アルゴリズム 4－9
（1988. 11. 25）

ＩＤ情報に基づく暗号鍵配送方式とその実現
―電子会議セキュリティシステムへの応用―

岡本栄司　　田中和恵

日本電気株式会社　Ｃ＆Ｃ情報研究所

最近、情報セキュリティの分野ではネットワークの大規模化に伴う暗号鍵管理の複雑化を克服する方式として、各ユーザの氏名などのＩＤ情報に基づく暗号鍵配送方式が話題になっている。そこで本報告では、その背景、原理、代表的アルゴリズムを紹介し、さらにその中から著者が提案したアルゴリズムを電子会議に適用した電子会議セキュリティシステムを示す。本システムでは単に鍵配送のみならず、音声ブレンディングも考慮した暗号化アルゴリズムを含む。音声ブレンディングとは、異なる場所からの音声を全て加算して各端末へ音声信号として送ることであり、暗号化に際しては工夫を要する。

ID-based Encryption Key Distribution Systems and Its Application
— Electronic Conference Security Systems —

Eiji OKAMOTO,　Kazue TANAKA

C&C Information Technology Research Laboratories, NEC Corporation

4-1-1, MIYAZAKI, MIYAMAE-KU, KAWASAKI, JAPAN 213

Recently, key-distribution systems based on identification information, such as names of each user, are brought up for discussion in the field of information security. They overcome growing intricacy of key management for encryption caused by enlargement of networks. This paper first summarizes its background, its principle and some of major algorithms. Then we propose a security system on electrical conferences, adopting one of the ID-based key-distribution system we introduced. The system has not only key-distribution function but also encryption algorithm considering voice blending. Voice blending is to accumulate all voices from different zones and send them to each terminal as a voice signal, and requires contrivances to encrypt.

１．はじめに

最近、情報ネットワークの進展に伴い、情報セキュリティの重要性が高まっている。情報に対するセキュリティとしては秘匿、認証が中心課題であるが、基本メカニズムとして暗号アルゴリズムが用いられる。暗号化ではパラメータとして鍵（キー）を使用する。暗号化の強さ・安全性をこの鍵に帰着させるのが現代の暗号化技術の特徴となっている。従って送信側と受信側で鍵さえ安全に管理すればよいことになる。ところがネットワークが大規模化すると、相手ユーザ毎に鍵を持つと鍵のディレクトリは膨大な量になる。また新たにユーザが加わるたびにそのディレクトリの更新が必要となる。そこで簡単に鍵を配送するとして、この数年来ＩＤ情報に基づく鍵配送方式が盛んに研究されている。ＩＤ情報とは、ユーザの名前等そのものであり、これを鍵の代わりに用いる方式である。当然、名前は誰でも知り得るのでそのまま従来の暗号化方式の鍵として使用しては秘密性が保てなくなる。そこで秘密性を保ちながら名前そのものを利用する方式が幾つか提案されてきた。

本報告では、ＩＤ情報に基づく鍵配送方式について、その紹介の意味を含めて生まれた背景、基本原理をまず述べ、次に代表的アルゴリズム例を与える。さらにその例の中から我々が提案したアルゴリズムを電子会議に適用した、電子会議セキュリティシステムを示す。電子会議には音声ブレンディングという暗号化とは相性の悪いメカニズムがある。即ち、離れた場所から発した複数の音声を数値的に全て加算し、各端末に送るものである。各人の音声を暗号化しておくと、ブレンディングする際に一旦元に戻してから加算し、再び暗号化するという操作が必要となる。そこで、その操作の不要な暗号化方式例も与え、その暗号の鍵は上記のＩＤ情報に基づく鍵配送方式により行なうという、電子会議セキュリティシステムを示す。なお、本報告はできる限りSelf-containedにまとめた。

２．ＩＤ情報に基づく鍵配送方式

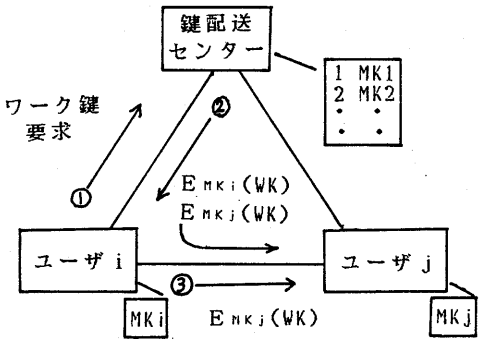
２．１　生まれた背景

暗号化のための鍵あるいは認証のためのコードを管理する方法として従来から知られていた方式は図１に示す２通りである。図１は暗号化の例を示している。

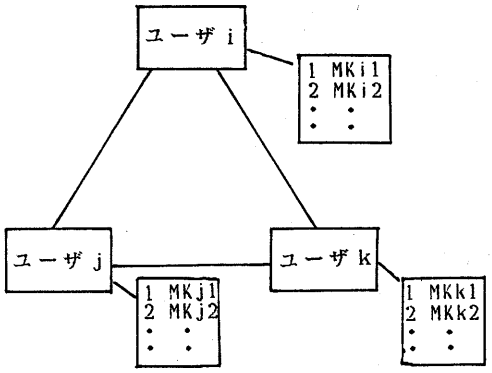
（ａ）は集中型鍵配送方式例[1]で、ユーザｉがユーザｊと暗号通信を行なう場合を想定している。各ユーザは自分と鍵配送センターとの間の鍵配送用鍵MKを秘密に保持し、鍵配送センターは全ての鍵配送用鍵を保有している。ユーザｉは、まずセンターへユーザｊとの間の暗号通信用鍵を要求する。するとセンターはランダムに鍵WKを生成しユーザｉとユーザｊに渡す。この際、WKを裸で渡しては第三者に漏れてしまうのでユーザｉには鍵 MKｉ（これが鍵配送用鍵）で暗号化したE_{MKi}(WK)を渡し、ユーザｊには同様にE_{MKj}(WK)を渡す。ここでE_{MK}( )はMKを鍵パラメータとする暗号化変換を示す。WKは使い捨て鍵であり、こうすることにより安全性が高まる。この集中型鍵配送方式では各ユーザは１つの秘密情報MKを持つだけでよいのでメモリ量は少なくてすむが、暗号通信のたびに通信相手とは異なるセンターに問い合わせる必要があるため、通信コストがかかる欠点がある。

図１の（ｂ）は分散型鍵配送方式例で、各ユーザは他ユーザとの間の鍵を

全て保有している[2]。この方式でも実際には暗号通信用鍵WKを当事者の一方がランダムに生成し、保管している鍵MKijを用いて暗号化したEMKij(WK)を相手に送るのが普通である。この分散型鍵配送方式では各ユーザの鍵ディレクトリが加入ユーザに比例して大きくなり、メモリコストがかかる。また新規ユーザ加入に際し、各ユーザの鍵ディレクトリの変更が必要となる。



(a) 集中型鍵配送方式例



(b) 分散型鍵配送方式例

図1　鍵配送方式

これらの方式の欠点は、公開鍵暗号系[3][4]を用いても解消しない。公開鍵暗号系は、暗号鍵と復合鍵を異なる鍵とし、一方の鍵をオープンにしても他方の鍵はわからないようにした暗号系である。数学的には両者は対応しているが実際上、計算が困難である。従って暗号鍵を電話帳のように公開しておき、対応する復号鍵は各人が秘密に保持すればよいことになる。例えばAがBにメッセージを送る場合には、Aは公開鍵ディレクトリから得たBの暗号鍵で暗号化してBに送り、Bは自分だけが持つ秘密鍵で復号する。逆に、復号鍵をオープンにして暗号鍵を秘密にした場合には所謂「ディジタル署名」が実現できる。即ち、送信者はメッセージに適当に冗長性を入れてから暗号化して相手に送り、受信者はそれを公開されている復号鍵で元に戻した時に正しく冗長性が入っていれば、真に正しい送信者から送られたと判定する。暗号鍵はその送信者のみ知っているため、正しく冗長性を入れられるのは送信者のみだからである。いずれの場合においても公開鍵ディレクトリは秘密にする必要は無い。しかしどこかで管理する形にすると(a)の集中型と同様の欠点を有し、各人が持つことにすると(b)の分散型と同様の欠点を有することになる。そこで各人が自分の公開鍵と秘密鍵を保持し、実際に通信を行なう直前に当事者が各自の公開鍵を送りあうことが考えられる。しかし、公開鍵から秘密鍵は計算できなくても、全く別な公開鍵と秘密鍵の対を計算することは誰でも可能である。従ってこの新たに発生した公開鍵を送られると、受け側ではその正当性を確認できなくなる。

これらの欠点を取り除く方式としてID情報に基づく鍵配送方式(ID-based KDS)は生まれた。

２．２　代表的な例

ここでは現時点で安全とみられている代表例を発表順に示す。なお、鍵配送法以外も簡単に触れる。

（ａ）公開鍵証明書[5]

１９７８年、L.Kohnfelderによって提案された。あらかじめ信頼できる管理機関が公開鍵暗号系の暗号鍵にディジタル署名を行なっておく。各人はこの署名付暗号鍵と対応する復号鍵を所持し、実際の通信に先だってこの暗号鍵を送りあう。第三者が勝手に使った暗号鍵には管理機関のディジタル署名がないので不正が判明できる。

（ｂ）対称鍵生成システム[6]

１９８４年にR.Blomが提案したＩＤ情報に基づく鍵生成法である。しきい値法を利用している。信頼できる管理機関は秘密の対称行列Ｄを持ち、あらかじめ各ユーザに$s_i = g_i \cdot D$を配布しておく。ここでg_iはユーザｉの行ベクトルで表わされたアドレスで、ID_iあるいはその変形である。ユーザｉとユーザｊの間の通信に際してはユーザｉは鍵を$s_i \cdot g_j^T$から得る。この鍵はs_iの定義から$g_i \cdot D \cdot g_i^T$に等しいのでユーザｊも得られる。ところでＤの次数をｋとすると、ｋ人が結託すると$g \cdot D = s$をｋ個集めることによりＤが求められる。従ってｋ－１人以下の結託しかあり得ないとすれば、安全とみられる。しきい値法を用いた方式は幾つか提案されている[7,8,9]。

（ｃ）ID-based Signature System[10]

１９８４年にA.Shamirが提案したＩＤ情報に基づく認証方式である。このとき、ID-based Cryptosystemの概念が初めて世に発表されたと言われているが、実際には今まで見てきたように前から似た考えはあった。ＩＤ情報に基づく認証方式としては他に岡本龍明が１９８６年に双方向通信を必要とするタイプであるが提案している[11]。さらに１９８６年にA.FiatとA.Shamirは、相手に秘密情報を全く漏らさずに（証明付）、認証を行なう方式を提案している[12]。

（ｄ）ID-based KDS[13]

１９８６年に著者が提案したＩＤ情報に基づく鍵配送方式である。現在までに適用環境に応じて数種類の方式が示されているが[14,15,16,17,18,19]、ここでは後の電子会議に用いる、最も基本的な型を示す。図２はそのプロトコルを表わしている。信頼できる管理センターは、大きな素数（２５６ビット程度）のｐ，ｑを生成し、

$$e \cdot d = 1 \pmod{(p-1)\cdot(q-1)} \quad (1)$$

を満たすｅ、ｄを求めておく。さらに、GF(p)、GF(q)で原始元となるようなαを定めておく。ユーザｋがネットワークに加入するときには、管理センタはユーザｋの身元を何らかの手段で確認した後、ユーザｋに(n, α, e, s_K)を渡す。ここで、

$$s_K = ID_k^{-d} \pmod{n} \quad (2)$$

$$n = p \cdot q \quad (3)$$

である。さて、実際にユーザｉとユーザｊが暗号用鍵を手に入れるには、ユーザｉは乱数r_iを生成し、

$$x_i = s_i \cdot \alpha^{r_i} \pmod{n} \quad (4)$$

をユーザｊに送り、ユーザｊも同様に乱数r_jを生成し、

$$x_j = s_j \cdot \alpha^{r_j} \pmod{n} \quad (5)$$

をユーザｉに送る。ユーザｉは、x_jを受け取ると

$$WK_i = (x_j^e \cdot ID_j)^{r_i} \pmod{n} \quad (6)$$

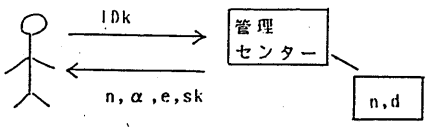
により鍵を得る。WK_iは実際には

$$WK_i = (s_j^e \cdot \alpha^{e r_i} \cdot ID_j)^{r_i} \pmod{n}$$

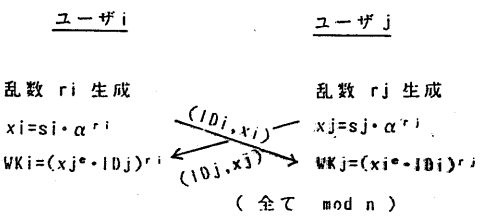
$$= \alpha^{e \cdot r_i \cdot r_j} \pmod{n} \quad (7)$$

なのでユーザｊの得たWK_jに等しい。

本方式の特長はそのシンプルさにある。



(a)ユーザ加入フェーズ



(b)鍵配送フェーズ

図2 ID-based KDS

(e)物理的セキュリティに依存する方式

物理的にメモリ内容を読めない構造のハードウェアがあれば、簡単にID情報に基づく鍵配送方式が作れることは以前から常識になっている。例えば、ネットワーク全体で1つのキーMKを定めてICカードに格納し、所有者にも認めないようにしておいて、ユーザiとユーザjの間の鍵WKを

$$WK=E_{MK}(ID_i * ID_j) \qquad (8)$$

のように作成する。ここで*はある対称演算を表わす。

しかし、この意味で実際に安全なハードウェアが存在するか否かは不明である。

3. 電子会議セキュリティシステム

電子会議あるいはTV会議のセキュリティを保つために考慮すべき事項は、2点ある。

(a) ネットワークの任意の端末から成るグループへの鍵の配布。

(b) 音声ブレンディング[20]を考慮した音声暗号方式。

但し、パソコン通信における電子会議のようなテキスト形態ではブレンディングの問題は生じないので、(a)のみが課題となる。

3.1 鍵の配布

ネットワーク加入者には、全員ICカードが配られているものとする。このICカードには、図2の加入フェーズ(a)の情報が書き込まれている。前記2.2の(d)で示したID-based KDSをほぼそのまま用いる。電子会議の発起人は乱数r_0、WKを生成し、全会議メンバに

$$x_0=s_0\cdot\alpha^{r_0}(\mathrm{mod}\ n) \qquad (9)$$

を送る。ここでr_0は乱数、発起人はユーザ0とした。会議メンバiはx_0を受け取ると乱数r_iを生成し、

$$x_i=s_i\cdot\alpha^{r_i}(\mathrm{mod}\ n) \qquad (10)$$

を返送し、

$$K_i=(x_0^e\cdot ID_0)^{r_i}(\mathrm{mod}\ n) \qquad (11)$$

を計算しておく。発起人はx_iを受け取ると

$$K_i=(x_i^e\cdot ID_i)^{r_0}(\mathrm{mod}\ n) \qquad (12)$$

からK_iを求め、

$$y_i=WK\cdot K_i^2 \ (\mathrm{mod}\ n) \qquad (13)$$

をメンバiに送る。メンバiはy_iを受け取って

$$WK=y_i / K_i^2(\mathrm{mod}\ n) \qquad (14)$$

を得る。式(10)-(13)を各メンバと行なうことによりWKを全メンバが共有できる。以上を図示したのが図3である。

発起人は各メンバと式(12)、(13)を実行しなければならないが、ソフトウェア的には同一でよい。

(注) 式(13)は1例である。任意の暗号化変換Eを用いて$y_i=E_{K_i}(WK)$としてもよい。

３．２　暗号化アルゴリズム

実際の情報の暗号化アルゴリズムは対象により異なる。映像やテキストに対してはそれぞれ適した従来の暗号に鍵WKを用いればよい。音声については、図４に示すようなブレンディング処理があるため一考を要する。対策には２通りあるが、それぞれ一長一短ある。

（１）ブレンディングに際しては音声を元に戻して加算し、再び暗号化する。この方式だと任意の暗号が使える。但し、中継点で音声が裸になるという弱点がある。

（２）線形暗号を用いる。線形暗号ならばブレンディング処理と暗号が可換なので中継点で元に戻す必要はなくなる。但し、線形暗号はセキュリティが低い欠点がある。即ち、平文と暗号文の対が幾つか与えられると線形変換を示す行列が解かれてしまう。この欠点を解決する方法として、文献[20]ではGSナップサック暗号を利用した暗号が示されたが、その後GSナップサック暗号は解読されてしまった。

そこで本報告では線形暗号の長所を生かし、実現しやすく強度を多少なりとも上げた暗号アルゴリズムを提案する。

入力系列を数の系列とみなし、ブロック化する。数の大きさは$0 \sim 2^m-1$とする。PCMなら$m=8$である。ブロックサイズbは大きい程セキュリティが高まるが遅延も大きくなる。PCMなら高々512であろう。さて、WKに依存してb次正則行列Hを定める。具体的な依存方法については、ここでは問わないこととする。

入力の１ブロックを

$$x=(x^{(1)},x^{(2)},\cdots,x^{(b)}) \qquad (15)$$

とすると、暗号アルゴリズムを

$$y=(2^h x+R)\cdot H \pmod w \qquad (16)$$

とする。ここで、Rはtビットの乱数、hはNを会議メンバーの上限として

$$2^h \geqq N\cdot(2^t-1) \qquad (17)$$

をみたす定数、wは

$$w \geqq 2^{h+m} \qquad (18)$$

をみたす定数である。

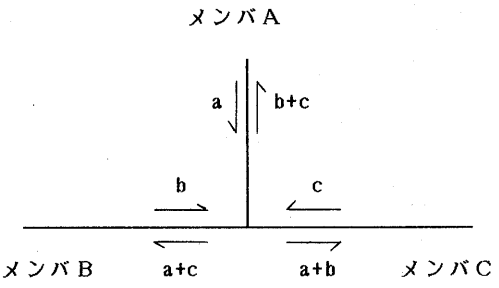


図４　電子会議における音声ブレンディング

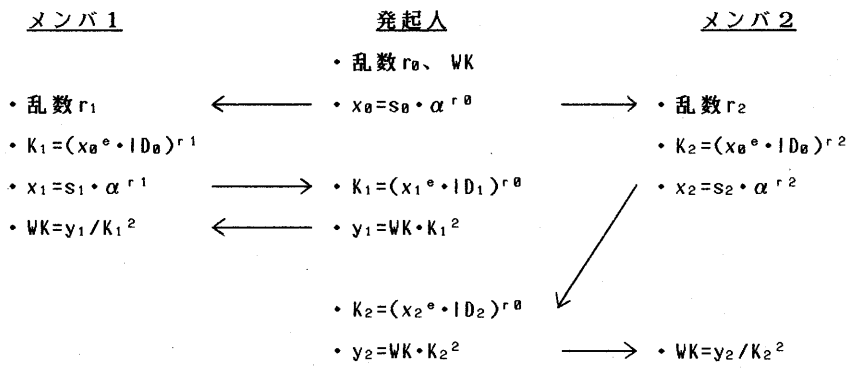


図３　電子会議における鍵配布

例として、２ヶ所からの音声

$$y_1=(2^h x_1+R_1)\cdot H \quad (19)$$

$$y_2=(2^h x_2+R_2)\cdot H \quad (20)$$

をブレンディングすると

$$Z=y_1+y_2$$
$$=(2^h(x_1+x_2)+R_1+R_2)\cdot H \quad (21)$$

となり、受信側では

$$Z\cdot H^{-1}=2^h(x_1+x_2)+R_1+R_2 \quad (22)$$

から下位よりhビット以上を切り取ればx_1+x_2を得る。ここで式(17)の条件からR_1+R_2の桁上がりがx_1+x_2の部分に及ぶことはない。

このアルゴリズムはかなりナップザック的色彩が濃いので、線形暗号よりは強いが、一般の暗号に比較すると弱い可能性がある。従って鍵wは必ず使い捨てにすべきである。なお、$t\neq 0$の場合は帯域が拡大する欠点もある。（t=0の場合は線形暗号となる。）

４.あとがき

ＩＤ情報に基づく鍵配送方式の紹介とそれを電子会議に適用した電子会議システムについて論じた。電子会議システムでは音声ブレンディングとの可換性をもつ暗号アルゴリズムについて言及した。

未筆ながら、貴重な意見を載いた日本電気株式会社情報研究部中村部長に深謝する。

[文献]

[1] R.E.Lennon:"Cryptography architecture for information security", IBM System J.,17,2, pp.138-150(1978).

[2] 田中:"鍵なしではまず解けなくなった最近の暗号方式",日経エレクトロニクス, 194, pp.168-108(1978).

[3] W.Diffie and M.E.Hellman: "New directions in cryptography",IEEE Trans. Inform. Theory IT-22,6, pp.644-654(1976).

[4] R.L.Rivest,A.Shamir and L.Adleman:"A method for digital signatures and public-key crypto systems", Common. ACM.,21,2, pp.120-126(1978).

[5] L.Kohnfelder:"Towards a practical public-key cryptosystem", B.S.Thesis, MIT, Cambridge, Mass.(1987).

[6] R.Blom:"An optical class of symmetric key generation systems",Proc. of Eurocrypt 84, pp. 335-338(1984).

[7] T.Matsumoto and H.Imai:"On the key predistribution system", Proc. of Crysto 87, pp.185-193 (1987).

[8] H.Tanaka:"A realization scheme for the identity-based cryptosystem", Proc. of Crypto87, pp. 340-349(1987).

[9] S.Tsujii,T.Itoh and K.Kurosawa:"ID-based cryptosystem using discreate logarithm problem", Electronics Letters, 23,24, pp. 1318-1320(1987).

[10] A.Shamir:"Identity-based cryptosystems and signature schemes", Proc. of Crypt 84, pp. 47-53(1984).

[11] 岡本龍明:"単一公開情報による複数利用者の認証方式", 信学論(D), J69-D,10, pp.1481-1489(1986).

[12] A.Fiat and A.Shamir:"How to prove yourself", Proc. of Crypto 86, pp.186-194(1986).

[13] 岡本栄司:"ＩＤに基づく鍵配送方式",信学技報IT86-53, pp.25-28 (1986).

[14] E.Okamoto:"Proposal for iden-

tity-based key distribution systems", Electronics Letters, 22, 24, pp.1283-1284(1986).
[15] E.Okamoto:"Key distribution systems based on identification information", Proc. of Crypto87, pp.194-202(1987).
[16] E.Okamoto and K.Tanaka:"Key distribution system based on identification information", Globecom87, 3.8.1-3.8.4(1987).
[17] E.Okamoto and K.Tanaka:"Identity-based information security management system for personal computer networks", IEEE JSAC on Personal Communications 2 (投稿中).
[18] E.Okamoto and K.Tanaka:"Key distribution system based on identification information", IEEE JSAC on Secure Communications (投稿中).
[19] E.Okamoto and K.Tanaka:"ID情報に基づく暗号鍵配送方式の提案", 信学論 (投稿中).
[20] 岡本栄司:"遠隔会議に於ける音声の一暗号化方式", 信学技報IT82-23, pp.29-33(1982).