symmetry

MDPI

Article

An Information Theoretically Secure E-Lottery Scheme Based on Symmetric Bivariate Polynomials

Zhe Xia [1], Yining Liu [2,*], Ching-Fang Hsu [3] and Chin-Chen Chang [4]

1 School of Computer Science, Wuhan University of Technology, Wuhan 430070, China; xiazhe@whut.edu.cn
2 School of Computer and Information Security, Guilin University of Electronic Technology, Guilin 541004, China
3 Computer School, Central China Normal University, Wuhan 430079, China; cherryjingfang@gmail.com
4 Department of Information Engineering and Computer Science, Feng Chia University, Taichung 43301, Taiwan; alan3c@gmail.com
* Correspondence: ynliu@guet.edu.cn

Received: 30 November 2018; Accepted: 3 January 2019; Published: 15 January 2019

Abstract: E-lottery schemes have attracted much interest from both industry and academia recently, because they are not only useful to raise funds for charity institutions, but also can be used as the major building blocks to design micro-payment systems. In the literature, a number of e-lottery schemes have been introduced over the last two decades. However, most of these schemes rely on some computational assumptions. In this paper, we introduce a novel e-lottery scheme that achieves information theoretical security. Our proposed scheme is designed using symmetric bivariate polynomials, and it satisfies the required security properties, such as correctness, unpredictability, verifiability, and robustness. Moreover, the winning number is generated in a distributed fashion, so that no trusted third party needs to be involved and the danger of a single point of failure is minimized.

Keywords: e-lottery; symmetric bivariate polynomial; verifiable secret sharing; information theoretical security

1. Introduction

Today, the lottery has grown into a multi-billion dollar industry, and it is very popular in peoples' daily life. In one aspect, it allows the players to bet on a small amount of money and get the chance to win a large fortune, and meanwhile, funds raised by the lottery are indispensable sources for various charity institutions. In another aspect, Rivest has shown in [1] that the lottery can be used as the major building block to design micro-payment systems. Therefore, it has attracted much interest from both industry and academia recently because of its practical importance, as well as theoretical potentials.

In general, a lottery scheme consists of the following participants, as shown in Figure 1: lottery issuers, players, and drawing centers. If a player wants to participate in a lottery game, she/he purchases the lottery tickets from some lottery issuer. Note that the player can purchase as many tickets as she/he likes, and each ticket costs her/him a small amount of money. Depending on the rules, in the lottery ticket, the player chooses either one number within some pre-defined large domain or several numbers in some pre-defined small domain. In this paper, we only consider the first case, since a lottery scheme designed in this case can be easily transformed into one that handles the second case, e.g., running the scheme several times in parallel. Once the ticket purchase phase finishes, the winning number is then generated by the drawing centers. If the player's selected number matches with the winning number, she/he wins, and the lottery ticket that contains the winning number can be used to claim the prize from the lottery issuer.

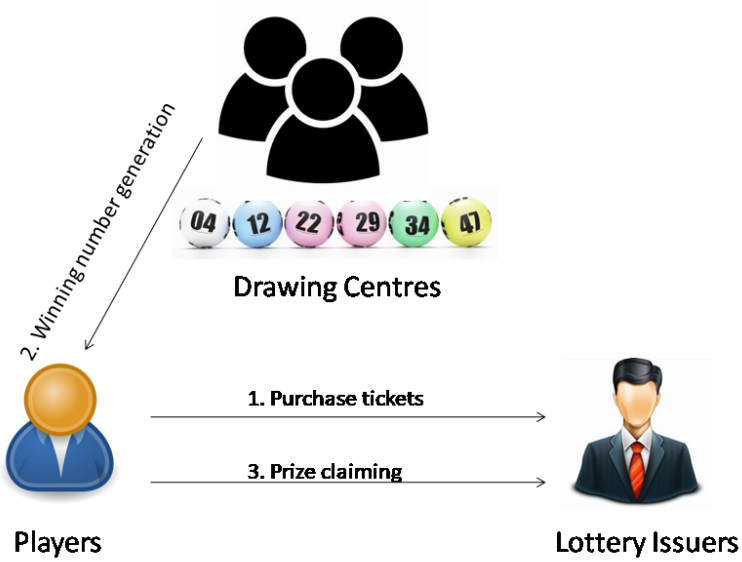

Figure 1. An illustration of the lottery game.

With the rapid development of technologies, designing the lottery systems using information technologies and implementing them over computer networks have become inevitable trends, and these systems are called e-lotteries. Although the e-lottery is helpful to simplify the ticket purchase experience (i.e., with computer-aided user interfaces) and makes the system more accessible by ordinary users (i.e., the tickets can be purchased remotely at the users' most convenient time), it also brings many new security issues compared with the traditional lottery systems. For example, a lottery system should guarantee that the winning number is randomly distributed in the pre-defined large domain, and it is unpredictable before its announcement. Note that these requirements ensure that each ticket will have a fair chance to win the prize. Moreover, the drawing phase should be transparent so that the validity of the winning number can be verified. Because computer networks are publicly accessible and they allow the users to communicate with each other without physical contact, the harmonization of these conflicting security requirements is challenging and needs the dedicated design and proper use of some advanced cryptographic techniques.

1.1. Related Works

The first e-lottery scheme was proposed by Goldschlag et al. [2], in which the winning number is generated using the delay function with the purchased tickets as its inputs. Informally, the delay function is a deterministic function that is not hard to compute, but still requires a significant amount of time to complete the computation. Therefore, the drawing phase can be verified by re-computing the delay function with the same inputs, and the unpredictability of the winning number relies on the fact that the players cannot compute the delay function effectively. To guarantee that the winning number is randomly distributed, the scheme requires an early registration of the players, and this step is later used to ensure that the number of participating players is not too small. Otherwise, the winning number may not contain enough entropy, and its distribution can be biased. However, this scheme has several limitations. Firstly, each player is allowed to purchase only one ticket. Secondly, it is not suitable to be used in some real-world e-lottery systems in which the winning number is generated periodically no matter how many tickets have been purchased. Thirdly, the delay function could be a single point of failure, and it may not be robust over time. A related e-lottery scheme has been introduced by Syverson [3] around the same time using weakly-secret bit commitment (WSBC). Note that WSBC has similar properties as the delay function such that once a secret has been committed, it can be read only after a pre-determined amount of time. In [4], Kushilevitz et al. introduced an

e-lottery scheme in which the delay function is used in the winning number verification rather than the winning number generation. This scheme does not need to employ a trusted third party (TTP), and the correctness of execution can be verified. Moreover, the early registration of players is not required, and each player is allowed to purchase multiple tickets.

The above schemes mainly focus on the generation of the winning number. In [5], Zhou et al. introduced an e-lottery scheme that focuses on fair payment for lottery tickets and prize claim. Moreover, the players' anonymity is considered to enhance the participation rate. The downside is that this scheme needs to employ an off-line TTP. The players and the lottery issuers exchange messages using verifiable encrypted signatures, and an off-line TTP needs to be involved if there is any dispute in the exchange. In this scheme, the delay function is also suggested to be used to prevent the last participating player from biasing the distribution of the winning number. Some other e-lottery schemes based on delay functions can be found in [6–8]. The design and implementation of large-scale lottery systems have been described in [9,10].

In the literature, several e-lottery schemes also have been introduced without using the delay function. In [11], the winning number is generated by aggregating the drawing centers' random values. The scheme relies on the homomorphic property of the Paillier encryption [12], and the winning number is retrieved in the drawing phase using the verifiable threshold decryption. Its benefit is that the winning number is independent of the players' tickets; hence, the e-lottery scheme is more versatile and suits more real-world applications. In [13,14], Lee et al. introduced two e-lottery schemes that further consider the protection of players' privacy and anonymity. This property is achieved using blind signatures. However, some TTP needs to be involved in the drawing phase to generate the winning number. In [15], Liu et al. extended Lee's schemes in two aspects. First, players' privacy is protected using an efficient oblivious transfer rather than blind signatures. Second, the drawing phase is carried out by a number of drawing centers in a distributed fashion using Lagrange interpolation of polynomials. Each drawing center can verify that her/his input has contributed to the winning number by checking whether her/his point satisfies the resulting polynomial. The benefit is that neither the delay function nor any TTP is required in the drawing phase.

1.2. Our Contributions

To the best of our knowledge, most of the existing e-lottery schemes rely on some computational assumptions. In other words, if the adversary has infinite computational power, the security properties in these existing schemes will be violated. In this paper, we introduce a novel e-lottery scheme that achieves information theoretical security. Our proposed scheme is designed using symmetric bivariate polynomials, and its security properties, such as correctness, unpredictability, verifiability, and robustness, can be guaranteed against the adversary who has unlimited resources. Moreover, the winning number is generated in a distributed fashion so that neither TTP nor the delay function needs to be involved; hence, the danger of a single point of failure is minimized. Note that our suggested method also can be used to improve some existing e-lottery schemes. For example, when it is used to generate the winning number in Lee's schemes [13,14], the TTP can be removed in the drawing phase.

1.3. Organization of the Paper

The rest of the paper is organized as follows: In Section 2, we outline some preliminaries. The models and definitions of e-lottery schemes are described in Section 3. In Section 4, we introduce our proposed e-lottery scheme, and its security and efficiency analyses are presented in Section 5. Finally, we conclude in Section 6.

2. Preliminaries

Symmetric bivariate polynomials have been widely used in the research of information technologies [16–20]. In this section, we describe the symmetric bivariate polynomial, as well as its properties that will be used in our proposed e-lottery scheme. Denote p as some large prime,

and all the computations are modulo p unless otherwise stated. The dealer $\mathcal{D}$ first chooses a random symmetric bivariate polynomial $f(x,y)$ over $\mathbb{Z}_p$ with degree at most $t-1$ in both x and y as:

$$f(x,y) = a_{0,0} + a_{1,0}x + a_{0,1}y + a_{1,1}xy + \cdots + a_{t-1,t-1}x^{t-1}y^{t-1}$$

such that $a_{i,j} = a_{j,i}$ for all $i,j \in \{0,1,\ldots,t-1\}$. Moreover, denote $\{\mathcal{P}_1,\mathcal{P}_2,\ldots,\mathcal{P}_n\}$ as a set of players and $\{w_1,w_2,\ldots,w_n\}$ as the public parameters associate with these players. $\mathcal{D}$ computes the shares $h_i(x) = f(x,w_i)$ for $i = 1,2,\ldots,n$ and sends them to the players through the secure channel. Note that each share $h_i(x)$ is a univariate polynomial with degree at most $t-1$ in x.

Pairwise key establishment: The players can use their shares to establish pairwise secret keys among them without interaction [21]. For example, the i^{th} player $\mathcal{P}_i$ and the j^{th} player $\mathcal{P}_j$ can establish a secret key between them as $k_{i,j} = h_i(w_j) = h_j(w_i) = k_{j,i}$. This is because in the symmetric bivariate polynomial $f(x,y)$, we always have $f(w_i,w_j) = f(w_j,w_i)$. Note that in [22,23], Stinson et al. also used this property to authenticate whether the shares $h_i(x)$ have been generated consistently.

Secret recovery: If t or more than t of these players work together and all these players are honest, they can recover the value $a_{0,0} = f(0,0)$ using their shares $h_i(x)$ through Lagrange interpolation. Without loss of generality, we assume that the players $\{\mathcal{P}_1,\mathcal{P}_2,\ldots,\mathcal{P}_t\}$ are involved. The value $a_{0,0}$ can be recovered as $a_{0,0} = \sum_{i=1}^{t} h_i(0)\cdot\mathcal{L}_i$, where $\mathcal{L}_i = \prod_{j=1,j\neq i}^{t} \frac{w_j}{w_j - w_i}$ is the Lagrange coefficient. Here, each $h_i(0)$ is a value within $\mathbb{Z}_p$.

Robust secret recovery: Even if some players are dishonest, the value $a_{0,0}$ still can be correctly recovered under some conditions [24]. The basic idea is as follows: suppose n players are all involved and that they reveal the values $h_i(0)$ for $i = 1,2,\ldots,n$, but some dishonest players might reveal incorrect $h_i(0)$ values. Now, every set containing t of the $h_i(0)$ values can be interpolated into a possible value of $a_{0,0}$, and there are in total $\binom{n}{t} = \frac{n!}{t!(n-t)!}$ number of such sets. If a particular value of $a_{0,0}$ appears in more than half of these sets, it can be treated as the correct value without ambiguity. The remaining issue is how many dishonest players can be tolerated in this method, and we denote this number as b. Obviously, $b < t$ must hold. Otherwise, these dishonest players can recover $a_{0,0}$ by themselves. Moreover, any two different univariate polynomials with degree $t-1$ agree on at most $t-1$ points. Recall that there are n players and that each player can generate one point; these two polynomials must differ at least $n-t+1$ points. By information theory, the error correction codes have the ability to correct less than $\frac{n-t+1}{2}$ errors. Hence, we have $\frac{n-t+1}{2} > b$, which further implies that $b < n/3$. Under this condition, either the Euclidean decoder or the Berlekamp–Massey decoder can be used to recover the value $a_{0,0}$ efficiently.

Homomorphic property in secret sharing: Note that the values $h_i(0)$ for $i = 1,2,\ldots,n$ can be considered as the shares of the secret $a_{0,0}$ using Shamir secret sharing [25]. In [26], Benaloh discovered the homomorphic property in secret sharing schemes. Denote $(s_1,s_2,\ldots,s_n)$ as a set of shares encoding the secret s and $(s'_1,s'_2,\ldots,s'_n)$ as another set of shares encoding the secret s'. Moreover, $\oplus$ and $\otimes$ are denoted as the operation of shares and operation of the secret, respectively. Then, the set $(s_1 \oplus s'_1, s_2 \oplus s'_2, \ldots, s_n \oplus s'_n)$ encodes the secret $s \otimes s'$. Obviously, Shamir secret sharing enjoys the $(+,+)$ homomorphic property.

3. Models and Definitions

Participants: There are four types of participants in an e-lottery system:

- Lottery issuers: They sell tickets to the players and provide the prize to the winner. We assume that the lottery issuers are honest.
- Players: They buy tickets and hope to win a large fortune.

- Drawing centers: They follow the public procedure to generate the winning number.
- Adversary: The adversary $\mathcal{A}$ is assumed to have unlimited computational resources, and $\mathcal{A}$ can control at most b of the drawing centers. Controlling a drawing center means learning its internal states, modifying its messages, disconnecting it, changing its intended behavior, and so on.

Communication model: We assume that the drawing centers are connected by pairwise secure channels, so that the messages exchanged among them cannot be intercepted or modified by the adversary $\mathcal{A}$. We also assume that there exists a common authenticated broadcast channel that is accessible by every participant. Moreover, we assume that the system is synchronized. Each drawing center can access a common global clock, and it can access some local source of randomness.

System model: An e-lottery scheme consists of the following three phases:

- Purchasing phase: The players can only purchase the tickets in this phase. To purchase a ticket, the player chooses a number in a pre-defined large domain and bets a small amount of money on it. Note that each player can purchase as many tickets as she/he likes. The purchased tickets are physically signed by these lottery issuers, so that they cannot be counterfeited by the players.
- Drawing phase: This phase begins after the purchasing phase. The drawing centers generate the winning number in a distributed fashion. The winning number is required to be randomly distributed in the pre-defined large domain, and it is unpredictable before its announcement. Moreover, this phase should be transparent so that the generation of the winning number can be verified.
- Claiming phase: Once the winning number is announced, the player who has selected the wining number can use her/his ticket to claim the prize from the lottery issuers.

Security properties: The following security properties are advocated in the majority of e-lottery schemes:

- Correctness: The proposed scheme will output the winning number that is randomly distributed in the pre-defined domain in the drawing phase.
- Unpredictability: The adversary cannot predict the winning number before it is announced. Note that the correctness property together with the unpredictability property guarantee that each player will have a fair chance to win the prize.
- Verifiability: It can be verified that the winning number is generated according to the public procedure.
- Robustness: The winning number is generated in a distributed fashion, so that neither TTP nor the delay function needs to be employed.

4. An E-Lottery Scheme with Information Theoretical Security

In this section, we describe our proposed e-lottery scheme with information theoretical security. Its design is inspired by the unconditionally-secure, verifiable secret sharing [22] and privacy preserving data aggregation [27,28], and we have incorporated the techniques in [29] to improve its round complexity.

4.1. The Proposed Scheme

Suppose n drawing centers $\{\mathcal{P}_1, \mathcal{P}_2, \ldots, \mathcal{P}_n\}$ are involved in generating the winning number in the drawing phase, and $\{w_1, w_2, \ldots, w_n\}$ are the public parameters associate with these drawing centers, respectively. The static adversary $\mathcal{A}$ can control at most b of these drawing centers, where $b < t$ and $n \geq t + 3b$. The word "static" means that $\mathcal{A}$ chooses the corruption drawing centers at the beginning of the scheme. Moreover, p is denoted as some large prime, and all the computations are assumed to be modulo p unless otherwise stated. The winning number is generated as follows:

1. Each drawing center $\mathcal{P}_k$ chooses a random symmetric bivariate polynomial with degree at most $t-1$ in both x and y:
$$f^{(k)}(x,y) = \sum_{i=0}^{t-1}\sum_{j=0}^{t-1} a_{i,j}^{(k)} x^i y^j$$
where $a_{i,j}^{(k)} = a_{j,i}^{(k)}$ for all $i,j \in \{0,1,\ldots,t-1\}$. Then, $\mathcal{P}_k$ computes $h_m^{(k)}(x) = f^{(k)}(x,w_m)$ and sends it to every other drawing center $\mathcal{P}_m$ through the pairwise secure channel. Note that each $h_m^{(k)}(x)$ is a univariate polynomial with degree at most $t-1$ in x. At the same time, each $\mathcal{P}_i$ sends to every $\mathcal{P}_j$ a random value $r_{i,j}^{(k)} \in \mathbb{Z}_p$ through the pairwise secure channel for $i,j \in \{1,2,\ldots,n\}$.
2. After receiving $h_m^{(k)}(x)$ from $\mathcal{P}_k$ and $r_{1,m}^{(k)}, r_{2,m}^{(k)}, \ldots, r_{n,m}^{(k)}$ from the other drawing centers, each $\mathcal{P}_m$ computes the value $c_{m,l} = h_m^{(k)}(w_l) + r_{m,l}^{(k)} + r_{l,m}^{(k)}$ for every $l \neq m$ and broadcasts these $c_{m,l}^{(k)}$ values.
3. Each $\mathcal{P}_m$ computes the maximum subset $\mathcal{G}_k \subseteq \{1,2,\ldots,n\}$ such that any ordered pair $(i,j) \in \mathcal{G}_k \times \mathcal{G}_k$ satisfies the equation $c_{i,j}^{(k)} = c_{j,i}^{(k)}$. If $|\mathcal{G}_k| \geq n-b$, then $\mathcal{P}_m$ broadcasts a bit $v^{(k)} = \texttt{SUCC}$ and puts the value k in a list $\mathcal{L}$. Otherwise, $\mathcal{P}_m$ simply broadcasts $v^{(k)} = \texttt{FAIL}$.
4. If $|\mathcal{L}| \geq n-b$, then each $\mathcal{P}_m$ broadcasts a bit $u = \texttt{SUCC}$ and computes her/his aggregated share as:
$$h_m(x) = \sum_{k\in\mathcal{L}} h_m^{(k)}(x)$$
Otherwise, $\mathcal{P}_m$ simply broadcasts $u = \texttt{FAIL}$ and stops.
5. If $u = \texttt{SUCC}$, each $\mathcal{P}_m$ computes $h_m(0)$ and sends it to the other drawing centers in $\mathcal{L}$ through the pairwise secure channels.
6. Finally, after receiving the $h_i(0)$ values from the other drawing centers in $\mathcal{L}$, each $\mathcal{P}_m$ computes the winning number $s = \sum_{k\in\mathcal{L}} a_{0,0}^{(k)}$ for at least $n-2b$ of the values she/he has received. Note that this operation can be computed efficiently using the error-correction codes.

4.2. Some Discussions

In order to simplify the above description, we have assumed in Step 1 that every drawing center can access some local source of randomness, and they can choose the random symmetric bivariate polynomial, as well as the random values in $\mathbb{Z}_p$. However, in some real-world environments, this assumption is too strong, and it will restrict the applications of the proposed e-lottery scheme. Here, we discuss how the leftover hash lemma [30] can be used to weaken this assumption.

Definition 1 (Universal hash function)**.** *For a keyed hash function* H *defined over* $(\mathsf{K},\mathsf{M},\mathsf{T})$*, where* K *is its key space,* M *is its message space, and* T *is its digest space, given an adversary* $\mathcal{A}$*, the attack game works as follows: the challenger first randomly selects a key* $k \in \mathsf{K}$ *and keeps* k *private and then* $\mathcal{A}$ *outputs two distinct messages* $m_0, m_1 \in \mathsf{M}$*. We say that* $\mathcal{A}$ *wins the game if* $\mathsf{H}_k(m_0) = \mathsf{H}_k(m_1)$*.* $\mathcal{A}$*'s advantage of winning the above game is denoted as* $\mathsf{Adv}_{\mathcal{A},\mathsf{H}}^{\mathsf{UHF}}$*. We say that* H *is an* ϵ*-bounded universal hash function (or* ϵ*-*UHF*), if* $\mathsf{Adv}_{\mathcal{A},\mathsf{H}}^{\mathsf{UHF}} \leq \epsilon$ *for all adversaries* $\mathcal{A}$ *(even inefficient ones).*

Lemma 1 (Leftover hash lemma)**.** *Let* H *be a* $(1+\alpha)/N$*-*UNF *defined over* $(\mathsf{K},\mathsf{M},\mathsf{T})$*, where* $N = |\mathsf{T}|$*. Let* $k, s_1, s_2, \ldots, s_m$ *be mutually independent random variables, where* k *is randomly distributed in* K*, and each* s_i *can be guessed with probability at most* γ*. Let* δ *be the statistical difference between* $(k, \mathsf{H}_k(s_1), \mathsf{H}_k(s_2), \ldots, \mathsf{H}_k(s_m))$ *and the uniform distribution on* $\mathsf{K} \times \mathsf{T}^m$*. Then, we have:*
$$\delta \leq \frac{1}{2} m \sqrt{N\gamma + \alpha}$$

To see how the leftover hash lemma can be used to weaken the above assumption, suppose $m = 1$ and the value s cannot be guessed with probability at most γ. Then, the leftover hash lemma says that

given whatever side information $\mathsf{I}(s)$ about s, for any adversary $\mathcal{A}$ (even with unlimited computational resources), the advantage in distinguishing $(k, \mathsf{I}(s), \mathsf{H}_k(s))$ from $(k, \mathsf{I}(s), t)$, where t is a truly-random element of T, is bounded by $\delta \leq \sqrt{N\gamma + \alpha}/2$. In other words, if γ are sufficiently small, the output of H will be indistinguishable from a truly random value. Therefore, when using the leftover hash lemma, we only need to assume that the drawing centers are able to generate some values that cannot be guessed with some small probability (e.g., passwords with enough entropy), but there is no need to assume that these values are randomly distributed in some pre-defined domain. In the following section, we still assume that every drawing center can access some local source of randomness in order to simplify the security analysis.

5. Security and Efficiency Analysis

In this section, we analyze the proposed e-lottery scheme and compare it with some existing schemes with respect to the security properties. Moreover, we analyze the computation and communication costs of generating the winning number in our proposed scheme.

5.1. Security Analysis

Theorem 1 (Correctness). *If $n \geq t + 3b$ and $b < t$, the proposed e-lottery scheme will output a winning number that is randomly distributed in $\mathbb{Z}_p$.*

Proof. Firstly, suppose the drawing center $\mathcal{P}_k$ is good in Step 1. In this case, $\mathcal{P}_k$ will randomly select a symmetric bivariate polynomial $f^{(k)}(x, y)$ over $\mathbb{Z}_p$ with degree at most $t-1$, and every other drawing center $\mathcal{P}_i$ will receive a univariate polynomial $h_i^{(k)}(x) = f^{(k)}(x, w_i)$ from $\mathcal{P}_k$. Because $f^{(k)}(x, y)$ is symmetric, we have $h_m^{(k)}(w_l) = h_l^{(k)}(w_m)$ for all good drawing centers $\mathcal{P}_m$ and $\mathcal{P}_l$. This further implies that the broadcast values $c_{m,l} = h_m^{(k)}(w_l) + r_{m,l}^{(k)} + r_{l,m}^{(k)}$ and $c_{l,m} = h_l^{(k)}(w_m) + r_{l,m}^{(k)} + r_{m,l}^{(k)}$ will match in Step 2. Hence, the good drawing centers $\mathcal{P}_m$ and $\mathcal{P}_l$ will be in the subset $\mathcal{G}_k$. Therefore, $v^{(k)} = \texttt{SUCC}$ for all good drawing centers in Step 3, and k will be included in the list $\mathcal{L}$. Otherwise, if a good drawing center $\mathcal{P}_i$ outputs $v^{(k)} = \texttt{FAIL}$, then the size of the maximum subset $\mathcal{G}_k$ is at most $n - b - 1$. Thus, every good drawing center outputs $v^{(k)} = \texttt{FAIL}$. In this case, k will not be included in the list $\mathcal{L}$.

Next, suppose there are T univariate polynomials $h_1^{(k)}(x), h_2^{(k)}(x), \ldots, h_T^{(k)}(x)$ with degree at most $t-1$, where $T > t$, and these polynomials are consistent, i.e., $h_i^{(k)}(w_j) = h_j^{(k)}(w_i)$ for all $i, j \in \{1, 2, \ldots, T\}$. Then, there exists a univariate polynomial $h^{(k)}(x)$ with degree at most $t-1$ such that $h^{(k)}(w_i) = h_i^{(k)}(0)$ for all $i \in \{1, 2, \ldots, T\}$, and any t of the values $h_i^{(k)}(0)$ can determine the value $h^{(k)}(0) = a_{0,0}^{(k)}$ without ambiguity. To see this, suppose $\mathcal{I}$ and $\mathcal{J}$ are two different t-subsets of $\{1, 2, \ldots, T\}$. The univariate polynomial $h_{\mathcal{I}}^{(k)}(x)$ can be computed such that $h_{\mathcal{I}}^{(k)}(w_i) = h_i^{(k)}(0)$ for all $i \in \mathcal{I}$. In particular, $h_{\mathcal{I}}^{(k)}(0)$ can be computed using the Lagrange interpolation as $h_{\mathcal{I}}^{(k)}(0) = \sum_{i \in \mathcal{I}} h_i^{(k)}(0) \cdot \mathcal{L}_i$, where $\mathcal{L}_i$ is the Lagrange coefficient. Note that similar properties also hold for the set $\mathcal{J}$. Moreover, the equation $h_{\mathcal{I}}^{(k)}(0) = h_{\mathcal{J}}^{(k)}(0)$ always holds because:

$$\begin{aligned}
h_{\mathcal{I}}^{(k)}(0) &= \sum_{i \in \mathcal{I}} h_i^{(k)}(0) \cdot \mathcal{L}_i \\
&= \sum_{i \in \mathcal{I}} \Big(\sum_{j \in \mathcal{J}} h_i^{(k)}(w_j) \cdot \mathcal{L}_j \Big) \cdot \mathcal{L}_i \\
&= \sum_{j \in \mathcal{J}} \Big(\sum_{i \in \mathcal{I}} h_j^{(k)}(w_i) \cdot \mathcal{L}_i \Big) \cdot \mathcal{L}_j \\
&= \sum_{j \in \mathcal{J}} h_j^{(k)}(0) \cdot \mathcal{L}_j \\
&= h_{\mathcal{J}}^{(k)}(0)
\end{aligned}$$

Furthermore, suppose at least $n-b$ drawing centers output $v^{(k)} = \texttt{SUCC}$. Then, we have $|\mathcal{G}_k| > n-b$. Because it is assumed that there are at most b bad drawing centers, there must exist more than $n-2b$ good ones in $\mathcal{G}_k$, and these good drawing centers $\mathcal{P}_i$ have consistent shares $h_i^{(k)}(x)$. Using the error correction codes, $h^{(k)}(0) = a_{0,0}^{(k)}$ can always be efficiently recovered by interpolating the $h_i^{(k)}(0)$ values. Similarly, thanks to the homomorphic property of secret sharing schemes, the interpolation of the values $h_i(0)$ (where $h_i(x) = \sum_{k\in\mathcal{L}} h_i^{(k)}(x)$ is the aggregated share) using the error correction codes can recover the winning number $s = \sum_{k\in\mathcal{L}} h^{(k)}(0) = \sum_{k\in\mathcal{L}} a_{0,0}^{(k)}$. If there exists at least one good drawing center in $\mathcal{L}$, the winning number s will be randomly distributed in $\mathbb{Z}_p$. In summary, based on the assumption that $b < n/4$, our proposed scheme satisfies the correctness property. □

Theorem 2 (Unpredictability). *If $b < t$, the adversary $\mathcal{A}$ controlling at most b of the drawing centers cannot guess the winning number with probability better than $1/p$ before it is announced in the drawing phase.*

Proof. We first assume that the symmetric bivariate polynomial $f(x,y) = \sum_{i=0}^{t-1}\sum_{j=0}^{t-1} a_{i,j}x^i y^j$ over $\mathbb{Z}_p$ is generated by a trusted dealer $\mathcal{D}$, and each drawing center $\mathcal{P}_i$ for $i = 1, 2, \ldots, n$ receives the univariate polynomial $h_i(x) = f(x, w_i)$. We show that the adversary $\mathcal{A}$ who controls at most $t-1$ drawing centers cannot recover the polynomial $f(x,y)$ because its threshold is t. To see this, $f(x,y)$ has t^2 coefficients, and since $a_{i,j} = a_{j,i}$ for all $i, j \in \{1, 2, \ldots, n\}$, $f(x,y)$ has $t^2/2$ different coefficients. Each drawing center $\mathcal{P}_i$ can evaluate her/his univariate polynomial $h_i(x)$ at t independent points. Therefore, $\mathcal{P}_1$ can obtain t independent equations. Although $\mathcal{P}_2$ also can obtain t equations, one of the equations is the same as $\mathcal{P}_1$'s equations; hence, $\mathcal{P}_2$ can obtain $t-1$ independent equations. Similarly, $\mathcal{P}_3$ can obtain $t-2$ independent equations, and so on. To solve the system of equations with $t^2/2$ unknowns, $t^2/2$ independent equations are needed. t shareholders can obtain $(t+1)t/2$ equations, which is enough, but $t-1$ shareholders can obtain $t(t-1)/2$ equations, which is not enough. Moreover, we show that $\mathcal{A}$ cannot predict the value $a_{0,0}$ with probability better than $1/p$. Note that each pair of drawing centers $\mathcal{P}_i$ and $\mathcal{P}_j$ can establish a pairwise key without interaction as $k_{i,j} = h_i(w_j) = h_j(w_i) = k_{j,i}$. Denote H as a $n \times t$ Vandermonde matrix that is publicly known and D as a $t \times t$ private matrix representing the coefficients of $f(x,y)$, and K is a $n \times n$ matrix representing the pairwise keys:

$$\mathsf{H} = \begin{bmatrix} 1 & w_1 & w_1^2 & \ldots & w_1^{t-1} \\ 1 & w_2 & w_2^2 & \ldots & w_2^{t-1} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 1 & w_n & w_n^2 & \ldots & w_n^{t-1} \end{bmatrix} \quad \mathsf{D} = \begin{bmatrix} a_{0,0} & a_{1,0} & \ldots & a_{t-1,0} \\ a_{0,1} & a_{1,1} & \ldots & a_{t-1,1} \\ \ldots & \ldots & \ldots & \ldots \\ a_{0,t-1} & a_{1,t-1} & \ldots & a_{t-1,t-1} \end{bmatrix}$$

$$\mathsf{K} = \begin{bmatrix} k_{1,1} & k_{1,2} & \ldots & k_{1,n} \\ k_{2,1} & k_{2,2} & \ldots & k_{2,n} \\ \ldots & \ldots & \ldots & \ldots \\ k_{n,1} & k_{n,2} & \ldots & k_{n,n} \end{bmatrix}$$

We have $\mathsf{K} = \mathsf{H} \cdot (\mathsf{H} \cdot \mathsf{D})^T$, and $\mathcal{P}_i$'s univariate polynomial $h_i(x)$ is the i^{th} column in the matrix $(\mathsf{H} \cdot \mathsf{D})^T$. Without loss of generality, we assume that $\mathcal{A}$ controls the drawing centers $\{\mathcal{P}_1, \mathcal{P}_2, \ldots, \mathcal{P}_{t-1}\}$. Hence, $\mathcal{A}$ learns the first $t-1$ rows, as well as the first $t-1$ columns of K, because K is symmetric. However, $\mathcal{A}$ cannot learn the value $k_{t,t}$. For every possible value $k_{t,t} \in \mathbb{Z}_p$, not only the entire matrix K can be determined since the rank of K is t, but also one can use the relationship $\mathsf{D} = \mathsf{H}^{-1} \cdot (\mathsf{H}^{-1} \cdot \mathsf{K})^T$ to construct a symmetric bivariate polynomial $f'(x,y) = \sum_{i=0}^{t-1}\sum_{j=0}^{t-1} b_{i,j}x^i y^j$, such that $b_{i,j} = b_{j,i}$ for all $i, j \in \{0, 1, \ldots, t-1\}$ and $f'(x, w_k) = h_k(x)$ for $k = 1, 2, \ldots, t-1$. Moreover, each different value $k_{t,t}$ maps to a unique value $b_{0,0}$. Therefore, this proves that if $\mathcal{D}$ is honest, $\mathcal{A}$ cannot guess the value $a_{0,0}$ with probability better than $1/p$.

In our proposed e-lottery scheme, each drawing center serves as the dealer to execute the above dealing phase once, and all these dealing phases are executed independently. Hence, if the

drawing center $\mathcal{P}_k$ is good, $\mathcal{A}$ cannot guess the value $a_{0,0}^{(k)}$ with probability better than $1/p$. Moreover, the winning number is $s = \sum_{k\in\mathcal{L}} a_{0,0}^{(k)}$, where $\mathcal{L}$ contains more than $n-2b$ good drawing centers. Therefore, $\mathcal{A}$ cannot guess the winning number s with probability better than $1/p$, and this finishes the proof for the unpredictable property. □

Theorem 3 (Verifiability). *In the proposed e-lottery scheme, it can be verified that the winning number is generated according to the public procedure.*

Proof. In the proposed e-lottery scheme, each drawing center first serves as the dealer to share a symmetric bivariate polynomial among all drawing centers, and then, these drawing centers work together to recover the wining number through polynomial interpolation. In the first phase, the drawing centers can verify whether their received univariate polynomials are consistent by checking whether the broadcast values $c_{i,j} = c_{j,i}$ for all $i, j \in \{1, 2, \ldots, n\}$. The following two properties are employed in this process: (1) if the dealer follows the protocol, all good drawing centers will output the bit `SUCC`; (2) if one good drawing center outputs the bit `FAIL`, all good drawing centers will output the same bit, and the dealer has violated the protocol. In the second phase, given that there are more than $n-b$ drawing centers in $\mathcal{L}$, the winning number always can be efficiently recovered using the error correction codes. This is because more than $2/3$ of the drawing centers in $\mathcal{L}$ are good. Moreover, once the winning number is recovered, the bad drawing centers in $\mathcal{L}$ can be identified, i.e., the winning number can be interpolated by the set that only contains good drawing centers, but it cannot be interpolated by the set that contains some bad ones. Therefore, it can be verified that the winning number is generated according to the public procedure. □

Theorem 4 (Robustness). *The proposed e-lottery scheme employs neither TTP nor the delay function, and the winning number is generated in a distributed fashion.*

Proof. The proof is obvious. Note that because neither TTP nor the delay function has been used in the proposed e-lottery scheme, the danger of a single point of failure is minimized. □

5.2. Comparison with Some Existing Works

Table 1 summarizes the comparison of our proposed e-lottery scheme with some existing schemes in the literature regarding the security properties (the abbreviation "IT security" stands for information theoretical security). To the best of our knowledge, our proposed scheme is the first e-lottery scheme that achieves information theoretical security.

Table 1. Comparison with some existing works IT, information theoretical.

	Correctness	**Unpredictability**	**Verifiability**	**Robustness**	**IT Security**
Goldschlag's scheme [2]	Yes	Yes	Yes	No	No
Kushilevitz's scheme [4]	Yes	Yes	Yes	No	No
Fouque's scheme [11]	Yes	Yes	Yes	Yes	No
Zhou's scheme [5]	Yes	Yes	Yes	No	No
Lee's scheme [13]	Yes	Yes	No	No	No
Liu's scheme [15]	Yes	Yes	Yes	Yes	No
Our proposed scheme	Yes	Yes	Yes	Yes	Yes

5.3. Efficiency Analysis

In Step 1, each drawing center $\mathcal{P}_k$ serves as the dealer to select a random symmetric bivariate polynomial $f^{(k)}(x,y) = \sum_{i=0}^{t-1}\sum_{j=0}^{t-1} a_{i,j}^{(k)} x^i y^j$ over $\mathbb{Z}_p$. There are in total t^2 coefficients in $f^{(k)}(x,y)$, but since $a_{i,j}^{(k)} = a_{j,i}^{(k)}$ for all $i, j \in \{0, 1, \ldots, t-1\}$, only $t^2/2$ coefficients need to be selected in $\mathbb{Z}_p$. Furthermore, $\mathcal{P}_k$ needs to evaluate $f^{(k)}(x, w_l)$, where $l \in \{1, 2, \ldots, n\}\backslash k$. The evaluation needs to

perform $n-1$ times, and each evaluation requires t multiplications and t^2 additions using Horner's algorithm. Therefore, the total computational cost in this step is $t(n-1)$ multiplications and $t^2(n-1)$ additions in $\mathbb{Z}_p$. Moreover, $\mathcal{P}_k$ sends the univariate polynomial $h_l^{(k)}(x) = f^{(k)}(x, w_l)$ over $\mathbb{Z}_p$ to each other drawing center. The communication cost in this step is $(n-1)t \cdot |p|$ bits. In Step 2, each drawing center $\mathcal{P}_k$ has n univariate polynomials over $\mathbb{Z}_p$ (one generated by herself/himself and $n-1$ received from the other drawing centers). For each of these univariate polynomial, $\mathcal{P}_k$ evaluates it $n-1$ times. Using Horner's algorithm, each evaluation takes t multiplications and t additions. Therefore, the total computational cost in this step is $(n^2-n)t$ multiplications and $(n^2-n)t$ additions in $\mathbb{Z}_p$. Moreover, each drawing center $\mathcal{P}_k$ broadcasts n^2-n values in $\mathbb{Z}_p$. Hence, the communication cost in this step is $(n^2-n) \cdot |p|$ bits. In Step 3, each drawing center $\mathcal{P}_k$ compares $(n^2-n)/2$ pairs of values in $\mathbb{Z}_p$ and broadcasts n bits. In Step 4, each $\mathcal{P}_k$ performs at most tn additions in $\mathbb{Z}_p$ and broadcasts 1 bit. In Step 5, each $\mathcal{P}_k$ sends a value in $\mathbb{Z}_p$ to all other drawing centers. The communication cost in this step is $(n-1) \cdot |p|$ bits. In Step 6, each $\mathcal{P}_k$ recovers the winning number using the error correction codes.

Our proposed e-lottery scheme is very efficient for use in real-world applications because of the following two reasons. Firstly, in our scheme, the modular p can be set as 128 bits or 256 bits; while in many existing works that use public key cryptosystems, this modular needs to be set as several thousand bits in order to achieve the same security level. Secondly, most of the computations in our scheme are modular multiplications and modular additions, and they are much more efficient compared with the modular exponentiations that are required in many existing works. To illustrate this, suppose the security level is set as 128 bits in some application. In other words, the adversary with unlimited computational resources cannot predict the winning number with probability better than $1/2^{128}$. Moreover, suppose $n = 9$ and $t = 3$ so that $t - 1 < n/4$ is satisfied. Using these system parameters, in Step 1, the computational cost for each drawing center is 24 multiplications and 72 additions in $\mathbb{Z}_p$, where the modular p is a 128-bit prime, and the communication cost is 3072 bits. In Step 2, each drawing center needs to compute 216 multiplications and additions in $\mathbb{Z}_p$, and she/he needs to sends 9216 bits to the other drawing centers. In Step 3, each drawing center needs to compare 36 pairs of values in $\mathbb{Z}_p$ and broadcasts nine bits. In Step 4, each drawing center performs 27 additions in $\mathbb{Z}_p$ and broadcasts 1 bit. In Step 5, the communication cost is 1024 bit. To achieve the same security level, Liu's scheme [15] needs to use a subgroup with order q, where q is a 256-bit prime, and the modular p' needs to be set as a 3072-bit prime according to the NIST recommendations. Each drawing center needs to perform nine full modular exponentiations in $\mathbb{Z}_{p'}$. Using the square-and-multiply algorithm, these modular exponentiations cost roughly 3456 multiplications in $\mathbb{Z}_{p'}$. Recall that p' is much larger than p; our proposed method therefore has computational advantages over Liu's scheme. Regarding the communication complexity, in Liu's scheme, each drawing center needs to broadcast a 3072-bit value and sends 2048-bit values to the other drawing centers. Although our proposed scheme is less efficient in communication costs, it is still acceptable for real-world applications. Moreover, our proposed scheme does not rely on any computational assumption, and this is a property that is not enjoyed in Liu's scheme.

We have to note that the degree t of the polynomial will affect both the security and efficiency of our proposed scheme. In one aspect, the degree of the polynomial defines the maximum allowed drawing centers controlled by the adversary. Hence, the polynomial with a higher degree can be used to design a scheme with better security. In another aspect, the polynomial with a higher degree will increase the computational costs of the proposed scheme. Therefore, this parameter needs to be selected carefully based on specific requirements.

6. Conclusions

In this paper, we have introduced an e-lottery scheme with the desirable security properties. In particular, the winning number is generated by a number of drawing centers in a distributed fashion, and this procedure can be verified. Before the winning number is announced, it cannot be guessed with a probability better than a pre-defined small value. These properties ensure that the scheme is

transparent and every player will have a fair chance to win the prize. Moreover, these properties are guaranteed without relying on computational assumptions. To the best of our knowledge, our scheme is the first e-lottery scheme that satisfies information theoretical security.

Author Contributions: Conceptualization: Z.X. and Y.l.; methodology: Z.X. and Y.L.; formal analysis: Z.X. and C.-F.H.; writing–original draft preparation: Z.X., Y.L., C.-F.H.; writing–review and editing: Z.X. and C.-C.C.; supervision: C.-C.C.; funding acquisition: Y.L.

Funding: This work was partially supported by the National Natural Science Foundation of China (Grant No. 61662016, 61772224), the Natural Science Foundation of Hubei Province (Grant No. 2017CFB303), and the Key Projects of Guangxi Natural Science Foundation (Grant No. 2018JJD170004).

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Rivest, R.L. Electronic lottery tickets as micropayments. In *Lecture Notes in Computer Science, Proceedings of the International Conference on Financial Cryptography, Anguilla, Anguilla, 24–28 February 1997*; Springer: Berlin, Germany, 1997; pp. 307–314.
2. Goldschlag, D.M.; Stubblebine, S.G. Publicly verifiable lotteries: Applications of delaying functions. In *Lecture Notes in Computer Science, Proceedings of the International Conference on Financial Cryptography, Anguilla, Anguilla, 23–25 February 1998*; Springer: Berlin, Germany, 1998; pp. 214–226.
3. Syverson, P. *Weakly Secret Bit Commitment: Applications to Lotteries and Fair Exchange*; Technical Report, NAVAL Research Lab Washington DC Center for High Assurance Computing Systems (CHACS); NAVAL Research Lab: Washington, DC, USA, 1998.
4. Kushilevitz, E.; Rabin, T. Fair e-lotteries and e-casinos. In *Lecture Notes in Computer Science, Proceedings of the Cryptographers' Track at the RSA Conference, San Francisco, CA, USA, 8–12 April 2001*; Springer: Berlin, Germany, 2001; pp. 100–109.
5. Zhou, J.; Tan, C. Playing lottery on the Internet. In *Lecture Notes in Computer Science, Proceedings of the International Conference on Information and Communications Security, Singapore, 9–12 December 2001*; Springer: Berlin, Germany, 2001; pp. 189–201.
6. Chow, S.S.; Hui, L.C.; Yiu, S.M.; Chow, K. Practical electronic lotteries with offline TTP. *Comput. Commun.* **2006**, *29*, 2830–2840. [CrossRef]
7. Liu, Y.; Hu, L.; Liu, H. Using an efficient hash chain and delaying function to improve an e-lottery scheme. *Int. J. Comput. Math.* **2007**, *84*, 967–970. [CrossRef]
8. Goldschlag, D.M.; Stubblebine, S.G.; Syverson, P.F. Temporarily hidden bit commitment and lottery applications. *Int. J. Inf. Secur.* **2010**, *9*, 33–50. [CrossRef]
9. Sako, K. Implementation of a digital lottery server on WWW. In *Secure Networking—CQRE [Secure]'99*; Springer: Berlin, Germany, 1999; pp. 101–108.
10. Konstantinou, E.; Liagkou, V.; Spirakis, P.; Stamatiou, Y.C.; Yung, M. Electronic national lotteries. In *Lecture Notes in Computer Science, Proceedings of the International Conference on Financial Cryptography, Key West, FL, USA, 9–12 February 2004*; Springer: Berlin, Germany, 2004; pp. 147–163.
11. Fouque, P.A.; Poupard, G.; Stern, J. Sharing decryption in the context of voting or lotteries. In *Lecture Notes in Computer Science, Proceedings of the International Conference on Financial Cryptography, Anguilla, Anguilla, 20-24 February 2000*; Springer: Berlin, Germany, 2000; pp. 90–104.
12. Paillier, P. Public-key cryptosystems based on composite degree residuosity classes. In *Lecture Notes in Computer Science, Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques, Prague, Czech Republic, 2–6 May 1999*; Springer: Berlin, Germany, 1999; pp. 223–238.
13. Lee, J.S.; Chan, C.S.; Chang, C.C. Non-iterative privacy preservation for online lotteries. *IET Inf. Secur.* **2009**, *3*, 139–147. [CrossRef]
14. Lee, J.S.; Chang, C.C. Design of electronic t-out-of-n lotteries on the Internet. *Comput. Stand. Interfaces* **2009**, *31*, 395–400. [CrossRef]
15. Liu, Y.N.; Cheng, C.; Jiang, T.; Chang, C.C. A practical lottery using oblivious transfer. *Int. J. Commun. Syst.* **2016**, *29*, 277–282. [CrossRef]
16. Marszałek, Z. Parallelization of modified merge sort algorithm. *Symmetry* **2017**, *9*, 176. [CrossRef]

17. Allem, L.E.; Hoppen, C. A pre-test for factoring bivariate polynomials with coefficients in F2. *Inf. Process. Lett.* **2017**, *121*, 22–28. [CrossRef]
18. Marszałek, Z.; Woźniak, M.; Połap, D. Fully Flexible Parallel Merge Sort for Multicore Architectures. *Complexity* **2018**, *2018*, 8679579. [CrossRef]
19. Nakatsukasa, Y.; Noferini, V.; Townsend, A. Vector spaces of linearizations for matrix polynomials: A bivariate polynomial approach. *SIAM J. Matrix Anal. Appl.* **2017**, *38*, 1–29. [CrossRef]
20. Plestenjak, B. Minimal determinantal representations of bivariate polynomials. *Linear Algebra Its Appl.* **2017**, *532*, 550–569. [CrossRef]
21. Blom, R. An optimal class of symmetric key generation systems. In *Lecture Notes in Computer Science, Proceedings of the Workshop on the Theory and Application of of Cryptographic Techniques, Paris, France, 9–11 April 1984*; Springer: Berlin, Germany, 1984; pp. 335–338.
22. Stinson, D.R.; Wei, R. Unconditionally secure proactive secret sharing scheme with combinatorial structures. In *Lecture Notes in Computer Science, Proceedings of the International Workshop on Selected Areas in Cryptography, Kingston, ON, Canada, 9–10 August 1999*; Springer: Berlin, Germany, 1999; pp. 200–214.
23. D'Arco, P.; Stinson, D.R. On unconditionally secure robust distributed key distribution centers. In *Lecture Notes in Computer Science, Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security, Queenstown, New Zealand, 1–5 December 2002*; Springer: Berlin, Germany, 2002; pp. 346–363.
24. Ben-Or, M.; Goldwasser, S.; Wigderson, A. Completeness theorems for non-cryptographic fault-tolerant distributed computation. In Proceedings of the ACM Twentieth Annual ACM Symposium on Theory of Computing, Chicago, IL, USA, 2–4 May 1988; pp. 1–10.
25. Shamir, A. How to share a secret. *Commun. ACM* **1979**, *22*, 612–613. [CrossRef]
26. Benaloh, J.C. Secret sharing homomorphisms: Keeping shares of a secret secret. In *Lecture Notes in Computer Science, Proceedings of the Conference on the Theory and Application of Cryptographic Techniques, Santa Barbara, CA, USA, 11–15 August 1986*; Springer: Berlin, Germany, 1986; pp. 251–260.
27. Liu, Y.; Guo, W.; Fan, C.I.; Chang, L.; Cheng, C. A practical privacy-preserving data aggregation (3PDA) scheme for smart grid. *IEEE Trans. Ind. Inform.* **2018**. [CrossRef]
28. Liu, Y.; Wang, Y.; Wang, X.; Xia, Z.; Xu, J.F. Privacy-preserving raw data collection without a trusted authority for IoT. *Comput. Netw.* **2018**. [CrossRef]
29. Gennaro, R.; Ishai, Y.; Kushilevitz, E.; Rabin, T. The round complexity of verifiable secret sharing and secure multicast. In Proceedings of the ACM Thirty-Third Annual ACM Symposium on Theory of Computing, Santa Barbara, CA, USA, 16–20 August 2001; pp. 580–589.
30. Håstad, J.; Impagliazzo, R.; Levin, L.A.; Luby, M. Construction of a pseudo-random generator from any one-way function. *SIAM J. Comput. Citeseer* **1993**, *28*, 12–24.