ONLINE VOTING USING POINT TO MULTIPOINT QUANTUM KEY DISTRIBUTION VIA PASSIVE OPTICAL NETWORKS

INVENTORS:

BERNARDO HUBERMAN

JING WANG

Abstract

In this patent, we propose using Point-to-Multipoint quantum key distribution (QKD) via time division multiplexing (TDM) and wavelength division multiplexing (WDM) in passive optical networks (PON) to improve the security of online voting systems.

Background

There are a number of proposals for secure online voting systems that offer a number of required properties, like completeness, privacy and fairness. Typically, these cryptographic voting schemes can be divided into three categories, based on the technique used to anonymize votes.

In schemes based on homomorphic encryption, voters submit encrypted votes that are never decrypted. Rather, the submitted ciphertexts are combined to produce a single ciphertext containing the election tally, which is then decrypted.

Blind signature schemes split the election authority into an authenticator and a tallier. The voter authenticates to the authenticator, presents a blinded vote, and obtains the authenticator's signature on the blinded vote. The voter unblinds the signed vote and submits it via an anonymized channel to the tallier.

Lastly, in mix network schemes voters authenticate and submit encrypted votes. Votes are anonymized using a mix, and anonymized votes are then decrypted.

All these schemes rely on the use of public and private keys that ensure completeness, privacy and fairness. But recent advances in quantum computing threaten the security of public key encryption which lies at the heart of all these systems.

This is where quantum key distribution (QKD) offers an advantage since the private keys that are generated via quantum mechanisms are provably secure.

Summary

The use of QKD in the service of voting suffers, however, from an almost fatal problem, i.e., that in order to generate keys for voters and verifiers, a point-to-point connection has to be physically established for each pair, rendering this impractical.

A solution of this problem is provided by our proposed (D4491) system to deploy a Point-to-Multipoint quantum key distribution (QKD) via time division multiplexing (TDM) and wavelength division multiplexing (WDM) in passive optical networks (PON).

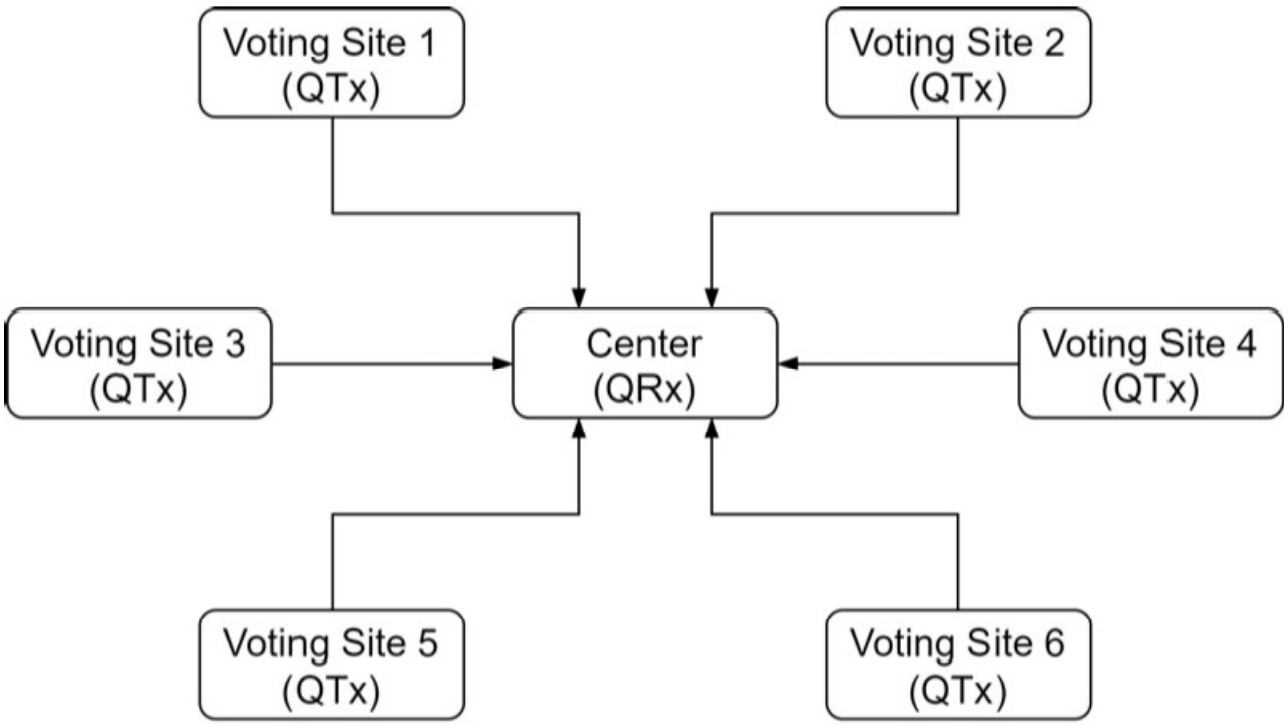
This would allow the voting authority to distribute private keys to all the voting participants, who could then use whatever electronic voting they prefer. As an example, blind signature schemes like those of Fujioka, Okamoto and Ohta, use Blind which use bit-commitment would greatly benefit from the use private keys delivered via QKD so as to provably secure.

To make this explicit, let's consider how one way bit-commitment works using private keys. is by having two parties, Alice and Bob, perform the following actions:

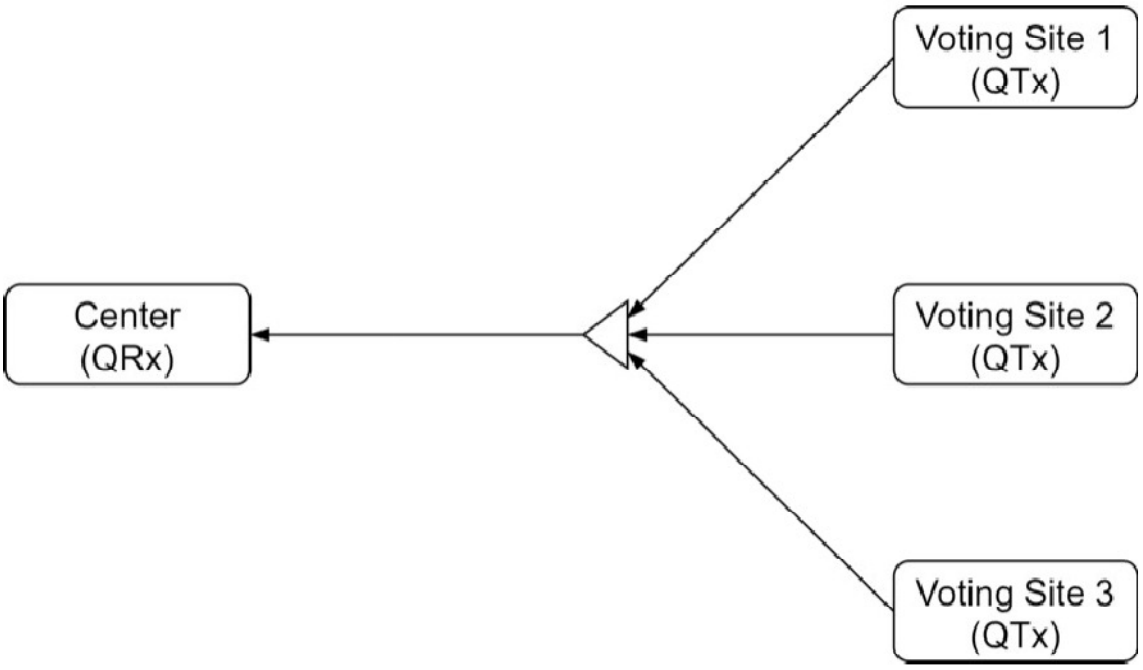
For the other voting schemes, private keys would replace the use of the public encryption they are based on, since public keys are being threatened by the advent of quantum computers.

To have a group of people vote, we propose the use of point-to-multipoint QKD to establish secure communications between voters and talliers.

To have provably secure online voting using point to multipoint deployment of private keys, two typical network topologies can be used. One is a star network topology, where pick their voters at voting sites which connect to a centralized counting center, as shown in the figure below.



The other topology is a passive optical network (PON), where multiple voting sites connect to the collection center via a splitter, as shown below.



References

D. Chaum, Elections with Unconditionally-Secret Ballots and Disruption Equivalent to breaking RSA. Advances in Cryptology-EUROCRYPT'88 Lecture Notes in Computer Science, 330, Springer (1988).

M. A. Herschberg, Secure Electronic Voting Over the World Wide Web, MS thesis MIT (1997).

K. Sako and J. Killian, Secure Voting Using Partially Compatible Homomorphisms, in Advances in Cryptology-CRYPTO '94, Lecture Notes in Computer Science, 839, Springer (1994).

M. Okhubo, F. Miura, M. Abe, A. Fujioka and T. Okamoto, An improvement on a Practical Secret Voting Scheme, 225, Information Security, Second International Workshop, ISW'99.