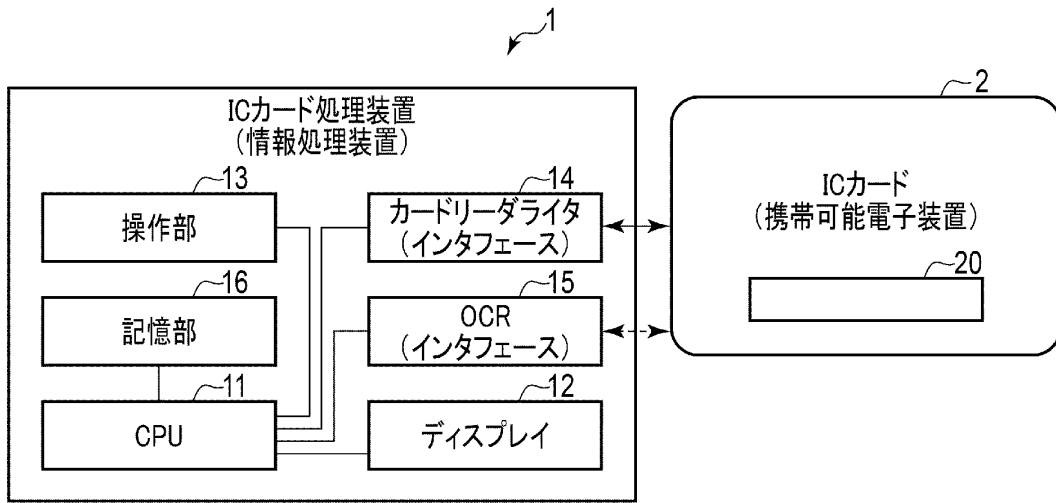
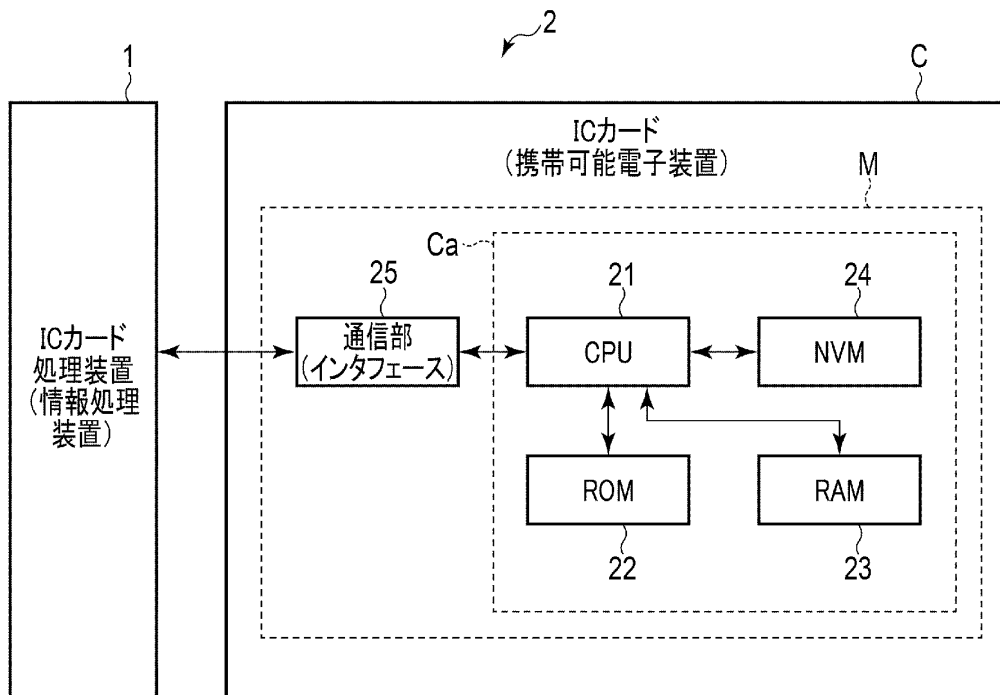


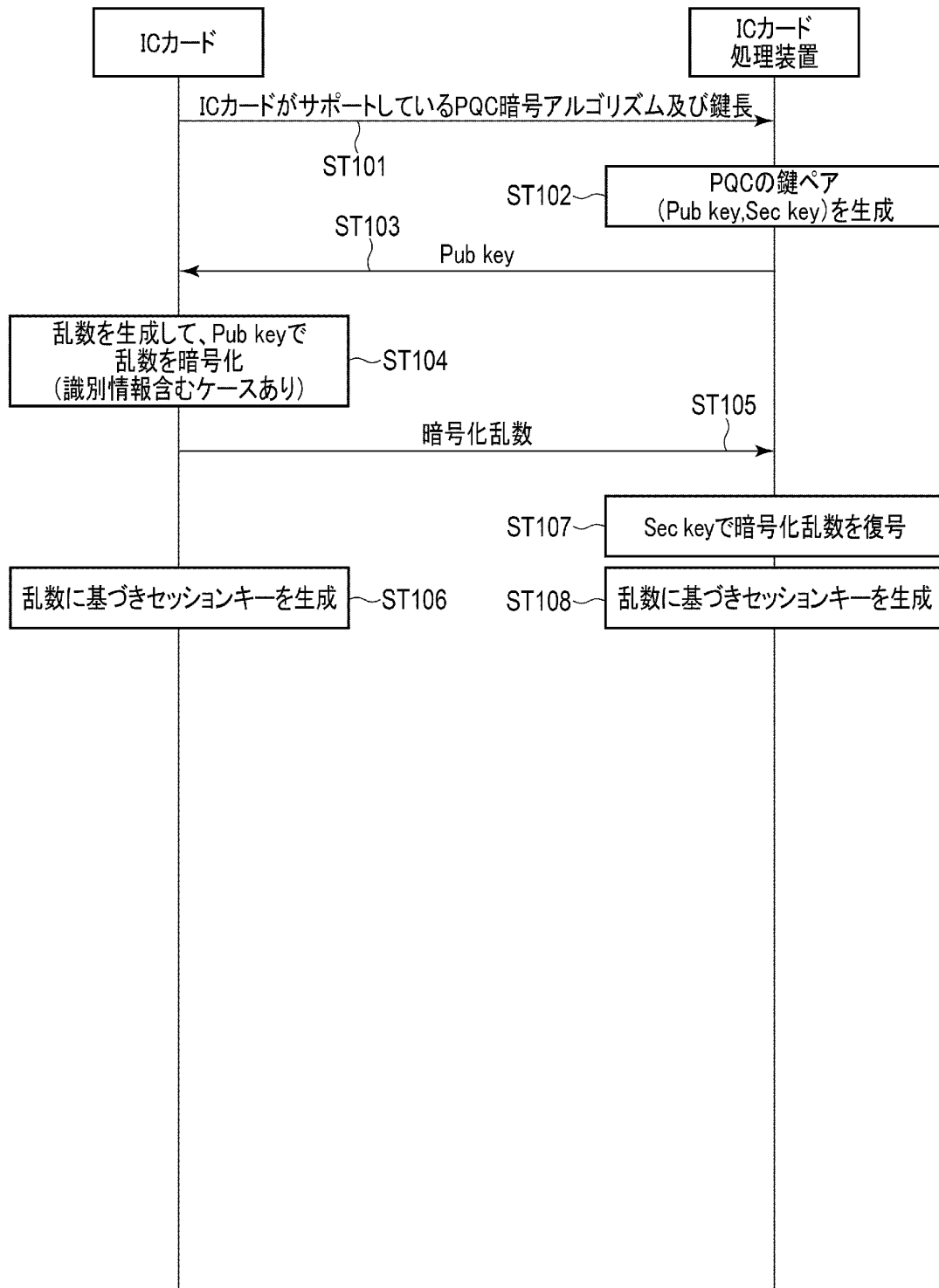
[図1]



[図2]

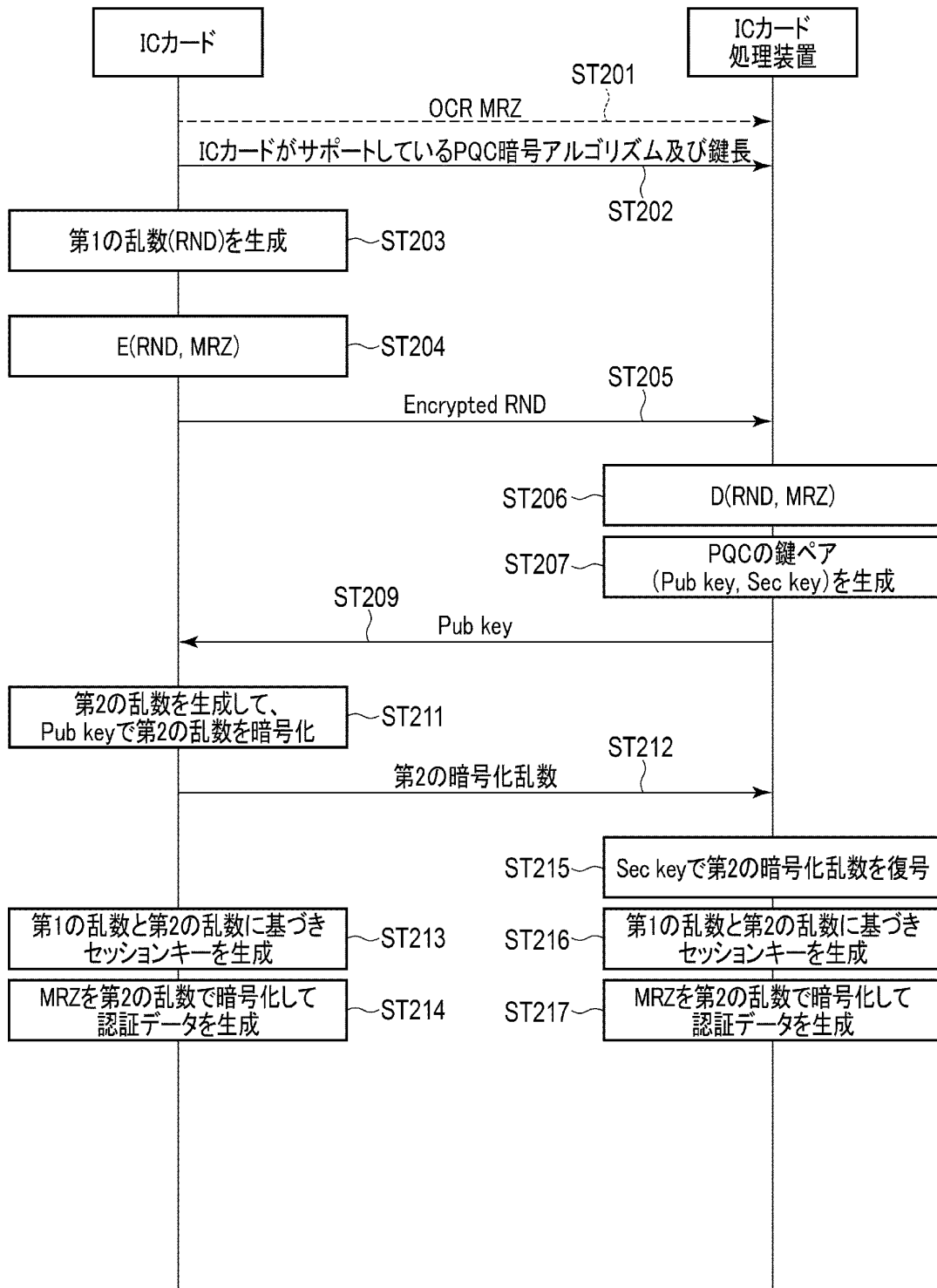


[図3]



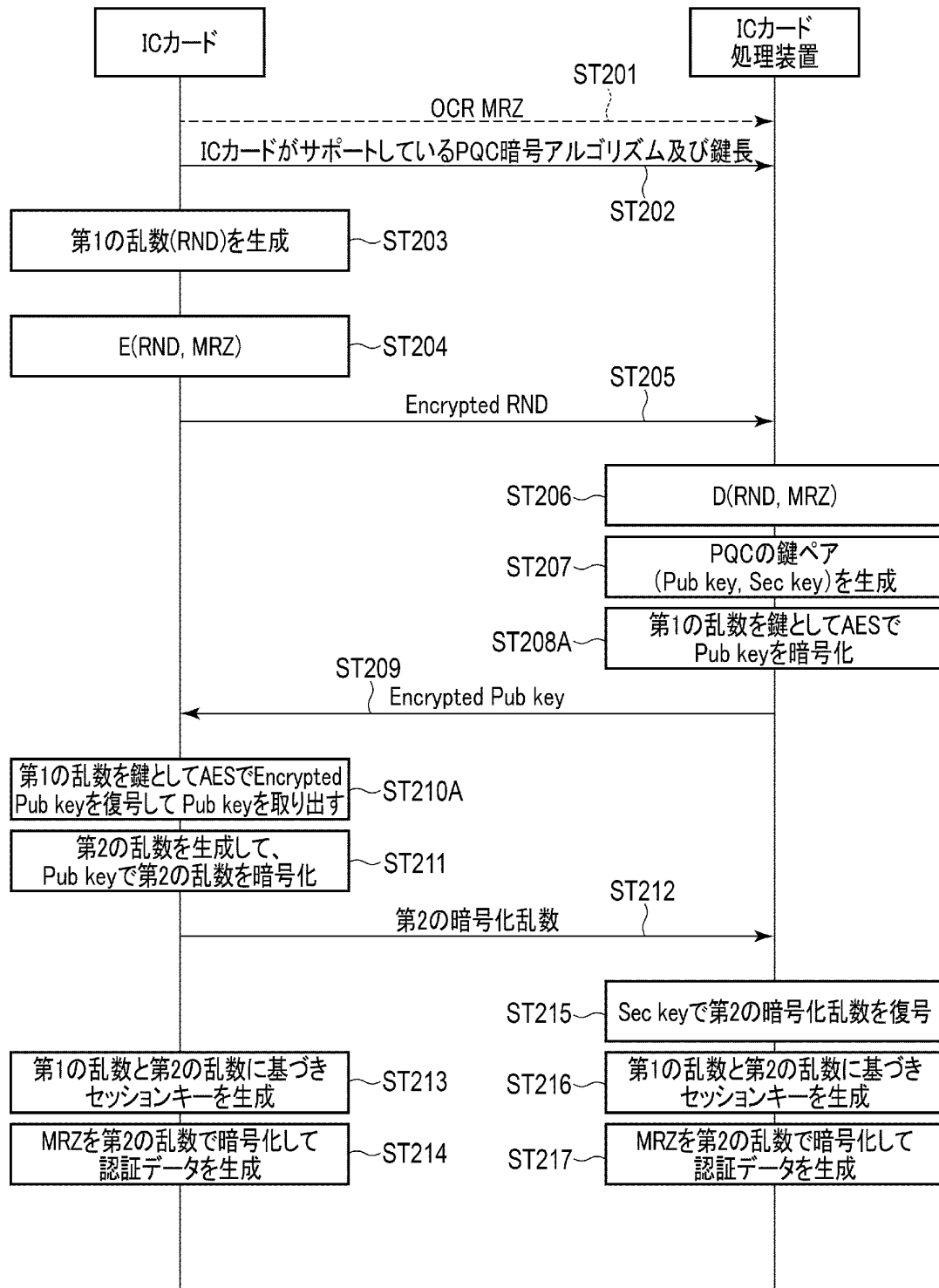
〈概念1〉

[図4]



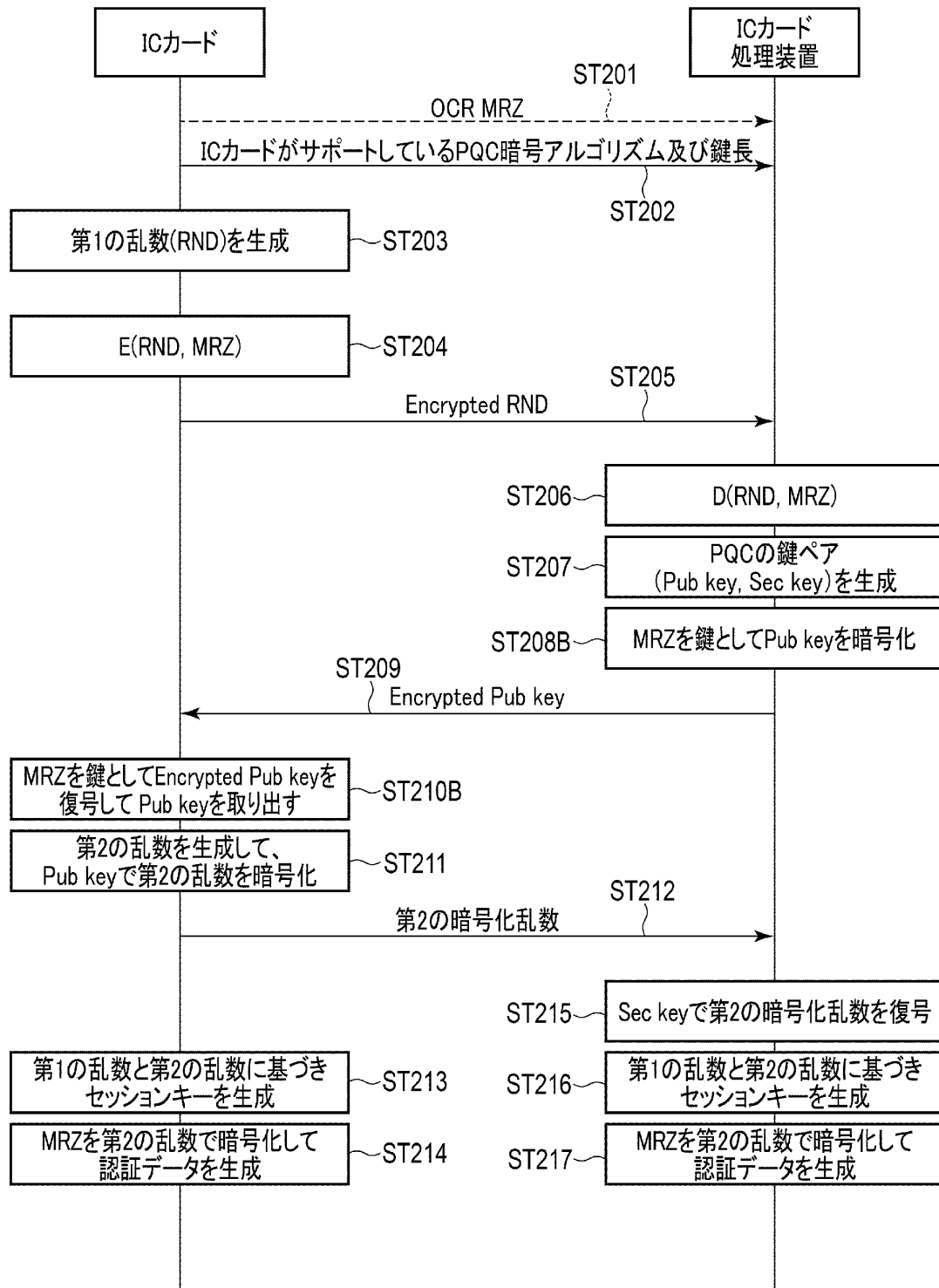
〈概念2-1〉

[図5]



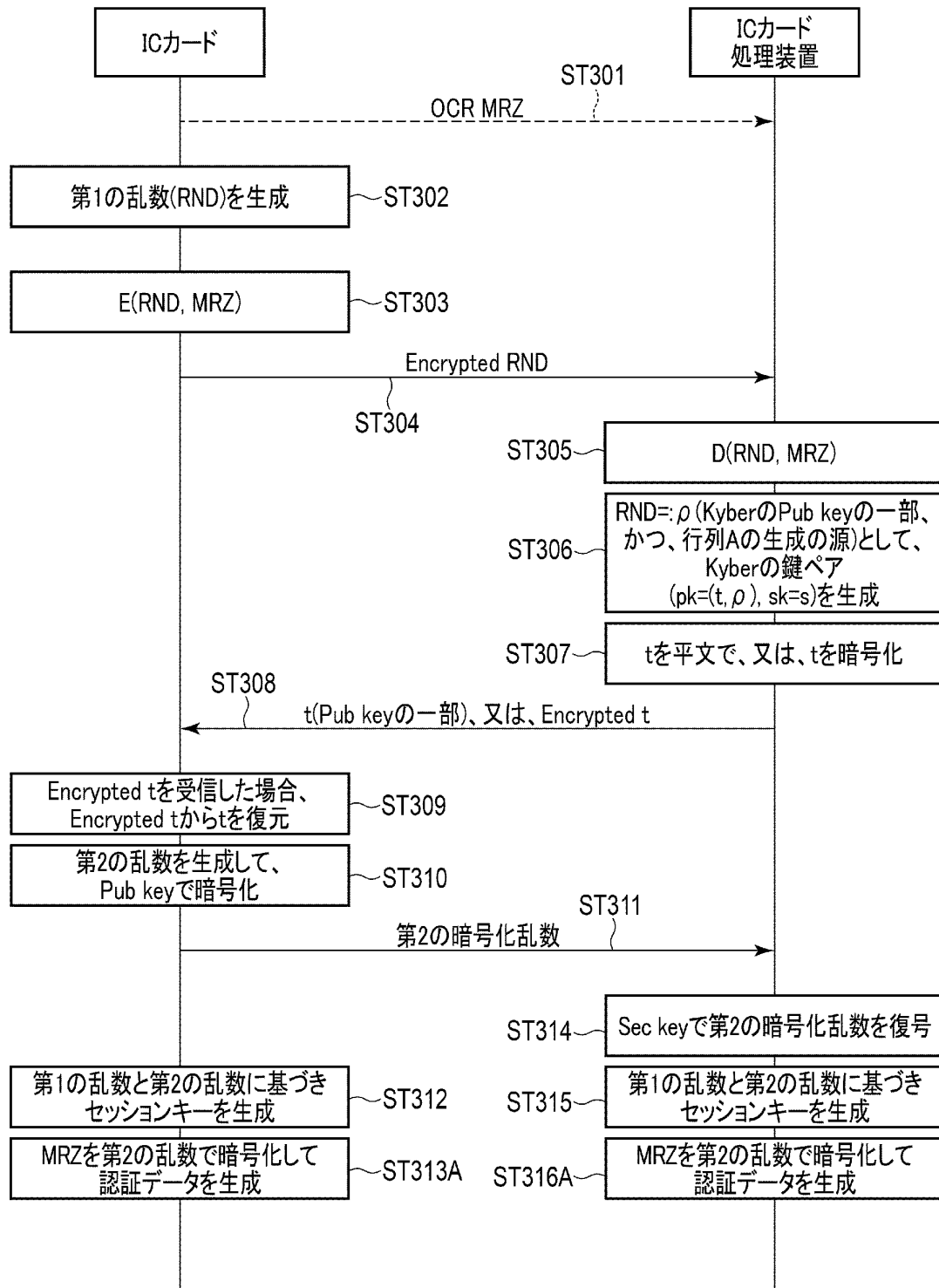
〈概念2-2〉

[図6]



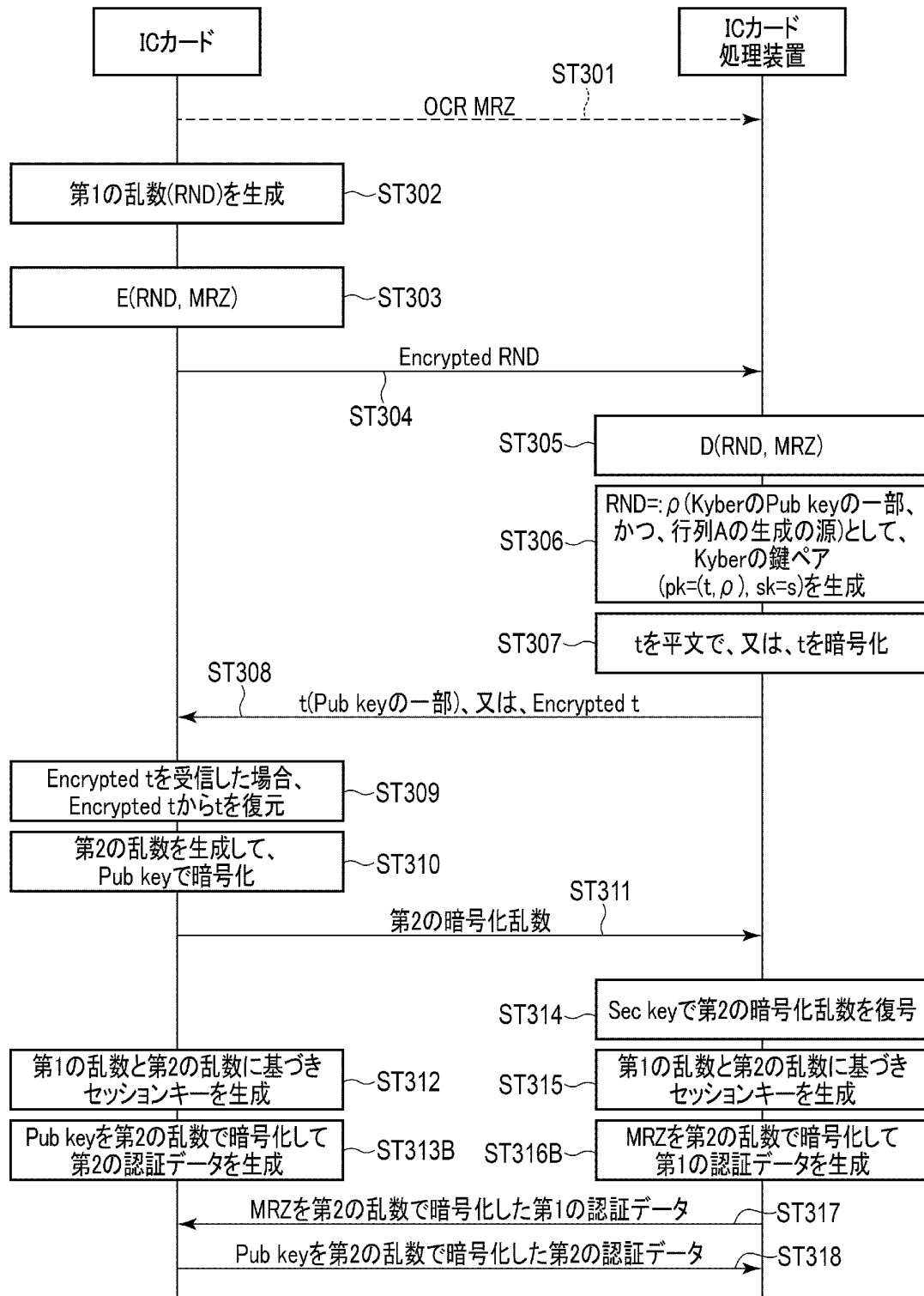
〈概念2-3〉

[図7]



〈概念3-1〉

[図8]



〈概念3-2〉

[図9]

Algorithm 1 Kyber.CPA.KeyGen(): key generation

```

1:  $[\rho], \sigma \leftarrow \{0, 1\}^{256}$ 
2:  $\mathbf{A} \sim R_q^{k \times k} := \text{Sam}([\rho])$ 
3:  $(\mathbf{s}, \mathbf{e}) \sim \beta_\eta^k \times \beta_\eta^k := \text{Sam}(\sigma)$ 
4:  $\mathbf{t} := \text{Compress}_q(\mathbf{A}\mathbf{s} + \mathbf{e}, d_t)$ 
5: return  $(pk := (\mathbf{t}, [\rho]), sk := \mathbf{s})$ 

```

[図10]

Algorithm 4 KYBER.CPAPKE.KeyGen(): key generation

Output: Secret key $sk \in \mathcal{B}^{12 \cdot k \cdot n / 8}$ **Output:** Public key $pk \in \mathcal{B}^{12 \cdot k \cdot n / 8 + 32}$

```

1:  $d \leftarrow \mathcal{B}^{32}$ 
2:  $\llbracket d \rrbracket \sigma := G(d)$ 
3:  $N := 0$ 
4: for  $i$  from 0 to  $k - 1$  do
5:   for  $j$  from 0 to  $k - 1$  do
6:      $\hat{A}[i][j] := \text{Parse}(\text{XOF}(\llbracket d \rrbracket, j, i))$ 
7:   end for
8: end for
9: for  $i$  from 0 to  $k - 1$  do
10:   $s[i] := \text{CBD}_{\eta_1}(\text{PRF}(\sigma, N))$ 
11:   $N := N + 1$ 
12: end for
13: for  $i$  from 0 to  $k - 1$  do
14:   $e[i] := \text{CBD}_{\eta_1}(\text{PRF}(\sigma, N))$ 
15:   $N := N + 1$ 
16: end for
17:  $\hat{s} := \text{NTT}(s)$ 
18:  $\hat{e} := \text{NTT}(e)$ 
19:  $\hat{t} := \hat{A} \circ \hat{s} + \hat{e}$ 
20:  $pk := (\text{Encode}_{12}(\hat{t} \bmod^+ q) \parallel \llbracket d \rrbracket)$ 
21:  $sk := \text{Encode}_{12}(\hat{s} \bmod^+ q)$ 
22: return  $(pk, sk)$ 

```

$\triangleright$ Generate matrix $\hat{A} \in R_q^{k \times k}$ in NTT domain

 $\triangleright$ Sample $s \in R_q^k$ from B_{η_1}

 $\triangleright$ Sample $e \in R_q^k$ from B_{η_1}

 $\triangleright pk := As + e$
 $\triangleright sk := s$
