Apprentissage avec erreurs (Anneaux)

Schéma de signature: GLYPH

- Pub: A, T et (C, Z_1, Z_2)
- Priv: S, E
- $W' = AZ_1 + Z_2 - TC$
- $W = AY_1 + Y_2$
- $Z_1 = SC + Y_1$
- $Z_2 = EC + Y_2$
- $T = AS + E$

$$
\begin{aligned}
W' &= AZ_1 + Z_2 - TC \\
&= A(SC + Y_1) + Z_2 - (AS + E)C \\
&= AY_1 + Z_2 - EC \\
&= AY_1 + EC + Y_2 - EC \\
&= AY_1 + Y_2 \\
&= W
\end{aligned}
$$

Apprentissage avec erreurs (Anneaux)

Établissement de clé: RLWE-KEX

- [Ding, 2012] A Simple Provably Secure Key Exchange Scheme Based on the Learning with Errors Problem

- Comme Diffie-Hellman mais basé sur $RLWE$ plutôt que DDH