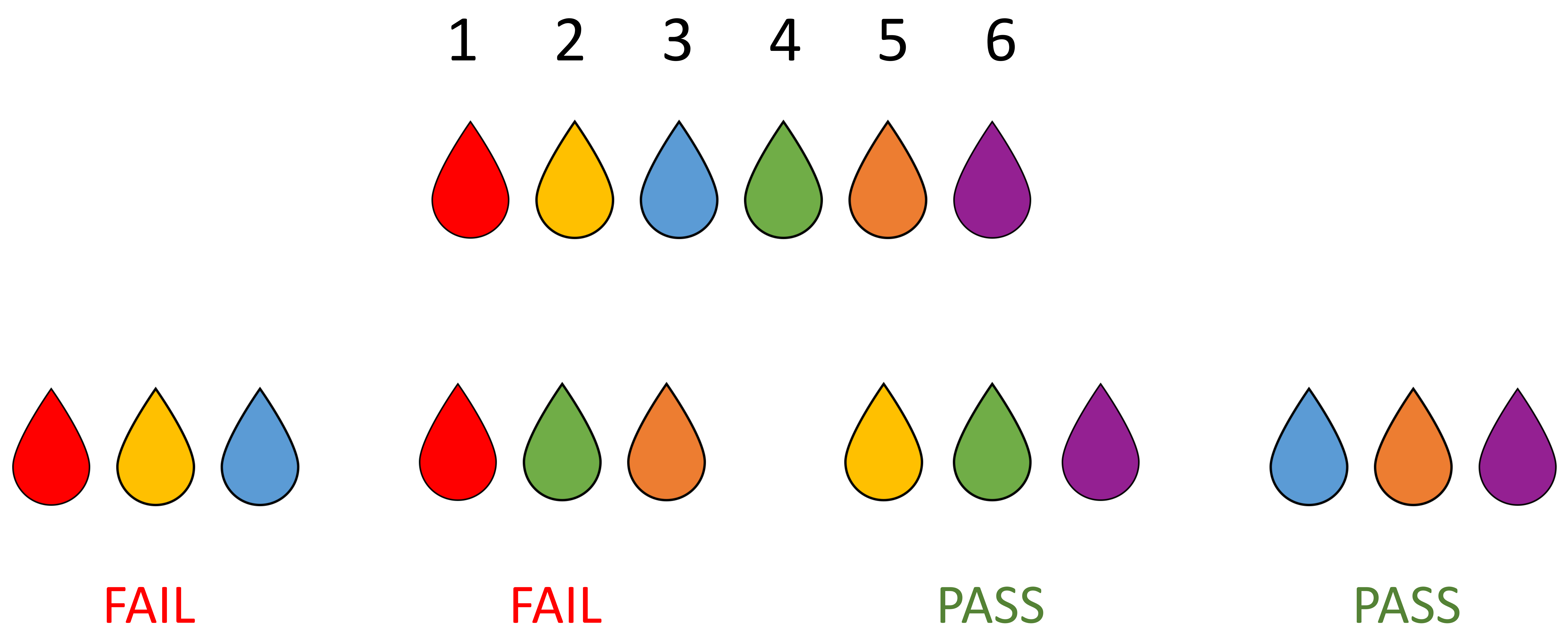
IV Workshop on Finite Fields and Applications

Joint work with Lucia Moura

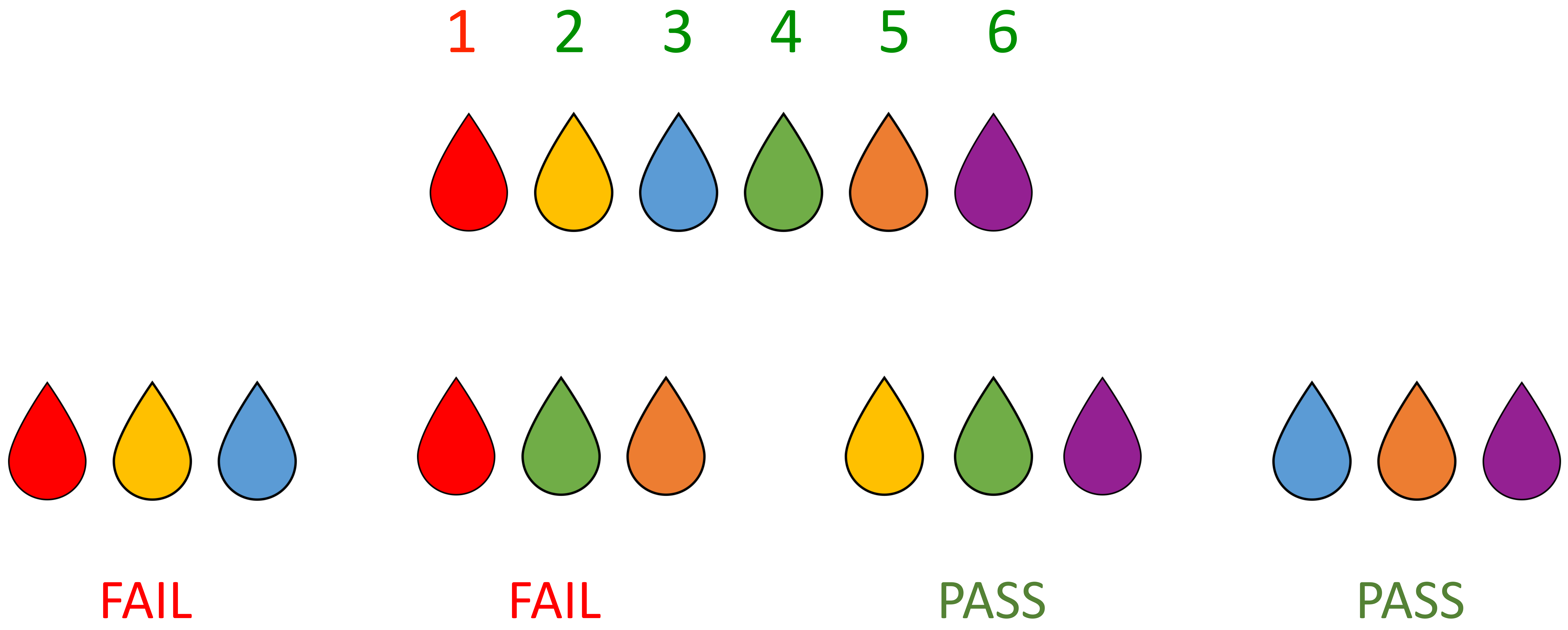
Combinatorial Group Testing



Combinatorial Group Testing

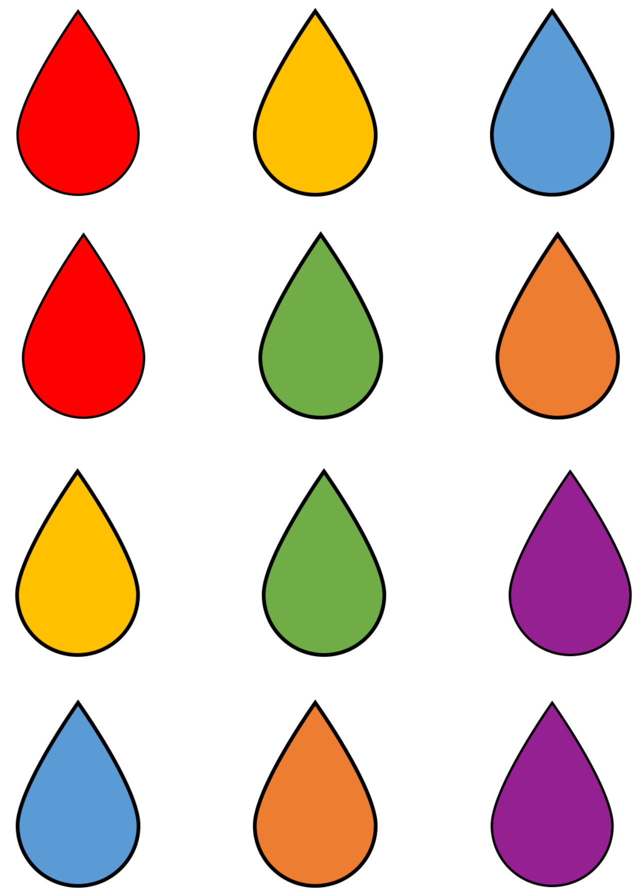


Combinatorial Group Testing



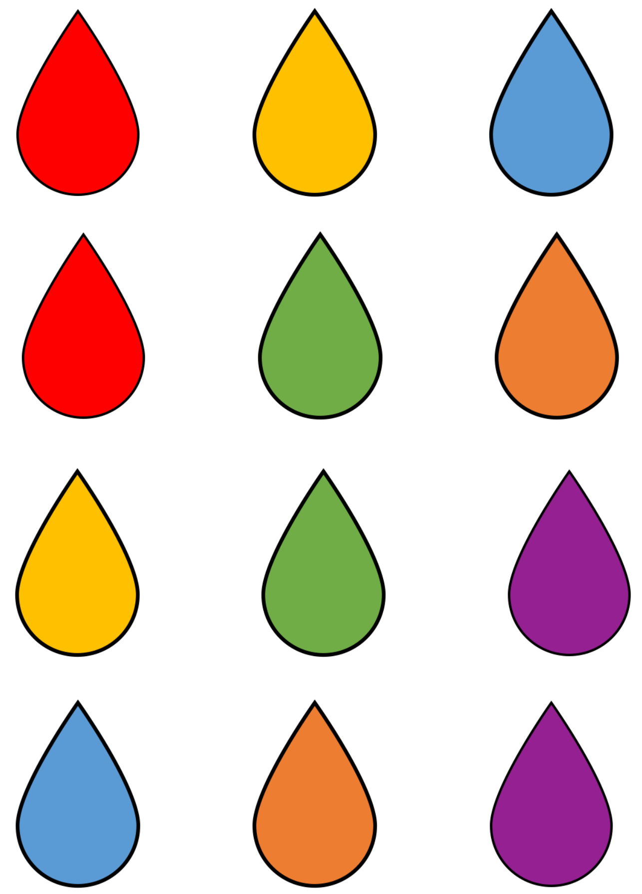
Cover-Free Families

	1	2	3	4	5	6	
Test 1	1	1	1	0	0	0	FAIL
Test 2	1	0	0	1	1	0	FAIL
Test 3	0	1	0	1	0	1	PASS
Test 4	0	0	1	0	1	1	PASS



Cover-Free Families

	1	2	3	4	5	6
Test 1	1	1	1	0	0	0
Test 2	1	0	0	1	1	0
Test 3	0	1	0	1	0	1
Test 4	0	0	1	0	1	1



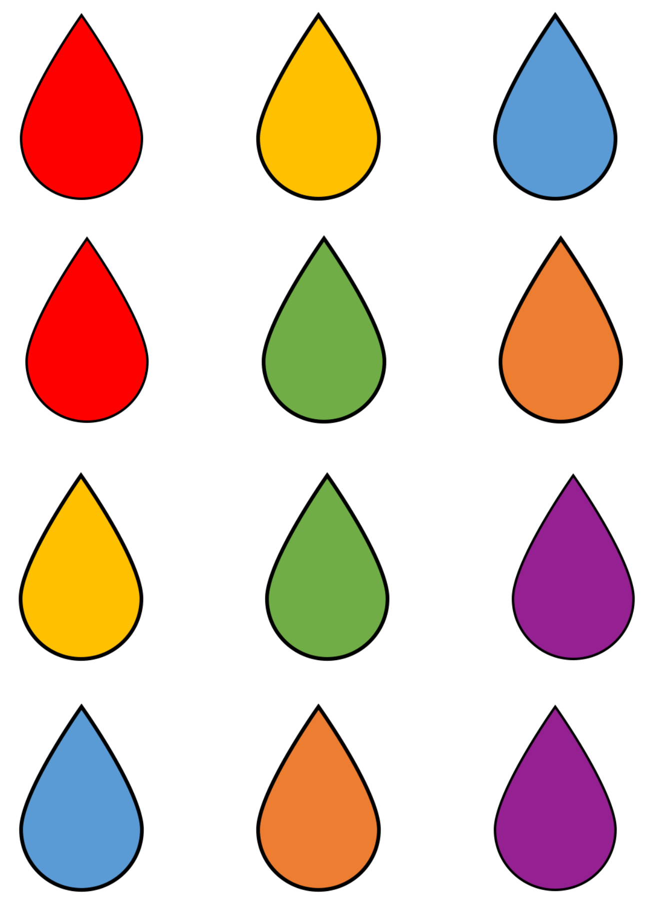
FAIL
FAIL
PASS
PASS

d – CFF(t, n)

No element is ***covered*** by the union of any other *d*.

Cover-Free Families

	1	2	3	4	5	6
Test 1	1	1	1	0	0	0
Test 2	1	0	0	1	1	0
Test 3	0	1	0	1	0	1
Test 4	0	0	1	0	1	1

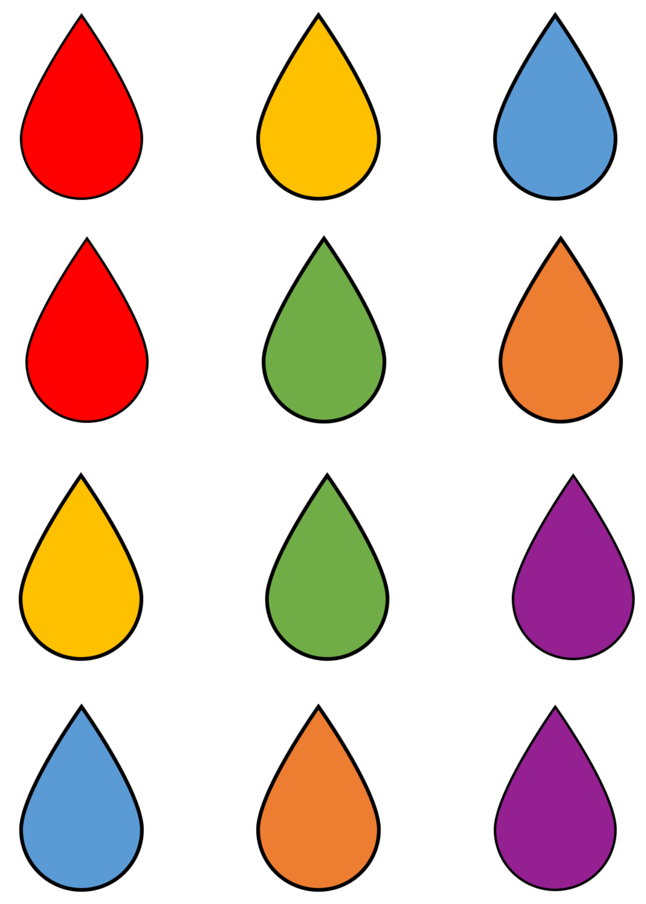


FAIL
FAIL
PASS
PASS

1 **– CFF(4, 6)**

Cover-Free Families

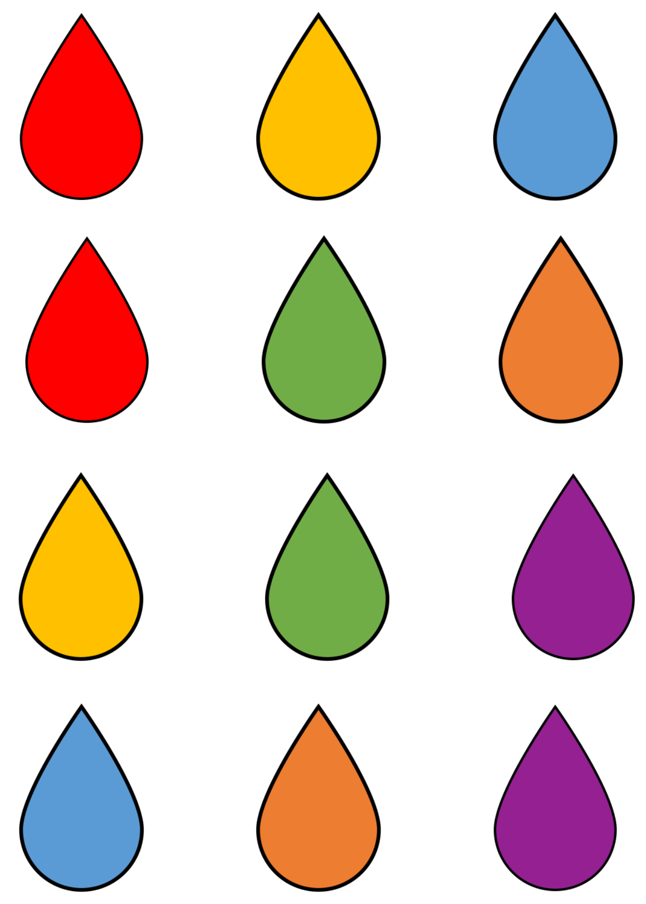
	1	2	3	4	5	6	
Test 1	1	1	1	0	0	0	FAIL
Test 2	1	0	0	1	1	0	FAIL
Test 3	0	1	0	1	0	1	PASS
Test 4	0	0	1	0	1	1	PASS



1 – CFF(4, 6)

Cover-Free Families

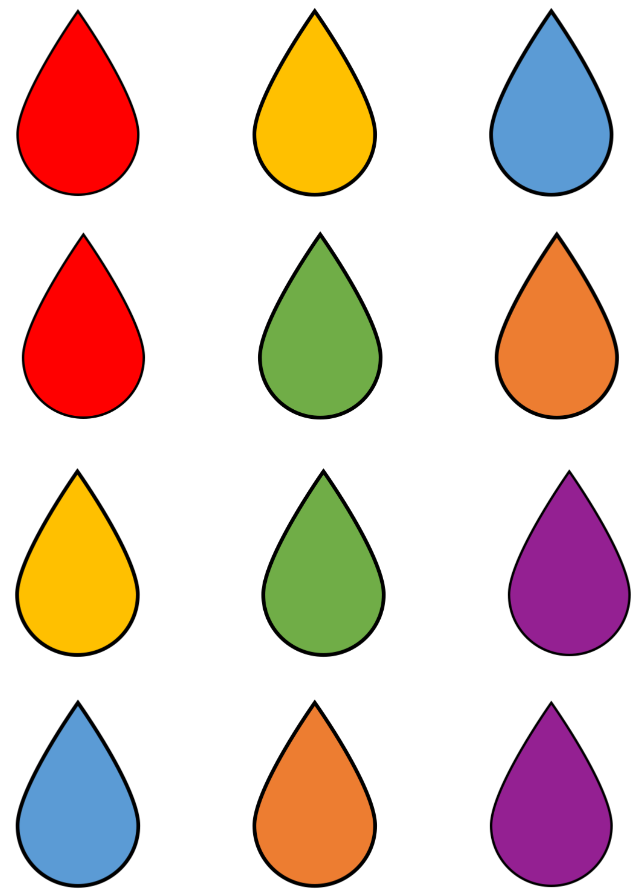
	1	2	3	4	5	6	
Test 1	1	1	1	0	0	0	FAIL
Test 2	1	0	0	1	1	0	FAIL
Test 3	0	1	0	1	0	1	PASS
Test 4	0	0	1	0	1	1	PASS



1 – CFF(4, 6)

Cover-Free Families

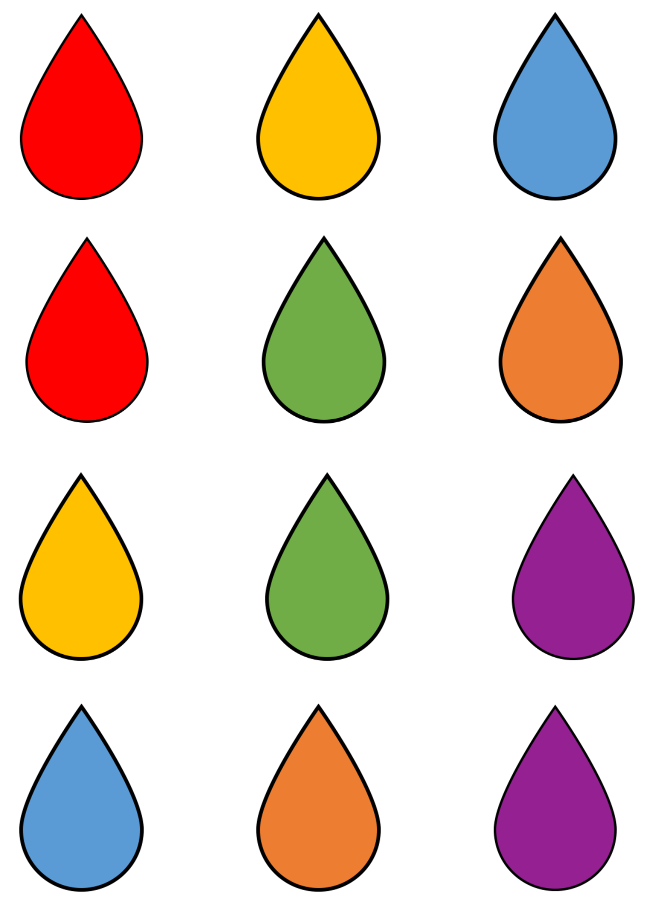
	1	2	3	4	5	6	
Test 1	1	1	1	0	0	0	FAIL
Test 2	1	0	0	1	1	0	FAIL
Test 3	0	1	0	1	0	1	PASS
Test 4	0	0	1	0	1	1	PASS



***1* – CFF(4, 6)**

Cover-Free Families

	1	2	3	4	5	6
Test 1	1	1	1	0	0	0
Test 2	1	0	0	1	1	0
Test 3	0	1	0	1	0	1
Test 4	0	0	1	0	1	1



FAIL

FAIL

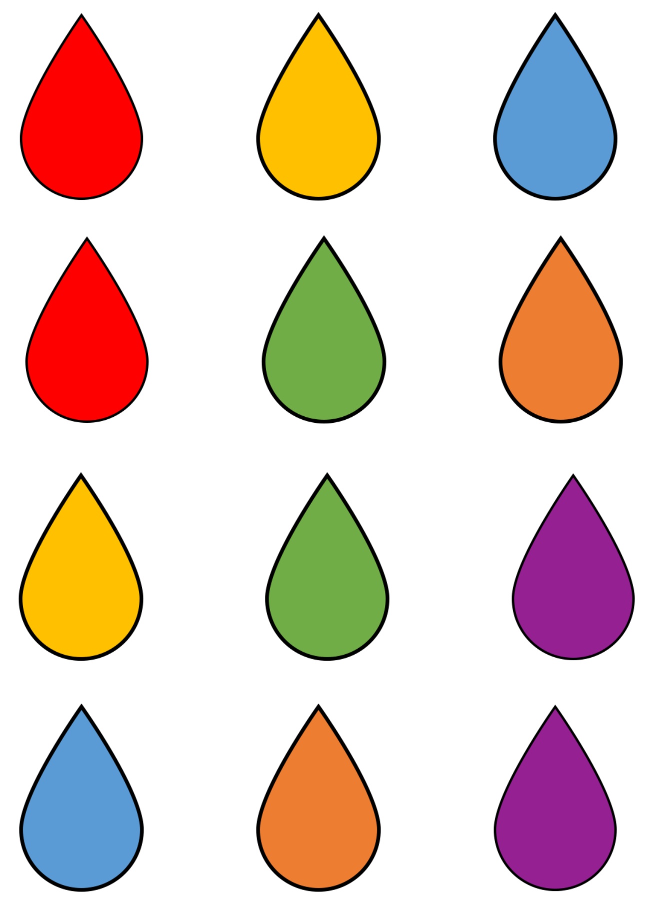
PASS

PASS

***1* – CFF(4, 6)**

Cover-Free Families

	1	2	3	4	5	6	Result
Test 1	1	1	1	0	0	0	FAIL
Test 2	1	0	0	1	1	0	FAIL
Test 3	0	1	0	1	0	1	PASS
Test 4	0	0	1	0	1	1	PASS



1 – CFF(4, 6)

Cover-free Families

	1	2	3	4	5	6	7	8	9	10	11	12
Test 1	1			1			1			1		
Test 2	1				1			1			1	
Test 3	1					1			1			1
Test 4		1		1					1		1	
Test 5		1			1		1					1
Test 6		1				1		1		1		
Test 7			1	1				1				1
Test 8			1		1				1	1		
Test 9			1			1	1				1	

2 - CFF(9, 12)

Cover-free Families

	1	2	3	4	5	6	7	8	9	10	11	12
Test 1	1			1			1			1		
Test 2	1				1			1			1	
Test 3	1					1			1			1
Test 4		1		1					1		1	
Test 5		1			1		1					1
Test 6		1				1		1		1		
Test 7			1	1				1				1
Test 8			1		1				1	1		
Test 9			1			1	1				1	

2 - CFF(9, 12)

Cover-Free Families

X

	B_1	B_2	B_3	B_4	B_5	B_6
1	1	1	1	0	0	0
2	1	0	0	1	1	0
3	0	1	0	1	0	1
4	0	0	1	0	1	1

Definition: Let d be a positive integer. A *d*-cover-free family, denoted $d - CFF(t, n)$, is a set system $\mathcal{F} = (X, \mathcal{B})$ with $|X| = t$ and $|\mathcal{B}| = n$ such that for any $d + 1$ subsets $B_{i_0}, B_{i_1}, \ldots, B_{i_d} \in \mathcal{B}$, we have:

$$\left| B_{i_0} \Big\backslash \left(\bigcup_{j=1}^{d} B_{i_j} \right) \right| \geq 1.$$

No element is ***covered*** by the union of any other d.

* Equivalent to disjunct matrices and superimposed codes.

Constructions of *d*-CFFs

n

t

1	1	1	0	0	0
1	0	0	1	1	0
0	1	0	1	0	1
0	0	1	0	1	1

- When ***d* = 1** we can use Sperner set systems, where *t* grows as $\log_2 n$ as $n \to \infty$;
- For $d \geq 2$, the best known **lower bound** on t for *d*-CFF(*t*, *n*) is given by

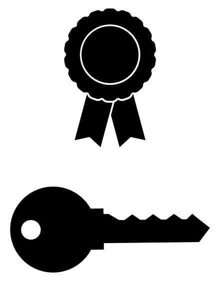
$$t \geq c \frac{d^2}{\log d} \log n$$

for some constant *c*;

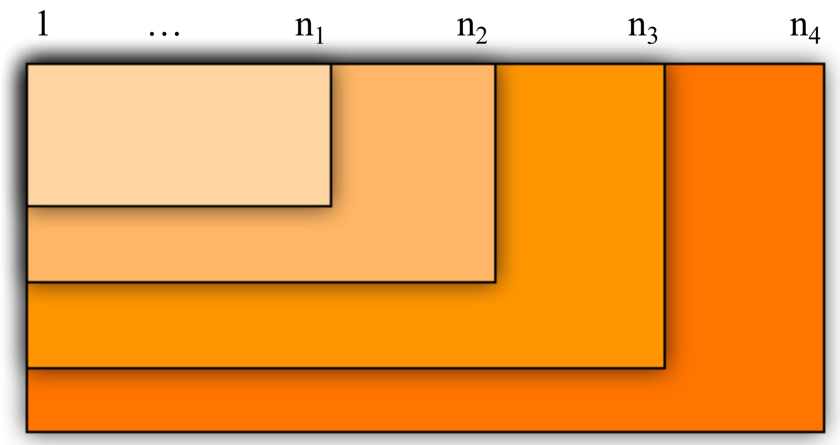
- Constructions based on Latin squares, OAs, PHFs, CAs, Codes, probabilistic algorithms, etc.
- **Constructions based on polynomials over finite fields.**

In this talk

1	1	1	0	0	0
1	0	0	1	1	0
0	1	0	1	0	1
0	0	1	0	1	1



- Applications of **cover-free families** in **cryptography**
- Cover-free families for ***dynamic applications***
- Embedding cover-free families with ***Finite Fields***
- Open problems



Cover-Free families

Applications in cryptography

- **Fault-tolerant Digital Signatures**
  - Fault-tolerant digital signatures
    - Idalino, Moura, Custodio, **Panario** (2015), Idalino, Moura, Adams, (2019)
  - Fault-tolerance in aggregation of signatures
    - Zaverucha, Stinson (2010). Idalino (2015). Hartung, Kaidel, Koch, Koch, Rupp (2016). Idalino, Moura (2018, 2021)
  - Fault-tolerance in batch verification
    - Pastuszak, Pieprzyk (2000). Zaverucha, Stinson (2009).
- **Post-quantum one-time and multiple-times signature schemes**
  - Pieprzyk, Wang, Xing (2003). Zaverucha and Stinson, (2011). Kalach and Safavi-Naini (2016).
- **Key distribution**
  - Key distribution patterns
    - Mitchell and Piper (1988)
  - Broadcast authentication
    - Safavi-Naini and Wang (1998) . Ling, Wang, Xing (2007).
  - Broadcast encryption
    - Gafni, Staddon, Yin (1999). D'Arco and Stinson (2003)
  - Traitor Tracing
    - Stinson and Wei (1998). Tonien and Safavi-Naini (2006)
- and many many others..

Cover-Free families

Applications in cryptography

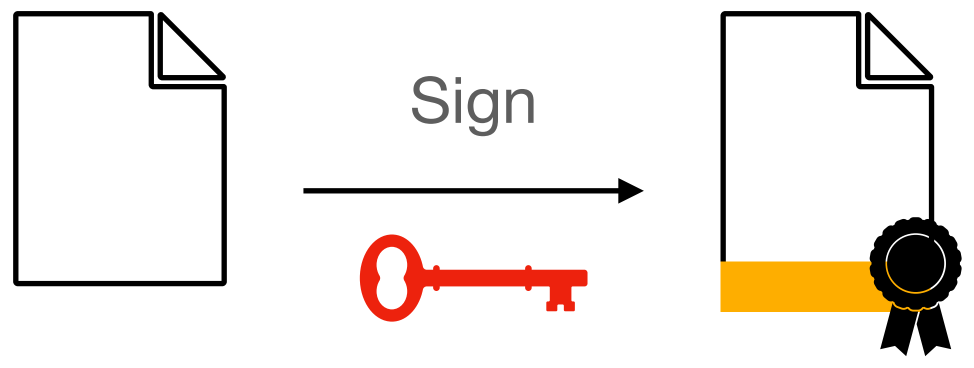
- **Fault-tolerant Digital Signatures**
  - Fault-tolerant digital signatures
    - Idalino, Moura, Custodio, **Panario** (2015), Idalino, Moura, Adams, (2019)
  - Fault-tolerance in aggregation of signatures
    - Zaverucha, Stinson (2010). Idalino (2015). Hartung, Kaidel, Koch, Koch, Rupp (2016). Idalino, Moura (2018, 2021)
  - Fault-tolerance in batch verification
    - Pastuszak, Pieprzyk (2000). Zaverucha, Stinson (2009).
- **Post-quantum one-time and multiple-times signature schemes**
  - Pieprzyk, Wang, Xing (2003). Zaverucha and Stinson, (2011). Kalach and Safavi-Naini (2016).
- **Key distribution**
  - Key distribution patterns
    - Mitchell and Piper (1988)
  - Broadcast authentication
    - Safavi-Naini and Wang (1998) . Ling, Wang, Xing (2007).
  - Broadcast encryption
    - Gafni, Staddon, Yin (1999). D'Arco and Stinson (2003)
  - Traitor Tracing
    - Stinson and Wei (1998). Tonien and Safavi-Naini (2006)
- and many many others..

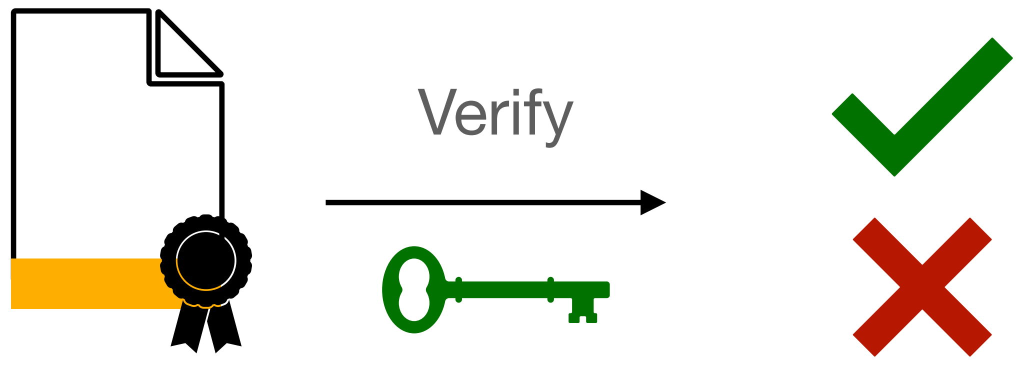
More applications and details:
IDALINO, T. B.; MOURA, L., A Survey of Cover-Free Families: Constructions, Applications, and Generalizations. New Advances in Designs, Codes and Cryptography. 86 (2024),

Applications in Cryptography

Digital Signatures

- Integrity and authenticity of digital documents





Applications in Cryptography

Digital Signatures

- Aggregation of signatures

Applications in Cryptography

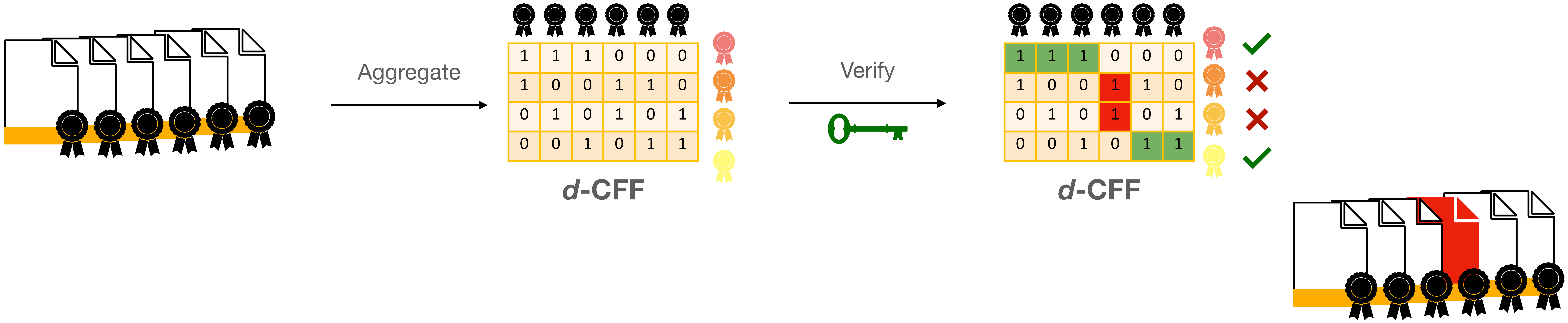
Digital Signatures

- Aggregation of signatures

Applications in Cryptography

Digital Signatures

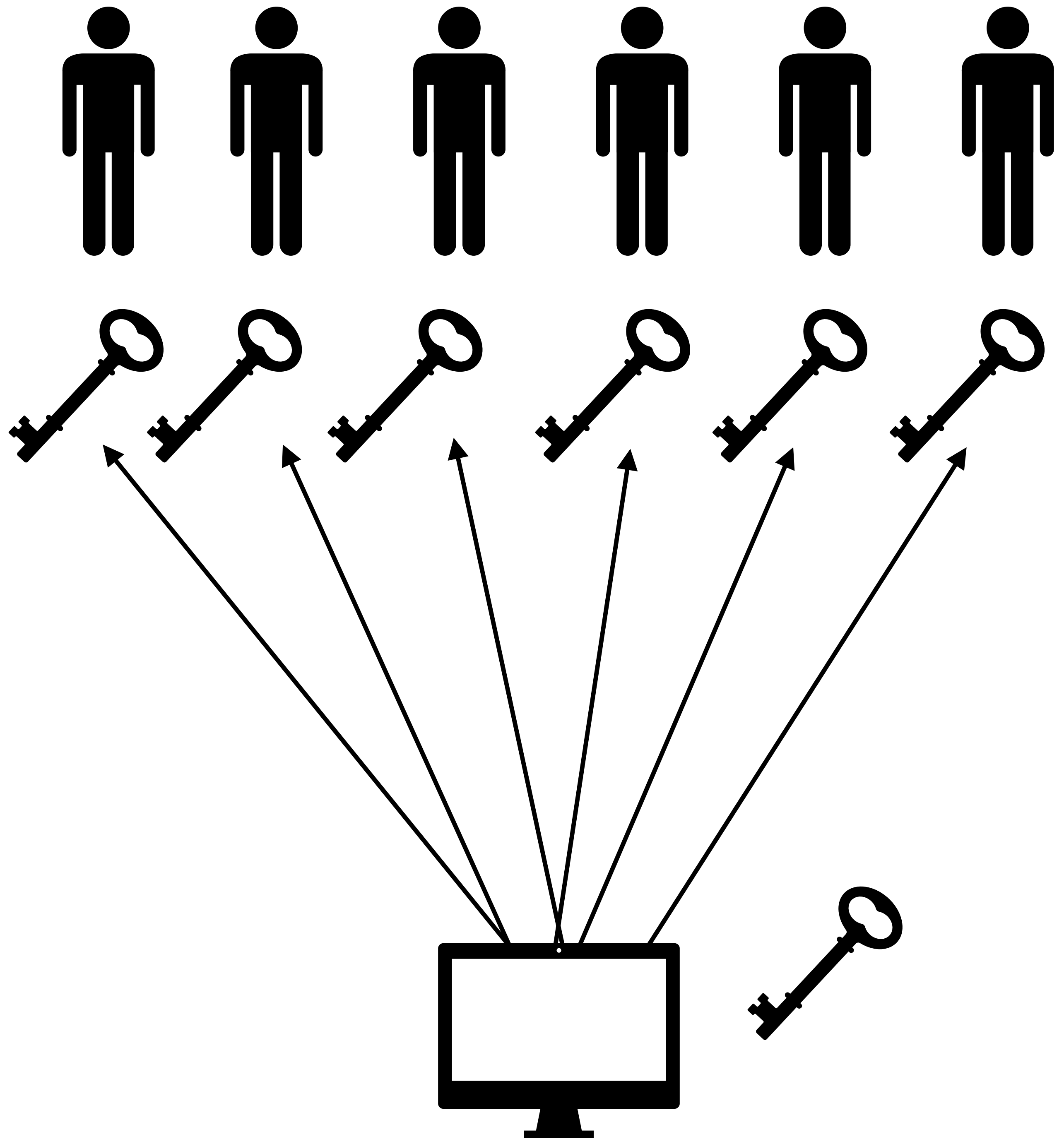
- Identify invalid digital signatures for batch verification and aggregation of signatures.
  - Zaverucha, Stinson (2010). Idalino (2015). Hartung, Kaidel, Koch, Koch, Rupp (2016). Idalino, Moura (2018, 2021).



Applications in Cryptography

Key Distribution

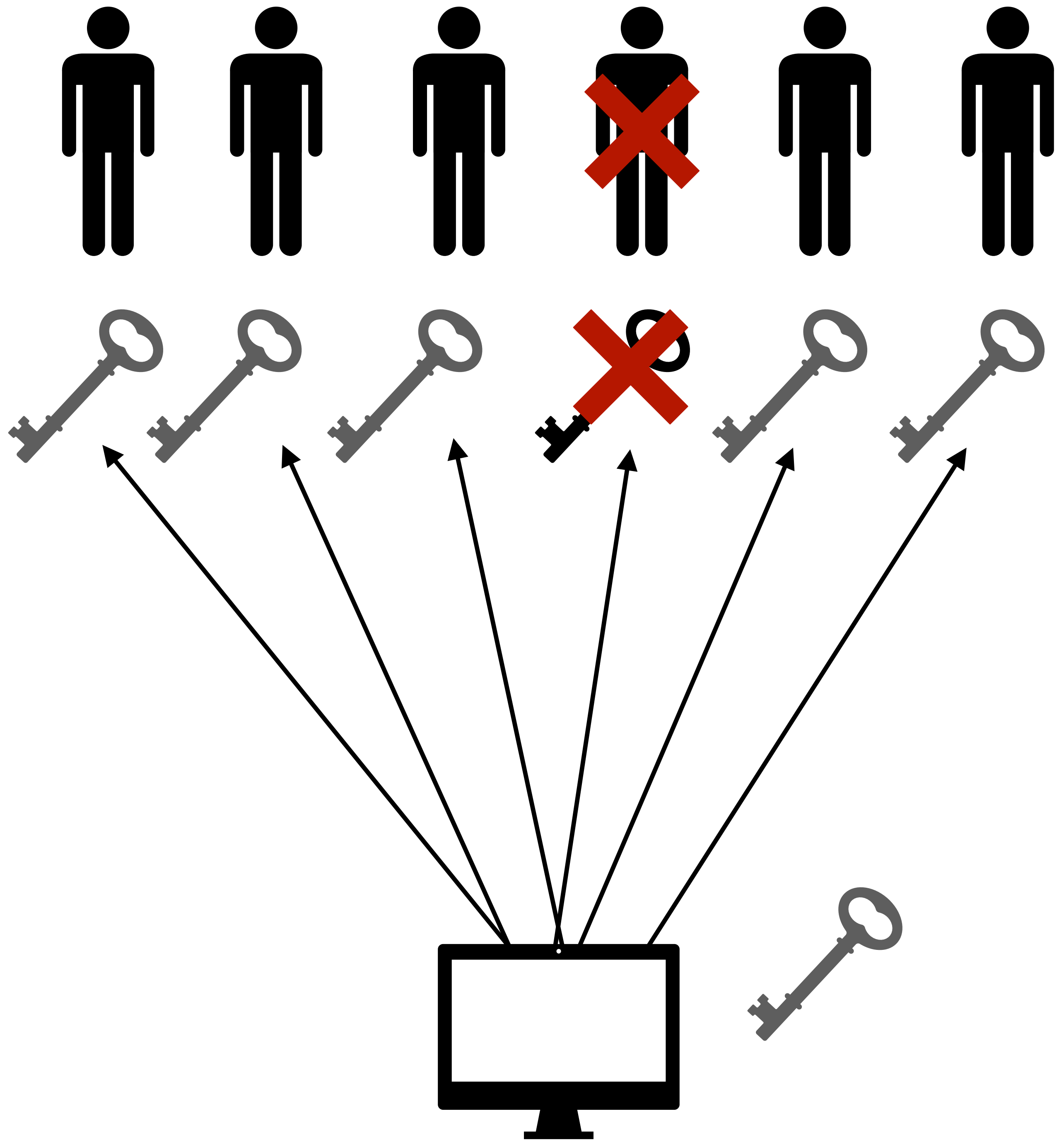
- Broadcast encryption:
  - server broadcasts encrypted content
  - all active subscribers should be able to decrypt it



Applications in Cryptography

Key Distribution

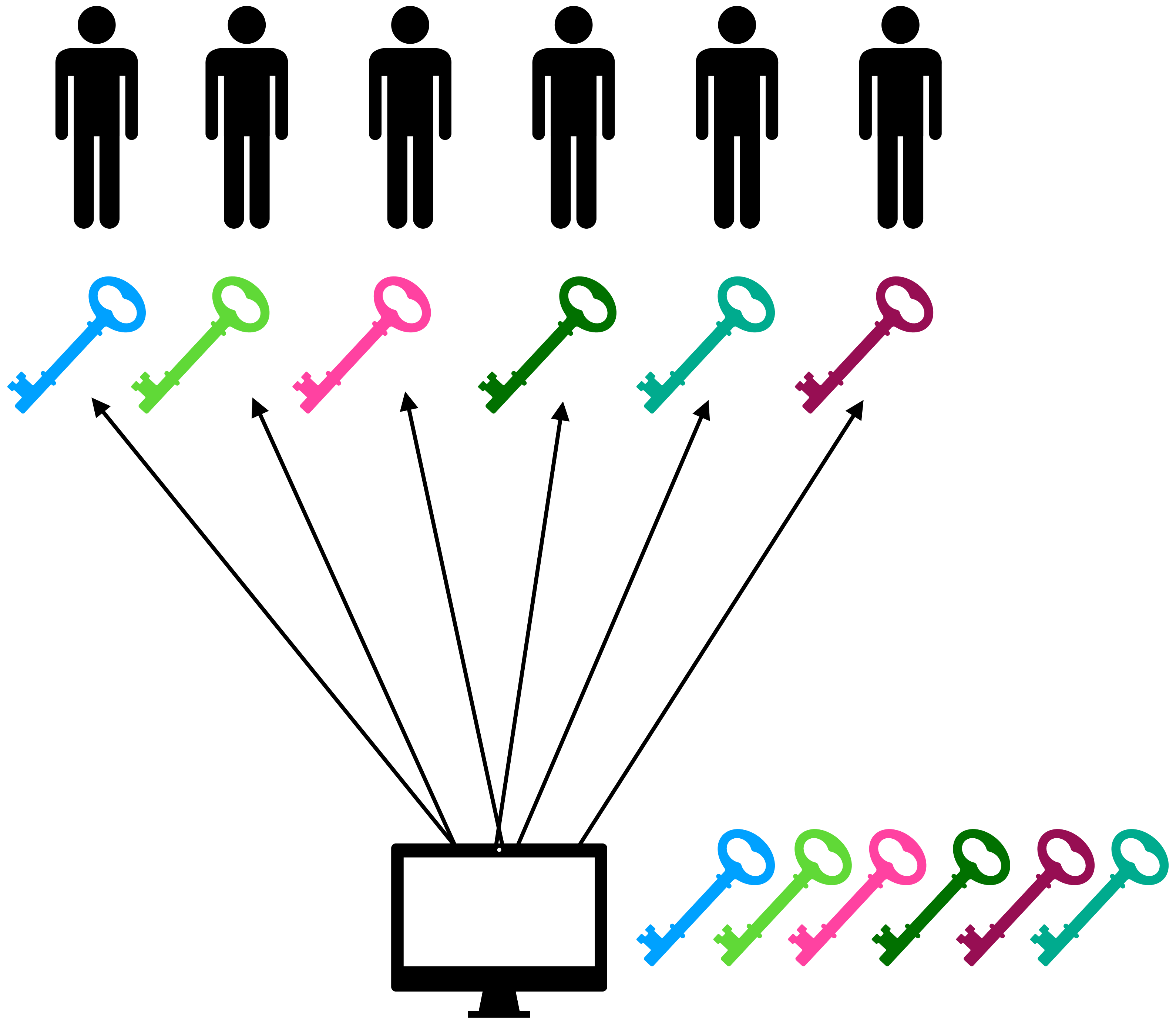
- Broadcast encryption:
  - server broadcasts encrypted content
  - only active subscribers should be able to decrypt it



Applications in Cryptography

Key Distribution

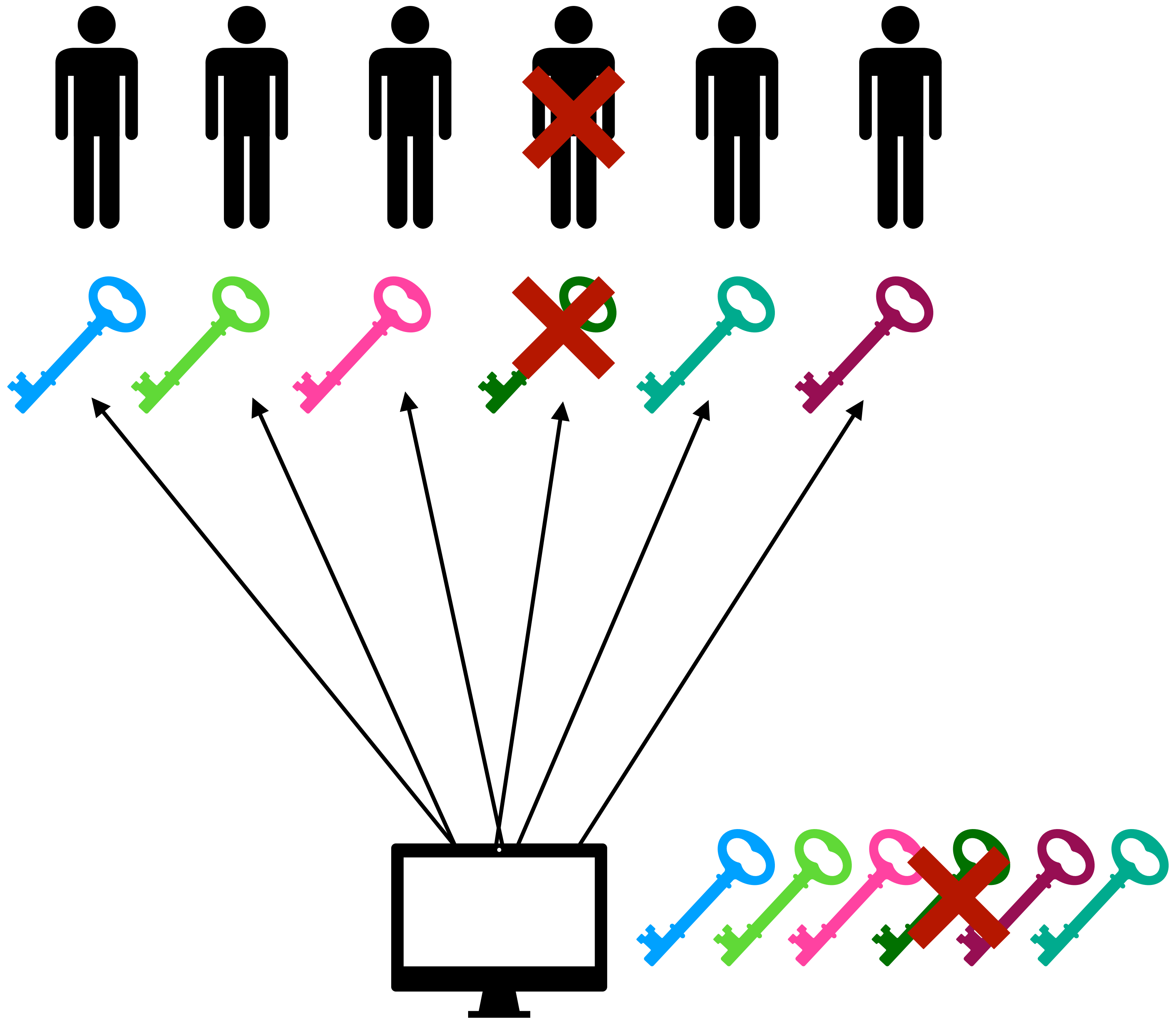
- Broadcast encryption:
  - server broadcasts encrypted content
  - only active subscribers should be able to decrypt it



Applications in Cryptography

Key Distribution

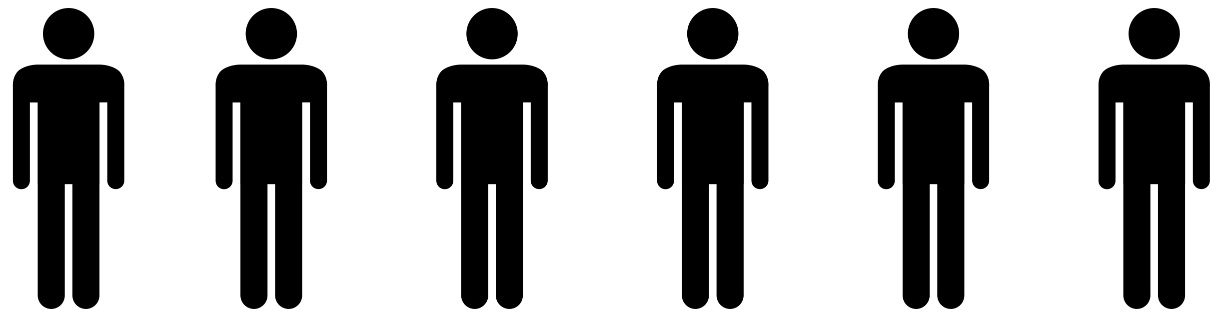
- Broadcast encryption:
  - server broadcasts encrypted content
  - only active subscribers should be able to decrypt it



Applications in Cryptography

Key Distribution

- Tolerance to “bad” participants with less keys.
  - Safavi-Naini and Wang (1998). Gafni, Staddon, Yin (1999). D’Arco and Stinson (2003).

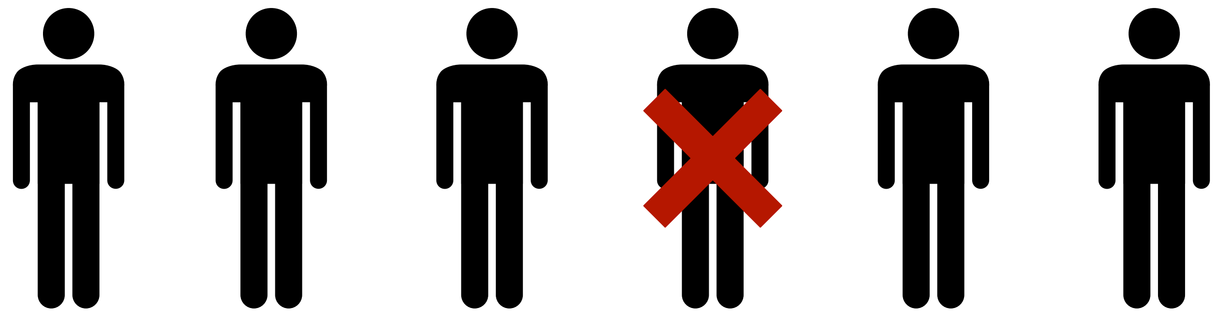


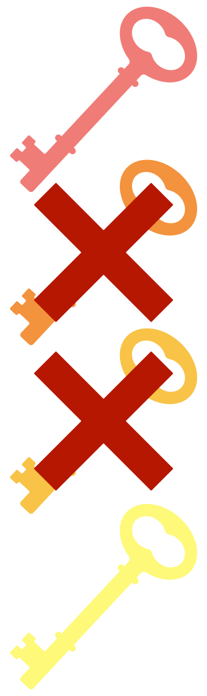
1	1	1	0	0	0
1	0	0	1	1	0
0	1	0	1	0	1
0	0	1	0	1	1

Applications in Cryptography

Key Distribution

- Tolerance to “bad” participants with less keys.
  - Safavi-Naini and Wang (1998). Gafni, Staddon, Yin (1999). D’Arco and Stinson (2003).



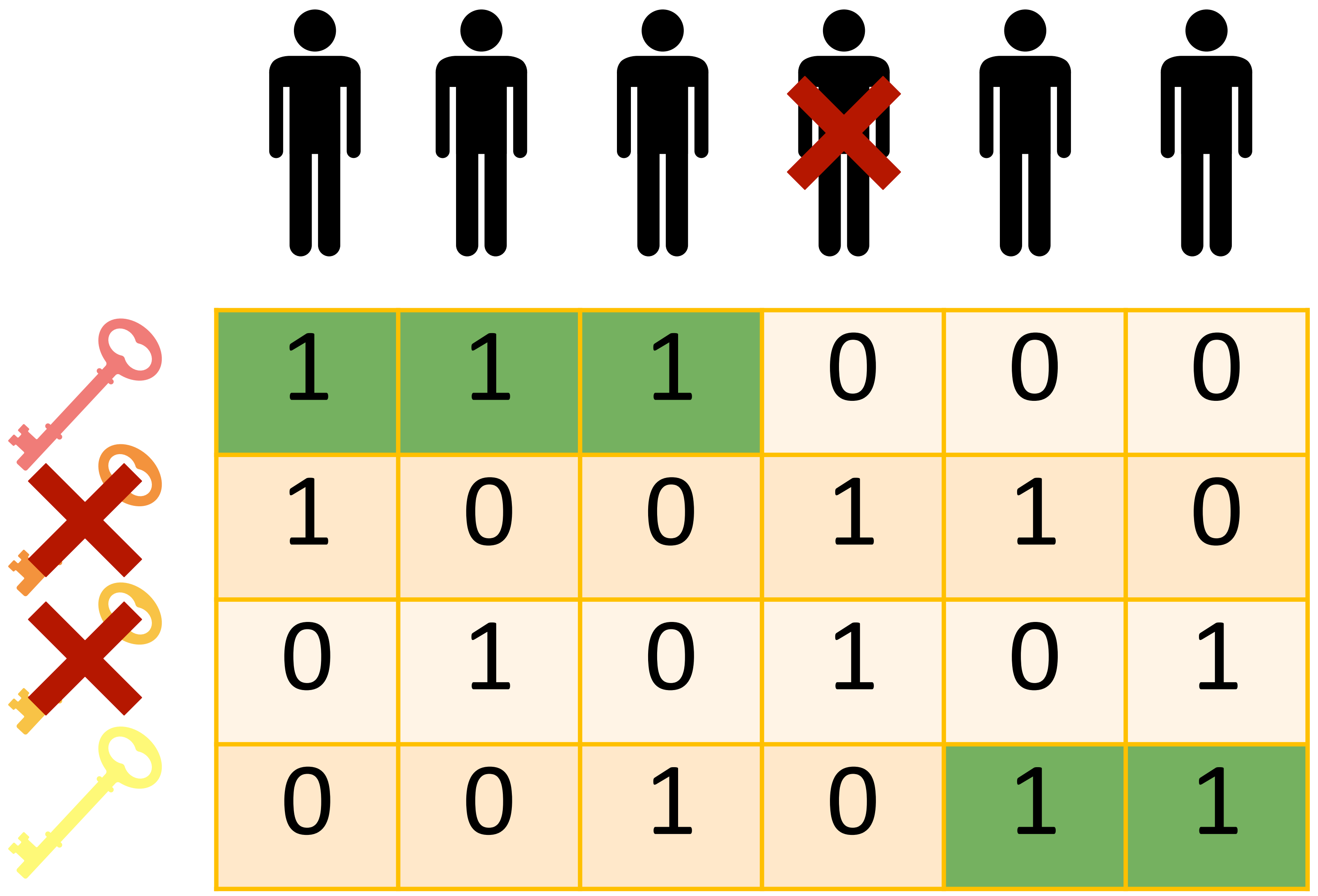


1	1	1	0	0	0
1	0	0	1	1	0
0	1	0	1	0	1
0	0	1	0	1	1

Applications in Cryptography

Key Distribution

- Tolerance to “bad” participants with less keys.
  - Safavi-Naini and Wang (1998). Gafni, Staddon, Yin (1999). D’Arco and Stinson (2003).



1	1	1	0	0	0
1	0	0	1	1	0
0	1	0	1	0	1
0	0	1	0	1	1

Dynamic applications

1	1	1	0	0	0
1	0	0	1	1	0
0	1	0	1	0	1
0	0	1	0	1	1

1	1	1	0	0	0
1	0	0	1	1	0
0	1	0	1	0	1
0	0	1	0	1	1

Dynamic applications

1	1	1	0	0	0
1	0	0	1	1	0
0	1	0	1	0	1
0	0	1	0	1	1

1	1	1	0	0	0
1	0	0	1	1	0
0	1	0	1	0	1
0	0	1	0	1	1

Dynamic applications

1	1	1	0	0	0
1	0	0	1	1	0
0	1	0	1	0	1
0	0	1	0	1	1

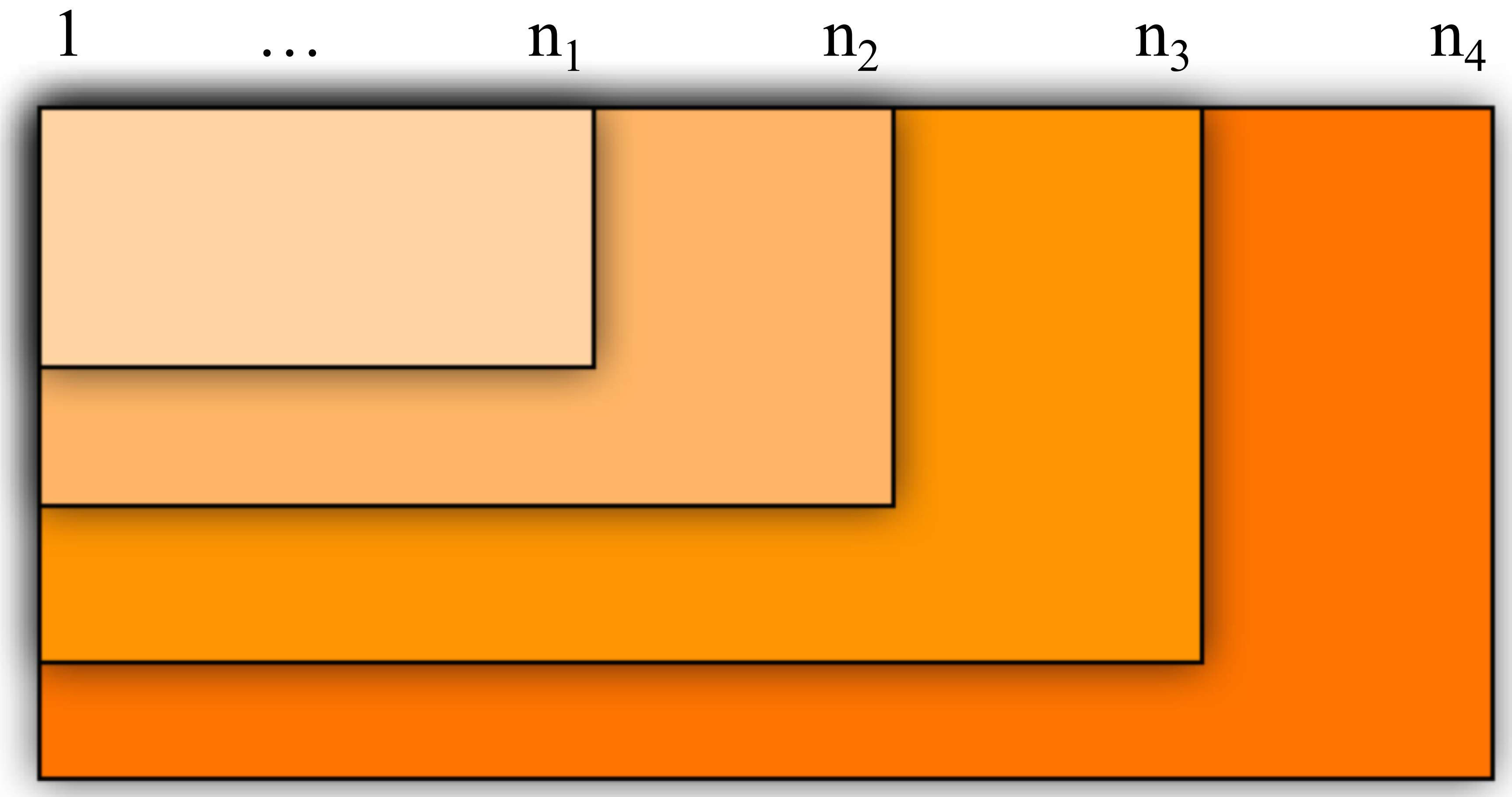
1	1	1	0	0	0
1	0	0	1	1	0
0	1	0	1	0	1
0	0	1	0	1	1

Dynamic applications

1	1	1	0	0	0
1	0	0	1	1	0
0	1	0	1	0	1
0	0	1	0	1	1

1	1	1	0	0	0
1	0	0	1	1	0
0	1	0	1	0	1
0	0	1	0	1	1

We need unbounded CFFs!



Unbounded CFFs

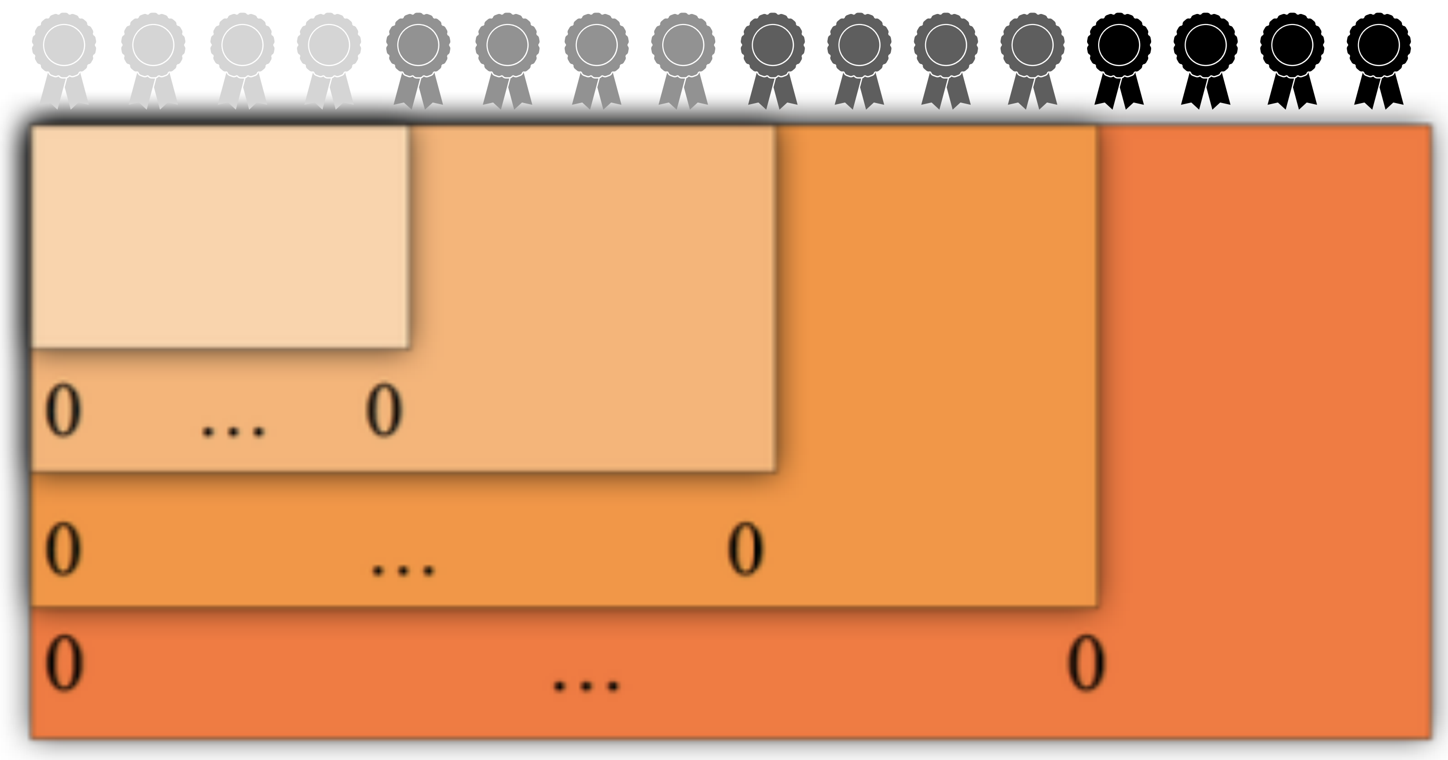
Approaches

- Unbounded approaches
  - Monotone (Hartung et al., 2016)
  - Nested (Idalino, Moura, 2018, 2021)
  - **Embedding** (Idalino, Moura, 2019)
- Compression Ratio: $\rho(n)$ iff n/t is $\Theta(\rho(n))$

Unbounded CFFs

Monotone Families

- Allows increase of *n* with fixed *d*.
- Rows of 0 required for aggregation of signatures.
- ρ(n) = 1 (number of rows is linear in n).

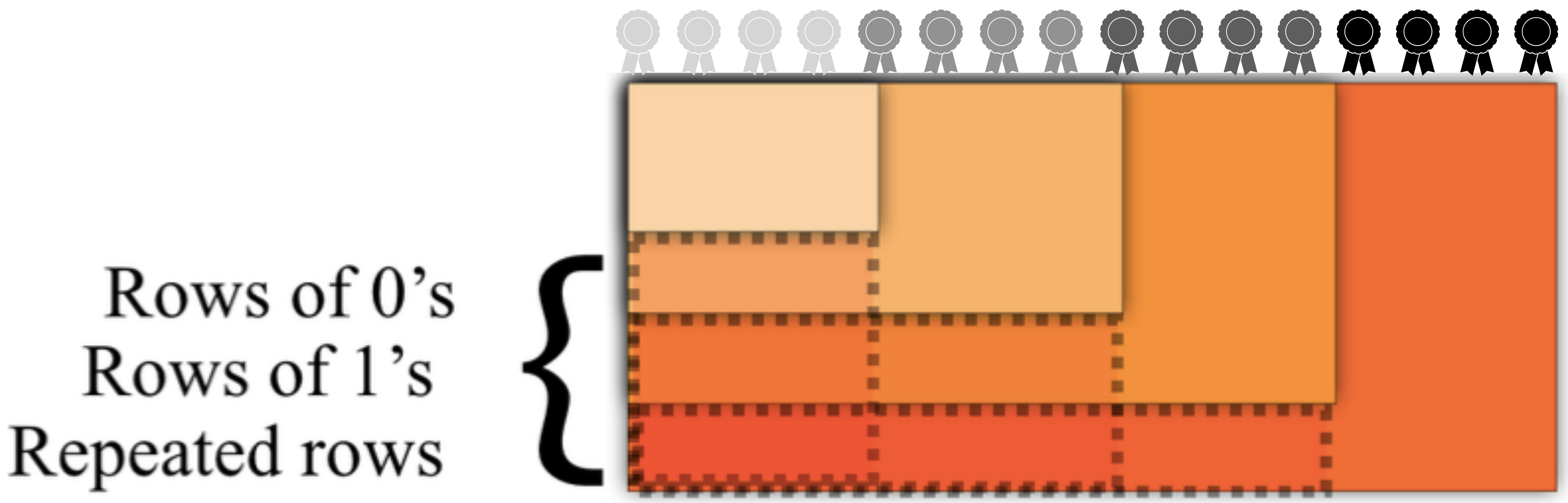


G. Hartung, B. Kaidel, A. Koch, J. Koch, A. Rupp, PKC 2016.

Unbounded CFFs

Nested Families

- Allows increase of n with fixed d.
- Applicable to aggregation of signatures.
- More flexible construction.
- Constructions with increasing compression ratio.



T. B. Idalino, L. Moura, IWOCA 2018.
T. B. Idalino, L. Moura, TCS 2021.

Unbounded CFFs

Embedding Families

- Increase of both n and d.
- Application in key distribution, etc.
- Construction of embedding families using polynomials over finite fields.

	d	n
d-CFFs	fixed	fixed
Monotone	fixed	increasing
Nested	fixed	increasing
Embedding	**increasing**	**increasing**

T. B. Idalino, L. Moura, ACM 2019.

Building CFFs with polynomials

Theorem (E, F, F 1985*): Let q be a prime power and k be a positive integer. If $q \geq dk + 1$ then there exists a d-CFF(q^2, q^{k+1}).

Example: $q = 3, k = 1$

polynomials of degree at most k over $\mathbb{F}_q$

$(\mathbb{F}_q, \mathbb{F}_q)$

	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
$(0,0)$	1	0	0	1	0	0	1	0	0
$(0,1)$	0	1	0	0	1	0	0	1	0
$(0,2)$	0	0	1	0	0	1	0	0	1
$(1,0)$	1	0	0	0	0	1	0	1	0
$(1,1)$	0	1	0	1	0	0	0	0	1
$(1,2)$	0	0	1	0	1	0	1	0	0
$(2,0)$	1	0	0	0	1	0	0	0	1
$(2,1)$	0	1	0	0	0	1	1	0	0
$(2,2)$	0	0	1	1	0	0	0	1	0

f(2) = 0

* P. Erdős, P. Frankl and Z. Furedi, Families of finite sets in which no set is covered by the union of r others, Israel J. Math., 51 (1985), 79–89.

Building CFFs with polynomials

Theorem (E, F, F 1985*): Let q be a prime power and k be a positive integer. If $q \geq dk + 1$ then there exists a d-CFF(q^2, q^{k+1}).

Example: $q = 3, k = 1$

polynomials of degree at most k over $\mathbb{F}_q$

$(\mathbb{F}_q, \mathbb{F}_q)$

	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
$(0,0)$	1	0	0	1	0	0	1	0	0
$(0,1)$	0	1	0	0	1	0	0	1	0
$(0,2)$	0	0	1	0	0	1	0	0	1
$(1,0)$	1	0	0	0	0	1	0	1	0
$(1,1)$	0	1	0	1	0	0	0	0	1
$(1,2)$	0	0	1	0	1	0	1	0	0
$(2,0)$	1	0	0	0	1	0	0	0	1
$(2,1)$	0	1	0	0	0	1	1	0	0
$(2,2)$	0	0	1	1	0	0	0	1	0

$$d \leq \frac{q-1}{k} = 2$$

2-CFF$(9,9)$

* P. Erdős, P. Frankl and Z. Furedi, Families of finite sets in which no set is covered by the union of r others, Israel J. Math., 51 (1985), 79–89.

Building CFFs with polynomials

Why is this a d-CFF(q^2, q^{k+1})?

- Any two columns will be in at most *k* tests together.
- The union of *d* columns will be in at most *dk* tests together with any other column.
  - Recall that each column has *q* 1's and $q \geq$ *dk* + *1* .
  - Therefore, no column is covered by the union of *d* others.

Building CFFs with polynomials

Theorem (E, F, F 1985*): Let q be a prime power and k be a positive integer. If $q \geq dk + 1$ then there exists a d-CFF(q^2, q^{k+1}).

Example: $q = 3, k = 1$

polynomials of degree at most k over $\mathbb{F}_q$

$(\mathbb{F}_q, \mathbb{F}_q)$

	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
$(0,0)$	1	0	0	1	0	0	1	0	0
$(0,1)$	0	1	0	0	1	0	0	1	0
$(0,2)$	0	0	1	0	0	1	0	0	1
$(1,0)$	1	0	0	0	0	1	0	1	0
$(1,1)$	0	1	0	1	0	0	0	0	1
$(1,2)$	0	0	1	0	1	0	1	0	0
$(2,0)$	1	0	0	0	1	0	0	0	1
$(2,1)$	0	1	0	0	0	1	1	0	0
$(2,2)$	0	0	1	1	0	0	0	1	0

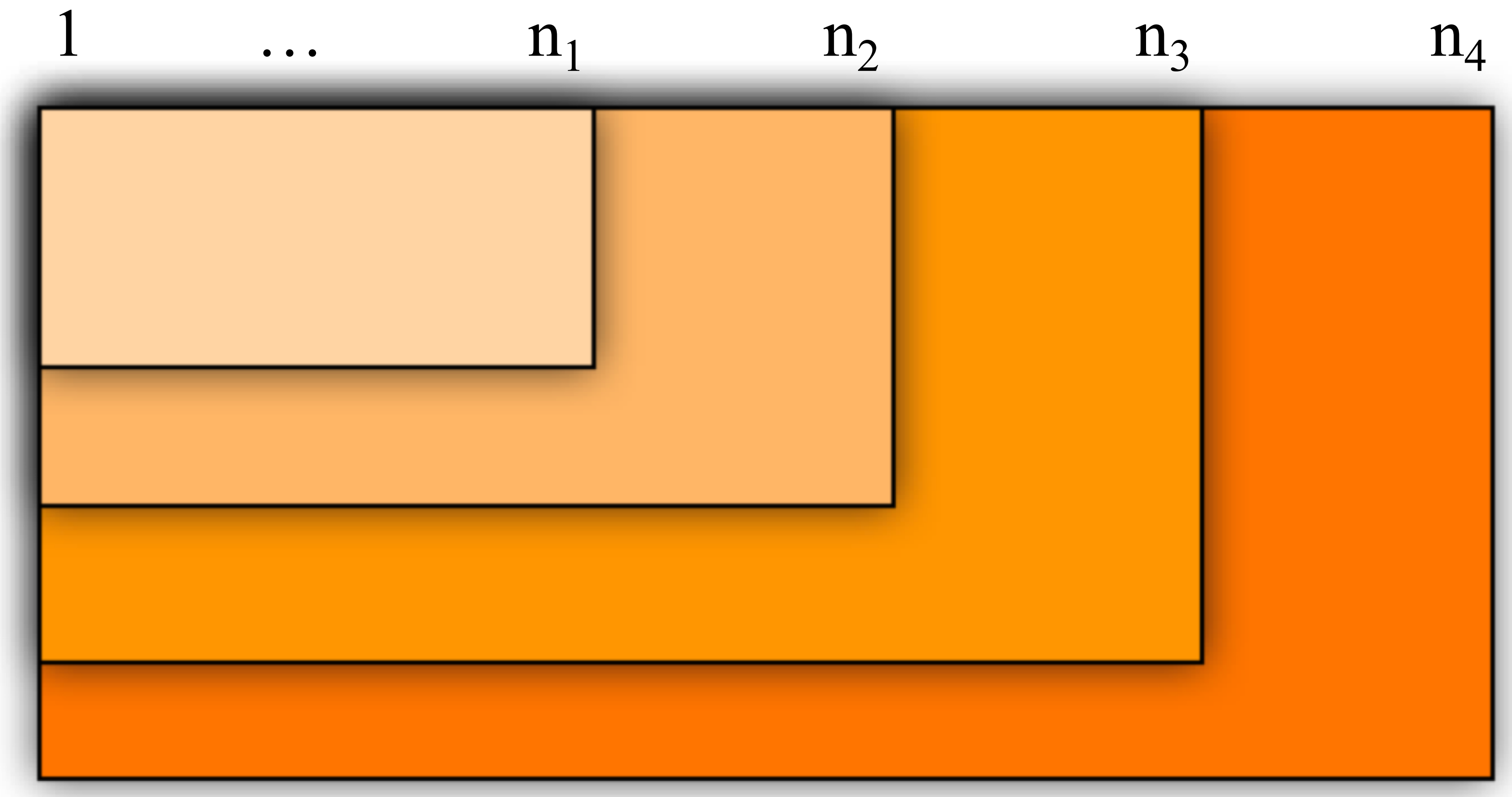
0-CFF(3,9)

1-CFF(6,9)

2-CFF(9,9)

Obs.: We only need q^2 rows when we are interested in the max *d*. For smaller values of *d* we need $t = (dk+1)q$

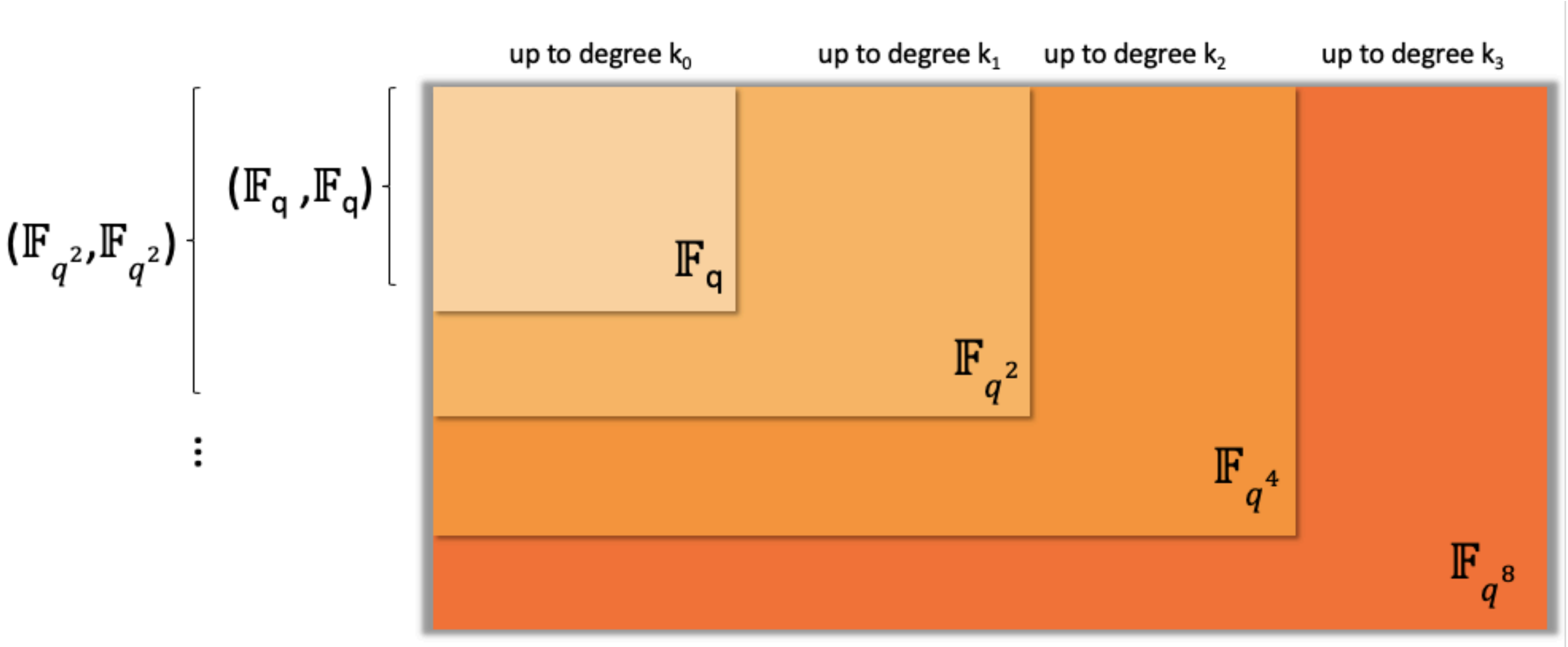
How can we build embedding CFFs?



Embedding cover-free families

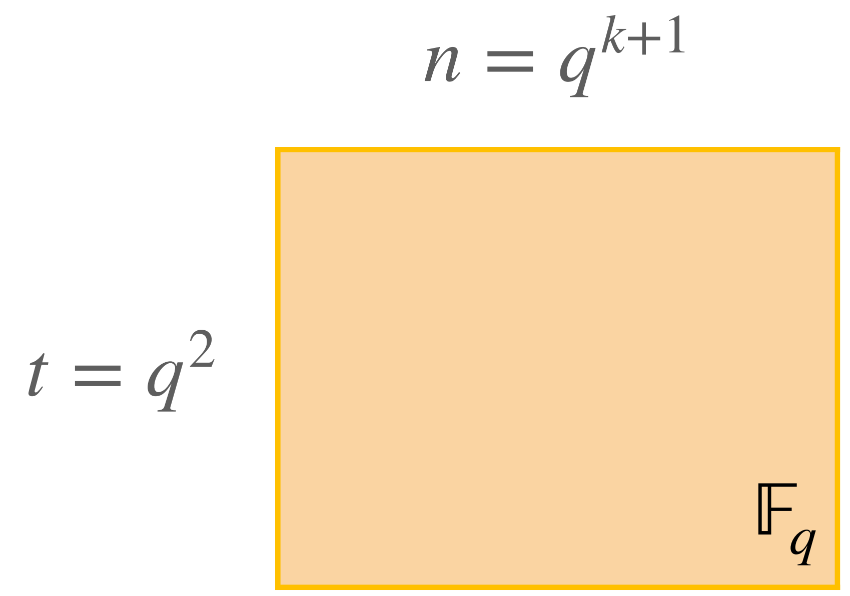
Construction

- Start with $\mathbb{F}_q$ and grow the construction with extension fields.
  - Tower of finite fields.

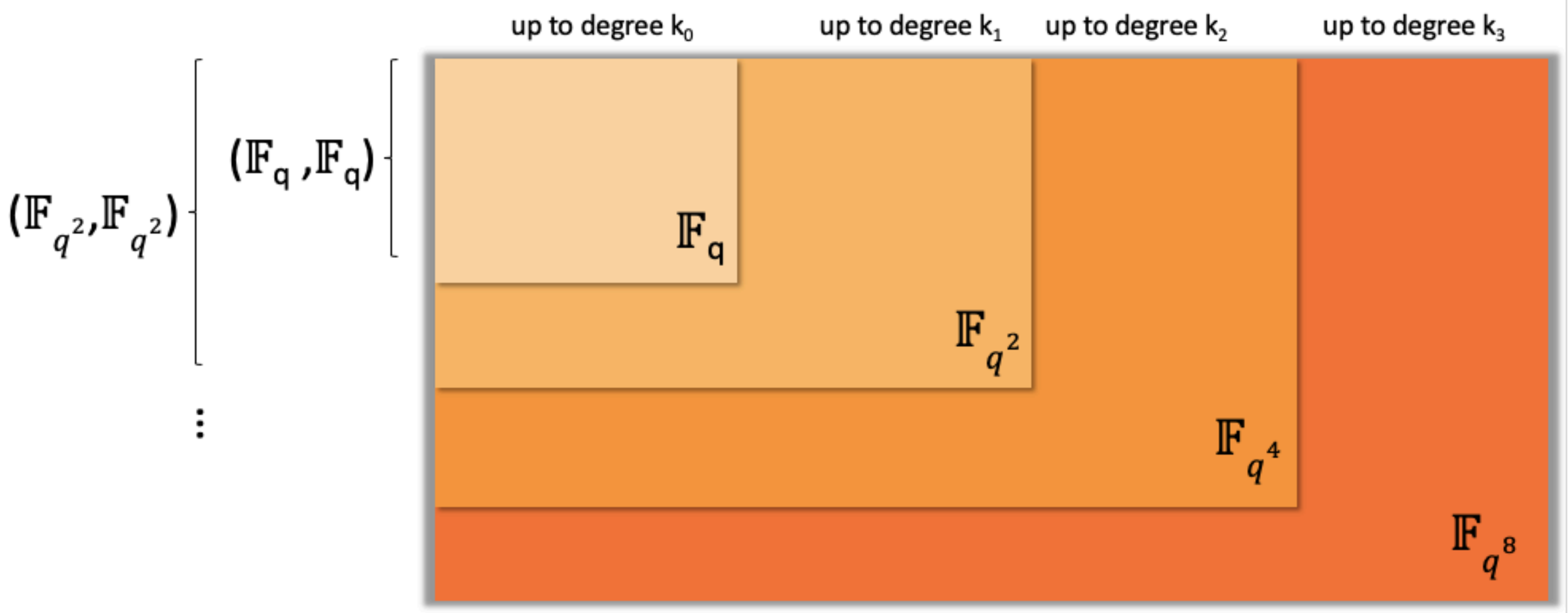


Embedding cover-free families

Construction



- Start with prime power q;
- consider a sequence of extension fields $\mathbb{F}_{q^{2^i}}$, with $i \geq 0$;
  - and integers k_i, d_i, for $q^{2^i} \geq d_i k_i + 1$.
- We get a sequence of CFFs with increasing *n* and *d*.



Embedding cover-free families

Example

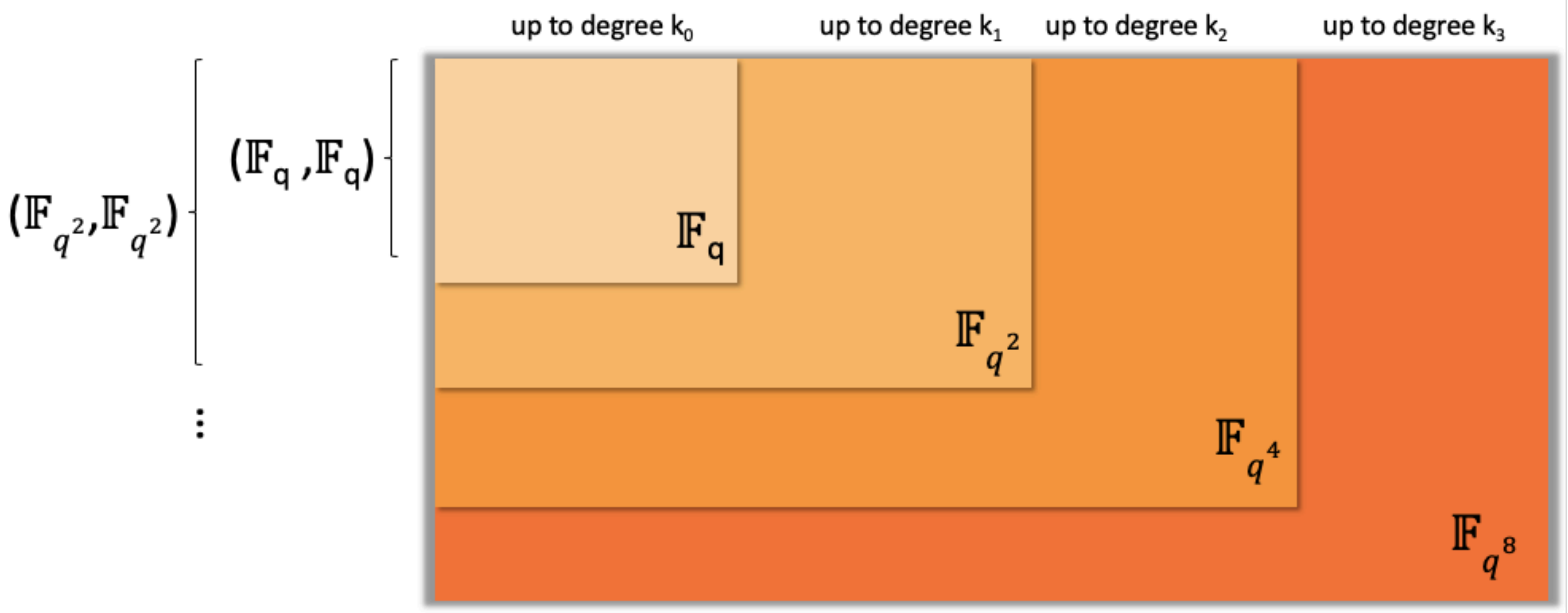
- Start with a 2-CFF$(9{,}9)$ over $\mathbb{F}_3$
  - $q = 3, d = 2, k = 1$
- Now consider $\mathbb{F}_9$
  - $q^2 = 9, d_1 = 4$ and $k_1 = 2$ (since $9 \geq 4 \times 2 + 1$)
- We get a 2-CFF$(9{,}9)$ embedded into a 4-CFF$(81{,}729)$

	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$	α	$\alpha+1$	$\dots$	$(2\alpha+2)x^2+$ $(2\alpha+2)x+$ $2\alpha+2$
$(0,0)$	1	0	0	1	0	0	1	0	0				
$(0,1)$	0	1	0	0	1	0	0	1	0				
$(0,2)$	0	0	1	0	0	1	0	0	1				
$(1,0)$	1	0	0	0	0	1	0	1	0				
$(1,1)$	0	1	0	1	0	0	0	0	1				
$(1,2)$	0	0	1	0	1	0	1	0	0				
$(2,0)$	1	0	0	0	1	0	0	0	1			$\dots$	
$(2,1)$	0	1	0	0	0	1	1	0	0				
$(2,2)$	0	0	1	1	0	0	0	1	0				
$\vdots$						$\dots$							
$(2\alpha+2, 2\alpha+2)$	0	0	0	1	0			$\dots$					

Embedding cover-free families

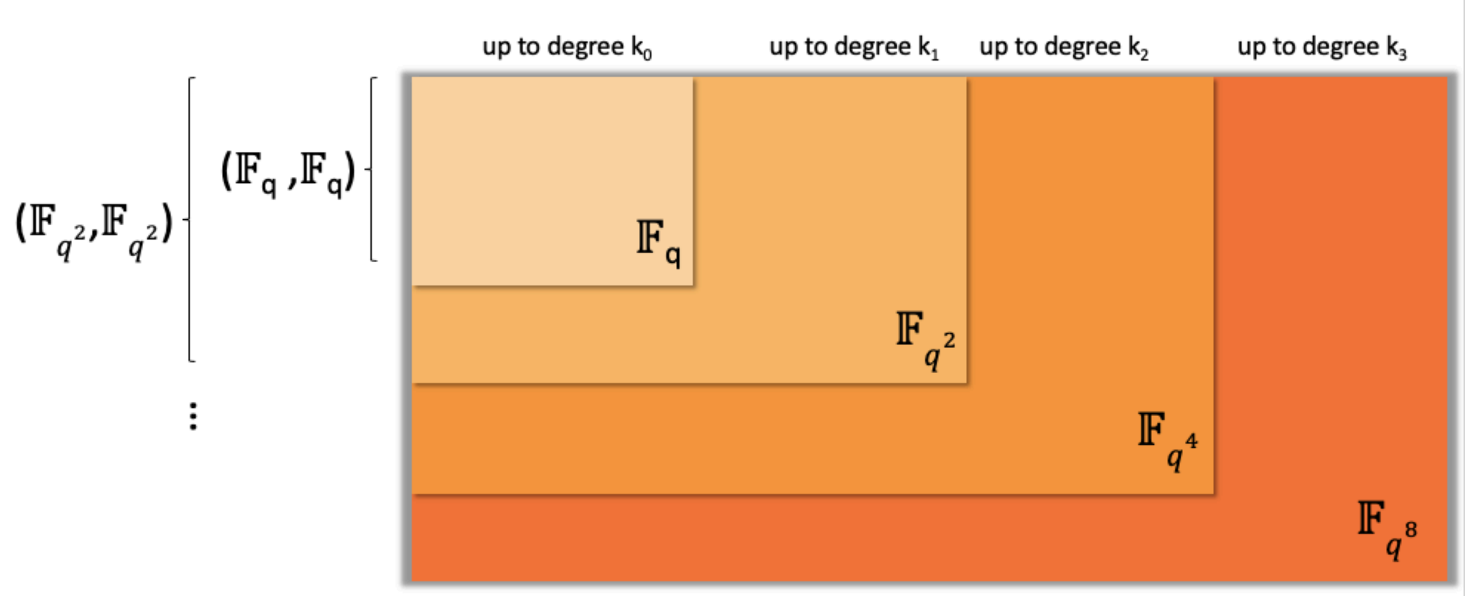
Many approaches with one construction

- Consider q^{2^i}, k_i, d_i, for $q^{2^i} \geq d_i k_i + 1$
  - Prioritize *d* increases (fix *k*)
  - Prioritize ratio increases (fix *d*)
  - Construct monotone families



Embedding cover-free families

Prioritize d increases



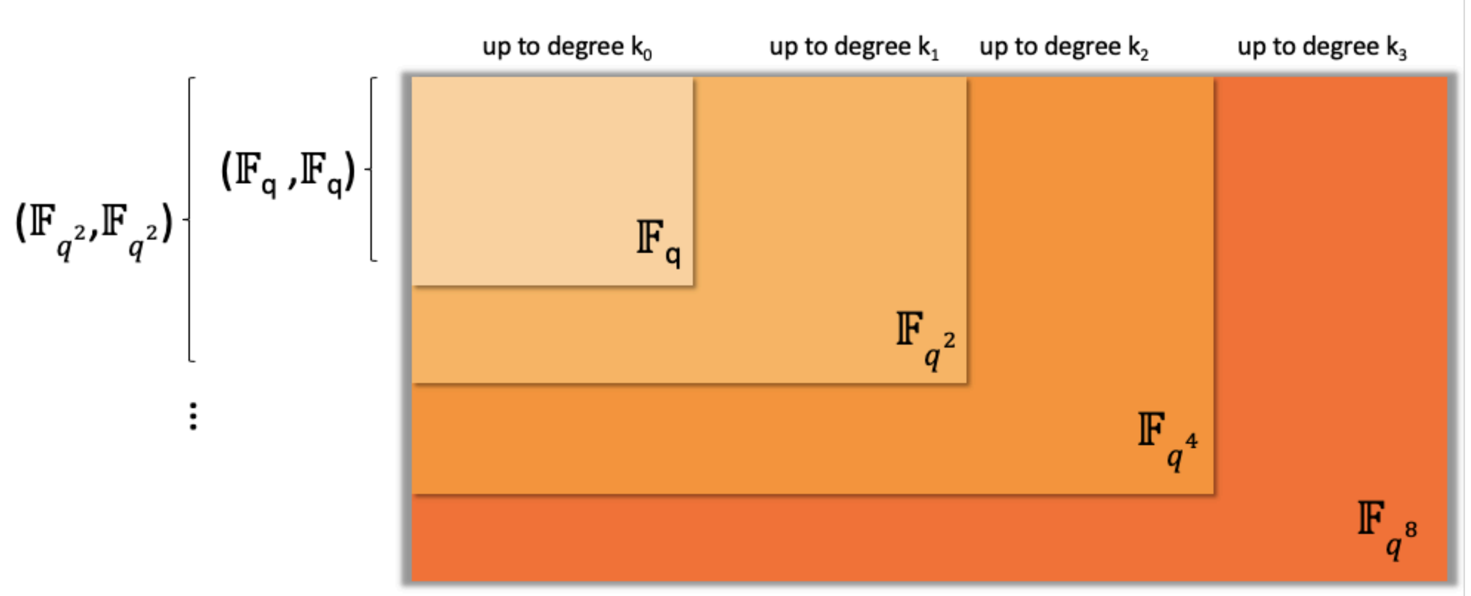
- Consider q^{2^i}, k_i, d_i, for $q^{2^i} \geq d_i k_i + 1$
- Fix k and increase d_i to its maximum
  - $q^{2^i} \geq d_i k + 1$
  - $d \approx \dfrac{n^{1/k+1}}{k}$

Prioritizing *d* increases with fixed k = 2.

i	q	k	d	n	t	n/t
0	4	2	1	64	12	5.33
1	16	2	7	4096	240	17.06
2	256	2	127	16777216	65280	257.00
3	65536	2	32767	281474976710656	4294901760	65537.00

Embedding cover-free families

Prioritize ratio increases



- Consider q^{2^i}, k_i, d_i, for $q^{2^i} \geq d_i k_i + 1$
- Fix *d* and increase k_i to its maximum
  - $q^{2^i} \geq d k_i + 1$
  - $\rho(n) = \dfrac{n}{\log n}$

Prioritizing *ratio* increases with fixed d = 2.

i	q	k	d	n	t	n/t
0	4	1	2	16	12	1.33
1	16	7	2	4294967296	240	17895697.07
2	256	127	2	256^{128}	65280	2.75×10^{303}
3	65536	32767	2	65536^{32768}	4294901760	6.04×10^{157816}

Embedding cover-free families

Construct monotone families

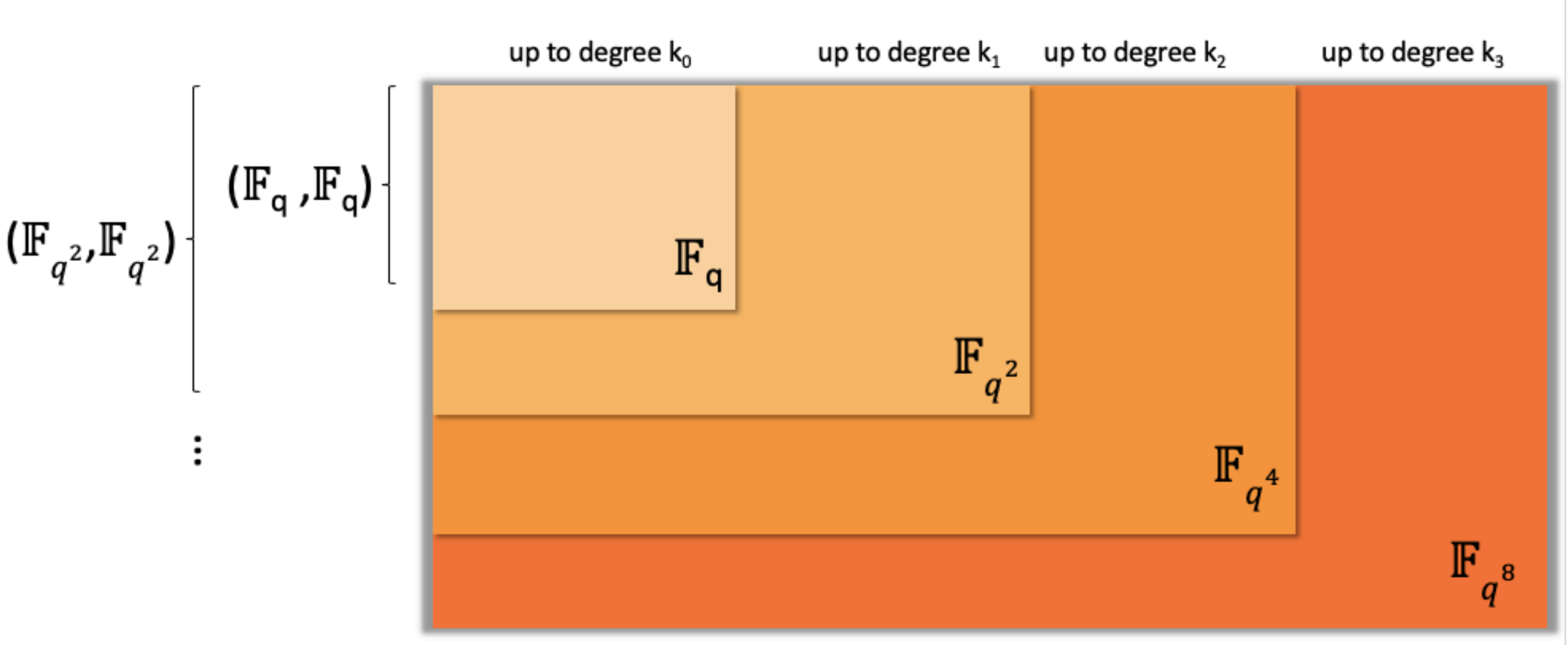
- Consider q^{2^i},k_i, d_i, for $q^{2^i} \geq d_i k_i + 1$
- Fix *d* and *k*
  - Select specific blocks of rows
  - We get monotone families with increasing ratio (better than Hartung et al.*)

	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$	α	$\alpha+1$	$\dots$	$(2\alpha+2)x^2+$ $(2\alpha+2)x+$ $2\alpha+2$
$(0,0)$	1	0	0	1	0	0	1	0	0				
$(0,1)$	0	1	0	0	1	0	0	1	0				
$(0,2)$	0	0	1	0	0	1	0	0	1				
$(1,0)$	1	0	0	0	0	1	0	1	0				
$(1,1)$	0	1	0	1	0	0	0	0	1				
$(1,2)$	0	0	1	0	1	0	1	0	0				
$(2,0)$	1	0	0	0	1	0	0	0	1			$\dots$	
$(2,1)$	0	1	0	0	0	1	1	0	0				
$(2,2)$	0	0	1	1	0	0	0	1	0				
$(\mathbb{F}_3, \mathbb{F}_9 \setminus \mathbb{F}_3)$						0							

* Hartung, Kaidel, Koch, Koch, Rupp (PKC 2016)

Yes, we can build embedding CFFs!

- One construction* can be explored in various ways.
- Different parameter choices give us different properties.
- Applications can give us insights on new ideas.

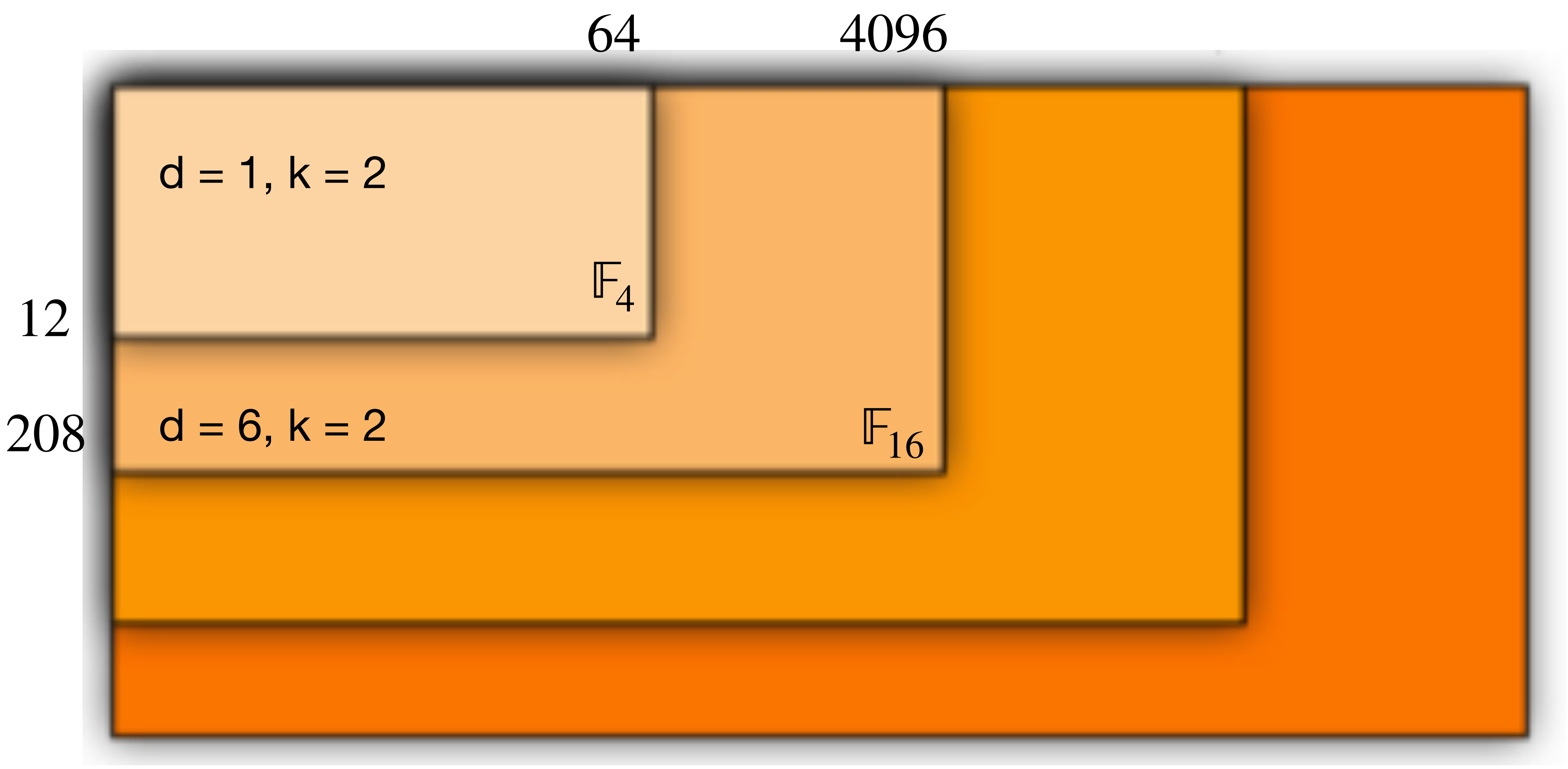


k	d	$\rho(n)$	Feature
fixed	$d \sim \frac{n^{1/(k+1)}}{k}$	$n^{1-\frac{2}{k+1}}$	increasing d
increasing	fixed	$\frac{n}{\log n}$	optimal ratio
fixed	fixed	$n^{1-\frac{1}{k+1}}$	monotone

* P. Erdős, P. Frankl and Z. Furedi, Families of finite sets in which no set is covered by the union of r others, Israel J. Math., 51 (1985), 79–89.

Embedding cover-free families

Gradual increase on n

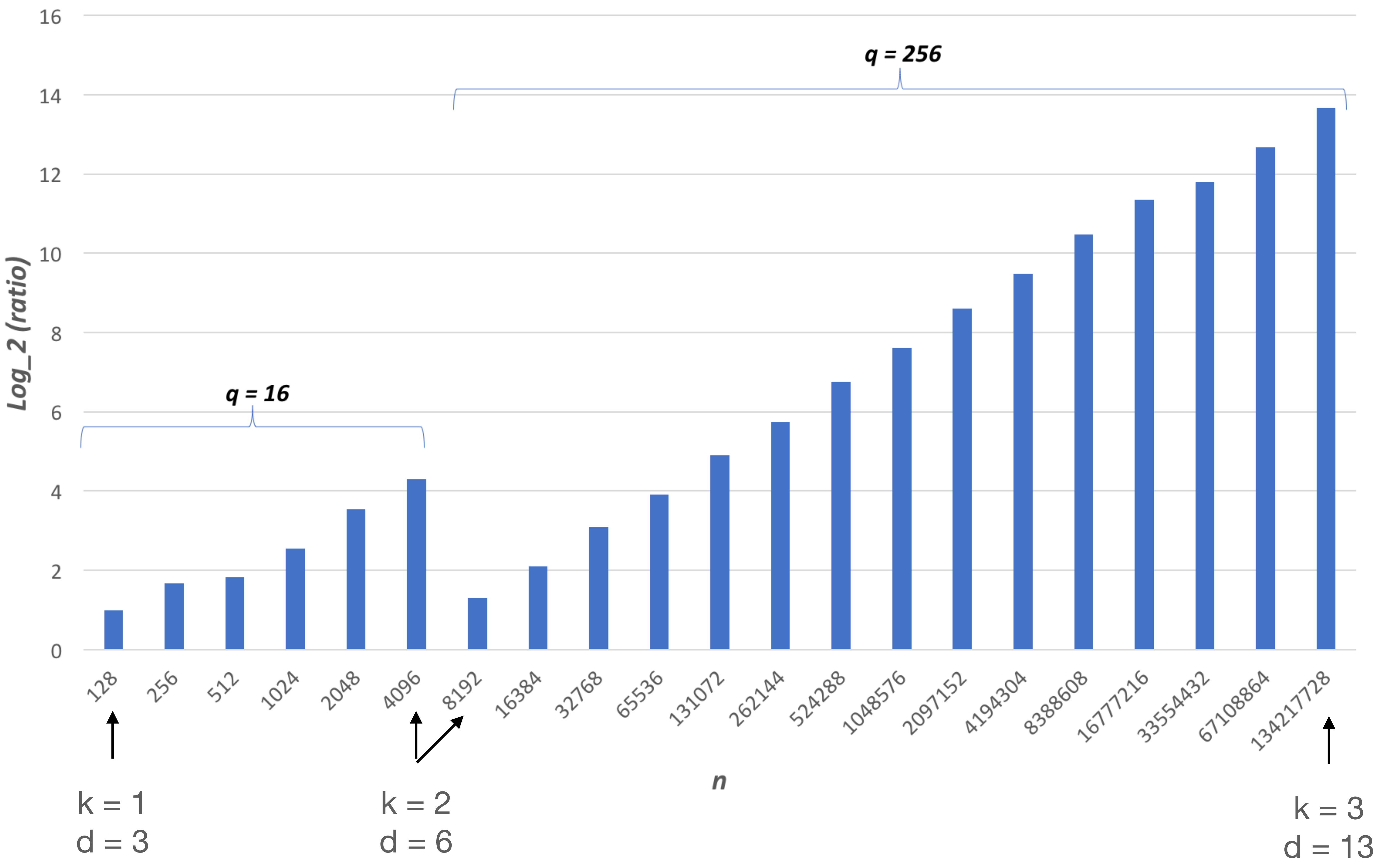


Embedding cover-free families

Gradual increase on n

- Gradual increase on *n* via moderate increase of *d* and *k* to smooth out compression ratio.

$q = 16, 256$
$1 \leq k \leq 3$
$d = \log_4 n$



Future Work

- Can we have embedding families with more gradual increase of n and smoother compression ratio?
- Is there any other way of constructing embedding CFFs?
- Other aspects of CFFs to be explored*.
  - Mixed properties and applications.

* Idalino, Moura. Structure-aware combinatorial group testing: a new method for pandemic screening. IWOCA (2022)

* Idalino, Moura. Group testing and cover-free families on hypergraphs. (2024?)

Thank you!

Feliz Aniversário, Daniel!

Thais Bardini Idalino - thais.bardini@ufsc.br

UFSC