Decision Diffie-Hellman仮定に基づく Timed-Release Encryptionの構成法について

加藤　聡子　　四方　順司　　松本　勉

横浜国立大学大学院環境情報学府/研究院
240-8501 神奈川県横浜市保土ヶ谷区常盤台 79-7

katou@mlab.jks.ynu.ac.jp, {shikata,tsutomu}@ynu.ac.jp

あらまし　Timed-Release Encryption(TRE) とは，特定の時刻以降にのみ復号可能な暗号化方式である．送信者に指定された時刻に時刻情報を放送する機関 (Server) から秘密情報を受信することで復号可能となる．既存の TRE の具体的な構成法は楕円曲線上のペアリングを利用している為，その安全性は Bilinear Diffie-Hellman 仮定に基づいている．本稿ではペアリングを用いずに Decision Diffie-Hellman 仮定に基づく新たな TRE の構成法を提案する．

Construction of Timed-Release Encryption Based on the Decision Diffie-Hellman Assumption

Satoko Kato　　Junji Shikata　　Tsutomu Matsumoto

Graduate School of Environment and Information Sciences,
Yokohama National University,
79-7, Tokiwadai, Hodogaya-ku, Yokohama-shi 240-8501, Japan

katou@mlab.jks.ynu.ac.jp, {shikata,tsutomu}@ynu.ac.jp

Abstract　The timed-release encryption (TRE for short) scheme enables a sender to secretly send a message so that even a legitimate receiver knows it only after the time which the sender has specified beforehand. In fact, TRE can be realized by the mechanism: the receiver can decrypt a ciphertext using secret information which a time-server broadcasts on the specific time. The existing constructions of TRE rely on bilinear pairing, and they are shown to be secure under the Bilinear Diffie-Hellman assumption. In this paper, we propose a construction of TRE without bilinear pairing, and we show our construction is secure under the traditional Decision Diffie-Hellman assumption.

1　はじめに

Timed-Release Encryption(TRE) とは特定の時刻以降にのみ復号可能な暗号化方式である．1993 年に May によりその概念 [1] が提案され，Rivest ら [3] によって時刻情報を鍵として復号させる TRE が提案された．時刻情報を放送/公開する第三者機関（Server）を設置し，受信者は送信者の指定する時刻に時刻情報を受信することで復号可能となる．つまり正当な受信者であっても，送信者に指定された時刻までは復号を行うことができないという特徴を持つ．

Rivest ら [3] の方式では，送信者は復号鍵を Server に送信する為，Server の不正により平文

に関する情報が漏洩する恐れがあり，Server に強い信頼を置く必要がある．これに対し，送信者と Server の通信をなくし，送信者が Server に情報を預けないようにすることで信頼を弱くする方法も示された [3] が，指定可能な時刻に制限が生じる．Blake ら [2] も送信者と Server との対話を不要とする公開鍵型 TRE を提案した．この方式では指定可能な時刻に制限はないが，構成法で楕円曲線上のペアリングを用いている為，安全性は Bilinear Diffie-Hellman 仮定に基づいている．しかし，ペアリングに関する計算量的な仮定は比較的新しい為，その扱いには注意が必要である．

そこで本稿では，既存 [2] で用いられているようなペアリングに関する計算量的な仮定を必要とせず，Decision Diffie-Hellman 仮定に基づく新たな TRE の具体的な構成法を提案する．送信者は Server と通信を行う必要があるが，Server に送信者の秘密情報を預けるわけではない．また，送信者は制限なく未来の時刻を指定時刻に設定できるという特徴を持つ．

本稿の構成は以下のとおりである．はじめに 2 節で関連研究について述べ，3 節で Decision Diffie-Hellman 仮定に基づく TRE のモデル，構成法，安全性に関して述べる．最後に 4 節にてまとめとする．

2 関連研究

Rivest ら [3] によって提案された方式の一つでは，送信者が Server に暗号化を依頼する為，Server に秘密情報を預ける必要がある．また，Server に情報を預けない場合のモデルでは，時刻毎に異なる秘密鍵，公開鍵のペアを Server が生成する．予め公開鍵のみを公開しておき，対応する秘密鍵はその時刻に放送/公開する．送信者は公開鍵を用いて暗号化を行うが，選択できる時刻は公開鍵が公開されている時刻までであり，指定できる時刻に制限が生まれる．これに対し，Blake ら [2] によって構成法でペアリングを用いた公開鍵型 TRE が提案された．Server の公開鍵を利用して暗号化鍵を生成する為，通信が不要であり，また指定可能な時刻に制限がない．

このペアリングを利用した構成法の下で，TRE に付加機能を加えた発展として Hwang ら [5] により，送信者の指定する時刻より前に公開時刻を変更可能とする方式が提案されている．また，吉田らにより複数存在する Server の中から受信者が任意に Server を選択する動的環境で利用可能な TRE が提案されている [6].

以下に公開鍵型 TRE について簡単に述べる．TRE[2] は以下の 5 つの多項式時間アルゴリズムから構成される．

• **TRE.Setup**：Server によって実行される鍵生成アルゴリズム．セキュリティパラメータ 1^k を入力として，マスター秘密鍵 msk と公開パラメータ $params$ を出力する．マスター秘密鍵 msk は Server が秘密に保有する．
• **User KeyGen**：受信者によって実行される鍵生成アルゴリズム．セキュリティパラメータ 1^k，公開パラメータ $params$ を入力として，受信者の秘密鍵 usk，公開鍵 upk を出力する．
• **Server Broadcast**：Server によって実行される時刻情報生成アルゴリズム．マスター秘密鍵 msk，公開パラメータ $params$，時刻 t を入力とし，時刻 t の秘密情報 x を出力する．これを時刻毎に生成，放送/公開する．
•**TRE.Enc**:送信者によって実行される暗号化アルゴリズム．平文 M, 公開パラメータ $params$, 受信者の公開鍵 upk, 時刻 t，ランダムな秘密の値 r を入力とし，暗号文 C を出力する．
•**TRE.Dec**:受信者によって実行される復号アルゴリズム．暗号文 C，公開パラメータ $params$, 公開時刻 t に対応する秘密情報 x，受信者の秘密鍵 usk を入力とし，平文 M（あるいは $\perp$）を出力する．

3 提案方式

本節では，提案方式のモデル，安全性及び構成法を示す．

提案方式はスタンダードモデルにおいて Decision Diffie-Hellman(DDH) 仮定の下で安全性を証明することができる (3.5 節参照).

その概要は，時刻毎に異なる秘密鍵，公開鍵のペアを Server が生成する．送信者は Server

に依頼をし，指定時刻の公開鍵を予め入手し，これを用いて暗号化を行う．公開鍵に対応する秘密鍵はその時刻に Server が公開/放送することで復号可能となる．その為，送信者と Server の相互通信が必要である．ここで，Server が記憶する必要があるものは自身の秘密鍵のみである．また，ある公開された関数に秘密鍵と時刻を入力すれば，その時刻の秘密鍵，公開鍵が出力される仕組みとし，生成した公開鍵やそれに対応する秘密鍵，または時刻に関して Server が記憶することは不要である．

3.1 Decision Diffie-Hellman 仮定

G を素数位数 q の巡回群、g を G の生成元、x, y, z を（Z_q 上の）ランダムな値とする。このとき、(G, q, g, g^x, g^y, g^{xy}) と (G, q, g, g^x, g^y, g^z) を識別する問題のことを Decision Diffie-Hellman (DDH) 問題という。また，この問題を多項式時間で解くことが困難であるとする仮定を Decision Diffie-Hellman(DDH) 仮定と呼ぶ．

3.2 モデル

本稿の TRE は Server, 暗号文の送信者，受信者の 3 者により，以下の 6 つの多項式時間アルゴリズムから構成される．Setup, User KeyGen については 2 節と同様であるが，本稿の TRE はモデルが異なる為，2 節とは異なるアルゴリズムを定義する．

• **TRE.Setup：**Server によって実行される鍵生成アルゴリズム．セキュリティパラメータ 1^k を入力として，マスター秘密鍵 msk と公開パラメータ $params$ を出力する．マスター秘密鍵 msk は Server が秘密に保有する．

• **Time Secret KeyGen：**Server によって実行される秘密鍵生成アルゴリズム．マスター秘密鍵 msk と公開パラメータ $params$，時刻 t を入力として，時刻 t に対応する秘密鍵 x を含む時刻情報 d_t を生成し，放送/公開する．

• **User KeyGen：** 受信者によって実行される鍵生成アルゴリズム．セキュリティパラメータ 1^k，公開パラメータ $params$ を入力として，秘密鍵 usk，公開鍵 upk を出力する．

• **Time Public KeyGen：**Server によって実行される公開鍵生成アルゴリズム．送信者から時刻 t に対応する公開鍵の要求を受けた場合に，マスター秘密鍵 msk，公開パラメータ $params$，時刻 t を入力とし，時刻 t の公開鍵 y を出力する．これを送信者に送信する．

•**TRE.Enc:**送信者によって実行される暗号化アルゴリズム．平文 M, 公開パラメータ $params$, 時刻 t に対応する公開鍵 y，時刻 t，ランダムな秘密の値 r を入力とし，暗号文 C を出力する．

•**TRE.Dec:**受信者によって実行される復号アルゴリズム．暗号文 C，公開パラメータ $params$, 公開時刻 t に対応する秘密鍵 x，受信者の秘密鍵 usk を入力とし，平文 M（あるいは $\perp$）を出力する．

Server はまず TRE.Setup を実行し，マスター秘密鍵 msk と公開パラメータ $params$ を生成する．msk は Server が秘密に保有し，$params$ は公開される．Server は次に Time Secret KeyGen を実行し，現在時刻 t に対応する秘密鍵 x を生成し，時刻 t 毎に放送/公開する．

この状況下で受信者は User KeyGen を実行し，受信者の秘密鍵 usk, 公開鍵 upk を生成する．

送信者は復号可能としたい時刻 t の公開鍵 y を Server に要求する．この依頼を受けて Server は Time Public KeyGen を実行し，送信者の指定する時刻 t の公開鍵 y を生成し，これを送信者に返す．

送信者は Server から公開鍵 y を受信すると TRE.Enc を実行し，平文 M を暗号化し，暗号文 C を生成する．この暗号文 C を受信者に送信する．

受信者は送信者に指定された時刻 t に Server から時刻情報 d_t を受信する．これを用いて TRE.Dec を実行し，暗号文 C を復号して平文 M を得る．

3.3 安全性

3.3 節のモデルにおける TRE では，以下の 3 つの安全性を定義する．

- 受信者に対する安全性 (Insider Security)
- Server に対する安全性 (Server Security)
- 第三者に対する安全性 (Outsider Security)

暗号文の正当な受信者が，送信者の指定する時刻より前に Server からの時刻情報を得ずに暗号文を解読しようとする攻撃が挙げられる．また，Server, 第三者が送信者，受信者間の通信路を盗聴することにより暗号文を得てこれを解読しようとする攻撃が挙げられる．この場合，攻撃者が Server の場合は任意の時刻の時刻情報を生成可能であり，また攻撃者が第三者の場合は指定時刻に時刻情報を受信すれば，復号に必要な秘密情報を得ることができる為，第三者による攻撃は Server による攻撃に包含される．従って，本節ではこれを除いた 2 つの安全性について定義する．

3.3.1 IND-TR-CPA$_{IS}$

受信者が送信者によって指定された時刻より前に平文を解読しようとする．このように攻撃者が受信者である場合に，受信者による選択平文攻撃に対する識別不可能性（IND-TR-CPA$_{IS}$）を定義する．IND-TR-CPA$_{IS}$ は，攻撃者 A_1 と IND-TR-CPA$_{IS}$ Challenger $\mathcal{C}$ との間における，IND-TR-CPA$_{IS}$ ゲームを用いて定義する．

• **Setup**：$\mathcal{C}$ は TRE.Setup(1^k) を実行し，マスター秘密鍵 msk，公開パラメータ $params$ を生成し，$params$ を A_1 に与える．また，User KeyGen (1^k, $params$) を実行し，出力された公開鍵 upk 及び秘密鍵 usk を A_1 に与える．
• **Phase 1**：A_1 は（upk, usk, $params$）を入力されて処理を開始する．A_1 は任意の時刻の秘密鍵 x を返す Extraction oracle に質問することができ，任意の時刻 t に対する Time Secret KeyGen(msk, $params$, t) を Extraction oracle から受け取る．
A_1 は平文 M_0, M_1 と時刻 t^* を出力する．この t^* に関して Extraction oracle に質問していないものとする．
• **Challenge**：$\mathcal{C}$ は ((M_0, M_1), t^*) を受け取るとランダムに $\theta \in \{0,1\}$ を選び，TRE.Enc(M_θ, $params$, y^*, t^*) を実行し，暗号文 C^* を出力する．これを A_1 に返す．
• **Guess**：A_1 は θ' を出力する．$\theta = \theta'$ ならば A_1 の攻撃成功となる．

ここで，A_1 のアドバンテージを以下のように定義する．
$Adv_{A_1}^{IND-TR-CPA_{IS}} = |Pr[\theta = \theta'] - 1/2|$

3.3.2 IND-TR-CPA$_{SS}$

Server が送信者と受信者間の通信を盗聴し，入手した暗号文から平文を解読しようとする．このような攻撃者による選択平文攻撃に対する識別不可能性（IND-TR-CPA$_{SS}$）は，攻撃者 A_2 と IND-TR-CPA$_{SS}$ Challenger $\mathcal{C}$ との間における IND-TR-CPA$_{SS}$ ゲームを用いて定義する．以下に示すゲームでは，攻撃者 A_2 は Server である為，マスター秘密鍵 msk を入手した攻撃者を想定する．

• **Setup**：$\mathcal{C}$ は TRE.Setup(1^k) を実行し，出力されたマスター秘密鍵 msk，公開パラメータ $params$ を A_2 に与える．
また，User KeyGen(1^k, $params$) を実行し，ユーザ秘密鍵 usk，公開鍵 upk を生成し，公開鍵 upk を A_2 に与える．
• **Phase 1**：A_2 は（upk, msk, $params$）を入力されて処理を開始する．A_2 は平文 M_0, M_1 と時刻 t^* を出力する．
• **Challenge**：$\mathcal{C}$ は ((M_0, M_1), t^*) を受け取るとランダムに $\theta \in \{0,1\}$ を選び，TRE.Enc(M_θ, $params$, y^*, t^*) を実行し，暗号文 C^* を出力する．これを A_2 に返す．
• **Guess**：A_2 は θ' を出力する．$\theta = \theta'$ ならば A_2 の攻撃成功となる．

ここで，A_2 のアドバンテージを以下のように定義する．
$Adv_{A_2}^{IND-TR-CPA_{SS}} = |Pr[\theta = \theta'] - 1/2|$

3.4 構成法

DDH 仮定に基づく TRE の構成法を示す．
• **TRE.Setup**
1. 二つの大きな素数 $p, q(q \mid p-1)$ を生成する．

2. 位数が q となる Z_p^* の部分群 G の生成元 α を生成する．
3. $s \in Z_q$ を選び，マスター秘密鍵 msk, 公開鍵 Pub, 公開パラメータ $params$ を生成する．
   衝突困難性を持つハッシュ関数
   $H : \{0,1\}^* \times Z_q \rightarrow Z_q$
   $msk = s,\ Pub = \alpha^s (mod\ p)$,
   $params = (p,\ q,\ \alpha,\ Pub,\ H)$

・Time Secret/Public KeyGen
時刻 $t, msk, params$ を用いて，時刻 t に対応する秘密鍵 x，公開鍵 y を生成する．
$x = H(t, s)$
$y = \alpha^x (mod\ p)$

・User KeyGen
受信者の秘密鍵 usk, 公開鍵 upk を生成する．
$u \in Z_q$
$usk = u,\ upk = \alpha^u (mod\ p)$

・TRE.Enc
1. 乱数 $r \in Z_q$ を選ぶ．
2. 付加情報 $C_t = \alpha^r (mod\ p)$ を生成する．
3. 平文 M を暗号化し，
   暗号文 $C_M = M\alpha^{ur} y^r = M\alpha^{r(u+H(t,s))}$ を生成する．
4. 暗号文 $C = (t,\ C_t,\ C_M)$ として，受信者に送信する．

・TRE.Dec
指定時刻 t の時刻情報 $d_t = (t,\ x)$ を受信する．
$C_M / C_t^{(u+x)} = C_M / \alpha^{r(u+H(t,s))} = M$

3.5 安全性証明

3.3 節で述べた安全性の定義を満たすことを以下で証明する．

3.5.1 IND-TR-CPA$_{IS}$

定理 1 提案方式は DDH 仮定の下で，攻撃者 A_1 に対し IND-TR-CPA$_{IS}$ の安全性を満たす．

証明 A_1 を IND-TR-CPA$_{IS}$ ゲームに $(1/2) + \epsilon$ の確率で勝利する攻撃者とし，A_1 を用いて DDH 問題を破る攻撃者 B を構成する．

Setup B は DDH Challenger から $(p,\ q,\ \alpha)$ と $(\alpha,\ \beta,\ \gamma,\ \delta) = (\alpha,\ \alpha^a,\ \alpha^b,\ \alpha^c)$ を受け取る．B の目的は $c = ab\ mod\ q$ となるか否かを優位な確率で判定することである．B は $msk = s \in Z_q$ を選び，$Pub = \alpha^s$ とする．また，B は $usk = u \in Z_q$，$upk = \alpha^u$ とする．B は A_1 に $params = (p,\ q,\ \alpha,\ Pub,\ H)$ を与える．A_1 は Insider attacker（受信者）であり，ユーザ秘密鍵 usk, 公開鍵 upk を持つことが自然であるといえる為，B は usk, upk を A_1 に与える．

Phase 1 B は A_1 からのクエリに答える前に $1 \leq j \leq q_{ex}$ となる j を選ぶ．時刻 t_j の公開鍵 y_j を DDH Challenger から受け取った値 $\beta = \alpha^a$ とする．その他の $t_i (\neq t_j)$ に関しては $x_i = H(t_i,\ s),\ y_i = \alpha^{x_i}$ とする．
B は A_1 から $\mathrm{t}_i \neq \mathrm{t}_j$ である t_i をクエリとして受け取った場合，x_i を返す．しかし，t_j をクエリとして受け取った場合 $\perp$ を返す．

Challenge A_1 は B に二つの平文 M_0, M_1 と指定時刻 $t^* (= t_i)$ を送信する．$t_i \neq t_j$ である場合，B が DDH 問題を解くことに関係しない為，$\perp$ を返す．$\mathrm{t}_i = \mathrm{t}_j$ の場合，$\theta \in \{0,1\}$ を選び，$C_t^* = \alpha^b$ とする．また，$C_M^* = \mathrm{M}_\theta \alpha^{bu} \delta$ とし，$C^* = (t^*, C_t^*, C_M^*)$ を A_1 に返す．

Guess A_1 は θ' を出力する．B は θ' の値から $\theta = \theta'$ ならば 1 を，$\theta \neq \theta'$ ならば 0 を出力する．ここでは出力値が 1 の場合 $c = ab$ が成り立ち，0 の場合 $c \neq ab$ が成り立つことを意味する．

$c = ab$ の場合 y^*, C^* は TRE の仕様通りに構成される y, C と同一の分布である為，仮定より A_1 は $(1/2) + \epsilon$ 以上の確率で $\theta = \theta'$ となる θ' を出力する．よって，$c = ab$ の場合に B は $(1/2) + \epsilon$ 以上の確率で 1 を出力する．つまり B は $(1/2) + \epsilon$ 以上の確率で $c = ab$ であることを判定できる．

$c \neq ab$ の場合 y^* は TRE の仕様通りに構成される y と同一の分布である．
また，$C^* = (t^*, \gamma, M_\theta \alpha^{bu} \delta) = (t^*, \alpha^b, M_\theta \alpha^{bu} \alpha^c)$ である．c が一様にランダムに選ばれている為，α^c は Z_p^* 上で一様分布であり，$M_\theta \alpha^{bu} \alpha^c$ も Z_p^* 上で一様分布である．よって，この c は θ の情

報を隠している為，A_1 が $\theta = \theta'$ となる θ' を出力する確率は $1/2$ である．従って，B の攻撃成功確率は以下のようになる．
$Adv(B) = Pr[B\ outputs\ 1 \mid c = ab] - Pr[B\ outputs\ 1 \mid c \neq ab] \geq ((1/2) + \epsilon) - (1/2) = \epsilon$

3.5.2 IND-TR-CPA$_{SS}$

定理 2　提案方式は DDH 仮定の下で，攻撃者 A_2 に対し IND-TR-CPA$_{SS}$ の安全性を満たす．

証明　A_2 を IND-TR-CPA$_{SS}$ ゲームに $(1/2) + \epsilon$ の確率で勝利する攻撃者とし，A_2 を用いて DDH 問題を破る攻撃者 B を構成する．

Setup　B は DDH Challenger から $(p,\ q,\ \alpha)$ と $(\alpha, \beta, \gamma, \delta)$=$(\alpha, \alpha^a, \alpha^b, \alpha^c)$ を受け取る．B の目的は $c = ab\ mod\ q$ となるか否かを優位な確率で判定することである．
B は $msk = s \in Z_q$ を選び，$Pub = \alpha^s$ を生成し，A_2 に $msk,\ params = (p,\ q,\ \alpha,\ Pub,\ H)$ を与える．また，B は $upk = \alpha^a$ を A_2 に与える．

Challenge　A_2 は B に二つの平文 M_0, M_1 と指定時刻 t^*, 指定時刻の秘密鍵 x^* 及び公開鍵 $y^* = \alpha^{x^*}$ を送信する．B は $\theta \in \{0, 1\}$ を選び，$C^*_M = M_\theta \delta \alpha^{bx^*}$, $C^*_t = \alpha^b$ とする．$C = (t^*, C^*_M, C^*_t)$ を A_2 に返す．

Guess　A_2 は θ' を出力する．B は θ' の値から $\theta = \theta'$ ならば 1 を，$\theta \neq \theta'$ ならば 0 を出力する．ここでは出力値が 1 の場合 $c = ab$ が成り立ち，0 の場合 $c \neq ab$ が成り立つことを意味する．

$c = ab$ の場合　upk, C^* は TRE の仕様通りに構成される upk, C と同一の分布である為，仮定より A_2 は $(1/2) + \epsilon$ 以上の確率で $\theta = \theta'$ となる θ' を出力する．よって，$c = ab$ の場合に B は $(1/2) + \epsilon$ 以上の確率で 1 を出力する．つまり B は $(1/2) + \epsilon$ 以上の確率で $c = ab$ であることを判定できる．

$c \neq ab$ の場合　upk は TRE の仕様通りに構成される upk と同一の分布である．また，C^*=$(t^*, \gamma, M_\theta \delta \alpha^{bx^*})$=$(t^*, \alpha^b, M_\theta \alpha^c \alpha^{bx^*})$ である．c が一様にランダムに選ばれている為，α^c は Z^*_p 上で一様分布であり，$M_\theta \alpha^c \alpha^{bx^*}$ も Z^*_p 上で一様分布である．よって，この c は θ の情報を隠している為，A_2 が $\theta = \theta'$ となる θ' を出力する確率は $1/2$ である．
従って，B の攻撃成功確率は以下のようになる．
$Adv(B) = Pr[B\ outputs\ 1 \mid c = ab] - Pr[B\ outputs\ 1 \mid c \neq ab] \geq ((1/2) + \epsilon) - (1/2) = \epsilon$

4　まとめ

Decision Diffie-Hellman 仮定に基づく TRE の具体的な構成法を示した．ペアリングを利用した構成法では Server または第三者が攻撃者であることを想定する場合，その安全性が TRE での選択暗号文攻撃に対する識別不可能性（IND-TR-CCA$_{SS,OS}$）を満たすことが示されている [5]．本方式に関しても，IND-TR-CCA$_{SS,OS}$ まで拡張し，安全性のレベルを高めることを検討していきたい．

参考文献

[1] T. C. May, "Time-release crypto," 1993.

[2] I. F. Blake, A. C-F. Chan, "Scalable, Server-Passive, User-Anonymous Timed Release Cryptography," Distributed Compuring Systems, ICDCS 2005, pp.504-513, IEEE, 2005.

[3] R. L. Rivest, A. Shamir, and D. A. Wagner, "Time-lock puzzles and timed-release crypto," MIT LCS Tech, Report MIT LCS TR-684,1996.

[4] J. H. Cheon, N. Hopper, Y. Kim, I. Osipkov, "Timed-Release and Key-Insulated Public Key Encryption," Financial Cryptography 2006, pp.191-205,2006.

[5] Y. Hwang, D. Yum, P. Lee, "Timed-release encryption with pre-open capability and its application to certified e-mail system," ISC 2005,LNCS3650, 2005.

[6] M. Yoshida, T. Fujiwara, "Flexible Timed-Release Encryption," IEICE Transactions 92-A(1), pp.222-225, 2009.