Africacrypt 2010, May 4, 2010

Information-Theoretically Secure Key-Insulated Multireceiver Authentication Codes

○Takenobu Seito

Tadashi Aikawa

Junji Shikata

Tsutomu Matsumoto

Yokohama National University, Japan

Overview

- Introduction.
- Information-theoretically secure Key-Insulated Multireceiver Authentication Codes(KI-MRA).
  - Model.
  - Security Notions and Their formalization.
  - Lower Bounds.
  - Direct/Generic Constructions.
- Conclusion.

Introduction

When **long-term use** of computationally secure cryptographic techniques (e.g. public-key encryption, digital signatures) is considered, there are two problems:

I. Computationally secure schemes might not maintain sufficient long-term security because of recent rapid development of algorithms and computer technologies.

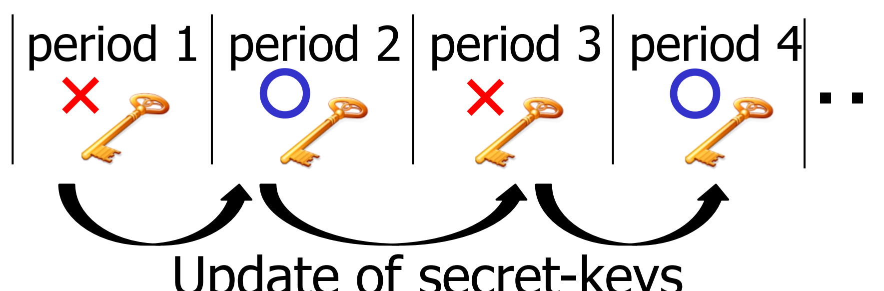
Solution: **Information-Theoretically secure scheme**

This scheme guarantees long-term security.

II. One of the most serious threats in cryptographic protocols is exposure of secret-keys (i.e. exposure of secret-keys leads to a total break of the system).

Solution: **Key-Insulated Scheme** [Dodis et al. 02, 03]

This scheme minimizes the risk of key-exposure.



Our Study

Our research topic is "authentication/signature schemes which have both information-theoretic and key-insulated security".

Especially...

We propose

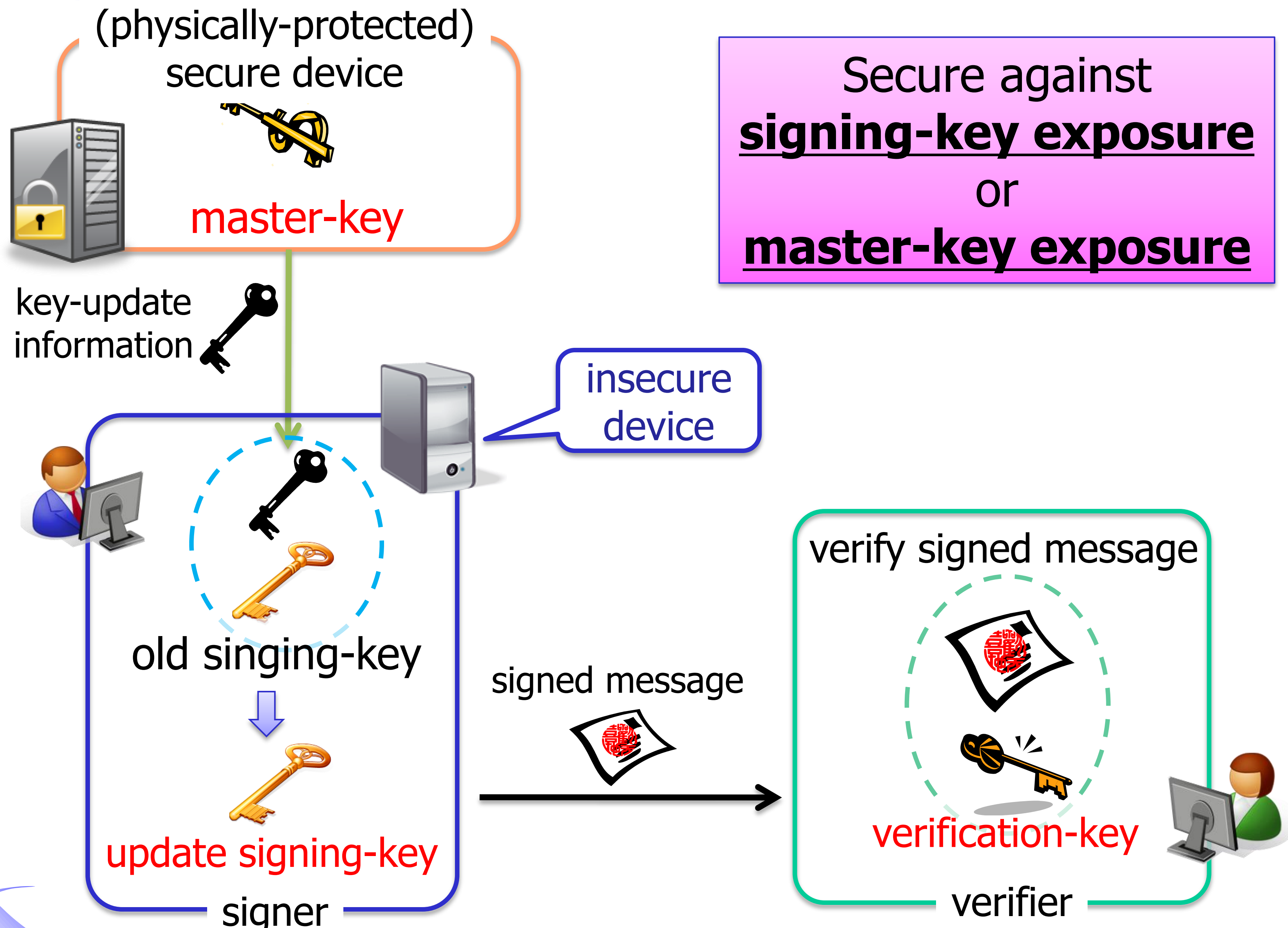
Information-Theoretically Secure Key-Insulated Multireceiver Authentication codes (KI-MRA).

Key-Insulated Security	Computational Security	Information-Theoretic Security
Confidentiality	[Dodis et al. 02]	[Hanaoka et al. 04]
Authenticity	[Dodis et al. 03]	**Our Research**

Fig. The area of our research.

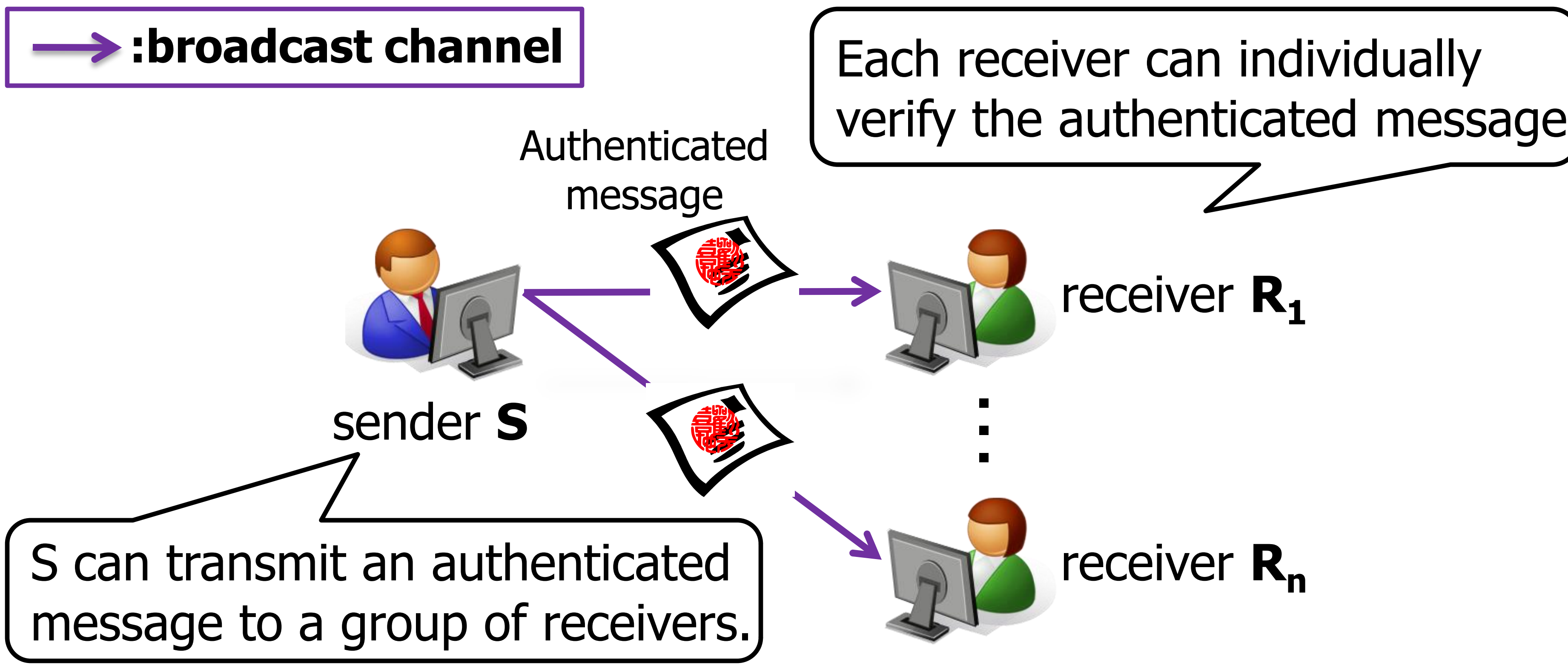
Key-Insulated Signature Schemes [Dodis et al. 03]

Secure against
signing-key exposure
or
master-key exposure



Multireceiver Authentication codes(MRA-codes)

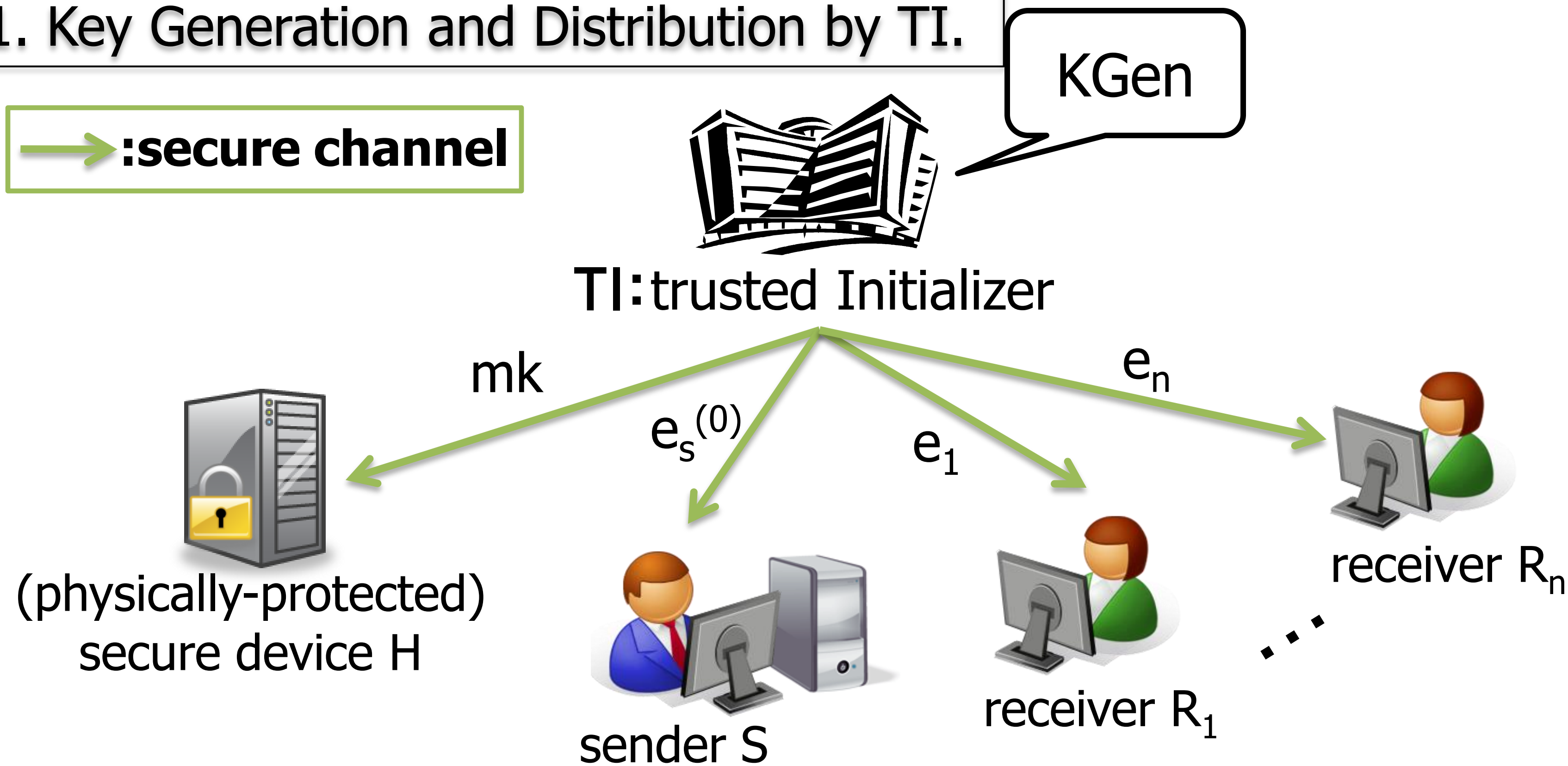
- One of the information-theoretically secure authentication schemes proposed by Desmedt et al. [Desmedt et al. 92].



We focus on this scheme and propose **Key-Insulated Multireceiver Authentication codes (KI-MRA)**.

KI-MRA -Model-

1. Key Generation and Distribution by TI.



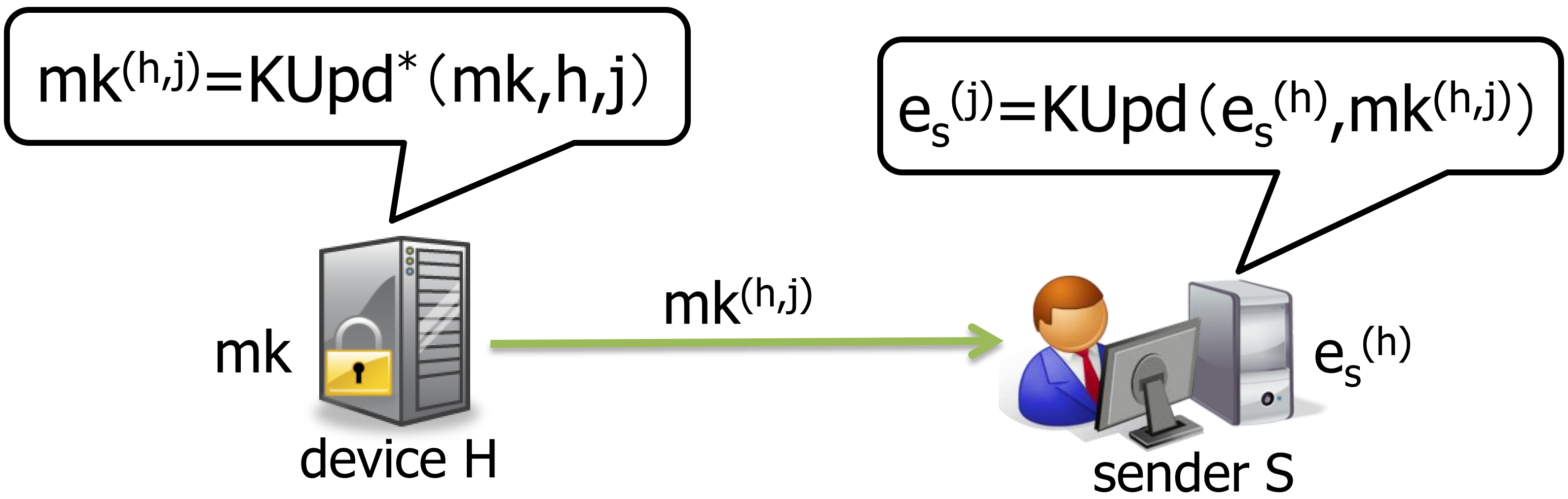
Assumption: Lifetime of the system is divided into **N periods**.

- KGen is a key generation algorithm.
- mk is a master-key.
- $e_s^{(0)}$ is an initial secret-key for the sender S.
- e_i is a secret-key for R_i(It will not be updated at each period).

KI-MRA -Model-

2. Updating sender's secret-keys for a period j from a period h.

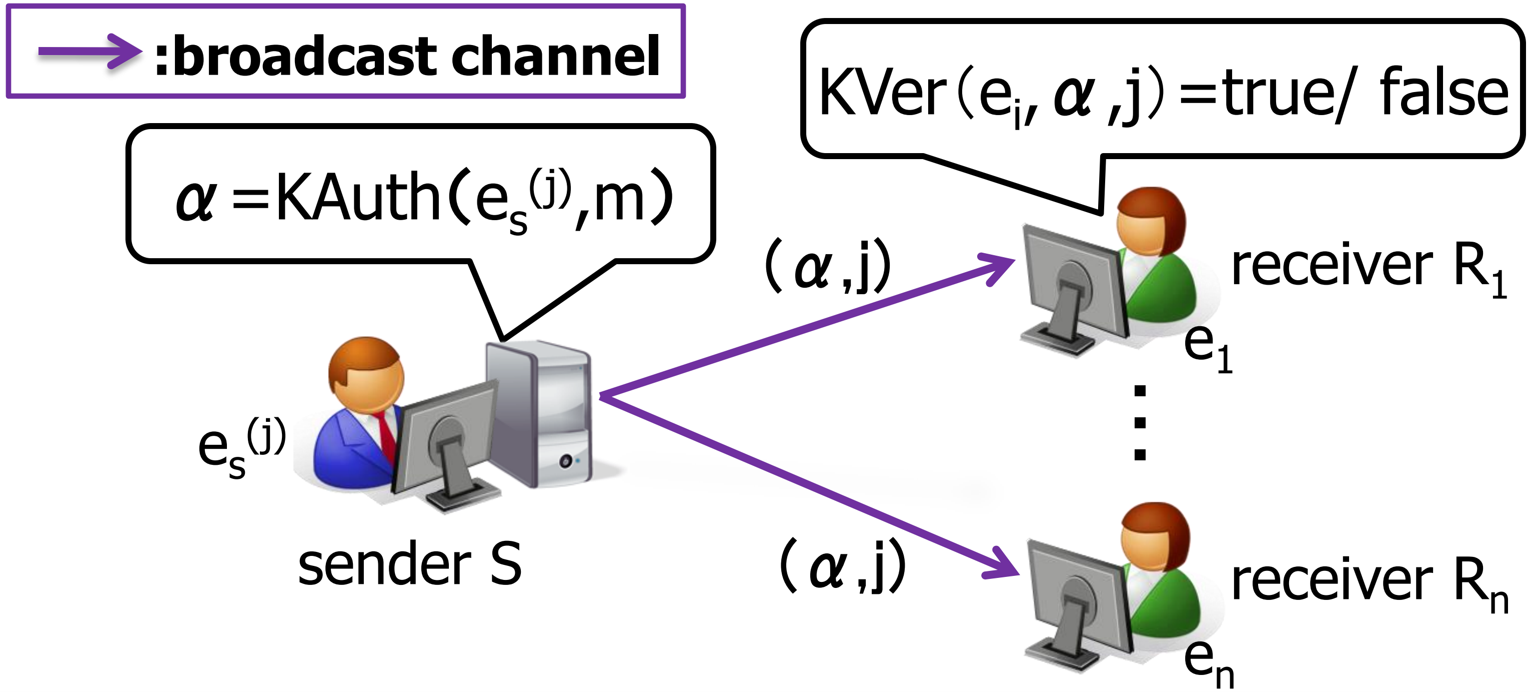
:secure channel



- KUpd* is a key-updating algorithm for the device H.
- Kupd is a key-updating algorithm for the sender S.
- $h \in \{0, 1, \ldots, N\}$, $j \in \{1, 2, \ldots, N\}$.
- $mk^{(h,j)}$ is key-updating information.

KI-MRA -Model-

3. Authentication / Verification at the period j.

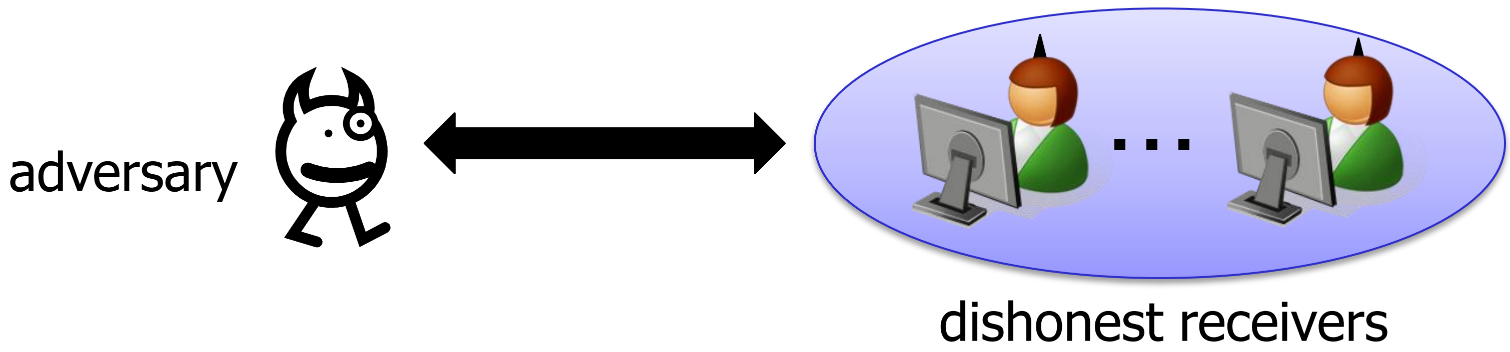


We consider the one-time model, in which the sender is allowed to generate and broadcast an authenticated message at most only once per period.

- KAuth is an authentication algorithm.
- KVer is a verification algorithm.
- m is a message.
- α is an authenticated message.

KI-MRA -Attacking Model-

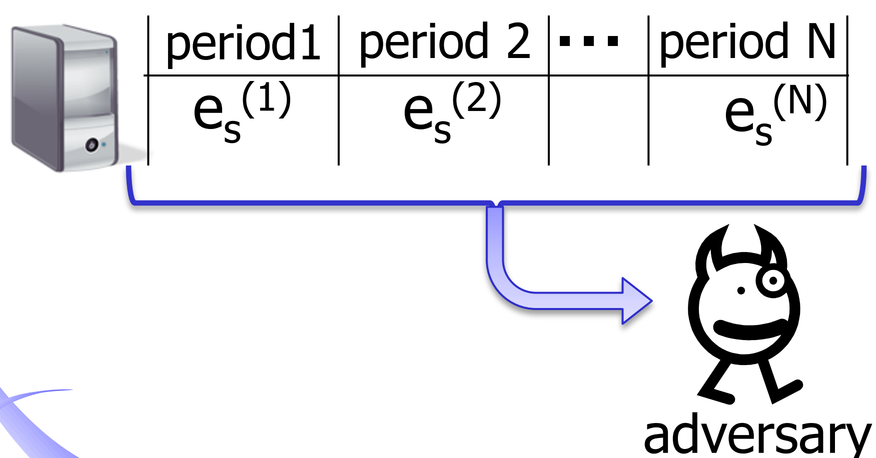
The adversary can corrupt at most ω dishonest receviers.



We consider the following two types of exposure:

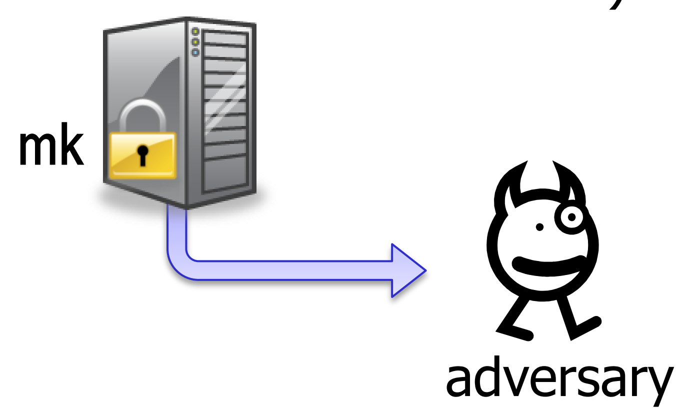
Type A

At most γ sender's secret-keys are exposed from the insecure device.



Type B

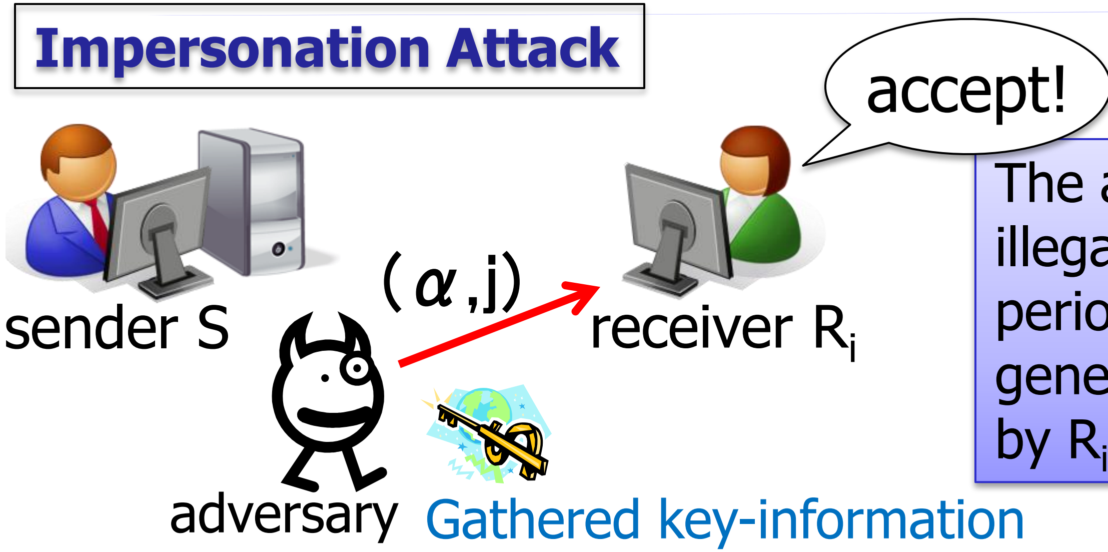
The master-key is exposed from the secure device.
(It means the device is robbed).



KI-MRA -Attacking Model-

Impersonation Attack

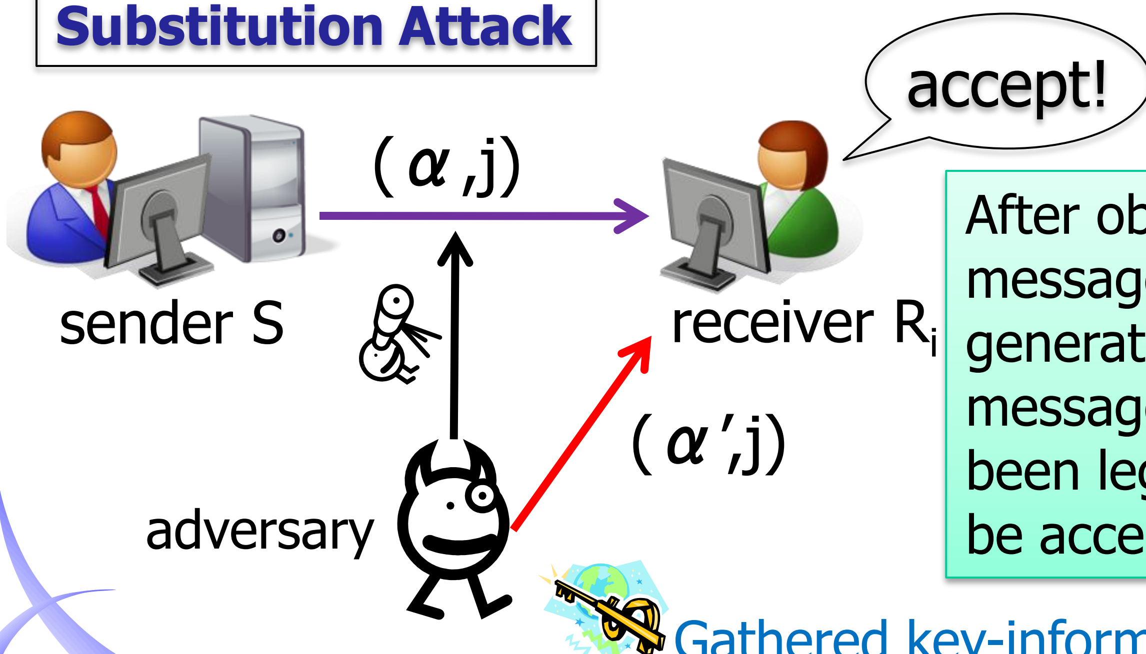
t: target period



The adversary tries to generate an illegal authenticated message at a period t, that has not been legally generated by S but will be accepted by R_i.

Substitution Attack

t: target period



After observing a valid authenticated message, the adversary tries to generate an illegal authenticated message at a period t, that has not been legally generated by S but will be accepted by R_i.

KI-MRA -Security Notions-

Definition.

KI-MRA Π is called $(n,\omega;N,\gamma;\varepsilon_A,\varepsilon_B)$-one-time secure if the following conditions are satisfied.

$$\max(P_{\Pi,IA}, P_{\Pi,SA}) \leq \varepsilon_A, \quad \max(P_{\Pi,IB}, P_{\Pi,SB}) \leq \varepsilon_B$$

- n is the number of receivers.
- ω is the number of dishonest receivers.
- N is the totality of periods.
- γ is the number of period at which sender's secret-keys may be exposed.

	Impersonation Attack	Substitution Attack
Type A	$P_{\Pi,IA}$	$P_{\Pi,SA}$
Type B	$P_{\Pi,IB}$	$P_{\Pi,SB}$

Fig. The combination between attacks and key-exposure types.

KI-MRA -Lower Bounds-

Theorem.

Lower bounds of success probabilities of attacks $P_{\Pi,IA}$, $P_{\Pi,SA}$, $P_{\Pi,IB}$, $P_{\Pi,SB}$ are as follows.

$$P_{\Pi,I_A}(R_i,W,\Gamma,t) \geq 2^{-I(A^{(t)};E_i^{(t)}|E_W,E_\Gamma)}$$

$$P_{\Pi,S_A}(R_i,W,\Gamma,t) \geq 2^{-I(\tilde{A}^{(t)};E_i^{(t)}|E_W,E_\Gamma,A^{(t)})}$$

$$P_{\Pi,I_B}(R_i,W,t) \geq 2^{-I(A^{(t)};E_i^{(t)}|E_W,MK)}$$

$$P_{\Pi,S_B}(R_i,W,t) \geq 2^{-I(\tilde{A}^{(t)};E_i^{(t)}|E_W,MK,A^{(t)})}$$

W is a set of ω dishonest receivers.
$R_i \notin W$ is a target verifier.
Γ is a set of key-exposed period.
$t \notin \Gamma$ is a period when attack will be done.

KI-MRA -Lower Bounds-

Theorem.

Let Π be an (n,ω;N,γ;1/q,1/q)-one-time secure KI-MRA. Then, we have the following lower bounds of memory sizes:

Sender's secret-keys at period j: $|\mathcal{E}_S^{(j)}| \geq q^{2(\omega+1)}$

Receiver R_i's secret-keys: $|\mathcal{E}_i| \geq q^{2(\gamma+1)}$

Master-keys: $|\mathcal{MK}| \geq q^{2\gamma(\omega+1)}$

Key-update information: $|\mathcal{I}^{(h,j)}| \geq q^{2(\omega+1)}$

Authenticated messages: $|\mathcal{A}^{(j)}| \geq 2^{H(M)} q^{\omega+1}$

($1 \leq i \leq n$, $0 \leq \omega < n$, $0 \leq \gamma < N$, $0 \leq h \leq N$, $1 \leq j \leq N$)

Our direct construction will meet all the above inequalities with equalities.

⇒ **The above bounds are tight!**

KI-MRA -Lower Bounds-

Note: The proposed lower bounds of KI-MRA are extension of those of MRA-codes[Safavi-Naini et al. 99].

In the case of γ =0:

Sender's secret-keys at period j: $|\mathcal{E}_S| \geq q^{2(\omega+1)}$

Receiver R_i's secret-keys: $|\mathcal{E}_i| \geq q^2$

Authenticated messages: $|\mathcal{A}| \geq 2^{H(M)} q^{\omega+1}$

($1 \leq i \leq n$, $0 \leq \omega < n$, $0 \leq h \leq N$, $1 \leq j \leq N$)

$(n,\omega;N,0;\varepsilon_A,\varepsilon_B)$-one-time secure KI-MRA = MRA-codes.

– Direct Construction –

A construction which uses polynomials over finite fields F_q (q: prime power).

This construction meets lower bounds with equalities
⇒It is optimal construction.

KI-MRA -Direct Construction-

1. Key Generation and Distribution by TI.

The master-key for the device H

$$F(x,z) := \sum_{i=0}^{\omega}\sum_{k=0}^{1} a_{i,0,k} x^i z^k, \quad mk(x,y,z) := \sum_{i=0}^{\omega}\sum_{j=1}^{\gamma}\sum_{k=0}^{1} a_{i,j,k} x^i y^j z^k$$

$$(a_{i,j,k} \in F_q)$$

The initial secret-key for sender

$$e_S^{(0)}(x, z) := F(x,z)$$

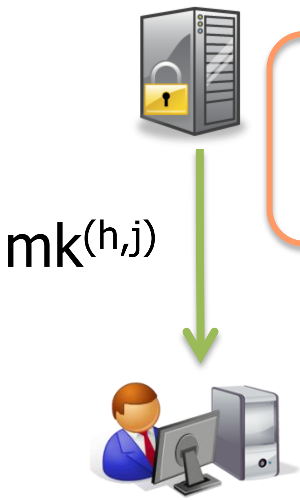
The receiver R_i's secret-key

$$e_i(y, z) := F(R_i,z) + mk(R_i,y,z)$$

$(R_i \in F_q \setminus \{0\}$: R_iのID$)$

KI-MRA -Direct Construction-

2. Updating sender's secret-keys for a period j from a period h.



The key-updating information

$$mk^{(h,j)}(x, z) := mk(x,j,z) - mk(x,h,z)$$

The sender's secret-key at the period j

$$\begin{aligned} e_S^{(j)}(x, z) &:= e_S^{(h)}(x, z) + mk^{(h,j)}(x, z) \\ &= F(x,z) + mk(x,h,z) + mk(x,j,z) - mk(x,h,z) \\ &= F(x.z) + mk(x,j,z) \end{aligned}$$

KI-MRA -Direct Construction-

3. Authentication / Verification at the period j.

Authentication

$$\alpha(x) := e_S^{(j)}(x, m) = F(x,m)+mk(x,j,m)$$

$$\alpha = (m, \alpha(x))$$

$\alpha(x)|_{x=R_i}$

(α, j)

R_i verifies whether these two values are equal.

Verification by R_i

$$e_i(y, z) := F(R_i, z) + mk(R_i, y, z)$$

$e_i(y, z)|_{y=j,\ z=m}$

KI-MRA -Direct Construction-

Theorem.
The proposed construction is (n,ω;N,γ;1/q,1/q)-one-time secure, and optimal.

Memory sizes of secret-keys and authenticated messages

Sender's secret-keys at period j: $|\mathcal{E}_S^{(j)}| = q^{2(\omega+1)}$

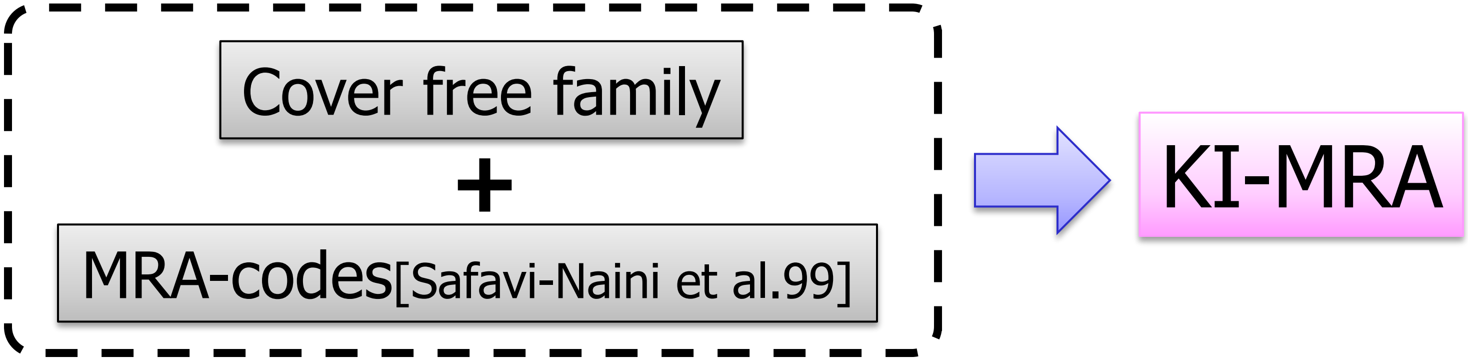
Receiver R_i's secret-keys: $|\mathcal{E}_i| = q^{2(\gamma+1)}$

Master-keys: $|\mathcal{MK}| = q^{2\gamma(\omega+1)}$

Key-update information: $|\mathcal{I}^{(h,j)}| = q^{2(\omega+1)}$

Authenticated messages: $|\mathcal{A}^{(j)}| = 2^{H(M)} q^{\omega+1}$

- Generic Construction -



<u>Merit</u>: A **flexibility** in choosing system parameters.

Cover free family (CFF) [Erdos et al.85]

Definition.

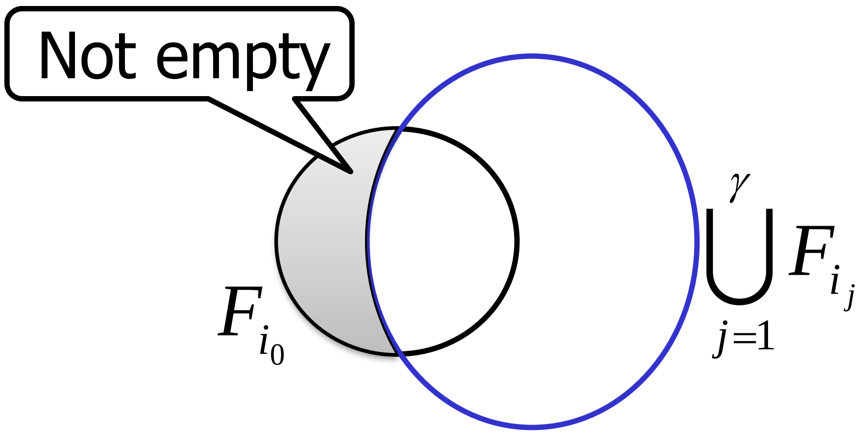
Let

- $\mathcal{L}=\{l_1, l_2, \ldots, l_d\}$ be a universal set.
- $\mathcal{F}=\{F_1, F_2, \ldots, F_N\}$ be a family of subsets of $\mathcal{L}$.

Then, we call it **(d, N, γ)-CFF** if

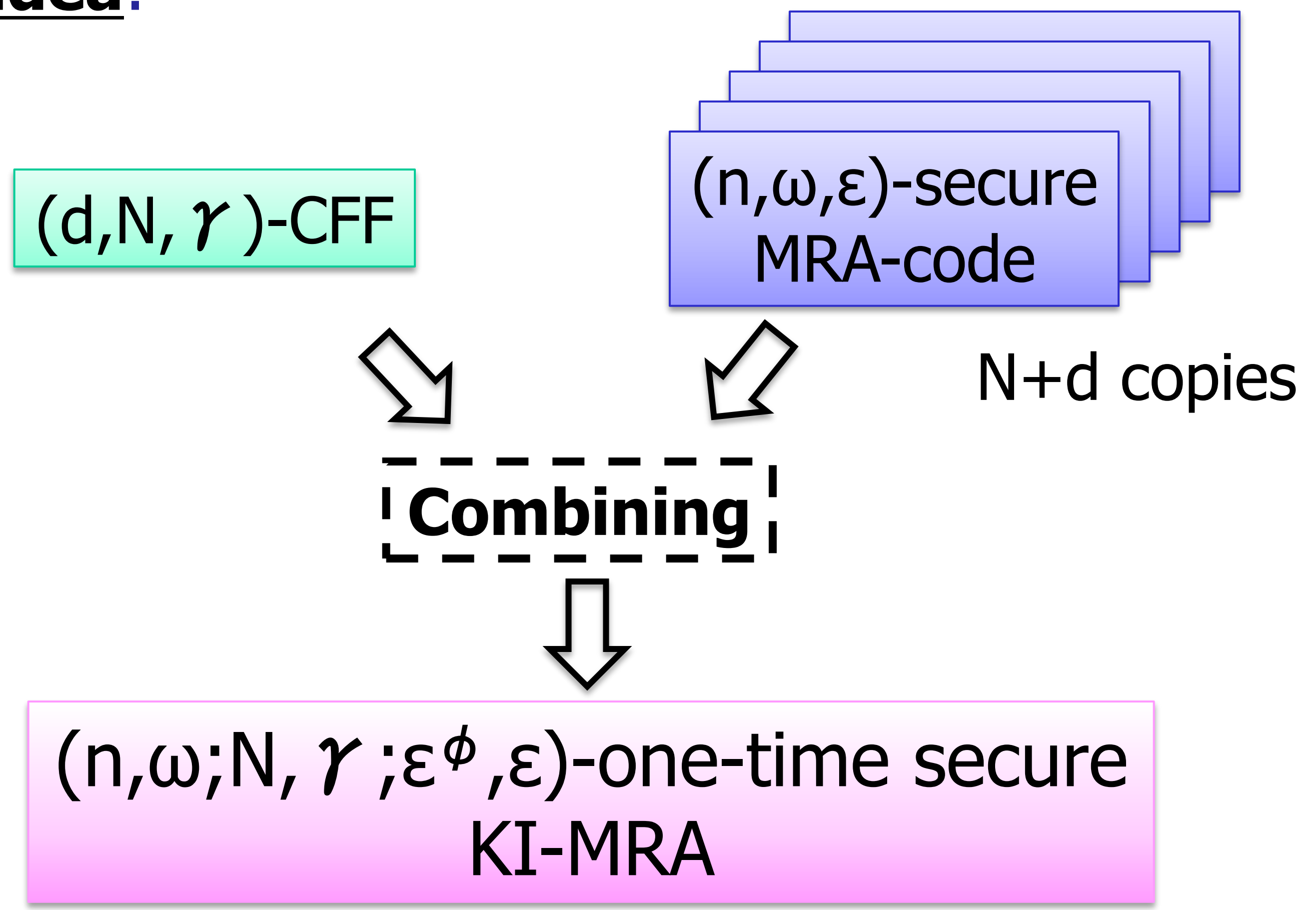
$$F_{i_0} \not\subset F_{i_1} \cup F_{i_2} \cup \ldots \cup F_{i_\gamma}$$

for all $F_{i_0}, F_{i_1}, F_{i_2}, \ldots, F_{i_\gamma} \in \mathcal{F} \, (F_{i_j} \neq F_{i_k}$, if $j \neq k)$



KI-MRA -Generic Construction-

- **Basic idea**:



[Note]

- n is the number of receivers
- ω is the number of dishonest receivers
- ε is a success probability of attacks

} of the underlying MRA-code.

KI-MRA -Generic Construction-

1. Key Generation and Distribution by TI.

$(u_0^{(j)}, v_{1,0}^{(j)}, v_{2,0}^{(j)}, \ldots, v_{n,0}^{(j)})$: the j-th output from MGen $(1 \le j \le N)$

$(u_1^{(l_g)}, v_{1,1}^{(l_g)}, v_{2,1}^{(l_g)}, \ldots, v_{n,1}^{(l_g)})$: the g-th output from MGen $(1 \le g \le d)$

※these keys are corresponding to $l_i \in \mathcal{L}$

The initial secret-key for the sender

$$e_S^{(0)} := (u_0^{(1)}, u_0^{(2)}, \ldots, u_0^{(N)}, U^{(0)}) \quad (U^{(0)} = \phi)$$

The receiver R_i's secret-key

$$e_i := (v_{i,0}^{(1)}, v_{i,0}^{(2)}, \ldots, v_{i,0}^{(N)}, v_{i,1}^{(l_1)}, v_{i,1}^{(l_2)}, \ldots, v_{i,1}^{(l_d)})$$

The master-key

$$mk := (u_1^{(l_1)}, u_1^{(l_2)}, \ldots, u_1^{(l_d)})$$

- MGen: a key generation algorithm of MRA-code.
- $u_0^{(j)}$, $u_1^{(j)}$: a secret-key for sender.
- $v_{i,0}^{(j)}$, $v_{i,1}^{(j)}$: a secret-key for receiver.

KI-MRA -Generic Construction-

2. Updating sender's secret-keys for a period j from a period h.

The key-updating information

$$mk^{(h,j)} := U^{(j)} \; (U^{(j)} := \{u_1^{(l)} \mid l \in F_j\})$$

$F_j \Leftrightarrow$ period j

mk$^{(h,j)}$

The sender's secret-key at the period j

$$e_S^{(j)} := (u_0^{(1)}, u_0^{(2)}, \ldots, u_0^{(N)}, U^{(j)})$$

exchange

Update

$$e_S^{(h)} = (u_0^{(1)}, u_0^{(2)}, \ldots, u_0^{(N)}, U^{(h)})$$

The sender's secret-key at the period h

KI-MRA -Generic Construction-

■ Security:

t: target period

$$U^{(j)} := \{u_1^{(l)} \mid l \in F_j\}$$

a set of sender's secret-keys corresponding to F_j.

The sender's secret-key at the period t

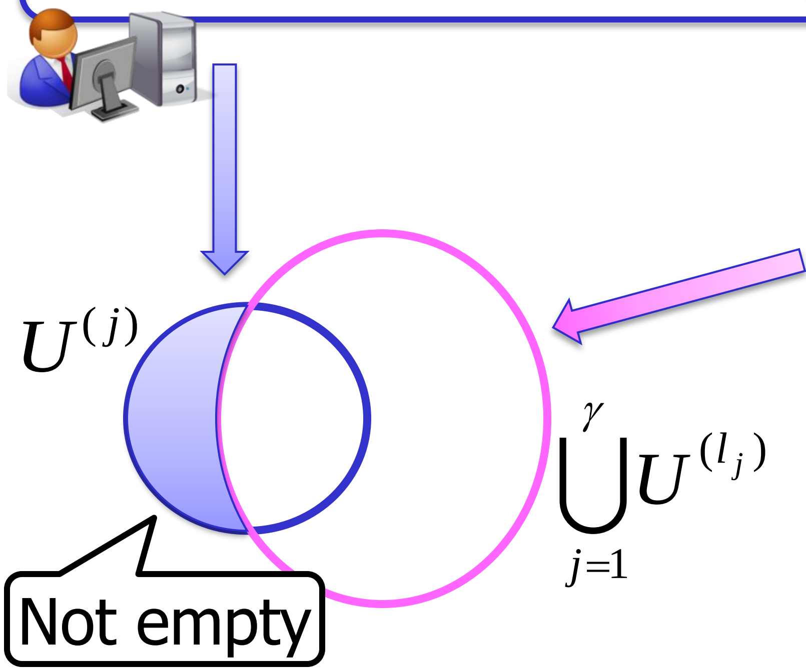
$$e_S^{(j)} := (u_0^{(1)}, u_0^{(2)}, \ldots, u_0^{(N)}, U^{(j)})$$

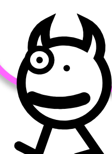
γ exposed secret-keys for the sender

$$e_S^{(l_1)} := (u_0^{(1)}, u_0^{(2)}, \ldots, u_0^{(N)}, U^{(l_1)})$$

$$\vdots$$

$$e_S^{(l_\gamma)} := (u_0^{(1)}, u_0^{(2)}, \ldots, u_0^{(N)}, U^{(l_\gamma)})$$





From the definition of CFF...

the adversary cannot obtain all information about the sender's secret-key at the target period t.

KI-MRA -Generic Construction-

3. Authentication / Verification at the period j.

Authentication

$$\alpha := (m, \delta_0^{(j)}, \delta_{i_1}^{(j)}, \delta_{i_2}^{(j)} \ldots, \delta_{i_{|Fj|}}^{(j)})$$

$$\left[\begin{array}{l} \delta_0^{(j)} := \mathrm{MAuth}(u_0^{(j)}, m) \\ \delta_0^{(j)} := \mathrm{MAuth}(u_1^{(i_g)}, m) \text{ for all } i_g \in F_j \end{array}\right.$$

(α,j)

Verification by R_i

$$\left[\begin{array}{l} \mathrm{MVer}(v_{i,0}^{(j)}, \delta_0^{(j)}) \stackrel{?}{=} true \\ \mathrm{MVer}(v_{i,1}^{(l_g)}, \delta_{l_g}^{(j)}) \stackrel{?}{=} true \text{ for all } l_g \in F_j \end{array}\right.$$

- MAuth: an authentication algorithm of MRA-code.
- MVer: a verification algorithm of MRA-code.

KI-MRA -Generic Construction-

Theorem.

The proposed construction is $(n,\omega;N,\gamma;\varepsilon^{\phi},\varepsilon)$-one-time secure.

Here, $\phi := \min(|F_{i0} - \{F_{i1} \cup \ldots F_{i\gamma}\}|)$,where the minimum is taken over all $F_{i0}, F_{i1}, \ldots, F_{i\gamma} \in \mathcal{F}$.

Conclusion

We studied Information-Theoretically Secure Key-Insulated Multireceiver Authentication codes (**KI-MRA**).

Our Results

- Newly introduced the model of KI-MRA.
- Defined and formalized security notions of KI-MRA.
- Derived lower bounds of success probabilities of attacks and memory sizes required for a secure KI-MRA(**tight**).
- Proposed two constructions:
  - Direct Construction(**optimal**)
  - Generic Construction

Thank you!

Appendix: Memory sizes of Constructions

Memory sizes of the generic construction

Sender's secret-keys at period j: $|\mathcal{E}_S^{(j)}| = (N + |F_j|)|\mathcal{U}|$

Receiver R_i's secret-keys: $|\mathcal{E}_i| = (N + d)|\mathcal{V}|$

Master-keys: $|\mathcal{MK}| = d|\mathcal{U}|$

Key-update information: $|\mathcal{I}^{(h,j)}| = |F_j||\mathcal{U}|$

Authenticated messages: $|\mathcal{A}^{(j)}| = (|F_j| + 1)|\mathcal{D}|$

Appendix: Formalization of $P_{\pi,IA}$

For any set of colluder W, any set of key-exposure periods Γ, any targeted honest receiver $R_i \notin W$ and target period $t \notin \Gamma$, then

$$P_{\Pi,IA}(R_i, W, \Gamma, t) := \max_{e_W} \max_{e_\Gamma} \max_{(\alpha,t)} \Pr(KVer(e_i, \alpha, t) = true \mid e_W, e_\Gamma)$$

- e_W: a set of the colluders' secret-keys.
- e_Γ: a set of sender's secret-keys exposed such that $e_s^{(t)} \notin e_\Gamma$.
- (α, t): an authenticated message.

Appendix : Formalization of $P_{\Pi,SA}$

For any set of colluder W, any set of key-exposure periods Γ, any targeted honest receiver $R_i \notin W$ and target period $t \notin \Gamma$, then

$$P_{\Pi,SA}(R_i, W, \Gamma, t) := \max_{e_W} \max_{e_\Gamma} \max_{(\alpha',t)} \max_{(\alpha,t)\neq(\alpha',t)} \Pr(KVer(e_i, \alpha, t) = true \mid e_W, e_\Gamma, (\alpha', t))$$

- e_W: a set of the colluders' secret-keys.
- e_Γ: a set of sender's secret-keys exposed such that $e_s^{(t)} \notin e_\Gamma$.
- (α', t), (α, t): an authenticated message.

Appendix: Formalization of $P_{\Pi,IB}$

For any set of colluder W, any targeted honest receiver $R_i \notin W$ and target period $t \notin \Gamma$, then

$$P_{\Pi,IB}(R_i, W, t) := \max_{e_W} \max_{mk} \max_{(\alpha,t)} \Pr(KVer(e_i, \alpha, t) = true \mid e_W, mk)$$

- e_W: a set of the colluders' secret-keys.
- mk: an exposed master-key.
- (α,t): an authenticated message.

Appendix: Formalization of $P_{\Pi,SB}$

For any set of colluder W, any targeted honest receiver $R_i \notin W$ and target period t $\notin \Gamma$, then

$$P_{\Pi,SB}(R_i, W, t) := \max_{e_W} \max_{mk} \max_{(\alpha',t)} \max_{(\alpha,t)\neq(\alpha',t)} \Pr(KVer(e_i, \alpha, t) = true \mid e_W, mk, (\alpha', t))$$

- e_W: a set of the colluders' secret-keys.
- mk: an exposed master-key.
- (α',t), (α,t): an authenticated message.