This dissertation documents the design and implementation of a potential solution to the questions posed in §\ref{sec:motivation}, while attempting to follow the constraints restricting the highlighted systems in the real world. In particular, I contribute the following:

* I create a client-server application simulating the device-server stack utilised by existing products, allowing secure transmission of video data from client to server and back again after performing inference.
* I use Microsoft’s Secure Encrypted Arithmetic Library (SEAL) [SEAL] to integrate the CKKS HE scheme [CKKS] for encrypting videos while they are away from the client.
* I implement a series of algorithms for enabling private and plain inference of video data to extract moving objects by producing a mask that can be applied to videos in the clear by the client.
* I investigate Gaussian Mixture Models (GMMs) for background subtraction, beginning with the work by Stauffer and Grimson [STAUFFER] then moving into more general Expectation-Maximisation GMM algorithms [SOURCE?].
* As an extension, I build a toy CKKS implementation called MeKKS based on the Homomorphic Encryption for Arithmetic of Approximate Numbers paper by Cheon et al. [HEAAN] to improve understanding of HE.
* I demonstrate the efficacy of my solution using timing, accuracy, and (hopefully) energy usage data to compare the results of plain video, CKKS encrypted data, and MeKKS encrypted data.