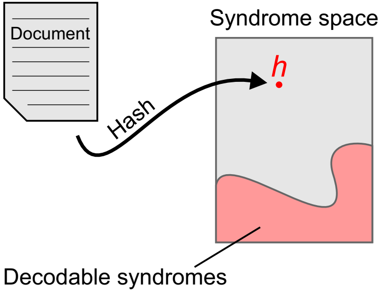
5. Other Cryptographic Constructions Relying on Coding Theory

- Code-Based Digital Signatures
- **The Courtois-Finiasz-Sendrier (CFS) Construction**
- Attacks against the CFS Scheme
- Parallel-CFS
- Stern's Zero-Knowledge Identification Scheme
- An Efficient Provably Secure One-Way Function
- The Fast Syndrome-Based (FSB) Hash Function

Two Methods to Achieve Code-Based Signatures

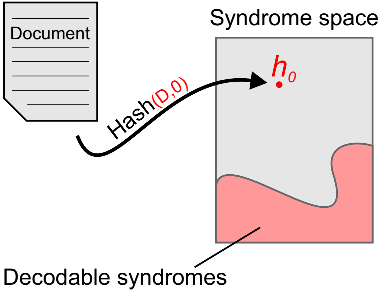


It is impossible to hash into decodable syndromes, but one can hash onto the space of all syndromes:

- the document hash is not always decodable

Two Methods to Achieve Code-Based Signatures

Adding a counter

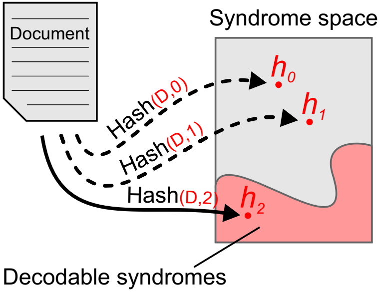


The first technique is to add a counter to the document:

- “append” the counter to the document
- the hash depends on both the document and the value of the counter

Two Methods to Achieve Code-Based Signatures

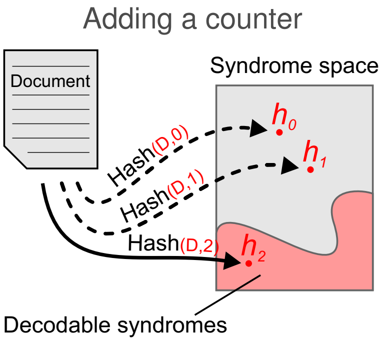
Adding a counter

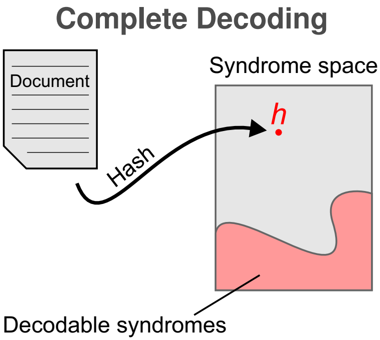


Increment the counter until a decodable syndrome is found:

- the signature is the decoding of this syndrome
- the counter is also part of the signature
  → it is needed for the verification

Two Methods to Achieve Code-Based Signatures

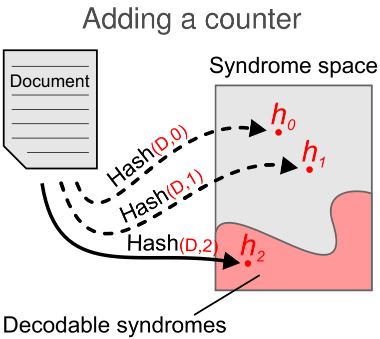


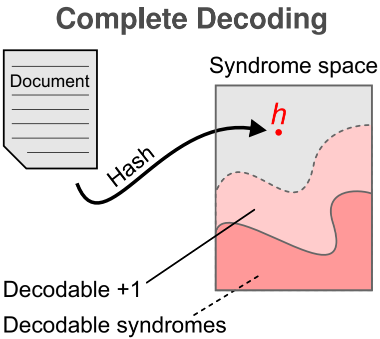


The second method is to perform complete decoding

- complete decoding means being able to decode any syndrome
- it requires modifying the decoding algorithm

Two Methods to Achieve Code-Based Signatures

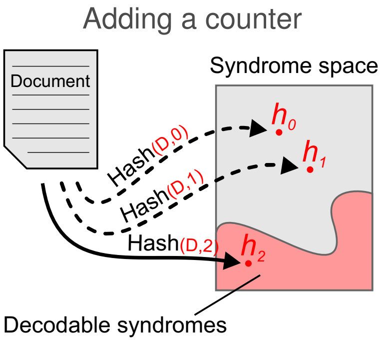


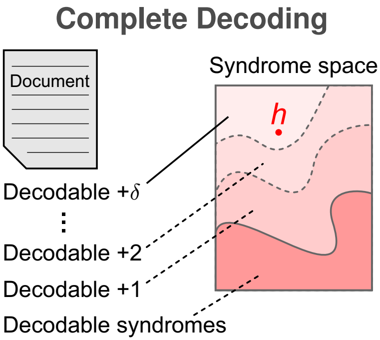


Use exhaustive search to decode 1 more error:

- add an error to the syndrome
- try to decode it
  → more syndromes are decodable this way

Two Methods to Achieve Code-Based Signatures



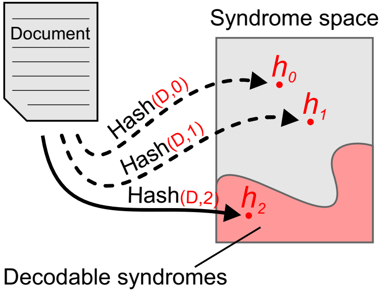


With an exhaustive search on δ more errors:

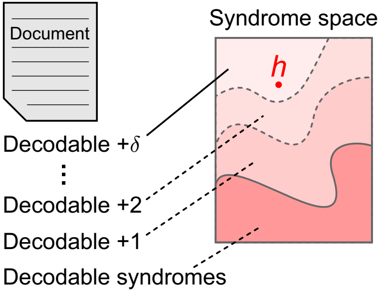
- we can reach the covering radius of the code
- the signature is the decoding of h
  → including the δ additional errors

Two Methods to Achieve Code-Based Signatures

Adding a counter



Complete Decoding



Both techniques are expensive:

- decodable syndromes must have high enough density
- covering radius and decoding capacity must be close

Requirements for Code-based Signature

As for public-key encryption, the decoding algorithm must remain secret:

- we need codes where the structure can be hidden
  $\rightarrow$ binary Goppa codes are one of very few candidates
- with the highest possible density of decodable syndromes

Requirements for Code-based Signature

As for public-key encryption, the decoding algorithm must remain secret:

- we need codes where the structure can be hidden
  $\rightarrow$ binary Goppa codes are one of very few candidates
- with the highest possible density of decodable syndromes

Density of decodable syndromes for a binary Goppa code

For a code of length $n = 2^m$ over $GF(2^m)$ correcting t errors:

- there are $\binom{n}{t}$ decodable syndromes
- among a total of 2^{mt} syndromes

The density is: $\dfrac{\binom{n}{t}}{2^{mt}} = \dfrac{\binom{2^m}{t}}{2^{mt}} \simeq \dfrac{\frac{(2^m)^t}{t!}}{2^{mt}} \simeq \dfrac{1}{t!}$

Requirements for Code-based Signature

As for public-key encryption, the decoding algorithm must remain secret:

- we need codes where the structure can be hidden
  $\rightarrow$ binary Goppa codes are one of very few candidates
- with the highest possible density of decodable syndromes

The first Niederreiter-based signature scheme was proposed by Courtois, Finiasz, and Sendrier in 2001:

- uses the techniques we presented
- with binary Goppa codes correcting very few errors (9 or 10)
- but codes with very long length (at least 2^{16}) to maintain a high security level

The CFS Signature Scheme with Counters

Signature:

input: a document D

$i \leftarrow 0$

loop // $t!$ iterations on average

  $h_i \leftarrow H(H(D)||i)$ // H is the public hash function

  Try to decode h_i

  if h_i *is a decodable syndrome* **then**

    $e \leftarrow$ decoding of h_i

    $s \leftarrow (e, i)$

    return s

  end

  $i \leftarrow i + 1$

end

Verification:

- extract $s = (e, i)$ from the document
- verify that $H(H(D)||i) = \text{Syndrome}(e)$.

The CFS Signature Scheme with Complete Decoding

Signature:

input: a document D

$h \leftarrow H(D)$

loop // also t! iterations on average

$e_\delta \leftarrow$ random error pattern of weight δ // can also be done "in order"

$h' = h \oplus \text{Syndrome}(e_\delta)$

Try to decode h'

if h' *is a decodable syndrome* **then**

$e \leftarrow$ decoding of h'

$s \leftarrow e \oplus e_\delta$

return s

end

end

Verification:

- extract s from the document
- verify that $H(D) = \text{Syndrome}(s)$.

5. Other Cryptographic Constructions Relying on Coding Theory

- Code-Based Digital Signatures
- The Courtois-Finiasz-Sendrier (CFS) Construction
- **Attacks against the CFS Scheme**
- Parallel-CFS
- Stern's Zero-Knowledge Identification Scheme
- An Efficient Provably Secure One-Way Function
- The Fast Syndrome-Based (FSB) Hash Function