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

GT Codes-Crypto - June 27, 2023

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

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

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

Multi-dimensional IPKP

Definition (IPKP [LP11])

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

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

for all $i \in [1, t]$.

Outline

Outline

MPC-in-the-Head

Generic paradigm by Ishai, Kushilevitz, Ostrovsky, and Sahai [IKOS07, IKOS09].

$$\text{MPC protocol} \implies \text{ZK-proof}$$

1. Prover splits secret and commits to the states;
2. Verifier sends a random challenge γ;
3. Prover simulates locally ("in the head") all the parties, and commits to the views;
4. Verifier chooses a random party i^* and asks to reveal all the views except i^*;
5. Verifier finally checks the views are consistent and with an honest execution of the MPC protocol.

MPC-in-the-Head and PKP

Name	Type	σ size
SUSHYFISH [Beu20]	5-round with helper	$\sim$12 kB
[BG22]	5-round using structure	$\sim$9 kB
[Fen22]	7-round	$\sim$13 kB

Table: Comparison of recent digital signature schemes based on PKP assumptions

Parameters in [BG22]

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

KZ attack cost depends on the challenge space (the number of possibilities for γ).
Increasing the challenge space leads to a decrease in τ.

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

Our parameters

Parameter Set	PKP parameters					MPC param.		pk size	σ size
	λ	q	n	m	t	N	τ		
[BG22]-fast	128	997	61	38	1	32	42	0.15 kB	9.90 kB
[BG22]-short	128	997	61	38	1	256	31	0.24 kB	8.81 kB
PERK-I-fast3	128	1021	79	35	3	32	30	0.15 kB	8.35 kB
PERK-I-fast5	128	1021	83	36	5	32	28	0.24 kB	8.03 kB
PERK-I-short3	128	1021	79	35	3	256	20	0.15 kB	6.56 kB
PERK-I-short5	128	1021	83	36	5	256	18	**0.24 kB**	**6.06 kB**
PERK-III-fast3	192	1021	112	54	3	32	46	0.23 kB	18.8 kB
PERK-III-fast5	192	1021	116	55	5	32	43	0.37 kB	18.0 kB
PERK-III-short3	192	1021	112	54	3	256	31	0.23 kB	15.0 kB
PERK-III-short5	192	1021	116	55	5	256	28	0.37 kB	13.8 kB
PERK-V-fast3	256	1021	146	75	3	32	61	0.31 kB	33.3 kB
PERK-V-fast5	256	1021	150	76	5	32	57	0.51 kB	31.7 kB
PERK-V-short3	256	1021	146	75	3	256	41	0.31 kB	26.4 kB
PERK-V-short5	256	1021	150	76	5	256	37	0.51 kB	24.2 kB

Table: Parameters of PERK signature scheme

Performances

Parameter Set	Keygen	Sign	Verify
PERK-I-fast3	77 k	7.6 M	5.3 M
PERK-I-fast5	88 k	7.2 M	5.1 M
PERK-I-short3	80 k	39 M	27 M
PERK-I-short5	92 k	36 M	25 M
PERK-III-fast3	167 k	16 M	13 M
PERK-III-fast5	184 k	15 M	12 M
PERK-III-short3	174 k	82 M	65 M
PERK-III-short5	194 k	77 M	60 M
PERK-V-fast3	297 k	36 M	28 M
PERK-V-fast5	322 k	34 M	27 M
PERK-V-short3	299 k	184 M	142 M
PERK-V-short5	329 k	170 M	131 M

Table: Performances of our implementation for different instances of PERK. The key generation numbers are in kilo CPU cycles, while the signing and verification numbers are in million CPU cycles.

Outline

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 $\max(1, \frac{n!}{q^m})$.

$\Longrightarrow$ equivalent to Gilbert-Varshamov bound

Georgiades algorithm [Geo92]

$$\begin{pmatrix} I_m & H' \end{pmatrix} \begin{pmatrix} x_1 \\ \hline x_2 \end{pmatrix} = y$$

$$x_1 = y - H' x_2$$

$\Rightarrow$ enumerate x_2 as every subpermutation of x of size $n - m$.

Georgiades algorithm [Geo92]

Proposition (Complexity)

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

$\Longrightarrow$ equivalent to Prange

Time-memory trade-off

$$\begin{pmatrix} \boldsymbol{H}_1 & \boldsymbol{H}_2 \end{pmatrix} \begin{pmatrix} \boldsymbol{x}_1 \\ \hline \boldsymbol{x}_2 \end{pmatrix} = \boldsymbol{y}$$

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

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

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

Time-memory trade-off

Proposition (Complexity)

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

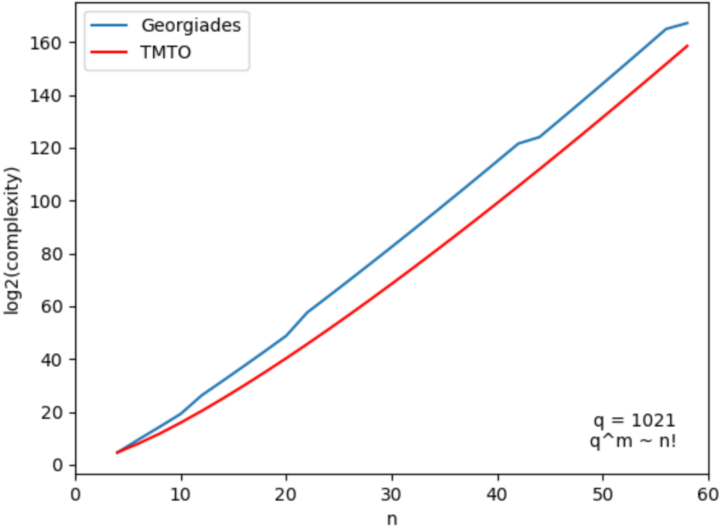
with

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

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

$\Longrightarrow$ equivalent to Birthday Decoding

Comparison


Georgiades
TMTO
log2(complexity)
n
q = 1021
q^m ~ 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

$$\begin{pmatrix} \boldsymbol{I}_{m-u} & \multicolumn{2}{c}{\boldsymbol{H}'} \\ \boldsymbol{0} & \boldsymbol{H}_2 & \boldsymbol{H}_3 \end{pmatrix} \begin{pmatrix} \boldsymbol{x}_1 \\ \hline \boldsymbol{x}_2 \\ \hline \boldsymbol{x}_3 \end{pmatrix} = \begin{pmatrix} \boldsymbol{y}_1 \\ \boldsymbol{y}_2 \end{pmatrix}$$

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

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

KMP algorithm [KMP19]

Proposition (Complexity)

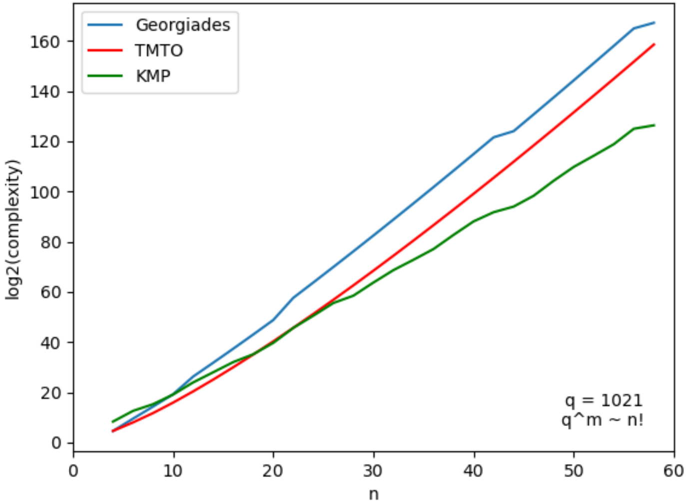
$$\mathcal{T} = \mathcal{O}\left(|L_1| + |L_2| + |L_1 \bowtie L_2|\right)$$

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]

Outline

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

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 $\langle \boldsymbol{x}_1, \ldots, \boldsymbol{x}_t \rangle$,

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

  of weight w.
- Define

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

  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

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

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

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

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

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

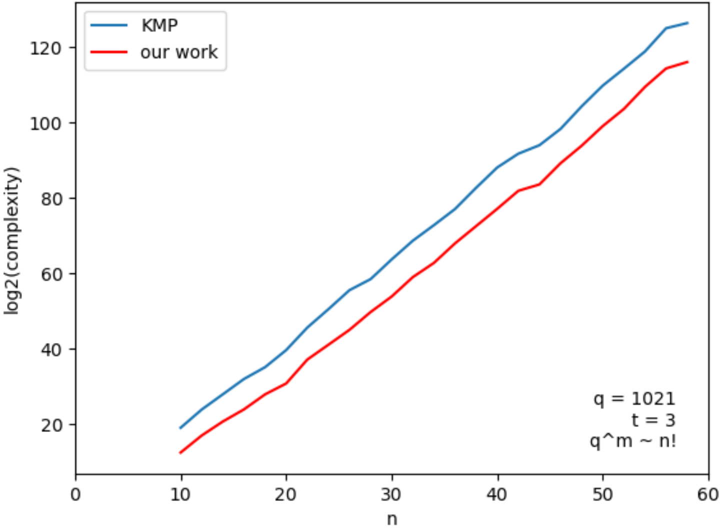
$$k = (n - m + u)/2\,,\; z \leq n - w$$

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

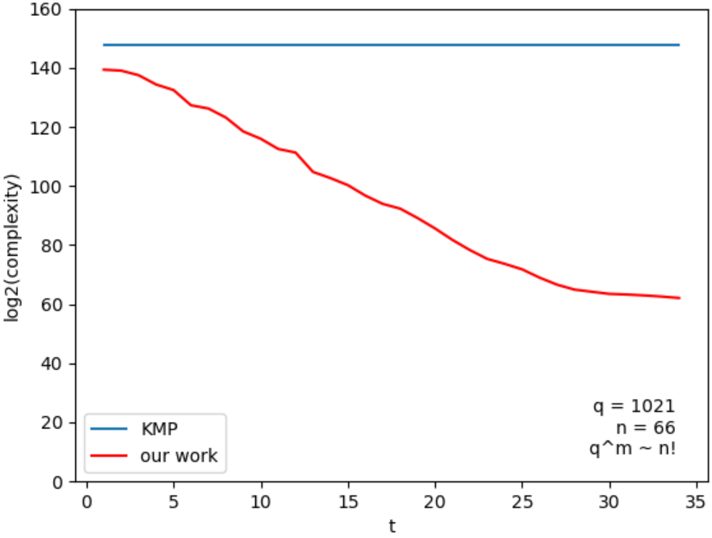
$$|L_1 \bowtie L_2| = \frac{|L_1| \times |L_2|}{q^u}$$

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

Comparison with KMP



Comparison with KMP for higher t



Outline

Multi-dimensional IPKP

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

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

for all $i \in [1, t]$.

Number of solutions

Proposition

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

$$\frac{n!}{q^{mt}}$$

$\mathrm{IPKP}_{q,m,n,1}$	$\text{r-IPKP}_{q,m,n,t}$	$\mathrm{IPKP}_{q,m,n,t}$
$\frac{n!}{q^m}$	$\frac{n!}{q^m} \cdot \frac{q^t-1}{q-1}$	$\frac{n!}{q^{mt}}$

Why do we need to consider multi-dimensional IPKP?

Normally with a random instance there is no solution for our parameters.
However, for the signature protocol there exists a permutation π that is a solution to multi-dimensional IPKP.

KMP algorithm, multi-dimensional

Only the size of $L_1 \bowtie L_2$ changes.

Proposition (Complexity)

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

with

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

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

SBC algorithm [SBC22]

KMP algorithm with ISD.

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

Link between **homogeneous** PKP and SEP [SBC22]

Definition (Permutation/Subcode Equivalence Problem (PEP/SEP))

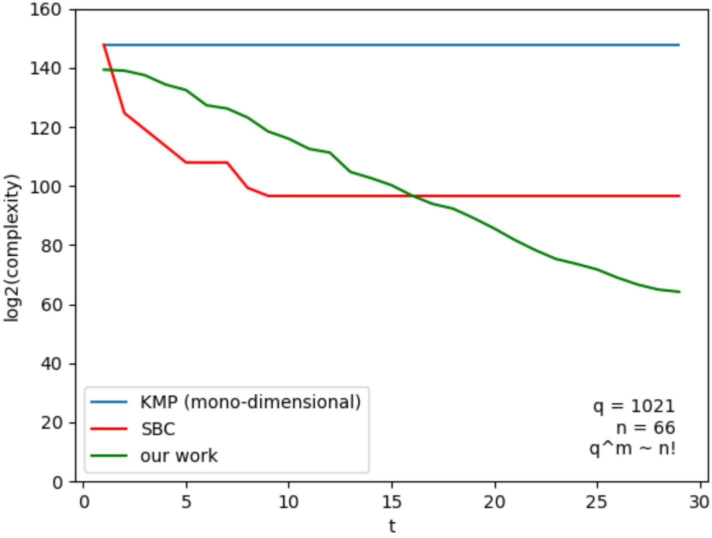
Let $k' \leq k \leq n$. Given two codes $\mathcal{C}[n, k]$ and $\mathcal{C}'[n, k']$, does there exists a permutation π such that

$$\pi[\mathcal{C}'] \subseteq \mathcal{C}?$$

IPKP	Equivalent problem	Parameters
$t < n - m$	SEP	$k = n - m, k' = t$
$t = n - m$	PEP	$k = k' = n - m$
$t > n - m$	SEP	$k = t, k' = n - m$

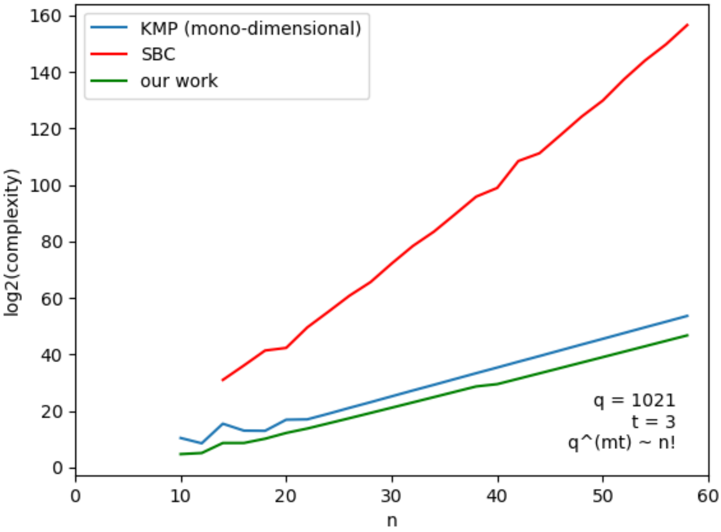
Table: Relations between PKP, SEP and PEP, and corresponding parameters

Comparison

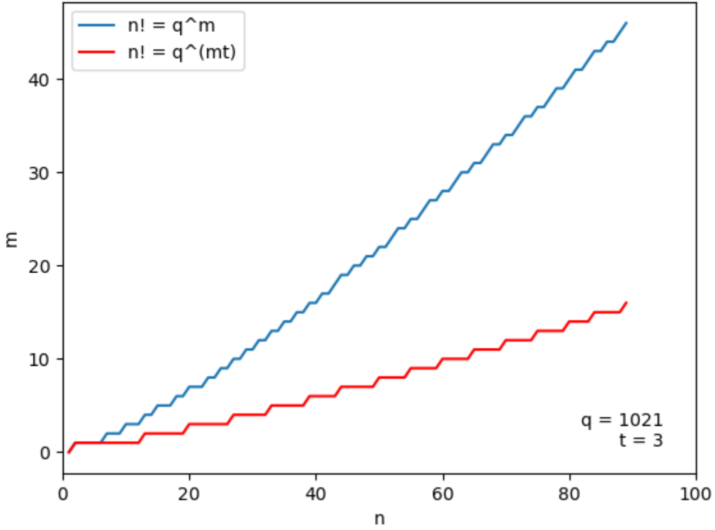

160
140
120
100
80
60
40
20
0
log2(complexity)
0
5
10
15
20
25
30
t
KMP (mono-dimensional)
SBC
our work
q = 1021
n = 66
q^m ~ n!

Outline

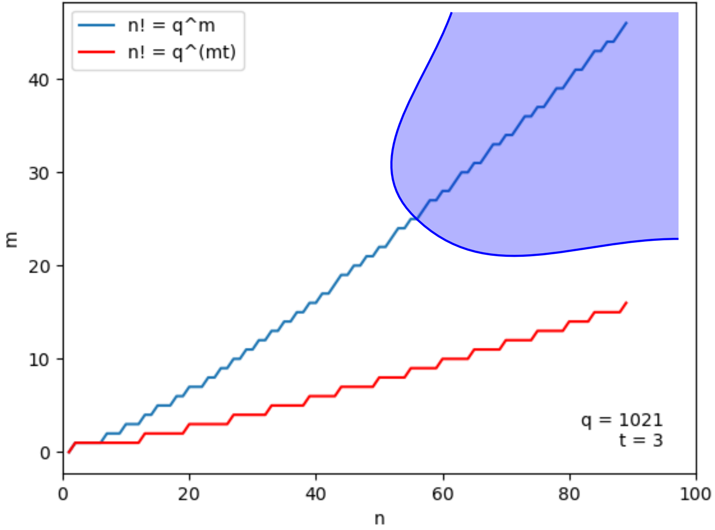
What happens with a different density?



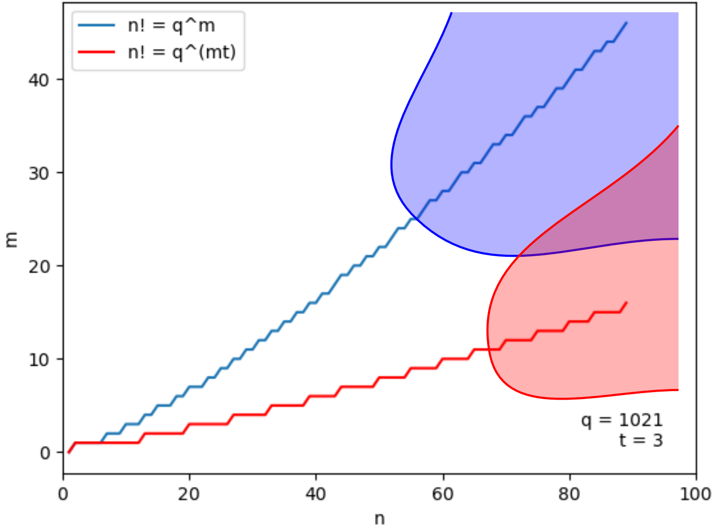
Mitigating both attacks



Mitigating both attacks



Mitigating both attacks



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

Thank you for your attention !

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.

References III

Yuval Ishai, Eyal Kushilevitz, Rafail Ostrovsky, and Amit Sahai.
Zero-knowledge from secure multiparty computation.
In David S. Johnson and Uriel Feige, editors, 39th ACM STOC, pages 21–30. ACM Press, June 2007.

Yuval Ishai, Eyal Kushilevitz, Rafail Ostrovsky, and Amit Sahai.
Zero-knowledge proofs from secure multiparty computation.
SIAM Journal on Computing, 39(3):1121–1152, 2009.

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.

References IV

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.

Rodolphe Lampe and Jacques Patarin.
Analysis of some natural variants of the pkp algorithm.
Cryptology ePrint Archive, 2011.

References V

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.

Paolo Santini, Marco Baldi, and Franco Chiaraluce.
Computational hardness of the permuted kernel and subcode equivalence problems.
Cryptology ePrint Archive, Report 2022/1749, 2022.
https://eprint.iacr.org/2022/1749.

References VI

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.