マスターキーの構成と安全性の検討

梅澤真美　(指導教官: 金子 晃)

1　はじめに

日常語としてのマスターキーとは，建物のすべての部屋の鍵を開けられる管理用の鍵のことである．本研究では，ある組織 (以下簡単のため会社とする) の長 (社長) が組織内の暗号通信で用いるために，各部署 (企画課，技術課，営業課，人事課) の長 (課長) の鍵，およびそのメンバーの鍵をすべて把握できる効率的なシステムを考える．

2　マスターキーの要求仕様と基本実装

はじめに要求される仕様を整理する．

1. 社長は，社員の全ての暗号文を読めるような鍵情報を保持する．
2. 各課長は，課内のすべての部下の暗号文を読めるような鍵情報を保持する．
3. 以上のほかは，社員同士は通常の暗号通信を行う．できれば ID 形公開鍵による暗号通信が望ましい．

まず，雛形として次のような手順を考える：

1. 社内で共用するパラメータ付き一方向性ハッシュ関数 $h(x, y)$ を用意する．
2. 社長は秘密の乱数 r を用意しマスターキーとする．
3. 社長は各課の ID eigyou 等々をマスターキーと合わせ，その課の秘密鍵 $s_{\text{eigyou}} = h(r, \text{eigyou})$ 等々を作成して当該の課長に手渡す．
4. 各課長は，部下の各々に対し，課の秘密鍵と，その部下の ID yamada.taro 等を合わせて，その人の秘密鍵 $t_{\text{yamada.taro}} = h(s_{\text{eigyou}}, \text{yamada.taro})$ を作り，本人に手渡す．

この後の各自の秘密鍵の使用法としては，例えば会社全体で巨大な可換群 G と位数の巨大な元 g を共有し，$g^{t_{\text{yamada.taro}}}$ を公開鍵として Diffie-Hellman 型の鍵交換を行い，それを用いて共通鍵暗号通信を行うか，El-Gamal 型の公開鍵暗号通信を行えばよい．

3　RSA 暗号系を用いたマスターキーの構成

上の仕組みを RSA 暗号を用いて構成する方法を示す。本物のマスターキーと同様，ある管理職が持っている鍵でその人の下部組織の発信した全ての暗号文を同じ復号関数でできることが重要である。

すなわち，

$$C_j = \text{Enc}(M_j, K_j), \quad j = 1, 2, \ldots, J$$

から，

$$M_j = \text{Dec}(C_j, K'_j), \quad j = 1, 2, \ldots, J$$

かつ，あるマスターキー K' について

$$M_j = \text{Dec}(C_j, K'), \quad j = 1, 2, \ldots, J$$

となるようなものである．

例として，次のようなものが考えられる：$p_j, q_j, j = 1, 2, \ldots, J$ を互いに異なる素数で，かつ

$$f_j = \text{LCM}(p_j - 1, q_j - 1), \quad j = 1, 2, \ldots, J$$

は 2 以外に共通因子を持たないようなものとする．(これは例えば，p_j, q_j をすべて co Sophie-Germain 素数に取れば実現できる.) $n_j = p_j q_j$ を法として，J 個の独立な RSA 暗号を用意し，それぞれの秘密鍵，公開鍵を d_j, e_j とする：$d_j e_j = 1 \mod f_j$. このとき，

$$F = 2\prod_{j=1}^{J}(f_j/2), \quad F_j = F/f_j$$

と置けば，F_j と f_j は互いに素となるので，各 j について $b_j F_j = 1 \mod f_j$ なる b_j を選べる．このとき，J が奇数なら

$$D = \sum_{j=1}^{J} d_j b_j F_j,$$

また J が偶数なら

$$D = \sum_{j=1}^{J} d_j b_j F_j + F/2,$$

と置けば，D はマスターキーとなる．

実際，任意の i に対して，暗号文 $C_i = M_i^{e_i} \mod n_i$ をとるとき，$M_i = C_i^{d_i} \mod n_i$ は当然として，

$$C_i^D = C_i^{d_i b_i F_i} C_i^{\sum_{j \neq i} d_j b_j F_j} \mod n_i$$

であり，ここで

$$C_i^{d_i b_i F_i} = C_i^{d_i b_i F_i \mod f_i} = C_i^{d_i} = M_i \mod n_i$$

また，

$$C_i^{\sum_{j \neq i} d_j b_j F_j} = C_i^{\sum_{j \neq i} d_j b_j F_j \mod f_i}$$

においては，構成法から明らかに，$j \neq i$ なる各 F_j は $f_i/2$ で割り切れているので，最後の指数 $\sum_{j \neq i} d_j b_j F_j$ は $f_i/2$ で割り切れる．更に，d_j, b_j, F_j はすべて奇数なので，個数 J が奇数なら，この指数は全体として偶数となり， 2 でも割り切れ，結局 f_i で割り切れることとなるから, C_i の冪を取れば 1 となる．また，J が奇数のときは，この指数に $F/2$ を足したものは偶数となり，この項はすべての $f_j/2$ で割り切れるので同じ結論を得る．よって $C_i^D = M_i \mod n_i$ が成り立つ．

このシナリオは n_i をグループ化できるので課長に

$$D_{\text{eigyou}} = \sum_{j \in \text{eigyou}} d_j b_j F_j + (\#\text{eigyou} + 1 \mod 2)\frac{F}{2}$$

等を渡すことで階層化が可能である．また，安全性については，個々の RSA 暗号の安全性と同等である．

この方式は，一応所期の要求を満たしているが，ここで示されたマスターキーは，J が大きいと個々のキー d_i に対して著しく巨大となり，すべての部屋の鍵の束に近いイメージである．また，マスターキーを持つ社長が全ての素数データを生成して部下に配布しなければならず，計算量の点であまり実用的ではない．

建物のマスターキーのように，マスターキーが個々のキーと同程度のサイズとなるようなものが理論的に構成可能かどうか，現在検討中である．

4 ElGamal暗号方式を用いたマスターキーの構成

全く同様の技法で，ElGamal 暗号系に対するマスターキーを構成可能である．p_j, $j = 1, 2, \ldots, J$ を互いに異なる素数で，かつ

$$f_j = (p_j - 1)/2, \quad j = 1, 2, \ldots, J$$

は互いに素となるように選ぶ．$\boldsymbol{F}_{p_j}^{\times}$ の生成元 g_j を選ぶ必要があるので，p_j をすべて co Sophie-Germain 素数に取るのが簡明である．p_j を法として，J 個の独立な ElGamal 暗号を用意し，それぞれのシステムパラメータを p_j, g_j, また秘密鍵，公開鍵を a_j, g^{a_j} とする．

$$F = \prod_{j=1}^{J} f_j, \quad F_j = F/f_j$$

と置けば，F_j と f_j, 更に $p_j - 1$ は互いに素となるので，各 j について $b_j F_j = 1 \mod p_j - 1$ なる b_j を選べる．(RSA のときと若干記号の意味を変えている.) このとき，J が奇数なら

$$D = \sum_{j=1}^{J} a_j b_j F_j,$$

また J が偶数なら

$$D = \sum_{j=1}^{J} a_j b_j F_j + F,$$

と置けば，D は ElGamal 暗号に対するマスターキーとなる．

実際，任意の i に対して，k をその場限りの乱数として，平文 M_i を $C_i = (C_{i1}, C_{i2}) := (g_i^k, g_i^{a_i k} M_i)$ により暗号化するとき，$M_i = C_{i2}/(C_{i1})^{a_i}$ は当然として，$C_{i2}/(C_i 1)^D = M_i$ ともなることが，以下のように分かる：

$$C_{i1}^D = (g_i^k)^D = (g_i^k)^{a_i b_i F_i} \cdot (g_i^k)^{\sum_{j \neq i} a_j b_j F_j}$$

であり，ここで

$$(g_i^k)^{a_i b_i F_i} = (g_i^k)^{a_i b_i F_i \mod (p_i - 1)} = (g_i^k)^{a_i} = g_i^{a_i k}$$

また，

$$(g_i^k)^{\sum_{j \neq i} a_j b_j F_j} = (g_i^k)^{\sum_{j \neq i} a_j b_j F_j \mod (p_i - 1)}$$

においては，構成法から明らかに，$j \neq i$ なる各 F_j は f_i で割り切れているので，最後の指数 $\sum_{j \neq i} a_j b_j F_j$ は $(p_i - 1)/2$ で割り切れる．更に，a_j, b_j, F_j はすべて奇数なので，個数 J が奇数なら，この指数は全体として偶数となり，従って 2 でも割り切れ，結局 $p_i - 1$ で割り切れることとなるから，g_i^k の冪を取れば 1 となる．また，J が奇数のときは，この指数に F を足したものは偶数となり，この項はすべての f_j で割り切れているので同じ結論を得る．よって $(g_i^k)^D = (g_i^k)^{a_i}$ が成り立ち，i 番目の ElGamal 暗号はこの鍵でも同じ復号関数で復号できる．

この方式を実現するには，社長は通常の ElGamal 暗号と異なり，すべての部下の秘密鍵 a_i を作って配布しなければならない．これは RSA の場合と同じである．

5 共通パラメータの ElGamal 暗号方式を用いたマスターキーの構成

RSA 暗号の場合は，同じ $n = pq$ を用いて複数の暗号を作ることは安全性の問題から全く実用的ではないが，ElGamal 暗号の場合は，群 G と生成元 g を共通パラメータとして複数の暗号が作れるので，そのような暗号系に対してマスターキーを作ることを考える．

G, g を離散対数のシステムパラメータとし，各部下用に秘密鍵 a_j $j = 1, \ldots, J$ を用意する．a_i はすべて奇数に選ぶ．更に，社長は $A = a_1 \cdots a_J$ を計算し，各部下用に公開鍵 g^{a_i}, $g^{a_i/A}$ を発表する．ここで，a_i/A は g の位数 ($G = \boldsymbol{F}_p^{\times}$ のときは $p - 1$) を法としての計算である．

i 番目の社員への ElGamal 暗号化は

$$M_i \mapsto C_{i1}, C_{i2}, C_{i3}) := (g^k, (g^{a_i/A})^k, g^{a_i k} M_i$$

とする．これは，この社員により復号鍵 $(K_1, K_2) = (a_i, 0)$ を用いて

$$(C_{i3}/C_{i2}^{K_2})/C_{i1}^{K_1} \tag{1}$$

N で復号される．これが M_i に戻ることは，実質的に ElGamal 暗号と同等なことから直ちに分かる．社長は，マスターキー $(K_1, K_2) = (0, A)$ を用いて (1) と同じ復号関数で復号する．この場合は

$$C_{i2}^{K_2} = ((g^{a_i/A})^k)^A = g^{a_i k}$$

となるので，やはり M_i が得られる．

この方式の安全性は，$g^{a_i/A}$ の公開が g^{a_i} の離散対数の解に有利な情報を与えているかどうかであるが，$g^{a_i/A}$ は敵が勝手に A を選んで $(g^{a_i})^{1/A}$ によりシミュレートできるので，何ら有効な情報を漏らしていないことが分かる．

6 ID ベース暗号への修正

s を社長が保持する秘密のシステムパラメータ，sP を公開のシステムパラメータ，Q_{ID_i} を公開鍵，sQ_{ID_i} をユーザー i の秘密情報とし，暗号化関数を

$$M_i \mapsto (C_{i1}, C_{i2}) := (ksP, M_i \oplus H(e(sP, kQ_{\mathrm{ID}_i})))$$

とするとき，復号関数は，復号鍵を (a, Q) として

$$C_{i2} \oplus H(e(aQ_{\mathrm{ID}_i} + Q, C_{i1}))$$

と少しひねったものとする．ユーザー i は復号鍵 $(a, Q) = (0, sQ_{\mathrm{ID}_i}$ を用いれば，通常の ID ベース暗号の原理で復号できる．また，社長は $(a, Q) = (s, \mathcal{O})$ を復号鍵として用いれば，同じ原理で復号できる．

参考文献

[1] NEC ソフトウェア北陸 “cybercrypt” http:www.//hnes.co.jp/sol-pro/sol-pd-3sol/cybercrypt/concept.jsp

[2] 岡本龍明, 山本博資:“現代暗号” (第 3 版), 産業図書, 2000.

[3] W. Stallings: “Cryptography and Network Security” (4-th ed.), Pearson Prentice Hall, 2006.

[4] D. Boneh, M. Franklin: “Identity-based encryption from the Weil pairing”, SIAM J. of Computing, **32**-3 (2003), 586–615.