$\cdots, x_n) = x_{u_1}^2$, hence $Q_{2^k}^{2^{m-1}} \circ \rho_1 \circ \hat{\phi}_2(x_1, \cdots, x_n) = (x_{u_1}^2)^{2^{m-1}} = x_{u_1}$. But $Q_{2^k}^{2^{m-1}} \circ \rho_1 \circ \hat{\phi}_{21} = Q_{2^k}^{2^{m-1}} \circ \rho_1 \circ \hat{\phi}_2 \circ \tilde{\phi}_1$ and both $Q_{2^k}^{2^{m-1}} \circ \rho_1 \circ \hat{\phi}_{21}$ and $\tilde{\phi}_1$ are linear. Therefore $Q_{2^k}^{2^{m-1}} \circ \rho_1 \circ \hat{\phi}_{21} \in L$. Now observe that $Q_{2^k}^{2^{m-1}} \circ \rho_1 \circ \hat{\phi}_{21}(x) = Q_{2^k}^{2^{m-1}} \circ \rho_1 \circ \hat{\phi}_{321}(x) = Q_{2^k}^{2^{m-1}} \circ \rho_1 \circ \phi_4^{-1} \circ F(x) = Q_{2^k}^{2^{m-1}} \circ \rho_1 \circ \phi_4^{-1}(y)$. Since $\rho_1 \circ \phi_4^{-1}(y)$ is linear, and $S \circ \rho_i \circ \hat{\phi}_{21}$, $T_1 \circ \rho_i \circ \hat{\phi}_{21}$, $T_2 \circ \rho_i \circ \hat{\phi}_{21}, i = 1, 2$ are all constants on W. It is clear that $Q_{2^k}^{2^{m-1}} \circ \rho_1 \circ \hat{\phi}_{21}|_W \in T$, Similarly $Q_{2^k}^{2^{m-1}} \circ \rho_2 \circ \hat{\phi}_{21}|_W \in T$. Therefore there exist equations in the form

$$\sum_{i=1}^{n+r} \tilde{a}_{i,k-1} \tilde{y}_i^{2^{k-1}} + \sum_{i=1}^{n+r} \tilde{a}_{i,k-2} \tilde{y}_i^{2^{k-2}} + \cdots + \sum_{i=1}^{n+r} \tilde{a}_{i,0} \tilde{y}_i + \tilde{d} + \sum_{i=1}^{n-l} \tilde{e}_i x_{v_i} = 0 \quad (4)$$

where $\tilde{a}_{i,k-1}, \cdots, \tilde{a}_{i,0}, \tilde{d}, \tilde{e}_i \in K$. Using the same method mentioned above, we can find a basis for K-linear space $\tilde{V}$ composing of all the equations in the form (4). Let $\dim \tilde{V} = D$ and $\{\tilde{a}_{i,k-1}^{(\rho)}, \tilde{a}_{i,k-2}^{(\rho)}, \cdots, \tilde{a}_{i,0}^{(\rho)}, \tilde{e}_i^{(\rho)}, \tilde{d}^{(\rho)} \mid 1 \le \rho \le D\}$ be the coefficient vectors corresponding to this basis of $\tilde{V}$. Without loss of generality, we assume $(\tilde{e}_1^{(\rho)}, \cdots, \tilde{e}_{n-l}^{(\rho)})$, $1 \le \rho \le k$ are linearly independent and the other vectors $(\tilde{e}_1^{(\rho)}, \cdots, \tilde{e}_{n-l}^{(\rho)}), 1 \le \rho \le \tilde{D}$ are their linear combinations. Let $\tilde{E}_\rho (1 \le \rho \le \tilde{D})$ denote equation

$$\sum_{i=1}^{n+r} \tilde{a}_{i,k-1}^{(\rho)} \tilde{y}_i^{2^{k-1}} + \sum_{i=1}^{n+r} \tilde{a}_{i,k-2}^{(\rho)} \tilde{y}_i^{2^{k-2}} + \cdots + \sum_{i=1}^{n+r} \tilde{a}_{i,0}^{(\rho)} \tilde{y}_i + \tilde{d} + \sum_{i=1}^{n-l} \tilde{e}_i^{(\rho)} x_{v_i} = 0$$

Substitute $\tilde{y} = y'$ into $\tilde{E}_\rho (1 \le \rho \le \tilde{D})$ and derive $\tilde{E}'_\rho (1 \le \rho \le \tilde{D})$. Doing a simple Gaussian elimination, from $\tilde{E}'_\rho (1 \le \rho \le \tilde{D})$, we can find two disjoint subsets of $\{v_1, \cdots, v_{n-l}\}$: $A'_2 = \{w'_1, \cdots, w'_{n-l-k}\}$ and $A_2 = \{w_1, \cdots, w_{n-l-k}\}$, and linear expressions

$$x_{w'_j} = \tilde{h}_j(x_{w_1}, \cdots, x_{w_{n-l-k}}), 1 \le j \le k. \quad (5)$$

Let $\tilde{W} = \{(x_1, \cdots, x_n) \in W \mid x_{w'_j} = \tilde{h}_j(x_{w_1}, \cdots, x_{w_{n-l-k}}), 1 \le j \le k\}$ then by the similar analysis in the step 1 of the attack, we can get that $Q_{2^k} \circ \rho_i \circ \hat{\phi}_{21}, i = 1, 2$ are constants on $\tilde{W}$. Let $Q_{2^k} \circ \rho_1 \circ \hat{\phi}_{21}|_{\tilde{W}}$, $Q_{2^k} \circ \rho_2 \circ \hat{\phi}_{21}|_{\tilde{W}}$ be c_1, c_2 respectively. Substitute (5) into $\tilde{y}_i$ and derive $\hat{y}_i, i = 1, \cdots, n+r$. The computational complexity of this step is about $O((n+r)^3 k^3)$

Step 3 of the attack.

For any $(x_1, \cdots, x_n) \in \tilde{W}$, we have

$$\phi_{4,1}^{-1}(\hat{y}) = \hat{\phi}_{321,1}(x_1, \cdots, x_n) = \phi_{1,1}(x_1, \cdots, x_n, 0, \cdots, 0) + c_1$$

So there must exist equations of the form $\sum_{i=1}^{n-l-k} \hat{a}_i x_{w_i} + \sum_{i=1}^{n+r} \hat{b}_i \hat{y}_i + \hat{d} = 0$. Similarly to the step 1 of the attack, we can derive a subspace $\tilde{W}$ of $\hat{W}$ on which $\phi_{1,1}(x_1, \cdots, x_n, 0, \cdots, 0)$ is a constant. Repeating similar steps, we derive in turn smaller and smaller affine subspace of $\tilde{W}$. On these subspace we have in turn $\phi_{1,2}(x_1, \cdots, x_n, 0, \cdots, 0), \cdots, \phi_{1,n}(x_1, \cdots, x_n, 0, \cdots, 0)$ are constants. Therefore they are all constants on the last subspace. Since ϕ_1 is an invertible map, $(x_1, \cdots, x_n)$ is a constant vector on that subspace, which implies that this affine subspace is a point. This point is exactly the plaintext.

This procedure takes no significant time compared to that of step1.

Since $k < n + r$. Then the total computational complexity of the attack is at most $O((n+r)^6)$.

V. Conclusion

In this paper, we use HOLE attack to break an implementation based on $Q_2{}^k$ -module proposed by Chou et al. The complexity of the computation needed to defeat this implementation is about $O((n+r)^6)$, where n+r is the number of the ciphertext variables. However it does not mean that all such type implementations are all insecure. For example the ones suggested in [9] seem different and we can't directly apply this method in this situation. As we have seen that linearization and its generalization HOLE all can be used to break some multivariate public key cryptosystems. For anyone who want to present an secure multivariate public key cryptosystem should take into account these methods.

References

[1] Shor, P., "Polynomial-time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer", SIAM Journal on Computing, 1997, 26(5): 1484-1509.

[2] Patarin, J., Goubin, L., "Trapdoor One-Way Permutations and Multivariate Polynomials", in Proceedings of International Conference on Information Security and Cryptology 1997, LNCS 1334, Berlin: Springer, 1997, 356-368.

[3] Moh, T., "A Public Key System with Signature and Master Key Functions", Communications in Algebra, 1999, 27(5): 2207-2222.

[4] Goubin, L., Courtois, N., "Cryptanalysis of the TTM cryptosystem", in Proceedings of Asiacrypt'2000, LNCS 1976, Berlin: 2000, 44-57

[5] Chen, J., Moh, T., "On the Goubin-Courtois attack on TTM". Cryptology ePrint Archive, 72, 2001. http://eprint.iacr.org/2001/072.
[6] Ding, J. T., Schmidt, D., "The New TTM Implementation is not Secure", in Proceedings of International Workshop on Coding, Cryptography and Combinatorics (CCC 2003), 2003, 106-121.
[7] Chou, C. Y., Guan, D. J., Chen J. M., "A Systematic Construction of a Q2k -module in TTM", Comm. Algebra, 2002, 30(2): 551-562.
[8] Ding, J. T., Hodges, T., "Cryptanalysis of an Implementation of the Tamed Transformation Method Cryptosystem", J. Algebra Appl., 2004, 3: 273-282.
[9] Wang, L. C., Chang, F. H., "Square-free Qk Components in TTM", Taiwanese Journal of Mathematics, 2003, 7(4): 615-629.