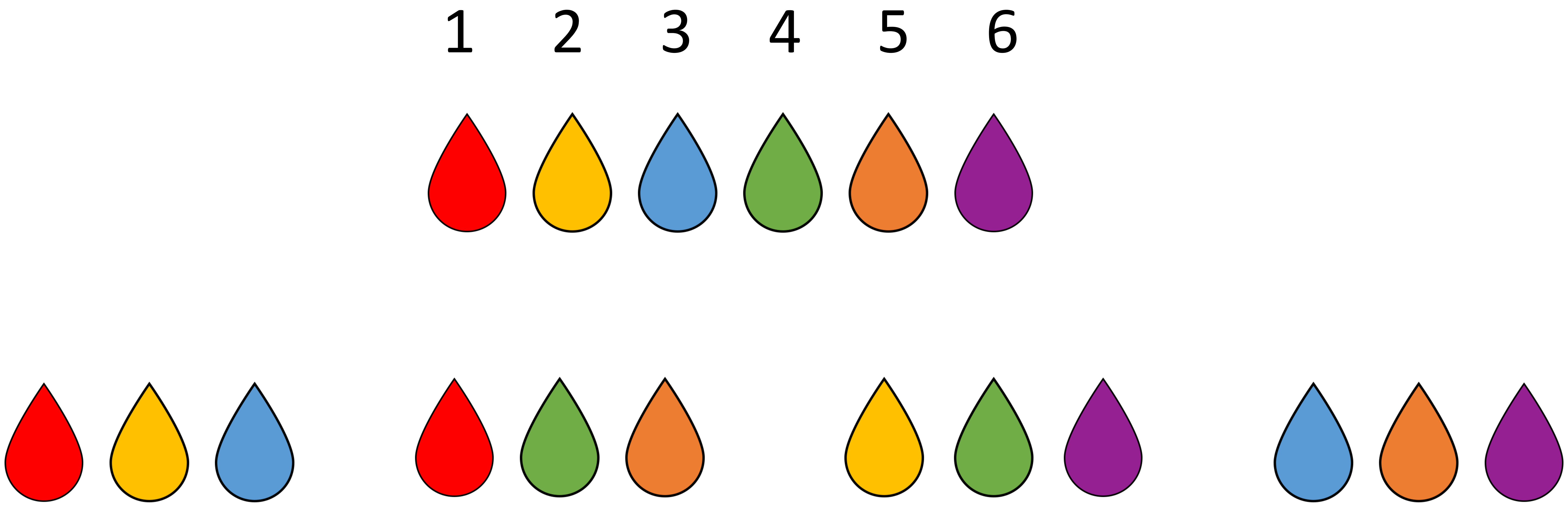
Matemática combinatória e aplicações em criptografia

Thaís Bardini Idalino

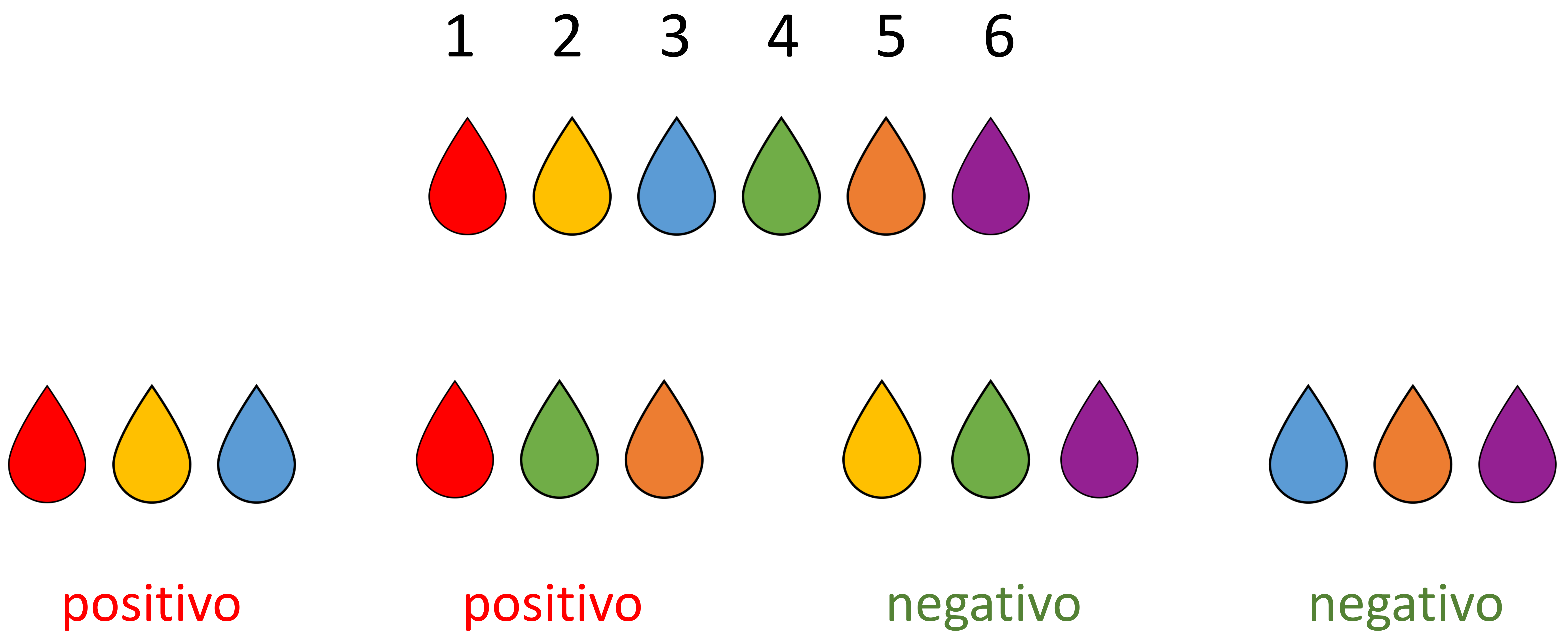
Departamento de Informática e Estatística
Universidade Federal de Santa Catarina


UFSC
Graduação
2009
2013
Mestrado
UFSC
uOttawa
PhD
2015
2019
Postdoc
SFU
SIMON FRASER UNIVERSITY
UFSC
2021

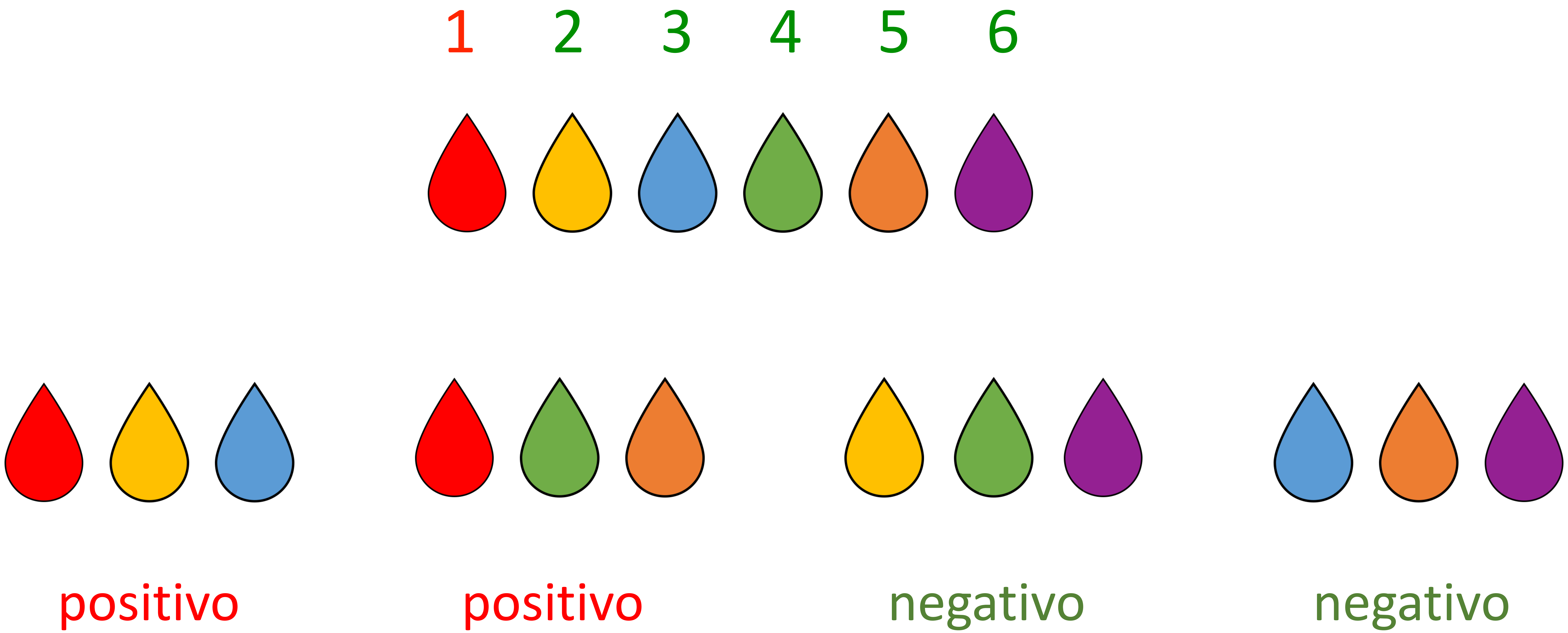
Combinatorial Group Testing



Combinatorial Group Testing



Combinatorial Group Testing

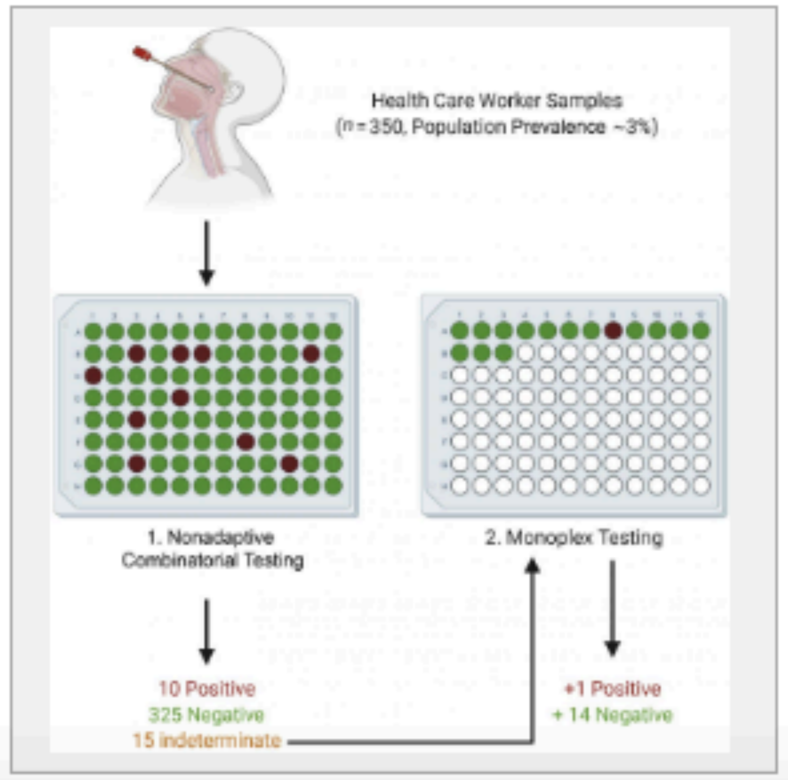


New testing strategy can speed up COVID-19 test results for healthcare workers

In The Journal of Molecular Diagnostics investigators share a new methodology for testing pooled samples that maximizes the proportion of samples resolved after a single round of testing

Peer-Reviewed Publication
ELSEVIER

Philadelphia, April 26, 2021 - Fast turnaround of COVID-19 test results for healthcare workers is critical. Investigators have now developed a COVID-19 testing strategy that maximizes the proportion of negative results after a single round of testing, allowing prompt notification of results. The method also reduces the need for increasingly limited test reagents, as fewer additional tests are required. Their strategy is described in *The Journal of Molecular Diagnostics*, published by Elsevier.



The Journal of Molecular Diagnostics, Vol. 23, No. 5, May 2021

ELSEVIER

the Journal of Molecular Diagnostics

jmdjournal.org

Check for updates

A Nonadaptive Combinatorial Group Testing Strategy to Facilitate Health Care Worker Screening during the Severe Acute Respiratory Syndrome Coronavirus-2 (SARS-CoV-2) Outbreak

John H. McDermott,*† Duncan Stoddard,‡ Peter J. Woolf,§ Jamie M. Ellingford,*† David Gokhale,*† Algy Taylor,* Leigh A.M. Demain,* William G. Newman,*† and Graeme Black*†

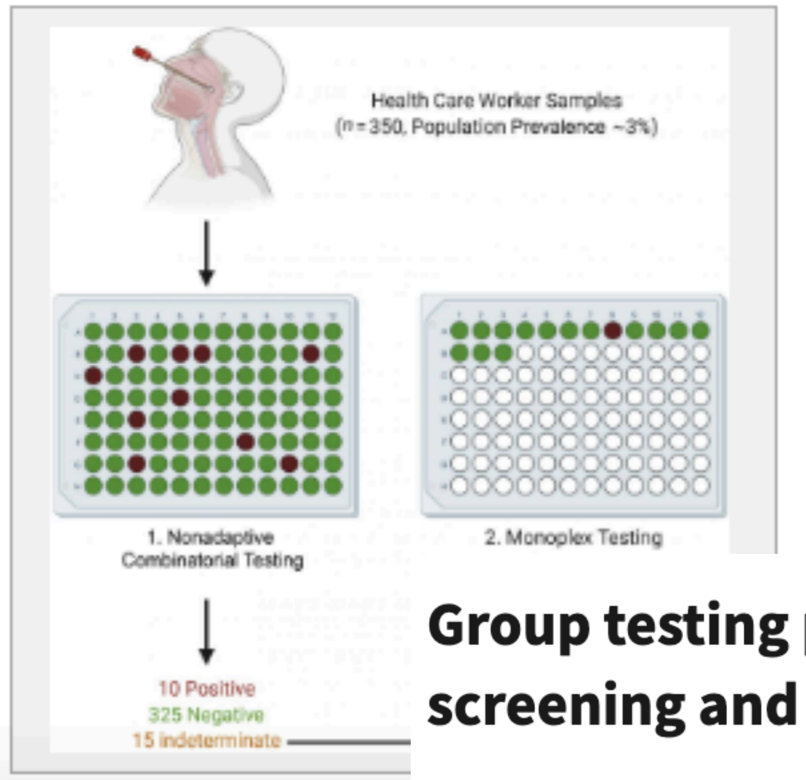
From the Manchester Centre for Genomic Medicine, St. Mary's Hospital, Manchester University NHS Foundation Trust, Manchester, United Kingdom; Division of Evolution and Genomic Sciences,† School of Biological Sciences, University of Manchester, Manchester, United Kingdom; DS Analytics and Machine Learning Ltd.,‡ London, United Kingdom; and Origami Assays,§ Ann Arbor, Michigan*

ting strategy can sp
19 test results for h

Molecular Diagnostics investigators share a r
hat maximizes the proportion of samples re:

blication

26, 2021 - Fast
VID-19 test results for
s is critical. Investigators
ed a COVID-19 testing
imizes the proportion of
negative results after a single round of
testing, allowing prompt notification of
results. The method also reduces the need
asingly limited test reagents, as
dditional tests are required. Their
is described in *The Journal of*
r Diagnostics, published by Elsevier.



METHODS article

Front. Public Health, 17 August 2021

Sec. Infectious Diseases: Epidemiology and Prevention

Volume 9 - 2021 | https://doi.org/10.3389/fpubh.2021.583377

Group Testing for SARS-CoV-2 Allows for Up to 10-Fold Efficiency Increase Across Realistic Scenarios and Testing Strategies

Updated

Claudio M. Verdun[1,2†] Tim Fuchs[1†] Pavol Harar[3,4†]

Dennis Elbrächter[5†] David S. Fischer[6] Julius Berner[5†]

Philipp Grohs[3,5,7] Fabian J. Theis[1,6] Felix Krahmer[1,8*]

nature › scientific reports › articles › article

Article | Open access | Published: 26 July 2023

Adaptive group testing strategy for infectious diseases using social contact graph partitions

Jingyi Zhang & Lenwood S. Heath

Scientific Reports **13**, Article number: 12102 (2023) | Cite this article

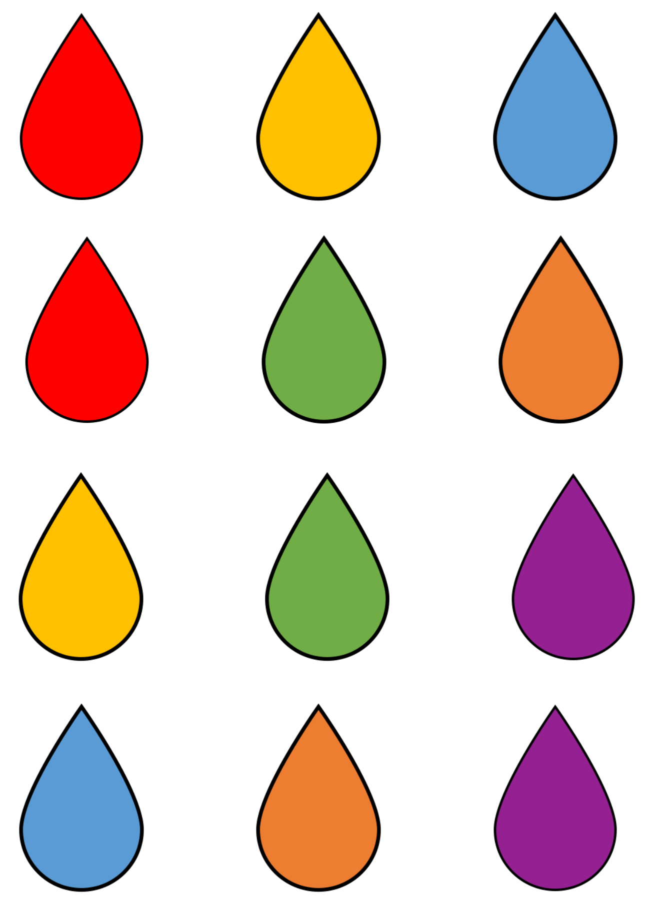
Group testing performance evaluation for SARS-CoV-2 massive scale screening and testing

Ozkan Ufuk Nalbantoglu[1,2,✉]

Author information Article notes Copyright and License information

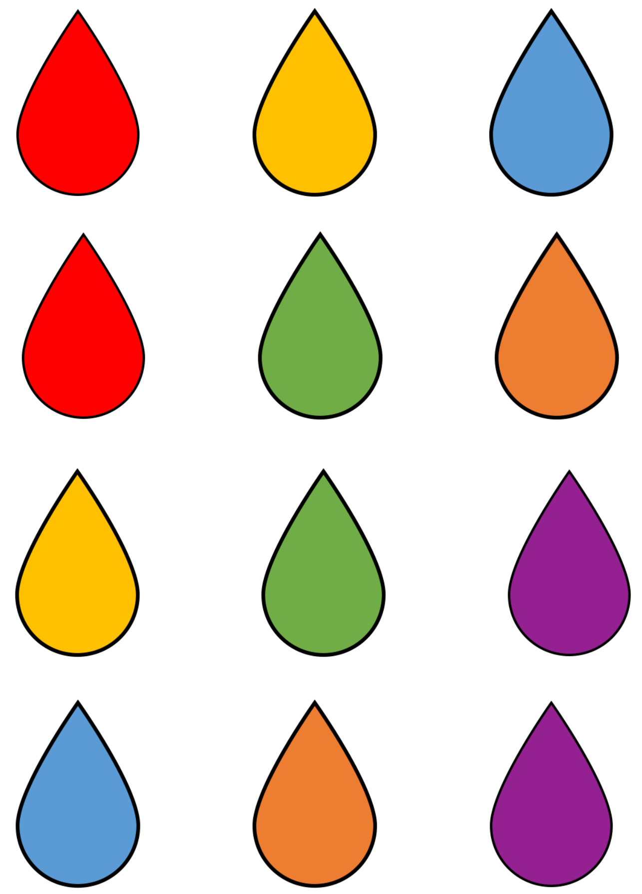
PMCID: PMC7330001 PMID: 32615934

Cover-Free Families

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

Cover-Free Families

	1	2	3	4	5	6
Teste 1	1	1	1	0	0	0
Teste 2	1	0	0	1	1	0
Teste 3	0	1	0	1	0	1
Teste 4	0	0	1	0	1	1



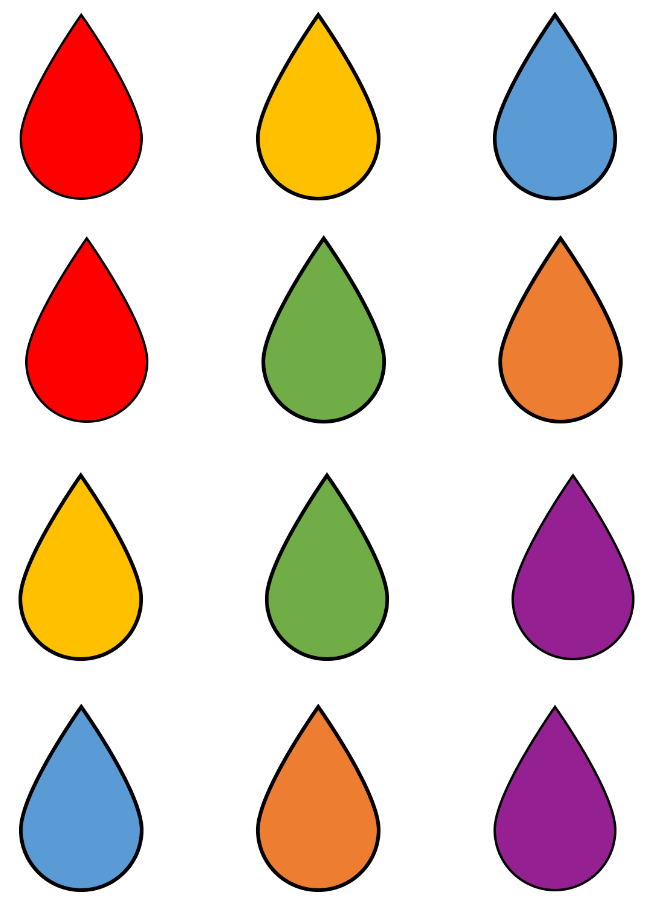
FAIL
FAIL
PASS
PASS

$\mathit{1}$ – CFF(4, 6)

Nenhum elemento é ***coberto*** por qualquer outro

Cover-Free Families

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



***1* – CFF(4, 6)**

Nenhum elemento é ***coberto*** por qualquer outro

Cover-Free Families

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

1 – CFF(4, 6)

Nenhum elemento é ***coberto*** por qualquer outro

Cover-Free Families

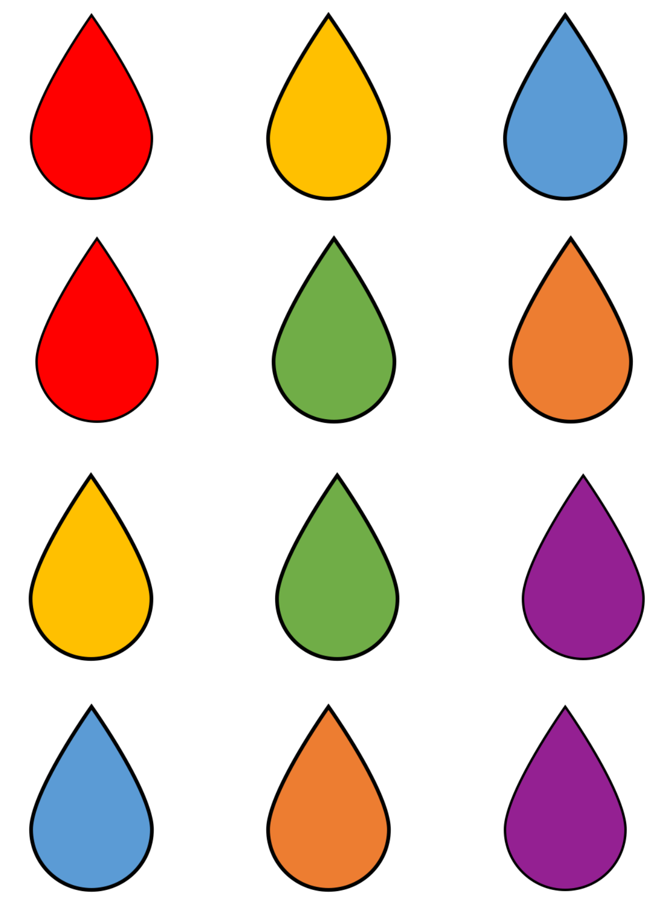
	1	2	3	4	5	6	
Teste 1	1	1	1	0	0	0	FAIL
Teste 2	1	0	0	1	1	0	FAIL
Teste 3	0	1	0	1	0	1	PASS
Teste 4	0	0	1	0	1	1	PASS

1 – CFF(4, 6)

Nenhum elemento é ***coberto*** por qualquer outro

Cover-Free Families

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



$\mathit{1}$ – CFF(4, 6)

Nenhum elemento é ***coberto*** por qualquer outro

Cover-Free Families

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

$\mathit{1}$ – CFF(4, 6)

Nenhum elemento é ***coberto*** por qualquer outro

Cover-Free Families

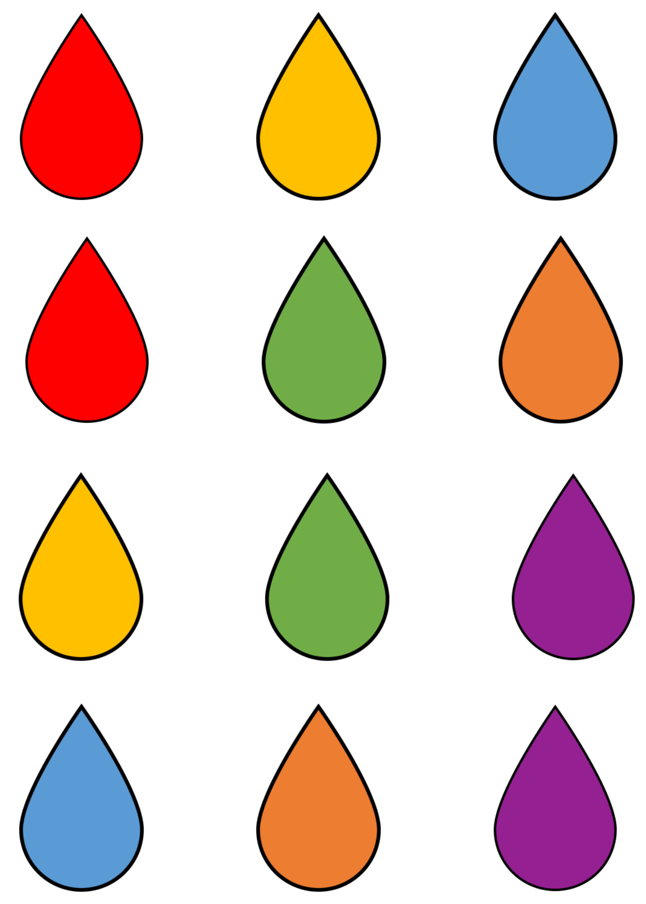
	1	2	3	4	5	6	
Teste 1	1	1	1	0	0	0	FAIL
Teste 2	1	0	0	1	1	0	FAIL
Teste 3	0	1	0	1	0	1	PASS
Teste 4	0	0	1	0	1	1	PASS

1 – CFF(4, 6)

Nenhum elemento é ***coberto*** por qualquer outro

Cover-Free Families

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

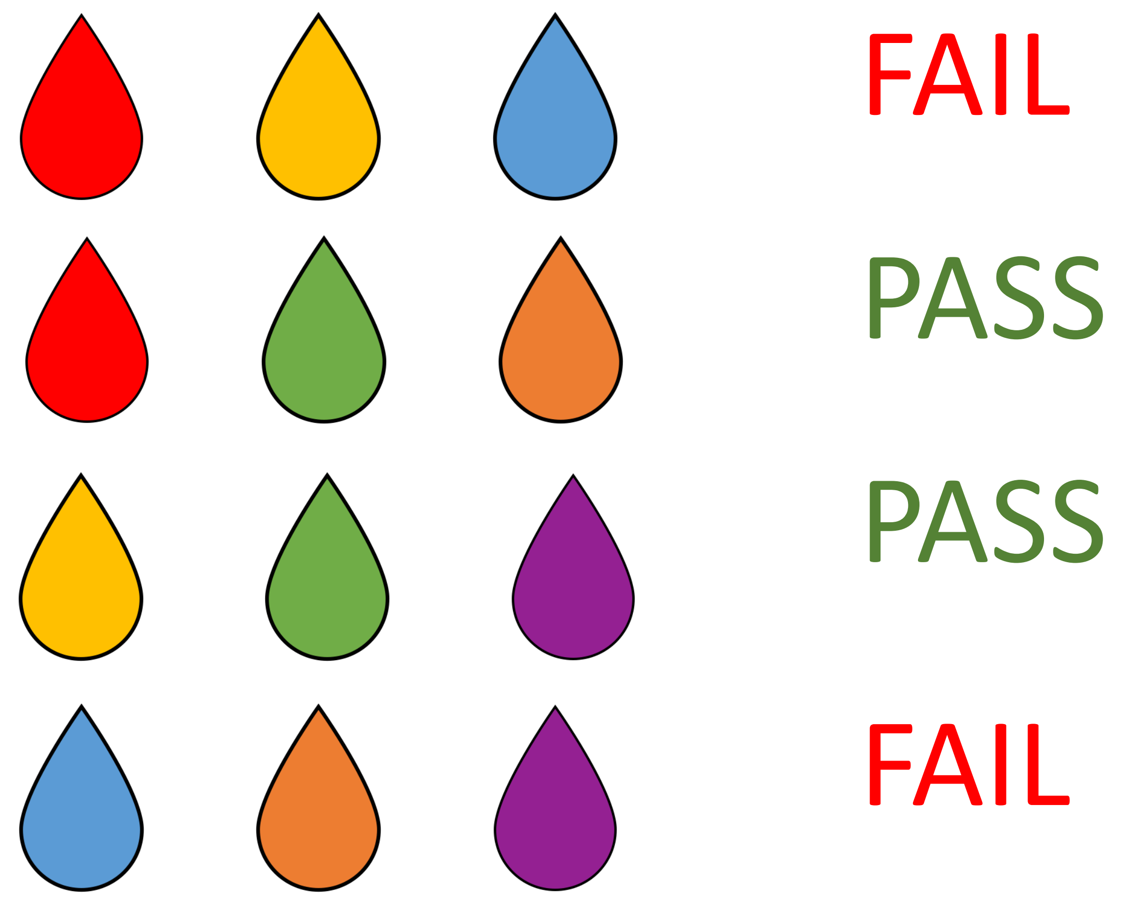


***1* – CFF(4, 6)**

Nenhum elemento é ***coberto*** por qualquer outro

Cover-Free Families

	1	2	3	4	5	6
Teste 1	1	1	1	0	0	0
Teste 2	1	0	0	1	1	0
Teste 3	0	1	0	1	0	1
Teste 4	0	0	1	0	1	1



***1* – CFF(4, 6)**

e assim por diante..

Nenhum elemento é ***coberto*** por qualquer outro

Cover-Free Families

	1	2	3	4	5	6
Teste 1	1	1	1	0	0	0
Teste 2	1	0	0	1	1	0
Teste 3	0	1	0	1	0	1
Teste 4	0	0	1	0	1	1

Em quaisquer 2 colunas, precisamos encontrar uma "matriz identidade" 2x2

$\mathit{1}$ – CFF(4, 6)

Nenhum elemento é ***coberto*** por qualquer outro

Cover-Free Families

	1	2	3	4	5	6
Teste 1	1	1	1	0	0	0
Teste 2	1	0	0	1	1	0
Teste 3	0	1	0	1	0	1
Teste 4	0	0	1	0	1	1

Em quaisquer 2 colunas, precisamos encontrar uma "matriz identidade" 2x2

***1* – CFF(4, 6)**

Nenhum elemento é ***coberto*** por qualquer outro

Cover-Free Families

	1	2	3	4	5	6
Teste 1	1	1	1	0	0	0
Teste 2	1	0	0	1	1	0
Teste 3	0	1	0	1	0	1
Teste 4	0	0	1	0	1	1

Em quaisquer 2 colunas, precisamos encontrar uma "matriz identidade" 2x2

1 – CFF(4, 6)

Nenhum elemento é ***coberto*** por qualquer outro

Cover-Free Families

	1	2	3	4	5	6
Teste 1	1	1	1	0	0	0
Teste 2	1	0	0	1	1	0
Teste 3	0	1	0	1	0	1
Teste 4	0	0	1	0	1	1

Em quaisquer 2 colunas, precisamos encontrar uma "matriz identidade" 2x2

$$\binom{6}{2} = 15$$

1 – CFF(4, 6)

Nenhum elemento é ***coberto*** por qualquer outro

Cover-Free Families

	1	2	3	4	5	6
Teste 1	1	1	1	0	0	0
Teste 2	1	0	0	1	1	0
Teste 3	0	1	0	1	0	1
Teste 4	0	0	1	0	1	1

1 – CFF(4, 6)

Essa não é uma 2-CFF!

Cover-Free Families

	1	2	3	4	5	6
Teste 1	1	1	1	0	0	0
Teste 2	1	0	0	1	1	0
Teste 3	0	1	0	1	0	1
Teste 4	0	0	1	0	1	1

1 – CFF(4, 6)

Essa não é uma 2-CFF!

Cover-free Families

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

2 - CFF(9, 12)

Nenhum elemento é ***coberto*** por quaisquer **dois** outros elementos

Cover-free Families

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

2 - CFF(9, 12)

Nenhum elemento é ***coberto*** por quaisquer **dois** outros elementos

Cover-free Families

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

2 - CFF(9, 12)

Nenhum elemento é ***coberto*** por quaisquer **dois** outros elementos

Cover-free Families

Em quaisquer 3 colunas, precisamos encontrar uma "matriz identidade" 3x3

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

2 - CFF(9, 12)

Nenhum elemento é ***coberto*** por quaisquer **dois** outros elementos

Cover-free Families

Em quaisquer 3 colunas, precisamos encontrar uma "matriz identidade" 3x3

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

2 - CFF(9, 12)

Nenhum elemento é ***coberto*** por quaisquer **dois** outros elementos

Cover-free Families

Em quaisquer 3 colunas, precisamos encontrar uma "matriz identidade" 3x3

$$\binom{12}{3} = 220$$

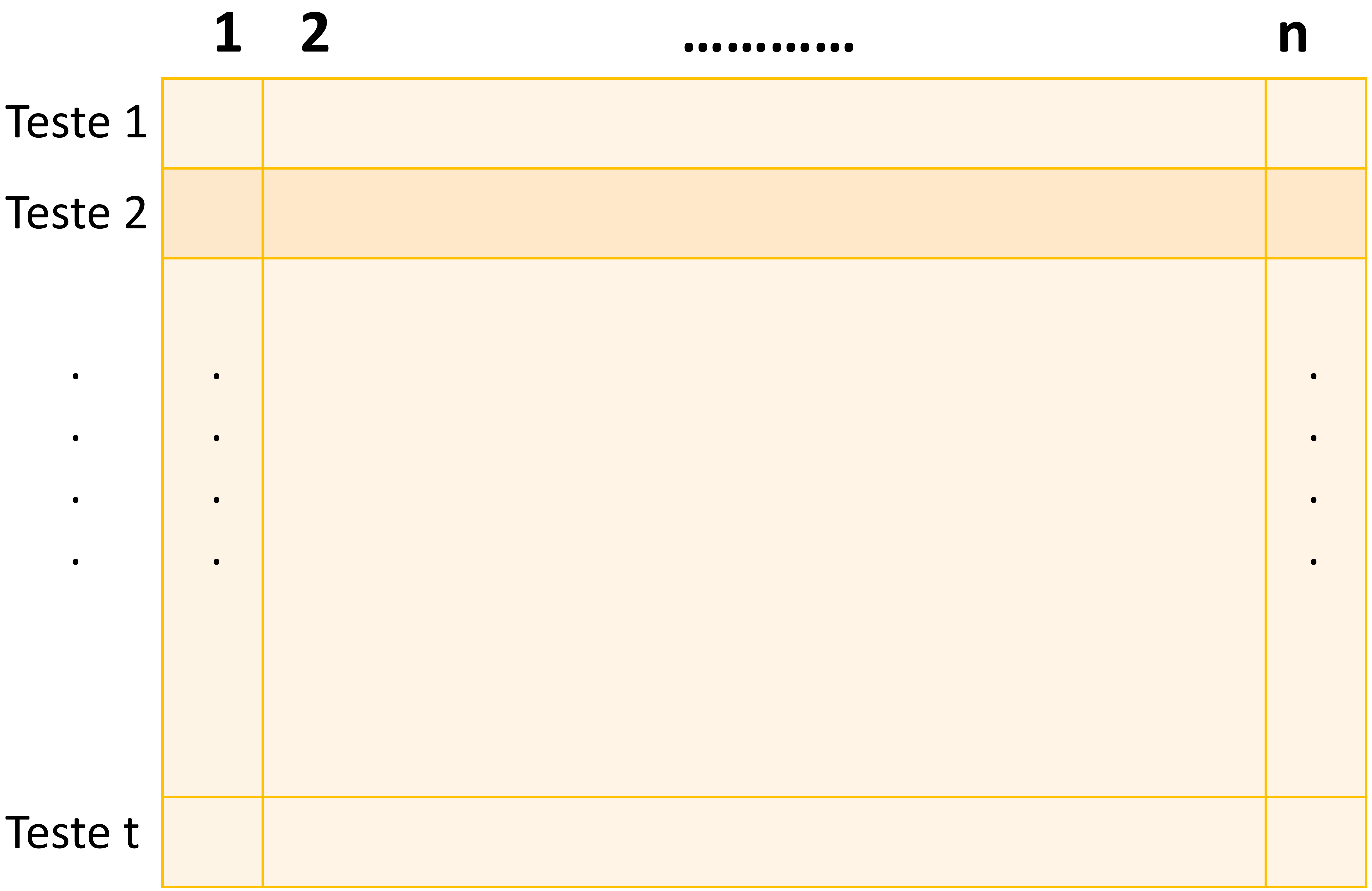
	1	2	3	4	5	6	7	8	9	10	11	12
Teste 1	1			1			1			1		
Teste 2	1				1			1			1	
Teste 3	1					1			1			1
Teste 4		1		1					1		1	
Teste 5		1			1		1					1
Teste 6		1				1		1		1		
Teste 7			1	1				1				1
Teste 8			1		1				1	1		
Teste 9			1			1	1				1	

2 - CFF(9, 12)

Nenhum elemento é ***coberto*** por quaisquer **dois** outros elementos

Cover-free Families

Em quaisquer d+1 colunas, precisamos encontrar uma "matriz identidade" (d+1)x(d+1)



d - CFF(t, n)

Nenhum elemento é ***coberto*** por quaisquer ***d*** outros elementos

Cover-Free Families

$X = \{1,2,3,4\}$

$B_1 = \{1,2\}$

$B_2 = \{1,3\}$

$B_3 = \{1,4\}$

$B_4 = \{2,3\}$

$B_5 = \{2,4\}$

$B_6 = \{3,4\}$

	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

_1_ – CFF(4, 6)

Nenhum elemento é ***coberto*** por qualquer outro

Cover-Free Families

$$
\begin{array}{cc|cccccc}
 & & B_1 & B_2 & B_3 & B_4 & B_5 & B_6 \\
\hline
\multirow{4}{*}{$X \left\{ \vphantom{\begin{array}{c}1\\2\\3\\4\end{array}} \right.$} & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\
 & 2 & 1 & 0 & 0 & 1 & 1 & 0 \\
 & 3 & 0 & 1 & 0 & 1 & 0 & 1 \\
 & 4 & 0 & 0 & 1 & 0 & 1 & 1
\end{array}
$$

Definição: Seja *d* um inteiro positivo. Uma *d*-cover-free family, chamada de $d - CFF(t, n)$, é uma coleção de subconjuntos $\mathscr{B} = \{B_1, B_2, \ldots, B_n\}$ de um conjunto $X = \{1,2,\ldots, t\}$ tal que para quaisquer $d + 1$ subconjuntos $B_{i_0}, B_{i_1}, \ldots, B_{i_d} \in \mathscr{B}$, nós temos que:

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

Nenhum elemento é ***coberto*** pela união de quaisquer outros *d* elementos.

Cover-free Families

$X = \{1,2,\ldots,9\}$

$B_1 \cup B_2 = \{1,2,3,4,5,6\}$

$B_3 - (B_1 \cup B_2) = \{7,8,9\}$

$B_4 - (B_1 \cup B_2) = \{7\}$

$B_5 - (B_1 \cup B_2) = \{8\}$

$B_6 - (B_1 \cup B_2) = \{9\}$

$B_7 - (B_1 \cup B_2) = \{9\}$

$B_8 - (B_1 \cup B_2) = \{7\}$

$B_9 - (B_1 \cup B_2) = \{8\}$

$B_{10} - (B_1 \cup B_2) = \{8\}$

$B_{11} - (B_1 \cup B_2) = \{9\}$

$B_{12} - (B_1 \cup B_2) = \{7\}$

	B_1	B_2	B_3	B_4	B_5	B_6	B_7	B_8	B_9	B_{10}	B_{11}	B_{12}
1	1			1			1			1		
2	1				1			1			1	
3	1					1			1			1
4		1		1					1		1	
5		1			1		1					1
6		1				1		1		1		
7			1	1				1				1
8			1		1				1	1		
9			1			1	1				1	

Estamos realmente economizando testes?

Construindo 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

- Para dados *d* e *n*, queremos uma *d* - CFF(t, n) com o menor *t* possível
- Quando $d = 1$ a construção de Sperner nos dá um *t* que cresce como $\log_2 n$ quando $n \to \infty$;
- Para $d \geq 2$, o melhor **lower bound** de t para uma *d*-CFF(*t*, *n*) é dado por

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

- Construções baseadas em polinômios, códigos de correção de erros, algoritmos probabilísticos, SAT solvers, etc.

Construção de Sperner

$d = 1$

- Dado *n*, escolha o menor valor *t* tal que

$$n \leq \binom{t}{\lfloor t/2 \rfloor}$$

- Considere $X = \{1,2,\ldots,t\}$
- Liste todos os subconjuntos de X de cardinalidade $\lfloor t/2 \rfloor$

Construção de Sperner

$d = 1$

Se n = 6, o menor t seria 4, já que

$$6 = \binom{4}{2}$$

Se n = 100, t = 9

$$100 \leq \binom{9}{4}$$

Se n = 1500, t = 13

$$1500 \leq \binom{13}{6}$$

$X = \{1,2,3,4\}$

$B_1 = \{1,2\}$

$B_2 = \{1,3\}$

$B_3 = \{1,4\}$

$B_4 = \{2,3\}$

$B_5 = \{2,4\}$

$B_6 = \{3,4\}$

	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

***1* – CFF(4, 6)**

Construção de polinômios

$d \geq 1$

	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(1) = 2

Construção de polinômios

$d \geq 1$

Theorem (E, F, F 1985*): Seja q uma potência de primo e k um inteiro positivo. Se $q \geq dk + 1$ então existe uma d-CFF(q^2, q^{k+1}).

Polinômios de grau até k
cujos coeficientes estão
em um conjunto especial $\mathbb{F}_q$

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

	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

$q = 3, k = 1$

$\mathbb{F}_3 = \mathbb{Z}_3 = \{0,1,2\}$

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

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.

E as aplicações em criptografia?

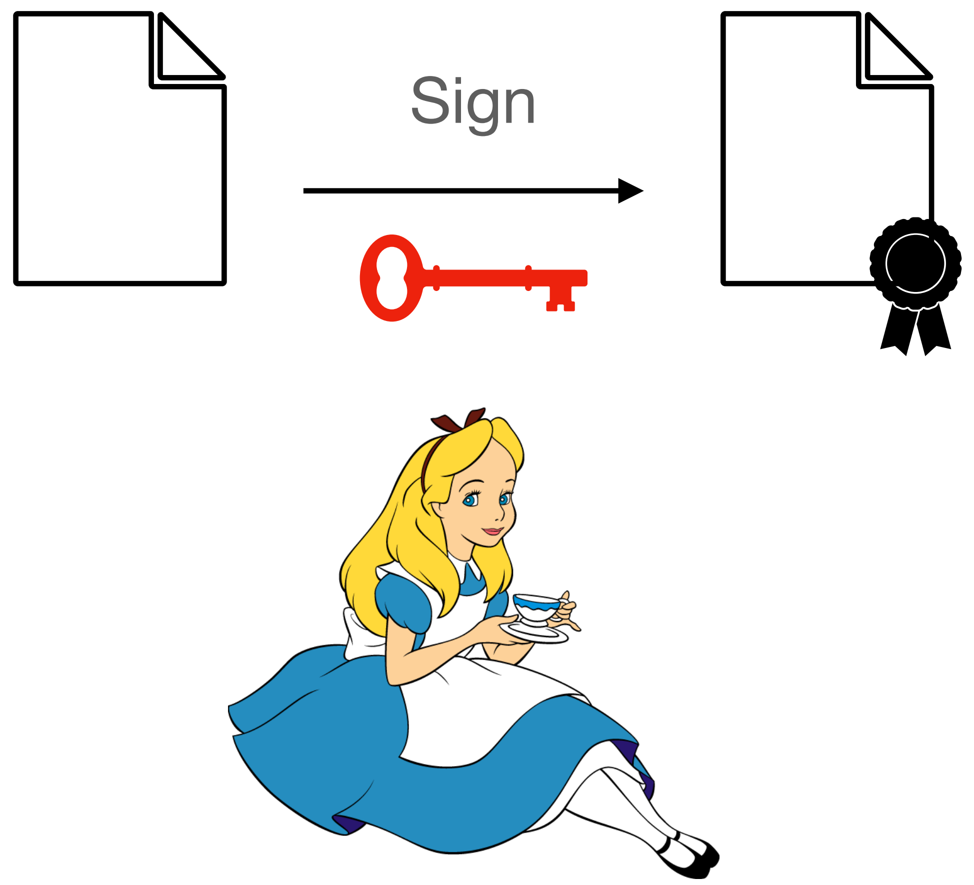
Aplicações em Criptografia

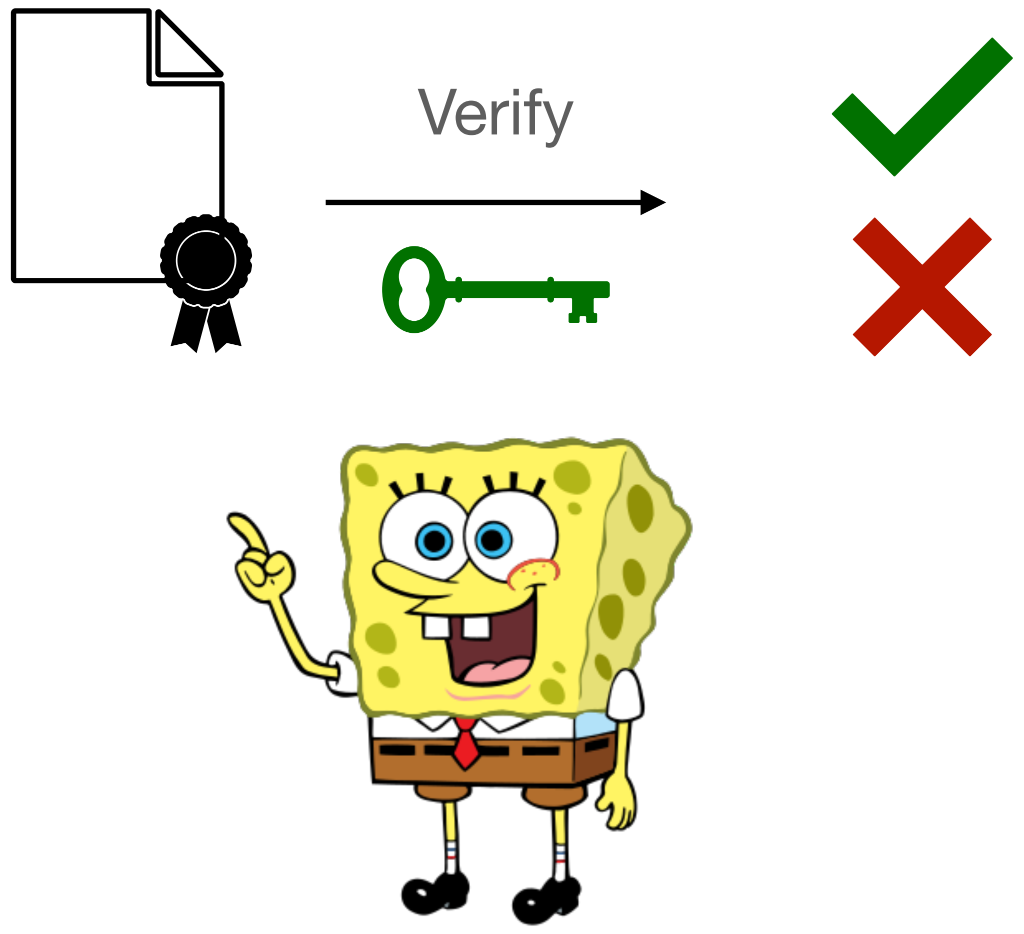
- **Fault-tolerant Digital Signatures**
  - Fault-tolerant digital signatures
    - Idalino, Moura, Custodio, Panario (2015), Idalino, Moura, Adams, (2019)
  - Fault-tolerance in aggregation of signatures
    - Zaverucha, Stinson (2010). Idalino (2015). Hartung, Kaidel, Koch, Koch, Rupp (2016). Idalino, 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)
- E muitas outras...

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

Assinaturas Digitais

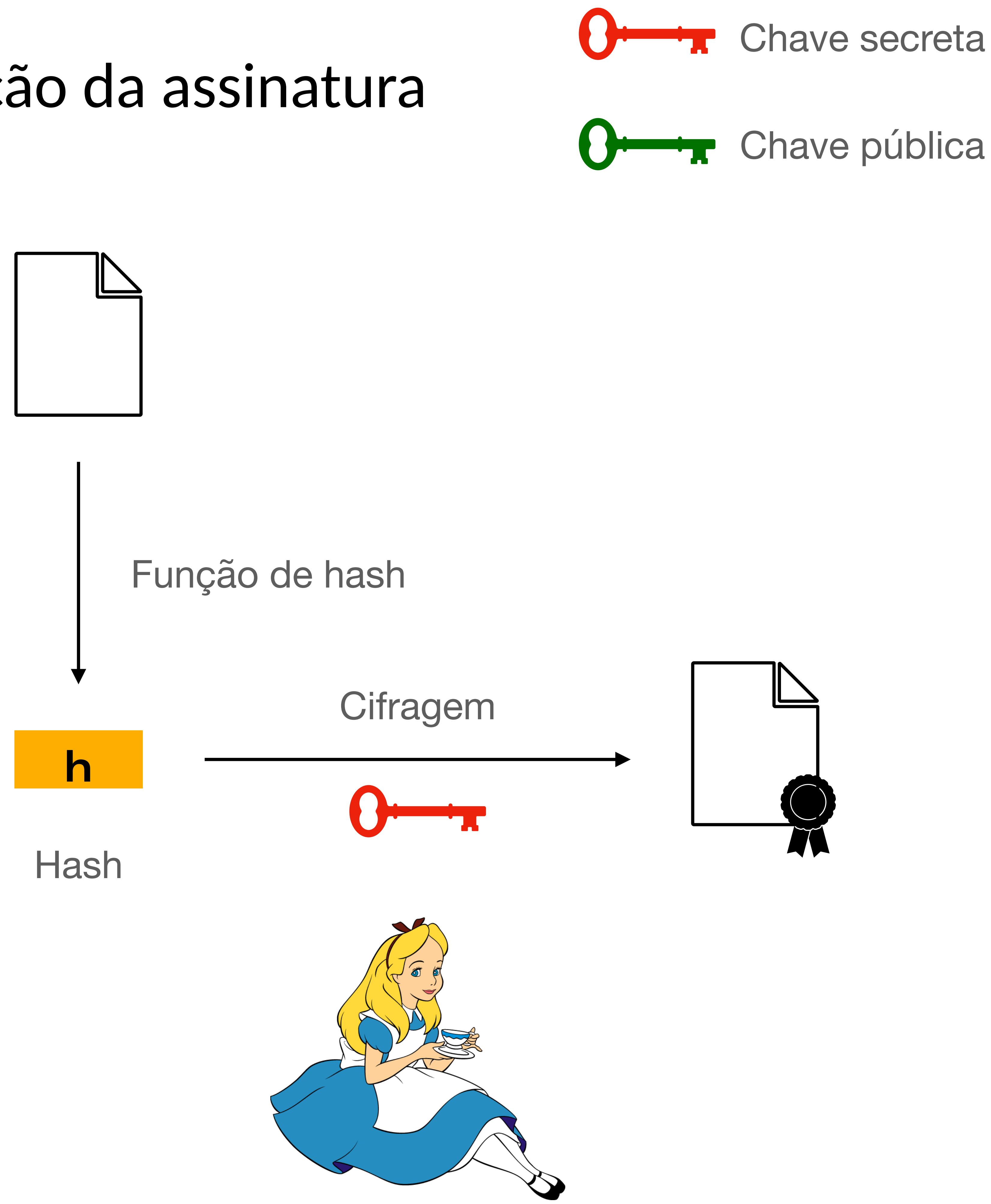
- Autenticidade e integridade de documentos eletrônicos
- Usam um par de chaves criptográficas





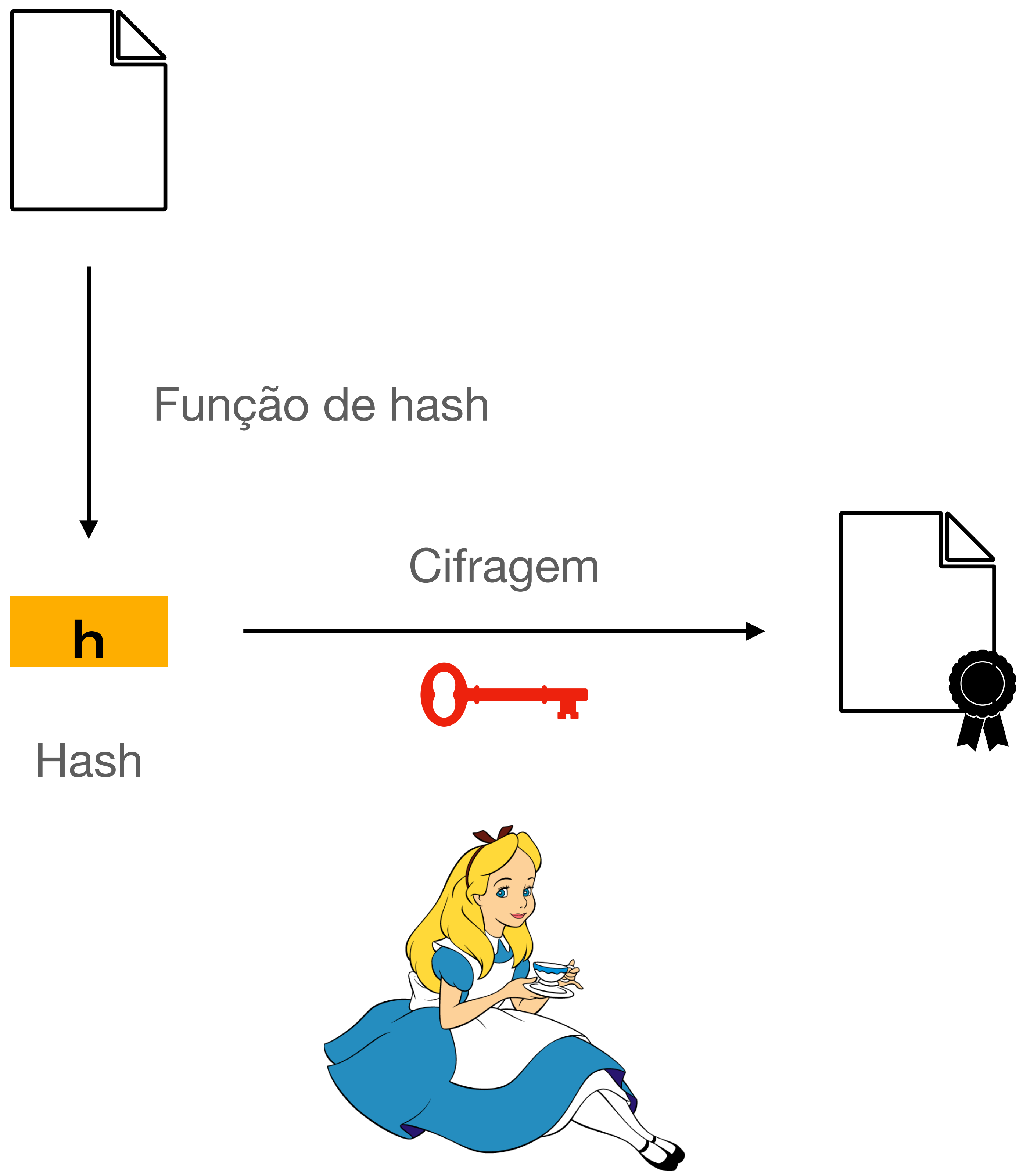
Assinaturas Digitais

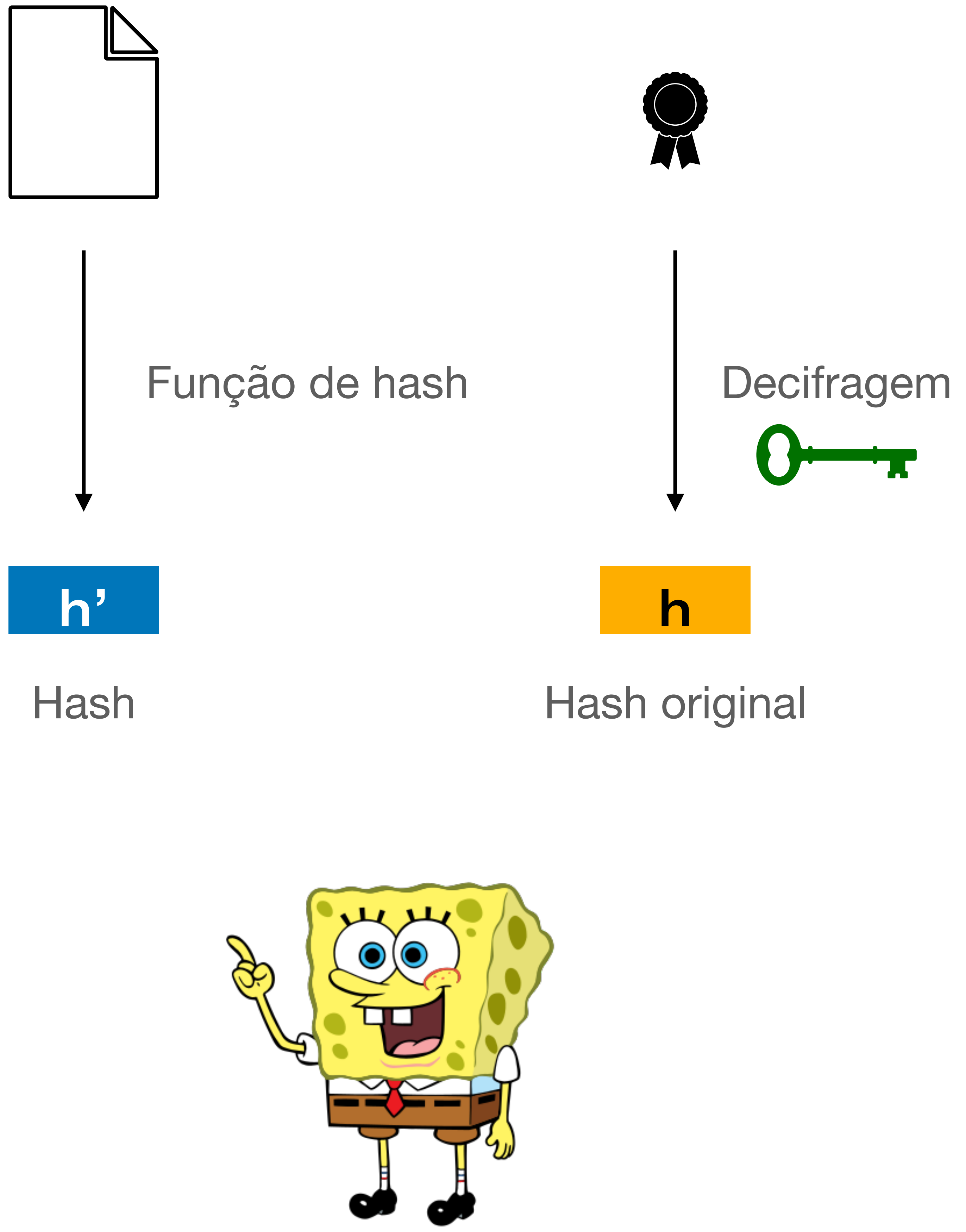
- Geração da assinatura



Assinaturas Digitais

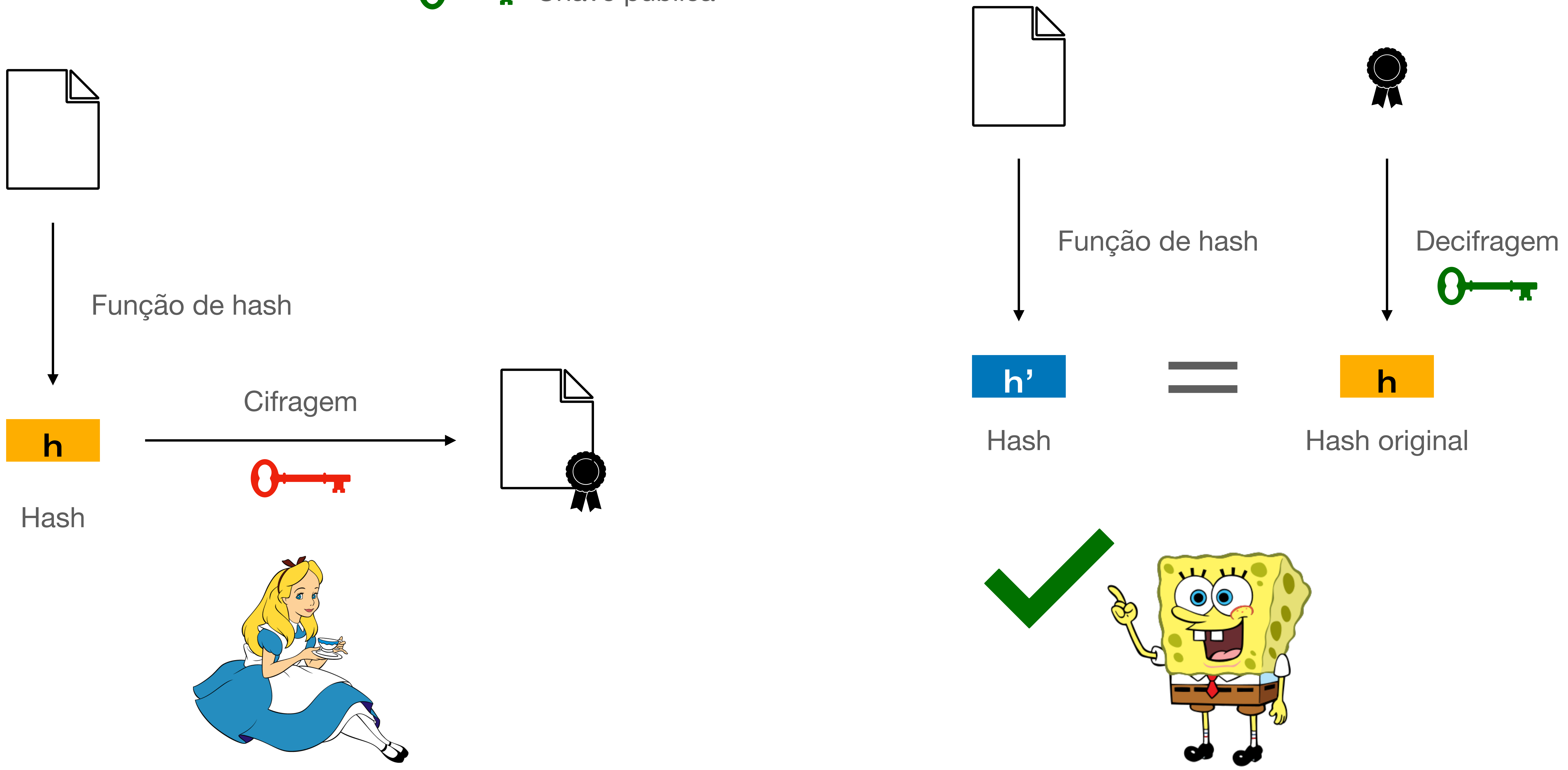
- Verificação da assinatura





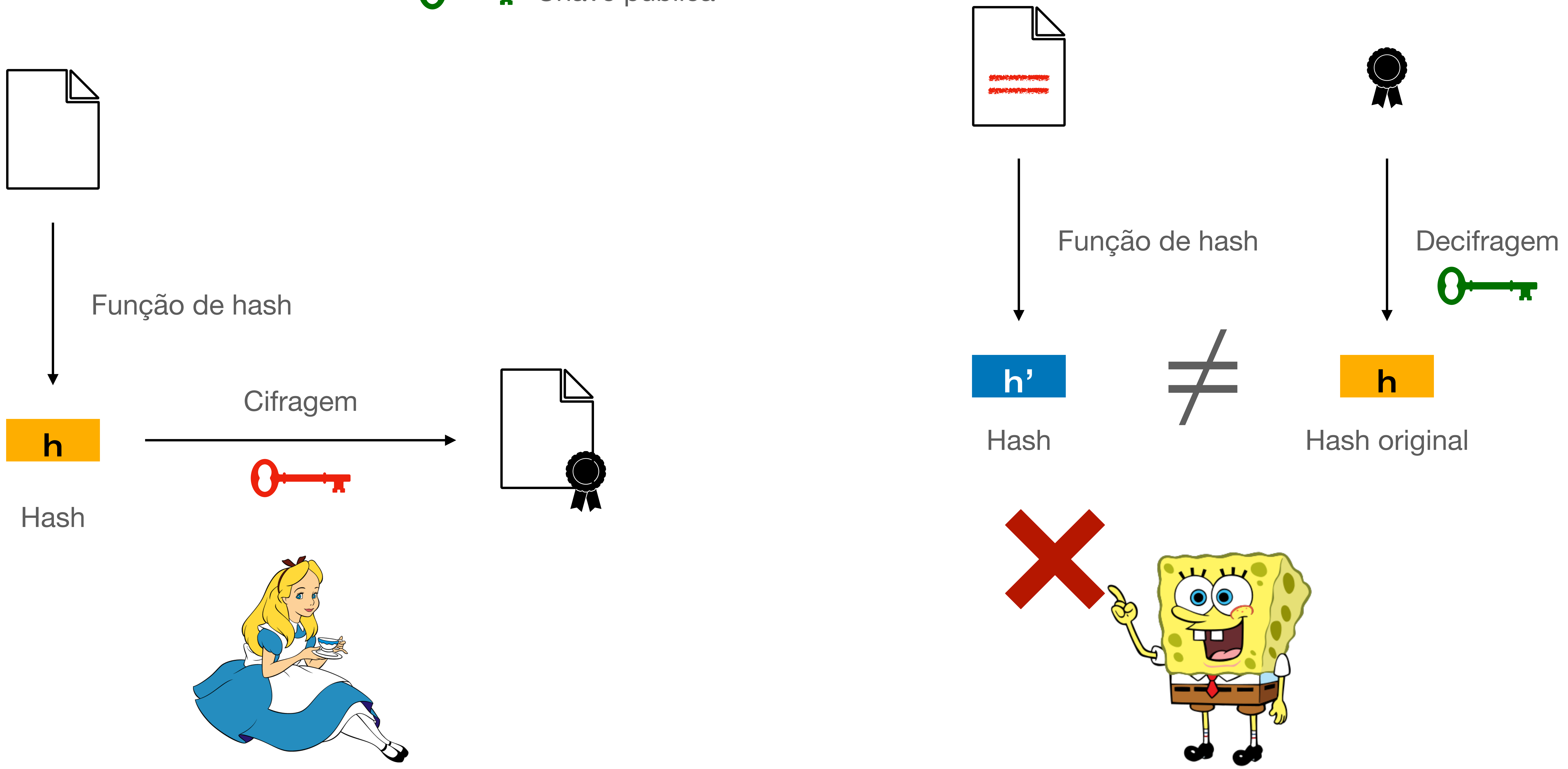
Assinaturas Digitais

- Verificação da assinatura



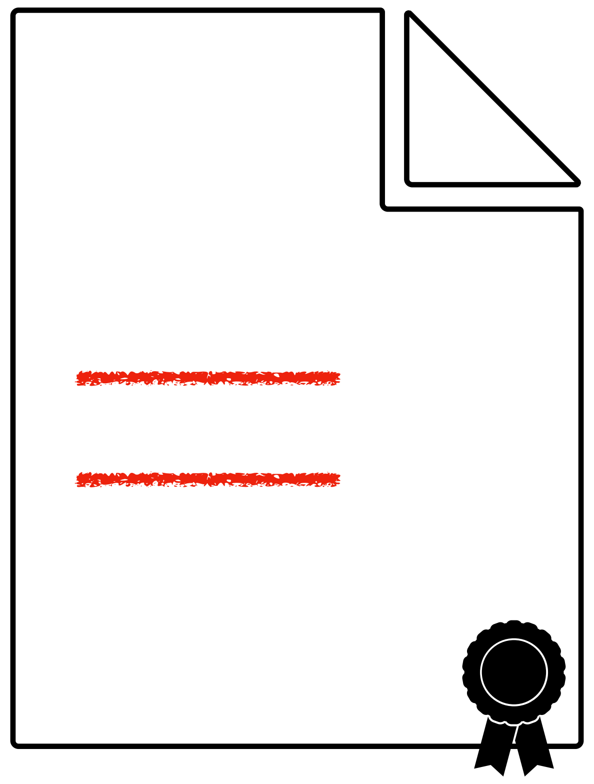
Assinaturas Digitais

- Verificação da assinatura



Integridade parcial de dados

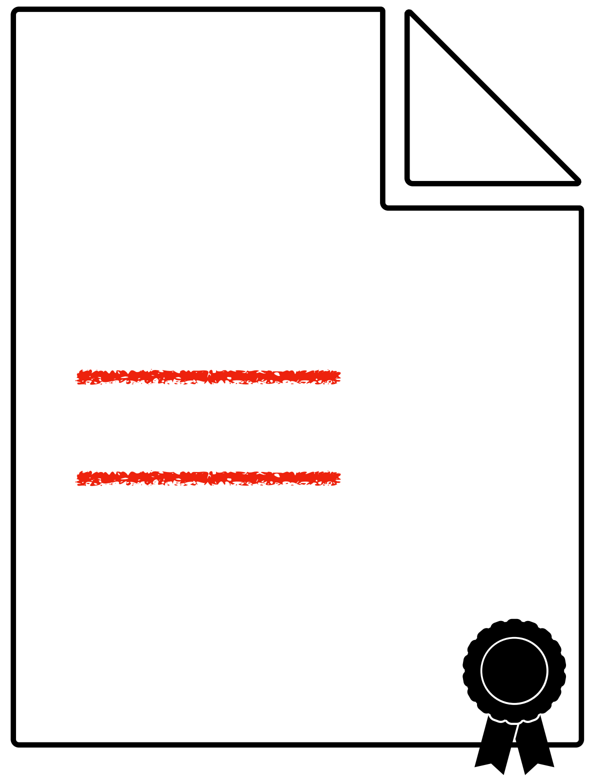
E se as modificações importam?



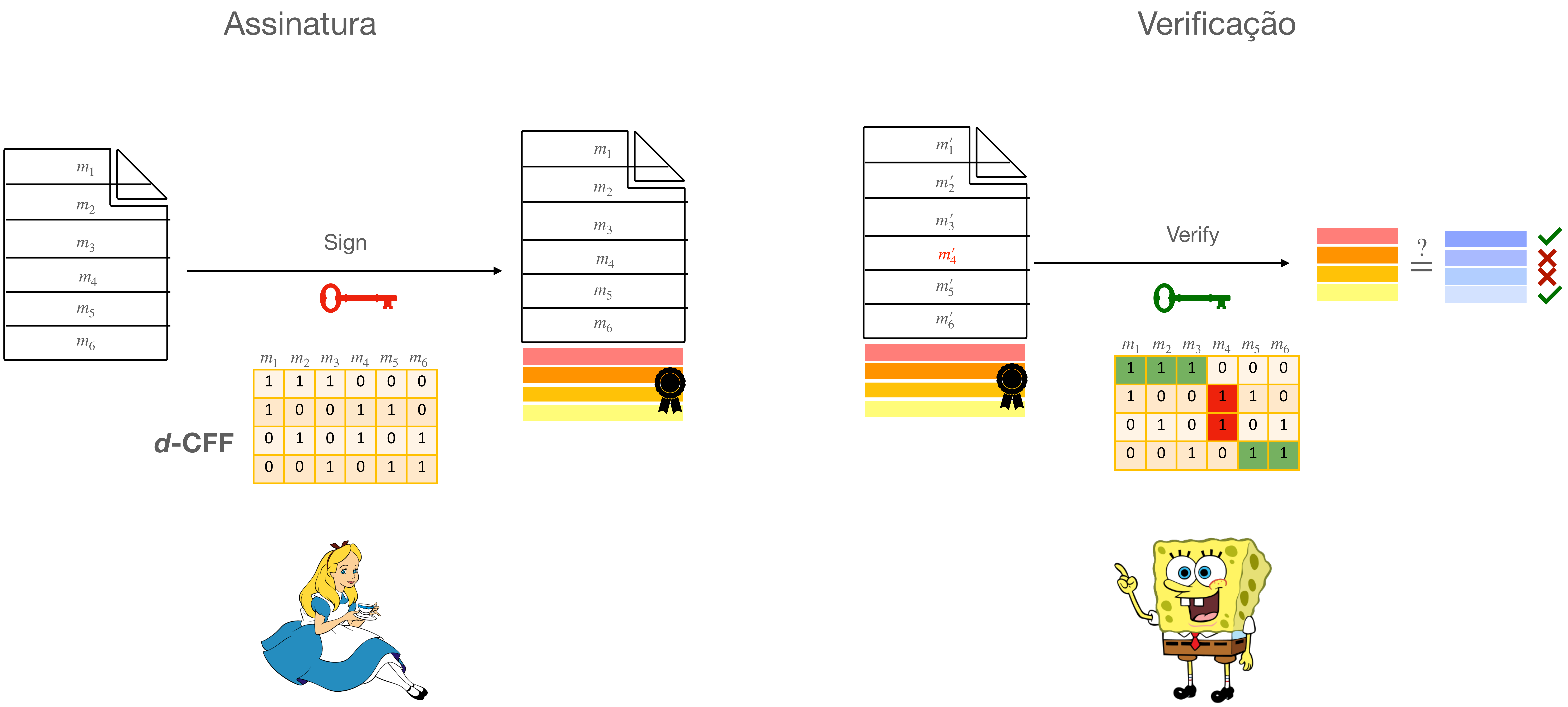
Integridade parcial de dados

E se as modificações importam?

- Um formulário assinado por uma instituição mas preenchido por outra pessoa
- Um documento assinado, com seções privadas que precisam ser escondidas
- Uma grande base de dados assinada, com algumas poucas modificações/erros



Integridade parcial de dados

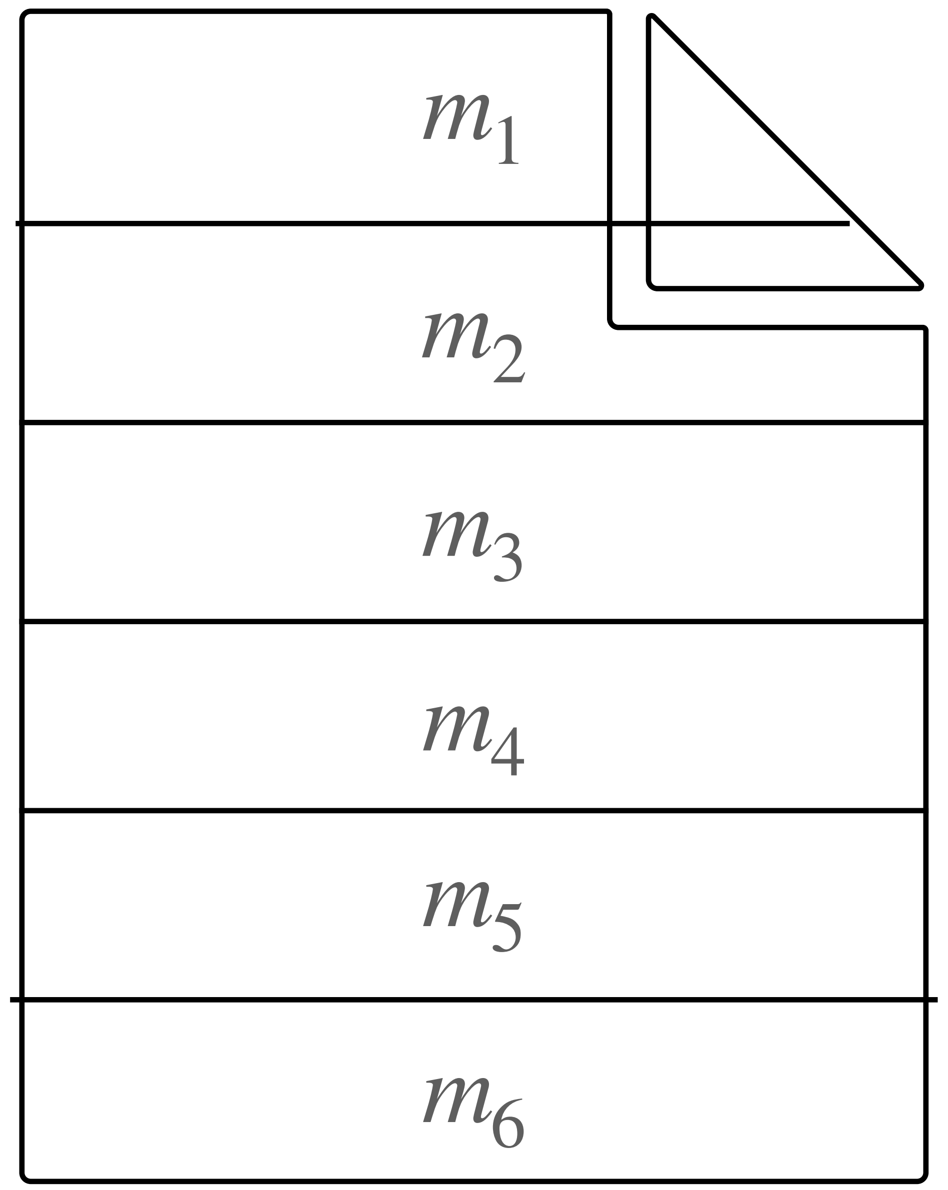


d-CFF

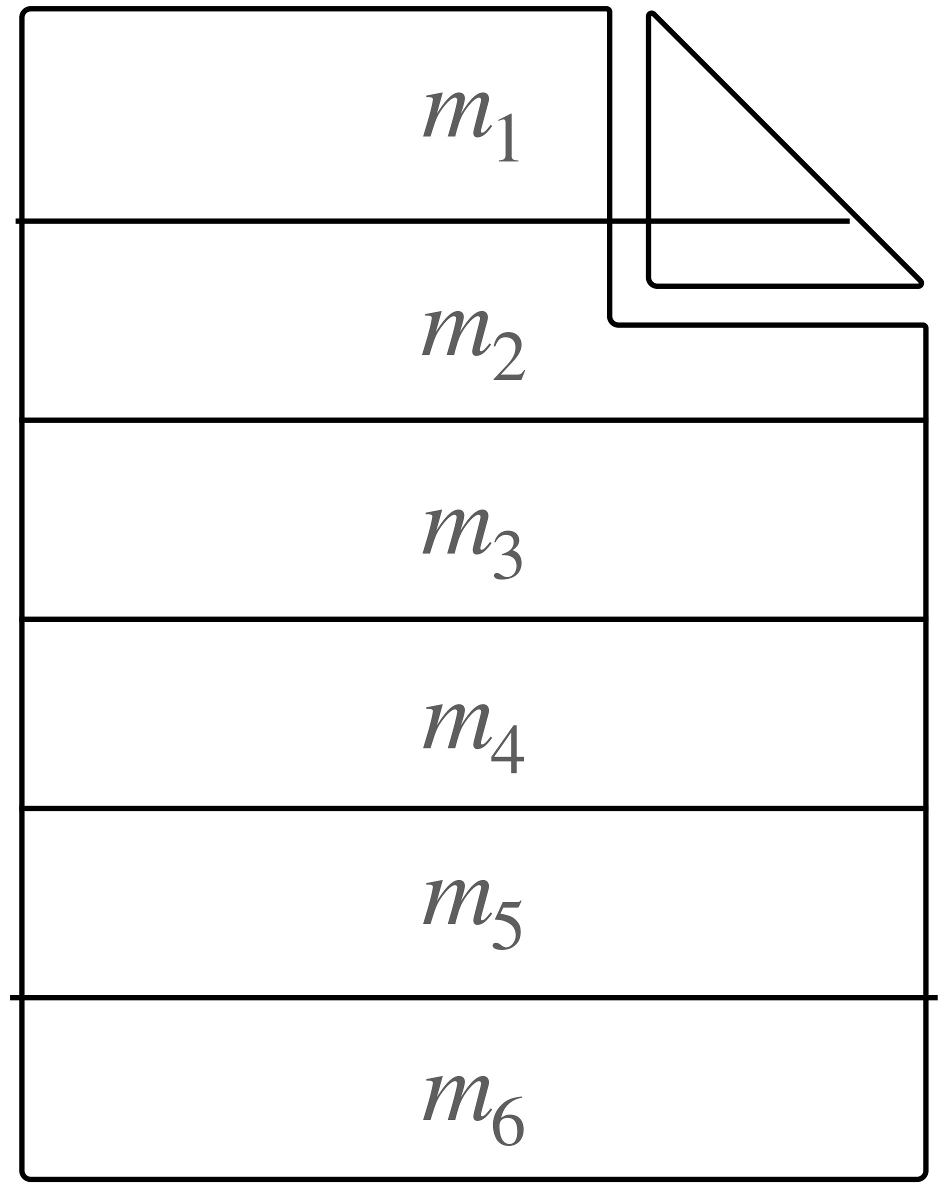
m_1	m_2	m_3	m_4	m_5	m_6
1	1	1	0	0	0
1	0	0	1	1	0
0	1	0	1	0	1
0	0	1	0	1	1

m_1	m_2	m_3	m_4	m_5	m_6
1	1	1	0	0	0
1	0	0	1	1	0
0	1	0	1	0	1
0	0	1	0	1	1

Integridade parcial de dados



Integridade parcial de dados



$h_1 = \text{Hash}(m_1)$

$h_2 = \text{Hash}(m_2)$

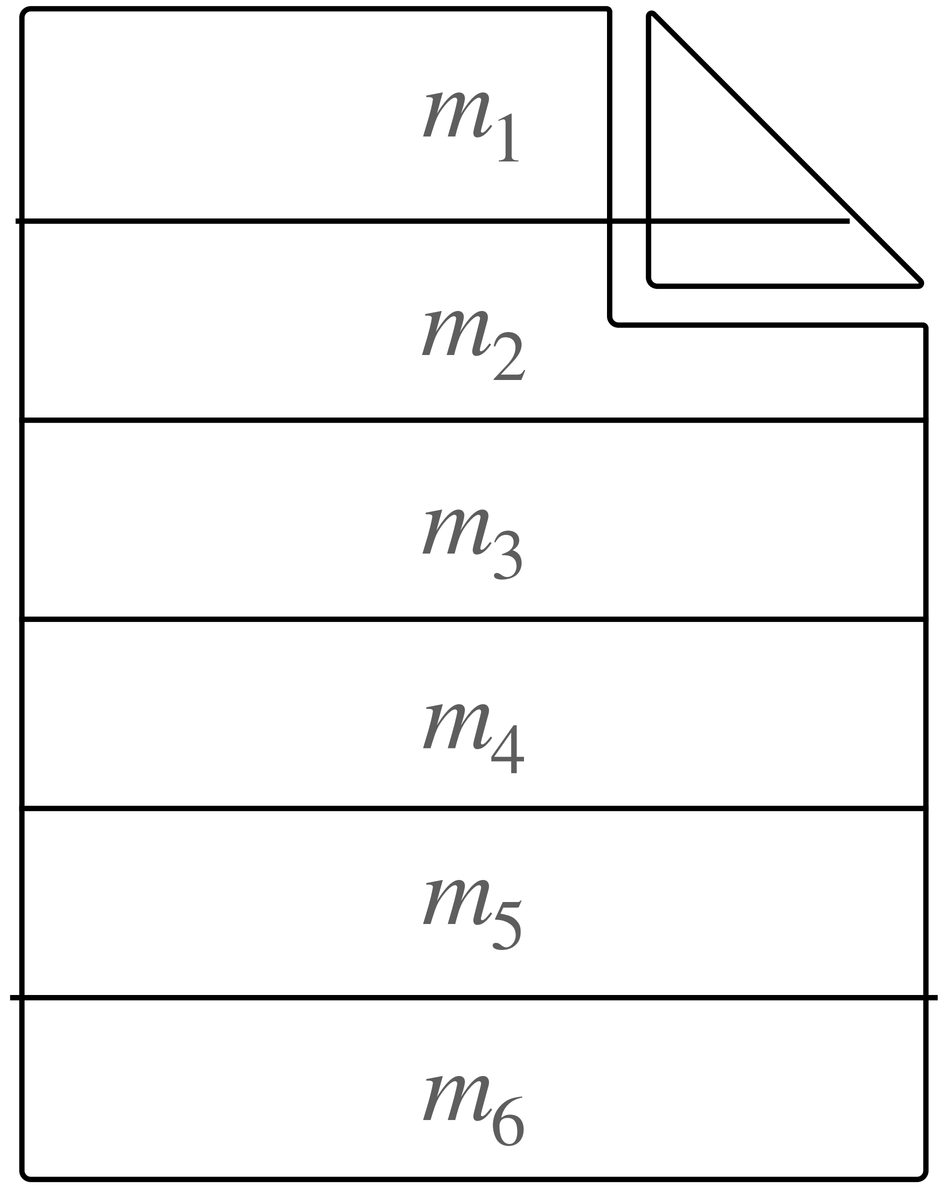
$h_3 = \text{Hash}(m_3)$

$h_4 = \text{Hash}(m_4)$

$h_5 = \text{Hash}(m_5)$

$h_6 = \text{Hash}(m_6)$

Integridade parcial de dados



Assinatura

$Hash(h_1 | h_2 | h_3)$

$Hash(h_1 | h_4 | h_5)$

$Hash(h_2 | h_4 | h_6)$

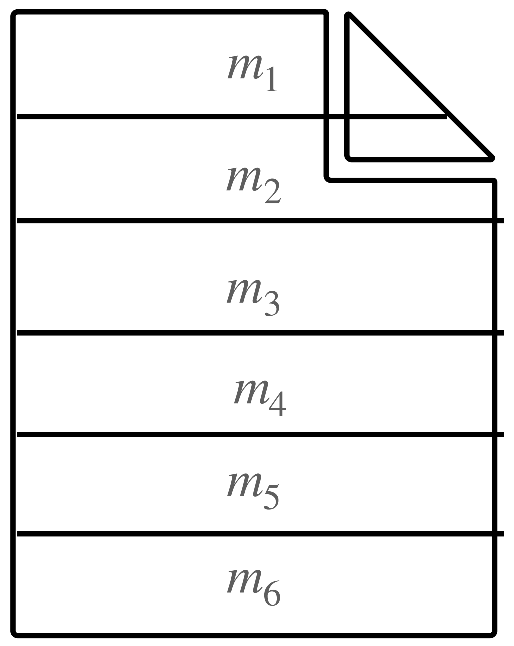
$Hash(h_3 | h_5 | h_6)$

_d_-CFF

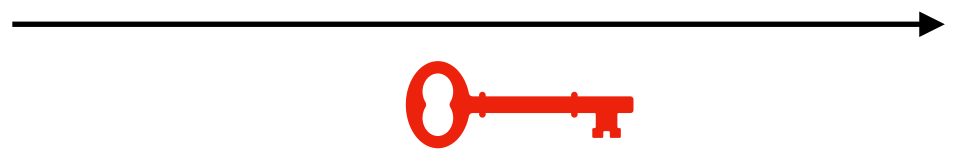
m_1	m_2	m_3	m_4	m_5	m_6
1	1	1	0	0	0
1	0	0	1	1	0
0	1	0	1	0	1
0	0	1	0	1	1

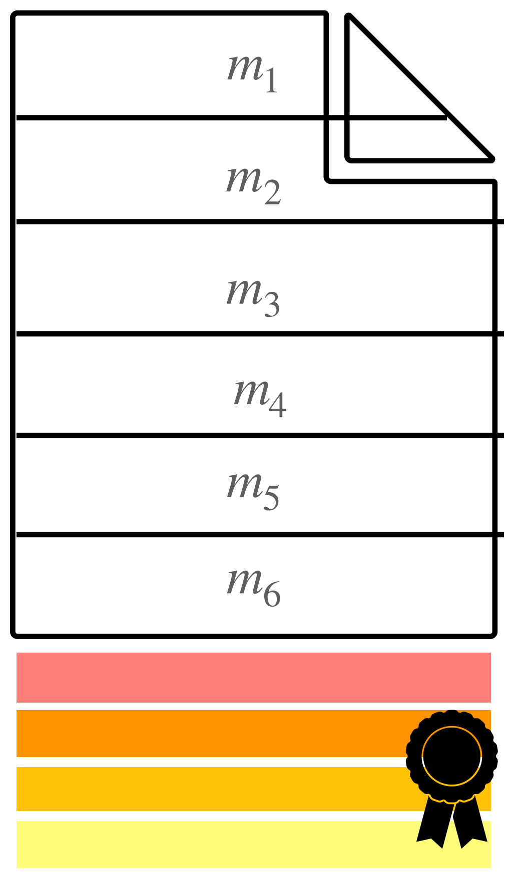
Integridade parcial de dados

Assinatura



Sign



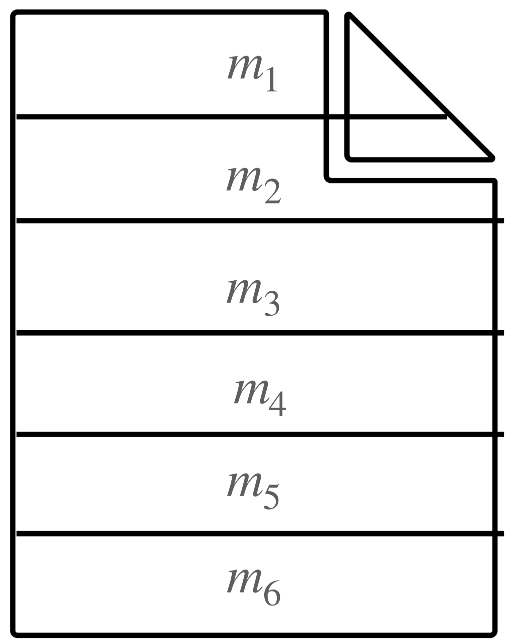


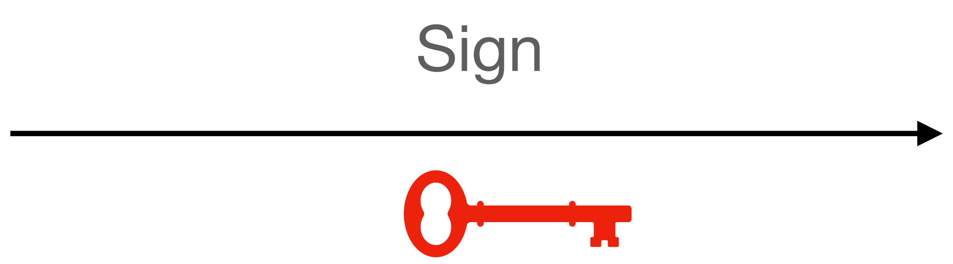
***d*-CFF**

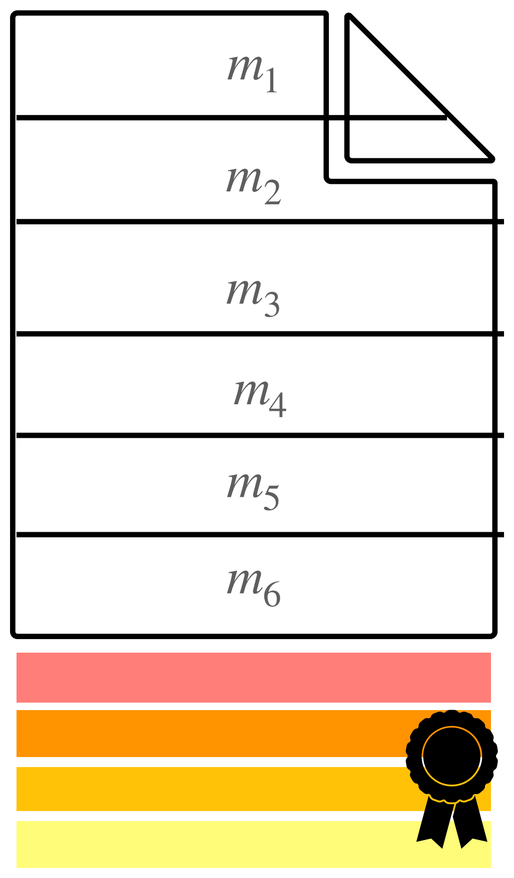
m_1	m_2	m_3	m_4	m_5	m_6
1	1	1	0	0	0
1	0	0	1	1	0
0	1	0	1	0	1
0	0	1	0	1	1

Integridade parcial de dados

Assinatura



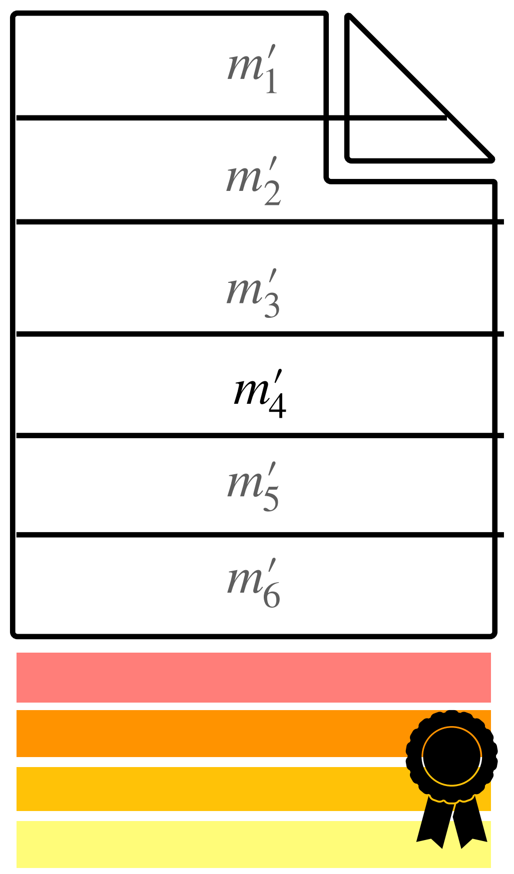


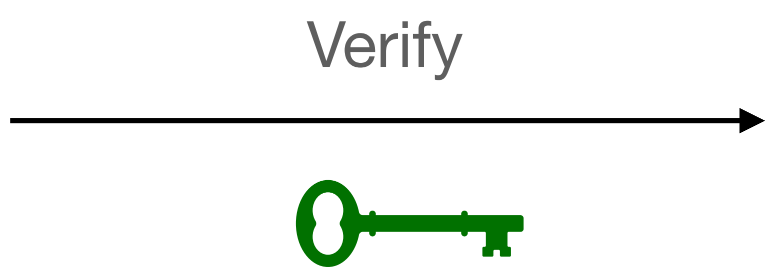


d-CFF

m_1	m_2	m_3	m_4	m_5	m_6
1	1	1	0	0	0
1	0	0	1	1	0
0	1	0	1	0	1
0	0	1	0	1	1

Verificação





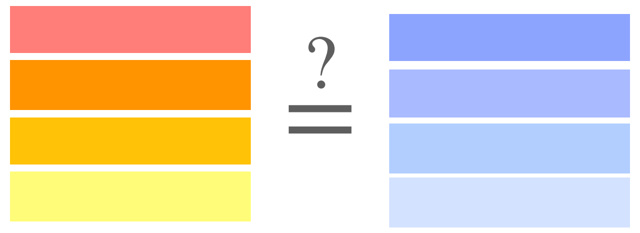
$Hash(h_1' \mid h_2' \mid h_3')$

$Hash(h_1' \mid h_4' \mid h_5')$

$Hash(h_2' \mid h_4' \mid h_6')$

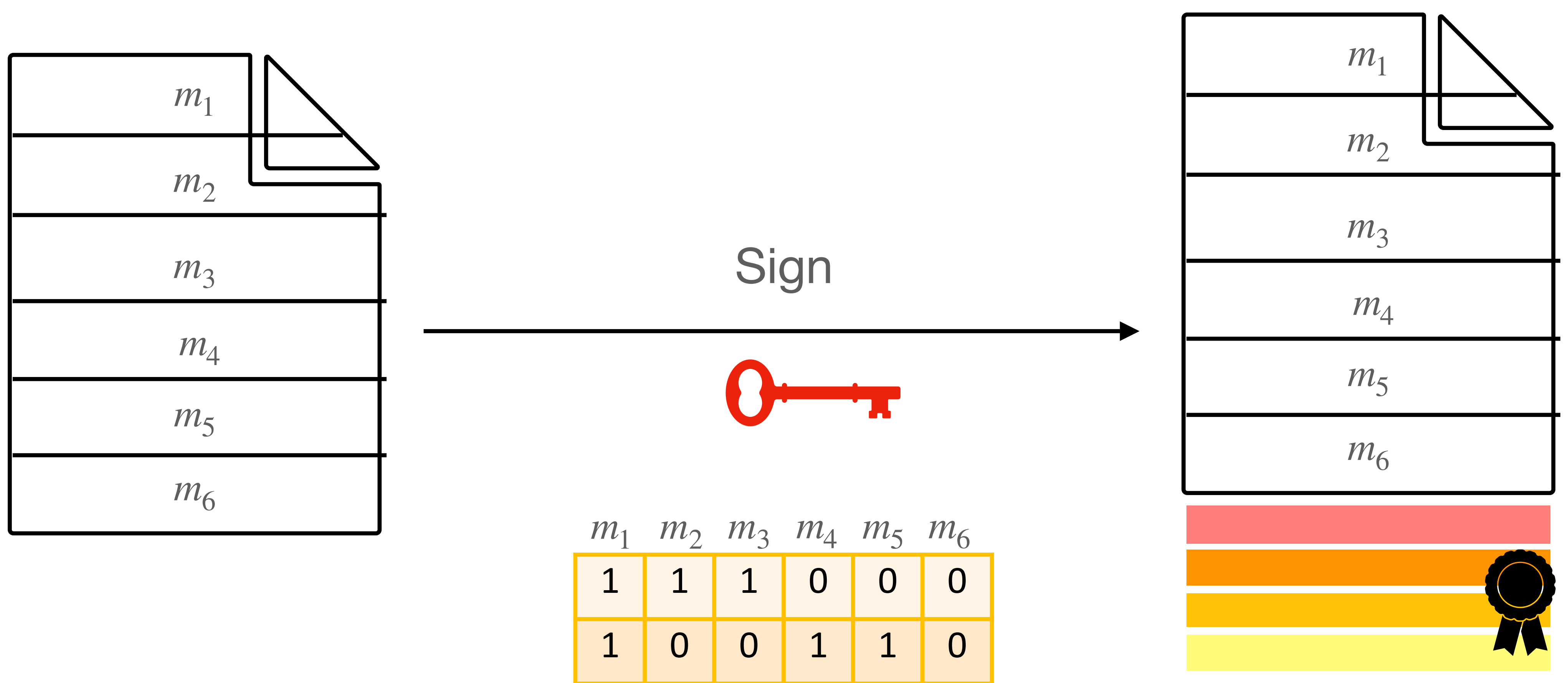
$Hash(h_3' \mid h_5' \mid h_6')$

m_1'	m_2'	m_3'	m_4'	m_5'	m_6'
1	1	1	0	0	0
1	0	0	1	1	0
0	1	0	1	0	1
0	0	1	0	1	1



Integridade parcial de dados

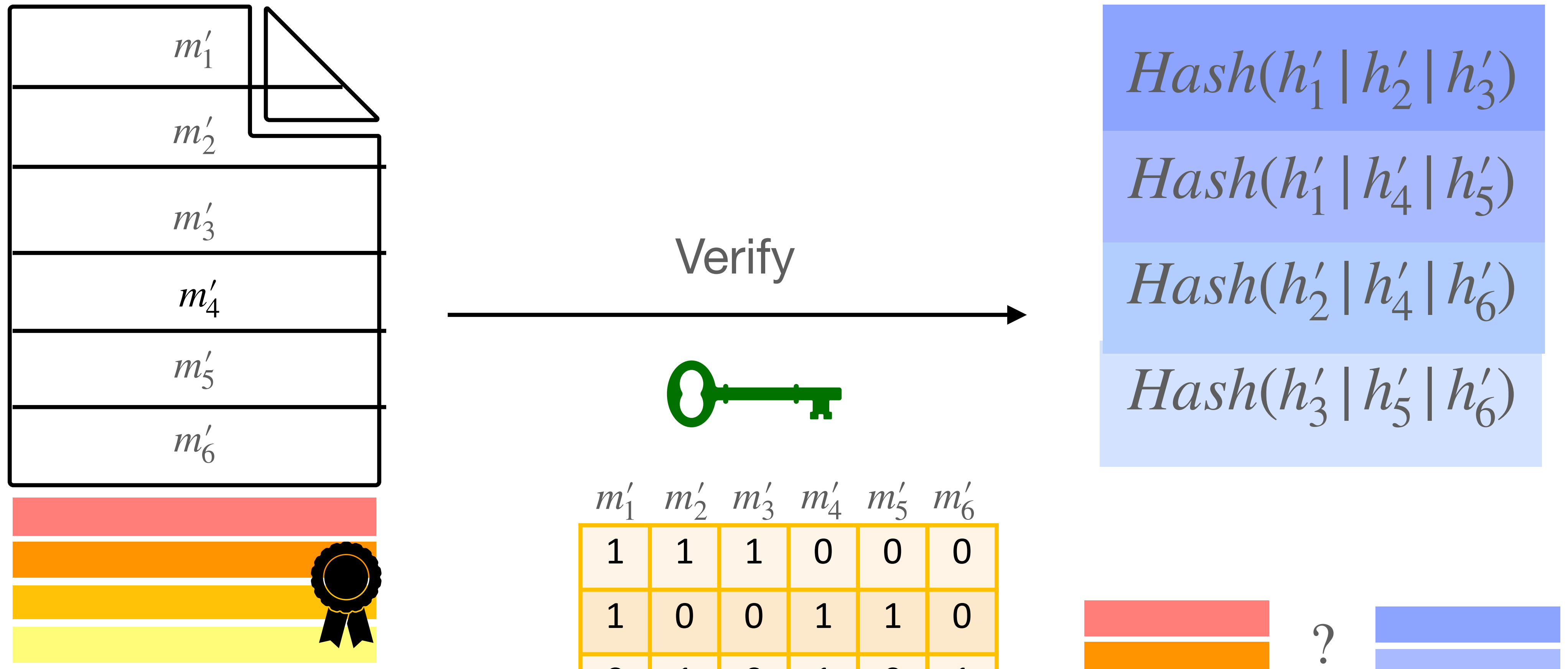
Assinatura



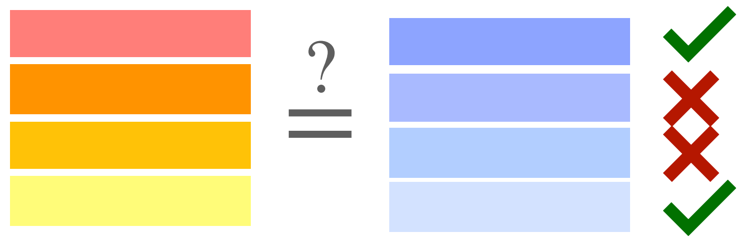
d-CFF

m_1	m_2	m_3	m_4	m_5	m_6
1	1	1	0	0	0
1	0	0	1	1	0
0	1	0	1	0	1
0	0	1	0	1	1

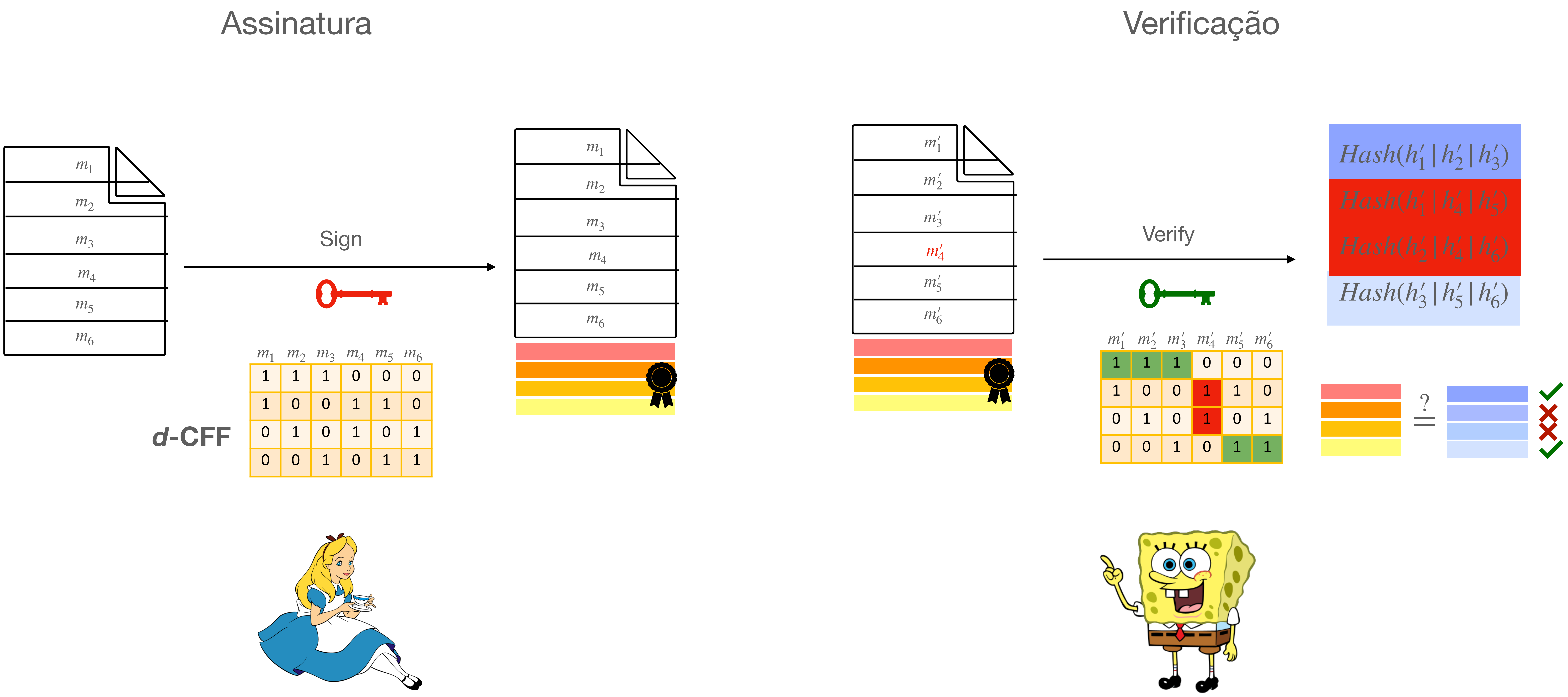
Verificação



m'_1	m'_2	m'_3	m'_4	m'_5	m'_6
1	1	1	0	0	0
1	0	0	1	1	0
0	1	0	1	0	1
0	0	1	0	1	1



Integridade parcial de dados



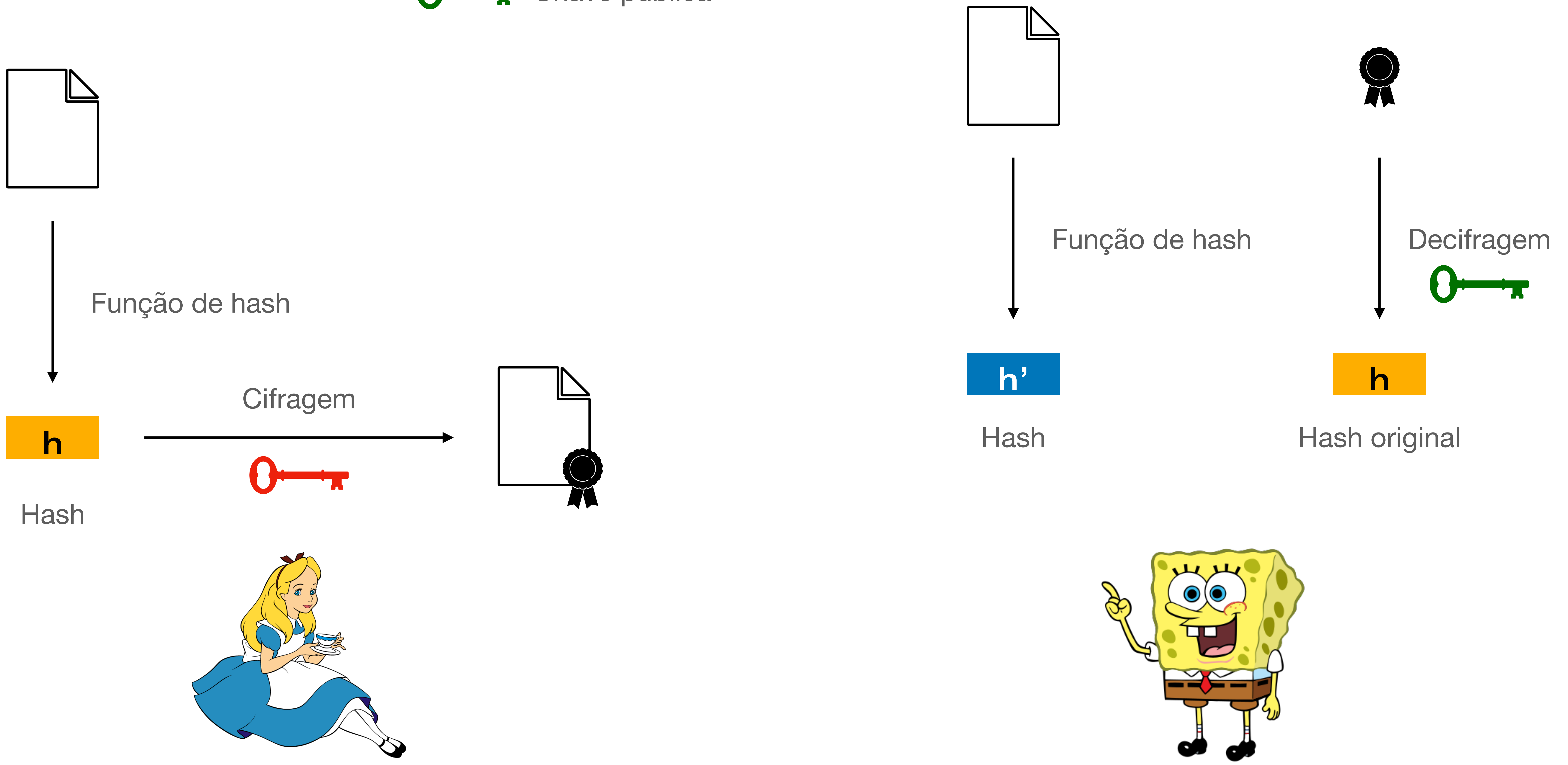
Integridade parcial de dados

- É possível garantir integridade parcial de dados assinados usando d-CFFs
  - as assinaturas aumentam um pouco (~t hashes a mais)
- É possível escolher o *n* e *d* para ter uma maior precisão na localização das modificações
- É importante considerar questões práticas*
  - como dividir um documento em blocos?
  - como a escolha da CFF afeta o tempo de geração/verificação da assinatura?

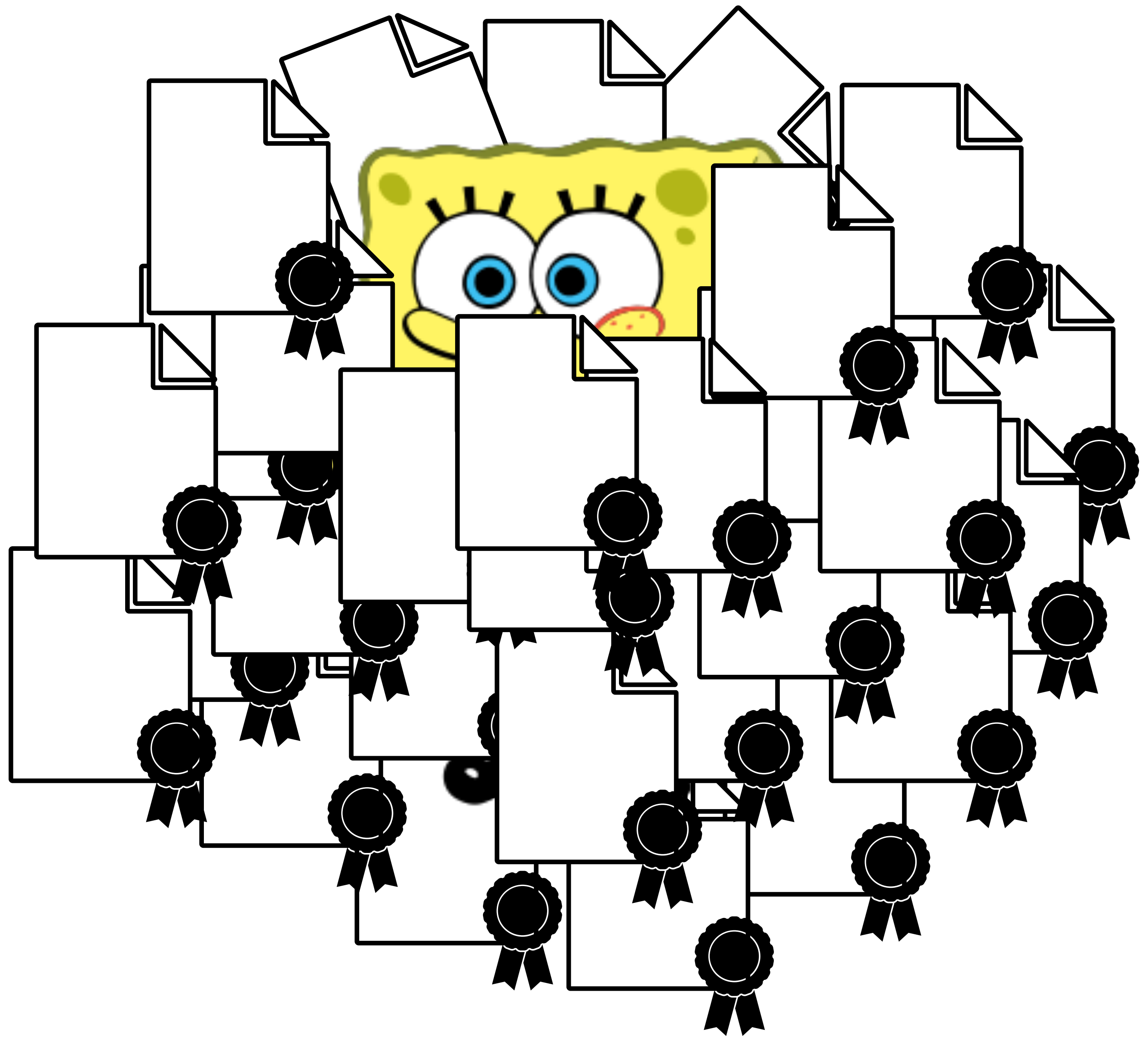
* Practical algorithms and parameters for modification-tolerant signature scheme. Anthony B. Kamers, Paola de O. Abel, Thaís B. Idalino, Gustavo Zambonin, Jean E. Martina. SBSeg 2024

Voltando às assinaturas digitais clássicas

- Verificação da assinatura



O que acontece se tivermos milhares de assinaturas?



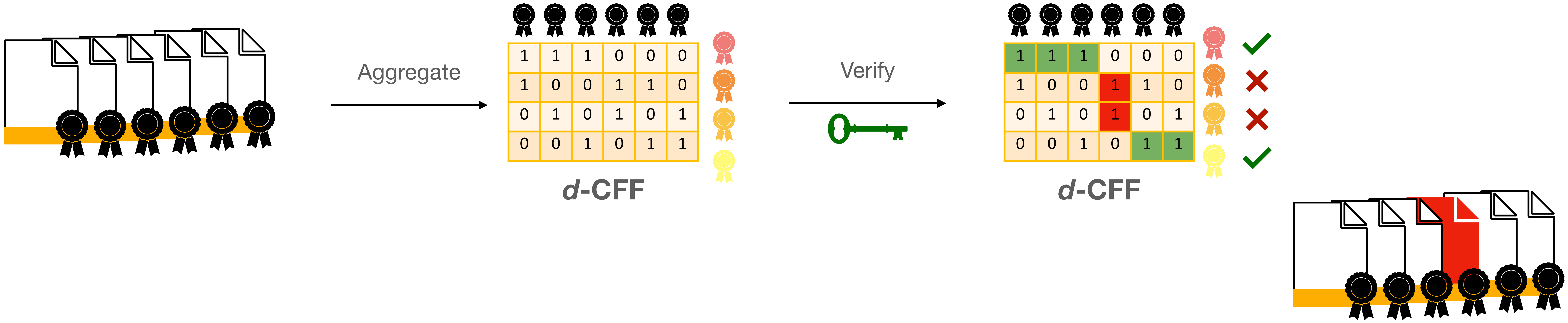
Agregação de assinaturas

Boneh, D., Gentry, C., Lynn, B., Shacham, H.: Aggregate and verifiably encrypted signatures from bilinear maps. In: Advances in Cryptology – EUROCRYPT 2003. Lecture Notes in Computer Science, vol. 2656, pp. 416–432 (2003)

Agregação de assinaturas

Agregação de assinaturas

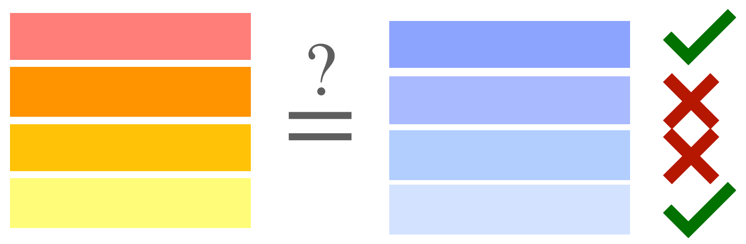
- Dadas *n* assinaturas, usamos uma *d*-CFF(t,n) para gerar *t* agregações
- Verificamos apenas *t* assinaturas e conseguimos identificar até *d* documentos modificados



Resumindo

- Matemática combinatória vai além do que vimos em INE5403
- Existem diversas sub-áreas de pesquisa dentro do assunto
- Diversos problemas interessantes podem se beneficiar de técnicas combinatórias
- Aplicações são uma boa fonte de inspiração na criação de novos objetos matemáticos

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



Obrigada!

Thaís Bardini Idalino
thais.bardini@ufsc.br