Code-Based Cryptography with Restricted Errors

Anna-Lena Horlemann

University of St. Gallen, Switzerland

CBCrypto, June 22th, 2021

Joint work with Marco Baldi, Massimo Battaglioni, Franco Chiaraluce, Karan Khathuria, Edoardo Persichetti, Paolo Santini and Violetta Weger.

Code-based cryptography

- Two general schemes for public key cryptosystems: *McEliece* (1978) and *Niederreiter* (1986).
- Related *signature scheme* by Courtois, Finiasz, Sendrier (2001), and other variants.
- Wave signature scheme (Debris-Alazard, Sendrier, Tillich), using high weight errors (2019).
- Code-based *zero-knowledge identification schemes*: Stern (1994), . . . , Cayrel-Véron-ElYousfiAlaoui (2011), . . .
- Can create signatures via the Fiat-Shamir transform (1986).

Main idea of code-based cryptosystems

- Decoding a random linear code is a hard problem.
- *Public key/information*: the parity check matrix of a random (looking) linear code, and a syndrome
- *Secret*: the solution to the corresponding syndrome decoding problem: usually a low-weight error vector (and/or the corresponding message/codeword)

$$\underbrace{\mathbf{s}}_{\text{syndrome}} = \underbrace{\mathbf{e}}_{\text{error vector}} \cdot \underbrace{\mathbf{H}^\top}_{\text{PC matrix}}$$

Main idea of code-based cryptosystems

- Decoding a random linear code is a hard problem.
- *Public key/information*: the parity check matrix of a random (looking) linear code, and a syndrome
- *Secret*: the solution to the corresponding syndrome decoding problem: usually a low-weight error vector (and/or the corresponding message/codeword)

$$\underbrace{\mathbf{s}}_{\text{syndrome}} = \underbrace{\mathbf{e}}_{\text{error vector}} \cdot \underbrace{\mathbf{H}^\top}_{\text{PC matrix}}$$

Various weights:

- Hamming weight
- rank weight
- Lee weight
- etc. (homogeneous weight, sum rank weight)

Reformulation and generalization

The syndrome decoding problem asks for a vector that is

1. an element of the coset of the subspace $\ker(\mathbf{H})$ given by $\mathbf{s}$,
2. in the sphere $\{\mathbf{x} \mid \mathrm{wt}(\mathbf{x}) = w\}$.

Reformulation and generalization

The syndrome decoding problem asks for a vector that is

1. an element of the coset of the subspace $\ker(\mathbf{H})$ given by $\mathbf{s}$,
2. in the sphere $\{\mathbf{x} \mid \mathrm{wt}(\mathbf{x}) = w\}$.

$\Longrightarrow$ we can replace 2) by any other property (or any set)

Reformulation and generalization

The syndrome decoding problem asks for a vector that is

1. an element of the coset of the subspace $\ker(\mathbf{H})$ given by $\mathbf{s}$,
2. in the sphere $\{\mathbf{x} \mid \mathrm{wt}(\mathbf{x}) = w\}$.

$\Longrightarrow$ we can replace 2) by any other property (or any set)

But what do we gain and what do we loose?

Reformulation and generalization

The syndrome decoding problem asks for a vector that is

1. an element of the coset of the subspace $\ker(\mathbf{H})$ given by $\mathbf{s}$,
2. in the sphere $\{\mathbf{x} \mid \mathrm{wt}(\mathbf{x}) = w\}$.

$\Longrightarrow$ we can replace 2) by any other property (or any set)

But what do we gain and what do we loose?

1. If we do not think about weights/distances any more, it is not code-based crypto.
2. For PKE we need an efficient "decoding" algorithm.
3. For identification schemes decoding is not necessary. But we need transitive linear maps on the property set (in the existing schemes).

The hardness of the more general SDP

Previously known:

1. Hamming SDP is NP-complete (Berlekamp et al. '78, Barg '94)
2. Probabilistic reduction for rank weight SDP from Hamming SDP (Gaborit-Zémor '16)

The hardness of the more general SDP

Previously known:

1. Hamming SDP is NP-complete (Berlekamp et al. '78, Barg '94)
2. Probabilistic reduction for rank weight SDP from Hamming SDP (Gaborit-Zémor '16)

Additive Weight Syndrome Decoding Problem (AW-SDP)

Let $\mathcal{A}$ be a ring with unity and $\mathrm{wt} : \mathcal{A} \to \mathcal{A}$ be a weight such that $\mathrm{wt}(0) = 0$, $\mathrm{wt}(x) > 0$ for any $x \neq 0$, extended addititvely to $\mathrm{wt}(x_1, \ldots, x_n) = \sum_{i=1}^{n} \mathrm{wt}(x_i)$.
On input $\mathbf{H} \in \mathcal{A}^{(n-k)\times n}$, $\mathbf{s} \in \mathcal{A}^{n-k}$ and $w \in \mathbb{N}$, decide whether there exists an $\mathbf{e} \in \mathcal{A}^n$ with $\mathrm{wt}(\mathbf{e}) = w$, such that $\mathbf{e}\mathbf{H}^\top = \mathbf{s}$.

The hardness of the more general SDP

Previously known:

1. Hamming SDP is NP-complete (Berlekamp et al. '78, Barg '94)
2. Probabilistic reduction for rank weight SDP from Hamming SDP (Gaborit-Zémor '16)

Additive Weight Syndrome Decoding Problem (AW-SDP)

Let $\mathcal{A}$ be a ring with unity and $\mathrm{wt} : \mathcal{A} \to \mathcal{A}$ be a weight such that $\mathrm{wt}(0) = 0$, $\mathrm{wt}(x) > 0$ for any $x \neq 0$, extended addititvely to $\mathrm{wt}(x_1, \ldots, x_n) = \sum_{i=1}^{n} \mathrm{wt}(x_i)$.
On input $\mathbf{H} \in \mathcal{A}^{(n-k)\times n}$, $\mathbf{s} \in \mathcal{A}^{n-k}$ and $w \in \mathbb{N}$, decide whether there exists an $\mathbf{e} \in \mathcal{A}^n$ with $\mathrm{wt}(\mathbf{e}) = w$, such that $\mathbf{e}\mathbf{H}^\top = \mathbf{s}$.

Theorem

The AW-SDP is NP-complete.

Proof: Adaption of the proof of the classical SDP.

Our idea: ID scheme with very simple additive weight

Definition (Restricted weight)

Consider a ring $\mathcal{A}$ with unity as alphabet.

$$\mathrm{wt}_{rst}(x) := \begin{cases} 0 & x = 0 \\ 1 & x \in \{\pm 1\} \\ \infty & \text{else} \end{cases}$$

$$\mathrm{wt}_{rst}(x_1, \ldots, x_n) := \sum_{i=1}^{n} \mathrm{wt}(x_i)$$

Our idea: ID scheme with very simple additive weight

Definition (Restricted weight)

Consider a ring $\mathcal{A}$ with unity as alphabet.

$$\mathrm{wt}_{rst}(x) := \begin{cases} 0 & x = 0 \\ 1 & x \in \{\pm 1\} \\ \infty & \text{else} \end{cases}$$

$$\mathrm{wt}_{rst}(x_1, \ldots, x_n) := \sum_{i=1}^{n} \mathrm{wt}(x_i)$$

The non-trivial spheres w.r.t. the restricted weight coincide with the Hamming- or Lee-spheres in the *restricted space* $\{0, \pm 1\}^n \subseteq \mathcal{A}^n$.

Coding theory for restricted errors

Restricted weight and minimum distance

Definition

Let $\mathbb{F}_q$ have characteristic ≥ 5. For $\mathbf{a} \in \mathbb{F}_q^n$, we define the *extended restricted weight* of $\mathbf{a}$ as

$$\widetilde{\mathrm{wt}}(\mathbf{a}) := \begin{cases} \#_1(\mathbf{a}) + 2 \cdot \#_2(\mathbf{a}) & \text{if } \mathbf{a} \in \{0, \pm 1, \pm 2\}^n, \\ \infty & \text{otherwise,} \end{cases}$$

where $\#_1(\mathbf{a})$ is the number of entries of $\mathbf{a}$ equal to ± 1 and $\#_2(\mathbf{a})$ is the number of entries equal to ± 2.
Let $\mathcal{C}$ be a linear code with length n over $\mathbb{F}_q$. We define its *extended restricted minimum distance* as

$$\widetilde{d} := \min\left\{\widetilde{\mathrm{wt}}(\mathbf{c}) \mid \mathbf{c} \in \mathcal{C} \cap (\{0, \pm 1, \pm 2\}^n \setminus \{\mathbf{0}_n\})\right\}.$$

If $\mathcal{C} \cap \{0, \pm 1, \pm 2\}^n = \{\mathbf{0}_n\}$, then we set $\widetilde{d} = \infty$.

(ext. restricted min. distance = min. Lee distance of restricted code)

Unique decodability

$E_{n,q,w} := \{\mathbf{e} \in \{0, \pm 1\}^n \mid \mathrm{wt}_H(\mathbf{e}) \leq w\}$

Theorem

Let $\mathcal{C} \subseteq \mathbb{F}_q^n$ have extended restricted minimum distance $\widetilde{d}$. For any parity-check matrix $\mathbf{H}$ for $\mathcal{C}$, and for all $w < \widetilde{d}/2$, there cannot exist two distinct vectors $\mathbf{e}, \mathbf{e}' \in E_{n,q,w}$ such that $\mathbf{e}\mathbf{H}^\top = \mathbf{e}'\mathbf{H}^\top$.

Unique decodability

$E_{n,q,w} := \{\mathbf{e} \in \{0, \pm 1\}^n \mid \mathrm{wt}_H(\mathbf{e}) \leq w\}$

Theorem

Let $\mathcal{C} \subseteq \mathbb{F}_q^n$ have extended restricted minimum distance $\widetilde{d}$. For any parity-check matrix $\mathbf{H}$ for $\mathcal{C}$, and for all $w < \widetilde{d}/2$, there cannot exist two distinct vectors $\mathbf{e}, \mathbf{e}' \in E_{n,q,w}$ such that $\mathbf{e}\mathbf{H}^\top = \mathbf{e}'\mathbf{H}^\top$.

Proof:

- $\mathbf{e}\mathbf{H}^\top = \mathbf{e}'\mathbf{H}^\top \iff (\mathbf{e} - \mathbf{e}')$ is codeword;
- $\mathbf{e} - \mathbf{e}' \in \{0, \pm 1, \pm 2\}^n$ and has extended restricted weight less than $\widetilde{d}$;
- $\mathbf{e} - \mathbf{e}' = \mathbf{0} \iff \mathbf{e} = \mathbf{e}'$.

Unique decodability

$E_{n,q,w} := \{\mathbf{e} \in \{0, \pm 1\}^n \mid \mathrm{wt}_H(\mathbf{e}) \leq w\}$

Theorem

Let $\mathcal{C} \subseteq \mathbb{F}_q^n$ have extended restricted minimum distance $\widetilde{d}$. For any parity-check matrix $\mathbf{H}$ for $\mathcal{C}$, and for all $w < \widetilde{d}/2$, there cannot exist two distinct vectors $\mathbf{e}, \mathbf{e}' \in E_{n,q,w}$ such that $\mathbf{e}\mathbf{H}^\top = \mathbf{e}'\mathbf{H}^\top$.

Proof:

- $\mathbf{e}\mathbf{H}^\top = \mathbf{e}'\mathbf{H}^\top \iff (\mathbf{e} - \mathbf{e}')$ is codeword;
- $\mathbf{e} - \mathbf{e}' \in \{0, \pm 1, \pm 2\}^n$ and has extended restricted weight less than $\widetilde{d}$;
- $\mathbf{e} - \mathbf{e}' = \mathbf{0} \iff \mathbf{e} = \mathbf{e}'$.

Note: If $\mathrm{char}(\mathbb{F}_q) = 3$, then $\mathbf{e} - \mathbf{e}' \in \mathbb{F}_3$ and similar result holds.

Gilbert-Varshamov bound

Theorem

For a given finite extended restricted minimum distance $\widetilde{d}$ and length n, there exists a code in $\mathbb{F}_q^n$ of dimension $\tilde{k}$, where

$$\begin{aligned}\tilde{k} &\geq n - 1 - \log_q \left(\widetilde{V}(n, \widetilde{d} - 1) \right) \\ &= n - 1 - \log_q \left(\sum_{i=0}^{\widetilde{d}-1} \sum_{j=\max\{0, i-n\}}^{\lfloor i/2 \rfloor} \binom{n}{j} \binom{n-j}{i-2j} 2^{i-j} \right).\end{aligned}$$

Gilbert-Varshamov bound

Theorem

For a given finite extended restricted minimum distance $\widetilde{d}$ and length n, there exists a code in $\mathbb{F}_q^n$ of dimension $\tilde{k}$, where

$$\begin{aligned}\tilde{k} &\geq n - 1 - \log_q\left(\widetilde{V}(n, \widetilde{d} - 1)\right) \\ &= n - 1 - \log_q\left(\sum_{i=0}^{\widetilde{d}-1} \sum_{j=\max\{0,i-n\}}^{\lfloor i/2 \rfloor} \binom{n}{j}\binom{n-j}{i-2j} 2^{i-j}\right).\end{aligned}$$

Definition

For a code with length n and dimension k over $\mathbb{F}_q$, we define the *extended restricted Gilbert-Varshamov distance* as

$$\widetilde{d}_{\mathsf{GV}} := \begin{cases} \infty & \text{if } \widetilde{V}(n, 2n) < q^{n-k-1}, \\ \max\left\{\widetilde{d} > 0 \;\middle|\; \widetilde{V}(n, \widetilde{d}) \leq q^{n-k-1}\right\} & \text{otherwise.} \end{cases}$$

Random codes and the GV-bound

Note that $\widetilde{V}(n, 2n) = 5^n$, and hence for large values of q and/or n (if $q > 5$), the restricted Gilbert-Varshamov distance is equal to ∞, as long as $k < n(1 - \log_q(5) - \frac{1}{n})$.

Theorem

Let $q > 5$ be an odd prime power and $k \leq n\left(1 - \log_q(5) - \epsilon\right)$, for $0 < \epsilon < 1 - \log_q(5)$. Let $\mathbf{G} \xleftarrow{\$} \mathbb{F}_q^{k \times n}$ with rank k. Then the code generated by $\mathbf{G}$ has extended restricted minimum distance $\widetilde{d} = \infty$ with probability at least $1 - q^{-\epsilon n}$.

Random codes and the GV-bound

Note that $\widetilde{V}(n, 2n) = 5^n$, and hence for large values of q and/or n (if $q > 5$), the restricted Gilbert-Varshamov distance is equal to ∞, as long as $k < n(1 - \log_q(5) - \frac{1}{n})$.

Theorem

Let $q > 5$ be an odd prime power and $k \leq n\left(1 - \log_q(5) - \epsilon\right)$, for $0 < \epsilon < 1 - \log_q(5)$. Let $\mathbf{G} \xleftarrow{\$} \mathbb{F}_q^{k \times n}$ with rank k. Then the code generated by $\mathbf{G}$ has extended restricted minimum distance $\widetilde{d} = \infty$ with probability at least $1 - q^{-\epsilon n}$.

$\implies$ In a random code with $k \leq n\left(1 - \log_q(5) - \epsilon\right)$ we can uniquely decode ANY $\mathbf{e} \in \{0, \pm 1\}^n$.

Now we can set up a zero-knowledge identification scheme (for security and simplicity over $\mathbb{F}_p$)

The CVE scheme with restricted errors

Public Data	Parameters $p, n, k \in \mathbb{N}$, parity-check matrix $\mathbf{H} \in \mathbb{F}_p^{(n-k)\times n}$
Private Key	$\mathbf{e} \in \mathrm{E}_{n,p,w}$
Public Key	$\mathbf{s} = \mathbf{e}\mathbf{H}^\top \in \mathbb{F}_p^{n-k}$

PROVER		VERIFIER
Choose $\mathbf{u} \xleftarrow{\$} \mathbb{F}_p^n$, $\tau \xleftarrow{\$} \widetilde{\mathfrak{M}}_n$		
Set $c_0 = \mathsf{Hash}\big(\tau, \mathbf{u}\mathbf{H}^\top\big)$		
Set $c_1 = \mathsf{Hash}\big(\tau(\mathbf{u}), \tau(\mathbf{e})\big)$		
	$\xrightarrow{c_0, c_1}$	
		Choose $z \xleftarrow{\$} \mathbb{F}_p^*$
	$\xleftarrow{z}$	
Set $\mathbf{y} = \tau(\mathbf{u} + z\mathbf{e})$		
	$\xrightarrow{\mathbf{y}}$	
		Choose $b \xleftarrow{\$} \{0, 1\}$
	$\xleftarrow{b}$	
If $b = 0$, set $f := \tau$		
If $b = 1$, set $f := \mathbf{e}' = \tau(\mathbf{e})$		
	$\xrightarrow{f}$	
		If $b = 0$, accept if $c_0 = \mathsf{Hash}\big(\tau, \tau^{-1}(\mathbf{y})\mathbf{H}^\top - z\mathbf{s}\big)$
		If $b = 1$, accept if $\mathbf{e}' \in \mathrm{E}_{n,p,w}$ and $c_1 = \mathsf{Hash}\big(\mathbf{y} - z\mathbf{e}', \mathbf{e}'\big)$

Comparison of signatures from ZK-ID schemes[1]

- security level $\lambda = 128$ bits
- seeds and hashes of 256 bits
- Restricted CVE parameters: $p = 31$, $n = w = 256$, $k = 204$

	CVE	AGS	Rest. CVE
Number of rounds	129	128	135
Public key size (bits)	832	1574	260
Average sig. size (kB)	43.263	41.040	30.373
Max sig. size (kB)	51.261	56.992	30.373

[1] Based on adaptations of known generic (birthday paradox) decoders.
Disclaimer: We are currently recomputing the parameters due to new subset sum solvers. The final sig. size will be slightly larger, but smaller than CVE/AGS.

More comparisons

- Restricted CVE: security 128 bits, public key size 260 bits, signature size 30 kB
- cRVDC-125 (Bellini et al., 2019, rank-metric code-based): security 125 bits, public key 1212 bits, average signature size 22 kB
- Durandal (Aragon et al., 2019, rank-metric code-based): security 128 bits (with some security concerns), public key size 15 kB, signature size ca. 4 kB
- LESS (Biass et al., 2020, code-equivalence-based): security 128 bits, public key size and signature size ca. 15 kB
- Wave (Debris-Alazard et al., 2019, code-based hash-and-sign): security 128 bits, public key size 3.2 MB, signature size ca. 1.6 kB

More comparisons

- Restricted CVE: security 128 bits, public key size 260 bits, signature size 30 kB
- cRVDC-125 (Bellini et al., 2019, rank-metric code-based): security 125 bits, public key 1212 bits, average signature size 22 kB
- Durandal (Aragon et al., 2019, rank-metric code-based): security 128 bits (with some security concerns), public key size 15 kB, signature size ca. 4 kB
- LESS (Biass et al., 2020, code-equivalence-based): security 128 bits, public key size and signature size ca. 15 kB
- Wave (Debris-Alazard et al., 2019, code-based hash-and-sign): security 128 bits, public key size 3.2 MB, signature size ca. 1.6 kB

$\Longrightarrow$ Restricted CVE minimizes public key size!

Summary and conclusions

- We studied the syndrome decoding problem for additive weights and showed that it is NP-complete.
- We derived GV bound to estimate minimum extended restricted distance of random codes.
- We derived generic decoder for special instance of restricted SDP.
- We used this in the CVE zero-knowledge identification scheme, and could reduce the used field size, for otherwise comparable parameters (length, dimension, security level).
- With Fiat-Shamir we can create digital signatures that have very small public key sizes.
- Due to smaller field size, and only ± 1-multiplication, implementation is very fast.

Summary and conclusions

- We studied the syndrome decoding problem for additive weights and showed that it is NP-complete.
- We derived GV bound to estimate minimum extended restricted distance of random codes.
- We derived generic decoder for special instance of restricted SDP.
- We used this in the CVE zero-knowledge identification scheme, and could reduce the used field size, for otherwise comparable parameters (length, dimension, security level).
- With Fiat-Shamir we can create digital signatures that have very small public key sizes.
- Due to smaller field size, and only ± 1-multiplication, implementation is very fast.

Thank you for your attention!

Questions? – Comments?