
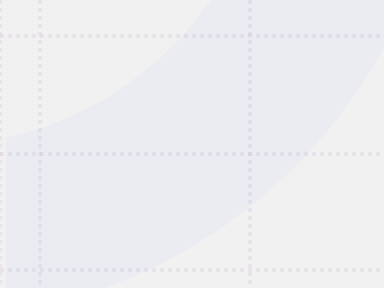


Distributed Minds

Naga Srihith Penjarla: A cybersecurity enthusiast currently working on the optimization of the AES algorithm in IoT devices in a secure multiparty computation setup at IIIT Bangalore.

Mayank Kabra: Worked on Field-Programmable Gate FPGA, Internet of Things (IoT), Vivado, GTKWave, programming of microcontrollers. Major interest in Hardware Design

Nandakishore Menon: A cybersecurity enthusiast, developer and Research Intern at IIIT Bangalore, working in the field of cryptography.



Using Multi-Party Computation Protocol to secure DNS in IoT Devices

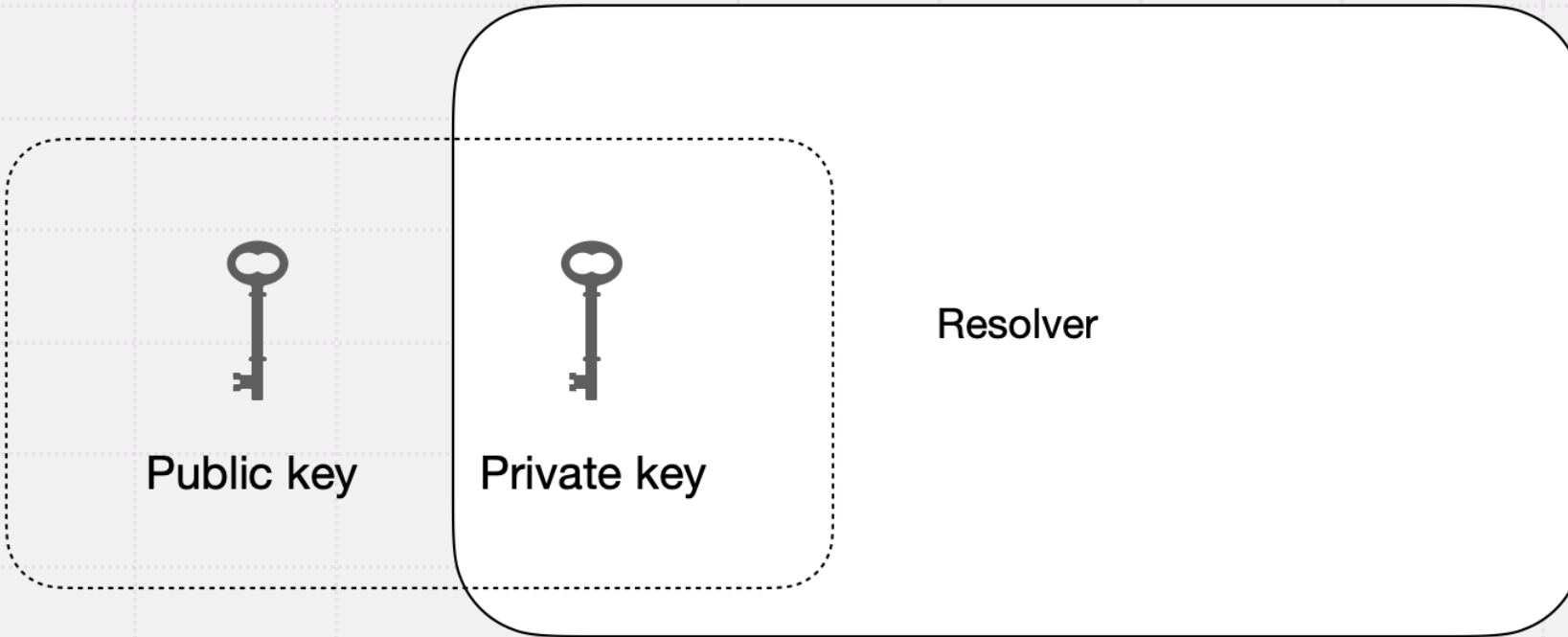
Motivation

IoT devices are vulnerable largely as these devices lack the necessary built-in security to counter threats.

We propose a solution to secure an ecosystem of IoT devices against man-in-the-middle attacks.

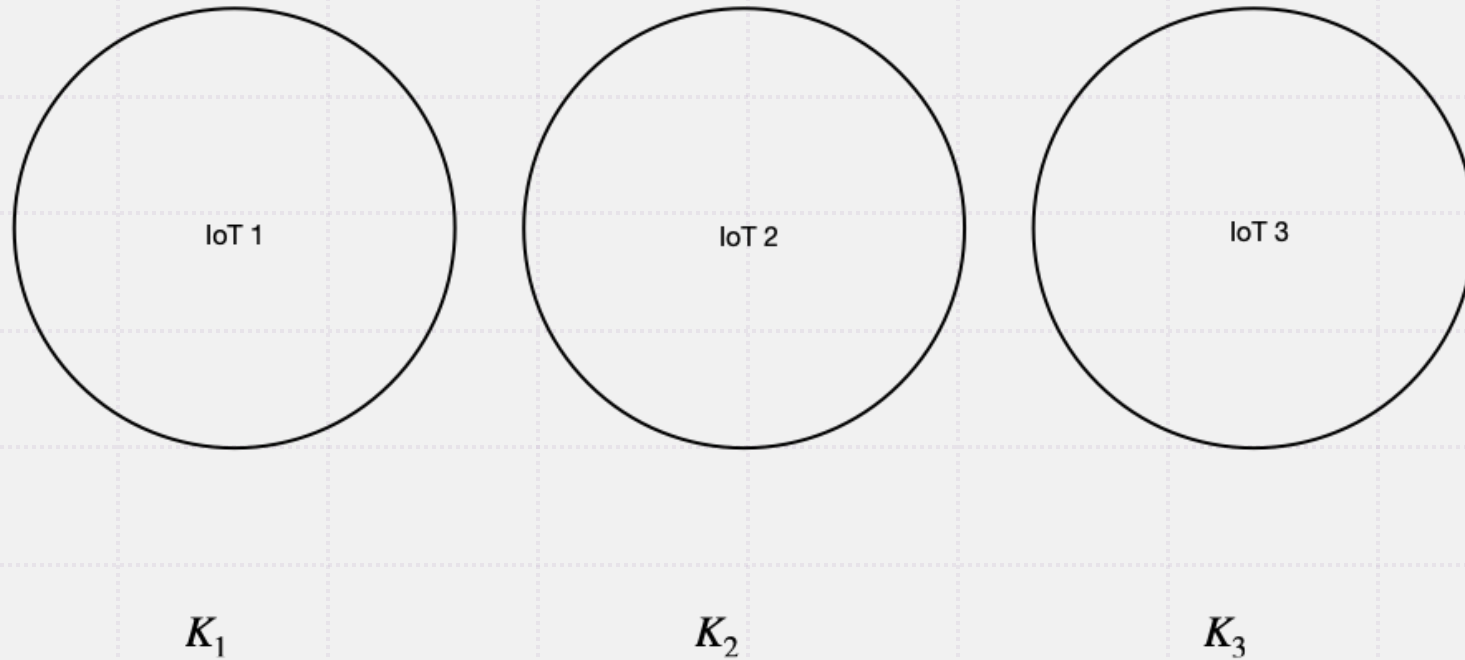
The attacker can compromise the session key by using malicious code or programs running at the client-side. We prevent this by keeping the session key distributed among multiple devices.

Server-side



- Asymmetric key pair
- Public key known to all the clients

Client-side



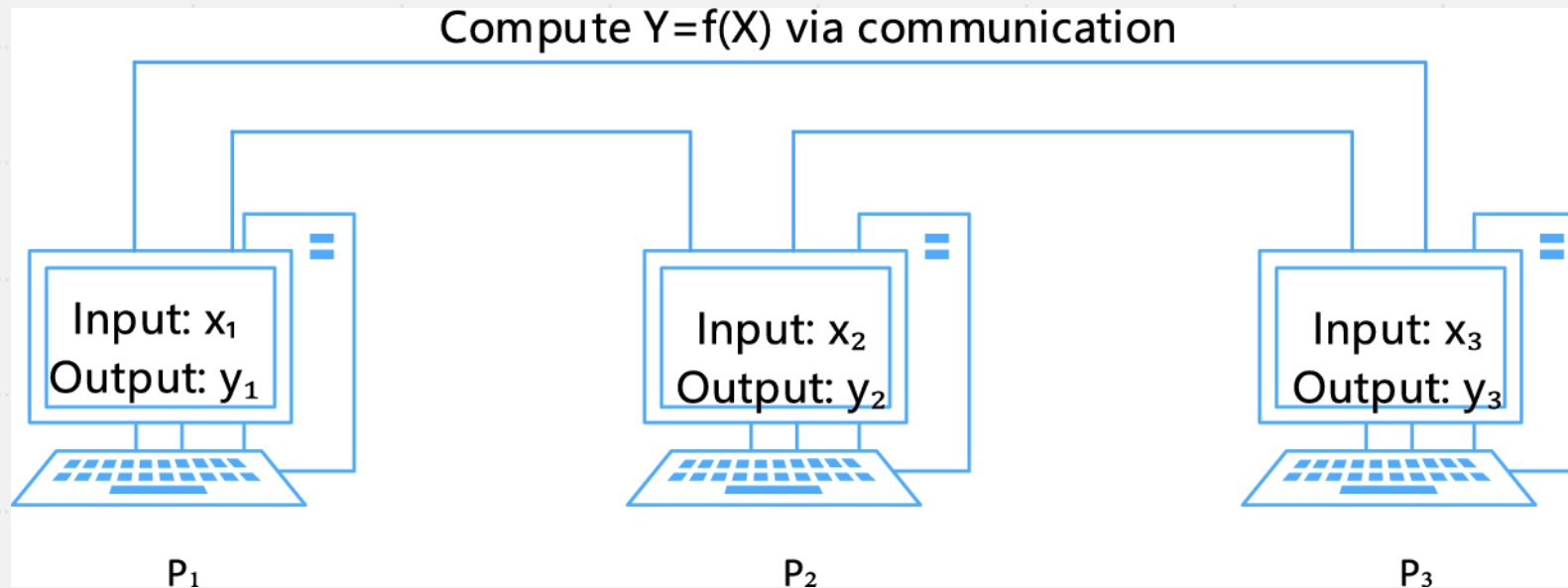
- Generation of key in shared format
- To avoid single point-of-compromise

Encrypting key to be sent to the resolver



- Encrypting the shared key with the public key of the resolver via MPC
- Key is communicated to the resolver before each query

MPC – Multiparty Computation



- Secure multiparty computation is used to encrypt the symmetric key K . The encrypted key will exist in shared form across the devices and no party shall have the whole key.

DNS Query

- Querying device secret shares the query
- The query is encrypted using the MPC protocol
- Encrypted query is constructed at the querying device
- Both the encrypted key & the encrypted query is now sent to the resolver

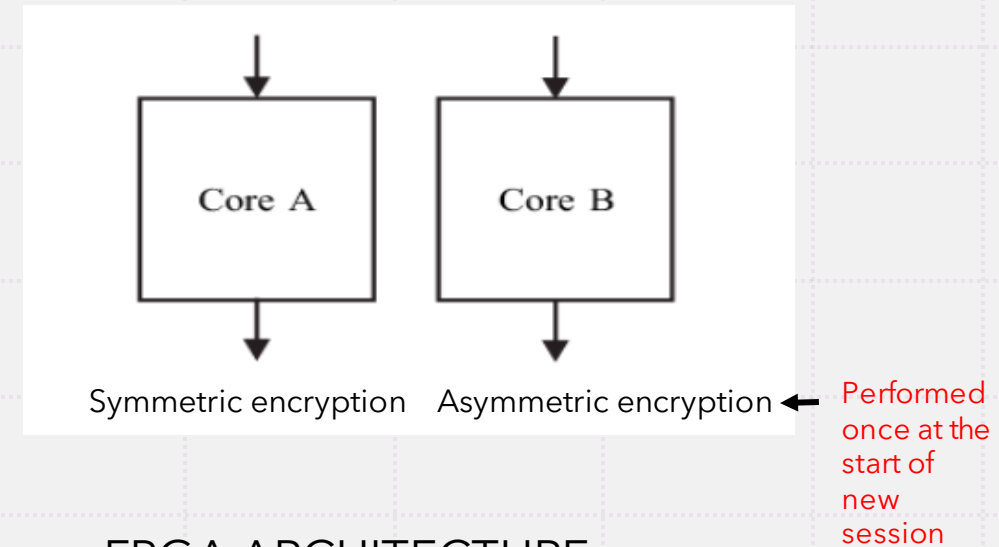
Caching

- Proxy server stores the encrypted queries/responses
- All the queries/responses are passed to and from the proxy server
- Flushes after the key is renewed or the TTL of a query is reached.

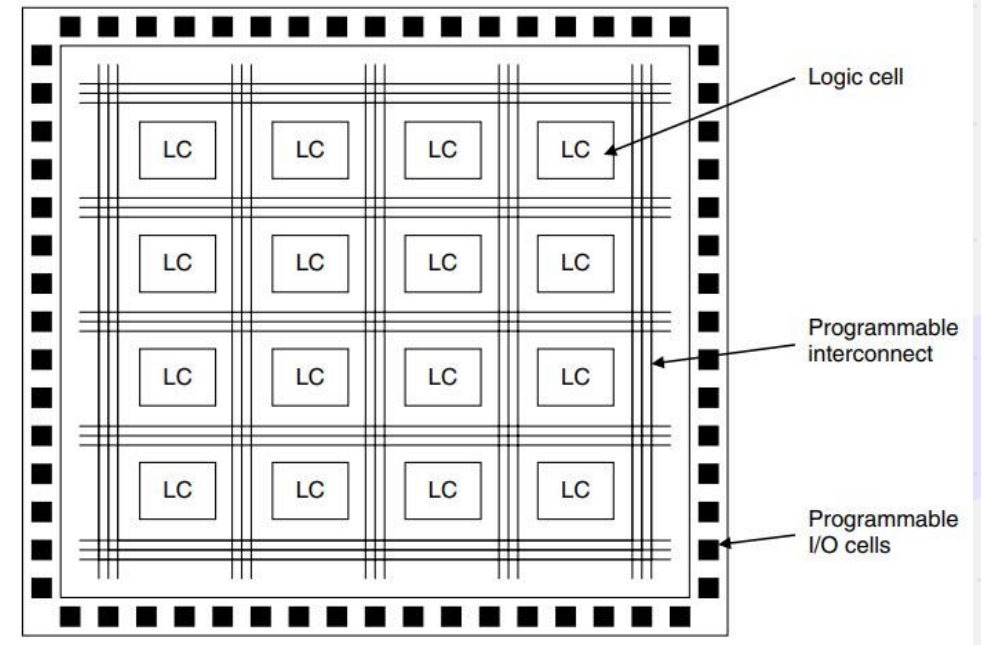
Implementation

- One way is to use a dual core microcontroller. Core A will be performing the symmetric encryption on the query, meanwhile Core B will wake-up from deep sleep mode and perform asymmetric encryption on the generated symmetric key only once in the session, e.g., ARM Cortex-M4 or M0+.
- Other way is to implement it on the FPGAs which are used as IoT devices. They can act as an accelerator to implement the encryption algorithms at the LUT and circuit level.

DUAL CORE ARCHITECTURE



FPGA ARCHITECTURE



Future Impact

- The protocol presented here is scalable to an n-party setup. This could enhance the security of an ecosystem of IoT devices that require internet access, as found in smart homes.
- Eliminates the need to generate keys for each session. This is especially useful when queries are made frequently, as it saves resources and time (since AES is faster than RSA) when compared to a standard DNS query using RSA.