Institute for Communications Engineering
School of Computation, Information and Technology
Technical University of Munich

CROSS and Restricted Decoding Problems

Sebastian Bitzer, Paolo Santini, Antonia Wachter-Zeh, Violetta Weger

Code-based Digital Signatures

Underlying problem is well trusted:

Syndrome Decoding Problem

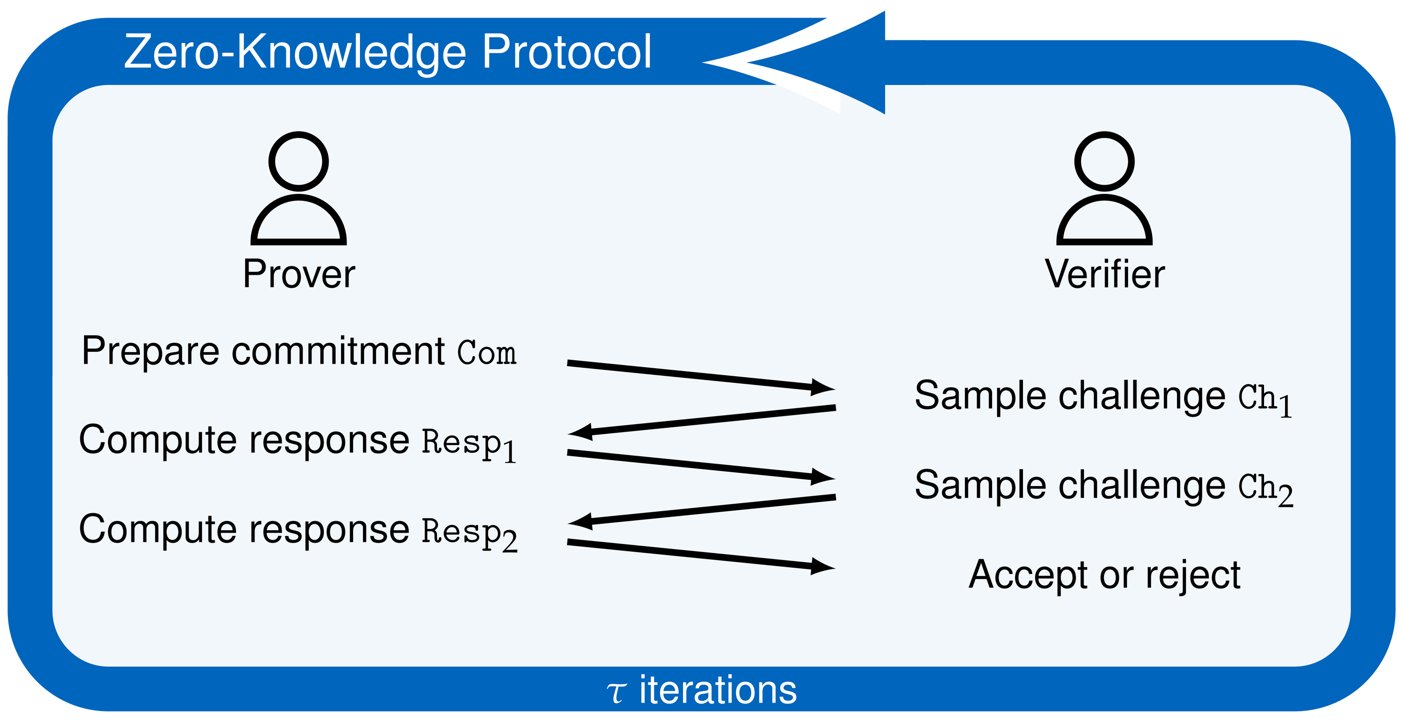
Let parity-check matrix $\mathbf{H} \in \mathbb{F}_p^{(n-k)\times n}$, syndrome $\mathbf{s} \in \mathbb{F}_p^{n-k}$ and weight w be given.
Find an error vector $e \in \mathbb{F}_p^n$ with $\mathbf{e}\mathbf{H}^\top = \mathbf{s}$ and $\mathrm{wt}_\mathrm{H}(e) = w$.

Hard to build efficient and secure signature schemes

Two main approaches

Hash-and-Sign [1]
Large public keys

Zero Knowledge [2]
Large signatures



Zero Knowledge

No information on the secret is revealed.

Completeness

Honest prover always gets accepted.

Soundness

Negligible probability of accepting impersonators.

CROSS: Design Rationale [3]

Standard Optimizations

- PRNG and Merkle trees
- unbalanced challenges

EUF-CMA Security

- Fiat-Shamir [4] transformed ZK-ID
- no further assumptions

CROSS
Codes and Restricted Objects Signature Scheme

Decoding Problem

- compact objects
- no trapdoor required

Efficient Arithmetic

- small Mersenne primes
- no permutations

International Team

- Clemson, PoliMI, TUM, UNIVPM
- `www.cross-crypto.com`

NIST Competition

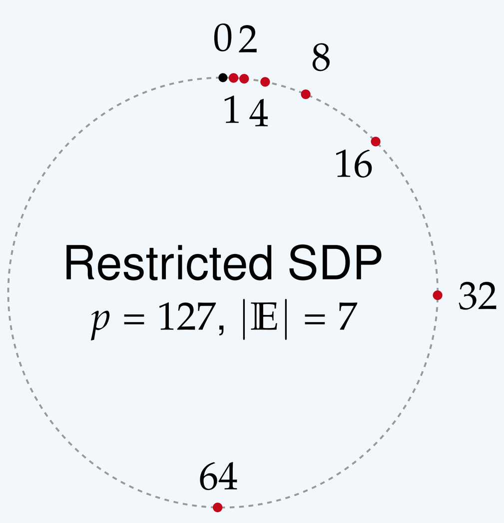
- standardization process [5]
- one of 40 candidates

The Underlying Hard Problem

Generalization of the classical SDP [6]:

Restricted Syndrome Decoding Problem

Let $\mathbb{E} \subset \mathbb{F}_p^*$, $\mathbf{H} \in \mathbb{F}_p^{(n-k)\times n}$, and $\mathbf{s} \in \mathbb{F}_p^{n-k}$.
Find $\mathbf{e} \in (\mathbb{E} \cup \{0\})^n$ with $\mathbf{e}\mathbf{H}^\top = \mathbf{s}$ and $\mathrm{wt}_\mathrm{H}(e) = w$.



For security category 1, the parameters of CROSS are

- random codes with $p = 127$, $n = 127$, $k = 76$,
- error values in $\mathbb{E} = \{1, 2, 4, 8, 16, 32, 64\}$, and $w = n$.

Modifying the Hard Problem

- Error set $\mathbb{E} = \{g^i \mid i \in \{1, \dots, z\}\} \subset \mathbb{F}_p^*$ with $g \in \mathbb{F}_p^*$ of prime order z.
- $(\mathbb{E}^n, \star)$ is group w.r.t. component-wise multiplication of vectors, denoted by $\star$.
- A subgroup is compactly represented as $G = \left\{e = g^x \mid x M^\top = \mathbf{0}\right\}$ with $M \in \mathbb{F}_z^{(n-m)\times n}$.

Restricted Syndrome Decoding Problem with Subgroup G

Let $M \in \mathbb{F}_z^{(n-m)\times n}$, $G = \left\{e = g^x \mid x M^\top = \mathbf{0}\right\}$, $\mathbf{H} \in \mathbb{F}_p^{(n-k)\times n}$, and $\mathbf{s} \in \mathbb{F}_p^{n-k}$.
Find a vector $\mathbf{e} \in G$ with $\mathbf{e}\mathbf{H}^\top = \mathbf{s}$.

$\Rightarrow$ solution unique w.h.p. for $z^m < p^{n-k}$

Example for R-SDP(G) instance

For $p = 7$ and $z = 3$, $g = 2$ has order 3, i.e., the error set is given by

$$\mathbb{E} = \{g^0 = 1,\ g^1 = 2,\ g^2 = 4\} \subset \mathbb{F}_7.$$

Let $n = 5$. To define a subgroup of $\mathbb{E}^5$ of order $m = 3$, we can use the parity-check matrix

$$M = \begin{pmatrix} 2 & 0 & 1 & 1 & 0 \\ 2 & 1 & 2 & 0 & 1 \end{pmatrix}, \text{ for which } (1, 2, 0, 1, 2)\cdot M^\top = (0, 0)\,.$$

Then, a valid error vector is computed as $e = \left(g^1 = 2, g^2 = 4, g^0 = 1, g^1 = 2, g^2 = 4\right) \in G$.
This error is the unique solution of the instance given by

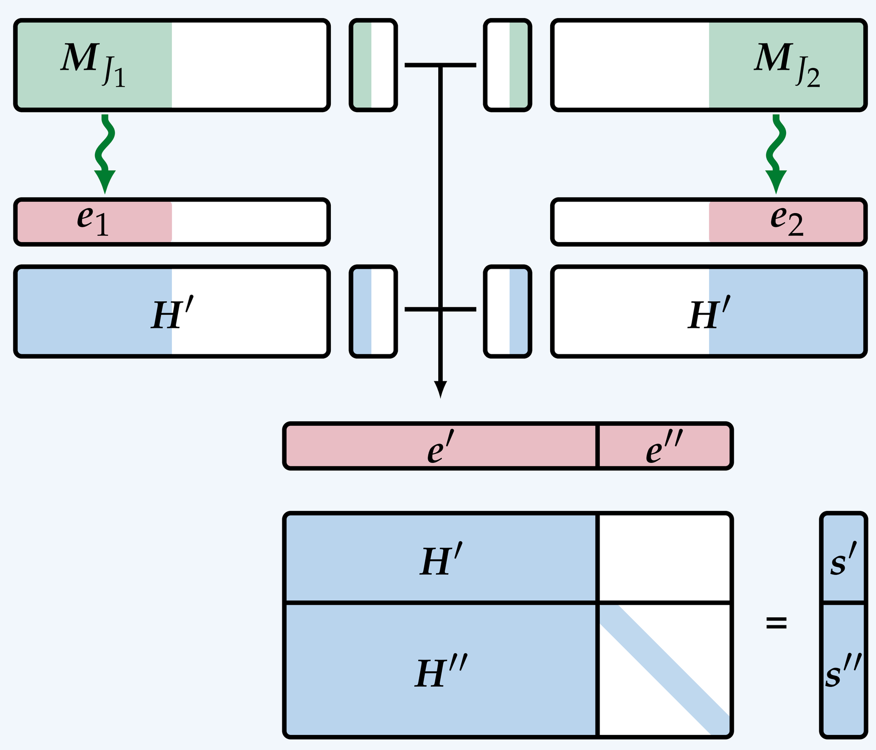
$$H = \begin{pmatrix} 1 & 0 & 6 & 1 & 5 \\ 0 & 1 & 0 & 3 & 4 \end{pmatrix} \text{ and } s = e \cdot H^T = (2, 5)\,.$$

For security category 1, the R-SDP(G) variant of CROSS uses

- random codes with $p = 509$, $n = 55$, $k = 36$,
- random subgroups with $z = 127$, $m = 25$.

A Meet-in-the-Middle Solver

Find subcodes of $\langle M \rangle$ of with support J_i of size $|J_i| = j_i$ and dimension $j_i - \rho_i$.



Bring H and M into quasi-systematic form w.r.t. J_1, J_2

Build lists $\mathcal{L}_1$, $\mathcal{L}_2$ of error vectors on J_1, J_2

Perform collision search on syndromes of small instances w.r.t. H and M

Enumerate solutions of small instance

Extend to full instance

Computational Complexity

Let $P(j_i, \rho_i)$ denote the probability that a subcode with dimension $j_i - \rho_i$ and support size j_i exists. Denote as $\mathcal{L}_i$ the list of errors e_i. Ignoring memory access cost and polynomial factors, the number of required operations is at least

$$\min_{j_1, j_2} \left\{ \frac{|\mathcal{L}_1| + |\mathcal{L}_2| + N_\mathrm{coll}}{1 + z^m p^{k-n}} + \frac{1}{P(j_1, \rho_1)\cdot P(j_2, \rho_2)} \right\},$$

where the list size is $|\mathcal{L}_i| = z^{\rho_i}$, and the number of collisions is given by

$$N_\mathrm{coll} = \frac{|\mathcal{L}_1| \cdot |\mathcal{L}_2|}{p^\ell \cdot z^{\ell'}},$$

since the effective syndromes sizes are $\ell = j_1 + j_2 - k$ and $\ell' = \max\{0, \rho_1 + \rho_2 - m\}$.

Further improvements?

References

[1] N. Courtois, M. Finiasz, N. Sendrier. ”How to achieve a McEliece-based digital signature scheme,” Asiacrypt, 2001.

[2] J. Stern, ”A new identification scheme based on syndrome decoding,” Annual International Cryptology Conference, 1993.

[3] M. Baldi A. Barenghi, S. Bitzer, P. Karl, F. Manganiello, A. Pavoni, G. Pelosi, P. Santini, J. Schupp, F. Slaughter, A. Wachter-Zeh, V. Weger, ”CROSS. Codes and restricted objects signature scheme,” Submission to NIST PQC Standardization Process, 2023.

[4] A. Fiat, A. Shamir, ”How to prove yourself: Practical solutions to identification and signature problems,” Crypto, 1986.

[5] NIST, ”Call for additional digital signature schemes for the post-quantum cryptography standardization process”, 2022

[6] 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.

6G-life
Deutsche Forschungsgemeinschaft
German Research Foundation