PERK: Compact Signature Scheme Based on a New Variant of the Permuted Kernel Problem

Slim Bettaieb[2], Loïc Bidoux[2], **Victor Dyseryn**[1], Andre Esser[2], Philippe Gaborit[1], Mukul Kulkarni[2], Marco Palumbi[2]

[1]XLIM, Université de Limoges, France
[2]Technology Innovation Institute, UAE

Journées C2 - October 16, 2023

In this talk

- What is this Permuted Kernel Problem (PKP)?
- Why is it so hard?
- What can we do with it?
- Why studying variants of PKP?

Permuted Kernel Problem

Definition (IPKP [Sha90])

Let $m < n$ be positive integers, Given

- $\boldsymbol{H} \in \mathbb{F}_q^{m \times n}$;
- $\boldsymbol{x} \in \mathbb{F}_q^{n}$;
- $\boldsymbol{y} \in \mathbb{F}_q^{m}$,

the Inhomogeneous Permuted Kernel Problem $\mathrm{IPKP}_{q,m,n}$ asks to find a permutation $\pi \in \mathcal{S}_n$ such that

$$\boldsymbol{H}\pi[\boldsymbol{x}] = \boldsymbol{y}.$$

Permuted Kernel Problem

Example

$\pi = id$

$$\begin{pmatrix} 0 & 1 & 1 & -1 & 0 \\ 1 & 1 & -1 & 0 & 1 \\ -1 & 1 & 0 & -1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ -1 \\ -1 \\ 1 \end{pmatrix} = \begin{pmatrix} \mathbf{1} \\ \mathbf{0} \\ \mathbf{-1} \end{pmatrix} \stackrel{?}{=} \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$$

Permuted Kernel Problem

Example

$\pi = (1, 2)$

$$\begin{pmatrix} 1 \\ 0 \\ -1 \\ -1 \\ 1 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 1 & 1 & -1 & 0 \\ 1 & 1 & -1 & 0 & 1 \\ -1 & 1 & 0 & -1 & 0 \end{pmatrix} \begin{pmatrix} \mathbf{0} \\ \mathbf{0} \\ \mathbf{0} \end{pmatrix} \stackrel{?}{=} \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$$

Permuted Kernel Problem

Example

$\pi = (1,2) \circ (2,3)$

$$
\begin{array}{cc}
 & \begin{pmatrix} 1 \\ -1 \\ 0 \\ -1 \\ 1 \end{pmatrix} \\
\begin{pmatrix} 0 & 1 & 1 & -1 & 0 \\ 1 & 1 & -1 & 0 & 1 \\ -1 & 1 & 0 & -1 & 0 \end{pmatrix} & \begin{pmatrix} \mathbf{1} \\ \mathbf{1} \\ \mathbf{1} \end{pmatrix} \stackrel{?}{=} \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}
\end{array}
$$

Comparison with Syndrome Decoding

Definition (Syndrome Decoding $\mathtt{SD}(n, k, w)$)

Given:

- $\boldsymbol{H} \in \mathbb{F}_q^{(n-k)\times n}$ a parity check matrix;
- $\boldsymbol{s} \in \mathbb{F}_q^{n-k}$ a syndrome,

the Syndrome Decoding Problem asks to find an error $\boldsymbol{e}$ of Hamming weight $w_h(\boldsymbol{e}) = w$, such that

$$\boldsymbol{s} = \boldsymbol{H}\boldsymbol{e}.$$

Permuted Kernel	Syndrome Decoding
$\lvert\mathcal{S}_n\rvert = n!$	$\lvert\mathbb{F}_q^n\rvert = q^n$

Number of solutions

Proposition

The average number of solutions for a random $\mathrm{IPKP}_{q,m,n}$ *instance is*

$$\frac{n!}{q^m}.$$

Since all existing attacks on IPKP and variants are combinatorial, they benefit from a speedup equal to $\max(1, \frac{n!}{q^m})$.

Coding theory equivalent: Gilbert-Varshamov bound

Systematic form

$$H\pi[x] = y$$

Systematic form

$$\underbrace{P H}_{H'} \pi[x] = \underbrace{P y}_{y'}$$

Georgiades algorithm [Geo92]

For $\pi[\boldsymbol{x}] = (\boldsymbol{x}_1, \boldsymbol{x}_2)$,

$$\left(\begin{array}{c|c} \boldsymbol{I}_m & \boldsymbol{H}' \end{array} \right) \begin{pmatrix} \boldsymbol{x}_1 \\ \hline \boldsymbol{x}_2 \end{pmatrix} = \boldsymbol{y}$$

Georgiades algorithm [Geo92]

For $\pi[\boldsymbol{x}] = (\boldsymbol{x}_1, \boldsymbol{x}_2)$,

$$\boldsymbol{x}_1 = \boldsymbol{y} - \boldsymbol{H}'\boldsymbol{x}_2$$

$\Rightarrow$ enumerate $\boldsymbol{x}_2$ as every subpermutation of $\boldsymbol{x}$ of size $n - m$.

Georgiades algorithm [Geo92]

Proposition (Complexity)

$$\mathcal{T} = \mathcal{O}\left(\frac{n!}{m!}\right)$$

Coding theory equivalent: Prange algorithm

Time-memory trade-off

$$\left(\begin{array}{c|c} \boldsymbol{H}_1 & \boldsymbol{H}_2 \end{array}\right) \left(\begin{array}{c} \boldsymbol{x}_1 \\ \hline \boldsymbol{x}_2 \end{array}\right) = \boldsymbol{y}$$

$$\boldsymbol{H}_1 \boldsymbol{x}_1 = \boldsymbol{y} - \boldsymbol{H}_2 \boldsymbol{x}_2$$

Time-memory trade-off

$$L_1 = \{(\boldsymbol{x}_1, \boldsymbol{H}_1\boldsymbol{x}_1) \mid \boldsymbol{x}_1 \in \mathbb{F}_q^{n/2} \text{ sub-permutation of } \boldsymbol{x}\}$$

$$L_2 = \{(\boldsymbol{x}_2, \boldsymbol{y} - \boldsymbol{H}_2\boldsymbol{x}_2) \mid \boldsymbol{x}_2 \in \mathbb{F}_q^{n/2} \text{ sub-permutation of } \boldsymbol{x}\}$$

$$L_1 \bowtie L_2 = \{(\boldsymbol{x}_1, \boldsymbol{x}_2) \mid \exists \boldsymbol{z}, (\boldsymbol{x}_1, \boldsymbol{z}) \in L_1 \text{ and } (\boldsymbol{x}_2, \boldsymbol{z}) \in L_2\}$$

Time-memory trade-off

Proposition (Complexity)

$$\mathcal{T} = \mathcal{O}\left(|L_1| + |L_2| + |L_1 \bowtie L_2|\right)$$
$$\mathcal{M} = \mathcal{O}\left(|L_1| + |L_2|\right)$$

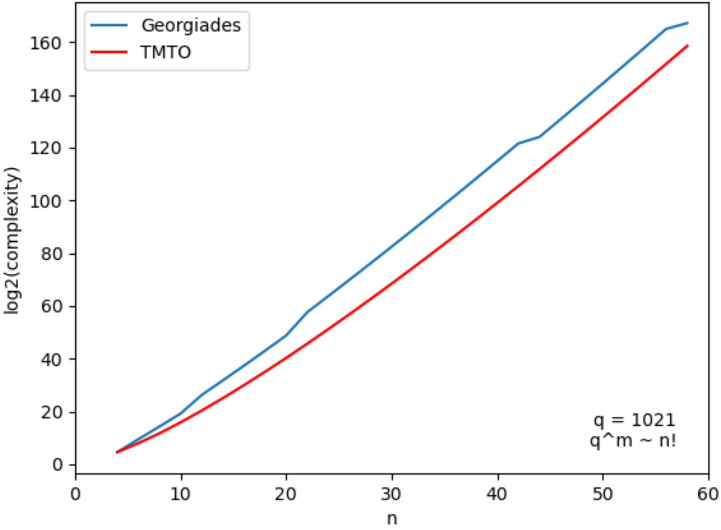
with

$$|L_1| = |L_2| = \frac{n!}{(n/2)!}$$

$$|L_1 \bowtie L_2| = \frac{|L_1| \times |L_2|}{q^m}$$

Coding theory equivalent: Birthday decoding

Comparison



Georgiades
TMTO
q = 1021
q^m ~ n!
log2(complexity)
n
0
20
40
60
80
100
120
140
160
0
10
20
30
40
50
60

KMP algorithm [KMP19]

Meet in the middle approach between Georgiades and TMTO

$$\begin{pmatrix} I_{m-u} & & H' & \\ \mathbf{0} & H_2 & & H_3 \end{pmatrix} \begin{pmatrix} x_1 \\ \hline x_2 \\ \hline x_3 \end{pmatrix} = \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$$

$$x_1 = y_1 - H'(x_2, x_3)$$

$$H_2 x_2 + H_3 x_3 = y_2$$

KMP algorithm [KMP19]

Proposition (Complexity)

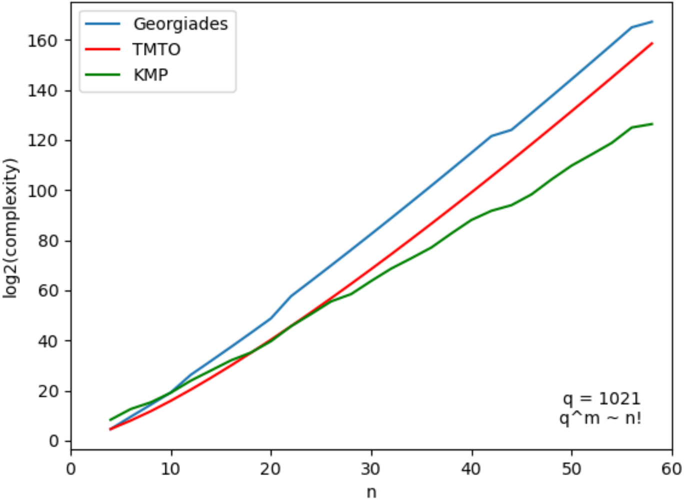
$$\mathcal{T} = \mathcal{O}\left(|L_1| + |L_2| + |L_1 \bowtie L_2|\right)$$

with

$$|L_1| = |L_2| = \binom{n}{(n-m+u)/2}\left((n-m+u)/2\right)!$$

$$|L_1 \bowtie L_2| = \frac{|L_1| \times |L_2|}{q^u}$$

Comparison



*KMP/SBC cost estimation courtesy of `https://github.com/Crypto-TII/CryptographicEstimators`

Other attacks on IPKP

- [BCCG93]
- [PC94]
- Joux-Jaulmes attack [JJ01]

Applications of PKP

Encryption	✗
Hash-and-sign	✗
Proof of Knowledge	✓

PKP-based proof of knowledge

Algorithm 2 The original 5-pass PKP identification protocol

$\mathcal{P}(\mathsf{sk}, \mathsf{pk})$		$\mathcal{V}(\mathsf{pk})$
$\sigma \xleftarrow{\$} S_n$ $\mathbf{r} \xleftarrow{\$} \mathbb{F}_p^n$ $\mathsf{C}_0 \leftarrow \mathrm{Com}(\sigma, \mathbf{Ar})$ $\mathsf{C}_1 \leftarrow \mathrm{Com}(\pi\sigma, \mathbf{r}_\sigma)$		
	$\xrightarrow{\mathsf{C}_0, \mathsf{C}_1}$	
		$c \xleftarrow{\$} \mathbb{F}_p$
	$\xleftarrow{c}$	
$\mathbf{z} \leftarrow \mathbf{r}_\sigma + c\mathbf{v}_{\pi\sigma}$		
	$\xrightarrow{\mathbf{z}}$	
		$b \xleftarrow{\$} \{0, 1\}$
	$\xleftarrow{b}$	

if $b = 0$ **then**
$\quad \mathsf{rsp} \leftarrow \sigma$
else
$\quad \mathsf{rsp} \leftarrow \pi\sigma$
end if		

	$\xrightarrow{\mathsf{rsp}}$	

		if $b = 0$ **then**
		$\quad$ accept if $\mathsf{C}_0 = \mathrm{Com}(\sigma, A\mathbf{z}_{\sigma^{-1}})$
		else
		$\quad$ accept if $\mathsf{C}_1 = \mathrm{Com}(\pi\sigma, \mathbf{z} - c\mathbf{v}_{\pi\sigma})$
		end if

PKP-based proof of knowledge

Prover$(\pi, \mathbf{H}, \mathbf{x}, \mathbf{y})$

$\theta \xleftarrow{\$} \{0,1\}^\lambda$
for $i \in \{N, \dots, 1\}$ **do**
  $\theta_i \xleftarrow{\$,\theta} \{0,1\}^\lambda,\ \phi_i \xleftarrow{\$,\theta_i} \{0,1\}^\lambda$
  if $i \neq 1$ **do**
    $\pi_i \xleftarrow{\$,\phi_i} \mathcal{S}_n,\ \mathbf{v}_i \xleftarrow{\$,\phi_i} \mathbb{F}_q^n$
    $r_{1,i} \xleftarrow{\$,\theta_i} \{0,1\}^\lambda,\ \mathsf{com}_{1,i} = \mathsf{Com}(r_{1,i},\ \phi_i)$
  else
    $\pi_1 = \pi_2^{-1} \circ \cdots \circ \pi_N^{-1} \circ \pi,\ \mathbf{v}_1 \xleftarrow{\$,\phi_1} \mathbb{F}_q^n$
    $r_{1,1} \xleftarrow{\$,\theta_1} \{0,1\}^\lambda,\ \mathsf{com}_{1,1} = \mathsf{Com}(r_{1,1},\ \pi_1 \,||\, \phi_1)$
  end
end
$\mathbf{v} = \mathbf{v}_N + \sum_{i \in [1,N-1]} \pi_N \circ \cdots \circ \pi_{i+1}[\mathbf{v}_i]$
$\mathsf{com}_1 = \mathsf{Hash}(\mathbf{H}\mathbf{v} \,||\, (\mathsf{com}_{1,i})_{i \in [1,N]})$

Prover → Verifier: com_1

Verifier$(\mathbf{H}, \mathbf{x}, \mathbf{y})$: $\kappa \xleftarrow{\$} \mathbb{F}_q^*$

Verifier → Prover: κ

$\mathbf{s}_0 = \kappa \cdot \mathbf{x}$
for $i \in [1, N]$ **do**
  $\mathbf{s}_i = \pi_i[\mathbf{s}_{i-1}] + \mathbf{v}_i$
end
$\mathsf{com}_2 = \mathsf{Hash}((\mathbf{s}_i)_{i \in [1,N]})$

Prover → Verifier: com_2

Verifier: $\alpha \xleftarrow{\$} [1, N]$

Verifier → Prover: α

$\mathbf{z}_1 = \mathbf{s}_\alpha$
if $i \neq 1$ **do**
  $z_2 = \pi_1 \,||\, (\theta_i)_{i \in [1,N] \setminus \alpha}$
else
  $z_2 = (\theta_i)_{i \in [1,N] \setminus \alpha}$
end
$\mathsf{rsp} = (\mathbf{z}_1, z_2, \mathsf{com}_{1,\alpha})$

Prover → Verifier: rsp

Verifier:
Compute $(\bar{\phi}_i, \bar{r}_{1,i}, \bar{\pi}_i, \bar{\mathbf{v}}_i)_{i \in [1,N] \setminus \alpha}$ from z_2
$\bar{\mathbf{s}}_0 = \kappa \cdot \mathbf{x}$
for $i \in [1, N] \setminus \alpha$ **do**
  $\bar{\mathbf{s}}_i = \bar{\pi}_i[\bar{\mathbf{s}}_{i-1}] + \bar{\mathbf{v}}_i$
end
$\bar{\mathbf{s}} = (\bar{\mathbf{s}}_1, \cdots, \bar{\mathbf{s}}_{\alpha-1}, \mathbf{z}_1, \bar{\mathbf{s}}_{\alpha+1}, \cdots, \bar{\mathbf{s}}_N)$

for $i \in [1, N] \setminus \alpha$ **do**
  if $i \neq 1$ **do**
    $\bar{\mathsf{com}}_{1,i} = \mathsf{Com}(\bar{r}_{1,i},\ \bar{\phi}_i)$
  else
    $\bar{\mathsf{com}}_{1,1} = \mathsf{Com}(\bar{r}_{1,1},\ \bar{\pi}_1 \,||\, \bar{\phi}_1)$
  end
end
$\bar{\mathsf{com}}_{1,\alpha} = \mathsf{com}_{1,\alpha},\ \bar{q} = \mathbf{H}\bar{\mathbf{s}}_N - \kappa \cdot \mathbf{y}$
$b_1 \longleftarrow (\mathsf{com}_1 = \mathsf{Hash}(\bar{q} \,||\, (\mathsf{com}_{1,i})_{i \in [1,N]}))$
$b_2 \longleftarrow (\mathsf{com}_2 = \mathsf{Hash}(\bar{\mathbf{s}}))$
return $b_1 \wedge b_2$

MPC-in-the-Head and PKP

Name	Type	σ size
Shamir [Sha90]	5-round	$\sim$28 kB
PKP-DSS	5-round	$\sim$21 kB
SUSHYFISH [Beu20]	5-round with helper	12-18 kB
[Fen22]	7-round	13-16 kB
[BG22]	5-round using structure	9-10 kB

Table: Comparison of recent digital signature schemes based on PKP assumptions for 128-bit security

Parameters in [BG22]

PKP parameters (q, n, m)	$\longrightarrow$	attacks on IPKP
MPC parameters (N, τ)	$\longrightarrow$	KZ attack on 5-round protocols [KZ20]

Increasing the challenge space leads to a decrease in τ.

	[BG22]	our work
Challenge space	$\mathbb{F}_q$	$\mathbb{F}_q^t$

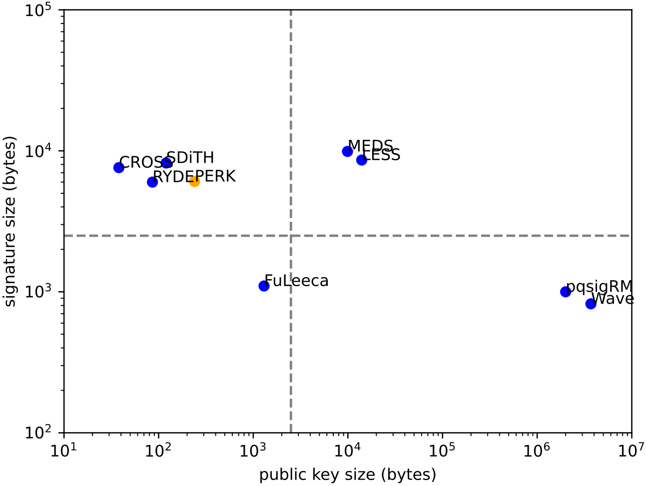
$t = 3 \longrightarrow$ 27% size decrease
$t = 5 \longrightarrow$ 33% size decrease

MPC-in-the-Head and PKP (with PERK)

Name	Type	σ size
Shamir [Sha90]	5-round	∼28 kB
PKP-DSS	5-round	∼21 kB
SUSHYFISH [Beu20]	5-round with helper	12-18 kB
[Fen22]	7-round	13-16 kB
[BG22]	5-round using structure	9-10 kB
PERK	5-round using structure	6-8 kB

Table: Comparison of recent digital signature schemes based on PKP assumptions for 128-bit security

Comparaison with NIST onramp code-based signatures



A variant of the Permuted Kernel Problem

Definition (r-IPKP)

Let $m < n$ and t be positive integers, Given

- $\boldsymbol{H} \in \mathbb{F}_q^{m \times n}$;
- $(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_t) \in (\mathbb{F}_q^n)^t$;
- $(\boldsymbol{y}_1, \ldots, \boldsymbol{y}_t) \in (\mathbb{F}_q^m)^t$,

the Relaxed Inhomogeneous Permuted Kernel Problem r-IPKP$_{q,m,n,t}$ asks to find a permutation $\pi \in \mathcal{S}_n$ such that

$$\boldsymbol{H}\pi\Big[\sum_{i\in[1,t]} \kappa_i \boldsymbol{x}_i\Big] = \sum_{i\in[1,t]} \kappa_i \boldsymbol{y}_i$$

for some $(\kappa_1, \ldots, \kappa_t) \in (\mathbb{F}_q)^t \setminus \{(0, \ldots, 0)\}$.

Coding theory equivalent: (Rank) Support Learning

Number of solutions

Proposition

The average number of solutions for a random r-IPKP$_{q,m,n,t}$ *instance is*

$$\frac{n!}{q^m} \cdot \frac{q^t - 1}{q - 1}$$

Idea of our attack

- Take the smallest weight vector $\boldsymbol{x}$ in $\langle \boldsymbol{x}_1, \ldots, \boldsymbol{x}_t \rangle$,

$$\boldsymbol{x} = \sum_{i \in [1,t]} \kappa_i \boldsymbol{x}_i$$

  of weight w.
- Define

$$\boldsymbol{y} = \sum_{i \in [1,t]} \kappa_i \boldsymbol{y}_i$$

  and solve IPKP instance $\boldsymbol{H}\pi[\boldsymbol{x}] = \boldsymbol{y}$.
- Adapt KMP algorithm to take advantage of the $n - w$ zeros in $\boldsymbol{x}$.

KMP adaptation with zeros

$$\begin{pmatrix} \mathbf{x}_1 \\ \hline \mathbf{x}_2 \\ \hline \mathbf{x}_3 \end{pmatrix} \begin{matrix} \leftarrow n-w-z \text{ zeros} \\ \\ \leftarrow z/2 \text{ zeros} \\ \\ \leftarrow z/2 \text{ zeros} \end{matrix}$$

$$\begin{pmatrix} \mathbf{I}_{m-u} & & \mathbf{H}' & \\ \mathbf{0} & \mathbf{H}_2 & & \mathbf{H}_3 \end{pmatrix} = \begin{pmatrix} \mathbf{y}_1 \\ \mathbf{y}_2 \end{pmatrix}$$

$$\mathbf{x}_1 = \mathbf{y}_1 - \mathbf{H}'(\mathbf{x}_2, \mathbf{x}_3)$$

$$\mathbf{H}_2\mathbf{x}_2 + \mathbf{H}_3\mathbf{x}_3 = \mathbf{y}_2$$

Our attack

Proposition (Complexity)

$$\mathcal{T} = \mathcal{O}\left(\mathcal{T}_{ISD} + \left(|L_1| + |L_2| + |L_1 \bowtie L_2|\right) P\right)$$

with

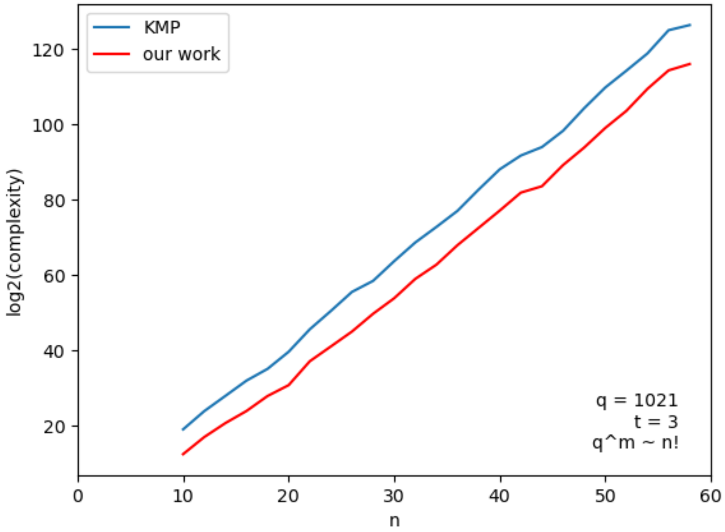
$$k = (n - m + u)/2\,,\; z \leq n - w$$

$$|L_1| = |L_2| = \binom{k}{z/2}\binom{n-z}{k-z/2}(k - z/2)!$$

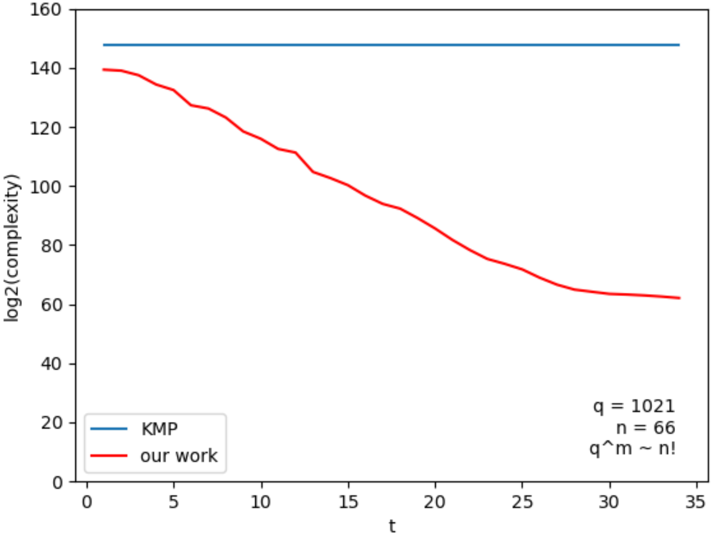
$$|L_1 \bowtie L_2| = \frac{|L_1| \times |L_2|}{q^u}$$

$$P = \frac{\binom{n}{n-w}}{\binom{n-2k}{n-w-z}\binom{k}{z/2}^2}$$

Comparison with KMP



Comparison with KMP for higher t



Conclusion

PERK was submitted to the NIST on-ramp call for digital signatures with the following augmented team:

Najwa Aaraj, Technology Innovation Institute, UAE

Slim Bettaieb, Technology Innovation Institute, UAE

Loïc Bidoux, Technology Innovation Institute, UAE

Alessandro Budroni, Technology Innovation Institute, UAE

Victor Dyseryn, XLIM, University of Limoges, France

Andre Esser, Technology Innovation Institute, UAE

Philippe Gaborit, XLIM, University of Limoges, France

Mukul Kulkarni, Technology Innovation Institute, UAE

Victor Mateu, Technology Innovation Institute, UAE

Marco Palumbi, Technology Innovation Institute, UAE

Lucas Perin, Technology Innovation Institute, UAE

Jean-Pierre Tillich, INRIA, Paris, France

Perspectives

- Combinatorial attacks
  - Refine our attack
  - Exploit the multiple instances directly in KMP?
- Algebraic attacks
  - Modelling of permutations in a PhD thesis [Sae17]
  - Polynomial attack when mt is sufficiently high (ongoing work)
  - No efficient attack derived so far in the typical regime
  - Work in progress

Questions?

Thank you for your attention !

https://pqc-perk.org

References I

- Thierry Baritaud, Mireille Campana, Pascal Chauvaud, and Henri Gilbert.
  On the security of the permuted kernel identification scheme.
  In Ernest F. Brickell, editor, CRYPTO'92, volume 740 of LNCS, pages 305–311. Springer, Heidelberg, August 1993.

- Ward Beullens.
  Sigma protocols for MQ, PKP and SIS, and Fishy signature schemes.
  In Anne Canteaut and Yuval Ishai, editors, EUROCRYPT 2020, Part III, volume 12107 of LNCS, pages 183–211. Springer, Heidelberg, May 2020.

References II

Loïc Bidoux and Philippe Gaborit.
Compact post-quantum signatures from proofs of knowledge leveraging structure for the PKP, SD and RSD problems.
In Codes, Cryptology and Information Security (C2SI), pages 10–42. Springer, 2022.

Thibauld Feneuil.
Building MPCitH-based signatures from MQ, MinRank, rank SD and PKP.
Cryptology ePrint Archive, Report 2022/1512, 2022.
https://eprint.iacr.org/2022/1512.

Jean Georgiades.
Some remarks on the security of the identification scheme based on permuted kernels.
Journal of Cryptology, 5(2):133–137, January 1992.

Éliane Jaulmes and Antoine Joux.
Cryptanalysis of PKP: A new approach.
In Kwangjo Kim, editor, PKC 2001, volume 1992 of LNCS, pages 165–172. Springer, Heidelberg, February 2001.

Eliane Koussa, Gilles Macario-Rat, and Jacques Patarin.
On the complexity of the permuted kernel problem.
Cryptology ePrint Archive, Report 2019/412, 2019.
https://eprint.iacr.org/2019/412.

Daniel Kales and Greg Zaverucha.
An attack on some signature schemes constructed from five-pass identification schemes.
In Stephan Krenn, Haya Shulman, and Serge Vaudenay, editors, CANS 20, volume 12579 of LNCS, pages 3–22. Springer, Heidelberg, December 2020.

References IV

Jacques Patarin and Pascal Chauvaud.
Improved algorithms for the permuted kernel problem.
In Douglas R. Stinson, editor, CRYPTO'93, volume 773 of LNCS, pages 391–402. Springer, Heidelberg, August 1994.

Mohamed Ahmed Saeed.
Algebraic approach for code equivalence.
PhD thesis, Normandie Université; University of Khartoum, 2017.

Adi Shamir.
An efficient identification scheme based on permuted kernels (extended abstract) (rump session).
In Gilles Brassard, editor, CRYPTO'89, volume 435 of LNCS, pages 606–609. Springer, Heidelberg, August 1990.