GENERIC SIGNATURE FROM NOISY SYSTEMS

TREY LI

ABSTRACT. This paper provides a cryptographic application to our previous paper [Li22h], where we considered noisy systems of discrete exponential equations over a land, which is a monoid without the requirement of associativity. In this paper we give a general methodology for signature scheme construction from noisy systems.

1. INTRODUCTION

In [Li22g] we give signature schemes from the multiple modular subset product with errors problem (M-MSPE) as well as the multiple modular subset sum with error problem (M-MSSE) and the learning parity with noise problem (LPN). In [Li22h] we give general language to this kind of problems by introducing noisy systems. In this paper we give a generic signature scheme from noisy systems over a uniquely generated land with inverse and with a unique solution (with overwhelming probability), where unique generation and existence of inverses are basic requirements for using the Fiat-Shamir transformation, and the requirement of overwhelming probability of unique solution is for the security reduction from the scheme to the underlying noisy system.

2. NOISY SYSTEMS

We review some concepts proposed in [Li22h].

A *land* is a monoid without the axiom of associativity. Typical examples are groups, rings, etc. A special example is integers with subtraction $(\mathbb{Z},-)$, which is a land but not a group. A land L is said to be *with inverse* if for every element $a \in L$ there is an element $b \in L$ such that $ab = 1$, where 1 is the identity of L.

A land homomorphism is a morphism between two lands that preserves the operation. A land isomorphism is a bijective land homomorphism.

Let $\approx$ be the generalized equals sign that captures both the equals sign $=$ and the isomorphism sign $\cong$. A *noisy (discrete exponential) equation* over a land L is an equation of the form

$$\left(\prod_{i=1}^{n} a_i^{x_i}\right) \cdot e \approx a,$$

where $a_1,\dots,a_n \in L$ and $a \in L$ are given, but $e \in L$ is not given, also $a_i^1 = a_i$ and $a_i^0 = 1$ (identity). The goal is to find $(x_1,\dots,x_n) \in \mathbb{Z}^n$. We call $a_1,\dots,a_n$ the bases and e the noise. A *noisy (discrete exponential equation) system* is a system of noisy discrete exponential equations. A *noisy (restoration) problem* is a problem that asks to solve a polynomial size noisy system with predefined base distribution $D_1(L)$ and noise distribution $D_2(L)$.

This is the 9th paper of the series. Previously: [Li22a; Li22b; Li22c; Li22d; Li22e; Li22f; Li22g; Li22h].

Date: October 9, 2022.

Email: treyquantum@gmail.com

3. IDEA

A signature scheme allows people to sign on a digital document such that no one else can forge a signature. This implies that the scheme does not leak the secret that the signer use to create signatures; and that the signer cannot deny her signatures.

There is a well-known generic way to construct a signature scheme: first create a Schnorr identification scheme then use the Fiat-Shamir transform to make it a signature scheme. We construct our scheme in the same way. In fact, our generic signature scheme is a generalization of the scheme in [Li22g] by using more general noisy problems than subset product with errors [Li22g; Li22d; Li22a].

4. GENERIC IDENTIFICATION SCHEME

Let $m,n,d \in \mathbb{N}$ with m polynomial in n and d superpolynomial in n. Let $L = \langle g \rangle$ be a land with inverse of order d generated by g. Let $D_1(L)$ and $D_2(L)$ be two distributions over L. We shall assume that the land operation as well as the sampling of $D_1(L)$ and $D_2(L)$ are efficient.

Let $M = \{a_{i,j}\}_{m\times n} \leftarrow D_1(L)^{m\times n}$. Let $(s,u) \leftarrow \mathbb{Z}_d^n \times D_2(L)^m$. Let $S = (S_1,\ldots,S_m)$ with $S_i = \left(\prod_{j=1}^n a_{i,j}^{s_j}\right) \cdot u_i$ for $i \in [m]$. The prover's private key is (s,u); the pubic key is (M,S).

(1) The prover samples $(x,e) \leftarrow \mathbb{Z}_d^n \times D_2(L)^m$; computes $A = (A_1,\ldots,A_m)$ with $A_i = \left(\prod_{j=1}^n a_{i,j}^{x_j}\right) \cdot e_i$ for $i \in [m]$; and sends A to the verifier as the commitment;
(2) The verifier samples $c \leftarrow \mathbb{Z}_d$ and sends it to the prover as the challenge;
(3) The prover computes $y = x - cs = (x_1 - cs_1, \ldots, x_n - cs_n) \pmod d$ and $v = eu^{-c} = (e_1 u_1^{-c}, \ldots, e_m u_m^{-c})$, and sends (y,v) to the verifier as the response;
(4) The verifier computes $B = (B_1,\ldots,B_m)$ with $B_i = \prod_{i=1}^n a_{i,j}^{y_j}$ for $i \in [m]$; computes $A' = B \cdot S^c \cdot v = (B_1 \cdot S_1^c \cdot v_1, \ldots, B_m \cdot S_m^c \cdot v_m)$; and accepts if $A' = A$ or rejects if $A' \neq A$.

5. CORRECTNESS

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

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

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

□

6. SECURITY

We assume that the adversary is given the public key pk and can eavesdrop previous executions of the protocol with respect to 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 what we assume is 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 2. If the underling noisy problem is hard and it has a unique solution with overwhelming probability, then the identification scheme is secure against impersonation.

Proof. We use the generic proving routine illustrated in [KL14, p. 457, 2nd edition] with the change that we argue that it also works for underlying problems with a unique solution with overwhelming probability rather than with probability 1.

Let $\mathcal{A}$ be any probabilistic polynomial time adversary, which is given pk and o_{sk}. Define a noisy system solver $\mathcal{B}$ as the following. $\mathcal{B}$ takes as input a noisy problem instance (M,S) (together with the ground land L). It runs $\mathcal{A}(pk) = \mathcal{A}(M,S)$. When $\mathcal{A}$ outputs A, $\mathcal{B}$ chooses a uniform $c_1 \leftarrow \mathbb{Z}_d$ 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 $c_2 \leftarrow \mathbb{Z}_d$; $\mathcal{A}$ responses with $(y^{(2)}, v^{(2)})$. If

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

and

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

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

$$c_1 \neq c_2$$

then $\mathcal{B}$ outputs $(y^{(1)} - y^{(2)})/(c_1 - c_2) \pmod{d}$. In the following let us keep in mind that (M,S) might not have a unique solution hence the two times that $\mathcal{A}$ impersonates are possibly with respect to two different solutions x and x' to (M,S), and therefore the output $(y^{(1)} - y^{(2)})/(c_1 - c_2) \pmod{d}$ of $\mathcal{B}$ might not be a solution to (M,S) even if $\mathcal{A}$ succeeds twice with $c_1 \neq c_2$.

Let ω be the randomness during the execution. Define $V(\omega,c) = 1$ if and only if the problem (M,S) has a unique solution and $\mathcal{A}$ correctly responds to challenge c when randomness ω is used in the rest of the execution; define $V'(\omega,c) = 1$ if and only if the problem (M,S) has nonunique solutions and $\mathcal{A}$ correctly responds to challenge c when randomness ω is used in the rest of the execution. For any fixed ω, define $\delta_\omega := \Pr_c[V(\omega,c) = 1]$ and $\delta'_\omega := \Pr_c[V'(\omega,c) = 1]$; with ω fixed, they are the probabilities over c that $\mathcal{A}$ responds correctly under the two situations of unique and nonique solutions of (M,S) respectively.

Denote $\delta(n)$ as the probability that $\mathcal{A}$ succeeds when (M,S) has a unique solution. We have

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

Denote $\delta'(n)$ as the probability that $\mathcal{A}$ succeeds when (M,S) has nonunique solutions. We have

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

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

$$\bar{\delta}(n) = \mathrm{P}\cdot\delta(n) + (1-\mathrm{P})\cdot\delta'(n).$$

In the following we show that this probability is negligible.

Denote P as the probability that (M,S) has a unique solution. By assumption, P is overwhelming.

Denote $\tilde{\delta}(n)$ as the probability that $\mathcal{B}$ succeeds. Note that $\mathcal{B}$ successfully solves (M,S) if (1) (M,S) has a unique solution and $\mathcal{A}$ succeeds twice with $c_1 \neq c_2$; or (2) (M,S) has nonunique solutions and $\mathcal{A}$ succeeds with twice with $c_1 \neq c_2$ and that the two times that $\mathcal{A}$ succeeds are with respect to the same solution $x^{(1)} = x^{(2)}$ to (M,S). Hence

$$\begin{aligned}
\tilde{\delta}(n) =& \mathrm{P}\cdot\Pr_{\omega,c_1,c_2}[V(\omega,c_1)\wedge V(\omega,c_2)\wedge c_1\neq c_2] \\
&+(1-\mathrm{P})\cdot\Pr_{\omega,c_1,c_2}[V'(\omega,c_1)\wedge V'(\omega,c_2)\wedge c_1\neq c_2 \wedge x^{(1)}=x^{(2)}] \\
\geq& \mathrm{P}\cdot\Pr_{\omega,c_1,c_2}[V(\omega,c_1)\wedge V(\omega,c_2)\wedge c_1\neq c_2] \\
\geq& \mathrm{P}\cdot\left(\Pr_{\omega,c_1,c_2}[V(\omega,c_1)\wedge V(\omega,c_2)] - \Pr_{\omega,c_1,c_2}[c_1=c_2]\right) \\
=& \mathrm{P}\cdot\left(\sum_{\omega}\Pr[\omega]\cdot(\delta_\omega)^2 - 1/d\right) \\
\geq& \mathrm{P}\cdot\left(\left(\sum_{\omega}\Pr[\omega]\cdot\delta_\omega\right)^2 - 1/d\right) \\
=& \mathrm{P}\cdot\left(\delta(n)^2 - 1/d\right),
\end{aligned}$$

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

Now by the assumption that the noisy problem (M,S) is hard, $\mathcal{B}$ succeeds with negligible probability. I.e. $\tilde{\delta}(n)$ is negligible. Also note that P is overwhelming and $1/d$ is negligible. Hence $\delta(n)$ is negligible.

Also $1-\mathrm{P}$ is negligible since P is overwhelming.

Therefore $\bar{\delta}(n) = \mathrm{P}\cdot\delta(n) + (1-\mathrm{P})\cdot\delta'(n)$ is negligible. I.e., $\mathcal{A}$ succeeds with negligible probability. Hence the scheme is secure.

□

7. Generic signature scheme

Let $m,n,d \in \mathbb{N}$ with m polynomial in n and d superpolynomial in n. Let $L = \langle g\rangle$ be a land with inverse of order d generated by g. Let $D_1(L)$ and $D_2(L)$ be two distributions over L with efficient sampling algorithms. The scheme is the following.

KeyGen(m,n,L):

- Sample $M = \{a_{i,j}\}_{m\times n} \leftarrow D_1(L)^{m\times n}$;
- Sample $(s,u) \leftarrow \mathbb{Z}_d^n \times D_2(L)^m$;
- Compute $S = (S_1,\ldots,S_m)$ with $S_i = \left(\prod_{j=1}^n a_{i,j}^{s_j}\right)\cdot u_i$ for $i \in [m]$;

- Output (sk, pk) with $sk := (s, u)$, $pk := (M, S)$.

Sign(sk, a):

- Sample $(x, e) \leftarrow \mathbb{Z}_d^n \times D_2(L)^m$ and compute $A = (A_1, \ldots, A_m)$ with $A_i = \left(\prod_{j=1}^n a_{i,j}^{x_j}\right) \cdot e_i$ for $i \in [m]$;
- Compute $c = H(A, a)$, where H is a cryptographic hash function;
- Compute $y = x - cs = (x_1 - cs_1, \ldots, x_n - cs_n) \pmod d$ and $v = eu^{-c} = (e_1 u_1^{-c}, \ldots, e_m u_m^{-c})$;
- 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 $A' = B \cdot S^c \cdot v = (B_1 \cdot S_1^c \cdot v_1, \ldots, B_m \cdot S_m^c \cdot v_m)$;
- Compute $c' = H(A', a)$;
- Accept if $c' = c$ or rejects if $c' \neq c$.

8. Correctness

Theorem 3. $c = c'$.

Proof. By a similar argument to the proof of Theorem 1, we have $A' = A$. Then $c' = H(A', a) = H(A, a) = c$. □

9. Security

The security is from Theorem 2 and 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 the underling noisy problem is hard and has a unique solution with overwhelming probability and that the hash function H is modeled as a random oracle, then our signature scheme is secure against impersonation.

Proof. Immediate from Theorem 2 and 4. □

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.
[Li22g] Trey Li. “Post-Quantum Signature from Subset Product with Errors”. 7th paper of the series. 2022, October 7.
[Li22h] Trey Li. “Discrete Exponential Equations and Noisy Systems”. 8th paper of the series. 2022, October 8.