A New Signature Scheme Based on $(U|U + V)$ Codes

Thomas Debris Alazard, Nicolas Sendrier, and Jean-Pierre Tillich

Digital Signature from Codes

Public Key: a binary code $C[n, k]$
Secret Key: the code structure

**Complete Decoding:** Find the codeword closest to a random word
$\rightarrow$ [CFS, 2001], extreme parameters, poor scaling

**Source Distortion:** Find a codeword close to a random word
$\rightarrow$ find a (secure) family of code for which decoding with an approximation factor is possible
CFS-Like Approach — Complete Decoding

Decoding $w$ errors in an $[n, k]$ code

How far the trapdoor allows you to decode

How far you should decode
Decoding $w$ errors in an $[n, k]$ code

A New Signature Scheme Based on $(U|U + V)$ Codes
Source Distortion with $(U | U + V)$ codes

Decoding $w$ errors in an $[n, k]$ code

A New Signature Scheme Based on $(U | U + V)$ Codes
A New Digital Signature Scheme Based on $(U|U + V)$ Codes

Public Key:

$$G = S \begin{pmatrix} G_U & G_U \\ 0 & G_V \end{pmatrix} P$$

with $G_U$ and $G_V$ random, $S$ non-singular, $P$ permutation.

Secret Key: $G_U$, $G_V$, and $P$

Signature: codeword $x$ close to Hash($Message$)

Verification: is $x$ a codeword close to Hash($Message$)?
Existential unforgeability under adaptive chosen message attacks (EUF-CMA) under two assumptions

\begin{align*}
\begin{cases}
\text{Indistinguishability of } (U|U+V) \text{ code} \\
\text{Hardness of Decoding One Out of Many (DOOM)}
\end{cases}
\end{align*}
## Parameters

<table>
<thead>
<tr>
<th>Security</th>
<th>Signature length (bits)</th>
<th>Public key size (MBytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>80</td>
<td>0.683</td>
</tr>
<tr>
<td></td>
<td>128</td>
<td>1.75</td>
</tr>
<tr>
<td></td>
<td>256</td>
<td>7.00</td>
</tr>
</tbody>
</table>

Thank you for your attention