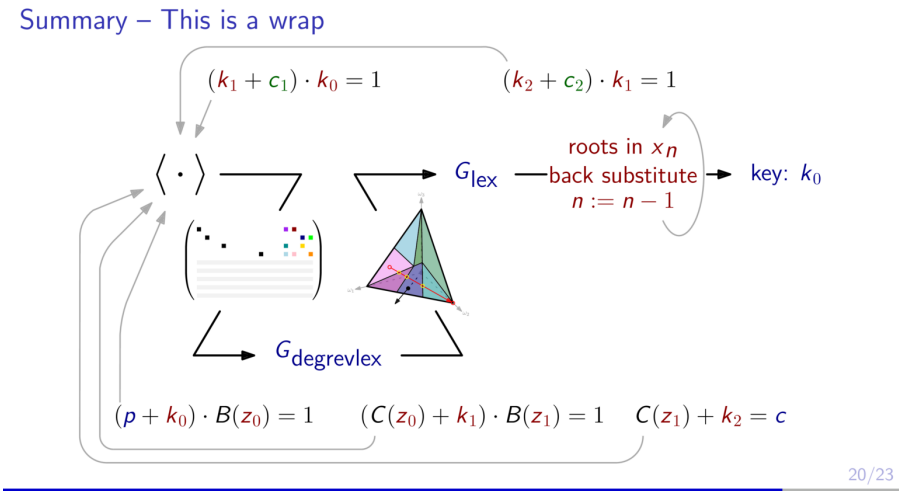
AOC Presentation

Introduction to GB Attacks on AOC

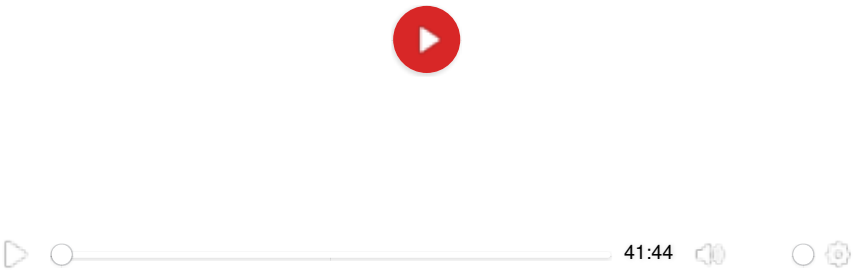
by Alan Szepieniec Aug 9, 2020 0 Comment

Next Wednesday, 12 August 2020 at 16:30 CET, our own Ferdinand Sauer will be giving an introductory presentation on Gröbner basis attacks in the context of attacking arithmetization-oriented ciphers. Be sure to tune in if you want to learn more about the attack space for AO ciphers like Rescue and Poseidon. Email us if you want access to the zoom link.

Update: Slides & VoD



Couldn't make it? Not to worry! Take a peek at the slides, and complement them by watching the recording.



Alan Szepieniec

Website: https://asdm.gmbh

Leave a Reply

Logged in as Jan Ferdinand Sauer Logout

Comment

Submit