Y. Wang's RLCE

National Institute of Standards and Technology
U.S. Department of Commerce

March 6, 2018

Outline

1. Motivation - McEliece / Niederreiter
2. Sidelnikov - Shestakov Attack
3. RLCE setup and algorithms
4. Sizes and performance

Motivation: McEliece / Niederreiter Review

Let $q = 2^m$.

- Let $n, k, d > 0$ with $n - k + 1 \geq d$.
- Let G be a $k \times n$ generator matrix for an $[n, k, d]$ generalized Reed Solomon code $\mathcal{C}$ over $GF(q)$.
- Let S be a randomly chosen $k \times k$ nonsingular matrix.
- Let $e \in GF(q)^n$ have weight at most $t = \lfloor (d-1)/2 \rfloor$.
- SG is the public key.
- To encrypt: $c = mSG + e$.

Decrypt

- $c = mSG + e$.
- Decode c using knowledge of G.
- $m = (mS)S^{-1}$.

Generalized Reed-Solomon Codes

- Let F be a finite field.
- Let $\alpha, x \in F^n$, with $x_i \neq 0$, α_i distinct.
- Define $G_{ij} := \alpha_j^i x_j$, i.e. $G = \begin{bmatrix} x_0 & x_1 & \dots & x_{n-1} \\ \alpha_0 x_0 & \alpha_1 x_1 & \dots & \alpha_{n-1} x_{n-1} \\ \vdots & & \ddots & \vdots \\ \alpha_0^{k-1} x_0 & \alpha_1^{k-1} x_1 & \dots & \alpha_{n-1}^{k-1} x_{n-1} \end{bmatrix}$.
- G is a generator matrix for the code $GRS_{n,k}(\alpha, x)$.
- Same as $\{(x_0 f(\alpha_0), \dots, x_{n-1} f(\alpha_{n-1})) | f \in GF(q)[x], \deg f < k\}$.

Sidelnikov - Shestakov Attack

- Observe that $GRS_{n,k}(\alpha, x) = GRS_{n,k}((a\alpha_0 + b, ..., a\alpha_{n-1} + b), (cx_0, ..., cx_{n-1}))$ for all b and nonzero $a, c \in F$.
- Assume $\alpha_0 = 0, \alpha_1 = 1$.
- Row reduce SG to produce $E(SG)$.
- This produces the following k equations: $x_j f_i(\alpha_j) = 0$ for $j < k, j \neq i$.
- Since deg $f_i < k$,

$$f_i(y) = c_i \prod_{j<k, j\neq i} (y - \alpha_j).$$

- Divide one row by another, coordinate-wise:

$$\frac{x_j f_0(\alpha_j)}{x_j f_i(\alpha_j)} = \frac{c_0(\alpha_j - \alpha_i)}{c_i(\alpha_j - \alpha_0)} \tag{1}$$

- First fix $i = 1$ and take $j \geq k$ to solve for α_j.
- Then use $j = k, k+1$ to solve for α_i, $i < k$.

- Let G' be the $k+1$ leftmost columns of G.
- Find a nontrivial c in the right kernel of SG', which are the leftmost $k+1$ columns in the public key.
- Then c is in the right kernel of G' as well.
- Let $G(\alpha', y')'$ and x' be similar truncations.
- Observe that $G(\alpha', c)'x' = G(\alpha, x')c = G'c = 0$, and use this to solve for x', assuming $x_0 = 1$.

- Let G'' be the truncation to the first k rows.
- $S = SG''(G'')^{-1}$.
- $G = S^{-1}(SG)$.

Setup

- Let $q = 2^m$.
- Let $n, k, d > 0$ with $n - k + 1 \geq d$.
- Let G_s be a $k \times n$ generator matrix for an $[n, k, d]$ generalized Reed Solomon code $\mathcal{C}$ over $GF(q)$.
- Let P_1 be a randomly chosen $n \times n$ permutation matrix.

More Setup

- Let $w \leq n$.
- Insert w random column vectors r_i into $G_s P_1$ after column $n - w$ (zero indexed) to produce G_1.
- $G_s P_1 = [g_0, \ldots, g_{n-1}]$.
- $G_1 = [g_0, \ldots, g_{n-w}, r_0, g_{n-w+1}, \ldots, g_{n-1}, r_{w-1}]$.
- Let S be a random dense $k \times k$ non-singular matrix.
- Let P_2 be an $(n + w) \times (n + w)$ permutation matrix.

Key Setup

- Let A_i be 2×2 non-singular matrices chosen randomly such that the product of the entries is nonzero, for $i < w$.
- Let $A = \begin{bmatrix} I_{n-w} & & & \\ & A_0 & & \\ & & \ddots & \\ & & & A_{w-1} \end{bmatrix}$.
- The public key is $G = SG_1AP_2$.
- The private key is (S, G_s, P_1, P_2, A).
- S may instead be chosen so that G is in row echelon form, making this a systematic scheme.

Encryption

- A message m is an element of $GF(q)^k$.
- $d \geq 2t + 1$ (usually).
- Choose $e \in GF(q)^{n+w}$ with $wt(e) \leq t$ randomly.
- Return $c = mG + e$.

Decryption

- Compute

$$\begin{aligned} cP_2^{-1}A^{-1} &= (mSG_1AP_2 + e)P_2^{-1}A^{-1} \\ &= mSG_1 + eP_2^{-1}A^{-1}. \end{aligned}$$

- Remove the w coordinates corresponding to the r_i's. This leaves a vector c' of length n.
- $c'P_1^{-1} = mSG_s + e'$ for some $e' \in GF(q)^n$ of weight at most t.
- Decode and truncate mSG_s to the first k terms to produce c_1.
- Let G_s' be the first k columns of G_s, and let $D = (SG_s')^{-1}$.
- $m = c_1D$.

Sidelnikov - Shestakov on RLCE

- $2w$ columns are randomized. Assume that they can be identified (filtration attack).
- if $w \geq n - k$, we can't establish the formula for polynomials f_i.
- If $w < n - k$ we can only recover x_j for $j < n - w$. Therefore, we must ensure that there are too many remaining x_j to guess.
- The probability is bounded by

$$\frac{1}{\left(1-\frac{n+w+1}{w}\right) w!}.$$

Some Notes

- The public key can be made smaller by using a systematic version of the scheme.
- The Berlekamp-Massey decoding algorithm is used to decode.

Parameters

κc	κq	n	k	t	w	sk	cipher	pk	mLen
128	80	630	470	80	160	310,116	988	188,001	550
128	80	532	376	78	96	179,946	785	118,441	4540
192	110	1000	764	118	236	747,393	1545	450,761	8820
192	110	846	618	114	114	440,008	1238	287,371	7320
286	144	1360	800	280	560	1,773,271	2640	1,232,001	11880
286	144	1160	700	230	311	1,048,176	2023	742,089	10230

	Goppa	RLCE
192	490	280
256	900	724

Figure: Public Key size in KB

Figure: Performance Comparison in Milliseconds

κc	RSA modulus	key setup		encryption		decryption	
	.	RSA	RLCE	RSA.	RLCE	RSA.	RLCE
128	3072	433.607	151.834	0.135540	0.360	6.576281	1.345
192	7680	9346.846	637.988	0.672769	0.776	75.075443	2.676
256	15360	80790.751	1587.330	2.498523	1.745	560.225740	9.383

Both RLCE and Open SSL RSA were performed on MacOS Sierra on a MacBook Pro with 2.9 GHz Intel Core i7.

References

- H. Niederreiter, *Knapsack-type cryptosystems and algebraic coding theory*, Problemy Upravlenija i Teorii Informacii, (1986) 15: pp. 159?166.
- S. Shestakov, V. Sidelnikov, *On insecurity of cryptosystems based on generalized Reed-Solomon codes*, 1992.
- Y. Wang, *RLCE Key Encapsulation Mechanism (RLCE-KEM) Specification*, 2017.
- C. Wieschebrink, *Cryptanalysis of the Niederreiter Public Key Scheme Based on GRS Subcodes*, `https://eprint.iacr.org/2009/452.pdf`, 2009.