1Y-3

ペアリングを用いた大小比較の秘匿計算の一手法

○宇都宮 秀利 † 毛利 公美 † 白石 善明 ‡ 土井 洋 ††

† 岐阜大学 ‡ 名古屋工業大学 †† 情報セキュリティ大学院大学

1 はじめに

暗号化された 2 つのデータについて，データを秘匿したまま平文の値の大小関係を求めたい場合がある．

例えば以下のような場合が挙げられる．個人の血圧や体重などのバイタルデータを本人もしくは医療機関が長期に渡ってサーバに蓄積し，ある閾値を超えるバイタルデータを示している日時を抽出するなどして健康管理に役立てることを考える．

プライバシーを考慮してデータを暗号化してサーバに預ける場合，データを秘匿したままその大小関係を求めることができるならば，閾値を暗号化してサーバに送ることで，データと閾値を秘密にしたまま当該日時を抽出することができる．しかしながら，一般には平文データを秘匿したままデータの大小を判別するのは容易ではない．

これに対する従来の解決法として，加法準同型暗号を用いた方式がいくつか提案されている [2,3,4]．しかしながらこれらの方式は，大小比較の計算に必要なサーバ数，通信回数の面で課題が残されている．本稿ではその解決法として，ペアリングを用いた準同型暗号に基づく方式を提案する．これにより，従来は複数の比較サーバと復号サーバで実現していた大小判定を，単一の比較サーバと復号サーバで実現できるようになり，通信回数も改善される．本研究では，ペアリングを用いた準同型暗号の中でも，実装を考慮して構造がシンプルな BGN 暗号 [1] を用いる．

2 BGN 暗号

本節では，提案方式で用いる BGN 暗号 [1] について説明する．BGN 暗号はペアリングを用いた準同型暗号で，従来方式で用いられていた加法準同型暗号が持つ加法準同型性に加え，1 回の乗法準同型性を合わせ持つという特徴がある．

2.1 準同型暗号

平文 m_1, m_2 に対する暗号文 $E(m_1), E(m_2)$ が与えられたとき，平文や秘密鍵なしに $E(m_1 \circ m_2)$ を求められるような暗号を準同型暗号という．ただし，$\circ$ は加算 $+$ や乗算・などの演算子である．$E(m_1), E(m_2)$ から $E(m_1 \circ m_2)$ を求めることを，$m_1 \circ m_2$ を暗号文上で計算すると表現する．

2.2 BGN 暗号

2.2.1 表記

- $\mathbb{G}$ と $\mathbb{G}'$ を位数が合成数 N の乗法についての有限巡回群とし，g を $\mathbb{G}$ の生成元とする．
- e は Weil ペアリングである．$e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}'$．全ての $u, v \in \mathbb{G}$ と $a, b \in \mathbb{Z}$ に対して，$e(u^a, v^b) = e(u, v)^{ab}$ が成り立つ．また，$e(g, g)$ は $\mathbb{G}'$ の生成元 g' となる．

2.2.2 BGN 暗号のアルゴリズム

鍵生成:

素数 q_1, q_2 から成る $N = q_1 q_2$ に対して，$(q_1, q_2, \mathbb{G}, \mathbb{G}', e)$ の組を生成する．秘密鍵 $SK = q_1$ に対する公開鍵 $PK = (N, \mathbb{G}, \mathbb{G}', e, g, h)$ を生成する．ここで g, h はそれぞれ，g は $\mathbb{G}$ のランダムな生成元，h は $h = u^{q_2}$ (u は $\mathbb{G}$ のランダムな生成元) で与えられる．

暗号化:

平文 m に対して，ランダムな値 $r \xleftarrow{R} \{0, 1, \cdots, N-1\}$ を選び，

$$E(m) = g^m h^r (\in \mathbb{G}) \tag{1}$$

を計算する．この $E(m)$ を平文 m に対する暗号文として出力する．

復号:

秘密鍵 $SK = q_1$ を用いて，

$$E(m)^{q_1} = (g^m h^r)^{q_1} = (g^{q_1})^m \tag{2}$$

を計算する．$(g^{q_1})^m$ を m について解くことで，暗号文 $E(m)$ から平文 m が得られる．これは m に関する離散対数問題となるため，m の値が大きいと解くことが出来ない．従って，平文 m の取りうる範囲は，$\{0, 1, ..., T\}$ $(T < q_2)$ に設定する必要がある．

2.2.3 BGN 暗号の準同型性

BGN 暗号は以下に示す加法及び乗法に対する準同型性を有する．

加法準同型性

ランダムな値 $r \in \{0, 1, \cdots, N-1\}$ を選び，

$$E(m_1 + m_2) = E(m_1)E(m_2)h^r = g^{m_1+m_2} h^{r'} \tag{3}$$

のように演算することで，$E(m_1), E(m_2)$ から，$m_1 + m_2$ に対する暗号文 $E(m_1 + m_2)$ を作ることができる．

乗法準同型性

$g' = e(g, g)$，$h' = e(g, h)$，$h = g^{\alpha q_2} (\alpha \in \mathbb{Z})$ とするとき，ランダムな値 $r \in \{0, 1, \cdots, N-1\}$ を選び，

$$E(m_1 m_2) = e(E(m_1), E(m_2))h'^r = g'^{m_1 m_2} h'^{\tilde{r}} \in \mathbb{G}' \tag{4}$$

のように演算することで，$E(m_1), E(m_2)$ から $m_1 m_2$ に対する暗号文 $E(m_1 m_2)$ を作ることができる．ただし，$e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}'$ であり，$E(m_1 m_2)$ は $\mathbb{G}'$ の元となるため，$E(m_1 m_2)$ に対して 2 回目以降の乗算を行うことはできない．

このように，ペアリング使用前後で暗号文の群が異なるため，以降では，

- ペアリング使用前の平文 m に対する暗号文：$E(m) \in \mathbb{G}$
- ペアリング使用後の平文 m に対する暗号文：$E'(m) \in \mathbb{G}'$

と表記して区別する．

なお，加法に関しては，任意の平文 m_1, m_2 に対する暗号文 $E'(m_1)$, $E'(m_2)$ が与えられたとき，$E'(m_1 + m_2)$ は，式 (3) の $E(m_1 + m_2)$ と同様に求められる．

以上より，BGN 暗号は任意回数の加法準同型性と，1 回の乗法準同型性を持つ．このことは，2 次以下の任意の多項式を暗号文上で計算できることを意味する．

2.2.4 BGN 暗号の安全性

BGN 暗号は，部分群判定仮定より，semantic secure であることが証明されている [1]．部分群判定仮定とは，位数が $N = q_1 q_2$ の $\mathbb{G}$ からランダムに選ばれた元と，位数 q_1 の $\mathbb{G}$ の部分群からランダムに選ばれた元を識別するのが困難であるという仮定である．

3 加法準同型暗号を用いた大小比較の秘匿計算方式のモデル (従来方式 [2,3,4])

図 1 に，加法準同型暗号を用いてデータを秘匿したまま大小判定を行う方式 (従来方式) のモデルを示す．

ユーザ

データ x, y を公開鍵 PK によって暗号化 $(E(x), E(y))$ し，それを大小比較サーバに送る．

大小比較サーバ群 (簡単のため 2 パーティとする)

ユーザの暗号化データ $E(x), E(y)$ を使い，2 つのデータ x, y の大小関係を求めるための計算式 c(大小比較式) を，2 パーティで協力して暗号文上で計算する．計算された大小比較式に対する暗号文 $E(c)$ を復号サーバへ送る．

復号サーバ

公開鍵/復号鍵ペアを生成．秘密鍵 SK を用いて，大小比較サーバ群から受けとった大小比較式の暗号文 $E(c)$ を復号する．その結果を大小比較サーバ群に返す．方式によっては，復号サーバなしで，大小比較サーバ群が閾値復号法によって復号を行う場合もある．

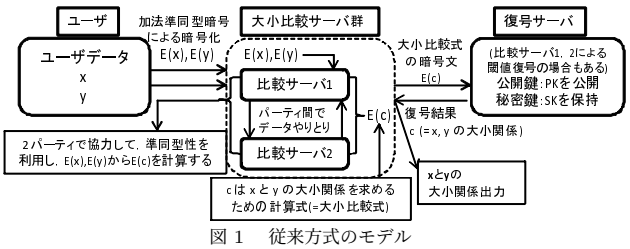

図 1 従来方式のモデル

大小比較式 c は，例えば [2] では x, y についての 2 次多項式，[3] ではさらに大きな次数の多項式の形をしている．この多項式を計算すると，結果として $c = 0$ or 1 のような値が得られ，$c = 1$ ならば $x > y$，$c = 0$ ならば $x \leq y$ というようにその値によって大小判定を行うことができる．

従来方式は加法準同型暗号を用いるため，単独パーティでは暗号文上で x, y についての乗算ができず，2 次以上の多項式を計算することができない．大小比較式中の乗算をデータを秘匿したまま計算するためには，2 パーティ以上でデータをやり取りして計算する必要がある．

このモデルでは，各サーバに対して平文 x, y は秘匿されている．各比較サーバは暗号化データのみを持っており復号の能力を持っていないため，平文

A Method of Secure Data Comparison Using Pairing

† Hidetoshi Utsunomiya and Masami Mohri·Gifu University

‡ Yoshiaki Shiraishi·Nagoya Institute of Technology †† Hiroshi Doi ·Institute of Information Security

データは得られない．復号サーバは復号の能力を持っているが，得られる暗号文は，x, y の大小関係のみを表す大小比較式の暗号文 $E(c)$ なので，平文データは得られない．閾値復号法による復号の場合も，各比較サーバは単独では暗号文を復号できないため，各サーバに対して平文は秘匿されているといえる．

4 ペアリングを用いた大小比較の秘匿計算方式 (提案方式)

ペアリングを用いた準同型暗号に基づき，データを秘匿したまま大小判定を行う方式を提案する．データの形式は長さ n のビット列データ $\boldsymbol{x} = (x_n, ..., x_1) \in \{0,1\}^n, \boldsymbol{y} = (y_n, ..., y_1) \in \{0,1\}^n (x_1, y_1$ を最下位ビットとする) を対象とし，これらのデータに対する大小比較式として，4.1 に示すような 2 次多項式 [2] を用いる．従来の方式では，大小比較のための 2 次多項式を単一パーティで計算することができなかったが，本研究では暗号文上で 2 次多項式を計算可能な BGN 暗号を用いることでこれを実現する．

4.1 大小比較式

ビット列データ $\boldsymbol{x} = (x_n, ..., x_1)$ と $\boldsymbol{y} = (y_n, ..., y_1)$ から計算できる大小比較式として，以下のような 2 次多項式 [2] c_i $(i = 1, 2, ..., n)$ を用いる．

$$c_i = y_i - x_i + 1 + \sum_{j=i+1}^{n} w_j \ (for\ i = 1, 2, ..., n) \tag{5}$$

ただし, $w_j = x_j \oplus y_j = x_j + y_j - 2x_j y_j$

この c_i について次のことが言える．

- $\boldsymbol{x} > \boldsymbol{y}$ なら，$c_i = 0$ となる i が 1 つ存在する．
- $\boldsymbol{x} \leq \boldsymbol{y}$ なら，$c_i = 0$ となる i は存在しない．

この性質より，$c_i (i = 1, 2, ..., n)$ のうち $c_i = 0$ を満たす c_i が存在するか否かによって大小比較を行うことができる．提案方式は，この c_i を暗号文上で計算し，復号結果が 0 になるものがあるかどうかで大小を判定する．

4.2 提案方式のモデル

ユーザ

ビット列データ $\boldsymbol{x} = (x_n, ..., x_1) \in \{0,1\}^n$, $\boldsymbol{y} = (y_n, ..., y_1) \in \{0,1\}^n$ を，BGN 暗号の公開鍵 PK によって暗号化する．生成された暗号文 $E(\boldsymbol{x}) = E(x_n), ..., E(x_1), E(\boldsymbol{y}) = E(y_n), ..., E(y_1)$ を大小比較サーバに送る．

大小比較サーバ

ユーザの暗号化データ $E(\boldsymbol{x}), E(\boldsymbol{y})$ を使い，2 つのデータ $\boldsymbol{x}, \boldsymbol{y}$ の大小関係を求めるための計算式 $\boldsymbol{c}$(大小比較式) を暗号文上で計算する．ただし，$\boldsymbol{c} = (c_1, ..., c_n)$ で，c_i は式 (5) に与えた次数が 2 次以下の式である．計算された大小比較式の暗号文 $E(\boldsymbol{c})$ を復号サーバへ送る．

復号サーバ

秘密鍵 SK を用いて，大小比較サーバから受けとった大小比較式の暗号化 $E(\boldsymbol{c})$ を復号する．その結果を大小比較サーバに返す．

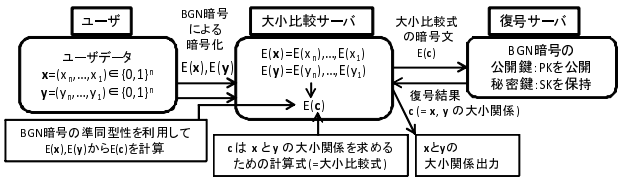

図 2　提案方式のモデル

4.3 提案方式の処理の流れ

1．データの暗号化

ユーザは，データ $\boldsymbol{x} = (x_n, ..., x_1)$, $\boldsymbol{y} = (y_n, ..., y_1)$ を，復号サーバの公開鍵で暗号化した $E(\boldsymbol{x}) = E(x_n), ..., E(x_1), E(\boldsymbol{y}) = E(y_n), ..., E(y_1)$ を大小比較サーバへ送る．

2．大小比較式の計算のための準備

大小比較サーバは，ユーザから受け取った暗号化データ $E(\boldsymbol{x}) = E(x_n), ..., E(x_1), E(\boldsymbol{y}) = E(y_n), ..., E(y_1)$ を，以下のようにして $E'(\boldsymbol{x}) = E'(x_n), ..., E'(x_1), E'(\boldsymbol{y}) = E'(y_n), ..., E'(y_1)$ に変換する．

$$E'(x_i) = e(E(1), E(x_i)) \ (for\ i = 1, 2, ..., n)$$

$\boldsymbol{y}$ についても同様である．これは暗号文の群を統一するための操作である．式 (5) の第 4 項を暗号文上で計算するためにペアリングを用いるが，ペアリングの使用前後では暗号文の群が異なるため，後の式 (6) の演算のために群を $\mathbb{G}'$ に統一しておく必要がある．

3．大小比較式の秘匿計算

大小比較サーバは，BGN 暗号の準同型性を利用して，$E'(c_i)$ $(for\ i = 1, 2, ..., n)$ を計算する．ただし，

$$c_i = y_i - x_i + 1 + \textstyle\sum_{j=i+1}^{n} w_j$$

$$w_j = x_j \oplus y_j = x_j + y_j - 2x_j y_j$$

である．具体的には以下の計算を行う．

$$E'(c_i) = E'(y_i) E'(x_i)^{-1} E'(1) \prod_{j=i+1}^{n} E'(x_j) E'(y_j) E'(x_j y_j)^{-2} \tag{6}$$

$$(\text{ただし，} E'(x_j y_j) = e(E(x_j), E(y_j)) \ )$$

4．ランダム化処理

大小比較サーバは，復号サーバに平文の値を推測されないようにランダム化を行う．そのために $E'(c_i)^{r_i} = E'(r_i c_i)$ (r_iは $r_i \in \mathbb{Z}_N$ のランダムな値) を計算する．さらに，大小比較サーバは，n 個の $E'(r_i c_i)$ $(i = 1, 2, ..., n)$ をランダムな順番に並び替えて，復号サーバへ送る．

5．大小比較式の復号

復号サーバは秘密鍵 SK を使って，$E'(r_i c_i)$ の復号結果が 0 になるものがあるか調べる．あれば 0 を，そうでなければ 1 を返す．

6．大小関係の出力

大小比較サーバは，5. の返り値が 0 であれば $\boldsymbol{x} > \boldsymbol{y}$ を，1 であれば $\boldsymbol{x} \leq \boldsymbol{y}$ を出力する．

5 提案方式に対する評価

5.1 安全性の評価

安全性の定義

大小比較サーバと復号サーバは，それぞれ honest but curious(プロトコルに従うが，不正に情報を入手しようとする) に振る舞うと仮定する．大小比較サーバが，ユーザの平文データに関する大小比較結果以外のいかなる情報も得られないとき，大小比較サーバはユーザにとって安全であると定義する．同様に，復号サーバが，ユーザの平文データに関する大小比較結果以外のいかなる情報も得られないとき，復号サーバはユーザにとって安全であると定義する．大小比較サーバと復号サーバがユーザにとって安全であるとき，この方式はユーザにとって安全であるとする．

(1) 大小比較サーバのユーザに対する安全性

大小比較サーバが得られるのは，BGN 暗号で暗号化されたデータと復号サーバからの返り値のみである．2.2.4 で示した BGN 暗号の安全性より暗号文からは平文についての情報を得られない．また，復号サーバからの返り値 (0 or 1) は大小関係のみを表すので，平文についての情報を得られない．よって大小比較サーバはユーザにとって安全である．

(2) 復号サーバのユーザに対する安全性

復号サーバが得られるのは，n 個のランダム値，または $n-1$ 個のランダム値と 1 個の 0 である．ランダム値からは，平文についての情報は得られない．得られる値に 0 が含まれる場合，ある i 番目の比較式 c_i が 0 になるということである．これは，式 (5) より $j = i+1, i+2, ..., n$ の x_j, y_j について，$x_j = y_j$ であることがわかってしまうことを意味する．しかし，4.3 の 4. において，全ての i の順番はランダムに並び替えられるため，この場合も平文についての情報は得られないと言える．よって復号サーバはユーザにとって安全である．

(1),(2) より提案方式はユーザにとって安全である．

5.2 従来法との比較

		提案方式	[2]の方式 (論文内5.2の方式)	[3]の方式	[4]の方式
データ形式		ビット列データ(長さn)	ビット列データ(長さn)	ビット列データ(長さn)	整数値(≠ビット列)
特徴		加法準同型性と1回の乗法準同型性を持つBGN暗号を用いる	加法準同型性を持つ暗号を用いる ユーザデータは秘密分散により2つのサーバに保存	加法準同型性を持つ暗号を用いる (t,m)閾値復号法による復号 (閾値として t= mを採用)	加法準同型性を持つ暗号を用いる (t,m)閾値復号法による復号 (閾値として t= mを採用)
計算量	暗号化(ユーザ処理)	$2nA_1$	0	$4nA_3$	$4B_4$
	比較式計算	$n(3C+B_1)$	$7nB_2$	$12ntA_3$	$5tB_4$
	復号	$(1/2)nB_1$	nB_2	$2tA_3$	$4tB_4$
通信回数		4	7	4	3
通信データ量(bit)		$3n \log_2 N_1$	$4n \log_2 N_1$	$10nt \log_2 N_3$	$10t \log_2 N_1$
比較式計算に必要なサーバ数		1	2	t	t

<計算量>
A：楕円スカラー倍算 $(A_1 > 6A_3)$, B：べき乗剰余演算 $(B_2 < B_1 \approx B_4)$, C：ペアリング演算
<データ量>
N_1：素因数分解不可能な大きさが必要, N_3：楕円離散対数計算不可能な大きさが必要 $(\log_2 N_1 > 6 \log_2 N_3)$

図 3　従来方式との比較

図 3 より，提案方式は従来方式に比べて比較式計算に必要なサーバ数を減らすことができ，通信回数に関して最も優れているということがわかる．

6 まとめ

本稿では，ペアリングを用いた準同型暗号に基づき，データを秘匿したまま大小判定を行う方式を提案した．ペアリングを用いることで単一パーティで大小比較式の秘匿計算が可能となり，従来方式より通信回数が改善されることを示した．

参考文献

[1] D. Boneh, E.-J. Goh, K. Nissim,“ Evaluating 2-DNF Formulas on Ciphertexts, ” TCC'05, LNCS vol.3378, pp.325-341, 2005.
[2] I.Damgård, M.Geisler, M.Krøigård,“ Homomorphic encryption and secure comparison, ”International Journal of Applied Cryptography, vol.1, No.1, pp.22-31, 2008.
[3] B.Schoenmakers, P.Tuyls,“ Practical Two-Party Computation based on the Conditional Gate, ”In Advances in Cryptology-ASIACRYPT'04, LNCS vol.3329, pp.119-136, 2004.
[4] F. Kerschabaum, D. Biswas, S. de Hoogh,“ Performance Comparison of Secure Comparison Protocols, ”2009 20th International Workshop on Database and Expert Systems Application, pp.133-136, 2009.