

Multivariate Quadratic Cryptography

Ward Beullens

July 26, 2022

Exercise session 1

Exercise 1. Are multivariate quadratic maps collision resistant? I.e., given a random quadratic map $\mathcal{P} : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^n$, is it hard to find \mathbf{x}, \mathbf{x}' such that $\mathbf{x} \neq \mathbf{x}'$ and $\mathcal{P}(\mathbf{x}) = \mathcal{P}(\mathbf{x}')$?

Hint: Suppose there is a collision $\mathbf{x} \neq \mathbf{x}'$ such that $\mathcal{P}(\mathbf{x}) = \mathcal{P}(\mathbf{x}')$. Then $\mathbf{x} - \mathbf{x}'$ is a non-zero vector in the kernel of the Jacobian matrix of \mathcal{P} at \mathbf{x} .

Definition 1 (Macaulay matrix). Let $p_1, \dots, p_m \in K[x_1, \dots, x_n]$ be a sequence of multivariate quadratic polynomials. We say the Macaulay matrix of p_1, \dots, p_m at degree D is the matrix whose $\binom{n+D}{D}$ columns correspond to monomials of degree at most D in the variables x_1, \dots, x_n , and whose $m \binom{n+D-2}{D-2}$ rows correspond to the polynomials of the form Mp_i , where M is a monomial of degree at most $D-2$ and $i \in \{1, \dots, m\}$.

Exercise 2 (Rank of Macaulay matrices of random quadratic polynomials). Let $p_1, \dots, p_m \in K[x_1, \dots, x_n]$ be a sequence of multivariate quadratic polynomials. Let $[p_1, \dots, p_k]_{\leq d}$ be the vectorspace spanned by all the polynomials of the form $x^\alpha p_i$, where x^α is a monomial of degree at most $d-2$, and where $1 \leq i \leq k$. That is, $[p_1, \dots, p_k]_{\leq d}$ corresponds to the span of the rows of the Macaulay matrix of p_1, \dots, p_k at degree d .

Clearly, we have $[p_1, \dots, p_k]_{\leq d-2} \cdot p_{k+1} \subset [p_1, \dots, p_k]_{\leq d} \cap [p_{k+1}]_{\leq d}$. Suppose that this is an equality for all $k \in \{0, \dots, m-1\}$ and all d , such that $[p_1, \dots, p_m]_{\leq d} \neq K[x_1, \dots, x_n]_{\leq d}$. (Random systems satisfy this property with high probability.)

- Prove that $\dim(K[x_1, \dots, x_n]_{\leq d})$ is equal to the coefficient of t^d in the power series expansion of

$$\frac{1}{(1-t)^{n+1}}.$$

- Prove that $\dim([p_1, \dots, p_m]_{\leq d})$ is equal to the coefficient of t^d in the power series expansion of

$$\frac{1 - (1-t)^m}{(1-t)^{n+1}},$$

for all d such that $[p_1, \dots, p_m]_{\leq d} \neq K[x_1, \dots, x_n]_{\leq d}$

- Conclude that the Macaulay matrix of p_1, \dots, p_m at degree D has full rank if there exists $d \leq D$ such that the coefficient of t^d in the power series expansion of

$$\frac{(1-t^2)^m}{(1-t)^{n+1}}$$

has a non-positive coefficient.

Exercise 3. Suppose $p_1(x) = \dots = p_m(x) = 0$ is a system of quadratic polynomials with a solution $x' \in K^n$. Prove that the Macaulay matrix of p_1, \dots, p_m is never full rank, by writing down a vector in the kernel.

XL algorithm. If $p_1(x) = \dots = p_m(x) = 0$ is a random system with a solution, then heuristically, the ranks of Macaulay matrices of this system are the same as those in Exercise 2, except that when the Macaulay matrix from Exercise 2 has full rank, the Macaulay matrix of a system with a solution has corank 1 instead. The XL algorithm works by constructing the Macaulay matrix at a degree D that is high enough such that the Macaulay matrix has a kernel of rank 1. Then the algorithm does linear algebra to find the vector from Exercise 3, from which the solution x can be recovered easily.

A naive implementation of Gaussian Elimination would require $O(\binom{n+D}{D}^3)$ multiplications. But the Macaulay matrix is very sparse (each row has at most $\binom{n+2}{2}$ non-zero entries), so with sparse linear algebra methods the kernel vector can be found with roughly

$$3 \binom{n+2}{2} \binom{n+D}{D}^2 \tag{1}$$

multiplications instead.

It is often beneficial to guess the values of a few variables before applying the XL algorithm. This reduces the number of variables, which often allows the algorithm to run at a lower degree D , which makes it much more efficient. The drawback is that if you make k guesses, the algorithm needs to be repeated roughly q^k times, so guessing k variables is beneficial if the cost of the XL algorithm is reduced by more than a factor q^k . This variant of the XL algorithm is often called HybridXL, because it is a hybrid between XL ($k = 0$) and exhaustive search ($k = n$).

Exercise 4 (Estimate the cost of solving the MQ problem). We estimate the cost of solving some multivariate quadratic systems, to illustrate the fact that finding a solution becomes much easier if more equations are given. Use Exercise 2 to find D , and use formula (1) for the cost of the linear algebra.

- Let $\mathcal{P} : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^m$, be a random quadratic map with $n = 40$ and $m = 80$, and $q = 256$. Give an estimate of the cost (number of field multiplications) of the XL algorithm to find \mathbf{x} , given $\mathcal{P}(\mathbf{x})$.
- Let $\mathcal{P} : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^m$, be a random quadratic map with $n = 40$ and $m = 40$, and $q = 256$. Find the optimal number of guesses for the HybridXL algorithm, and estimate the cost of running the algorithm.

You might want to use a computer algebra system for your calculations.

Answer: Solving the first system takes 2^{69} multiplications, the operating degree is $D = 8$. Solving the second algorithm takes 2^{129} multiplications. Answer: $D = 18$ and 3 guesses for $k = 3$ guesses and 18.

Excercise session 2: Breaking a simplified version of the Matsumoto-Imai scheme.

Let $K = GF(q)$ be a finite field of order q , and let L be a field extension of degree n . Let θ be an integer such that $\gcd(1 + q^\theta, q^n - 1) = 1$.

Exercise 5. Consider the exponentiation map $E_\theta : L \rightarrow L : x \mapsto x^{q^\theta + 1}$. Prove that E_θ is a bijection. Give a polynomial-time algorithm that given θ and $y \in L$, outputs $E_\theta^{-1}(y) \in L$.

Exercise 6. Let $T : L \rightarrow K^n$ and $S : K^n \rightarrow L$ be invertible K -linear maps (L is a K -vector space of dimension n). Prove that $F = T \circ E_\phi \circ S$ is a multivariate quadratic map.

In 1988, Matsumoto and Imai [1] proposed a variant of the following public-key cryptosystem: Fix public parameters q, n, θ . The private key consists of two randomly chosen invertible linear maps $T : L \rightarrow K^n$ and $S : K^n \rightarrow L$, the public key is the multivariate map $P : K^n \rightarrow K^n = T \circ E_\theta \circ S$. To encrypt a message $m \in K^n$, a user just evaluates $P(m)$, which he can send over the wire. Given, T and S , one can efficiently decrypt the ciphertext $P(m) = T \circ E_\theta \circ S(m)$ by first undoing T , then undoing E_θ , and finally undoing S .

Exercise 7. Show that the Matsumoto-Imai scheme is not secure with the parameters $q = 256, n = 41, \theta = 1$. That is, give an efficient algorithm that given a public key $P : K^n \rightarrow K^n$, and a ciphertext $c = P(m) \in K^n$ outputs the message $m \in K^n$.

Hint 1: We saw that the relation $y = x^{q^\theta+1}$ becomes quadratic when viewed over K , wouldn't it be nice if this implied some other equation that becomes linear in the coefficients of x and y instead?

Hint 2: Raise both sides of the equation to the power q and multiply both sides by yx .

Hint 3: If you know that input-output pairs of the cryptosystem satisfy some polynomial equations with (not too many) unknown coefficients, you can just evaluate P on a lot of inputs, and solve for the coefficients.

Exercise 8. Implement your attack. Download [a SAGE file](#) and a [public key and ciphertext](#), and recover the message.

References

- [1] Tsutomu Matsumoto and Hideki Imai. Public quadratic polynomial-tuples for efficient signature-verification and message-encryption. In C. G. Günther, editor, *EUROCRYPT'88*, volume 330 of *LNCS*, pages 419–453, Davos, Switzerland, May 25–27, 1988. Springer, Heidelberg, Germany. [\(document\)](#)