ABSTRACT

In a center, a Fourier transformation with a weighting function and a center matrix are applied to the identifier of each entity (steps 2-1, 2-2), which is then randomized by one-time pass random number data generated by a manual operation at each entity, thereby generating a secret private key peculiar to each entity (steps 2-3 ~ 2-5). The center also generates an identifier transformation algorithm based on the one-time pass random number data and the Fourier transformation with a weighting function (step 2-6). Thereafter, the center distributes the identifier transformation algorithm and the secret private key to each entity. Each entity applies the identifier transformation algorithm and the secret private key to the identifier of another entity with which to communicate, for thereby generating a common cryptokey for cryptographic communications between the entities.