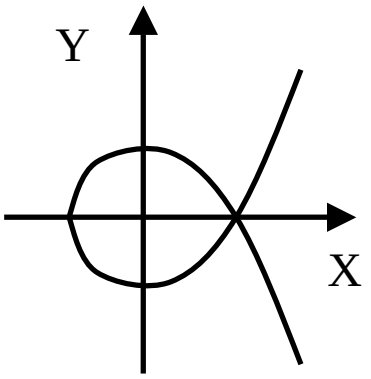
Mebius

楕円曲線を利用した
ネットワークセキュリティシステム
構築の検討

2004年11月22日

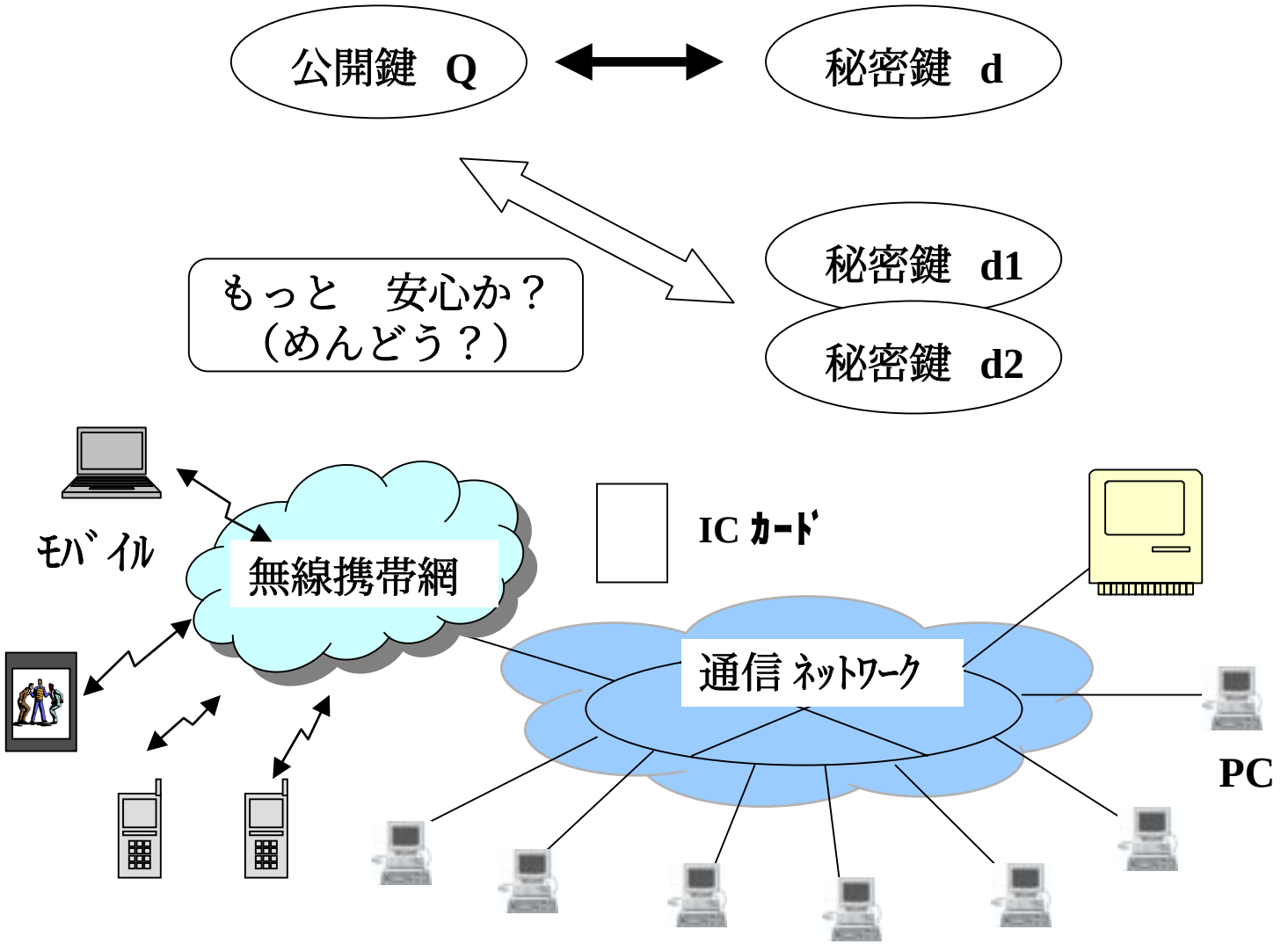


株式会社　メビウス

〒220-0073 横浜市西区岡野1-14-1
http://www.mebius.co.jp

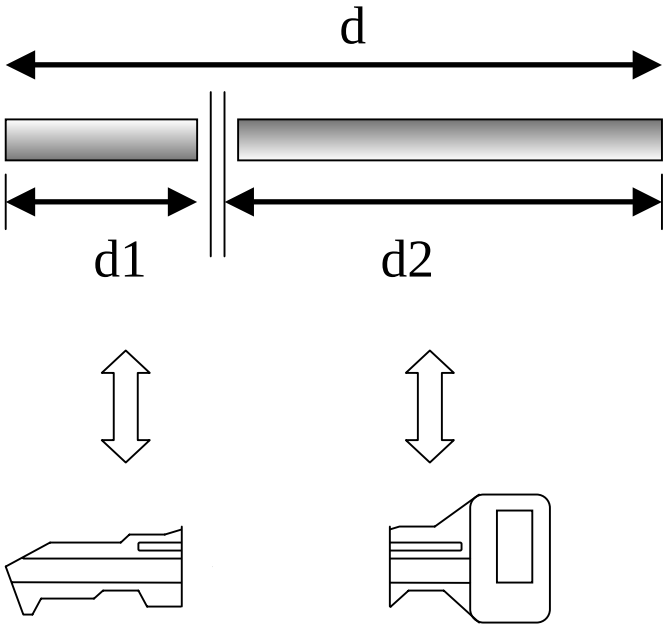
概要

公開鍵暗号システム

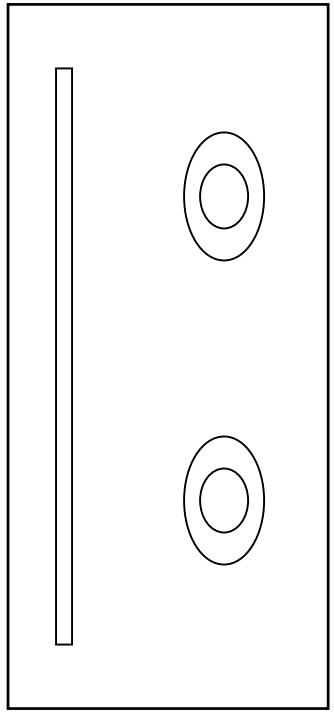


複数の秘密鍵の運用

1. 長い秘密鍵の分割



2. 独立に処理できる秘密鍵の構成



d1

個人管理

d2

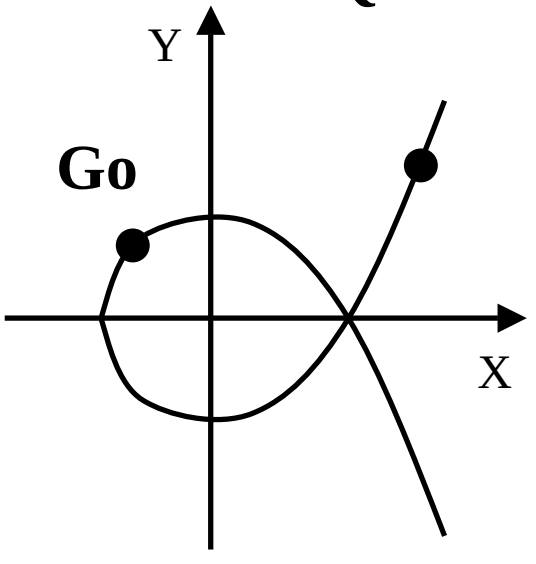
信頼できる第三者管理

(door)

システムの構成方式

楕円曲線の離散対数問題に着目

Q = d・Go



$Y^2 = X^3 + a*x + c$

#E(Fq) = u*s (s ; 大きな素数)

公開鍵 Q 和の形式

Q = f・Go + g・Ge

秘密鍵　{ f , g } 組

生成元　Go , Ge 独立

Q ⟺ { f , g}

(1対1)

1. 楕円曲線の安全性の確保
2. 暗号化、復号化の方式
3. 電子署名の作成、検証
4. 運用例
   鍵の管理

2個の生成元を持つ楕円曲線

安全な楕円曲線を用意
（1個の生成元　Go）

$$Y^2 = X^3 + a*X + b$$

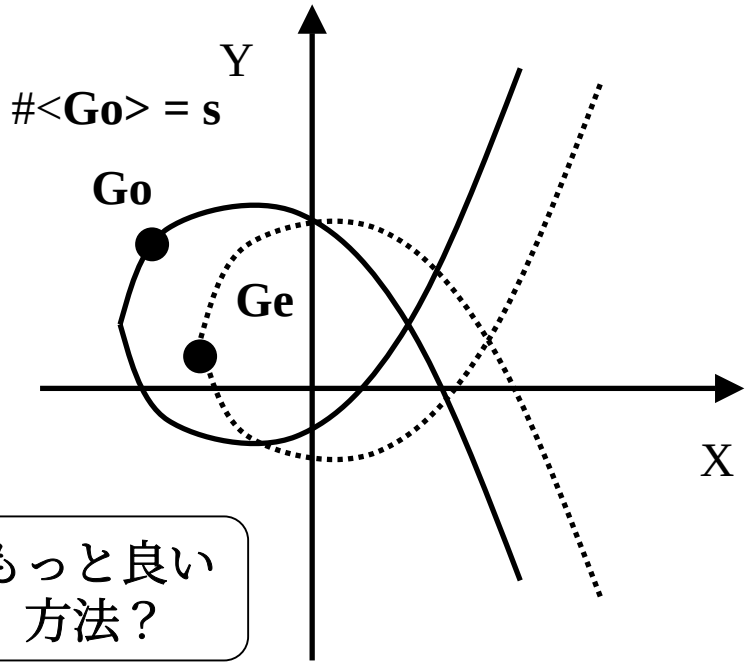
定義体　$a, b \in Fq$　（　$q = p^n$ ）

定義体の代数拡大
Fq(ρ)

Goとは別の巡回群の
生成元Ge

$$Ge = (xe , \rho)$$

$$m \cdot Go \neq n \cdot Ge \quad (m , n \in Z)$$



もっと良い
方法？

Fq に付加する ρ

$$f(X) = X^3 + a*X + b$$

(a)　$xe \in Fq$　　$\tau = f(xe)$

(b)　$\tau = t^2$ となる　$t \in Fq$
が存在しない。

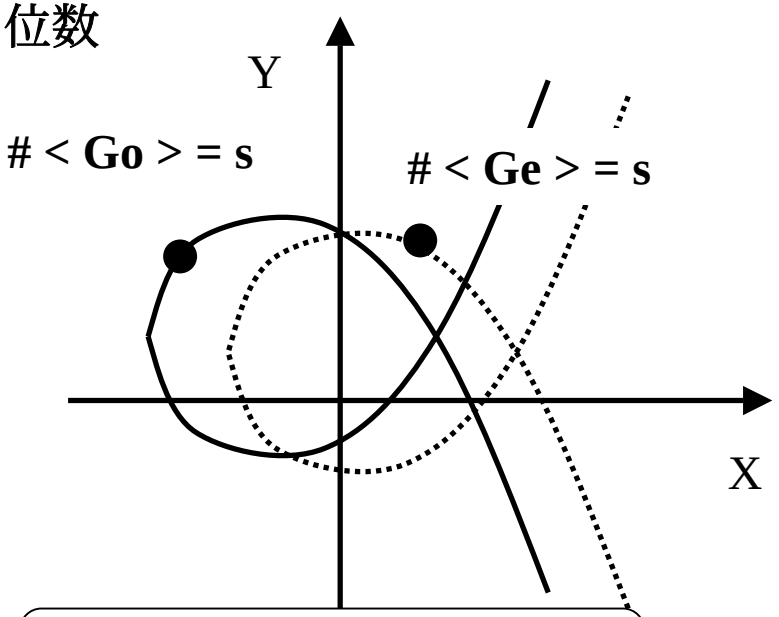
(c)　$\rho = \sqrt{\ } \tau$

楕円曲線の位数の評価

Fq(ρ)の位数　　q^2

#E(Fq) = u*s　　定義体**Fq**の楕円曲線の位数
s ; 大きな素数

#E(Fq(ρ))　　定義体**Fq (ρ)**の楕円曲線の位数



種数１以上にも適用可能？

ハッセの定理

$$1 + q - 2\sqrt{q} \leqq \#E(Fq) \leqq 1 + q + 2\sqrt{q}$$
$$1 + q^2 - 2q \leqq \#E(Fq(\rho)) \leqq 1 + q^2 + 2q$$

これより
 # E(Fq (ρ))　　(# E(Fq)) * (# E(Fq))

 # E(Fq) ≧ **# < Go > = s**
 # E(Fq (ρ)) ≧ **(# < Go >) * (# < Ge>)**

暗号化 , 復号化の方式

送信者

通信相手ユーザ

通信相手の
公開鍵の取得

通信相手ユーザの
公開鍵 Q1 , Q2
ベースポイント Go,Ge

公開鍵 Q = f・Go＋g・Ge
Q1 = f・Go , Q2 = g・Ge
ベースポイント Go, Ge
秘密鍵 { f , g }

暗号化

暗号データの送信

復号化

乱数 κ、τ の生成

κ・Go = R1、
τ・Ge = R2
κ・Q1 + τ・Q2 ＝T
＝(Tx , Ty)
c = π（Tx）⊕ m
(m ;**平文** c ; **暗号文**)

{R1 , R2 , c}

f・R1 + g・R2 = T
= (Tx , Ty)
m = π（Tx）⊕ c

秘密鍵 f , g は、
独立に処理可能

電子署名作成、検証の方式

送信者

通信相手ユーザ

公開鍵　Q = f・Go＋g・Ge
ベースポイント　Go, Ge
秘密鍵 { f , g }

送信元の
公開鍵 Q の取得

ベースポイント Go, Ge

電子署名の作成

電子署名の検証

乱数 κ、τ 生成
ハッシュ値 e1 = H(m1)
平文 m (m1 , m2)　e2 = H(m2)

電子署名の
データ送信

R1 = κ・Go = (r1 , y1)、
R2 = τ・Ge = (r2 , y2)
電子署名 S

$$\begin{pmatrix} \frac{e1 + f}{\kappa} & \frac{r1}{\kappa} \\ \frac{g}{\tau} & \frac{e2 + r2}{\tau} \end{pmatrix}$$

{ R1 , R2 , S, m1,m2 }

$C = S^{-1}$
R = r1・Go + r2・Ge
e1 = H(m1) , e2=H(m2)

(e1・Go , e2・Ge) C + (Q , R) C
＝（ κ・Go , τ・Ge ）= (R1 , R2)

(注) ECDSA
c(e+r*d)・Go = R1

電子署名S分割による生成

部署A

秘密鍵　f

$R1 = \kappa \cdot Go = (r1, y1)$

$e1 = H(m1)$

$S1 = \begin{pmatrix} \frac{e1 + f}{\kappa} & \frac{r1}{\kappa} \end{pmatrix}$

部署B

秘密鍵　g

$R2 = \tau \cdot Go = (r2, y2)$

$e2 = H(m2)$

$S2 = \begin{pmatrix} \frac{g}{\tau} & \frac{e2 + r2}{\tau} \end{pmatrix}$

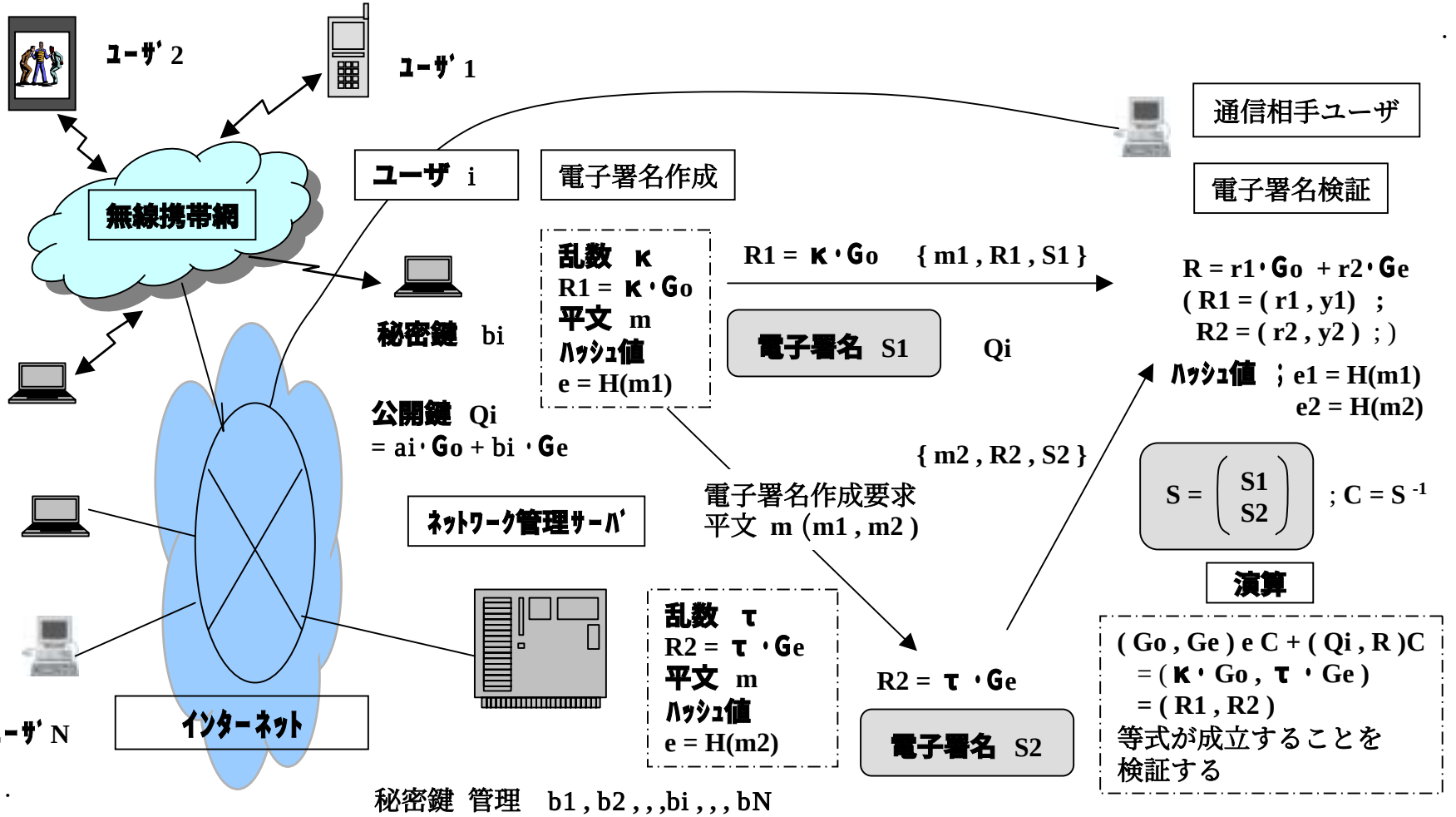
多重署名とは異なる？

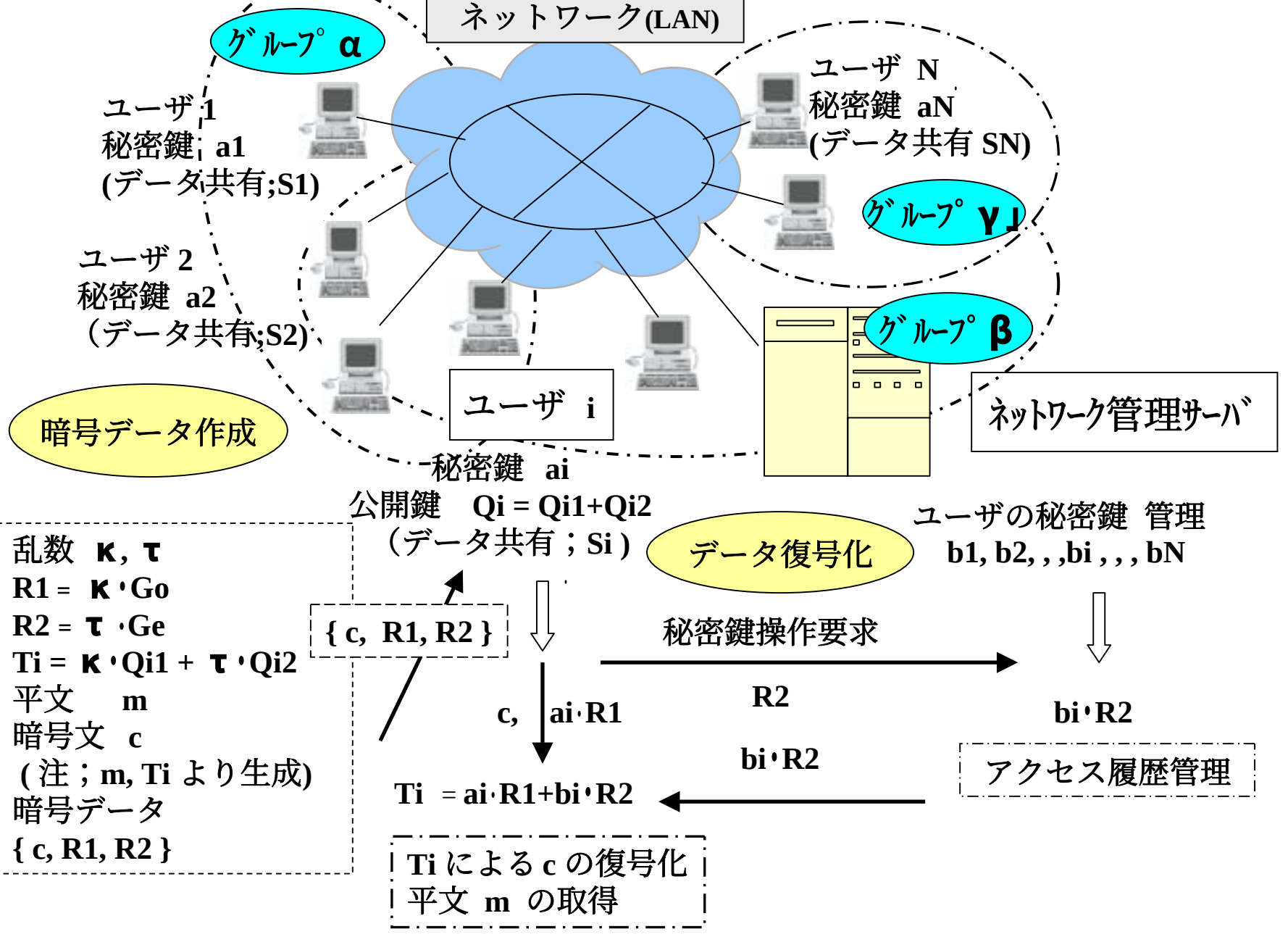
合成

$S = \begin{pmatrix} S1 \\ S2 \end{pmatrix}$

分散して存在するデータの
関連付けの正当性を保障する。

移動体端末での電子署名の運用例




ネットワーク(LAN)
グループ α
ユーザ 1
秘密鍵 a1
(データ共有;S1)
ユーザ N
秘密鍵 aN
(データ共有 SN)
グループ γ
ユーザ 2
秘密鍵 a2
(データ共有;S2)
グループ β
ユーザ i
ネットワーク管理サーバ
暗号データ作成
秘密鍵 ai
公開鍵 Qi = Qi1+Qi2
(データ共有 ; Si)
データ復号化
ユーザの秘密鍵 管理
b1, b2, , ,bi , , , bN
乱数 κ, τ
R1 = κ・Go
R2 = τ ・Ge
Ti = κ・Qi1 + τ・Qi2
平文 m
暗号文 c
(注 ; m, Ti より生成)
暗号データ
{ c, R1, R2 }
{ c, R1, R2 }
秘密鍵操作要求
R2
c, ai・R1
bi・R2
bi・R2
アクセス履歴管理
Ti = ai・R1+bi・R2
Ti による c の復号化
平文 m の取得

本報告のまとめ

1. 公開鍵Q に対して、秘密鍵を { f , g }2個
   持たせる方式を、楕円曲線を利用して
   検討した。

2. 暗号化、復号化方式
   電子署名作成、検証方式にを構成した。

3. 秘密鍵2個もたせることで、きめ細かい
   通信の制御が可能となる見通しが得られた。

4. 応用の検討、プログラム化については、
   今後の課題としたい。