Selected Areas in Cryptology - Part 1: Post-quantum cryptography

Exercise sheet 2, 19 February 2024

1. Let us consider the following problem. Given matrices $\mathbf{C}^{(1)}$, $\mathbf{C}^{(2)}$, $\mathbf{D}^{(1)}$, $\mathbf{D}^{(2)} \in \mathcal{M}_{n\times n}(q)$ (the space of matrices over $\mathbb{F}_q$ of size $n \times n$), find $\mathbf{A}, \mathbf{B} \in \mathrm{GL}_n(q)$ (the space of invertible matrices over $\mathbb{F}_q$ of size $n \times n$), such that

$$\mathbf{D}^{(1)} = \mathbf{A}\mathbf{C}^{(1)}\mathbf{B}$$
$$\mathbf{D}^{(2)} = \mathbf{A}\mathbf{C}^{(2)}\mathbf{B}.$$

   (a) Write down the multivariate system of equations that this problem reduces to. **Hint:** For instance, the entries of some matrix $\mathbf{M}$ can be denoted as $(m_{1,1}, \ldots, m_{1,n}, \ldots m_{n,1}, \ldots, m_{n,n})$. Then, the equations representing $\mathbf{M}^{(1)}\mathbf{M}^{(2)} = \mathbf{P}$, for some matrix $\mathbf{P}$ are

$$p_{i,j} = \sum_{t=1}^{n} m_{i,t}^{(1)} m_{t,j}^{(2)}, \text{ for all } 1 \leq i \leq j \leq n.$$

   (b) What is the degree of this system, and what is the number of variables (unknowns) and equations?

   (c) Can you find a better modelisation for this problem? **Hint:** You can find one that results in a linear system of equations.

2. Write down a UOV toy example with $v = 3$ vinegar variables and $m = 2$ oil variables over $\mathbb{F}_3$. You need to detail the three steps: key generation, signing, and verification. Recall, that the number of equations in the central map is chosen to be equal to the number of variables. **Hint:**

   (a) Choose randomly the central map f.

   (b) Choose a random linear map $\mathbf{S}$, making sure it is invertible (use Magma or SageMath if needed).

   (c) Compute the public map p from f and $\mathbf{S}$. Key generation is done;

   (d) Choose $H(\mathrm{m}) = (1, 1)$ (the hash of a message m).

   (e) Fix randomly the vinegar variables.

(f) Solve the linear system to find the assignment of the oil variables. If there is no solution, go back to the previous step and choose another random assignment for the vinegar variables.

(g) Multiply the solution with $\mathbf{S}^{-1}$ on the left. State what the signature is.

(h) For the verification, check whether the vector that was sent as a signature, is indeed a preimage of $H(\mathrm{m}) = (1, 1)$ under p.

3. Calculate the public key, secret key and signature sizes (in bytes) for a UOV key with parameters $v = 66$, $m = 44$, $q = 2^8$. **Hint:** Find the number of elements over $\mathbb{F}_q$ that you need to store. This coincides with the number of bytes.

4. Consider the *direct* attack on a UOV instance with parameters $v = 66$, $m = 44$, $q = 2^8$.

   (a) Write down the multivariate system of equations that this problem reduces to. **Hint:** See Exercise 1 for what this answer should look like.

   (b) What is the degree of this system, and what is the number of variables (unknowns) and equations?

   (c) What is the complexity of solving this system using a Gröbner-based algorithm?

5. Consider the *reconciliation* attack on a UOV instance with parameters $v = 66$, $m = 44$, $q = 2^8$. Answer the following questions only for the systems that are created in the **first two** iterations of the loop.

   (a) Write down the multivariate system of equations that this problem reduces to. **Hint:** See Exercise 1 for what this answer should look like.

   (b) What is the degree of this system, and what is the number of variables (unknowns) and equations?

   (c) What is the complexity of solving this system using a Gröbner-based algorithm?

6. Consider the *intersection* attack (the version described on the slides - no need to go into the generalisation that you might find in the literature) on a UOV instance with parameters $v = 66$, $m = 44$, $q = 2^8$.

(a) Write down the multivariate system of equations that this problem reduces to. **Hint:** See Exercise 1 for what this answer should look like.

(b) What is the degree of this system, and what is the number of variables (unknowns) and equations?

(c) What is the complexity of solving this system using a Gröbner-based algorithm?