Constructions of Unconditionally Secure Broadcast Encryption from Key Predistribusion Systems with Trade-offs between Communication and Storage

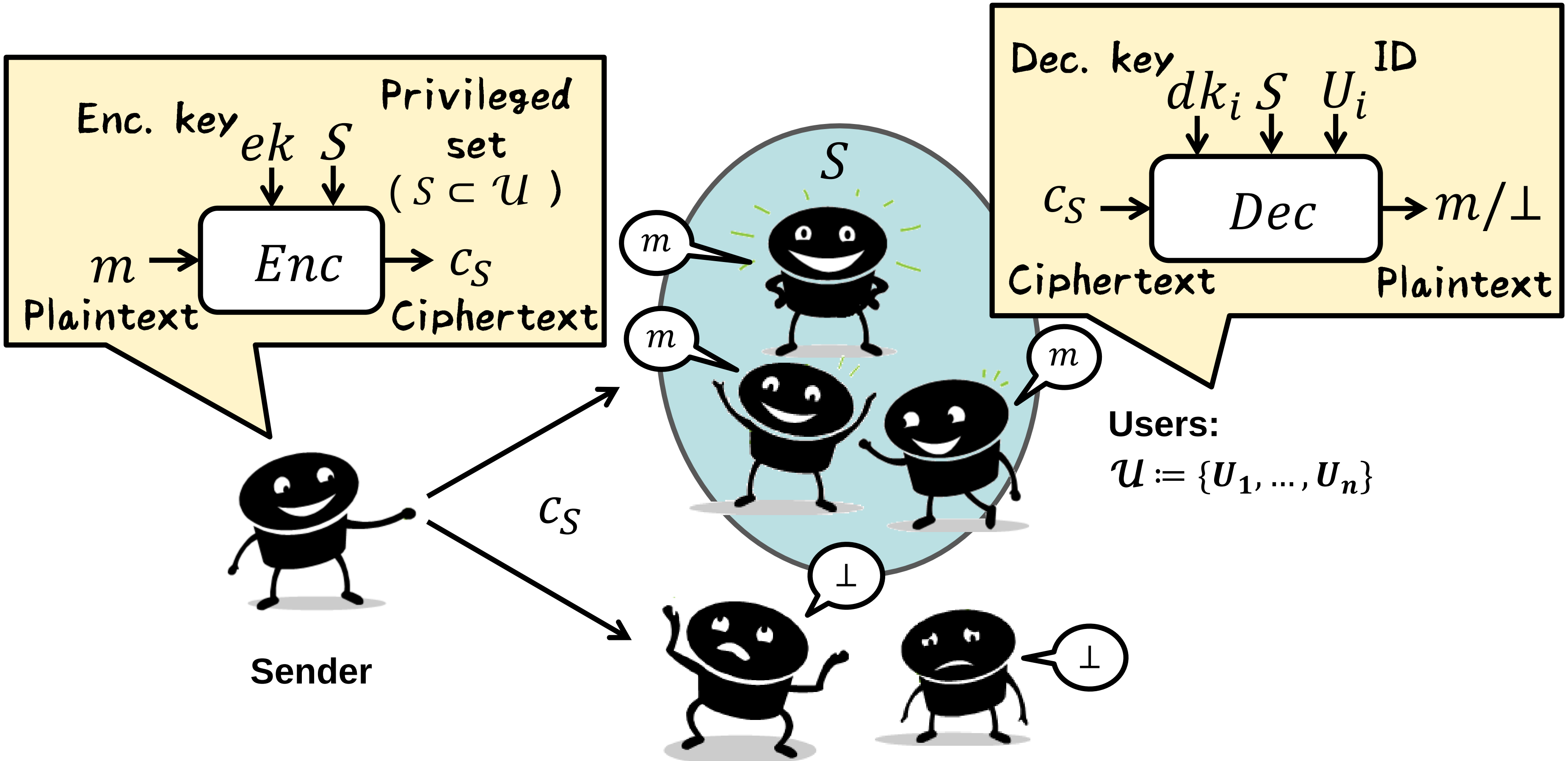
Yohei Watanabe and Junji Shikata

Yokohama National University, Japan

ProvSec 2015

Broadcast Encryption (BE) [Ber91,FN93]

Allows a sender to choose a subset of a user set (called a *privileged set*) so that only a user in the privileged set can decrypt a ciphertext.



Unconditionally Secure BESs

There are two types of BESs:

✓ Suppose that $\boldsymbol{n}$ is the number of users and $\boldsymbol{\omega}$ is the number of colluders.

- $(\boldsymbol{t}, \leq \boldsymbol{\omega})$**-one-time secure BES** **[BC94,KYDB98,LS98,PGM04]**
  - Number of privileged users: **exactly $\boldsymbol{t}$ ($|S| = t$)**.
  - Secret-key sizes: **smaller**.

Our Target

- $(\leq \boldsymbol{n}, \leq \boldsymbol{\omega})$**-one-time secure BES** **[BC94, FN93]**
  - Number of privileged users: **no limitation ($1 \leq |S| \leq n$)**.
  - Secret-key sizes: ***significantly* larger**.

There are trade-offs between the secret-key and ciphertext sizes.

- Analysis by deriving lower bounds on sizes of secret keys.
- Analysis by proposing constructions (deriving upper bounds on the secret-key sizes).

This Work

YNU

Trade-offs in $(t, \leq \omega)$-one-time Secure BESs

- **Analysis by deriving lower bounds on sizes of secret keys where the ciphertext sizes are …**

  i. ***equal*** to the plaintext sizes [BC94,KYDB98]

  ii. ***integer multiple*** of plaintext sizes[BMS96]

  iii. ***Any*** sizes[PGM04]

Tight!

- **Analysis by proposing constructions (deriving upper bounds) where the ciphertext sizes are …**

  a. ***equal*** to the plaintext sizes[BSH+93]

  b. ***integer multiple*** of plaintext sizes[BMS96]

  c. ***Any*** sizes[PGM04]

  (d. t times larger than the plaintext sizes (trivially constructed from one-time pads).)

Tight bounds for the case that the ciphertext sizes are larger than the plaintext sizes: Open problem !

Trade-offs in $(\leq n, \leq \omega)$-one-time Secure BESs

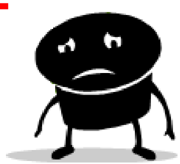
- **Analysis by deriving lower bounds on sizes of secret keys where the ciphertext sizes are …**

  i. ***equal*** to the plaintext sizes [BC94]

  ii. ~~***integer multiple*** of plaintext sizes~~

  iii. ~~***Any*** sizes~~

Unknown…



Tight!

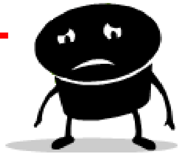
- **Analysis by proposing constructions (deriving upper bounds) where the ciphertext sizes are …**

  a. ***equal*** to the plaintext sizes[FN93]

  b. ~~***integer multiple*** of plaintext sizes~~

  c. ~~***Any*** sizes~~

Unknown…



(d. At most n times larger than the plaintext sizes (trivially constructed from one-time pads).)

Tight bounds for the case that the ciphertext sizes are larger than the plaintext sizes: Open problem !

Trade-offs in $(\leq n, \leq \omega)$-one-time Secure BESs

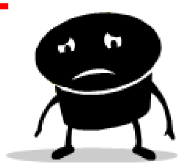
- **Analysis by deriving lower bounds on sizes of secret keys where the ciphertext sizes are …**

  i. ***equal*** to the plaintext sizes [BC94]

  ii. ~~***integer multiple*** of plaintext sizes~~

  iii. ~~***Any*** sizes~~

Unknown…



Tight!

- **Analysis by proposing constructions (deriving upper bounds) where the ciphertext sizes are …**

  a. ***equal*** to the plaintext sizes[FN93]

  b. ***integer multiple* of plaintext sizes**

  c. ~~***Any*** sizes~~

  (d. At most n times larger than the plaintext sizes (trivially constructed from one-time pads).)

This Work !

Tight bounds for the case that the ciphertext sizes are larger than the plaintext sizes: Open problem !

Our Contribution

We propose a generic construction of $(\leq n, \leq \omega; \delta)$-one-time secure BESs for the case that the maximum ciphertext size is δ time larger than the plaintext size ($\delta \in [n] := \{1, 2, \dots, n\}$).

- **From δ key predistribution systems (KPSs)[Blo85,MI88]**

However, for fixed n, ω and δ, there are many possible combinations of the KPSs in our construction methodology.

➡ **We show which combination is the best one in the sense that the secret-key size can be minimized.**

We also succeed in improving the practicality of BESs.

✓ Let $n = 100$ and the plaintext size is 100MB.

Our Result

Ciphertext size	$\delta = 1$ (100MB)	$\cdots$	$\delta = 10$ (1GB)	$\cdots$	$\delta = 100$ (10GB)
$\omega = 3$	16.2TB	$\cdots$	13GB	$\cdots$	100MB
$\omega = 4$	392.6TB	$\cdots$	25.8GB	$\cdots$	100MB
$\omega = 5$	7.5PB	$\cdots$	38.2GB	$\cdots$	100MB

Why the One-time Model?

In this work, we consider the one-time model, where …

- **Sender encrypts a plaintext and broadcasts a ciphertext only once.**

Why are BESs considered in such a restricted model?

Because it makes the analysis more simplified!
Model and security formalization often become complicated in a multiple-time model.

Actually, related works[FN93,BC94,KYDB98,PGM04] and the following recent works are dealt with the one-time models.

- Oblivious polynomial evaluation[TND+15]
- Key distribution[SJ11]
- Authentication codes[TSND09, NSS08]

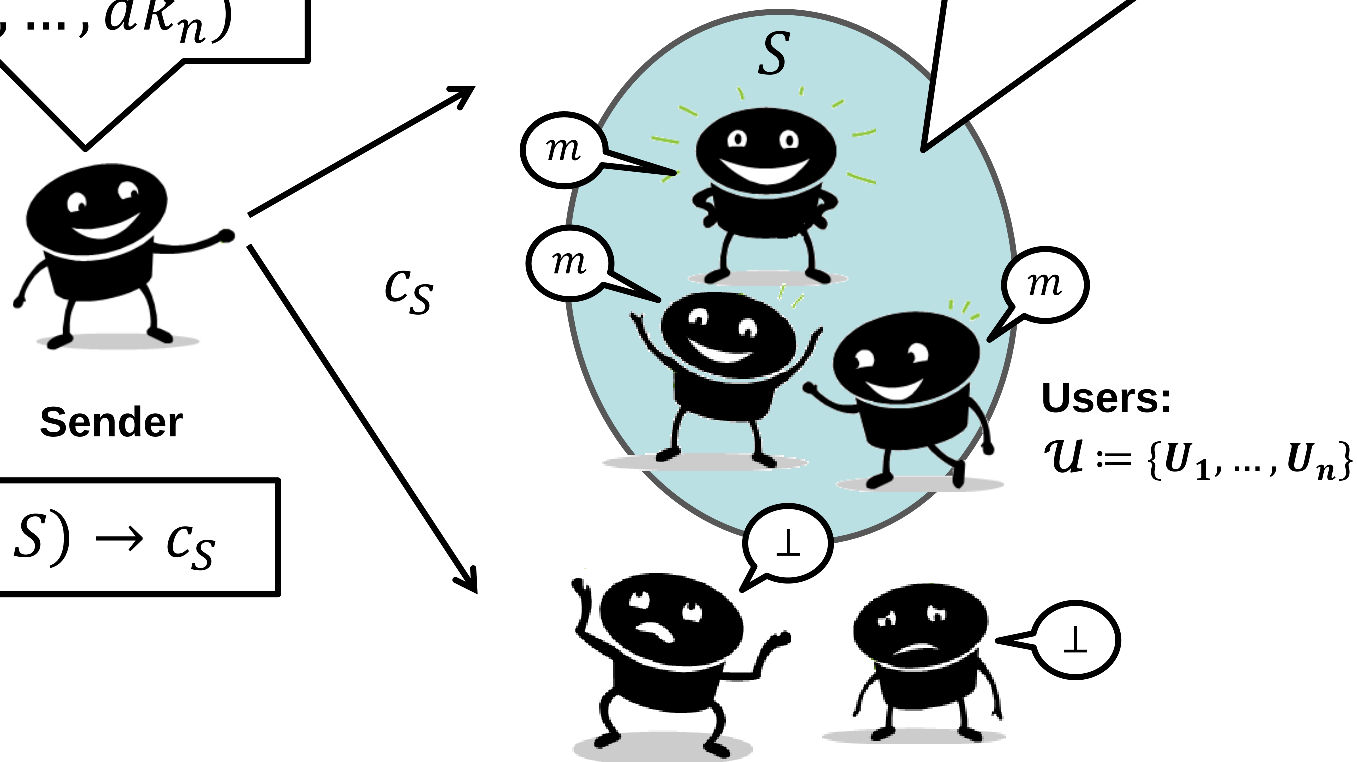
We believe our result will be a basis for analyzing multiple-time BESs.

$(\leq n, \leq \omega)$-one-time Secure BES: Model

1. $\mathrm{Setup}(n) \rightarrow (ek, dk_1, \ldots, dk_n)$

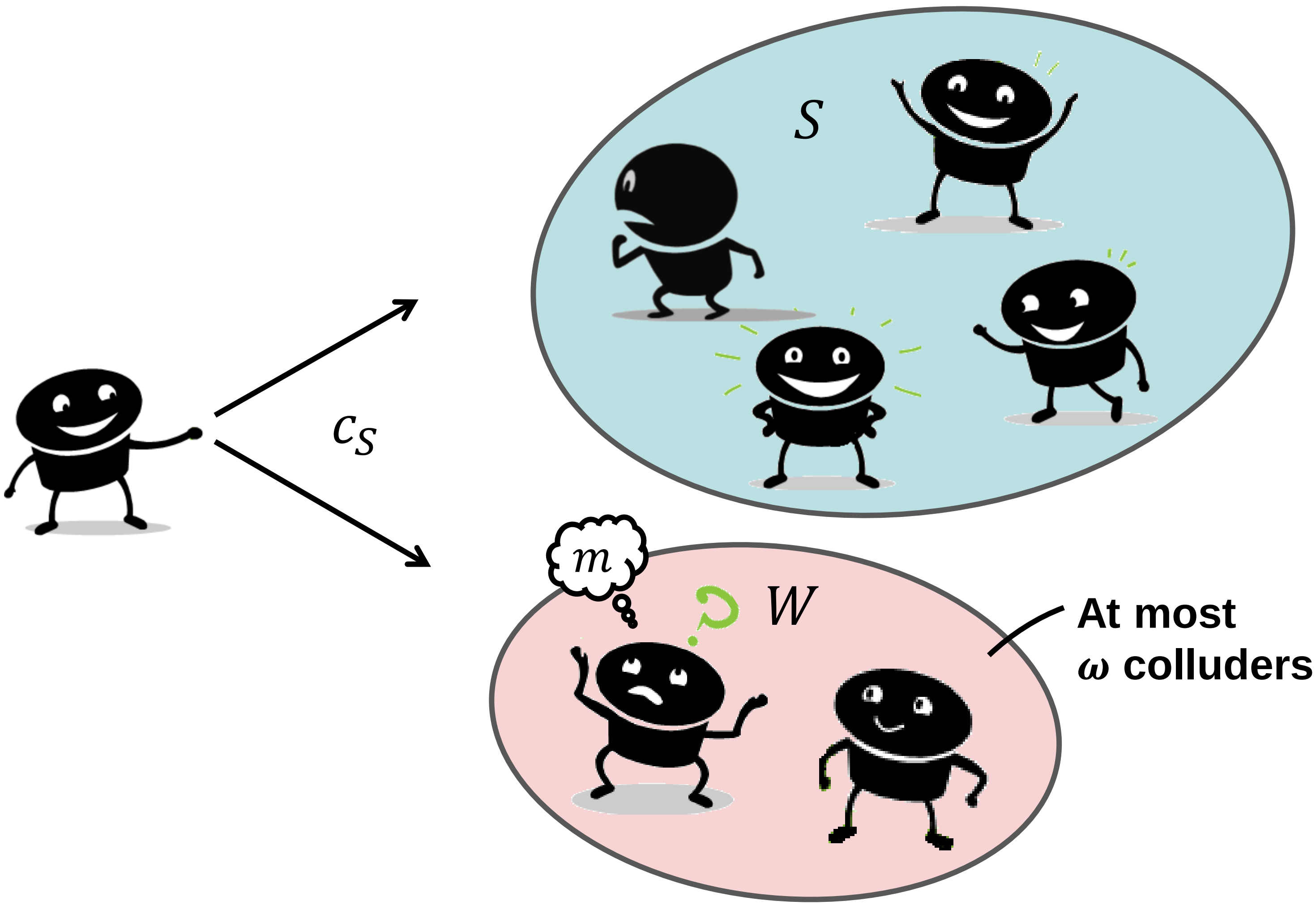
2. $Enc(ek, m, S) \rightarrow c_S$

3. $Dec(dk_i, c_S, S, U_i) \rightarrow m$ if $U_i \in S$.
   $Dec(dk_i, c_S, S, U_i) \rightarrow \perp$ if $U_i \notin S$.



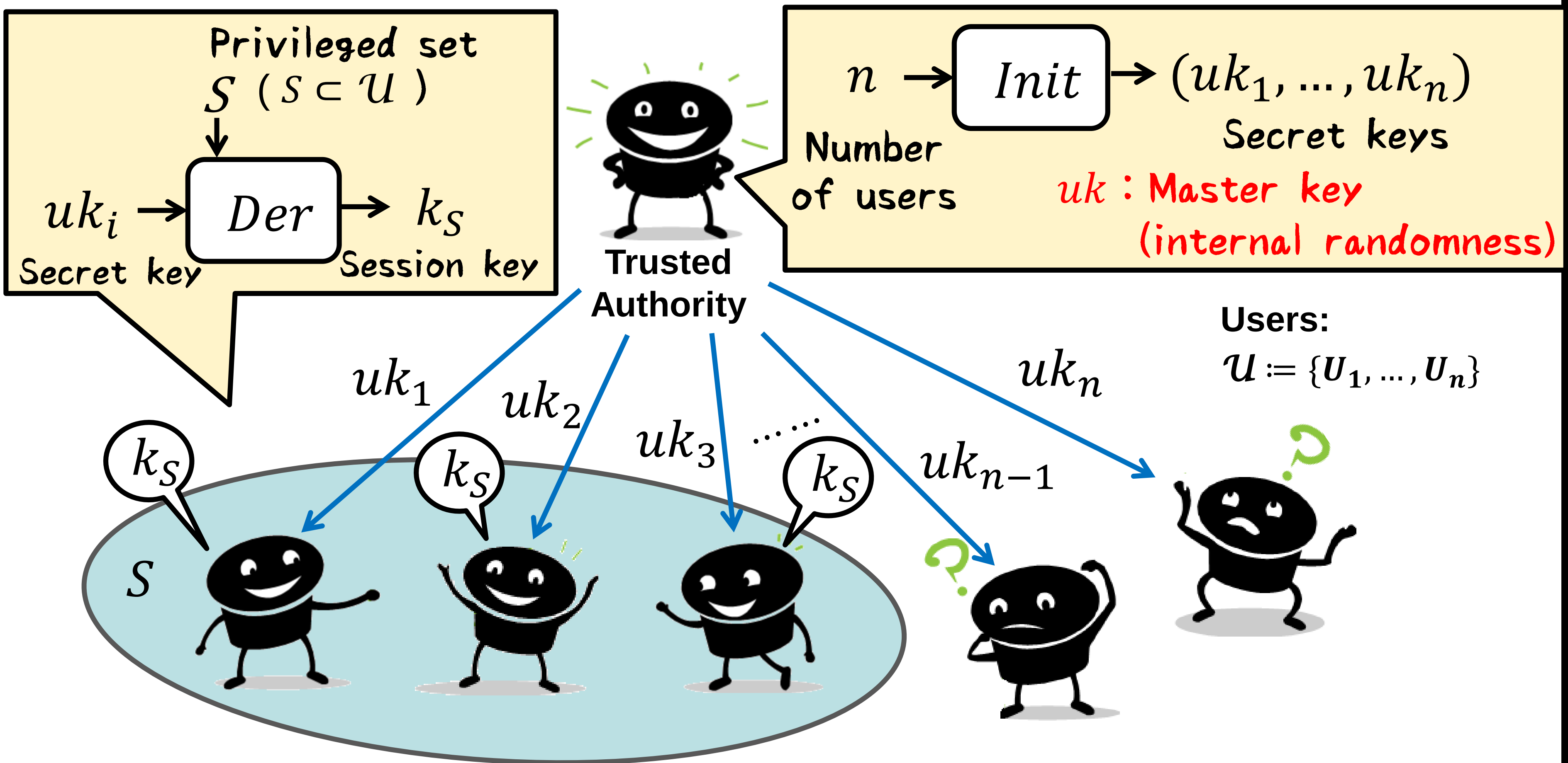
$(\leq n, \leq \omega)$-one-time Secure BES: Security

- At most ω colluders who are not included in S cannot get any information on the plaintext m from the ciphertext c_S.

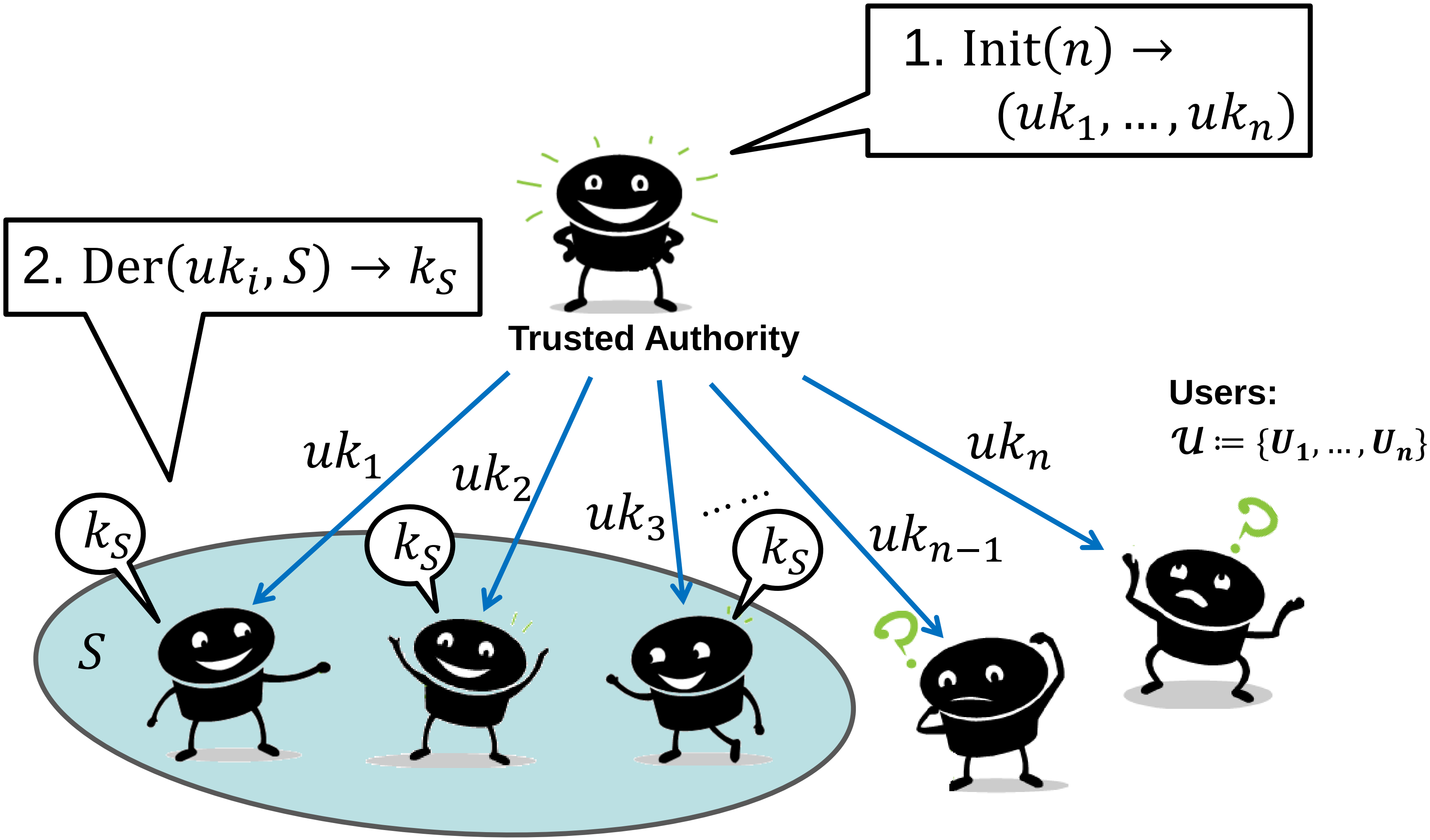


Key Predistribution System: KPS

- **Each user U_i can choose arbitrary subset $S \subset \mathcal{U}$ s. t. $U_i \in S$ and generate a common key k_S for S without any interaction.**

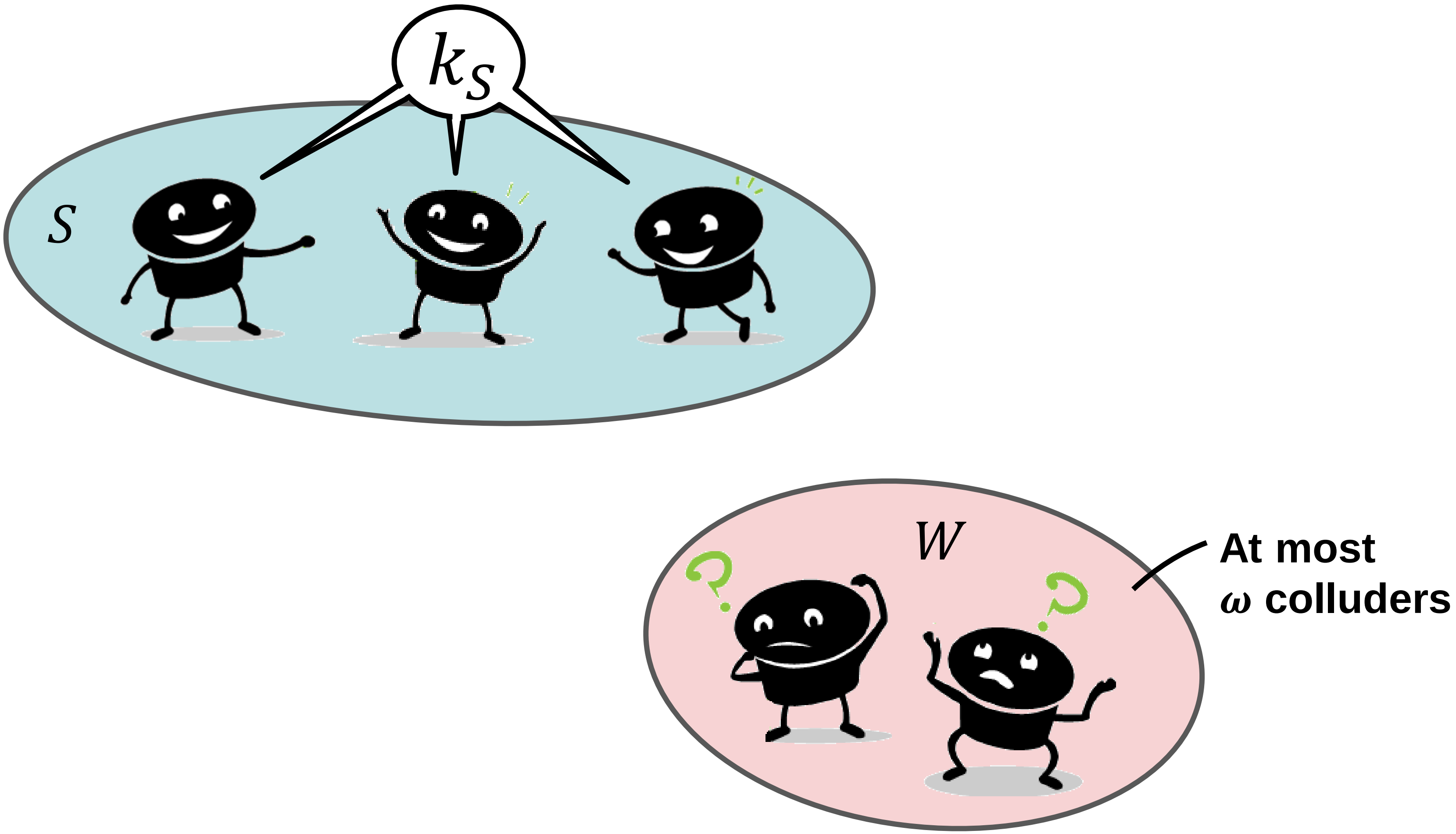


$(\leq n, \leq \omega)$-KPS: Model



$(\leq n, \leq \omega)$-KPS: Security

- At most ω colluders who are not included in S cannot get any information on the session key k_S from their secret keys.



Existing Constructions of $(\le n, \le \omega)$-one-time Secure BESs

Only two constructions of $(\le \boldsymbol{n}, \le \boldsymbol{\omega})$-one-time secure BESs are known so far.

- $(\le n, \le \omega; 1)$**-one-time secure BES (i.e. $\boldsymbol{\delta} = \mathbf{1}$) [FN93]:**
  - Can be constructed from $(\le \boldsymbol{n}, \le \boldsymbol{\omega})$**-KPS**.
- $(\le n, \le \omega; n)$**-one-time secure BES (i.e. $\boldsymbol{\delta} = \boldsymbol{n}$):**
  - Can be constructed from $\boldsymbol{n}$ $(\le \mathbf{1}, \le \mathbf{0})$**-KPSs** (i.e. n one-time pads).

Our Construction:

- $(\le n, \le \omega; \delta)$**-one-time secure BES for arbitrary $\boldsymbol{\delta} \in \{\mathbf{1}, \dots \boldsymbol{n}\}$.**
  - Constructed from $\boldsymbol{\delta}$ $(\le \boldsymbol{n}', \le \boldsymbol{\omega}')$**-KPSs**.

Remark

Our construction includes the above two constructions as special cases. Namely, our construction can be considered as an extension of those.

Our Construction: Basic Idea

$(\leq n, \leq \omega; \delta)$**-one-time secure BES** $\boldsymbol{\Pi}$

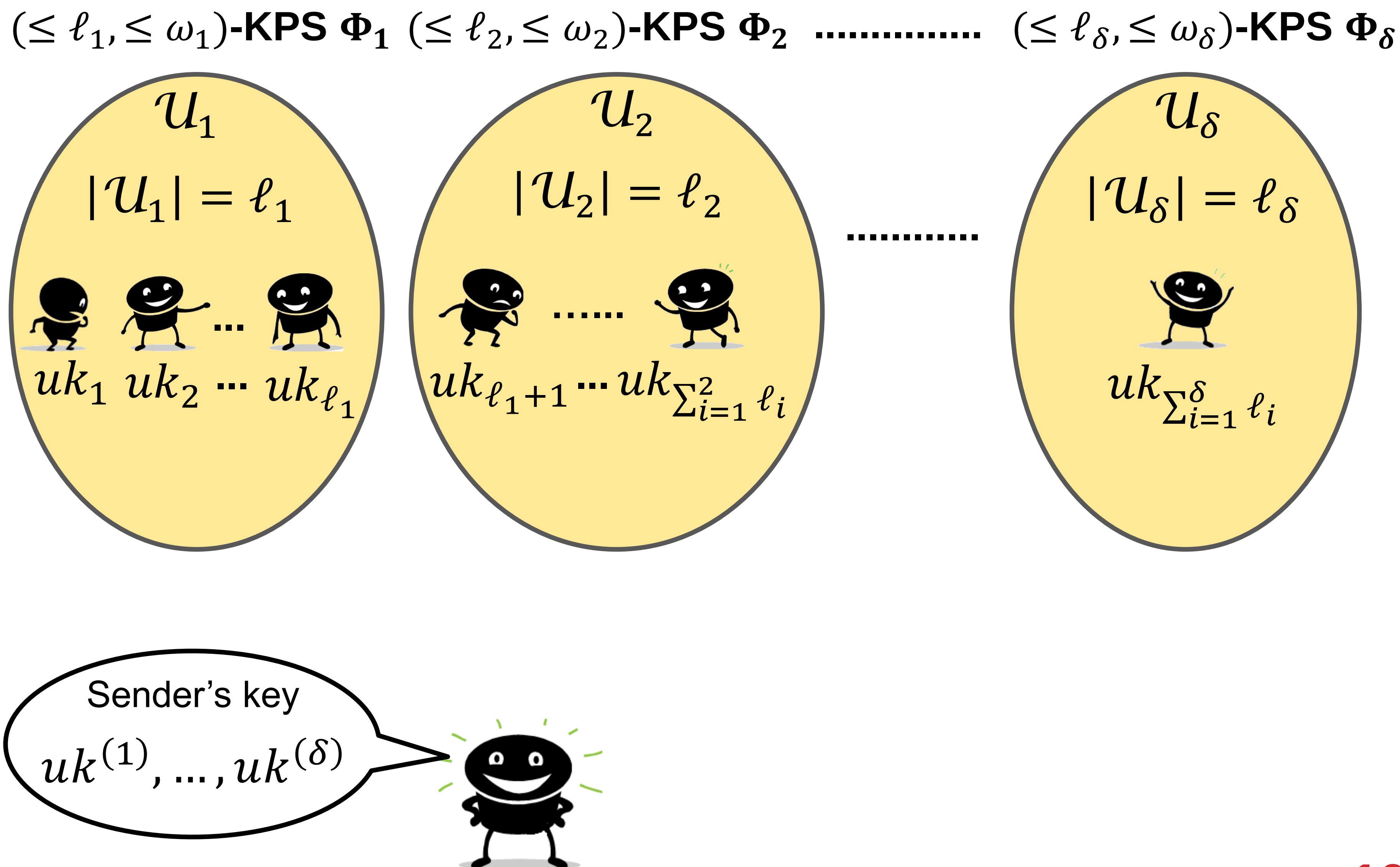
$\mathcal{U}$

$|\mathcal{U}| = n$

Split into $\boldsymbol{\delta}$ **disjoint sets**

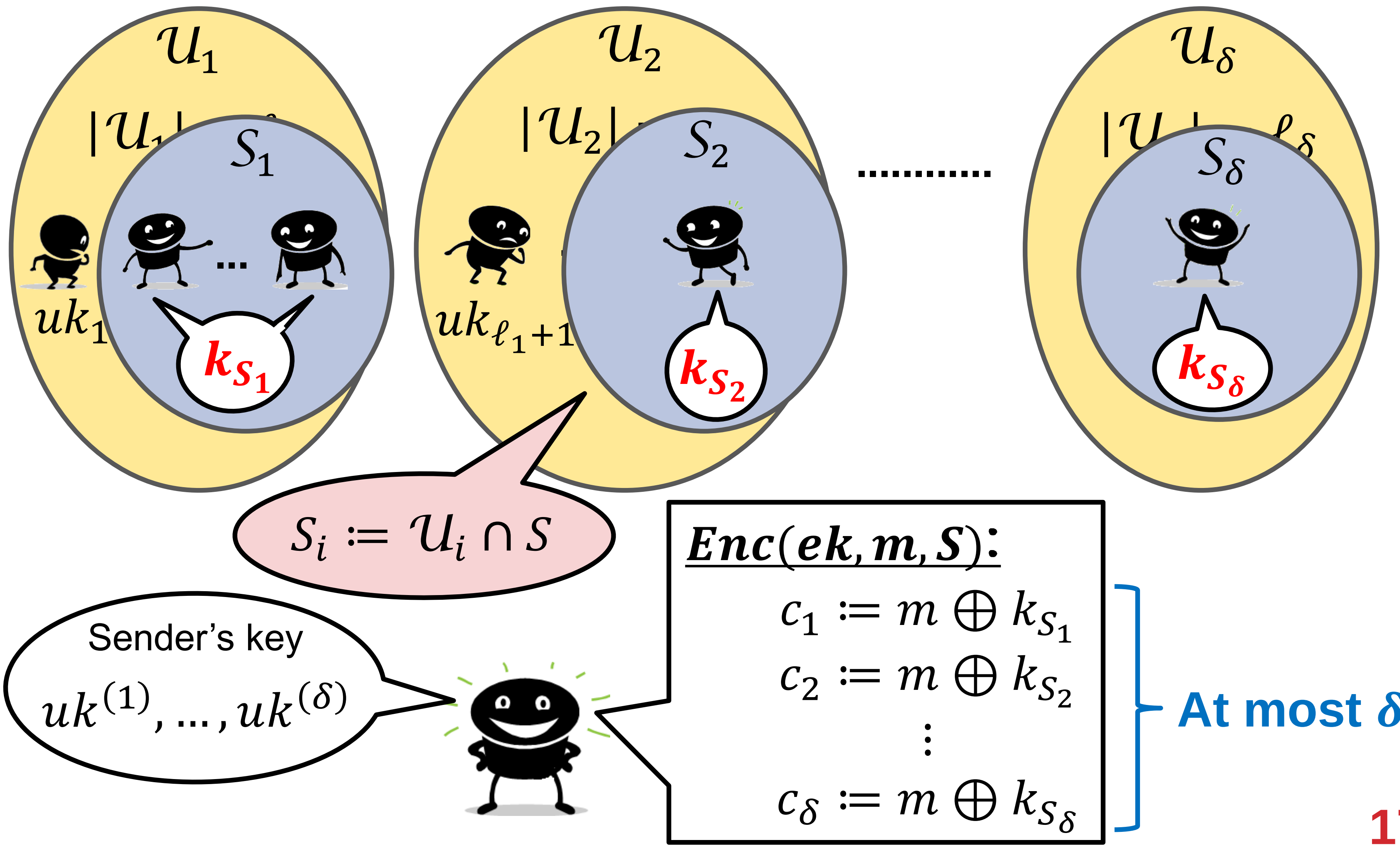
$\mathcal{U}_1$	$\mathcal{U}_2$	....	$\mathcal{U}_\delta$
$\lvert\mathcal{U}_1\rvert = \ell_1$	$\lvert\mathcal{U}_2\rvert = \ell_2$	....	$\lvert\mathcal{U}_\delta\rvert = \ell_\delta$
$(\leq \ell_1, \leq \omega_1)$**-KPS** $\boldsymbol{\Phi_1}$	$(\leq \ell_2, \leq \omega_2)$**-KPS** $\boldsymbol{\Phi_2}$	....	$(\leq \ell_\delta, \leq \omega_\delta)$**-KPS** $\boldsymbol{\Phi_\delta}$
$\omega_1 := \min\{\omega, \ell_1 - 1\}$	$\omega_2 := \min\{\omega, \ell_2 - 1\}$		$\omega_\delta := \min\{\omega, \ell_\delta - 1\}$

Simple Construction from KPSs



Simple Construction from KPSs

$(\leq \ell_1, \leq \omega_1)$**-KPS** $\boldsymbol{\Phi_1}$ $(\leq \ell_2, \leq \omega_2)$**-KPS** $\boldsymbol{\Phi_2}$ **..............** $(\leq \ell_\delta, \leq \omega_\delta)$**-KPS** $\boldsymbol{\Phi_\delta}$



Optimal Parameters for Minimal Keys

$\mathcal{U}_1$	$\mathcal{U}_2$		$\mathcal{U}_\delta$
$\lvert\mathcal{U}_1\rvert = \ell_1$	$\lvert\mathcal{U}_2\rvert = \ell_2$	....	$\lvert\mathcal{U}_\delta\rvert = \ell_\delta$
$(\leq \ell_1, \leq \omega_1)$-**KPS** $\boldsymbol{\Phi_1}$	$(\leq \ell_2, \leq \omega_2)$-**KPS** $\boldsymbol{\Phi_2}$	....	$(\leq \ell_\delta, \leq \omega_\delta)$-**KPS** $\boldsymbol{\Phi_\delta}$
$\omega_1 \coloneqq \min\{\omega, \ell_1 - 1\}$	$\omega_2 \coloneqq \min\{\omega, \ell_2 - 1\}$		$\omega_\delta \coloneqq \min\{\omega, \ell_\delta - 1\}$

There are many combination of $\ell_1, \ell_2, \dots, \ell_\delta$ **s.t.** $\boldsymbol{n} = \sum_{i=1}^{\delta} \ell_i$.

⇨ **Which combination is the best one?**

(which one minimizes the secret-key size?)

We define the following set:

$$\mathcal{L}(n,\delta) \coloneqq \{L \coloneqq (\ell_1, \ell_2, \dots, \ell_\delta) \in N^\delta \mid (\ell_1 \geq \cdots \geq \ell_\delta) \wedge \textstyle\sum_{i=1}^{\delta} \ell_i = n\}.$$

We clarify optimal conditions of $L \in \mathcal{L}(n,\delta)$ **for minimizing secret-key sizes**

Optimal Parameters for Minimal Keys

Theorem. Suppose that the most efficient construction[FN93] is applied to the underlying $(\leq \ell_i, \leq \omega_i)$-KPS Φ_i in $(\leq n, \leq \omega; \delta)$-one-time secure BES Π. Then, the secret-key sizes are given by

$$(\boldsymbol{i})\ \log|\mathcal{EK}| \coloneqq \sum_{\boldsymbol{i=1}}^{\boldsymbol{\delta}} \log\left|\mathcal{UK}^{(i)}\right| = \sum_{\boldsymbol{i=1}}^{\boldsymbol{\delta}} \sum_{\boldsymbol{j=0}}^{\boldsymbol{\omega_i}} \binom{\boldsymbol{\ell_i}}{\boldsymbol{j}} \log|\mathcal{M}|,$$

$$(\boldsymbol{ii})\ \sum_{\boldsymbol{i=1}}^{\boldsymbol{n}} \log|\mathcal{DK}_i| \coloneqq \sum_{\boldsymbol{i=1}}^{\boldsymbol{n}} \log|\mathcal{UK}_i| = \sum_{\boldsymbol{i=1}}^{\boldsymbol{\delta}} \left(\boldsymbol{\ell_i} \sum_{\boldsymbol{j=0}}^{\boldsymbol{\omega_i}} \binom{\boldsymbol{\ell_i - 1}}{\boldsymbol{j}} \right) \log|\mathcal{M}|.$$

$\boldsymbol{L} \in \mathcal{L}(n, \delta)$ **minimizes the encryption-key size** if it satisfies the following:

$$\begin{cases} \forall \boldsymbol{L} & \text{if } \boldsymbol{\omega = 0}, \\ \boldsymbol{L = (n - (\delta - 1), 1, \dots, 1)} & \text{if } \boldsymbol{\omega = 1}, \\ \boldsymbol{\ell_1 - \ell_\delta = 0} & \text{if } \boldsymbol{\omega \geq 2 \wedge n/\delta \in \mathrm{N}}, \\ \boldsymbol{\ell_1 - \ell_\delta = 1} & \text{otherwise.} \end{cases}$$

$\boldsymbol{L} \in \mathcal{L}(n, \delta)$ **minimizes the decryption-key size** if it satisfies the following:

$$\begin{cases} \forall \boldsymbol{L} & \text{if } \boldsymbol{\omega = 0}, \\ \boldsymbol{\ell_1 - \ell_\delta = 0} & \text{if } \boldsymbol{\omega \geq 1 \wedge n/\delta \in \mathrm{N}}, \\ \boldsymbol{\ell_1 - \ell_\delta = 1} & \text{otherwise.} \end{cases}$$

Proof of Theorem: Basic Idea

$$\sum_{i=1}^{\delta}\sum_{j=0}^{\omega_i}\binom{\ell_i}{j} = \sum_{j=1}^{\omega_1}\binom{\ell_1}{j} + \sum_{j=1}^{\omega_2}\binom{\ell_2}{j} + \sum_{j=1}^{\omega_3}\binom{\ell_3}{j} + \cdots + \sum_{j=1}^{\omega_\delta}\binom{\ell_\delta}{j}$$

$$\delta\left\{\begin{array}{lllllll}
 & \delta \text{ terms} & & k_1 \text{ terms} & & k_{\omega-1} \text{ terms} & k_\omega \text{ terms} \\
= & \binom{\ell_1}{0} & + & \binom{\ell_1}{1} & + \cdots + & \binom{\ell_1}{\omega-1} & + \binom{\ell_1}{\omega\,(=\omega_1)} \\
+ & \binom{\ell_2}{0} & + & \binom{\ell_2}{1} & + \cdots + & \binom{\ell_2}{\omega-1} & + \binom{\ell_2}{\omega(=\omega_2)} \\
+ & \binom{\ell_3}{0} & + & \binom{\ell_3}{1} & + \cdots + & \binom{\ell_3}{\omega-1(=\omega_3)} & \\
+ & \cdots\cdots\cdots\cdots & & & & & \\
+ & \binom{\ell_\delta}{0} & + & \binom{\ell_\delta}{1(=\omega_\delta)} & & &
\end{array}\right.$$

$$= \sum_{j=1}^{\delta}\binom{\ell_j}{0} + \sum_{j=1}^{k_1}\binom{\ell_j}{1} + \cdots + \sum_{j=1}^{k_{\omega-1}}\binom{\ell_j}{\omega-1} + \sum_{j=1}^{k_\omega}\binom{\ell_j}{\omega}$$

Proof of Theorem: Main Lemmas

$$\sum_{\boldsymbol{i=1}}^{\boldsymbol{\delta}}\sum_{\boldsymbol{j=0}}^{\boldsymbol{\omega_i}}\binom{\boldsymbol{\ell_i}}{\boldsymbol{j}}=\sum_{j=1}^{\delta}\binom{\ell_j}{0}+\sum_{j=1}^{k_1}\binom{\ell_j}{1}+\cdots+\sum_{j=1}^{k_{\omega-1}}\binom{\ell_j}{\omega-1}+\sum_{j=1}^{k_\omega}\binom{\ell_j}{\omega}$$

We show which $\boldsymbol{L} \in \boldsymbol{\mathcal{L}}(\boldsymbol{n},\boldsymbol{\delta})$ minimizes $\sum_{j=1}^{k_i}\binom{\ell_j}{i}$ $(1 \le i \le \omega)$**:**

Lemma 1 for the case $\boldsymbol{k_i = \delta}$ and **Lemma 2 for the case $\boldsymbol{k_i < \delta}$.**

Lemma 1. For any $a, j \in \mathbf{N}$ and any $r \in [a]$, choose any $b_i \in \mathbf{Z}$ $(1 \le i \le j)$ s.t. $b_1 \ge \cdots \ge b_j \ge r-a$ and $\sum_{i=1}^{j} b_i = 0$. Then, it holds

$$\boldsymbol{j\binom{a}{r} \le \binom{a+b_1}{r}+\binom{a+b_2}{r}+\cdots+\binom{a+b_j}{r}}.$$

The equality holds if and only if $r = 1$.

Lemma 2. For any $a, j \in \mathbf{N}$ and any $r \in \{2, \ldots, a\}$, choose any $b_i \in \mathbf{Z}$ $(1 \le i \le j)$ s.t. $b_1 \ge \cdots \ge b_k \ge r-a > b_{k+1} \ge \cdots \ge b_j > -a$ and $\sum_{i=1}^{j} b_i = 0$. Then, it holds

$$\boldsymbol{j\binom{a}{r} < \binom{a+b_1}{r}+\binom{a+b_2}{r}+\cdots+\binom{a+b_k}{r}}.$$

Concluding Remarks

- **We proposed generic constructions of $(\leq n, \leq \omega; \delta)$-one-time secure BESs for arbitrary $\delta \in \{1, \dots, n\}$.**
  - From δ $(\leq \ell_i, \leq \omega_i)$-KPSs.
  - Natural extension of existing schemes.
- **We showed which $L \in \mathcal{L}(n, \delta)$ for KPSs is the best one.**
  - Secret-key size is minimized when δ subsets are as equal in size as possible (e.g. $\ell_1 = \cdots = \ell_\delta$ if $\mathrm{n}/\delta \in \mathbf{N}$).
- **Tight bounds on the secret-key sizes required for $(\leq n, \leq \omega; \delta)$-one-time secure BESs for any $\delta \in [n]$ are not known.**
  - Existing lower bounds: only for the case $\delta = 1$.
  - Existing upper bounds: only for the case $\delta = 1$ and $\delta = n$.
  - **Our results also showed upper bounds for any $\delta \in [n]$.**

⇒ **Next challenge task: deriving lower bounds for any $\delta \in [n]$.**