Identification Scheme For Constrained IoT Devices
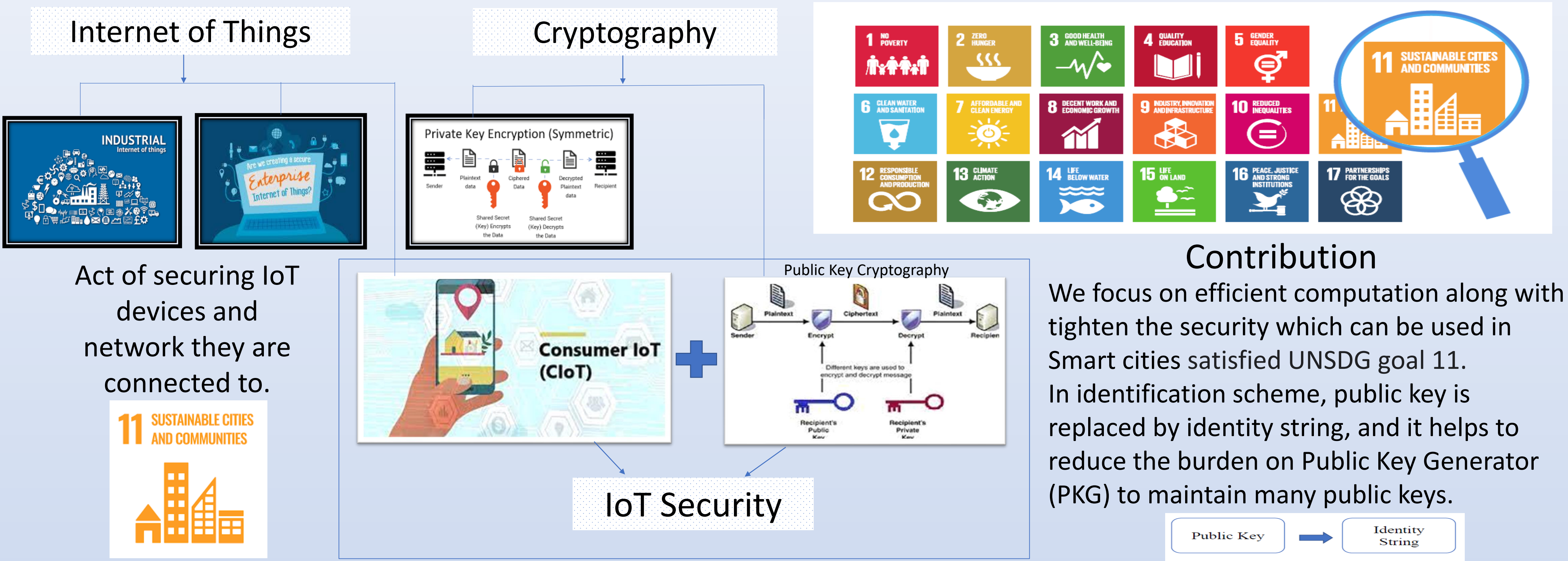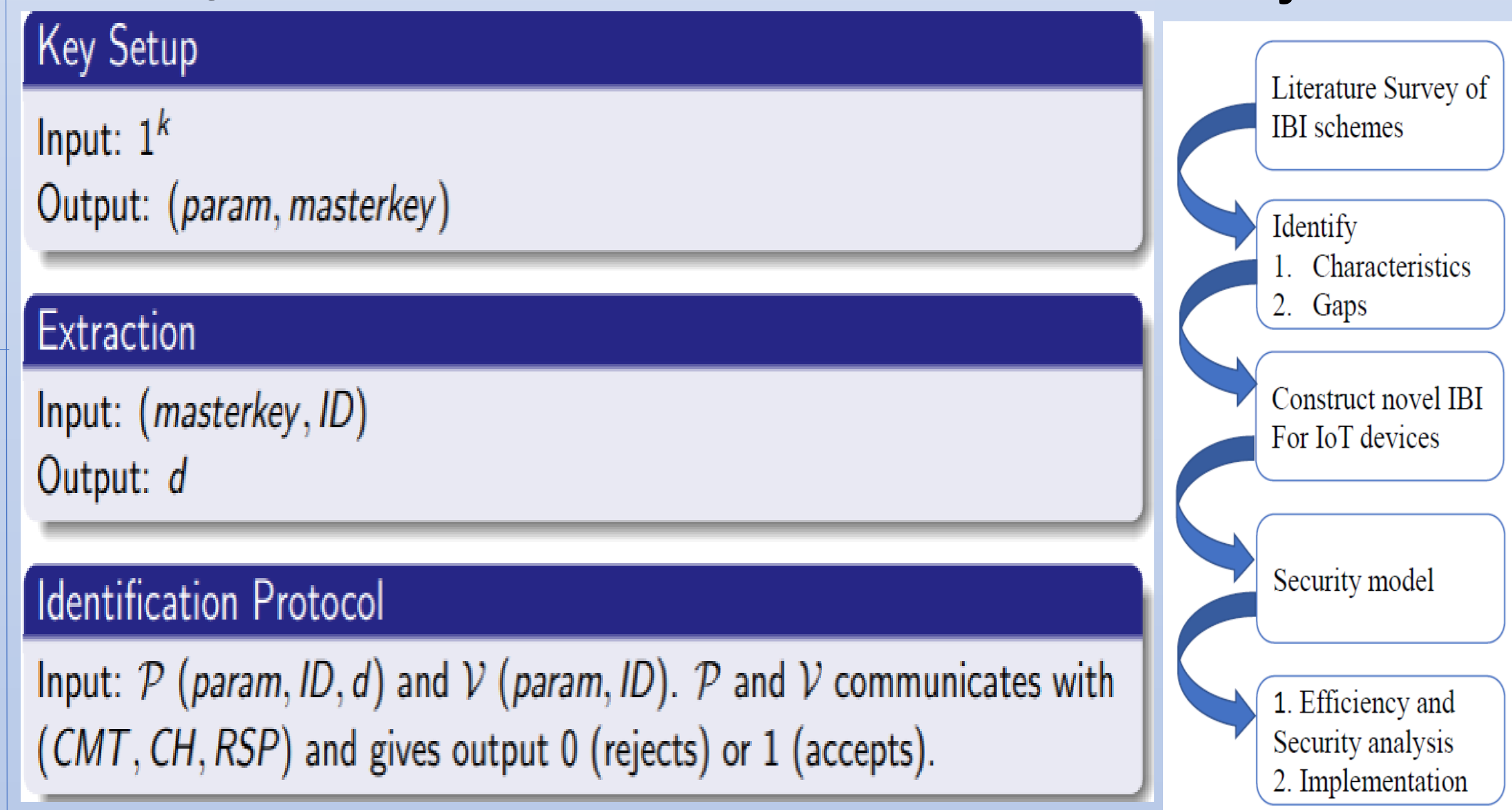
Presenter: Apurva Kiran Vangujar; Supervisor: Dr. Paolo Palmieri; Co-Supervisor: Dr. Dirk Pesch

Internet of Things

Act of securing IoT devices and network they are connected to.

11 SUSTAINABLE CITIES AND COMMUNITIES

Cryptography

Private Key Encryption (Symmetric)

Consumer IoT (CIoT)

Public Key Cryptography

IoT Security

1 NO POVERTY
2 ZERO HUNGER
3 GOOD HEALTH AND WELL-BEING
4 QUALITY EDUCATION
5 GENDER EQUALITY
6 CLEAN WATER AND SANITATION
7 AFFORDABLE AND CLEAN ENERGY
8 DECENT WORK AND ECONOMIC GROWTH
9 INDUSTRY INNOVATION AND INFRASTRUCTURE
10 REDUCED INEQUALITIES
11 SUSTAINABLE CITIES AND COMMUNITIES
12 RESPONSIBLE CONSUMPTION AND PRODUCTION
13 CLIMATE ACTION
14 LIFE BELOW WATER
15 LIFE ON LAND
16 PEACE, JUSTICE AND STRONG INSTITUTIONS
17 PARTNERSHIPS FOR THE GOALS

Contribution

We focus on efficient computation along with tighten the security which can be used in Smart cities satisfied UNSDG goal 11.
In identification scheme, public key is replaced by identity string, and it helps to reduce the burden on Public Key Generator (PKG) to maintain many public keys.

Public Key → Identity String
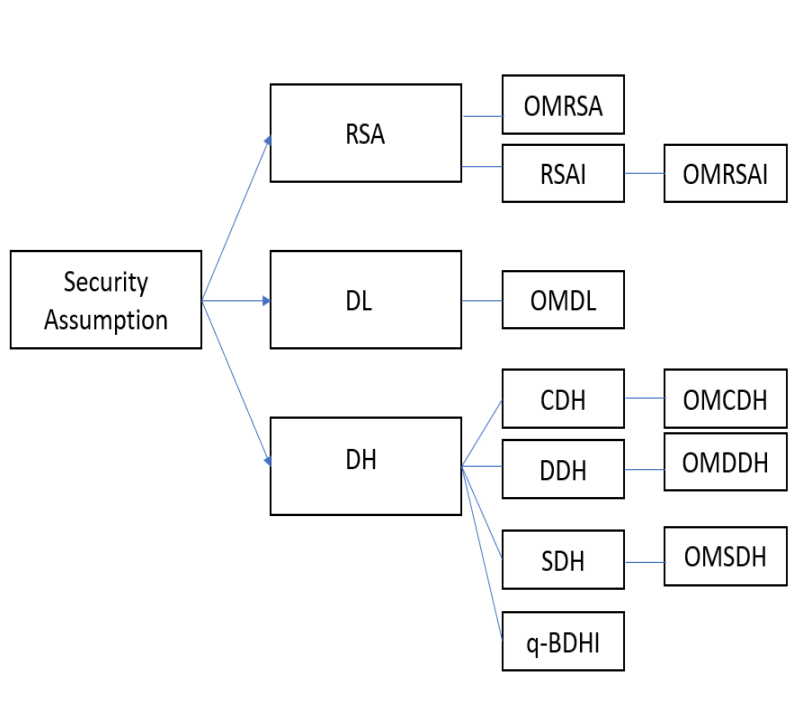
Literature Survey Results

1. Our objective was to compare and contrast various IBI schemes based on various scheme assumptions in order to determine whether they could be used in IoT devices or not.
2. There is a high potential for applying CDH, DDH, and q-SDH assumptions in any type of IoT environment, including group, hierarchical, and so on.
3. .As with DL, OMDL has an application in MANETS. A new scheme that is based on DL assumptions can be made and used to make MANETS more secure.

Identity-Based Identification (IBI) Scheme

Key Setup

Input: 1^k

Output: $(param, masterkey)$

Extraction

Input: $(masterkey, ID)$

Output: d

Identification Protocol

Input: $\mathcal{P}(param, ID, d)$ and $\mathcal{V}(param, ID)$. $\mathcal{P}$ and $\mathcal{V}$ communicates with (CMT, CH, RSP) and gives output 0 (rejects) or 1 (accepts).

Objectives

Literature Survey of IBI schemes

Identify
1. Characteristics
2. Gaps

Construct novel IBI For IoT devices

Security model

1. Efficiency and Security analysis
2. Implementation

Motivation

Security Assumption → RSA → OMRSA, RSAI → OMRSAI
DL → OMDL
DH → CDH → OMCDH, DDH → OMDDH, SDH → OMSDH, q-BDHI
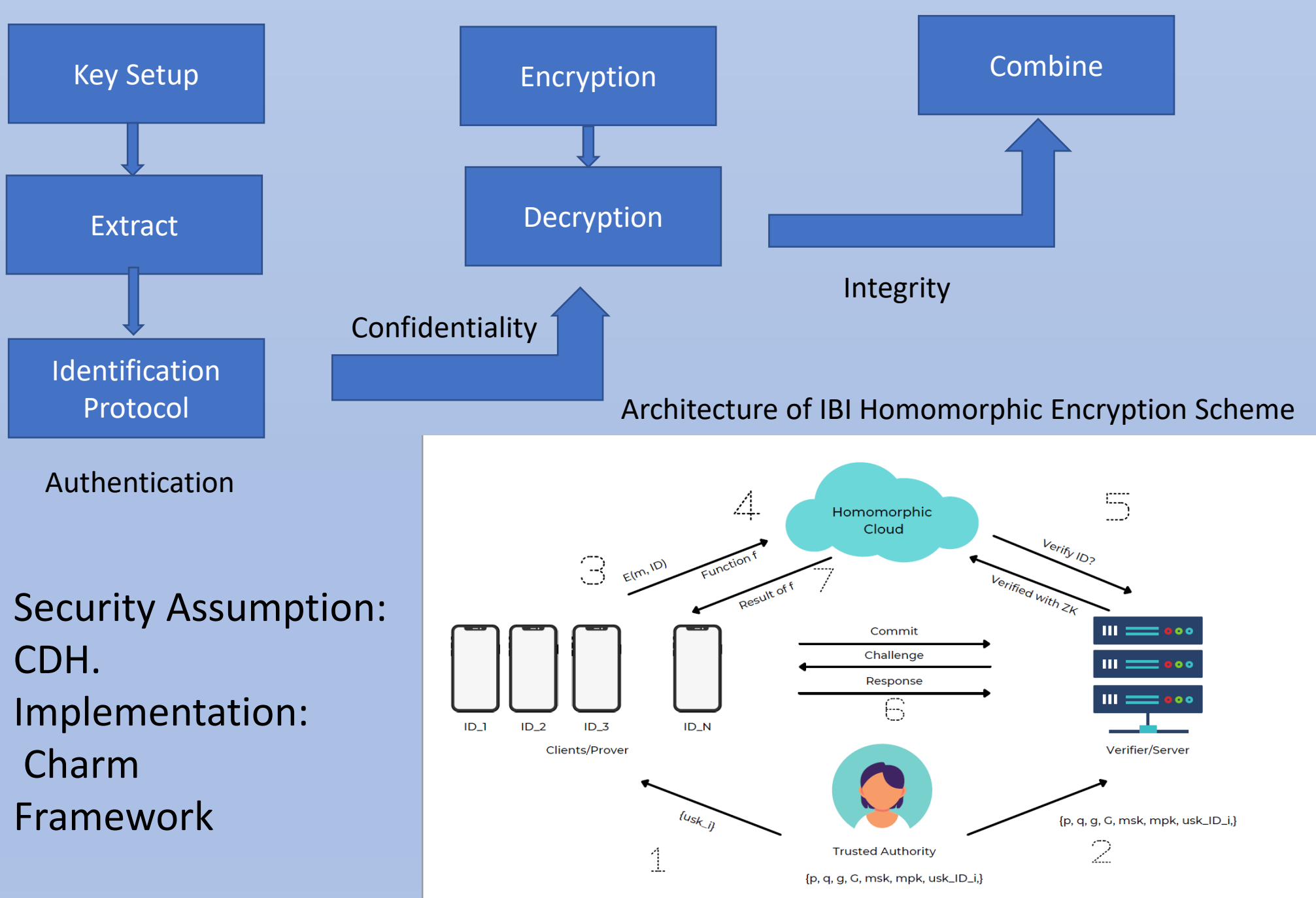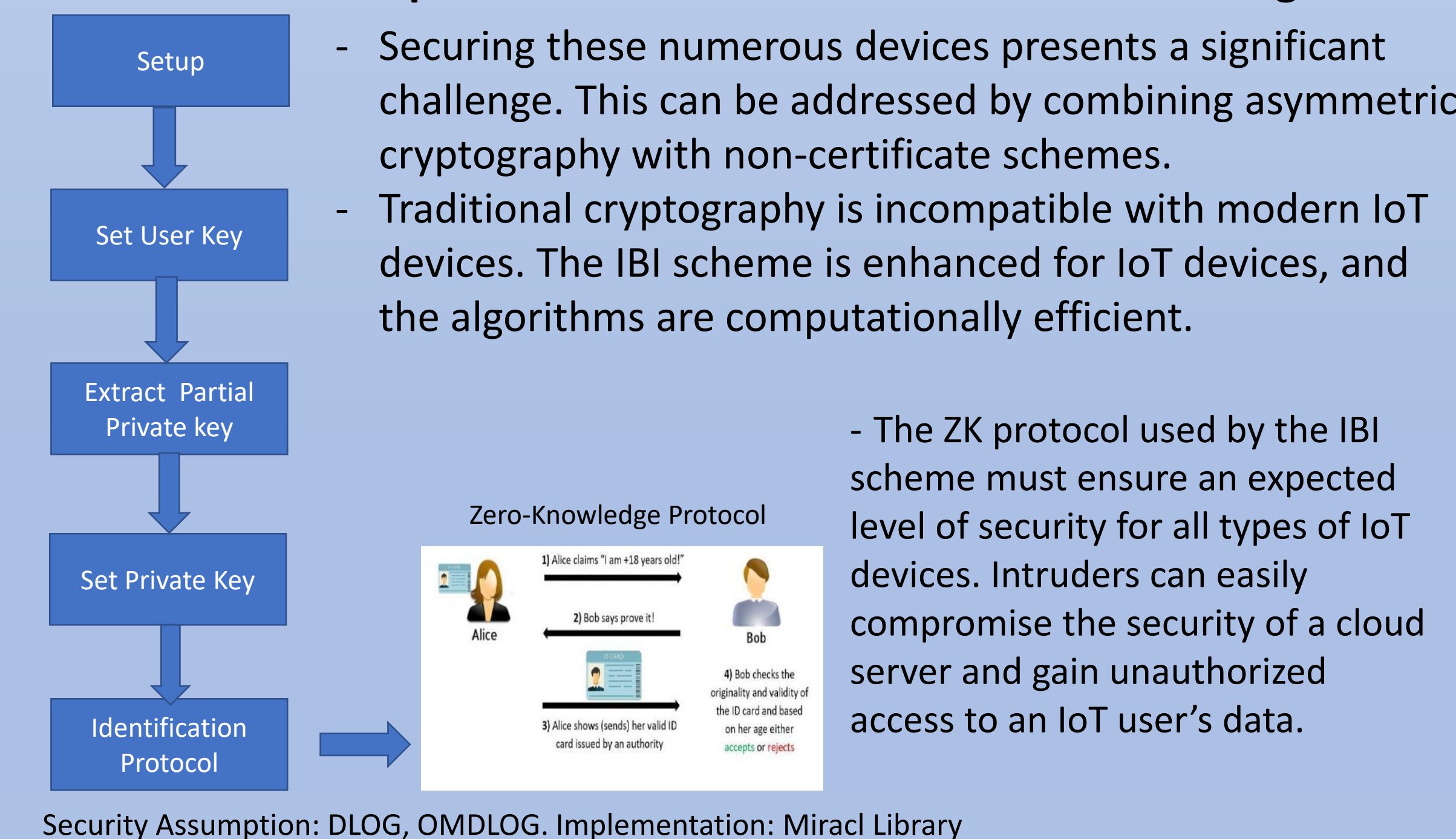
1. Our target is securing all IoT devices under **one roof**.
2. Multiple IoT devices focus on **tight security** and **more efficiency**
3. It **verifies** large number of IoT devices at a **one time**.

IBI Homomorphic Encryption Scheme

Key Setup → Extract → Identification Protocol

Encryption → Decryption

Combine

Confidentiality

Integrity

Authentication

Architecture of IBI Homomorphic Encryption Scheme

Security Assumption: CDH.
Implementation: Charm Framework

Certificateless Group Identification Scheme for Internet of Things

Setup → Set User Key → Extract Partial Private key → Set Private Key → Identification Protocol

- Securing these numerous devices presents a significant challenge. This can be addressed by combining asymmetric cryptography with non-certificate schemes.
- Traditional cryptography is incompatible with modern IoT devices. The IBI scheme is enhanced for IoT devices, and the algorithms are computationally efficient.

Zero-Knowledge Protocol

- The ZK protocol used by the IBI scheme must ensure an expected level of security for all types of IoT devices. Intruders can easily compromise the security of a cloud server and gain unauthorized access to an IoT user's data.

Security Assumption: DLOG, OMDLOG. Implementation: Miracl Library

CONCLUSION

This project would be helpful to improve the smart cities security. Our objective was to compare various IBI schemes based on various scheme assumptions in order to determine whether they could be used in IoT devices or not. There is a great deal of work that can be done to extend the IBI scheme's application to the IoT. This way, most of the benefits of the IBI scheme can be kept for IoT devices and their communication