Hindawi
Journal of Sensors
Volume 2021, Article ID 8860487, 9 pages
https://doi.org/10.1155/2021/8860487

Research Article

Research on a Traceability Scheme for a Grain Supply Chain

MiaoLei Deng[1,2] **and Pan Feng**[1,2]

[1]*College of Information Science and Engineering, Henan University of Technology, Zhengzhou 450001, China*
[2]*International Union Laboratory of Grain Information Processing, Henan University of Technology, Zhengzhou 450001, China*

Correspondence should be addressed to MiaoLei Deng; dmlei2003@163.com

Received 3 May 2020; Revised 3 December 2020; Accepted 4 January 2021; Published 18 January 2021

Academic Editor: Roberto Paolesse

The frequent occurrence of food safety accidents and the globalization of food import and export circulation make it very important to establish a food traceability system. Due to the bulk and low-value characteristics of grain, it is difficult to achieve traceability in a single unit like meat products; as grain has a longer supply chain, involving much more links and even more complicated factors, it is easy to cause information disconnection. In response to the above problems, this paper has done the following tasks: First, propose a RFID-based grain supply chain traceability model, which mainly describes the information flow and grain flow in the grain traceability system, and secondly, in combination with the GTIN coding standard in the GS1 system, a stage traceability code is set for each batch of grains at each link, providing a method for uniquely identifying the batch of grains at that link, to improve the accuracy of grain traceability. In addition, in order to enable consumers to inquire all the detailed information of the grain in the supply chain through a traceability code, the PRESENT algorithm and the format-preserving algorithm are used to encrypt the traceability codes of each link and generate a final traceability code. Finally, a security and performance analysis of the proposed traceability scheme was carried out. The results show that the proposed scheme is safe and effective, ensuring the safety and traceability of the traceability system of the grain supply chain.

1. Introduction

The current situation of global food production makes consumers pay more and more attention to the safety of food and the traceability of the food supply chain. Although countries and regions around the world have adopted many strict measures on food control, food safety incidents on the global level are still frequent [1–3]. The most illustrative point is that the New York Times has articles on the topic of "food safety" every month [4]. Achieving traceability in the food supply chain can ensure the safety and quality of food and increase consumer confidence. In the related research so far, food traceability and identification methods are mainly divided into three categories: physical methods, biological methods, and chemical methods. Among them, physical methods mainly refer to near-infrared spectroscopy technology and RFID technology [5, 6]. The chemical method is to select and analyze the characteristic factors that can characterize geographic information and then use chemometric methods to analyze the food to identify the origin of the food [7–10]. Mainly used for agricultural products such as rice and vegetables, biological methods are mainly suitable for the traceability of livestock meat products, through DNA sequence detection or iris feature technology [11–14] to achieve traceability. Among them, the system based on RFID technology to achieve traceability is the most extensive. For meat products, an electronic ear tag is usually assigned to a single animal. The RFID tag records relevant information of the animal, including information about vaccinations, birthplace, growth, and other relevant environmental information. For fresh foods such as vegetables and fruits, it is generally only necessary to record the origin information in the tag [15, 16]. However, grain has the characteristics of bulk and low value, and during the process from planting to sale, it needs to go through many links such as storage, transportation, and processing, and the containers that hold the grain in each link are frequently changed. Based on the above reasons, the problem of information disconnection in the supply chain of grain is prone to occur, which ultimately leads to low traceability accuracy and difficulty in traceability.

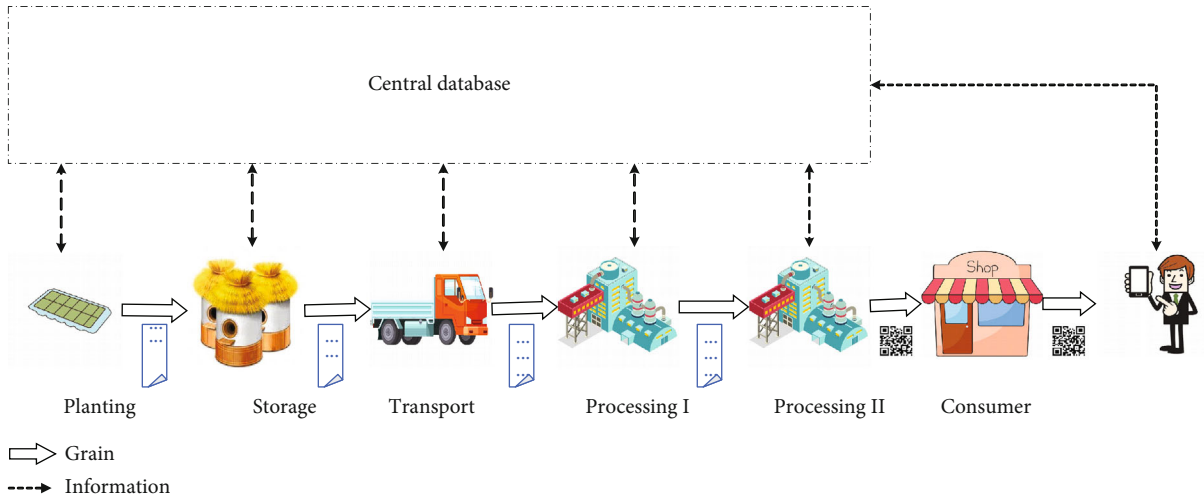


Figure 1: The grain supply chain traceability model.

Most of the existing grain traceability systems only pay attention to the information of the planting process, mainly because it is difficult to accurately locate the batch information of the grain to be traced. Therefore, to realize the effective traceability of grain, the traceability code must be used to correspond the information flow of grain in the production and circulation process with the grain flow. The traceability code is used as the information carrier to realize batch positioning and improve the accuracy of grain traceability, which is beneficial to the construction of grain traceability system. In the existing related research, Yang et al., [17, 18] through the analysis of fruit and vegetable logistics and the study of coding standards, proposed a coding method combining product coding and process coding and a geographic coordinate-based agricultural product traceability coding scheme. Zheng et al. [19] design the traceability code based on the UCC/EAN-128 encoding rules for cereal and oil products. Qu et al. [20] use a combination of location code, plot code, production date, production batch, and check code to design the traceability code. Li et al. [21] used an improved AES algorithm that outputs encrypted decimal numbers of equal length to implement an aquatic product traceability code encryption algorithm; Zheng et al. [22] designed a traceability code for agricultural products based on the GS1 coding system but did not design the final traceability code.

Comprehensive analysis of existing traceability code coding schemes, there are problems such as long length, poor versatility, weak encryption, or even no encryption. This paper takes grain as the research object, proposes a grain traceability model based on RFID technology, and designs stage traceability codes for each link of the supply chain based on the GTIN coding standard in the GS1 system to achieve precise positioning to each link. In addition, the improved PRESENT algorithm and format-preserving algorithm are used to generate a final traceability code. The safety and performance analysis of the traceability code scheme for the grain supply chain at the end of this paper shows that the proposed scheme is both safe and effective.

2. Grain Supply Chain Traceability Model

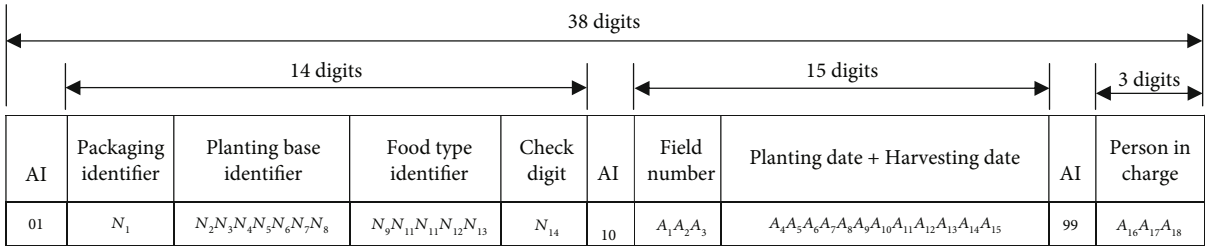
The grain supply chain involves five links: planting, storage, transportation, processing, and sales. At the planting stage, an RFID tag is allocated to each batch of grain, and the traceability code at each link stage is written into the RFID tag, which is circulated in the supply chain along with the grain. To prevent tampering in any link, all the participants in the supply chain link jointly maintain a central database. Participants in the link can share all the information. All the links must upload their stage traceability codes to the central database. The model is shown below:

Figure 1 shows the flow of grain and information of the supply chain. During the planting stage, grain is coded in units of fields. During the storage and transportation stages, the grains are coded in units of warehouses and transport vehicles; the processing link is divided into two stages. Processing stage I is similar to the previous link and is coded in the workshop. In processing stage II, the final traceability code and related information are printed on the outer packaging of the product in the form of a QR code. In the sales stage, consumers can use the final traceability code to query the product information by scanning the QR code on the outer packaging of the product.

3. Stage Traceability Code

Many links exist in the grain supply chain. A stage traceability code must be able to uniquely locate a certain batch of grain at a certain link, such that the relevant status information of the grain at the corresponding link corresponds to the stage traceability code on a one-to-one bases. These codes are stored in a central database.

3.1. Stage Traceability Code Coding Scheme. GS1 (Globe standard 1) is an organization established by the United States Uniform Code Committee in 1973. The organization has a system of global identification standards. To achieve code universality, GS1 issues a 14-digit pure global trade item code



AI	Packaging identifier	Planting base identifier	Food type identifier	Check digit	AI	Field number	Planting date + Harvesting date	AI	Person in charge
01	N_1	$N_2N_3N_4N_5N_6N_7N_8$	$N_9N_{11}N_{11}N_{12}N_{13}$	N_{14}	10	$A_1A_2A_3$	$A_4A_5A_6A_7A_8A_9A_{10}A_{11}A_{12}A_{13}A_{14}A_{15}$	99	$A_{16}A_{17}A_{18}$

Figure 2: Planting coding structure.

AI	Packaging identifier	Granary base identifier	Food type identifier	Check digit	AI	Warehouse number	Inbound date + Outbound date	AI	Person in charge
01	N_1	$N_2N_3N_4N_5N_6N_7N_8$	$N_9N_{11}N_{11}N_{12}N_{13}$	N_{14}	10	$A_1A_2A_3$	$A_4A_5A_6A_7A_8A_9A_{10}A_{11}A_{12}A_{13}A_{14}A_{15}$	99	$A_{16}A_{17}A_{18}$

Figure 3: Storage coding structure.

AI	Packaging identifier	Transport base identifier	Food type identifier	Check digit	AI	Vehicle number	Transport start and end dates	AI	Person in charge
01	N_1	$N_2N_3N_4N_5N_6N_7N_8$	$N_9N_{11}N_{11}N_{12}N_{13}$	N_{14}	10	$A_1A_2A_3$	$A_4A_5A_6A_7A_8A_9A_{10}A_{11}A_{12}A_{13}A_{14}A_{15}$	99	$A_{16}A_{17}A_{18}$

Figure 4: Transport coding structure.

AI	Packaging identifier	Processing base identifier	Food type identifier	Check digit	AI	Workshop number	Date of entry + Date of shipment	AI	Person in charge
01	N_1	$N_2N_3N_4N_5N_6N_7N_8$	$N_9N_{11}N_{11}N_{12}N_{13}$	N_{14}	10	$A_1A_2A_3$	$A_4A_5A_6A_7A_8A_9A_{10}A_{11}A_{12}A_{13}A_{14}A_{15}$	99	$A_{16}A_{17}A_{18}$

Figure 5: Processing stage I coding structure.

(GTIN-14) that used to encode various supply chain stages. To facilitate identification and expansion, the structure of the traceability code at each stage of the design is similar, including key information such as the base and the person in charge and is a 38-dight decimal number. The specific coding structure is shown in Figures 2–5.

Stage traceability code of planting link = AI (01) + packaging identifier + planting base identifier + food type identifier + check digit + AI (10) + field number + planting date + harvesting date + AI (99) + responsible person code. During the planting process, the grain is numbered in batches in field units. For example, field 001 is planted on January 2, 2019, and harvested on October 15. For example, the grain code supervised by person in charge 002 is (01) 1 6902591 10102 8 (10) 001 190102191015 (99) 002.

The stage traceability code for storage links = AI (01) + packaging identifier + granary base identifier + food type identifier + check digit + AI (10) + warehouse number + inbound date + outbound date + AI (99) + responsible person code. Similar to the planting link, the storage links are numbered in warehouse units. For example, the stage code for a batch of grain entering the warehouse on October 20, 2019, is as follows: (01) 1 6972325 10102 5 (10) 028 191020200115 (99) 105.

The stage traceability code for transport links = AI (01) + packaging identifier + transport base identifier + food type identifier + check digit + AI (10) + vehicle number + transport start and end dates + AI (99) + responsible person code. The transport link is numbered in transport vehicles units. For example, the stage code of the grain transported by the No. 205 vehicle from January 16, 2020, to January 20, 2020, is (01) 1 6922807 10102 9 (10) 205 200116200120 (99) 322.

The stage traceability code for processing link I = AI (01) + packaging identifier + processing base identifier +

food type identifier + check digit + AI (10) + warehouse number + date of entry + date of shipment + AI (99) + responsible person code. Processing link I is numbered in the workshop units. For example, a batch of grain stage codes processed by workshop No. 114 supervised by the person in charge No. 922 is (01) 1 6972163 10102 7 (10) 114 200120200425 (99) 922.

3.2. Explanation of Code Coding Scheme

3.2.1. Application Identifier (AI). Additional information refers to the manufacturing attribute information associated with some products, such as production date and batch number. Each item of additional information has a corresponding application identifier that identifies the meaning of the data and the format of the additional information. In addition, neither the additional information nor its application identifier can be used alone. It can only be used as subsidiary information of the main information, GTIN-14 and must be used in series with GTIN-14. One code can reference multiple additional information items. The application identifier consists of 2-4 digits. Whose meanings in the coding structure of each stage as shown in Figures 2–5 are shown in Table 1:

The GTIN corresponding to the application identifier "01" includes GTIN-8, GTIN-12, GTIN-13, and GTIN-14. The batch number data corresponding to the application identifier "10" can be alphanumeric characters and can have variable lengths (up to 20 digits). Taking the planting stage as an example, the field number, planting date, and harvesting date are recorded as the batch number consist of 15 digits: 001 190102191015. The data corresponding to the application identifier "91-99" can be encoded using any internal company information technique and have variable length with a maximum of 90 digits. All the links in this paper use the number 99 as the code identifier of the person in charge.

The packaging identifier can distinguish between different packaging levels, different packaging types, and different packaging quantities. The number of packaging instructions ranges from 1 to 8, and in the coding scheme in this article $N1 = 1$, which is the smallest unit.

3.2.2. Base Identifier. The manufacturer identification code is used as the base code. If the base code does not include a manufacturer identification code, a unique base identification code is assigned to the base code by the traceability system.

3.2.3. Grain Type Identification Code. This paper divides grain types into the following five categories; the identification codes for each type are shown in Table 2:

3.2.4. Check Digit. The check digit is used to check the correctness of the coding. The calculation of the check digit follows the standard check code calculation method specified by GS1.

3.2.5. Batch Number. As mentioned above, the field number, planting date, and harvesting date are recorded as batch numbers in the coding structure proposed in this paper. Taking the planting stage as an example, the field number is 001, the planting date is 190102, and the harvesting date is 191015; thus, the number is 001 190102191015.

3.2.6. Responsible Person Code. The responsible person is the person in charge of this batch of grain at this stage, responsible for maintaining supervision. When a safety problem occurs, the blame falls on the responsible person.

Table 1: Values and meanings of AI.

AI	Meaning
01	Global trade item number
10	Batch number
99	Company internal information

Table 2: Grain type identification code.

Grain type	Rice	Wheat	Tuber crops	Coarse cereals	Dry legume grains
Code	10102	10103	10104	10105	10106

4. Final Traceability Code

The final traceability code is used by consumers to perform queries to retrieve traceability information. The final traceability code is obtained by extracting, integrating, and encrypting the traceability code from each link stage. The final traceability code is calculated from the stage traceability codes, so a change to a traceability code at any stage will cause the final traceability code to change.

4.1. The PRESENT Encryption Algorithm. PRESENT is an ultralightweight symmetric block cipher algorithm based on the SPN structure design. Bogdanov et al. [23] were the first to propose the PRESENT algorithm which has excellent performance in hardware implementations and a concise round function design. PRESENT consists of 31 rounds, and its encryption process consists of three parts: an XOR operation, a linear bitwise permutation, and a nonlinear substitution layer. The nonlinear layer uses a single 4-bit S-box S, which is applied 16 times in parallel in each round. The block length is 64 bits, and two key lengths (80 and 128 bits) are supported. The key length of the PRESENT algorithm used in this paper is 80 bits. The algorithm description is shown in Figure 6:

The S-box is the only nonlinear transformation component in the PRESENT algorithm. Therefore, maintaining the security of the S-box is crucial to the PRESENT algorithm. The security of the S-box is crucial to the algorithm. However, Chen et al. [24] and Liu et al. [25] pointed out through analysis that the S-box of the PRESENT algorithm was unable to effectively resist differential analysis; Wang et al. [26] used a combination of inverse mapping on the finite field and affine transformation to construct a new S-box, analyzed it, and revealed that the new S-box was improved with regard to many safety performance

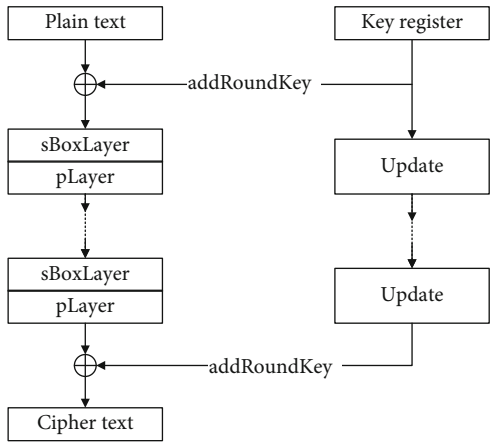


Figure 6: PRESENT algorithm description diagram.

indicators. The improved S-box used in this paper is shown in Table 3:

4.2. Format-Preserving Encryption Algorithm. Similar to the AES algorithm, the PRESENT algorithm performs encryption in the form of binary digits. For ease of presentation, the output format encrypted by the PRESENT algorithm is hexadecimal in this paper. However, the format of the encrypted result is chaotic and is not a decimal number that is easy to identify. In 2019, Liu et al. [27] proposed a format-preserving encryption algorithm. Although this algorithm uses the PRESENT algorithm for encryption, it uses only the encryption result size to generate a 10-digit permutation table. However, adding plain text and key correspondences individually, and then, performing a modulo operation achieves format preservation. Therefore, this paper improves the encryption scheme proposed in [27]; the modulo operation is performed, and the resulting 16-digit decimal number is used as the final traceability code.

4.3. Coding Scheme of Final Traceability Code. The process to generate the final traceability code is as follows:

(1) Extract 16 digits from the traceability code at each stage

Taking the planting stage as an example, take its 7 digits of planting base code +6 digits of harvest date code +3 digits of person in charge.

(2) Use the PRESENT algorithm for encryption

Because the key length is 80 bits, the extracted 16-digit traceability code +4 digits of the transaction time is used as the encryption key.

(3) Encryption using the format-preserving encryption algorithm

For ease of description, the relevant notations used for are defined in Table 4.

Table 3: Improved S-box.

Input	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
Output	7	F	C	6	8	1	D	9	A	4	B	3	2	E	0	5

The final traceability code generation process is shown in Figure 7.

As shown in the figure above, the final traceability code generation process must be encrypted by three times PRESENT algorithms and one time format-preserving algorithm. It is worth mentioning that this process involves the transaction time and dynamic key of each link. For the transaction time, the transaction time between each pair of links is written into the tag by the latter link. The random performance of this transaction time effectively prevents counterfeiting, and a dynamic key is generated by the processing link, which further strengthens the security of the algorithm.

5. Example

5.1. Extracting the Stage Traceability Code. Sixteen digits need to be extracted from the 38-digit stage traceability code, and these 16 digits must be able to uniquely locate a certain batch of grain at a certain stage. Again taking the planting stage as an example, we use 7 digits of the planting base code +3 digits of the responsible person identification code. The 16 digits after each link extraction are shown in Table 5:

5.2. Encryption Using the PRESENT Algorithm. Taking the planting and storage stage transactions as an example, if the two-stage transaction time is 12 : 25, then F0 = 69025911910150021225, and so on, F2 = 69228072001203221005 and F3 = 69721632004259221515.

The encryption result after applying the PRESENT algorithm three times is as follows:

$$\begin{aligned} T_0 &= E(F_1, F_0) \\ &= E(6972325200115105, 69025911910150021225) \\ &= \text{BA73E22132B8049C}, \\ T_1 &= E(T_0, F_2) \\ &= E(\text{BA73E22132B8049C}, 69228072001023221005) \\ &= \text{FB307794C422D82}, \\ T_2 &= E(T_1, F_3) \\ &= E(\text{FB3071794C422D82}, 69721632001029221515) \\ &= \text{C4BF100D5963FA9D}. \end{aligned} \tag{1}$$

5.3. Encryption Using the Format-Preserving Encryption Algorithm. If the dynamic key K = 23B86620C325B1AD, we add the PRESENT encryption result T_2, and the dynamic

Table 4: Notations used in the encryption process.

Notation	Description
F_0	Stage traceability code after extraction during planting (16 digits) + time of the transactions (4 digits)
F_1	Stage traceability code after extraction during storage (16 digits)
F_2	Stage traceability code after extraction during transportation (16 digits) + time of the transactions (4 digits)
F_3	Stage traceability code after extraction during processing I (16 digits) + time of the transactions (4 digits)
$E(p, k)$	Encryption operation with p as plain text and k as key
T_0	$T_0 = E(F_1, F_0)$
T_1	$T1 = E(T_0, F_2)$
T_2	$T2 = E(T_1, F_3)$
K	One-time secret dynamic key
C	Final traceability code

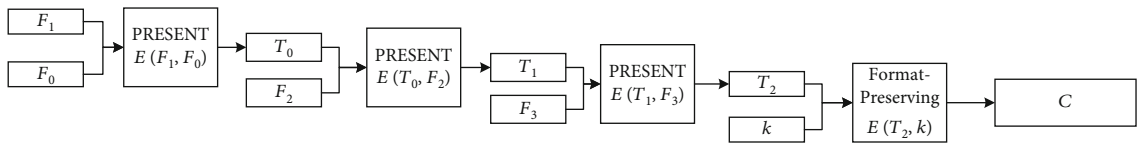


Figure 7: The final traceability code generation process.

Table 5: 16-digit stage traceability code after extraction.

Link	Stage traceability code after extraction
Planting stage	6902591 191015 002
Storage stage	6972325 200115 105
Transport stage	6922807 200120 322
Processing stage I	6972163 200425 922

Table 6: Information available in each link.

Link	Information known at each stage (including speculative)
Planting stage	F_0
Storage stage	$F_0\ F_1$
Transport stage	$F_0\ F_1\ F_2$
Processing stage I	$F_0\ F_1\ F_2\ F_3\ K$

key K in a one-to-one correspondence and apply the modulo operation:

$$\begin{aligned} &(12+2)\%10=4 \quad (4+3)\%10=7 \quad (11+11)\%10=2 \quad (16+8)\%10=4,\\ &(1+6)\%10=7 \quad (0+6)\%10=6 \quad (0+2)\%10=2 \quad (13+0)\%10=3,\\ &(5+12)\%10=7 \quad (9+3)\%10=2 \quad (6+2)\%10=8 \quad (3+5)\%10=8,\\ &(16+11)\%10=7 \quad (10+1)\%10=1 \quad (9+10)\%10=9 \quad (13+13)\%10=6. \end{aligned} \tag{2}$$

Therefore, the final traceability code C = 4724762372887196. The decryption process involves subtracting the one-to-one correspondence between C and K; then, the modulo operation can obtain $T2$, to which the PRESENT decryption algorithm is then applied three times.

6. Security Analysis

As mentioned above, in the grain supply chain model designed in this paper, the stage codes assigned to each batch of grain at each stage are recorded in the database. The stage code is displayed only in each link of the supply chain and is used primarily to indicate the source information of the grain to the participants in the supply chain. The final traceability code is used for consumer inquiries and should be encrypted and protected from batch forgery. Therefore, the security analysis focuses mainly on the illegal addition of stage codes and batch forgery of the final traceability code.

6.1. Illegal Addition of Stage Codes by Internal Links. Regarding the stage codes, if a certain internal link wants to incorporate unqualified grains into a certain batch of grain, that

Table 7: The running time of the encryption process of the final traceability code.

Number of runs	Running time (ms)										AVG (ms)
100	5	7	8	5	7	7	7	6	6	8	6.6
1000	57	60	60	57	63	61	59	61	68	57	60.3
10000	606	608	677	585	598	712	625	662	613	610	629.6
100000	6180	6403	6303	6534	6458	6441	6302	6365	6351	6376	6371.3

Table 8: Comparison of PRESENT algorithm and other algorithms.

Cipher	Key bits	Block bits	Cycles per block	Logic process (μm)	Area (GE)
PRESENT-80	80	64	32	0.18	1570
AES-128	128	128	1032	0.35	3400
DES	56	64	144	0.18	2309
HIGHT	128	64	1	0.25	3048

batch must be assigned a stage traceability code. However, the number of stage codes that can be generated for each batch of grain is certain. Therefore, it is not feasible for internal links to add a stage code for illegal grain batches to mix them into qualified products.

6.2. Forging the Final Traceability Code. In addition, because the final traceability code is consumer-oriented and open, most of the existing traceability codes are long, weak, or even unencrypted. Therefore, even if a one-time traceability code is used, because no encryption exists, it is easy for an illegal manufacturer to crack the coding rules for the traceability codes. Then, the traceability codes can be forged in batches, which can result in large losses. The final traceability code generation formula designed in this paper is as follows:

$$C = E_2(E_1(E_1(E_1(F_1, F_0), F_2), F_3), K). \quad (3)$$

It can be seen from the above formula that the final traceability code is generated through three times PRESENT algorithms and one time format-preserving encryption algorithm. Moreover, the S-box of the PRESENT algorithm used in this paper is improved, with a higher encryption strength. This approach is sufficiently robust to prevent external cracking by external illegal manufacturers.

If the internal link of the supply chain attempts to forge the final code in batches, because each link writes the stage code for this link in the RFID tag, the information available for each link when operating with this batch of grain is shown in Table 6.

As shown in Table 6, the information known in each of the three links of planting, storage, and transportation is not sufficient to generate the legal final traceability code. Only processing stage I possesses all the information needed to generate the final traceability code but that processing stage is at the final manufacturer. In addition, if processing stage I attempts to forge the grain source, an unqualified grain forgery source will be used to generate the final code so that if a food security problem exists, the responsibility will appear to shift to the other links. However, due to the existence of a central database, all the legal final traceability codes must have legal stage codes that are recognizable by the other links. Therefore, processing stage I also cannot forge food sources.

In summary, the grain supply chain traceability plan designed in this paper can prevent illegal mixing of unqualified grains in various internal links and can effectively prevent bulk forgeries of final traceability codes by illegal manufacturers.

7. Performance Analysis

The generation process of the final traceability code of this paper mainly uses the PRESENT algorithm, which is a lightweight block encryption algorithm. The pseudo code is described as follows:

This paper tested the process of generating the final traceability code, and its running time is shown in the following Table 7:

As shown in the above table, the final traceability code generation process was performed 10 times of encryption 100 times, 1000 times, 10000 times, and 100000 times. It can be calculated that it takes approximately 0.63 milliseconds to generate a final traceability code.

Table 8 lists the PRESENT algorithm and DES, AES, and HIGHT algorithm performance comparison.

It can be clearly seen from the above table that the PRESENT algorithm is an ultralightweight cryptographic algorithm with low power consumption and is suitable for resource-constrained food supply chain environments.

8. Conclusions and Prospects

This paper mainly completes the following three aspects of work: designing a grain traceability model, designing a set of stage traceability code coding schemes, and designing a final traceability code encryption scheme. Each batch of grain and its corresponding RFID tag are circulated through the supply chain to solve the problem of information disconnection. In addition, we analyzed the performance and security of the proposed coding scheme. Among them, the designed stage traceability code holds the key information of each link

in 38 decimal digits, meeting the traceability code requirements for versatility, ease of use, simplicity, and scalability. The resulting 16-bit final traceability code is both short and has strong encryption that can effectively prevent the traceability code forgeries by external illegal manufacturers or even internal participants.

In recent years, blockchain technology has attracted attention from various fields due to its decentralized and nontamperable features. These features make blockchain technology well able to meet the requirements of food traceability for the authenticity and traceability of information in the supply chain. In 2019, Azzi et al. [28] analyzed the advantages and challenges brought by the introduction of blockchain into the supply chain field and proposed relevant theories for establishing an efficient supply chain based on blockchain technology; Creydt et al. [29] pointed out that the combination of blockchain technology and the Internet of Things can completely change the field of food industry; Feng [30] first proposed the combination of blockchain and RFID technology for traceability of agricultural product supply chains and analyzed the advantages and disadvantages of such a traceability system. Mondal et al. [31] used an identity verification protocol based on object proofs to achieve a complete food supply chain traceability architecture by integrating RFID sensors at the physical layer and integrating blockchain technology at the network layer. Blockchain technology has great development potential in the field of food traceability. Therefore, in future-related research, we can use RFID tags, sensors, and many other Internet of Things devices to scan and track food information, use a reasonable coding scheme for unit identification, and use blockchain technology to record food information of the supply chain, in order to realize the traceability of bulk products such as grain in the supply chain.

Data Availability

Source codes of improved PRESENT algorithm used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare no conflicts of interest in relation to this work.

Acknowledgments

This work was supported by the National Nature Science Foundation of China (No. U1304606).

References

[1] J. M. Soon, A. K. M. Brazier, and C. A. Wallace, "Determining common contributory factors in food safety incidents - a review of global outbreaks and recalls 2008-2018," *Trends in Food Science and Technology*, vol. 97, pp. 76–87, 2020.

[2] N. Chammem, M. Issaoui, A. I. D. de Almeida, and A. M. Delgado, "Food crises and food safety incidents in European Union, United States, and Maghreb Area: current risk communication strategies and new approaches," *Journal of AOAC International*, vol. 101, no. 4, pp. 923–938, 2018.

[3] Y. Liu, H. Li, H. L. Yan, and L. L. Cai, "Whole-process control technology of typical rice field polluted with cadmium in Hunan: a case study," *Chinese Agricultural Science Bulletin*, vol. 35, pp. 94–99, 2019.

[4] K. Behnke and M. F. W. H. A. Janssen, "Boundary conditions for traceability in food supply chains using blockchain technology," *International Journal of Information Management*, vol. 52, article 101969, 2020.

[5] Y. Zhang, Y. Ruan, F. Liu, and J. Shang, "Research on meat food traceability system based on RFID technology," in *2019 IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC)*, pp. 2172–2175, Chengdu, China, March 2019.

[6] X. M. Zhao and J. H. Liu, "Advances in the application of RFID technology in food traceability systems," *Food & Machinery*, vol. 35, no. 2, pp. 212–216+225, 2019.

[7] M. Ferreiro-Gonzalez, G. F. Barbero, J. A. Alvarez, A. Ruiz, M. Palma, and J. Ayuso, "Authentication of virgin olive oil by a novel curve resolution approach combined with visible spectroscopy," *Food Chemistry*, vol. 220, pp. 331–336, 2017.

[8] A. Valdés, A. Beltrán, C. Mellinas, A. Jiménez, and M. C. Garrigós, "Analytical methods combined with multivariate analysis for authentication of animal and vegetable food products with high fat content," *Trends in Food Science & Technology*, vol. 77, pp. 120–130, 2018.

[9] J. Zhao, A. Li, X. Jin, and L. Pan, "Technologies in individual animal identification and meat products traceability," *Biotechnology and Biotechnological Equipment*, vol. 34, no. 1, pp. 48–57, 2020.

[10] D. Psomiadis, N. Zisi, C. Koger, B. Horvath, and B. Bodiselitsch, "Sugar-specific carbon isotope ratio analysis of coconut waters for authentication purposes," *Journal of Food Science and Technology*, vol. 55, no. 8, pp. 2994–3000, 2018.

[11] D. P. Kalogianni, "DNA-based analytical methods for milk authentication," *European Food Research and Technology*, vol. 244, no. 5, pp. 775–793, 2018.

[12] A. Galimberti, F. de Mattia, A. Losa et al., "DNA barcoding as a new tool for food traceability," *Food Research International*, vol. 50, no. 1, pp. 55–63, 2013.

[13] L. di Stasio, P. Piatti, E. Fontanella et al., "Lamb meat traceability: the case of Sambucana sheep," *Small Ruminant Research*, vol. 149, pp. 85–90, 2017.

[14] A. I. Awad, "From classical methods to animal biometrics: a review on cattle identification and tracking," *Computers and Electronics in Agriculture*, vol. 123, pp. 423–435, 2016.

[15] M. Hate, S. Jadhav, and H. Patil, "Vegetable traceability with smart irrigation," in *2018 International Conference on Smart City and Emerging Technology (ICSCET)*, p. 15, Mumbai, India, January 2018.

[16] H. Gao, Z. Wang, and Y. Liu, "Application of intelligent traceability management system in agriculture-take Aodong fruit and vegetable planting cooperative as an example," *Journal of Physics: Conference Series*, vol. 1302, article 022046, 2019.

[17] X. T. Yang, J. P. Qian, and C. H. Sun, "Design and application of safe production and quality traceability system for vegetable," *Transactions of the Chinese Society of Agricultural Engineering*, vol. 24, no. 3, pp. 162–166, 2008.

[18] X. T. Yang, J. P. Qian, and Z. Zhang, "Design of agricultural product trace coding based on geography coordinate and multi-encrypt," *Transactions of the Chinese Society of Agricultural Engineering*, vol. 25, no. 7, pp. 131–135, 2009.

[19] H. G. Zheng, S. H. Liu, H. Meng, and P. J. He, "Design and implementation of quality traceability label for cereal and oil products based on UCC/EAN-128 bar code," in *Proceedings of 2010 World Automation Congress*, pp. 469–473, Beijing China, 2010.

[20] X. H. Qu, D. F. Zhuang, and D. S. Qiu, "Studies on GIS based tracing and traceability of safe crop product in China," *Agricultural Sciences in China*, vol. 6, no. 6, pp. 724–731, 2007.

[21] W. Y. Li, C. H. Sun, and X. X. Liu, "Design and implementation of encryption algorithm for aquatic products traceability code," *Transactions of the Chinese Society for Agricultural Machinery*, vol. 43, no. 4, pp. 106–112, 2012.

[22] L. H. Zheng, R. H. Ji, and M. J. Wang, "Design and application of traceable unified coding scheme for agricultural products," *Transactions of The Chinese Society of Agricultural Machinery*, vol. 50, pp. 385–392, 2019.

[23] A. Bogdanov, L. R. Knudsen, G. Leander et al., "PRESENT: an ultra-lightweight block cipher," *Proceedings of Cryptographic Hardware and Embedded Systems-CHES 2007-9th International Workshop*, , , pp. 450–466, Springer, 2007.

[24] W. J. Chen, S. Y. Zhao, R. J. Zou, and X. N. Zhang, "The differential fault attack of PRESENT cipher," *Journal of the University of Electronic Science and Technology of China*, vol. 48, pp. 865–869, 2019.

[25] G. Q. Liu and C. H. Jin, "Differential cryptanalysis of PRESENT-like cipher," *Designs, Codes and Cryptography*, vol. 76, no. 3, pp. 385–408, 2015.

[26] Y. Wang, G. H. Wei, and Y. T. Zhang, "Improvement and simulation design of PRESENT algorithm," *Computer Engineering and Design*, vol. 38, pp. 2347–2352, 2017.

[27] B. T. Liu, R. X. Peng, R. X. Wu, H. F. Ding, and M. M. Xie, "Lightweight format-preserving encryption algorithm oriented to number," *Journal of Computer Research and Development*, vol. 56, pp. 1488–1497, 2019.

[28] R. Azzi, R. K. Chamoun, and M. Sokhn, "The power of a blockchain-based supply chain," *Computers & Industrial Engineering*, vol. 135, pp. 582–592, 2019.

[29] M. Creydt and M. Fischer, "Blockchain and more - algorithm driven food traceability," *Food Control*, vol. 105, pp. 45–51, 2019.

[30] T. Feng, "An agri-food supply chain traceability system for China based on RFID & blockchain technology," in *2016 13th International Conference on Service Systems and Service Management (ICSSSM)*, pp. 1–6, Kunming, China, July 2016.

[31] S. Mondal, K. P. Wijewardena, S. Karuppuswami, N. Kriti, D. Kumar, and P. Chahal, "Blockchain inspired RFID-based information architecture for food supply chain," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 5803–5813, 2019.