

(19) 日本国特許庁(JP)

(12) 特許公報(B2)

(11) 特許番号

特許第3657439号
(P3657439)

(45) 発行日 平成17年6月8日(2005.6.8)

(24) 登録日 平成17年3月18日(2005.3.18)

(51) Int. Cl.⁷

H04L 9/08
G09C 1/00

F I

H04L 9/00 601D
G09C 1/00 630D
G09C 1/00 630E
H04L 9/00 601E

請求項の数 19 (全 60 頁)

<p>(21) 出願番号 特願平10-263498 (22) 出願日 平成10年9月17日(1998.9.17) (65) 公開番号 特開平11-168459 (43) 公開日 平成11年6月22日(1999.6.22) 審査請求日 平成13年8月21日(2001.8.21) (31) 優先権主張番号 特願平9-271589 (32) 優先日 平成9年10月3日(1997.10.3) (33) 優先権主張国 日本国(JP)</p>	<p>(73) 特許権者 000005108 株式会社日立製作所 東京都千代田区丸の内一丁目6番6号 (74) 代理人 100084032 弁理士 三品 岩男 (72) 発明者 山▲崎▼ 正憲 神奈川県川崎市麻生区王禅寺1099番地 株式会社日立製作所 システム開発研究 所内 (72) 発明者 西岡 玄次 神奈川県川崎市麻生区王禅寺1099番地 株式会社日立製作所 システム開発研究 所内</p>
---	---

最終頁に続く

(54) 【発明の名称】 同報暗号通信における暗復号化鍵の配送方法

(57) 【特許請求の範囲】

【請求項1】

通信回線を介して接続された複数の送信者側装置、複数の受信者側装置および鍵管理者側装置を有する通信システムにおいて、前記送信者側装置が行う同報暗号通信の暗復号化鍵を、前記送信者側装置および前記受信者側装置間で共有するための鍵配送方法であって、

前記鍵管理者側装置が、自装置の演算装置により、有限集合 S の部分集合 S' に対応させて受信者側装置 x の受信者秘密情報 s_x を生成し、前記通信回線を介して自装置の通信装置から当該受信者側装置 x に送信すると共に、当該自装置の演算装置により送信者側装置 A の送信者識別情報 t_A を生成し、前記受信者秘密情報 s_x および前記送信者識別情報 t_A を自装置の記憶装置に記憶する第1ステップと、

前記送信者側装置 A が、自装置の演算装置により自身の送信者秘密情報 G_A を生成し、当該送信者秘密情報 G_A より暗復号化鍵 K_A を計算し、前記送信者秘密情報 G_A および前記暗復号化鍵 K_A を自身の記憶装置に記憶する第2ステップと、

前記鍵管理者側装置が、前記通信回線を介して自装置の通信装置から前記送信者側装置 A に、自装置の記憶装置に記憶されている前記送信者識別情報 t_A を送信し、自装置の記憶装置に記憶されている前記受信者秘密情報 s_x を出力し、且つ、前記送信者側装置 A が、自装置の演算装置により、自装置の記憶装置に記憶されている前記送信者秘密情報 G_A と前記鍵管理者側装置から受信した前記送信者識別情報 t_A とを少なくとも作用させて、鍵配送情報 W を生成すると共に、前記鍵管理者側装置より出力された前記受信者秘密情報

10

20

報 s_x と自装置の記憶装置に記憶されている前記送信者識別情報 t_A とを少なくとも作用させて、前記送信者側装置 A に対する前記受信者側装置 x の受信者識別情報 r_x を生成し、前記鍵配送情報 W および前記受信者識別情報 r_x を自装置の記憶装置に記憶する第 3 ステップと、

前記送信者側装置 A が、自装置の通信装置により、自装置の記憶装置に記憶されている前記受信者識別情報 r_x を前記通信回線を介して前記受信者側装置 x に送信すると共に、自装置の記憶装置に記憶されている前記鍵配送情報 W を前記通信回線を介して前記複数の受信者側装置各々に同報送信する第 4 ステップと、

前記受信者側装置 x が、自装置の演算装置により、前記鍵管理者側装置より出力された前記受信者秘密情報 s_x と、前記送信者側装置 A から受信した前記鍵配送情報 W および前記受信者識別情報 r_x とから、前記送信者側装置 A が行う同報暗号通信の暗復号化鍵 K_A を算出し、自装置の記憶装置に記憶する第 5 ステップと、を有し、

前記受信者秘密情報 s_x 、前記鍵配送情報 W および前記受信者識別情報 r_x は、前記受信者秘密情報 s_x 、前記鍵配送情報 W および前記受信者識別情報 r_x と前記複数の受信者側装置各々が保持する他の情報とより、前記暗復号化鍵 K_A が導出可能な関係をもって作成されること

を特徴とする鍵配送方法。

【請求項 2】

請求項 1 記載の鍵配送方法であって、

前記第 2 ステップにおいて、前記送信者側装置 A は、自装置の演算装置により、暗復号化鍵を変更するための変数情報 r_A 、 r_A' を作成し、当該変数情報 r_A 、 r_A' を前記送信者秘密情報 G_A に作用させて前記暗復号化鍵 K_A を計算すると共に、前記送信者秘密情報 G_A を出力し、

前記第 3 ステップにおいて、前記鍵管理者側装置は、自装置の演算装置により、前記送信者識別情報 t_A と前記送信者側装置 A より出力された前記送信者秘密情報 G_A とを作用させたデータ W' を生成すると共に、前記受信者秘密情報 s_x と送信者識別情報 t_A とを作用させたデータ r_x' を生成し、自装置の通信装置により、前記通信回線を介して前記送信者側装置 A に前記データ W' および前記データ r_x' を送信し、且つ、前記送信者側装置 A は、自装置の演算装置により、前記鍵管理者側装置から受信した前記データ W' に前記変数情報 r_A を作用させて前記鍵配送情報 W を生成し、前記鍵管理者側装置から受信した前記データ r_x' に前記変数情報 r_A' を作用させて前記送信者側装置 A に対する前記受信者側装置 x の受信者識別情報 r_x を生成すること

を特徴とする鍵配送方法。

【請求項 3】

通信回線を介して接続された複数の送信者側装置、複数の受信者側装置および鍵管理者側装置を有する通信システムにおいて、前記送信者側装置が行う同報暗号通信の暗復号化鍵を、前記送信者側装置および前記受信者側装置間で共有するための鍵配送方法であって、

前記鍵管理者側装置が、自装置の演算装置により、
鍵管理者秘密情報として、

【数 1】

数1

$$e_i \in Z, \quad (1 \leq i \leq m)$$

を生成し、送信者側装置 A の送信者識別情報として、

10

20

30

40

【数2】

数2

$$t_A \in \mathbb{Z}$$

を生成し、受信者側装置 x の受信者秘密情報として、

$S_{k,m}$ と、

【数3】

数3

$$s_x(\sigma_x) \in \mathbb{Z}$$

10

(但し、集合

【数4】

数4

$$S_{km} = \{\sigma \mid 1 \text{ 対 } 1 \text{ 写像 } \sigma : A = \{1, 2, \dots, k\} \rightarrow B = \{1, 2, \dots, m\}, 0 < k < m\}$$

に対して、 $S_{k,m}$ のとき

20

【数5】

数5

$$\sigma \sim \sigma' \iff \sigma(A) = \sigma'(A)$$

とし、このとき、 \sim は $S_{k,m}$ 上の同値関係となり、

【数6】

数6

$$\tilde{S}_{km} = S_{km} / \sim$$

30

とする) とを生成し、前記鍵管理者秘密情報 e_i 、前記送信者識別情報 t_A および前記受信者秘密情報 $s_x(\sigma_x)$ を自装置の記憶装置に記憶すると共に、前記受信者秘密情報 $s_x(\sigma_x)$ を出力するステップと、

前記送信者側装置 A が、自装置の演算装置により、

【数7】

数7

- $g_A \in G_A$
- $L_A = \text{ord}_{G_A}(g_A)$

40

(但し、

【数8】

数8

$$\text{ord}_{G_A}(g)$$

は、

【数9】

数9

$$g^a = 1 (\in G_A)$$

10

なる最小の正整数 a を表す) なる送信者秘密情報 g_A 、 L_A および有限アーベル群 G_A を生成し、前記送信者秘密情報 g_A 、 L_A および有限アーベル群 G_A を自装置の記憶装置に記憶すると共に、前記送信者秘密情報 g_A を出力するステップと、

前記鍵管理者側装置が、自装置の演算装置により、

自装置の記憶装置に記憶されている前記鍵管理者秘密情報 e_i 、前記送信者識別情報 t_A および前記受信者秘密情報 $s_x(x)$ 、 x から、受信者識別データ

【数10】

数10

$$s_x(\sigma_x, A) = t_A s_x(\sigma_x) \sum_{i=1}^k e_{\sigma_x(i)}$$

30

を計算し、自装置の記憶装置に記憶すると共に、自装置の通信装置により、前記通信回線を介して前記送信者側装置 A に、前記受信者識別データ $s_x(x, A)$ を送信し、且つ、当該演算装置により、前記送信者側装置 A より出力された前記送信者秘密情報 g_A と、前記鍵管理者秘密情報 e_i と、前記送信者識別情報 t_A とから、鍵配送データ

【数11】

数11

$$y_{Ai} = g_A^{t_A e_i} (\in G_A) \quad (1 \leq i \leq m)$$

40

を算出し、自装置の記憶装置に記憶すると共に、当該通信装置により、前記通信回線を介して前記送信者側装置 A に、前記鍵配送データ y_{Ai} を送信するステップと、

前記送信者側装置 A が、自装置の演算装置により、

整数 r 、 r' を生成し、前記鍵管理者側装置から受信した受信者識別データ $s_x(x, A)$ と、前記送信者秘密情報 L_A と、前記整数 r' とから

【数12】

数12

$$r_x(\sigma_x, A)s_x(\sigma_x, A) \equiv r' \pmod{L_A}$$

なる受信者識別情報 $r_x(\sigma_x, A)$ を計算し、自装置の記憶装置に記憶すると共に、自装置の通信装置により、前記通信回線を介して前記受信者側装置 x に、前記受信者識別情報 $r_x(\sigma_x, A)$ を送信し、且つ、当該演算装置により、前記鍵管理者側装置から受信した前記鍵配送データ y_{A_i} と、前記整数 r とから、鍵配送情報

【数13】

数13

$$z_{A_i} = y_{A_i}^r \pmod{G_A} \quad (1 \leq i \leq m)$$

を計算し、自装置の記憶装置に格納すると共に、当該通信装置により、前記通信回線を介して前記複数の受信者側装置各々に前記鍵配送情報 z_{A_i} を同報送信するステップと、前記受信者側装置 x が、自装置の演算装置により、前記送信者側装置 A から受信した前記受信者識別情報 $r_x(\sigma_x, A)$ および前記鍵配送情報 z_{A_i} と、前記鍵管理者側装置より出力された前記受信者秘密情報 $s_x(\sigma_x)$ とから、

【数14】

数14

$$K_A = \left(\prod_{i=1}^k z_{A_{\sigma_x(i)}} \right)^{r_x(\sigma_x, A)s_x(\sigma_x)} \pmod{G_A} \quad 30$$

により、前記送信者側装置 A が

【数15】

数15

$$K_A = g_A^{rr'} \pmod{G_A}$$

によって生成して同報通信に用いる暗復号化鍵 K_A を計算し、自装置の記憶装置に記憶するステップと、を有することを特徴とする鍵配送方法。

【請求項4】

通信回線を介して接続された複数の送信者側装置、複数の受信者側装置および鍵管理者側装置を有する通信システムにおいて、前記送信者側装置が行う同報暗号通信の暗復号化鍵を、前記送信者側装置および前記受信者側装置間で共有するための鍵配送方法であって、

前記鍵管理者側装置が、自装置の演算装置により、鍵管理者秘密情報として、

【数16】

数16

$$e_i \in \mathbb{Z} \quad (1 \leq i \leq m)$$

を生成し、送信者側装置Aの送信者識別情報として、

【数17】

数17

$$t_A \in \mathbb{Z}$$

10

を生成し、受信者側装置xの受信者秘密情報として、

 S_{km} と、

【数18】

数18

$$s_x(\sigma_x) \in \mathbb{Z}$$

(但し、集合

20

【数19】

数19

$$S_{km} = \{\sigma \mid 1 \text{ 対 } 1 \text{ 写像 } \sigma : A = \{1, 2, \dots, k\} \rightarrow B = \{1, 2, \dots, m\}, 0 < k < m\}$$

に対して、 S_{km} のとき

【数20】

数20

30

$$\sigma \sim \sigma' \iff \sigma(A) = \sigma'(A)$$

とし、このとき、 \sim は S_{km} 上の同値関係となり、

【数21】

数21

$$\tilde{S}_{km} = S_{km} / \sim$$

40

とする)とを生成して、前記鍵管理者秘密情報 e_i 、前記送信者識別情報 t_A および前記受信者秘密情報 $s_x(\sigma_x)$ を自装置の記憶装置に記憶すると共に、前記受信者秘密情報 $s_x(\sigma_x)$ を出力するステップと、
前記送信者側装置Aが、自装置の演算装置により、
前記送信者側装置Aの送信者秘密情報として、

【数22】

数22

 P_A, Q_A : 素数

$$L_A = \text{lcm}(\text{ord}_{P_A}(g_A), \text{ord}_{Q_A}(g_A))$$

$$g_A \in \mathbb{Z}, 0 < g_A < N_A$$

10

を生成し、前記送信者側装置 A の送信者公開情報として、

【数23】

数23

$$N_A (= P_A Q_A)$$

を生成し、前記送信者秘密情報 P_A 、 Q_A 、 L_A 、 g_A および前記送信者公開情報 N_A を
自装置の記憶装置に記憶すると共に、前記送信者秘密情報 g_A を出力するステップと、

20

前記鍵管理者側装置が、自装置の演算装置により、

自装置の記憶装置に記憶されている前記鍵管理者秘密情報 e_i 、前記送信者識別情報 t_A
および前記受信者秘密情報 $s_x(x)$ 、 x から、受信者識別データ

【数24】

数24

$$s_x(\sigma_x, A) = t_A s_x(\sigma_x) \sum_{i=1}^k e_{\sigma_x(i)}$$

30

を計算し、自装置の記憶装置に記憶すると共に、自装置の通信装置により、前記通信回線
を介して前記送信者側装置 A に、前記受信者識別データ $s_x(x, A)$ を送信し、且つ

、当該演算装置により、前記送信者側装置 A より出力された前記送信者秘密情報 g_A と、
自装置の記憶装置に記憶されている前記鍵管理者秘密情報 e_i および前記送信者識別情報

t_A とから、鍵配送データ

【数25】

数25

$$y_{Ai} = g_A^{t_A e_i} \text{ mod } N_A \quad (1 \leq i \leq m)$$

40

を算出し、自装置の記憶装置に記憶すると共に、当該通信装置により、前記通信回線を介
して前記送信者側装置 A に、前記鍵配送データ y_{Ai} を送信するステップと、

前記送信者側装置 A が、自装置の演算装置により、

整数 r 、 r' を生成し、前記鍵管理者側装置から受信した前記受信者識別データ $s_x(x, A)$ と、
自装置の記憶装置に記憶されている前記送信者秘密情報 L_A と、前記整数 r' とから

50

【数26】

数26

$$r_x(\sigma_x, A)s_x(\sigma_x, A) \equiv r' \pmod{L_A}$$

なる受信者識別情報 $r_x(\sigma_x, A)$ を計算し、自装置の記憶装置に記憶すると共に、自装置の通信装置により、前記通信回線を介して前記受信者側装置 x に、前記受信者識別情報 $r_x(\sigma_x, A)$ を送信し、且つ、当該演算装置により、前記鍵管理者側装置から受信した前記鍵配送データ y_{A_i} と前記整数 r とから、鍵配送情報

【数27】

数27

$$z_{A_i} = y_{A_i}^r \pmod{N_A} \quad (1 \leq i \leq m)$$

を計算し、自装置の記憶装置に記憶すると共に、当該通信装置により、前記鍵配送情報 z_{A_i} を、前記通信回線を介して前記複数の受信者側装置各々に同報送信するステップと、前記受信者側装置 x が、自装置の演算装置により、前記送信者側装置 A から受信した前記受信者識別情報 $r_x(\sigma_x, A)$ および前記鍵配送情報 z_{A_i} と、前記鍵管理者側装置より出力された前記受信者秘密情報 $s_x(\sigma_x)$ とから

【数28】

数28

$$K_A = \left(\prod_{i=1}^k z_{A_{\sigma_x(i)}} \right)^{r_x(\sigma_x, A)s_x(\sigma_x)} \pmod{N_A}$$

により、前記送信者側装置 A が

【数29】

数29

$$K_A = g_A^{rr'} \pmod{N_A}$$

によって生成し同報通信に用いる暗復号化鍵 K_A を計算し、自装置の記憶装置に記憶するステップと、を有すること

を特徴とする鍵配送方法。

【請求項5】

請求項3または4記載の鍵配送方法であって、

前記送信者側装置 A が、

前記鍵管理者側装置が、自装置の演算装置により、前記鍵管理者秘密情報 e_i 、前記送信者識別情報 t_A 、前記受信者秘密情報 $s_x(\sigma_x)$ を生成するのに先だって、前記秘密情報 L_A を生成して出力し、

10

20

30

40

50

前記鍵管理者側装置が、自装置の演算装置により、
前記送信者側装置 A より出力された前記送信者秘密情報 L_A から

【数 3 0】

数30

$$e_i \in \mathbb{Z}, \quad 0 < e_i < L_A, \quad (1 \leq i \leq m)$$

$$t_A \in \mathbb{Z}, \quad 0 < t_A < L_A$$

$$s_x(\sigma_x) \in \mathbb{Z}, \quad 0 < s_x(\sigma_x) < L_A$$

10

となる前記鍵管理者秘密情報 e_i 、前記送信者識別情報 t_A 、前記受信者秘密情報 s_x (x) を生成し、前記送信者秘密情報 L_A 、前記鍵管理者秘密情報 e_i 、前記送信者識別情報 t_A 、前記受信者秘密情報 s_x (x) から

【数 3 1】

数31

$$s_x(\sigma_x, A) = t_A s_x(\sigma_x) \sum_{i=1}^k e_{\sigma_x(i)} \pmod{L_A}$$

20

となる前記受信者識別データ s_x (x, A) を計算すること
を特徴とする鍵配送方法。

【請求項 6】

請求項 3 または 4 記載の鍵配送方法であって、さらに、
前記送信者側装置 A が、自装置の演算装置により、
前記整数 r の値を変更し、変更後の前記整数 r に従って、前記暗復号化鍵 K_A の値を再計算すると共に、変更後の前記整数 r に従って、前記鍵配送情報 z_{A_i} を再計算して、自装置の通信装置により、前記通信回線を介して前記複数の受信者側装置各々に再同報送信するステップと、

30

前記受信者側装置 x が、自装置の演算装置により、
再同報送信された前記鍵配送情報 z_{A_i} に従って、前記暗復号化鍵 K_A を再計算するステップと、を有すること
を特徴とする鍵配送方法。

【請求項 7】

請求項 3 または 4 記載の鍵配送方法であって、
前記送信者側装置 A が、自装置の演算装置により、
前記整数 r' の値を、暗号化して同報通信する情報もしくは情報の種類の各々に対応して複数生成し、前記情報もしくは情報の種類毎に、当該情報もしくは情報の種類に対応して生成した前記整数 r' に従って、前記暗復号化鍵 K_A を計算すると共に、前記受信者側装置 x に復号化を許可する前記情報もしくは情報の種類に対応して生成した前記整数 r' に従って前記受信者識別情報 r_x (x, A) を計算して、自装置の通信装置により、前記通信回線を介して前記受信者側装置 x に送信し、

40

前記受信者側装置 x が、自装置の演算装置により、
受信した前記受信者識別情報 r_x (x, A) に従って、当該受信者側装置 x に復号化

50

が許可された前記情報もしくは情報の種類に対応する前記暗復号化鍵 K_A を計算することを特徴とする鍵配送方法。

【請求項 8】

請求項 3 または 4 記載の鍵配送方法であって、
前記送信者側装置 A が、自装置の演算装置により、
前記受信者側装置 x であることを主張する受信者側装置に前記受信者識別情報 $r_x (x, A)$ を送信するのに先だって、当該受信者側装置が、前記受信者秘密情報 $s_x (x)$ を所持していることを、当該受信者側装置が前記受信者側装置 x である場合にも前記受信者秘密情報 $s_x (x)$ が前記送信者側装置 A に秘密化される方式によって認証するステップを備えたこと
 を特徴とする鍵配送方法。

10

【請求項 9】

請求項 3、4 または 8 記載の鍵配送方法であって、
前記送信者側装置 A が、自装置の演算装置により、
前記受信者側装置 x に前記受信者識別情報 $r_x (x, A)$ を送信する際に、当該受信者識別情報 $r_x (x, A)$ に対応する前記暗復号化鍵 K_A によって暗号化されて同報通信される情報もしくは情報の種類に対する料金を、前記受信者側装置 x に対する課金情報として算出するステップを有すること
 を特徴とする鍵配送方法。

20

【請求項 10】

通信回線を介して接続された複数の送信者側装置、複数の受信者側装置および鍵管理者側装置を有する通信システムであって、
前記鍵管理者側装置は、演算装置と、記憶装置と、通信装置と、入出力装置とを有し、
前記鍵管理者側装置の演算装置は、
鍵管理者秘密情報として、

【数 3 2】

数32

$$e_i \in \mathbb{Z}, \quad (1 \leq i \leq m)$$

30

を生成し、自装置の記憶装置に記憶する処理と、
送信者側装置 A の送信者識別情報として、

【数 3 3】

数33

$$\bullet t_A \in \mathbb{Z}$$

40

を生成、自装置の記憶装置に記憶する処理と、
受信者側装置 x の受信者秘密情報として、
 $x \quad S_{k_m}$ 、および、

【数34】

数34

$$\bullet s_x(\sigma_x) \in Z$$

(但し、集合

【数35】

10

数35

$$S_{km} = \{\sigma \mid 1 \text{ 対 } 1 \text{ 写像 } \sigma : A = \{1, 2, \dots, k\} \rightarrow B = \{1, 2, \dots, m\}, 0 < k < m\}$$

に対して、 \sim は S_{km} のとき、

【数36】

数36

20

$$\sigma \sim \sigma' \stackrel{\text{def}}{\iff} \sigma(A) = \sigma'(A)$$

とし、このとき、 \sim は S_{km} 上の同値関係となり、

【数37】

数37

$$\tilde{S}_{km} = S_{km} / \sim$$

30

とする)を生成、自装置の記憶装置に記憶する処理と、

自装置の記憶装置に記憶されている前記鍵管理者秘密情報 e_i 、前記送信者識別情報 t_A および前記受信者秘密情報 s_x (x)、 x から、受信者識別データ

【数38】

数38

40

$$s_x(\sigma_x, A) = t_A s_x(\sigma_x) \sum_{i=1}^k e_{\sigma_x(i)}$$

を計算し、自装置の記憶装置に記憶する処理と、

前記送信者側装置 A より出力された送信者秘密情報 g_A と、自装置の記憶装置に記憶さ

50

れている前記鍵管理者秘密情報 e_i および前記送信者識別情報 t_A とから、鍵配送データ
【数39】

数39

$$y_{Ai} = g_A^{t_A e_i} \quad (\in G_A) \quad (1 \leq i \leq m)$$

を算出し、自装置の記憶装置に記憶する処理と、を行い、
前記鍵管理者側装置の入出力装置は、
前記送信者側装置 A より出力された前記送信者秘密情報 g_A を入力する処理と、
前記鍵管理者側装置の演算装置が生成した前記受信者秘密情報 s_x 、 $s_x(\sigma_x)$ を出力する処理と、を行い、
前記鍵管理者側装置の通信装置は、
前記鍵管理者側装置の演算装置が生成した前記受信者識別データ $s_x(\sigma_x, A)$ および前記鍵配送データ y_{A_i} を、前記通信回線を介して前記送信者側装置 A に送信する処理を行い、
前記送信者側装置 A は、演算装置と、記憶装置と、通信装置と、入出力装置とを有し、
前記送信者側装置 A の演算装置は、
【数40】

10

20

数40

- $g_A \in G_A$
- $L_A = \text{ord}_{G_A}(g_A)$

(但し、
【数41】

数41

$$\text{ord}_{G_A}(g)$$

は、
【数42】

30

数42

$$g^a = 1 \quad (\in G_A)$$

なる最小の正整数 a を表す) なる送信者秘密情報 g_A 、 L_A および有限アーベル群 G_A を生成し、自装置の記憶装置に記憶する処理と、
整数 r 、 r' を生成し、自装置の記憶装置に記憶する処理と、
前記鍵管理者側装置から受信した前記受信者識別データ $s_x(\sigma_x, A)$ と、自装置の記憶装置に記憶されている前記送信者秘密情報 L_A および前記整数 r' とから
【数43】

40

数43

$$r_x(\sigma_x, A) s_x(\sigma_x, A) \equiv r' \pmod{L_A}$$

50

なる受信者識別情報 $r_x(x, A)$ を計算し、自装置の記憶装置に記憶する処理と、
前記鍵管理者側装置から受信した前記鍵配送データ y_{A_i} と、自装置の記憶装置に記憶
されている前記整数 r とから、鍵配送情報

【数44】

数44

$$z_{A_i} = y_{A_i}^r \quad (\in G_A) \quad (1 \leq i \leq m)$$

10

を計算し、自装置の記憶装置に記憶する処理と、を行い、
前記送信者側装置 A の入出力装置は、
前記送信者側装置 A の演算装置が生成した前記送信者秘密情報 g_A を出力する処理を行
い、

前記送信者側装置 A の通信装置は、
前記通信回線を介して前記鍵管理者側装置から前記受信者識別データ $s_x(x, A)$
および前記鍵配送データ y_{A_i} を受信する処理と、

前記送信者側装置 A の演算装置が生成した前記受信者識別情報 $r_x(x, A)$ を、前
記通信回線を介して前記受信者装置 x に送信する処理と、

20

前記送信者側装置 A の演算装置が生成した前記鍵配送情報 z_{A_i} を、前記通信回線を介
して前記複数の受信者側装置に同報送信する処理と、を行い、

前記受信者側装置 x は、演算装置と、記憶装置と、通信装置と、入出力装置とを有し、
前記受信者側装置 x の演算装置は、

前記送信者側装置 A から受信した前記受信者識別情報 $r_x(x, A)$ および前記鍵配
送情報 z_{A_i} と、前記鍵管理者側装置から出力された前記受信者秘密情報 g_x 、 $s_x(x)$
とから、

【数45】

数45

$$K_A = \left(\prod_{i=1}^k z_{A_{\sigma_x(i)}} \right)^{r_x(\sigma_x, A) s_x(\sigma_x)} \quad (\in G_A)$$

30

により、前記送信者側装置 A が

【数46】

数46

$$K_A = g_A^{rr'} \quad (\in G_A)$$

40

によって生成し、同報通信に用いる暗復号化鍵 K_A を計算し、自装置の記憶装置に記憶す
る処理を行い、

前記受信者側装置 x の入出力装置は、
前記鍵管理者側装置より出力された前記受信者秘密情報 g_x 、 $s_x(x)$ を入力する
処理を行い、

前記受信者側装置 x の通信装置は、
前記通信回線を介して前記送信者側装置 A から前記受信者識別情報 $r_x(x, A)$ お
よび前記鍵配送情報 z_{A_i} を受信する処理を行うこと

を特徴とする通信システム。

50

【請求項 11】

通信回線を介して接続された複数の送信者側装置、複数の受信者側装置および鍵管理者側装置を有する通信システムに用いられる鍵管理者側装置であって、
演算装置と、記憶装置と、通信装置と、入出力装置とを有し
前記演算装置は、
鍵管理者秘密情報として、

【数 47】

数47

$$e_i \in \mathbb{Z}, \quad (1 \leq i \leq m)$$

10

を生成し、前記記憶装置に記憶する処理と、
送信者側装置 A の送信者識別情報として、

【数 48】

数48

$$t_A \in \mathbb{Z}$$

を生成し、前記記憶装置に記憶する処理と、
受信者側装置 x の受信者秘密情報として、

x $S_{k,m}$ 、および、

【数 49】

数49

$$s_x(\sigma_x) \in \mathbb{Z}$$

20

(但し、集合

【数 50】

数50

30

$$S_{km} = \{\sigma \mid 1 \text{ 対 } 1 \text{ 写像 } \sigma : A = \{1, 2, \dots, k\} \rightarrow B = \{1, 2, \dots, m\}, 0 < k < m\}$$

に対して、 $\sigma, \sigma' \in S_{k,m}$ のとき

【数 51】

数51

$$\sigma \sim \sigma' \stackrel{\text{def}}{\iff} \sigma(A) = \sigma'(A)$$

40

とし、このとき、 \sim は $S_{k,m}$ 上の同値関係となり、

【数 52】

数52

$$\tilde{S}_{km} = S_{km} / \sim$$

とする) を生成し、前記記憶装置に記憶する処理と、

前記記憶装置に記憶されている前記鍵管理者秘密情報 e_i 、前記送信者識別情報 t_A お

50

よび前記受信者秘密情報 s_x (x)、 x から、受信者識別データ
【数 5 3】

数53

$$s_x(\sigma_x, A) = t_A s_x(\sigma_x) \sum_{i=1}^k e_{\sigma_x(i)}$$

を計算し、前記記憶装置に記憶する処理と、

前記送信者側装置 A より出力された送信者秘密情報 g_A と、前記記憶装置に記憶されて
いる前記鍵管理者秘密情報 e_i および前記送信者識別情報 t_A から、鍵配送データ

【数 5 4】

数54

$$y_{Ai} = g_A^{t_A e_i} \in G_A \quad (1 \leq i \leq m)$$

を算出し、前記記憶装置に記憶する処理と、を行い、

前記入出力装置は、

前記送信者側装置 A より出力された前記送信者秘密情報 g_A を入力する処理と、

前記演算装置が生成した前記受信者秘密情報 x 、 s_x (x) を出力する処理と、を
行い、

前記通信装置は、

前記演算装置が生成した前記受信者識別データ s_x (x , A) および前記鍵配送デー
タ y_{Ai} を、前記通信回線を介して前記送信者装置 A に送信する処理を行うこと

を特徴とする鍵管理者側装置。

【請求項 1 2】

通信回線を介して接続された複数の送信者側装置、複数の受信者側装置および鍵管理者
側装置を有する通信システムに用いられる送信者側装置であって、

演算装置と、記憶装置と、通信装置と、入出力装置とを有し、

前記演算装置は、

【数 5 5】

数55

$$g_A \in G_A$$

$$L_A = \text{ord}_{G_A}(g_A)$$

(但し、

【数 5 6】

数56

$$\text{ord}_{G_A}(g)$$

は、

10

20

30

40

【数57】

数57

$$g^a = 1 \ (\in G_A)$$

なる最小の正整数 a を表す) なる送信者秘密情報 g_A 、 L_A および有限アーベル群 G_A を生成し、前記記憶装置に記憶する処理と、

整数 r 、 r' を生成し、前記記憶装置に記憶する処理と、

前記鍵管理者側装置から受信した受信者識別データ $s_x(x, A)$ と、前記記憶装置に記憶されている前記送信者秘密情報 L_A および前記整数 r' とから

10

【数58】

数58

$$r_x(\sigma_x, A) s_x(\sigma_x, A) \equiv r' \pmod{L_A}$$

なる受信者識別情報 $r_x(x, A)$ を計算し、前記記憶装置に記憶する処理と、

前記鍵管理者側装置から受信した鍵配送データ y_{A_i} と、前記記憶装置に記憶されている前記整数 r とから、鍵配送情報

【数59】

20

数59

$$z_{A_i} = y_{A_i}^r \ (\in G_A) \quad (1 \leq i \leq m)$$

を計算し、前記記憶装置に記憶する処理と、

【数60】

数60

$$K_A = g_A^{r r'} \ (\in G_A)$$

30

に従って同報通信に用いる暗復号化鍵 K_A を計算し、前記記憶装置に記憶する処理と、を行い、

前記入出力装置は、

前記演算装置が生成した前記送信者秘密情報 g_A を出力する処理を行い、

前記通信装置は、

前記演算装置が生成した前記受信者識別情報 $r_x(x, A)$ を、前記通信回線を介して前記受信者側装置 x に送信する処理と、

前記演算装置が生成した前記鍵配送情報 z_{A_i} を、前記通信回線を介して前記複数の受信者側装置に同報送信する処理と、を行うこと

40

ことを特徴とする送信者側装置。

【請求項13】

通信回線を介して接続された複数の送信者側装置、複数の受信者側装置および鍵管理者側装置を有する通信システムに用いられる受信者側装置であって、

演算装置と、記憶装置と、通信装置と、入出力装置とを有し

前記演算装置は、

送信者側装置 A から受信した受信者識別情報 $r_x(x, A)$ および鍵配送情報 z_{A_i} と、前記鍵管理者側装置から受信した受信者秘密情報 x 、 $s_x(x)$ とから

【数61】

数61

$$K_A = \left(\prod_{i=1}^k z_{A\sigma_x(i)} \right)^{r_x(\sigma_x, A) s_x(\sigma_x)} \quad (\in G_A)$$

により、前記送信者側装置 A が

【数62】

数62

$$K_A = g_A^{rr'} \quad (\in G_A)$$

によって生成し、同報通信に用いる暗復号化鍵 K_A を計算し、前記記憶装置に記憶する処理を行い、

前記入出力装置は、

前記鍵管理者側装置より出力された前記受信者秘密情報 $s_x(x)$ を受信する処理を行い、

前記通信装置は、

前記通信回線を介して前記送信者側装置 A から前記受信者識別情報 $r_x(x, A)$ および前記鍵配送情報 $z_{A i}$ を受信する処理を行うこと

を特徴とする受信者側装置。

【請求項14】

通信回線を介して接続された複数の送信者側装置、複数の受信者側装置および鍵管理者側装置を有する通信システムに用いられる受信者側装置であって、

本体装置と、補助装置とを有し、

前記補助装置は、補助用演算装置と、補助用接続装置と、補助用記憶装置とを有し、

前記補助用演算装置は、

前記補助用接続装置に接続された前記鍵管理者側装置から受信者秘密情報 $s_x(x)$ を取り込んで前記補助用記憶装置に記憶する処理と、

前記補助用接続装置に接続された前記本体装置から送信者側装置 A の鍵配送情報 $z_{A i}$ を取り込み、前記鍵配送情報 $z_{A i}$ と、前記補助用記憶装置に記憶した前記受信者秘密情報 $s_x(x)$ とから、

【数63】

数63

$$\xi_x(\sigma_x, A) = \left(\prod_{i=1}^k z_{A\sigma_x(i)} \right)^{s_x(\sigma_x)} \quad \text{mod } N_A$$

を計算し、計算結果 $\xi_x(x, A)$ を前記補助用接続装置に接続された前記本体装置に出力する処理と、

前記本体装置は、本体用演算装置と、本体用接続装置と、本体用通信装置とを有し、

前記本体用演算装置は、

前記送信者側装置 A から受信した鍵配送情報 $z_{A i}$ を、前記本体用接続装置に接続された前記補助装置に出力する処理と、

前記送信者側装置 A から受信した受信者識別情報 $r_x(x, A)$ と、前記本体用接続装置に接続された前記補助装置から入力された前記 $\xi_x(x, A)$ とから、

10

20

30

40

50

【数64】

数64

$$K_A = \xi_x(\sigma_x, A)^{r_x(\sigma_x, A)} \bmod N_A$$

に従って、前記送信者側装置 A が

【数65】

数65

$$K_A = g_A^{rr'} (\in G_A)$$

10

によって生成し、同報通信に用いる暗復号化鍵 K_A を計算する処理と、を行い、

前記本体用通信装置は、

前記通信回線を介して前記送信者側装置 A から前記鍵配送情報 z_{A_i} および前記受信者識別情報 $r_x(x, A)$ を受信する処理を行うこと

を特徴とする受信者側装置。

【請求項15】

通信回線を介して接続された複数の送信者側装置、複数の受信者側装置および鍵管理者側装置を有する通信システムにおいて、前記鍵管理者側装置および受信者側装置 x に接続して用いられる補助装置であって、

20

補助用演算装置と、補助用接続装置と、補助用記憶装置とを有し、

前記演算装置は、

前記補助用接続装置に接続された前記鍵管理者側装置から受信者秘密情報 $s_x(x)$ 、 x を取り込んで前記補助用記憶装置に記憶する処理と、

前記補助用接続装置に接続された前記受信者側装置 x から送信者側装置 A の鍵配送情報 z_{A_i} を取り込み、前記鍵配送情報 z_{A_i} と、前記補助用記憶装置に記憶した前記受信者秘密情報 $s_x(x)$ とから、

【数66】

数66

$$\xi_x(\sigma_x, A) = \left(\prod_{i=1}^k z_{A\sigma_x(i)} \right)^{s_x(\sigma_x)} \bmod N_A$$

30

を計算し、計算結果 $\xi_x(x, A)$ を前記補助用接続装置に接続された前記受信者側装置 x に出力する処理と、を行うこと

を特徴とする補助装置。

【請求項16】

通信回線を介して接続された複数の送信者側装置、複数の受信者側装置および鍵管理者側装置を有する通信システムにおいて、前記鍵管理者側装置における処理をコンピュータに実行させるプログラムを記憶した記憶媒体であって、

40

当該プログラムは、コンピュータに、

鍵管理者秘密情報として、

【数67】

数67

$$e_i \in \mathbb{Z}, \quad (1 \leq i \leq m)$$

を、演算装置を用いて生成し、記憶装置に記憶する処理と、

50

送信者側装置 A の送信者識別情報として、
【数 68】

数68

$$t_A \in \mathbb{Z}$$

を、前記演算装置を用いて生成し、前記記憶装置に記憶する処理と、
受信者側装置 x の受信者秘密情報として、
x S_{km}、および、
【数 69】

数69

$$s_x(\sigma_x) \in \mathbb{Z}$$

(但し、集合
【数 70】

数70

$$S_{km} = \{\sigma \mid 1 \text{ 対 } 1 \text{ 写像 } \sigma : A = \{1, 2, \dots, k\} \rightarrow B = \{1, 2, \dots, m\}, 0 < k < m\}$$

に対して、
【数 71】

数71

$$\sigma \sim \sigma' \stackrel{\text{def}}{\iff} \sigma(A) = \sigma'(A)$$

とし、このとき、 \sim は S_{km} 上の同値関係となり、
【数 72】

数72

$$\tilde{S}_{km} = S_{km} / \sim$$

とする)を、前記演算装置を用いて生成し、前記記憶装置に記憶する処理と、
前記受信者秘密情報 s_x 、 $s_x(\sigma_x)$ を出力する処理と、
前記記憶装置に記憶されている前記鍵管理者秘密情報 e_i 、前記送信者識別情報 t_A および前記受信者秘密情報 $s_x(\sigma_x)$ 、 s_x から、受信者識別データ
【数 73】

数73

$$s_x(\sigma_x, A) = t_A s_x(\sigma_x) \sum_{i=1}^k e_{\sigma_x(i)}$$

を、前記演算装置を用いて計算し、前記記憶装置に記憶する処理と、
前記受信者識別データ $s_x(\sigma_x, A)$ を、前記通信回線を介して前記送信者側装置 A
に、前記通信装置を用いて送信する処理と、
前記送信者側装置 A より出力された前記送信者秘密情報 g_A を入力する処理と、

10

20

30

40

50

前記送信側装置 A より出力された前記送信者秘密情報 g_A と、前記記憶装置に記憶されている前記鍵管理者秘密情報 e_i および前記送信者識別情報 t_A とから、鍵配送データ

【数 7 4】

数74

$$y_{Ai} = g_A^{t_A e_i} (\in G_A) \quad (1 \leq i \leq m)$$

を、前記演算装置を用いて算出し、前記記憶装置に記憶する処理と、

前記記憶装置に記憶されている前記鍵配送データ $y_{A i}$ を、前記通信回線を介して前記送信者側装置 A に前記通信装置を用いて送信する処理と、

を実行させることを特徴とするプログラムが記憶された記憶媒体。

【請求項 1 7】

通信回線を介して接続された複数の送信者側装置、複数の受信者側装置および鍵管理者側装置を有する通信システムにおいて、前記送信者側装置における処理をコンピュータに実行させるプログラムを記憶した記憶媒体であって、

当該プログラムは、コンピュータに、

【数 7 5】

数75

$$g_A \in G_A$$

$$L_A = \text{ord}_{G_A}(g_A)$$

(但し、

【数 7 6】

数76

$$\text{ord}_{G_A}(g)$$

は、

【数 7 7】

数77

$$g^a = 1 (\in G_A)$$

なる最小の正整数 a を表す) なる送信者秘密情報 g_A 、 L_A および有限アーベル群 G_A を、演算装置を用いて生成し、記憶装置に記憶する処理と、

前記送信者秘密情報 g_A を出力する処理と、

整数 r 、 r' を前記演算装置を用いて生成し、前記記憶装置に記憶する処理と、

前記通信回線を介して前記鍵管理者側装置から受信者識別データ $s_x (x, A)$ を、前記通信装置を用いて受信する処理と、

前記鍵管理者側装置から受信した前記受信者識別データ $s_x (x, A)$ と、前記記憶装置に記憶されている前記送信者秘密情報 L_A および前記整数 r' とから、

10

20

30

40

【数78】

数78

$$r_x(\sigma_x, A) s_x(\sigma_x, A) \equiv r' \pmod{L_A}$$

なる受信者識別情報 $r_x(\sigma_x, A)$ を、前記演算装置を用いて計算し、前記記憶装置に記憶する処理と、

前記受信者識別情報 $r_x(\sigma_x, A)$ を、前記通信回線を介して前記受信者側装置 x に送信する処理と、

前記通信回線を介して前記鍵管理者側装置から鍵配送データ y_{A_i} を、前記通信装置を用いて受信する処理と、

前記鍵管理者側装置から受信した鍵配送データ y_{A_i} と、前記記憶装置に記憶されている前記整数 r とから、鍵配送情報

【数79】

数79

$$z_{A_i} = y_{A_i}^r \pmod{G_A} \quad (1 \leq i \leq m)$$

を、前記演算装置を用いて計算し、前記記憶装置に記憶する処理と、

前記鍵配送情報 z_{A_i} を、前記通信回線を介して前記複数の受信者側装置に、前記通信装置を用いて同報送信する処理と、

【数80】

数80

$$K_A = g_A^{rr'} \pmod{G_A}$$

に従って同報通信に用いる暗復号化鍵 K_A を、前記演算装置を用いて計算し、前記記憶装置に記憶する処理と、 を実行させること

を特徴とするプログラムが記憶された記憶媒体。

【請求項18】

通信回線を介して接続された複数の送信者側装置、複数の受信者側装置および鍵管理者側装置を有する通信システムにおいて、前記受信者側装置における処理をコンピュータに実行させるプログラムを記憶した記憶媒体であって、

当該プログラムは、コンピュータに、

前記通信回線を介して送信者側装置 A から受信者識別情報 $r_x(\sigma_x, A)$ および鍵配送情報 z_{A_i} を、通信装置を用いて受信する処理と、

前記鍵管理者側装置より出力された前記受信者秘密情報 $s_x(\sigma_x)$ を入力する処理と、

前記送信者側装置 A から受信した受信者識別情報 $r_x(\sigma_x, A)$ および前記鍵配送情報 z_{A_i} と、前記鍵管理者側装置より出力された前記受信者秘密情報 $s_x(\sigma_x)$ とから、

【数 8 1】

数81

$$K_A = \left(\prod_{i=1}^k z_{A\sigma_x(i)} \right)^{r_x(\sigma_x, A)g_x(\sigma_x)} \quad (\in G_A)$$

により、前記送信者側装置 A が

10

【数 8 2】

数82

$$K_A = g_A^{rr'} \quad (\in G_A)$$

によって生成し、同報通信に用いる暗復号化鍵 K_A を、演算装置を用いて計算し、記憶装置に記憶する処理と、 を実行させること

20

を特徴とするプログラムが記憶された記憶媒体。

【請求項 19】

通信回線を介して接続された複数の送信者側装置、複数の受信者側装置および鍵管理者側装置を有する通信システムであって、

前記鍵管理者側装置は、演算装置と、記憶装置と、通信装置と、入出力装置とを有し、

前記鍵管理者側装置の演算装置は、

鍵管理者秘密情報として、

【数 8 3】

数83

30

$$e_i \in \mathbb{Z} \quad (1 \leq i \leq m)$$

を生成する処理と、

送信者側装置 A の送信者識別情報として、

【数 8 4】

数84

40

$$t_A \in \mathbb{Z}$$

を生成し、前記記憶装置に記憶する処理と、

受信者側装置 x の受信者秘密情報として、

x S_{k m}、および、

【数85】

数85

$$s_x(\sigma_x) \in Z$$

(但し、集合

【数86】

数86

10

$$S_{km} = \{\sigma \mid 1\text{対}1\text{写像 } \sigma : A = \{1, 2, \dots, k\} \rightarrow B = \{1, 2, \dots, m\}, 0 < k < m\}$$

に対して、 \sim は S_{km} のとき

【数87】

数87

$$\sigma \sim \sigma' \stackrel{\text{def}}{\iff} \sigma(A) = \sigma'(A)$$

20

とし、このとき、 \sim は S_{km} 上の同値関係となり、

【数88】

数88

$$\tilde{S}_{km} = S_{km} / \sim$$

30

とする)を生成し、前記記憶装置に記憶する処理と、

前記記憶装置に記憶されている前記鍵管理者秘密情報 e_i 、前記送信者識別情報 t_A および前記受信者秘密情報 $s_x(x)$ 、 x から、受信者識別データ

【数89】

数89

$$s_x(\sigma_x, A) = t_A s_x(\sigma_x) \sum_{i=1}^k e_{\sigma_x(i)}$$

40

を生成し、前記記憶装置に記憶する処理と、

前記送信者側装置Aより出力された前記送信者秘密情報 g_A と、前記記憶装置に記憶されている前記鍵管理者秘密情報 e_i および前記送信者識別情報 t_A とから、鍵配送データ

【数90】

数90

$$y_{Ai} = g_A^{t_{Ac}i} \bmod N_A \quad (1 \leq i \leq m)$$

を算出し、前記記憶装置に記憶する処理と、を行い、

前記鍵管理者側装置の入出力装置は、

前記送信者側装置Aより出力された前記送信者秘密情報 g_A を入力する処理と、

前記鍵管理者側装置の演算装置が生成した前記受信者秘密情報 $s_x, s_x(x)$ を出力する処理と、

前記鍵管理者側装置の通信装置は、

前記鍵管理者側装置の演算装置が生成した前記受信者識別データ $s_x(x, A)$ および前記鍵配送データ y_{Ai} を、前記通信回線を介して前記送信者側装置Aに送信する処理を行い、

前記送信者側装置Aは、演算装置と、記憶装置と、通信装置と、入出力装置とを有し、

前記送信者側装置Aの演算装置は、

前記送信者側装置Aの送信者秘密情報として、

【数91】

数91

P_A, Q_A : 素数

$$L_A = \text{lcm}(\text{ord}_{P_A}(g_A), \text{ord}_{Q_A}(g_A))$$

$$g_A \in \mathbb{Z}, 0 < g_A < N_A$$

を生成し、自装置の記憶装置に記憶する処理と、

前記送信者側装置Aの送信者公開情報として、

【数92】

数92

$$N_A (= P_A Q_A)$$

を生成し、自装置の記憶装置に記憶する処理と、

整数 r, r' を生成し、前記記憶装置に記憶する処理と、

前記鍵管理者側装置から受信した受信者識別データ $s_x(x, A)$ と、自装置の記憶装置に記憶されている前記送信者秘密情報 L_A および前記整数 r' とから

10

20

30

40

【数93】

数93

$$r_x(\sigma_x, A) s_x(\sigma_x, A) \equiv r' \pmod{L_A}$$

なる受信者識別情報 $r_x(\sigma_x, A)$ を計算し、自装置の記憶装置に記憶する処理と、
前記鍵管理者側装置から受信した鍵配送データ y_{A_i} と、自装置の記憶装置に記憶され
ている前記整数 r とから、鍵配送情報

10

【数94】

数94

$$z_{Ai} = y_{Ai}^r \pmod{N_A} \quad (1 \leq i \leq m)$$

を計算し、自装置の記憶装置に記憶する処理と、を行い

前記送信者側装置 A の入出力装置は、

前記送信者側装置 A の演算装置が生成した前記送信者秘密情報 g_A を出力する処理を行
い、

20

前記送信者側装置 A の通信装置は、

前記通信回線を介して前記鍵管理者側装置から前記受信者識別データ $s_x(\sigma_x, A)$
および前記鍵配送データ y_{A_i} を受信する処理と、

前記送信者側装置 A の演算装置が生成した前記受信者識別情報 $r_x(\sigma_x, A)$ を、前
記通信回線を介して前記受信者側装置 x に送信する処理と、

前記送信者側装置 A の演算装置が生成した前記鍵配送情報 z_{A_i} を、前記通信回線を介
して前記複数の受信者側装置に同報送信する処理と、を行い、

前記受信者装置 x は、演算装置と、記憶装置と、通信装置と、入出力装置とを有し、

前記受信者側装置 x の演算装置は、

30

前記送信者側装置 A から受信した前記受信者識別情報 $r_x(\sigma_x, A)$ および前記鍵配
送情報 z_{A_i} と、前記鍵管理者側装置から受信した前記受信者秘密情報 $s_x(\sigma_x)$
) とから、

【数95】

数95

$$K_A = \left(\prod_{i=1}^k z_{A\sigma_x(i)} \right)^{r_x(\sigma_x, A) s_x(\sigma_x)} \pmod{N_A}$$

40

により、前記送信者側装置 A が

【数96】

数96

$$K_A = g_A^{rr'} \pmod{N_A}$$

によって生成し、同報通信に用いる暗復号化鍵 K_A を計算し、自装置の記憶装置に記憶する処理を行い、

前記受信者側装置 x の入出力装置は、

前記鍵管理者側装置より出力された前記受信者秘密情報 x 、 $s_x(x)$ を入力する処理を行い、

前記受信者側装置 x の通信装置は、

前記通信回線を介して前記送信者側装置 A から前記受信者識別情報 $r_x(x, A)$ および前記鍵配送情報 z_{A_i} を受信する処理を行うこと

を特徴とする通信システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、同報暗号通信における復号に用いる鍵を限定された受信者に配送する鍵配送の技術に関するものである。

【0002】

【従来の技術】

従来より、同報暗号通信の技術として、幾つかの方式が提案されている。

【0003】

たとえば、文献「S.J.Kent:Security requirement and protocols for a broadcast scenario, IEEE Trans. Commun., COM-29,6,pp.778-786(1981)」に記載のコピー鍵方式が知られている。

【0004】

このコピー鍵方式は、同報暗号通信の基本的な方式であり、従来の1対1の暗号個別通信を単純に同報通信に拡張したものである。すなわち、この方式では、1種類の鍵のコピーを送信者と複数の正規の受信者に配送する。そして、送信者は配送されたコピー鍵を用いて情報を暗号化して送信し、正規の各受信者は配送されたコピー鍵を用いて暗号化された情報を復号化する。

【0005】

また、このコピー鍵のように、送信者と受信者が共通に用いる鍵である共通鍵を、秘密裏に限定された受信者に配送する技術としては、文献「李、常盤他：多重化・多重分離法を用いた同報通信、1986年暗号と情報セキュリティシンポジウム」に記載の中国人の剰余定理を用いた情報系列の多重化・多重分離法による鍵配送方式や、文献「満保他：効率的な同報暗号通信方式、信学技法 ISEC93-34(1993-10)」に記載の方式などが知られている。

【0006】

中国人の剰余定理を用いて情報系列の多重化・多重分離法を行う方式は、次の処理を行うものである。

【0007】

(1) 鍵生成処理：

受信者 i ($1 \leq i \leq r$) に対して、互いに素な s 個の整数 g_1, g_2, \dots, g_s ($r \leq s$) を作成し、 g_i を受信者 i の秘密情報として、予め受信者 i に配布する。

【0008】

(2) 暗号化処理：

多重化すべき s 個の情報系列を M_1, M_2, \dots, M_s とする。送信者は、多重化送信文

10

20

30

40

50

F を、

【 0 0 0 9 】

【 数 9 7 】

数97

$$F = \sum_{i=1}^k A_i G_i M_i \text{ mod } G$$

10

【 0 0 1 0 】

により計算し、これを同報送信する。但し、 G 、 G_i 、 A_i は、

【 0 0 1 1 】

【 数 9 8 】

数98

$$G = \prod_{i=1}^k g_i,$$

20

$$G_i = G/g_i,$$

$$A_i G_i \equiv 1 \pmod{g_i}$$

【 0 0 1 2 】

において、 A_i が最小の整数となる関係にある。

【 0 0 1 3 】

(3) 復号化処理 :

30

受信者 i は、多重化送信文 F から g_i を用いて、

【 0 0 1 4 】

【 数 9 9 】

数99

$$M_i = F \text{ mod } g_i$$

【 0 0 1 5 】

40

により、 M_i を分離化する。

【 0 0 1 6 】

ここで、 M_i は、受信者 i に配送すべき共通鍵であってよい。したがって、この方式によれば、限定された受信者のみに秘密裏にコピー鍵を配送することができる。

【 0 0 1 7 】

次に、文献「満保他：効率的な同報暗号通信方式、信学技法 ISEC93-34 (1993-10)」に記載の方式は、次の処理を行うものである。

【 0 0 1 8 】

(1) 鍵生成処理 :

信頼できるセンタは、次の情報を作成する。

50

【 0 0 1 9 】

秘密情報：

【 0 0 2 0 】

【 数 1 0 0 】

数100

$$P = 2p + 1, Q = 2q + 1 : \text{素数 } (p, q : \text{素数})$$

$$e_i \in \mathbb{Z}, 0 < e_i < L \quad (1 \leq i \leq m)$$

10

【 0 0 2 1 】

公開情報：

【 0 0 2 2 】

【 数 1 0 1 】

数101

$$g \in \mathbb{Z}, 0 < g < N$$

20

$$N = PQ$$

$$v_i = g^{e_i} \bmod N \quad (1 \leq i \leq m).$$

【 0 0 2 3 】

センタは、 S に対して、

【 0 0 2 4 】

【 数 1 0 2 】

30

数102

$$s_\sigma \sum_{i=1}^k e_{\sigma(i)} \equiv 1 \pmod{L}$$

【 0 0 2 5 】

なる S を計算し、受信者 U の秘密情報として配布する。但し、集合 $S = \{ f \mid 1 \text{対} 1 \text{写像 } f : A = \{ 1, 2, \dots, k \} \rightarrow B = \{ 1, 2, \dots, m \}, m > k \}$ とする。 40

【 0 0 2 6 】

(2) 鍵配送処理：

送信者は整数 r をランダムに選び、共通鍵

【 0 0 2 7 】

【 数 1 0 3 】

数103

$$K = g^r \bmod N$$

【0028】

を限定された受信者との間で共有することを目的として、

【0029】

【数104】

10

数104

$$z_i = v_i^r \bmod N \quad (1 \leq i \leq m)$$

【0030】

を計算し、 z_i ($1 \leq i \leq m$) を同報送信する、

受信者 U は、

【0031】

【数105】

20

数105

$$K = \left(\prod_{i=1}^k z_{\sigma(i)} \right)^{s_\sigma} \bmod N$$

【0032】

にて、共通鍵 K を計算する。

【0033】

【発明が解決しようとする課題】

前述した中国人の剰余定理を用いた多重化方法を利用した鍵配送では、受信者一人一人用の共通鍵のデータをシリアルに並べて送信するので、受信者数に比例して同報通信するデータの長さが長くなる。このため、衛星放送サービスのように数百万人以上の受信者を対象とする通信には適していない。

【0034】

これに対して、文献「満保他：効率的な同報暗号通信方式、信学技法 ISEC93-34 (1993-10)」に記載の方式によれば、受信者数が大きい場合であっても共通鍵配送のためのデータを小さくできる。しかし、この方式では、任意の受信者集合に属する限定された受信者のみと鍵共有を行なうことができない。

30

40

【0035】

また、いずれの方式の場合も、送信者が複数存在する場合には、受信者は情報を受信する送信者毎に、それぞれ、前述した秘密情報入手、管理しなければならない。

【0036】

そこで、本発明は、受信者が唯一の秘密情報によって、複数の送信者からの個々の共通鍵の配送を受けることのできる鍵配送システムを提供することを課題とする。また、このような鍵配送システムにおいて、任意の送信者と任意の受信者集合に属する受信者のみとのデータ暗復号のための共通鍵の共有を可能とすること、および、受信者数が大きい場合に

50

、これに伴い共通鍵配送のための同報通信データを長くする必要がない共通鍵配送を実現することを課題とする。

【0037】

【課題を解決するための手段】

前記課題達成のために、本発明は、複数の送信者と、複数の受信者とが存在する通信システムにおいて、前記送信者が行う同報暗号通信の暗復号化鍵を、前記送信者と前記受信者との間で共有するための鍵配送方法であって、

鍵管理者を設け、当該鍵管理者において、前記送信者と前記受信者との間で鍵を共有するために用いる、前記複数の送信者について共通の第1鍵情報を作成して所定の受信者に配布するとともに、前記送信者と前記受信者との間で鍵を共有するために用いる第2鍵情報を作成して前記送信者に配布し、

前記送信者は、前記受信者が前記第1鍵情報を用いて当該送信者が同報通信に用いる暗復号化鍵を算出するための第3鍵情報を、前記鍵管理者から配布された第2鍵情報を用いて生成して、当該送信者と鍵を共有する前記受信者に送信し、前記受信者は、前記鍵管理者から配布された第1鍵情報と前記送信者から配布された第3鍵情報とを用いて、第3鍵情報を配布した前記送信者が同報通信に用いる暗復号化鍵を入手することを特徴とする。

【0038】

本鍵配送方法によれば、各受信者は、秘密情報として鍵管理者から配布された第1鍵情報のみを所持すればよく、新たな送信者の暗復号化鍵を入手する場合にも、新たな秘密情報の配布を受ける必要がない。

【0039】

より詳細には、本発明は、前記課題達成のために、たとえば、複数の送信者と、複数の受信者と、鍵管理者とが存在する通信システムを用い、前記送信者が行う同報暗号通信の暗復号化鍵を、前記受信者に配送する鍵配送方法であって、鍵管理者において、鍵管理者秘密情報として、

【0040】

【数106】

数106

$$e_i \in \mathbb{Z}, \quad (1 \leq i \leq m)$$

【0041】

を作成し、送信者Aの送信者識別情報として、

【0042】

【数107】

数107

$$t_A \in \mathbb{Z}$$

【0043】

を作成し、受信者xの受信者秘密情報として、

$s_{x, k, m}$ と、

【0044】

【数108】

数108

$$s_x(\sigma_x) \in \mathbb{Z}$$

【0045】

(但し、集合

【0046】

【数109】

10

数109

$$S_{km} = \{\sigma \mid 1 \text{ 対 } 1 \text{ 写像 } \sigma: A = \{1, 2, \dots, k\} \rightarrow B = \{1, 2, \dots, m\}, 0 < k < m\}$$

【0047】

に対して、 $\sigma, \sigma' \in S_{km}$ のとき

【0048】

【数110】

20

数110

$$\sigma \sim \sigma' \stackrel{\text{def}}{\iff} \sigma(A) = \sigma'(A)$$

【0049】

とし、このとき、 \sim は S_{km} 上の同値関係となり、

【0050】

【数111】

30

数111

$$\tilde{S}_{km} = S_{km} / \sim$$

【0051】

とする) とを作成し、受信者秘密情報 s_x 、 $s_x(x)$ を受信者 x に配布するステップと

、

送信者 A において、

【0052】

【数112】

40

数112

$$\bullet g_A \in G_A$$

$$\bullet L_A = \text{ord}_{G_A}(g_A)$$

50

【 0 0 5 3 】

(但し、

【 0 0 5 4 】

【 数 1 1 3 】

数113

$$\text{ord}_{G_A}(g)$$

10

【 0 0 5 5 】

は、

【 0 0 5 6 】

【 数 1 1 4 】

数114

$$g^a = 1 \quad (\in G_A)$$

20

【 0 0 5 7 】

なる最小の正整数 a を表す) なる送信者秘密情報 g_A 、 L_A および有限アーベル群 G_A を作成し、送信者秘密情報 g_A を鍵管理者に送信するステップと、

鍵管理者において、鍵管理者秘密情報 e_i 、送信者識別情報 t_A および受信者秘密情報 s_X (X)、 X から、受信者識別データ

【 0 0 5 8 】

【 数 1 1 5 】

数115

$$s_X(\sigma_X, A) = t_A s_X(\sigma_X) \sum_{i=1}^k e_{\sigma_X(i)}$$

30

【 0 0 5 9 】

を計算し、受信者識別データ $s_X(X, A)$ を送信者 A に送信し、送信者 A から受信した g_A と、鍵管理者秘密情報 e_i と、送信者識別情報 t_A から、鍵配送データ

【 0 0 6 0 】

【 数 1 1 6 】

40

数116

$$y_{Ai} = g_A^{t_A e_i} \quad (\in G_A) \quad (1 \leq i \leq m)$$

【 0 0 6 1 】

を算出し、鍵配送データ y_{Ai} を送信者 A に送信するステップと、

送信者 A において、整数 r 、 r' を生成し、鍵管理者から受信した受信者識別データ $s_X(X, A)$ と、送信者秘密情報 L_A と、整数 r' から

【 0 0 6 2 】

50

【数117】

数117

$$r_x(\sigma_x, A) s_x(\sigma_x, A) \equiv r' \pmod{L_A}$$

【0063】

なる受信者識別情報 $r_x(x, A)$ を計算し、受信者識別情報 $r_x(x, A)$ を受信者 x に送信し、鍵管理者から受信した鍵配送データ y_{Ai} と、整数 r から、鍵配送情報

10

【0064】

【数118】

数118

$$z_{Ai} = y_{Ai}^r \pmod{G_A} \quad (1 \leq i \leq m)$$

【0065】

を計算し、鍵配送情報 z_{Ai} を、各受信者に同報送信するステップと、
受信者 x において、送信者 A から受信した受信者識別情報 $r_x(x, A)$ および鍵配送情報 z_{Ai} と、鍵管理者から配布された受信者秘密情報 $s_x(x)$ から、

20

【0066】

【数119】

数119

$$K_A = \left(\prod_{i=1}^k z_{A\sigma_x(i)} \right)^{r_x(\sigma_x, A) s_x(\sigma_x)} \pmod{G_A}$$

30

【0067】

により、送信者 A が

【0068】

【数120】

数120

$$K_A = g_A^{rr'} \pmod{G_A}$$

40

【0069】

によって生成し、同報通信に用いる暗復号化鍵 K_A を計算するステップと、を有することを特徴とする。

【0070】

この鍵配送方法によれば、受信者は送信者毎に異なる秘密鍵を持つ必要がない他、同報暗号通信において、受信者数が大きい場合であっても、これに伴い鍵配送情報の長さを長くする必要がない。また、本鍵配送方法においては、鍵管理者のみが秘密裏に所持する送信者識別情報によって、受信者秘密情報は送信者に対して秘密化され、受信者に対して送信

50

者秘密情報はより強固に秘密化されるので、不正に対する安全性が向上する。

【0071】

【発明の実施の形態】

以下、本発明に係る鍵配送システムの実施形態について説明する。

【0072】

まず、本発明の第1実施形態について説明する。

【0073】

図1に、本発明の第1実施形態に係る鍵配送システムの構成を示す。

【0074】

図示するように、本システムは、相互に通信回線400で接続された鍵管理者側装置100、送信者側装置200、受信者側装置300から構成される。鍵管理者側装置100は、システムに唯一の鍵管理者組織が使用する装置であり、送信者装置200、受信者側装置300はシステム中に複数存在する。

【0075】

図2に、鍵管理者側装置100の構成を示す。

【0076】

図示するように、鍵管理者側装置100は、乱数生成器101、素数生成器102、べき乗算器103、剰余演算器104、演算装置105、メモリ106、通信装置107から構成される。また、鍵管理者側装置100には、オフラインで受信者に配送する受信者側携帯装置306が接続される。

【0077】

図3に、送信者側装置200の構成を示す。

【0078】

図示するように、送信者側装置200は、乱数生成器201、素数生成器202、べき乗算器203、剰余演算器204、演算装置205、メモリ206、通信装置207、暗復号化装置208、認証装置209、課金装置210から構成される。

【0079】

図4に、受信者側装置300の構成を示す。

【0080】

図示するように、受信者側装置300は、べき乗算器301、剰余演算器302、演算装置303、メモリ304、通信装置305、鍵管理者からオフラインで配送された受信者側携帯装置306、暗復号化装置307、認証装置308から構成される。

【0081】

以下、本システムが行う準備処理、鍵配送処理、そして暗復号化処理の3つの処理について説明する。

【0082】

では、まず、準備処理について説明する。

【0083】

(1) 準備処理

1 送信者Aは、送信者側装置200内の乱数生成器201、素数生成器202、べき乗算器203、剰余演算器204、および演算装置205を用いて、次の情報を作成し、そのうち、公開情報のみを公開する。

【0084】

秘密情報：

【0085】

【数121】

数121

P_A, Q_A : 素数

$$L_A = \text{lcm}(\text{ord}_{P_A}(g_A), \text{ord}_{Q_A}(g_A))$$

$$g_A \in \mathbf{Z}, \quad 0 < g_A < N_A$$

10

【0086】

公開情報：

【0087】

【数122】

数122

20

$$N_A (= P_A Q_A)$$

【0088】

秘密情報はメモリ206に格納する。また、秘密情報 g_A 、 L_A を通信装置207を用いて鍵管理者に送信する。

【0089】

2 信頼できる鍵管理者は、鍵管理者側装置100内の演算装置105を用いて、次の情報を作成する。

【0090】

30

鍵管理者秘密情報：

【0091】

【数123】

数123

$$e_i \in \mathbf{Z} \quad (1 \leq i \leq m)$$

【0092】

40

送信者Aの送信者識別情報：

【0093】

【数124】

数124

$$t_A \in \mathbf{Z}, \quad 0 < t_A < L_A$$

【0094】

50

受信者 x の受信者秘密情報：

【 0 0 9 5 】

【 数 1 2 5 】

数125

$$s_x(\sigma_x) \in \mathbf{Z}, \quad 0 < t_A < L_A$$

【 0 0 9 6 】

これらは、 x とともに全てメモリ 1 0 6 に格納する。

【 0 0 9 7 】

ただし、集合

【 0 0 9 8 】

【 数 1 2 6 】

数126

$$S_{km} = \{ \sigma \mid 1 \text{ 対 } 1 \text{ 写像 } \sigma : A = \{1, 2, \dots, k\} \rightarrow B = \{1, 2, \dots, m\}, 0 < k < m \}$$

【 0 0 9 9 】

に対して、 \sim 、 $\overset{\text{def}}{\iff}$ S_{km} のとき、

【 0 1 0 0 】

【 数 1 2 7 】

数127

$$\sigma \sim \sigma' \quad \overset{\text{def}}{\iff} \quad \sigma(A) = \sigma'(A)$$

【 0 1 0 1 】

とする。このとき、 \sim は S_{km} 上の同値関係となり、

【 0 1 0 2 】

【 数 1 2 8 】

数128

$$\tilde{S}_{km} = S_{km} / \sim$$

【 0 1 0 3 】

とする。

【 0 1 0 4 】

また、鍵管理者は、メモリ 1 0 6 から受信者秘密情報 $s_x(\sigma_x)$ を取り出し、 x とともに受信者側携帯装置 3 0 6 に格納し、これを受信者 x にオフラインで配布する。もちろん、他の方法によって受信者に配布するようにしてもよい。

【 0 1 0 5 】

次に、鍵配送処理について説明する。

【 0 1 0 6 】

(2) 鍵配送処理

10

20

30

40

50

本鍵配送処理における、鍵管理者、送信者、および受信者間の情報の流れを図5に示す。

【0107】

1 鍵管理者は、鍵管理者側装置100内の剰余演算器104、演算装置105を用いて、送信者Aから受信した L_A と、鍵管理者秘密情報 e_i と、受信者秘密情報 $s_x(\sigma_x)$ と、送信者識別情報 t_A から、

【0108】

【数129】

数129

$$s_x(\sigma_x, A) = t_A s_x(\sigma_x) \sum_{i=1}^k e_{\sigma_x(i)} \bmod L_A$$

【0109】

なる受信者 x の受信者識別データ $s_x(\sigma_x, A)$ を計算し、通信装置107を用いて送信者Aに送信する。

【0110】

また、鍵管理者は、鍵管理者側装置100内のべき乗算器103、剰余演算器104、演算装置105を用いて、送信者Aから受信した g_A と、送信者Aの送信者公開情報 N_A と、鍵管理者秘密情報 e_i から、

【0111】

【数130】

数130

$$y_{Ai} = g_A^{t_A e_i} \bmod N_A \quad (1 \leq i \leq m)$$

【0112】

なる送信者Aの送信者鍵配送データ y_{Ai} を計算し、通信装置107を用いて送信者Aに送信する。

【0113】

2 送信者Aは、送信者側装置200内の乱数生成器201により、乱数 r 、 r' を作成しメモリ206に格納する。さらに、べき乗算器203、剰余演算器204、演算装置205を用いて、この乱数 r 、 r' と、自身の秘密情報 g_A と、自身の公開情報 N_A から、

【0114】

【数131】

数131

$$K_A = g_A^{rr'} \bmod N_A$$

【0115】

なるデータ暗号化鍵 K_A を計算してメモリ206に格納し、受信者 x との間で鍵 K_A を共有することを目的として、剰余演算器204、演算装置205を用いて、自身の秘密情報 L_A と、乱数 r' と、鍵管理者から受信した受信者 x の受信者識別データ $s_x(\sigma_x, A)$ から、

【0116】

10

20

30

40

50

【数132】

数132

$$r_x(\sigma_x, A) s_x(\sigma_x, A) \equiv r' \pmod{L_A}$$

【0117】

なる受信者 x の受信者識別情報 $r_x(\sigma_x, A)$ を計算し、通信装置 207 を用いて受信者 x に送信する。

10

【0118】

また、送信者 A は、送信者側装置 200 内のべき乗算器 203、剰余演算器 204、演算装置 205 を用いて、自身の公開情報 N_A と、乱数 r と、鍵管理者から受信した送信者鍵配送データ y_{A_i} から、

【0119】

【数133】

数133

$$z_{A_i} = y_{A_i}^r \pmod{N_A} \quad (1 \leq i \leq m)$$

20

【0120】

なる受信者鍵配送データ z_{A_i} を計算し、通信装置 207 を用いて受信者に同報送信する。

【0121】

ここで、以上の処理において、 $r_x(\sigma_x, A)$ 、 z_{A_i} を作成する処理の一部を、鍵管理者が行う理由の一つは、送信者 A に対して、受信者 x の受信者秘密情報 $s_x(\sigma_x)$ 、送信者識別番号 t_A を秘密にすることにより、送信者 A の不正を防止するためである。

【0122】

3 受信者 x は、送信者 A から受信した鍵配送データ z_{A_i} および受信者識別情報 $r_x(\sigma_x, A)$ 、鍵管理者から配送された受信者秘密情報 $s_x(\sigma_x)$ 、公開された送信者公開情報 N_A から、

30

【0123】

【数134】

数134

$$K_A = \left(\prod_{i=1}^k z_{A_{\sigma_x(i)}} \right)^{r_x(\sigma_x, A) s_x(\sigma_x)} \pmod{N_A}$$

40

【0124】

により、データ暗号化鍵 K_A を計算し、メモリ 304 に格納する。

【0125】

以上の処理で、送信者 A と受信者 x は鍵 K_A を共有できる。他の任意の送信者と受信者についても同様にして鍵を共有できる。また、この際、送信者 A が同報送信する受信者鍵配送データ z_{A_i} は、各受信者について共通である。

【0126】

また、以上の処理において、受信者 x が送信者 A より受けとる鍵配送データ z_{A_i} および受信者識別情報 $r_x(\sigma_x, A)$ は、受信者に対して秘密化されている送信者 A の送信者識別

50

番号 t_A が作用したものとなっている。したがって、以上の送信者識別番号 t_A を用いる構成により、受信者 x が送信者 A より受けとった鍵配送データ z_{Ai} 、受信者識別情報 $r_x(x, A)$ 、他の送信者 B の公開情報 N_B 、他の送信者 B が同報通信した鍵配送データ z_{Bi} より、他の送信者 B のデータ暗号化鍵 K_B を割り出すことを、きわめて困難とすることができる。

【0127】

以下、暗復号化処理について説明する。

【0128】

(3) 暗復号化処理

1 送信者 A は、送信者側装置 200 内の暗復号化装置 208 を用いて、鍵配送処理で作成した共通鍵 K_A により、データ P を暗号化する。そして、暗号文 $C = E(K_A : P)$ を通信装置 207 を用いて受信者 x に送信する。

【0129】

2 受信者 x は、受信者側装置 300 内の通信装置 305 を用いて暗号文 C を受信し、暗復号化装置 307 を用いてメモリ 304 に格納していた共通鍵 K_A により暗号文 C を復号化し、データを得る。

【0130】

以上、本発明の第 1 実施形態について説明した。

【0131】

従来の技術では、新規に送信者がシステムに参入する際、受信者秘密情報 $s_x(x)$ を、送信者自身が作成し受信者にオフラインで配布する必要があった。これに対し、第 1 実施形態に係る鍵配送システムによれば、新規参入の送信者 A は、送信者秘密情報 P_A 、 Q_A 、 L_A 、 g_A と、送信者公開情報 N_A を作成するだけでよい。また、受信者が持つ受信者秘密情報は、全ての送信者に対して唯一であり、新たな送信者からデータを受信したい場合に、新たな受信者秘密情報を入手する必要がない。

【0132】

また、受信者識別情報 $r_x(x, A)$ によって、任意の受信者集合に属する受信者のみとのデータ暗復号のための共通鍵の共有を可能とすることができる。また、受信者数が多い場合であっても、共通鍵配送のために同報通信する鍵配送データ z_{Ai} を、これに伴い長くする必要がない。

【0133】

なお、以上の処理において、あらかじめ、送信者 A が送信者秘密情報 L_A を鍵管理者に送信しておき、準備処理の段階で、鍵管理者は、送信者 A から受信した送信者秘密鍵 L_A から

【0134】

【数135】

数135

$$e_i \in \mathbf{Z}, \quad 0 < e_i < L_A, \quad (1 \leq i \leq m)$$

$$t_A \in \mathbf{Z}, \quad 0 < t_A < L_A$$

$$s_x(\sigma_x) \in \mathbf{Z}, \quad 0 < s_x(\sigma_x) < L_A$$

【0135】

となる鍵管理者秘密情報 e_i 、送信者識別情報 t_A 、受信者秘密情報 $s_x(x)$ を作成し、鍵配送処理の段階で、鍵管理者は、送信者秘密情報 L_A 、鍵管理者秘密情報 e_i 、送信者識

10

20

30

40

50

別情報 t_A 、受信者秘密情報 $s_x(x)$ から、

【0136】

【数136】

数136

$$s_x(\sigma_x, A) = t_A s_x(\sigma_x) \sum_{i=1}^k e_{\sigma_x(i)} \pmod{L_A}$$

10

【0137】

によって、受信者識別データ $s_x(x, A)$ を計算するようにしてもよい。

【0138】

次に、本発明の第2実施形態について説明する。

【0139】

本発明の第2実施形態は、上記の第1実施形態における受信者側携帯装置306に、図6に示すように、べき乗算器3036、剰余演算器3063、演算装置3061、メモリ3062を備えるようにしたものである。そして、上記の第1実施形態の受信者側装置300におけるデータ暗号化鍵 K_A の計算処理の一部を、受信者側携帯装置306で実施する

20

【0140】

すなわち、第2実施形態では、(1)準備処理の段階で、鍵管理者は x と受信者秘密情報 $s_x(x)$ とを、受信者携帯装置306(ICカード等)に格納して、受信者 x に配布する。

【0141】

そして、(2)鍵配送処理において、受信者 x は、受信者側装置300内のメモリに格納されている鍵配送データ z_{Ai} を受信者携帯装置306に出力する。次に、受信者携帯装置306内で、べき乗算器3064、剰余演算器3063を用いて、受信者秘密情報 $s_x(x)$ 、 $s_x(x)$ 、鍵配送データ z_{Ai} および送信者公開情報 N_A から、

30

【0142】

【数137】

数137

$$\xi_x(\sigma_x, A) = \left(\prod_{i=1}^k z_{A\sigma_x(i)} \right)^{s_x(\sigma_x)} \pmod{N_A}$$

40

【0143】

を計算し、この計算結果 $\xi_x(x, A)$ を受信者側装置300に出力する。

【0144】

次に、受信者側装置300内のべき乗算器301、剰余演算器302、演算装置303を用いて、受信者側装置300に出力された $\xi_x(x, A)$ と、メモリ304に格納している受信者識別鍵 $r_x(x, A)$ および送信者公開情報 N_A から、

【0145】

【数138】

数138

$$K_A = \xi_x(\sigma_x, A)^{r_x(\sigma_x, A)} \bmod N_A$$

【0146】

により、データ暗号化鍵 K_A を計算し、メモリ 304 に格納する。

【0147】

このように受信者秘密情報 $s_x(x)$ が受信者側携帯装置 306 外部に出力しないようにすることにより、これが電子的複写などにより盗難されることを防ぐことができる。

【0148】

以上、本発明の第2実施形態について説明した。

【0149】

次に、本発明の第3実施形態について説明する。

【0150】

本発明の第3実施形態は、上記の第1実施形態において、

【0151】

【数139】

数139

$$K_A = g_A^{rr'} \bmod N_A$$

【0152】

の r の値を短時間毎に、周期毎に変更し、変更後の r を用いた z_{Ai} を周期的に同報通信することにより、送信者側装置 200 および受信者側装置 300 で計算するデータ暗復号化鍵 K_A の更新を行うものである。

【0153】

また、 r' の値を送信データ固有の値とすることで、送信者が同報送信するデータの識別を行うようにしたものである。すなわち、受信者 x がある同報データもしくは同報データの集合を復号するために、ある送信者から得た識別鍵 $r_x(x, A)$ はその同報データ固有のものであり、別の同報データもしくは同報データの集合を取得するためには、その送信者から別の同報データもしくは同報データの集合用の別の $r_x(x, A)$ を得る必要がある。

【0154】

以上、本発明の第3実施形態について説明した。

【0155】

次に、本発明の第4実施形態について説明する。

【0156】

本発明の第4実施形態は、上記の第1実施形態において、特定の受信者の認証を行い、送信者が鍵 K_A を用いて暗号化し送信した有償のデータ P に対する、鍵 K_A を共有する受信者への課金を行うものである。

【0157】

すなわち、第4実施形態では、さらに、以下の処理を行う。

【0158】

(1) 準備処理

1 鍵管理者は、鍵管理者側装置 100 内の演算装置 105 を用いて、予め受信者 x の番号 UID_x を作成し、これを受信者秘密情報 $s_x(x)$ と一緒に受信者携帯装置 306

10

20

30

40

50

内のメモリ3061に格納して配布する。また、 UID_x を、 $s_x(x)$ と対応させて、鍵管理者側装置100内のメモリ106に格納しておく。

【0159】

2 送信者Aは、送信者側装置200内の演算装置205を用いて、自身の番号 BID_A を作成し、メモリ206に格納しておく。また、 BID_A を通信装置207を用いて鍵管理者に送信する。

【0160】

3 鍵管理者は、鍵管理者側装置100内の通信装置107によって送信者Aの番号 BID_A を受信し、メモリ106に送信者識別情報 t_A と対応させて格納する。

【0161】

4 受信者xは、受信者側装置300内の認証装置308を用いて、受信者秘密情報 $s_x(x)$ から認証用の情報を作成し、送信者Aに送信する。

【0162】

5 送信者Aは、該認証用の情報を、送信者側装置200内の認証装置209によって確認する。

【0163】

この認証の方法は、受信者が $s_x(x)$ を知らない限り、認証が成立しない認証方法であれば、従来知られている各種認証方式を用いてかまわない(ただし、このとき、送信者は受信者秘密鍵 $s_x(x)$ 自体は知ることができないようにする必要がある)。

【0164】

たとえば、RSA(文献「R. L. Rivest, A. Shamir, L. Adelman. :A method for obtaining digital signatures and publickey cryptosystems, Commun. of the ACM, Vol. 21, No.2, pp.120-126, 1987.」に掲載)による署名を用いた方法によって、受信者xの認証を、以下の処理によって行えばよい。

【0165】

1:鍵管理者は、受信者xに対して、

【0166】

【数140】

数140

$$s'_x y_x \equiv 1 \pmod{\text{lcm}(p_x - 1, q_x - 1)}$$

$$n_x = p_x q_x \quad (p_x, q_x : \text{素数})$$

【0167】

なる (y_x, n_x) を予め送信者に配布する。ただし、公開された関数に対して、 $s'_x = (s_x(x))$ とする。

【0168】

2:受信者xは、受信者側装置300内の認証装置308を用いて、同報送信データであるWのハッシュ値を、公開情報である一方向性ハッシュ関数hにより計算し($0 < h(W) < n_x$)、 $h(W)$ に対する署名を秘密鍵 s'_x を用いて、

【0169】

【数141】

数141

$$\text{sgn}_x(h(W)) = h(W)^{s'_x} \pmod{n_x}$$

10

20

30

40

50

【0170】

にて作成し、データの送信要求とともに通信装置305を用いて送信者Aに送信する。

【0171】

3:送信者Aは、認証装置209を用いて、

【0172】

【数142】

数142

$$\text{sgn}_x(h(W))^{y_x} \equiv h(W) \pmod{n_x}$$

10

【0173】

が成立することを確認する。

【0174】

6 さて、認証を行った後に、送信者Aは、送信者側装置200内の通信装置207を用いて、自身の番号 BID_A と受信者xの番号 UID_x を鍵管理者に送信する。

【0175】

7 鍵管理者は、鍵管理者側装置100内の演算装置105を用いて、受信した送信者番号 BID_A と受信者番号 UID_x に対応した、送信者識別鍵 t_A と受信者秘密情報 s_x (20
x) から、

【0176】

【数143】

数143

$$s_x(\sigma_x, A) = t_A s_x(\sigma_x) \sum_{i=1}^k e_{\sigma_x(i)} \pmod{L_A}$$

30

【0177】

となる受信者識別データ $s_x(x, A)$ を計算し、送信者Aに送信する。

【0178】

8 送信者Aは、送信者側装置200内の剰余演算器204、演算装置205を用いて、鍵管理者から受信した受信者識別データ $s_x(x, A)$ から、

【0179】

【数144】

数144

$$r_x(\sigma_x, A) s_x(\sigma_x, A) \equiv r' \pmod{L_A}$$

40

【0180】

となる受信者識別情報 $r_x(x, A)$ を計算し、通信装置207により受信者xに送信する。その際、共通鍵 K_A によって、暗号化して配信するデータ(受信者が送信要求したデータ)が有償の場合、送信者Aは、課金装置210を用いて受信者xに対して課金する。

【0181】

以上、本発明の第4実施形態について説明した。

【0182】

50

次に、本発明の第5実施形態について説明する。

【0183】

本発明の第5実施形態は、従来の技術の欄で述べたコピー鍵方式を、図1に示した複数の送信者と複数の受信者と鍵管理者が存在するシステムに拡張したものである。

【0184】

図7に、本発明の第5実施形態に係る鍵管理者側装置100の構成を示す。図示するように、鍵管理者側装置100は、乱数生成器111、演算装置112、メモリ113、通信装置114から構成される。また、図8に、本発明の第5実施形態に係る送信者側装置200の構成を示す。図示するように、送信者側装置200は、乱数生成器211、演算装置212、暗復号化装置213、メモリ214、通信装置215から構成される。また、図9に、本発明の第5実施形態に係る受信者側装置300の構成を示す。図示するように、受信者側装置300は、演算装置311、暗復号化装置312、メモリ313、通信装置314から構成される。

10

【0185】

本実施形態では、まず、準備処理として、以下の処理を行う。

【0186】

(1) 準備処理

1 鍵管理者は、鍵管理者側装置100内の乱数生成器111を用いて、秘密情報 K_0 を生成しメモリ113に格納する。また、送信者と受信者に配布する。

【0187】

2 送信者Aは、送信者側装置200内の乱数生成器211を用いて送信者識別情報 BID_A を生成し、通信装置114により受信者に送信する。

20

【0188】

その後、鍵配送処理として、以下の処理を行う。

【0189】

(2) 鍵配送処理

1 送信者Aは、送信者側装置200内の演算装置205を用いて、鍵管理者から配布された秘密鍵情報 K_0 と送信者識別情報 BID_A から、適当な一方向性関数 F により、共通鍵 $K_A' = F(K_0, BID_A)$ を計算する。

【0190】

2 受信者は、受信者側装置300内の演算装置312を用いて、鍵管理者から配布された秘密情報 K_0 と送信者から受信した送信者識別情報 BID_A から、一方向性関数 F により、共通鍵 $K_A' = F(K_0, BID_A)$ を計算する。

30

【0191】

3 送信者Aは、送信者側装置200内の乱数生成器211を用いて適当な整数 r を作成し、通信装置215により受信者に送信する。また、演算装置212を用いて、整数 r と共通鍵 K_A' から、適当な関数 F' によりデータ暗復号化鍵 $DK = F'(r, K_A')$ を計算し、メモリ214に格納する。

【0192】

4 受信者は、受信者側装置300内の演算装置312を用いて、送信者Aから受信した整数 r と、共通鍵 K_A' から、関数 F' により、データ暗復号化鍵 $DK = F'(r, K_A')$ を計算して、メモリ314に格納する。

40

【0193】

上記の鍵配送処理により、データ暗復号化鍵 DK の配送が行われた後、暗復号化処理は、以下の要領で行う。

【0194】

(3) 暗復号化処理

1 送信者Aは、データ暗復号化鍵 DK を用いて、送信者側装置200内の暗復号化装置203により配信データ P を暗号化し、通信装置205により受信者に送信する。

【0195】

50

2 受信者は、受信者側装置 300 内の通信装置 305 により暗号化された配信データ P を受信し、データ暗復号化鍵 DK を用いて暗復号化装置 303 により復号化する。

【0196】

以上説明した本発明の第 5 実施形態によっても、受信者は、単一の秘密情報で、複数の送信者と、各送信者個々の共通鍵を共有することができる。

【0197】

次に、本発明の第 6 実施形態について説明する。

【0198】

本発明の第 6 実施形態は、送信者と受信者が、受信者の個別の鍵を使った暗号通信により、共通鍵を共有するものである。

10

【0199】

本実施形態に係る全体のシステム、鍵管理者側装置 100、送信者側装置 200、受信者側装置 300 の構成は、上述した本発明の第 5 実施形態のものと同様である。

【0200】

さて、本実施形態では、準備処理において、以下の処理を行う。

【0201】

(1) 準備処理

1 鍵管理者は、鍵管理者側装置 100 内の乱数生成器 111 を用いて受信者 x の秘密情報 s_x を作成し、受信者に配布する。さらに、乱数生成器 111 を用いて送信者 A の番号 BID_A を作成し、送信者 A および受信者 x に配布する。

20

【0202】

2 送信者 A は、送信者側装置 200 内の乱数生成器 211 を用いて共通鍵 K_A を作成する。

【0203】

その後、鍵配送処理において、以下の処理を行う。

【0204】

(2) 鍵配送処理

1 鍵管理者は、鍵管理者側装置 100 内の演算装置 112 を用いて、送信者 A の番号 BID_A と受信者秘密情報 s_x から、適当な一方向性関数 F により $K_{AX} = F(s_x, K_A)$ なる、受信者 x および送信者 A 間でのセッション鍵 K_{AX} を計算し、メモリ 113 に格納する。

30

【0205】

2 受信者 x は、受信者側装置 300 内の演算装置 312 を用いて、送信者 A の番号 BID_A と自身の秘密情報 s_x から、一方向性関数 F により $K_{AX} = F(s_x, BID_A)$ を計算し、メモリ 313 に格納する。

【0206】

3 送信者 A は、送信者側装置 200 内の暗復号化装置 213 を用いて、セッション鍵 K_{AX} により共通鍵 K_A を暗号化し、その結果、得られた鍵配送データ K_{CX} を、通信装置 215 により受信者に送信する。さらに、乱数生成器 211 を用いて、適当な整数 r を作成し、通信装置 215 により受信者に送信するとともに、演算装置 212 を用いて、整数 r と共通鍵 K_A から、適当な関数 F' によりデータ暗復号化鍵 $DK = F'(r, K_A)$ を計算し、メモリ 214 に格納する。

40

【0207】

4 受信者 x は、受信者側装置 300 内の暗復号化装置 303 を用いて、送信者 A から受信した鍵配送データ K_{CX} をセッション鍵 K_{AX} により復号化する。そして、演算装置 302 を用いて、復号化した共通鍵 K_A と受信した整数 r から、関数 F' により、データ暗復号化鍵 $DK = F'(r, K_A)$ を計算し、メモリ 303 に格納する。

【0208】

上記の鍵配送処理により、データ暗復号化鍵 DK の配送が行われた後、暗復号化処理は、以下の要領で行う。

50

【0209】

1 送信者Aは、送信者側装置200内の暗復号化装置203を用いて、データ暗復号化鍵DKにより配信データPを暗号化し、通信装置205により受信者xに送信する。

【0210】

2 受信者xは、受信者側装置300内の通信装置305により暗号化された配信データPを受信する。そして、暗復号化装置303を用いて、受信した配信データPをデータ暗復号化鍵DKにより復号する。

【0211】

なお、送信者Aは、共通鍵 K_A の値を周期的に変更することで、データ暗復号化鍵DKの値を周期的に変更することができる。

10

【0212】

以上説明した本発明の第6実施形態によっても、受信者は、単一の秘密情報で、複数の送信者と、各送信者個々の共通鍵を共有することができる。

【0213】

次に、本発明の第7実施形態について説明する。

【0214】

本発明の第7実施形態は、上記の第6実施形態と同様、送信者と受信者が、受信者の個別の鍵を使った暗号通信により、共通の鍵を共有するものである。

【0215】

本実施形態に係る全体のシステム、鍵管理者側装置100、送信者側装置200、受信者側装置300の構成は、上述した本発明の第5実施形態のものと同様である。

20

【0216】

本発明の第7実施形態では、準備処理において、以下の処理を行う。

【0217】

(1) 準備処理

1 鍵管理者は、鍵管理者側装置100内の乱数生成器111、演算装置112を用いて、適当な公開鍵暗号Eに従った受信者xの秘密鍵 s_x および公開鍵 p_x を作成し、 s_x を受信者に配布する。さらに、乱数生成器111により送信者Aの番号 BID_A を作成し、送信者Aおよび受信者xに配布または送信する。

【0218】

2 送信者Aは、送信者側装置200内の乱数生成器201を用いて共通鍵 K_A を作成し、メモリ114に格納する。

30

【0219】

その後、鍵配送処理として、以下の処理を行う。

【0220】

(2) 鍵配送処理

1 送信者Aは、送信者側装置200内の暗復号化装置213を用いて、前記適当な公開鍵暗号Eにより、受信者公開鍵 p_x と共通鍵 K_A から鍵配送データ $K_{CX} = E(p_x, K_A)$ を計算する。その後、通信装置215により K_{CX} を受信者xに送信する。

【0221】

2 受信者xは、受信者側装置300内の暗復号化装置313を用いて、送信者Aから受信した鍵配送データ K_{CX} を自身の秘密鍵 s_x により復号化し、復号化した共通鍵 K_A をメモリ314に格納する。

40

【0222】

3 送信者Aは、送信者側装置200内の乱数生成器201を用いて適当な整数rを生成し、通信装置215により受信者xに送信する。また、演算装置212を用いて、整数rと共通鍵 K_A から、適当な関数Fによりデータ暗復号化鍵 $DK = F(r, K_A)$ を計算し、メモリ204に格納する。

【0223】

4 受信者xは、受信者側装置300内の演算装置312を用いて、共通鍵 K_A と送信

50

者から受信した整数 r から、関数 F によりデータ暗復号化鍵 $DK = (r, K_A)$ を計算し、メモリ 314 に格納する。

【0224】

上記の鍵配送処理により、データ暗復号化鍵 DK の配送が行われた後、暗復号化処理は、以下の要領で行う。

【0225】

(3) 暗復号化処理

1 送信者 A は、送信者側装置 200 内の暗復号化装置 203 を用いて、データ暗復号化鍵 DK により配信データ P を暗号化し、通信装置 205 により受信者 x に送信する。

【0226】

2 受信者 x は、受信者側装置 300 内の通信装置 305 を用いて、暗号化された配信データ P を受信する。そして、暗復号化装置 303 を用いて、受信した配信データ P をデータ暗復号化鍵 DK により復号化する。

【0227】

3 送信者 A は、共通鍵 K_A の値を周期的に変更することによりデータ暗復号化鍵 DK を変更する。

【0228】

以上説明した本発明の第7実施形態によっても、受信者は、単一の秘密情報で、複数の送信者と、各送信者個々の共通鍵を共有することができる。

【0229】

次に、本発明の第8実施形態について説明する。

【0230】

本発明の第8実施形態は、上述した本発明の第6および第7実施形態において、送信者による鍵配送データ K_{Cx} の受信者への送信を、以下のように修正したものである。

【0231】

すなわち、第8実施形態では、送信者 A は、受信者全体の集合をいくつかの部分集合にわけ、次に、鍵配送データ K_{Ci} ($1 \leq i \leq n$ ただし、 n は受信者数) を受信者に送信する際、前記受信者の部分集合毎に通信チャンネルを割り当て、送信者側装置 200 内の通信装置 215 により受信者に送信する。

【0232】

一方、任意の受信者 x は、自身の属する部分集合に割り当てられた通信チャンネルを通じて、受信者側装置 300 内の通信装置 305 により、鍵配送データ K_{Cx} を受信する。

【0233】

以上、本発明の第8実施形態について説明した。

【0234】

次に、本発明の第9実施形態について説明する。

【0235】

本実施形態に係る全体のシステム、鍵管理者側装置 100、送信者側装置 200、受信者側装置 300 の構成は、上述した本発明の第1実施形態のものと同様である。

【0236】

以下、本システムが行う準備処理、鍵配送処理、そして暗復号化処理の3つの処理について説明する。

【0237】

では、まず、準備処理について説明する。

【0238】

(1) 準備処理

1 送信者 A は、送信者側装置 200 内の乱数生成器 201、素数生成器 202、べき乗算器 203、剰余演算器 204、および演算装置 205 を用いて、次の情報を作成し、そのうち、公開情報のみを公開する。

【0239】

10

20

30

40

50

秘密情報：

【 0 2 4 0 】

【 数 1 4 5 】

数145

P_A, Q_A : 素数

$$L_A = \text{lcm}(\text{ord}_{P_A}(g_A), \text{ord}_{Q_A}(g_A))$$

10

$$g_A \in \mathbb{Z}, \quad 0 < g_A < N_A$$

【 0 2 4 1 】

公開情報：

【 0 2 4 2 】

【 数 1 4 6 】

20

数146

$$N_A (= P_A Q_A)$$

【 0 2 4 3 】

秘密情報はメモリ 206 に格納する。また、秘密情報 g_A 、 L_A を通信装置 207 を用いて鍵管理者に送信する。

【 0 2 4 4 】

30

2 信頼できる鍵管理者は、鍵管理者側装置 100 内の演算装置 105 を用いて、次の情報を作成する。

【 0 2 4 5 】

鍵管理者秘密情報：

【 0 2 4 6 】

【 数 1 4 7 】

数147

$$\bullet e_i \in \mathbb{Z} \quad (1 \leq i \leq m)$$

40

【 0 2 4 7 】

送信者 A の送信者識別情報：

【 0 2 4 8 】

【 数 1 4 8 】

数148

$$\bullet t_A \in \mathbb{Z}, \quad 0 < t_A < L_A$$

【0249】

受信者 x の受信者秘密情報：

【0250】

【数149】

10

数149

$$\bullet s_x(\sigma_x) \in \mathbb{Z}, \quad 0 < t_A < L_A$$

【0251】

これらは、 x とともに全てメモリ106に格納する。

【0252】

ただし、集合

【0253】

【数150】

20

数150

$$S_{km} = \{\sigma \mid 1 \text{ 対 } 1 \text{ 写像 } \sigma : A = \{1, 2, \dots, k\} \rightarrow B = \{1, 2, \dots, m\}, 0 < k < m\}$$

【0254】

に対して、 $\sigma, \sigma' \in S_{km}$ のとき、

【0255】

【数151】

30

数151

$$\sigma \sim \sigma' \stackrel{\text{def}}{\iff} \sigma(A) = \sigma'(A)$$

【0256】

とする。このとき、 \sim は S_{km} 上の同値関係となり、

【0257】

【数152】

40

数152

$$\tilde{S}_{km} = S_{km} / \sim$$

【0258】

とする。

【0259】

50

また、鍵管理者は、メモリ106から受信者秘密情報 $s_x(x)$ を取り出し、 x とともに受信者側携帯装置306に格納し、これを受信者 x にオフラインで配布する。もちろん、他の方法によって受信者に配布するようにしてもよい。

【0260】

次に、鍵配送処理について説明する。

【0261】

(2) 鍵配送処理

1 鍵管理者は、鍵管理者側装置100内の剰余演算器104、演算装置105を用いて、送信者Aから受信した L_A と、鍵管理者秘密情報 e_i と、受信者秘密情報 $s_x(x)$ と、送信者識別情報 t_A から、

【0262】

【数153】

数153

$$\rho_x(\sigma_x(i), A) = t_A s_x(\sigma_x) e_{\sigma_x(i)} \bmod L_A \quad (1 \leq i \leq k)$$

【0263】

なる受信者 x の受信者識別データ $\rho_x(x(i), A)$ を計算し、通信装置107を用いて送信者Aに送信する。

【0264】

また、鍵管理者は、鍵管理者側装置100内のべき乗算器103、剰余演算器104、演算装置105を用いて、送信者Aから受信した g_A と、送信者Aの送信者公開情報 N_A と、鍵管理者秘密情報 e_i から、

【0265】

【数154】

数154

$$y_{Ai} = g_A^{t_A e_i} \bmod N_A \quad (1 \leq i \leq m)$$

【0266】

なる送信者Aの送信者鍵配送データ y_{Ai} を計算し、通信装置107を用いて送信者Aに送信する。

【0267】

2 送信者Aは、送信者側装置200内の乱数生成器201により、乱数 r 、 r' を作成しメモリ206に格納する。さらに、べき乗算器203、剰余演算器204、演算装置

【0268】

【数155】

数155

$$K_A = g_A^{rr'} \bmod N_A$$

【0269】

10

20

30

40

50

なるデータ暗号化鍵 K_A を計算してメモリ 206 に格納し、受信者 x との間で鍵 K_A を共有することを目的として、剰余演算器 204、演算装置 205 を用いて、自身の秘密情報 L_A と、乱数 r' と、鍵管理者から受信した受信者 x の受信者識別データ $r_x(\sigma_x(i), A)$ から、

【0270】

【数156】

数156

$$\sum_{i=1}^k r_x(\sigma_x(i), A) \rho_x(\sigma_x(i), A) \equiv r' \pmod{L_A}$$

10

【0271】

なる受信者 x の受信者識別情報 $r_x(\sigma_x(i), A)$ を計算し、通信装置 207 を用いて受信者 x に送信する。

【0272】

また、送信者 A は、送信者側装置 200 内のべき乗算器 203、剰余演算器 204、演算装置 205 を用いて、自身の公開情報 N_A と、乱数 r と、鍵管理者から受信した送信者鍵配送データ y_{Ai} から、

20

【0273】

【数157】

数157

$$z_{Ai} = y_{Ai}^r \pmod{N_A} \quad (1 \leq i \leq m)$$

【0274】

なる受信者鍵配送データ z_{Ai} を計算し、通信装置 207 を用いて受信者に同報送信する。

【0275】

ここで、以上の処理において、 $r_x(\sigma_x(i), A)$ 、 z_{Ai} を作成する処理の一部を、鍵管理者が行う理由の一つは、送信者 A に対して、受信者 x の受信者秘密情報 $s_x(\sigma_x(i))$ 、送信者識別番号 t_A を秘密にすることにより、送信者 A の不正を防止するためである。

30

【0276】

3 受信者 x は、送信者 A から受信した鍵配送データ z_{Ai} および受信者識別情報 $r_x(\sigma_x(i), A)$ 、鍵管理者から配送された受信者秘密情報 $s_x(\sigma_x(i))$ 、公開された送信者公開情報 N_A から、

【0277】

【数158】

40

数158

$$K_A = \left(\prod_{i=1}^k z_{A\sigma_x(i)}^{r_x(\sigma_x(i), A)} \right)^{s_x(\sigma_x(i))} \pmod{N_A}$$

【0278】

により、データ暗号化鍵 K_A を計算し、メモリ 304 に格納する。

50

【0279】

以上の処理で、送信者Aと受信者xは鍵 K_A を共有できる。他の任意の送信者と受信者についても同様にして鍵を共有できる。また、この際、送信者Aが同報送信する受信者鍵配送データ z_{Ai} は、各受信者について共通である。

【0280】

また、以上の処理において、受信者xが送信者Aより受けとる鍵配送データ z_{Ai} および受信者識別情報 $r_x(x(i), A)$ は、受信者に対して秘密化されている送信者Aの送信者識別番号 t_A が作用したものとなっている。したがって、以上の送信者識別番号 t_A を用いる構成により、受信者xが送信者Aより受けとった鍵配送データ z_{Ai} 、受信者識別情報 $r_x(x(i), A)$ 、他の送信者Bの公開情報 N_B 、他の送信者Bが同報通信した鍵配送データ z_{Bi} より、他の送信者Bのデータ暗号化鍵 K_B を割り出すことを、きわめて困難とすることができる。

10

【0281】

以下、暗復号化処理について説明する。

【0282】

(3) 暗復号化処理

1 送信者Aは、送信者側装置200内の暗復号化装置208を用いて、鍵配送処理で作成した共通鍵 K_A により、データPを暗号化する。そして、暗号文 $C = E(K_A : P)$ を通信装置207を用いて受信者xに送信する。

【0283】

2 受信者xは、受信者側装置300内の通信装置305を用いて暗号文Cを受信し、暗復号化装置307を用いてメモリ304に格納していた共通鍵 K_A により暗号文Cを復号化し、データを得る。

20

【0284】

以上、本発明の第9実施形態について説明した。

【0285】

本実施形態に係る鍵配送システムにおいても、上述した第1実施形態と同様、新規参入の送信者Aは、送信者秘密情報 P_A 、 Q_A 、 L_A 、 g_A と、送信者公開情報 N_A を作成するだけでよい。また、受信者が持つ受信者秘密情報は、全ての送信者に対して唯一であり、新たな送信者からデータを受信したい場合に、新たな受信者秘密情報を入手する必要がない。

30

【0286】

また、受信者識別情報 $r_x(x(i), A)$ によって、任意の受信者集合に属する受信者のみとのデータ暗復号のための共通鍵の共有を可能とすることができる。また、受信者数が多い場合であっても、共通鍵配送のために同報通信する鍵配送データ z_{Ai} を、これに伴い長くする必要がない。

【0287】

なお、以上の処理において、あらかじめ、送信者Aが送信者秘密情報 L_A を鍵管理者に送信しておき、準備処理の段階で、鍵管理者は、送信者Aから受信した送信者秘密鍵 L_A から、

【0288】

40

【数159】

数159

$$e_i \in \mathbb{Z}, \quad 0 < e_i < L_A, \quad (1 \leq i \leq m)$$

$$t_A \in \mathbb{Z}, \quad 0 < t_A < L_A$$

$$s_x(\sigma_x) \in \mathbb{Z}, \quad 0 < s_x(\sigma_x) < L_A$$

10

【0289】

となる鍵管理者秘密情報 e_i 、送信者識別情報 t_A 、受信者秘密情報 $s_x(\sigma_x)$ を作成し、鍵配送処理の段階で、鍵管理者は、送信者秘密情報 L_A 、鍵管理者秘密情報 e_i 、送信者識別情報 t_A 、受信者秘密情報 $s_x(\sigma_x)$ から、

【0290】

【数160】

数160

20

$$\rho_x(\sigma_x(i), A) = t_A s_x(\sigma_x) e_{\sigma_x(i)} \bmod L_A \quad (1 \leq i \leq k)$$

【0291】

によって、受信者識別データ $\rho_x(\sigma_x(i), A)$ を計算するようにしてもよい。

【0292】

次に、本発明の第10実施形態について説明する。

【0293】

30

本発明の第10実施形態は、上記の第9実施形態において、受信者側装置300におけるデータ暗号化鍵 K_A の計算処理の一部を、受信者側携帯装置306で実施するようにしたものである。本実施形態で用いる受信者側携帯装置306の構成は、上述した本発明の第2実施形態のものと同様である。

【0294】

本実施形態では、(1)準備処理の段階で、鍵管理者は受信者秘密情報 $s_x(\sigma_x)$ を、受信者携帯装置306(ICカード等)に格納して、受信者 x に配布する。

【0295】

そして、(2)鍵配送処理において、受信者 x は、受信者側装置300内のメモリに格納されている鍵配送データ z_{A_i} を受信者携帯装置306に出力する。次に、受信者携帯装置306内で、べき乗算器3064、剰余演算器3063を用いて、受信者秘密情報 $s_x(\sigma_x)$ 、鍵配送データ z_{A_i} および送信者公開情報 N_A から、

40

【0296】

【数161】

数161

$$\xi_x(\sigma_x(i), A) = z_{A\sigma_x(i)}^{s_x(\sigma_x)} \bmod N_A \quad (1 \leq i \leq k)$$

【0297】

を計算し、この計算結果 $\xi_x(\sigma_x(i), A)$ を受信者側装置300に出力する。

10

【0298】

次に、受信者側装置300内のべき乗算器301、剰余演算器302、演算装置303を用いて、受信者側装置300に出力された $\xi_x(\sigma_x(i), A)$ と、メモリ304に格納している受信者識別鍵 $r_x(\sigma_x(i), A)$ および送信者公開情報 N_A から、

【0299】

【数162】

数162

$$K_A = \prod_{i=1}^k \xi_x(\sigma_x(i), A)^{r_x(\sigma_x(i), A)} \bmod N_A$$

20

【0300】

により、データ暗号化鍵 K_A を計算し、メモリ304に格納する。

【0301】

このように受信者秘密情報 $s_x(\sigma_x)$ が受信者側携帯装置306外部に出力しないようにすることにより、これが電子的複写などにより盗難されることを防ぐことができる。

30

【0302】

以上、本発明の第10実施形態について説明した。

【0303】

次に、本発明の第11実施形態について説明する。

【0304】

本発明の第11実施形態は、上記の第9実施形態において、

【0305】

【数163】

数163

$$K_A = g_A^{rr'} \bmod N_A$$

40

【0306】

の r の値を短時間毎に、周期毎に変更し、変更後の r を用いた z_{A_i} を周期的に同報通信することにより、送信者側装置200および受信者側装置300で計算するデータ暗復号化鍵 K_A の更新を行うものである。

【0307】

50

また、 r' の値を送信データ固有の値とすることで、送信者が同報送信するデータの識別を行うようにしたものである。すなわち、受信者 x がある同報データもしくは同報データの集合を復号するために、ある送信者から得た識別鍵 $r_x(x(i), A)$ はその同報データ固有のものであり、別の同報データもしくは同報データの集合を取得するためには、その送信者から別の同報データもしくは同報データの集合用の別の $r_x(x(i), A)$ を得る必要がある。

【0308】

以上、本発明の第11実施形態について説明した。

【0309】

次に、本発明の第12実施形態について説明する。

10

【0310】

本発明の第12実施形態は、上記の第9実施形態において、特定の受信者の認証を行い、送信者が鍵 K_A を用いて暗号化し送信した有償のデータ P に対する、鍵 K_A を共有する受信者への課金を行うものである。

【0311】

すなわち、第12実施形態では、さらに、以下の処理を行う。

【0312】

(1) 準備処理

1 鍵管理者は、鍵管理者側装置100内の演算装置105を用いて、予め受信者 x の番号 UID_x を作成し、これを受信者秘密情報 $s_x(x)$ と一緒に受信者携帯装置306内のメモリ3061に格納して配布する。また、 UID_x を、 $s_x(x)$ と対応させて、鍵管理者側装置100内のメモリ106に格納しておく。

20

【0313】

2 送信者 A は、送信者側装置200内の演算装置205を用いて、自身の番号 $BI D_A$ を作成し、メモリ206に格納しておく。また、 $BI D_A$ を通信装置207を用いて鍵管理者に送信する。

【0314】

3 鍵管理者は、鍵管理者側装置100内の通信装置107によって送信者 A の番号 $BI D_A$ を受信し、メモリ106に送信者識別情報 t_A と対応させて格納する。

【0315】

4 受信者 x は、受信者側装置300内の認証装置308を用いて、受信者秘密情報 $s_x(x)$ から認証用の情報を作成し、送信者 A に送信する。

30

【0316】

5 送信者 A は、該認証用の情報を、送信者側装置200内の認証装置209によって確認する。

【0317】

この認証の方法は、上述した本発明の第4実施形態と同様、受信者が $s_x(x)$ を知らない限り、認証が成立しない認証方法であれば、従来知られている各種認証方式を用いてかまわない(ただし、このとき、送信者は受信者秘密鍵 $s_x(x)$ 自体は知ることができないようにする必要がある)。

40

【0318】

6 さて、認証を行った後に、送信者 A は、送信者側装置200内の通信装置207を用いて、自身の番号 $BI D_A$ と受信者 x の番号 UID_x を鍵管理者に送信する。

【0319】

7 鍵管理者は、鍵管理者側装置100内の演算装置105を用いて、受信した送信者番号 $BI D_A$ と受信者番号 UID_x に対応した、送信者識別鍵 t_A と受信者秘密情報 $s_x(x)$ から、

【0320】

【数164】

数164

$$\rho_x(\sigma_x(i), A) = t_A s_x(\sigma_x) e_{\sigma_x(i)} \bmod L_A \quad (1 \leq i \leq k)$$

【0321】

となる受信者識別データ $x(\sigma_x(i), A)$ を計算し送信者 A に送信する。

【0322】

8 送信者 A は、送信者側装置 200 内の剰余演算器 204、演算装置 205 を用いて、鍵管理者から受信した受信者識別データ $x(\sigma_x(i), A)$ から、

【0323】

【数165】

数165

$$\sum_{i=1}^k r_x(\sigma_x(i), A) \rho_x(\sigma_x(i), A) \equiv r' \pmod{L_A}$$

【0324】

となる受信者識別情報 $r_x(\sigma_x(i), A)$ を計算し、通信装置 207 により受信者 x に送信する。その際、共通鍵 K_A によって、暗号化して配信するデータ（受信者が送信要求したデータ）が有償の場合、送信者 A は、課金装置 210 を用いて受信者 x に対して課金する。

【0325】

以上、本発明の各実施形態について説明した。

【0326】

なお、以上に説明した鍵管理者側装置 100、送信者側装置 200、受信者側装置 300 の各処理は、コンピュータに各処理を実行させる手順を記述したプログラムを実行させることにより実現するようにしてもよい。この場合、各処理を実行させる手順を記述した各プログラムは、記憶媒体に格納して各コンピュータに供給するようにしてもよい。あるいは、ネットワークなどの通信媒体を介して各コンピュータに供給するようにしてもよい。

【0327】

【発明の効果】

以上説明したように、本発明によれば、受信者が唯一の秘密情報によって、複数の送信者から個々の共通鍵の配送を受けることができる。また、一部の発明においては、このような鍵配送システムにおいて、任意の送信者と任意の受信者集合に属する受信者のみとのデータ暗復号のための共通鍵の共有を可能とすることができる。また、受信者数が大きい場合であっても、これに伴い共通鍵配送のための同報通信データを長くする必要がなくなる。

【図面の簡単な説明】

【図1】本発明の第1実施形態に係る鍵配送システムの構成を示すブロック図である。

【図2】本発明の第1実施形態に係る鍵管理者側装置の構成を示すブロック図である。

【図3】本発明の第1実施形態に係る送信者側装置の構成を示すブロック図である。

【図4】本発明の第1実施形態に係る受信者側装置の構成を示すブロック図である。

【図5】本発明の第1実施形態における鍵配送処理による情報の流れを示した図である。

【図6】本発明の第2実施形態に係る受信者側携帯装置の構成を示すブロック図である。

10

20

30

40

50

【図7】本発明の第5実施形態に係る鍵管理者側装置の構成を示すブロック図である。

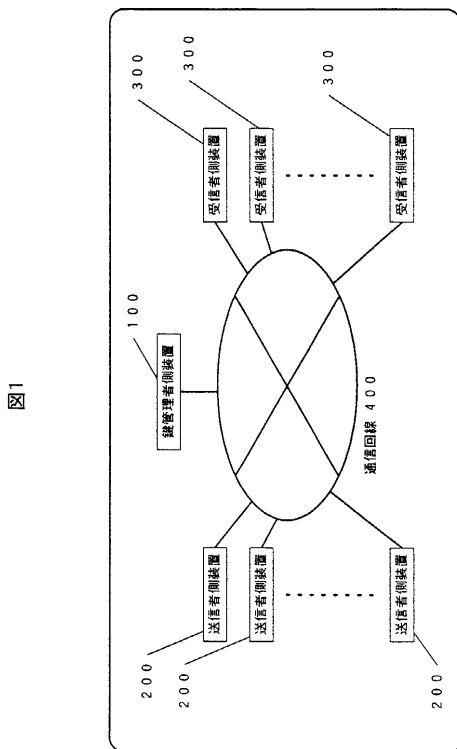
【図8】本発明の第5実施形態に係る送信者側装置の構成を示すブロック図である。

【図9】本発明の第5実施形態に係る受信者側装置の構成を示すブロック図である。

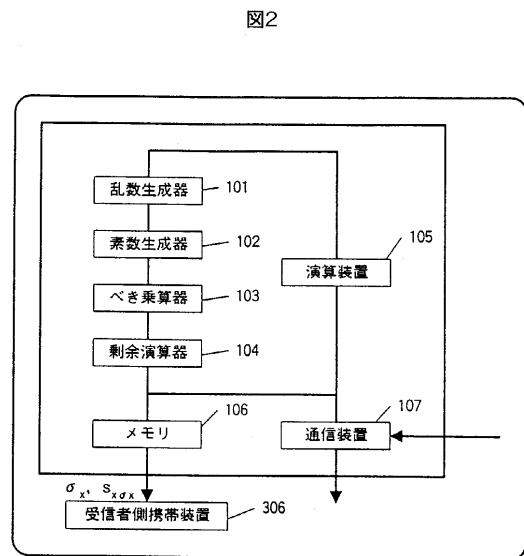
【符号の説明】

- 100 鍵管理者側装置
- 101、111、201、211、311 乱数生成器
- 102、202 素数生成器
- 103、203、301、3064 べき乗算器
- 104、204、302、3063 剰余演算器
- 105、112、205、212、303、312、3061 演算装置
- 106、113、206、214、304、314、3062 メモリ
- 107、114、207、215、305、315 通信装置
- 200 送信者側装置
- 208、213、307、313 暗復号化装置
- 209、308 認証装置
- 210 課金装置
- 300 受信者側装置
- 306 受信者側携帯装置

【図1】

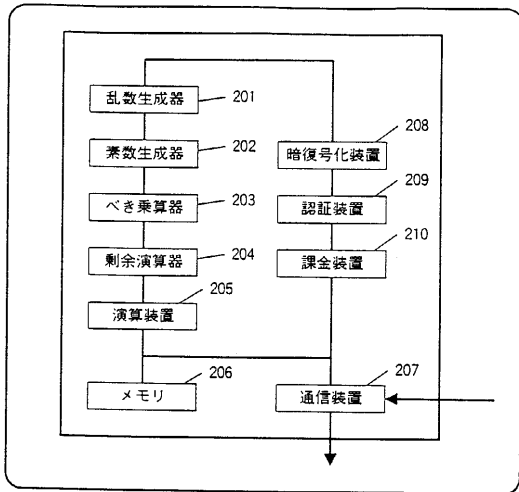


【図2】



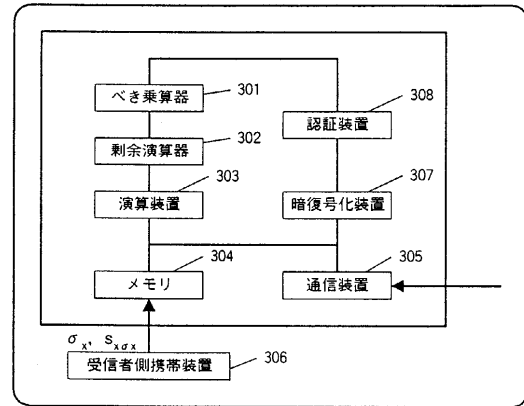
【 図 3 】

図3



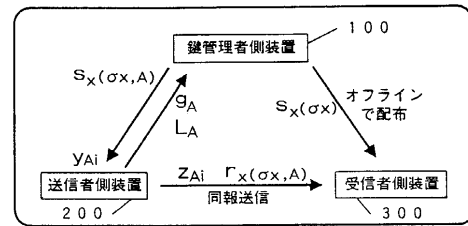
【 図 4 】

図4



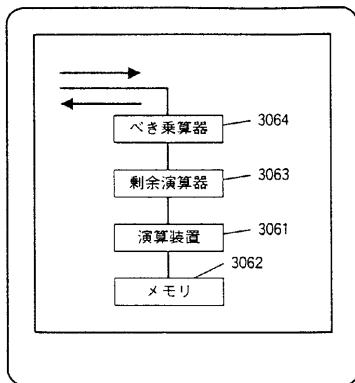
【 図 5 】

図5



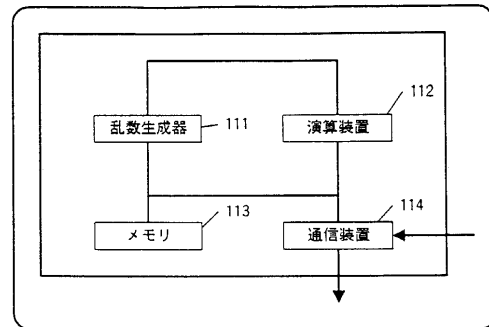
【 図 6 】

図6



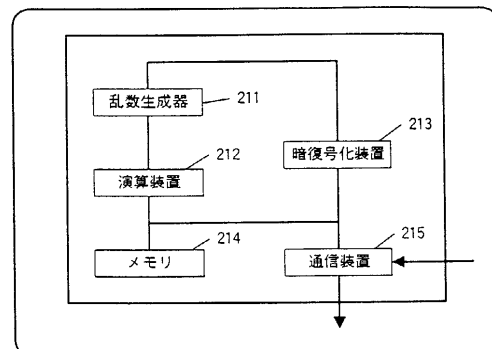
【 図 7 】

図7



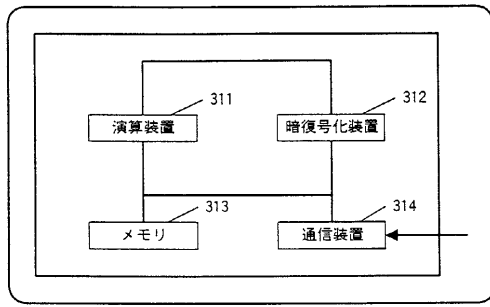
【 図 8 】

図8



【 図 9 】

図9



フロントページの続き

(72)発明者 松井 進

神奈川県川崎市麻生区王禅寺1099番地 株式会社日立製作所 システム開発研究所内

審査官 石田 信行

(56)参考文献 特開平08-087235(JP,A)

特開平01-177229(JP,A)

特開平06-202558(JP,A)

特開平10-164045(JP,A)

特開平08-097813(JP,A)

特開平03-082239(JP,A)

特開平03-016339(JP,A)

特開平02-054644(JP,A)

特開昭63-070634(JP,A)

(58)調査した分野(Int.Cl.⁷, DB名)

H04L 9/08

G09C 1/00