CROSS

Codes & Restricted Objects Signature Scheme

- Marco Baldi
- Alessandro Barenghi
- Sebastian Bitzer
- Patrick Karl
- Felice Manganiello
- Alessio Pavoni
- Gerardo Pelosi
- Paolo Santini
- Jonas Schupp
- Freeman Slaughter
- Antonia Wachter-Zeh
- Violetta Weger

Post-Quantum Cryptography Workshop
Oxford, September 5, 2023

Technische Universität München

CROSS in a nutshell

Fiat-Shamir transformation of ZK interactive proof of knowledge

Main ingredients:

- **Restricted Syndrome-Decoding Problem (R-SDP)** and **R-SDP**(G)
- **CVE-style ZK protocol**
- **Optimizations** to reduce signature size

CROSS in a nutshell

Fiat-Shamir transformation of ZK interactive proof of knowledge

Main ingredients:

- **Restricted Syndrome-Decoding Problem (R-SDP)** and **R-SDP**(G)
  - ☺ not so different from non-binary SDP
  - ☺ compact messages and objects, especially with R-SDP(G)
  - ☺ efficient arithmetic
- **CVE-style ZK protocol**
- **Optimizations** to reduce signature size

CROSS in a nutshell

Fiat-Shamir transformation of ZK interactive proof of knowledge

Main ingredients:

- **Restricted Syndrome-Decoding Problem (R-SDP)** and **R-SDP**(G)
  - ☺ not so different from non-binary SDP
  - ☺ compact messages and objects, especially with R-SDP(G)
  - ☺ efficient arithmetic
- **CVE-style ZK protocol**
  - ☺ simple and efficient
  - ☺ good trade-off between signature size and computational overhead
- **Optimizations** to reduce signature size

CROSS in a nutshell

Fiat-Shamir transformation of ZK interactive proof of knowledge

Main ingredients:

- **Restricted Syndrome-Decoding Problem (R-SDP)** and **R-SDP**(G)
  - ☺ not so different from non-binary SDP
  - ☺ compact messages and objects, especially with R-SDP(G)
  - ☺ efficient arithmetic
- **CVE-style ZK protocol**
  - ☺ simple and efficient
  - ☺ good trade-off between signature size and computational overhead
- **Optimizations** to reduce signature size
  - ☺ transparent from the security point of view

Restricted Syndrome Decoding Problem

Let $\mathbb{E} \subseteq \mathbb{F}_q^*$, with $z = |\mathbb{E}|$.

Restricted Syndrome Decoding Problem (R-SDP) (Baldi et al., 2020)

Given $\mathbf{H} \in \mathbb{F}_q^{(n-k)\times n}$, $\mathbf{s} \in \mathbb{F}_q^{n-k}$, $w \in \mathbb{N}$, find $\mathbf{x} \in (\{0\} \cup \mathbb{E})^n$ such that $\mathbf{x}\mathbf{H}^\top = \mathbf{s}$ and $\mathrm{wt}(\mathbf{x}) = w$.

Restricted Syndrome Decoding Problem

Let $\mathbb{E} \subseteq \mathbb{F}_q^*$, with $z = |\mathbb{E}|$.

Restricted Syndrome Decoding Problem (R-SDP) (Baldi et al., 2020)

Given $\mathbf{H} \in \mathbb{F}_q^{(n-k)\times n}$, $\mathbf{s} \in \mathbb{F}_q^{n-k}$, $w \in \mathbb{N}$, find $\mathbf{x} \in (\{0\} \cup \mathbb{E})^n$ such that $\mathbf{x}\mathbf{H}^\top = \mathbf{s}$ and $\mathrm{wt}(\mathbf{x}) = w$.

Baldi et al., 2023: study of ISD algorithms for R-SDP

Restricted Syndrome Decoding Problem

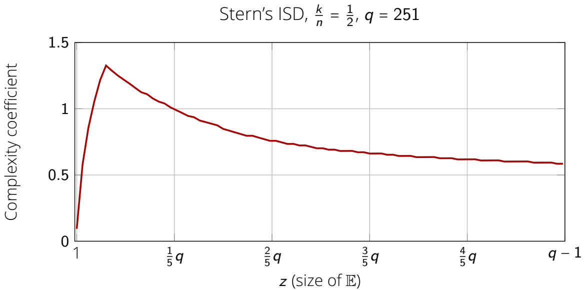
Let $\mathbb{E} \subseteq \mathbb{F}_q^*$, with $z = |\mathbb{E}|$.

Restricted Syndrome Decoding Problem (R-SDP) (Baldi et al., 2020)

Given $\mathbf{H} \in \mathbb{F}_q^{(n-k)\times n}$, $\mathbf{s} \in \mathbb{F}_q^{n-k}$, $w \in \mathbb{N}$, find $\mathbf{x} \in (\{0\} \cup \mathbb{E})^n$ such that $\mathbf{x}\mathbf{H}^\top = \mathbf{s}$ and $\mathrm{wt}(\mathbf{x}) = w$.

Baldi et al., 2023: study of ISD algorithms for R-SDP

Unique solution: decrease $z \implies$ larger w



Restricted Syndrome Decoding Problem

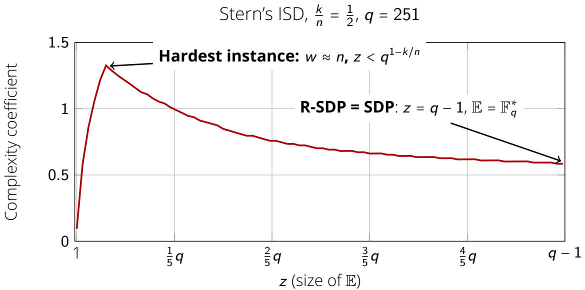
Let $\mathbb{E} \subseteq \mathbb{F}_q^*$, with $z = |\mathbb{E}|$.

Restricted Syndrome Decoding Problem (R-SDP) (Baldi et al., 2020)

Given $\mathbf{H} \in \mathbb{F}_q^{(n-k)\times n}$, $\mathbf{s} \in \mathbb{F}_q^{n-k}$, $w \in \mathbb{N}$, find $\mathbf{x} \in (\{0\} \cup \mathbb{E})^n$ such that $\mathbf{x}\mathbf{H}^\top = \mathbf{s}$ and $\mathrm{wt}(\mathbf{x}) = w$.

Baldi et al., 2023: study of ISD algorithms for R-SDP

Unique solution: decrease $z \implies$ larger w



Smaller codes

With respect to SDP, we can use shorter codes (smaller n)

R-SDP with restricted group and R-SDP(G)

The restriction used in CROSS

Let $g \in \mathbb{F}_q$ with $\operatorname{ord}(g) = z$ and $\mathbb{E} = \{g^i \mid i \in [0; z-1]\} = \{1, g, g^2, \cdots, g^{z-1}\}$

We consider $w = n$ and solution space $\mathbb{E}^n = \left\{ \left(g^{i_1}, g^{i_2}, \cdots, g^{i_n}\right) \middle| \left(i_1, i_2, \cdots, i_n\right) \in \mathbb{Z}_z^n \right\}$

R-SDP with restricted group and R-SDP(G)

The restriction used in CROSS

Let $g \in \mathbb{F}_q$ with $\mathrm{ord}(g) = z$ and $\mathbb{E} = \{g^i \,|\, i \in [0; z-1]\} = \{1, g, g^2, \cdots, g^{z-1}\}$

We consider $w = n$ and solution space $\mathbb{E}^n = \left\{ \left(g^{i_1}, g^{i_2}, \cdots, g^{i_n}\right) \middle| \left(i_1, i_2, \cdots, i_n\right) \in \mathbb{Z}_z^n \right\}$

Let $\mathbf{b}_1, \cdots, \mathbf{b}_m \in \mathbb{E}^n$ and

$$G = \langle \mathbf{b}_1, \cdots, \mathbf{b}_m \rangle = \left\{ \mathbf{b}_1^{c_1} \star \mathbf{b}_2^{c_2} \star \cdots \star \mathbf{b}_m^{c_m} \mid \left(c_1, \cdots, c_m\right) \in \mathbb{F}_z^m \right\} \le \mathbb{E}^n$$

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

Given $\mathbf{H} \in \mathbb{F}_q^{(n-k)\times n}$, $\mathbf{s} \in \mathbb{F}_q^{n-k}$ and $G \le \mathbb{E}^n$, find $\mathbf{x} \in G$ such that $\mathbf{x}\mathbf{H}^\top = \mathbf{s}$.

When $G = \mathbb{E}^n$, R-SDP(G) is the same as R-SDP

SDP vs R-SDP vs R-SDP(G)

With R-SDP(G), messages and codes get even shorter

	SDP	R-SDP	R-SDP(G)
Solution space	Hamming sphere with radius $w \leq n - k$	$\mathbb{E}^n$	$G \leq \mathbb{E}^n$
Group description	-	$g \in \mathbb{F}_q^*$	$\mathbf{M}_G \in \mathbb{F}_z^{m \times n}$
Element size	Positions and values: $w\left(\log_2(n) + \log_2(q-1)\right)$	Exponents: $n \log_2(z)$	m coeffs over $\mathbb{F}_z$: $m \log_2(z)$
Transitive maps			
Map size			
Code length			

SDP vs R-SDP vs R-SDP(G)

With R-SDP(G), messages and codes get even shorter

	SDP	R-SDP	R-SDP(G)
Solution space	Hamming sphere with radius $w \leq n-k$	$\mathbb{E}^n$	$G \leq \mathbb{E}^n$
Group description	-	$g \in \mathbb{F}_q^*$	$\mathbf{M}_G \in \mathbb{F}_z^{m\times n}$
Element size	Positions and values: $w\left(\log_2(n) + \log_2(q-1)\right)$	Exponents: $n\log_2(z)$	m coeffs over $\mathbb{F}_z$: $m\log_2(z)$
Transitive maps			
Map size			
Code length			

SDP vs R-SDP vs R-SDP(G)

With R-SDP(G), messages and codes get even shorter

	SDP	R-SDP	R-SDP(G)
Solution space	Hamming sphere with radius $w \leq n - k$	$\mathbb{E}^n$	$G \leq \mathbb{E}^n$
Group description	-	$g \in \mathbb{F}_q^*$	$\mathbf{M}_G \in \mathbb{F}_z^{m \times n}$
Element size	Positions and values: $w\left(\log_2(n) + \log_2(q-1)\right)$	Exponents: $n \log_2(z)$	m coeffs over $\mathbb{F}_z$: $m \log_2(z)$
Transitive maps			
Map size			
Code length			

SDP vs R-SDP vs R-SDP(G)

With R-SDP(G), messages and codes get even shorter

	SDP	R-SDP	R-SDP(G)
Solution space	Hamming sphere with radius $w \leq n - k$	$\mathbb{E}^n$	$G \leq \mathbb{E}^n$
Group description	-	$g \in \mathbb{F}_q^*$	$\mathbf{M}_G \in \mathbb{F}_z^{m \times n}$
Element size	Positions and values: $w\left(\log_2(n) + \log_2(q-1)\right)$	Exponents: $n \log_2(z)$	m coeffs over $\mathbb{F}_z$: $m \log_2(z)$
Transitive maps	Monomial transformations	$\mathbf{d} \in \mathbb{E}^n$	$\mathbf{d} \in G$
Map size	$n\left(\log_2(n) + \log_2(q-1)\right)$	$n \log_2(z)$	$m \log_2(z)$
Code length			

SDP vs R-SDP vs R-SDP(G)

With R-SDP(G), messages and codes get even shorter

	SDP	R-SDP	R-SDP(G)
Solution space	Hamming sphere with radius $w \leq n - k$	$\mathbb{E}^n$	$G \leq \mathbb{E}^n$
Group description	-	$g \in \mathbb{F}_q^*$	$\mathbf{M}_G \in \mathbb{F}_z^{m \times n}$
Element size	Positions and values: $w\left(\log_2(n) + \log_2(q-1)\right)$	Exponents: $n \log_2(z)$	m coeffs over $\mathbb{F}_z$: $m \log_2(z)$
Transitive maps	Monomial transformations	$\mathbf{d} \in \mathbb{E}^n$	$\mathbf{d} \in G$
Map size	$n\left(\log_2(n) + \log_2(q-1)\right)$	$n \log_2(z)$	$m \log_2(z)$
Code length		Less than SDP	Less than R-SDP

Cryptanalysis

For each security category, computationally-friendly parameters:

- for R-SDP: $q = 127$, $g = 2$, $z = 7$
- for R-SDP(G): $q = 509$, $g = 16$, $z = 127$

Cryptanalysis

For each security category, computationally-friendly parameters:

- for R-SDP: $q = 127$, $g = 2$, $z = 7$
- for R-SDP(G): $q = 509$, $g = 16$, $z = 127$

Considered attacks:

	R-SDP	**R-SDP(G)**
Decoding attacks	Tailor BJMM to $q = 127$, $g = 2$	
Algebraic attacks	Polynomial system (syndrome eqs + group eqs)	

Cryptanalysis

For each security category, computationally-friendly parameters:

- for R-SDP: $q = 127$, $g = 2$, $z = 7$
- for R-SDP(G): $q = 509$, $g = 16$, $z = 127$

Considered attacks:

	R-SDP	**R-SDP(G)**
Decoding attacks	Tailor BJMM to $q = 127$, $g = 2$	
Algebraic attacks	Polynomial system (syndrome eqs + group eqs)	

Personal communication by Briaud and Øygarden

" Our results seem to confirm that the algebraic modeling is solved at a degree which is linear in n *provided that the code rate* $R = k/n$ *is a constant. This approach does not threaten the current parameters of CROSS."*

Cryptanalysis

For each security category, computationally-friendly parameters:

- for R-SDP: $q = 127$, $g = 2$, $z = 7$
- for R-SDP(G): $q = 509$, $g = 16$, $z = 127$

Considered attacks:

	R-SDP	**R-SDP(G)**
Decoding attacks	Tailor BJMM to $q = 127$, $g = 2$	Use rank-deficient submatrices of $\mathbf{M}_G$ for enumeration in Stern/Dumer ISD
Algebraic attacks	Polynomial system (syndrome eqs + group eqs)	**???**

Personal communication by Briaud and Øygarden

" Our results seem to confirm that the algebraic modeling is solved at a degree which is linear in n *provided that the code rate* $R = k/n$ *is a constant. This approach does not threaten the current parameters of CROSS."*

The CROSS ZK proof of knowledge

Private Key: restricted vector $\mathbf{e} \in G$
Public Key: group $G \leq \mathbb{E}^n$, parity-check matrix $\mathbf{H}$, syndrome $\mathbf{s} = \mathbf{H}\mathbf{e}^\top$

PROVER		VERIFIER
Sample $\texttt{Seed} \xleftarrow{\$} \{0;1\}^\lambda$, $(\mathbf{u}', \mathbf{e}') \xleftarrow{\texttt{Seed}} \mathbb{F}_q^n \times G$ \\\\Randomness		
Compute $\mathbf{d} \in G$ such that $\mathbf{d} \star \mathbf{e}' = \mathbf{e}$\\\\$\mathbf{d}$ is uniformly random over G		
Set $\mathbf{u} = \mathbf{d} \star \mathbf{u}'$ and $\widetilde{\mathbf{s}} = \mathbf{u}\mathbf{H}^\top$		
Set $c_0 = \text{Hash}\big(\widetilde{\mathbf{s}}, \mathbf{d}\big)$, $c_1 = \text{Hash}\big(\mathbf{u}', \mathbf{e}'\big)$\\\\Commitments		
	$\xrightarrow{(c_0, c_1)}$	
	$\xleftarrow{\beta}$	Sample $\beta \xleftarrow{\$} \mathbb{F}_q^*$
Compute $\mathbf{y} = \mathbf{u}' + \beta\mathbf{e}'$ \\\\Uniformly random over $\mathbb{F}_q$		
Set $h = \text{Hash}(\mathbf{y})$ \\\\First response		
	$\xrightarrow{h}$	
		Sample $b \xleftarrow{\$} \{0, 1\}$
	$\xleftarrow{b}$	
If $b = 0$, set $\texttt{rsp} = \big(\mathbf{y}, \mathbf{d}\big)$ \\\\Second response (the larger one)		
If $b = 1$, set $\texttt{rsp} = \texttt{Seed}$\\\\Second response (the shorter one)		
	$\xrightarrow{\texttt{rsp}}$	
		Verify c_b using $\texttt{rsp}$

The CROSS ZK proof of knowledge

Private Key: restricted vector $\mathbf{e} \in G$
Public Key: group $G \leq \mathbb{E}^n$, parity-check matrix $\mathbf{H}$, syndrome $\mathbf{s} = \mathbf{H}\mathbf{e}^\top$

PROVER		VERIFIER
Sample $\texttt{Seed} \xleftarrow{\$} \{0;1\}^\lambda$, $(\mathbf{u}', \mathbf{e}') \xleftarrow{\texttt{Seed}} \mathbb{F}_q^n \times G$ \\\\Randomness Compute $\mathbf{d} \in G$ such that $\mathbf{d} \star \mathbf{e}' = \mathbf{e}$\\\\$\mathbf{d}$ is uniformly random over G Set $\mathbf{u} = \mathbf{d} \star \mathbf{u}'$ and $\widetilde{\mathbf{s}} = \mathbf{u}\mathbf{H}^\top$ Set $c_0 = \text{Hash}(\widetilde{\mathbf{s}}, \mathbf{d})$, $c_1 = \text{Hash}(\mathbf{u}', \mathbf{e}')$\\\\Commitments		
	$\xrightarrow{(c_0, c_1)}$	
	$\xleftarrow{\beta}$	Sample $\beta \xleftarrow{\$} \mathbb{F}_q^*$
Compute $\mathbf{y} = \mathbf{u}' + \beta\mathbf{e}'$ \\\\Uniformly random over $\mathbb{F}_q$ Set $h = \text{Hash}(\mathbf{y})$ \\\\First response		
	$\xrightarrow{h}$	
		Sample $b \xleftarrow{\$} \{0, 1\}$
	$\xleftarrow{b}$	
If $b = 0$, set $\texttt{rsp} = (\mathbf{y}, \mathbf{d})$ \\\\Second response (the larger one) If $b = 1$, set $\texttt{rsp} = \texttt{Seed}$\\\\Second response (the shorter one)		
	$\xrightarrow{\texttt{rsp}}$	
		Verify c_b using $\texttt{rsp}$

Standard optimizations: PRNG trees, fixed-weight challenges,...

The CROSS ZK proof of knowledge

Private Key: restricted vector $\mathbf{e} \in G$
Public Key: group $G \leq \mathbb{E}^n$, parity-check matrix $\mathbf{H}$, syndrome $\mathbf{s} = \mathbf{H}\mathbf{e}^\top$

PROVER		VERIFIER
Sample $\texttt{Seed} \xleftarrow{\$} \{0;1\}^\lambda$, $(\mathbf{u}', \mathbf{e}') \xleftarrow{\texttt{Seed}} \mathbb{F}_q^n \times G$ \\Randomness Compute $\mathbf{d} \in G$ such that $\mathbf{d} \star \mathbf{e}' = \mathbf{e}$\\$\mathbf{d}$ is uniformly random over G Set $\mathbf{u} = \mathbf{d} \star \mathbf{u}'$ and $\widetilde{\mathbf{s}} = \mathbf{u}\mathbf{H}^\top$ Set $c_0 = \text{Hash}(\widetilde{\mathbf{s}}, \mathbf{d})$, $c_1 = \text{Hash}(\mathbf{u}', \mathbf{e}')$\\Commitments		
	$\xrightarrow{(c_0, c_1)}$	
	$\xleftarrow{\beta}$	Sample $\beta \xleftarrow{\$} \mathbb{F}_q^*$
Compute $\mathbf{y} = \mathbf{u}' + \beta\mathbf{e}'$ \\Uniformly random over $\mathbb{F}_q$ Set $h = \text{Hash}(\mathbf{y})$ \\First response		
	$\xrightarrow{h}$	
		Sample $b \xleftarrow{\$} \{0,1\}$
	$\xleftarrow{b}$	
If $b = 0$, set $\texttt{rsp} = (\mathbf{y}, \mathbf{d})$ \\Second response (the larger one) If $b = 1$, set $\texttt{rsp} = \texttt{Seed}$\\Second response (the shorter one)		
	$\xrightarrow{\texttt{rsp}}$	
		Verify c_b using $\texttt{rsp}$

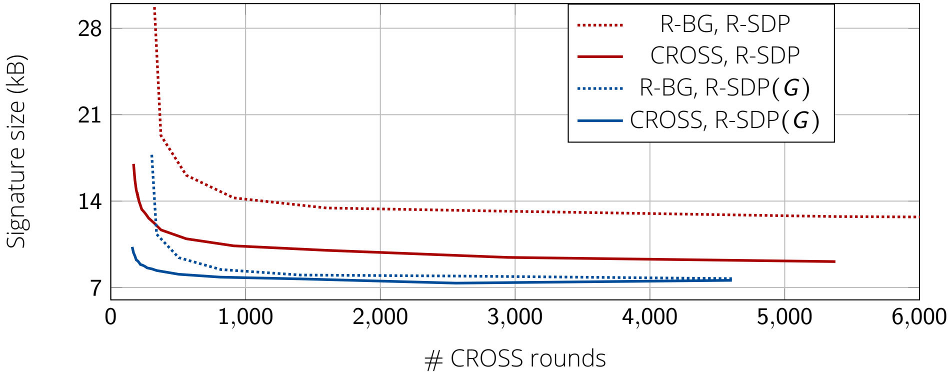
Standard optimizations: PRNG trees, fixed-weight challenges,...

Forgeries: attack by Kales and Zaverucha, 2020, adapted to fixed-weight challenges

Why such a simple ZK protocol?

Baldi et al., 2023: R-BG protocol, soundness error $\varepsilon \approx \max\left\{\frac{1}{N}; \frac{1}{q-1}\right\}$

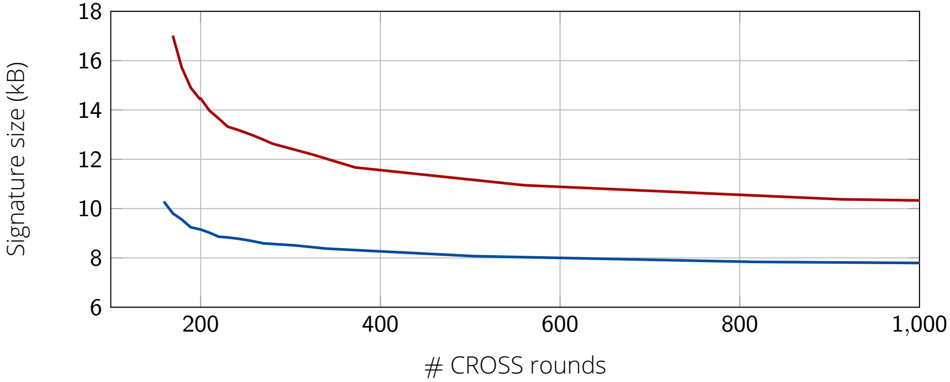
Computational cost: one round of R-BG is $\approx N$ rounds of CROSS



Why such a simple ZK protocol?

Baldi et al., 2023: R-BG protocol, soundness error $\varepsilon \approx \max\left\{\frac{1}{N}; \frac{1}{q-1}\right\}$

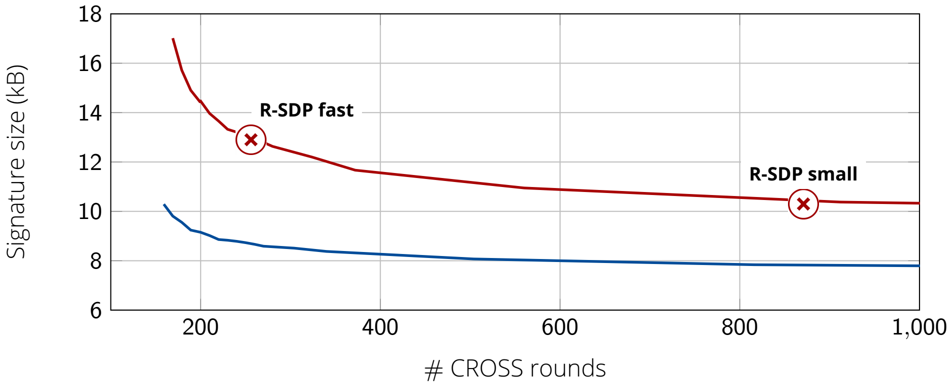
Computational cost: one round of R-BG is $\approx N$ rounds of CROSS



Why such a simple ZK protocol?

Baldi et al., 2023: R-BG protocol, soundness error $\varepsilon \approx \max\left\{\frac{1}{N}; \frac{1}{q-1}\right\}$

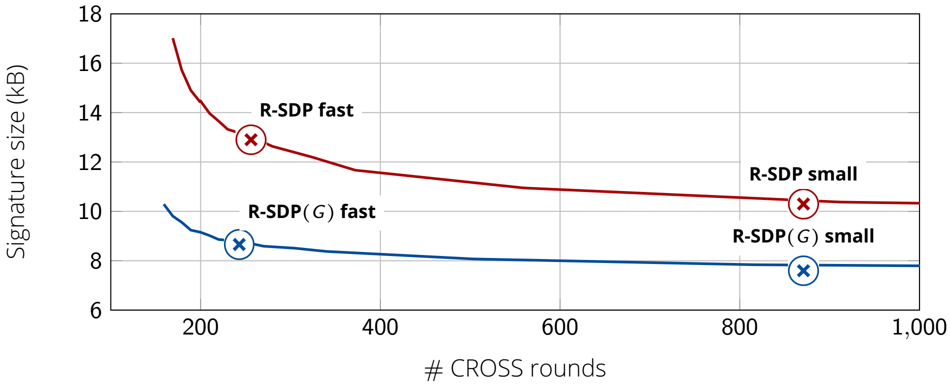
Computational cost: one round of R-BG is $\approx N$ rounds of CROSS



Why such a simple ZK protocol?

Baldi et al., 2023: R-BG protocol, soundness error $\varepsilon \approx \max\left\{\frac{1}{N}; \frac{1}{q-1}\right\}$

Computational cost: one round of R-BG is $\approx N$ rounds of CROSS



Performances (NIST category 1)

Table: Parameter choices, signature sizes and timings for both **CROSS**-R-SDP and **CROSS**-R-SDP(G), for NIST security category **1**. Measurements collected on an Intel Core i7-12700 clocked at 5.0 GHz.

Algorithm ID	**Type**	(n, k, m)	**# rounds**	**Sign. Size** (kB)	**Sign** (MCycles)	**Verify** (MCycles)
CROSS-R-SDP	**fast**	$(127, 76, -)$	256	12.9	6.8	3.2
	short		871	10.3	22.0	10.3
CROSS-R-SDP(G)	**fast**	$(42, 23, 24)$	243	8.7	3.1	2.1
	short		871	7.6	11.0	7.8

Performances (NIST category 1)

Table: Parameter choices, signature sizes and timings for both **CROSS**-R-SDP and **CROSS**-R-SDP(G), for NIST security category **1**. Measurements collected on an Intel Core i7-12700 clocked at 5.0 GHz.

Algorithm ID	Type	(n, k, m)	# rounds	Sign. Size (kB)	Sign (MCycles)	Verify (MCycles)
CROSS-R-SDP	**fast**	$(127, 76, -)$	256	12.9	6.8	3.2
	short		871	10.3	22.0	10.3
CROSS-R-SDP(G)	**fast**	$(42, 23, 24)$	243	8.7	3.1	2.1
	short		871	7.6	11.0	7.8

Performances (NIST category 1)

Table: Parameter choices, signature sizes and timings for both **CROSS**-R-SDP and **CROSS**-R-SDP(G), for NIST security category 1. Measurements collected on an Intel Core i7-12700 clocked at 5.0 GHz.

Algorithm ID	**Type**	(n, k, m)	**# rounds**	**Sign. Size** (kB)	**Sign** (MCycles)	**Verify** (MCycles)
CROSS-R-SDP	**fast**	$(127, 76, -)$	256	12.9	6.8	3.2
	short		871	10.3	22.0	10.3
CROSS-R-SDP(G)	**fast**	$(42, 23, 24)$	243	8.7	3.1	2.1
	short		871	7.6	11.0	7.8

- ☺ Elements of G are smaller than 2λ
- ☺ Computation time split in half between modular arithmetic and SHA-3/SHAKE computations
- ☺ Simple operations (basic symmetric primitives, vector/matrix operations among small elements) and no permutations: straightforward **constant-time implementation**
- ☺ Ongoing AVX2 optimized implementation (around 4× boost expected)

Thanks for the attention! Questions?

CROSS: Codes & Restricted Objects Signature Scheme

Brought to you by the wonderful CROSS team :)

`https://www.cross-crypto.com/`

References

- D. Kales, G. Zaverucha. ”An attack on some signature schemes constructed from five-pass identification schemes.” International Conference on Cryptology and Network Security. Cham: Springer International Publishing, 2020.
- J. Stern. “Designing identification schemes with keys of short size”. In: Advances in Cryptology—CRYPTO’94: 14th Annual International Cryptology Conference Santa Barbara, California, USA August 21–25, 1994 Proceedings. Springer. 2001, pp. 164–173
- M. Baldi, M. Battaglioni, F. Chiaraluce, A.L. Horlemann-Trautmann, E. Persichetti, P. Santini, V. Weger, (2020). A new path to code-based signatures via identification schemes with restricted errors. arXiv preprint arXiv:2008.06403.. ”A new path to code-based signatures via identification schemes with restricted errors.” arXiv preprint arXiv:2008.06403 (2020)
- F. Manganiello, and F. Slaughter. ”Generic Error SDP and Generic Error CVE.” Cryptology ePrint Archive (2023).

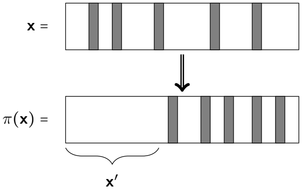
References

- M. Baldi, S. Bitzer, A. Pavoni, P. Santini, A. Wachter-Zeh, V. Weger, (2023). Zero Knowledge Protocols and Signatures from the Restricted Syndrome Decoding Problem. Cryptology ePrint Archive. ”Zero Knowledge Protocols and Signatures from the Restricted Syndrome Decoding Problem.” Cryptology ePrint Archive, 2023
- Bitzer, Sebastian, et al, ”Generic Decoding of Restricted Errors.” 2023 IEEE International Symposium on Information Theory (ISIT). IEEE, 2023
- Bidoux, Loïc, and Philippe Gaborit. ”Compact Post-quantum Signatures from Proofs of Knowledge Leveraging Structure for the SD, MQ, PKP and RSD Problems.” International Conference on Codes, Cryptology, and Information Security. Cham: Springer Nature Switzerland, 2023

R-SDP vs SDP: Information Set Decoding

Prange's ISD

1) choose an information set J
2) "hope" $\mathbf{x}' = \mathbf{x}_J = (0, \cdots, 0)$
3) repeat until 2) is true

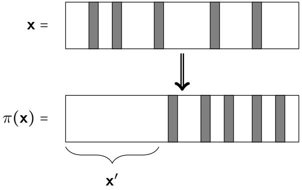


Running time is $T_{ISD} = N_{Guess}$

R-SDP vs SDP: Information Set Decoding

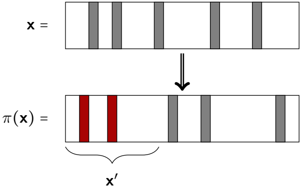
Prange's ISD

1) choose an information set J
2) "hope" $\mathbf{x}' = \mathbf{x}_J = (0, \cdots, 0)$
3) repeat until 2) is true



Advanced ISD

1) choose a set J, $|J| \geq k$
2) "hope" $\mathbf{x}' = \mathbf{x}_J$ has low weight
3) enumerate candidates for $\mathbf{x}'$
4) repeat until 2) is true



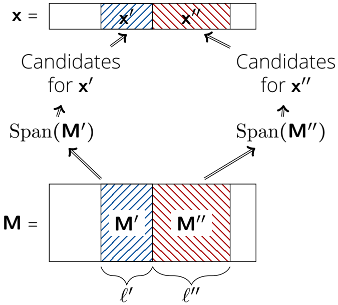
Running time is $T_{ISD} = N_{Guess} \cdot T_{Enumeration}$

R-SDP is harder than SDP: the intuition

Any ISD requires to guess many entries of $\mathbf{x}$: with SDP, there are always at least k zeros. With full weight R-SDP, $\mathbf{x}'$ has always full weight!

Employing G to speed up ISD

We search for two rank-deficient matrices $\mathbf{M}' \in \mathbb{F}_z^{m\times\ell'}$, $\mathbf{M}'' \in \mathbb{F}_z^{m\times\ell''}$:



$$\mathrm{Rank}(\mathbf{M}') = m' < \min\{m, \ell'\}$$

$$\mathrm{Rank}(\mathbf{M}'') = m'' < \min\{m, \ell''\}$$

We can build lists for Stern/Dumer ISD with reduced cost:

$$\#\text{ candidates for } \mathbf{x}' = z^{m'} < \min\left\{z^m, z^{\ell'}\right\}$$

$$\#\text{ candidates for } \mathbf{x}'' = z^{m''} < \min\left\{z^m, z^{\ell''}\right\}$$

Example

Let $q = 11$ and $g = 4$, with $\mathrm{ord}(g) = z = 5$:

$$\mathbb{E} = \left\{1 = g^0, \quad 4 = g^1, \quad 5 = g^2, \quad 9 = g^3, \quad 3 = g^4\right\}.$$

Let

$$\mathbf{b}_1 = (1,4,9,5,3) \qquad \mathbf{b}_2 = (5,9,4,9,3) \qquad \mathbf{b}_3 = (9,9,4,1,1) \qquad \text{(entries over } \mathbb{F}_q\text{)}$$

$$\ell(\mathbf{b}_1) = (0,1,3,2,4) \quad \ell(\mathbf{b}_2) = (2,3,1,3,4) \quad \ell(\mathbf{b}_3) = (3,3,1,0,0) \quad \text{(entries over } \mathbb{F}_z\text{)}$$

Example

Let $q = 11$ and $g = 4$, with $\mathrm{ord}(g) = z = 5$:

$$\mathbb{E} = \left\{1 = g^0, \quad 4 = g^1, \quad 5 = g^2, \quad 9 = g^3, \quad 3 = g^4\right\}.$$

Let

$$\mathbf{b}_1 = (1,4,9,5,3) \qquad \mathbf{b}_2 = (5,9,4,9,3) \qquad \mathbf{b}_3 = (9,9,4,1,1) \qquad \text{(entries over } \mathbb{F}_q\text{)}$$

$$\ell(\mathbf{b}_1) = (0,1,3,2,4) \quad \ell(\mathbf{b}_2) = (2,3,1,3,4) \quad \ell(\mathbf{b}_3) = (3,3,1,0,0) \quad \text{(entries over } \mathbb{F}_z\text{)}$$

The group $G = \langle \mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3 \rangle$ has maximum order $z^3 = 125$; its associated subspace is generated by

$$\mathbf{M} = \begin{pmatrix} \ell(\mathbf{b}_1) \\ \ell(\mathbf{b}_2) \\ \ell(\mathbf{b}_3) \end{pmatrix} = \begin{pmatrix} 0 & 1 & 3 & 2 & 4 \\ 2 & 3 & 1 & 3 & 4 \\ 3 & 3 & 1 & 0 & 0 \end{pmatrix}$$

Example

Let $q = 11$ and $g = 4$, with $\mathrm{ord}(g) = z = 5$:

$$\mathbb{E} = \left\{1 = g^0, \quad 4 = g^1, \quad 5 = g^2, \quad 9 = g^3, \quad 3 = g^4\right\}.$$

Let

$$\mathbf{b}_1 = (1,4,9,5,3) \qquad \mathbf{b}_2 = (5,9,4,9,3) \qquad \mathbf{b}_3 = (9,9,4,1,1) \qquad \text{(entries over } \mathbb{F}_q\text{)}$$

$$\ell(\mathbf{b}_1) = (0,1,3,2,4) \quad \ell(\mathbf{b}_2) = (2,3,1,3,4) \quad \ell(\mathbf{b}_3) = (3,3,1,0,0) \quad \text{(entries over } \mathbb{F}_z\text{)}$$

The group $G = \langle \mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3 \rangle$ has maximum order $z^3 = 125$; its associated subspace is generated by

$$\mathbf{M} = \begin{pmatrix} \ell(\mathbf{b}_1) \\ \ell(\mathbf{b}_2) \\ \ell(\mathbf{b}_3) \end{pmatrix} = \begin{pmatrix} 0 & 1 & 3 & 2 & 4 \\ 2 & 3 & 1 & 3 & 4 \\ 3 & 3 & 1 & 0 & 0 \end{pmatrix}$$

The vector $\mathbf{a} = (9,4,1,4,5)$ is in G and $\ell_G(\mathbf{a}) = (3,0,2)$; indeed

$$(3,0,2) \cdot \mathbf{M} = (3,1,0,1,2)$$

$$\ell^{-1}\big((3,1,0,1,2)\big) = \left(g^3, g^1, g^0, g^1, g^2\right) = (9,4,1,4,5)$$

Algebraic attacks to R-SDP

Goal: find $\mathbf{x} \in \mathbb{E}^n = \{g^i \mid i = 0, 1, \cdots, z-1\}^n$ such that $\mathbf{H}\mathbf{x}^\top = \mathbf{s}$

Algebraic attacks to R-SDP

Goal: find $\mathbf{x} \in \mathbb{E}^n = \{g^i \mid i = 0, 1, \cdots, z-1\}^n$ such that $\mathbf{H}\mathbf{x}^\top = \mathbf{s}$

Treat $x_1, \cdots, x_n$ as unknowns and build the following system:

$$\begin{cases} \mathbf{H}\mathbf{x}^\top = \mathbf{s} & \text{linear eqs in } n \text{ unknowns,} \\ x_i^z = 1, \quad \forall i = 1, \cdots, n & \text{nonlinear eqs in } n \text{ unknowns} \end{cases}$$

Algebraic attacks to R-SDP

Goal: find $\mathbf{x} \in \mathbb{E}^n = \{g^i \mid i = 0, 1, \cdots, z-1\}^n$ such that $\mathbf{H}\mathbf{x}^\top = \mathbf{s}$

Treat $x_1, \cdots, x_n$ as unknowns and build the following system:

$$\begin{cases} \mathbf{H}\mathbf{x}^\top = \mathbf{s} & \text{linear eqs in } n \text{ unknowns,} \\ x_i^z = 1, \ \forall i = 1, \cdots, n & \text{nonlinear eqs in } n \text{ unknowns} \end{cases}$$

Complexity of solving with F5 algorithm for Grobner basis:

$$O\left(\binom{n + d_{\mathrm{reg}}}{d_{\mathrm{reg}}}^{\omega}\right)$$

Algebraic attacks to R-SDP

Goal: find $\mathbf{x} \in \mathbb{E}^n = \{g^i \mid i = 0, 1, \cdots, z-1\}^n$ such that $\mathbf{H}\mathbf{x}^\top = \mathbf{s}$

Treat $x_1, \cdots, x_n$ as unknowns and build the following system:

$$\begin{cases} \mathbf{H}\mathbf{x}^\top = \mathbf{s} & \text{linear eqs in } n \text{ unknowns,} \\ x_i^z = 1, \ \forall i = 1, \cdots, n & \text{nonlinear eqs in } n \text{ unknowns} \end{cases}$$

Complexity of solving with F5 algorithm for Grobner basis:

$$O\left(\binom{n + d_{\mathrm{reg}}}{d_{\mathrm{reg}}}^{\omega}\right)$$

For CROSS parameters, experiments suggest that d_{reg} is linear in n: complexity is exponential in n