Round 1 Submission

Gustavo Banegas  
Qualcomm, France

Kévin Carrier  
CY Cergy-Paris University, France

André Chailloux  
Inria, France

Alain Couvreur  
Inria, and Laboratoire d’Informatique de l’École polytechnique (LIX), UMR 7161, CNRS, École polytechnique, Institut Polytechnique de Paris, Palaiseau, France

Thomas Debris-Alazard  
Inria, and Laboratoire d’Informatique de l’École polytechnique (LIX), UMR 7161, CNRS, École polytechnique, Institut Polytechnique de Paris, Palaiseau, France

Philippe Gaborit  
University of Limoges, France

Pierre Karpman  
Université Grenoble Alpes, France

Johanna Loyer  
Inria, France

Ruben Niederhagen  
Academia Sinica, Taiwan, and University of Southern Denmark, Denmark

Nicolas Sendrier  
Inria, France

Benjamin Smith  
Inria, and Laboratoire d’Informatique de l’École polytechnique (LIX), UMR 7161, CNRS, École polytechnique, Institut Polytechnique de Paris, Palaiseau, France

Jean-Pierre Tillich  
Inria, France
Notation and Conventions

\( x := y \) \hspace{1cm} x \) is defined to be equal to \( y \)

\( \#S \) \hspace{1cm} Cardinality of the finite set \( S \)

\( \mathbb{Z} \) \hspace{1cm} The ring of integers

\([a, b] \) \hspace{1cm} \([a, b] := \{ i \in \mathbb{Z} \mid a \leq i \leq b \}\)

\([a, b) \) \hspace{1cm} \([a, b) := \{ i \in \mathbb{Z} \mid a \leq i < b \}\)

\( \mathbb{F}_q \) \hspace{1cm} The \( q \)-ary finite field (\( q = 3 \) in all of our concrete parameter sets)

\( x \in \mathbb{F}_q^n \) \hspace{1cm} \( x = (x_0, \ldots, x_{n-1}) \in \mathbb{F}_q^n \), vectors in row notation generally use bold letters

\( x(i) \) \hspace{1cm} Alternative notation for \( x_i \), convenient when not a single letter, e.g. \( e_V(i) \)

\( x \hspace{1cm} \mathcal{J}(\cdot) \) \hspace{1cm} \( i \in \mathcal{J} \) for \( \mathcal{J} \subseteq [0, n) \)

\( (x \parallel y) \) \hspace{1cm} Concatenation of vectors \( x \) and \( y \)

\( \text{Supp}(x) \) \hspace{1cm} Support of \( x \), the set \( \{ i \in [0, n), x_i \neq 0 \} \)

\( |x| \) \hspace{1cm} Hamming weight of \( x \in \mathbb{F}_q^n \), \# \text{Supp}(x)

\( a \cdot x \) \hspace{1cm} Scalar product \( a \cdot x := (ax_i)_{0 \leq i < n} \) for \( a \in \mathbb{F}_q \) and \( x \in \mathbb{F}_q^n \)

\( \langle x, y \rangle \) \hspace{1cm} Inner product \( \langle x, y \rangle := \sum_{i=1}^{n} x_i y_i \in \mathbb{F}_q \) for \( x \) and \( y \) in \( \mathbb{F}_q^n \)

\( M \in \mathbb{F}_q^{r \times n} \) \hspace{1cm} \((M_{i,j})_{0 \leq i < r, 0 \leq j < n} \), \( r \times n \) matrix over \( \mathbb{F}_q \). Matrices generally use capital bold letters

\( M(i, j) \) \hspace{1cm} Alternative notation for \( M_{i,j} \), convenient when not a single letter, e.g. \( M_V(i, j) \)

\( \text{row}(M, i) \) \hspace{1cm} \( i \)-th row of \( M \)

\( \text{col}(M, i) \) \hspace{1cm} \( i \)-th column of \( M \)

\( M_i \) \hspace{1cm} Alternative notation for \( \text{row}(M, i) \)

\( M_{\mathcal{J}} \) \hspace{1cm} \((M_{i,j})_{0 \leq i < r, j \in \mathcal{J}} \) for \( M \in \mathbb{F}_q^{r \times n} \) and \( \mathcal{J} \subseteq [0, n) \)

\( \langle \cdot \rangle \) \hspace{1cm} Raw span of \( M \)

\( x \ast M \) \hspace{1cm} Row-wise star product, \( x \ast M := (x_j M_{i,j})_{0 \leq i < r, 0 \leq j < n} \)

\( M^\top \) \hspace{1cm} Transposition of \( M \)

\( \mathfrak{S}_n \) \hspace{1cm} Group of permutations of \([0, n)\)

\( x^\pi \) \hspace{1cm} \( x^\pi := (x_{\pi(i)})_{i \leq 0 < n} \), for \( x \in \mathbb{F}_q^n \) and \( \pi \in \mathfrak{S}_n \)

\( M^\pi \) \hspace{1cm} \( M^\pi := (M_{i,\pi(j)})_{0 \leq i < r, 0 \leq j < n} \) for \( M \in \mathbb{F}_q^{r \times n} \) and \( \pi \in \mathfrak{S}_n \)

\( x \sim_{\mathcal{D}} X \) \hspace{1cm} Variable \( x \) sampled from the set \( X \) according to the distribution \( \mathcal{D} \)

\( x \sim \) \hspace{1cm} Variable \( x \) sampled uniformly at random from the finite set \( X \)
Information set
An information set for a matrix $M \in F_q^{(r+g) \times n}$ (where $g \geq 0$) is a set $\mathcal{J} \subseteq [0,n)$ of cardinality $r$ such that $M_{\mathcal{J}} \in F_q^{(r+g) \times r}$ has full rank.

Systematic form
A matrix $M \in F_q^{r \times n}$ is in systematic form if $M = (\text{Id}_r \mid R)$ where $\text{Id}_r$ is the $r \times r$ identity matrix.

Linear code
An $[n, k]_q$-code $C$ is defined to be a $k$-dimensional subspace of $F_q^n$.

Generator matrix
A generator matrix for a linear $[n, k]_q$-code $C$ is a matrix $G \in F_q^{k \times n}$ whose rows form a basis of $C$; that is,
$$C = \{ xG : x \in F_q^k \}.$$ 

Dual code
The dual of an $[n, k]_q$-code $C$ is the $[n, n-k]_q$-code defined by
$$C^\perp := \{ c^\perp \in F_q^n : \forall c \in C, \langle c, c^\perp \rangle = 0 \}.$$ 

Parity-check matrix
A parity-check matrix for an $[n, k]_q$-code $C$ is a matrix $H \in F_q^{(n-k) \times n}$ whose rows form a basis of the dual $C^\perp$. Note that
$$C = \{ c \in F_q^n : \text{He}^\top = 0 \}.$$
1. Introduction

Wave is a code-based hash-and-sign signature scheme introduced in [DST19]. Wave instantiates the theoretical framework of Gentry, Peikert and Vaikuntanathan [GPV08] using a novel code-based trapdoor: its security is proven to inherit from the hardness of two well-identified problems for which the best known attacks rely on generic decoding algorithms [DST19]. With appropriate parameters, Wave can therefore offer high security against classical and quantum adversaries.

This document specifies the Wave scheme, and proposes highly conservative parameter sets for signatures targeting NIST post-quantum security levels I, III, and V. It also describes a portable C reference implementation for Wave instances with those parameters.

Wave enjoys short signatures and fast verification, even with conservative parameters. Table 2 gives a preview of our results: Wave signature sizes are highly competitive with structured lattice-based signatures such as Falcon [FHK+17] and CRYSTAL-S/Dilithium [LDK+20], and signatures can be verified in milliseconds on a PC platform. Wave public keys are generator matrices for random-looking linear codes, so they are decidedly on the large side (especially given our conservative parameter choices): this is the main drawback of Wave. However, in use-cases where large public keys can be stored, Wave can be a strong candidate for high-security quantum-safe signatures.

Table 2. Signature length and verification speed results for Wave instances. Timings count millions of cycles used on average by the (non-optimized) reference implementation, running on an Intel Core i5-1135G7 platform at 2.40GHz. See §5 for more detailed figures.

<table>
<thead>
<tr>
<th>Wave instance</th>
<th>Post-quantum security target</th>
<th>Signature length (Bytes)</th>
<th>Public key size (Bytes)</th>
<th>Key generation (MCycles)</th>
<th>Signing (MCycles)</th>
<th>Verification (MCycles)</th>
<th>Verification2 (MCycles)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Wave822</td>
<td>Wave1249</td>
<td>Wave1644</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Level I</td>
<td>Level III</td>
<td>Level V</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Signature</td>
<td></td>
<td>822</td>
<td>1249</td>
<td>1644</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>length (Bytes)</td>
<td></td>
<td>3677 390</td>
<td>7 867 598</td>
<td>13 632 308</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Public key</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>size (Bytes)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

1 Signatures are compressed to variable-length byte arrays, which may in fact be shorter than this bound.

2 Verification where the public key is pre-loaded in bitsliced format, and does not require conversion from the transport format: see §5 for details.

We give a brief high-level overview of the scheme in §2, and explain the design rationale in §3. We formally specify the scheme in §4, present performance results for the reference implementation in §5, and link to Known Answer Tests in §6. To justify the security of our proposed instances, we summarize the security proof for Wave in §7 and survey the best known attacks in §8.
Wave is based on the GPV framework [GPV08]; as such, it is built on a trapdoor function. The Wave trapdoor, detailed in §3, is based on permuted generalized \((U|U + V)\)-codes.

**Definition 1.** Let \(n, k_U, \) and \(k_V\) be integers with \(n\) even and \(k_U, k_V \leq n/2\). Let \(U\) be an \([n/2, k_U]_q\)-code with generator (resp. parity-check) matrix \(G_U\) (resp. \(H_U\)), and let \(V\) be an \([n/2, k_V]_q\)-code with generator (resp. parity-check) matrix \(G_V\) (resp. \(H_V\)). Let \(\pi\) be a permutation in \(\mathcal{S}_n\), and let \(b\) and \(c\) be vectors in \(\mathbb{F}_q^{n/2}\) with \(c(i) \neq 0\) for all \(i \in [0, n/2]\).

The permuted generalized \((U|U + V)\)-code associated to \((U, V, \pi, b, c)\) is the \([n, k_U + k_V]_q\)-code admitting the generator matrix \(G\) and parity-check matrix \(H\) defined by

\[
G = \left( \frac{G_U}{b \times G_V} \right) \pi \quad \text{and} \quad H = \left( \frac{d \times H_U}{-c \times H_V} \right) \pi
\]

where \(d := 1 + b \times c\).

A Wave public key is a parity-check matrix, in systematic form, of a permuted generalized \((U|U + V)\)-code over \(\mathbb{F}_3\). The associated private key is the underlying structure: the codes \(U\) and \(V\), vectors \(b\) and \(c\), and permutation \(\pi\). Table 3 sketches the Wave signature scheme; the full specification begins in §4.

**Table 3.** Sketch of the Wave signature scheme.

<table>
<thead>
<tr>
<th>System parameters:</th>
<th>field size</th>
<th>sec. level</th>
<th>codelength</th>
<th>weight</th>
<th>(U)-dimension</th>
<th>(V)-dimension</th>
<th>dimension</th>
</tr>
</thead>
<tbody>
<tr>
<td>(q = 3)</td>
<td>(\lambda)</td>
<td>(n)</td>
<td>(w)</td>
<td>(k_U)</td>
<td>(k_V)</td>
<td>(k := k_U + k_V)</td>
<td></td>
</tr>
</tbody>
</table>

**Private key:** \((U, V, \pi, b, c)\) defining a permuted generalized \((U|U + V)\)-code.

**Public key:** \(R \in \mathbb{F}_3^{(n-k) \times k}\) such that \((\text{Id}_{n-k} \mid R)\) is a parity-check matrix of the permuted generalized \((U|U + V)\)-code associated to the secret key.

**Signature** on a message \(m\) under a public key \(R\): \(\sigma = (\text{salt}, e) \in \mathbb{F}_2^\lambda \times \mathbb{F}_3^k\) such that

\[
|e| + |\text{Hash}(m \parallel \text{salt}) - eR^\top| = w.
\]

(1)

**Verification** of a signature \(\sigma = (\text{salt}, e)\) on a message \(m\) under a public key \(R\): Accept if (and only if) Equation (1) holds.

The binary vector \(\text{salt}\) in the signature is a (random) salt required by the security proof. Given a signature \((\text{salt}, e)\) on \(m\) under \(R\), the vector \(x := (\text{Hash}(m \parallel \text{salt}) - eR^\top, e)\) is in fact the unique vector of Hamming weight \(w\) satisfying \(x(\text{Id}_{n-k} \mid R)^\top = \text{Hash}(m \parallel \text{salt})\) and \(x_{[n-k,n]} = e\). The original description of Wave [DST19] took \((\text{salt}, x)\) to be the signature. Here, however, we follow the approach of [BDNS21]: \(x\) can be immediately recovered from \(m, \text{salt}, \) and \(e\) (by definition), so \((\text{salt}, e)\) can serve as the signature, thus reducing the signature size from \(2\lambda\) bits and \(n\) trits to \(2\lambda\) bits and \(k\) trits.
3. Design Rationale: The Wave Trapdoor

The design of Wave follows the “hash and sign” approach à la GPV [GPV08] in the same spirit as some lattice-based schemes including Falcon [FKH+17], but in an error-correcting code-based context. While the trapdoors in [GPV08] and [FKH+17] rely on short bases of lattices, the Wave trapdoor is based on permuted generalized \((U|U+V)\)-codes (as in Definition 1).

3.1. Weight and the general decoding problem. Wave security inherits from the hardness of the Decoding Problem (DP): given an \([n, k]_q\)-code \(C\) (a subspace of \(\mathbb{F}_q^n\) of dimension \(k\)), a distance \(w\), and a point \(y\) in the ambient space \(\mathbb{F}_q^n\), the aim is to find a \(x\) in \(C\) at Hamming distance \(w\) from \(y\), that is, differing from \(y\) on exactly \(w\) coordinates.

After sixty years of research on DP, the best approach when the \(C\) has no special structure—and in particular, when it is random—is to take advantage of linearity: \(C\) is a vector space of dimension \(k\), so one can simply compute \(x \in C\) by fixing \(k\) coordinates. If \(y\) is uniformly distributed over \(\mathbb{F}_q^n\), then the resulting \(x\) has \(x(i) - y(i)\) “controlled” on exactly \(k\) coordinates, while the remaining \(n-k\) coordinates are uniformly distributed. In particular, there will typically be \((n-k)(q-1)/q\) non-zero coordinates among these \(n-k\) coordinates. Depending on the decoding problem to be solved, “close” (small \(w\)) or “far away” (large \(w\)), the best strategy is to carefully choose \(x(i)\) on the \(k\) controlled coordinates \(i\). If one chooses \(j \leq k\) coordinates where \(x(i) \neq y(i)\), then \(|x - y|\) is typically \(j + \frac{q-1}{q}(n-k)\). We can therefore easily compute codewords at distances in \([\frac{q-1}{q}(n-k), k + \frac{q-1}{q}(n-k)]\). Any chosen distance \(w\) outside this interval is unlikely to be reached, so the procedure must be repeated a prohibitive number of times for any probability of success.

Figure 1 illustrates the situation. Surprisingly, no known algorithm can solve DP for random codes in polynomial time (in \(w\)) outside the “easy” interval in the middle.

![Figure 1. Hardness (with respect to \(w\)), given a random \([n, k]_q\)-code \(C \subseteq \mathbb{F}_q^n\) and \(y \in \mathbb{F}_q^n\), of finding \(x \in C\) at Hamming distance \(w\) from \(y\).](image)

3.2. The Wave trapdoor. To construct a Wave trapdoor, we sample random codes \(U\) and \(V\) in \(\mathbb{F}_q^{n/2}\) of dimensions \(k_U\) and \(k_V\), respectively, a permutation \(\pi\) in \(\mathbb{S}_n\), and vectors \(b\) and \(c\) in \(\mathbb{F}_q^{n/2}\) with \(c(i) \neq 0\) for \(i \in \{0, n/2\}\). These are all kept secret, and the permuted generalized \((U|U+V)\)-code

\[ C := \left\{ ((x_U + b \ast x_V) \mid (c \ast x_U + d \ast x_V))^\pi : x_U \in U \text{ and } x_V \in V \right\} \subseteq \mathbb{F}_q^n \]

of length \(n\) and dimension \(k := k_U + k_V\) is made public (here \(d := 1 + b \ast c\)).

Given a uniform random \(y\) in \(\mathbb{F}_q^n\), we can find \(x \in C\) at the chosen distance

\[ w := 2k_U + 2 \frac{q-1}{q}(n/2 - k_U) \]

from \(y\) using the following procedure, if we know \(U\), \(V\), \(\pi\), \(b\), and \(c\):

1. Compute any \(x_V \in V\).
(2) From \( y \) and the knowledge of the secret permutation \( \pi \), decompose \( y \) as \( (y_L, y_R)^\pi \) with \( y_L \) and \( y_R \) in \( \mathbb{F}_q^{n/2} \).

(3) Using the knowledge of \( x_V \), compute some \( x_U \in U \) such that for \( k_U \) of the coordinate indices \( i \), we have

\[ x_U(i) \neq y_L(i) - b(i)x_V(i) \quad \text{and} \quad c(i)x_U(i) \neq y_R(i) - d(i)x_V(i) \tag{2} \]

(4) Output \( x := ((x_U + b \cdot x_V) \parallel (c \cdot x_U + d \cdot x_V)) ^\pi \in C \).

By assumption \( c \) has only non-zero components and \( d = 1 + b \cdot c \), so Condition (2) can be satisfied provided \( q \geq 3 \), which we assume from now on. Furthermore, as \( (y_L,y_R) \) is uniformly distributed, \( y_L(i) - x_U(i) - b(i)x_V(i) \) and \( y_R(i) - c(i)x_U(i) - d(i)x_V(i) \) will be uniformly distributed on the other \( n/2 - k_U \) coordinates. The Hamming distance is invariant under permutations, so \( \left| (y_L \parallel y_R)^\pi - ((x_U + b \cdot x_V) \parallel (c \cdot x_U + d \cdot x_V))^\pi \right| \) will typically be \( w \), as claimed.

Decoding without the secret structure \((U,V,\pi,b,c)\) of the permutated generalized \((U|U+V)\)-code \( C \) is hard, given the discussion above, if the value of \( w \) falls outside the “easy” interval \([q^{-1}(1-k), q^{-1}(n-k)]\), where \( k = k_U + k_V \). This condition holds when \( k_U > k_V \), which is a requirement of Wave.

### 3.3. Signing with the trapdoor.

To sign a message \( m \), the signer hashes it (with a random salt \( \text{salt} \)) to a random vector \( y \in \mathbb{F}_q^n \). The trapdoor computes a codeword \( x \in C \) at a distance of \( w \) from \( y \). The signature of \( m \) is represented by \( x \). To verify the signature, we must check that \( x \) belongs to \( C \) and that the Hamming distance between \( x \) and the hash of \( m \) with \( \text{salt} \) is exactly \( w \). If the public code \( C \) has no apparent structure to be exploited—that is, it is indistinguishable from a random code—then any adversary seeking to forge a signature must produce a codeword at distance \( w \) from a random target, which has a prohibitive cost because \( w \) is outside \([q^{-1}(1-k), q^{-1}(n-k)]\); this ensures the security of the signature scheme. (We give more detailed security analyses in §7 and §8.)

This naive signing algorithm is easily broken: a few signatures \( x \) in the permuted generalized \((U|U+V)\)-code are enough to recover the trapdoor and thus break the scheme [DST17, §5.1]. In the same way as for other [GPV08]-like schemes, security requires the distribution of signatures to be independent of the trapdoor, so that signatures cannot leak any information on the secret. In particular, \( x_V \) and \( x_U \) must be carefully sampled.

In [DST19], a safe distribution of signatures was achieved through rejection sampling; but this can be problematic for implementation safety and efficiency, especially when constant-time signing is required. We will see that by carefully choosing some internal distributions we can achieve secure signature distributions, and thus avoid rejection sampling entirely without impacting security.
4. Specifications

The specification of an instance of Wave, for any given security level $\lambda$, requires the following parameters:

- The main parameters $n, k, w$;
- additional parameters $k_U, k_V, g$ (used for key generation and signing);
- internal discrete distributions $\mathcal{D}_V$ on $[0, k_V - g]$ and $\mathcal{D}_U(t)$ on $[0, t]$, for $t$ in $[0, n/2]$;
- a decoder output support $\text{Accept} \subseteq [0, n/2] \times [0, w/2]$, and
- a cryptographic hash function $\text{Hash} : \{0, 1\}^* \rightarrow \mathbb{F}_3^{n-k}$.

Table 4 gives the values of these parameters in the Wave instances proposed for security levels I, III, and V.

<table>
<thead>
<tr>
<th>Instance</th>
<th>Main parameters</th>
<th>Additional parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Code length</td>
<td>Code dimension</td>
</tr>
<tr>
<td>Wave822 (Level I)</td>
<td>128</td>
<td>8576</td>
</tr>
<tr>
<td>Wave1249 (Level III)</td>
<td>192</td>
<td>12544</td>
</tr>
<tr>
<td>Wave1644 (Level V)</td>
<td>256</td>
<td>16512</td>
</tr>
</tbody>
</table>

A full implementation of an instance of Wave requires several algorithmic choices which affect efficiency and security (e.g. ensuring the constant-time property). For our reference implementation, they are given in appendix:

- The hash function in §A,
- bit-sliced ternary arithmetic in §B.1,
- sampling ternary vectors in §B.2,
- sampling and applying permutations in §B.3,
- master key for generating and permuting secret matrices §B.4,
- Gaussian elimination variants in §B.5.

The reference implementation prioritises constant-time key generation and constant-time signing. Other choices are possible, depending on the context and security requirements. The complexity bottleneck of both key generation and signing is (by far) Gaussian elimination; relaxing the constant-time constraint may significantly improve signing time.

4.1. Useful Algorithms: Gaussian Elimination and Variants. Gaussian elimination on an $r \times n$ full-rank matrix $A$ produces another matrix $A'$ whose rows span the same vector space and which contains an $r \times r$ identity sub-matrix, in the columns indexed by an information set $J \subseteq [0, n)$ of size $r$. This set corresponds to the “pivot” positions.
We will define three Gaussian elimination algorithms: Systematic, Partial, and Extended. Appendix B.5.1 proposes constant-time versions of these algorithms.

**Systematic Gaussian elimination.** Algorithm 1 defines Gaussian elimination on a matrix $A \in \mathbb{F}_3^{n \times r}$ permuted with $\sigma \in S_n$, using the columns of $A^\sigma$ as pivot positions and “pushing” failing pivot positions to the right. A constant-time version appears in Appendix B.5.1.

**Algorithm 1 SystGaussElim — Systematic Gaussian Elimination**

Input: $A \in \mathbb{F}_3^{n \times r}$ and $\sigma \in S_n$.
Output: $A_{\text{syst}} \in \mathbb{F}_3^{n \times r}$ and $\pi \in S_n$.

Requirements:
1. $\langle A^\pi \rangle = \langle A_{\text{syst}} \rangle$,
2. $A_{\text{syst}} = (\text{Id}_r \mid B)$,
3. $\pi$ is “close” to $\sigma$, and

   \[ \pi(i) = \sigma(\ell_i) \text{ for all } i \in [0, r), \text{ where } \ell_i = \min \{ j \in [0, n) \mid \text{rank}(A^\sigma_{[0,j]}) = i \} , \]

   \[ \pi(i) = \sigma(\ell_i) \text{ for all } i \in [r, n), \text{ where } \ell_i = \min \{ \{0, n) \setminus \{\sigma^{-1} \circ \pi(j), j \in [0, i)\} \} . \]

**Remark 1.** Note that, over $\mathbb{F}_3$, the case $\pi = \sigma$ in Algorithm 1 happens 56% of the time.

**Partial Gaussian elimination.** Algorithm 2 defines Gaussian elimination $A \in \mathbb{F}_3^{n \times r}$ but stopping $g$ steps before the end, that is, after $k - g$ pivots. A constant-time version appears in Appendix B.5.1.

**Algorithm 2 PartialGaussElim — Partial Gaussian Elimination**

Input: $A \in \mathbb{F}_3^{n \times r}$ and $g \leq r$ be an integer.
Output: $A_{\text{partSyst}} \in \mathbb{F}_3^{n \times r}$ or ⊥.

Requirements:
1. Output is ⊥ if and only if $\text{rank}(A_{[0, r-g]}) < r - g$,
2. $\langle A_{\text{partSyst}} \rangle = \langle A \rangle$,
3. $A_{\text{partSyst}} = \begin{pmatrix} \text{Id}_{r-g} & R \end{pmatrix}$.

**Extended Gaussian elimination.** The Gaussian elimination algorithms above are not sufficient for Wave signing. We also need the “extended” Gaussian elimination defined by Algorithm 3, which outputs a matrix in extended systematic form.

**Definition 2** (Extended systematic form). A matrix $A \in \mathbb{F}_3^{n \times r}$ is in extended systematic form if

\[
\text{for all } i \in [0, r), \begin{cases} \text{A}(i, i) \neq 0 \implies \text{A}(i, i) = 1 \text{ and } |\text{col}(\text{A}, i)| = 1 , \\
\text{A}(i, i) = 0 \implies |\text{row}(\text{A}, i)| = 0 . \end{cases}
\]

We propose a constant-time version of Algorithm 3 in §B.5.2. Basically, Algorithm 3, on input $(A, g)$ with $A \in \mathbb{F}_3^{n \times r}$, tries to compute an extended systematic form by first adding $g$ extra (zero) rows and then performing a Gaussian elimination. It succeeds if and only if the first $r + g$ columns of this new matrix have the same rank as $A$. 

8
provides domain separation). More precisely, we propose using SHAKE256 by mk to regenerate $H$.

We sample the random matrices $H$ that in Definition 1. About the secret key.

The secret key is defined to be $\sigma$-parametrized.

Output: $V = \{0\}^{n/2}$. In practice,

Input: $A \in F_3^{r \times n}$ and $g \leq (n - r)$ be an integer.

Output: $A_{\text{extSyst}} \in F_3^{(r+g) \times n}$ or $\perp$.

Requirements:

1. Output is $\perp$ if and only if $\text{rank}(A_{[0,r)}) < r$;
2. $\langle A_{\text{extSyst}} \rangle = \langle A \rangle$;
3. $A_{\text{extSyst}}$ is in extended systematic form.

4.2. Wave Key Generation. The secret key in Wave is defined to be the underlying structure of a permuted generalized $(U|U + V)$-code while the public key is—up to some transformation, oblivious of the secret—a parity-check matrix $(Id_{n-k} | R)$ for this code. To improve verification speed we follow [BDNS21], taking as the public key a matrix $M(R) \in F_3^{(n-k) \times k}$ that can be publicly computed from $R \in F_3^{(n-k) \times k}$ (and reciprocally) as in Definition 3.

**Definition 3.** If $R \in F_3^{(n-k) \times k}$, then we define $M(R)$ to be the matrix in $F_3^{k \times (n-k)}$ such that

$$
\text{row}(M(R), 2i) := \text{col}(R, 2i) + \text{col}(R, 2i + 1)
$$

and if $k$ is odd,

$$
\text{row}(M(R), k - 1) := -\text{col}(R, k - 1).
$$

**Algorithm 4** Key Generation

Output: $V = \{0\}^{n/2}$.

1: \hspace{1em} $G_V \leftarrow F_3^{k \times n/2}$
2: \hspace{1em} $H_V \leftarrow \text{Orthogonal}(G_V)$ \hspace{1em} $\triangleright H_V \in F_3^{(n/2-kU) \times n/2}$ of full rank such that $G_V H_V^\top = 0$
3: \hspace{1em} $H_U \leftarrow F_3^{(n/2-kU) \times n/2}$
4: \hspace{1em} $b \leftarrow F_3^{n/2}$
5: \hspace{1em} $c \leftarrow \{0\}^{n/2}$ \hspace{1em} $\triangleright$ Coordinates of $c$ are non-zero
6: \hspace{1em} $d \leftarrow 1 + b \times c$
7: \hspace{1em} $H \leftarrow \begin{pmatrix} d \times H_U & -b \times H_U \\ -c \times H_V & H_V \end{pmatrix}$
8: \hspace{1em} $\sigma \leftarrow G_n$
9: \hspace{1em} $(Id_k \parallel R) \leftarrow \text{SystGaussElim}(H, \sigma)$ \hspace{1em} $\triangleright$ Algorithm 1, $\sigma$ may differ from $\sigma$
10: \hspace{1em} $M \leftarrow M(R)$ \hspace{1em} $\triangleright$ As in Definition 3
11: \hspace{1em} $\text{return } (pk = M, sk = (H_U, G_V, b, c))$

**About the secret key.** The secret key is defined to be $V = \{0\}^{n/2}$. In practice, we sample the random matrices $H_U$ and $G_V$ using pseudorandom generator seeded with a master key $mk$, so we can store the much more compact ($mk, \sigma, b, c$) as the secret key and regenerate $H_V$ and $G_V$ as needed. We sample the matrices using an XOF $f_{mk}$ parametrized by $mk$: for example, \( f_{mk}(\"U\mid i \) gives the $i$-th column of $H_V$ (including the constant "U" provides domain separation). More precisely, we propose using SHAKE256($mk \parallel \cdot$) for $f_{mk}$. 


4.3. Wave Signature. Wave signing is built around a decoder algorithm, for which there are multiple equivalent descriptions; here, we describe it in terms of noisy codewords. There are two steps. First, a decoding relative to the code \( V \) (\( \text{Decode}_V \)), producing an error pattern \( e_V \); then, a decoding relative to the code \( U \) and dependent on \( e_V \) (\( \text{Decode}_U \)), producing an error pattern \( e_U \). These error patterns are combined to produce the signature.

**Algorithm 5 Wave Signature**

Input: a message \( m, \ sk = (H_U, G_V, \pi, b, c) \)
Output: \((s, \text{salt})\)

1: repeat
2: \( \text{salt} \leftarrow \$\{0,1\}^{2\lambda} \quad \triangleright \lambda \in \{128, 192, 256\} \) denotes the security level
3: \( x \leftarrow \text{Hash}(m \parallel \text{salt}) \quad \triangleright x \in \mathbb{F}_3^{n-k} \)
4: \( y = (y_L \parallel y_R) \leftarrow (x \parallel 0^k)^{\pi-1} \)
5: \( y_V \leftarrow y_R - c \cdot y_L \quad \triangleright \text{Algorithm 6} \)
6: \( e_V \leftarrow \text{Decode}_V(y_V, G_V) \)
7: \( y_U \leftarrow y_L - b \cdot y_V \quad \triangleright \text{simplification of } y_U = (1 + c \cdot b) \cdot y_L - b \cdot y_R \)
8: \( e_U \leftarrow \text{Decode}_U(y_U, e_V, b, c, H_U) \quad \triangleright \text{Algorithm 7} \)
9: \( e_L \leftarrow e_U + b \cdot e_V \)
10: \( e_R \leftarrow c \cdot e_L + e_V \quad \triangleright \text{simplification of } e_R = c \cdot e_U + (1 + b \cdot c) \cdot e_V \)
11: until \((|e_V|, n/2 - w + |e_L \cdot e_R|) \notin \text{Accept} \)
12: \( e \leftarrow (e_L \parallel e_R)^\pi \)
13: \( s \leftarrow e_{[n-k,n]} \)
14: return \((s, \text{salt})\)

**Remark 2.** The signatures such that \((|e_V|, n/2 - w + |e_L \cdot e_R|) \notin \text{Accept} \) are rejected and the signature process restarts. The probability of rejection is negligible in practice, less than \(2^{-68} \) in our reference implementation. However, this rejection sampling is formally required to guarantee that the Rényi divergence between the output distributions of the actual algorithm and its “ideal” version is small enough (see §7).

**Proposition 1.** Let \((pk = M, sk = (H_U, G_V, \pi, b, c))\) be a valid Wave keypair. On input \( m \) and \( sk \), Algorithm 5 outputs \((s, \text{salt})\) such that

\[
|s| + |\text{Hash}(m \parallel \text{salt}) - sR^\top| = w
\]

where \( R \) is such that \( M = M(R) \) (as in Definition 3).

**Proof.** Propositions 2 and 3 show that Algorithms 6 (\( \text{Decode}_V \)) and 7 (\( \text{Decode}_U \)) output \( e_V \) and \( e_U \) satisfying

(i) \( y_V - e_V \in \langle G_V \rangle \),
(ii) \( y_U - e_U \) \( H_U^\top = 0_{n/2-k_U} \), and
(iii) \(|e| = |e_L| + |e_R| = w\).

In the notation of Algorithm 4,

\[
H = \begin{pmatrix}
\frac{d \cdot H_U}{-c \cdot H_V} & -b \cdot H_U \\
-c \cdot H_V & H_V
\end{pmatrix}
\]

where \( d = 1 + b \cdot c \) and \( H_V \) satisfies

\[
G_V H_V^\top = 0_{k \times (n-k)}.
\]
Therefore, according to Condition (i),
\[(y_V - e_V)H^T_V = 0_{n/2-k_V}.\] (4)

Now
\[((e_L \parallel e_R) - (y_L \parallel y_R))H^T\]
\[= \left(\left(\left((e_L - y_L) \ast d - (e_R - y_R) \ast b\right)H^T_U \parallel \left(-(e_L - y_L) \ast c + (e_R - y_R)\right)H^T_V\right)\right),\] (5)

but
\[(e_L - y_L) \ast d - (e_R - y_R) \ast b = (e_L - y_L) \ast (d - c \ast b) - (e_V - y_V) \ast b\]
\[= e_L - y_L - (e_V - y_V) \ast b\]
\[= e_U - y_U\] (6)

and
\[-(e_L - y_L) \ast c + e_R - y_R = e_V - y_V,\] (7)

so plugging Equations (6) and (7) into Equation (5) gives
\[((e_L \parallel e_R) - (y_L \parallel y_R))H^T = ((e_U - y_U)H^T_U \parallel (e_V - y_V)H^T_V).\]

Now using Condition (ii) and Equation (4) yields
\[((e_L \parallel e_R)^\pi - (y_L \parallel y_R)^\pi) (H^\pi)^T = ((e_L \parallel e_R) - (y_L \parallel y_R))H^T = 0_{n-k}.\] (8)

By the definitions of $\pi$ and $\text{SystGaussElim}$, there exists a non-singular matrix $S \in \mathbb{F}_3^{(n-k) \times (n-k)}$ corresponding to the Gaussian elimination such that
\[SH^\pi = (\text{Id}_{n-k} \mid R).\]

Therefore Equation (8) becomes
\[0_{n-k} = ((e_L \parallel e_R)^\pi - (y_L \parallel y_R)^\pi)(SH^\pi)^T\]
\[= ((e_L \parallel e_R)^\pi - (y_L \parallel y_R)^\pi)(\text{Id}_{n-k} \mid R)^T\]
but since $e = (e_L \parallel e_R)^\pi$ and $(y_L \parallel y_R)^\pi = (x \parallel 0_k)$ we have
\[0_{n-k} = (e - (x \parallel 0_k))(\text{Id}_{n-k} \mid R)^T\]
\[= e_{[0,n-k]} - x + e_{[n-k,n]}R^T\]
\[= e_{[0,n-k]} - \text{Hash}(m \parallel \text{salt}) + sR^T.\]

Therefore,
\[|s| + |\text{Hash}(m \parallel \text{salt}) - sR^T| = |s| + |e_{[0,n-k]}|\]
\[= |e_{[n-k,n]}| + |e_{[0,n-k]}|\]
\[= |e|\]

and we conclude the proof by applying Condition (iii). □

**Leakage-free signatures.** One of the key properties of Wave is that the vector $e$ in Instruction 12 of Algorithm 5 has been proven to be uniformly distributed over words of Hamming weight $w$ (see [DST19, §5]). In particular, its distribution is independent of the secrets involved in the signing process: even with the knowledge of the secret key, signatures
are indistinguishable from random words of weight $w$. This property implies that \texttt{Wave}
 is a hash-and-sign signature scheme immune to leakage attacks. We stress, however, that
this property only holds if \texttt{Wave} is properly implemented. Some implementation mistakes,
such as incorrect sampling of random data in $\texttt{Decode}_V$ or $\texttt{Decode}_V$, may produce valid
but biased signatures, opening the door to statistical attacks. Some possible biases are
described in \cite{DST17, §5.1}.

4.3.1. \textit{Decoder for }$V$. The input to $\texttt{Decode}_V$ in Instruction 6 of Algorithm 5 is a matrix
$G_V \in \mathbb{F}_3^{k_V \times n/2}$ and a word $y_V \in \mathbb{F}_3^{n/2}$ and the output is a word $e_V \in \mathbb{F}_3^{n/2}$ such that $y_V - e_V \in \langle G_V \rangle$. It is also required (to avoiding leakage) that over all possible uniformly distributed
inputs $(G_V, y_V)$, the weight distribution of the output $e_V$ is close to the distribution $\mathcal{D}$ of
$|e_L + e_R|$ when $(e_L \parallel e_R)$ is uniformly distributed over words of Hamming weight $w$ in $\mathbb{F}_3^2$.

The algorithm $\texttt{Decode}_V$ first splits $[0, n/2)$ in two by choosing uniformly a set $L \subseteq [0, n/2)$
of $k_V - g$ indices\(^\text{1}\). Without loss of generality, given $x \in \mathbb{F}_3^{n/2}$, we define $x^{(0)}$ and $x^{(1)}$ by
writing $x$ (up to a permutation) as follows
\begin{equation}
x = \begin{bmatrix} k_V - g & n/2 - k_V + g \end{bmatrix}
\begin{bmatrix} x^{(0)} & x^{(1)} \end{bmatrix}
\end{equation}
with the left part $x^{(0)}$ indexed by $L$. $\texttt{Decode}_V$ selects a word $e_V = (e^{(0)} \parallel e^{(1)})$ such that $e^{(1)}$
is uniformly distributed in $\mathbb{F}_3^{n/2-k_V+g}$ and $e^{(0)}$ is chosen with a weight $t$ sampled from $\mathcal{D}_V$.
The weight of $e^{(1)}$ follows a binomial distribution with parameters $(n/2 - k_V + g, 2/3)$, say $B_V$. The distribution $\mathcal{D}_V$ is chosen such that $\mathcal{D}_V + B_V^2$ is close to $\mathcal{D}$.

\begin{algorithm}
\begin{algorithmic}[1]
\Function{Decode}_V (y_V, G_V) \EndFunction
\State $t \leftarrow \mathcal{D}_V[0, k_V - g]$
\Repeat
\State $\pi \leftarrow \mathcal{S}_{n/2}$
\State $y \leftarrow y_V^\pi$
\State $G \leftarrow \text{PartialGaussElim}(G_V^\pi, g)$
\Until $G \neq \bot$
\State $x \leftarrow (\mathbb{F}_3 \setminus \{0\})^t \times \{0\}^{k_V - g - t} \times \mathbb{F}_3^g$
\State $e \leftarrow y + (x - y^{(0)})G$
\Comment{$y = (y^{(0)} \parallel y^{(1)}) \in \mathbb{F}_3^{n/2}$ with $y^{(0)} \in \mathbb{F}_3^{k_V - g}$}
\State return $e_V = e^{\pi^{-1}}$
\end{algorithmic}
\end{algorithm}

\textbf{Proposition 2.} \textit{On input }$(y_V, G_V)$, the vector $e_V \in \mathbb{F}_3^{n/2}$ output by Algorithm 6 satisfies
$y_V - e_V \in \langle G_V \rangle$.

\textit{Proof.} By definition, $y - e \in \langle G \rangle = \langle G_V^\pi \rangle$ in Instruction 9. The result follows on
applying $\pi^{-1}$. \hfill \square

\(^\text{1}\)The gap $g$ is a system parameter such that the submatrix formed by any $k_V - g$ columns of $G_V$ has full
rank with overwhelming probability.

\(^\text{2}\)The distribution of $|x + y|$ when $x$ and $y$ are independently distributed according to $\mathcal{D}_V$ and $B_V$.\hfill
Remark 3. As it is described, Algorithm 6 samples a random permutation $\pi$ and implicitly defines a set $L = \pi([0, k_V - g])$. While $L$ must be distributed uniformly, this is not required for $\pi$ (which must only have $L$ as its first $k_V - g$ entries). In practice (as in §B.3.2), $\pi$ is sampled so that $\pi([0, k_V - g))$ and $\pi([0, t))$ are uniformly distributed in $[0, n/2)$ and $\pi([0, k_V - g))$, respectively.

Remark 4. Instructions 4 and 5 of Decode$_V$ sample a permutation and apply it to a vector; this may be implemented as a single subroutine. Using the procedure suggested in §B.3.2, the call would be

$$(\pi, y) \leftarrow \text{RandPerm}_V(n/2, k_V - g, t, y_V)$$

where the arguments $k_V - g$ and $t$ are provided to ensure that both $\pi([0, k_V - g))$ and $\pi([0, t))$ are uniformly distributed (see Algorithm 27).

4.3.2. Decoder for $U$. The input of Decode$_U$ in Instruction 8 of Algorithm 5 is a matrix $H_U \in \mathbb{F}_3^{(n/2-k_U) \times n/2}$ and a vector $y_U \in \mathbb{F}_3^{n/2}$, and the output a vector $e_U \in \mathbb{F}_3^{n/2}$ such that $(y_U - e_U)H_U^\top = 0_{n/2-k_U}$. The target distribution for $e_U$ is conditioned by the result $e_V$ of the first decoding. It is shown in [DST19, §5] that, conditioned on $t := |e_V|$, the output $e_U$ is correctly distributed if and only if the number

$$j = \# (\{0, n/2\} \setminus (\text{Supp}(e_V) \cup \text{Supp}(e_U)))$$

of positions that are simultaneously null in $e_U$ and $e_V$ follows a prescribed distribution, dependent on $t$.

Algorithm 7 (Decode$_U$) splits $[0, n/2)$ in two by sampling an integer $\ell \in [0, t]$ according to $D_U(t)$ where $t = |e_V|$, and then uniformly sampling a set $L \subseteq [0, n/2)$ of $n/2-k_U+g$ indices containing exactly $\ell$ elements of Supp$(e_V)$. Without loss of generality, given $x \in \mathbb{F}_3^{n/2}$ we define $x^{(0)}$ and $x^{(1)}$ by writing $x$ (up to a permutation) as follows

$$x = \begin{cases} n/2 - k_U + g & \\ x^{(0)} & \\ \ell & \\ x^{(1)} & \\ t - \ell & \\ k_U - g \end{cases}$$

(10)

with the left part $x^{(0)}$ being indexed by $L$. The $t$ positions of Supp$(e_V)$ are depicted with $\ell$ of them being on the left block and the other $t - \ell$ being full right but they could be anywhere within their blocks. The algorithm selects a word $e = (e^{(0)} \parallel e^{(1)})$, which will be equal to $e_U$ up to some permutation, such that $e^{(0)}$ is uniformly distributed in $\mathbb{F}_3^{n/2-k_U+g}$ and $e^{(1)}$ is chosen to reach the final signature weight (see below). The value of $j$ is controlled by $\ell$, which is distributed according to $D_U(t)$. As for $V$, an appropriate choice of the distribution $D_U(t)$ allows a distribution of $j$ that is close to the target distribution.

**About the choice of $e^{(1)}$.** The choice of $e^{(1)} \in \mathbb{F}_3^{k_U-g}$ in Instruction 20 of Algorithm 7 is such that both $e_L = e_U + b \cdot e_V$ and $e_R = c \cdot e_L + e_V$ (from which a signature is built in Instructions 9-14 of Algorithm 5) have $k_U - g$ non-zero coordinates on $\pi([n/2 - k_U + g, n/2))$, as shown in Lemma 3. This will follow from the fact that $e_U$ and $e_V$ satisfy

$$e_U(i) = (c(i) - b(i))e_V(i) \quad \text{if } i \in \pi([n/2 - k_U + g, n/2)) \cap \text{Supp}(e_V),$$

$$e_U(i) \in \mathbb{F}_3 \setminus \{0\} \quad \text{if } i \in \pi([n/2 - k_U + g, n/2)) \setminus \text{Supp}(e_V).$$

(11)
Algorithm 7 Decode$_U$

1: function Decode$_U(y_U, e_V, b, c, H_U)$
2: \( t \leftarrow |e_V| \)
3: \( \ell \leftarrow U_{[0, t]}^f \)
4: repeat
5: \( \pi \leftarrow \{ \pi \in S_{n/2} \mid \#(\pi([0, n/2 - k_U + g]) \cap \text{Supp}(e_V) = \ell \} \)
6: \( y \leftarrow y_U^\pi \)
7: \( v \leftarrow ((c - b) \times e_V)^\pi \)
8: \( v^{(0)} \leftarrow v_{[0, n/2 - k_U + g]} \)
9: \( v^{(1)} \leftarrow v_{[n/2 - k_U + g, n/2]} \)
10: \( s \leftarrow (e_V \times e_V)^\pi \)
11: \( s^{(0)} \leftarrow s_{[0, n/2 - k_U + g]} \)
12: \( s^{(1)} \leftarrow s_{[n/2 - k_U + g, n/2]} \)
13: \( H \leftarrow \text{ExtGaussElim}(H_U^y, g) \) \( \triangleright H \in \mathbb{F}_3^{(n/2 - k_U + g) \times n/2} \)
14: until \( H \neq \perp \)
15: repeat
16: \( z^{(0)} \leftarrow (H_{i,i})_{0 \leq i < n/2 - k_U + g} \)
17: \( e^{(0)} \leftarrow \frac{1}{3}\mathbb{F}_3^{n/2 - k_U + g} \)
18: \( e^{(0)} \leftarrow (1 - z^{(0)}) \times e^{(0)} \)
19: \( e^{(1)} \leftarrow \frac{1}{3}(\mathbb{F}_3 \setminus \{0\})^{k_U - g} \)
20: \( e^{(1)} \leftarrow v^{(1)} + (1 - s^{(1)}) \times e^{(1)} \)
21: \( e^{(0)} \leftarrow e^{(0)} + (y - \langle e^{(0)} \parallel e^{(1)} \rangle) H^\top \)
22: \( i \leftarrow |s^{(0)} \times e^{(0)} - v^{(0)}| \)
23: \( j \leftarrow n/2 - k_U + g - \ell - |1 - s^{(0)} \times e^{(0)}| \)
24: until \( (2j + i = n - w) \) \( \triangleright \) check final weight
25: \( e \leftarrow (e^{(0)} \parallel e^{(1)} \rangle \)
26: return \( e_U = e^{\pi_{-1}} \)

Proposition 3. On input \((y_U, e_V, b, c, H_U)\), Algorithm 7 outputs \(e_U\) satisfying

\[
(y_U - e_U) H_U^\top = 0_{n/2 - k_U} \tag{12}
\]

Furthermore, if \(e_L := e_U + b \times e_V\) and \(e_R := c \times e_L + e_V\), then

\[
|e_L| + |e_R| = w. \tag{13}
\]

Proof. See Appendix D. \(\square\)

Remark 5. As it is described, Algorithm 7 samples an integer \(\ell\) according to \(D_U(t)\), then, uniformly, a permutation \(\pi\) such that \#\(L \cap \text{Supp}(e_V) = \ell\) where \(L = \pi([0, n/2 - k_U + g])\). The set \(L\) must be distributed uniformly with an intersection of size \(\ell\) with \(\text{Supp}(e_V)\), but uniformity among all permutations is not required for \(\pi\) which must only have \(L\) as its first \(n/2 - k_U + g\) entries.
Remark 6. The \(n/2 - k_U + g\) leftmost positions, corresponding to \(L\), include an information set (for \(H_U\)) plus \(g\) additional coordinates

\[
x = \begin{bmatrix} x^{(0)} & x^{(1)} \end{bmatrix}
\]

The \(g\) extra coordinates are depicted on the left here, but they could be anywhere; they are not necessarily disjoint from the \(\ell\) positions of \(\text{Supp}(e_V)\). Vector operations will use the vectors \(z^{(0)} \in \mathbb{F}_2^{n/2-k_U+g}\) and \(s = (s^{(0)} || s^{(1)}) \in \mathbb{F}_2^{n/2}\) as masks to select the various regions.

Remark 7. There is a rejection condition \(n - 2j - i = w\) to ensure the final weight is correct. This condition is oblivious of private information: its failure doesn’t require a new permutation or Gaussian elimination, only fresh values of \(e^{(0)}\) and \(e^{(1)}\).

Remark 8. Instructions 5, 6, 7 and 10 sample a permutation and apply it to several vectors. This may be implemented as a single subroutine. Using the procedure suggested in §B.3.3, the call would be

\[
\pi, (x') \leftarrow \text{RandPerm}_U(n/2, n/2 - k_U + g, \ell, \text{Supp}(e_V), x)
\]

where the vectors \(y_V\), \((c - b) * e_V\), and \(e_V * e_V\) are packed into \(x\) (that is, \(x(i) = (y_V(i) \parallel (c_i - b_i)e_V(i) \parallel e_V(i)^2)\)) and the output \(x'\) is unpacked to produce the permuted vectors (see Algorithm 28).

4.4. Wave Verification. To verify Wave signatures, we follow the approach of [BDNS21].

**Algorithm 8 Verification for Wave signatures.**

Input: \(m \in \{0, 1\}^*\), \(\sigma = (\text{salt}, s) \in \{0, 1\}^{2\lambda} \times \mathbb{F}_3^k\), \(M \in \mathbb{F}_3^{k \times (n-k)}\)

Output: True or False

1: \(x \leftarrow \text{Hash}(m || \text{salt})\)
2: for \(0 \leq i < (k - 1)/2\) do  
   \(\triangleright \) handle entries of \(s\) in pairs
3: \((\widehat{s}(2i), \widehat{s}(2i + 1)) \leftarrow (s(2i) + s(2i + 1), s(2i) - s(2i + 1))\)  
   \(\triangleright \) \((2i, 2i + 1)\)-th entries of \(\widehat{s}\)
4: if \(\widehat{s}(2i) = 1\) then
5: \(x \leftarrow x + \text{row}(M, 2i)\)  
   \(\triangleright \) add \(2i\)-th row of \(M\)
6: else if \(\widehat{s}(2i) = 2\) then
7: \(x \leftarrow x - \text{row}(M, 2i)\)  
   \(\triangleright \) subtract \(2i\)-th row of \(M\)
8: if \(\widehat{s}(2i + 1) = 1\) then
9: \(x \leftarrow x + \text{row}(M, 2i + 1)\)  
   \(\triangleright \) add \((2i + 1)\)-th row of \(M\)
10: else if \(\widehat{s}(2i + 1) = 2\) then
11: \(x \leftarrow x - \text{row}(M, 2i + 1)\)  
   \(\triangleright \) subtract \((2i + 1)\)-th row of \(M\)
12: if \(k\) is odd then
13: \(\triangleright \) handle last entry if necessary
14: if \(s(k - 1) = 1\) then
15: \(x \leftarrow x + \text{row}(M, k - 1)\)
16: else if \(s(k - 1) = 2\) then
17: \(x \leftarrow x - \text{row}(M, k - 1)\)
18: return \(|s| + |x| = w\)
Proposition 4. Given a putative Wave signature \((s, \text{salt})\) on a message \(m\) under a valid Wave public key \(M\), Algorithm 8 returns true if and only if
\[
|s| + |\text{Hash}(m \parallel \text{salt}) - sR^\top| = w
\]
where \(R\) is such that \(M = M(R)\) (as in Definition 3).

Proof. In the notation of Algorithm 8, let \(\hat{s}\) be defined by
\[
\begin{align*}
\hat{s}(2i) &:= s(2i) + s(2i + 1) \\
\hat{s}(2i + 1) &:= s(2i) - s(2i + 1)
\end{align*}
\]
for \(0 \leq i < \frac{k - 1}{2}\) and let \(\hat{s}(k - 1) := s(k - 1)\) if \(k\) is odd. At the end of the execution of Algorithm 8, we have
\[
x = \text{Hash}(m \parallel \text{salt}) + \hat{s}M. \tag{15}
\]
Notice that
\[
sR^\top = -\hat{s}M. \tag{16}
\]
because (from Definition 3)
\[
\begin{align*}
\hat{s}(2i) \cdot \text{row}(M, 2i) + \hat{s}(2i + 1) \cdot \text{row}(M, 2i + 1) \\
&= -(s(2i) \cdot \text{col}(R, 2i) + s(2i + 1) \cdot \text{col}(R, 2i + 1))
\end{align*}
\]
for \(0 \leq i < (k - 1)/2\), and
\[
\hat{s}(k - 1) \cdot \text{row}(M, k - 1) = -s(k - 1) \cdot \text{col}(R, k - 1)
\]
if \(k\) is odd. Combining Equations (15) and (16) and using Proposition 1 concludes the proof. \(\square\)

Algorithm 8 implicitly uses Equation (16) to replace the standard Wave verification equation
\[
|s| + |\text{Hash}(m \parallel \text{salt}) - sR^\top| = w
\]
with the equivalent equation
\[
|s| + |\text{Hash}(m \parallel \text{salt}) + \hat{s}M| = w.
\]
The point of verifying with the product \(\hat{s}M\) rather than \(sR^\top\) is explained in [BDNS21]: since the vector \(s\) is supposed to have high weight, the vector \(\hat{s}\) has many zeroes, and so \(\hat{s}M\) is easier to compute than \(sR^\top\). The coefficients of the vector \(\hat{s}\) can easily be computed on the fly as the signature vector \(s\) is read (or decompressed).

Indeed, in any given Wave signature verification using Algorithm 8, roughly \(|s|/2\) of the \(\hat{s}(i)\) are zero, so almost half of the rows of the public key \(M\) are never read, let alone operated on. Given the size of Wave public keys, the latency involved in loading key data from memory is often a bottleneck in practice.
5. Performance Analysis

Our performance analysis is based on the reference implementation, which is written in pure portable C99, and not optimized for any specific architecture; in particular, it does not take advantage of vectorization such as Intel AVX instructions (which were shown in [BDNS21] to significantly improve Wave implementation performance).

Table 5 provides signature and key sizes for each instance for easy reference. Note that the compressed encoding for signatures yields variable-length signatures, and we list the maximum sizes here (see Appendix C.2 for further details).

Table 5. Key and signature sizes for Wave instances.

<table>
<thead>
<tr>
<th>Instance</th>
<th>Signature (B)</th>
<th>Private key (B)</th>
<th>Public key (B)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wave822</td>
<td>≤ 822</td>
<td>18 900</td>
<td>3 677 390</td>
</tr>
<tr>
<td>Wave1249</td>
<td>≤ 1 249</td>
<td>27 630</td>
<td>7 867 598</td>
</tr>
<tr>
<td>Wave1644</td>
<td>≤ 1 644</td>
<td>36 360</td>
<td>13 632 308</td>
</tr>
</tbody>
</table>

Table 6 presents cycle counts for our programs on an Intel i5-1135G7 platform. We provide two counts for signature verification. The first corresponds to the crypto_sign_open function from the NIST API, which must first decode the public key from its transport format (i.e., trits packed into a byte array, five trits to a byte, as in Appendix C.1) to an array of bitsliced ternary vectors (as in Appendix B.1). This process is expensive—especially given the size of the public key—and much more expensive than the subsequent testing of the verification equation!

Given the size of the public key, Wave is probably best-suited to applications where the public key is stored on the device in advance of verification (rather than being transmitted with the message). In these cases, we have the option of converting from transport to format at the time of storage, rather than re-converting for each verification. The second Verification column in Table 6 corresponds to this scenario: the bitsliced public key is already loaded, and the cycle count corresponds to pure verification using the verify function. While the bitsliced representation imposes a space overhead of 25%, the massive speedup of over two full orders of magnitude may more than justify this approach.
Table 6. Cycle counts for the Wave reference implementation. Programs were executed on an Intel i5-1135G7 with CPU frequency 2.4 GHz and maximum CPU frequency 4.2 GHz running Arch Linux (kernel 6.3.1). We compiled the code using GCC version 13.1.1 with compiler options `-O3` and `-march=native`. Each program was run 100 times with random inputs (using random 100-byte messages). Cycles were counted using the `rdtsc` instruction included in the file `cpucycles.h`.

<table>
<thead>
<tr>
<th>Instance</th>
<th>Key generation</th>
<th>Signing</th>
<th>Verification (transport PK)</th>
<th>Verification (bitsliced PK)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wave822</td>
<td>Average</td>
<td>14 468 000 043</td>
<td>1 160 793 621</td>
<td>205 829 565</td>
</tr>
<tr>
<td></td>
<td>Median</td>
<td>13 946 196 718</td>
<td>1 156 182 078</td>
<td>206 097 247</td>
</tr>
<tr>
<td></td>
<td>Lowest</td>
<td>13 672 518 457</td>
<td>1 094 264 195</td>
<td>191 450 426</td>
</tr>
<tr>
<td></td>
<td>Highest</td>
<td>18 892 143 347</td>
<td>1 367 744 577</td>
<td>236 350 926</td>
</tr>
<tr>
<td>Wave1249</td>
<td>Average</td>
<td>47 222 134 806</td>
<td>3 507 016 206</td>
<td>464 110 855</td>
</tr>
<tr>
<td></td>
<td>Median</td>
<td>46 285 891 873</td>
<td>3 534 752 493</td>
<td>467 362 945</td>
</tr>
<tr>
<td></td>
<td>Lowest</td>
<td>44 658 551 430</td>
<td>3 233 442 565</td>
<td>420 729 318</td>
</tr>
<tr>
<td></td>
<td>Highest</td>
<td>55 561 328 781</td>
<td>3 695 446 731</td>
<td>491 116 604</td>
</tr>
<tr>
<td>Wave1644</td>
<td>Average</td>
<td>108 642 333 507</td>
<td>7 936 541 947</td>
<td>813 301 900</td>
</tr>
<tr>
<td></td>
<td>Median</td>
<td>106 259 626 687</td>
<td>7 851 475 371</td>
<td>806 856 892</td>
</tr>
<tr>
<td></td>
<td>Lowest</td>
<td>104 525 692 173</td>
<td>7 608 672 796</td>
<td>782 171 263</td>
</tr>
<tr>
<td></td>
<td>Highest</td>
<td>117 900 860 252</td>
<td>8 225 419 171</td>
<td>817 790 558</td>
</tr>
</tbody>
</table>

Table 7. Hyperlinks to KATs with SHA2-256 checksums.

<table>
<thead>
<tr>
<th>Instance</th>
<th>Hyperlink</th>
<th>sha256sum</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wave822</td>
<td>PQCsignKAT_18900</td>
<td>ace94f3e8e1f692632758decb5471e7408bb7669f4d3a59647046e20bb0404b5</td>
</tr>
<tr>
<td>Wave1249</td>
<td>PQCsignKAT_27629</td>
<td>75e85be5bdcf300fcbcd898ee7d84a2475c5f17af06c1349eb9ded34605798e17</td>
</tr>
<tr>
<td>Wave1644</td>
<td>PQCsignKAT_36359</td>
<td>e67a83c9abdf143b4ab01ff5f2692d54534a3de1c3943165d907f077cee07356</td>
</tr>
</tbody>
</table>

6. Known Answer Tests

Wave may be implemented in many different ways, but it is crucial to respect the constraints imposed by the chosen parameters. Further, when utilizing a pseudorandom generator, it is important to ensure the reproducibility of the results.

In order to achieve this reproducibility, we provide Known Answer Test (KAT) values for each instance of Wave on our website. Table 7 provides hyperlinks to the KATs, with SHA2-256 checksums of each KAT file (which may be recomputed with `sha256sum`) to ensure integrity.
7. Provable Security

We now present a security argument for Wave against classical and quantum adversaries. We consider the standard EUF-CMA definition for signature schemes, where adversaries with access to a signing oracle must forge a signature on a new (non-queried) message. Since we are designing a post-quantum signature scheme, we will work in the Quantum Random Oracle Model (QROM), where the main hash function Hash used in our signature scheme is modelled as a truly random function with black-box access only; quantum adversaries have quantum access to this black box.

For quantum adversaries, $\lambda$ bits of security corresponds to a quantum adversary running in time $2^\lambda$. As per NIST guidelines, adversaries are restricted to $q_S = 2^{64}$ classical signing queries, no matter the intended security level.

7.1. Hard problems. We begin by defining the problems to which we will reduce the EUF-CMA security of Wave. First, recall the classic decoding problem DP over $\mathbb{F}_3$:

**Problem 1.** The Decoding Problem $\text{DP}(n, k, w)$ is:
- Input: $(H, s)$ where $H$ resp. $s$ are uniformly distributed over $\mathbb{F}_3^{(n-k) \times n}$ resp. $\mathbb{F}_3^{n-k}$.
- Output: a vector $e$ in $\mathbb{F}_3^n$ of Hamming weight $w$ such that $eH^\top = s$.

Forging a Wave signature on a given message resembles solving a DP instance where $H$ and $s$ represent the public key and the hash of that message, respectively. However, our adversary’s goal is to forge a signature on a freely chosen message, so it is more appropriate to consider a multi-target variant of DP.

**Problem 2.** The Decoding One Out of Many Problem $\text{DOOM}(n, k, w, N)$ is:
- Input: $(H, s_1, \ldots, s_N)$ where $H$ resp. the $s_i$ are uniformly distributed over $\mathbb{F}_3^{(n-k) \times n}$ resp. $\mathbb{F}_3^{n-k}$.
- Output: a vector $e \in \mathbb{F}_3^n$ of Hamming weight $w$, and $i \in [1, N]$ such that $eH^\top = s_i$.

Forging Wave signatures does not directly imply solving DP or DOOM, because Wave public keys are parity-check matrices not of truly random codes\(^3\), but of permuted generalized $(U|U+V)$-codes (see Definition 1). However, if Wave public keys are indistinguishable from random parity-check matrices, then security reduces to DOOM. (This is similar to McEliece-like cryptosystems [McE78, ABC+20], where security reduces to the decoding problem provided distinguishing Goppa codes from random is sufficiently hard.)

**Problem 3** (The Distinguishing Wave Keys Problem $\text{DWK}(n, k_U, k_V)$). Given $H \in \mathbb{F}_3^{(n-(k_U+k_V)) \times n}$, decide whether $H$ has been chosen uniformly at random or among parity-check matrices of permuted generalized $(U|U+V)$-codes where $U$ resp. $V$ has dimension $k_U$ resp. $k_V$.

7.2. Signature Distribution and Rényi Divergence. Wave security reduces to the hardness of Problems 2 and 3. We use the Rényi divergence to achieve a tight reduction, as in [LPSS17, Pre17, BLR+18] for LWE and lattice-based cryptosystems. Recall that if $\mathcal{P}$ and $\mathcal{Q}$ are distributions with $\text{Supp}(\mathcal{P}) \subseteq \text{Supp}(\mathcal{Q})$, then their Rényi divergence of order $\alpha$ (where $\alpha > 0$ and $\alpha \neq 1$) is

$$R_\alpha(\mathcal{P}||\mathcal{Q}) := \left( \sum_{x \in \text{Supp}(\mathcal{P})} \frac{\mathcal{P}(x)^\alpha}{\mathcal{Q}(x)^{\alpha-1}} \right)^{1/(\alpha-1)}.$$

\(^3\)A code is random if its parity-check matrix is uniformly drawn at random.
Wave signing uses internal distributions \(D_V\) and \(D_U\) to ensure signatures are properly distributed. Algorithm 5 constructs vectors \(e_V\) (using Algorithm 6, governed by \(D_V\)) and \(e_U\) (using Algorithm 7, governed by \(D_U\)), and then defines \(e_L := e_U + b \ast e_V\) and \(e_R := c \ast e_U + (1 + b \ast c) \ast e_V\). As shown in [DST19, §5.1], for Algorithm 5 to return signatures distributed as random words of Hamming weight \(w\), it suffices that the distributions \(Q\) and \(Q^{\text{ideal}}\) match, where

- \(Q\) is the distribution of \(|e_V|\) and \(n/2 - w + |e_L \ast e_R|\) in Algorithm 5 given \(D_U\) and \(D_V\); and
- \(Q^{\text{ideal}}\) is the distribution of \(|e_L - c \ast e_R|\) and \(n/2 - w + |e_L \ast e_R|\) on random words \((e_L \parallel e_R)\) of Hamming weight \(w\).

Cutting \(Q\) to some interval \(\text{Accept} \subseteq [0, n/2] \times [0, w/2]\) (as in Instruction 11 of Algorithm 5) to ensure that its support is included the support of \(Q^{\text{ideal}}\), we obtain

\[
R_{2\lambda}(Q||Q^{\text{ideal}}) = 1 + \varepsilon_{\text{Renyi}}. \tag{17}
\]

The internal distributions \(D_V\) and \(D_U\) must therefore be chosen to ensure that \(\varepsilon_{\text{Renyi}}\) is sufficiently small. In our reference implementation, the \(D_V\) and \(D_U\) included in Wave822, Wave1249, and Wave1644 all give

\[
\varepsilon_{\text{Renyi}} \leq 2^{-68}.
\]

### 7.3. Statement of the security reduction.

**Theorem 1.** Fix any \(\lambda \in \mathbb{N}\), and consider a quantum adversary \(A\) running in time \(2^\lambda\) limited to \(q_S = 2^{64}\) classical signing queries that tries to break the EUF-CMA security of an instance of Wave. In the QROM, we have

\[
\text{Adv}^{\text{EUF-CMA}}_{\text{Wave}}(A) \leq \sqrt{2}(1 - \varepsilon_{\text{Renyi}})^{q_S}\left(\text{Adv}^{\text{DOOM}}_{\text{Wave}}(2^\lambda) + \text{Adv}^{\text{DWK}}_{\text{Wave}}(2^\lambda) + \frac{q_S^2}{2\lambda_0}\right)
\]

where

- \(\text{Adv}^{\text{EUF-CMA}}_{\text{Wave}}(A)\) is the probability that \(A\) breaks the EUF-CMA security of Wave;
- \(\varepsilon_{\text{Renyi}}\) is defined in Equation (17);
- \(\text{Adv}^{\text{DOOM}}_{\text{Wave}}(2^\lambda)\) is the maximum probability that a quantum algorithm running in time \(2^\lambda\) solves DOOM (Problem 2) for the Wave parameters \(n, k,\) and \(w\) (the parameter \(N\) is not restricted, and in the quantum setting we even allow adversaries quantum access to the syndromes: that is, adversaries can efficiently compute the unitary \(|i\rangle|0\rangle \rightarrow |i\rangle|s_i\rangle\));
- \(\text{Adv}^{\text{DWK}}_{\text{Wave}}(2^\lambda)\) is \(|p - \frac{1}{2}|\), where \(p\) is the maximum probability that a quantum algorithm running in time \(2^\lambda\) solves DWK (Problem 3) for the Wave parameters;
- \(\lambda_0\) is the size of the salt. In our case, we always have \(\lambda_0 \geq 256\) hence \(\frac{q_S^2}{2\lambda_0} \leq 2^{-128}\).

The above also holds for classical adversaries in the Random Oracle Model (if the best considered attacks against Problems 2 and 3 are also classical).

Theorem 1 is proven by combining two existing results (which hold both in the ROM against classical adversaries and the QROM against quantum adversaries):

1. The results of [CD20] show that if Wave produces an ideal distribution of signatures (i.e., \(Q\) matches \(Q^{\text{ideal}}\)) then it reduces tightly to Problems 2 and 3.
2. Then, the results of [Pre17, Section 3.3 of the Eprint version] show that moving from an ideal signing distribution to a real distribution (i.e., replacing \(Q^{\text{ideal}}\) with \(Q\)) induces a multiplicative loss of \(\sqrt{2}(1 - \varepsilon_{\text{Renyi}})^{q_S}\) in the EUF-CMA advantage.
The internal distributions in Wave822, Wave1249, and Wave1644 all have $\varepsilon_{\text{Renyi}} \leq 2^{-68}$, so $(1 + \varepsilon_{\text{Renyi}})^{q^3} \leq \sqrt{2}$. Plugging this into Theorem 1 yields

$$\text{Adv}_{\text{Wave}}^{\text{EUF-CMA}}(A) \leq 2 \left( \text{Adv}_{\text{DOOM}}^{\text{DOOM}}(2^\lambda) + \text{Adv}_{\text{DWK}}^{\text{DWK}}(2^\lambda) + \frac{q^3}{2^{2w}} \right)$$

for all three instances, so their security tightly reduces to Problems 2 and 3. We discuss the best known attacks on these problems in §8.

8. Best Known Attacks

We now present the best known attacks on DOOM (which we call message attacks) and DWK (which we call key attacks). Both classes of attacks rely on algorithms to solve DP. While this classic problem has been widely studied [Pra62, Ste88, Dum91, FS09, Ber10, BLP11, MMT11, BJMM12, MO15, BM17, KT17, BM18, Kir18, BBSS20, CDMT22], much less has been done for DP instance in the context of working over $F_3$ instead of $F_2$ [BCDL19, Bri21, CDE21, KL22, Sen23].

8.1. Classical attacks. The best known attacks on DP and DOOM use the Information Set Decoding (ISD) framework of [FS09], which is a refinement of Prange’s algorithm [Pra62]. The idea is to find a single solution to DP in $F_3^\ell$ with weight $w$ by identifying exponentially many solutions to a simplified DP instance in $F_3^\ell$ with weight $p$, for chosen $\ell \leq n$ and $p \leq w$. For each potential solution, we can efficiently verify if it yields a complete solution to DP. This entire process is repeated until a solution is discovered. Several algorithms exist for listing solutions to this sub-problem: [Ste88] and [Dum91] take advantage of the birthday paradox while [MMT11] and [BJMM12] combine the so-called representation technique with merging techniques.

In the binary case ($q = 2$), the best known ISD ([BM18] with the correction in [CDMT22, Appendix B]) lists solutions to the sub-problem by searching for pairs of near-neighbours in some lists. Near-neighbours-based decoders designed for the ternary setting may have better asymptotic complexities than the ISD techniques mentioned above. However, an efficient near-neighbours search algorithm requires fuzzy hashing functions that associate close vectors. One of the best known ways to design a good fuzzy hashing function is to use a list decoder of a polar code, resulting in an $O(n \log(n))$ overhead (compared to other ISDs) that we take into account when setting parameters.

8.1.1. Classical message attacks. The ISD framework with Wagner’s algorithm [BCDL19] is the best known algorithm to find solutions for the sub-DP instance in the Wave context ($w/n \approx 0.89$ and $k/n = 1/2$). This involves creating lists of vectors corresponding to $e'' \in F_3^{k+\ell}$ with $|e''| = p$. In the DOOM solver of [Sen11], one of the lists is filled with some restrictions $s''_i$s of the $s_i$ over their last $k+\ell$ coordinates. The lists are then filtered to include only $e''$ for which $e''H''^T = s''_i$ for some $i$ (the sub-problem), where $H'' \in F_3^{(n-k)\times(k+\ell)}$ is some sub-matrix of $H$. The lists are merged using a binary merging tree, keeping only the pairs of vectors whose first coordinates sum to zero. Ultimately, we obtain a list of vectors from which we can deduce multiple solutions to the DP sub-instance, and thus to the full DP instance. Otherwise, the process is repeated until a solution is found.

8.1.2. Classical key attacks. One way to solve DWK, i.e. to distinguish the public key $H$ (a parity-check matrix of some permuted generalized $(U|U + V)$-code) from a randomly uniform matrix in $F_3^{(n-k)\times n}$ is to exhibit a codeword of form $(u, u)$ of weight $t$, where $t$ is a parameter that can be chosen. Indeed, these words may be more likely to appear in
a \((U|U + V)\)-code than in a random code [Sen23]. The best known classical attack uses ISD to find such vectors satisfying \(eH^\top = 0\). Within this range of parameters, Wagner’s algorithm [SS81] does not perform better than just having two merging steps and using the representation technique of [MMT11]. This attack computes multiple solutions to the DP sub-instance, and then checks if one of the candidate solutions satisfies the general DP.

8.2. **Quantum attacks.** Code-based problems, and more specifically decoding problems, have resisted quantum attacks very well so far. The best known quantum attacks on these various decoding problems are also based on ISD. Many quantum algorithms have been studied; for simpler examples such as Prange’s algorithm, a direct application of quantum amplitude amplification gives a quadratic advantage [Ber10], but we cannot get the same improvement for advanced ISD algorithms which list many solutions to a sub-problem. This has been extensively studied for a binary alphabet in [KT17], and extended in [Kir18, BBSS20]. Quantum algorithms for DP and DOOM have also been studied in the ternary setting of Wave [CDE21, Bri21].

8.2.1. **Quantum message attacks.** We employ the quantum ISD framework, where the sub-problem solver utilizes the quantum Wagner algorithm [CDE21]. In this quantum setting, the list of \(s_i\) is replaced by their quantum superposition, and the number of such elements can exceed the number in the classical setting. The classical lists are merged, and the merging of a classical list with the list in quantum superposition is accomplished using Grover’s algorithm [Gro96] to yield a quantum superposition of candidate solutions. If the probability of success is lower than \(1 - o(1)\), we apply amplitude amplification before the measurement to obtain a DP solution. We rely on the analysis of [CDE21] as well as the DOOM analysis of [Bri21], which provides the best quantum algorithm in this scenario.

8.2.2. **Quantum key attacks.** To find a codeword \((u, u)\) of weight \(t\), the best known attack also uses quantum ISD, finding the solutions to the sub-problem using quantum Wagner [CDE21]. As above, amplitude amplification can be applied to get a DP solution with high probability. Again, we combine the analyses of [CDE21] and (the classical) [Sen23] to study the best quantum algorithms here.

8.3. **Claimed security levels.** Table 8 lists the claimed security levels \(\lambda\) for Wave822, Wave1249, and Wave1644 against the attacks listed above. All our best classical and quantum attacks require \(\text{poly}(n)2^{an+o(n)}\) elementary operations for some \(\alpha\), where \(n\) is the code length. We ignore the \(\text{poly}(n)\) factor and the \(o(n)\) when estimating our security levels. Omitting these large overheads make our parameters very conservative.

We also ignore the cost of memory access, even though these algorithms can use a very large amount of memory: for example, the DOOM attack above requires space equal to its running time. In the quantum setting, these overheads are increased by the fact that the best known quantum attacks use a large amount of QRAM (Quantum Random Access Memory), whose feasibility is still in question [JR23]. This makes our security levels even more conservative in the quantum setting.
Table 8. Claimed security levels for Wave instances. In this context, $\lambda$ bits of security indicate that the most efficient known attacks on DOOM and key distinguishing all require a minimum time of $2^\lambda$ to execute.

<table>
<thead>
<tr>
<th>Wave822</th>
<th>NIST Post-Quantum</th>
<th>Classical (bits)</th>
<th>Quantum (bits)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Level I</td>
<td>128</td>
<td>77</td>
</tr>
<tr>
<td>Wave1249</td>
<td>Level III</td>
<td>192</td>
<td>117</td>
</tr>
<tr>
<td>Wave1644</td>
<td>Level V</td>
<td>256</td>
<td>157</td>
</tr>
</tbody>
</table>

9. Advantages and Limitations

9.1. Advantages.

- **Short signature length**: at most 822 bytes for NIST Level I, and scaling linearly with the security parameter.

- **Fast verification**, with scope for further significant speed-ups in dedicated implementations (as in [BDNS21]).

- **Proven secure** under well identified code-based hardness assumptions, in the ROM and the QROM with tight reductions.

- The scheme is **immune to statistical attacks** by design, and the reference implementation is immune to statistical attacks from any adversary limited to $2^{64}$ queries to a signing oracle.

9.2. Limitations.

- Large public keys: 3.6MB for NIST Level I, and scaling quadratically with the security parameter.

- Signing and key generation rely on inherently slow Gaussian elimination on large matrices. Accelerating these primitives while ensuring implementation safety is a significant challenge.

- We assume the hardness of DWK, distinguishing permuted generalized $(U|U+V)$-codes from random codes. This assumption is fairly new (it was introduced in 2018) but we have reasons to argue for its hardness: for example, these permuted generalized $(U|U+V)$-codes have a lot of inner entropy. The only exploitable structure seems to be the existence of small codewords, which we already fully exploit in our security analysis. We believe our parameters are extremely conservative with respect to these codes, providing a comfortable security margin against possible attacks on a relatively new problem, but further analysis may show that we can reduce parameter sizes, thus improving key sizes and performance.

- The parameters include the internal discrete distributions $D_V$ and $D_U(t)$, which condition the decoder output distribution (which must be close to uniform to guarantee security: see §7), Adding rejection sampling if necessary. The internal distributions in our implementation were computed by an ad-hoc procedure (taking a few hours). They produce an output distribution which is close enough to uniform, with a Rényi divergence $\leq 1 + 2^{-68}$, without rejection sampling. At the moment,
the internal distributions are given as tables of numbers. Tools will be provided to guarantee their correctness.

References


[CDE21] André Chailloux, Thomas Debris-Alazard, and Simona Etinski. Classical and quantum algorithms for generic syndrome decoding problems and applications to the Lee metric. In Jung Hee


In order to sign any messages with Wave, we need to define a hash function into $\mathbb{F}_{3}^{n-k}$. We use the hash function as defined in [BDNS21, §3.1]. We recall here its specifications.

The **Hash** (Algorithm 9) defines a cryptographic hash function $\{0, 1\}^{*} \rightarrow \mathbb{F}_{3}^{n-k}$ by wrapping the standard SHA3-512 hash function with the following two functions:

1. **Ternarize** : $\{0, 1\}^{*} \times \mathbb{Z}_{\geq 0} \rightarrow \mathbb{F}_{3}^{\tau}$ (Algorithm 10) views its input $((x_0, x_1, \ldots), \tau)$ as the vector of coefficients in the little-endian binary expansion of an integer $x$, together with a length $\tau$, and returns the ternary vector of length $\tau$ representing the little-endian ternary expansion of $x \mod 3\tau$.

2. **Expand** : $\{0, 1\}^{2\lambda} \rightarrow \mathbb{F}_{3}^{\tau}$ (Algorithm 11) is a pseudorandom function ($\lambda$ denotes the security parameter). **Expand** applies SHAKE256 to its input to produce a long stream of pseudorandom bytes, which we view as integers in $[0, 256)$. The non-negative integers less than $3^{\tau} = 243$ are in bijection with $\mathbb{F}_{3}^{\tau}$, so if a byte is less than 243 we convert it to an element of $\mathbb{F}_{3}^{\tau}$ with **Ternarize** and concatenate it to the output; otherwise we skip the byte. We continue processing bytes until we have produced $\tau$ elements of $\mathbb{F}_{3}$ (discarding the last few trits if $\tau$ is not a multiple of 5).

The collision- and preimage-resistance of **Hash** are derived from the properties of SHA3-512 using standard (concatenation) hash combiner arguments (see e.g. [Jou04, §4] and [Leh10]). **Ternarize** simply transcodes its input, so the composition of **Ternarize** and SHA3-512 preserves the security properties of SHA3-512. The composition of **Expand** and SHA3-512 has weaker preimage and collision resistance (because bytes in $[243, 256)$ are discarded), but it still has strong pseudorandomness properties, and it is relatively fast to compute. The concatenation of the two has the security of the strong hash, and the good pseudorandomness of both.

---

**Algorithm 9** Hashing from $\{0, 1\}^{*}$ to $\mathbb{F}_{3}^{n-k}$ in Wave.

1: function Hash($m$) ▷ $m \in \{0, 1\}^{*}$
2: $h \leftarrow \text{Truncate}(\text{SHA3-512}(m), 2\lambda)$ ▷ Truncate SHA3-512 output to first $2\lambda$ bits
3: $t \leftarrow \text{Ternarize}(h, \lceil 2\lambda/\log_2(3) \rceil)$ ▷ Algorithm 10
4: $p \leftarrow \text{Expand}(h, n - k - \lceil 2\lambda/\log_2(3) \rceil)$ ▷ Algorithm 11
5: return $(t, p)$

---

**Algorithm 10** Converting integer values to ternary vectors of a specified length, corresponding to the little-endian ternary expansion of the input.

1: function Ternarize($x, \tau$) ▷ $x \geq 0$ and $\tau > 0$
2: $v \leftarrow 0 \in \mathbb{F}_{3}^{\tau}$
3: for $0 \leq i < \tau$ do
4: $(x, v(i)) \leftarrow (\lfloor x/3 \rfloor, x \mod 3)$
5: return $v$ ▷ $v \in \mathbb{F}_{3}^{\tau} \cong \{0, 1, 2\}^{\tau}$ such that $x = \sum_{i=1}^{\tau} v(i)3^{i-1}$
Algorithm 11 Expand a binary seed to a pseudo-random stream of ternary values. The random bytestream may be instantiated with an XOF or a stream cipher. The expected number of bytes drawn from the stream is \((256\tau)/(243 \times 5) \approx 0.21\tau\).

1: function Expand\((h, \tau)\) \hfill \triangleright h \in \{0, 1\}^{2^\lambda} \text{ and } \tau > 0
2: stream = pseudorandom bytestream obtained via SHAKE256\((h)\)
3: \((p, r) \leftarrow ((), \tau)\) \hfill \triangleright p: empty vector over \(\mathbb{F}_3\)
4: while \(r > 0\) do
5: \(b \leftarrow\) next byte from stream, viewed as an integer in \([0, 255]\)
6: if \(b < 243\) then
7: \((p, r) \leftarrow (p, \text{Ternarize}(b, \min(5, r)), r)\) \hfill \triangleright \text{Algorithm 10}
8: return \(p\) \hfill \triangleright p \in \mathbb{F}_3^\tau

Appendix B. Specification toward a Constant Time Implementation

B.1. Bitsliced Arithmetic over \(\mathbb{F}_3\). The reference implementation uses the following bitsliced \(\mathbb{F}_3\)-vector arithmetic. An element \(a\) of \(\mathbb{F}_3\) is represented as a pair of bits \((a_h, a_\ell)\):

\[
0 \leftrightarrow (0, 0), \quad 1 \leftrightarrow (0, 1), \quad 2 \leftrightarrow (1, 1).
\]

All the arithmetic can be expressed with binary operations, addition, multiplication, and inclusive or denoted ‘\(|\)’. Addition and subtraction in \(\mathbb{F}_3\) requires 7 binary operations, negation in \(\mathbb{F}_3\) requires 1 binary operation, and multiplication in \(\mathbb{F}_3\) requires 3 binary operations.

\[
c = a + b \iff \begin{cases} c_h = (a_\ell + b_h)(a_h + b_\ell) \\ c_\ell = (a_\ell + b_\ell) | (a_h + b_\ell + b_h) \end{cases}
\]

\[
c = a - b \iff \begin{cases} c_h = (a_\ell + b_\ell + b_h)(a_h + b_\ell) \\ c_\ell = (a_\ell + b_\ell) | (a_h + b_h) \end{cases}
\]

\[
c = -a \iff \begin{cases} c_h = a_\ell + a_\ell \\ c_\ell = a_\ell \end{cases}
\]

\[
c = a \times b \iff \begin{cases} c_h = (a_\ell + b_h) a_\ell b_\ell \\ c_\ell = a_\ell b_\ell \end{cases}
\]

This representation and the corresponding arithmetic fits well with bit slicing techniques and the above operations apply conveniently to vectors. A ternary vector \(x = (x_i)_{0 \leq i < n}\) where \(x_i \leftrightarrow (x_{i,h}, x_{i,\ell})\) is represented by \((x_h, x_\ell)\) with \(x_h = (x_{i,h})_{0 \leq i < n}\) and \(x_\ell = (x_{i,\ell})_{0 \leq i < n}\).
The vector operations can be computed for logical operations $\&$ and $\oplus$ on binary words:

\[
\begin{align*}
\mathbf{c} = \mathbf{a} + \mathbf{b} & \iff \begin{cases} 
\mathbf{c}_h = (\mathbf{a}_\ell \oplus \mathbf{b}_h) \& (\mathbf{a}_h \oplus \mathbf{b}_\ell) \\
\mathbf{c}_\ell = (\mathbf{a}_\ell \oplus \mathbf{b}_\ell) \mid (\mathbf{a}_h \oplus \mathbf{b}_h)
\end{cases} \\
\mathbf{c} = \mathbf{a} - \mathbf{b} & \iff \begin{cases} 
\mathbf{c}_h = (\mathbf{a}_\ell \oplus \mathbf{b}_\ell \oplus \mathbf{b}_h) \& (\mathbf{a}_h \oplus \mathbf{b}_\ell) \\
\mathbf{c}_\ell = (\mathbf{a}_\ell \oplus \mathbf{b}_\ell) \mid (\mathbf{a}_h \oplus \mathbf{b}_h)
\end{cases} \\
\mathbf{c} = -\mathbf{a} & \iff \begin{cases} 
\mathbf{c}_h = \mathbf{a}_h \oplus \mathbf{a}_\ell \\
\mathbf{c}_\ell = \mathbf{a}_\ell
\end{cases} \\
\mathbf{c} = \mathbf{a} \star \mathbf{b} & \iff \begin{cases} 
\mathbf{c}_h = (\mathbf{a}_h \oplus \mathbf{b}_h) \& \mathbf{a}_\ell \& \mathbf{b}_\ell \\
\mathbf{c}_\ell = \mathbf{a}_\ell \& \mathbf{b}_\ell
\end{cases}
\end{align*}
\]

B.2. Sampling Trits. The purpose is to efficiently produce—close to—indeendent and uniform trits from independent and uniform bits. The description assumes a binary pseudorandom generator $\text{prng}$ initialized with $\text{seed}$, e.g. any XOF with input $\text{seed}$. The instruction $\text{randbits}(a, \text{prng})$ draws the next $a$ bits of $\text{prng}$ and returns the corresponding integer in $[0, 2^a)$. It can be used in Algorithm 12 to produce a pseudorandom ternary vector of length $n$ from $\text{seed}$. This algorithm admits as parameters the integers $a$ and $b$, it will output independent uniform trits if $3^b \geq 2^a$.

**Limitation.** If Algorithm 12 is used in a cryptographic context it will leak some information about $\text{seed}$ as the number of rejection in the calls to $\text{randtrits}()$ will depend of $\text{seed}$. To avoid leakage of possibly meaningful secret information we will favor conversions which are oblivious to their inputs and outputs.

B.2.1. Oblivious Conversion. The conversion algorithm can be made oblivious to the $\text{prng}$ output by removing the rejection as shown in Algorithm 13.

<table>
<thead>
<tr>
<th>Algorithm 12</th>
<th>Pseudorandom Sampling of Ternary Vectors</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>function</strong></td>
<td>$\text{prng}_3(n, \text{seed})$</td>
</tr>
<tr>
<td>$\text{prng} \leftarrow \text{prng_init}(\text{seed})$</td>
<td></td>
</tr>
<tr>
<td>$i \leftarrow 0$</td>
<td></td>
</tr>
<tr>
<td><strong>repeat</strong></td>
<td></td>
</tr>
<tr>
<td>$x_i, \ldots, x_{i+b-1} \leftarrow \text{randtrits}(a, b, \text{prng})$</td>
<td></td>
</tr>
<tr>
<td>$i \leftarrow i + b$</td>
<td></td>
</tr>
<tr>
<td><strong>until</strong> $i \geq n$</td>
<td></td>
</tr>
<tr>
<td><strong>return</strong> $x_0, \ldots, x_{n-1}$</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Algorithm 13</th>
<th>Binary to Ternary Conversion Without Rejection</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>With modulo</strong></td>
<td></td>
</tr>
<tr>
<td><strong>function</strong> $\text{randtrits}(a, b, \text{prng})$</td>
<td></td>
</tr>
<tr>
<td>$y \leftarrow \text{randbits}(a, \text{prng})$</td>
<td></td>
</tr>
<tr>
<td><strong>for</strong> $i = 0, \ldots, b - 1$ <strong>do</strong></td>
<td></td>
</tr>
<tr>
<td>$x_i \leftarrow y \mod 3$</td>
<td></td>
</tr>
<tr>
<td>$y \leftarrow \lfloor y/3 \rfloor$</td>
<td></td>
</tr>
<tr>
<td><strong>return</strong> $x_0, \ldots, x_{b-1}$</td>
<td></td>
</tr>
</tbody>
</table>

| **Without modulo** |
| **function** $\text{randtrits}(a, b, \text{prng})$ |
| $y \leftarrow \text{randbits}(a, \text{prng})$ |
| **for** $i = 0, \ldots, b - 1$ **do** |
| $x_i \leftarrow 3 \cdot (y \mod 2^a)$ |
| $y \leftarrow \lfloor y/2^a \rfloor$ |
| **return** $x_0, \ldots, x_{b-1}$ |
**Limitation.** With this modification, no information will leak, however the output won’t be uniformly distributed. The variant without modulo has the same distribution overall and avoids the division by 3, see [Lem19]. In both case, the entropy is

\[
H_{a,b} = - \frac{r(q+1)}{2^a} \log_2 q + \frac{1}{2^a} - \frac{3^b - r}{2^a} \log_2 q = b \cdot (\log_2 3 - \delta_{a,b})
\]

where \( q \) and \( r \) denote the quotient and the remainder of the Euclidean division of \( 2^a \) by \( 3^b, 2^a = q3^b + r \). The quantity \( \delta_{a,b} \) measures the loss of entropy per trit, for instance \( \delta_{64,32} = 8.5 \times 10^{-12} \).

### B.2.2. Bitsliced Conversion

Whenever required, the reference implementation will use Algorithm 14 to draw random bits with the appropriate method and convert them to ternary. The function `randtrits()` generates 128 random bits, two 64-bit words, and interleaves two calls to `convert()`, each consuming 64 bits with the property stated in Proposition 5, to return a bitsliced ternary vector of length 64, as defined in §B.1.

#### Algorithm 14 Bitsliced Ternary Conversion \((a = 64, b = 32)\)

1: `function randtrits(prng)`
2: \( x \leftarrow \text{randbits}(a, \text{prng}) \)
3: \( r \leftarrow \text{convert}(x) \)
4: \( x' \leftarrow \text{randbits}(a, \text{prng}) \)
5: \( r' \leftarrow \text{convert}(x') \)
6: \( y_h \leftarrow ((r \& Hi) \gg 1) \oplus (r' \& Hi) \)
7: \( y_l \leftarrow (r \& Lo) \oplus ((r' \& Lo) \ll 1) \oplus y_h \)
8: `return y`

1: `function convert(x)`
2: \( r \leftarrow 0 \)
3: for \( i = 0, \ldots, 7 \) do
4: \( (x, v_i) \leftarrow \text{mul}_{64}(x, 81) \)
5: \( r \leftarrow v_i \oplus (r \ll 8) \)
6: \( y \leftarrow (((r + Y_4) \& (r+2Y_4) \& E_6) \oplus ((r+2Y_4) \& E_7)) \)
7: \( r \leftarrow r + (y \gg 6) \times 37 \)
8: \( y \leftarrow (((r+Y_3) \& (r+2Y_3) \& E_4) \oplus ((r+2Y_3) \& E_5)) \)
9: \( r \leftarrow r + (y \gg 4) \times 7 \)
10: \( y \leftarrow (((r+Y_2) \& (r+2Y_2) \& E_2) \oplus ((r+2Y_2) \& E_3)) \)
11: \( r \leftarrow r + (y \gg 2) \)
12: `return r`

#### Constants (hexadecimal):

- \( Lo = 0x5555555555555555 \)
- \( Hi = 0xAAAAAAAAAAAAAAAA \)
- \( E_2 = 0x0404040404040404 \)
- \( E_3 = 0x0808080808080808 \)
- \( E_4 = 0x1010101010101010 \)
- \( E_5 = 0x2020202020202020 \)
- \( E_6 = 0x4040404040404040 \)
- \( E_7 = 0x8080808080808080 \)
- \( Y_2 = 0x0101010101010101 \)
- \( Y_3 = 0x0707070707070707 \)
- \( Y_4 = 0x2525252525252525 \)

For \( 0 \leq x, y, u, v < 2^{64} \)

\[
(u, v) \leftarrow \text{mul}_{64}(x, y) \quad \text{if } u + 2^{64}v = xy
\]

#### Proposition 5

On input \( x = \sum_{i=0}^{63} x_i 2^i \), a 64-bit integer, the function `convert()` of Algorithm 14 returns a 64-bit integer \( r = \sum_{i=0}^{31} u_i 4^i \) such that \( x/2^{64} = \sum_{i=0}^{31} u_i/3^{i+1} \) with \( u_i \in \{0, 1, 2\} \). If \( x \) is uniformly distributed in \( \{0, 1\}^{64} \) then the random variable \((u_i)_{0 \leq i < 32}\) which takes its value in \( \{0, 1, 2\}^{32} \) has an entropy

\[
H = 32 (\log_2 3 - \delta) \text{ with } \delta \approx 8.5 \times 10^{-12}
\]

Note that the uniform distribution over \( \{0, 1, 2\}^{32} \) has entropy \( 32 \log_2 3 \).

### B.3. Sampling Permutations and Permuting by Sorting

We give in this section specifications (as implemented in the reference implementation) to sample permutations in constant time. Recall that key generation and signing in Wave involve many permutation
samples, sometimes uniform as in Algorithm 4 or sometimes with some constraint as in Algorithms 6 and 7.

In this section, $\mathbb{F}$ is defined as any finite arbitrary alphabet. In practice $\mathbb{F}$ is chosen as $\mathbb{F}_\ell^k$ for some small $\ell$, typically it is equal to one or two.

We propose to sample permutations by sorting. Notice that it delegates all security related implementation issues to the sorting algorithm. In particular, sorting networks allows the sorting of an array with complexity $O(n(\log n)^2)$ which is oblivious to the data being sorted. Efficient cryptography oriented implementations are available, see djbsort [Ber] for instance. Another option is merge sort, as in [WSN18] for instance.

Algorithm 15 RandPerm – Permutation Sampling by Sorting

```
1: function RandPerm(n, z) ▷ z ∈ $\mathbb{F}^n$
2:   repeat
3:     for $i = 0, \ldots, n-1$ do
4:         $r_i \leftarrow [0, 2^B)$ ▷ B an integer, external parameter
5:         $x \leftarrow \text{sort}((r_i, i, z_i)_{0 \leq i < n})$ ▷ sort according to $r_i$
6:     until $(r_{j-1} \neq r_j, 0 < j < n)$
7:   for $i = 0, \ldots, n-1$ do
8:     $(\ast, \sigma(i), y_i) \leftarrow x_i$
9: return $(\sigma, y)$ ▷ $\sigma \in S_n$, $y = z^\sigma$
```

B.3.1. Sampling Permutations for Algorithm 4 (Key Generation). Algorithm 15 produces a uniform permutation. The sample is rejected if some $r_i$ for $i \in [0, n)$ collide. The rejection probability is upper bounded by a constant smaller than $1/2$ if $B \geq 2 \log_2 n$. If the sampler admits a vector as additional input, it returns the vector permuted according to the sampled permutation.

B.3.2. Sampling Permutations for Algorithm 6 (Decode). The call $\text{RandPerm}_V(n, k, t)$ will return a permutation $\pi$ of $[0, n)$ such that ($t \leq k$)

(i) $\pi([0, k))$ is uniformly selected in $[0, n)$,

(ii) $\pi([0, t))$ is uniformly selected in $\pi([0, k))$.

If a vector $z \in \mathbb{F}^n$ is provided as input, the permuted vector $y = z^\pi$ is returned in addition to $\pi$.

Connection with Decode. Using notation of Algorithm 6, Instructions 4 and 5 will be replaced by

$$(\pi, y) \leftarrow \text{RandPerm}_V(n/2, k_V - g, t, y_V).$$

The returned permutation does not need to be uniformly distributed, but simply, as specified above, namely $\pi([0, k_V - g))$ and $\pi([0, t))$ are uniformly distributed in $[0, n)$. These conditions are ensured by Instruction 6 of Algorithm 16. Also, no information must leak about $t$, $y_V$, or the permutation $\pi$. 

Algorithm 16 RandPerm$_V$

1: function RandPerm$_V$(n, k, t, z) \[\triangleright k < n, t \leq k; z \in \mathbb{F}^n\]
2: repeat
3: for $i = 0, \ldots, n - 1$ do
4: \[r_i \leftarrow \{0, 2^B\} \quad \triangleright B \text{ an integer, external parameter}\]
5: \[x \leftarrow \text{sort} ((r_i, i, z_i)_{0 \leq i < n}) \quad \triangleright \text{sort according to } r_i\]
6: until $r_{k-1} \neq r_k$ and $r_{t-1} \neq r_t$
7: for $i = 0, \ldots, n - 1$ do
8: \[(*, \pi(i), y_i) \leftarrow x_i\]
9: return $(\pi, y)$

If the sorting algorithm is oblivious to the data it processes, then this is also the case for Algorithm 16 with the exception of the test $r_{t-1} \neq r_t$ at Instruction 6 which must be implemented without revealing information about $t$.

B.3.3. Sampling Permutations for Algorithm 7 (Decode$_V$). The call RandPerm$_V$(n, k, ℓ, J) will return a permutation $\pi$ of $[0, n)$ such that

(i) $\pi([0, k - \ell))$ is uniformly selected in $[0, n) \setminus J$,

(ii) $\pi([k - \ell, k))$ is uniformly selected in $J$.

If a vector $z \in \mathbb{F}^n$ is provided, the permuted vector $y = z^\pi$ is returned in addition to $\pi$. The algorithm will proceed in two steps

1. Permute $[0, n)$ randomly with the positions of $J$ coming last,

2. Swap the last $\ell$ entries of the following blocks, the first one is given by coordinates $[0, k)$ and the second one by $[k, n)$, to ensure $\ell$ elements of $J$ in the first $k$ entries.

Instruction 6 will make a check after Step (1) to ensure that the first $k - \ell$ entries of the permutation are uniformly distributed in $[0, n) \setminus J$ (true if and only if $r_{k-\ell-1} \neq r_{k-\ell}$ and the last $\ell$ entries of the permutation are uniformly distributed in $J$ (true if and only if $r_{n-\ell-1} \neq r_{n-\ell}$).

**Connection with Decode$_V$**. Using notation of Algorithm 7, Instructions 5, 6, 7 and 10 will be replaced by

$$(\pi, x) \leftarrow \text{RandPerm}_V(n/2, n/2 - k_V + g, \ell, \text{Supp}(e_V), x)$$

where $x_i = (y_V(i), (c_i - b_i)e_V(i), e_V(i)^2)$, $i \in [0, n/2)$. It is required that the first $n/2 - k_V + g$ entries of $\pi$ consist of $\ell$ positions uniformly chosen in $\text{Supp}(e_V)$ and $n/2 - k_V + g - \ell$ positions uniformly chosen in $[0, n) \setminus \text{Supp}(e_V)$. Algorithm 17 complies to those constraints. Also, no information must leak about $\ell, J, x$, or the permutation $\pi$.

If the sorting algorithm is oblivious to the data it processes, then this is also the case for Algorithm 17 with the exception of the tests $r_{k-\ell-1} \neq r_{k-\ell}$ and $r_{n-\ell-1} \neq r_{n-\ell}$ at Instruction 6 which must be implemented without revealing information about $\ell$. 

32
Algorithm 17 RandPerm<sub>U</sub>

Input: : integers \( n, k < n, \ell, J \subseteq [0, n], z \in \mathbb{F}^n \)  \( \triangleright \) assume \( \#J \leq n-k \)
Output: : \((\pi(i))_{0 \leq i < n}, y = z^\pi \) with \( \pi \in \mathcal{S}_n \) such that \( \# \pi([0,k)) \cap J = \ell \)
1: \textbf{repeat}
2: \hspace{1em} \textbf{for} \( i = 0, \ldots, n-1 \) \textbf{do}
3: \hspace{2em} \( r_i \leftarrow \frac{s}{2} \cdot 2^B \) \( \triangleright B \) an integer, external parameter
4: \hspace{2em} \( r_i \leftarrow r_i + (i \in J) \cdot 2^B : 0 \) \( \triangleright \) coordinates in \( J \) will be last after sorting
5: \hspace{2em} \( x \leftarrow \text{sort}((r_i, i, z_i)_{0 \leq i < n}) \) \( \triangleright \) sort according to \( r_i \) in increasing order
6: \hspace{2em} \textbf{until} \( r_{k-\ell-1} \neq r_{k-\ell} \) and \( r_{n-\ell-1} \neq r_{n-\ell} \)
7: \hspace{2em} \textbf{for} \( i = 0, \ldots, k-1 \) \textbf{do} \( \triangleright \) fix size loop for constant time
8: \hspace{3em} \( (x_{k-1-i}, x_{n-1-i}) \leftarrow (i < \ell) \cdot (x_{n-1-i}, x_{k-1-i}) : (x_{k-1-i}, x_{n-1-i}); \) \( \triangleright \) swap if \( i < \ell \)
9: \hspace{2em} \textbf{for} \( i = 0, \ldots, n-1 \) \textbf{do}
10: \hspace{3em} \( (\ast, \pi(i), y_i) \leftarrow x_i \)
11: \textbf{return} \((\pi, y)\)

B.3.4. Permuting Vectors. It is also possible to permute a vector according to a permutation by sorting. If the input permutation \( \pi \) is given as a sequence of integers \((\pi(i))_{0 \leq i < n}\), sorting this sequence will apply the inverse permutation. Interestingly, applying the inverse of a given permutation is what is needed most of the time in Wave. As an additional (almost free) feature, Algorithm 18 may return the inverse permutation as a sequence of integers.

Algorithm 18 VectInvPerm – Apply (the Inverse of) a Permutation to a Vector

1: \textbf{function} VectInvPerm\((z, \pi)\) \( \triangleright z \in \mathbb{F}^n, \pi \in \mathcal{S}_n \)
2: \hspace{1em} \( x \leftarrow \text{sort}((\pi(i), i, z_i)_{0 \leq i < n}) \) \( \triangleright \) sort according to first coordinate in increasing order
3: \hspace{1em} \textbf{for} \( i = 0, \ldots, n-1 \) \textbf{do}
4: \hspace{2em} \( (\ast, \sigma(i), y_i) \leftarrow x_i \)
5: \hspace{1em} \textbf{return} \( y, \sigma \) \( \triangleright y = z^{\pi^{-1}} \) \( \sigma = \pi^{-1} \)

B.3.5. Permuting the Columns of a Matrix. As for the coordinates of a vector, permuting the columns of a matrix can be achieved in constant time with an oblivious sorting algorithm. The principle of Algorithm 18 can be applied, but with an alphabet \( \mathbb{F} \) large enough to accommodate the columns of a matrix. The reference implementation uses an ad hoc procedure deriving from \texttt{djbsort} [Ber] to produce a sorting network and uses it to conditionally swap the columns of a matrix.

B.4. Master Key to Generate the Secret Matrices. As the key generation (Algorithm 4) is described, the secret matrices \( H_U \) and \( G_V \) are needed only once per signature in Algorithm 5, when a Gaussian elimination is performed. Columns are permuted just before the elimination. Suppose that a master key \( mk \) is used for generating matrices \( H_U \) and \( G_V \), its \( i \)-th column is equal to \( f_{mk}(X, i) \), \( X \in \{H_U, G_V\} \) where \( f_{mk}() \) is some, appropriately keyed (here \( mk \)), one-way function. The \( i \)-th column of \( X^\pi \) is equal to \( f_{mk}(X, \pi(i)) \) and the matrix \( X^\pi \) can be generated without leaking information about \( \pi \) assuming that the execution of \( f_{mk}(X, i) \) leaks no information on \( i \). For instance assuming we want to generate \( G_V \) and \( H_U \) at run time (using \texttt{prng}_3() as in Algorithm 12):
• the $i$-th column of $G_V$ is the output of $\text{prng}_3(k_V, \text{mk} \parallel 0 \parallel i)$

• the $i$-th column of $H_U$ is the output of $\text{prng}_3(n/2 - k_V, \text{mk} \parallel 1 \parallel i)$

where $\parallel$ denotes the concatenation. Concatenating a ‘0’ or a ‘1’ separates the pseudorandom generator domains for cases ‘$V$’ and ‘$U$’.

B.5. Gaussian Elimination and its Variants in Constant Time. It is assumed that the reader is familiar with the basic concepts. The Gaussian elimination on an $r \times n$ full rank matrix $A$ will produce another matrix $A'$ spanning the same vector space and which contains an $r \times r$ identity sub-matrix, indexed by some set $J$. The pivot positions are the elements of $J$, ordered from top to bottom. The pivots are selected in order one at a time. A failing pivot is a column (position) that is dependent of the previously selected pivot columns and that could not be included in the identity block. Note that for a given information set $J$ the transformed matrix is essentially unique. Changing the order of the pivots in $J$ will simply change the row order accordingly in the resulting matrix. Recall that, $M_i$ denotes the $i$-th row of the matrix $M$.

B.5.1. Systematic Gaussian Elimination. In the key generation routine, Algorithm 4, the purpose is to reach a (strict) systematic form for an input matrix of size $r \times n$ (assuming it has full rank $r$), that is a matrix $A_{\text{syst}} = (\text{Id}_r \mid R)$ where $\text{Id}_r$ is the $r \times r$ identity matrix and such that $A$ and $A_{\text{syst}}$ span the same row vector space. This systematic form exists if and only if the leftmost $r \times r$ block of $A$ is non-singular. Else a few columns of $A$ may have to be permuted to reach the desired form.

In the current context the columns of a matrix $A$ are permuted with $\sigma \in \mathcal{S}_n$ before the Gaussian elimination and the call in Instruction 9 of Algorithm 4 is

$$(A_{\text{syst}} = (\text{Id}_r \mid R), \pi) \leftarrow \text{SystGaussElim}(A, \sigma)$$

where $A^\sigma$ and $A_{\text{syst}}$ span the same row-space and $\pi \in \mathcal{S}_n$ is “close” to $\sigma$; the Gaussian elimination uses the columns of $A^\sigma$ as pivots from left to right and “push” the failing pivot positions right, yielding

$$\forall i \in [0, r), \; \pi(i) = \sigma(\ell) \text{ where } \ell = \min \{ j \in [0, n) \mid \text{rank} (A^\sigma_{[0,j]}) = i \}$$

and

$$\forall i \in [0, r)n, \; \pi(i) = \sigma(\ell) \text{ where } \ell = \min \{ [0, n) \setminus \{ \sigma^{-1} \circ \pi(j), j \in [0, i) \} \}.$$ 

Key security. If $(A, \pi)$ is private and $A_{\text{syst}}$ is public and obtained as above, it should be noted that $\pi$ is not uniformly distributed in $\mathcal{S}_n$. However, no security penalty incurs as $A_{\text{syst}}$ would be the result of the Gaussian elimination on $SA^\sigma$ for any non-singular $r \times r$ matrix $S$. Revealing $SA^\sigma$ for random uniform $\sigma$ and $S$ is innocuous (within the security assumptions) and publishing $A_{\text{syst}}$ rather than $SH^\sigma$ provides an information that anyone could have computed easily from public data.

Implementation security. Still the implementation of the Gaussian elimination could give rise to timing or cache attacks. For instance, if $A = H$ as in Instruction 7 of Algorithm 4, the special form and content of $H$ could induce secret dependent timing variations, typically because some columns of $d \star H_U$ or $b \star H_U$ can be null depending on secret information. This could be easily avoided by multiplying $H$ on the left by a random non-singular matrix $S$ before the Gaussian elimination, or, probably less expensive, by a careful implementation of the Gaussian elimination, making sure that the timing and memory.
access pattern of each pivot elimination is independent of the coordinates of this particular column. Note that timing or memory access variations due to pivot failures do not need to be masked as they would also happen if the Gaussian elimination was applied to $SH^\tau$, and this latter matrix could be safely revealed.

**Basic Gaussian elimination in constant time.** Algorithm 19 uses the constant time routine $\text{Reduce}_j()$ defined in §B.5.2. This algorithm will be used in a context (Instruction 9 in Algorithm 4) where it can be not oblivious to pivot failure, but oblivious to everything else: an adversary can only learn which column indices led to a failing pivot. Indeed, this algorithm will be used to output the public key, when revealing pivot failures it only reveals positions where a Gaussian elimination may fail on the public matrix.

**Algorithm 19** Systematic Gaussian Elimination in constant time

1: function $\text{CTSystGaussElim}(M, \pi)$ \hspace{1cm} $\triangleright$ $M \in \mathbb{F}_3^{k \times n}$
2: $j \leftarrow 0$
3: $\ell \leftarrow n - 1$
4: while $j < k$ and $j < \ell$ do
5:     for $i = j + 1, \ldots, k - 1$ do
6:         $M_j, M_i \leftarrow \text{Reduce}_j(M_j, M_i)$ \hspace{1cm} $\triangleright$ defined in §B.5.2
7:     if $M_{jj} \neq 0$ then
8:         $M_j \leftarrow M_{jj}^{-1} M_j$
9:     for $i = 0, \ldots, j - 1$ do
10:        $M_i \leftarrow M_i - M_{ij} M_j$
11:     $j \leftarrow j + 1$
12: else
13:     $M \leftarrow \text{SwapColumns}(M, j, \ell)$
14:     $\ell \leftarrow \ell - 1$
15:     $\pi \leftarrow \pi \circ (j \ell)$ \hspace{1cm} $\triangleright \pi(j), \pi(\ell) \leftarrow \pi(\ell), \pi(j)$
16: return $(M, \pi)$

**Gaussian elimination with abort in constant time.** Algorithm 20 is a variant of Algorithm 19 but with abort. Algorithm 20 will be used in a context, the generation of $H_V$ in Instruction 2 of Algorithm 4, where rejection is not allowed unless to weaken the security reduction. Basically, $H_V$ is computed by performing a Gaussian elimination of $G_V$ and revealing the failing pivot indices may reveal information on the particular permutation drawn for a secret matrix generation. It is why the algorithm always compute pivots with Instructions 5 and 6 (defined in §B.5.2). The computation of these pivots may fail. It is why the algorithm also outputs some integer $p$. Checking that $p$ is equal to $k$ or not enables to verify the success or not of the Gaussian elimination.

**Partial Gaussian elimination in constant time.** The constant time partial Gaussian elimination on $M \in \mathbb{F}_3^{k \times n}$ will stop the process $g$ steps before the end, that is after $k - g$ pivots in constant time (Instructions 5 and 6). In the current context Algorithm 21 will be called with a value of $g$ such the first $k - g$ pivots may fail (with a probability $\approx 1/2^{64}$) but the algorithm will stop in any case after $k - g$ iterations. The algorithm also outputs an integer $p$ which gives the number of successful pivots. Checking that $p$ is equal or not to $k - g$ enables to verify the success or not of the partial Gaussian elimination.
Algorithm 20 Gaussian Elimination “with Abort” in constant time

1: function CTGE\(_{\text{abort}}\)(M) \(\triangleright M \in \mathbb{F}_3^{k \times n}\)
2: \(p \leftarrow 0\)
3: for \(\ell = 0, \ldots, k - 1\) do
4: \(\text{for } i = \ell + 1, \ldots, k - 1\) do
5: \(M_\ell, M_i \leftarrow \text{Reduce}_\ell(M_\ell, M_i)\) \(\triangleright \text{defined in } \S B.5.2\)
6: \(M_\ell \leftarrow \text{Normalize}_\ell(M_\ell)\)
7: \(p \leftarrow p + M_\ell,\ell\) \(\triangleright \text{Addition in } \mathbb{Z}\)
8: for \(i = 0, \ldots, \ell - 1\) do
9: \(M_i \leftarrow M_i - M_i,\ell \cdot M_\ell\)
10: return \((M, p)\)

Algorithm 21 Partial Gaussian Elimination in constant time

1: function CTPartialGaussElim(M, g) \(\triangleright M \in \mathbb{F}_3^{k \times n}\)
2: \(p \leftarrow 0\)
3: for \(\ell = 0, \ldots, k - g - 1\) do
4: \(\text{for } i = \ell + 1, \ldots, k - 1\) do
5: \(M_\ell, M_i \leftarrow \text{Reduce}_\ell(M_\ell, M_i)\) \(\triangleright \text{defined in } \S B.5.2\)
6: \(M_\ell \leftarrow \text{Normalize}_\ell(M_\ell)\)
7: \(p \leftarrow p + M_\ell,\ell\) \(\triangleright \text{Addition in } \mathbb{Z}\)
8: for \(i = 0, \ldots, \ell - 1\) do
9: \(M_i \leftarrow M_i - M_i,\ell \cdot M_\ell\)
10: return \((M, p)\)

Application to Algorithm 6 (CTDecode\(_V\)). As Decode\(_V\) was specified in Algorithm 6, the matrix \(G_V\) is permuted, then a \(g\)-partial systematic form is computed. For a constant time implementation failure and rejection is not allowed. To this end, Instruction 6 will be replaced by

\[(G, p) \leftarrow \text{CTPartialGaussElim}(G^\pi_V, g)\]

which tries to compute the permuted matrix \(G^\pi_V\), possibly using a master key \(mk\), in a \(g\)-partial systematic form. Checking that \(p\) is equal to \(k_V - g\) will enable to test if the algorithm has been successful. It will lead to a constant time specification of Decode\(_V\) as CTDecode\(_V\) in Algorithm 27.

B.5.2. Extended Gaussian Elimination in Constant Time. The Gaussian elimination algorithms in constant time proposed above are not sufficient for the signing algorithm, in particular Algorithm 7 which needs to compute the \(g\)-extended systematic form (see Definition 2) of some matrix. In this context, rejection is also not allowed without weakening the security reduction, and revealing the failing pivot indices may reveal information on the particular permutation drawn for a particular signature generation. We must produce an algorithm which is completely oblivious to its input. This is achieved by adding zero rows at the bottom of the matrix (according to Lemma 2 in Appendix §D, a matrix \(A \in \mathbb{F}_3^{(r+g) \times n}\) in extended systematic form has exactly \(g\) zero rows) and then performing a Gaussian elimination oblivious to the failing pivots.
Algorithm 22, on input \((A', g)\) with \(A' \in \mathbb{F}_3^{r \times n}\), tries to compute an extended systematic form of \(A'\) by first adding \(g\) extra (zero) rows to form a matrix \(A \in \mathbb{F}_3^{(r+d) \times n}\). It succeeds if and only if the first \(r + g\) columns of \(A\) have the same rank as \(A'\). If it fails, the output \(A\) will be such that \(\langle A' \rangle = \langle A \rangle\) but it won’t be in extended systematic form; the weight of the main diagonal will be equal to \(\text{rank}(A'_{[0, r+g]}) < r\).

**Algorithm 22** Extended Gaussian Elimination in constant time

1: function CTExtGaussElim\((A', g)\) \(\triangleright A' \in \mathbb{F}_3^{r \times n}, g \leq n - r\)
2: \(A \leftarrow \text{stack}(A', 0^{g \times n})\) \(\triangleright A = \begin{bmatrix} A' \\ 0 \end{bmatrix} \) \(r\) rows
3: \(p \leftarrow 0\)
4: for \(\ell = 0, \ldots, r + g - 1\) do
5: for \(i = \ell + 1, \ldots, r + g - 1\) do
6: \(A_{\ell}, A_i \leftarrow \text{Reduce}_\ell(A_{\ell}, A_i)\)
7: \(A_{\ell} \leftarrow \text{Normalize}_\ell(A_{\ell})\)
8: \(p ' p + A_{\ell, '}\) \(\triangleright\) Addition in \(\mathbb{Z}\)
9: for \(i = 0, \ldots, \ell - 1\) do
10: \(A_i \leftarrow A_i - A_{i, '} \cdot A_{\ell}\)
11: return \((A, p)\) \(\triangleright A \in \mathbb{F}_3^{(r+g) \times n}\)

The functions \(\text{Normalize}_\ell\) and \(\text{Reduce}_\ell\) are defined as

\[
\text{Normalize}_\ell(x) := \begin{cases} x & \text{if } x_\ell = 0 \\ x^{-1}_\ell \cdot x & \text{if } x_\ell \neq 0 \end{cases}
\]

\[
\text{Reduce}_\ell(x, y) := \begin{cases} (y, x) & \text{if } x_\ell = 0 \\ (x, y - (y_\ell x^{-1}_\ell) \cdot x) & \text{if } x_\ell \neq 0 \end{cases}
\]

Both functions enjoy simple secure implementations, for instance, using properties of \(\mathbb{F}_3\):

\[
\text{Normalize}_\ell(x) = (1 + x_\ell - x_\ell^2) \cdot x
\]

\[
\text{Reduce}_\ell(x, y) = (x_\ell^2 \cdot x + (1 - x_\ell^2) \cdot y, (1 - x_\ell^2 - x_\ell y_\ell) \cdot x + x_\ell^2 \cdot y)
\]

and thus the whole procedure can be securely implemented.

**Proposition 6.** If \(A' \in \mathbb{F}_3^{r \times n}\) is such that \(r = \text{rank}(A') = \text{rank}(A'_{[0, r+g]})\), then the output \(A\) of Algorithm 22 on input \((A', g)\) is an extended systematic form of \(A'\).

**Proof.**

(1) Let us first remark that if \((x', y') = \text{Reduce}_\ell(x, y)\) then \((x', y')\) spans the same space as \((x, y)\) and \(y'_\ell = 0\). The matrix \(A\) is modified in place. Initially it spans the same vector space as \(A'\), and this property remains true during all the computation, as Instruction 6, 7, and 10 will not change the spanned space. So we have \(\langle A \rangle = \langle A' \rangle\) at all times. It remains to prove that \(A\) is in extended systematic form.
(2) Let us prove by induction on $\ell$ that at the beginning of the $\ell$-th iteration the matrix $A$ has the following form

\[ A = \begin{array}{c|c}
\ell \\
\hline
B & C \\
& 0 \\
\hline
\ell & 0 \\
\end{array} \quad g - j \tag{18} \]

with $B \in F_3^{\ell \times n}$ in extended systematic form and $j = \ell - \text{rank}(B)$. It is true for $\ell = 0$, with $C = A'$ and $B$ has vanished. During the $\ell$-th iteration, the algorithm will explore the $\ell$-th column of $A$ below $B$ (in grey above).

- First case: the leftmost column of $C$ has a non-zero coefficient. Instructions 4, 5 and 6 will transform $C$ into a matrix of same size, spanning the same space, of the following form:

\[ C' = \begin{array}{c|c|c}
\ell + 1 \\
\hline
\ell + 1 & 0 \\
\hline
\ell + 1 & 0 \\
\end{array} \]

The remainder of $A$ is unchanged by Instructions 5, 6 and 7. Instructions 8 and 9 will eliminate the $\ell$-th column of $B$ by removing a multiple of $A_\ell$, the $\ell$-th row of $A$ (also the top row of $C$) is added at the bottom of $B$ leading, after elimination to a matrix $B' \in F_3^{(\ell+1) \times n}$ of the form

\[ B' = \begin{array}{c|c}
\ell + 1 \\
\hline
\ell + 1 & 0 \\
\hline
\ell + 1 & 0 \\
\end{array} \]

If $B$ is in extended systematic form, so is $B'$. Finally, at the end of the $\ell$-th iteration, the matrix $A$ becomes

\[ A = \begin{array}{c|c|c}
\ell + 1 \\
\hline
\ell + 1 & B' & C' \\
\hline
\ell + 1 & 0 & 0 \\
\hline
\ell + 1 & 0 & g - j \\
\end{array} \quad \text{after the $\ell$-th iteration with successful pivot} \]

which is compliant with the induction condition at the start of the $(\ell + 1)$-th iteration.

- Second case: the leftmost column of $C$ is null. The following lemma is needed.

**Lemma 1.** In (18), if the first column of $C$ is null then $g - j > 0$.  

38
Proof. The first $r + g$ column of $B$ have rank $\ell - j = \text{rank}(B)$. To comply with the rank condition of the statement, the first $r + g$ columns of $A$ must have rank $r = \text{rank}(A)$, thus the first $r + g - \ell$ columns of $C$ must have rank $r - \text{rank}(B) = r + j - \ell = \text{rank}(C)$, and in particular $r + j - \ell \geq r + g - \ell$, that is $g \geq j$. If $g = j$ then the first $r + g - \ell$ columns of $C$ would have rank $r + g - \ell$. This cannot happen if the first column of $C$ is null, hence $g > j$. □

Instructions 5, 6 and 7 will move $C$ down by one row and, because $g - j > 0$, insert one of the $g - j$ all-zero bottom rows as the new $\ell$-th row

\[
A = \begin{bmatrix}
\ell \\
B \\
0 \\
\vdots \\
0 \\
d - j - 1
\end{bmatrix}
\]

With $A_\ell$ null now, Instructions 8 and 9 do nothing and at the end of the $\ell$-th iteration the matrix $A$ becomes

\[
\begin{bmatrix}
\ell + 1 \\
0 \\
B' \\
0 \\
C' \\
g - j - 1
\end{bmatrix}
\]

after the $\ell$-th iteration with failing pivot

Since $B'$ is obtained by adding an all-zero row at the bottom of $B$, it remains in extended systematic form. The rank default of $B'$ is increased by one and becomes $j + 1 = \ell + 1 - \text{rank}(B')$.

When $\ell = r - g$, everything vanishes except $B$ in (18), and thus $A$ is in extended systematic form. □

**Application to Algorithm 7** (CTDecode$_U$). As Decode$_U$ was specified in Algorithm 7, the matrix $H_U$ is permuted, then a $g$-extended systematic form is computed. For a constant time implementation failure and rejection is not allowed. To this end, Instruction 13 will be replaced by

\[
(H, p) \leftarrow \text{CTExtGaussElim}(H_U^T, g)
\]

which tries to compute the permuted matrix $H_U^T$, possibly using a master key $mk$, in a $g$-extended systematic form. Checking that $p$ is equal to $n/2 - k_U$ will enable to test if the algorithm has been successful. It will lead to a constant time specification of Decode$_U$ as CTDecode$_U$ in Algorithm 28.

**B.6. Wave Key Generation and Signing in Constant Time.** Algorithms 23 and 26 are a specification of Wave Key Generation and Signing in constant time. Contrary to the
specifications of the main part of the document, it is specified how to produce matrices $G$ and $H$ thanks to a master key (see §B.4), how to sample permutations (see §B.3), how to perform Gaussian elimination and its variants (see §B.5) as well as sampling random elements in their domain (see §B.2). Let us stress that all algorithms are implementation choices, there are a particular instantiation of algorithms presented in the main part of the document and they were specified to reach a constant time implementation.

**Algorithm 23** Key Generation in constant time

Output: \[
\begin{align*}
\text{pk} &= M \in \mathbb{F}_3^{k \times (n-k)} \\
\text{sk} &= (mk, b, c, \pi) \in \mathbb{F}_3^\lambda \times \mathbb{F}_3^{n/2} \times \mathbb{F}_2^{n/2} \times \mathcal{S}_n
\end{align*}
\]

1. repeat
2. \[mk \leftarrow \{0, 1\}^\lambda \quad \triangleright \pi_{id} \text{ the identity permutation}
3. \(G \leftarrow \text{RandMatPerm}(k_V, n/2, mk \parallel 0, \pi_{id}) \quad \triangleright \text{Algorithm 24}
4. \((G_V, p) \leftarrow \text{CTGE}_{\text{abort}}(G) \quad \triangleright \text{Algorithm 21}
5. \text{until } p = k_V
6. (\text{Id}_{k_V} \mid R_V) \leftarrow G_V
7. H_V \leftarrow (-R_V^T \mid \text{Id}_{n/2-k_V})
8. b \leftarrow \mathbb{F}_3^{n/2}
9. c \leftarrow (\mathbb{F}_3 \setminus \{0\})^{n/2}
10. d \leftarrow 1 + b \star c
11. \pi, x \leftarrow \text{RandPerm}(n, (d, -b)) \quad \triangleright \text{Algorithm 15, } x = (d, -b)^\pi
12. (M, \pi) \leftarrow \text{WavePublicKey}(mk, H_V, \pi, x, c) \quad \triangleright \text{Algorithm 25, } \pi \text{ may change}
13. return \(\text{pk} = R, \text{sk} = (mk, b, c, \pi))

**Algorithm 24** Pseudorandom (Permuted) Matrix

1. function RandMatPerm \((n, k, \text{seed}, \pi)\)
2. for \(i = 0, \ldots, n - 1\) do
3. \[x_i \leftarrow \text{prng}_3(k, \text{seed} \parallel \pi(i)) \quad \triangleright \text{Algorithm 12 (p. 29)}
4. return MatrixFromColumns\((x_0, \ldots, x_{n-1})\)
Appendix C. Key Representation and Compressing Signatures

C.1. Key Representation. To store public and private keys as byte arrays, we need to convert trits into bytes efficiently. We do this using a simple arithmetic encoding, packing five trits $v_0, \ldots, v_4$ in $\{0, 1, 2\}$ into the one-byte integer $v_0 + 3v_1 + 9v_2 + 27v_3 + 81v_4$. This approach uses 242 of the 256 values that one byte can take, giving a storage efficiency of $242/256 = 94.5\%$. We could achieve a higher efficiency by packing more trits together in larger words, at the cost of more computation (and the specification of a byte order). On balance, we decided that five-trits-per-byte provides a good trade-off between storage efficiency, computational cost, and specification complexity.

C.2. Compressing Signatures. As with keys, Wave signatures can be stored and transmitted using the five-trits-per-byte encoding above. This would result in a signature size of, e.g., $[4288/5] = 845$ bytes (plus 32 salt bytes) for Wave822 (at NIST security Level I).
But \textbf{Wave} signature vectors have high weight by definition, so their true entropy is lower than that of a random ternary vector. This makes signature compression a viable option. We considered several standard compression techniques, including arithmetic coding and combinadics, before settling on Huffman coding.
We use a static Huffman encoding to encode three trits at a time, with codewords based on the expected average weight of a signature. Therefore, no information about the encoding needs to be transmitted with a compressed signature: hard-coded encoding and decoding routines can be used (see `util/compress.c` in the reference implementation).

The lossless compression of the signature involves only public information, so has no impact on the security of the overall signature scheme. This encoding is purely a trade-off between computational effort and resulting signature length. Better compression may be achieved by tweaking the parameters of the compression routine, or by using a different compression algorithm. The theoretical upper limit of the signature size for any signature encoding is the length of a non-compressed signature, the lower limit is defined by the entropy of an individual signature.

C.3. Bounding signature lengths. The use of Huffman coding (and variations in Wave signature vector weights) results in a varying signature length. We limit the maximum signature size by defining `CRYPTO_BYTES` in such a way that at fewer than one in $2^{61}$ signatures are expected to exceed the maximum signature length. In this case, re-signing with a new salt gives a short compressed signature with high probability, without leaking any information on the private key.

To model perfect compression, we define the parameter $p = \frac{w}{n}$, where $w$ is the weight and $n$ is the length. This gives trit probabilities $P(0) = 1 - p$, $P(1) = \frac{p}{2}$, and $P(2) = \frac{p}{2}$, so the average encoding for a word of length $\frac{n}{2}$ and weight $t$ is

$$\left(\frac{n}{2} - t\right) \log_2 \left(\frac{1}{1-p}\right) + t \log_2 \left(\frac{2}{p}\right).$$

On the other hand, the probability that a signature vector has weight exactly $t$ is

$$P(\text{signature weight} = t) = \binom{n}{\frac{n}{2}} p^t (1-p)^{\frac{n}{2} - t}.$$

To define the maximum signature size for Wave822 (NIST Level I), we first computed the probability that a random Wave822 signature would compress perfectly to a given length. We then compressed many random Wave822 signature vectors to determine how close our Huffman compression is to a perfect compression, used this difference as an offset from the theoretical signature length with probability $2^{-61}$, and took the resulting signature length of 790 bytes (plus salt) as our maximum signature length for Wave822. We scaled the maximum length for the other security levels accordingly.

Table 9 lists some candidate bounds on signature lengths, together with the corresponding probabilities of rejection and re-signing.
Table 9. Probability of rejection and re-signing for various signature length bounds.

<table>
<thead>
<tr>
<th>Instance</th>
<th>Security</th>
<th>Signature length bound (B)</th>
<th>P(Re-signing)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Salt</td>
<td>Vector</td>
<td>Total</td>
</tr>
<tr>
<td>Wave822</td>
<td>Level I</td>
<td>32</td>
<td>741</td>
</tr>
<tr>
<td></td>
<td></td>
<td>32</td>
<td>790</td>
</tr>
<tr>
<td>Wave1249</td>
<td>Level III</td>
<td>64</td>
<td>1085</td>
</tr>
<tr>
<td></td>
<td></td>
<td>64</td>
<td>1185</td>
</tr>
<tr>
<td>Wave1644</td>
<td>Level V</td>
<td>64</td>
<td>1424</td>
</tr>
<tr>
<td></td>
<td></td>
<td>64</td>
<td>1580</td>
</tr>
</tbody>
</table>

Appendix D. Proof of Proposition 3

We use in this section notations of Algorithm 7.

Proposition 3. On input $(y_U, e_V, b, c, H_U)$, Algorithm 7 outputs $e_U$ satisfying

$$(y_U - e_U)H_U^\top = 0_{n/2-k_U} \quad (12)$$

Furthermore, if $e_L := e_U + b \ast e_V$ and $e_R := c \ast e_L + e_V$, then

$$|e_L| + |e_R| = w. \quad (13)$$

The proof of this proposition will rely on the following lemmas.

Lemma 2. Let $A_{\text{extSyst}} \in \mathbb{F}_3^{(r+g)\times n}$ be the output of Algorithm 3 given as input $A \in \mathbb{F}_3^{r\times n}$ with $r = \text{rank}(A) < n$. Let,

$$J = \{i \in [0, r+g), A_{\text{extSyst}}(i, i) \neq 0\}.$$ 

We have,

$$\#J = r$$

and

$$\forall s \in \mathbb{F}_3^{r+g}, \text{ Supp}(s) \subseteq J \implies (s, 0_{n-r-g})A_{\text{extSyst}}^\top = s.$$ 

Proof. First, $\langle A_{\text{extSyst}} \rangle = \langle A \rangle$ and $r = \text{rank}(A) < n$. We deduce that $\text{rank}(A_{\text{partSyst}})$ is equal to $r < r+g$. Therefore, as the matrix $\text{rank}(A_{\text{partSyst}})$ is in extended systematic form (see Definition 2), it has exactly $r$ non-zero rows, and $g$ zero rows. Furthermore, the set $J$ is an information set for $A_{\text{extSyst}}$. We deduce that it has cardinal $\text{rank}(A_{\text{partSyst}}) = r$ and as the columns of $A_{\text{extSyst}}$ restricted to it form an identity matrix we have

$$\forall s \in \mathbb{F}_3^{r+g}, \text{ Supp}(s) \subseteq J \implies (s, 0_{n-r-g})A_{\text{extSyst}}^\top = s$$

which concludes the proof. \qed

In what follows we use notation of Algorithm 7 (Decode$_U$).

Lemma 3. Let $e_L = e_U + b \ast e_V$ and $e_R = c \ast e_L + d \ast e_V$ where $c_a \neq 0$ for all $a$. We have,

$$\forall i \in \pi([n/2-k_U + g, n/2)), \ e_L(i)e_R(i) \neq 0.$$
Lemma 4. Let $e_L = e_U + b \ast e_V$ and $e_R = c \ast e_L + e_V$ where $c_a \neq 0$ for all $a$. In Instruction 22 and 23, $i$ and $j$ verify
\begin{align}
j &= \# \{ a \in [0,n/2) : e_L(a) = e_R(a) = 0 \} \quad \text{(19)}
\end{align}
and
\begin{align}
i &= \# \{ a \in [0,n/2) : e_L(a) \neq e_R(a) \text{ and } e_L(a)e_R(a) = 0 \} . \quad \text{(20)}
\end{align}

Proof. Let us first prove Equation (19). Let,
\begin{align}
m := \# \{ a \in [0,n/2) : e_L(a) = e_R(a) = 0 \} .
\end{align}
Our aim is to show that $m = j$. First, according to Lemma 3,
\begin{align}
m &= \# \{ a \in \pi ([0,n/2 - k_U + g)) : e_L(a) = e_R(a) = 0 \} . \quad \text{(21)}
\end{align}
We have for all $b \in [0,n/2 - k_U + g)$,
\begin{align}
e_L(\pi(b)) &= e_U(\pi(b)) + (b \ast e_V)(\pi(b)) \\
&= e(0)(b) + (b \ast e_V)(\pi(b)) \quad \text{(22)}
\end{align}
and
\begin{align}
e_R(\pi(b)) &= (c \ast e_L)(\pi(b)) + e_V(\pi(b)) \\
&= c(\pi(b))e(0)(b) + \left(1 + b(\pi(b))c(\pi(b)) \right)e_V(\pi(b)) . \quad \text{(23)}
\end{align}
Combining these two equations with Equation (21) and the fact that $c_a \neq 0$ for all $a$ shows
\begin{align}
m &= \# \{ b \in [0,n/2 - k_U + g) : e_V(\pi(b)) = 0 \text{ and } e(0)(b) = 0 \} .
\end{align}
Therefore,
\begin{align}
m &= \frac{n}{2} - k_U + g - \underbrace{\# \{ b \in [0,n/2 - k_U + g) : e_V(\pi(b)) \neq 0 \}}_{\ell = \text{see Instruction 5}} \\
&\quad - \underbrace{\# \{ b \in [0,n/2 - k_U + g) : e_V(\pi(b)) = 0 \text{ and } e(0)(b) \neq 0 \}}_{= |1 - s(0)|e(0)}
\end{align}
showing that $m = j$ as defined in Instruction 23.
Let us prove now Equation (20). Let,
\[ q := \# \{ a \in [0, n/2) : e_L(a) \neq e_R(a) \text{ and } e_L(a)e_R(a) = 0 \} . \]
Our aim is to show that \( q = i \). First, according to Lemma 3,
\[ q = \# \{ a \in \pi ([0, n/2 - k_U + g)) : e_L(a) \neq e_R(a) \text{ and } e_L(a)e_R(a) = 0 \} \]
where,
\[
\begin{align*}
q_1 &:= \# \{ a \in \pi ([0, n/2 - k_U + g)) : e_L(a) = 0 \text{ and } e_R(a) \neq 0 \}, \\
q_2 &:= \# \{ a \in \pi ([0, n/2 - k_U + g)) : e_L(a) \neq 0 \text{ and } e_R(a) = 0 \} .
\end{align*}
\]
Using Equations (22) and (23) and the fact that \( c_a \neq 0 \) for all \( a \), we obtain,
\[ q_1 = \# \left\{ b \in [0, n/2 - k_U + g) : e_V(\pi(b)) \neq 0 \text{ and } e^0(b) = -\left( b \star e_V \right)(\pi(b)) \right\} . \]
\[ q_2 = \# \left\{ b \in [0, n/2 - k_U + g) : e_V(\pi(b)) \neq 0 \text{ and } e^0(b) = -\left( (c + b) \star e_V \right)(\pi(b)) \right\} . \]
Notice now that when \( e_V(\pi(b)) \neq 0 \), as \( c_a \neq 0 \) for all \( a \), we necessarily have
\[ -\left( b \star e_V \right)(\pi(b)) \neq (c - b) \star e_V(\pi(b)) \]
and,
\[ -\left( (c + b) \star e_V \right)(\pi(b)) \neq (c - b) \star e_V(\pi(b)) . \]
Therefore,
\[ q = q_1 + q_2 \]
\[ = \# \left\{ b \in [0, n/2 - k_U + g) : e_V(\pi(b)) \neq 0 \text{ and } e^0(b) \neq (c - b) \star e_V(\pi(b)) \right\} . \]
which is equal \( |s^{(0)} \star e^{(0)} - v^{(0)}| = i \) and it concludes the proof. \( \square \)

**Lemma 5.** In Instruction 18, \( e^{(0)} \) verifies,
\[ e^{(0)}(H_{[0,n/2-k_U+g]})^\top = 0_{n/2-k_U+g} . \]

**Proof.** First, in Instruction 18, \( e^{(0)} \) is equal to
\[ (1 - z^{(0)}) \star f \]
for some \( f \in \mathbb{F}_3^{n/2-k_U+g} \). The matrix \( H \) has been obtained in Instruction 13 via a \texttt{ExtGaussElim} (Algorithm 3), therefore it is in extended systematic form (see Definition 2). In particular, \( H_{[0,n/2-k_U+g]} \) is full of zero except on the diagonal where there are potentially some 1’s. Therefore, by definition of \( z^{(0)} \) in Instruction 16,
\[ (1 - z^{(0)}) \star f = f \left( \operatorname{Id}_{n/2-k_U+g} - H_{[0,n/2-k_U+g]} \right)^\top \]
Furthermore, using once again that \( H_{[0,n/2-k_U+g]} \) has only 0 or 1 on its diagonal, and otherwise is 0, we obtain
\[ (1 - z^{(0)}) \star f \left( H_{[0,n/2-k_U+g]} \right)^\top = 0_{n/2-k_U+g} . \]
which concludes the proof of the lemma.

Equipped with Lemmas 3, 4 and 5 we are now ready to prove Proposition 3.

Proof of Proposition 3. Let us first show Equation (13). By Lemma 4 and Instruction 24 we have

\[ n - |(e_L, e_R)| = 2j + i \quad \text{and} \quad 2j + i = n - w \]

showing that \(|e_L| + |e_R| = w\).

Let us now prove Equation (12) given in the proposition. Notice that \(y_U = y^{e-1}\) and \(e_U = e^{e-1}\) where \(e\) is given in Instruction 25. Therefore,

\[ (y_U - e_U) H_U^T = (y - e) (H_U^e)^T. \]  \(\tag{24}\)

Recall now that \(H\) has been computed in Instruction 13 via \texttt{ExtGaussElim} (Algorithm 3), and therefore is in extended systematic form (see Definition 2). Let,

\[ J = \{ i \in [0, n/2 - k_U + g), \ H_{i,i} \neq 0 \}. \]

By definition, we have

\[
\left\{ \begin{array}{l}
\forall i \in J : \ H_{i,i} = 1 \quad \text{and} \quad |\text{col}(H, i)| = 1, \\
\forall i \in [0, n/2 - k_U + g) \setminus J : \ |\text{row}(H, i)| = 0.
\end{array} \right.
\]

where \(|\text{col}(H, i)| (\text{resp. } \text{row}(H, i))\) is defined as the \(i\)-th column (resp. row) of \(H\). But as \(\langle H \rangle = \langle H_U^e \rangle\), the set \(J\) is an information set of \(H_U^e\). We deduce that it exists a non-singular \(S \in \mathbb{F}_3^{(n/2-k_U) \times (n/2-k_U)}\) such that \(SH_U^e \in \mathbb{F}_3^{(n/2-k_U) \times n/2}\) verifies

\[ \forall j \in J, \ \text{row}(SH_U^e, j) = \text{row}(H, j) \]

Therefore,

\[ \forall j \in J, \ (y - e) H^T(j) = 0 \implies (y - e) (H_U^e)^T = 0_{n/2-k_U} \]  \(\tag{25}\)

Let \(e_{\text{new}}^{(0)}\) as in Instruction 21 and \(e_{\text{old}}^{(0)}\) as in Instruction 18. According to Lemma 5,

\[ e_{\text{new}}^{(0)} = e_{\text{old}}^{(0)} + y H^T - e^{(1)}(H_{[n/2-k_U+g,n/2]}^e)^T \]  \(\tag{26}\)

where \(e^{(1)}\) is given in Instruction 20. Notice now that \((e\) is given in Instruction 25\)

\[ eH^T = e_{\text{new}}^{(0)} (H_{[0,n/2-k_U+g]})^T + e^{(1)}(H_{[n/2-k_U+g,n/2]}^e)^T \]

Using Equation (26) and Lemma 5, we get

\[ e_{\text{new}}^{(0)} (H_{[0,n/2-k_U+g]})^T = yH^T (H_{[0,n/2-k_U+g]})^T - e^{(1)}(H_{[n/2-k_U+g,n/2]}^e)^T (H_{[0,n/2-k_U+g]})^T \]

Therefore,

\[ (y - e) H^T = yH^T - yH^T (H_{[0,n/2-k_U+g]})^T \]
\[ + e^{(1)}(H_{[n/2-k_U+g,n/2]}^e)^T - e^{(1)}(H_{[n/2-k_U+g,n/2]}^e)^T (H_{[0,n/2-k_U+g]})^T \]  \(\tag{27}\)

Recall now that,

\[ \forall i \in J : \ H_{i,i} = 1 \quad \text{and} \quad |\text{col}(H, i)| = 1 \]

We deduce that for any \(x \in \mathbb{F}_3^{n/2-k_U+g}\),

\[ \forall j \in J, \ x(H_{[0,n/2-k_U+g]})^T(j) = x(j). \]
Plugging this in Equation (27) shows that

\[ \forall j \in J, \quad (y - e)H^T(j) = 0. \]

Therefore, according to (25),

\[ (y - e)(H^T_U)^\top = 0_{n/2-k_U} \]

which concludes the proof by using Equation (24). \qed