論文内容の要旨

論文題目

Efficient Encryption Schemes based on Lattice Problem and Hidden Subgroup Problem

(格子問題と隠れ部分群問題に基づく効率的な暗号化方式)

氏名　吉野 雅之

はじめに

ネットワーク技術の進歩に伴い，組織外の計算器資源を動的に活用する情報システムが広がりを見せる一方，情報システムからの情報漏洩の危険性が指摘されている．本論文では，情報システムにおいて、データを安全に保護する暗号化方式に関する研究成果を報告する．まず，安全かつ効率的な対称型述語暗号の研究成果を報告する．標準的な暗号化方式では，暗号文は復号のみが可能な処理であるが，本研究成果を用いると，暗号文における述語処理が実現可能である．さらに，長期間に渡る情報システムの利用に備え，暗号化方式は強力な量子計算機による暗号解析にも対抗する必要がある．次いで, 暗号化方式の安全性評価に関連する, 最短近似ベクトル問題の計算手法の研究成果を報告し，最後に最短近似ベクトル問題を安全性の根拠とする暗号化方式を報告する．

対称型述語暗号の研究

述語暗号は，暗号文と暗号化トークンにおける述語を，秘密鍵を所有しない第三者が処理可能な暗号化方式である．特に，暗号文と暗号化トークンを作成する鍵を秘密裏に管理する方式を対称型述語暗号と呼ぶ．一般に，用いる群の数が少ない述語暗号は性能が良い．そこで，性能を重視し，利用する群の数を 3 つに絞った対称型述語暗号の研究成果を報告する．

準備として，3 素数の積からなる合成数位数の双線形群を説明する．セキュリティパラメータ sp を入力とし，相異なる素数 p1，p2，p3 を含む，組(p1，p2，p3，G，GT，e)を出力する，合成数位数の双線形群の生成アルゴリズムを A とする．G と GT を位数 N=p1p2p3 の巡回乗法群とし，そのペアリング写像 e(G×G→GT)は，以下の性質(双線形性と非退化)を満たす．

- 双線形性: $^{\forall}g, ^{\forall}h \in \mathbb{G}, a, b \in \mathbb{Z}_N, \hat{e}(g^a, h^b) = \hat{e}(g, h)^{ab}$
- 非退化: 任意の $g \in \mathbb{G}$ に対し, 全ての $h \in \mathbb{G}$ に対して $\hat{e}(g, h) = 1$ が成り立つならば, $g = 1$ である.

記号 G1，G2，G3 は G の部分群であるとし，その位数はそれぞれ p1，p2，p3 とする．n 次元ベクトルを $\mathbf{x}=(x_1, \cdots x_n)$，$\mathbf{y}=(y_1, \cdots y_n)$かつ x_i，$y_i \in Z_N$ とし，内積$\langle \mathbf{x}, \mathbf{y} \rangle$を $x_1y_1+\cdots x_ny_n$ とする．

提案する対称型述語暗号は，以下 4 つの関数で構成される．

- Setup(sp) : セキュリティパラメータ sp を引数とする．生成アルゴリズム A を実行し，(p1，p2，p3，G，GT，e)を得る．ただし $G=G_1 \times G_2 \times G_3$ である．次に，一様ランダムに G_1，G_2，G_3 の生成元 g_1, g_2, g_3 と, $q_{1,i}, q_{2,i} \in Z_{p1}, r_{1,i}, r_{2,i} \in Z_{p3}(i=1, \cdots n)$を生成する. 公開パラメータを N(=p1p2p3)，G，GT，e の組，秘密鍵 SK を生成元 g_1，g_2，g_3 と，素数位数 p1，p2，p3，乱数 $q_{1,i}$，$q_{2,i}$，$r_{1,i}$，$r_{2,i}(i=1, \cdots n)$の組とする．
- Encrypt(SK，$\mathbf{x}$)：一様ランダムに生成した乱数 $S \in Z_{p1}$，α_1，$\alpha_2 \in Z_{p2}$，$U_{1,i}$，$U_{2,i} \in Z_{p3}(i=1, \cdots n)$，$U_1 \in Z_{p1}$，$U_2 \in Z_{p2}$ を用い，平文を表わす n 次元ベクトル $\mathbf{x}$ を暗号化した暗号文 CT を出力する．

$$CT := \begin{cases} C_{1,i} = g_1^{Sq_{1,i}} g_2^{\alpha_1 x_i} g_3^{U_{1,i}} \quad (i = 1, \ldots, n) & C_{2,i} = g_1^{Sq_{2,i}} g_2^{\alpha_2 x_i} g_3^{U_{2,i}} \quad (i = 1, \ldots, n) \\ C_1 = g_1^S & C_2 = g_1^{U_1} g_2^{U_2} \prod_{i=1}^n g_3^{-U_{1,i} r_{1,i} - U_{2,i} r_{2,i}} \end{cases}$$

- GenToken(SK，$\mathbf{y}$)：一様ランダムに生成した乱数 $T \in Z_{p3}$，β_1，$\beta_2 \in Z_{p2}$，$V_{1,i}$，$V_{2,i} \in Z_{p1}(i=1, \cdots n)$，$V_1 \in Z_{p2}$，$V_2 \in Z_{p3}$ を用い，平文を表わす n 次元ベクトル $\mathbf{y}$ を暗号化した暗号化トークン TK を出力する．

$$TK := \begin{cases} K_{1,i} = g_1^{V_{1,i}} g_2^{\beta_1 y_i} g_3^{T r_{1,i}} \quad (i = 1, \ldots, n) & K_{2,i} = g_1^{V_{2,i}} g_2^{\beta_2 y_i} g_3^{T r_{2,i}} \quad (i = 1, \ldots, n) \\ K_1 = \prod_{i=1}^n g_1^{-V_{1,i} q_{1,i} - V_{2,i} q_{1,i}} g_2^{V_1} g_3^{V_2} & K_2 = g_3^T \end{cases}$$

- Check(CT，TK)：正規ペアリング写像 $\mathbf{E}$ を用い，$\mathbf{E}$(CT，TK)=1 ならば 1 を，$\mathbf{E}$(CT，TK)≠1 ならば 0 を出力する. ただし, $\mathbf{E}(CT, TK) = e(C_{1,1}, K_{1,1}) \cdots e(C_{1,n}, K_{1,n}) e(C_{2,1}, K_{2,1}) \cdots e(C_{2,n}, K_{2,n}) e(C_1, K_1) e(C_2, K_2)$である.

従来の対称型述語暗号に比べると，提案法は用いる群の数を 3 つに絞ったために性能が良く，かつ，同等の安全性をより厳しい Non-Intractive な仮定で証明できる. 表 1 における記号 Non-I は Non-Intractive，記号 I は Intractive である.

表 1 ：述語暗号の性能(群の数)と安全性

述語暗号	用いる群の数	安全性モデル		仮定
		暗号文	暗号化トークン	
従来法 1(公開型)	3	*Selectively Secure*	–	I
従来法 2(公開型)	3	*Adaptively Secure*	–	Non-I
従来法 3(対称型)	4	*Selectively Secure*	*Selectively Secure*	I
提案法 (対称型)	3	*Selectively Secure*	*Selectively Secure*	Non-I

SVP 近似アルゴリズムの高速化の研究

最短ベクトル問題(SVP : Shortest Vector Problem)は，量子計算機でも解読困難とされる NP 困難な問題の一つである．一方で，SVP の近似解は，その近似度次第では古典計算機でも多項式時間で解読できる．そこで，暗号化方式の安全性を評価する上で重要な指標である，SVP 近似アルゴリズムに関する研究成果を報告する．

正則行列 $\mathbf{B} \in Z^{n \times n}$ を，n 本の線形独立ベクトル $\mathbf{b1}$，$\cdots \mathbf{bn}$ から構成される，ラティスの基底とする．直交ベクトル $\mathbf{ai} \in Q$ は，$\mathbf{b1}$，$\cdots \mathbf{bn}$ が張る(i-1)次空間と内積$\langle \mathbf{x}, \mathbf{y} \rangle$に関し，直交する．基底 $\mathbf{b1}$，$\cdots \mathbf{bn}$，直交ベクトル $\mathbf{a1}$，$\cdots \mathbf{an}$ は，任意の i(1≦i≦n)において，式 $\mathbf{bi}=u(i, 1)\mathbf{a1}+\cdots+u(i, n)\mathbf{an}$ を満たす. ただし，u(i，j)=1(i=j)かつ $u(i, j)=\langle \mathbf{bi}, \mathbf{aj} \rangle / \langle \mathbf{aj}, \mathbf{aj} \rangle$，(i>j)である

SVP 近似問題の解読手法である RSR(Random Sampling Reduction)を説明する．SVP 近似アルゴリズムが出力する第一基底 $\mathbf{b1}$ と各直交ベクトル $\mathbf{ai}(1 \leqq i \leqq n)$は, 関係式$||\mathbf{ai}||^2 = q^{i-1} ||\mathbf{b1}||^2$(ただし,

3/4≦q<1)を近似的に満たす．従って，添字 i の値が大きくなるにつれ，||**ai**||は小さくなる．この性質を利用し，RSR では，包含関係式 ui∈(-1/2, 1/2](1≦i<n-μ)，ui∈(-1, 1](n-μ≦i<n)，ui=1(i=n)を満たす，ベクトル **b**=u1**a1**+…＋un**an** を探索する．

しかし，上記の RSR は，十分に短いベクトルが見つかるまで，ほぼ全ての係数 ui の計算を繰り返す必要がある．そこで，効率的に ui を計算可能な，RSRwP(Random Sampling Reduction with Precomputation)を提案した．ベクトル **b** の探索は，包含関係式 ui∈(-1/2, 1/2](1≦i≦βk)，ui∈(-1, 1](βk<i≦βk+μ)，ui∈(-1/2, 1/2](βk+μ<i<n)，ui=1(i=n)に従う．ただし，k<βk<n-μ とする．

提案法 RSRwP では一度だけ係数 u(βk+u)＋…u(n-1)を計算すればよい。その結果、従来法 RSR に比べ，RSRwP は計算量が $O(n^2(k/6)^{k/4})$から $O(k^2\log^2 k(k/6)^{k/4})$に改善した．ただし，k はユーザが指定するパラメータである．RSRwP と RSR の実計算量の見積もりの比較結果を表 2 にまとめる．100 次元では，RSRwP は RSR よりも 35.4%高速であり，最も次元が高い 1000 次元では RSR の 130 倍以上も高速である．

表 2：実計算量の見積(k，μ) = (24，13)

次元 (n)	100	200	500	1000
RSRwP	$2^{24.836}$	$2^{24.838}$	$2^{24.853}$	$2^{24.902}$
RSR	$2^{25.273}$	$2^{27.280}$	$2^{29.929}$	$2^{31.930}$
比率	1.354	5.434	33.734	130.504

ラティス暗号の研究

SVP に関連する暗号化方式である GGH 暗号の安全性を改良した，GGH+暗号を報告する．

GGH+暗号の鍵生成では，直交に近いラティスを構成するよう，基底 **R** を式(**R**←αn^{β}**I**+**P**)に従い，作成する．ただし，α∈Z，1/2≦β<1,n^{β}∈Z，I は単位行列，$p_{i,j}$は置換行列 **P** の要素，$p_{i,j}$∈{-1，0，1}である．次に，**R** の逆行列 **Q** が以下の条件式を満たすかを確認する．満たさない場合は，基底 **R** を再生成する．

$$|q_{i,i}| \le \frac{1}{\alpha n^{\beta}} \text{ かつ } |q_{i,j}|_{j\neq i} < \frac{2}{\alpha^2 n^{2\beta}}$$

$q_{i,j}$を **Q** の要素とする．**Q** が上記の条件を満たせば，**R**(と **Q**)を秘密鍵，**R** の正規エルミート形式を公開鍵 **B** とする．

GGH+暗号における暗号化では，SVP 近似アルゴリズムに対する暗号文の安全性を向上させるため，従来方式よりも(ノルムが)大きな n 次元のベクトル **e** を平文として用いる．ベクトル **e** の要素 e_i はメッセージのバイナリ値(0, 1)に基づき，一様ランダムに二つの集合から選択する．即ち，e_i∈{-s, ‥-1,1, …s}，ただし#{e_i}=n-k かつ e_i∈{-h，h}，ただし#{e_i}=k とする．

生成したベクトル **e** と公開鍵 **B** を用い，GGH+暗号の暗号文を表わす n 次元ベクトル **c** を式(**c**←e-**Bx**)で作成する．復号は，式(**t**←**Qc**-「**Qc**」)よりベクトル **t** を計算し，次いで **Rt**+**Ra**∈{-h, h}∪{-s, ‥-1,1, …s}を満たすベクトル **a** を探索する．最後に，ベクトル **e** を式(**e**←**t**+**a**)より求め，平文を復号する．

GGH+暗号の安全性は，特殊な最近ベクトル問題である唯一最短ベクトル問題に帰着される．この唯一最短ベクトル問題の解読可否は，最短ベクトルと 2 番目に短い第 2 最短ベクトルとの比率で評価できる．GGH+暗号では最短ベクトルがベクトル **e**，第 2 最短ベクトルが最も短い基底であり，式(γ=min||r_i||/||**e**||)で評価できる．即ち、比率γがある閾値を超える場合，暗号文 c が解読可能である．最も強力な SVP 近似アルゴリズムである BKZ に最大値(ブロック長 85)を設定した場合，その閾値は $0.48(1.01)^n$ である．GGH+暗号に各種パラメータ(α=4，β=12，s=3，k=10，h=7，n=400)を設定すると，γ≒5.1<11.63≒$0.48(1.01)^n$ であり，実用的な低次元でも GGH+暗号の安全性が保証可能である．

まとめ

○ 性能に優れた，3 つの群を用いる対称型述語暗号を提案し，Non-intractive な仮定で安全性を証明した.

○ SVP 近似アルゴリズムの一種である RSR に事前計算を導入し，より計算効率の高い RSRwP を提案した.

○ SVP 近似アルゴリズムに耐性を有する GGH+暗号を提案し，その安全性を評価した.