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

Attacks against a Signature Scheme

As for public-key encryption, there are two kinds of attacks.

Key recovery attacks:

- try to recover the secret key from the public key
- identical to key attacks against McEliece

  → only with different parameters (t small and n large)

Nothing different than in McEliece, we will not discuss these here.

Attacks against a Signature Scheme

As for public-key encryption, there are two kinds of attacks.

Key recovery attacks:

- try to recover the secret key from the public key
- identical to key attacks against McEliece

  → only with different parameters (t small and n large)

Forgery attacks:

- try to create a valid document-signature pair
- similar to message attacks against McEliece
- but with no constraint on the document

  → the attacker can choose the document freely

Forgery Attacks

Counter version

- choose a document D
- pick a counter i
- compute the hash $h = H(H(D)||i)$
- decode h as an error of weight t

⚠ h is probably not decodable!

Forgery Attacks

Counter version

- choose a document D
- pick a counter i
- compute the hash $h = H(H(D)||i)$
- decode h as an error of weight t

⚠ h is probably not decodable!

Complete decoding version

- choose a document D
- compute the hash $h = H(D)$
- decode h as an error of weight $t + \delta$

Forgery Attacks

Counter version

- choose a document D
- pick a counter i
- compute the hash $h = H(H(D)||i)$
- decode h as an error of weight t

⚠ h is probably not decodable!

Complete decoding version

- choose a document D
- compute the hash $h = H(D)$
- decode h as an error of weight $t + \delta$

Requires to solve a Syndrome Decoding instance:

- ISD
- GBA

Forgery Attacks

Counter version

- choose a document D
- pick many counters i
- compute the hash $h = H(H(D)||i)$
- decode h as an error of weight t

⚠ some h_i are decodable!

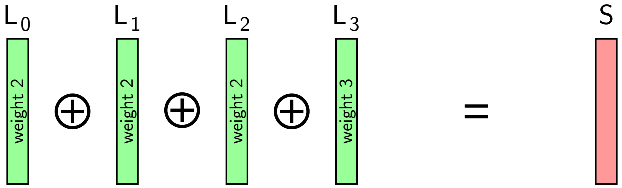
Complete decoding version

- choose many documents D
- compute the hash $h = H(D)$
- decode h as an error of weight $t + \delta$

Requires to solve a Syndrome Decoding instance:

- ISD: best example of Decoding One Out of Many
- GBA: build a list of syndromes

Example of Generalized Birthday Attack

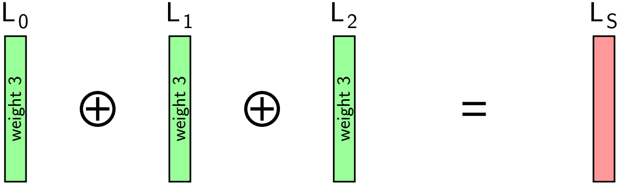


For parameters $n = 2^{16}$ and $t = 9$, the syndromes are 144 bits long.

- the normal GBA setup is to build 4 lists
- it targets a single syndrome S
- lists of $2^{\frac{144}{3}} = 2^{48}$ elements would find a solution

  → impossible with lists L_i of weight 2 : $\binom{2^{16}}{2} = 2^{31}$

Example of Generalized Birthday Attack

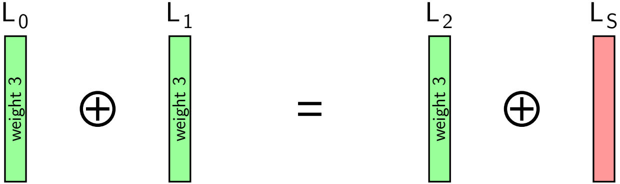


For parameters $n = 2^{16}$ and $t = 9$, the syndromes are 144 bits long.

- for CFS we target a list L_S of syndromes
- lists L_i are a little too small with size $\binom{2^{16}}{3} = 2^{45.4}$
- L_S has to be made larger to compensate

  → L_S has size $2^{60.1}$

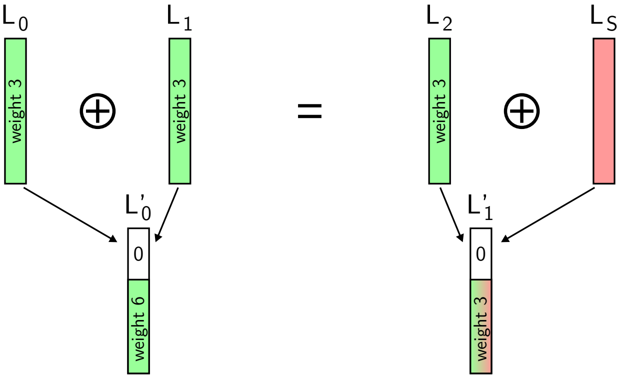
Example of Generalized Birthday Attack



As usual in GBA, lists are merged by pair:

- L_0 with L_1 and L_2 with L_S

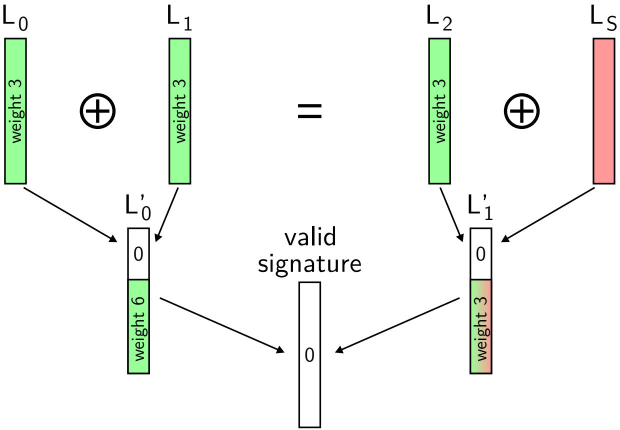
Example of Generalized Birthday Attack



As usual in GBA, lists are merged by pair:

- L_0 with L_1 and L_2 with L_S
- 48 bits of the syndromes are zeroed (96 remain)

Example of Generalized Birthday Attack



L'_0 contains $\binom{2^{16}}{6} \times 2^{-48} = 2^{38.5}$ elements

L'_1 contains $\binom{2^{16}}{3} \times 2^{60.1} \times 2^{-48} = 2^{57.5}$ elements

} 1 solution is found on average

Security of the CFS Signature

With the GBA attack, the security of CFS is a little above $2^{\frac{mt}{3}}$:

- for $t = 9$, a security of 2^{80} requires $m = 26$
- the public key is then a 234×2^{26} binary matrix

  → its size is over 1 gigabyte!

Security of the CFS Signature

With the GBA attack, the security of CFS is a little above $2^{\frac{mt}{3}}$:

- for $t = 9$, a security of 2^{80} requires $m = 26$
- the public key is then a 234×2^{26} binary matrix

  → its size is over 1 gigabyte!

There are two choices:

- significantly increase t

  → but signature cost is dependent on t!
- or find a way to maintain the security closer to $2^{\frac{mt}{2}}$

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