FSU: Identity-based Authenticated Key Exchange

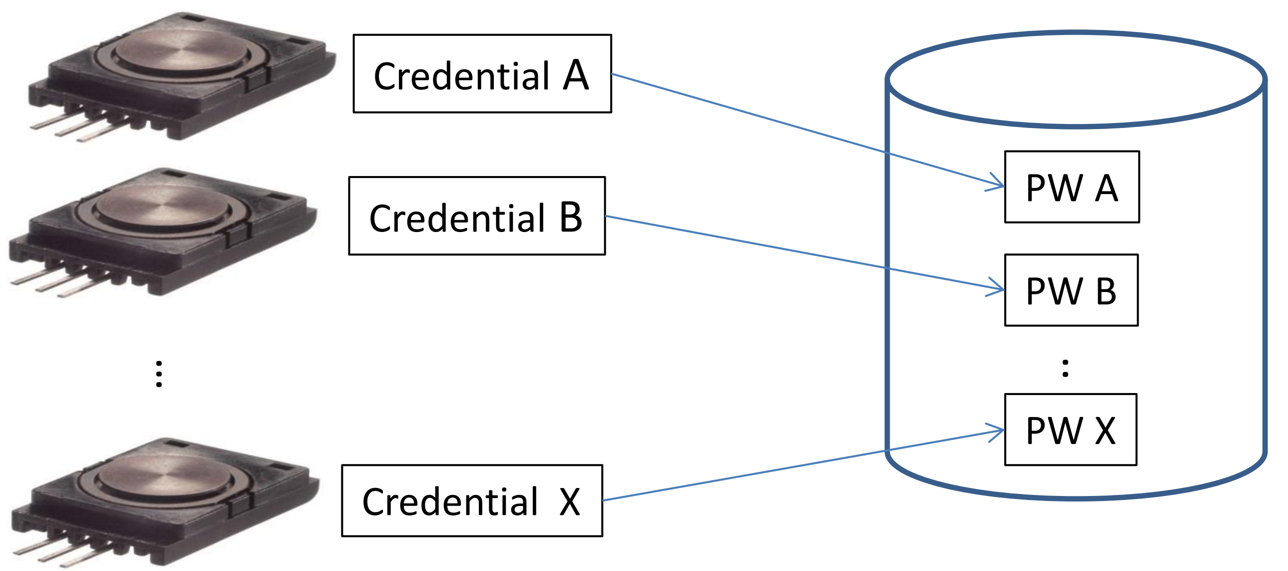
draft-kato-fsu-key-exchange-00.txt
draft-kato-optimal-ate-pairings-00.txt
draft-kasamatsu-bncurves-01.txt

KATO, Akihiro
NTT Software Corp

CFRG, IETF 94, Yokohama
2015 November 2nd

Management of credentials on IoT

- Typical credentials.
  - Pre-Shared
  - Raw Public Key
  - Certificate
- 2-3 billion devices will be wirelessly connected by 2020.
- A management of credentials will be one of problem.



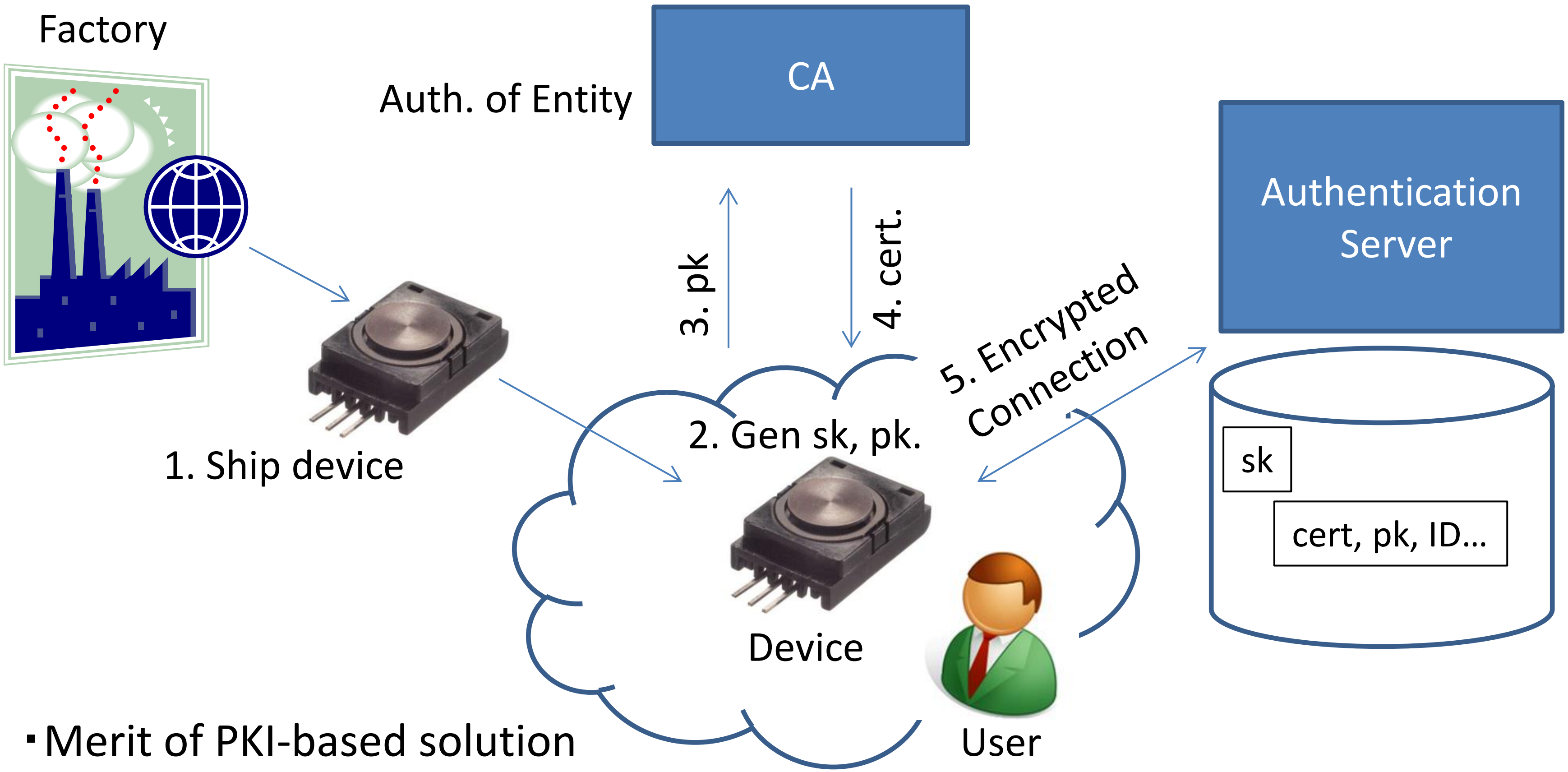
PSK-Based Credential

- Example 1. Venders set both of ID and PW as “Admin”. Users change PW and ID.
- Example 2. Venders set both of ID and PW as complicated one. Users should not change ID and PW.
- Example 3. Venders set both of ID and PW as complicated one. Users change PW and ID.

Problems for management of a large number of credentials.

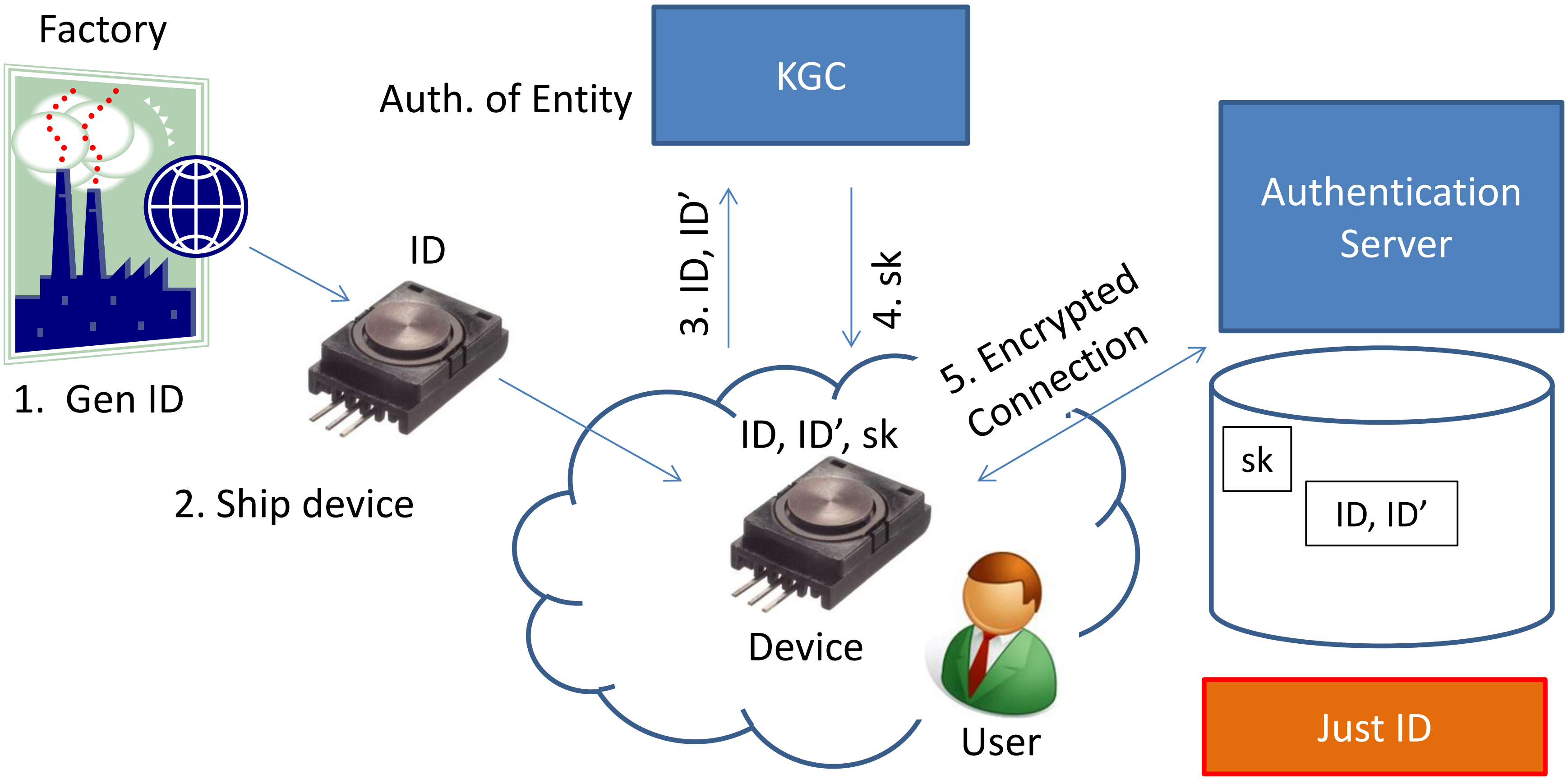
- Management cost of ID and PW, for Ex1 and EX3, will enlarge.
- Security level reduced by list-based attack.

PKI-Based Credential



- Merit of PKI-based solution
  - Low Management cost at server, comparison with PSK.
  - Credentials are automatically chosen at random.

ID-Based Credential

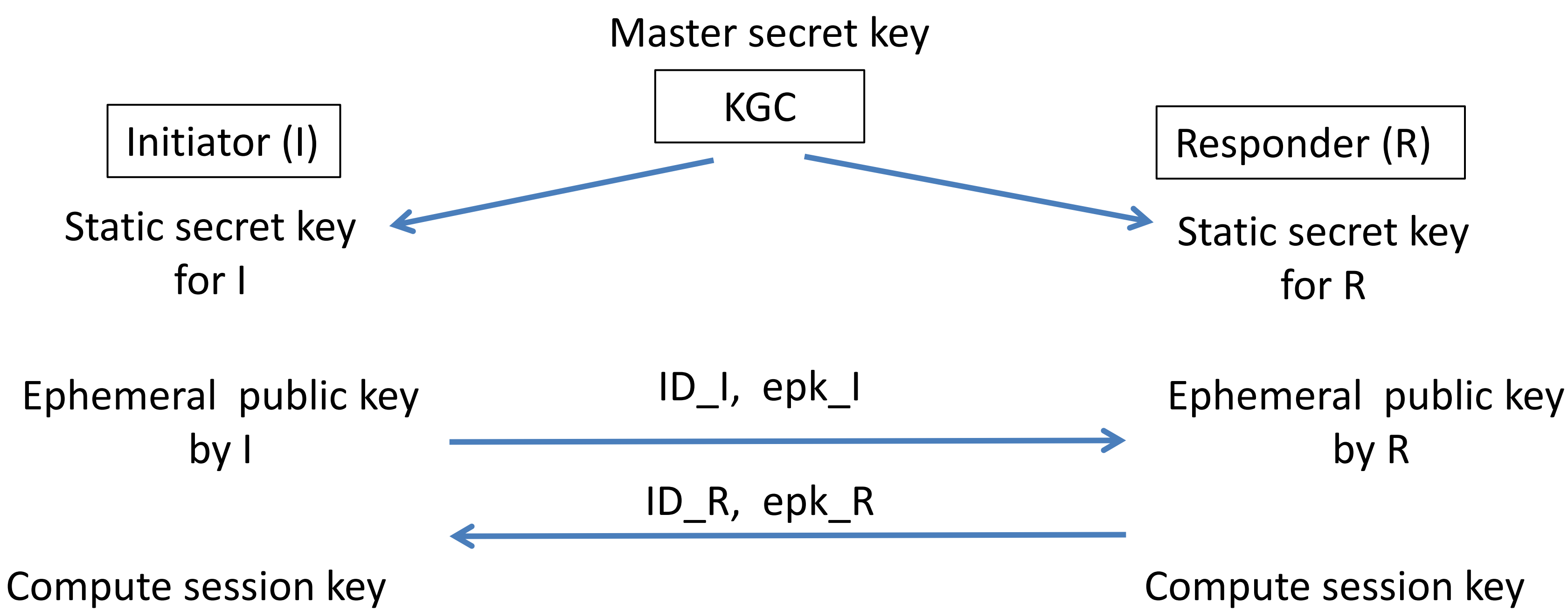


Merit of ID-Based for large number of Cred.

- Low cost of generation of sk and pk for Device and Factory.
- Centralization of key generation.
- ID can be ruled.
- If ID lists are provided, KGC can previously generate secret keys.

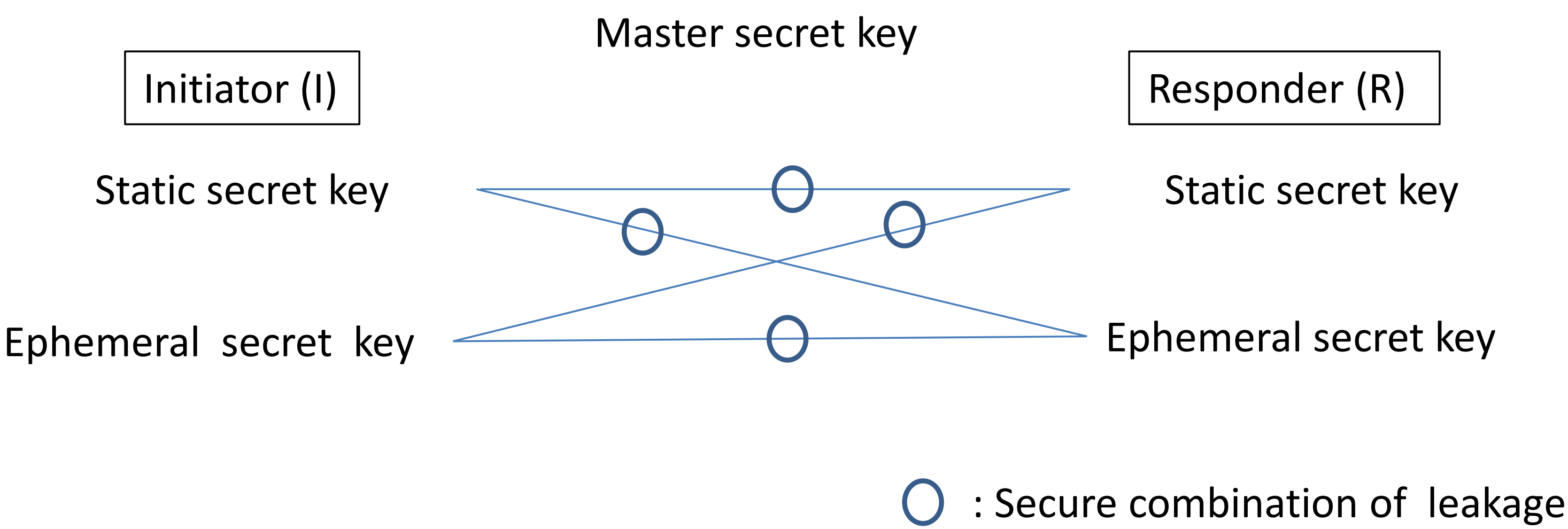
FSU Key Exchange Protocol

- FSU is an identity-based authenticated key exchange(ID-AKE) protocol.
- FSU is only 2-pass scheme.



Security of FSU

- FSU is proven to be secure in id-eCK security model.
- id-eCK security model is one of the most strongest security model against secret key leakage.
- Session key will be safe, even if attacker get any non-trivial combination of master key, static key, and ephemeral key.



Protection of session key

- Id-eCK security implies resistance of following security threats:
  - MitM(resistance to man in the middle attacks)
  - wPFS(weak perfect forward security)
  - KCI(resistance to key compromise impersonation attacks)
  - RLE(resilience to leakage of ephemeral private keys)

Comparison with other ID-AKE

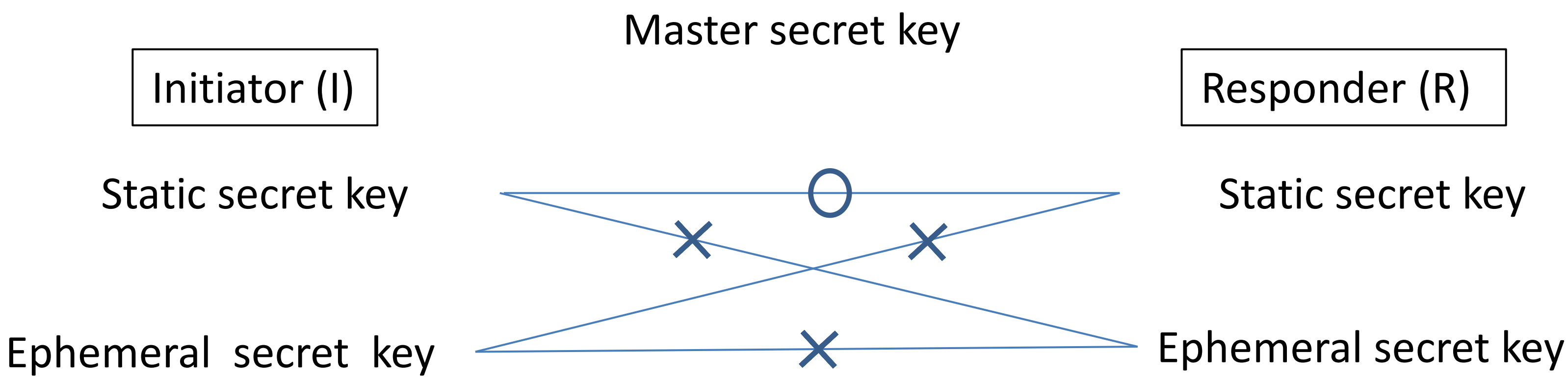
1. RFC6539:IBAKE
2. ISO/IEC FDIS 11770-3 p68 F.3 IBAKE following Smart-Chen-Cheng (SCC)

	Security Model	Connection times	Pairing times	Key Size (Oct)	Payload Size(Oct)
FSU	eCK	2	8	32	98
IBAKE	CK	3	3 × (ENC+DEC)*1	32	414
SCC	CK	2	4	32	33

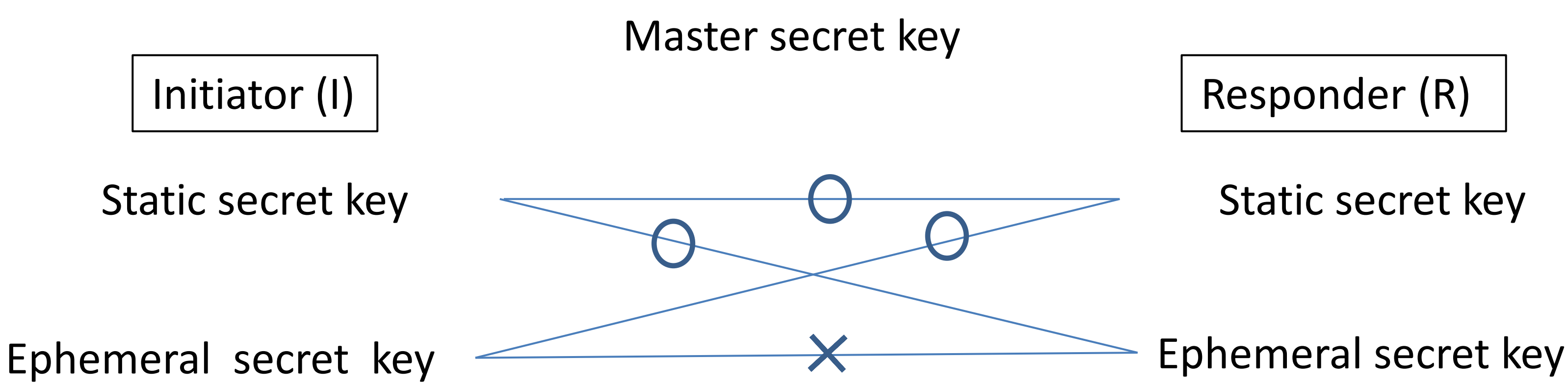
*1:Pairing times of IBAKE depends Enc and Dec of IBE.

Security of IBAKE and SCC

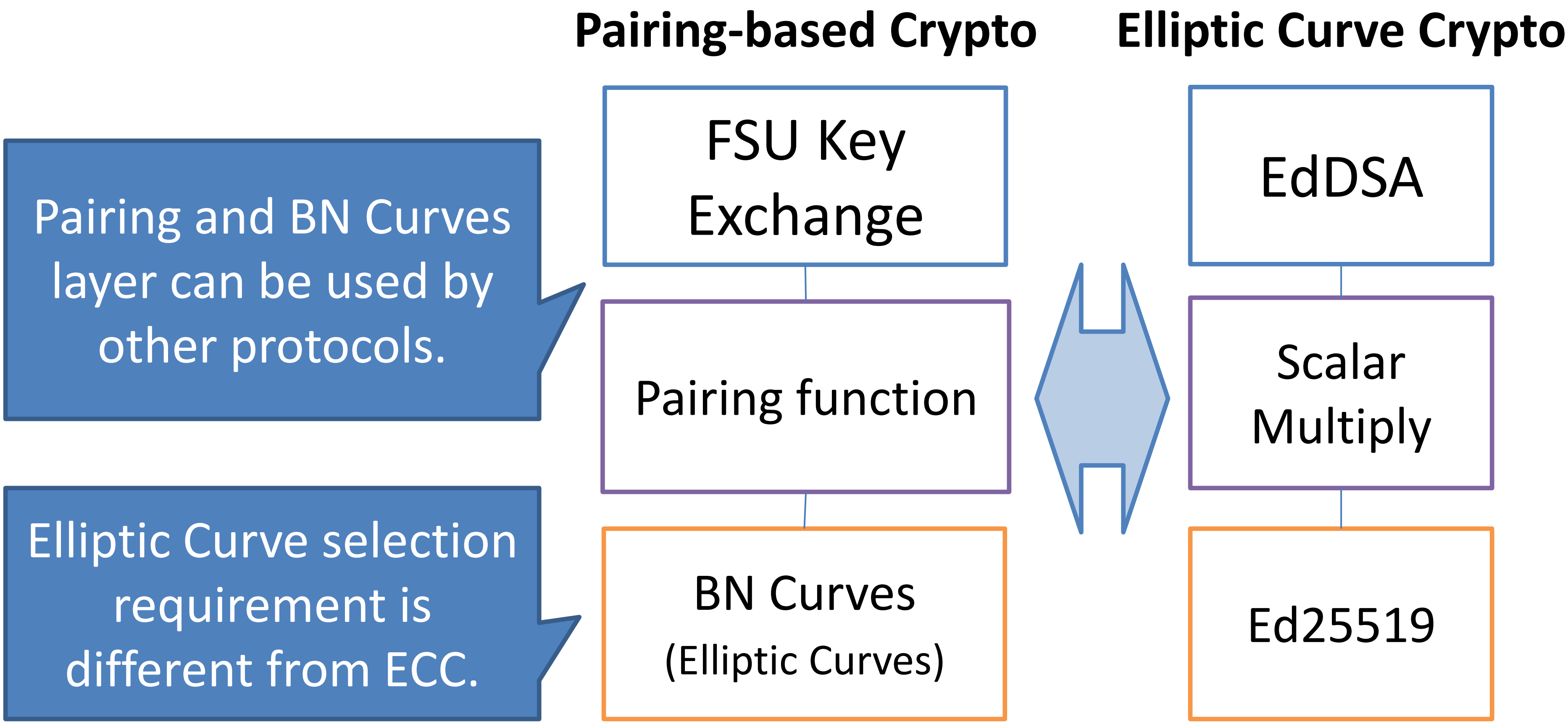
Security Model of IBAKE



Security Model of SCC



Why we wrote three IDs.



Our selects.

- Pairing
  We choose:
  – Optimal Ate Pairing that is fastest pairing algorithm now.
    - Its computation time is about ten-times or more as fast as Tate Pairing which is defined by Boneh-Franklin (RFC5091).
    - *draft-kato-optimal-ate-pairings* specifies algorithms and test vectors which are suitable four BN-curves.
- Elliptic Curves
  We choose:
  – Barreto-Naehrig curves (BN-curves) that have 128-bit security and are suitable for pairing-based cryptography.
    - *draft-kasamatsu-bncurves* specifies domain parameters of four 254-bit BN-curves.

Security of Pairing over BN-curves

- Pairing map G_1 * G_2 -> G_T
  - G_1, G_2 are group of elliptic curve.
  - G_T is finite field F_{p^12}
- All BN-curves have(written in our draft) have 128-bit security.
  - The order of G_1 and G_2 is 254-bit.
  - The order of G_T is 254*12-bit.
  - Hardness of ECDLP and FFDLP is 128-bit security.

Future work

- We are going to standardize key generation center for ID-based Crypto.

Any comments and questions?

- draft-kato-fsu-key-exchange-00.txt
- draft-kato-optimal-ate-pairings-00.txt
- draft-kasamatsu-bncurves-01.txt

My office is here ;-).

We are here.