MAYO update

Ward Beullens,
Fabio Campos,
Sofía Celi,
Basil Hess, and
Matthias J. Kannwischer.

9/24/2025

Overview

- Short intro to MAYO
- Round 2 updates
- Update about Wedge attack

MAYO: A little oil can go a long way

Whip map $P: \mathbb{F}_q^n \to \mathbb{F}_q^m$ with small space O up to a larger map $P^\star: \mathbb{F}_q^{kn} \to \mathbb{F}_q^m$, that vanishes on a larger oil space O^k.

$P: \mathbb{F}_q^n \to \mathbb{F}_q^m$

$P^\star: \mathbb{F}_q^{kn} \to \mathbb{F}_q^m$

Whipping Oil-and-Vinegar

Choose matrices $E_{i,j}$ for all $0 \leq i \leq j \leq k$ and set

$$P^{\star}(x_1, \ldots, x_k) = \sum_i E_{ii} P(x_i) + \sum_{i<j} E_{ij} P'(x_i, x_j)$$

If P vanishes on O, then $P^{\star}$ vanishes on O^k, which has dimension $k * \dim(O)$, so if $ko > m$ we can use $P^{\star}$ as a trapdoor function.

New Hardness assumption:

Systems P^* of this form are preimage resistant. When P is uniformly random.

Attacks do not seem to be able to exploit this structure, all known attacks are completely generic.

Security Analysis

Assume that:

1) Oil-and-Vinegar maps P are indistinguishable from random MQ maps. ☺
2) Whipping up a random map P, results in a (multi-target) preimage resistant MQ map $P^{\star}$.

Then the MAYO signature scheme is EUF-CMA secure.
(for appropriately chosen parameters)

Overview

Short intro to MAYO

Round 2 updates

Update about Wedge attack

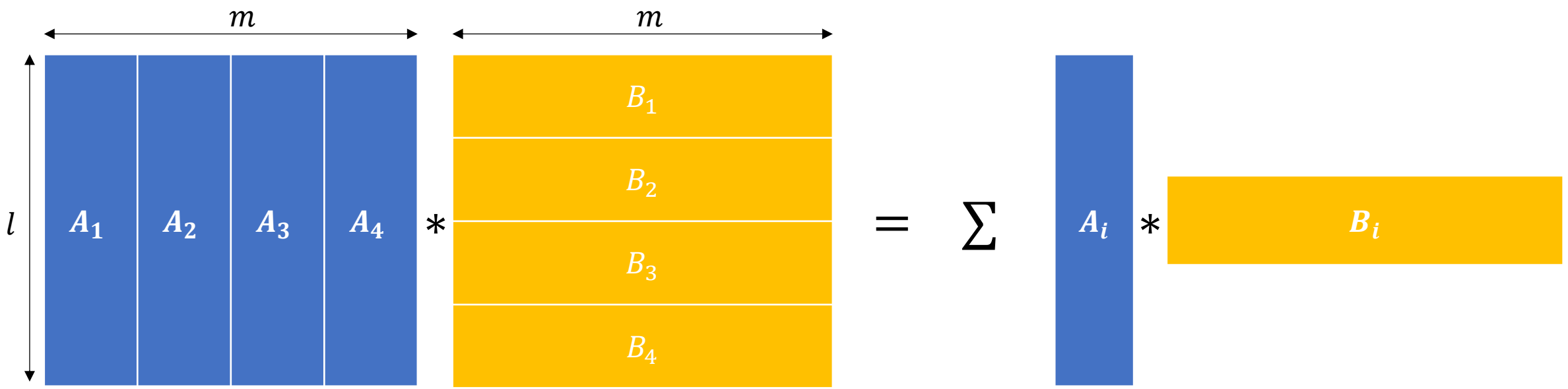
Round 2 updates

- New “nibble-sliced” representation of public keys
  -> up to 3.2x faster signing and verification

- Tweaked parameters for better security.
  Higher restart probability (improve testing coverage) + Security margin against underdetermined system solving

- More implementations: ARM Neon + Cortex M4 optimized implementation

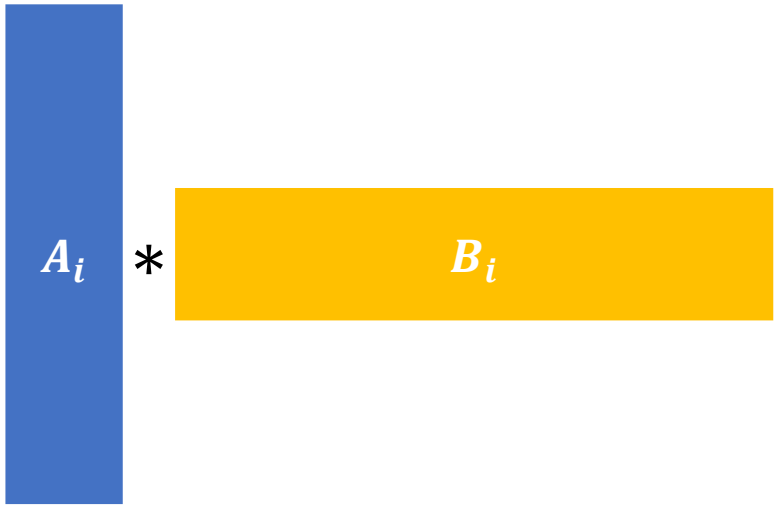
Step 1: split A and B in narrow strips



A_i have width $t \approx \log_q l$, where l is the height of A, and q is the size of the finite field.

Step 2: Multiplication by table lookup

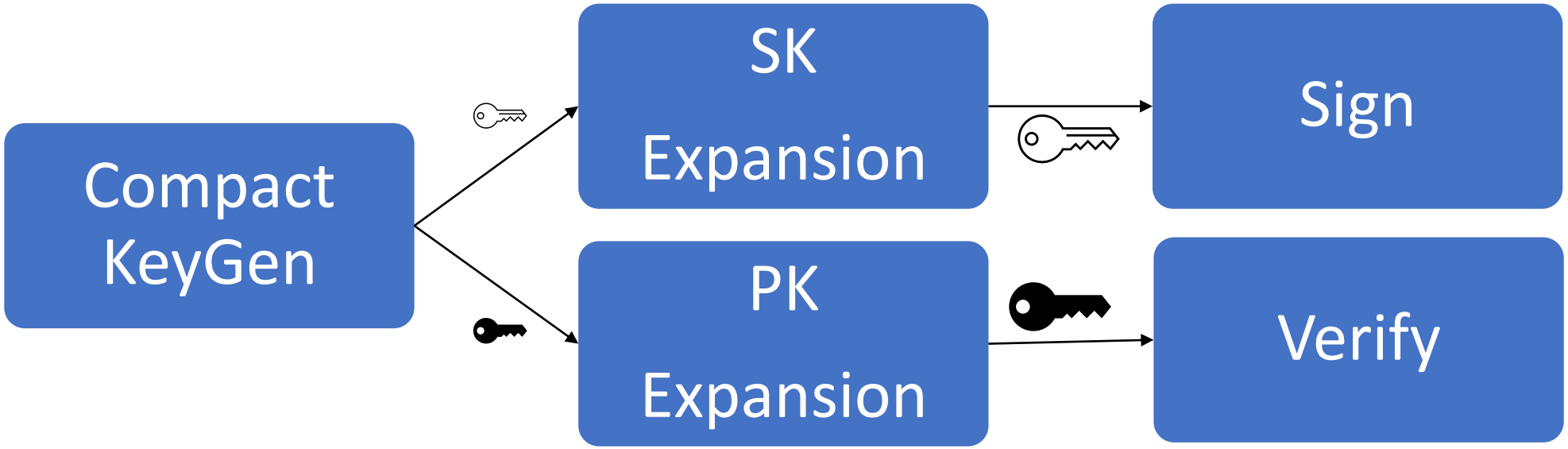
- Make a table that contains all the linear combinations of rows of B_i.
  (Table has size $q^t n = ln$, requires ln additions to construct)



- Compute $A_i * B_i$ by looking up each row in the table. (l lookups of rows of n elements)

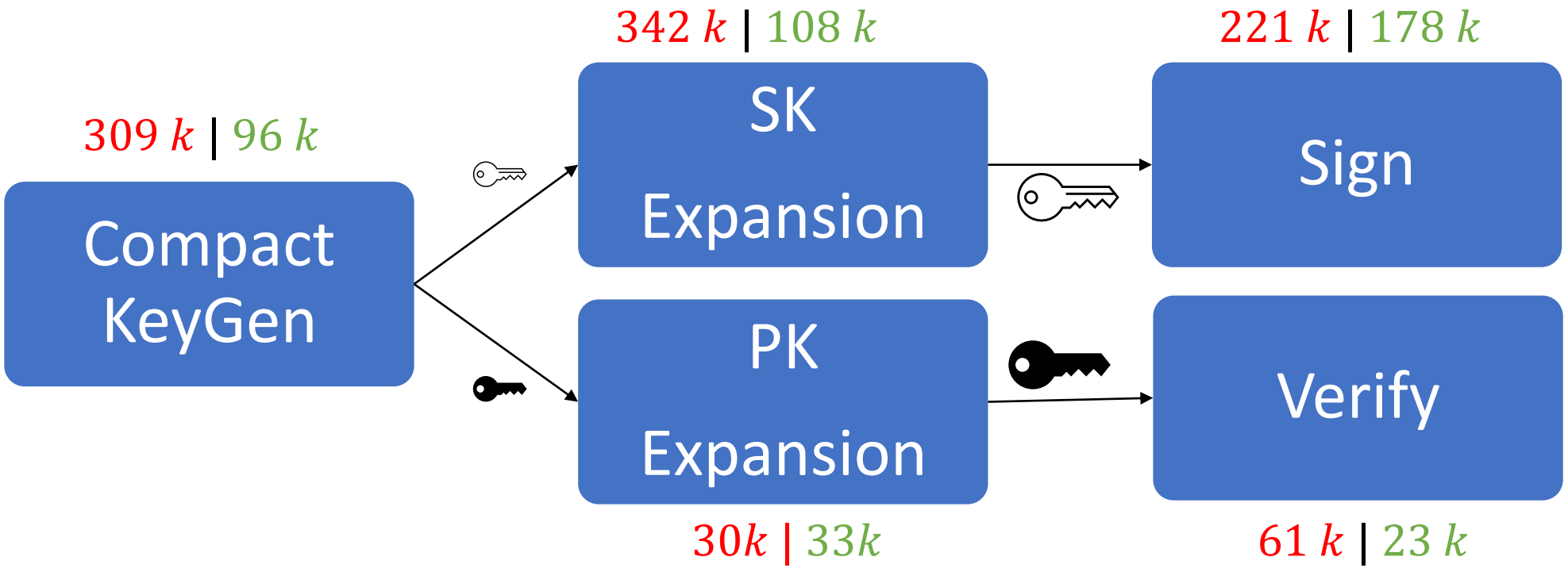
- Cost is $O(ln)$ and needs to be repeated $\frac{m}{\log_q l}$ times, so total cost is $O(\frac{lmn}{\log_q l})$

5-part API



Ice Lake cycle count MAYO 2

AVX2 + AESNI Round1 | Round2 implementation



Overview

Short intro to MAYO

Round 2 updates

Update about Wedge attack

Wedges, oil, and vinegar
An analysis of UOV in characteristic 2

Lars Ran

Radboud Universiteit Nijmegen, Netherlands
lars.ran@ru.nl

Abstract. The Unbalanced Oil and Vinegar construction (UOV) has been the backbone of multivariate cryptography since the fall of HFE-based schemes. In fact, 7 UOV-based schemes have been submitted to the NIST additional call for signatures, and 4 of these made it to the second round. For efficiency considerations, most of these schemes are defined over a field of characteristic 2. This has as a side effect that the polar forms of the UOV public maps are not only symmetric, but also alternating.
In this work, we propose a new key-recovery attack on UOV in characteristic 2 that makes use of this property. We consider the polar forms of the UOV public maps as elements of the exterior algebra. We show that these are contained in a certain subspace of the second exterior power that is dependent on the oil space. This allows us to define relations between the polar forms and the image of the dual of the oil space under the Plücker embedding. With this, we can recover the secret oil space using sparse linear algebra.
This new attack has an improved complexity over previous methods and reduces the security by 4, 11, and 20 bits for `uov-Ip`, `uov-III`, and `uov-V`, respectively. Furthermore, the attack is applicable to MAYO_2 and improves on the best attack by 28 bits.

1 Introduction

Since factorization of $15 = 3 \cdot 5$ by a quantum computer, society is taking the threat of quantum computers more and more seriously. Since these machines could potentially break currently used public-key cryptography such as RSA and ECDSA, this is not unwarranted. In order to be one step ahead, different institutes, such as NIST, began an effort to standardize new cryptographic schemes that should be quantum resistant. In the meantime, many schemes have been proposed, a lot of schemes have been broken, and a few remain standing. This led NIST to standardize three schemes last year, based on lattices and hashes [16,15,17]. However, lattices and hashes are not the only viable hardness assumptions, and to diversify such assumptions, NIST opened an additional call for digital signature schemes.

The Multivariate Quadratic (MQ) problem is among these potential hard problems. This problem assumes that it is hard to find a solution to a (large enough) quadratic system of equations over a finite field. There are two main

Wedge attack ePrint 2025/1143

- In, Lars Ran gives a new Key recovery attack against UOV in characteristic 2, using the exterior algebra.
- Since a MAYO public key has the structure of a UOV key, the approach also applies to MAYO
- Attack is easy to analyze (as opposed to more structured UOV variants like SNOVA), and only applies to MAYO2:
- Bottleneck is computing the kernel of a matrix with $2^{47.4}$ rows and columns
  -> Estimated bit cost of 2^{113}.
- It does not seem possible to parallelize the attack efficiently.

Possible tweak for MAYO2 params

	n #variables	m #equations	o $dim(O)$	k Whipping parameter	PK Size (Bytes)	Signature Size (Bytes)
Round 2	81	64	17	4	4913	186
Proposal for Round 3	96	64	16	4	4368 (-11%)	216 (+16%)

Possible tweak for MAYO2 params

	n #variables	m #equations	o $dim(O)$	k Whipping parameter	PK Size (Bytes)	Signature Size (Bytes)
Round 2	81	64	17	4	4913	186
Proposal for Round 3	96	64	16	4	4368 (-11%)	216 (+16%)

We decided to keep $m = 64$, since 64 field elements fit in one AVX2 register to avoid significant penalty on performance.

Possible tweak for MAYO2 params

	n #variables	m #equations	o $dim(O)$	k Whipping parameter	PK Size (Bytes)	Signature Size (Bytes)
Round 2	81	64	17	4	4913	186
Proposal for Round 3	96	64	16	4	4368 (-11%)	216 (+16%)

We decided to keep $m = 64$, since 64 field elements fit in one AVX2 register to avoid significant penalty on performance.

Conclusion: Because of the conceptual simplicity of MAYO public keys the **Wedge attack is easy to analyze** in the MAYO context, moreover it can be **mitigated rather cheaply**.

Bonus slide: Advanced constructions 💛 MAYO

- MAYO is cheap to prove in zero-knowledge:
  Example: MAYO1 with VOLE-in-the-head proof
  - Including SHAKE256: 29KB proof size, 80ms proving, 45ms verification
  - Without SHAKE256: 7.5KB proof size, 51ms proving, 37ms verification

Yields practical anonymous credentials and blind signatures!

- MAYO signing is cheap to thresholdize:
  Example: MAYO1 with 4 out of 10 signing
  Distributed signing takes < 90ms (not optimized yet)