安全でコンパクトかつ高速な代数的トーラス暗号

Secure, Compact, and Efficient Algebraic Torus-Based Cryptography

米村　智子　　村谷　博文
■ YONEMURA Tomoko　■ MURATANI Hirofumi

“代数的トーラス暗号”は離散対数問題に基づく公開鍵暗号で，安全性，コンパクト性，及び高速性に優れ，幅広い応用が期待される。公開鍵暗号はネットワーク セキュリティを実現するために不可欠な技術であり，この技術を用いることで，送信者と受信者の間で鍵をあらかじめ共有することなく，ネットワークを介して見知らぬ相手と安全に通信を開始できる。

東芝は，安全性と高速性を両立する代数的トーラス暗号のパラメータ設計法を開発した。これにより，安全性を保ちながら代数的トーラスの基本演算のサイズを小さくすることに成功し，その結果，処理速度はだ円曲線暗号とほぼ同等で，鍵サイズはだ円曲線暗号に迫る大きさにできることがわかった。

Algebraic torus-based cryptography are a secure, compact, and efficient means of public-key cryptography based on a discrete logarithm problem. Cryptography is essential in the implementation of a network security system, enabling strangers to engage in secure communication via the network without the need for sharing of keys between the sender and receiver.

Toshiba has developed a parameter selection method for algebraic torus-based cryptography from the viewpoints of both security and efficiency. More specifically, we have obtained parameters that can achieve smaller size of the fundamental arithmetic in the algebraic torus while maintaining security. As a result, the speed of algebraic torus-based cryptography is comparable to and the key size is close to those of an elliptic curve-based cryptography.

1　まえがき

暗号技術は情報セキュリティを実現する基盤技術として幅広く利用されている。**図1**に示すように，暗号は共通鍵暗号と公開鍵暗号に大別される。

東芝は，比較的新しい公開鍵暗号であり，安全性を保証しながら処理速度や鍵サイズの点で有利な“代数的トーラス暗号”を研究開発している。その結果，次世代の公開鍵暗号として期待されている“だ円曲線暗号”と同程度の処理速度が，代数的トーラス暗号で達成できることがわかってきた。

ここでは，代数的トーラス暗号の概要，及びパラメータ設計法開発の背景と現状について述べる。

2　公開鍵暗号方式の相互関係

今日までに様々な公開鍵暗号が提案されているが，それらの相互関係を，以下の観点から示したのが**図2**である。

(1)　具体的な暗号スキーム（方式）
(2)　スキームが定義されている集合
(3)　安全性の根拠となる問題

暗号スキームには多数あるが，図2には代表例として，Rivest，Shamir，Adlemanの提案による有名な“RSA暗号”，1976年DiffieとHellmanの提案による最初の公開鍵方式である“DH鍵配送”，及び2000年にCramerとShoupによって提案され最強の安全性を持つ“CS暗号”を図示した。また，いくつかの専門用語が含まれているが，それらの意味は3章～6章で詳しく述べる。

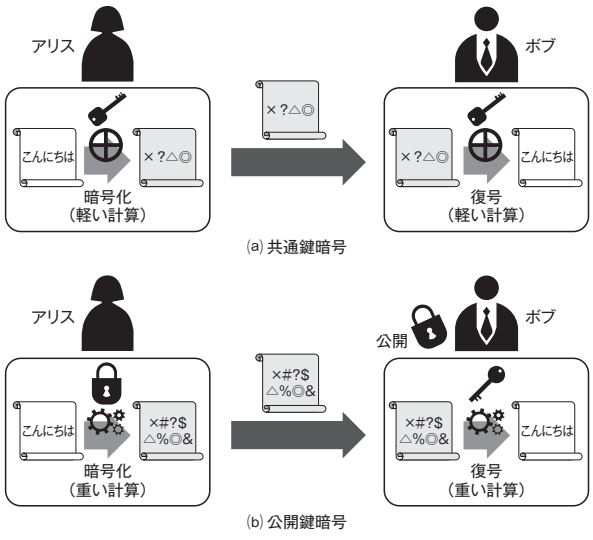

図1. 共通鍵暗号と公開鍵暗号 — 共通鍵暗号では暗号化鍵と復号鍵に同一の鍵を用いるが，公開鍵暗号では暗号化鍵と復号鍵に異なる鍵を用い，暗号化鍵は公開されている。
Secret-key cryptography and public-key cryptography

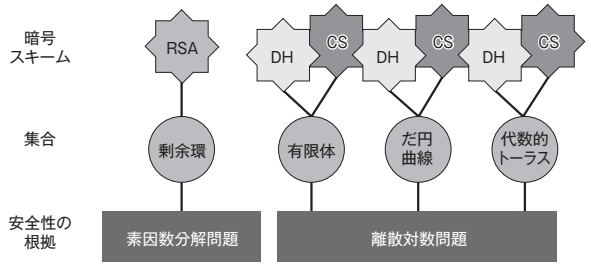

図2. 公開鍵暗号の相互関係 — 今日までに提案されている有名な公開鍵暗号の相互の関係を，暗号スキーム，集合，及び安全性の根拠という三つの観点から整理した。

Interrelationships among public-key cryptography schemes

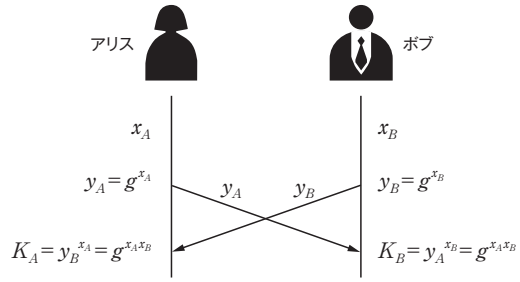

図3. DH鍵配送方式 — DH鍵配送においてアリスとボブが行う操作を示す。秘密情報x_Aを用いた操作はアリスが行う左側の計算にしか登場せず，秘密情報x_Bを用いた操作はボブが行う右側の計算にしか登場しない。公開情報y_Aとy_Bはアリスとボブの中間にあり，第三者も知ることができる。

Diffie-Hellman (DH) key exchange

暗号の安全性の根拠となるものに，“素因数分解問題”と“離散対数問題”がある。以下では代数的トーラス暗号と関係のある離散対数問題に焦点を絞って説明する。離散対数問題が定義される集合として“有限体”，“だ円曲線”，及び“代数的トーラス”の三つがある。

1970年代の最初の公開鍵暗号は，有限体を用いて構成された。その後，1980年代には，だ円曲線を用いるとより短い鍵サイズで暗号が構成できることがわかった。更に，2000年代になって，代数的トーラスを利用した暗号が提案された[1]。このような新しい集合の採用は，高速でコンパクトな暗号の探索の歴史と重なっている。

だ円曲線の離散対数問題に基づく暗号スキームは多数あるが，それらを総称してだ円曲線暗号と呼ぶ。代数的トーラス暗号も特定の方式を指すのではなく，代数的トーラスで構成された暗号スキームの総称である。

3　DH鍵配送

DH鍵配送の目的は，送受信者が安全ではない通信路を用いて，秘密裏に同一の鍵を共有することで，DH鍵配送の操作は，**図3**に示すように，次のようなステップで行われる。

ステップ1　　アリスは正の整数x_Aをランダムに選択し，x_Aを秘密にして保持する。

ステップ2　　アリスは公開情報gを用いて，$y_A=g^{x_A}$を計算し，y_Aを公開する。

ステップ3　　アリスはボブが公開するy_Bを用いて，$K_A=y_B^{x_A}$を計算する。

ボブもアリスと同様の手続きを実行するならば，最終的にボブは$K_B=y_A^{x_B}$を保持する。K_AとK_Bはともに$g^{x_Ax_B}$と等しいので，アリスとボブはK_AとK_Bを同一の鍵（共通鍵）として共有することができ，これ以後の通信を，この共通鍵を用いた暗号で保護する。

注意したいのは，ステップ2とステップ3の計算$y=g^x$は単にべき乗するのではなく，結果が常に一定のけた数に収まるように，結果を整数pで割った余りに置き換えることである。もし，通常の意味で$y=g^x$を計算したのならば，対数関数$x=\log_g y$を用いてxを簡単に計算できる。したがって，通信路上を流れる公開情報y_Aとy_Bから，アリスとボブの秘密情報x_Aとx_Bが求まり，第三者にも共通鍵が計算できてしまう。

一方，結果をpで割った余りで置き換えると，xとyが連続的な関係を持たない。このとき，yとgを与えられてxを求める問題を離散対数問題という。次章では，離散対数問題とは何かを数値例を用いて説明する。

4　有限体と離散対数問題

四則演算（加減乗除）が定義されている数の集合を，数学では体（たい）と呼ぶ。身近な数である実数は体の一つである。実数の場合は要素数が無限であるが，体の中には要素数が有限であるような体もある。そのような体を有限体と呼ぶ。ここでは要素の個数がp個の有限体を記号F_pで表すことにする。

有限体の具体例として，$F_5=\{0,1,2,3,4\}$を考える。この集合において，乗算は**表1**のように行うものとする。表1は，要素

表1. 有限体の乗算表

Multiplication in finite field F_5

×		F_5の要素				
		0	1	2	3	4
F_5の要素	0	0	0	0	0	0
	1	0	1	2	3	4
	2	0	2	4	1	3
	3	0	3	1	4	2
	4	0	4	3	2	1

の間で通常の乗算を行い，結果が4より大きくなったときは，5で割った余りで置き換えることによって導かれる。加減算も同様に定義され，除算は乗算表から導出できる。

ここで，簡単な離散対数問題の例を示す。有限体F_5で3^xが4となるときのxを求めてみよう。xを1から順に大きくしてみると，$3^2 \div 5$の余りは4であることから，x=2のとき結果が4となることがわかる。

有限体F_5ではpが5と小さかったのでxを総当たりで計算できた。しかし，極めて大きなp，例えば十進数で600けた程度のpに対して離散対数問題を解こうとすると，その計算量は膨大になり，事実上不可能であることが知られている。

5　だ円曲線上の演算の離散対数問題

DH鍵配送は，提案時には有限体上の離散対数問題に基づいて構成された。一方，だ円曲線上の点の加算に関しても離散対数問題が定義される。

典型的なだ円曲線を**図4**に示す。だ円曲線上に与えられた点Aと点Bから，別のだ円曲線上の点Cを以下の手順で決めることができる。

(1)　点Aと点Bを通る直線lを引く。

(2)　直線lとだ円曲線の交点から，横軸に垂直な直線mを引く。

(3)　直線mとだ円曲線の交点を点Cとする。

この点Cの座標値は点Aと点Bの座標値を加算したものと定義し，記号C=A+Bで表す。

次に，だ円曲線上で点Gを一つ決めて，点Gを何回加算すれば与えられた点Yと一致するか，という問題を考える。すなわち，次式となるスカラ値xを求める問題である。

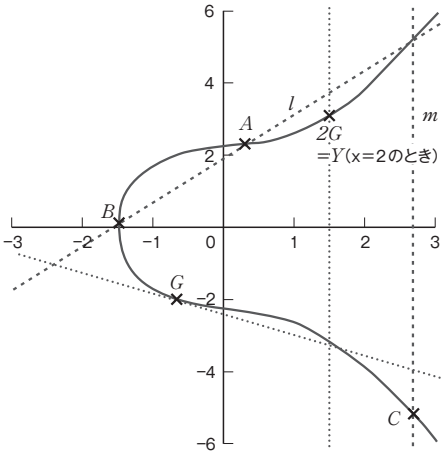

図4．だ円曲線上の点の加算 — だ円曲線上の点Aと点B及びそれらの加算の結果である点Cの位置関係を示す。実線はだ円曲線を表し，点A，点B，点Cは破線で表した直線lと直線mによって関係付けられている。

Point addition in elliptic curve

$$Y = \underbrace{G + G + \cdots + G}_{x\text{個}} = xG$$

これがだ円曲線上の離散対数問題であり，曲線上にとれる点の個数が極めて大きいとき，例えば十進数で70けた程度の個数のときなど，離散対数問題は事実上解けない。

有限体に比べると集合のサイズがけた数で9分の1程度に小さくなるため，コンパクトな暗号を構成することができる。

6　代数的トーラスの離散対数問題

代数的トーラスは，有限体の要素の中から少数の要素だけを抜き出して作られる部分集合であって，その乗算は有限体の乗算と同じ操作で行われる。このため，有限体やだ円曲線上の点の加算と同様に，代数的トーラス上でも離散対数問題が定義される。

要素を抜き出すときには，代数的トーラス全体がより小さな有限体に含まれることのないようにする（**図5**）。これにより，代数的トーラスは要素の個数が比較的大きい有限体の安全性を保つと考えられる。大きな個数の要素の集合，例えば十進数で200けた程度の個数の要素の集合に対して，代数的トーラス上の離散対数問題が解けない。

有限体に比べると，集合のサイズがけた数で3分の1程度に小さく，安全な暗号を構成することができる。

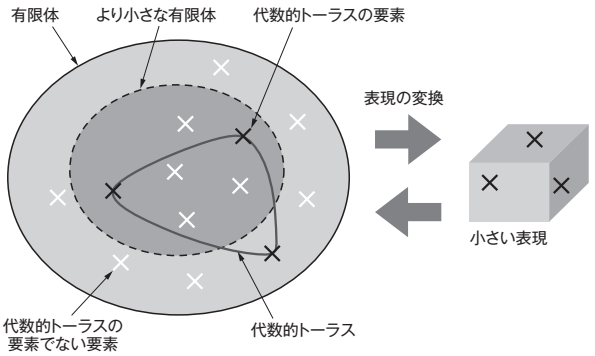

図5．代数的トーラスの性質 — 代数的トーラスは有限体の部分集合であり，より小さな有限体に包含されないようにする。また，代数的トーラスはその要素の個数に見合ったサイズで表現される。

Properties of algebraic torus

7　コンパクトで安全な代数的トーラスの設計

7.1　処理速度の比較

代数的トーラス，だ円曲線，有限体を用いたDH鍵配送の鍵サイズと処理時間の比較を**図6**に示す。

図6から，代数的トーラスの処理時間はだ円曲線と同程度

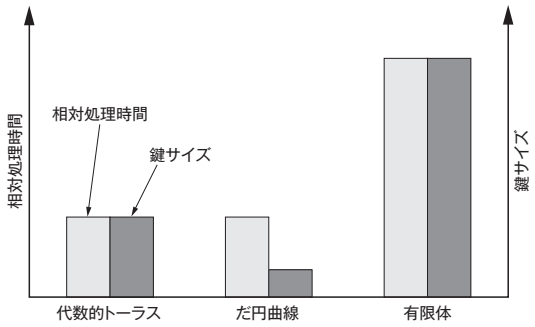

図6. DH鍵配送の鍵サイズと処理時間の比較 — 代数的トーラスと有限体は相対処理時間と鍵サイズがつり合っており，だ円曲線はつり合っていない。今後，代数的トーラスの鍵サイズをだ円曲線と同等まで小さくすることで，相対処理時間はだ円曲線より小さく抑えられる可能性がある。

Comparison of key size and calculation time of DH key exchange

であり，有限体の3分の1程度であることがわかる。代数的トーラスの鍵サイズは有限体と比べるとはるかに小さく，だ円曲線暗号に近い。現時点では，だ円曲線暗号に対して鍵サイズで優位性があるとは言えないが，処理時間は既にほぼ同等である。これらの結果は，次節で述べるパラメータ探索の結果得られたものである。

今後，鍵サイズの改良と更なる高速実装の検討を行うことで，だ円曲線に対して処理時間で優位になる可能性もある。

7.2 代数的トーラスのパラメータ探索

ここでは，登山ルートの開拓になぞらえてパラメータ設計の概要を述べる。**図7**は，有限体，代数的トーラス，及びだ円曲線を山のイメージで示したものである。各山頂の高さが安全性を，すそ野の幅が鍵サイズを表している。

代数的トーラスは，有限体の部分集合として定義されるため，対応する有限体と相互に行き来することができる。図7では，山頂に架かっている橋でこれを表現しており，代数的トーラスの安全性の担保にもなっている。

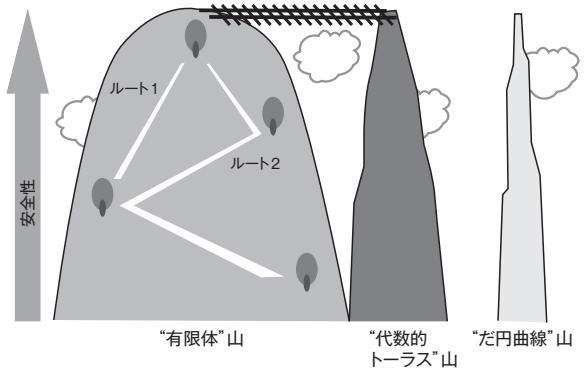

図7. パラメータ探索のイメージ — “有限体”山の登山ルート（ルート1，ルート2）を開拓することが，パラメータ探索に相当する。より簡単な登山ルートを見いだせれば，実現される暗号の計算も容易になる。

Image of parameter selection

与えられた制約条件を満たすような“有限体”山の登山ルートを開拓することが，代数的トーラスのパラメータ探索に相当する。より簡単な登山ルートを見いだせれば，実現される暗号処理（暗号化と復号）の計算も容易になる。

図7の登山ルート1は従来から知られていたルートであり，比較的標高の高い登山口から一気に山頂にたどり着くルートである。ルート2は当社が新たに見いだしたルートで，比較的低い標高にある登山口から，3回のステップで山頂を目指すルートである。登山口の標高は代数的トーラスの基本演算のサイズに対応するため，ルート1よりもルート2で構成された暗号のほうが，演算が簡単になる。

当社はこのようなパラメータ探索により，安全性と高速性を両立するパラメータを導出した[2]。

8 あとがき

コンパクトで高速に処理できる代数的トーラス暗号の研究開発について背景と現状を述べた。

当社は，代数的トーラスを導出する有限体の構成法に工夫を凝らすことによって，安全性と高速性を両立するパラメータを導出した。現状では，処理時間は有限体より小さく，だ円曲線暗号とほぼ同等である。また，鍵サイズは有限体よりはるかに小さく，だ円曲線暗号に迫る大きさである。

今後は，更なる鍵サイズの改良と高速実装の検討を行い，鍵サイズと処理時間で圧倒的に優位な方式の開発を進める。

文 献

(1) Rubin, K. ; Silverberg, A. "Torus-Based Cryptography". Advances in Cryptology－CRYPTO2003, Vol. 2729 of LNCS. Santa Barbara, California, USA, 2003-08, International Association for Cryptologic Research. Springer-Verlag, 2003, p.349－365.
(2) 米村智子，ほか．代数的トーラス上の暗号系 ― 安全性と効率を両立するパラメータ生成法．信学技報．ISEC2008-67, 108, 207, 2008, p.25－32.

米村 智子 YONEMURA Tomoko
研究開発センター コンピュータ・ネットワークラボラトリー。暗号技術の研究・開発に従事。電子情報通信学会会員。
Computer & Network Systems Lab.

村谷 博文 MURATANI Hirofumi, D.Sc.
研究開発センター コンピュータ・ネットワークラボラトリー主任研究員，理博。暗号技術及び暗号応用システムの研究・開発に従事。電子情報通信学会，情報処理学会，IEEE会員。
Computer & Network Systems Lab.