A Verifiable Secure Metering Scheme with Shadow-Self-Refreshing

Jiin-Chiou Cheng[1], Jiun-Ming Chen[2], and Chi-Sung Laih[3]
[1,3]Dep. of Electrical Engineering, National Cheng Kung University, Tainan, Taiwan, R.O.C.
[2]Dep. of Mathematics, National Taiwan University, Taipei, Taiwan, R.O.C.
E-mail:[1]chiou@mail.stut.edu.tw, [2]jmchen@ntu.edu.tw, [3]laihcs@eembox.ncku.edu.tw

Abstract-*Metering schemes were first suggested by Naor and Pinkas in 1998 in order to decide the advertisement charge for website server. They can be applied widely in the measure of impact for websites. Several popular portal sites usually charge the advertising expense with its impact. So, secure metering scheme should have a necessity of existence in modern commercial for exhibiting impact accurately. Up to now, most metering schemes may achieve the measure of impact; however, they all have some shortcomings, e.g. vulnerability for collusion attack, and lack for verification of shadow. In this work, we endeavor to construct a scheme without the above flaws, and propose a novel and secure metering scheme in which there are several features worthy to notice: security against collusion attack, verifiable shadow, and shadow-self-update. We give a complete analysis of security for the proposed scheme, including its resistance to active attacks and passive attacks. Also the evaluation of performance of our scheme is displayed. From the viewpoint of security and convenience, our proposed scheme is superior to the other existing ones.*

Keywords: Metering Scheme, Modified Weil Pairing, Forward Security, Verifiable Secret Shadow.

1 Introduction

A metering scheme is a protocol which measures the number of times that website is impacted by clients (players). A website is popular if the number of times visited by players is obviously more than other websites. So the number of times of website impacted by players should be an important reference index. In many websites, the measurement of the number of the visitor is usually designed and then displayed on the homepage to emphasize its being popular among surfing people. However, usually the measured count is not objective and reasonable. The number of the visitor is counted once again while the website is refreshed by the player. Thus when the identical player refreshes the website one hundred times, the number of visitors of the specific website is added one hundred times. Although such an unreasonable mechanism of measurement has been improved by software technique, a lot of non-impersonal processes about measuring the number of visitors still exist in many websites.

Certain commercial or entertaining behavior, e.g., voting for stars or goods, usually appears in several websites. Such a behavior of voting need a impersonal measurement more. It is better that each participant only has one vote even if the participant votes many times. To achieve the precise measurement, adopting metering schemes is a workable way.

2 Previous work

Naor and Pinkas [11] introduced metering schemes firstly in 1998. Their proposed schemes are all based on Shamir's (t, n) secret sharing. When one player visits certain website, he should give a secret share to the specific website. Then, when the website has received t secret shares from t distinct players, it is able to reconstruct the primary secret and prove that it has been visited by t different visitors. After checking and confirming this primary secret, the audit agency may be asked to pay money corresponding to the t amount of visitors to the website for advertisement fee. In their schemes, the robustness has been considered. However, their method is inefficient since the website is required to receive especially two verification polynomials $A(x, S \circ \tau)$ and $B(x, S \circ \tau)$ from the audit agency at every period of time τ, and exploit them in verification phase. Their schemes are all one-time-pad. It might bring the communication cost as entering the next period of time. Moreover, the websites in Naor and Pinkas' schemes incline to suffer from collusion attack, where the fact is pointed out by W. Ogata and K. Kurosawa [12]. To ameliorate the weakness, W. Ogata and K. Kurosawa proposed a new unconditional-security metering scheme in 2000 [12]. Their scheme is similar to Naor and Pinkas' schemes, but adopts three-dimensional polynomial for key polynomial rather than two-dimensional polynomial. Their scheme can prevent any two players from collusion attack. However it still happens to have one serious shortcoming that a collusion between one player and one website is possible. In 2000, C. Blundo, A. D. Bonis and B. Masucci introduced the concept of multi-pricing [3]. They define metering scheme with pricing in teams of entropy, and give three requirements for metering system. They also derive a lower bound for the size of players' information and websites' information respectively. Their proposed scheme satisfies the three requirements for metering system. However, a serious drawback exists in their scheme: While the player C_i visits the website S_j during the period of time τ, he will send to the website $h-l$ points $P_{l+1}(i, j \circ \tau), ..., P_h(i, j \circ \tau)$. Since the authentication of these points is not carried out, the website S_j might be cheated and receives a fake subsecret from the player C_i. Thus, the website S_j will fail to reconstruct the primary secret during the current period of time. In 2001, C. Blundo, A. D. Bonis, B. Masucci and D. R. Stinson proposed another scheme[2] similar to the prior one. The scheme provides the mechanism of dynamic multi-pricing. According to their proposition, the website S_j has to receive several fixed points $Q(x, j \circ \tau)$ evaluated at $h - h_j^\tau$ points other than $x = 1, 2, 3, ..., n$ in advance at the beginning of the period of time τ. The idea does not seem to be wise because of the difficulty of the prediction of the number of points sent to the specific website S_j. Moreover, the problem for the authentication on the subsecrets received by the website still exists in this scheme. Later, B. Masucci and D. R. Stinson rewrite the metering scheme with pricing [10] which integrates their prior papers [3] and [2]. In the rewritten metering scheme, the foundation of dynamic multi-pricing is rearranged. During the end of the period of time τ, if the website has received r points from the players, where $r < h$, h represents the least number of points to reconstruct the primary secret, then he will ask the audit agency for help and request $h - r$ points, evaluated at points other than $x = 1, 2, 3, ..., n$. With the original r points, the website can recover the primary secret at the current period of time. This way is cleverer than the prior one. However, the authentication is still not solved.

In the paper, we propose a novel metering scheme with verifiable secret shadow, shadow-self-refreshing, verifiable fragment-proof, and security against collusion attack. These features do not exist simultaneously in well-known metering schemes.

3 Our scenario and model

- **Our scenario:**

  Suppose there exists a community with numerous players and there are many websites in the community. Popular websites have offered a best field of advertisements and their advertising benefit is relatively large. In general, the advertisement fee is charged according to the amount of visitors by which website is visited during certain period of time. To count the number of visitors accurately, appropriate metering scheme is necessary. Recently there are metering schemes designed by means of software technique. However they are not secure perfectly and vulnerable to replay attack.

- **Our model:**

  The framework of our model is illustrated in Fig. 1. Each player U_i , $i = 1, 2, ..., n$ is equiped with a distinct shadow by the Trusted Audit Agency (TAA) in advance. While visiting a website, he/she utilizes his/her shadow to sign the website (in fact, to sign the ID, say w_l, of the website). The signature signed by each player may be verified. In addition, each player can refresh his/her shadow with itself while being at the end of certain period of time.

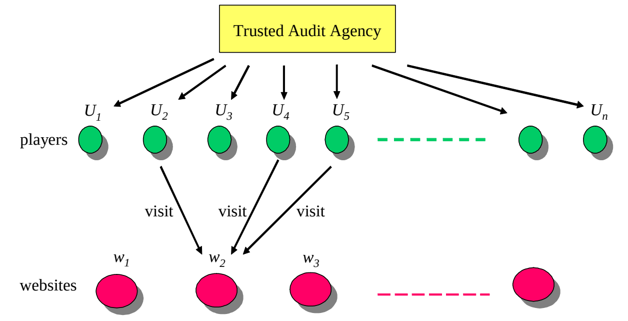

Fig. 1 Our framework of model

- Collusion attack is always a concern in metering schemes. Our proposed scheme is able to prevent the following two kinds of collusion attacks, and has the feature of forward security.

  - **Collusion Attack Type I:** The collusion behavior happens in the situation that two or more websites collaborate to derive the primary proof with their less fragment-proofs obtained from players (visitors).

- **Collusion Attack Type II:** The collusion behavior happens in the situation that players (visitors) and websites collaborate to derive the primary proof.
- **Forward Security:** Websites can not derive the primary proof regarding the current period of time with the help of the previous fragment-proofs or primary proofs.

4 Proposed scheme

We propose a verifiable secure metering scheme. Our metering scheme possesses four features simultaneously, which do not ever exist in known metering schemes: verifiable secret shadow, shadow-self-refreshing, verifiable fragment-proof, and security against collusion attack [10].

4.1 Preliminaries

Suppose $E(F_p)$ is a supersingular elliptic curve defined by the Weierstrass equation $y^2 = x^3 + 1$ over F_p, where $p = 2 \bmod 3$ and $p = 6q - 1$ for some large prime $q > 3$. With the assumptions in [4], $E(F_p)$ will form a cyclic group of order $p + 1$. From Lagrange's Theorem, the group $E(F_p)$ should contain order-q points, which forms a cyclic subgroup G_1 of order-q. For the prime q, the extension field F_{p^2} also has *the* multiplicative subgroup of order-q. We denote the multiplicative subgroup as G_2. Refer to [4], a modified Weil paring is defined as a map:

$$\hat{e} : G_1 \times G_1 \longrightarrow G_2.$$

The modified Weil paring possesses the following properties:

- Bilinearity: $\hat{e}(P, Q + R) = \hat{e}(P, Q)\hat{e}(P, R)$ and $\hat{e}(Q + R, P) = \hat{e}(Q, P)\hat{e}(R, P)$ for any P, Q, $R \in G_1\backslash\{\mathcal{O}\}$.
- Non-degeneracy: If $\mathcal{G}$ is a generator of G_1, then $\hat{e}(\mathcal{G}, \mathcal{G})$ is a generator of G_2.
- Commutativity: $\hat{e}(P, Q) = \hat{e}(Q, P)$ for any P, $Q \in G_1\backslash\{\mathcal{O}\}$.
- Efficient computation: For all P, $Q \in G_1\backslash\{\mathcal{O}\}$, there exists a efficient algorithm for $\hat{e}(P, Q)$.

4.2 Scheme

The proposed scheme consists of the following steps: key-generation, shadow-refreshing, visit, proof-combination, and proof-verification.

- **Key-Generation Phase:** Suppose TAA possesses a pair of private/public keys: private key k_{TA} and public key $Q_{TA} = k_{TA}\mathcal{G}$, and its public key is known by all websites and players.

  (a). Based on Shamir's (t, n) secret sharing, TAA randomly chooses r and $a_j \in Z_q^*$, $1 \leq j \leq t - 1$, and computes $R = r\mathcal{G}$ and $A_j = a_j\mathcal{G}$. With r and a_j, $1 \leq j \leq t - 1$, TAA constructs a polynomial of degree $t - 1$: $f_\tau(x) = k_{TA} + (\tau - 1)r + \tau \sum_{j=1}^{t-1} a_j x^j \bmod q$, in which τ, $1 \leq \tau \leq \tau_{\max}$, represents certain period of time in the entire game. Next, he computes $s_i^{(1)} = f_1(i) \bmod q$ and $\delta_i = r + \sum_{j=1}^{t-1} a_j i^j \bmod q$ for $i = 1, 2, ..., n$, where $s_i^{(1)}$ is the secret shadow of player U_i at the first period of time and δ_i is the update parameter for player U_i. The primary proof is defined as $Sign_l^{(\tau)} = f_\tau(0)H(w_l)$ for a specific website w_l during the period of time τ, where $w_l \in Z_q^*$ denotes the ID of the l-th website and $H(\cdot)$ is a one-way hash function from $\{0, 1\}^*$ to $G_1\backslash\{\mathcal{O}\}$.

  (b). TAA keeps r and $a_j \in Z_q^*$, $1 \leq j \leq t - 1$, secret and publishes the system parameters R and A_j, $1 \leq j \leq t - 1$. Before the start of the game, TAA commits the secret shadow $s_i^{(1)}$ and the update parameter δ_i to player U_i, $1 \leq i \leq n$, respectively via a secure channel. Each player U_i might check the soundness of $s_i^{(1)}$ and δ_i by means of the following relations, referring to **A.1** and **A.2**:

  $$s_i^{(1)}\mathcal{G} \overset{?}{=} Q_{TA} + \sum_{j=1}^{t-1} i^j A_j, \qquad (1)$$

  $$\delta_i\mathcal{G} \overset{?}{=} R + \sum_{j=1}^{t-1} i^j A_j. \qquad (2)$$

  If one of the above relations does not hold, the player U_i can request TAA to recommit $s_i^{(1)}$ and δ_i.

- **Shadow-Refreshing Phase:** Whenever being at the end of the current period of time τ, the player U_i can refresh his/her shadow without interaction by the old shadow $s_i^{(\tau)}$ and the update parameter δ_i:

  $$s_i^{(\tau+1)} = s_i^{(\tau)} + \delta_i, \quad 1 \leq \tau \leq \tau_{\max}, \qquad (3)$$

where $s_i^{(\tau+1)}$ denotes the new shadow owned by the player U_i at the period of time $\tau+1$.

- **Visit Phase:**

(a). During the period of time $\tau+1$, while the player U_i visits the website w_l, in which $w_l \in Z_q^*$ denotes the ID of the l-th website, he/she processes the following operation:

$$Sign_{il}^{(\tau+1)} = s_i^{(\tau+1)} H(w_l), \tag{4}$$

where $Sign_{il}^{(\tau+1)}$ is called a fragment-proof. Next, he/she transmits $\{Sign_{il}^{(\tau+1)}, w_l, U_i\}$ to the website w_l for legal entering.

(b). When receiving $\{Sign_{il}^{(\tau+1)}, w_l, U_i\}$ from the player U_i, the validity of the fragment-proof $Sign_{il}^{(\tau+1)}$ is verified as follows, referring to **A.3**:

$$\begin{aligned}\hat{e}(Sign_{il}^{(\tau+1)}, \mathcal{G}) &\overset{?}{=} \hat{e}(H(w_l), Q_{TA}) \\ &\cdot \hat{e}(H(w_l), \tau R) \cdot \hat{e}(H(w_l), (\tau+1)\sum_{j=1}^{t-1} i^j A_j).\end{aligned} \tag{5}$$

If the above holds, the website w_l accepts the fragment-proof and let the player U_i login. Otherwise, refuse the fragment-proof and the player U_i.

- **Proof-Combination Phase:**

(a). When the amount of fragment-proofs received by the website w_l exceeds t during the period of time $\tau+1$, the website w_l processes the operation of proof-combination to obtain the primary proof. The website w_l picks arbitrary t fragment-proofs, without loss generality, say $Sign_{il}^{(\tau+1)}$, $1 \le i \le t$, collected by the website w_l, and performs the following computation:

$$Sign_l^{(\tau+1)} = \sum_{i=1}^{t} \left[Sign_{il}^{(\tau+1)} c_i \right]. \tag{6}$$

where $c_i = \prod_{1 \le j \le t, j \ne i} \frac{j}{j-i}$. The Equation (6) refers to **A.4**. The compound proof $Sign_l^{(\tau+1)}$ might be verified using the following check, referring to **A.5**:

$$\hat{e}(Sign_l^{(\tau+1)}, \mathcal{G}) \overset{?}{=} \hat{e}(H(w_l), Q_{TA}) \hat{e}(H(w_l), \tau R). \tag{7}$$

Finally, the website w_l sends $\{Sign_l^{(\tau+1)}, w_l\}$ to request payment according to their prior contract.

(b). If the number r of fragment-proofs received by the website w_l is less than t at the end of the period of time $\tau+1$, then the website w_l sends TAA the message "I (website w_l) have received r fragment-proofs from players during the period of time $\tau+1$" [10]. TAA will send the website w_l other $(t-r)$ fragment-proofs, which are generated by means of new $(t-r)$ shadows different from $s_i^{(\tau+1)}$, $i = 1, 2, 3, ..., n$. When the website w_l receives these extra fragment-proofs, with the original r fragment-proofs, it is able to derive the primary proof $Sign_l^{(\tau+1)}$. Finally, the website w_l sends $\{Sign_l^{(\tau+1)}, w_l\}$ to TAA for requesting payment.

- **Proof-Verification Phase:**
When TAA receives $\{Sign_l^{(\tau+1)}, w_l\}$ from the website w_l, he verifies the correctness of the fragment-proof $Sign_l^{(\tau+1)}$ by the same procedure as (7). If it holds, TAA approves that i). at least t players have visited the website w_l during the period of time $\tau+1$ or ii). only r players visit the website w_l if the website w_l has ever requested TAA to assist generating the primary proof in Proof Combination Phase. Thus, pay the money of t amount or r amount to the website w_l according to the prior contract.

5 Analysis of security

Theorem 1 (Existential Unforgeability against Adaptive Chosen Message Attack). In the random oracle model, the fragment-proof of our scheme is existentially unforgeable against the adaptive chosen message attack.

Proof. In the random oracle model, suppose an attacker (forger) $\mathcal{F}$ has the following capacity: being capable of forging the valid fragment-proof of our scheme with success probability $\epsilon_{\mathcal{F}}$ in time cost $\tau_{\mathcal{F}}$ after querying the hashing random oracle q_H times and the signing random oracle q_{sig} times. A simulator (reductionor) $\mathcal{R}$ attempts to utilize the capacity of such a forger to break a computationally hard problem - CDH problem: given $s\mathcal{G}$ and $h'\mathcal{G} \in G_1 \backslash \{\mathcal{O}\}$, find $h's\mathcal{G} \in G_1 \backslash \{\mathcal{O}\}$, where h' and s are random numbers in Z_q^*. Without loss of generality, we omit the superscript τ and subscript i of $s_i^{(\tau)}$. We will derive the relation between $\epsilon_{\mathcal{F}}$ and $\epsilon_{\mathcal{R}}$, where $\epsilon_{\mathcal{F}}$ and $\epsilon_{\mathcal{R}}$ denote the success probabilities of forger $\mathcal{F}$ and reductionor $\mathcal{R}$ respectively. In the proof of reduction under random oracle model, $\mathcal{R}$ must simulate the key generation, the hashing random oracle $\mathcal{H}^R$, the signing random oracle $\mathcal{S}^R$ and the verifying random oracle $\mathcal{V}^R$. Their distributions have to be indistinguishable from the ones which the forger $\mathcal{F}$ expects.

While the forger $\mathcal{F}$ queries the signing random oracle with w, the reductionor $\mathcal{R}$ simulates the signing random oracle $\mathcal{S}^R$ and the hashing random oracle $\mathcal{H}^R$ in the following manner [6]: First, $\mathcal{R}$ is given $Q(= s\mathcal{G})$ and $H'(= h'\mathcal{G}) \in G_1 \backslash \{\mathcal{O}\}$ by simulating the key generation, and sends $Q_i^{(\tau)}$ to the forger $\mathcal{F}$. Next, for $j = 1$ to $q_H + q_{sig} + 1$, do

(i) If the query w happens in the past, $\mathcal{R}$ returns the same hash value and the same signature as the answers of querying the hashing random oracle and the signing random oracle respectively.

(ii) Otherwise, $\mathcal{R}$ chooses l randomly from $[1, q_H + q_{sig} + 1]$.

- If $l \neq j$, pick $h_j \in Z_q^*$ at random and let $H(w) = h_j\mathcal{G}$ and $Sign_j = h_j \times s\mathcal{G} = h_j s\mathcal{G}$. Update the hashing and signing database with the new tuple $(w, Sign_j, h_j\mathcal{G}, h_j)$, and return the new $Sign_j$ as the answer of querying the signing random oracle.
- If $l = j$, then assume $H(w)$ is equal to $h'\mathcal{G}$, and let $Sign_j$ be $\perp$, which will fail in the verification. Update the hashing and signing database with the new tuple $(w, \perp, h'\mathcal{G}, \perp)$, and $\mathcal{R}$ aborts the querying this time.

At each simulation of $\mathcal{S}^R$, the signature created by reductionor $\mathcal{R}$ will fail in the verification with the probability $1/(q_H + q_{sig} + 1)$. So, after querying the signing random oracle q_{sig} times, $\Pr[\mathcal{R}\ fails] = q_{sig}/(q_H + q_{sig} + 1)$. Therefore, $\Pr[\mathcal{R}\ succeeds] = 1 - q_{sig}/(q_H + q_{sig} + 1)$.

While the forger $\mathcal{F}$ queries the verifying random oracle with $(w^*, Sign_j^*)$, the reductionor $\mathcal{R}$ simulates the verifying random oracle $\mathcal{V}^R$ as follows: check whether $(w^*, Sign_j^*)$ is a valid signature employing the verification equation (5). If so and $H(w^*) = h'\mathcal{G}$, then return "verification successful" and $Sign_j^*(= h's\mathcal{G})$. The reductionor $\mathcal{R}$ outputs the result $Sign_j^*$ of CDH problem: given $s\mathcal{G}$ and $h'\mathcal{G} \in G_1 \backslash \{\mathcal{O}\}$, find $h's\mathcal{G} \in G_1 \backslash \{\mathcal{O}\}$.

To sum up, $\mathcal{R}$ succeeds in solving CDH problem with the probability $\epsilon_{\mathcal{R}} = (1 - q_{sig}/(q_H + q_{sig} + 1)) \cdot \epsilon_{\mathcal{F}} \cdot (1/(q_H + 1)) = \epsilon_{\mathcal{F}}/(q_H + q_{sig} + 1)$ in the time cost $\tau_{\mathcal{R}} = \tau_{\mathcal{F}} + (q_H + q_{sig} + 1) \cdot \{2[\mathbf{pm}]\}$, where $[\mathbf{pm}]$ denotes the time cost of point multiplication. Thus, we obtain an upper bound of success that our scheme is attacked:

$$\mathbf{Suc}^{\mathrm{Ours}}(w; q_H, q_{sig}, \tau_{\mathcal{F}}) \leq (q_H + q_{sig} + 1)\mathbf{Suc}^{\mathrm{CDH}}(w; \tau_{\mathcal{R}}),$$

where $\tau_{\mathcal{R}} = \tau_{\mathcal{F}} + (q_H + q_{sig} + 1) \cdot \{2[\mathbf{pm}]\}$. □

Assumption 2 (BDL problem is hard). By a suitable choice on the size p of an elliptic curve, the Bilinear Discrete Logarithm problem on supersingular curves should remain hard. For such a curve $E(F_p)$, the complexity to solve the problem can be expressed as sub_exp(p^c) for $c \leq 6$ [8]. The sub_exp$(\cdot)$ denotes a subexponential function which grows much slower than exponentials but much faster than polynomials.

Theorem 3 (Security against Collusion Attack Type I). Two or more websites can not collaborate to derive the primary proof with their less fragment-proofs obtained from visitors respectively.

Proof. Suppose w_a derives the primary proof $Sign_a^{(\tau)}$ by collaborating with w_b at the period of time τ. For w_a and w_b, we assume that they have received the fragment-proofs $\{Sign_{ia}^{(\tau)} | 1 \leq i \leq u\}$ and $\{Sign_{ib}^{(\tau)} | u + 1 \leq i \leq t\}$ respectively at the end of the period of time τ. To derive $Sign_a^{(\tau)}$, from (6) the number of $Sign_{ia}^{(\tau)}$ must be at least t. However website w_a only has the account u for $Sign_{ia}^{(\tau)}$ so far. To complement the vacancies, website w_a collaborates with w_b to derive $\{Sign_{ia}^{(\tau)} | u + 1 \leq i \leq t\}$ from $\{Sign_{ib}^{(\tau)} | u + 1 \leq i \leq t\}$. But the derivation fails due to

$$Sign_{ia}^{(\tau)} = f_\tau(i)H(w_a) = (k_{TA} + \tau r - r + \tau \sum_{j=1}^{t-1} a_j i^j)H(w_a)$$

and

$$Sign_{ib}^{(\tau)} = f_\tau(i)H(w_b) = (k_{TA} + \tau r - r + \tau \sum_{j=1}^{t-1} a_j i^j)H(w_b).$$

Unless we can solve the hard problem of Bilinear Discrete Logarithm (BDL) to get $f_\tau(i)(= s_i^{(\tau)})$ from $Sign_{ib}^{(\tau)}$, it is impossible to derive $\{Sign_{ia}^{(\tau)} | u + 1 \leq i \leq t\}$ from $\{Sign_{ib}^{(\tau)} | u + 1 \leq i \leq t\}$. *So two or more websites can not collaborate to derive the primary proof with their less fragment-proofs obtained from visitors respectively.* □

Theorem 4 (Security against Collusion Attack Type II). Players (visitors), the account of which is less than the threshold t, and websites can not collaborate to derive the primary proof.

Proof. Suppose a specific website w_l would like to collude with numerous players less than the number of t to extract the primary proof $Sign_l^{(\tau)}$ at the period of time τ. Each player only provides one fragment-proof at every period of time anyway and can not give other evidences beneficial for the derivation of the primary proof. Thus the website w_l can not derive the primary proof as long as the number of players colluded with is

Table 1. Evaluation of performance of our scheme

	Evaluation of performance
compu. cost for TAA during Key-Gen. Phase	$\approx nt[\mathbf{m}]$
compu. cost per player during Key-Gen. Phase	$\approx t[\mathbf{pm}]$
commu. cost for TAA during Key-Gen. Phase	$\approx 2n\|q\|$
compu. cost per player during Visit Phase	$\approx 3[\mathbf{pm}] + 4[\mathbf{w}]$
compu. cost per website during Proof-Comb. Phase	$\approx t[\mathbf{pm}] + (t-1)[\mathbf{pa}] + [\mathbf{w}]$

n: # of players participating the game.
$[\mathbf{m}]$: modular multiplication, $[\mathbf{w}]$: modified Weil pairing.
$[\mathbf{pa}]$: point addition, $[\mathbf{pm}]$: point multiplication.

less than the threshold t. *So Players (visitors), the account of which is less than the threshold t, and websites can not collaborate to derive the primary proof.* □

Theorem 5 (Forward Security). Website can not derive the primary proof regarding the current period of time from the previous primary proof or fragment-proofs.

Proof. (a). Suppose a specific website w_l obtains the primary proof $Sign_l^{(\tau)}$ during the period of time τ. At the next period of time $\tau+1$, the website attempts to derive the primary proof $Sign_l^{(\tau+1)}$ with the help of $Sign_l^{(\tau)}$. From the definition of the primary proof $Sign_l^{(\tau)}$, we have $Sign_l^{(\tau)} = (k_{TA} + \tau r - r)H(w_l)$. Parsing $Sign_l^{(\tau+1)}$, we infer the following relation:

$$\begin{aligned} Sign_l^{(\tau+1)} &= f_{\tau+1}(0)H(w_l) \\ &= (k_{TA} + \tau r)H(w_l) \\ &= (k_{TA} + \tau r - r)H(w_l) + rH(w_l) \\ &= Sign_l^{(\tau)} + rH(w_l). \end{aligned}$$

So, it is infeasible obviously to attempt to derive $Sign_l^{(\tau+1)}$ with the previous primary proof $Sign_l^{(\tau)}$ because of unknown r. (b). Similarly, it is hard to attempt to derive $Sign_l^{(\tau+1)}$ with the previous fragment-proofs $Sign_{il}^{(\tau)}$, $1 \le i \le t$, due to the same cause. □

6 Evaluation of performance

In our scheme, each player U_i $(1 \le i \le n)$ is assigned a secret shadow $s_i^{(1)}$ and an updated parameter δ_i by TAA via a secure channel before the start of the game. The assignment procedure happens once only throughout the game.

During Key-Generation Phase, TAA needs to compute $n(t+1) \approx nt$ modular multiplications in order to obtain $s_i^{(1)}$ and δ_i $(1 \le i \le n)$, and each player U_i needs to compute $(t+1)$ point multiplications to check the soundness of $s_i^{(1)}$ and δ_i come from TAA. The communication cost is about $2n|q|$ bits during the phase. During Shadow-Refreshing Phase, player U_i can refresh his secret shadow easily with modular addition, where the computation cost is ignored while compared with modular multiplication. During Visit Phase, each player U_i needs to compute one point multiplication to obtain $Sign_{il}^{(\tau+1)}$ while visiting the website w_l. In the meanwhile, to verify the fragment-proof $Sign_{il}^{(\tau+1)}$, player U_j needs to compute two point multiplications $\tau \cdot R$ and $(\tau+1) \cdot \sum_{j=1}^{t-1} i^j A_j$ and four modified Weil pairings $\hat{e}(Sign_{il}^{(\tau+1)}, \mathcal{G})$, $\hat{e}(H(w_l), Q_{TA})$, $\hat{e}(H(w_l), \tau R)$ and $\hat{e}(H(w_l), (\tau+1)\sum_{j=1}^{t-1} i^j A_j)$. During Proof-Combination Phase, the website w_l needs to compute t point multiplications and $t-1$ point additions in order to extract the primary proof $Sign_l^{(\tau+1)}$. In addition, he also needs to compute one modified Weil pairing $\hat{e}(Sign_l^{(\tau+1)}, \mathcal{G})$ for verifying the primary proof $Sign_l^{(\tau+1)}$. We summarize the above inferences about performance in Table 1.

7 Discussion and conclusion

We exhibited some advantages of our scheme in the paper. Our scheme is able to prevent two kinds of collusion attacks: **Collusion Attack Type I** and **Collusion Attack Type II**, and is equipped with verifiable secret shadow, shadow-self-refreshing, verifiable fragment-proof and forward security. Up to now, no secure metering scheme with all the above features exists at the same time.

References

[1] W. Diffie and M. Hellman, "New Directions in Cryptography," *IEEE Trans. Information Theory*, Vol. 22, pp. 644-654, 1976.

[2] C. Blundo, A. D. Bonis, B. Masucci and D. R. Stinson, "Dynamic Multi-threshold Metering Schemes," *SAC* 2000, LNCS 2012, pp. 130-144, 2001.

[3] C. Blundo, A. D. Bonis and B. Masucci, "Metering Schemes with Pricing," *DISC* 2000, LNCS 1914, pp. 194-208, 2000.

[4] D. Boneh and M. Franklin, "Identity-Based Encryption From The Weil Pairing," *Proc. Crypto'01,* LNCS 2139, pp. 213-229, Aug. 2001.

[5] M. Bellare and P. Rogaway, "Random Oracles Are Practical: A Paradigm for Designing Efficient Protocols," *Proc. First ACM Computer and Comm. Security,* pp. 62-73, 1993.

[6] M. Bellare and P. Rogaway, "The exact security of digital signature - How to sign with RSA and Rabin," *Proc. Eurocrypt'*96, LNCS 1070, pp. 399-416, 1996.

[7] P. Barreto, H. Y. Kim, B. Lynn, and M. Scott, "Efficient Algorithms for Pairing-Based Cryptosystems," *Proc. Crypto'*02, LNCS 2442, pp. 354-369, Aug. 2002.

[8] W. Mao, *Modern Cryptography -Theory and Practice,* ch13-16, Prentice Hall Company, 2004.

[9] A. Menezes, *Elliptic Curve Public Key Cryptosystems*, Kluwer Academic Publishers, 1995.

[10] B. Masucci and D. R. Stinson, "Efficient Metering Schemes with Pricing," *IEEE Transtions on Information Theory*, vol. 47,No. 7, pp. 2835-2844, 2001.

[11] M. Naor and B. Pinkas, "Secure and Efficient Metering," *Proc. Eurocrypt'*98, LNCS 1403, pp.576-590, 1998.

[12] W. Ogata and K. Kurosawa, "Provably Secure Metering Scheme," *Proc. Asiacrypt* 2000, LNCS 1976, pp. 388-398, 2000.

[13] T. Rabin and M. Ben-Or, "Verifiable Secret Sharing and Multi-party Protocols with Honest Majority," *Proc.* 26th *ACM symp. Theory of Computing*, pp. 73-85, 1989.

[14] M. Rosing, *Implementing Elliptic Curve Cryptography*, Manning Publications Company, 1999.

[15] A. Shamir, "How to Share a Secret," *Comm. ACM*, Vol. 22, pp. 612-613, 1979.

Appendix:

A.1

From $f_\tau(x) = k_{TA} + (\tau - 1)r + \tau \sum_{j=1}^{t-1} a_j x^j \bmod q$, letting $1 \leftarrow \tau$ and $i \leftarrow x$, we have $f_1(i) = k_{TA} + \sum_{j=1}^{t-1} a_j i^j \bmod q$ for $i = 1, 2, ..., n$, i.e., $s_i^{(1)} = k_{TA} + \sum_{j=1}^{t-1} a_j i^j \bmod q$. So it is obvious that $s_i^{(1)}\mathcal{G} = Q_{TA} + \sum_{j=1}^{t-1} i^j A_j$.

A.2

By the definition $\delta_i = r + \sum_{j=1}^{t-1} a_j i^j \bmod q$, multiplying the two sides of the equation with $\mathcal{G}$, (2) may be acquired effortlessly.

A.3

From $f_\tau(x) = k_{TA} + (\tau - 1)r + \tau \sum_{j=1}^{t-1} a_j x^j \bmod q$, setting $1 \leftarrow x$ and $\tau + 1 \leftarrow \tau$, we obtain the relation $s_i^{(\tau+1)} = f_{\tau+1}(i) = k_{TA} + \tau r + (\tau + 1) \sum_{j=1}^{t-1} a_j i^j \bmod q$. According to (4), the signature for $H(w_l)$ by the secret shadow $s_i^{(\tau+1)}$ may be rewritten as follows:

$$\begin{aligned} & Sign_{il}^{(\tau+1)} \\ = \; & s_i^{(\tau+1)} H(w_l) \\ = \; & k_{TA} H(w_l) + \tau r H(w_l) + (\tau + 1) \sum_{j=1}^{t-1} a_j i^j H(w_l). \end{aligned}$$

Substituting the signature into the following modified Weil pairing, we have (5):

$$\begin{aligned} & \hat{e}(Sign_{il}^{(\tau+1)}, \mathcal{G}) \\ = \; & \hat{e}(k_{TA} H(w_l) + \tau r H(w_l) + (\tau + 1) \sum_{j=1}^{t-1} a_j i^j H(w_l), \mathcal{G}) \\ = \; & \hat{e}(k_{TA} H(w_l), \mathcal{G}) \hat{e}(\tau r H(w_l), \mathcal{G}) \hat{e}((\tau + 1) \sum_{j=1}^{t-1} a_j i^j H(w_l), \mathcal{G}) \\ = \; & \hat{e}(H(w_l), Q_{TA}) \hat{e}(H(w_l), \tau R) \hat{e}(H(w_l), (\tau + 1) \sum_{j=1}^{t-1} i^j A_j) \end{aligned}$$

A.4

According to Shamir-SS, while known arbitrary t-pair shadows $(i, f(i))$, $i = 1, 2, ..., t$, the polynomial chosen formerly to generate the n-pair shadows can be recovered as the following.

$$f_{\tau+1}(x) = \sum_{i=1}^{t} \left[f_{\tau+1}(i) \prod_{1 \le j \le t, j \ne i} \frac{x - j}{i - j} \right] \bmod q.$$

Because that the master secret $k_{TA} + \tau r$ regarding the period of time τ is placed in the position of constant coefficient of polynomial. We can extract it by setting $x = 0$ for the above polynomial.

$$k_{TA} + \tau r = f_{\tau+1}(0) = \sum_{i=1}^{t} \left[f_{\tau+1}(i) \prod_{1 \le j \le t, j \ne i} \frac{j}{j - i} \right] \bmod q.$$

For convenience, we define $c_i = \prod_{1 \le j \le t, j \ne i} \frac{j}{j-i}$ and $s_i^{(\tau+1)} = f_{\tau+1}(i)$. Thus, an useful equation will be obtained as follows.

$$f_{\tau+1}(0) = \sum_{i=1}^{t} s_i^{(\tau+1)} c_i \bmod q.$$

The above equation implies that the master secret $f_{\tau+1}(0)$ may be recovered from summing arbitrary t shadows $s_i^{(\tau+1)}$ multiplied by their corresponding constants c_i.

Multiply the two sides of the above equation with $H(w_l)$, we can derive (6):

$$Sign_l^{(\tau+1)} = \sum_{i=1}^{t} \left[Sign_{il}^{(\tau+1)} c_i \right],$$

where $Sign_l^{(\tau+1)} = f_{\tau+1}(0) H(w_l)$ and $Sign_{il}^{(\tau+1)} = s_i^{(\tau+1)} H(w_l)$.

A.5

Since the master secret of TAA is $k_{TA} + \tau r$ during the period of time τ, the signature of $H(w_l)$ signed by the master secret is $Sign^{(\tau+1)} = (k_{TA} + \tau r) H(w_l)$. Substituting $Sign^{(\tau+1)}$ into the modified Weil pairing, we acquire (7):

$$\begin{aligned} \hat{e}(Sign_l^{(\tau+1)}, \mathcal{G}) &= \hat{e}((k_{TA} + \tau r) H(w_l), \mathcal{G}) \\ &= \hat{e}((k_{TA} H(w_l) + \tau r H(w_l)), \mathcal{G}) \\ &= \hat{e}(k_{TA} H(w_l), \mathcal{G}) \hat{e}(\tau r H(w_l), \mathcal{G}) \\ &= \hat{e}(H(w_l), Q_{TA}) \hat{e}(H(w_l), \tau R). \end{aligned}$$