Secure Secret Sharing in the Cloud

Ching-Chun Chang
Department of Computer Science
University of Warwick
United Kingdom
Email: c.chang.2@warwick.ac.uk

Chang-Tsun Li
School of Computing and Mathematics
Charles Sturt University
Australia
Email: chli@csu.edu.au

***Abstract*—In this paper, we show how a dealer with limited resources is possible to share the secrets to players via an untrusted cloud server without compromising the privacy of the secrets. This scheme permits a batch of two secret messages to be shared to two players in such a way that the secrets are reconstructable if and only if two of them collaborate. An individual share reveals absolutely no information about the secrets to the player. The secret messages are obfuscated by encryption and thus give no information to the cloud server. Furthermore, the scheme is compatible with the Paillier cryptosystem and other cryptosystems of the same type. In light of the recent developments in privacy-preserving watermarking technology, we further model the proposed scheme as a variant of reversible watermarking in the encrypted domain.**

***Keywords*-secret sharing; cloud computing; homomorphic encryption; reversible watermarking; multimedia security**

I. Introduction

Secret sharing is a study in cryptography invented independently by Blakley [1] and Shamir [2]. In general, there is one dealer who splits a secret into shares for n players and only when any group of t or more players work collectively will the secret be reconstructed from their shares. Any $t-1$ shares reveals restrictively no information about the secret. This refers to as a (t, n)-threshold secret sharing scheme. Conventionally, n shares are of at least the same size of the secret itself. This n-fold increase in required storage is, however, space inefficient and thus has led to the notion of multi-secret sharing [3]–[5]. Over the past decade, businesses and individuals have entrusted an increasing amount of data to the cloud for the purposes of processing and storage. In the meanwhile, the advances in cloud computing have also led to growing concerns for data privacy. A standard solution to the concerns over privacy would be to encrypt the data. However, the desired functionality may not be achievable on the encrypted data. To address this problem, Rivest *et al.* [6] introduced the notion of homomorphic encryption, which permits mathematical operations to be performed on the encrypted data. In reality, encryption algorithms are in-built features in many widely available devices, while secret sharing algorithms have rather limited availability to the public. In addition to this, many secret sharing algorithms are patented and thus there are restrictions on the commercial use of these intellectual properties. For these reasons, it is of great interest to study secure secret sharing in the cloud, or from a scientific point of view, secret sharing in the encrypted domain.

In this paper, we propose a multi-secret sharing scheme that permits a cloud server to split a batch of two encrypted messages into two shares. The proposed scheme is secure in two ways. First, the encrypted data gives no information about the secrets to the cloud server. Second, an individual share gives no information about the secrets to the player. In light of the recent developments in privacy-preserving watermarking technology, we further model the proposed secret sharing scheme as a reversible watermarking scheme that embeds the watermark payload into an encrypted media producing two marked and encrypted medias. Only by pooling two marked medias together will the watermark payload be detected and the host media be recovered. The remainder of this paper is organised as follows. Section II presents the proposed secret sharing scheme. Section III models the proposed scheme as a reversible watermarking scheme for an authentication application. Section IV concludes our work and outlines the directions for future research.

II. Secret Sharing

Let Alice and Bob denote two players, Clare denote a cloud server, and Dave denote a dealer. Suppose that Dave wishes to share a batch of two secrets x and y to Alice and Bob through Clare. To begin with, Dave encrypts x and y into $\mathcal{E}(x)$ and $\mathcal{E}(y)$ and uploads them collectively to Clare. Then, Clare creates two shares $\mathcal{E}(\alpha)$ and $\mathcal{E}(\beta)$ for Alice and Bob, respectively. Finally, Alice and Bob download their respective shares and work collaboratively in order to disclose the secrets. We assume that Dave has the public key for encryption and both Alice and Bob have the private key for decryption. We further assume that Clare is an honest-but-curious party that is interesting in learning the secret information, but does not deviate from the protocol specification. An overview of the protocol is shown schematically in Fig. 1.

This work is supported by the EU Horizon 2020 - Marie Sklodowska-Curie Actions through the project entitled Computer Vision Enabled Multimedia Forensics and People Identification (Project No. 690907, Acronym: IDENTITY).

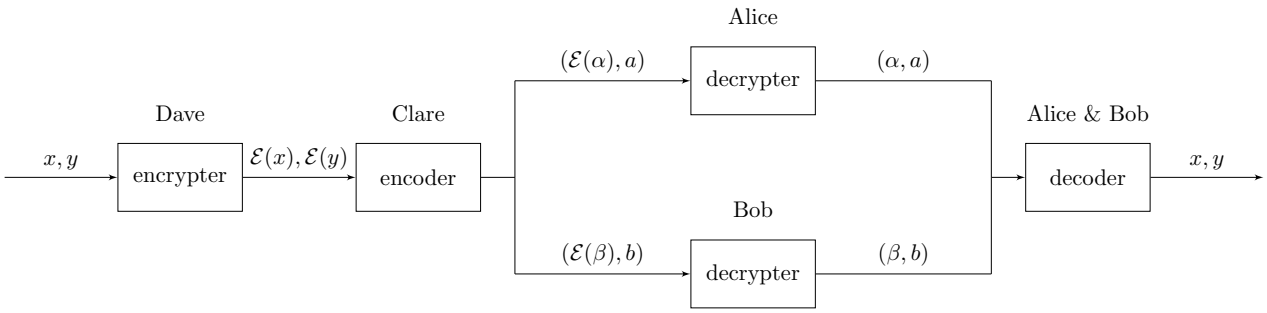

Figure 1. A protocol of secure secret sharing in the cloud.

The scheme is demonstrated with the Paillier cryptosystem [7], and yet is by no means limited to this particular homomorphic cryptosystem. Before we proceed further, let us first describe the homomorphic properties of the Paillier cryptosystem. Let m_1 and m_2 be two arbitrary messages, $\mathcal{E}(\cdot)$ be the encryption function, and $\mathcal{D}(\cdot)$ be the decryption function. The message space and ciphertext space of the Paillier cryptosystem are defined as the additive group $\mathcal{M} = \mathbb{Z}/n\mathbb{Z}$ and the multiplicative group $\mathcal{C} = \mathbb{Z}/n^2\mathbb{Z}^*$, respectively, where n is the product of two large primes p and q. The Paillier cryptosystem permits homomorphic addition:

$$\mathcal{D}(\mathcal{E}(m_1) \cdot \mathcal{E}(m_2) \bmod n^2) \equiv m_1 + m_2 \mod n, \quad (1)$$

and homomorphic multiplication:

$$\mathcal{D}(\mathcal{E}(m_1)^{m_2} \bmod n^2) \equiv m_1 \cdot m_2 \mod n. \quad (2)$$

Through the use of homomorphic operations, two shares are created by

$$\begin{aligned} \mathcal{E}(\alpha) &\equiv \mathcal{E}(x)^a \cdot \mathcal{E}(y)^b \equiv \mathcal{E}(ax + by) \mod n^2, \\ \mathcal{E}(\beta) &\equiv \mathcal{E}(x)^b \cdot \mathcal{E}(y)^a \equiv \mathcal{E}(bx + ay) \mod n^2, \end{aligned} \quad (3)$$

where a and b are any integers that satisfy

$$\begin{aligned} \gcd(a + b, n) &= 1, \\ \gcd(a - b, n) &= 1. \end{aligned} \quad (4)$$

It would not be difficult to find proper a and b since n is the product of two primes. Given that $a^2 - b^2 \equiv (a+b) \cdot (a-b) \bmod n$, we derive

$$\gcd(a^2 - b^2, n) = 1. \quad (5)$$

This also implies

$$\gcd(b^2 - a^2, n) = 1. \quad (6)$$

The proof for Eq. (6) will be given later. Clare distributes $(\mathcal{E}(\alpha), a)$ to Alice and $(\mathcal{E}(\beta), b)$ to Bob. After decryption, Alice and Bob obtain

$$\begin{aligned} \alpha &\equiv \mathcal{D}(\mathcal{E}(\alpha)) \equiv ax + by \mod n, \\ \beta &\equiv \mathcal{D}(\mathcal{E}(\beta)) \equiv bx + ay \mod n. \end{aligned} \quad (7)$$

By pooling (α, a) and (β, b) together, they compute

$$\begin{aligned} a\alpha - b\beta &\equiv (a^2x + aby) - (b^2x + aby) \\ &\equiv (a^2 - b^2)x \mod n. \end{aligned} \quad (8)$$

We know that $\exists!(a^2 - b^2)^{-1}$ such that

$$(a^2 - b^2) \cdot (a^2 - b^2)^{-1} \equiv 1 \mod n, \quad (9)$$

since $\gcd(a^2 - b^2, n) = 1$. This modular multiplicative inverse can be calculated by the extended Euclidean algorithm. Thus, the secret x is unveiled by

$$x \equiv (a\alpha - b\beta) \cdot (a^2 - b^2)^{-1} \mod n. \quad (10)$$

In the same way, the secret y is uncovered by

$$y = (b\alpha - a\beta) \cdot (b^2 - a^2)^{-1} \mod n. \quad (11)$$

Now, we give the proof for Eq. (6). More precisely, we wants to prove the statement that $\gcd(-c, n) = 1$ when $\gcd(c, n) = 1$, where c is an arbitrary integer. To prove the statement by contradiction, we assume that

$$\gcd(-c, n) = t \neq 1, \quad (12)$$

when $\gcd(c, n) = 1$. Since $-c \equiv n - c \mod n$, Eq. (12) can be rewritten as $\gcd(n - c, n) = t$. This assumption implies that there exists integers r_1 and r_2 such that

$$\begin{aligned} n - c &= t \cdot r_1, \\ n &= t \cdot r_2. \end{aligned} \quad (13)$$

Thus,

$$t \cdot r_2 - c = t \cdot r_1, \quad (14)$$

and then

$$c = t \cdot (r_2 - r_1). \quad (15)$$

From Eq. (15), we can infer that $\gcd(c, n) = t \neq 1$, which contradicts our initial assumption that $\gcd(c, n) = 1$. Therefore, the given statement has been demonstrated.

III. Reversible Watermarking

Considering the recent advances in privacy-preserving watermarking technology, we introduce an extension of the proposed scheme for reversible watermarking in the encrypted domain. The reader is referred to [8]–[10] for more interesting combination of secret sharing and information hiding. Digital watermarking is the practice of imperceptibly embedding a watermark into a host media (*e.g.* audio, image and video) and a watermark is usually a piece of information associated with host media (*e.g.* digital identity and digital signature) [11]. In general, there are three parties involved in a watermarking protocol: a party who encodes the watermark with the host media, a party who decodes the watermark from the marked media, and an adversary who has malicious intent against the protocol. The malicious adversary is often modelled as a noisy channel between the encoder and the decoder and the watermark can be either fragile or robust against the channel noise depending on the applications. Conventionally, robust watermarking is in favour of copyright protection [12], whereas fragile watermarking is advantageous to integrity verification [13]. In some medical and military applications, even the imperceptibly distortion introduced by watermarking might be undesirable. This has given rise to the notion of reversible watermarking in which an additional requirement on reversing the watermarking process is imposed [14]–[18]. In other words, the objective is not only to detect the watermark, but also to recover the host media. Recently, there are a surge of research interest in reversible watermarking in the encrypted domain due to the privacy concerns in cloud computing. This modern research topic concerning the host media that has been obscured by encryption and permitting the function of watermarking to be outsourced to an untrusted cloud server without giving away the information privacy [19]–[24].

Let Dave be a sender who wishes to embed a watermark payload into a host media and shares the marked media to two recipients Alice and Bob. Only by pooling two marked media together will the watermark payload be detected and the host media be recovered. Nevertheless, due to limited resources, Dave has to entrust the function of watermarking to an untrusted cloud server Clare. Let us assume that the encryption key is publicly known, while the decryption key is only known to Alice and Bob. For concreteness, we let the host media be a digital image and yet the host media is by no means limited to the digital content of this type. Let $\mathbf{I}$ denote an 8-bit digital image such that

$$\mathbf{I} := (\mathbf{bit}_1||\mathbf{bit}_2||\dots||\mathbf{bit}_8), \tag{16}$$

where '||' is the concatenation operator and

$$\begin{aligned} \mathbf{bit}_1 &:= (bit_{1,1}||bit_{1,2}||\dots), \\ \mathbf{bit}_2 &:= (bit_{2,1}||bit_{2,2}||\dots), \\ &\cdots \\ \mathbf{bit}_8 &:= (bit_{8,1}||bit_{8,2}||\dots) \end{aligned} \tag{17}$$

are eight sequences of bits corresponding to eight bit-planes. Let a pair of two large primes p and q be the private key and $n = pq$ be the public key. To make the given image be compatible with the Paillier cryptosystem, we convert the bits into decimal integers in $\mathbb{Z}/n\mathbb{Z}$ sequentially in such a way that a collection of $\log_2 n$ bits in a certain bit-plane is converted to an integer. In practice, we would convert a collection of $\lfloor \log_2 n \rfloor$ bits into an integer instead since the value of $\log_2 n$ is not necessarily an integer. We refer to this discrete random variable as a symbol and denote it by x. Hence, an encrypted image can be written as

$$\mathcal{E}(\mathbf{I}) := (\mathcal{E}(\mathbf{x}_1)||\mathcal{E}(\mathbf{x}_2)||\dots||\mathcal{E}(\mathbf{x}_8)), \tag{18}$$

where

$$\begin{aligned} \mathcal{E}(\mathbf{x}_1) &:= (\mathcal{E}(x_{1,1})||\mathcal{E}(x_{1,2})||\dots), \\ \mathcal{E}(\mathbf{x}_2) &:= (\mathcal{E}(x_{2,1})||\mathcal{E}(x_{2,2})||\dots), \\ &\cdots \\ \mathcal{E}(\mathbf{x}_8) &:= (\mathcal{E}(x_{8,1})||\mathcal{E}(x_{8,2})||\dots) \end{aligned} \tag{19}$$

are eight sequences of encrypted symbols corresponding to eight bit-planes. The watermarking process is performed sequentially on some selected encrypted symbols until all the payload is embedded. The other unselected encrypted symbols remain intact during the process. Due to the fidelity constraint, we select the symbols that are composed of bits from the insignificant bit-planes for watermarking.

For conciseness, we describe only how a single host symbol is processed. Let x be a host symbol and y be a watermark symbol. To start with, Dave encrypts x and y into $\mathcal{E}(x)$ and $\mathcal{E}(y)$ and uploads them collectively to Clare. By means of the proposed method, two shares $\mathcal{E}(\alpha)$ and $\mathcal{E}(\beta)$ are created. Alice and Bob download their respective shares and decrypt them into α and β. This procedure will be carried out iteratively until all the symbols are downloaded and decrypted. Then, Alice and Bob form their respective meaningful marked images by converting the symbols back into bits, as illustrated in Fig. 2. The host symbols and watermark symbols are reconstructable when two marked images are pooled together. The joint procedure of watermark detection and host recovery is identical to the procedure of secret reconstruction.

(a) Alice's marked image (b) Bob's marked image

Figure 2. Two recipients' marked images.

IV. Conclusion

In this paper, we propose a $(2, 2)$-threshold multi-secret sharing scheme in the encrypted domain. The scheme is compatible with the Paillier cryptosystem and other homomorphic cryptosystems of the same type. In addition to this, an application to reversible watermarking in the encrypted domain is discussed. We wish that this work can be of inspiration to the multimedia security and its associated communities. From our perspective, a study towards a more general (t, n)-threshold multi-secret sharing scheme in the encrypted domain is of great research interest. Furthermore, an extension to verifiable secret sharing [25], in which the dealer and players are not always assumed to be honest, deserves further consideration.

Acknowledgement

The authors would like to thank the anonymous reviewers for their insightful comments and suggestions.

References

[1] G. R. Blakley, "Safeguarding cryptographic keys," in *Proc. AFIPS Nat. Comput. Conf. (NCC'79)*, New York, NY, USA, Jun. 1979, pp. 313–317.

[2] A. Shamir, "How to share a secret," *Commun. ACM*, vol. 22, no. 11, pp. 612–613, Nov. 1979.

[3] M. Franklin and M. Yung, "Communication complexity of secure computation (extended abstract)," in *Proc. 24th Ann. ACM Symp. Theory Comput. (STOC'92)*, Victoria, BC, Canada, May 1992, pp. 699–710.

[4] C. Blundo, A. De Santis, G. Di Crescenzo, A. G. Gaggia, and U. Vaccaro, "Multi-secret sharing schemes," in *Proc. 14th Ann. Int. Cryptology Conf. (CRYPTO'94)*, Santa Barbara, CA, USA, Aug. 1994, pp. 150–163.

[5] C.-W. Chan and C.-C. Chang, "A scheme for threshold multi-secret sharing," *Appl. Math. Comput.*, vol. 166, no. 1, pp. 1–14, Jul. 2005.

[6] R. L. Rivest, L. Adleman, and M. L. Dertouzos, "On data banks and privacy homomorphisms," in *Foundations of Secure Computation*, R. A. DeMillo *et al.*, Eds. Orlando, FL, USA: Academic Press, Inc., 1978, pp. 169–180.

[7] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in *Proc. 18th Ann. Int. Conf. Theory Appl. Cryptographic Techn. (EUROCRYPT'99)*, Prague, Czech Republic, May 1999, pp. 223–238.

[8] P.-Y. Lin, J.-S. Lee, and C.-C. Chang, "Distortion-free secret image sharing mechanism using modulus operator," *Pattern Recognition*, vol. 42, no. 5, pp. 886–895, May 2009.

[9] C.-C. Chang, Y.-H. Chen, and H.-C. Wang, "Meaningful secret sharing technique with authentication and remedy abilities," *Inf. Sci.*, vol. 181, no. 14, pp. 3073–3084, Jul. 2011.

[10] J.-S. Lee and Y.-R. Chen, "Selective scalable secret image sharing with verification," *Multimedia Tools Appl.*, vol. 76, no. 1, pp. 1–11, Jan. 2017.

[11] I. J. Cox, M. L. Miller, and J. A. Bloom, *Digital Watermarking*. San Francisco, CA, USA: Morgan Kaufmann Publishers Inc., 2002.

[12] I. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," *IEEE Trans. Image Process.*, vol. 6, no. 12, pp. 1673–1687, Dec. 1997.

[13] C.-T. Li, "Digital fragile watermarking scheme for authentication of JPEG images," *IEE Proc. - Vision, Image Signal Process.*, vol. 151, no. 6, pp. 460–466, Dec. 2004.

[14] T. Kalker and F. M. J. Willems, "Capacity bounds and constructions for reversible data-hiding," in *Proc. 14th Int. Conf. Digital Signal Process. (DSP'02)*, Santorini, Greece, Jul. 2002, pp. 71–76.

[15] J. Tian, "Reversible data embedding using a difference expansion," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 13, no. 8, pp. 890–896, Aug. 2003.

[16] C.-T. Li, "Reversible watermarking scheme with image-independent embedding capacity," *IEE Proc. - Vision, Image, Signal Process.*, vol. 152, no. 6, pp. 779–786, Dec. 2005.

[17] Z. Ni, Y.-Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 16, no. 3, pp. 354–362, Mar. 2006.

[18] D. M. Thodi and J. J. Rodriguez, "Expansion embedding techniques for reversible watermarking," *IEEE Trans. Image Process.*, vol. 16, no. 3, pp. 721–730, Mar. 2007.

[19] X. Zhang, "Reversible data hiding in encrypted image," *IEEE Signal Process. Lett.*, vol. 18, no. 4, pp. 255–258, Apr. 2011.

[20] K. Ma, W. Zhang, X. Zhao, N. Yu, and F. Li, "Reversible data hiding in encrypted images by reserving room before encryption," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 3, pp. 553–562, Mar. 2013.

[21] J. Zhou, W. Sun, L. Dong, X. Liu, O. C. Au, and Y. Y. Tang, "Secure reversible image data hiding over encrypted domain via key modulation," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 26, no. 3, pp. 441–452, Mar. 2016.

[22] Z. Qian and X. Zhang, "Reversible data hiding in encrypted images with distributed source encoding," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 26, no. 4, pp. 636–646, Apr. 2016.

[23] H.-T. Wu, Y.-M. Cheung, and J. Huang, "Reversible data hiding in Paillier cryptosystem," *J. Visual Commun. Image Representation*, vol. 40, pt. B, pp. 765–771, Oct. 2016.

[24] F. Huang, J. Huang, and Y.-Q. Shi, "New framework for reversible data hiding in encrypted domain," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 12, pp. 2777–2789, Dec. 2016.

[25] B. Chor, S. Goldwasser, S. Micali, and B. Awerbuch, "Verifiable secret sharing and achieving simultaneity in the presence of faults," in *Proc. 26th Ann. Symp. Found. Comput. Sci. (SFCS'85)*, Portland, OR, USA, Oct. 1985, pp. 383–395.