符号理論･暗号理論

- No.11 電子署名 -

渡辺　裕

Coding Theory / Cryptography

- No.11 Digital Signature -

Hiroshi Watanabe

電子署名 (1)

- 定義
  - 電子文書に与える電子的なサイン
- 特徴
  - 本人確認，偽造・改竄(かいざん)の防止が目的
  - 公開鍵暗号方式に基づくデジタル署名
    - RSA, DSA, ECDSA
    - 「電子署名及び認証業務に関する法律に基づく特定認証業務の認定に係る指針」の第3条
- 存在的偽造不可能性
  - EUF-CMA: Existential Unforgeability against Adaptive Chosen Message Attacks

Digital Signature (1)

- Definition
  - Electronic signature given to digital document
- Characteristics
  - Purpose is Personal identification, prevent falsification
  - Digital signature based on Public key encryption
    - RSA, DSA, ECDSA
    - Japanese law for digital signature
- EUF-CMA: Existential Unforgeability against Adaptive Chosen Message Attacks

電子署名 (2)

- 電子署名モデル
  - 鍵生成アルゴリズム
    - 署名が必要なユーザが使用
    - セキュリティパラメータを乱数として入力
    - 公開鍵と秘密鍵を出力
  - 署名生成アルゴリズム
    - 公開鍵(検証鍵)を他人に公表
    - 秘密鍵(署名鍵)とメッセージを生成アルゴリズムに入力
    - メッセージに対する署名者の署名文を出力
  - 検証アルゴリズム
    - メッセージと署名文を受信
    - 公開鍵を用いて署名文が有効かどうかを検証

Digital Signature (2)

- Digital signature model
  - Key generation algorithm
    - User who requires signature uses
    - Input security parameter randomly
    - Output public and private key
  - Signing algorithm
    - Open public (verifying) key to others
    - Input message and private (signing) key
    - Output signature to message
  - Verifying algorithm
    - Receive message and signature
    - Verify by public key, message and signature

公開鍵の認証 (1)

- 公開鍵を公開するためには信頼できる第3者が必要
- 公開鍵を公開鍵の持ち主と対応させる手法
  - 信頼できる第三者機関(Trusted Third party)が各人のIDと公開鍵を対応付けた表(公開鍵簿)を作成し公開する
  - 信頼できる第三者機関(達)が認証局を運営し, PKI(Public Key Infrastructure)の仕組みを用いる事で各人のIDと公開鍵を対応付ける
- 認証局の例: MS Internet explorer → Tool → Internet Option → Content → Certificate

Verification of public key (1)

- Trusted third party is required to open public key
- Ways to correspond public key to its owner
  - Trusted Third party open table showing each ID and public key
  - Trusted third party operates certificate authority, uses framework of PKI(Public Key Infrastructure) to match personal ID and public key
- Example of certificate authority: MS Internet explorer → Tool → Internet Option → Content → Certificate

公開鍵の認証 (2)

- ITU-T X509の証明書フォーマット
  - Version 1項目(必須)
    - バージョン情報(version)
    - シリアル番号(serialNumber)
    - 署名アルゴリズム情報(signature.algorithmIdentifier)
    - 発行認証局名(issuer)
    - 有効期限(validity)
    - 被発行者名(subject)
    - 公開鍵情報(subjectPublicKeyInfo)

Verification of public key (2)

- ITU-T X509 Certificate format
  - Version 1 item (mandatory)
    - Version
    - SerialNumber
    - Signature.algorithmIdentifier
    - Issuer
    - Validity
    - Subject
    - SubjectPublicKeyInfo

公開鍵の認証 (3)

- ITU-T X509の証明書フォーマット(続き)
  - Version 2項目(任意)
    - 認証局のオブジェクトID（issuerUniqueID）
    - 被発行者のオブジェクトID（subjectUniqueID）
  - Version 3項目(任意)
    - 鍵の利用目的（keyUsage）
    - 証明書ポリシー（certificatePolicies）
    - 廃棄リスト配布ポイント（cRLDistributionPoints）など

Verification of public key (3)

- ITU-T X509 Certificate format (Contd.)
  - Version 2 item (option)
    - issuerUniqueID
    - subjectUniqueID
  - Version 3 item (option)
    - keyUsage
    - certificatePolicies
    - cRLDistributionPoints
    - Etc.

署名方式 (1)

- RSA署名
  - RSA問題を基にした署名方式
  - EUF-CMA安全ではない
- ElGamal署名
  - 素体の乗法群上の離散対数問題を基にした署名方式
  - EUF-CMA安全であろうと予想されているもののEUF-CMA安全であるかどうか分かっていない
- DSA署名
  - ElGamal署名の変形版で米国NISTの標準暗号になっているが, 安全性については同様

Signature Algorithm (1)

- RSA signature
  - Signature algorithm based on RSA problem
  - Not safe in terms of EUF-CMA
- ElGamal signature
  - Based on discrete exponential over group
  - Expected to be EUF-CMA safety, but unknown
- DSA signature
  - Variation of ElGamal signature, USA NIST standard, safety is the same situation

署名方式 (2)

- Schnorr署名
  - 乗法群上の離散対数問題の困難性とランダムオラクル仮定のもとEUF-CMA安全である事が示されている署名方式
  - ElGamal署名と同程度の効率

- ランダムオラクル
  - ハッシュ関数が「十分ランダムに振舞う」という事を理想化した概念
  - ランダムオラクル仮定は「ランダムオラクルが存在する」という仮定
  - ランダムオラクルはあくまで現実を理想化したものであり現実的には存在し得ない

Signature Algorithm (2)

- Schnorr signature
  - EUF-CMA safety is shown based on difficulty of discrete exponential problem over group and oracle hypothesis
  - Similar efficiency with ElGamal signature

- “Random oracle”
  - Idealistic concept that hash function behave sufficiently in random
  - Random oracle hypothesis is the one that random oracle exists
  - Random oracle does not exist in practice

署名方式 (3)

- Cramer-Shoup署名
  - ランダムオラクルのような理想化された仮定を用いないで安全性が示せる効率的な署名方式
  - 強RSA仮定のもとEUF-CMA安全
  - RSA暗号の数倍程度の計算量で署名作成・検証が可能

- ECDSA署名
  - 楕円曲線DSA (Elliptic Curve DSA)
  - 楕円曲線の方程式を $E = y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ は加算・乗算に関して群をなす
  - 楕円曲線上の点でDSAを定義

Signature Algorithm (3)

- Cramer-Shoup signature
  - Efficient and sage without idealistic hypothesis like random oracle
  - EUF-CMA safety with strong RSA assumption
  - Signature generation and verification can be done with several times larger complexity than RSA

- ECDSA signature
  - Elliptic Curve DSA
  - Equation of elliptic curve
    $E=y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6$ will be a group over addition and multiplication
  - Define DSA on elliptic curve

RSA問題

- RSA Security社
  - ロナルド･リベスト (Ron Rivest), アディ･シャミア (Adi Shamir), レオナルド･エーデルマン (Len Adleman)

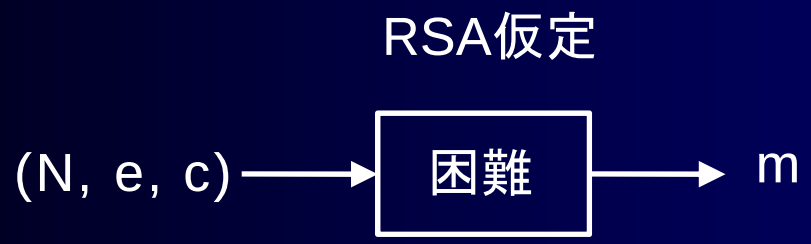
- RSA問題
  - 桁数が大きい合成数の素因数分解問題が困難
  - RSA-129 問題(Rivest, 1970)
    - 129桁の数が2個の素数P, Qの積になっている
    - 素数P, Qを求めるには莫大な計算時間がかかる
    - 114381625757888867669235779976146612010218296721242362562561842935706935245733897830597123563958705058989075147599290026879543541=(3490529510847650949147849619903898133417764638493387843990820577)*(327691329932667095499619881908344614131776429679929425397982885 33)

RSA problem

- RSA, Security division of EMC
  - Ron Rivest, アディ･シャミア, Len Adleman
- RSA problem
  - Difficulty of prime number factorization to a large order number
  - RSA-129 problem (Rivest, 1970)
    - 129 order number is created with two prime numbers P and Q
    - Needs immense computational time to obtain prime numbers P, Q
    - 114381625757888867669235779976146612010218296721242362562561842935706935245733897830597123563958705058989075147599290026879543541
      =(3490529510847650949147849619903898133417764638493387843990820577)*
      (327691329932667095499619881908344614131776429679929425397982885 33)

RSA仮定

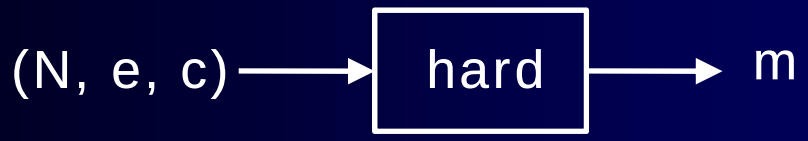
- RSA問題の定義
  - 与えられた(N,e,c)から、$c = m^e \pmod N$を満たすmを求める問題をRSA問題という
- RSA仮定の定義
  - RSA問題を効率的に解くアルゴリズムは存在しないとする仮定をRSA仮定という。



RSA hypothesis

- Definition of RSA problem
  - Search m which satisfy $c = m^e \pmod N$ from given (N,e,c)
- Definition of RSA hypothesis
  - Efficient algorithm to solve RSA problem does not exist

RSA hypothesis



RSA暗号とRSA署名

- RSA暗号
  - 暗号化には公開鍵が，復号には秘密鍵が用いられる
    - 平文m→公開鍵e(暗号化) →暗号文c1
    - 暗号文c1→秘密鍵d(復号) →平文m

$$c_1 = m^e \pmod{N} \qquad m = c_1^d \pmod{N}$$

- RSA署名
  - 署名生成には秘密鍵が，署名検証には公開鍵が用いられる
    - 文書→秘密鍵(署名生成) →署名値
    - 署名値→公開鍵(署名検証) →文書

RSA Encryption and Signature

- RSA encryption
  - Public key for encryption, private key for decoding
    - Message m→ public key e (encryption) →cipher c1
    - Cipher c1→private key d(decoding) →message m

$$c_1 = m^e (mod\ N) \qquad m = c_1^d (mod\ N)$$

- RSA signature
  - Private key for generation, public key for verification
    - Message →private key(generation) →signature
    - signature→public key(verification) →message

ElGamal署名（1）

- ElGamal署名はElGamal暗号とは異なる
- システムパラメータ
  - H:数学的に安全なハッシュ関数
  - p: pを法とする整数の乗法群Z_p^*上で離散対数問題が困難であるような大きな素数
  - g: Z_p^*のランダムな原始根
- 鍵生成
  - $1<x<q$ なる整数xをランダムに選ぶ
  - $y=g^x \bmod p$ を計算
  - 公開鍵は(p,g,y)
  - 秘密鍵はx

ElGamal Signature (1)

- ElGamal signature is different from ElGamal encryption
- System parameter
  - H:mathematically safe hash function
  - p: large prime number which has difficulty of discrete exponential problem over integer group Z_p^*
  - g: random prime root of Z_p^*
- Key generation
  - Select integer x (1<x<q) randomly
  - $y=g^x \bmod p$
  - Public key is (p,g,y)
  - Private key is x

ElGamal署名 (2)

- 署名生成
  - 署名する平文をmとする
  - $0<k<p-1$ かつ $\gcd(k,p-1)=1$となるkをランダムに選ぶ
  - $r \equiv g^k \bmod p$を計算
  - $s \equiv (H(m) - x\, r)\, k^{-1} \bmod p-1$を計算
  - もしs=0であればkを選ぶところからやり直す
  - 整数の組 (r, s)がmに対する署名となる

- 署名検証(平文 m と署名 (r, s) の検証)
  - $0<r<p$ かつ $0<s<p-1$かどうかを確かめる
  - $g^{H(m)} \equiv y^r r^s \bmod p$かどうかを確かめる
  - 両方成立すれば受理

ElGamal Signature (2)

- Signature generation
  - Let a message be m
  - Select k with $0<k<p-1$ and $\gcd(k,p-1)=1$ randomly
  - $r \equiv g^k \bmod p$
  - $s \equiv (H(m) - x\, r)\, k^{-1} \bmod p-1$
  - If s=0, change k
  - Integer pair (r, s) is signature for m

- Signature verification (message m and signature (r, s))
  - Verify $0<r<p$ and $0<s<p-1$
  - Verify $g^{H(m)} \equiv y^r\, r^s \bmod p$
  - If both hold, accept

DSA署名 (1)

- ElGamal署名の変形で, 署名長が短い
- システムパラメータ
  - H:数学的に安全なハッシュ関数
  - p, q: 素数, qはp-1の約数
  - g: Z_p^*の位数qの元
- 鍵生成
  - $0<x<p-1$ なる整数xをランダムに選ぶ
  - $0<k<q$なる整数kをランダムに選ぶ
  - $y=g^x \bmod p$ を計算
  - 公開鍵は(p,q,g,y)
  - 秘密鍵はx

DSA Signature (1)

- Variation of ElGamal signature, short length signature
- System parameter
  - H: mathematically safe hush function
  - p, q: prime numbers, q is a divisor of p-1
  - g: element of order q of Z_p^*
- Key generation
  - Select integer x (0<x<p-1) randomly
  - Select integer k (0<k<q) randomly
  - $y=g^x \bmod p$
  - Public key is (p,q,g,y)
  - Private key is はx

DSA署名 (2)

- 署名生成
  - 署名する平文をmとする
  - 0<k<qなる整数kをランダムに選ぶ
  - $r \equiv (g^k \bmod p) \bmod q$ を計算
  - $s \equiv (H(m) - x\, r)\, k^{-1} \bmod q$を計算
  - 整数の組 (r, s)がmに対する署名となる
- 署名検証
  - $t=(H(m)s^{-1}) \bmod q$, $u=(rs^{-1}) \bmod q$
  - $r \equiv (g^t\, y^u \bmod p) \bmod q$ かどうかを確かめる
  - 成立すれば受理

DSA Signature (2)

- Signature generation
  - Let a message be m
  - Select integer k (0<k<q) randomly
  - $r \equiv (g^k \bmod p) \bmod q$
  - $s \equiv (H(m) - x\, r)\, k^{-1} \bmod q$
  - Integer pair (r, s) is signature for m
- Signature verification
  - $t=(H(m)s^{-1}) \bmod q$, $u=(rs^{-1}) \bmod q$
  - Verify $r \equiv (g^t\, y^u \bmod p) \bmod q$
  - If it holds, accept

ハッシュ関数

- ハッシュ関数とは
  - 与えられた原文から固定長の疑似乱数を生成する演算手法
  - 生成した値は「ハッシュ値」と呼ばれる
  - 「要約関数」「メッセージダイジェスト」とも呼ばれる

- ハッシュ関数の応用
  - 通信回線を通じてデータを送受信する際に，経路の両端でデータのハッシュ値を求めて両者を比較すれば，データが通信途中で改ざんされていないか調べることができる
  - 不可逆な一方向関数を含むため、ハッシュ値から原文を再現することはできず，また同じハッシュ値を持つ異なるデータを作成することは極めて困難
  - 暗号化の補助や，ユーザ認証やデジタル署名などに応用

Hash function

- Hash function
  - Calculation method to generate fixed length pseudo random number for given original message
  - Generated value is called “hash value”
  - Sometimes called “Message digest”

- Application of hash function
  - When send and receive data through communication channel, by comparing hash values at two piers, falsification of data can be checked
  - It includes irreversible function, an original message cannot be reproduced from hash value
  - Help encryption and digital signature

電子署名とハッシュ関数の組み合わせ

- RSA署名とハッシュ関数の組み合わせ
  - 署名生成
    - 文書→ハッシュ値→秘密鍵(署名生成) →署名値
  - 署名検証
    - 署名値→公開鍵(署名検証) →ハッシュ値1
    - 文書→ハッシュ値2
    - ハッシュ値1とハッシュ値2を比較

Combination of Digital Signature and Hash Function

- Combination of RSA signature and hash function
  - Signature generation
    - message→hash value→private key (signature generation) →signature
  - Signature verification
    - Signature→public key (signature verification) →hash value1
    - Message→hash value2
    - Compare hash value 1 and hash value 2

電子署名法

- 電子署名及び認証業務に関する法律(2000)
  - 電磁的記録の真正な成立の推定
  - 特定認証業務に関する認定の制度
- 特定認証業務
  - 認定の対象，認定の基準，帳簿類の保存義務，認定の更新期間等を規定

アルゴリズム	鍵長さ	備考
RSA	1024bit以上	
ESIGN	1024bit以上，検証用べき乗指数8以上	ハッシュ関数はSHA-1
DSA	1024bit以上	
ECDSA	160bit以上	

Digital Signature Law

- Japanese law for digital signature and certification operation (2000)
  - Estimation of true existence of electronic record
  - System for special certification operation
- Special certification operation
  - Define certification target, criteria, duty to keep record, update period

Algorithm	Key length	Note
RSA	>1024bit	
ESIGN	>1024bit, power>8 for verification	Hash function is SHA-1
DSA	>1024bit	
ECDSA	>160bit	