Vol.2022-DPS-190 No.22
Vol.2022-CSEC-96 No.22
2022/3/10

同種写像問題に基づくパスワードベース認証付き鍵共有について

岡村貴仁 [1]　有田正剛 [1]

概要：現在の公開鍵暗号化スキームの多くは、離散対数問題に基づいている。しかし、量子計算機が出現すると、量子アルゴリズムを使用して簡単に破れる。そこで、量子計算機に対応可能な難問として、同種写像問題が注目されている。同種写像問題は、離散対数問題と数学的構造としては似ている為、暗号設計上、同じように扱えることが期待できる。同種写像問題を用いた量子計算機に対応可能な鍵共有方式として、CSIDH が提案されている。本論文では、暗号通信において一般的に使われている認証付き鍵共有の中で、CSIDH を用いたパスワードベースの認証付き鍵共有に注目し、研究する。CSIDH を用いたパスワードベースの認証付き鍵共有に対するオフライン辞書攻撃の危険性を提示し、オフライン辞書攻撃に対応可能な改良案を提案する。

キーワード：同種写像問題，CSIDH，パスワードベース認証付き鍵共有，オフライン辞書攻撃

Study on Password-based Key Agreement Protocol using The Isogeny Problem

TAKAHITO OKAMURA[1]　SEIKO ARITA [1]

Abstract: Many of the current public key encryption schemes are based on the discrete logarithm problem. However, with the advent of quantum computers, they can be easily broken using quantum algorithms. Therefore, the isogeny problem is attracting attention as a difficult problem that can be handled by quantum computers. The isogeny problem has a similar mathematical structure to the discrete logarithm problem, so it can be treated in the same way in cryptographic design. CSIDH has been proposed as a key sharing scheme for quantum computers using the homomorphic mapping problem. In this paper, we focus on password-based authenticated key sharing using CSIDH among the commonly used authenticated key sharing schemes for cryptographic communication. We present the dangers of offline dictionary attacks on password-based authenticated key sharing using CSIDH and propose possible improvements to cope with offline dictionary attacks.

Keywords: Homogeneous mapping problem, CSIDH, Password-based authenticated key sharing, Offline dictionary attacks

1. はじめに

現在の公開鍵暗号化スキームの多くは、離散対数問題に基づいている。代表的な公開鍵暗号としては、Diffie-Hellman 鍵交換方式や楕円曲線暗号がある。しかし、これら離散対数問題に基づいた公開鍵暗号は、量子計算機が出現すると、量子アルゴリズムを使用して簡単に破れる。そこで、量子計算機に対応可能な難問として、同種写像問題が注目されている。同種写像とは、楕円曲線と楕円曲線の間の写像である。同種写像問題は、離散対数問題と数学的構造としては似ている為、暗号設計上、同じように扱えることが期待される。同種写像問題を用いた量子計算機に対応可能な Diffie-Hellman タイプの鍵交換方式としては、CSIDH[1]が提案されている。

また、Diffie-Hellman 鍵交換方式など、インターネット上で暗号通信を行う際には、常に攻撃者から盗聴や改ざんが行われる危険性がある。こうした攻撃を防ぐ為に一般的に用いられているのが、通信相手の認証を行った上で暗号化した鍵を共有し、通信を行う認証付き鍵共有である。

本研究では、認証付き鍵共有の中で、CSIDH を用いたパスワードベースの認証付き鍵共有に注目し、研究する。CSIDH を用いたパスワードベースの認証付き鍵共有に対するオフライン辞書攻撃の危険性を提示し、提示したオフライン辞書攻撃に対応可能な改良案を研究する。

2. 準備

2.1 同種写像

楕円曲線とは、$4A^3 + 27B^2 \neq 0$である、$A, B \in \mathbb{F}_q$について

$$y^2 = x^3 + Ax + B$$

で定義される代数曲線をいう。ここで、$\mathbb{F}_q$は位数qの有限体である。

楕円曲線E_1からE_2への射$\varphi : E_1 \rightarrow E_2$が$\varphi(0_{E_1}) = (0_{E_2})$を満たすとき、射$\varphi$を同種写像という。同種写像は群準同型となる。

1 情報セキュリティ大学院大学
Graduate School of Information Security

Vol.2022-DPS-190 No.22
Vol.2022-CSEC-96 No.22
2022/3/10

以下に同種写像の例を示す。

例：
まず、$\mathbb{F}_q$上の点A, Bを$B \neq 0,\ D = A^2 - 4B \neq 0$とする。
また、楕円曲線Eを$y^2 = x(x^2 + Ax + B)$、E'を$Y^2 = X(X^2 - 2AX + D)$と定義する。
同種写像φは$E \to E'$への同種写像である。

$\varphi(x, y) = \left(\frac{y^2}{x^2}, \frac{y(B-x^2)}{x^2}\right) = \left(\frac{x(x^2+Ax+B)}{x^2}, \frac{y(B-x^2)}{x^2}\right)$となり、

同種写像φのカーネル$\ker(\varphi)$は、 $\ker(\varphi) = \{0_E, (0,0)\}$である。
同種写像φの次数は$\deg\phi = 2$となる。

2.2 同種写像問題

素数pと定数gが与えられたとき、$y = g^a \bmod p$からaを求める問題を離散対数問題という。

一方で、同種写像問題は、楕円曲線Eとそれに同種である楕円曲線E'から、同種写像$\varphi: E \to E'$を求める問題である。

図 1 に示すように、離散対数問題と同種写像問題は数学的構造としては似ている為、暗号設計上、同じように扱えることが期待できる。

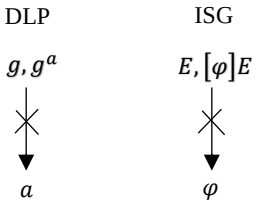

図 1　離散対数問題と同種写像問題
Figure 1　Discrete logarithm problem and isogeny problem

2.3 同種写像とイデアルの関係[2]

$p \equiv 3 \bmod 4$を 3 より大きい素数とする。$\mathbb{F}_p$上のモンゴメリ曲線Eとして、方程式$y^2 = x^3 + Ax^2 + x$(ここで、$A \in \mathbb{F}_p \setminus \{\pm 2\}$)を定義する。

有限体$\mathbb{F}_q$上の楕円曲線Eに対して不変量tを$t = q + 1 - \#E(\mathbb{F}_q)$と定義する。この$t$に対して$p|t$が成り立つ時$E$を超特異（supersingular）であるという。$\overline{\mathbb{F}}_q$上の超特異楕円曲線は全て$\mathbb{F}_{q^2}$上で定義されることが知られている[4]。

Eを$\mathbb{F}_p$で定義された超特異楕円曲線とし、πをEのフロベニウス自己準同型とする。Eの$\mathbb{F}_p$自己準同型環$\mathcal{O}$は、

$\mathbb{Z}[\pi]$または$\mathbb{Z}\left[\frac{1+\pi}{2}\right]$ のいずれかと同型である。

すべてのイデアルが単項イデアルであるような整数環を単項イデアル整域といい、単項イデアル整域からどれだけ離れているかを測るものをイデアル類群という[5]。

イデアル類群$\mathrm{cl}(\mathcal{O})$は、$\mathbb{F}_p$自己準同型環$\mathcal{O}$を持つ超特異楕円曲線の集合$\mathcal{E}\ell\ell_p(\mathcal{O})$に作用する。

$$\mathrm{cl}(\mathcal{O}) \times \mathcal{E}\ell\ell_p(\mathcal{O}) \to \mathcal{E}\ell\ell_p(\mathcal{O})$$
$$([\mathfrak{a}], E) \mapsto [\mathfrak{a}]E = E/E[\mathfrak{a}]$$

ここで、$E[\mathfrak{a}] = \cap_{\alpha \in \mathfrak{a}} \ker\alpha$である。

3. 同種楕円曲線の計算

アルゴリズム 1[1]に示すように、超特異である$E: Y^2Z = X^3 + aX^2Z + XZ^2$ 、整数のリスト$(e_1, \ldots, e_n)$を入力し、$\left[\mathfrak{l}_1^{e_1}, \cdots, \mathfrak{l}_n^{e_n}\right]E$ のモンゴメリ係数を出力する。
ここで、$\mathbb{Z}[\pi_p]$の整イデアル$\mathfrak{l}_i\ (i = 1, \ldots, n)$を$(l_i, \pi_p - 1)$とし、 $\mathbb{Z}[\pi_p]$の整イデアル$\bar{\mathfrak{l}}_i\ (i = 1, \ldots, n)$を $(l_i, \pi_p + 1)$とする。l_iは小さな素数である。

アルゴリズム 1 の概略図として、図 2 では、まず$\mathfrak{l}_1$でE_aから$E_{a'}$へ、$\mathfrak{l}_2$で$E_{a'}$から$E_{a''}$へ、以後同様に同種写像を写していき、最終的に$[\mathfrak{a}]$でE_aから同種写像を写した結果である$[\mathfrak{a}]E_a$へと辿り着く。

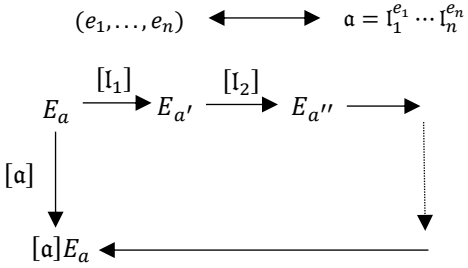

図 2　アルゴリズム 1 の概略図
Figure 2　Schematic of Algorithm 1

Vol.2022-DPS-190 No.22
Vol.2022-CSEC-96 No.22
2022/3/10

アルゴリズム 1：同種楕円曲線の計算

Algorithm1: Computation of isogeneous elliptic curves

入力: 超特異である$E: Y^2Z = X^3 + aX^2Z + XZ^2$、整数のリスト $(e_1, \ldots, e_n)$
出力:$[\mathfrak{l}_1^{e_1} \cdots \mathfrak{l}_n^{e_n}]E$ のモンゴメリ係数

ここで、$\mathbb{Z}[\pi_p]$の整イデアル$\mathfrak{l}_i\ (i = 1, \ldots, n)$ を $(l_i, \pi_p - 1)$ にし、 $\mathbb{Z}[\pi_p]$の整イデアル$\bar{\mathfrak{l}_i}\ (i = 1, \ldots, n)$を $(l_i, \pi_p + 1)$とする。
l_iは小さな素数である。

1. あるiについて$e_i \neq 0$である間：
2. ランダムに選んだ $x \in \mathbb{F}_p$ をサンプリングする。:
3. $x(P) \leftarrow x$
4. $x^3 + ax^2 + x$が$\mathbb{F}_p$の平方の場合は、$s \leftarrow +1$を設定する。それ以外の場合は、$s \leftarrow -1$を設定する。:
5. $S = \{i \mid sign(e_i) = s\}$とする：
6. $S = \emptyset$の場合：
7. 2 行目に戻る
8. そうでない場合：
9. $k \leftarrow \prod_{i \in S} \ell_i$, $x(P) \leftarrow x(((p + 1)/k)P)$
10. 全ての$i \in S$について：
11. $x(Q) \leftarrow x((k/\ell_i)P)$
12. $Q \neq (0:1:0)$の場合：
13. ℓ_i 同種写像φを計算する
φ:ker $\varphi = \langle Q \rangle$を持つ$E_a \to E_{a'}$, $E_a: Y^2Z = X^3 + aX^2Z + XZ^2$
14. $a \leftarrow a'$, $x(P) \leftarrow x(\varphi(P))$, $k \leftarrow k/\ell_i$, $x(P_0) \leftarrow x(\varphi(P_0))$, $e_i \leftarrow e_i - s$
15. end if(13 行目)
16. end for(11 行目)
17. end while(2 行目)
18. モンゴメリ係数aを返す

4. CSIDH[1]

CSIDH(Commutative Supersingular Isogeny Diffie-Hellman)(図 3)は、イデアル類群の超特異楕円曲線の集合への群作用を用いて鍵共有を実現する、同種写像を用いた Diffie-Hellman タイプの鍵交換スキームである（2.3 節を参照)。

1. pを$p = 4 \cdot \ell_1 \cdots \ell_n - 1$を満たす素数にする。ここで、$\ell_1, \cdots, \ell_n$は小さな異なる奇素数である。
2. pと$E_0 : Y^2Z = X^3 + XZ^2$ を公開パラメータにする。
3. $\{-m, \cdots, m\}^n$から整数ベクトル $(e_1, \ldots, e_n)$をランダムに選択する。ここで、整数ベクトル（$e_1, \ldots, e_n$）は秘密鍵である。
4. アリスは$[\mathfrak{a}] = [\mathfrak{l}_1^{e_{A_1}} \cdots \mathfrak{l}_n^{e_{A_n}}] \in \mathrm{cl}(\mathbb{Z}[\pi_p])$を選ぶ。ここで、$\mathfrak{l}_i = (l_i, \pi_p - 1)$ である。アリスは公開鍵$E_A = [\mathfrak{a}]E_0$を計算する。
5. ボブは$[\mathfrak{b}] = [\mathfrak{l}_1^{e_{B_1}} \cdots \mathfrak{l}_n^{e_{B_n}}] \in \mathrm{cl}(\mathbb{Z}[\pi_p])$を選ぶ。ここで、$\mathfrak{l}_i = (l_i, \pi_p - 1)$ である。ボブは公開鍵$E_B = [\mathfrak{b}]E_0$を計算する。
6. アリスは、ボブの公開鍵を適用して、$E_{AB} = [\mathfrak{a}]E_B$を得る。
7. ボブは、アリスの公開鍵を適用して、$E_{BA} = [\mathfrak{b}]E_A$を得る。
8. 共有秘密は、最終曲線の曲線係数、$E_{AB} = E_{BA}$である。

	Alice	Bob
秘密鍵	$[\mathfrak{a}] = [\mathfrak{l}_1^{e_{A_1}} \cdots \mathfrak{l}_n^{e_{A_n}}] \in \mathrm{cl}(\mathbb{Z}[\pi_p])$	$[\mathfrak{b}] = [\mathfrak{l}_1^{e_{B_1}} \cdots \mathfrak{l}_n^{e_{B_n}}] \in \mathrm{cl}(\mathbb{Z}[\pi_p])$
公開鍵	$E_A = [\mathfrak{a}]E_0$	$E_B = [\mathfrak{b}]E_0$

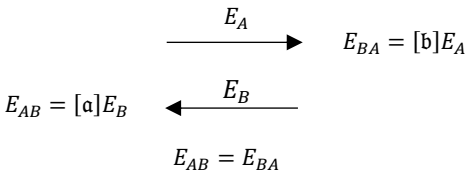

図 3　CSIDH
Figure 3　CSIDH

5. 認証付き鍵共有

Diffie-Hellman 鍵交換方式など、インターネット上で暗号通信を行う際には、常に攻撃者から盗聴や改ざんが行われる危険性がある。こうした攻撃を防ぐ為に一般的に用いられているのが、通信相手の認証を行った上で暗号化した鍵を共有し、通信を行う認証付き鍵共有である。

認証付き鍵共有として研究が行われているものには、主に二つの方式がある。一つが、PKI ベースの鍵共有と呼ばれる、認証基盤として公開鍵インフラストラクチャ（PKI）を利用する鍵共有方式で、もう一つが、パスワードベースの認証付き鍵共有(PAKE)と呼ばれる認証としてパスワードを用いる鍵共有方式である。その他にも、ID ベースの暗号や認証を用いた ID ベースの認証付き鍵共有などの方式が研究されている[5]。

一例として、STS（Station-to-Stasion）プロトコルと呼ばれる認証鍵プロトコルを紹介する[7]。このプロトコルの基本バージョンでは、鍵の確立に使用されるパラメータは固定されており、すべてのユーザーが知っていると仮定する。また、ここでは、Alice が Bob の公開鍵を知っており、その逆も同様であると仮定している。

図 4 に示すように、

1. Alice が乱数xを作成し、α^xを Bob に送信する。
2. Bob は乱数yを作成し、セッション鍵$K = \alpha^{xy}$を計算する。
3. Bob は、α^yと、適切な対象暗号化アルゴリズムE（すなわち、$E_K(s_B\{\alpha^y, \alpha^x\})$）を用いて、$K$で暗号化された自分の署名からなるトークンをを返信する。
4. Alice はKを計算し、Kを使ってトークンを復号化し、Bob の公開鍵を使って Bob の署名を検証する。
5. Alice は Bob に、暗号化された署名である$E_K(s_A\{\alpha^x, \alpha^y\})$を送信する。
6. 最後に、Bob は同様にKと Alice の公開鍵を使って Alice の暗号化された署名を検証する。

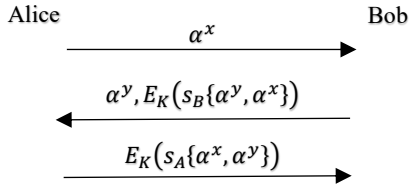

図 4　STS プロトコル
Figure 4　STS protocol

5.1 Kawashima らによる鍵共有スキーム$\prod_{\mathrm{CSIDH}}$[7]

Kawashima ら[7]によって提案された$\prod_{\mathrm{CSIDH}}$は、古典的な Diffie-Hellman の代わりに Diffie-Hellman タイプの鍵交換スキーム CSIDH を使用するため、量子耐性が期待される。

図 5 のようになるが、公開鍵である$\mathfrak{A}$、$\mathfrak{B}$といった長期的な鍵と、$\mathfrak{R}$、$\mathfrak{S}$といった一時的な鍵を組み合わせることで、認証付きの鍵が得られる仕組みとなっている。

$\prod_{\mathrm{CSIDH}}$の安全性としては、CSIDH のギャップ問題がランダム自己帰着性を持つことに基づいている。

p : CSIDH の素数

$$E \in \mathcal{EB}_p(\mathcal{O})\left(\mathcal{O} = \mathbb{Z}\left[\sqrt{-p}\right]\right)$$

	Alice	Bob
秘密鍵	$[\mathfrak{a}] \leftarrow cl(\mathcal{O})$	$[\mathfrak{b}] \leftarrow cl(\mathcal{O})$
公開鍵	$\mathfrak{A} = [\mathfrak{a}]E$	$\mathfrak{B} = [\mathfrak{b}]E$
	$[\mathfrak{r}] \leftarrow cl(\mathcal{O})$	$[\mathfrak{s}] \leftarrow cl(\mathcal{O})$
	$\mathfrak{R} = [\mathfrak{r}]E$	$\mathfrak{S} = [\mathfrak{s}]E$

$$k \leftarrow H\begin{pmatrix} ctxt \parallel \mathcal{M}([\mathfrak{a}]\mathfrak{S}) \parallel \\ \mathcal{M}([\mathfrak{r}]\mathfrak{B}) \parallel \\ \mathcal{M}([\mathfrak{r}]\mathfrak{S}) \end{pmatrix} \quad \mathfrak{S} \quad k \leftarrow H\begin{pmatrix} ctxt \parallel \mathcal{M}([\mathfrak{s}]\mathfrak{A}) \parallel \\ \mathcal{M}([\mathfrak{b}]\mathfrak{R}) \parallel \\ \mathcal{M}([\mathfrak{s}]\mathfrak{R}) \end{pmatrix}$$

$$ctxt = \hat{A} \parallel \hat{B} \parallel \mathcal{M}(\mathfrak{A}) \parallel \mathcal{M}(\mathfrak{B}) \parallel \mathcal{M}(\mathfrak{R}) \parallel \mathcal{M}(\mathfrak{S})$$

図 5　認証付き鍵共有$\prod_{\mathrm{CSIDH}}$
Figure 5　Authenticated key sharing $\prod_{\mathrm{CSIDH}}$

6. パスワードベースの認証付き鍵共有(PAKE)

認証鍵共有では、認証用に鍵を生成し用いる。パスワードベースの認証鍵共有では、認証にパスワードを使用する。このパスワードを知っているのはユーザーと共有に使うサーバーのみである。また、一般的にパスワードを直接保存する代わりにパスワードにハッシュ関数を適用したハッシュ値を保存する。パスワードを直接保存するのではなく、ハッシュ値を保存する理由は、悪意ある攻撃者に見られたとしてもパスワードが分からないようにする為である。パスワードベースの認証鍵共有の課題として、オフライン辞書攻撃によって、パスワードが解読されてしまう可能性があり、オフライン辞書攻撃を防ぐことが重要である。

実用性を考えると、認証鍵共有スキームに加えて、パスワードベースの認証鍵共有スキームが望まれるが、安全性証明のついた CSIDH ベースの認証鍵共有スキームはまだ確立していない。

6.1 オフライン辞書攻撃

辞書に書かれたパスワードのハッシュ値と、入手したパスワードデータのハッシュ値を順番に照合し、一致するものがあればそのハッシュ値に対応するパスワードが求められる攻撃である。直接辞書に書かれたハッシュ関数のみならず、ユーザーから漏洩したセッション鍵を対象とすることも考えられる。

7. CSIDH を用いたパスワードベースの認証付き鍵共有

CSIDH を用いたパスワードベースの認証付き鍵共有としては、最初の試みとして図 6 のような方式が考えられる。認証用に使うパスワードはπとする。

1. Alice は$[\mathfrak{a}] = \left[\mathfrak{l}_1^{e_{A_1}} \cdots \mathfrak{l}_n^{e_{A_n}}\right] \in \mathrm{cl}\left(\mathbb{Z}\left[\pi_p\right]\right)$を選ぶ。ここで、$\mathfrak{l}_i = (\mathfrak{l}_i, \pi_p - 1)$ である。
2. Bob は$[\mathfrak{b}] = \left[\mathfrak{l}_1^{e_{B_1}} \cdots \mathfrak{l}_n^{e_{B_n}}\right] \in \mathrm{cl}\left(\mathbb{Z}\left[\pi_p\right]\right)$を選ぶ。ここで、$\mathfrak{l}_i = (\mathfrak{l}_i, \pi_p - 1)$ である。
3. 選んだ秘密鍵$[\mathfrak{a}]$を用いて、Alice は公開鍵$E_A = [\mathfrak{a}]E_0$を計算し、Bob にE_Aを送信する。
4. 選んだ秘密鍵$[\mathfrak{b}]$を用いて、Bob は公開鍵$E_B = [\mathfrak{b}]E_0$を計算し、Alice にE_Bを送信する。
5. Alice はE_Bを用いて、$E_{AB} = [\mathfrak{a}]E_B$を計算する。
6. Bob はE_Aを用いて、$E_{BA} = [\mathfrak{b}]E_A$を計算する。
7. パスワードπを用いて Alice はセッション鍵$K_{AB} = KDF(E_A, E_B, E_{AB}, \pi)$を得る。
8. パスワードπを用いて Bob はセッション鍵$K_{BA} = KDF(E_A, E_B, E_{BA}, \pi)$を得る。
9. 共有秘密が$K_{AB} = K_{BA}$となり、認証付き鍵共有が成立する。

Vol.2022-DPS-190 No.22
Vol.2022-CSEC-96 No.22
2022/3/10

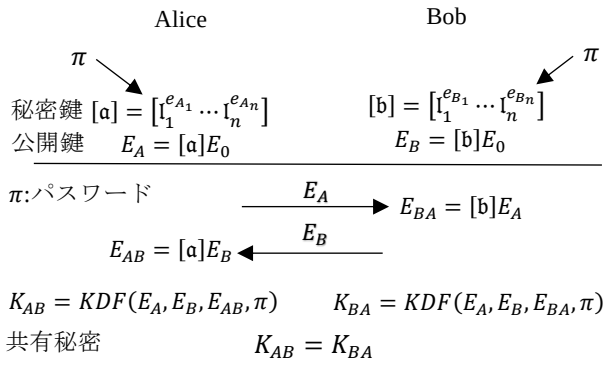

図 6　CSIDH を用いたパスワードベースの認証付き鍵共有

Figure 6　Password-based using CSIDH Authenticated key sharing

7.1 オフライン辞書攻撃の危険性

図 7 のような方式では、図 8 のようにオフライン辞書攻撃が発生してしまう。

まず、攻撃者$\mathcal{A}$は Alice と仮のパスワードπ'を用いてセッションを実行する。

Alice は正しいセッション鍵$K_{AB} = \mathrm{KDF}(E_A, E_B, E_{AB}, \pi)$を得る。

次に、攻撃者$\mathcal{A}$は Alice のセッション鍵K_{AB}を入手したとする。

攻撃者$\mathcal{A}$は各パスワード候補τを用いて$K_{BA}' = \mathrm{KDF}(E_A, E_B, E_{BA}, \tau)$を計算する。

$\mathrm{K_{AB}} = \mathrm{K_{BA}}'$となれば$\tau = \pi$であり攻撃は成立する。不成立ならば攻撃者$\mathcal{A}$は改めてパスワード候補を推測し、繰り返す。

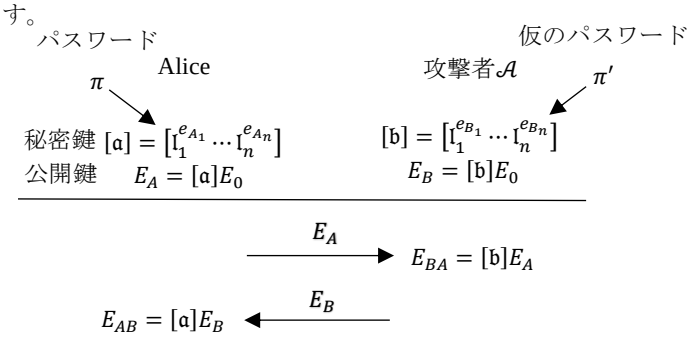

図 7　CSIDH を用いたパスワードベースの認証付き鍵共有へのオフライン辞書攻撃

Figure 7　Offline Dictionary Attack on Password-based using CSIDH Authenticated key sharing

7.2 Terada らの CSIDH を用いたパスワードベースの認証付き鍵共有[8]

前節までの方式では、オフライン辞書攻撃が発生してしまう為、Terada ら[8]によって別の CSIDH を用いたパスワードベースの認証付き鍵共有が提案されている。図 8 に示す。

1. Alice は$[\mathfrak{a}] = \left[\mathfrak{l}_1^{e_{A_1}} \cdots \mathfrak{l}_n^{e_{A_n}}\right]$を選択し、$E_A = [\mathfrak{a}]E_0$を計算し、Bob にパスワード$\pi$で暗号化したメッセージ$\hat{A} = Enc_\pi(E_A)$を送信する。

2. Bob は$[\mathfrak{b}] = \left[\mathfrak{l}_1^{e_{B_1}} \cdots \mathfrak{l}_n^{e_{B_n}}\right]$を選択し、$E_B = [\mathfrak{b}]E_0$を計算し、Alice にパスワード$\pi$で暗号化したメッセージ$\hat{B} = Enc_\pi(E_B)$を送信する。

3. Alice は$E_B = Enc_{pw}^{-1}(E_B)$を復号化し、共有秘密$[\mathfrak{a}]E_B$を計算する。

4. Bob は$E_A = Enc_{pw}^{-1}(E_A)$を復号化し、共有秘密 $[\mathfrak{b}]E_A$を計算する。

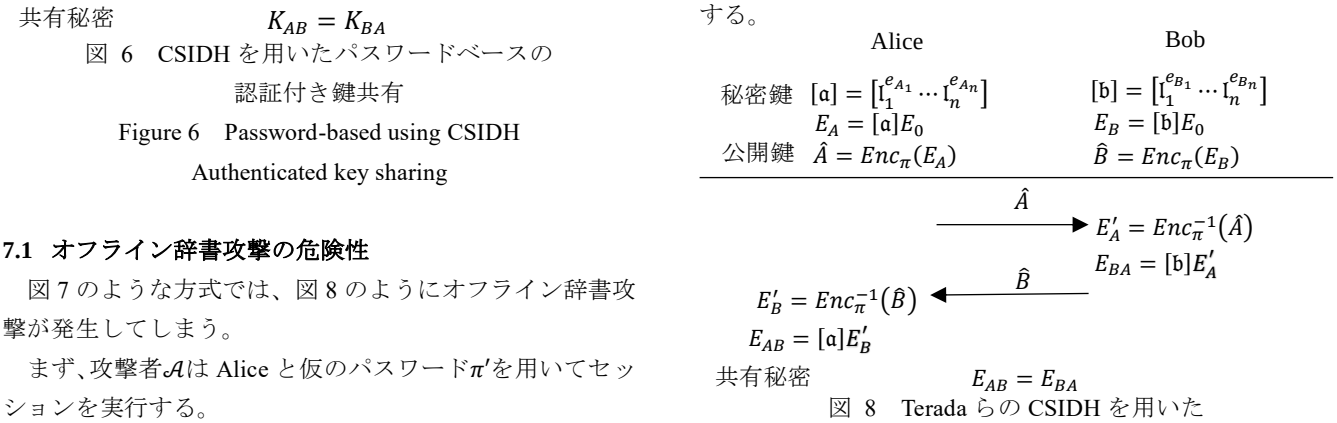

図 8　Terada らの CSIDH を用いたパスワードベースの認証付き鍵共有

Figure 8　Password-based key sharing with authentication using CSIDH by Terada et al.

7.3 Terada らの方式へのオフライン辞書攻撃の危険性

前節で説明した Terada らの CSIDH を用いたパスワードベースの認証付き鍵共有にも、Azarderakhsh ら[9]によってオフライン辞書攻撃の危険性が存在すると示されている。

まず、図 9 に示すように、攻撃者$\mathcal{A}$は Alice が Bob に対して送信しているメッセージ$\hat{A}$を観察する。

攻撃者$\mathcal{A}$は仮のパスワードπ'を用いてE_Aを復号化する。

$$E_A = Enc_{\pi'}^{-1}(\hat{A})$$

この時、攻撃者$\mathcal{A}$は、パスワードごとに$E_A = Enc_{\pi'}^{-1}(\hat{A})$が超特異楕円曲線であるかを確認する。条件が満たされるまで仮のパスワードを変えながら攻撃を繰り返し、条件が満たされた場合、オフライン辞書攻撃が成立する：$\pi' = \pi$。

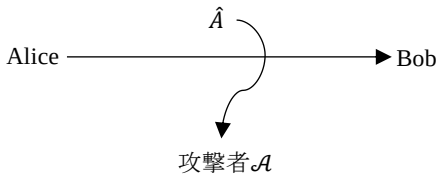

図 9　Terada らの方式へのオフライン辞書攻撃

Figure 9　Offline dictionary attack on the method of Terada et al.

8. オフライン辞書攻撃に対応する為の改良案

6 章で説明したオフライン辞書攻撃を防ぐ為には、Alice と Bob が共有しているE_{AB}にもパスワードπが必要にしな

Vol.2022-DPS-190 No.22
Vol.2022-CSEC-96 No.22
2022/3/10

ければならない。そこで、公開鍵にパスワードπを組み込み、それを共有する改良案を 2 つ提案する。

8.1 CSIDH を用いたパスワードベースの認証付き鍵共有の改良案 1

図 10 に示すように、認証用に使うパスワードはπとする。ハッシュ関数$H:\{0,1\}^* \to cl(\mathbb{Z}[\pi_p])$を用意する。

1. Alice は$[\mathfrak{a}] = [\mathfrak{l}_1^{e_{A_1}} \cdots \mathfrak{l}_n^{e_{A_n}}] \in \mathrm{cl}(\mathbb{Z}[\pi_p])$を選択し、$E_A = H(\pi)[\mathfrak{a}]E_0$を計算し、Bob に$E_A$を送信する。
2. Bob は$[\mathfrak{b}] = [\mathfrak{l}_1^{e_{B_1}} \cdots \mathfrak{l}_n^{e_{B_n}}] \in \mathrm{cl}(\mathbb{Z}[\pi_p])$を選択し、$E_B = H(\pi)[\mathfrak{b}]E_0$を計算し、Alice に$E_B$を送信する。
3. Alice はE_Bを用いて、$E_{AB} = [\mathfrak{a}]E_B$を計算する。
4. Bob はE_Aを用いて、$E_{BA} = [\mathfrak{b}]E_A$を計算する。
5. パスワードπを用いて Alice はセッション鍵$K_{AB} = KDF(E_A, E_B, E_{AB}, \pi)$を得る。
6. パスワードπを用いて Bob はセッション鍵$K_{BA} = KDF(E_A, E_B, E_{BA}, \pi)$を得る。
7. 共有秘密が$K_{AB} = K_{BA}$となり、認証付き鍵共有が成立する。

ハッシュ関数
$H:\{0,1\}^* \to cl(\mathbb{Z}[\pi_p])$

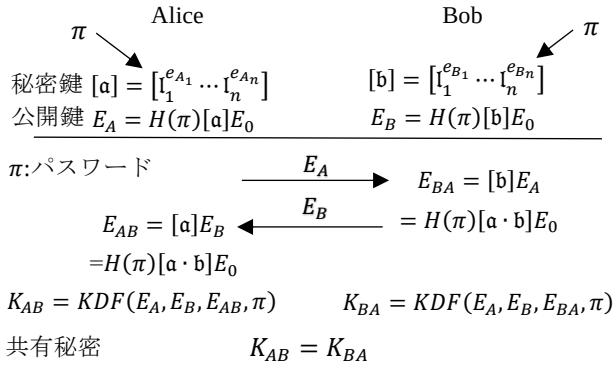

図 10 CSIDH を用いたパスワードベースの認証付き鍵共有の改良案 1

Figure 10 Proposed improvements to password-based authenticated key sharing using CSIDH 1

8.2 改良案 1 のオフライン辞書攻撃への安全性の考察

図 11 に示すように

1. 攻撃者$\mathcal{A}$は Alice と仮のパスワードπ'を用いてセッションを実行する。
2. Alice はセッション鍵$\mathrm{K_{AB}} = \mathrm{KDF}(\mathrm{E_A}, \mathrm{E'_B}, \mathrm{E'_{AB}}, \pi)$を入手する。
3. 攻撃者$\mathcal{A}$は Alice のセッション鍵$K_{AB} = \mathrm{KDF}(E_A, E'_B, E'_{AB}, \pi)$を入手したとする。
4. 攻撃者$\mathcal{A}$はパスワード候補τにを用いて$\mathrm{K'_{BA}} = \mathrm{KDF}(\mathrm{E_A}, \mathrm{E'_B}, \mathrm{E_{BA}}, \tau)$を計算する。
5. オフライン辞書攻撃を行う為には、K_{AB}中のE'_{AB}に組み込まれている仮のパスワードπ'をτに切り替えなければならない。しかし、攻撃者$\mathcal{A}$は$[\mathfrak{a}\cdot\mathfrak{b}]E_0$の情報を持っていないことから困難であると考える。

ハッシュ関数
$H:\{0,1\}^* \to cl(\mathbb{Z}[\pi_p])$

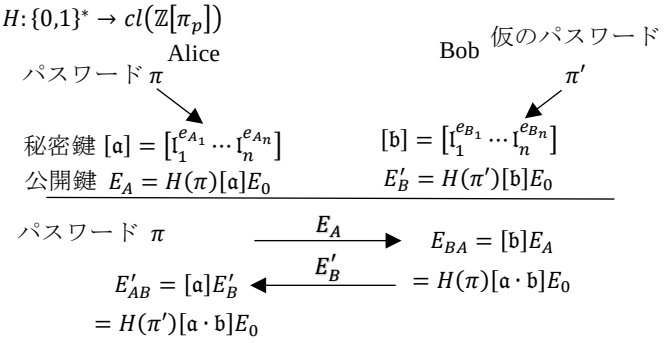

図 11 改良案 1 へのオフライン辞書攻撃への安全性の考察

Figure 11 Security Considerations for Offline Dictionary Attacks on Improvement Proposal 1

8.3 CSIDH を用いたパスワードベースの認証付き鍵共有の改良案 2

図 12 に示すように、認証用に使うパスワードはπとする。ハッシュ関数$H:\{0,1\}^* \to cl(\mathbb{Z}[\pi_p])$を用意する。

1. Alice は$[\mathfrak{a}] = [\mathfrak{l}_1^{e_{A_1}} \cdots \mathfrak{l}_n^{e_{A_n}}] \in \mathrm{cl}(\mathbb{Z}[\pi_p])$を選択し、楕円曲線$E_A = H(\pi)[\mathfrak{a}]E_0$、楕円曲線$E_A$上の点$P_A = H(\pi)\mathfrak{a}P_0$を計算し、Bob に$E_A$を送信する。
2. Bob は$[\mathfrak{b}] = [\mathfrak{l}_1^{e_{B_1}} \cdots \mathfrak{l}_n^{e_{B_n}}] \in \mathrm{cl}(\mathbb{Z}[\pi_p])$を選択し、楕円曲線$E_B = H(\pi)[\mathfrak{b}]E_0$、楕円曲線$E_B$上の点$P_B = H(\pi)\mathfrak{b}P_0$を計算し、Alice に$E_B$を送信する。
3. Alice はE_B、P_Bを用いて、$E_{AB} = [\mathfrak{a}]E_B$、$P_{AB} = H(\pi)\mathfrak{a}P_B$を計算する。
4. Bob はE_A、P_Aを用いて、$E_{BA} = [\mathfrak{b}]E_A$、$P_{BA} = H(\pi)\mathfrak{b}P_A$を計算する。
5. パスワードπを用いて Alice はセッション鍵$K_{AB} = KDF(E_A, E_B, E_{AB}, P_A, P_B, P_{AB}, \pi)$を得る。
6. パスワードπを用いて Bob はセッション鍵$K_{BA} = KDF(E_A, E_B, E_{BA}, P_A, P_B, P_{AB}, \pi)$を得る。
7. 共有秘密が$K_{AB} = K_{BA}$となり、認証付き鍵共有が成立する。

Vol.2022-DPS-190 No.22
Vol.2022-CSEC-96 No.22
2022/3/10

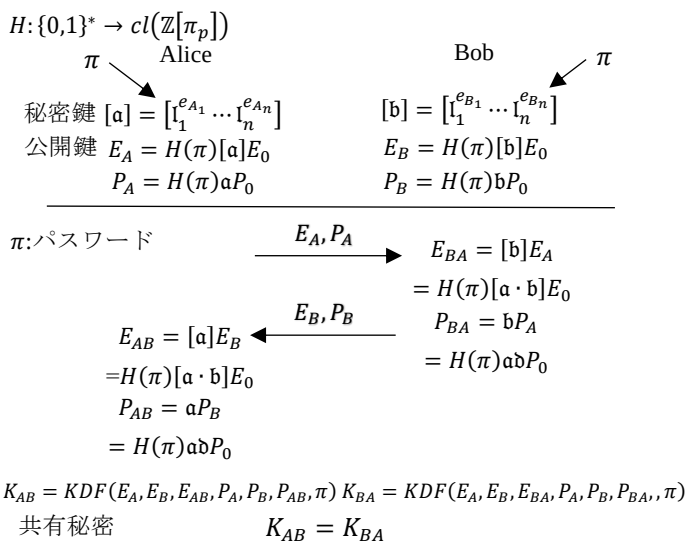

図 12　CSIDH を用いたパスワードベースの認証付き鍵共有の改良案 2

Figure 12　Proposed improvements to password-based authenticated key sharing using CSIDH 2

8.4 改良案 2 のオフライン辞書攻撃への安全性の考察

図 13 に示すように

1. 攻撃者$\mathcal{A}$は Alice と仮のパスワードπ'を用いてセッションを実行する。
2. Alice はセッション鍵 $K_{AB} = KDF(E_A, E'_B, E'_{AB}, P_A, P'_B, P'_{AB}, \pi)$を入手する。
3. 攻撃者$\mathcal{A}$は Alice のセッション鍵 $K_{AB} = KDF(E_A, E'_B, E'_{AB}, P_A, P'_B, P'_{AB}, \pi)$を入手したとする。
4. 攻撃者$\mathcal{A}$はパスワード候補τを用いて $K'_{BA} = KDF(E_A, E'_B, E_{BA}, P_A, P'_B, P_{AB}, \tau)$を計算する。
5. オフライン辞書攻撃を行う為には、K_{AB} 中のE'_{AB}、P'_{AB} に組み込まれている仮のパスワードπ'をτに切り替えなければならない。しかし、攻撃者$\mathcal{A}$は$[\mathfrak{a}\cdot\mathfrak{b}]E_0$や$\mathfrak{a}\mathfrak{b}P_0$ の情報を持っていないことから困難であると考える。

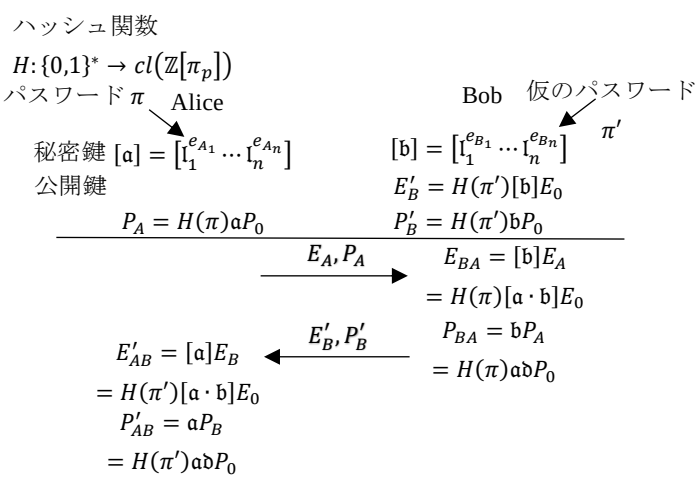

図 13　改良案 2 へのオフライン辞書攻撃への安全性の考察

Figure 13　Security Considerations for Offline Dictionary Attacks on Improvement Proposal 2

9. おわりに

本研究では、認証付き鍵共有の中で、CSIDH を用いたパスワードベースの認証付き鍵共有に注目し、研究を行った。

7 章で紹介した CSIDH を用いたパスワードベースの認証付き鍵共有は、オフライン辞書攻撃の危険性がある。そこで、本研究ではオフライン辞書攻撃を防ぐ為の改良案を提案した。オフライン辞書攻撃を防ぐ為には、Alice と Bob が共有しているE_{AB}にもパスワードπが必要にしなければならない。改良案 1 では、公開鍵である楕円曲線E_A、E_Bにハッシュ化したパスワード$H(\pi)$を組み込む。その公開鍵を共有することで、互いに共有するE_{AB}にもパスワードを組み込み、オフライン辞書攻撃を防げるようにした。改良案 2 では、新たに楕円曲線E_A、E_B上の点P_A、P_Bを楕円曲線E_A、E_Bと共に公開鍵として用いる。そして、楕円曲線E_A、E_B上の点P_A、P_Bにハッシュ化したパスワード$H(\pi)$を組み込む。楕円曲線E_A、E_Bと共に、ハッシュ化したパスワード$H(\pi)$を組み込んだ楕円曲線E_A、E_B上の点P_A、P_Bを共有することで、互いに共有するP_{AB}にもパスワードを組み込み、オフライン辞書攻撃を防げるようにした。2 つの改良案を比較すると、改良案 2 では、楕円曲線に加えて、楕円曲線上の点も共有することになる。その為、改良案 2 は改良案 1 よりも計算量が多くなるという問題点がある。

今後の課題としては、6 章で考察した 2 つの改良案のオフライン辞書攻撃への安全性について、フォーマルな安全性証明を行う必要がある。また、実装を行うことも必要である。

参考文献

[1] Wouter Castryck, Tanja Lange, Chloe Martindale,Lorenz Panny, and Joost Renes. CSIDH: an efficient post-quantum commutative group action. In International Conference on the Theory and Application of Cryptology and Information Security, pages 395–427. Springer, 2018.

[2] Tako Boris Fouotsa and Christophe,SimS: a Simplification of SiGamal, PetitPQCrypto 2021.

[3] 山岸純一, 相賀陸, 趙晋輝 ,”SIDH 鍵交換方式に対する Fault 攻撃”, FIT2018（第 17 回情報科学技術フォーラム）, https://www.ieice.org/publications/conference-FIT-DVDs/FIT2018/data/pdf/L-018.pdf(最終閲覧日 2022 年 1 月 18 日)

[4] tsujimotter のノートブック, “二次体 Q(√-5) のイデアル類群と xx + 5yy 型の二次形式”, https://tsujimotter.hatenablog.com/entry/ideal-class-group-and-quadratic-form,(最終閲覧日 2022 年 1 月 18 日)

[5] 岡本龍明, ”鍵交換：現代暗号の誕生とその発展”, https://www.jstage.jst.go.jp/article/essfr/1/4/1_4_4_70/_pdf , (最終閲覧日 2022 年 1 月 18 日)

[6] Diffie, W.; van Oorschot, P.; Wiener, M. (June 1992). "Authentication and authenticated key exchanges". Designs, Codes and Cryptography. 2 (2): 107–125. doi:10.1007/BF00124891.

[7] Tomoki Kawashima, Katsuyuki Takashima, Yusuke Aikawa, Tsuyoshi Takagi, An Efficient Authenticated Key Exchange from Random Self-Reducibility on CSIDH, Cryptology ePrint Archive, Report 2020/1178, 2020. https://eprint.iacr.org/2020/1178.

[8] Shintaro Terada and Kazuki Yoneyama. Password-Based Authenticated Key Exchange from Standard Isogeny Assumptions. In Ron Steinfeld and Tsz Hon Yuen, editors, Provable Security, pages 41–56, Cham, 2019. Springer International Publishing.

[9] Reza Azarderakhsh, David Jao, Brian Koziel, Jason T. LeGrow, Vladimir Soukharev, and Oleg Taraskin, How Not to Create an Isogeny-Based PAKE. Cryptology ePrint Archive, Report 2020/361, 2020. https://eprint.iacr.org/2020/361.