Brief Papers

Quantum Cryptanalysis on a Multivariate Cryptosystem Based on Clipped Hopfield Neural Network

Songsong Dai

***Abstract*— Shor's quantum algorithm and other efficient quantum algorithms can break many public-key cryptographic schemes in polynomial time on a quantum computer. In response, researchers proposed postquantum cryptography to resist quantum computers. The multivariate cryptosystem (MVC) is one of a few options of postquantum cryptography. It is based on the NP-hardness of the computational problem to solve nonlinear equations over a finite field. Recently, Wang *et al.* (2018) proposed a MVC based on extended clipped hopfield neural networks (eCHNN). Its main security assumption is backed by the discrete logarithm (DL) problem over Matrics. In this brief, we present quantum cryptanalysis of Wang *et al.*'s eCHNN-based MVC. We first show that Shor's quantum algorithm can be modified to solve the DL problem over Matrics. Then we show that Wang *et al.*'s construction of eCHNN-based MVC is not secure against quantum computers; this against the original intention of that multivariate cryptography is one of a few options of postquantum cryptography.**

***Index Terms*— Clipped Hopfiled neural network, Diffie-Hellman key exchange scheme, discrete logarithm (DL) problem, multivariate cryptography, quantum algorithm.**

I. Introduction

In 1994, Shor [1] showed a quantum algorithm that solves factorization and discrete logarithm (DL) problems in polynomial time. This means that quantum computers can break the public-key cryptosystems based on these problems. Moreover, Shor's algorithm can also efficiently calculate the elliptic curve DLs (ECDL) problem [2] and then break the cryptography based on ECDL problem. The implementation of Shor's algorithm over elliptic curves is given in [3]–[5]. In response, postquantum cryptography have been proposed to resist quantum computers. The goal of postquantum cryptography is to develop postquantum cryptosystems that are secure even when the attacker has a large quantum computer. They are constructed based on other computational problems that are believed hard to solve even for quantum computers. The multivariate cryptosystems (MVCs) [7], as one of a few options of postquantum cryptography, has drawn considerable attention. A MVC has a set of multivariate quadratic polynomials over a finite field and is based on the difficulty of solving a system of these multivariate polynomials. Construction and cryptanalysis of MVCs play an important role in postquantum cryptography. In the last two decades, researchers have developed several construction methods of MVCs. Some construction methods are still viable. For example, the Rainbow signature scheme [8] and unbalance Oil and Vinegar scheme [9] resisted rigorous cryptanalysis for more than 15 years and are therefore believed to have high security. Other construction methods are not as secure as was claimed initially. For example, tame transformation signatures (TTS) scheme [10] was broken exactly because of the usage of sparse polynomials [11].

Manuscript received 3 June 2019; revised 1 August 2020, 22 November 2020, and 4 February 2021; accepted 11 February 2021. Date of publication 1 March 2021; date of current version 2 September 2022. This work was supported in part by the National Science Foundation of China under Grant 62006168 and in part by the Natural Science Foundation of Zhejiang Province of China under Grant LQ21A010001.

The author is with the School of Electronics and Information Engineering, Taizhou University, Taizhou 318000, China (e-mail: ssdai@tzc.edu.cn).

Digital Object Identifier 10.1109/TNNLS.2021.3059434

As a scheme of postquantum cryptography, quantum security is one of the most fundamental and important problems. However, quantum security of a postquantum cryptosystem is elusive. Because most existing security analysis deal with classical attackers and only a few quantum algorithms are developed for postquantum cryptography. There are two cases: one is that a scheme of postquantum cryptosystem is classical insecure, then obviously it is quantum insecure since quantum computers can efficiently simulate classical computers, the other is that the scheme is quantum insecure, but maybe classical secure, examples include RSA and ECC. This brief analyzes the security of a scheme of postquantum cryptosystem from the perspective of quantum attack and shows that it is insecure against quantum computers.

Recently, Wang *et al.* [12] proposed a MVC based on extended Clipped Hopfield Neural Networks (eCHNN), briefly, eCHNN-MVC. In Wang *et al.*'s eCHNN-MVC, the weight matrices are generated by the Diffie-Hellman key exchange scheme (DHKES) in matrix field. Then its security assumption is backed by the hardness of the DL problem over matrices.

This brief shows that the DL problem over matrices can be solved by Shor's DL quantum algorithm, thus Wang *et al.*'s eCHNN-MVC is not secure on quantum computers and their approach deviates from the objective of postquantum cryptography. For simplicity, some symbols and notations from Wang *et al.*'s brief [12] are employed in this brief.

II. Related Work

A. Shor's Algorithm for DL

Let $G =< t >$ be a cyclic group generated by an element t, with the multiplicative operation. The DL problem is the problem to find r such that $s = t^r$ for given t and s.

Shor's DL quantum algorithm includes the following steps [2], [6].

1) Initializing three quantum registers
$$|\Psi\rangle = |0, 0, 0\rangle. \tag{1}$$
2) Choosing q which belongs to $[n, 2n]$.
3) Putting in the first two registers in the uniform superposition of all possible classical inputs $|a\rangle$ and $|b\rangle$ (mod n) and computing $t^a \cdot s^b \mod p$ and putting it in the third register, we get
$$\frac{1}{n}\sum_{a=0}^{n-1}\sum_{b=0}^{n-1}|a, b, t^a \cdot s^b\rangle. \tag{2}$$
4) Using the quantum Fourier transform to take $|a\rangle$ to
$$\frac{1}{q^{1/2}}\sum_{c=0}^{q-1}\exp(2\pi iac/q)|c\rangle \tag{3}$$
and take $|b\rangle$ to
$$\frac{1}{q^{1/2}}\sum_{d=0}^{q-1}\exp(2\pi ibd/q)|d\rangle. \tag{4}$$

Thus, take $|a, b\rangle$ to

$$\frac{1}{q}\sum_{c=0}^{q-1}\sum_{d=0}^{q-1}\exp\left(\frac{2\pi i(ac+bd)}{q}\right)|c, d\rangle. \tag{5}$$

Then we get

$$\frac{1}{nq}\sum_{a,b=0}^{n-1}\sum_{c,d=0}^{q-1}\exp\left(\frac{2\pi i(ac+bd)}{q}\right)|c, d, t^a\cdot s^b\rangle. \tag{6}$$

5) Observing the state. The probability of finding the result $|c, d, t^k \mod p\rangle$ is

$$\Pr\left(|c, d, t^k \mod p\rangle\right) = \left|\frac{1}{nq}\sum_{\substack{(a,b)\\ a-rb=k}}\exp\left(\frac{2\pi i(ac+bd)}{q}\right)\right|^2 \tag{7}$$

where the sum is over all pairs (a, b) satisfying

$$t^a\cdot s^b = t^k \mod p. \tag{8}$$

6) The probability can be written as

$$\Pr\left(|c, d, t^k \mod p\rangle\right) = \left|\frac{1}{nq}\sum_{b=0}^{n-1}\exp\left(\frac{2\pi ibt}{q}\right)\exp\left(\frac{2\pi i\upsilon}{q}\right)\right|^2. \tag{9}$$

where

$$t = cr + d - \frac{r\{cn\}_q}{n} \tag{10}$$

$$\upsilon = \left(\frac{br}{n} - \lfloor\frac{br-k}{n}\rfloor\right)\{cp\}_q \tag{11}$$

and $\{cn\}_q$ denotes $cn \mod q$ with $-(q/2) < cn \le (q/2)$.

7) Recovering r from the pair (c, d). Let ρ be the closest integer to (t/q), then

$$|\{t\}_q| = \left|cr + d - \frac{r\{cn\}_q}{n} - \rho q\right| \le \frac{1}{2} \tag{12}$$

and

$$|\{cn\}_q| \le q/12. \tag{13}$$

This further reduces to

$$\left|\frac{d}{q} + r\left(\frac{cn-\{cn\}_q}{q}\right)\right| \le \frac{1}{2q}. \tag{14}$$

A candidate r is obtained by approximating (d/q) to the nearest multiple of $(1/n)$ and dividing the result $(\mod n)$ by the number

$$c' = \frac{cn-\{cn\}_q}{q}. \tag{15}$$

After obtaining a candidate r, the values (r, c, d) are put into the functions (12) and (13). If both functions hold, then there is a reasonable chance that the result is accurate. If the functions do not hold, then run the quantum computer again.

Therefore, we can get r with a high probability.

B. Shor's Algorithm for ECDL

Let $E = \{(x, y)|y^2 = x^3+ax+b \mod p\}$ be an elliptic curve over the finite field $\mathbb{F}_p$, $A = (x_A, y_A)$ and $B = (x_B, y_B)$ the two points, then the ECDL problem is to find r such that $B = rA \mod p$.

It is quite straightforward to use Shor's algorithm for ECDL problem [2], [6].

1) Initializing three quantum registers

$$|\Psi\rangle = |\mathcal{O}, \mathcal{O}, \mathcal{O}\rangle \tag{16}$$

where $\mathcal{O}$ is the point at infinity in the elliptic curve group $E(\mathbb{F}_p)$.

2) Choosing q which belongs to $[n, 2n]$.
3) Putting in the first two registers in the uniform superposition of all possible classical inputs $|a\rangle$ and $|b\rangle$ $(\mod n)$ and computing $aA + bB \mod p$ and putting it in the third register, we get

$$\frac{1}{n}\sum_{a=0}^{n-1}\sum_{b=0}^{n-1}|a, b, aA+bB\rangle. \tag{17}$$

4) Using the quantum Fourier transform to take $|a\rangle$ to

$$\frac{1}{q^{1/2}}\sum_{c=0}^{q-1}\exp(2\pi iac/q)|c\rangle \tag{18}$$

and take $|b\rangle$ to

$$\frac{1}{q^{1/2}}\sum_{d=0}^{q-1}\exp(2\pi ibd/q)|d\rangle. \tag{19}$$

Thus, take $|a, b\rangle$ to

$$\frac{1}{q}\sum_{c=0}^{q-1}\sum_{d=0}^{q-1}\exp\left(\frac{2\pi i(ac+bd)}{q}\right)|c, d\rangle. \tag{20}$$

Then we get

$$\frac{1}{nq}\sum_{a,b=0}^{n-1}\sum_{c,d=0}^{q-1}\exp\left(\frac{2\pi i(ac+bd)}{q}\right)|c, d, aA+bB\rangle. \tag{21}$$

5) Observing the state. The probability of finding the result $|c, d, kA \mod p\rangle$ is

$$\Pr(|c, d, kA \mod p\rangle) = \left|\frac{1}{nq}\sum_{\substack{(a,b)\\ a-rb=k}}\exp\left(\frac{2\pi i(ac+bd)}{q}\right)\right|^2 \tag{22}$$

where the sum is over all pairs (a, b) satisfying

$$aA + bB = kA \mod p. \tag{23}$$

6) Just the same as the Shor's algorithm for the DL problem over finite field, the probability can be written as

$$\Pr(|c, d, kA \mod p\rangle) = \left|\frac{1}{nq}\sum_{b=0}^{n-1}\exp\left(\frac{2\pi ibt}{q}\right)\exp\left(\frac{2\pi i\upsilon}{q}\right)\right|^2 \tag{24}$$

where

$$t = cr + d - \frac{r\{cn\}_q}{n} \tag{25}$$

$$\upsilon = \left(\frac{br}{n} - \lfloor\frac{br-k}{n}\rfloor\right)\{cp\}_q \tag{26}$$

and $\{cn\}_q$ denotes $cn \mod q$ with $-(q/2) < cn \le (q/2)$.

7) Recovering r from the pair (c, d). Let ρ be the closest integer to (t/q), then

$$|\{t\}_q| = \left|cr + d - \frac{r\{cn\}_q}{n} - \rho q\right| \le \frac{1}{2} \tag{27}$$

and

$$|\{cn\}_q| \le q/12. \tag{28}$$

This further reduces to

$$\left|\frac{d}{q} + r\left(\frac{cn-\{cn\}_q}{q}\right)\right| \le \frac{1}{2q}. \tag{29}$$

A candidate r is obtained by approximating (d/q) to the nearest multiple of $(1/n)$ and dividing the result $(\bmod n)$ by the number

$$c' = \frac{cn - \{cn\}_q}{q}. \tag{30}$$

After obtain a candidate r, the values (r, c, d) are putted into the functions (27) and (28). If both functions hold, then there is a reasonable chance that the result is accurate. If the functions do not hold, then run the quantum computer again.

Therefore, we can get r with a high probability.

III. Description of the Wang *et al.*'s eCHNN-MVC

Wang *et al.*'s eCHNN-MVC is composed of two part: *weight matrices generation* and *threshold vector synchronization*. The former mainly generates a weight matrix pair based on the DHKES over matrix field; the latter mainly generates a threshold vector based on the weight matrix pair.

A. Weight Matrices Generation for eCHNN-MVC

Wang *et al.* [12] first presented the weight matrix pair generation based on the DHKES in matrix field.

Let T and T^{-1} be two nth-order matrices, p be a prime, then the weight matrix pair T_k and T_k' could be generated in the following steps.

1) Alice chooses an integer x and sends Bob

$$T_A = T^x \mod p \tag{31}$$
$$T_A' = \left(T^{-1}\right)^x \mod p. \tag{32}$$

2) Bob chooses an integer y and sends Alice

$$T_B = T^y \mod p \tag{33}$$
$$T_B = \left(T^{-1}\right)^y \mod p. \tag{34}$$

3) Bob calculates

$$T_k = T_A^y \mod p \tag{35}$$
$$T_k' = \left(T_A'\right)^y \mod p \tag{36}$$

and Alice calculates

$$T_k = T_B^x \mod p \tag{37}$$
$$T_k' = \left(T_B'\right)^x \mod p. \tag{38}$$

Because

$$T_k = T_B^x = T^{xy} = T_A^b \mod p \tag{39}$$
$$T_k' = \left(T_B'\right)^x = \left(T'\right)^{xy} = \left(T_A'\right)^b \mod p. \tag{40}$$

Then T_k and T_k' are used as the weight matrices.

For example

Example 1: Let $T = \begin{pmatrix} 4 & 5 \\ 2 & 3 \end{pmatrix}$ and $p = 17$, then we have $< T >_{17} = \{I, T, T^2, \ldots, T^{15}\}$ because of $T^{16} \mod 17 = I$, where $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Let $x = 5$ and $y = 7$, then $T_A = T^5 \mod 17 = \begin{pmatrix} 15 & 16 \\ 13 & 12 \end{pmatrix}$, $T_B = T^7 \mod 17 = \begin{pmatrix} 5 & 6 \\ 7 & 6 \end{pmatrix}$, and $T_k = T_B^x = T_A^y = T^{xy} = \begin{pmatrix} 10 & 11 \\ 10 & 9 \end{pmatrix}$.

B. Threshold Vector Synchronization for eCHNN-MVC

Based on the base matrix T_k, the generation of the threshold vector ϑ could be described as the following steps [12].

1) Alice and Bob first agree on a vector $Q = (q_1, q_2, \ldots, q_n)$.
2) Alice chooses a vector $V_A = (a_1, a_2, \ldots, a_u)$ as her private key and gets

$$H_A = \sum_{j=0}^{u} T_k^{a_j} \mod p \tag{41}$$

then sends Bob

$$P_A = QH_A \mod p. \tag{42}$$

3) Bob chooses a vector $V_B = (b_1, b_2, \ldots, b_v)$ as his private key and gets

$$H_B = \sum_{j=0}^{v} T_k^{b_j} \mod p \tag{43}$$

then sends Alice

$$P_B = QH_B \mod p. \tag{44}$$

4) Alice calculates

$$\vartheta_A = P_B H_A \mod p \tag{45}$$

and Bob calculates

$$\vartheta_B = P_A H_B \mod p. \tag{46}$$

It is easy to know that $\vartheta_A = \vartheta_B$, then it is used as the threshold vector ϑ.

Then the encryption could be written as

$$C = f\left(T_k^r M + \sum_{j=0}^{r} T_k^j \vartheta\right) \tag{47}$$

where $f(\cdot)$ is the following function

$$f(a) = \begin{cases} a \mod p, & \text{if } a \geq 0 \\ p - |a| \mod p, & \text{if } a < 0. \end{cases} \tag{48}$$

M is the message and C is the cipher text. Alice sends (C, r) to Bob. Then Bob gets M from

$$M = f\left(T_k'^r\left(C - f\left(\sum_{j=0}^{r} T_k^j \vartheta\right)\right)\right). \tag{49}$$

IV. Shor's Discrete Logarithm Quantum Algorithm for Matrices

Let T be a nth-order matrix $(\bmod p)$, that is, $T^n = I \mod p$, where I denotes the identity matrix. Then denote the set of matrices generated from T by $M_n(T) = \{I, T, T^2, \ldots, T^{n-1}\}$.

Wang *et al.* [12] introduced the DL problem on matrix field as the problem: given two matrices $T, S \in M_n(T)$ and a prime p, find an integer r such that $T^r \equiv S \mod p$.

It is quite straightforward to use Shor's DL quantum algorithm for matrices.

1) Initializing three quantum registers

$$|\Psi\rangle = |1, 1, I\rangle \tag{50}$$

where I is the identity matrix.
2) Choosing q which belongs to $[n, 2n]$.

TABLE I
SHOR'S QUANTUM ALGORITHM FOR THREE TYPES OF DL PROBLEMS

Steps	DL problem over finite field [1]	DL problem over elliptic curves [2]	DL problem over matrices
1, Initialization $\|\Psi\rangle$	$\|0,0,0\rangle$	$\|\mathcal{O},\mathcal{O},\mathcal{O}\rangle$	$\|1,1,I\rangle$
2, Choose q	from $[n,2n]$		
3, Compute	$\frac{1}{n}\sum_{a=0}^{n-1}\sum_{b=0}^{n-1}\|a,b,t^a\cdot s^b\rangle$	$\frac{1}{n}\sum_{a=0}^{n-1}\sum_{b=0}^{n-1}\|a,b,aA+\cdot bB\rangle$	$\frac{1}{n}\sum_{a=0}^{n-1}\sum_{b=0}^{n-1}\|a,b,T^a\cdot S^b\rangle$
4, Quantum Fourier transform	$f(a,b,c,d)\|c,d,t^a\cdot s^b\rangle$	$f(a,b,c,d)\|c,d,aA+bB\rangle$	$f(a,b,c,d)\|c,d,T^a\cdot S^b\rangle$
	where $f(a,b,c,d)=\frac{1}{nq}\sum_{a,b=0}^{n-1}\sum_{c,d=0}^{q-1}\exp\left(\frac{2\pi i(ac+bd)}{q}\right)$		
5, Observe the state	$\|c,d,t^k\rangle$	$\|c,d,kB\rangle$	$\|c,d,T^k\rangle$
	where $t^a\cdot t^b=t^k \mod p$	where $aA+tB=kB$	where $T^a\cdot T^b=T^k \mod p$
6 and 7, Compute r	from $\left\|\frac{d}{q}+r\left(\frac{cn-\{cn\}_q}{q}\right)\right\|\le\frac{1}{2q}$		

3) Putting in the first two registers in the uniform superposition of all possible classical inputs $|a\rangle$ and $|b\rangle$ ($\bmod n$) and computing $T^a\cdot S^b \mod p$ and putting it in the third register, we get

$$\frac{1}{n}\sum_{a=0}^{n-1}\sum_{b=0}^{n-1}|a,b,T^a\cdot S^b\rangle. \tag{51}$$

4) Using the quantum Fourier transform to take $|a\rangle$ to

$$\frac{1}{q^{1/2}}\sum_{c=0}^{q-1}\exp(2\pi iac/q)|c\rangle \tag{52}$$

and take $|b\rangle$ to

$$\frac{1}{q^{1/2}}\sum_{d=0}^{q-1}\exp(2\pi ibd/q)|d\rangle. \tag{53}$$

Thus, take $|a,b\rangle$ to

$$\frac{1}{q}\sum_{c=0}^{q-1}\sum_{d=0}^{q-1}\exp\left(\frac{2\pi i(ac+bd)}{q}\right)|c,d\rangle. \tag{54}$$

Then we get

$$\frac{1}{nq}\sum_{a,b=0}^{n-1}\sum_{c,d=0}^{q-1}\exp\left(\frac{2\pi i(ac+bd)}{q}\right)|c,d,T^a\cdot S^b\rangle. \tag{55}$$

5) Observing the state. The probability of finding the result $|c,d,T^k \mod p\rangle$ is

$$\Pr\left(|c,d,T^k \mod p\rangle\right)=\left|\frac{1}{nq}\sum_{\substack{(a,b)\\ a-rb=k}}\exp\left(\frac{2\pi i(ac+bd)}{q}\right)\right|^2 \tag{56}$$

where the sum is over all pairs (a,b) satisfying

$$T^a\cdot S^b=T^k \mod p. \tag{57}$$

6) Just the same as the Shor's algorithm for the DL problem over finite field, the probability can be written as

$$\Pr\left(|c,d,T^k \mod p\rangle\right)=\left|\frac{1}{nq}\sum_{b=0}^{n-1}\exp\left(\frac{2\pi ibt}{q}\right)\exp\left(\frac{2\pi iv}{q}\right)\right|^2 \tag{58}$$

where

$$t=cr+d-\frac{r\{cn\}_q}{n} \tag{59}$$

$$v=\left(\frac{br}{n}-\lfloor\frac{br-k}{n}\rfloor\right)\{cp\}_q \tag{60}$$

and $\{cn\}_q$ denotes $cn \mod q$ with $-(q/2)<cn\le(q/2)$.

7) Recovering r from the pair (c,d). Let ρ be the closest integer to (t/q), then

$$|\{t\}_q|=\left|cr+d-\frac{r\{cn\}_q}{n}-\rho q\right|\le\frac{1}{2} \tag{61}$$

and

$$|\{cn\}_q|\le q/12. \tag{62}$$

This further reduces to

$$\left|\frac{d}{q}+r\left(\frac{cn-\{cn\}_q}{q}\right)\right|\le\frac{1}{2q}. \tag{63}$$

A candidate r is obtained by approximating (d/q) to the nearest multiple of $(1/n)$ and dividing the result ($\bmod n$) by the number

$$c'=\frac{cn-\{cn\}_q}{q}. \tag{64}$$

After obtaining a candidate r, the values (r,c,d) are put into the functions (61) and (62). If both functions hold, then there is a reasonable chance that the result is accurate. If the functions do not hold, then run the quantum computer again.

Therefore, we can get r with a high probability.

V. CRYPTANALYSIS OF THE THRESHOLD VECTOR SYNCHRONIZATION

Alice uses the vector $V_A=(a_1,a_2,\ldots,a_u)$ as her private key and the vector P_A as her public key. Bob uses the vector $V_B=(b_1,b_2,\ldots,b_u)$ as his private key and the vector P_B as his public key. Since

$$H_A=\sum_{j=0}^{u}T_k^{a_j} \mod p \tag{65}$$

$$P_A=QH_A \mod p \tag{66}$$

$$H_B=\sum_{j=0}^{v}T_k^{a_j} \mod p \tag{67}$$

$$P_B=QH_B \mod p \tag{68}$$

and

$$\vartheta = P_A H_B = P_B H_A \mod p. \tag{69}$$

It can be viewed as $P_A = QH_A \mod p$, $P_B = QH_B \mod p$, and $\vartheta = QH_AH_B$ briefly.

Thus, H_A and H_B can be viewed as the substitutes of the private key V_A and V_B. It is not needed to find vectors V_A and V_B, we need only to get a pair of matrices $\widetilde{H}_A$ and $\widetilde{H}_B$ such that $Q\widetilde{H}_A = P_A = QH_A$ and $Q\widetilde{H}_B = P_B = QH_B$.

Then Bob can calculate

$$Q^{-1} = \left(q_1^{-1}, q_2^{-1}, \ldots, q_n^{-1}\right) \mod p \tag{70}$$

and $\widetilde{H}_A = Q^{-1}P_A$ which can be viewed as the substitute of H_A because $Q\widetilde{H}_A = QQ^{-1}P_A = P_A = QH_A$. Similarly, Alice can calculate $\widetilde{H}_B = Q^{-1}P_B$ as the substitute of H_B.

Example 2: Let $p = 17$, if Alice and Bob agree on the vector $Q = (6, 7)$, Alice's public key is $P_A = \begin{pmatrix} 15 & 16 \\ 13 & 12 \end{pmatrix}$, and Bob's public key is $P_B = \begin{pmatrix} 5 & 6 \\ 7 & 6 \end{pmatrix}$. Then they can get $Q^{-1} = (6^1, 7^{-1}) \mod 17 = (3, 5)$. Moreover, Bob can get $\widetilde{H}_A = Q^{-1}P_A \mod 17 = (8, 6)$ as the substitute of Alice's private key H_A, he does not need to find V_A. Similarly, Alice can get $\widetilde{H}_B = Q^{-1}P_B \mod 17 = (16, 14)$ as the substitute of Bob's private key H_B.

VI. Conclusion

In this brief, we present quantum cryptanalysis of Wang *et al.*'s eCHNN-MVC, as well as a practical method for solving the DL problem over matrices. Inspired by Eicher and Opoku's work, we modified Shor's quantum algorithm to solve this problem. It turns out that this problem can be solved efficiently on a quantum computer and therefore should not be used as a basis for postquantum cryptography. To see more clearly how a quantum computer will solve different types of DL problem, we summarized Shor's quantum algorithm for these problems in Table I.

As mentioned in [12], Wang *et al.*'s eCHNN-MVC tried to be a potential alternative for postquantum cryptography. It also is secure against several classical attacks and allows hardware realization practicality. However, this brief shows that Wang *et al.*'s approach, although worthwhile studying, is not quantum-secure since the usage of the DHKES over matrices. Thus, their approach is deviates from the original intention of postquantum cryptography.

Acknowledgment

The author would like to thank the referees and associate editor for their valuable comments and recommendations, as these led him to an improvement of this brief.

References

[1] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM J. Comput.*, vol. 26, no. 5, pp. 1484–1509, Oct. 1997.

[2] J. Eicher and Y. Opoku, "Using the quantum computer to break elliptic curve cryptosystems," Univ. Richmond, Richmond, VA, USA, Tech. Rep., Jul. 1997, no. 2, p. 28.

[3] J. Proos and C. Zalka, "Shor's discrete logarithm quantum algorithm for elliptic curves," *Quantum Inf. Comput.*, vol. 3, no. 4, pp. 317–344, 2003.

[4] P. Kaye, "Optimized quantum implementation of elliptic curve arithmetic over binary fields," *Quantum Inf. Comput.*, vol. 5, no. 6, pp. 474–491, 2005.

[5] D. Cheung, D. Maslov, J. Mathew, and D. Pradhan, "On the design and optimization of a quantum polynomial-time attack on elliptic curve cryptography," in *Proc. 3rd Workshop Quantum Comput., Commun., Cryptogr.* (Lecture Notes in Computer Science), vol. 5106. Berlin, Germany: Springer, 2008, pp. 96–104.

[6] S. Y. Yan, *Quantum Computational Number Theory*. Cham, Switzerland: Springer, 2015.

[7] S. Tsujii, T. Itoh, A. Fujioka, K. Kurosawa, and T. Matsumoto, "A public-key cryptosystem based on the difficulty of solving a system of nonlinear equations," *Syst. Comput. Jpn.*, vol. 19, no. 2, pp. 10–18, Feb. 1988.

[8] J. Ding and D. Schmidt, "Rainbow, a new multivariable polynomial signature scheme," in *Proc. ACNS* (Lecture Notes in Computer Science), vol. 3531. Berlin, Germany: Springer, 2005, pp. 164–175.

[9] A. Kipnis, J. Patarin, and L. Goubin, "Unbalanced oil and vinegar signature schemes," in *Proc. Int. Conf. Theory Appl. Cryptograph. Techn.* Berlin, Germany: Springer, 1999, pp. 206–222.

[10] B. Y. Yang and J. M. Chen, "Building secure tame-like multivariate public-key cryptosystems: The new TTS," in *Proc. Australas. Conf. Inf. Secur. Privacy*. Berlin, Germany: Springer, 2005, pp. 518–531.

[11] J. Ding, D. Schmidt, and Z. Yin, "Cryptanalysis of the new TTS scheme in CHES 2004," *Int. J. Inf. Secur.*, vol. 5, no. 4, pp. 231–240, 2006.

[12] J. Wang, L.-M. Cheng, and T. Su, "Multivariate cryptography based on clipped hopfield neural network," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 29, no. 2, pp. 353–363, Feb. 2018.