

replacement of the variable i . In this case, the replacement table itself is the secret key sk_2 . The encrypted data generation unit 102 stores the value of the replaced variable i in a variable j . The secret key sk_1 and the secret key sk_2 may be the same, but using different secret keys increases the security of the encrypted data.

The encrypted data generation unit 102 stores the output value in step S1305 as c_j (S1307). The encrypted data generation unit 102 decreases the value of the variable i by 1 (S1308). The encrypted data generation unit 102 determines whether or not the value of the variable i after the decrement is less than 1 (S1309).

When the encrypted data generation unit 102 determines that the value of the variable i after the decrement is 1 or more (step S1309: No), the process returns to step S1301. If it is determined that the value of the variable i after the decrement is less than 1 (S1309: Yes), the encrypted data generation unit 102 outputs the random number r and the created n pieces of c_j as encrypted data ($rc_n c_{n-1} \dots c_1$) (S1310) and ends the encrypted data generation processing.

FIG. 7 is an explanatory diagram illustrating a specific example of the encrypted data generation processing described in FIG. 6. An example of processing for generating encrypted data of base-10 integer 101 will be described. The base-10 integer 101 can be expressed by (1011) as 4-bit data. The secret