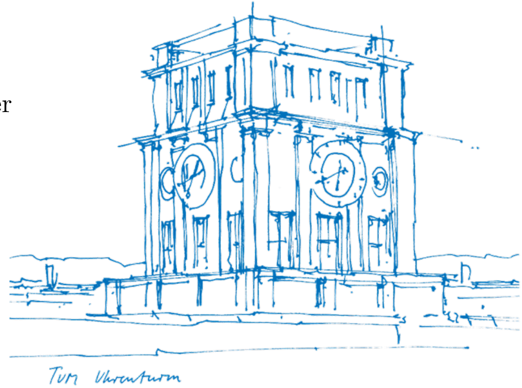
Zero Knowledge Protocols and Signatures from the Restricted Syndrome Decoding Problem

Marco Baldi, Sebastian Bitzer, Alessio Pavoni,

Paolo Santini, Antonia Wachter-Zeh, Violetta Weger

Technical University of Munich
Università Politecnica delle Marche



PKC 2024

CROSS in a Nutshell

CROSS

Codes and Restricted Objects Signature Scheme

CROSS in a Nutshell

CROSS

Codes and Restricted Objects Signature Scheme

CVE-like ZK Protocol

→ simple and efficient

→ standard optimizations

Restricted Decoding Problems

→ related to classical SDP

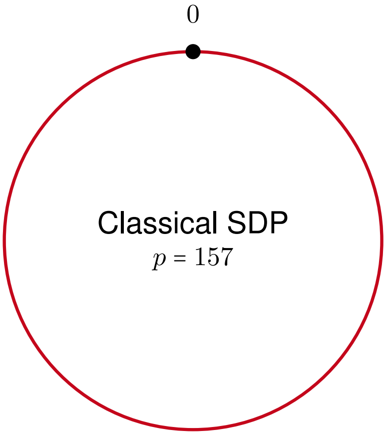
→ enable compact signatures

Restricting SDP

Syndrome Decoding Problem (SDP)

Given: $\boldsymbol{H} \in \mathbb{F}_p^{(n-k)\times n}$, $\boldsymbol{s} \in \mathbb{F}_p^{n-k}$, and $w \in \mathbb{N}$.

Find: $\boldsymbol{e} \in \mathbb{F}_p^n$ with $\boldsymbol{H}\boldsymbol{e} = \boldsymbol{s}$ and $\mathrm{wt}(\boldsymbol{e}) = w$.

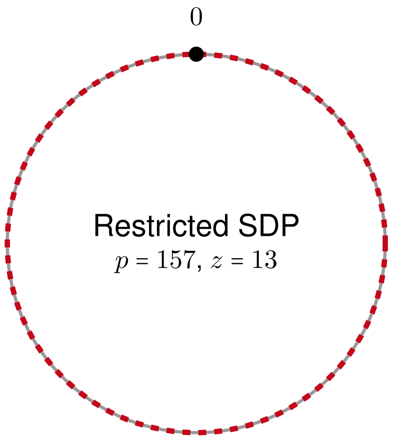


Restricting SDP

Restricted SDP (R-SDP)

Given: $\boldsymbol{H} \in \mathbb{F}_p^{(n-k)\times n}$, $\boldsymbol{s} \in \mathbb{F}_p^{n-k}$, and $w \in \mathbb{N}$,
restriction $\mathbb{E}$ of size $z = |\mathbb{E}|$.

Find: $\boldsymbol{e} \in (\mathbb{E} \cup \{0\})^n$ with $\boldsymbol{He} = \boldsymbol{s}$ and $\mathrm{wt}(\boldsymbol{e}) = w$.

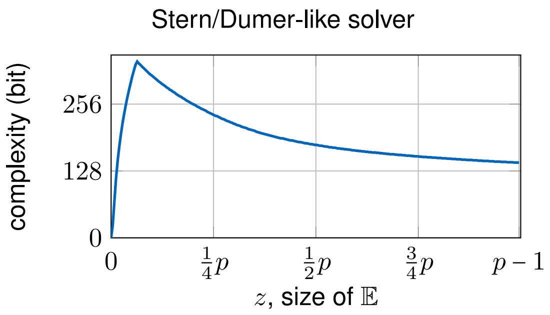


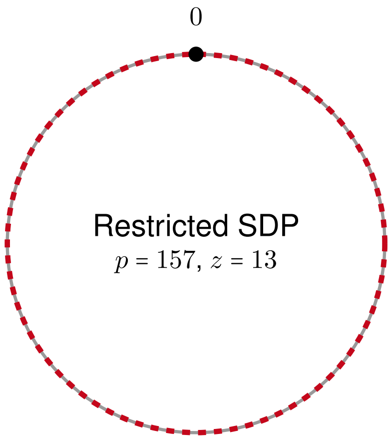
Restricting SDP

Restricted SDP (R-SDP)

Given: $\boldsymbol{H} \in \mathbb{F}_p^{(n-k)\times n}$, $\boldsymbol{s} \in \mathbb{F}_p^{n-k}$, and $w \in \mathbb{N}$,
restriction $\mathbb{E}$ of size $z = |\mathbb{E}|$.

Find: $\boldsymbol{e} \in (\mathbb{E} \cup \{0\})^n$ with $\boldsymbol{H}\boldsymbol{e} = \boldsymbol{s}$ and $\mathrm{wt}(\boldsymbol{e}) = w$.



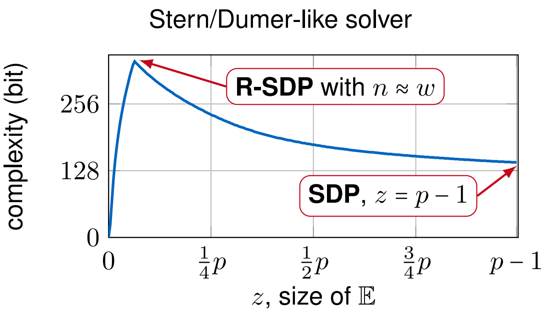


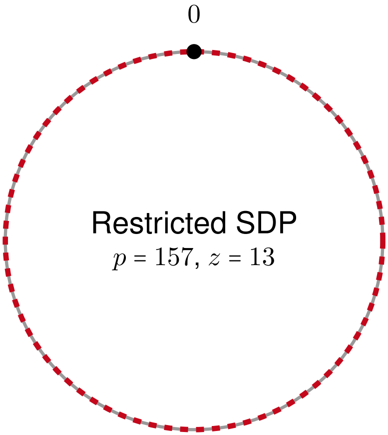
Restricting SDP

Restricted SDP (R-SDP)

Given: $\boldsymbol{H} \in \mathbb{F}_p^{(n-k)\times n}$, $\boldsymbol{s} \in \mathbb{F}_p^{n-k}$, and $w \in \mathbb{N}$,
restriction $\mathbb{E}$ of size $z = |\mathbb{E}|$.

Find: $\boldsymbol{e} \in (\mathbb{E} \cup \{0\})^n$ with $\boldsymbol{H}\boldsymbol{e} = \boldsymbol{s}$ and $\mathrm{wt}(\boldsymbol{e}) = w$.





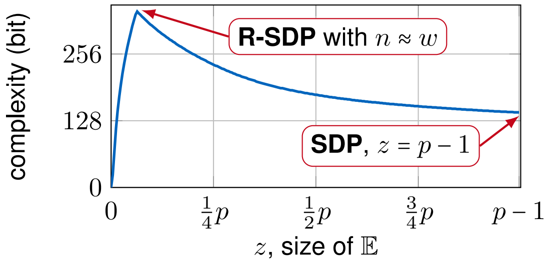
Restricting SDP

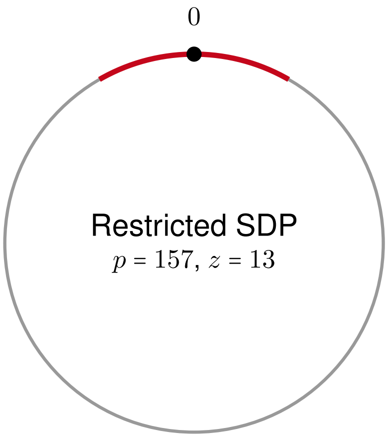
Restricted SDP (R-SDP)

Given: $\boldsymbol{H} \in \mathbb{F}_p^{(n-k)\times n}$, $\boldsymbol{s} \in \mathbb{F}_p^{n-k}$, and $w \in \mathbb{N}$,
restriction $\mathbb{E}$ of size $z = |\mathbb{E}|$.

Find: $\boldsymbol{e} \in (\mathbb{E} \cup \{0\})^n$ with $\boldsymbol{H}\boldsymbol{e} = \boldsymbol{s}$ and $\mathrm{wt}(\boldsymbol{e}) = w$.

Stern/Dumer-like solver



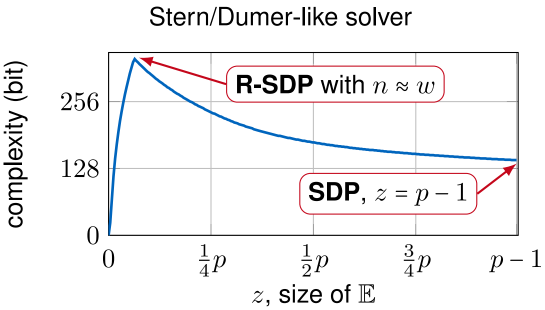


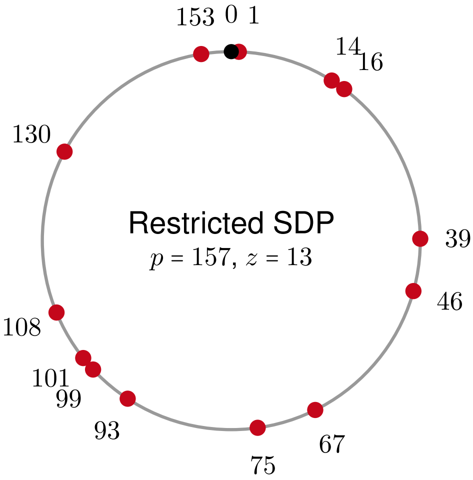
Restricting SDP

Restricted SDP (R-SDP)

Given: $\boldsymbol{H} \in \mathbb{F}_p^{(n-k)\times n}$, $\boldsymbol{s} \in \mathbb{F}_p^{n-k}$, and $w \in \mathbb{N}$,
restriction $\mathbb{E}$ of size $z = |\mathbb{E}|$.

Find: $\boldsymbol{e} \in (\mathbb{E} \cup \{0\})^n$ with $\boldsymbol{H}\boldsymbol{e} = \boldsymbol{s}$ and $\mathrm{wt}(\boldsymbol{e}) = w$.



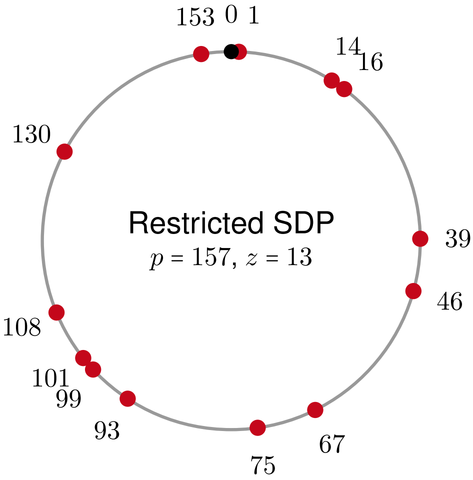


Designing $\mathbb{E}$

Error set $\mathbb{E}$ should

→ avoid additive structure

→ allow for efficient schemes



Designing $\mathbb{E}$

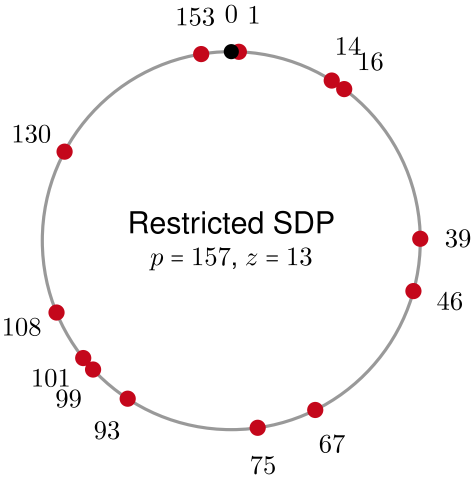
Error set $\mathbb{E}$ should

→ avoid additive structure

→ allow for efficient schemes

Multiplicative Restriction

Let $g \in \mathbb{F}_p^*$ of order z.
Set $\mathbb{E} = \{g^0, g^1, \ldots, g^{z-1}\} \leq \mathbb{F}_p^*$.

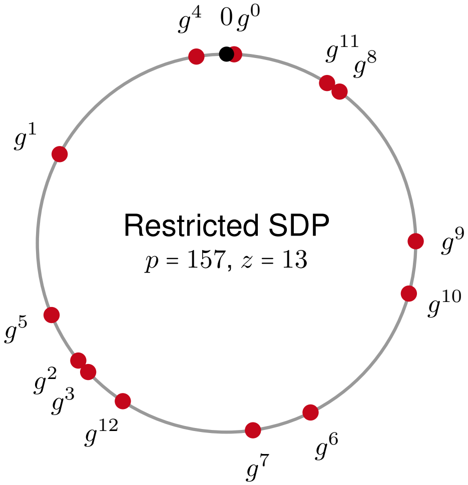


Designing $\mathbb{E}$

Error set $\mathbb{E}$ should
- → avoid additive structure
- → allow for efficient schemes

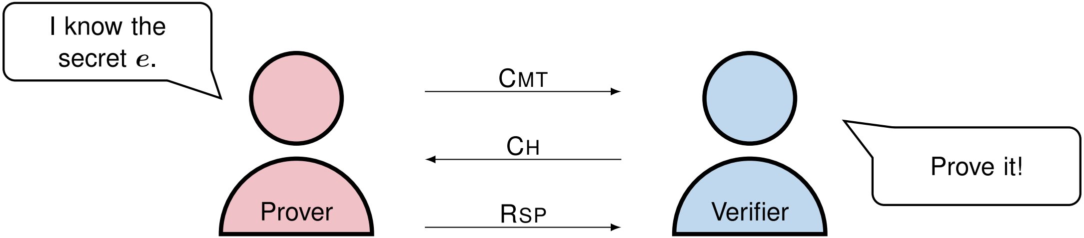
Multiplicative Restriction

Let $g \in \mathbb{F}_p^*$ of order z.
Set $\mathbb{E} = \{g^0, g^1, \ldots, g^{z-1}\} \leq \mathbb{F}_p^*$.

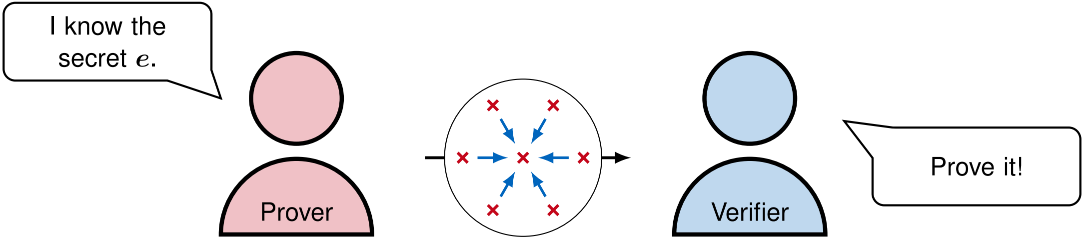


Disclaimer: not all, but many subgroups work nicely

R-SDP in Zero-Knowledge Protocols

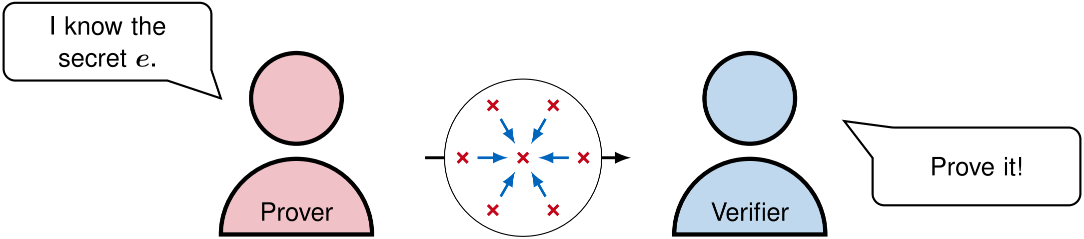


R-SDP in Zero-Knowledge Protocols



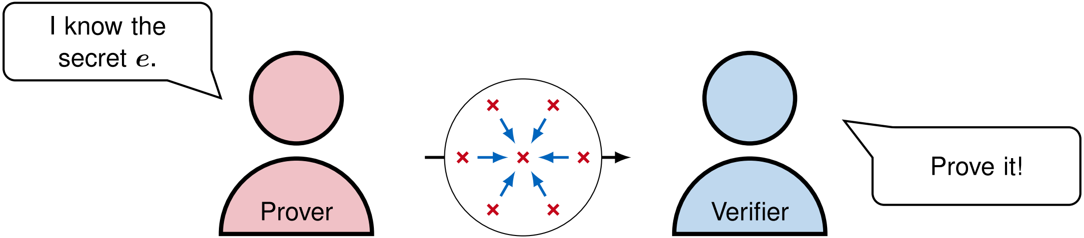
error $\boldsymbol{e}'$	map σ: $\boldsymbol{e}' = \sigma(\boldsymbol{e})$

R-SDP in Zero-Knowledge Protocols



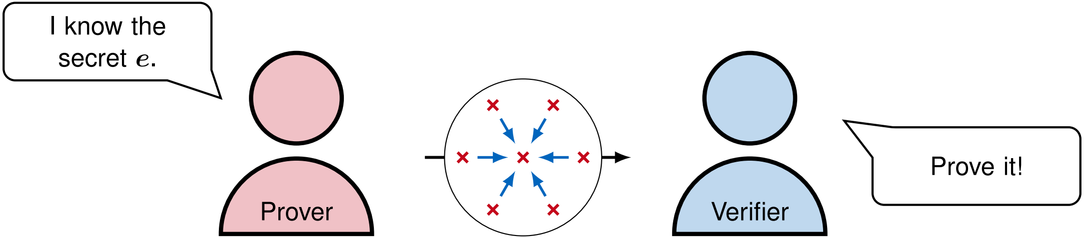
	error e'	map σ: $e' = \sigma(e)$
SDP	Hamming sphere	$S_n \rtimes (\mathbb{F}_p^*)^n$

R-SDP in Zero-Knowledge Protocols



	error e'	map σ: $e' = \sigma(e)$
SDP	Hamming sphere	$S_n \rtimes (\mathbb{F}_p^*)^n$
R-SDP	restricted sphere	$S_n \rtimes \mathbb{E}^n$

R-SDP in Zero-Knowledge Protocols

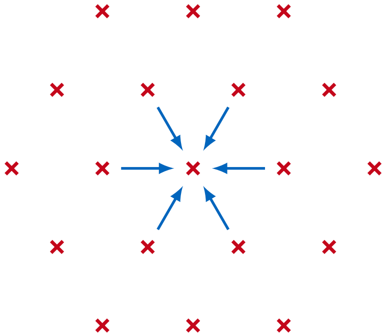


	error e'	map σ: $e' = \sigma(e)$
SDP	Hamming sphere	$S_n \rtimes (\mathbb{F}_p^*)^n$
R-SDP	restricted sphere	$S_n \rtimes \mathbb{E}^n$
$w = n$	$\mathbb{E}^n$	$\mathbb{E}^n$

Beyond R-SDP

Observation: $\mathbb{E}^n$ has group structure

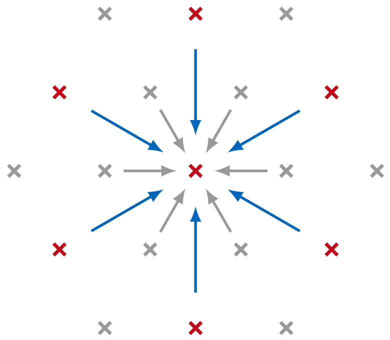
errors and maps in $\mathbb{E}^n$



Beyond R-SDP

errors and maps in $\mathbb{E}^n$

Observation: $\mathbb{E}^n$ has group structure



errors and maps in $G \leq \mathbb{E}^n$

Beyond R-SDP

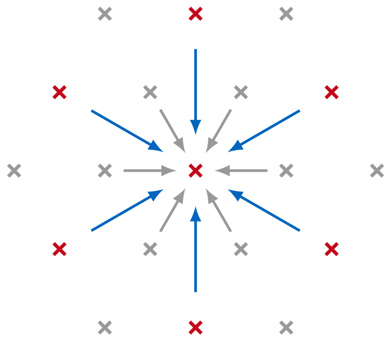
Observation: $\mathbb{E}^n$ has group structure

R-SDP(G): R-SDP with Subgroup G

Given: $\boldsymbol{H} \in \mathbb{F}_p^{(n-k)\times n}$, $\boldsymbol{s} \in \mathbb{F}_p^{n-k}$,
random subgroup $G \leq \mathbb{E}^n$ of order z^m.

Find: $\boldsymbol{e} \in G$ with $\boldsymbol{H}\boldsymbol{e} = \boldsymbol{s}$.

errors and maps in $\mathbb{E}^n$



errors and maps in $G \leq \mathbb{E}^n$

Beyond R-SDP

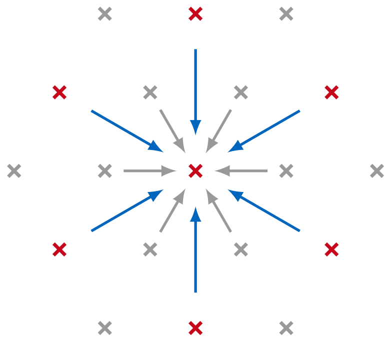
errors and maps in $\mathbb{E}^n$

Observation: $\mathbb{E}^n$ has group structure

R-SDP(G): R-SDP with Subgroup G

Given: $\boldsymbol{H} \in \mathbb{F}_p^{(n-k)\times n}$, $\boldsymbol{s} \in \mathbb{F}_p^{n-k}$,
random subgroup $G \leq \mathbb{E}^n$ of order z^m.

Find: $\boldsymbol{e} \in G$ with $\boldsymbol{H}\boldsymbol{e} = \boldsymbol{s}$.



errors and maps in $G \leq \mathbb{E}^n$

(!) solvers use subgroup restriction

Beyond R-SDP

errors and maps in $\mathbb{E}^n$

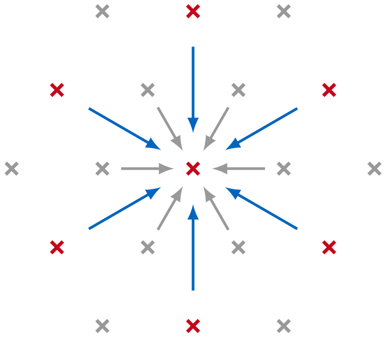
Observation: $\mathbb{E}^n$ has group structure

R-SDP(G): R-SDP with Subgroup G

Given: $\boldsymbol{H} \in \mathbb{F}_p^{(n-k)\times n}$, $\boldsymbol{s} \in \mathbb{F}_p^{n-k}$,
random subgroup $G \leq \mathbb{E}^n$ of order z^m.

Find: $\boldsymbol{e} \in G$ with $\boldsymbol{H}\boldsymbol{e} = \boldsymbol{s}$.

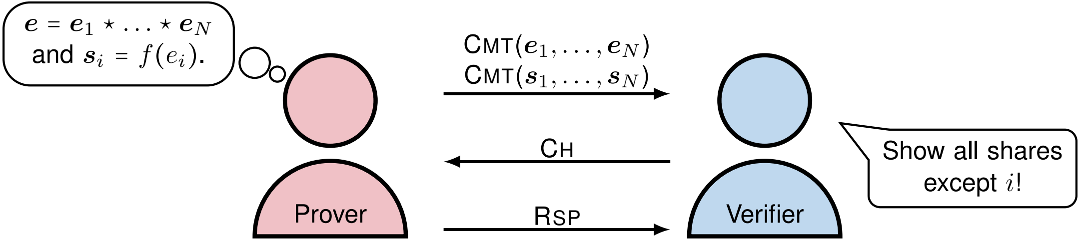
- (!) solvers use subgroup restriction
- ☺ elements of G smaller than 2λ



errors and maps in $G \leq \mathbb{E}^n$

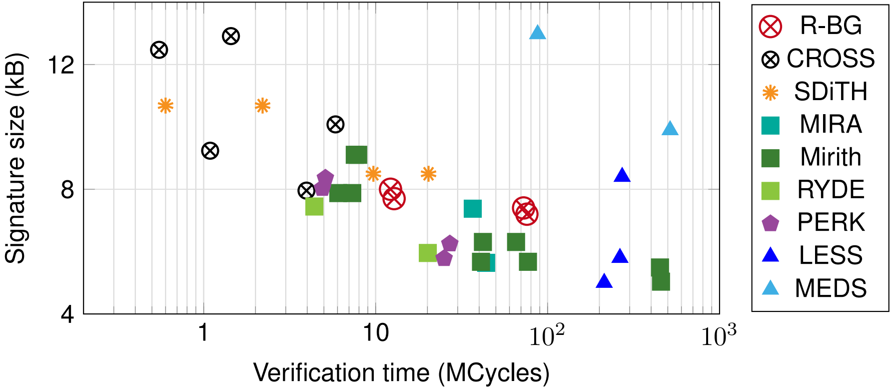
Adapting Modern Zero-Knowledge Protocols: R-BG

Bidoux, L., & Gaborit, P. (2022). Compact post-quantum signatures from proofs of knowledge leveraging structure for the PKP, SD and RSD problems. *C2SI*



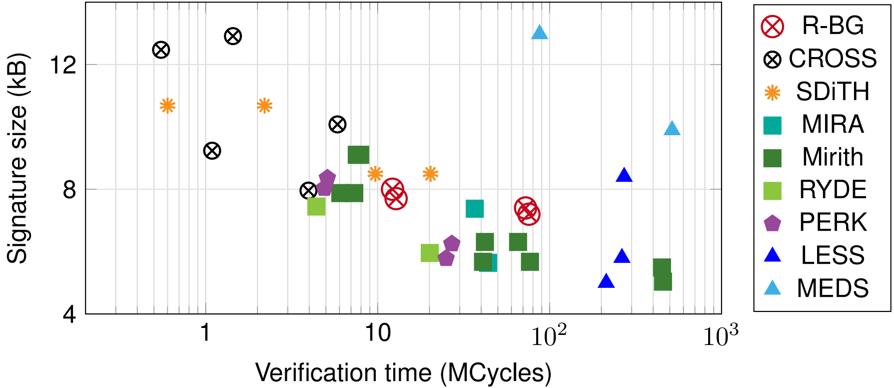
Comparison with NIST submissions

PQShield. (2023). *Post-Quantum Signatures Zoo*. https://pqshield.github.io/nist-sigs-zoo/



Comparison with NIST submissions

PQShield. (2023). *Post-Quantum Signatures Zoo*. https://pqshield.github.io/nist-sigs-zoo/



Proof of concept implementation is promising ✓

Conclusion

R-SDP and R-SDP(G)

- ☺ generalize the classical SDP,
- ☺ enable compact messages,
- ☺ can be combined with various ZKPs.

Conclusion

R-SDP and R-SDP(G)

- ☺ generalize the classical SDP,
- ☺ enable compact messages,
- ☺ can be combined with various ZKPs.

Can one

- ? improve solvers?
- ? tailor protocols to R-SDP and RSDP(G)?
- ? develop subgroup variants of other problems?

Conclusion

R-SDP and R-SDP(G)

- generalize the classical SDP,
- enable compact messages,
- can be combined with various ZKPs.

Can one

- improve solvers?
- tailor protocols to R-SDP and RSDP(G)?
- develop subgroup variants of other problems?

more on CROSS:

Conclusion

R-SDP and R-SDP(G)

- generalize the classical SDP,
- enable compact messages,
- can be combined with various ZKPs.

Can one

- improve solvers?
- tailor protocols to R-SDP and RSDP(G)?
- develop subgroup variants of other problems?

more on CROSS:

Thank you!

Questions?