TOSHIBA
Leading Innovation

Secure Multicast Group Management and Key Distribution in IEEE 802.21

○ Yoshikazu Hanatani (Toshiba)
Naoki Ogura (Toshiba)
Yoshihiro Ohba (Toshiba Electronics Asia)
Lidong Chen (NIST)
Subir Das (Applied Communication Sciences)

© 2016 Toshiba Corporation

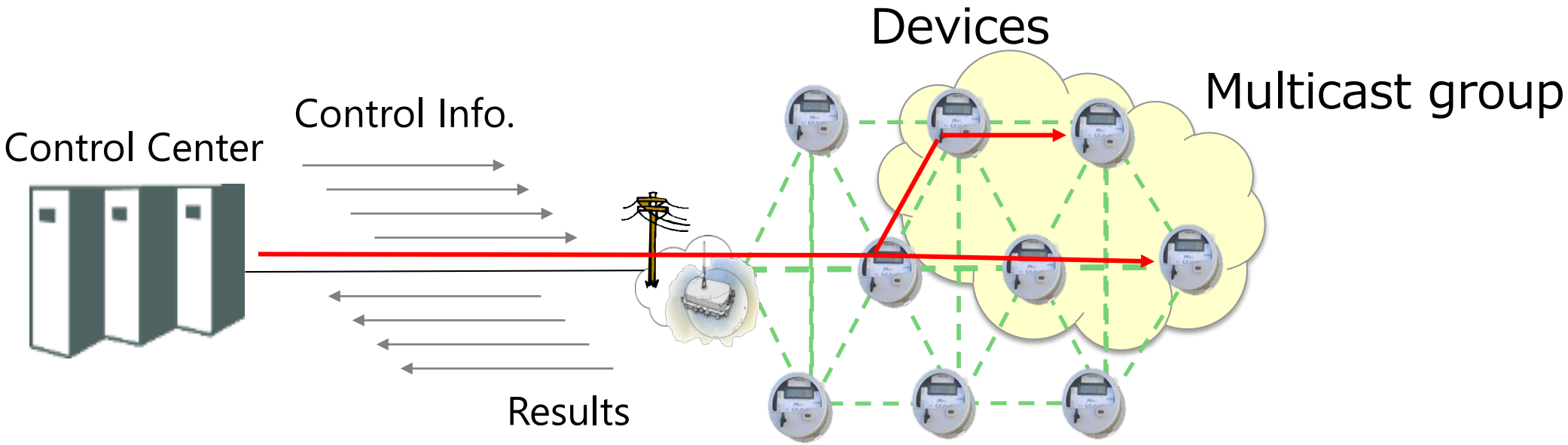
Outline

- Use case
- IEEE 802.21
- Group Key Distribution Protocol
- Security analysis
- Prototype Results
- Conclusion

© 2016 Toshiba Corporation

Use Case

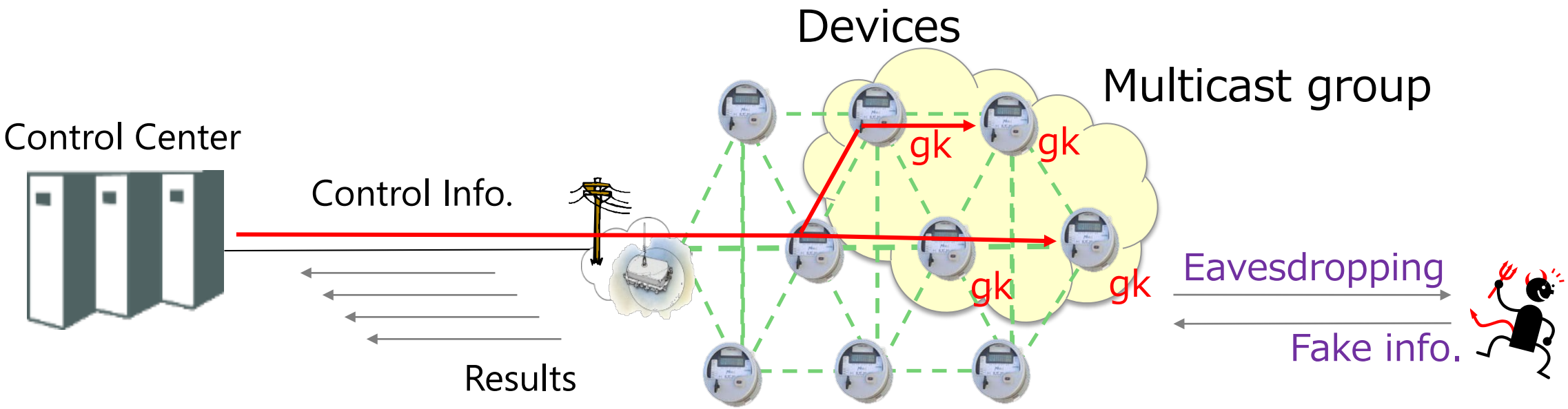
- **In IoT deployment, one 'Control Center' needs to manage a large number of devices.**
- **A system sending control information to each device by unicast communication is not resource efficient and may have the scalability issue.**
- **A multicast communication is proved to be very useful for managing a large number of devices (e.g., configuring parameters, updating firmware).**



© 2016 Toshiba Corporation

Use Case Contd..

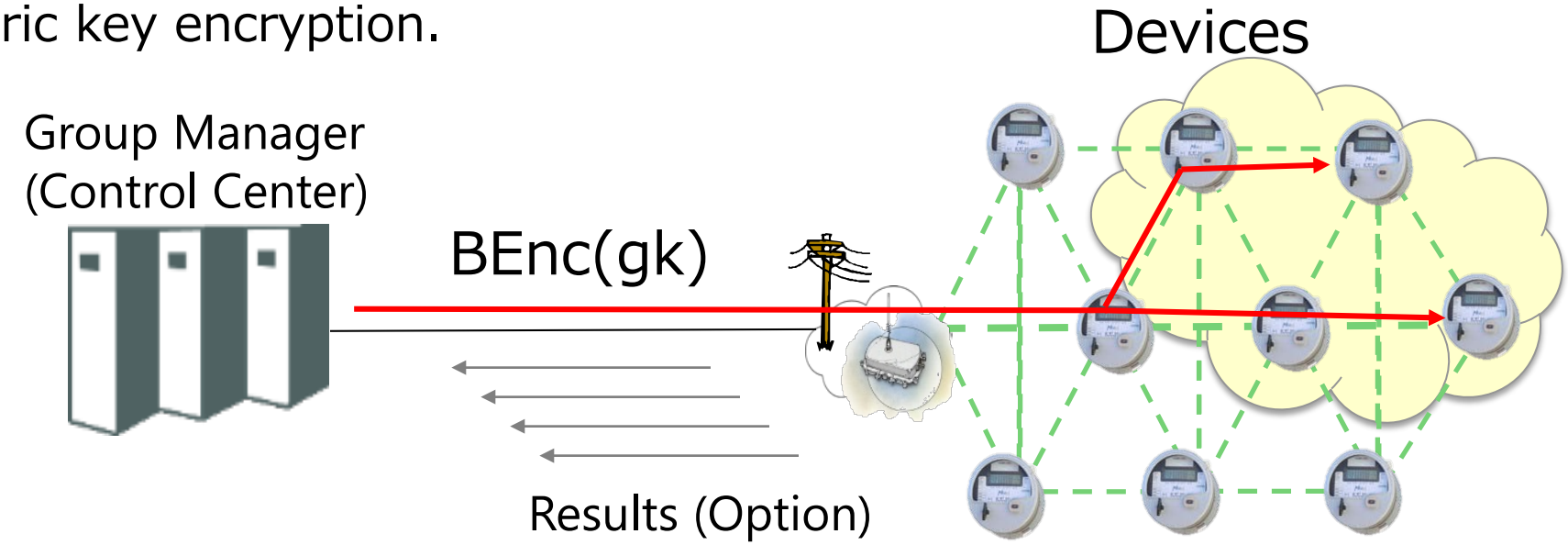
- **A shared key is used to protect each unicast communication**
  - The shared key can be established by various standards-based key exchange protocols
  - Number of unicast session = number of shared keys
- **However, the multicast communication can be protected by a single group key**
  - How to securely distribute the group key?
  - Standards-based key distribution protocol is good for industry



© 2016 Toshiba Corporation

Group Key Distribution Protocol in IEEE 802.21

- **IEEE 802.21 specifies a framework and signaling protocol that can be used to securely distribute the group key to a multicast group**
  - Can be transported over IP and over link layer
- **Group Manager (Control Center) generates and distributes group keys to the group members (a.k.a. devices).**
  - The group key is protected by a scalable broadcast encryption mechanism using a symmetric key encryption.



© 2016 Toshiba Corporation

Past Work

- **RFC 6407: Group Domain of Interpretation**
  - Key manager sends an initial group key to each group member by a secure unicast communication.
  - The protocol allows group key distribution for rekeying by a logical key hierarchy.
- **ISO/IEC 11770-5:2011 Group key management**
  - Specify a group key management by a logical key hierarchy.
- **Broadcast encryption: [FN93], [NNL01] etc.**
  - Distributing a group key for decrypting contents only to compliant devices.
  - Used in AACS copy-protection system.

© 2016 Toshiba Corporation

Contribution to this Paper

- **Described a group key distribution protocol in IEEE 802.21**

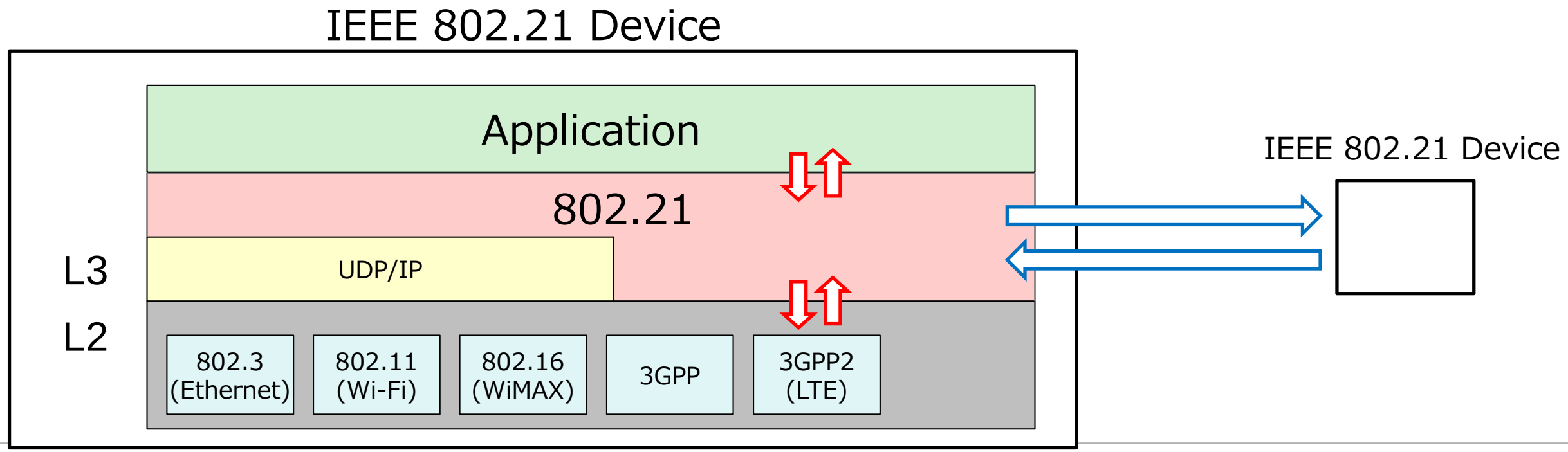
- **Provided a formal security proof of the group key distribution protocol**
  - Define a relaxed security model
  - The protocol is secure in the relaxed security model.
  - The relaxed security model is weaker than a current security model

- **Prototype Implementation Results**

© 2016 Toshiba Corporation

IEEE 802.21 : Media Independent Services

- **Provide a media independent framework, services and signaling protocol**
  - Interfaces to Lower-layer and to Upper-layer
  - Define Protocol messages
  - Security mechanisms for protecting the messages
  - Messages can be transported over IP (port assigned by IANA) and over link layer



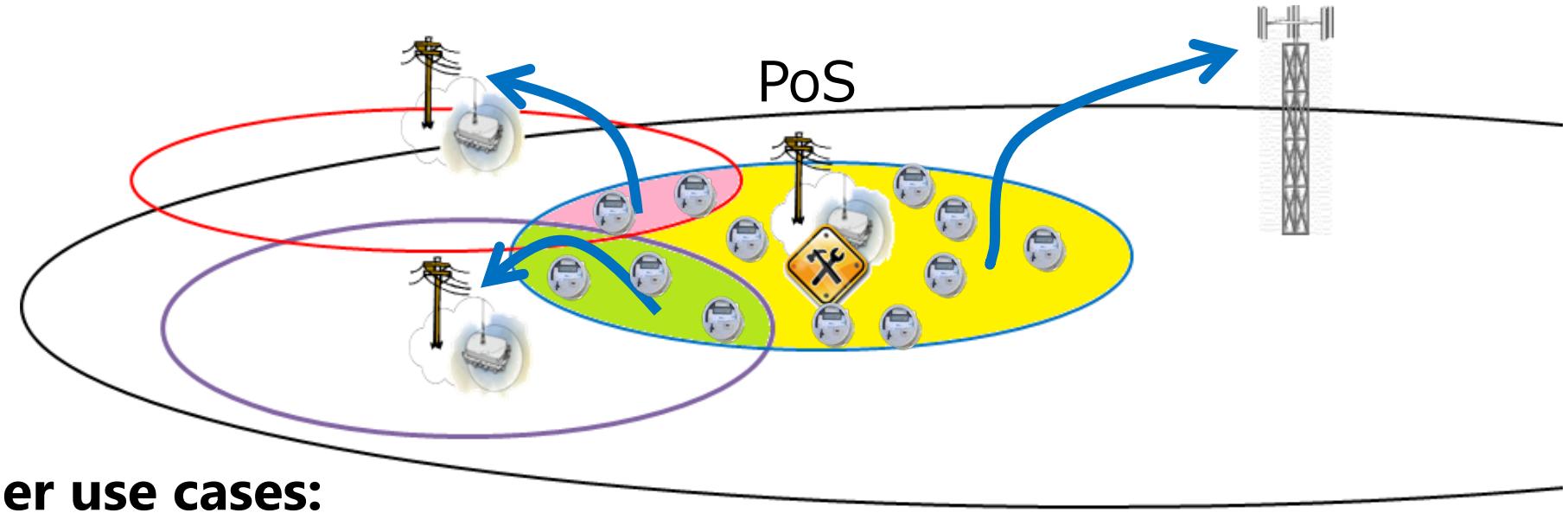
© 2016 Toshiba Corporation

Use case of multicast communication in IEEE 802.21

Devices access a network via a Point of Services (PoS)

When PoS needs maintenance or malfunctioning, PoS sends alternative PoS's information to devices.

The devices can dynamically change the PoS without disrupting the network access and services



- **Other use cases:**
  - Load balancing
  - Configuration parameters update or Firmware update.

© 2016 Toshiba Corporation

Multicast Security Mechanism in IEEE 802.21

- Multicast Group Management
- Group Key Distribution Protocol
- Certification Distribution Protocol
- Message protection by Group key and Digital signature

© 2016 Toshiba Corporation

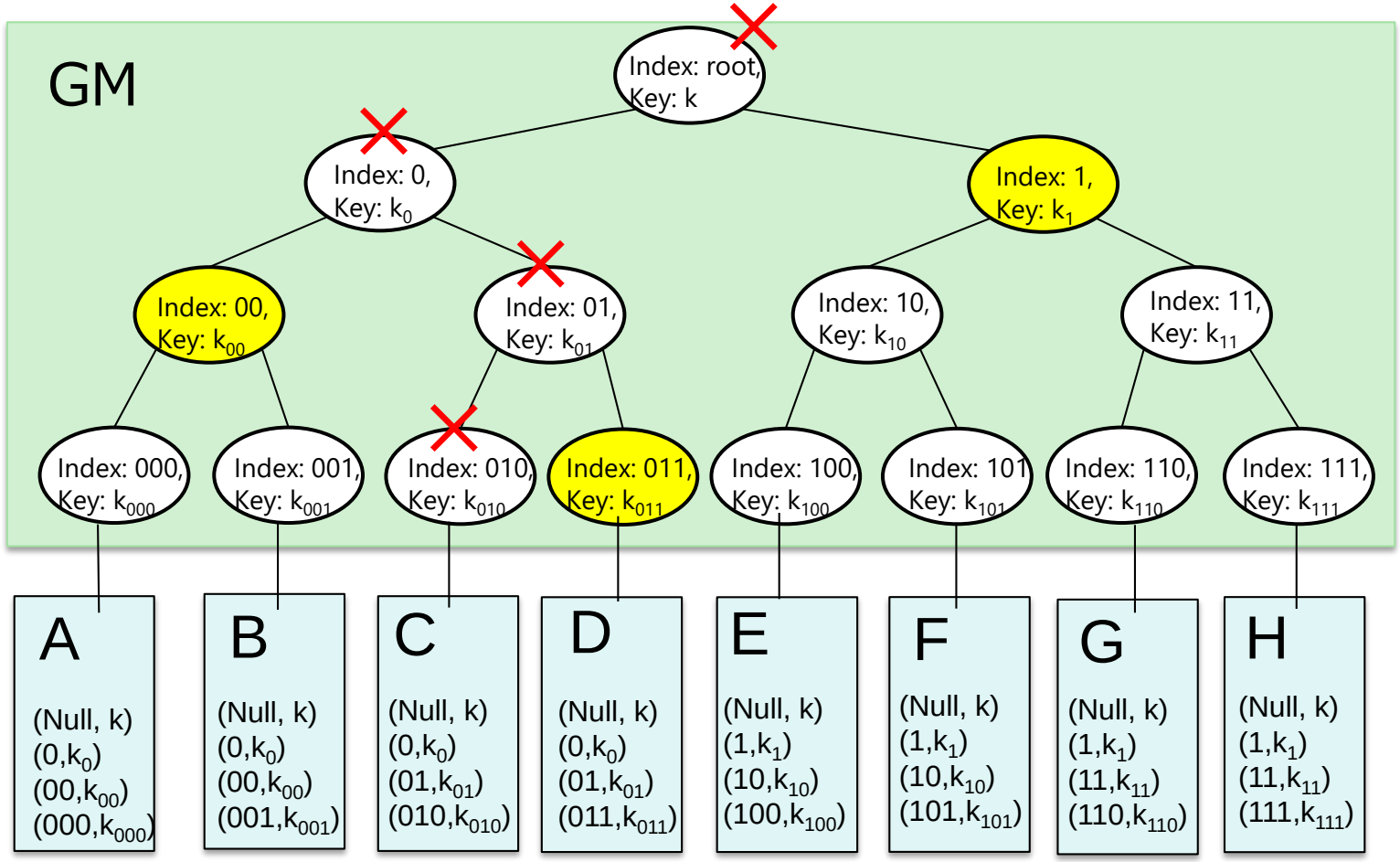
Outline

- Use Case
- IEEE 802.21
- **Group Key Distribution Protocol**
- **Security analysis**
- **Prototype Results**
- **Conclusion**

© 2016 Toshiba Corporation

Complete Subtree Method

- **GM has all node keys in a management tree.**
- **Each leaf node is assigned to a device.**
- **Each device has a part of node key as its own device key.**



Ex1. GM wants to send $gk1$ to all devices.

Send (root, $Enc(k, gk1)$)

Ex2. GM wants to send $gk2$ to devices excluding C.

Send $(00, Enc(k_{00}, gk2))$, $(011, Enc(k_{011}, gk2))$, $(1, Enc(k_1, gk2))$

© 2016 Toshiba Corporation

Ciphersuites for the group key distribution

- **Key wrapping $\mathcal{KW}$**
  - AES-Key_Wrapping-128 or AES-ECB-128
  - $\mathcal{KW}$ satisfies IND-RPA (Indistinguishability against Random Plaintext Attack)

$$k \leftarrow KeyGen(\kappa)$$

$$c \leftarrow Wrap(k, mk)$$

$$mk \leftarrow Unwrap(k, c) \text{ when } c = Wrap(k, mk)$$

- **Digital signature Σ**
  - ECDSA_P256_SHA256
  - Σ satisfies EUF-CMA (Existential Unforgeability against Chosen Message Attack)

$$(pk, sk) \leftarrow KeyGen_{\Sigma}(\kappa)$$

$$\sigma \leftarrow Sign(sk, m)$$

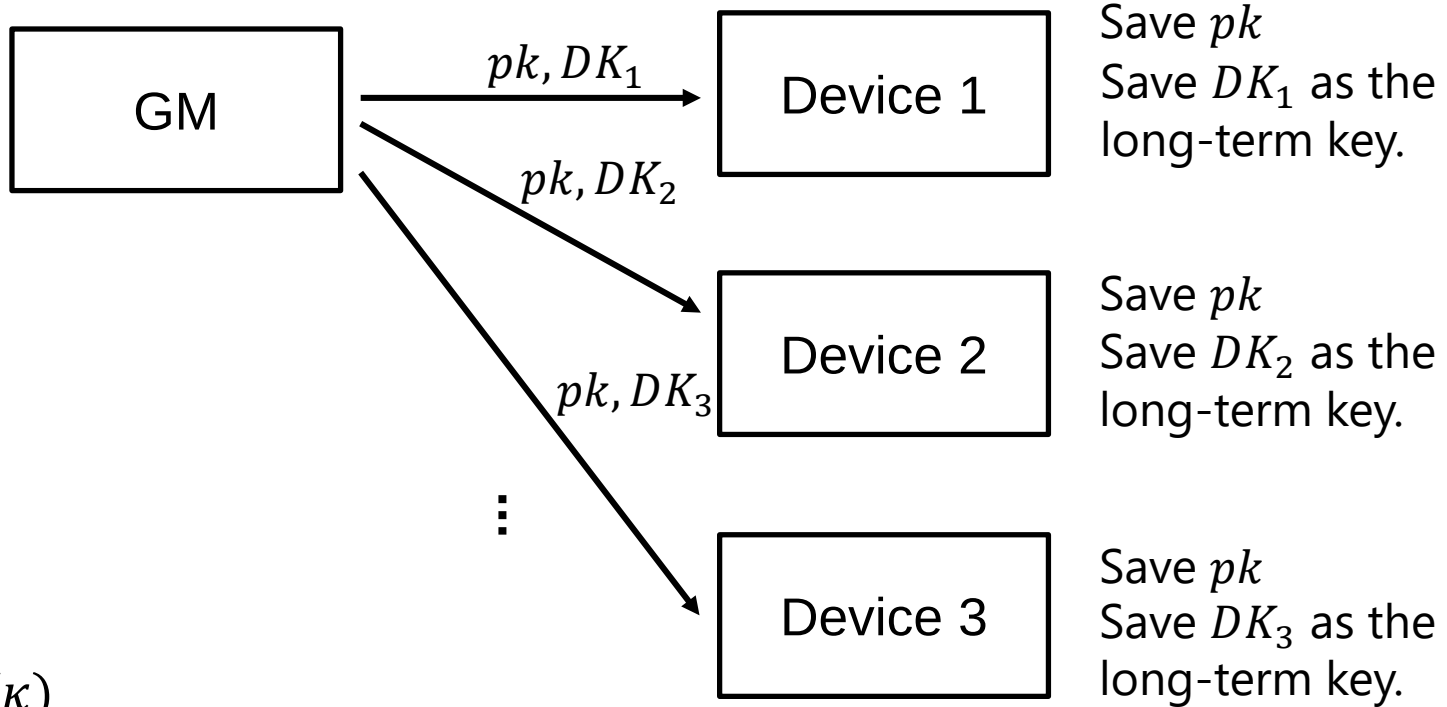
$$1 \leftarrow Verif(pk, m, \sigma) \text{ when } \sigma = Sign(sk, m)$$

© 2016 Toshiba Corporation

Group key distribution protocol in IEEE 802.21

- **Provisioning**
  - The maximum number of devices : 2^n
  - $\mathcal{U}$: A set of all device to be managed. $|\mathcal{U}| \leq 2^n$

1. Generate a binary tree T with depth n.
2. Assign (I_i, k_i) to each node in T.
   - I_i is ID of the node.
   - $k_i \leftarrow KeyGen(\kappa_i)$
3. Assign a leaf node and corresponding device key DK to a device $\in \mathcal{U}$.
4. Generate verification key and signing key $(pk, sk) \leftarrow KeyGen_{\Sigma}(\kappa)$



This step may need individual secure channel.
IEEE 802.21 does not specify the provisioning protocol

© 2016 Toshiba Corporation

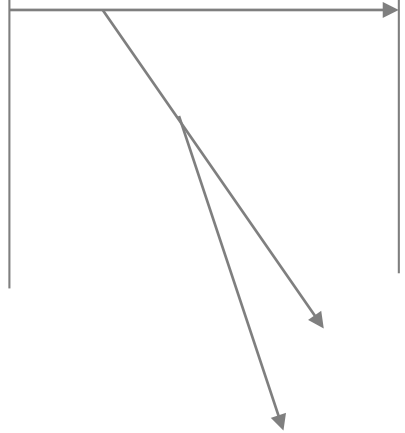
Group key distribution protocol using typical option

pk : verification key
sk : signing key
T : all device keys

GM

1. Choose $S \subseteq \mathcal{U}$ where $\mathcal{U}$ is a set of all available device in T
2. Decide a group identifier GI
3. Pick current sequence number SN for GI
4. Choose $mgk \in_R \{0,1\}^{\ell}$ and $SAID$ for mgk
5. Compute all (I_i, c_i) from $\mathcal{U}$, S, and T using CS method where $c_i = Wrap(k_{I_i}, mgk)$
6. Set a destination and pick current sequence number sq for the destination
7. $\sigma \leftarrow Sign(sk,\ GI||SN||\{I_i\}||\{c_i\}||SAID||sq)$

Multicast the green-colored elements



Device 1

pk : verification key
DK_1 : all device keys

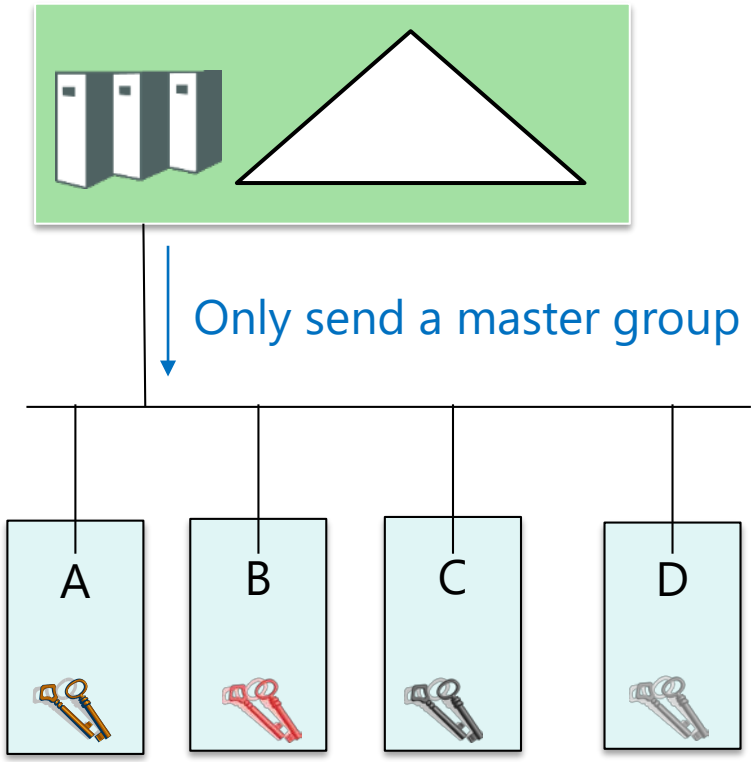
1. Check sq to prevent a replay attack
2. If $1 \neq Verif(pk, GI||SN||\{I_i\}||\{c_i\}||SAID||sq, \sigma)$, the message is dropped.
3. If $\exists\ I_j$ such that $(I_j, k_j) \in DK_1$ and $I_j \in \{I_i\}$,
   - $mgk \leftarrow Unwrap(k_j, c_j)$
   - $gsk \leftarrow KDF(mgk)$
   - Record $(GI, SN, SAID, gsk)$
   - Join group GI
4. Otherwise
   - Delete $(GI, * * *)$ if it is recorded.
   - Leave group GI

© 2016 Toshiba Corporation

Comparison

IEEE 802.21 (Complete Subtree)

Common Tree T is used for all groups
→ The size of device keys is independent of the number of groups



At most one decryption

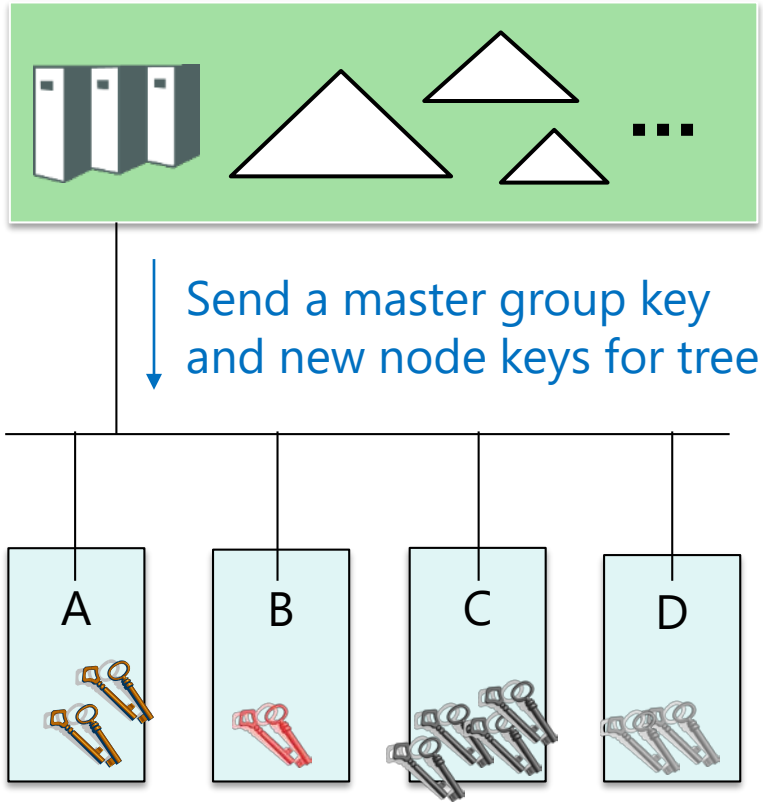
Storage cost

Communication cost

Computational cost

GDOI (Logical Key Hierarchy)

Trees are generated for each group
→ The size of device keys depends on the number of groups



Multiple decryptions are required

© 2016 Toshiba Corporation

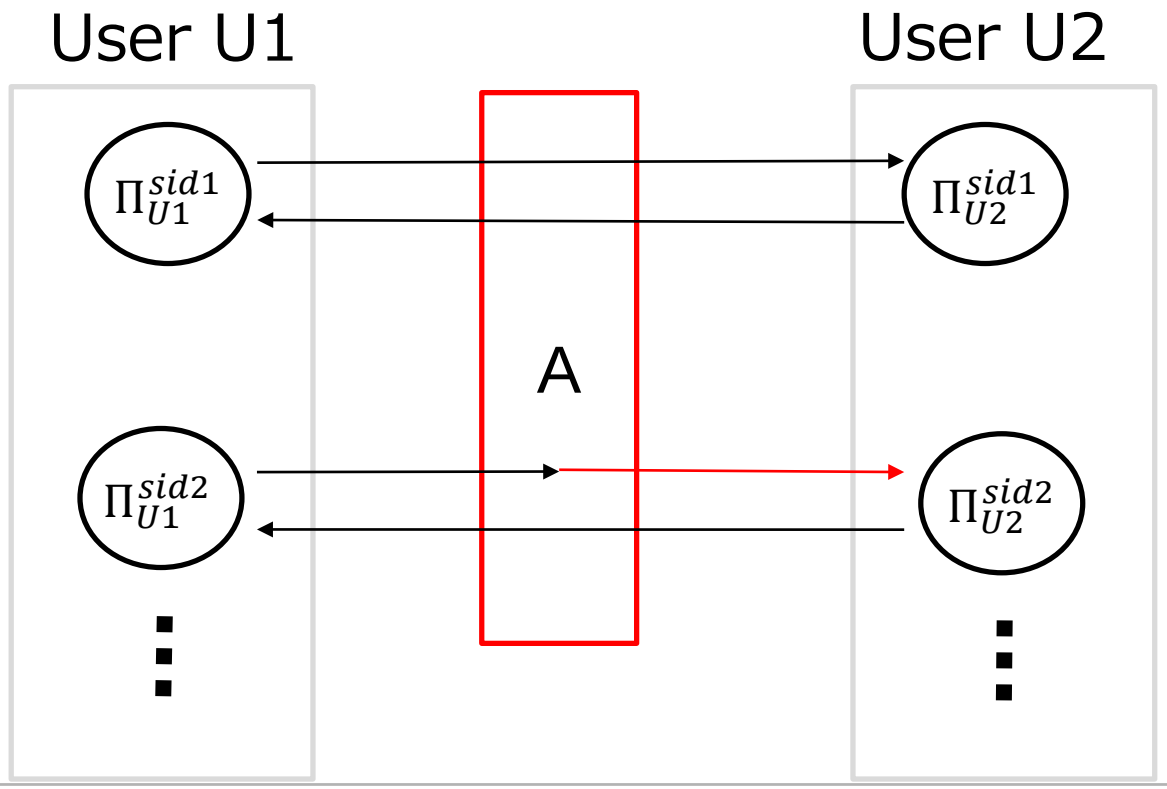
Outline

- Use Case
- IEEE 802.21
- Group Key Distribution Protocol
- **Security analysis**
- **Prototype Results**
- **Conclusion**

© 2016 Toshiba Corporation

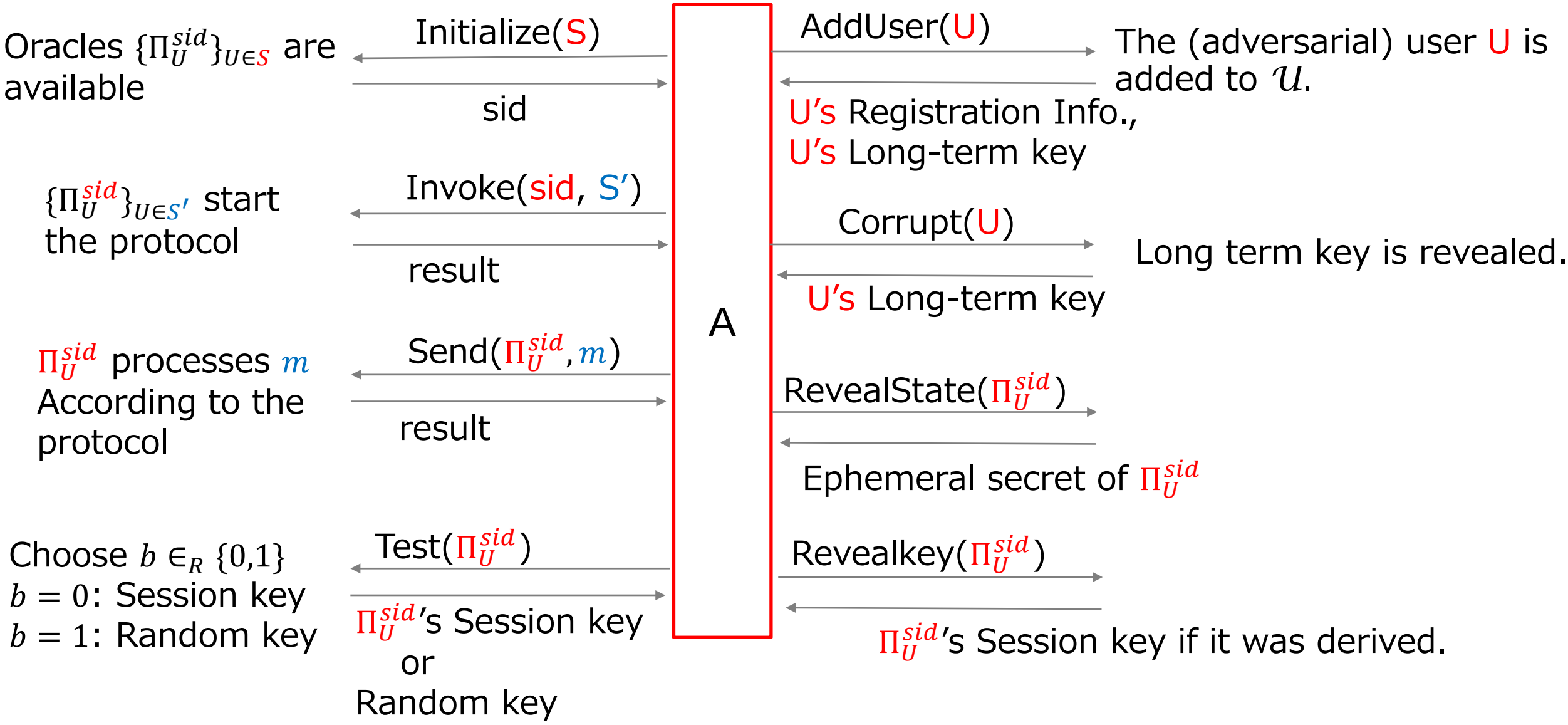
Security Model : Communication

- **All participants of the protocol are represented by oracles.**
- **The adversary A can get and modify all messages in communication channels.**



© 2016 Toshiba Corporation

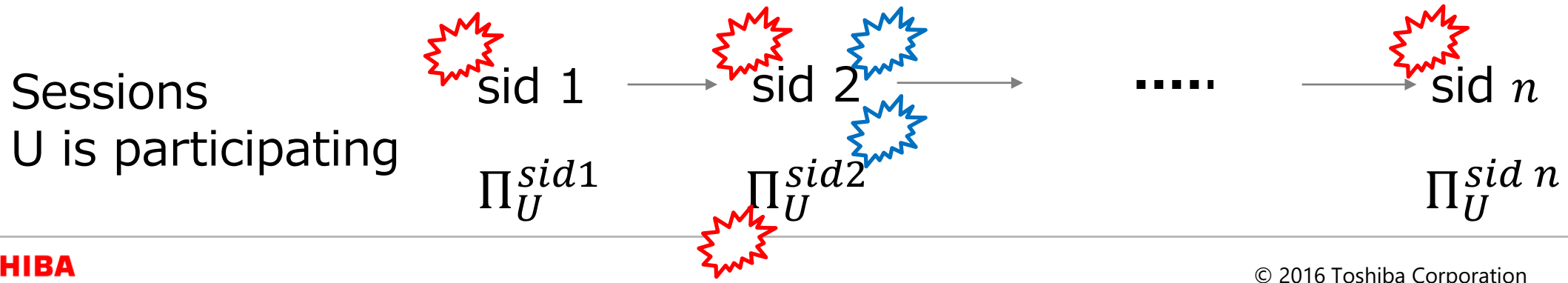
Security Model: Queries for adversary A



© 2016 Toshiba Corporation

Security model: Freshness of sid

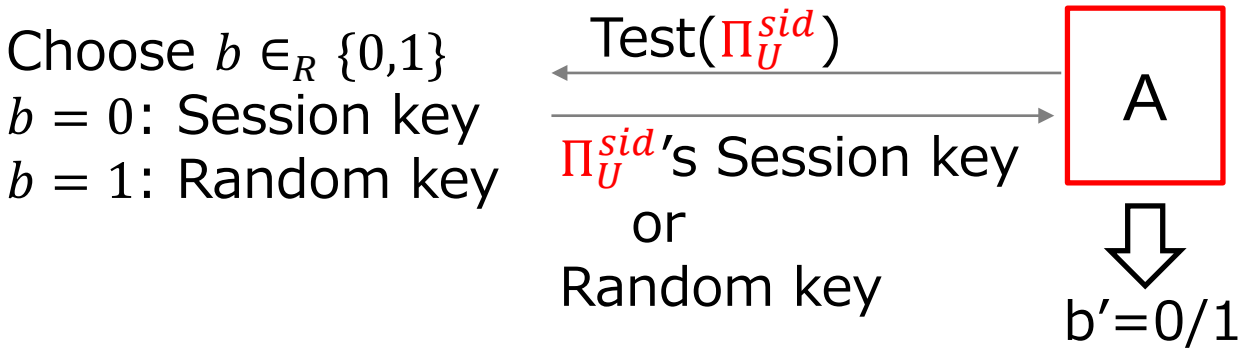
- **We say session sid is *Fresh* if all of the following conditions are satisfied.**
  - *A* has not obtained the long term key of a participant in the session sid by the adversarial queries, directly.
    - There are no Π_U^{sid} who are added by AddUser(U).
    - There are no Π_U^{sid} who issued Corrupt(U).
  - *A* does not obtained an internal state of a participant in the session sid by the adversarial queries, directly.
    - There are no Π_U^{sid} who issued RevealState(Π_U^{sid}) before stopping Π_U^{sid}.
  - *A* does not obtained a session key of the session sid by the adversarial queries, directly.
    - There are no Π_U^{sid} who issued RevealKey(Π_U^{sid}) before stopping Π_U^{sid}.



© 2016 Toshiba Corporation

Security for group session key

We say *A* wins when b = b′ and sid is *Fresh* where *A* issued *Test*(Π_U^{sid}).



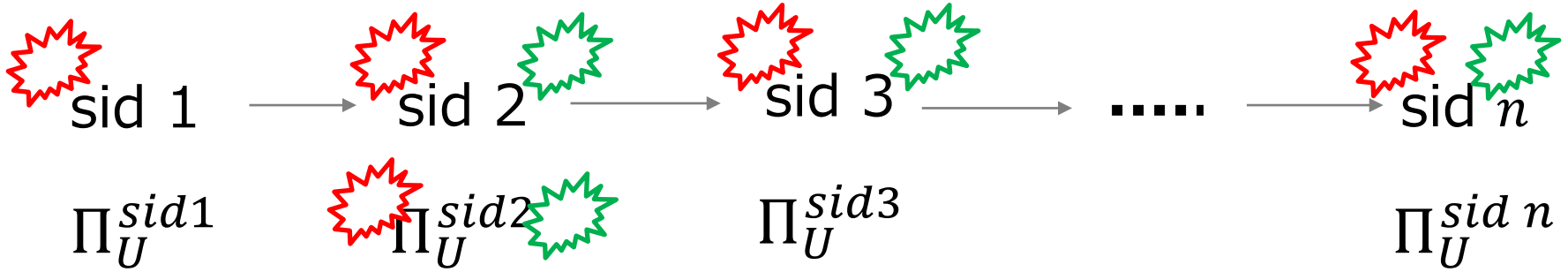
Advantage of A: $\mathrm{Adv}^{\mathrm{ake}-b}_{\mathcal{A}_{AKE},\mathrm{P}}(\kappa) = |\Pr[A\ wins] - 1/2|$

The group key distribution protocol is secure if $\mathrm{Adv}^{\mathrm{ake}-b}_{\mathcal{A}_{AKE},\mathrm{P}}(\kappa)$ is negligible.

© 2016 Toshiba Corporation

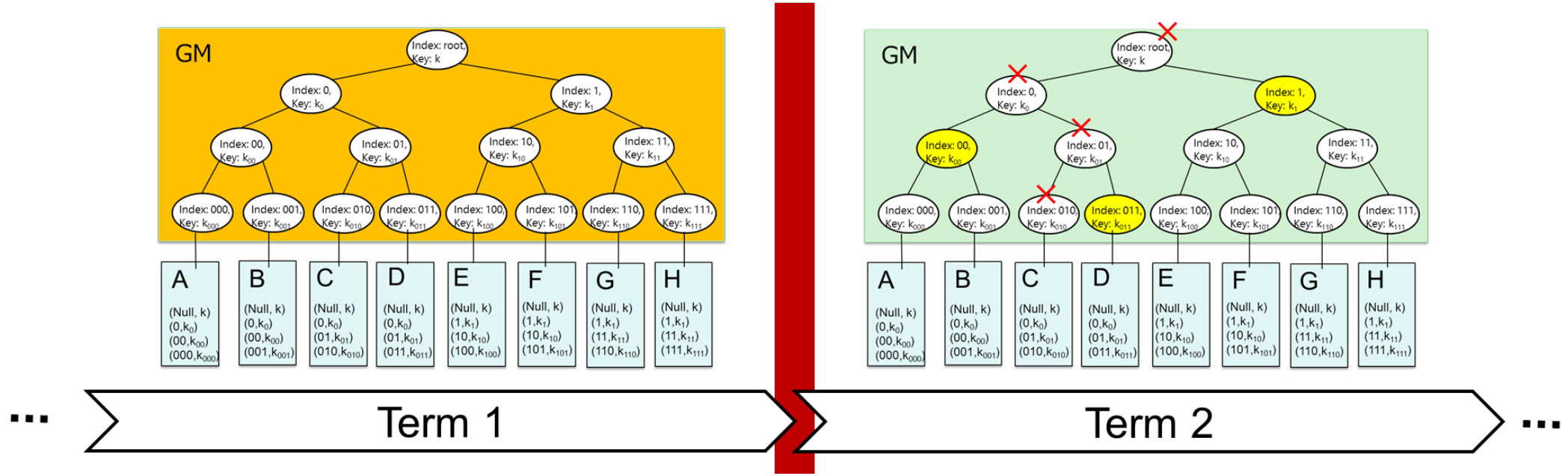
Comparison with [BBM09] model

- **Our model: When U is just corrupted, freshness of all sid that U participated are lost.**
  - *A* has not obtained the long term key of a participant in the session sid by the adversarial queries, directly.
    - There are no Π_U^{sid} who issued Corrupt(U).
  - Our model does not capture Perfect Forward Security.
- **[BBM09]: Freshness of sid is NOT lost just by corrupting the participant.**
  - The freshness is lost when *A* issues a query using the corrupted Π_U^{sid}.
  - [BBM] model captures Perfect Forward Security.



© 2016 Toshiba Corporation

Is the model reasonable?



- **The device keys (Long-term key) of 802.21 are static.**

  → If a device key is revealed, all sessions using the device key are compromised. So, it does not satisfy the security in [BBM09].

- **We can reduce the damage by regularly updating the tree.**

© 2016 Toshiba Corporation

Computational Assumptions and Theorem

- **Computational assumptions**
  - Σ satisfies EUF-CMA security

    $\mathrm{Adv}^{\mathrm{kw.rpa}}_{\mathcal{A},\mathcal{KW}}(\kappa)$ is negligible.

  - $\mathcal{KW}$ satisfies IND-RPA security

    $\mathrm{Adv}^{\mathrm{euf-cma}}_{\mathcal{A},\Sigma}(\kappa)$ is negligible.

- **Theorem: Σ satisfies EUF-CMA security and $\mathcal{KW}$ satisfies IND-RPA security, the group key distribution protocol in IEEE 802.21 satisfies the security on group keys, and**

$$\mathrm{Adv}^{\mathrm{gk}-b}_{\mathcal{A}_{AKE},\mathrm{P}}(\kappa) \leq \frac{(2N-1)\cdot n_s \cdot n_g^*}{2} \cdot \mathrm{Adv}^{\mathrm{kw.rpa}}_{\mathcal{A},\mathcal{KW}}(\kappa) + \mathrm{Adv}^{\mathrm{euf}-cma}_{\mathcal{A},\Sigma}(\kappa)$$

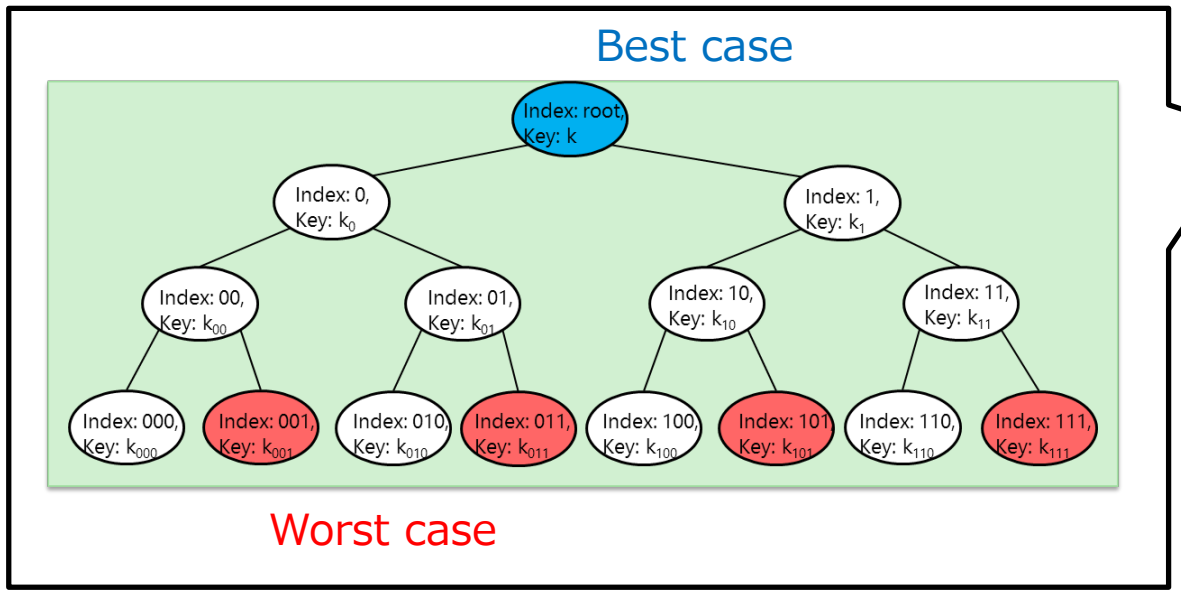
© 2016 Toshiba Corporation

Outline

- Use Case
- IEEE 802.21
- Group Key Distribution Protocol
- Security analysis
- **Prototype Results**
- **Conclusion**

© 2016 Toshiba Corporation

Prototype Results



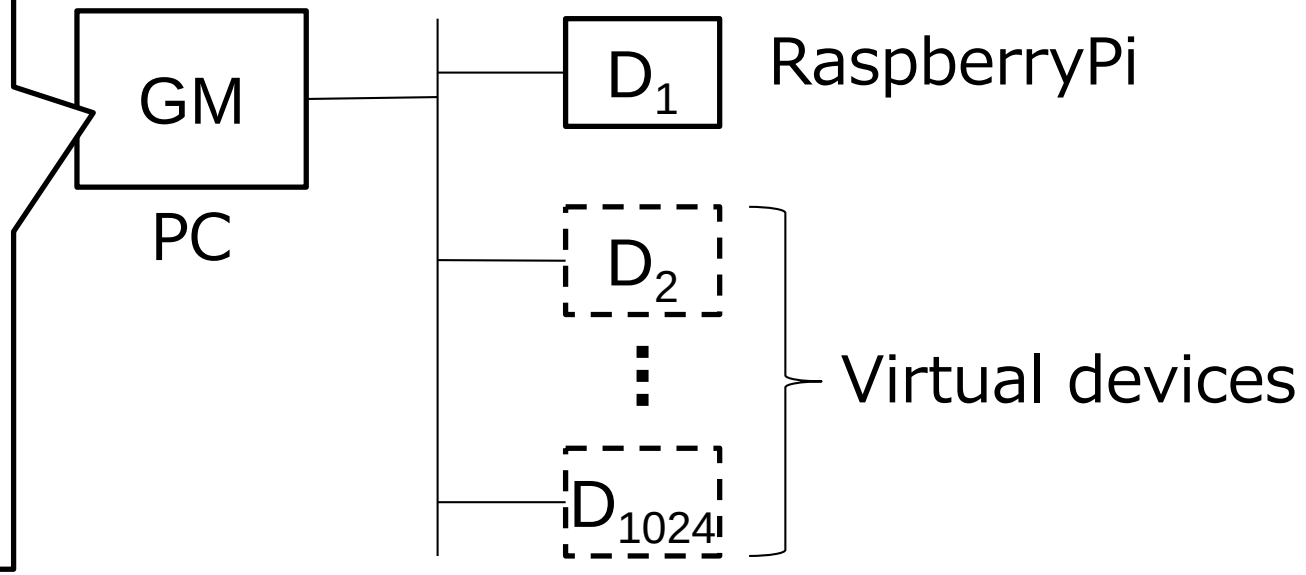


Table 2. Processing times

	GM		Receiver	
	Average [msec]	Max [msec]	Average [msec]	Max [msec]
Best case	4.71	4.74	265.15	303.59
Worst case	83.80	85.01	4253.91	4276.05

ECDSA verification time is dominant.

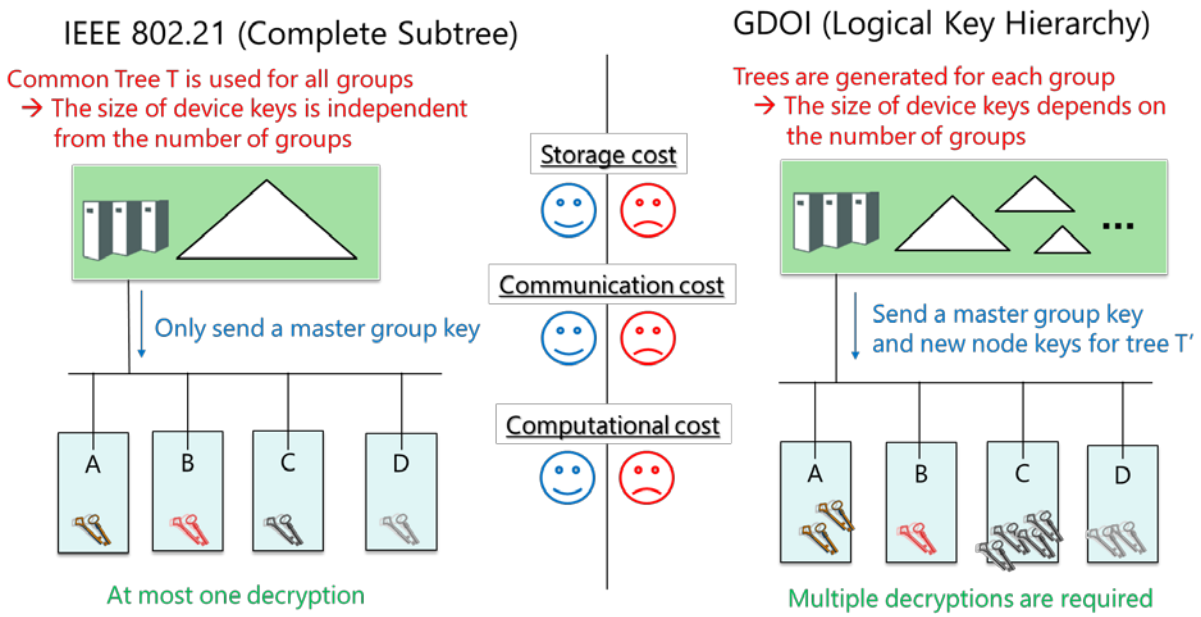
Table 3. Protocol message size

	Message size[bytes]
Best case	272
Worst case	18336

© 2016 Toshiba Corporation

Conclusion

- **IEEE 802.21 specifies a group key distribution protocol**
- **The group key distribution protocol with typical options is secure in the active attack model without PFS**
- **Comparing with GDOI, it has better performance when there are multiple groups**
- **Early prototype implementation results are reported**



© 2016 Toshiba Corporation