A New Perspective on Key Switching for BGV-like Schemes

Johannes Mono, Tim Güneysu

February 22, 2024

The homomorphic quest

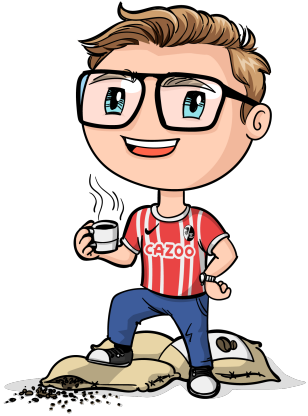
SECURITY ENGINEERING

What even is this key switching thingy?

Why should I care about improving it?

Okay, fine. How can we improve it?

Hi!



- I do crypto research
- I like football
- I like coffee
- I love food

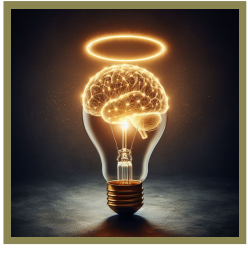
SECURITY ENGINEERING

Why repackaging food is really annoying and how to improve it

Johannes Mono, Tim Güneysu

February 22, 2024

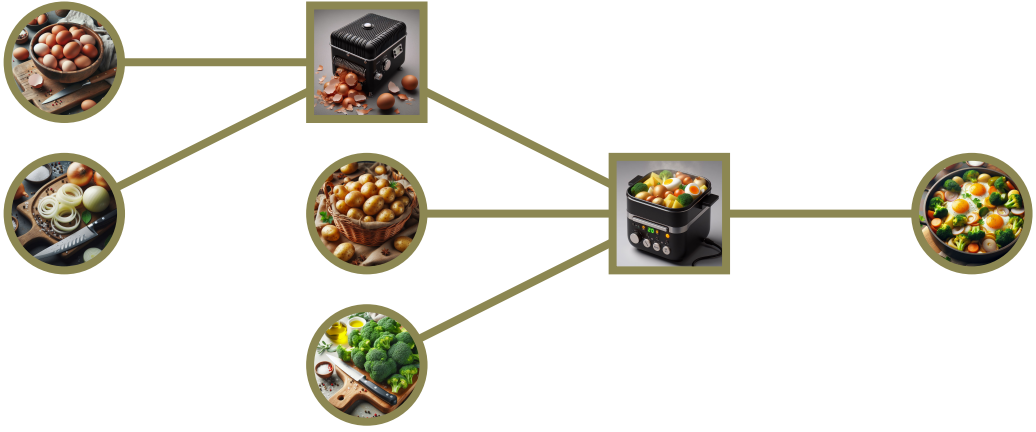
A foody inspiration



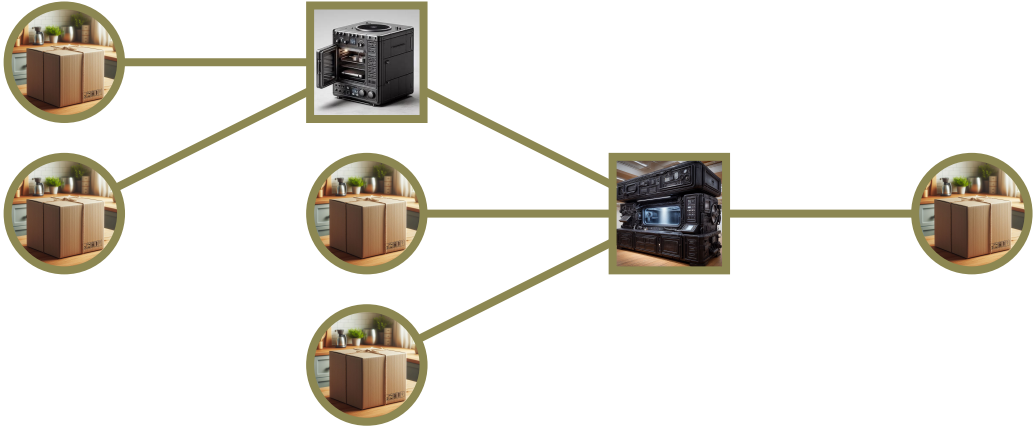
Food: Hot & Easy

Sends us your ingredients and recipe, receive your food - hot & easy!

Outsourcing our stew pot



Keeping our ingredients secret



Cooking up metaphors

Packing up an ingredient

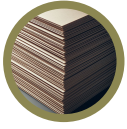
RLWE: Learning with Errors over the ring $\mathcal{R}_q = \mathbb{Z}_q[X]/(X^N + 1)$

$$a \leftarrow R_q, \quad s \leftarrow \chi_s, \quad e \leftarrow \chi_e, \quad m \leftarrow \mathcal{R}_p$$

$-a \cdot s$

e

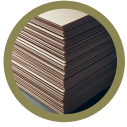
m



a

$-a \cdot s + e + m$

Unpacking the food



a $\quad -a \cdot s + e + m$ $\quad s$


$m + e$ $\quad m$

$(c_0, c_1) = (-a \cdot s + e + m, a)$ $\quad \rightarrow \quad c(s) = c_0 + c_1 \cdot s$

Cooking homomorphically

$c(s)$

(c_0, c_1)

$c'(s)$

(c'_0, c'_1)

$+$

$(c + c')(s)$

$(c_0 + c'_0, c_1 + c'_1)$

Cooking homomorphically, but in annoying

$c(s)$

(c_0, c_1)

$c'(s)$

(c'_0, c'_1)

$\boxdot$

$(c \cdot c')(s)$

$(c_0 \cdot c'_0, c_0 \cdot c'_1 + c_1 \cdot c'_0, c_1 \cdot c'_1)$

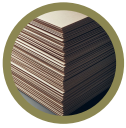
Repackaging the food

(c_0, c_1, c_2) $\qquad$ $(c_0 + \widetilde{c}_0, c_1 + \widetilde{c}_1)$

$c_2 \cdot s^2$ $\qquad$ $\widetilde{c}_0 + \widetilde{c}_1 \cdot s + e$

A special ingredient






$-a \cdot s$ e s^2 a $-a \cdot s + e + s^2$

$$\mathsf{ksk} = \left(\mathsf{ksk}_0, \mathsf{ksk}_1\right) = \left(-a \cdot s + e + s^2, a\right)$$

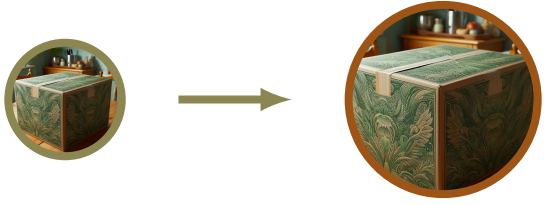
Using our special ingredient

$$
\begin{aligned}
\big(c_2 \cdot \mathsf{ksk}\big)(s) &= c_2 \cdot \mathsf{ksk}_0 + c_2 \cdot \mathsf{ksk}_1 \cdot s \\
&= c_2 \cdot \big(-a \cdot s + e + s^2 \big) + c_2 \cdot a \cdot s \\
&= c_2 \cdot s^2 + c_2 \cdot e
\end{aligned}
$$

Using our special ingredient. Well, almost.

$$
\begin{aligned}
\big(c_2 \cdot \mathsf{ksk}\big)(s) &= c_2 \cdot \mathsf{ksk}_0 + c_2 \cdot \mathsf{ksk}_1 \cdot s \\
&= c_2 \cdot \big(-a \cdot s + e + s^2 \big) + c_2 \cdot a \cdot s \\
&= c_2 \cdot s^2 + c_2 \cdot e \\
&\leq ||\mathcal{R}_q \cdot e||
\end{aligned}
$$

Plugging the leak with modulus extension



$\mathcal{R}_q$ $\mathcal{R}_{qP}$

$$\mathsf{ksk} = \left(\mathsf{ksk}_0, \mathsf{ksk}_1\right) = \left(-a \cdot s + e + Ps^2, a\right)$$

Plugging the leak with modulus extension

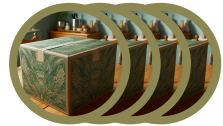
$$
\begin{aligned}
\tfrac{1}{P}\big(c_2 \cdot \mathsf{ksk}\big)(s) &= \tfrac{1}{P}\big(c_2 \cdot \mathsf{ksk}_0 + c_2 \cdot \mathsf{ksk}_1 \cdot s\big) \\
&= \tfrac{1}{P} c_2 \cdot \big(-a \cdot s + e + P s^2\big) + \tfrac{1}{P} c_2 \cdot a \cdot s \\
&= c_2 \cdot s^2 + \tfrac{c_2}{P} \cdot e \\
&\leq \tfrac{||\mathcal{R}_q \cdot e||}{P}
\end{aligned}
$$

Plugging the leak with decomposition

$\mathcal{D}$

$\mathcal{R}_q$ $\xrightarrow{\omega = 4}$ $(\mathcal{R}_\beta)^\omega$

$$c_2 = \beta^3 c_2^{(3)} + \beta^2 c_2^{(2)} + \beta c_2^{(1)} + c_2^{(0)}$$



$$\mathsf{ksk}_0 = \begin{cases} -a^{(0)} \cdot s + e^{(0)} + s^2 \\ -a^{(1)} \cdot s + e^{(1)} + \beta s^2 \\ -a^{(2)} \cdot s + e^{(2)} + \beta^2 s^2 \\ -a^{(3)} \cdot s + e^{(3)} + \beta^3 s^2 \end{cases}$$

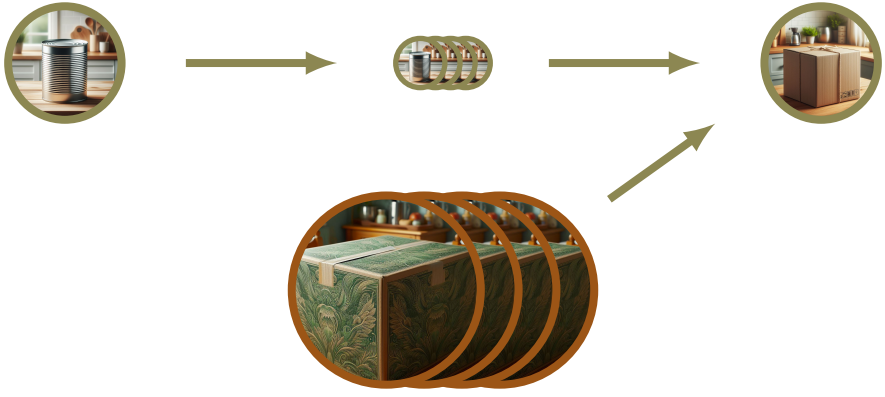
Plugging the leak with decomposition

$$
\begin{aligned}
\langle \mathcal{D}(c_2), \mathsf{ksk} \rangle(s) &= \langle \mathcal{D}(c_2), \mathsf{ksk}_0 \rangle + \langle \mathcal{D}(c_2), \mathsf{ksk}_1 \rangle \cdot s \\
&= \langle c_2^{(k)}, -a^{(k)} \cdot s + e^{(k)} + \beta^k s^2 \rangle + \langle c_2^{(k)}, a^{(k)} \rangle \cdot s \\
&= c_2 \cdot s^2 + \langle c_2^{(k)}, e^{(k)} \rangle \\
&\qquad \leq \omega \cdot ||\mathcal{R}_\beta \cdot e^{(k)}||
\end{aligned}
$$

Plugfusing our special ingredient

$$\mathsf{ksk} = \begin{cases} \left(-a^{(0)}s + e^{(0)} + Ps^2, a^{(0)}\right) \\ \left(-a^{(1)}s + e^{(1)} + \beta Ps^2, a^{(1)}\right) \\ \left(-a^{(2)}s + e^{(2)} + \beta^2 Ps^2, a^{(2)}\right) \\ \left(-a^{(3)}s + e^{(3)} + \beta^3 Ps^2, a^{(3)}\right) \end{cases}$$

Using our special ingredient. This time for real.



Using our special ingredient. This time for real.

$$\frac{1}{P}\langle \mathcal{D}(c_2), \mathsf{ksk}\rangle(s) = \frac{1}{P}\left(\langle \mathcal{D}(c_2), \mathsf{ksk}_0\rangle + \langle \mathcal{D}(c_2), \mathsf{ksk}_1\rangle \cdot s\right)$$

$$= \frac{1}{P}\left(\langle c_2^{(k)}, -a^{(k)} \cdot s + e^{(k)} + \beta^k s^2\rangle + \langle c_2^{(k)}, a^{(k)}\rangle \cdot s\right)$$

$$= c_2 s^2 + \frac{\langle c_2^{(k)}, e^{(k)}\rangle}{P}$$

$$\leq \omega \cdot \frac{||\mathcal{R}_\beta \cdot e^{(k)}||}{P}$$

On our journey, one step at a time

SECURITY ENGINEERING

What even is this key switching thingy?

Why should I care about improving it?

Okay, fine. How can we improve it?

Why key switching is really annoying

SECURITY ENGINEERING

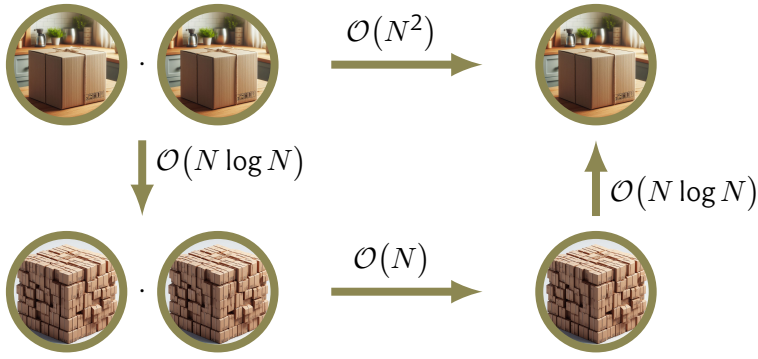
- We need it after every multiplication or rotation.
- It is really slow:
  - How relevant is it to bootstrapping?
  - How relevant to a matrix multiplication?
  - How much slower is it compared to a multiplication?

Why key switching is really annoying

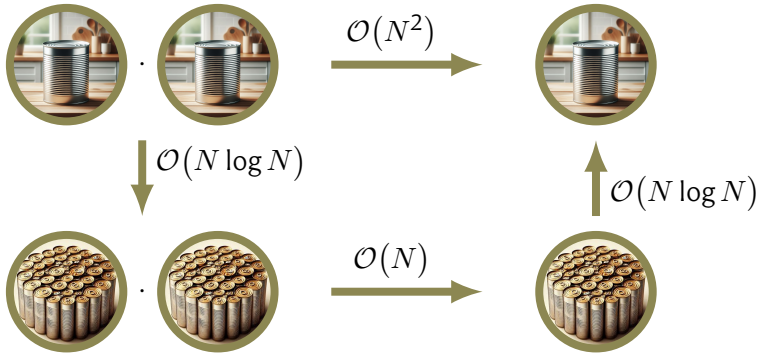
SECURITY ENGINEERING

- We need it after every multiplication or rotation.
- It is really slow:
  - How relevant is it to bootstrapping? $\approx 40\%$
  - How relevant to a matrix multiplication? $> 50\%$
  - How much slower is it compared to a multiplication? $\approx 11\times$

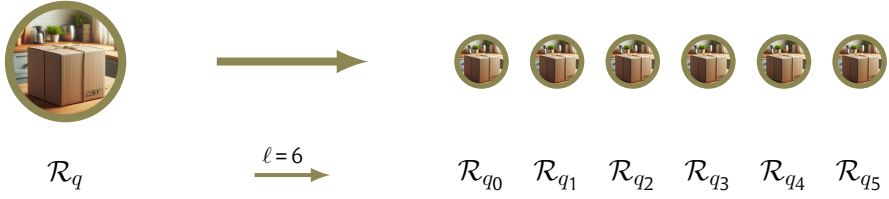
Package theoretic transform



Can theoretic transform



Residue package system



Repackaging parameters

SECURITY ENGINEERING

$\omega = 1$

$P \approx q_i^6$

$\omega = 2$

$P \approx q_i^3$

$\omega = 3$

$P \approx q_i^2$

$\omega = 6$

$P \approx q_i$

Repackaging food surely, but slowly

$\mathcal{R}_{q_0}$	$c_2^{(0)}$
$\mathcal{R}_{q_1}$	$c_2^{(0)}$
$\mathcal{R}_{q_2}$	$c_2^{(1)}$
$\mathcal{R}_{q_3}$	$c_2^{(1)}$

$\mathcal{R}_{P_0}$

$\mathcal{R}_{P_1}$

Repackaging food surely, but slowly


$\mathcal{R}_{q_0}$	$c_2^{(0)}$	$\left(c_2^{(0)}, c_2^{(1)}\right)$
$\mathcal{R}_{q_1}$	$c_2^{(0)}$	$\left(c_2^{(0)}, c_2^{(1)}\right)$
$\mathcal{R}_{q_2}$	$c_2^{(1)}$	$\left(c_2^{(0)}, c_2^{(1)}\right)$
$\mathcal{R}_{q_3}$	$c_2^{(1)}$	$\left(c_2^{(0)}, c_2^{(1)}\right)$
$\mathcal{R}_{P_0}$		$\left(c_2^{(0)}, c_2^{(1)}\right)$
$\mathcal{R}_{P_1}$		$\left(c_2^{(0)}, c_2^{(1)}\right)$

Repackaging food surely, but slowly



$\mathcal{R}_{q_0}$	$c_2^{(0)}$	$(c_2^{(0)}, c_2^{(1)})$	$(c_2^{(0)}, c_2^{(1)})$
$\mathcal{R}_{q_1}$	$c_2^{(0)}$	$(c_2^{(0)}, c_2^{(1)})$	$(c_2^{(0)}, c_2^{(1)})$
$\mathcal{R}_{q_2}$	$c_2^{(1)}$	$(c_2^{(0)}, c_2^{(1)})$	$(c_2^{(0)}, c_2^{(1)})$
$\mathcal{R}_{q_3}$	$c_2^{(1)}$	$(c_2^{(0)}, c_2^{(1)})$	$(c_2^{(0)}, c_2^{(1)})$
$\mathcal{R}_{P_0}$		$(c_2^{(0)}, c_2^{(1)})$	$(c_2^{(0)}, c_2^{(1)})$
$\mathcal{R}_{P_1}$		$(c_2^{(0)}, c_2^{(1)})$	$(c_2^{(0)}, c_2^{(1)})$

Repackaging food surely, but slowly






$\mathcal{R}_{q_0}$	$c_2^{(0)}$	$(c_2^{(0)}, c_2^{(1)})$	$(c_2^{(0)}, c_2^{(1)})$	$\left\langle (c_2^{(0)}, c_2^{(1)}), \mathsf{ksk}_i \right\rangle = c_i'$
$\mathcal{R}_{q_1}$	$c_2^{(0)}$	$(c_2^{(0)}, c_2^{(1)})$	$(c_2^{(0)}, c_2^{(1)})$	$\left\langle (c_2^{(0)}, c_2^{(1)}), \mathsf{ksk}_i \right\rangle = c_i'$
$\mathcal{R}_{q_2}$	$c_2^{(1)}$	$(c_2^{(0)}, c_2^{(1)})$	$(c_2^{(0)}, c_2^{(1)})$	$\left\langle (c_2^{(0)}, c_2^{(1)}), \mathsf{ksk}_i \right\rangle = c_i'$
$\mathcal{R}_{q_3}$	$c_2^{(1)}$	$(c_2^{(0)}, c_2^{(1)})$	$(c_2^{(0)}, c_2^{(1)})$	$\left\langle (c_2^{(0)}, c_2^{(1)}), \mathsf{ksk}_i \right\rangle = c_i'$
$\mathcal{R}_{P_0}$		$(c_2^{(0)}, c_2^{(1)})$	$(c_2^{(0)}, c_2^{(1)})$	$\left\langle (c_2^{(0)}, c_2^{(1)}), \mathsf{ksk}_i \right\rangle = c_i'$
$\mathcal{R}_{P_1}$		$(c_2^{(0)}, c_2^{(1)})$	$(c_2^{(0)}, c_2^{(1)})$	$\left\langle (c_2^{(0)}, c_2^{(1)}), \mathsf{ksk}_i \right\rangle = c_i'$

Repackaging food surely, but slowly







$\mathcal{R}_{q_0}$	$c_2^{(0)}$	$(c_2^{(0)}, c_2^{(1)})$	$(c_2^{(0)}, c_2^{(1)})$	$\left\langle (c_2^{(0)}, c_2^{(1)}), \mathsf{ksk}_i \right\rangle = c'_i$	c'_i
$\mathcal{R}_{q_1}$	$c_2^{(0)}$	$(c_2^{(0)}, c_2^{(1)})$	$(c_2^{(0)}, c_2^{(1)})$	$\left\langle (c_2^{(0)}, c_2^{(1)}), \mathsf{ksk}_i \right\rangle = c'_i$	c'_i
$\mathcal{R}_{q_2}$	$c_2^{(1)}$	$(c_2^{(0)}, c_2^{(1)})$	$(c_2^{(0)}, c_2^{(1)})$	$\left\langle (c_2^{(0)}, c_2^{(1)}), \mathsf{ksk}_i \right\rangle = c'_i$	c'_i
$\mathcal{R}_{q_3}$	$c_2^{(1)}$	$(c_2^{(0)}, c_2^{(1)})$	$(c_2^{(0)}, c_2^{(1)})$	$\left\langle (c_2^{(0)}, c_2^{(1)}), \mathsf{ksk}_i \right\rangle = c'_i$	c'_i
$\mathcal{R}_{P_0}$		$(c_2^{(0)}, c_2^{(1)})$	$(c_2^{(0)}, c_2^{(1)})$	$\left\langle (c_2^{(0)}, c_2^{(1)}), \mathsf{ksk}_i \right\rangle = c'_i$	c'_i
$\mathcal{R}_{P_1}$		$(c_2^{(0)}, c_2^{(1)})$	$(c_2^{(0)}, c_2^{(1)})$	$\left\langle (c_2^{(0)}, c_2^{(1)}), \mathsf{ksk}_i \right\rangle = c'_i$	c'_i

Repackaging food surely, but slowly










$\mathcal{R}_{q_0}$	$c_2^{(0)}$	$(c_2^{(0)}, c_2^{(1)})$	$(c_2^{(0)}, c_2^{(1)})$	$\left\langle (c_2^{(0)}, c_2^{(1)}), \mathsf{ksk}_i \right\rangle = c'_i$	c'_i	$\frac{1}{P}(c'_i + \delta_i) = \widetilde{c}_i$
$\mathcal{R}_{q_1}$	$c_2^{(0)}$	$(c_2^{(0)}, c_2^{(1)})$	$(c_2^{(0)}, c_2^{(1)})$	$\left\langle (c_2^{(0)}, c_2^{(1)}), \mathsf{ksk}_i \right\rangle = c'_i$	c'_i	$\frac{1}{P}(c'_i + \delta_i) = \widetilde{c}_i$
$\mathcal{R}_{q_2}$	$c_2^{(1)}$	$(c_2^{(0)}, c_2^{(1)})$	$(c_2^{(0)}, c_2^{(1)})$	$\left\langle (c_2^{(0)}, c_2^{(1)}), \mathsf{ksk}_i \right\rangle = c'_i$	c'_i	$\frac{1}{P}(c'_i + \delta_i) = \widetilde{c}_i$
$\mathcal{R}_{q_3}$	$c_2^{(1)}$	$(c_2^{(0)}, c_2^{(1)})$	$(c_2^{(0)}, c_2^{(1)})$	$\left\langle (c_2^{(0)}, c_2^{(1)}), \mathsf{ksk}_i \right\rangle = c'_i$	c'_i	$\frac{1}{P}(c'_i + \delta_i) = \widetilde{c}_i$
$\mathcal{R}_{P_0}$		$(c_2^{(0)}, c_2^{(1)})$	$(c_2^{(0)}, c_2^{(1)})$	$\left\langle (c_2^{(0)}, c_2^{(1)}), \mathsf{ksk}_i \right\rangle = c'_i$	c'_i	
$\mathcal{R}_{P_1}$		$(c_2^{(0)}, c_2^{(1)})$	$(c_2^{(0)}, c_2^{(1)})$	$\left\langle (c_2^{(0)}, c_2^{(1)}), \mathsf{ksk}_i \right\rangle = c'_i$	c'_i	

Another step for food repackaging awaits us

SECURITY ENGINEERING

What even is this key switching thingy?

Why should I care about improving it?

Okay, fine. How can we improve it?

Best food repackaging in town

Kim, Polyakov, Zucca: Revisiting Homomorphic Encryption Schemes for Finite Fields

- Extensive summary of key switching with all known variants
- Computational analysis, but no complexity or parameter analysis

Kim, Lee, Seo, Song: Accelerating HE Operations from Key Decomposition Technique

- Non-optimal complexity analysis (leading to wrong conclusions)
- Double-decomposition technique for key switching

Our improvements

- A new perspective on key switching
- Simple guidelines for optimal key switching parameters
- Introducing and revisiting ideas for better parameters
- Reducing the number of multiplications in key switching
- Improved analysis for the double-decomposition technique

The old perspective

SECURITY ENGINEERING

Kim, Lee, Seo, Song:

$(\omega + 2)\ (\ell + k)$

ℓ: number of primes in q

k: number of primes in P

ω: decomposition number

$$
\begin{aligned}
& k \in \mathcal{O}(1) \\
\Rightarrow\quad & \omega \in \mathcal{O}(\ell) \\
\Rightarrow\quad & \mathcal{O}(\ell^2)
\end{aligned}
$$

A new perspective

SECURITY ENGINEERING

Our Perspective:

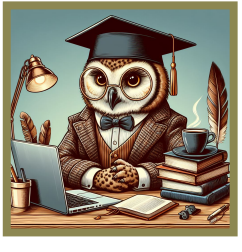
$(\omega + 2)\ (\ell + k)\ \mathcal{O}(N \log N)$

ℓ: number of primes in q

k: number of primes in P

ω: decomposition number

$$
\begin{aligned}
& 1 \leq \omega \leq \ell \\
\Rightarrow\ & k \in \mathcal{O}(\ell/\omega) \\
\Rightarrow\ & \mathcal{O}(\omega\ell\, N \log N)
\end{aligned}
$$



$\mathcal{O}(\omega\ell)$

Kim, Lee, Seo, Song:

$(\omega + 2)\ (\ell + k)$

ℓ: number of primes in q

k: number of primes in P

ω: decomposition number

$$
\begin{aligned}
& k \in \mathcal{O}(1) \\
\Rightarrow\ & \omega \in \mathcal{O}(\ell) \\
\Rightarrow\ & \mathcal{O}(\ell^2)
\end{aligned}
$$

Our guidelines

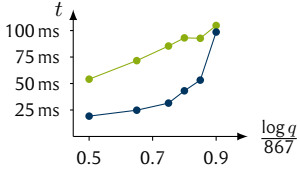
SECURITY ENGINEERING

1. Calculate how large q must be
2. Calculate how small N can be
3. Choose $\omega \geq 2$ as small as possible
4. Choose P accordingly

The double-decomposition technique

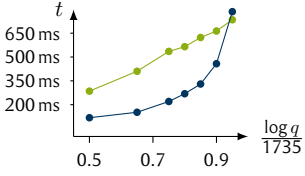
Memory optimum: $\omega = 1$
Computational optimum: $\omega = \ell$

A more comparable comparison



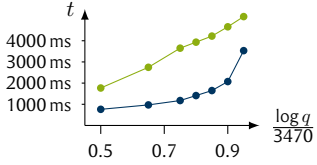
$N = 2^{15}$

$\log q \leq 867$



$N = 2^{16}$

$\log q \leq 1735$



$N = 2^{17}$

$\log q \leq 3470$

- single-decomposition technique
- double-decomposition technique

The end

What even is this key switching thingy?

Why should I care about improving it?

Okay, fine. How can we improve it?

johannes.mono@rub.de

https://eprint.iacr.org/2023/1642