代数的トーラスを用いた暗号圧縮技術

安全性を維持しつつ，暗号メッセージを3分の1以下に圧縮する

公開鍵暗号は，ネットワーク セキュリティなどの基盤技術として幅広く利用され，近年では小型機器にも適用されています。一方，解読が困難な暗号の鍵サイズは年々大きくなっています。これに伴い，暗号メッセージのサイズも増大します。

暗号圧縮技術を用いると，安全性を維持しつつ，暗号メッセージのサイズを3分の1以下に圧縮できます。これにより，メモリ容量や通信帯域が十分でない機器でも，安全性を損なわずに公開鍵暗号を利用することができます。

今回，実用的な多くの公開鍵暗号に対して，あらゆる鍵サイズの暗号メッセージも圧縮できる技術を開発しました。今後は，圧縮率のいっそうの改善に加え，圧縮されたメッセージに対する暗号処理の効率化を検討していきます。

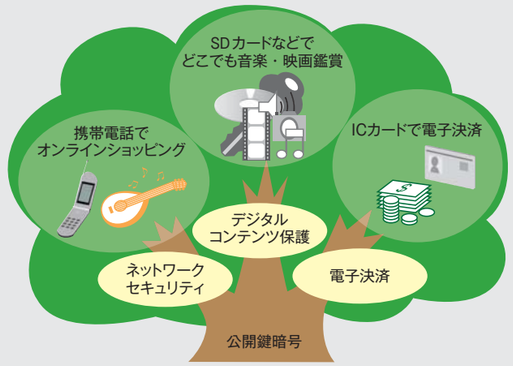

図1. 暗号技術の利用シーン ― 公開鍵暗号は，ネットワーク セキュリティ，デジタルコンテンツ保護，電子決済などの基盤技術として幅広く利用されています。

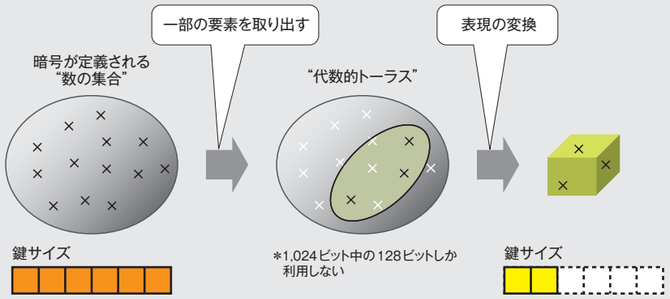

図2. 暗号圧縮の原理 ― 暗号が定義される数の集合について，暗号化に用いられる要素を代数的トーラスと呼ばれる部分集合から選択し，表現を小さく変換します。

表1. 暗号の鍵サイズ

利用時期（年）	共通鍵暗号（ビット）	公開鍵暗号（ビット）		
	AES	DSA，D-H	RSA	ECDSA
～2010	128	1,024	1,024	160
2011～2030	128	2,048	2,048	224
2030～	128	3,072	3,072	256

AES（Advanced Encryption Standard）：NIST（米国商務省国立標準技術研究所）により選定された次世代標準暗号方式
DSA（Digital Signature Algorithm）：NISTにより開発されたデジタル署名方式
D-H：Diffie-Hellman鍵交換プロトコル
ECDSA：だ円DSA

出典：NIST SP 800-57
http://csrc.nist.gov/publications/nistpubs/

表2. 暗号圧縮技術の比較

提案年	提案者	圧縮率	問題点
2003	Rubin（スタンフォード大学） Silverberg（オハイオ州立大学）	3分の1	パラメータ制約あり
2004	van Dijk（フィリップス／マサチューセッツ工科大学） Woodruff（マサチューセッツ工科大学）	3分の1以下	付加入力が大
2005	van Dijk（マサチューセッツ工科大学），ほか	3分の1以下	パラメータ制約あり
2006	東　芝	3分の1以下	上記の問題を解決

暗号圧縮の必要性

ICカードで電子決済，携帯電話でオンライン ショッピング，今では一般的となったこれらのサービスの安全性を支えているのが暗号技術です（**図1**）。暗号には大きく分けて2種類の機能があります。一つ目は，個人情報など他人に知られたくない情報の秘匿です。二つ目は，初めて通信する相手と安全な通信が開始できることです。これらの機能は，それぞれ共通鍵暗号と公開鍵暗号が担っています。共通鍵暗号に比べると，公開鍵暗号は鍵が長く処理も重いことが知られています。しかしながら，ネットワークが発達した今日において欠かすことのできない重要な技術であるため，小型機器でも方式や実装を工夫して利用されるようになってきました。

一方で，計算機の進歩とともに攻撃者の能力も上がり，解読が困難とされる暗号の鍵の長さは年々大きくなっています（**表1**）。この鍵サイズの増大が問題になることがあります。公開鍵暗号では，暗号メッセージのサイズは鍵サイズ程度となるため，鍵よりも小さいメッセージを暗号化する際には，暗号メッセージの方が元のメッセージよりも長くなります。つまり，大きなビット数で小さいメッセージを表しており，むだが生じます。しかしながら，鍵サイズは安全性の要件から決まるため，小さいメッセージだからといって勝手に変更して小さくすることはできません。この問題を解決するのが，暗号圧縮技術です。

暗号圧縮技術を用いると，安全性を維持しつつ暗号メッセージのサイズを3分の1以下に圧縮できます。これにより，メモリ容量や通信帯域が十分ではない機器でも，安全性を損なうことなく公開鍵暗号を利用できるようになります。システム全体の安全性は，そこで組み合わされている暗号のうち，もっとも低い安全性で決まります。したがって，暗号圧縮技術を用いて，暗号処理能力の低い機器で利用される公開鍵暗号の安全性を引き上げることは，システム全体の安全性を高めることにつながります。

暗号圧縮とその課題

公開鍵暗号は，素因数分解問題に基づく方式と，離散対数問題に基づく方式に分類されます。暗号圧縮は後者の方式に対して可能です。

暗号圧縮の原理を説明します。暗号で用いる鍵のサイズが1,024ビットであるとは，別な見かたをすれば，暗号が定義される数の集合が1,024ビットであるということです。ここで，1,024ビットの暗号を用いて128ビットのメッセージを暗号化する場合を考えます。この場合，実際の暗号化に用いるのは，数の集合のうち一部の要素で十分です。そこで，使用する要素を代数的トーラス(注1)と呼ばれる部分集合から選択すると，表現を小さく変換できます（**図2**）。部分集合として代数的トーラスを用いても，元の暗号の安全性は維持されることが示されています。

これまでに，いくつかの暗号圧縮技術が提案されています（**表2**）。しかしながら，効率よく圧縮できる条件があり，条件から外れた場合には，圧縮の際に非常に大きな付加入力が必要となるという問題がありました。

パラメータ制約のない暗号圧縮

東芝は，大きな付加入力なしには圧縮できないとされていた場合について，今回，円分多項式間の恒等式を用いて変換できることを示し，具体的な変換方法を提案しました。これにより，小さな付加入力で任意の鍵サイズの暗号メッセージが圧縮可能になりました。

今後の展望

公開鍵暗号の鍵サイズは，今後も更に増大し続けると考えられます。一方，ユビキタス コンピュータ，ユビキタス ネットワークの実現された社会(注2)においては，情報端末の多様化が進み，より小さなメモリ容量や通信帯域を持つ機器での公開鍵暗号の利用も増えると予想されます。これら二つの相反する要求に対応していくためには，圧縮率のいっそうの改善が効果的です。

また，暗号メッセージの圧縮に加えて，小さな表現のまま暗号化や復号の処理を効率よく行うことも，多様な応用を考えるうえで重要な課題の一つです。今後も，様々な小型機器における制約を考慮し，暗号圧縮技術の実用化について検討していきます。

（注1） トーラスとは，ドーナツ状のチューブにおいて，チューブの直径とチューブで作られた輪の直径のように，周期が二つある面を言う。代数的トーラスとはここから派生し，数の集合の中から，ある規則で数を選んで作った集合のこと。このような数の集合は，複数の周期を持つという特徴がある。

（注2） いつでも，どこでも，だれでもが，コンピュータ ネットワークをはじめとしたネットワークにつながることにより，様々なサービスが提供され，人々の生活が豊かになる社会。

米村　智子

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