SOK it to the IoT

Michael Scott, Kealan McCusker
MIRACL

October 18, 2016

Introduction

- SOK protocol
  - Type - 1 Pairing
  - Type - 3 Pairing
- The Apache Milagro Crypto Library
- IoT
- Distributed trust authorities

SOK Type-1 Pairing

- Non-interactive authenticated key exchange protocol
- Type-1 pairing – supersingular elliptic curve
  - $g = e(P, Q), P \in \mathbb{G}_1, Q \in \mathbb{G}_1, g \in \mathbb{G}_T$
  - $\mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_T$
  - $\mathbb{G}_1$ group of points on the curve over the base field $\mathbb{F}_p$
  - $\mathbb{G}_T$ are elements in the subgroup embedded in the finite extension field $\mathbb{F}_{p^k}$
  - All groups are of prime order q

SOK Type-1 Pairing (cont)

- Bilinearity property
  - $e(sA, B) = e(A, sB) = e(A, B)^s, A \in \mathbb{G}_1, B \in \mathbb{G}_1$
- Symmetric
  - $e(A, B) = e(B, A)$
- Embedding degree $k = 2$
  - $p = 1526$ for AES-128 bit security

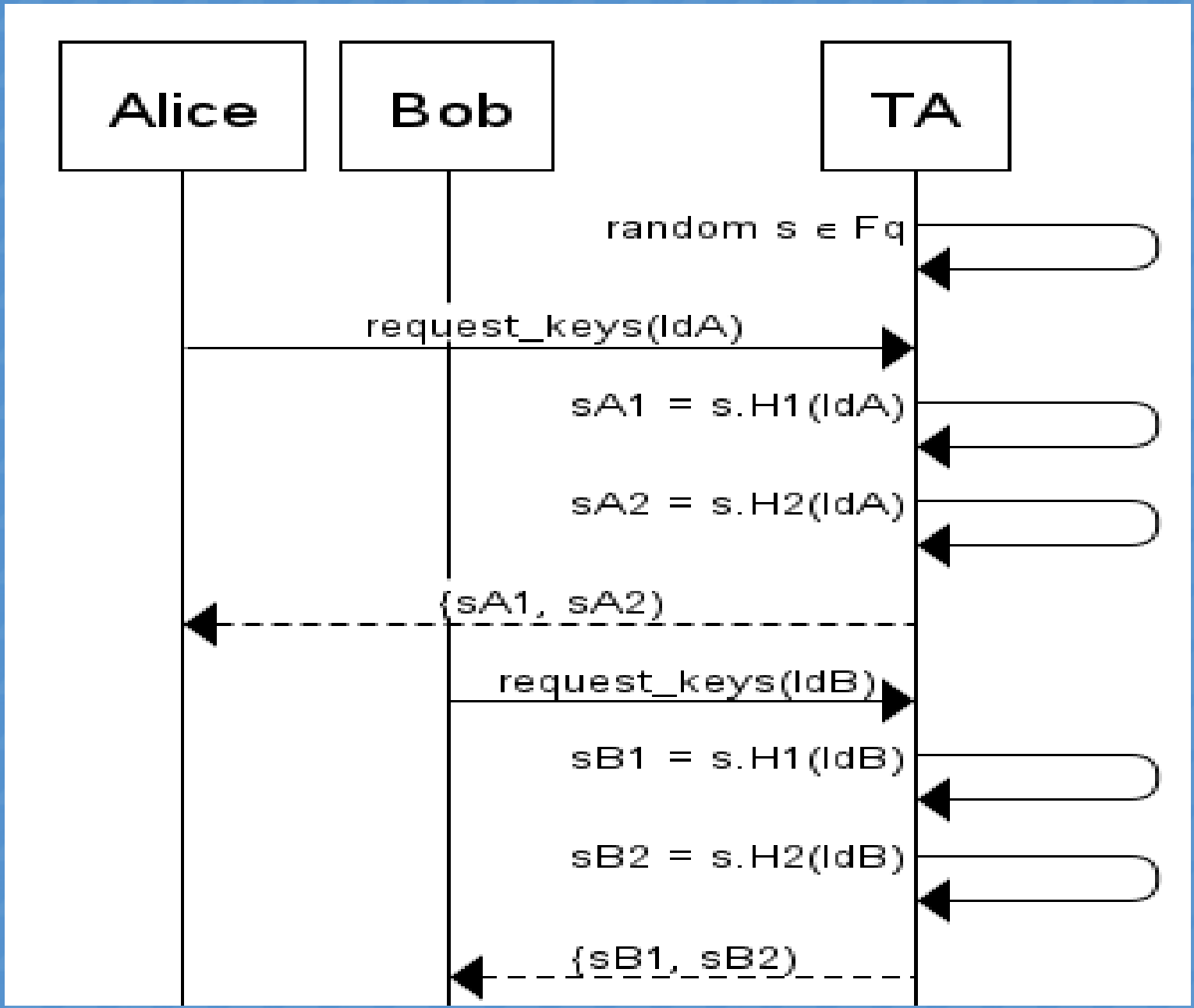
SOK Type-3 Pairing

- Type-3 pairing – non-supersingular pairing friendly elliptic curves
  - $\mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$
  - $\mathbb{G}_1$ group of points on the curve over the base field $\mathbb{F}_p$
  - $\mathbb{G}_2$ are group of points on the twist of the curve over an extension field
  - $\mathbb{G}_T$ are elements in the subgroup embedded in the finite extension field $\mathbb{F}_{p^k}$
  - All groups are of prime order q

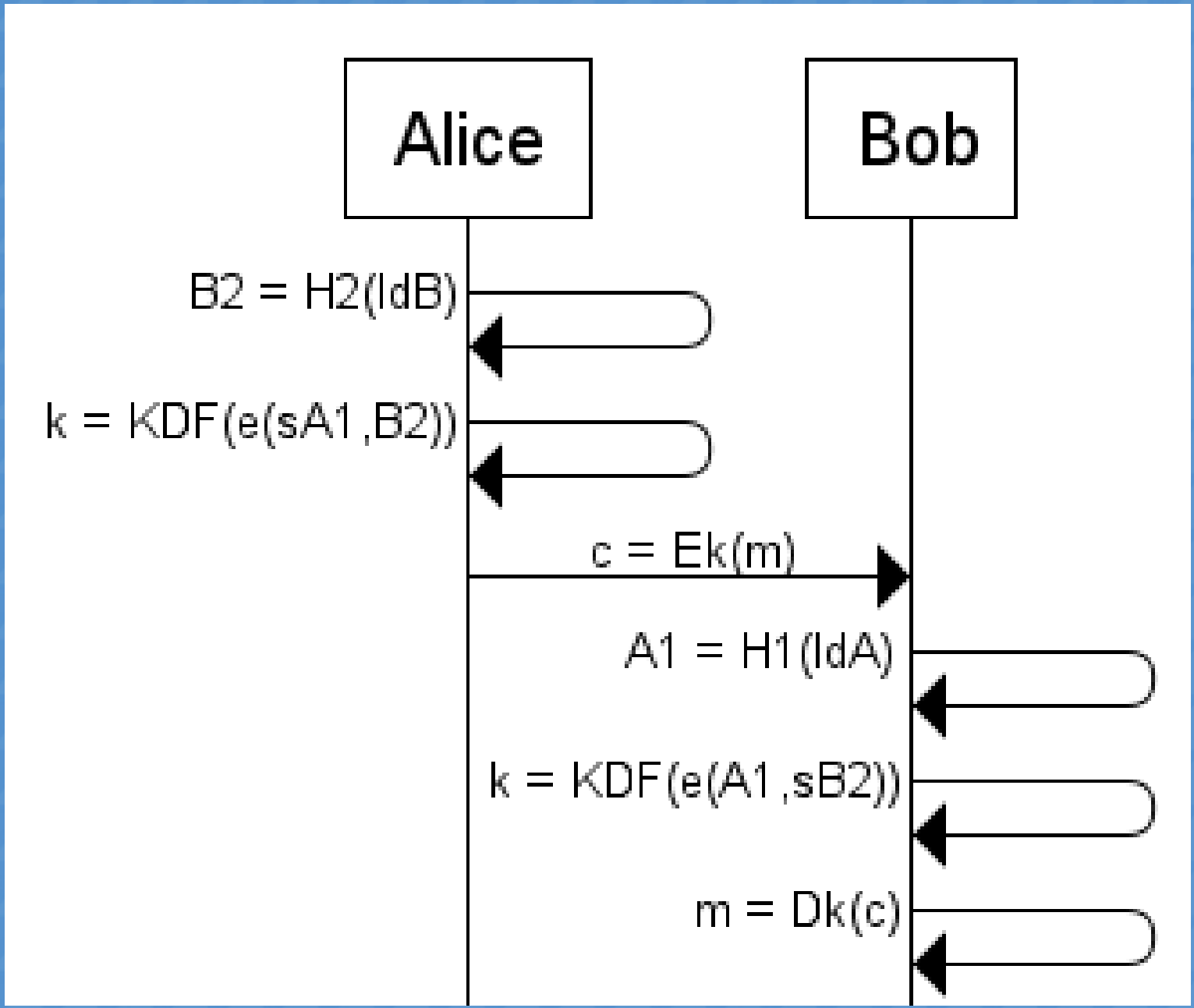
SOK Type-3 Pairing (cont)

- Bilinearity property
  - $e(sA, B) = e(A, sB) = e(A, B)^s, A \in \mathbb{G}_1, B \in \mathbb{G}_2$
- Asymmetric
  - $e(A, B) = e(B, A)$
- BN Curves – Embedding degree $k = 12$
  - $p = 256$ for AES-128 bit security
- Sender (left-hand) and receiver (right-hand) keys

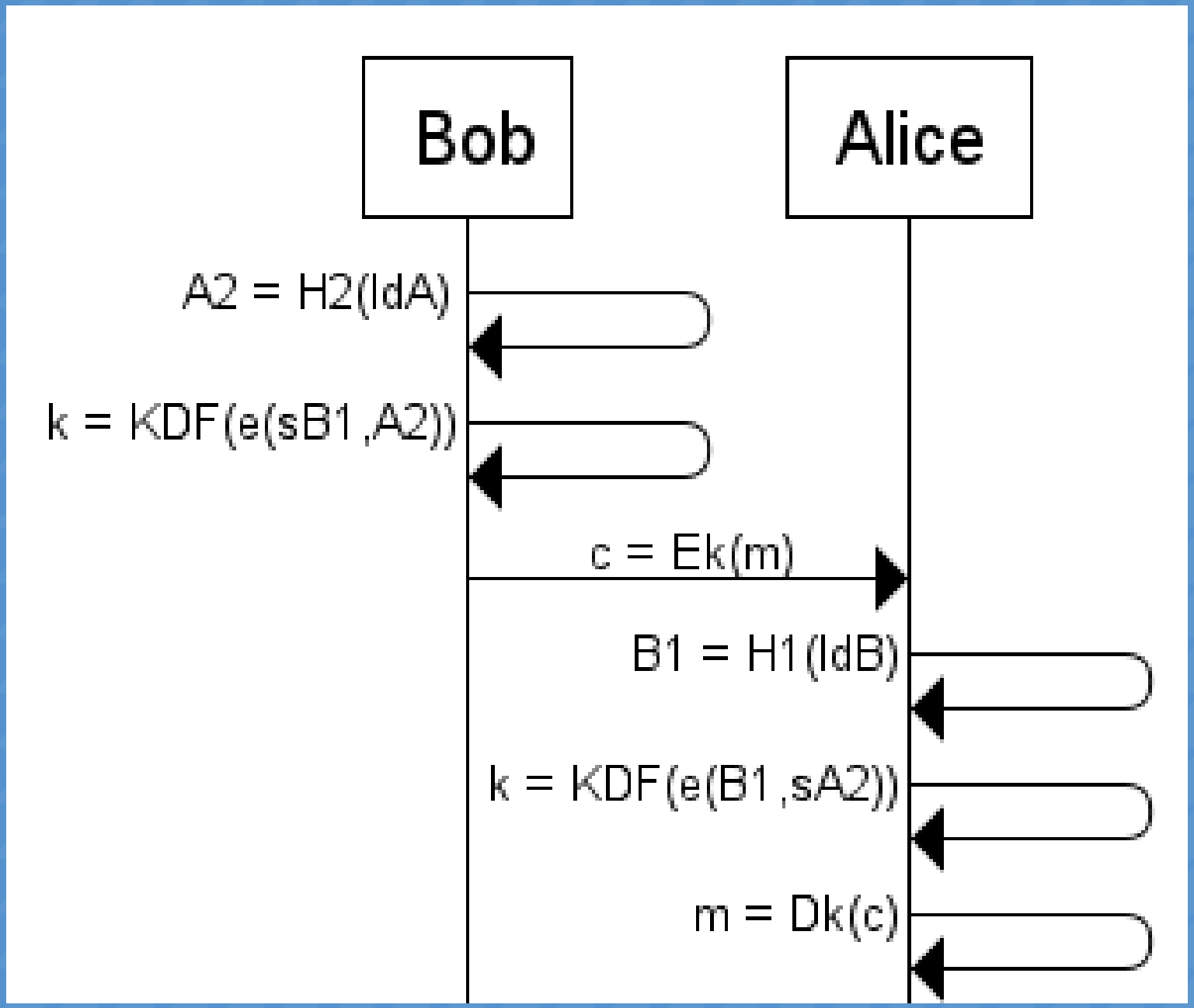
SOK protocol – setup



SOK protocol – key agreement 1



SOK protocol – key agreement 2



The Apache Milagro Crypto Library

- AMCL `https://github.com/MIRACL/amcl.git`
- Support for the Internet of Things
  - Self-contained
  - Portable – no assembly language
  - Optimized for size not speed
  - Configurable for 16/32/64 bit machines
  - Security level equivalent to 128 – 256-bit AES
  - Small code base
- Multi-lingual crypto library – Java, GO, JavaScript, C#, Rust, Swift, C

The Apache Milagro Crypto Library (cont)

- Supported primitives
  - AES/128/192/256
  - SHA256/384/512
  - ECDH, ECDSA, ECIES for prime field elliptic curves
  - RSA/2048/3072/4096
  - X509 support
  - Pairing based cryptography - BN / BLS curves
- Weierstrass, Edwards and Montgomery curve types
- Protects against side-channel attacks - avoid unpredictable program branches

Implementation

- Raspberry Pi computer (32-bit, Version 1, 700MHz)
- AES-128 security level

curve	time	ROM	RAM
256 bit BN	86ms	85K	8K
455 bit BLS	455ms	85K	16K

Table 1: SOK Performance

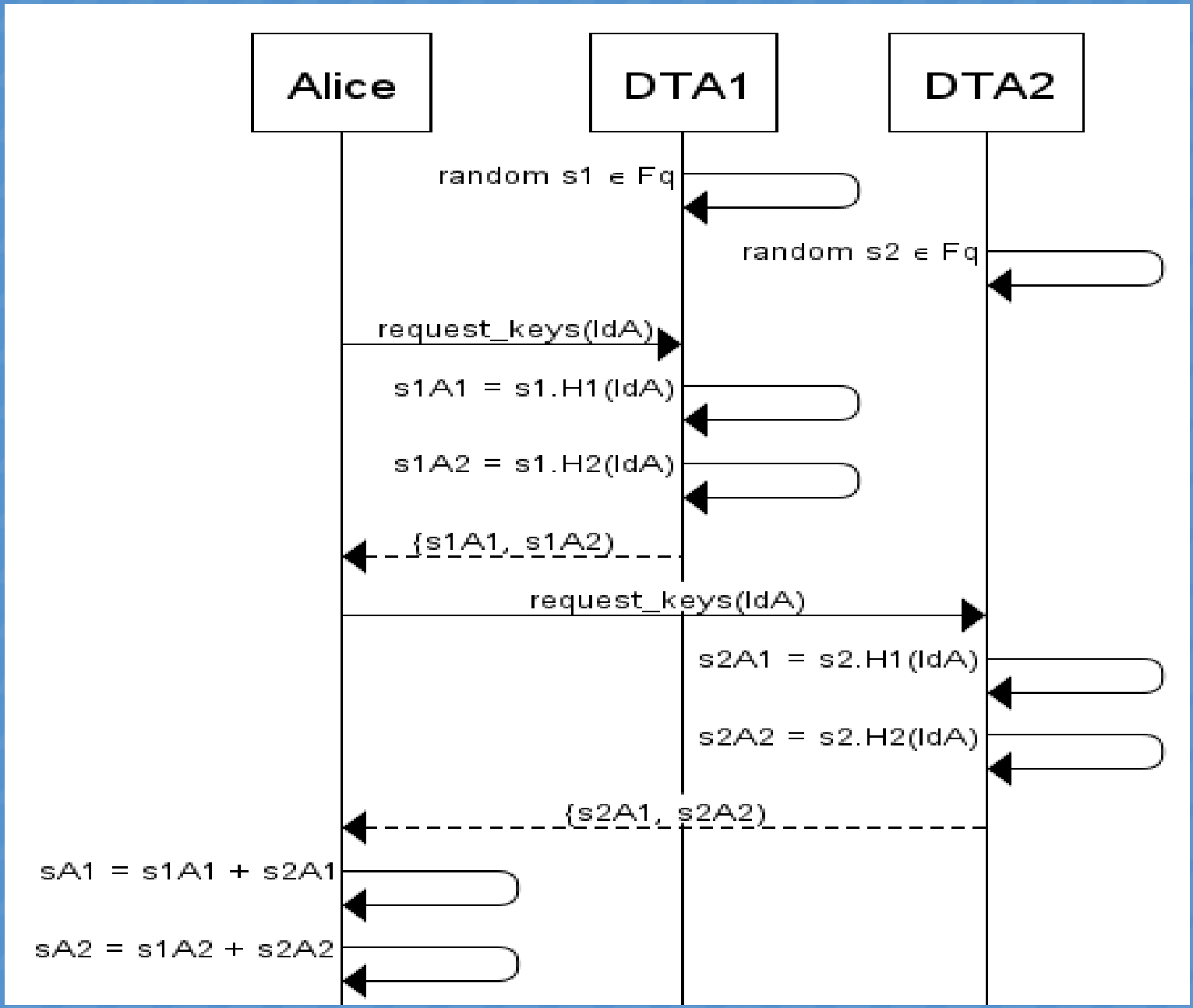
IoT

- Device has serial number that acts as its identity
- Device manufacture acts as TA
- SOK is run at start-up
  - mutually authenticated encrypted channel
  - Store table of AES keys in immediate network
  - Diffie-Hellman
- Devices could be divided into senders and receivers
  - Receivers could be data aggregators – more secure
  - Receiver could be network access point
- Energy constrained devices – less radio operations

Distributed Trust Authority (DTA)

- Distribute trust - multiple DTAs
- No single-point-of-failure
- Each DTA has unique secret s_1, s_2 etc.
- Each DTA generates shares of SOK secrets
- Point addition it used to combine SOK secret on device

Distributed Trust Authority (cont)



Thank You