Quantum Tokens for Digital Signatures

Abstract:

The fisherman caught a quantum fish. "Fisherman, please let me go", begged the fish, "and I will grant you three wishes". The fisherman agreed. The fish gave the fisherman a quantum computer, three quantum signing tokens and his classical public key. The fish explained: "To sign your three wishes, use the tokenized signature scheme on this quantum computer, then show your valid signature to the king, who owes me a favor".

The fisherman used one of the signing tokens to sign the document "give me a castle!" and rushed to the palace. The king executed the classical verification algorithm using the fish's public key, and since it was valid, the king complied.

The fisherman's wife wanted to sign ten wishes using their two remaining signing tokens. The fisherman did not want to cheat, and secretly sailed to meet the fish. "Fish, my wife wants to sign ten more wishes". But the fish was not worried: "I have learned quantum cryptography following the previous story (The Fisherman and His Wife by the brothers Grimm). The quantum tokens are consumed during the signing. Your polynomial wife cannot even sign four wishes using the three signing tokens I gave you".

"How does it work?" wondered the fisherman. "Have you heard of quantum money? These are quantum states which can be easily verified but are hard to copy. This tokenized quantum signature scheme extends Aaronson and Christiano's quantum money scheme, and a variant by Zhandry, which is why the signing tokens cannot be copied".

"Does your scheme have additional fancy properties?" the fisherman asked. "Yes, the scheme has other security guarantees: revocability, testability and everlasting security. Furthermore, if you're at sea and your quantum phone has only classical reception, you can use this scheme to transfer the value of the quantum money to shore", said the fish, and swam away.

Joint work with Shalev Ben-David. https://arxiv.org/abs/1609.09047