CONCLUSION

In this paper, we formalized the ConBE primitive. In ConBE, anyone can send secret messages to any subset of the group members, and the system does not require a trusted key server. Neither the change of the sender nor the dynamic choice of the intended receivers require extra rounds to negotiate group encryption/decryption keys. Following the ConBE model, we instantiated an efficient ConBE scheme that is secure in the standard model. As a versatile cryptographic primitive, our novel ConBE notion opens a new avenue to establish secure broadcast channels and can be expected to secure numerous emerging distributed computation applications.