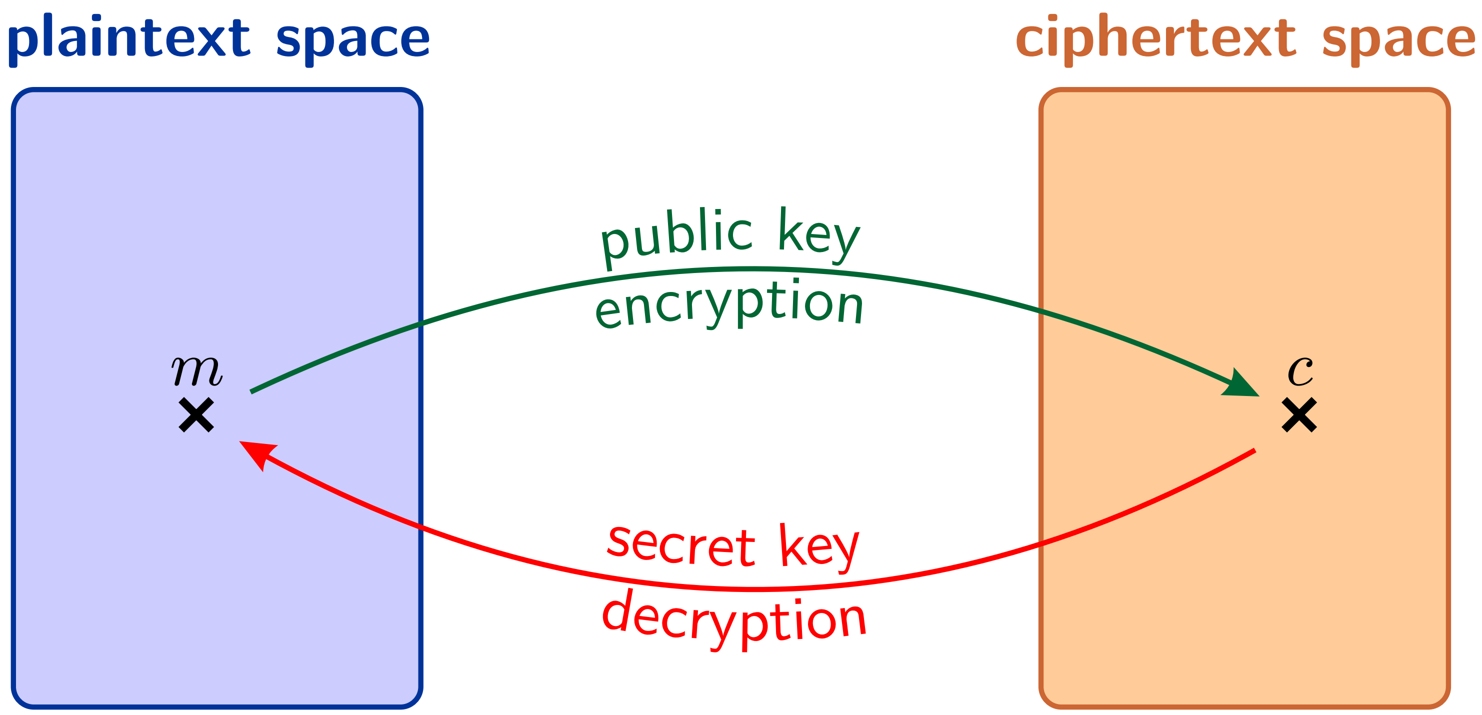
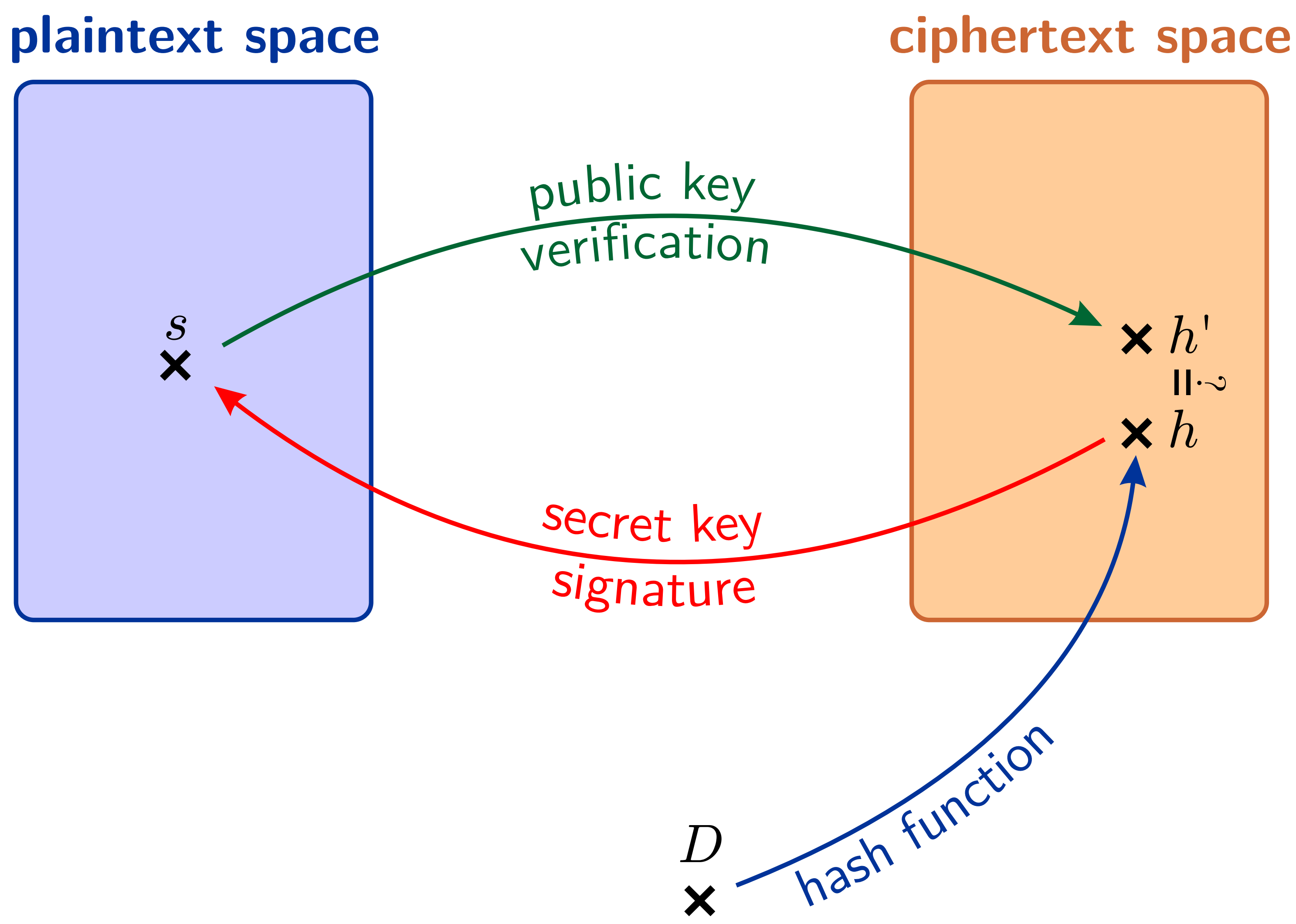
Parallel-CFS
Strengthening the CFS McEliece-Based Signature Scheme

Matthieu Finiasz

ENSTA ParisTech

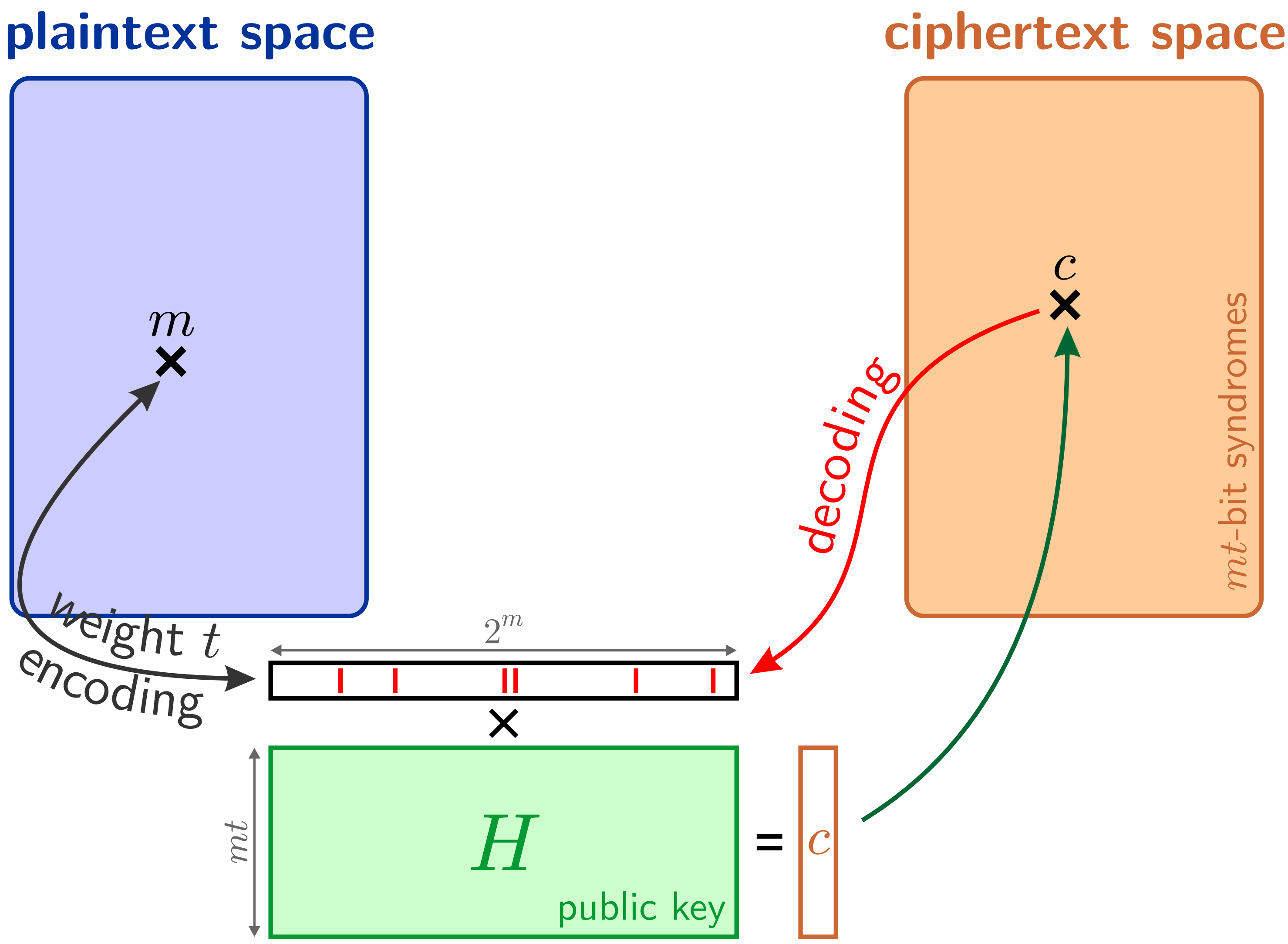


- Any public key encryption can be turned into a signature.

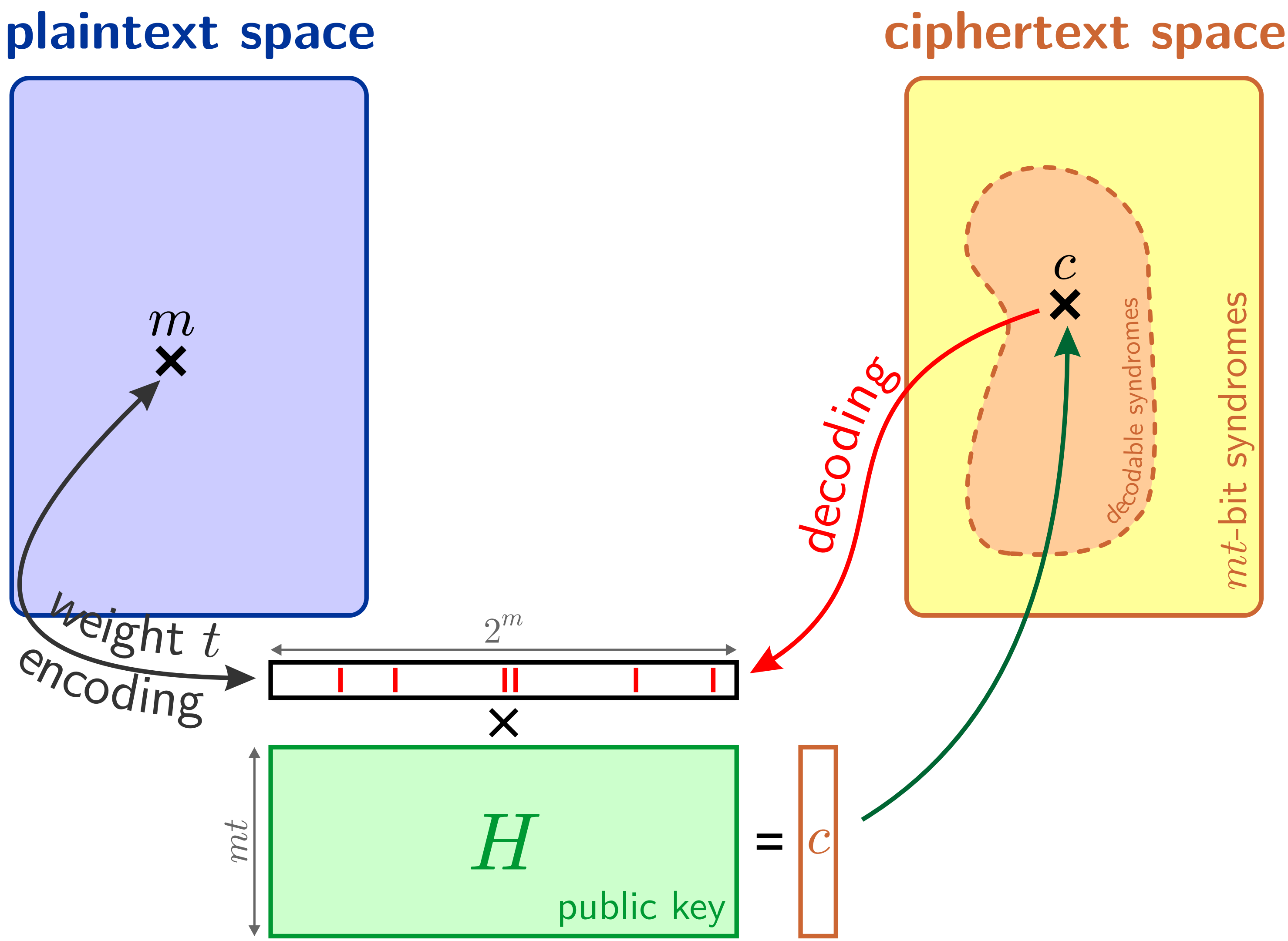


- The document is simply hashed into a random ciphertext.

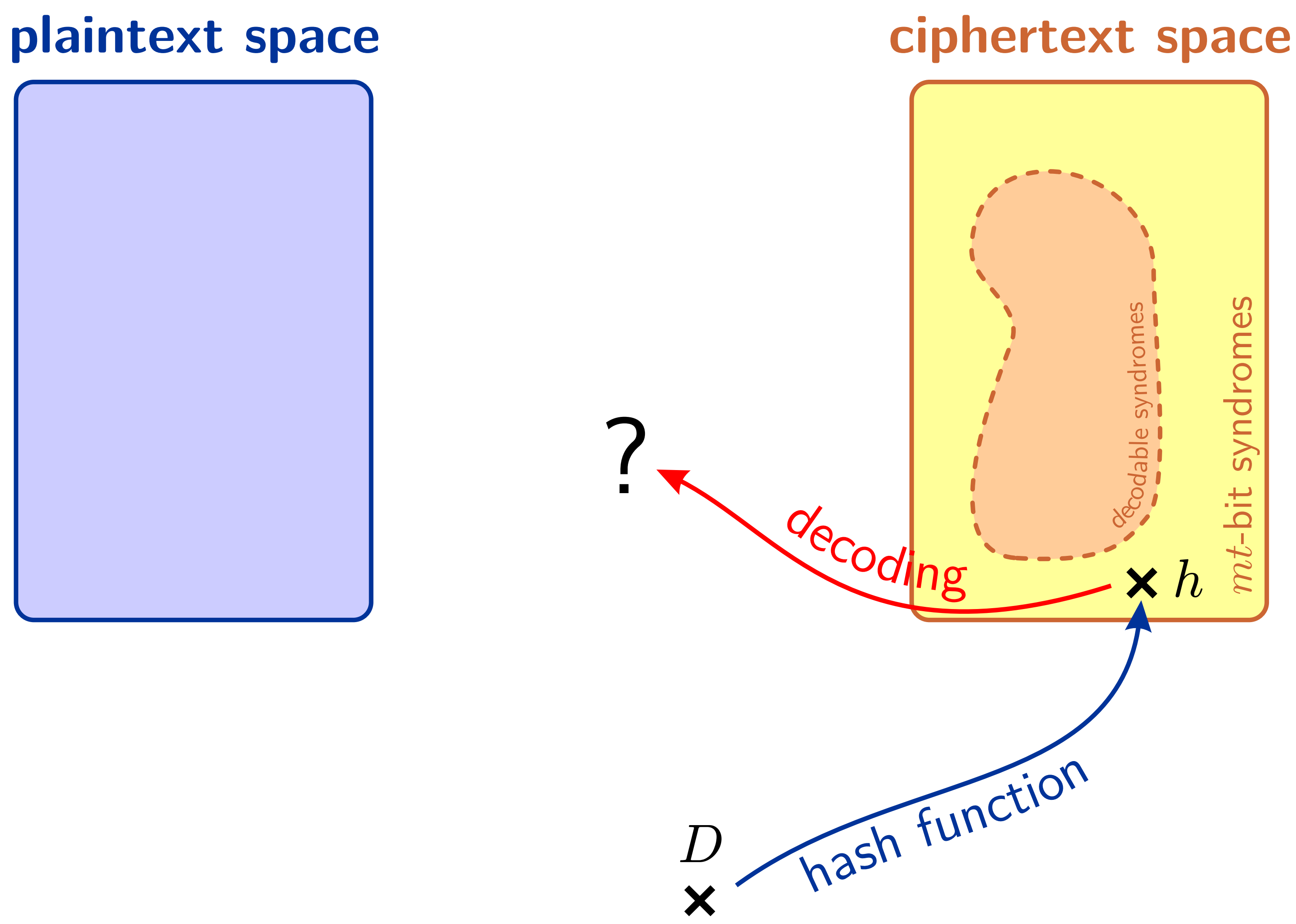
The Niederreiter Cryptosystem



- H is a scrambled Goppa code parity check matrix.

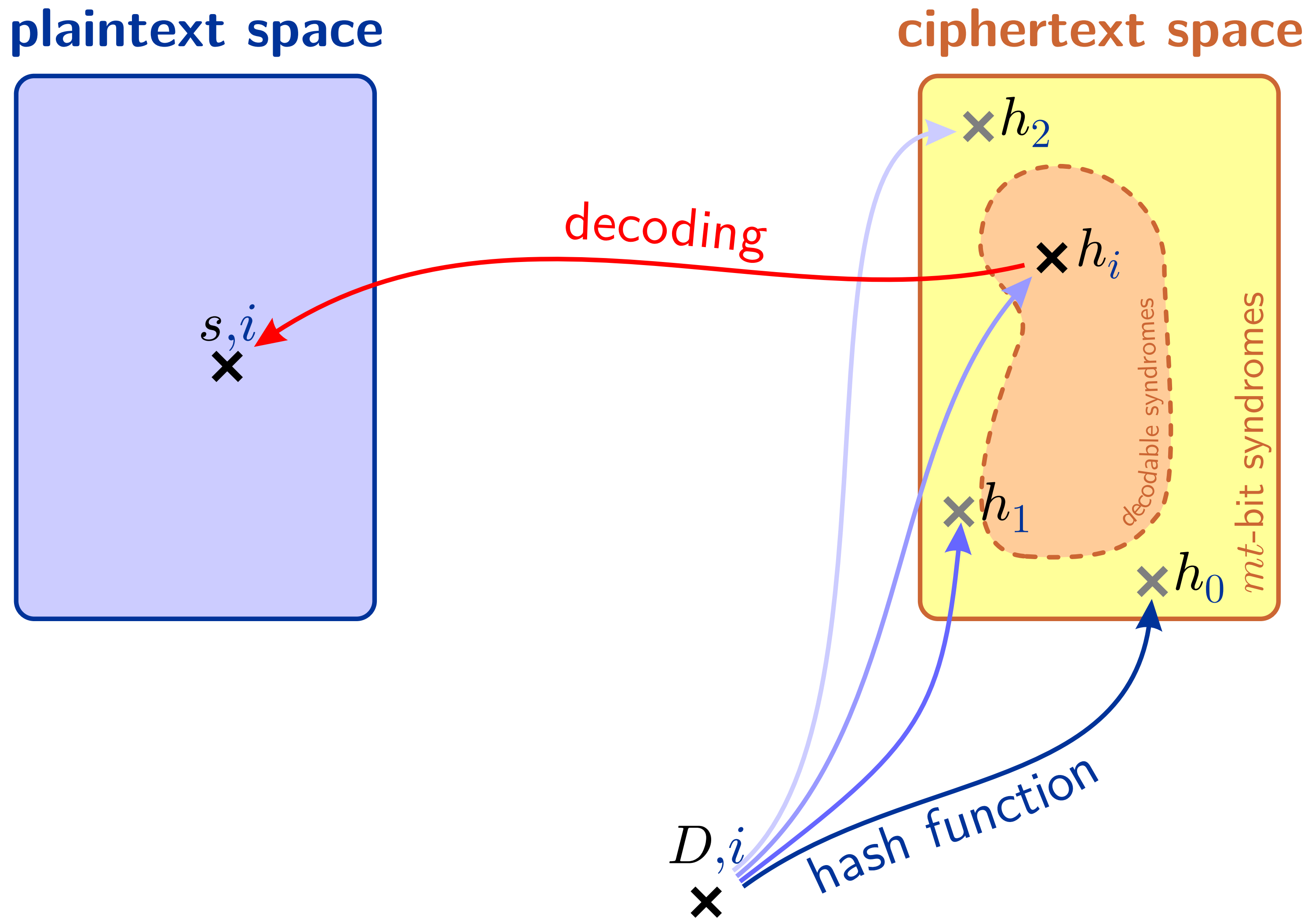


- Ciphertexts are always decodable syndromes...



- Random syndromes are not decodable.

The CFS Signature Scheme
[Courtois-Finiasz-Sendrier 2001]



- A counter i is appended to the document D.

The CFS Signature Scheme
[Courtois-Finiasz-Sendrier 2001]

- Key generation works like for Niederreiter.

- Signature repeats the following steps:
  - compute $h_i = h(D, i)$,
  - try to decode the syndrome h_i into s, success $\sim \frac{1}{t!}$
  - the signature is (s, i_0) for the first decodable h_{i_0}.

- Verification is simple and fast:
  - compute $h_{i_0} = h(D, i_0)$,
  - compute e_s, the word of weight t corresponding to s,
  - compare h_{i_0} and $H \times e_s$.

- When attacking Niederreiter, one has to find the error pattern corresponding to a given syndrome:

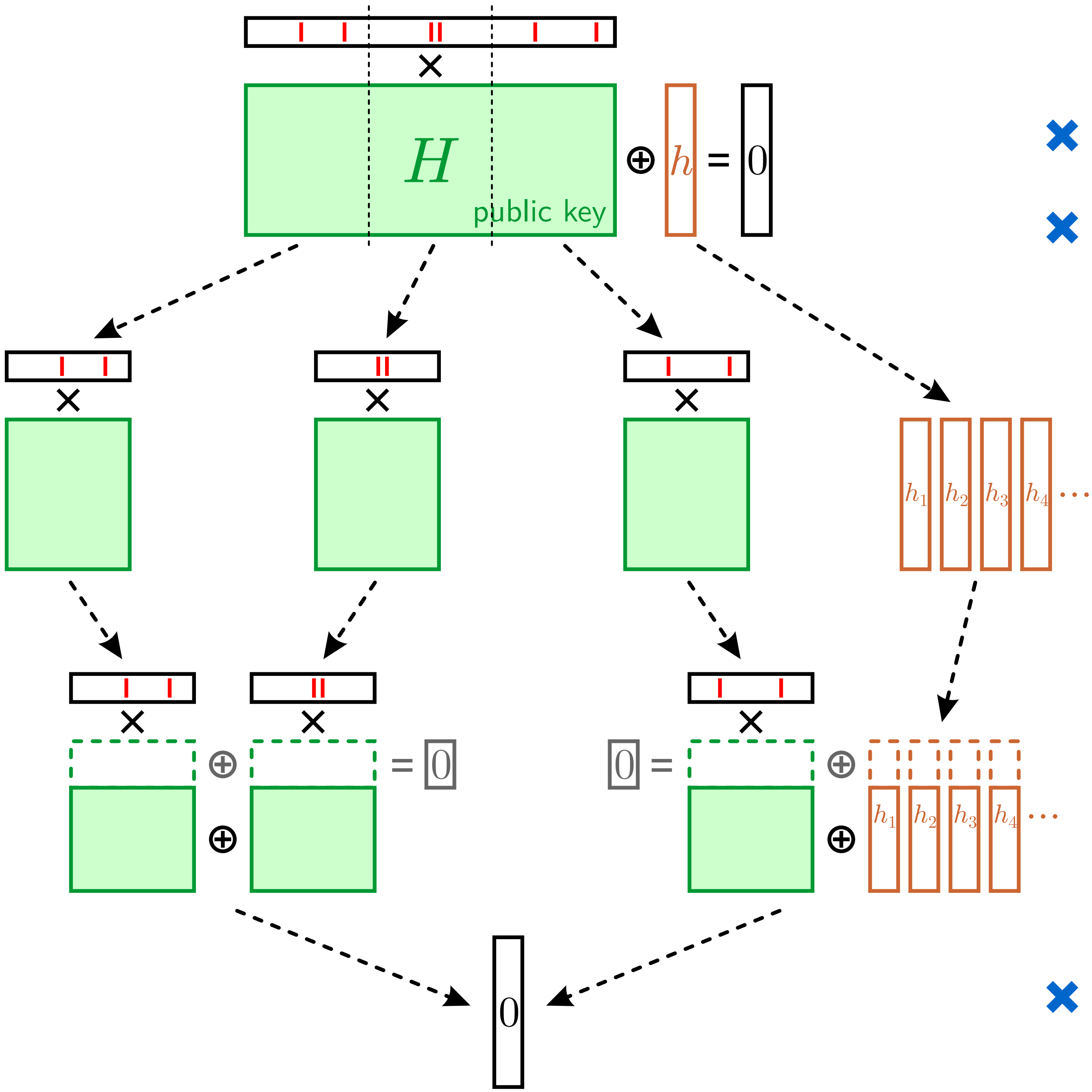
Syndrome Decoding (SD)

Input: A binary matrix H, a weight t and a target syndrome s.
Problem: Find e of weight at most t such that $H \times e = s$.

- When attacking CFS, one has to find an error pattern corresponding to one of the h_i:

One out of Many Syndrome Decoding (OMSD)

Input: A binary matrix H, a weight t and a set $\mathcal{L}$ of syndromes.
Problem: Find e of weight at most t such that $H \times e \in \mathcal{L}$.



- Build 4 lists
- Merge them
  - zero some bits
- Lists remain small

- The size of the lists of low weight syndromes is limited
  - it is compensated by a larger list of hashes.
- One obtains the following complexity formulas:

$$\text{Complexity} = L\log(L), \ \text{with}$$

$$L = \min\left(\frac{2^{mt}}{\binom{2^m}{t-\lfloor t/3\rfloor}}, \sqrt{\frac{2^{mt}}{\binom{2^m}{\lfloor t/3\rfloor}}}\right).$$

- Asymptotically the cost of an attack is $2^{\frac{mt}{3}}$ instead of $2^{\frac{mt}{2}}$ for SD.

Parallel-CFS

- Instead of signing one hash, one uses two (or i) different hash functions and signs each hash.

- Instead of signing one hash, one uses two (or i) different hash functions and signs each hash.
- Using a counter is no longer possible:
  - using different counters makes parallelism useless,
  - with one counter, the probability of having 2 decodable syndromes simultaneously is too small:
    → cost of signing would be $t!^2$ instead of $t!$,

- Instead of signing one hash, one uses two (or i) different hash functions and signs each hash.
- Using a counter is no longer possible:
  - using different counters makes parallelism useless,
  - with one counter, the probability of having 2 decodable syndromes simultaneously is too small:
    → cost of signing would be $t!^2$ instead of $t!$,
- We use a CFS variant based on complete decoding:
  - the signature is a word of weight $t + \delta$,
  - δ positions are searched for exhaustively,
  - cost/signature size are roughly the same

- Using the CFS variant allows to sign almost every hash:
  - signing every hash requires to know the covering radius
  - δ is chosen so that $\binom{2^m}{t+\delta} > 2^{mt}$,
    → mostly negligible probability of non signability.

- Allowing $t+\delta$ errors makes OMSD attacks easier:
  - the first 3 lists can be larger,
  - when $\binom{2^m}{t+\delta} = 2^{mt}$ the attack costs exactly $2^{\frac{mt}{3}}$.
- To simplify computations we consider $\binom{2^m}{t+\delta} = 2^{mt}$,
  - in practice the 3 lists can be slightly larger, but the gain in terms of attack cost is negligible.

Attacking Parallel-CFS

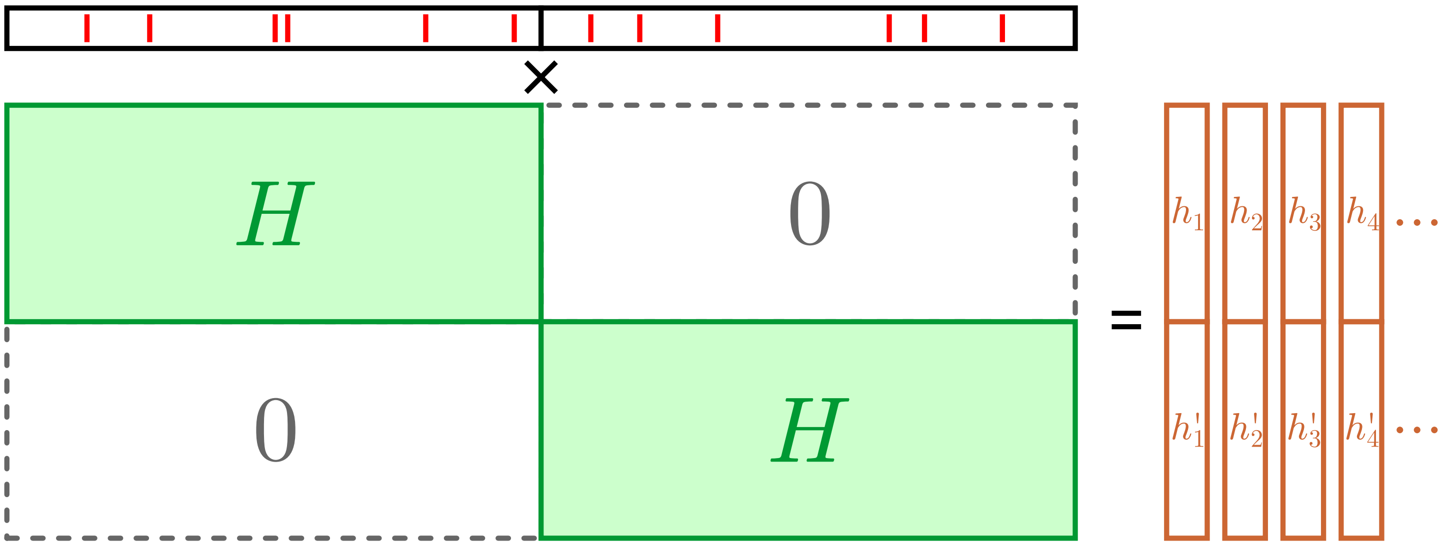
- There is not a unique way of attacking Parallel-CFS.

- Using two independent SD attacks:
  - the cost of such an attack is well known

    [Finiasz, Sendrier - Asiacrypt 2009]
  - gives a reference security of the order of $2^{\frac{mt}{2}}$.

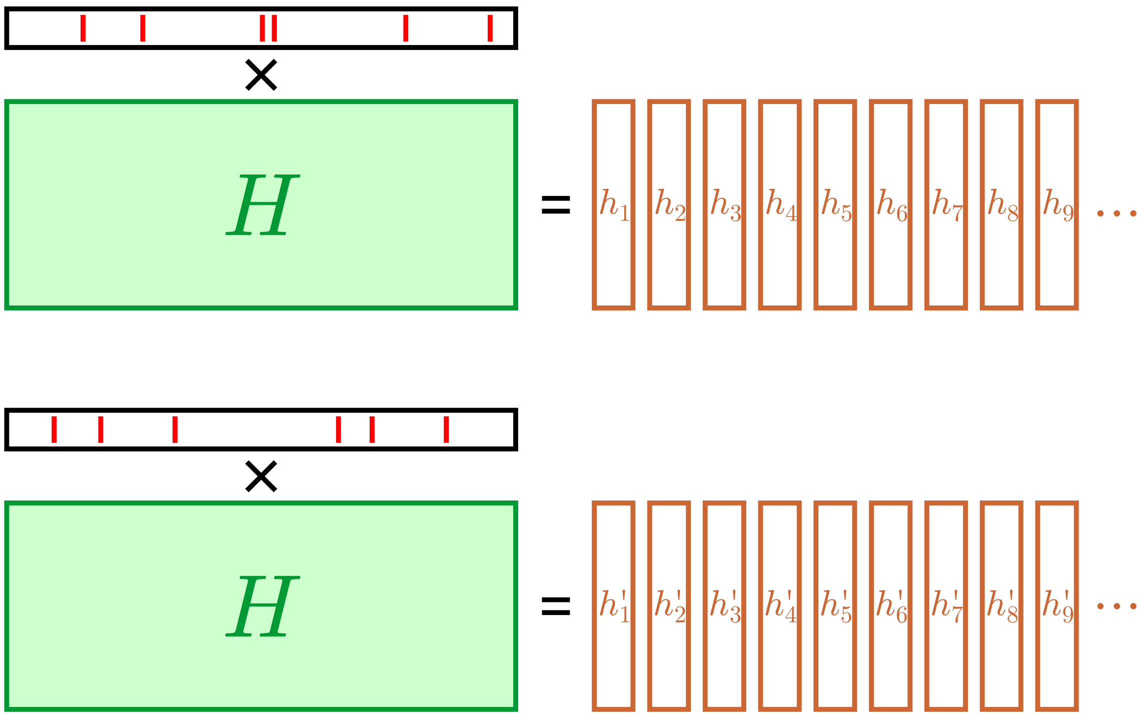
- Using OMSD two strategies are possible:
  - attack both instances in parallel,
  - attack them sequentially.

- This strategy considers one "double size" instance:



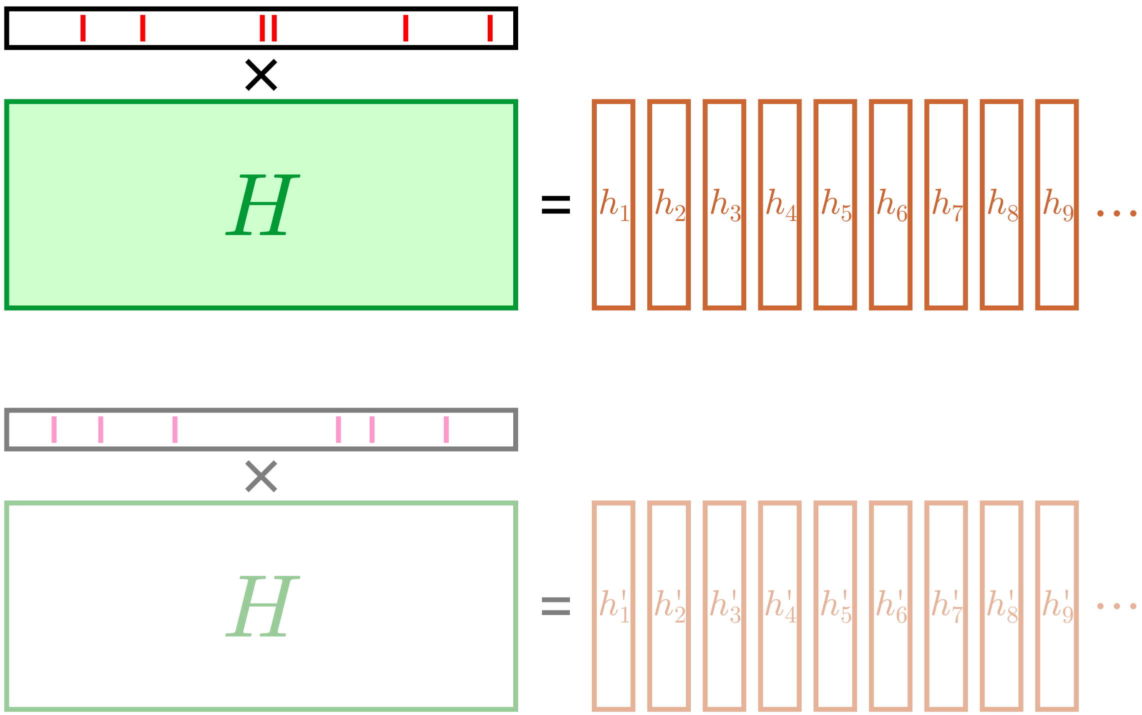
- Here, the cost of the attack is of the order of $2^{\frac{2}{3}mt}$,
  - this attack is more expensive than direct SD attacks.

- One has to solve two instances with "linked" syndromes:



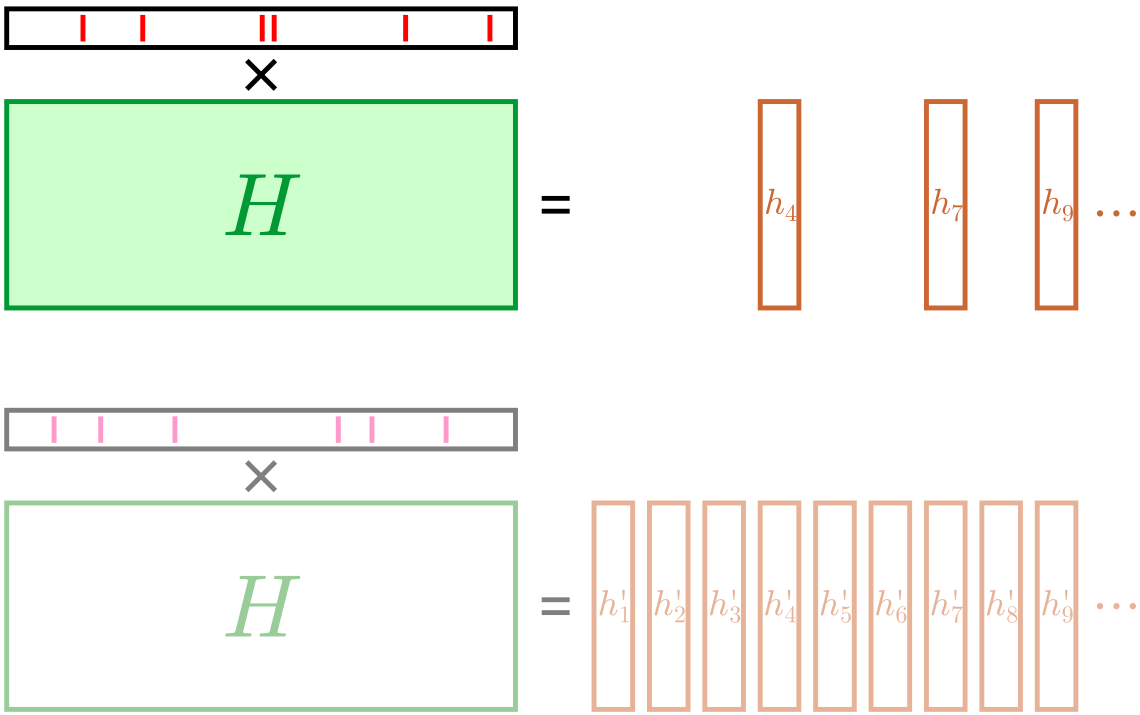
- The forgeries must be for h_i and h'_i with the same i.

- One has to solve two instances with "linked" syndromes:



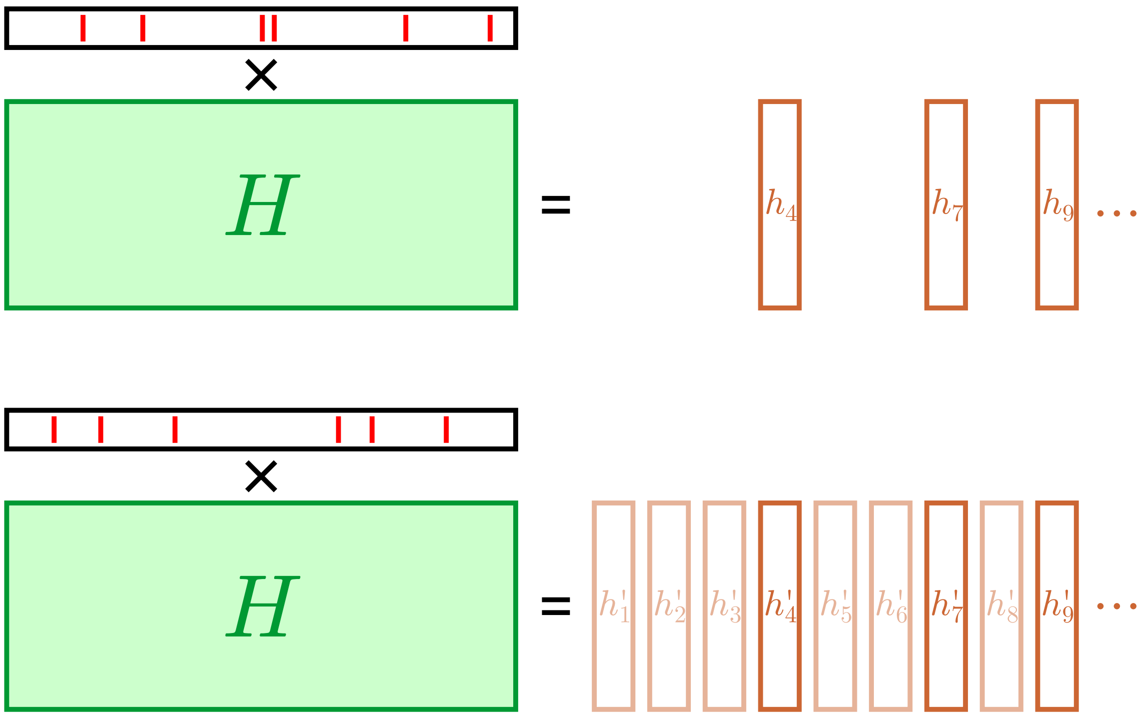
- Start by solving the first instance

- One has to solve two instances with “linked” syndromes:



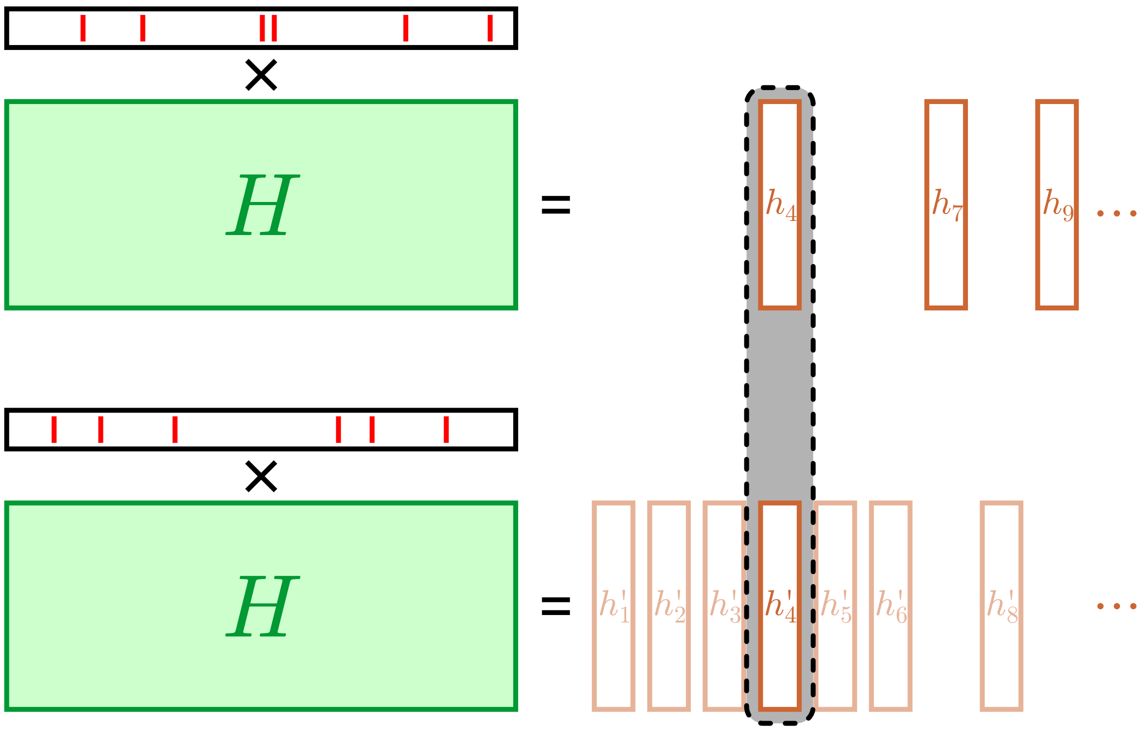
- Start by solving the first instance
  - find several solutions, and keep them

- One has to solve two instances with "linked" syndromes:



- Start by solving the first instance
  - find several solutions, and keep them
  - solve the second instance with the associated list.

- One has to solve two instances with "linked" syndromes:



- The same technique can be chained i times for order i parallel-CFS,
  - each step will reduce the number of target syndromes.

- The attack complexity depends on the costs of finding:
  - 2^{c_1} solutions with unlimited target syndromes,
  - $2^{c_{j+1}}$ solutions given 2^{c_j} target syndromes.
- The cost of this attack is asymptotically:

$$\text{Complexity} = iL\log(L), \text{ with } L = 2^{\frac{2^i-1}{2^{i+1}-1}mt}.$$

- The exponent follows the series $\frac{1}{3}, \frac{3}{7}, \frac{7}{15}, \frac{15}{31}\ldots$
  - asymptotic complexity can never reach $2^{\frac{mt}{2}}$,
  - $i = 2$ or 3 is already very close.

Parameter Examples

Fast signature

parameters				ISD security	security against (chained) GBA	sign. failure probability	public key size	sign. cost	sign. size
m	t	δ	i						
20	8	2	1	$2^{81.0}$	$2^{59.1}$	~ 0	20.0 MB	$2^{15.3}$	98
–	–	–	2	–	$2^{75.7}$	~ 0	–	$2^{16.3}$	196
–	–	–	3	–	$2^{82.5}$	~ 0	–	$2^{16.9}$	294
16	9	2	1	$2^{76.5}$	$2^{53.6}$	2^{-155}	1.1 MB	$2^{18.5}$	81
–	–	–	2	–	$2^{68.7}$	2^{-154}	–	$2^{19.5}$	162
–	–	–	3	–	$2^{74.9}$	2^{-153}	–	$2^{20.0}$	243
18	9	2	1	$2^{84.5}$	$2^{59.8}$	2^{-1700}	5.0 MB	$2^{18.5}$	96
–	–	–	2	–	$2^{76.5}$	2^{-1700}	–	$2^{19.5}$	192
–	–	–	3	–	$2^{83.4}$	2^{-1700}	–	$2^{20.0}$	288
19	9	2	1	$2^{88.5}$	$2^{62.8}$	~ 0	10.7 MB	$2^{18.5}$	103
–	–	–	2	–	$2^{80.5}$	~ 0	–	$2^{19.5}$	206
–	–	–	3	–	$2^{87.7}$	~ 0	–	$2^{20.0}$	309
15	10	3	1	$2^{76.2}$	$2^{55.6}$	~ 0	0.6 MB	$2^{21.8}$	90
–	–	–	2	–	$2^{71.3}$	~ 0	–	$2^{22.8}$	180
–	–	–	3	–	$2^{77.7}$	~ 0	–	$2^{23.4}$	270
16	10	2	1	$2^{86.2}$	$2^{59.1}$	2^{-13}	1.2 MB	$2^{21.8}$	90
–	–	–	2	–	$2^{75.7}$	2^{-12}	–	$2^{22.8}$	180
–	–	–	3	–	$2^{82.5}$	$2^{-11.3}$	–	$2^{23.4}$	270
17	10	2	1	$2^{90.7}$	$2^{62.5}$	2^{-52}	2.7 MB	$2^{21.8}$	98
–	–	–	2	–	$2^{80.0}$	2^{-51}	–	$2^{22.8}$	196
–	–	–	3	–	$2^{87.2}$	2^{-50}	–	$2^{23.4}$	294

parameters				ISD security	security against (chained) GBA	sign. failure probability	public key size	sign. cost	sign. size
m	t	δ	i						
20	8	2	1	$2^{81.0}$	$2^{59.1}$	~ 0	20.0 MB	$2^{15.3}$	98
–	–	–	2	–	$2^{75.7}$	~ 0	–	$2^{16.3}$	196
–	–	–	3	–	$2^{82.5}$	~ 0	–	$2^{16.9}$	294
16	9	2	1	$2^{76.5}$	$2^{53.6}$	2^{-155}	1.1 MB	$2^{18.5}$	81
–	–	–	2	–	$2^{68.7}$	2^{-154}	–	$2^{19.5}$	162
–	–	–	3	–	$2^{74.9}$	2^{-153}	–	$2^{20.0}$	243
18	9	2	1	$2^{84.5}$	$2^{59.8}$	2^{-1700}	5.0 MB	$2^{18.5}$	96
–	–	–	2	–	$2^{76.5}$	2^{-1700}	–	$2^{19.5}$	192
–	–	–	3	–	$2^{83.4}$	2^{-1700}	–	$2^{20.0}$	288
19	9	2	1	$2^{88.5}$	$2^{62.8}$	~ 0	10.7 MB	$2^{18.5}$	103
–	–	–	2	–	$2^{80.5}$	~ 0	–	$2^{19.5}$	206
–	–	–	3	–	$2^{87.7}$	~ 0	–	$2^{20.0}$	309
15	10	3	1	$2^{76.2}$	$2^{55.6}$	~ 0	0.6 MB	$2^{21.8}$	90
–	–	–	2	–	$2^{71.3}$	~ 0	–	$2^{22.8}$	180
–	–	–	3	–	$2^{77.7}$	~ 0	–	$2^{23.4}$	270
16	10	2	1	$2^{86.2}$	$2^{59.1}$	2^{-13}	1.2 MB	$2^{21.8}$	90
–	–	–	2	–	$2^{75.7}$	2^{-12}	–	$2^{22.8}$	180
–	–	–	3	–	$2^{82.5}$	$2^{-11.3}$	–	$2^{23.4}$	270
17	10	2	1	$2^{90.7}$	$2^{62.5}$	2^{-52}	2.7 MB	$2^{21.8}$	98
–	–	–	2	–	$2^{80.0}$	2^{-51}	–	$2^{22.8}$	196
–	–	–	3	–	$2^{87.2}$	2^{-50}	–	$2^{23.4}$	294

Parameter Examples
Short Signatures

parameters				ISD security	security against (chained) GBA	sign. failure probability	public key size	sign. cost	sign. size
m	t	δ	i						
20	8	2	1	$2^{81.0}$	$2^{59.1}$	~ 0	20.0 MB	$2^{15.3}$	98
–	–	–	2	–	$2^{75.7}$	~ 0	–	$2^{16.3}$	196
–	–	–	3	–	$2^{82.5}$	~ 0	–	$2^{16.9}$	294
16	9	2	1	$2^{76.5}$	$2^{53.6}$	2^{-155}	1.1 MB	$2^{18.5}$	81
–	–	–	2	–	$2^{68.7}$	2^{-154}	–	$2^{19.5}$	162
–	–	–	3	–	$2^{74.9}$	2^{-153}	–	$2^{20.0}$	243
18	9	2	1	$2^{84.5}$	$2^{59.8}$	2^{-1700}	5.0 MB	$2^{18.5}$	96
–	–	–	2	–	$2^{76.5}$	2^{-1700}	–	$2^{19.5}$	192
–	–	–	3	–	$2^{83.4}$	2^{-1700}	–	$2^{20.0}$	288
19	9	2	1	$2^{88.5}$	$2^{62.8}$	~ 0	10.7 MB	$2^{18.5}$	103
–	–	–	2	–	$2^{80.5}$	~ 0	–	$2^{19.5}$	206
–	–	–	3	–	$2^{87.7}$	~ 0	–	$2^{20.0}$	309
15	10	3	1	$2^{76.2}$	$2^{55.6}$	~ 0	0.6 MB	$2^{21.8}$	90
–	–	–	2	–	$2^{71.3}$	~ 0	–	$2^{22.8}$	180
–	–	–	3	–	$2^{77.7}$	~ 0	–	$2^{23.4}$	270
16	10	2	1	$2^{86.2}$	$2^{59.1}$	2^{-13}	1.2 MB	$2^{21.8}$	90
–	–	–	2	–	$2^{75.7}$	2^{-12}	–	$2^{22.8}$	180
–	–	–	3	–	$2^{82.5}$	$2^{-11.3}$	–	$2^{23.4}$	270
17	10	2	1	$2^{90.7}$	$2^{62.5}$	2^{-52}	2.7 MB	$2^{21.8}$	98
–	–	–	2	–	$2^{80.0}$	2^{-51}	–	$2^{22.8}$	196
–	–	–	3	–	$2^{87.2}$	2^{-50}	–	$2^{23.4}$	294

Conclusion

- Resisting OMSD attacks required to notably increase CFS parameters.
- Parallel-CFS offers a way to keep parameters as small as possible:
  - key size remains the same as for CFS,
  - OMSD attacks cost the same as direct SD attacks,
  - signature time and size are doubled.
- Parallel-CFS is not the most efficient signature scheme, but at least it is practical.