氏名（本籍）	いわ　ざき　じゅん　や 岩　　﨑　　淳　　也
学 位 の 種 類	博　士（情報科学）
学 位 記 番 号	情　博　第　５８４号
学位授与年月日	平成２７年３月２５日
学位授与の要件	学位規則第４条第１項該当
研究科、専攻	東北大学大学院情報科学研究科（博士課程）情報基礎科学科学専攻
学位論文題目	Password-Protected Secret Sharing Scheme （パスワード付き秘密分散共有方式）
論文審査委員	（主査）東北大学教　授　静谷　啓樹 東北大学教　授　青木　孝文　東北大学教　授　篠原　歩 東北大学准教授　磯辺　秀司

論文内容の要旨

1 Introduction

A file-hosting service enables us to easily store and access documents and data from mobile terminals as well as PC's, and to share them with others. Although the file-hosting service is so popular in the Internet community, we should note that there is a latent risk that we would lose the files we have stored.

In order to safely store some secret documents or data distributedly in several servers via insecure networks such as the Internet, Bagherzandi, Jarecki, Saxena and Lu proposed a password-protected secret sharing (PPSS, for short) scheme [1] in 2011. They proposed two PPSS protocols which achieve the following three properties: (**i**) both are secure against the corruption of the coalition of servers of size less than the specified threshold, which means that one can obtain no useful information about the password and the document even if some servers are corrupted, (**ii**) the user can be authenticated with a single password by all the servers, and (**iii**) there is no useful information about the password and the document in the interaction in a form that no polynomial time adversary can extract. In this thesis, we explore securer PPSS schemes, and propose some protocols.

We first consider security notions for PPSS schemes. Bagherzandi et al. focused on the interaction between the user and the servers, and formulated a security notion which we call the PPSS-security. A PPSS protocol is PPSS-secure if no polynomial time adversary could determine, on any given two documents and any public parameter, which document is stored in the public parameter, even though he is allowed to adaptively interact with the servers and the user in impersonating manner. They proposed the protocol PPSS_2 which is PPSS-secure. In contrast, we focus on the process of generating a public parameter. Since the public parameter involves some information about the stored document in general, for any given public parameter, an adversary may obtain the stored document without corrupting the servers or impersonating the user. We propose another security notion for PPSS schemes with respect to the public parameter, named pparam-security. Intuitively, the pparam-security means that any public parameter does not contain any clue to the stored document in a way that an adversary could recognize. We show that PPSS_2 is not pparam-secure. We then give a protocol which is pparam-secure but not PPSS-secure. These results indicate that the pparam-security is independent of the PPSS-security in a sense that the pparam-security does not imply the PPSS-security in general and vice versa.

We next propose two PPSS protocols. One is ePPSS_2, an enhanced version of PPSS_2, where we prove that the protocol ePPSS_2 is both PPSS-secure and pparam-secure in the random oracle model. The other is a protocol named sPPSS which is both PPSS-secure and pparam-secure in the standard model. All the known protocols, including ePPSS_2, are provably secure in the random oracle model [1, 2, 3]. Hence, the protocol sPPSS is, to our best knowledge, the first protocol which is secure in the standard model.

2 Preliminaries

In this chapter, we describe notions and notations that are used through this thesis.

3 Security Notions for Password-Protected Secret Sharing Scheme

In this chapter, we focus on a public parameter which is generated by initialization algorithm on an input (p, d) of a password and a document, and we propose another PPSS security notion called the pparam-security. A pparam-attack game, for a PPSS scheme $\mathcal{P}$ between an adversary $\mathcal{A}$ and a challenger $\mathcal{C}$ is as follows:

Initialization phase: $\mathcal{C}$ first executes the setup algorithm Setup on input 1^k, and gets a setup parameter λ. Then $\mathcal{C}$ sends λ to $\mathcal{A}$. $\mathcal{A}$ chooses two documents d_1 and d_2, and sends them to $\mathcal{C}$. $\mathcal{C}$ chooses $\beta \in_r \{1, 2\}$. Then $\mathcal{C}$ executes Init on an input (λ, p, d_β), and gets a pair $(\mathrm{pub}, \mathrm{sec})$, where $\mathrm{pub} = (\mathrm{pub}_1, \mathrm{pub}_2, \mathrm{pub}_3)$ is a public parameter and sec is a set of the secret seeds. Finally, $\mathcal{C}$ sends the public parameter pub to $\mathcal{A}$.

Attack phase: $\mathcal{A}$ is allowed to interact with $\mathcal{C}$. In each interaction, $\mathcal{A}$ sends any public parameters $\mathrm{pub}' = (\mathrm{pub}'_1, \mathrm{pub}'_2, \mathrm{pub}'_3)$ to $\mathcal{C}$. $\mathcal{C}$ plays the role in computing the "inverse" of Initialization procedure if $\mathrm{pub}_1 = \mathrm{pub}'_1$ and $\mathrm{pub}_3 \neq \mathrm{pub}'_3$. Then $\mathcal{C}$ returns a document d which satisfies $\mathsf{Init}(\lambda, p, d) = (\mathrm{pub}', \mathrm{sec}')$ for some password p and set sec' of secret seeds. Otherwise, $\mathcal{C}$ returns a special symbol $\perp$.

Challenge phase: $\mathcal{A}$ sends $\beta' \in \{1, 2\}$.

For $\beta = 1, 2$ and a security parameter k, let $P^{\beta}_{\text{pparam-atk}}(k)$ denote the probability that $\mathcal{A}$ sends 1 in Challenge phase of the pparam-attack game under the condition that $\mathcal{C}$ chooses β in Initialization phase, where the probability is taken over the random tapes of $\mathcal{A}$ and $\mathcal{C}$.

For a security parameter k and an adversary $\mathcal{A}$, we define $\mathrm{Adv}_{\mathcal{A}}(k)$ by

$$\mathrm{Adv}_{\mathcal{A}}(k) = \left| P^{1}_{\text{pparam-atk}}(k) - P^{2}_{\text{pparam-atk}}(k) \right|.$$

Definition 3.6 (pparam-security)**.** *A PPSS scheme $\mathcal{P}$ is (T, ϵ, q_A)-pparam-secure if for any security parameter k and any adversary $\mathcal{A}$, $\mathrm{Adv}_{\mathcal{A}}(k) < \epsilon$ holds under the following conditions:*

1. *$\mathcal{A}$ is allowed to enter Attack phase at most q_A times, and*

2. *the running time of $\mathcal{A}$ is at most T.*

Intuitively, a PPSS protocol is pparam-secure if no polynomial time adversary could determine, on any given two documents and any public parameter, which document is stored in the public parameter, even though he is allowed to adaptively receive sample pairs of the public parameter and the stored document.

We show that the protocol PPSS_2 [1] is not pparam-secure.

Proposition 3.8. *For the protocol* PPSS_2*, there exists a PPT adversary* $\mathcal{A}$ *such that* $\mathrm{Adv}_{\mathcal{A}}(k) = 1$*, that is, the protocol* PPSS_2 *is not* $(T, 1, 1)$*-pparam-secure.*

We next reveal the relationship between the pparam-security and the PPSS-security. We propose a protocol named Protocol 3.2 in this thesis, and show that the protocol is pparam-secure but not PPSS-secure.

Proposition 3.9. *Assume that the following properties hold:*

- *the protocol* PPSS_2 *is* $(T, \epsilon, 0)$*-pparam-secure, and*
- *the proof system* $(\mathcal{P}(\mathcal{L}_E^{\mathrm{pub}}), \mathcal{V}(\mathcal{L}_E^{\mathrm{pub}}))$ *used in Protocol 3.2 is* $(T_S, 1, q_H^S, \epsilon_{\mathrm{ZK}}, \epsilon_{\mathrm{SS}})$*-SS-NIZK.*

Then Protocol 3.2 is (T', ϵ', q_A)*-pparam-secure, where* $T' \leq T - T_S - q_A f_A$, $q_A \leq q_H^S$ and $\epsilon' \leq 2\epsilon + 6\epsilon_{\mathrm{SS}}$ *for some polynomial* f_A *in* n, t *and* k*.*

Proposition 3.10. *Protocol 3.2 is not PPSS-secure.*

Propositions 3.9 and 3.10 indicate that the pparam-security is independent of the PPSS-security in a sense that the pparam-security does not imply the PPSS-security in general and vice versa.

We then improve the protocol PPSS_2 by using the twin-encryption version of the ElGamal encryption scheme [4], and show that the improved protocol ePPSS_2 is pparam-secure.

Theorem 3.11. *Assume that the following properties hold:*

- *the protocol* PPSS_2 *is* $(T, \epsilon, 0)$*-pparam-secure, and*
- *the proof system* $(\mathcal{P}(\mathcal{L}_E^{\mathrm{pub}}), \mathcal{V}(\mathcal{L}_E^{\mathrm{pub}}))$ *used in the protocol* ePPSS_2 *is* $(T_S, 1, q_H^S, \epsilon_{\mathrm{ZK}}, \epsilon_{\mathrm{SS}})$*-SS-NIZK.*

Then the protocol ePPSS_2 *is* (T', ϵ', q_A)*-pparam-secure, where* $T' \leq T - T_S - q_A f_A$, $q_A \leq q_H^S$ and $\epsilon' \leq 2\epsilon + 6\epsilon_{\mathrm{SS}}$ *for some polynomial* f_A *in* n, t *and* k*.*

Theorem 3.12. *Assume that the following properties hold:*

- *the* DDH *problem is* $(T_{\mathrm{ddh}}, \epsilon_{\mathrm{ddh}})$*-hard,*
- *the proof systems* $(\mathcal{P}(\mathcal{L}_{S1}^{\mathrm{pub}}), \mathcal{V}(\mathcal{L}_{S1}^{\mathrm{pub}}))$, $(\mathcal{P}(\mathcal{L}_{U}^{\mathrm{pub}}), \mathcal{V}(\mathcal{L}_{U}^{\mathrm{pub}}))$ *and* $(\mathcal{P}(\mathcal{L}_{S2}^{\mathrm{pub},j}), \mathcal{V}(\mathcal{L}_{S2}^{\mathrm{pub},j}))$ *used in the protocol* PPSS_2 *are* $(T_S, q_P^S, q_H^S, \epsilon_{\mathrm{SS}}, \epsilon_{\mathrm{ZK}})$*-SS-NIZK, and*
- *the proof system* $(\mathcal{P}(\mathcal{L}_E^{\mathrm{pub}}), \mathcal{V}(\mathcal{L}_E^{\mathrm{pub}}))$ *is* $(T_S, 1, q_H^S, \epsilon_{\mathrm{SS}}, \epsilon_{\mathrm{ZK}})$*-SS-NIZK.*

Then the protocol ePPSS_2 *is* $(n, t, q_U, q_S, T, \epsilon)$*-PPSS-secure, where*

$$\max\{nq_U, q_S\} \leq q_P^S, q_H^S, \quad T \leq T_{\mathrm{ddh}} - 4T_S - q_U f^U - q_S f^S - f^I$$

for some polynomials f^U, f^S *and* f^I *in* n, t *and* k*, and*

$$\begin{aligned}\epsilon \leq\ & 8\epsilon_{\mathrm{ZK}} + (4nq_U q_S + 6nq_U - 4nq_S + 6q_S)\epsilon_{\mathrm{SS}} + (2q_U q_S + 3q_U + 2q_S + 7)\epsilon_{\mathrm{ddh}} \\ & + \frac{36 q_U q_S (q-1)}{q^2} + \frac{8q_U(4q^2 - 5q + 2)}{q^3} + \frac{q_S(13q^3 - 32q^2 + 42q - 16)}{q^4} + \frac{3}{q}.\end{aligned}$$

4 Password-Protected Secret Sharing Scheme without Random Oracles

In this chapter, we propose a PPSS scheme sPPSS, and show that the protocol is PPSS-secure and pparam-secure in the standard model.

Theorem 4.3. *The encryption scheme of Libert and Yung [5] is (T, ϵ, q_A)-IND-CCA secure, then the protocol* sPPSS *is (T', ϵ, q_A)-pparam-secure, where $T' \leq T - q_A f_A$ for some polynomial f_A in n, t and k.*

Theorem 4.4. *Assume that the following properties hold:*

- *the DLIN problem is $(T_{\text{DLIN}}, \epsilon_{\text{DLIN}})$-hard,*
- *the SD problem is $(T_{\text{SD}}, \epsilon_{\text{SD}})$-hard,*
- *the proof systems $(\mathcal{P}(\mathcal{L}_{S1}^{\text{pub}}), \mathcal{V}(\mathcal{L}_{S1}^{\text{pub}}))$, $(\mathcal{P}(\mathcal{L}_{U}^{\text{pub}}), \mathcal{V}(\mathcal{L}_{U}^{\text{pub}}))$ and $(\mathcal{P}(\mathcal{L}_{S2}^{\text{pub},j}), \mathcal{V}(\mathcal{L}_{S2}^{\text{pub},j}))$ used in the protocol* sPPSS *are $(T_S, q_P^S, \epsilon_{\text{SS}}, \epsilon_{\text{ZK}})$-SS-NIZK, and*
- *a signature scheme Σ chosen in Step 5 of* Setup *of the protocol* sPPSS *is a one-time signature.*

Then the protocol sPPSS *is $(n, t, q_U, q_S, T, \epsilon)$-PPSS-secure, where*

$$\max\{nq_U, q_S\} \leq q_P^S,\ T \leq \max\{T_{\text{SD}}, T_{\text{DLIN}}\} - 3T_S - q_U f^U - q_S f^S - f^I,$$

for some polynomials f^U, f^S and f^I in n, t and k, and

$$\epsilon \leq 6\epsilon_{\text{ZK}} + 9\epsilon_{\text{SD}} + (2n(q_U - 1)q_S + 2q_U + 1)\epsilon_{\text{DLIN}} + 2n((q_U - 1)q_S + 2q_U)\epsilon_{\text{SS}} + \omega(k),$$

where ω is negligible in k.

5 Conclusion

In this thesis, we have explored securer PPSS schemes, and proposed some protocols.

In Chapter 3, we have investigated security notions for PPSS schemes. First, we first have proposed another security notion for PPSS schemes, named pparam-security. The pparam-security intuitively means that any public parameter does not include any clue to the stored document in a way that an adversary could recognize. We have shown that the protocol PPSS_2 proposed in [1] is not pparam-secure. We then have given a protocol which is pparam-secure but not PPSS-secure. These results indicate that the pparam-security is logically independent of the PPSS-security in a sense that the pparam-security does not imply the PPSS-security in general and vice versa. Finally we have proposed the enhanced protocol ePPSS_2, and shown that ePPSS_2 is pparam-secure and PPSS-secure. This protocol is the first protocol which is both PPSS-secure and pparam-secure.

In Chapter 4, we have proposed the protocol sPPSS which is both pparam-secure and PPSS-secure in the standard model. All the known PPSS protocols, including ePPSS_2, are provably secure in the random oracle model. The protocol sPPSS is, to our best knowledge, the first PPSS protocol which is secure in the standard model.

References

[1] A. Bagherzandi, S. Jarecki, N. Saxena and Y. Lu, "Password-Protected Secret Sharing," Proc. CCS'11, pp.433-444, 2011.

[2] J. Camenisch, A. Lysyanskaya and G. Neven, "Practical Yet Universally Composable Two-Server Password-Authenticated Secret Sharing," Proc. CCS'12, pp.525–536, 2012.

[3] J. Camenisch, A. Lehmann, A. Lysyanskaya and G. Neven, "Memento: How to Reconstruct Your Secrets from a Single Password in a Hostile Environment," CRYPTO'14, LNCS, vol.8617, pp.256-275, Springer, 2014.

[4] P. A. Fouque and D. Pointcheval, "Threshold Cryptosystems Secure against Chosen-Ciphertext Attacks," ASIACRYPT'01, LNCS, vol.2248, pp.351-368, Springer, 2001.

[5] B. Libert and M. Yung, "Non-interactive CCA-secure Threshold Cryptosystems with Adaptive Security: New Framework and Constructions," TCC'12, LNCS, vol.7194, pp.75–93, 2012.

論文審査結果の要旨

いわゆるクラウド・コンピューティング環境においてストレージ・サービスを提供するサイトは、サイバー攻撃によるファイルの流出や、ハードウェア障害によるファイルの消失などの危険を常に抱えているため、利用者側にもセキュリティ対策が必要である。そこで、単一のパスワードで保護されたファイルを複数のサイトに分散して保存することにより、いくつかのサイトで流出が発生してもファイルは秘密に保たれ、またいくつかのサイトでデータが消失しても正当な利用者ならファイルを復元できる技術が考案された。これがパスワード付秘密分散共有(PPSS)方式である。著者は現代の情報社会で有用なこの技術に着目し、既存方式の安全性の再検討を通じて、より安全な方式の構築に取り組んできた。本論文は、その成果をまとめたものであり、全編5章からなる。

第1章は序論である。

第2章は、概念や記号の定義と説明に充てた準備の章である。

第3章では、既存の方式の安全性を再検討し、より安全な新しい方式を安全性証明とともに与えている。まず、既存の方式が満足している基本的安全性だけでは対応できそうもない状況が存在することを指摘し、その状況に対抗できる安全性を定式化して「公開パラメータ安全性」と名付け、実際、既存の方式が公開パラメータ安全性を満たしていないことを証明した。さらに、公開パラメータ安全性は満たすが基本的安全性は満たさない方式例を与えることで、二つの安全性概念が片方に包含される関係にはないことを示した。以上を踏まえて新しいPPSS方式を提案し、判定版Diffie-Hellman問題が困難であるとの仮定のもと、それが基本的安全性と公開パラメータ安全性の両方を満たすことを証明した。これらの結果は、PPSS方式の安全性に関する従来の理論を革新するものとして高く評価できる。

第4章では、条件が厳しい枠組みの中でも安全と証明できる方式を提案している。第3章における安全性証明は、ランダム・オラクル・モデルと呼ばれる理想的な枠組みでのものであった。これに対して、より現実に近い標準モデルと呼ばれる枠組みがあり、一般に、前者で安全と証明されても後者では安全とは言えない。ここでは、部分群判定問題と指数の線形性判定問題が困難であるとの仮定のもと、標準モデルの枠組みで基本的安全性と公開パラメータ安全性の両方を証明できる初めてのPPSS方式を提案しており、理論上、興味深い結果を与えている。

第5章は結論である。

以上、要するに本論文は、PPSS方式に対する新たな安全性概念を見出して定式化するとともに、その安全性と従来の安全性のどちらも満足する方式の存在を構成的に証明することでPPSS方式の理論を深化させたものであり、情報基礎科学及び暗号理論の発展に寄与するところが少なくない。

よって、本論文は、博士（情報科学）の学位論文として合格と認める。