SECURITY OF AUDIO SECRET SHARING SCHEME ENCRYPTING AUDIO SECRETS WITH BOUNDED SHARES

Shinya Washio and Yodai Watanabe

Department of Computer Science and Engineering, University of Aizu
Aizu-Wakamatsu City, Fukushima 9658580, Japan

ABSTRACT

Secret sharing is a method of encrypting a secret into multiple pieces called shares so that only qualified sets of shares can be employed to reconstruct the secret. Audio secret sharing (ASS) is an example of secret sharing whose decryption can be performed by human ears. This paper examines the security of an audio secret sharing scheme encrypting audio secrets with bounded shares, and optimizes the security with respect to the probability distribution used in its encryption.

Index Terms— Audio Secret Sharing, Information-Theoretic Security, Variation Distance

1. INTRODUCTION

A secret sharing (SS) scheme is a cryptosystem that encrypts a secret into multiple pieces called shares so that only qualified sets of shares can be employed to reconstruct the secret. Therefore the SS scheme is one of the most fundamental technologies to realize secure access control. A typical example of secret sharing schemes is a (k, n)-threshold secret sharing scheme, which was originated by Shamir [1] and Blakley [2] independently. In (k, n)-threshold secret sharing schemes, a secret is encrypted into n shares in such a way that any k or more shares can be employed to reconstruct the secret, while no $k-1$ or less shares leak any information about the secret.

In the ordinary secret sharing schemes, secrets and shares are both numerical data, and their encryption and decryption are performed by computers. In contrast, there exist secret sharing schemes whose decryption does not require any numerical computations but can be performed by a human. A visual secret sharing (VSS) scheme, which originated from Naor and Shamir [3], is an example of such secret sharing schemes. In VSS schemes, secrets and shares are both visual data such as printed texts, hand written notes, pictures, and so on. The schemes encrypt a visual secret into visual shares so that humans can recover the visual secret with their eyes by superposing a qualified set of visual shares printed on transparencies. Figure 1 illustrates an example of two shares and their superposition of a $(2, 2)$-threshold VSS scheme.

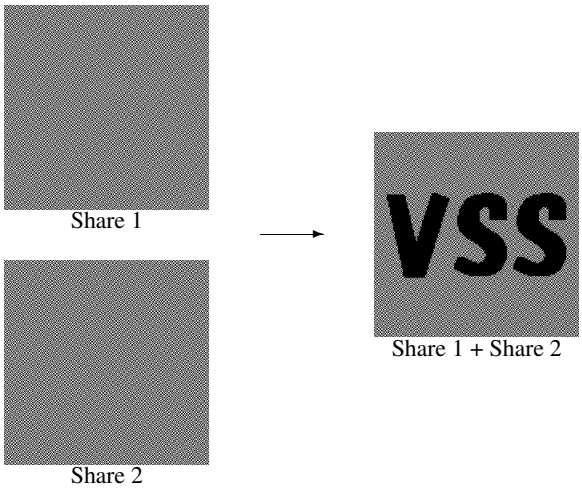

Fig. 1. Two shares and their superposition of a $(2, 2)$-threshold VSS scheme

An audio secret sharing (ASS) scheme is another example of secret sharing schemes whose decryption can be performed by human without any numerical computations. The scheme encrypts a secret into audio shares so that humans can recover the secret with their ears by playing a qualified set of audio shares simultaneously. Here, in contrast to VSS schemes, there have been proposed two types of ASS schemes, which differ in the types of secrets. More precisely, Desmedt et al. [4] proposed information-theoretically secure schemes that encrypt a binary string secret, while Ehdaie et al. [5] proposed schemes that can encrypt an audio secret. Figure 2 illustrates an example of two shares and their superposition of a $(2, 2)$-threshold ASS scheme proposed by Desmedt et al. [4]. Although it is an advantage of the latter schemes that they can encrypt arbitrary audio secrets, the security analysis in [5] is invalid because the analysis is essentially based on impossible requirement that the amplitude of the audio shares should be uniformly distributed over (the whole) $\mathbb{R}$; in fact, such shares should have infinite amount of acoustic energy, and also, such shares can no longer be approximated by any acoustic waves

This work was supported in part by a Grant-in-Aid for Young Scientists (B) No. 21700021, and Fukushima Prefectural Foundation for Advancement of Science and Education.

978-1-4799-2893-4/14/$31.00 ©2014 IEEE

Table 1. Comparison among audio and visual secret sharing schemes

	ASS				VSS
	Desmedt et al. [4]	Ehdaie et al. [5]	Yoshida & Watanabe [6]	This work	Naor & Shamir [3]
Secret	Binary string	Audio	Audio	Audio	Visual
Share	Audio	Audio	Audio	Audio	Visual
Distribution	Uniform over a finite set	Uniform over $\mathbb{R}$	Normal over $\mathbb{R}$	Normal over $[-B, B]$	Uniform over a finite set

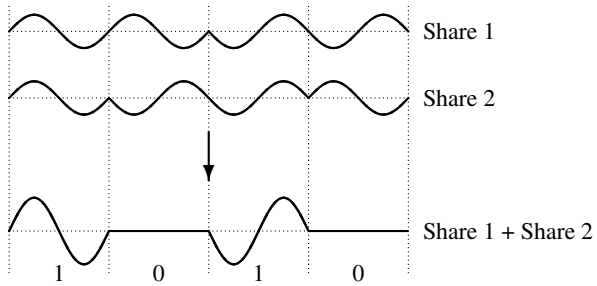

Fig. 2. Two shares and their superposition of an ASS scheme proposed by Desmedt et al. [4]

with bounded amplitude (with probability 1). To solve this problem, Yoshida and Watanabe [6] used a normal distribution over $\mathbb{R}$ for the encryption of ASS schemes encrypting audio secrets, and evaluated their security. The aim of this work is to improve the result of [6] so that shares of ASS schemes encrypting audio secrets should have bounded amplitude with probability 1; for this purpose, this work uses a normal distribution over a bounded domain for the encryption of an ASS scheme encrypting audio secrets, and evaluates its security. Table 1 summarizes the existing works on ASS and VSS schemes as well as this work.

The rest of this paper is organized as follows. In Section 2, we provide notations and definitions that will be used later. Section 3 is devoted to evaluating the security of an audio secret sharing scheme encrypting audio secrets with bounded shares. Section 4 concludes this paper with mentioning problems for future work.

2. PRELIMINARIES

In this section, we provide notations and definitions that will be used later. For details of definitions in information theory and secret sharing, see, e.g., [7, 8, 9].

Let $\mathcal{P} = \{P_1, \cdots, P_n\}$ and $\mathcal{S}$ be finite sets. For $\boldsymbol{s} = (s_1, \cdots, s_n) \in \mathcal{S}^{|\mathcal{P}|}$ and $a \subset \mathcal{P}$, let $[\boldsymbol{s}]_a$ denote an element of $\{\emptyset \cup \mathcal{S}\}^{|\mathcal{P}|}$ such that

$$([\boldsymbol{s}]_a)_i = \begin{cases} s_i & \text{for } P_i \in a, \\ \emptyset & \text{for } P_i \notin a. \end{cases}$$

For a set $\mathcal{M}$, let $\mathfrak{R}(\mathcal{M})$ denote the set of all random variables over $\mathcal{M}$.

The normal distribution $N(\mu, \sigma^2)$ with mean μ and variance σ^2 is a probability distribution with a probability density function

$$p_{N(\mu,\sigma^2)}(x) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{(x-\mu)^2}{2\sigma^2}}.$$

It is straightforward to confirm that

$$\int_a^b p_{N(\mu,\sigma^2)}(x)dx = \frac{1}{2}\Big(\mathrm{erf}\Big(\frac{b-\mu}{\sqrt{2}\sigma}\Big) - \mathrm{erf}\Big(\frac{a-\mu}{\sqrt{2}\sigma}\Big)\Big),$$

where $\mathrm{erf}(x)$ is the error function defined by

$$\mathrm{erf}(x) = \frac{2}{\sqrt{\pi}} \int_0^x e^{-t^2} dt.$$

For probability distributions p and q over a measurable space $(\mathcal{X}, \mu)$, the *variation distance* $d(p, q)$ *between* p *and* q is defined by

$$d(p, q) = \frac{1}{2} \int_{x \in \mathcal{X}} \big|p(x) - q(x)\big| d\mu(x).$$

It is conventional to use the mutual information to measure the statistical independence between random variables. Here, the mutual information $I(X : Y)$ between random variables X and Y can be written as

$$I(X : Y) = D(p(x, y)||p(x)p(y)),$$

where $D(p||q)$ is the relative entropy between probability distributions p and q over $(\mathcal{X}, \mu)$ defined by

$$D(p||q) = \int_{x \in \mathcal{X}} p(x) \log \frac{p(x)}{q(x)} d\mu(x).$$

Note that the relative entropy $D(p||q)$ is defined for probability distributions p and q such that

$$\{x|p(x) > 0\} \supset \{x|q(x) > 0\},$$

which is inconvenient for our purpose. Therefore, we define the independence $d(X : Y)$ between random variables X and Y by using the variation distance instead of the relative entropy as

$$d(X : Y) = d(p(x, y), p(x)p(y)).$$

It should be stated that the security described by the variation distance has already been considered in existing works; for

example, the universal composability [10] in quantum cryptography is defined by use of the trace distance, which is the quantum generalization of the variation distance.

Let $\mathcal{P} = \{P_1, \cdots, P_n\}$ be a set of participants, and let $2^{\mathcal{P}}$ denote the set of all the subsets of $\mathcal{P}$. Let $\mathcal{M}$ and $\mathcal{S}$ be sets of all possible values of secrets and shares, respectively. In an SS scheme, a secret $m \in \mathcal{M}$ is encrypted into $(s_1, \cdots, s_n) \in \mathcal{S}^n$, called shares, and each share s_i is distributed to the corresponding participant P_i. Here, any element of $A_Q \subset 2^{\mathcal{P}}$ can reconstruct m with their shares, while any element of $A_F \subset 2^{\mathcal{P}}$ can obtain no information about m. The set A_Q and A_F are called the qualified set and the forbidden set, respectively, and the pair of A_Q and A_F, $\Gamma = (A_Q, A_F)$, is called an access structure on $\mathcal{P}$. Formal definitions of an access structure and a secret sharing scheme are described below.

Definition 1 (Access structure)**.** Let $\mathcal{P}$ be a finite set, and let A_Q and A_F be subsets of $2^{\mathcal{P}}$. A pair of sets A_Q and A_F, $\Gamma = (A_Q, A_F)$, is called an *access structure on* $\mathcal{P}$ if A_Q and A_F satisfy the following conditions:

$$A_Q \cap A_F = \emptyset,$$
$$a \in A_Q \wedge a \subset b \to b \in A_Q,$$
$$b \in A_F \wedge a \subset b \to a \in A_F.$$

For an access structure $\Gamma = (A_Q, A_F)$, A_Q and A_F are called the *qualified set* and the *forbidden set*, respectively.

Definition 2 (Secret sharing scheme)**.** Let $\mathcal{P}$, $\mathcal{M}$ and $\mathcal{S}$ be finite sets, and $\Gamma = (A_Q, A_F)$ be an access structure on $\mathcal{P}$. Let $\mathrm{Enc}(\cdot)$ be a probabilistic function from $\mathcal{M}$ to $\mathcal{S}^{|\mathcal{P}|}$ and $\mathrm{Dec}(\cdot)$ be a deterministic function from $\{\emptyset \cup \mathcal{S}\}^{|\mathcal{P}|}$ to $\mathcal{M}$. A pair of functions Enc and Dec, $SS = (\mathrm{Enc}, \mathrm{Dec})$, is called a *secret sharing scheme realizing* Γ if Enc and Dec satisfy the following conditions:

$$\forall a \in A_F \forall M \in \mathfrak{R}(\mathcal{M})\big(d(M : [\mathrm{Enc}(M)]_a) = 0\big),$$
$$\forall a \in A_Q \forall m \in \mathcal{M}\big(\mathrm{Dec}([\mathrm{Enc}(m)]_a) = m\big).$$

This definition is slightly different from but is equivalent to the standard one (see e.g. [9]).

Example 1 ((k, n)-threshold access structure)**.** A (k, n)-*threshold access structure on a finite set* $\mathcal{P}$ consists of the qualified set A_Q and the forbidden set A_F given by

$$A_Q = \big\{a \subset \mathcal{P} \big| k \leq |a|\big\} \quad \text{and} \quad A_F = \big\{a \subset \mathcal{P} \big| k > |a|\big\}.$$

In particular, a $(2, 2)$-threshold access structure on $\mathcal{P} = \{P_1, P_2\}$ consists of the qualified set A_Q and the forbidden set A_F given by

$$A_Q = \big\{\{P_1, P_2\}\big\} \quad \text{and} \quad A_F = \big\{\emptyset, \{P_1\}, \{P_2\}\big\}.$$

A secret sharing scheme realizing a (k, n)-threshold access structure is called a (k, n)-*threshold secret sharing scheme*.

3. MAIN RESULTS

In this section, we evaluate the security of an audio secret sharing scheme encrypting audio secrets with bounded shares. First, we provide a formal definition of ASS schemes and a construction of the simplest ASS scheme, namely a $(2, 2)$-threshold ASS scheme.

Definition 3 (ϵ-secure audio secret sharing scheme [6])**.** Let $\mathcal{P}$ be a finite set, and $\Gamma = (A_Q, A_F)$ be an access structure on $\mathcal{P}$. Let $\mathcal{M}$ and $\mathcal{S}$ be subsets of $\mathbb{R}$ or $\mathbb{Z}$. Let $\mathrm{Enc}(\cdot)$ be a probabilistic function from $\mathcal{M}$ to $\mathcal{S}^{|\mathcal{P}|}$ and $\mathrm{Dec}(\cdot)$ be a deterministic function from $\{\emptyset \cup \mathcal{S}\}^{|\mathcal{P}|}$ to $\mathcal{M}$. For $\epsilon \geq 0$, a pair of functions Enc and Dec, $ASS = (\mathrm{Enc}, \mathrm{Dec})$, is called an *$\epsilon$-secure audio secret sharing scheme realizing* Γ if Dec is defined by $\mathrm{Dec}([s]_a) = \sum_{i:P_i \in a} s_i$ for $s \in \mathcal{S}^{|\mathcal{P}|}$ and $a \subset \mathcal{P}$, and Enc and Dec satisfy the following conditions:

$$\forall a \in A_F \forall M \in \mathfrak{R}(\mathcal{M})\big(d(M : [\mathrm{Enc}(M)]_a) \leq \epsilon\big),$$
$$\forall a \in A_Q \exists \alpha \neq 0 \forall m \in \mathcal{M}\big(\mathrm{Dec}([\mathrm{Enc}(m)]_a) = \alpha m\big).$$

Construction 1 ($(2, 2)$-threshold audio secret sharing scheme)**.** Let $\mathcal{S}$ and $\mathcal{M}$ be subsets of $\mathbb{R}$ and $\mathbb{Z}$, respectively, bounded by $B > 0$: $\mathcal{S} = \big\{s \in \mathbb{R}\big||s| \leq B\big\}$ and $\mathcal{M} = \big\{z \in \mathbb{Z}\big||z| \leq B\big\}$. For $\alpha > 0$, $m \in \mathcal{M}$ and $s_1, s_2 \in \mathcal{S}$, define Enc and Dec by

$$\mathrm{Enc}(m) = \Big(\frac{\alpha}{2}m + r, \frac{\alpha}{2}m - r\Big), \quad \mathrm{Dec}(s_1, s_2) = s_1 + s_2,$$

respectively, where r is a random variable (whose distribution should be chosen to minimize ϵ).

Let $N_\Delta(\mu, \sigma^2)$ be the normal distribution with mean μ and variance σ^2 over bounded domain $[-\Delta, \Delta]$; its density function is given by

$$p_{N_\Delta(\mu,\sigma^2)}(x) = \begin{cases} \frac{c^{-1}}{\sqrt{2\pi\sigma^2}} e^{-\frac{(x-\mu)^2}{2\sigma^2}} & \text{if } -\Delta \leq x \leq \Delta, \\ 0 & \text{otherwise,} \end{cases}$$

where c^{-1} is a normalization constant defined by

$$c = \int_{\mu-\Delta}^{\mu+\Delta} p_{N(\mu,\sigma^2)}(x)dx = \mathrm{erf}\Big(\frac{\Delta}{\sqrt{2}\sigma}\Big).$$

If we require that shares s_1 and s_2 should be bounded as $|s_1|, |s_2| \leq B$, then it follows from $|m| \leq B$ that $|r| \leq \big(1 - \frac{\alpha}{2}\big)B$. Therefore, we consider a normal distribution over $\big[-\big(1 - \frac{\alpha}{2}\big)B, \big(1 - \frac{\alpha}{2}\big)B\big]$:

Theorem 1. An ASS scheme $ASS = (\mathrm{Enc}, \mathrm{Dec})$ defined by Construction 1 with $\alpha < 1$ and $r \sim N_{(1-\frac{\alpha}{2})B}(0, (\beta B)^2)$ is ϵ-secure, where $\epsilon = \mathrm{erf}\big(\frac{\alpha}{\sqrt{8}\beta}\big)/\mathrm{erf}\big(\frac{2-\alpha}{\sqrt{8}\beta}\big)$.

Proof. Let M and S_i ($i \in \{1, 2\}$) denote the random variables representing a secret and two shares, respectively. We

begin with the definition of the independence between M and S_1:

$$\begin{aligned} d(M:S_1) &= d(p(m,s_1), p(m)p(s_1)) \\ &= \frac{1}{2}\sum_m \int \left| p(m)p(s_1|m) - p(m)p(s_1) \right| ds_1 \\ &= \frac{1}{2}\sum_m p(m) \int \Big| \sum_{m'} p(m')p(s_1|m) \\ &\qquad\qquad - \sum_{m'} p(m')p(s_1|m') \Big| ds_1 \\ &\le \sum_{m,m'} p(m)p(m') d(p(s_1|m), p(s_1|m')) \\ &\le \max_{m,m'} d(N_\Delta(\tfrac{\alpha}{2}m, (\beta B)^2), N_\Delta(\tfrac{\alpha}{2}m', (\beta B)^2)) \end{aligned}$$

with $\Delta = \big(1 - \frac{\alpha}{2}\big)B$. Since $|m|, |m'| \le B$ and

$$d(N_\Delta(\mu, \sigma^2), N_\Delta(\mu', \sigma^2)) = \frac{\operatorname{erf}\left(\frac{|\mu - \mu'|}{\sqrt{8}\sigma}\right)}{\operatorname{erf}\left(\frac{\Delta}{\sqrt{8}\sigma}\right)},$$

it follows that

$$\begin{aligned} d(M:S_1) &\le \max_{m,m'} \frac{\operatorname{erf}\Big(\frac{\left|\frac{\alpha}{2}m - \frac{\alpha}{2}m'\right|}{\sqrt{8}\beta B}\Big)}{\operatorname{erf}\left(\frac{(2-\alpha)B}{\sqrt{8}\beta B}\right)} \\ &\le \frac{\operatorname{erf}\Big(\frac{\frac{\alpha}{2}2B}{\sqrt{8}\beta B}\Big)}{\operatorname{erf}\left(\frac{(2-\alpha)B}{\sqrt{8}\beta B}\right)} = \frac{\operatorname{erf}\left(\frac{\alpha}{\sqrt{8}\beta}\right)}{\operatorname{erf}\left(\frac{2-\alpha}{\sqrt{8}\beta}\right)}. \end{aligned}$$

In the same way, we have $I(M:S_2) \le \operatorname{erf}\big(\frac{\alpha}{\sqrt{8}\beta}\big)/\operatorname{erf}\big(\frac{2-\alpha}{\sqrt{8}\beta}\big)$. Since the forbidden set of a $(2,2)$-threshold access structure on $\{P_1, P_2\}$ is given by $A_F = \big\{\emptyset, \{P_1\}, \{P_2\}\big\}$, these two inequalities yield that ASS is ϵ-secure, where $\epsilon = \operatorname{erf}\big(\frac{\alpha}{\sqrt{8}\beta}\big)/\operatorname{erf}\big(\frac{2-\alpha}{\sqrt{8}\beta}\big)$. This completes the proof. □

In the above theorem, we have required that each share should be bounded. This allows not only practical implementation, but also the optimization (i.e. minimization) of ϵ with respect to the variance parameter β. Note that $N_\Delta(\mu, \sigma^2)$ becomes the uniform distribution over $[\mu - \Delta, \mu + \Delta]$ in the limit $\sigma \to \infty$. Therefore, the following lemma states that ϵ takes the optimum (i.e. minimum) value of $\frac{\alpha}{2-\alpha}$ when r is uniformly distributed over $\big[-\big(1 - \frac{\alpha}{2}\big)B, \big(1 - \frac{\alpha}{2}\big)B\big]$.

Lemma 2. Let ϵ be as above. Then

$$\inf_{\beta > 0} \epsilon = \lim_{\beta \to \infty} \frac{\operatorname{erf}\big(\frac{\alpha}{\sqrt{8}\beta}\big)}{\operatorname{erf}\big(\frac{2-\alpha}{\sqrt{8}\beta}\big)} = \frac{\alpha}{2-\alpha}.$$

Proof. The first equality follows from Lemma 3 (see below), and the second one from L'Hopital's rule. □

Lemma 3. Let $f(x)$ and $F(x)$ be functions on $\mathbb{R}$ defined by

$$f(x) = ce^{-sx^2} \quad \text{and} \quad F(x) = \int_0^x f(z)dz$$

for $c, s > 0$. Then, the function of x defined by $F(ax)/F(bx)$ is monotone increasing for $x > 0$ and $0 < a < b$.

Proof. Lemma 4 (see below) gives

$$\left(\frac{F(ax)}{F(bx)}\right)' = \frac{F(ax)}{xF(bx)}\left(\frac{axf(ax)}{F(ax)} - \frac{bxf(bx)}{F(bx)}\right) > 0.$$

This completes the proof. □

Lemma 4. Let $f(x)$ and $F(x)$ be as above. Then, the function of x defined by $xf(x)/F(x)$ is monotone decreasing for $x > 0$.

Proof. Since $0 < f(x) < c$ for $x > 0$,

$$0 < F(x) = \int_0^x f(z)dz < \int_0^x cdz = cx.$$

Therefore

$$\left(\frac{xf(x)}{F(x)}\right)' = \frac{f(x)}{F(x)}\left(1 + \frac{xf'(x)}{f(x)} - \frac{xf(x)}{F(x)}\right) < \frac{f(x)g(x)}{F(x)},$$

where we have defined $g(x) = 1 - 2sx^2 - e^{-sx^2}$. By this definition,

$$g(0) = 0 \quad \text{and} \quad g'(x) = 2sx(e^{-sx^2} - 2) < 0,$$

and so $g(x) < 0$. Consequently,

$$\left(\frac{xf(x)}{F(x)}\right)' < \frac{f(x)g(x)}{F(x)} < 0.$$

This completes the proof. □

4. CONCLUSION

In this paper, we considered ASS schemes encrypting audio secrets with bounded shares. In particular, we evaluated the security of an ASS scheme whose encryption uses a random variable sampled according to a normal distribution over a bounded domain. The result indicates that the security is optimized when the variance of the normal distribution approaches infinity; in other words, the random variable is sampled according to the uniform distribution over the domain.

In contrast to the ordinary cryptosystems, users even without special knowledge can directly participate in the computation of the ASS decryption. This may increase their confidence and interest in the computation of cryptosystems, which could yield "unusual" applications of ASS schemes. Search for such applications, as well as the optimization of the upper bound ϵ on the mutual information with respect to all probability distributions over a bounded domain, will be the subject of future work.

5. REFERENCES

[1] Adi Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, 1979.

[2] George Robert Blakley, "Safeguarding cryptographic keys," in *Proceedings of the National Computer Conference*, Monval, NJ, USA, 1979, pp. 313–317, AFIPS Press.

[3] Moni Naor and Adi Shamir, "Visual cryptography," in *Proceedings of Advances in Cryptology – Eurocrypt '94*, Perugia, Italy, 1994, vol. 950 of *Lecture Notes in Computer Science*, pp. 1–12, Springer-Verlag.

[4] Yvo Desmedt, Shuang Hou, and Jean-Jacques Quisquater, "Audio and optical cryptography," in *Proceedings of Advances in Cryptology – ASIACRYPT '98*, Kazuo Ohta and Dingyi Pei, Eds., Beijing, China, 1998, vol. 1514 of *Lecture Notes in Computer Science*, pp. 392–404, Springer-Verlag.

[5] Mohammad Ehdaie, Taraneh Eghlidos, and Mohammad Reza Aref, "A novel secret sharing scheme from audio perspective," in *Proceedings of International Symposium on Telecommunications (IST 2008)*, Tehran, Iran, 2008, pp. 13–18, IEEE.

[6] K. Yoshida and Y. Watanabe, "Security of audio secret sharing scheme encrypting audio secrets," in *Proceedings of International Conferece for Internet Technology and Secured Transactions (ICITST 2012)*, London, UK, 2012, pp. 294–295, IEEE.

[7] Thomas M. Cover and Joy A. Thomas, *Elements of Information Theory*, Wiley-Interscience, 2nd edition, 2006.

[8] Imre Csiszár and János Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems*, Cambridge University Press, 2nd edition, 2011.

[9] Douglas Robert Stinson, *Cryptography: Theory and Practice*, Chapman & Hall, CRC, 3rd edition, 2005.

[10] Renato Renner and Robert König, "Universally composable privacy amplification against quantum adversaries," in *Proceedings of Theory of Cryptography Conference (TCC 2005)*, Joe Kilian, Ed., Cambridge, MA, USA, 2005, vol. 3378 of *Lecture Notes in Computer Science*, pp. 407–425, Springer-Verlag.