# 符号ベースのマルチレシーバー KEM の構成について

## Construction of Code-based Multi-receiver KEMs

安光一平・ネットワーク分科会・情報セキュリティ大学院大学

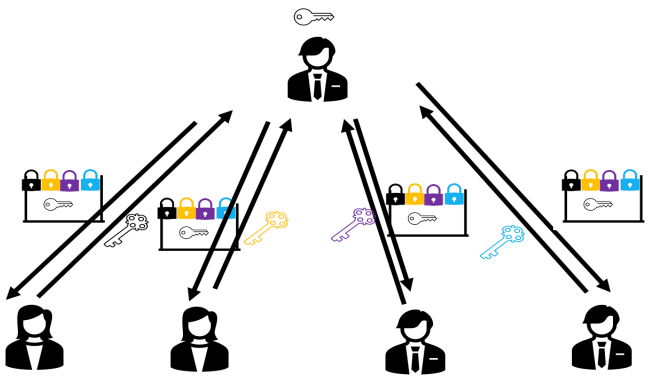
The messaging applications we use in our daily life allow for smooth communication remotely. Multi-receiver KEMs are used as a method of session key sharing in group chats. When quantum computers are put into practical use, there is concern that the public key cryptography currently in use will be broken. It is necessary to construct a multi-receiver KEM using quantum computer cryptography. In this presentation, we propose a secure code-based multi-receiver KEM construction.

## 研究背景

我々が普段使用しているメッセージアプリは、遠隔での円滑なやり取りを可能にしている。グループチャットでのセッション鍵共有の方法として利用されているのがマルチレシーバーKEMである。量子コンピュータが実用化されると、現在使用されている公開鍵暗号が解かれることが懸念されている。耐量子計算機暗号を用いたマルチレシーバーKEM の構成が必要である。本発表では安全な符号ベースのマルチレシーバーKEMの構成を提案する。

## マルチレシーバーKEMとは

マルチレシーバーKEMとは公開鍵を利用し、一対多でのセッション鍵共有を実現する暗号技術である。



## マルチレシーバー PKE

改良型FO変換に入力する条件を満たしたマルチレシーバー PKEを実現できればマルチレシーバー KEMが構成できる。
符号ベースのKEMであるBIKEをもとに、以下の(N+2,1)QCSD 仮定に基づいたマルチレシーバーPKEを実現した。

- $\mathbf{mSetup}(\lambda) \to (pp)$
(1) $\mathbf{g} \xleftarrow{\$} \mathcal{R}$
(2) **return** $pp = \mathbf{g}$
- $\mathbf{mKeyGen}(pp) \to (pk, sk)$
(1) $h_0, h_1 \xleftarrow{\$} \mathcal{R}(|h_0|, |h_1| = w/2 : odd)$
(2) $f \leftarrow h_1 + g \cdot h_0$
(3) **return** $pk = f, sk = h_0$
- $\mathbf{mEncrypt}(pp, (pk_i)_{i\in[N]}, M \in \mathcal{R}) \to \vec{ct}$
(1) $r_0 = (e_{N+1}, e_0) \xleftarrow{\$} \mathcal{R} \times \mathcal{R}(|e_{N+1}| + |e_0| = t)$
(2) $r_i = e_{1,i} \xleftarrow{\$} \mathcal{R}, (|e_{1,i}| = t/2)(1 \leqq i \leqq N)$
(3) $ct_0 = \mathbf{mEnc}^{\mathrm{i}}(pp; r_0)$
(4) **for** $i \in [N]$**do**
(5) $\widehat{ct_i} = \mathbf{mEnc}^{\mathrm{d}}(pp, pk_i, M; r_0, r_i)$
(6) **return** $\vec{ct} = (ct_0, \widehat{ct_0}, \cdots, \widehat{ct_N})$

- $\mathbf{mEnc}^{\mathrm{i}}(pp; r_0) \to ct_0$
(1) $(e_{N+1}, e_0) \leftarrow r_0$
(2) $u \leftarrow e_{N+1} \cdot g + e_0$
(3) **return** $ct_0 = u$
- $\mathbf{mEnc}^{\mathrm{d}}(pp, pk_i; r_0, r_i) \to \widehat{ct_i}$
(1) $e_{N+1} \leftarrow r_0, e_{1,i} \leftarrow r_i$
(2) $v_i \leftarrow e_{N+1} \cdot f_i + e_{1,i} + RS.Encode(M)$
(3) **return** $\widehat{ct_i} = v_i$

- $\mathbf{mDecrypt}(sk_i, ct_i) \to M$
(1) $l_i \leftarrow v_i - u \cdot h_0$
(2) **return** $M = RS.Decode(l_i)$

## (N+2,1)-QCSD 仮定

(N+2,1)-QCSD 符号は以下のパリティチェック行列を持つ。

(N+2,1)-QCSD 仮定とは、(N+2,1)-QCSD 符号の探索問題及び決定問題を解くことが困難であることをいう。

$$\begin{pmatrix} 1 & 0 & \cdots & \cdots & 0 & h_0 \\ 0 & 1 & \ddots & & \vdots & h_1 \\ \vdots & \vdots & & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & \cdots & 1 & h_{N+1} \end{pmatrix}$$

## 暗号文の構造