

Can AVSS all most surly terminate?

David Ponnarovsky

July 15, 2022

1 Setting.

We examine quantum protocols for AVSS in an asynchronous environment under Byzantine attack. Asynchronous means that the adversary chooses when each message gets to its destination. Byzantine attack defines faulty parties as parties that could do any computation, restricted only to information constraints. And by being quantum, the parties and the dealer could exchange qubits (states) and perform and compute any quantum circuit.

As classic randomization can be achieved by doing measurements, we will allow ourselves to assume that the protocols perform only unitary operations and measurements and still be relevant to randomized protocols.

Verifiable Secret Sharing is a double stages protocol. In the first stage, the dealer sends his secret to every party; then, the parties should vote if the dealer is honest in the second stage.

Theorem [FLP85]. Any protocol \mathcal{P} solving consensus in the asynchronous model that is resilient to even just one crash failure must have an infinite execution.

[COMMENT] Todo: cite the paper of Ittai Abraham, Danny Dolev, Gilad Stern [2020], and explain their results. [DBLP:conf/podc/AbrahamDS20]

Those results raise the following question: whether the above lower bound is still held for quantum protocols? In other words, is there a quantum protocol that is both tolerances for faults and all most surely terminates? Another interesting question, can indistinguishability boosting be done even if the parties act quantumly?

Theorem 1. Suppose that \mathcal{P} is an AVSS protocol that tolerates $f = 1$ Byzantine faults and **all most surly** terminates. Then for every $\Gamma \in (0, 1)$ at least one of the following options is possible.

1. A faulty dealer D has attack in which he wins with probability at least Γ .
2. A faulty party B has attack in which he wins with probability at least $1 - \Gamma$.

2 Strategy.

Definition. Well defined protocol.

Definition. Prefix running. **[COMMENT]** Complete this Definition.

Lemma I. Let \mathcal{P} be a protocol that terminates all most surely. Then for every $\varepsilon > 0$, **[COMMENT]** Add here, for every less than f non-honest parties... there exist M such the for every $j > M$ the probability that p_i act non trivially on j -th qubit is less than ε .

Proof. Fix a less than f non-honest parties and assume by contradiction, that there exist $\varepsilon > 0$ such for infinitely many j the probability that P_i act non trivially on j -th qubit is grater then ε . Then for infinitely many t 's:

$$\begin{aligned} \Pr[\text{Rounds}(\mathcal{P}) > t] &\geq \Pr[\text{Time}(\mathcal{P}) > t] \\ &\geq \Pr[\exists p_i \text{ read } m_t^{t'}] \\ &\geq \Pr[\exists p_i \text{ act on } m_t^{t'}] \geq \varepsilon \end{aligned}$$

which contradict the fact that \mathcal{P} terminate a.s.

Lemma II. Let \mathcal{P} be a protocol (which could use a random and quantum bits) that terminates all most surely. Then for every pair $\delta, \varepsilon > 0$ and a fixed less than f non-honest parties there exists a quantum circuit $U_{\delta, \varepsilon}$ which, with at least $1 - \delta$ probability, ε -approximates the running of protocol. When we think over secrets which shared by D as an input state $|\psi_D\rangle$ for $U_{\delta, \varepsilon}$. the That it:

$$\Pr[\|U_{\delta, \varepsilon}|\psi_D\rangle - \mathcal{P}(|\psi_D\rangle)\| < \varepsilon] > 1 - \delta$$

Proof. Consider first only a deterministic non honest parties, and denote them by p_1, p_2, \dots, p_l . By the fact that the protocol ends with probability a.s we know that for any $\delta > 0$ there exists t_0 such that for any $t > t_0$ the

$$\Pr[\mathcal{P} \text{ take time } > t] < \delta$$

Now, by the determinism of the faults parties we know that for each party p_i there exist a function $f_i : \text{running history} \rightarrow \{\Sigma\}^n$ which for any run at length t steps returns the n messages which will sent to the other parties.

By **Lemma I** we know that there is M such that the probability that f_i will act not trivially on the coordinates greater then M is less then δ . Let f' be the function which read only the first M bits of given input and return:

$$f'(x_1, \dots, x_\infty) = f(x_1, \dots, x_M, 0, 0, \dots)$$

As we know for any $n', \varepsilon' > 0$ there is a finite set of states which is ε' -approximate any state over less than n' qubits.

[COMMENT] Enter here the fact that the error grow additively Using the fact that any under the promise that any a set of gates approximate by $\varepsilon \dots \Rightarrow$ take $\varepsilon' = \frac{1}{t}\varepsilon$.

$$\begin{aligned} & \Pr [\|U_{\delta,\varepsilon} |\psi_D\rangle - \mathcal{P}(|\psi_D\rangle)\| < \varepsilon] \\ &= \Pr [\|U_{\delta,\varepsilon} |\psi_D\rangle - \mathcal{P}(|\psi_D\rangle)\| < \varepsilon | T < t] \Pr [T < t] \\ &+ \Pr [\|U_{\delta,\varepsilon} |\psi_D\rangle - \mathcal{P}(|\psi_D\rangle)\| < \varepsilon | T > t] \Pr [T > t] \\ &\geq \overbrace{\Pr [\|U_{\delta,\varepsilon} |\psi_D\rangle - \mathcal{P}(|\psi_D\rangle)\| < \varepsilon | T < t]}^1 \Pr [T < t] \\ &\geq 1 - \delta \quad \square \end{aligned}$$

Assume that the dealer D is honest, then we can separate the running into two phase, The first one is the initialization of the input state, then the second is the actually sharing.

Assume by induction that there is a circuit $U_{\varepsilon,\delta}$ that simulate runs conditional that the original. for every running with length less than t there exist a

From now on, we will think over the protocol as a finite depth quantum circuit, which measure only in the end.

Definition.

Lemma II. Denote by $H_{succ,1} \subset \mathcal{H}$ the subspace such that for every

$$\forall |\psi\rangle \in \text{Image}(U_{\delta,\varepsilon} H_{succ,1}) \Rightarrow \langle \psi | \overbrace{11\dots 11}^{\text{n-f}} \text{junk} \rangle > \frac{1}{\sqrt{2}}$$

Similarly let H_{fail} be the space of inputs that $U_{\delta,\varepsilon}$ doesn't get in into agreement over them (the complementary of H_{succ}). Then for every $|\xi\rangle \in H_{fail}$ there exists $|\eta\rangle \in H_{succ}$ and single-qubit operation $P : \mathcal{H}_2 \rightarrow \mathcal{H}_2$ such that $P \otimes I |\xi\rangle = |\eta\rangle$.

Proof of Theorem 1. Consider $\Gamma > 0$ and assume that the first option doesn't hold. i.e for a.s terminate protocol \mathcal{P} , a faulty dealer doesn't have a strategy in which he wins with probability greater than Γ . In particular, when the dealer shares some $|\xi\rangle \in H_{fail}$.

Fix $\varepsilon, \delta > 0$ such that with probability at least $1 - \delta$ the gate $U_{\delta,\varepsilon}$ approximates \mathcal{P} . Hence we get that

$$\langle \xi | U_{\delta,\varepsilon} | \mathbf{GHZ} \rangle > \frac{1}{\sqrt{2}}$$

In particular. let's look at strategy in which the dealer sends for $n - 2$ parties the secret $|1\rangle$ and for the remaining party B he sends the secret $|0\rangle$. In that case, the corresponded input for the circuit $U_{\delta,\varepsilon}$ will be

$$|\psi_D\rangle = |1111\dots 11 \overbrace{0}^{\text{B's share}} 111\dots 11 \overbrace{000\dots 0}^{\text{ancillaries}} \rangle$$

We will think over the protocol as a quantum circuit from now on. In addition, we will part the circuit into three vertical parts R_A, R_B, R_C associated with parties A, B , and C , respectively. Each connection (edge, shared gate) between the parts matches a state exchanging. Visual demonstration can be find in **Figure 1**.

Definition. We will say that a pure state is an **un-committed ket** if it matches a case that the non-faulty parties points different values for the secret.

Lemma II. Consider a gate U which act on n qubits and commute with permutations (symmetrically to the inputs pins). If adversary enters $\Theta(n)$ of the input, then he can ensures that the circuit will outputs will have a constant weight over **uncommitted ket**.

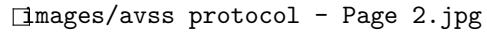
images/avss protocol - Page 2.jpg

Figure 1: U_ε illustration.

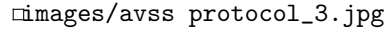
images/avss protocol_3.jpg

Figure 2: U_ε illustration.

Lemma II. Consider the case when the dealer D is faulty. Then the resulting state of the computation over the input has nonzero weight for the an uncommitted ket.

Lemma III. Consider the case when the party B is faulty. Then he could boost indistinguishability, which mean that he could amplify the weight of uncommitted ket.