POST-QUANTUM SIGNATURE FROM SUBSET PRODUCT WITH ERRORS

TREY LI

ABSTRACT. We propose a new identification scheme and a new signature scheme from the multiple modular subset product with errors problem; as well as a new identification scheme and a new signature scheme from the multiple modular subset sum with errors problem.

1. INTRODUCTION

In [Li22e] and [Li22f] we have proposed a key exchange scheme and a public key cryptosystem from different settings of the multiple modular subset product with errors problem (M-MSPE), which are conjectured to be quantum hard.

In this paper we propose a post-quantum signature scheme from another setting of M-MSPE. We first construct an analogue of the Schnorr identification scheme using M-MSPE, then use the Fiat-Shamir transformation to transform it into a signature scheme.

We then give simplified versions of the schemes based on the multiple modular subset sum with errors problem (M-MSSE). A special case of M-MSSE is the learning parity with noise problem (LPN), which is M-MSSE with the modulus $q = 2$.

2. HARD PROBLEM

The general version of M-MSPE is the multiple modular unique factorization domain subset product with errors problem (M-MUSPE) [Li22d], which is defined over unique factorization domains (UFD). M-MSPE is the concrete M-MUSPE with the UFD the ring $\mathbb{Z}$ of rational integers.

In [Li22e] and [Li22f] we used different settings of M-MSPE to construct key exchange scheme and public key cryptosystem. We call them M-MSPE$_{KE}$ and M-MSPE$_{PKC}$ respectively. The difference between M-MSPE$_{KE}$ and M-MSPE$_{PKC}$ is that in M-MSPE$_{KE}$ all the error primes are sampled from the whole error set L; while in M-MSPE$_{PKC}$ the error primes are sampled from either the first or the second half of L according to the message bit. The common parts are that both M-MSPE$_{KE}$ and M-MSPE$_{PKC}$ use two sets of primes, P and L, for the bases and errors respectively; that both give out $n+1$ MSPE instances; and that both ask for binary solutions $x \in \{0,1\}^n$.

In this paper, we use the M-MSPE in [Li22e, Section 2] with the following changes: (1) both the bases and errors are sampled from $\mathbb{Z}_q^\times$ rather than from integers factored over two sets of primes P and L respectively; (2) the modulus q is not required to be within $[(n2^n)^{2n+1}, (n2^n)^{n^2/8}]$ but can be much smaller such as $q \approx 2^n$ or even smaller; (3) the solution x is not required to be in $\{0,1\}^n$ but $\mathbb{Z}_{q-1}^n$; also (4) we use $\geq 2n$ MSPE instances to form an M-MSPE so that the solution x is unique with overwhelming probability.

This is the 7th paper of the series. Previously: [Li22a; Li22b; Li22c; Li22d; Li22e; Li22f].

Date: October 7, 2022.

Email: treyquantum@gmail.com

Note that the corresponding settings of (1) and (2) in both [Li22e] and [Li22f] were due to the needs of decoding in the key exchange and the public key cryptosystem. Now since we do not need decoding in our identification scheme nor signature scheme, we do not need P nor L, nor a large q.

Setup

Let $n \in \mathbb{N}$ and let q be a prime.

Let O_x with respect to some $x = (x_1, \ldots, x_n) \in \mathbb{Z}_{q-1}^n$ be an oracle which samples $a_1, \ldots, a_n, e \leftarrow \mathbb{Z}_q^\times$, computes $X = \prod_{i=1}^n a_i^{x_i} \cdot e \pmod q$, and outputs the instance $(a_1, \ldots, a_n, X)$.

Problem

M-MSPE is given access to O_x, find x.[1]

3. IDEA

An identification scheme involves two parties, the prover and the verifier. Both of them have access to the same public key. The prover wants to convince the verifier that she owns the corresponding private key of the public key. They interact as the following. The prover first sends a commitment to the verifier; the verifier then sends a challenge to the prover; the prover then sends a response to the verifier; in the end the verifier accepts or rejects the prover's claim about her possession of the secret key.

To see the idea of our scheme, let us review the classical Schnorr identification scheme. It is constructed from the discrete logarithm problem (DLP).

Let $G = \langle g \rangle$ be a DLP group of order q generated by $g \in G$. The prover's secret key is a random element $s \leftarrow \mathbb{Z}_q$; the public key is $h = g^s$.

(1) The prover samples $x \leftarrow \mathbb{Z}_q$ and sends $t = g^x$ to the verifier as the commitment;
(2) The verifier samples $c \leftarrow \mathbb{Z}_q$ and sends it to the prover as the challenge;
(3) The prover computes $y = x - cs \pmod q$ and sends it to the verifier as the response;
(4) The verifier accepts if $g^y h^c = t$ or rejects if $g^y h^c \neq t$.

Using the Fiat-Shamir transformation, the Schnorr identification scheme is transformed into a signature.

Let a be a message. The prover now acts as the signer. Her private and public keys remain the same. The signing is the following.

$\mathsf{Sign}(sk, a)$:
(1) Sample $x \leftarrow \mathbb{Z}_q$ and compute $t = g^x$;
(2) Compute $c = H(t, a)$;
(3) Compute $y = x - cs \pmod q$;
(4) Output (y, c) as the signature.

The verification is the following.

$\mathsf{Verify}(pk, a, y, c)$:
(1) Compute $t' = g^y h^c$;
(2) Compute $c' = H(t', a)$;
(3) Accept if $c' = c$ or reject if $c' \neq c$.

The ideas of our identification scheme and signature are to replace DLP by M-MSPE.

[1] A variation of the problem is to use different moduli q in different MSPE instants.

4. IDENTIFICATION SCHEME

Let $n \in \mathbb{N}$, $m \geq 2n$, and q be a prime. The prover's private key is $(s,u) \leftarrow \mathbb{Z}_{q-1}^n \times (\mathbb{Z}_q^\times)^m$. Her public key is (M,S), where $M = \{a_{i,j}\}_{m\times n}$ is a base matrix, and $S = (S_1,\ldots,S_m)$ is an M-MSPE product sequence with $S_i = \left(\prod_{j=1}^n a_{i,j}^{s_j}\right) \cdot u_i \pmod q$ for $i \in [m]$.

(1) The prover samples $(x,e) \leftarrow \mathbb{Z}_{q-1}^n \times (\mathbb{Z}_q^\times)^m$; computes $A = (A_1,\ldots,A_m)$ with $A_i = \left(\prod_{j=1}^n a_{i,j}^{x_j}\right) \cdot e_i \pmod q$ for $i \in [m]$; and sends A to the verifier as the commitment;
(2) The verifier samples $c \leftarrow \mathbb{Z}_{q-1}$ and sends it to the prover as the challenge;
(3) The prover computes $y = x - cs = (x_1 - cs_1,\ldots,x_n - cs_n) \pmod{q-1}$ and $v = e/u^c = (e_1/u_1^c,\ldots,e_m/u_m^c) \pmod q$, and sends (y,v) to the verifier as the response;
(4) The verifier computes $B = (B_1,\ldots,B_m)$ with $B_i = \prod_{i=1}^n a_{i,j}^{y_j} \pmod q$ for $i \in [m]$; computes $A' = B \cdot S^c \cdot v = (B_1 \cdot S_1^c \cdot v_1,\ldots,B_m \cdot S_m^c \cdot v_m) \pmod q$; and accepts if $A' = A$ or rejects if $A' \neq A$.

5. CORRECTNESS

Correctness is about whether the verification succeeds when every party in the scheme is honest.

THEOREM 1. If every party in the identification scheme is honest then $A' = A$.

Proof. For each $i \in [m]$, we have

$$\begin{aligned}
A_i' &= B_i \cdot S_i^c \cdot v_i \pmod q \\
&= \left(\prod_{j=1}^n a_{i,j}^{y_j}\right) \cdot \left(\left(\prod_{j=1}^n a_{i,j}^{s_j}\right) \cdot u_i\right)^c \cdot \frac{e_i}{u_i^c} \pmod q \\
&= \left(\prod_{j=1}^n a_{i,j}^{y_j + cs_j}\right) \cdot u_i^c \cdot \frac{e_i}{u_i^c} \pmod q \\
&= \left(\prod_{j=1}^n a_{i,j}^{x_j}\right) \cdot e_i \pmod q \\
&= A_i.
\end{aligned}$$

□

6. SECURITY OF HONEST-VERIFIER ZERO KNOWLEDGE

To prove that the execution of the identification scheme does not leak information about the private key (x,u), we want to prove the existence of a simulator that simulates the transcript distribution.

THEOREM 2. There exists a probabilistic polynomial time simulator $\mathcal{S}$ that simulates the transcript distribution $(t,c,y,v) := (M^x e, c, x - cs, e/u^c)$.

Proof. $\mathcal{S}$ samples $c',y',v' \leftarrow \mathbb{Z}_{q-1}$ and $t' \leftarrow M^{y'} \cdot (M^s u)^{c'} \cdot v' \pmod q$, and outputs (t',c',y',v'). It is not hard to see that this is the same distribution as the real transcript distribution. □

7. Security against impersonation

The security against impersonation is about the nonexistence of adversaries who do not have the private key (s,u) but still convince the verifier to accept.

We shall assume that the adversary is given the public key pk and can eavesdrop previous executions of the protocol for the same private key sk. Let o_{sk} be the oracle that each time invokes a fresh execution of the protocol and returns the full transcript (t,c,y) of the execution. Then we assume that the adversary is given pk and o_{sk}.

An identification scheme is said to be secure against impersonation if for all probabilistic polynomial time adversaries $\mathcal{A}$, there is a negligible function μ such that the probability that $\mathcal{A}$ (given pk and o_{sk}) convinces the verifier is $\leq \mu$.

Theorem 3. If M-MSPE is hard, then the identification scheme is secure against impersonation.

Proof. We use the generic proving routine illustrated in [KL14, p.457, 2nd edition], with the only difference that we need the uniqueness of solution of M-MSPE, while in [KL14] the DLP naturally has a unique solution.

Let $\mathcal{A}$ be any probabilistic polynomial time adversary, which is given pk and o_{sk}. Define an M-MSPE solver $\mathcal{B}$ as the following. $\mathcal{B}$ takes as input M,S and $\mathbb{Z}_q^\times$. It runs $\mathcal{A}(pk) = \mathcal{A}(M,S)$. When $\mathcal{A}$ outputs A, $\mathcal{B}$ chooses a uniform $c_1 \leftarrow \mathbb{Z}_{q-1}$ as the challenge and gives it to $\mathcal{A}$; $\mathcal{A}$ responses with $(y^{(1)},v^{(1)})$. $\mathcal{B}$ then runs $\mathcal{A}(pk)$ a second time with c_1 replaced by an independent $c_2 \leftarrow \mathbb{Z}_{q-1}$; $\mathcal{A}$ responses with $(y^{(2)},v^{(2)})$. If

$$\left(\prod_{i=1}^{n} a_{i,j}^{y_j^{(1)}}\right) \cdot S_i^{c_1} \cdot v_i^{(1)} \pmod q = A_i$$

and

$$\left(\prod_{i=1}^{n} a_{i,j}^{y_j^{(2)}}\right) \cdot S_i^{c_2} \cdot v_i^{(2)} \pmod q = A_i$$

for all $i \in [m]$ and that

$$c_1 \neq c_2$$

then $\mathcal{B}$ outputs

$$(y^{(1)} - y^{(2)})/(c_1 - c_2) \pmod{q-1}.$$

Let ω be the randomness during the execution. Define $V(\omega,c) = 1$ if and only if the target M-MSPE (M,S) has a unique solution and that $\mathcal{A}$ correctly responds to challenge c when randomness ω is used in the rest of the execution. For any fixed ω, define $\delta_\omega := \Pr_c[V(\omega,c) = 1]$; with ω fixed, this is the probability over c that $\mathcal{A}$ responds correctly.

Denote $\delta(n)$ as the probability that $\mathcal{A}$ succeeds. We have

$$\delta(n) = \Pr_{\omega,c}[V(\omega,c) = 1] = \sum_{\omega} \Pr[\omega] \cdot \delta_\omega.$$

Again, from [Li22d] we have that the M-MSPE has a unique solution with overwhelming probability P. Suppose that this is the case, then $\mathcal{B}$ successfully solves the M-MSPE (M,S)

whenever $\mathcal{A}$ succeeds twice and $c_1 \neq c_2$. We therefore have

$$\begin{aligned}
\Pr[\mathcal{B} \text{ succeeds}] &= \mathrm{P} \cdot \Pr_{\omega,c_1,c_2}[V(\omega,c_1) \wedge V(\omega,c_2) \wedge c_1 \neq c_2] \\
&\geq \mathrm{P} \cdot \left(\Pr_{\omega,c_1,c_2}[V(\omega,c_1) \wedge V(\omega,c_2)] - \Pr_{\omega,c_1,c_2}[c_1 = c_2] \right) \\
&= \mathrm{P} \cdot \left(\sum_{\omega} \Pr[\omega] \cdot (\delta_\omega)^2 - 1/(q-1) \right) \\
&\geq \mathrm{P} \cdot \left((\sum_{\omega} \Pr[\omega] \cdot \delta_\omega)^2 - 1/(q-1) \right) \\
&= \mathrm{P} \cdot \left(\delta(n)^2 - 1/(q-1) \right),
\end{aligned}$$

where the second-to-last step uses Jensen's inequality.

Notice that if M-MSPE is hard then $\Pr[\mathcal{B} \text{ succeeds}]$ is negligible. Also P is overwhelming and $1/(q-1)$ is negligible. Hence $\delta(n)$ is negligible. I.e., $\mathcal{A}$ succeeds with negligible probability and thus the scheme is secure. □

8. SIGNATURE

Let $n \in \mathbb{N}$, $m \geq 2n$, and q be a prime. The Fiat-Shamir transformation turns our identification scheme into the following signature.

KeyGen(n,m,q):

- Sample $M = \{a_{i,j}\}_{m \times n} \leftarrow (\mathbb{Z}_q^\times)^{m \times n}$;
- Sample $(s,u) \leftarrow \mathbb{Z}_{q-1}^n \times (\mathbb{Z}_q^\times)^m$;
- Compute $S = (S_1,\ldots,S_m)$ with $S_i = \left(\prod_{j=1}^n a_{i,j}^{s_j} \right) \cdot u_i \pmod q$ for $i \in [m]$;
- Output (sk,pk) with $sk := (s,u)$, $pk := (M,S)$.

Sign(sk,a):

- Sample $(x,e) \leftarrow \mathbb{Z}_{q-1}^n \times (\mathbb{Z}_q^\times)^m$ and compute $A = (A_1,\ldots,A_m)$ with $A_i = \left(\prod_{j=1}^n a_{i,j}^{x_j} \right) \cdot e_i \pmod q$ for $i \in [m]$;
- Compute $c = H(A,a)$, where H is a cryptographic hash function;
- Compute $y = x - cs = (x_1 - cs_1,\ldots,x_n - cs_n) \pmod{q-1}$ and $v = e/u^c = (e_1/u_1^c,\ldots, e_m/u_m^c) \pmod q$;
- Output (y,v,c) as the signature.

Verify(a,y,v,c,pk):

- Compute $B = (B_1,\ldots,B_m)$ with $B_i = \prod_{i=1}^n a_{i,j}^{y_j}$ for $i \in [m]$;
- Compute $A' = B \cdot S^c \cdot v = (B_1 \cdot S_1^c \cdot v_1,\ldots,B_m \cdot S_m^c \cdot v_m) \pmod q$;
- Compute $c' = H(A',a)$;
- Accept if $c' = c$ or rejects if $c' \neq c$.

9. CORRECTNESS AND SECURITY

The correctness is obvious from the correctness of the identification scheme. We see the security via the following well-known theorem.

THEOREM 4. [KL14, p.454 Theorem 12.10] If an identification scheme is secure against impersonation and the hash function is modeled as a random oracle, then the signature scheme that results by applying the Fiat-Shamir transform is secure against impersonation.

THEOREM 5. If M-MSPE is hard and the hash function H is modeled as a random oracle, then our signature scheme is secure against impersonation.

Proof. Immediate from Theorem 3 and 4. □

10. EFFICIENCIES

We do not calculate the concrete complexities. Instead, we point out the relation between our schemes and the Schnorr schemes. Intuitively, if both DLP and M-MSPE use the same modulus q, then creating an M-MSPE is creating an $m \times (n+1)$ matrix of DLPs and then multiply every $n+1$ of them together to get m MSPE products.

11. SIMPLIFICATION

More efficient schemes are immediate by taking discrete logarithms of the M-MSPE schemes. The resulting schemes are based on M-MSSE. In the following we define M-MSSE using a prime modulus q instead of composite $q-1$.

Setup

Let $n \in \mathbb{N}$ and let q be a prime.

Let O_x with respect to some $x \in \mathbb{Z}_q^n$ be the oracle that each time samples $a_1,\ldots,a_n,e \leftarrow \mathbb{Z}_q$, computes $X = \left(\sum_{i=1}^n x_i a_i\right) + e \pmod q$, and outputs the instance $(a_1,\ldots,a_n,X)$.

Problem

M-MSSE is given access to O_x, find x.

When $q=2$ it is LPN[2].

12. IDENTIFICATION SCHEME

Let $n \in \mathbb{N}$, $m \geq 2n$, and $q \geq 2$ be a prime. The prover's private key is $(s,u) \leftarrow \mathbb{Z}_q^n \times \mathbb{Z}_q^m$. Her public key is (M,S), where $M = \{a_{i,j}\}_{m\times n} \leftarrow \mathbb{Z}_q^{m\times n}$ is the base matrix, and $S = (S_1,\ldots,S_m)$ is the M-MSSE sum sequence with $S_i = \left(\sum_{j=1}^n s_j a_{i,j}\right) + u_i \pmod q$ for $i \in [m]$.

(1) The prover samples $(x,e) \leftarrow \mathbb{Z}_q^n \times \mathbb{Z}_q^m$; computes $A = (A_1,\ldots,A_m)$ with $A_i = \left(\sum_{j=1}^n x_j a_{i,j}\right) + e_i \pmod q$ for $i \in [m]$; and sends A to the verifier as the commitment;
(2) The verifier samples $c \leftarrow \mathbb{Z}_q$ and sends it to the prover as the challenge;
(3) The prover computes $y = x - cs = (x_1 - cs_1,\ldots,x_n - cs_n) \pmod{q-1}$ and $v = e - cu = (e_1 - cu_1,\ldots,e_m - cu_m) \pmod q$, and sends (y,v) to the verifier as the response;
(4) The verifier computes $B = (B_1,\ldots,B_m)$ with $B_i = \sum_{i=1}^n y_j a_{i,j} \pmod q$ for $i \in [m]$; computes $A' = B + c\cdot S + v = (B_1 + cS_1 + v_1,\ldots,B_m + cS_m + v_m) \pmod q$; and accepts if $A' = A$ or rejects if $A' \neq A$.

THEOREM 6. If every party in the identification scheme is honest then $A' = A$.

[2]Here we take the typical setting of LPN with uniform coefficient and noise distributions.

Proof. For each $i \in [m]$, we have

$$\begin{aligned} A'_i &= B_i + cS_i + v_i \pmod q \\ &= \left(\sum_{j=1}^{n} y_j a_{i,j}\right) + c\left(\left(\sum_{j=1}^{n} s_j a_{i,j}\right) + u_i\right) + (e_i - cu_i) \pmod q \\ &= \left(\sum_{j=1}^{n} \left[(y_j + cs_j)\cdot a_{i,j}\right]\right) + cu_i + (e_i - cu_i) \pmod q \\ &= \left(\sum_{j=1}^{n} x_j a_{i,j}\right) + e_i \pmod q \\ &= A_i. \end{aligned}$$

□

13. Security of honest-verifier zero knowledge

Theorem 7. There exists a probabilistic polynomial time simulator $\mathcal{S}$ that simulates the transcript distribution $(t, c, y, v) := (Mx + e, c, x - cs, e - cu)$.

Proof. $\mathcal{S}$ samples $c', y', v' \leftarrow \mathbb{Z}_{q-1}$ and $t' \leftarrow My' + c'(Ms + u) + v' \pmod q$, and outputs (t', c', y', v'). It is the same distribution as the real transcript distribution. □

14. Security against impersonation

Theorem 8. If M-MSSE is hard, then the identification scheme is secure against impersonation.

Proof. The proof is almost the same as that of Theorem 3 with the formulas about the M-MSPE scheme replaced by the corresponding formulas about the M-MSSE scheme. □

15. Signature

Let $n \in \mathbb{N}$, $m \geq 2n$, and $q \geq 2$ be a prime. The Fiat-Shamir transformation turns the identification scheme into the following signature.

KeyGen(n, m, q):

- Sample $M = \{a_{i,j}\}_{m \times n} \leftarrow \mathbb{Z}_q^{m \times n}$;
- Sample $(s, u) \leftarrow \mathbb{Z}_q^n \times \mathbb{Z}_q^m$;
- Compute $S = (S_1, \ldots, S_m)$ with $S_i = \left(\sum_{j=1}^{n} a_{i,j} s_j\right) + u_i \pmod q$ for $i \in [m]$;
- Output (sk, pk) with $sk := (s, u)$, $pk := (M, S)$.

Sign(sk, a):

- Sample $(x, e) \leftarrow \mathbb{Z}_{q-1}^n \times \mathbb{Z}_q^m$ and compute $A = (A_1, \ldots, A_m)$ with $A_i = \left(\sum_{j=1}^{n} a_{i,j} x_j\right) + e_i \pmod q$ for $i \in [m]$;
- Compute $c = H(A, a)$, where H is a cryptographic hash function;
- Compute $y = x - cs = (x_1 - cs_1, \ldots, x_n - cs_n) \pmod{q-1}$ and $v = e - cu = (e_1 - cu_1, \ldots, e_m - cu_m) \pmod q$;
- Output (y, v, c) as the signature.

Verify(a, y, v, c, pk):

- Compute $B = (B_1, \ldots, B_m)$ with $B_i = \sum_{i=1}^{n} a_{i,j} y_j$ for $i \in [m]$;
- Compute $A' = B + S^c + v = (B_1 + cS_1 + v_1, \ldots, B_m + cS_m + v_m) \pmod{q}$;
- Compute $c' = H(A', a)$;
- Accept if $c' = c$ or rejects if $c' \neq c$.

The correctness and security are similar to the scheme based on M-MSPE. The efficiency is improved in the obvious way with multiplications replaced by additions.

REFERENCES

[KL14] Jonathan Katz and Yehuda Lindell. *Introduction to Modern Cryptography, Second Edition*. 2nd. Chapman & Hall/CRC, 2014. ISBN: 1466570261.

[Li22a] Trey Li. "Subset Product with Errors over Unique Factorization Domains and Ideal Class Groups of Dedekind Domains". 1st paper of the series. 2022, October 1.

[Li22b] Trey Li. "Jacobi Symbol Parity Checking Algorithm for Subset Product". 2nd paper of the series. 2022, October 2.

[Li22c] Trey Li. "Power Residue Symbol Order Detecting Algorithm for Subset Product over Algebraic Integers". 3rd paper of the series. 2022, October 3.

[Li22d] Trey Li. "Multiple Modular Unique Factorization Domain Subset Product with Errors". 4th paper of the series. 2022, October 4.

[Li22e] Trey Li. "Post-Quantum Key Exchange from Subset Product with Errors". 5th paper of the series. 2022, October 5.

[Li22f] Trey Li. "Post-Quantum Public Key Cryptosystem from Subset Product with Errors". 6th paper of the series. 2022, October 6.