

CD MEDS CD

Matrix Equivalence Digital Signature

Tung Chou, Ruben Niederhagen, Edoardo Persichetti,
Lars Ran, Tovahery Hajatiana Randrianarisoa,
Krijn Reijnders, Simona Samardjiska, Monika Trimoska

Krijn Reijnders
SIAM AG - Advances in
Code-based Signatures
July 12th, 2023

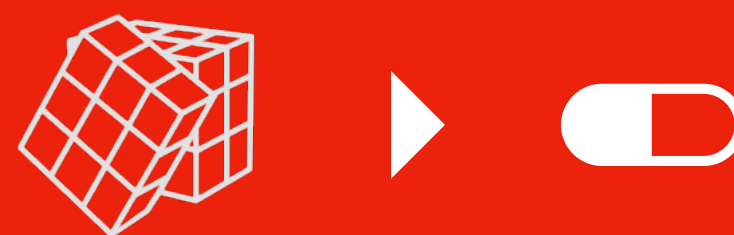
MEDS: a new code-based signature scheme

1



Matrix Code
Equivalence

2



From MCE
to MEDS

3



Performance