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関する研究

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

岡村貴仁・ネットワーク分科会・情報セキュリティ大学院大学

Abstruct : 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 homomorphic mapping problem is attracting attention as a difficult problem that can be handled by quantum computers. The homogeneous mapping 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.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.

1.背景

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。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。

2.目的

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。

3.認証付き鍵共有

ディッフィーヘルマン鍵交換方式など、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。

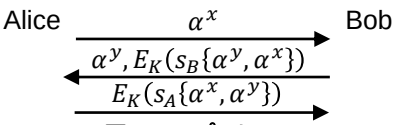

図1.STSプロトコル

4. CSIDHを用いたパスワードベースの認証付き鍵共有

寺田らによって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が、オフライン辞書攻撃の危険性が存在する。

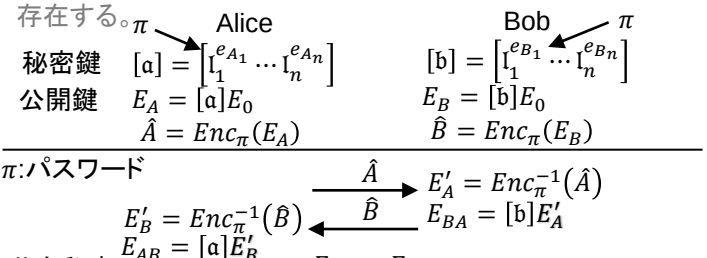

図2.寺田らのCSIDHを用いたパスワードベースの認証付き鍵共有

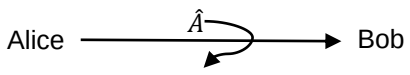

図3.寺田らの方式へのオフライン辞書攻撃

For パスワード候補π':
$E'_A = Enc_{\pi'}^{-1}(\hat{A})$
if E'_A:超特異楕円曲線
return π'

5.オフライン辞書攻撃に対応する為の改良案

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

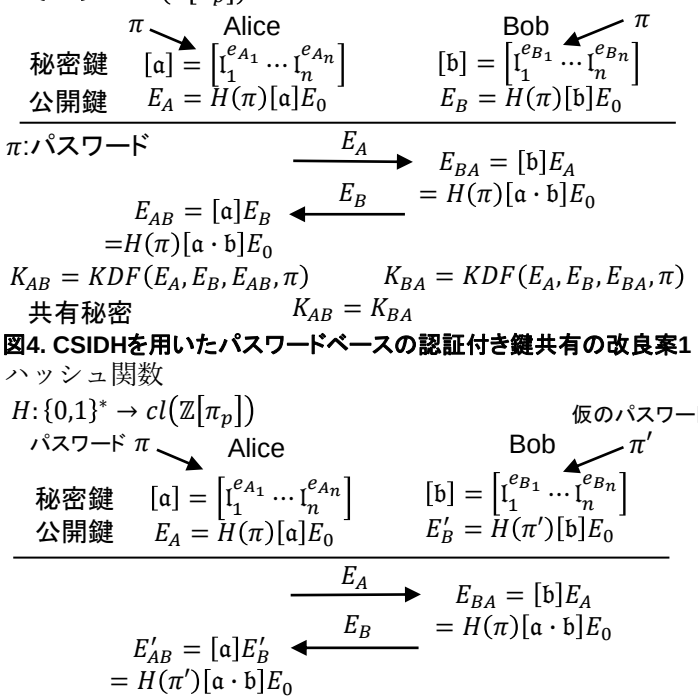

図4. CSIDHを用いたパスワードベースの認証付き鍵共有の改良案1

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

図5.改良案1のオフライン辞書攻撃への安全性の考察

① Aliceは$K_{AB} = \mathrm{KDF}(E_A, E'_B, E'_{AB}, \pi)$を入手。
② 攻撃者$\mathcal{A}$はパスワード候補τについて
$K'_{BA} = KDF(E_A, E'_B, E_{BA}, \tau)$を計算。
③ 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。

→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