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 aforementioned real-world systems. In particular, the contribution of the work is:

* The creation of 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.
* The use of 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.
* The implementation of 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.
* An investigation of Gaussian Mixture Models (GMMs) for HE encrypted background subtraction, beginning with the work by Stauffer and Grimson [STAUFFER] then moving into more general Expectation-Maximisation GMM algorithms [SOURCE?].
* As an extension, the fabrication of a CKKS implementation from scratch, called MeKKS, based on the Homomorphic Encryption for Arithmetic of Approximate Numbers paper by Cheon et al. [HEAAN] to improve understanding of HE.
* A demonstration of the efficacy of the above solutions using timing, accuracy, and \textit{(hopefully)} energy usage data to compare inference of CKKS and MeKKS solutions to plain videos, highlighting the advantages of the MeKKS implementation being targeted to this application over the more generic CKKS.