HDEF-ECDH 詳細評価報告書

2001 年 1 月 9 日

1. HDEF-ECDH

本評価の対象である HDEF-ECDH は，楕円曲線上の DH 問題の困難性にもとづく鍵配送法であり，具体的には以下のプロトコルである．

[初期設定]
ユーザ A は以下の初期設定を行う．

1. trace 3 の素数位数楕円曲線 E_A/F_{pA} を生成する．
2. ベースポイント $G_A \in E_A(F_{pA})$をランダムに選ぶ.
3. 整数 x_A ($0 < x_A < p_A-2$) をランダムに選び，秘密鍵とする．
4. $Y_A = x_A \cdot G_A$ を計算し，($E_A/F_{pA}, Y_A, G_A$)を公開鍵とする．

同様にしてユーザ B も公開鍵($E_B / F_{pB}, Y_B, G_B$)を計算する．

[プロトコル]
ユーザ A

1. r_A ($0 < r_A < p_B-2$) となる任意の整数を選ぶ.
2. $R_A = r_A \cdot G_B$ を E_B/F_{pB} 上で計算する．
3. R_A を B に送る．

ユーザ B

1. r_B ($0 < r_B < p_A-2$) となる任意の整数を選ぶ.
2. $R_B = r_B \cdot G_A$ を E_A / F_{pA} 上で計算する．
3. R_B を A に送る．

[鍵共有]
ユーザ A は

$$K_A = x_A R_B, \quad K_B = r_A Y_B$$

を計算し，ユーザ B は

$$K_B = x_B R_A, \quad K_A = r_B Y_A$$

を計算し，(K_A, K_B)を共有する．

HDEF は，以下の特徴を持つ．

1. ユーザごとに異なる楕円曲線を用いることを想定している．
2. トレース 3 の楕円曲線を用いる．そのような楕円曲線の構成方法としては虚数乗法法を用いている．
3. プロトコル自体は，標準的に利用されている ECDH[DH 76]を２重に用いているに過ぎない．

2. Primitive の安全性

HDEF は ECDH を２重に用いているだけなので，その安全性は楕円曲線上の DH 問題[DH 76]に trivial に帰着される[Miyaji 99]． 楕円曲線上の DH 問題は楕円曲線上の離散対数問題を解かなければ，解けないだろうと強く信じられている．したがって，HDEF が安全となるには，楕円曲線上の離散対数問題を解くことが困難な楕円曲線を用いればよい．具体的には， Pohlig-Hellman アルゴリズム[PH 78]，baby-step giant-step アルゴリズム[Knuth 73]，Pollard's rho アルゴリズム[Pollard 78]，SSSA 攻撃[Semaev 98, Smart 99, SA 98], MOV 攻撃[MOV 91], FR 帰着法[FR 94, SU 98]および Weil descent 攻撃[GHS 00, Arita 00]に対して安全な楕円曲線を用いればよい．

しかし，HDEF では，使用する楕円曲線を，trace 3 の楕円曲線に限定している．これは，不可解な限定である．確かに，応募者の主張するように，trace 3 の楕円曲線を用いれば，FR 条件[SU 98]（ MOV 攻撃や FR 帰着法が適用できないための条件． 有限体 GF(q)上の楕円曲線上の位数 n のベースポイントを用いるとき，$1 \leqq k \leqq \log q$ に対して $q^k \neq 1 \bmod n$ であること．）の検証は不要となる（ただし，自己評価書の定理１の証明には不備がある．本節末尾の注を参照）． しかし，FR 条件の検証はもともと極めて容易であり， それが不要になることに，さしたる意義は認め難い．自己評価書において応募者は，FR 条件について初めて explicit な条件を明らかにしたと主張しているが，そもそも FR 条件自体が，極めて explicit な条件であり，応募者のこのような主張は理解できない．

さらに，HDEF では 楕円曲線を虚数乗法法[Morain 91]によって生成することになっている．そのため，HDEF で用いる楕円曲線は，判別式の非常に小さな虚 2 次体を虚数乗法にもつ楕円曲線に限定される．実際，暗号技術仕様書では判別式を 403 に固定した生成法が実用的アルゴリズム（アルゴリズム 3）として提案されているが，これは，使用する楕円曲

線を極めて狭い範囲に限定していることを意味する.

以上のように，HDEF では，使用する楕円曲線が,
1. trace が 3 に等しい.
2. 判別式の小さな虚 2 次体を虚数乗法にもつ
という 2 重の意味で限定されている.

使用する楕円曲線の範囲をこのように限定することは，相応のメリットがない限り，受け入れることはできないことである.

注

標数 p の素体上定義された trace 3 の素数位数 n = p - 2 の楕円曲線を考える.
暗号技術仕様書あるいは自己評価書の定理 1 系 1 では，$p^k - 1 = 0 \bmod n$ ならば $k > \log p$ となることが証明されているが，証明には不備がある.

今，trace が 3 なので，$p^k = 2^k \bmod n$ である．定理 1 の証明は，右辺の 2^k が n を越えないことに依存している．しかし，$k = \log p$ のとき，2^k は n を越えるので，証明のロジックは成立しない.

もっとも，$k=\log p$ のときは, n が 2^k-1 を割るとすると，ビット長を考慮して，$n=2^k-1$ であり，$p=n+2=2^k+1$ となり，p が k+1 ビットになってしまうので，系 1 自体は正しいことがわかる.

3. 推奨パラメータの安全性

ファイル TestVector**.txt に記載された推奨パラメータの楕円曲線が, 既知の攻撃法に対して安全か否か，確認する． 以下，P を定義体の位数，A および B を楕円曲線の定義式 $y^2=x^3+Ax+B$ に現れる係数，R をベースポイント G の位数，X をベースポイント G の x 座標，Y をベースポイントの y 座標とする.

[TestVector01.txt]
P = 730750818665451459523961714499640833062084344321
A = 730750818665451459523961714499640833062084344318
B = 145650976250847204316161868675773209711877624364

R = 730750818665451459523961714499640833062084344319
X = 0
Y = 52469857950549509428091575437710679925149893202O

P が素数であることを Mathematica Ver.4 の PrimeQ コマンドによって確認した．点 G が位数 R = 730750818665451459523961714499640833062084344319 をもつことを付録の Mathematica プログラム elliptic.m の JPower コマンドによって確認した．よって，上記パラメータで指定された楕円曲線の位数は R の整数倍に等しいが，Hasse-Weil bound を考慮すると，R に等しいことがわかり，楕円曲線の trace は確かに(P+1)-R=3 である．

・ ベースポイント G の位数 R は 160 ビットであり, 素数であることを Mathematica Ver.4 の PrimeQ コマンドによって確認した．よって，G は 160 ビット素数位数の巡回群を生成するので，Pohlig-Hellman アルゴリズム，baby-step giant-step アルゴリズム，Pollard's rho アルゴリズムによる攻撃は不可能である．

・ ベースポイント G の位数 R は P と異なる素数なので，SSSA 攻撃は不可能である．

・ FR 条件をチェックする．trace が 3 に等しいので，

$$P = 2 \mod R.$$

よって，

$$P^k = 2^k \mod R$$

である． 右辺が１に等しくなる可能性は k=log(2,R)=160 のときのみだが，

$$2^{160} = 730750818665451458679723118216642186593848198657 \mod R$$

となり，１とはならない．よって，１以上 160 以下の k に対して， P^k を R でわった余りとして 1 は現れていない．したがって，MOV 攻撃もしくは FR 帰着法による攻撃は不可能である．

・ 有限体として素体 GF(p)を用いているので，Weil descent 攻撃は不可能である．

[TestVector02.txt]

P = 730750818665451460784894131765992686631311662321
A = 730750818665451460784894131765992686631311662318
B = 23600091099418029634485507695627384893545644182O
R = 730750818665451460784894131765992686631311662319

X = 0
Y = 228816326668861720431540364037409019159730897276

P が素数であることを Mathematica Ver.4 の PrimeQ コマンドによって確認した．点 G が位数 R = 730750818665451460784894131765992686631311662319 をもつことを付録の Mathematica プログラム elliptic.m の JPower コマンドによって確認した．よって，上記パラメータで指定された楕円曲線の位数は R の整数倍に等しいが，Hasse-Weil bound を考慮すると，R に等しいことがわかり，楕円曲線の trace は確かに(P+1)-R=3 である．

・ ベースポイント G の位数 R は 160 ビットであり，素数であることを Mathematica Ver.4 の PrimeQ コマンドによって確認した．よって，G は 160 ビット素数位数の巡回群を生成するので，Pohlig-Hellman アルゴリズム，baby-step giant-step アルゴリズム，Pollard's rho アルゴリズムによる攻撃は不可能である．

・ ベースポイント G の位数 R は P と異なる素数なので，SSSA 攻撃は不可能である．
・ FR 条件をチェックする．trace が 3 に等しいので，

$$P = 2 \mod R.$$

よって，

$$P^k = 2^k \mod R$$

である． 右辺が 1 に等しくなる可能性は k=log(2,R)=160 のときのみだが，

$$2^{160} = 730750818665451457418790700950290333024620880657 \mod R$$

となり，1 とはならない． よって，1 以上 160 以下の k に対して， P^k を R でわった余りとして 1 は現れていない．したがって，MOV 攻撃もしくは FR 帰着法による攻撃は不可能である．

・有限体として素体 GF(p)を用いているので，Weil descent 攻撃は不可能である．

[TestVector03.txt]

P = 730750818665451459229743719868495026423191597789
A = 730750818665451459229743719868495026423191597786
B = 139179486141137491708756227029055585426263133617
R = 730750818665451459229743719868495026423191597787
X = 0
Y = 266943320732342502723756480673036105031314450306

P が素数であることを Mathematica Ver.4 の PrimeQ コマンドによって確認した．点 G が位数 R = 730750818665451459229743719868495026423191597787 をもつことを付録の Mathematica プログラム elliptic.m の JPower コマンドによって確認した．よって，上記パラメータで指定された楕円曲線の位数は R の整数倍に等しいが，Hasse-Weil bound を考慮すると，R に等しいことがわかり，楕円曲線の trace は確かに(P+1)-R=3 である．

・ ベースポイント G の位数 R は 160 ビットであり，素数であることを Mathematica Ver.4 の PrimeQ コマンドによって確認した．よって，G は 160 ビット素数位数の巡回群を生成するので，Pohlig-Hellman アルゴリズム，baby-step giant-step アルゴリズム，Pollard's rho アルゴリズムによる攻撃は不可能である．

・ ベースポイント G の位数 R は P と異なる素数なので，SSSA 攻撃は不可能である．
・ FR 条件をチェックする．trace が 3 に等しいので，

$$P = 2 \mod R.$$

よって，

$$P^k = 2^k \mod R$$

である． 右辺が 1 に等しくなる可能性は k=log(2,R)=160 のときのみだが，

$$2^{160} = 730750818665451458973941112847787993232740945189 \mod R$$

となり，1 とはならない． よって，1 以上 160 以下の k に対して， P^k を R でわった余りとして 1 は現れていない．したがって，MOV 攻撃もしくは FR 帰着法による攻撃は不可能である．

・有限体として素体 GF(p)を用いているので，Weil descent 攻撃は不可能である．

[TestVector04.txt]

P = 730750818665451459198492848174143520152072948273
A = 730750818665451459198492848174143520152072948270
B = 392044336886008105126536977708138035824575383106
R = 730750818665451459198492848174143520152072948271
X = 0
Y = 486582519794961249490277721522110499659853067816

P が素数であることを Mathematica Ver.4 の PrimeQ コマンドによって確認した．点 G が位

数 R = 730750818665451459198492848174143520152072948271 をもつことを付録の Mathematica プログラム elliptic.m の JPower コマンドによって確認した．よって，上記パラメータで指定された楕円曲線の位数は R の整数倍に等しいが，Hasse-Weil bound を考慮すると，R に等しいことがわかり，楕円曲線の trace は確かに(P+1)-R=3 である．

・ ベースポイント G の位数 R は 160 ビットであり，素数であることを Mathematica Ver.4 の PrimeQ コマンドによって確認した．よって，G は 160 ビット素数位数の巡回群を生成するので，Pohlig-Hellman アルゴリズム，baby-step giant-step アルゴリズム，Pollard's rho アルゴリズムによる攻撃は不可能である．

・ ベースポイント G の位数 R は P と異なる素数なので，SSSA 攻撃は不可能である．
・ FR 条件をチェックする．trace が 3 に等しいので，

$$P = 2 \mod R.$$

よって，

$$P^k = 2^k \mod R$$

である． 右辺が 1 に等しくなる可能性は k=log(2,R)=160 のときのみだが，

$$2^{160} = 730750818665451459005191984542139499503859594705 \mod R$$

となり，1 とはならない． よって，1 以上 160 以下の k に対して， P^k を R でわった余りとして 1 は現れていない．したがって，MOV 攻撃もしくは FR 帰着法による攻撃は不可能である．

・有限体として素体 GF(p)を用いているので，Weil descent 攻撃は不可能である．

[TestVector05.txt]

P = 730750818665451459126950136883240050376259393371
A = 730750818665451459126950136883240050376259393368
B = 476911273963212365552018367489394946363485353968
R = 730750818665451459126950136883240050376259393369
X = 0
Y = 494562264743653621892043368414284409149270854431

P が素数であることを Mathematica Ver.4 の PrimeQ コマンドによって確認した．点 G が位数 R = 730750818665451459126950136883240050376259393369 をもつことを付録の Mathematica プログラム elliptic.m の JPower コマンドによって確認した．よって，上記パ

ラメータで指定された楕円曲線の位数は R の整数倍に等しいが，Hasse-Weil bound を考慮すると，R に等しいことがわかり，楕円曲線の trace は確かに(P+1)-R=3 である．

・ ベースポイント G の位数 R は 160 ビットであり，素数であることを Mathematica Ver.4 の PrimeQ コマンドによって確認した．よって，G は 160 ビット素数位数の巡回群を生成するので，Pohlig-Hellman アルゴリズム，baby-step giant-step アルゴリズム，Pollard's rho アルゴリズムによる攻撃は不可能である．

・ ベースポイント G の位数 R は P と異なる素数なので，SSSA 攻撃は不可能である．
・ FR 条件をチェックする．trace が 3 に等しいので，

$$P = 2 \mod R.$$

よって，

$$P^k = 2^k \mod R$$

である． 右辺が 1 に等しくなる可能性は k=log(2,R)=160 のときのみだが，

$$2^{160} = 730750818665451459076734695833042969279673149607 \mod R$$

となり，1 とはならない． よって，1 以上 160 以下の k に対して， P^k を R でわった余りとして 1 は現れていない．したがって，MOV 攻撃もしくは FR 帰着法による攻撃は不可能である．

・有限体として素体 GF(p)を用いているので，Weil descent 攻撃は不可能である．

[TestVector06.txt]

P = 730750818665451459198607253088958998584102121931
A = 730750818665451459198607253088958998584102121928
B = 216251692378742053047702251484483205374718844579
R = 730750818665451459198607253088958998584102121929
X = 0
Y = 65706536962916211491355005501385062856143559021 9

P が素数であることを Mathematica Ver.4 の PrimeQ コマンドによって確認した．点 G が位数 R = 730750818665451459198607253088958998584102121929 をもつことを付録の Mathematica プログラム elliptic.m の JPower コマンドによって確認した．よって，上記パラメータで指定された楕円曲線の位数は R の整数倍に等しいが，Hasse-Weil bound を考慮すると，R に等しいことがわかり，楕円曲線の trace は確かに(P+1)-R=3 である．

・ ベースポイント G の位数 R は 160 ビットであり，素数であることを Mathematica Ver.4 の PrimeQ コマンドによって確認した．よって，G は 160 ビット素数位数の巡回群を生成するので, Pohlig-Hellman アルゴリズム, baby-step giant-step アルゴリズム, Pollard's rho アルゴリズムによる攻撃は不可能である．

・ ベースポイント G の位数 R は P と異なる素数なので，SSSA 攻撃は不可能である．
・ FR 条件をチェックする．trace が 3 に等しいので，

$$P = 2 \mod R.$$

よって，

$$P^k = 2^k \mod R$$

である． 右辺が 1 に等しくなる可能性は k=log(2,R)=160 のときのみだが，

$$2^{160} = 730750818665451459005077579627324021071830421047 \mod R$$

となり，1 とはならない． よって，1 以上 160 以下の k に対して， P^k を R でわった余りとして 1 は現れていない．したがって，MOV 攻撃もしくは FR 帰着法による攻撃は不可能である．

・ 有限体として素体 GF(p)を用いているので，Weil descent 攻撃は不可能である．

[TestVector07.txt]

P = 730750818665451462386049986465664716475320520871
A = 730750818665451462386049986465664716475320520868
B = 337729189819406031122274533307407198959445110966
R = 730750818665451462386049986465664716475320520869
X = 4
Y = 697875110732474572726452229761998351885441669220

P が素数であることを Mathematica Ver.4 の PrimeQ コマンドによって確認した．点 G が位数 R = 730750818665451462386049986465664716475320520869 をもつことを付録の Mathematica プログラム elliptic.m の JPower コマンドによって確認した．よって，上記パラメータで指定された楕円曲線の位数は R の整数倍に等しいが，Hasse-Weil bound を考慮すると，R に等しいことがわかり，楕円曲線の trace は確かに(P+1)-R=3 である．

・ ベースポイント G の位数 R は 160 ビットであり，素数であることを Mathematica Ver.4

の PrimeQ コマンドによって確認した．よって，G は 160 ビット素数位数の巡回群を生成するので, Pohlig-Hellman アルゴリズム, baby-step giant-step アルゴリズム, Pollard's rho アルゴリズムによる攻撃は不可能である．

・ ベースポイント G の位数 R は P と異なる素数なので，SSSA 攻撃は不可能である．
・ FR 条件をチェックする．trace が 3 に等しいので，

$$P = 2 \mod R.$$

よって，

$$P^k = 2^k \mod R$$

である． 右辺が１に等しくなる可能性は k=log(2,R)=160 のときのみだが，

$$2^{160} = 730750818665451455817634846250618303180612022107 \mod R$$

となり，1 とはならない． よって，１以上 160 以下の k に対して， P^k を R でわった余りとして 1 は現れていない．したがって，MOV 攻撃もしくは FR 帰着法による攻撃は不可能である．

・ 有限体として素体 GF(p)を用いているので，Weil descent 攻撃は不可能である．

[TestVector08.txt]

P = 730750818665451459190432643819831024291181008521
A = 730750818665451459190432643819831024291181008518
B = 468003416420854875555883526200458145639263628500
R = 730750818665451459190432643819831024291181008519
X = 0
Y = 735859695726529371891451312827099582618870253 56

P が素数であることを Mathematica Ver.4 の PrimeQ コマンドによって確認した．点 G が位数 R = 730750818665451459190432643819831024291181008519 をもつことを付録の Mathematica プログラム elliptic.m の JPower コマンドによって確認した．よって，上記パラメータで指定された楕円曲線の位数は R の整数倍に等しいが，Hasse-Weil bound を考慮すると，R に等しいことがわかり，楕円曲線の trace は確かに(P+1)-R=3 である．

・ ベースポイント G の位数 R は 160 ビットであり，素数であることを Mathematica Ver.4 の PrimeQ コマンドによって確認した．よって，G は 160 ビット素数位数の巡回群を生成するので, Pohlig-Hellman アルゴリズム, baby-step giant-step アルゴリズム, Pollard's rho

アルゴリズムによる攻撃は不可能である.

・ ベースポイント G の位数 R は P と異なる素数なので, SSSA 攻撃は不可能である.
・ FR 条件をチェックする. trace が 3 に等しいので,

$$P = 2 \mod R.$$

よって,

$$P^k = 2^k \mod R$$

である. 右辺が 1 に等しくなる可能性は k=log(2,R)=160 のときのみだが,

$$2^{160} = 730750818665451459013252188896451995364751534457 \mod R$$

となり, 1 とはならない. よって, 1 以上 160 以下の k に対して, P^k を R でわった余りとして 1 は現れていない. したがって, MOV 攻撃もしくは FR 帰着法による攻撃は不可能である.

・ 有限体として素体 GF(p)を用いているので, Weil descent 攻撃は不可能である.

[TestVector09.txt]

P = 730750818665451459161278109657831935625339375671
A = 730750818665451459161278109657831935625339375668
B = 522654829037395571375403512611405218323164759398
R = 730750818665451459161278109657831935625339375669
X = 3
Y = 392269006137421807971165556386331216620312619150

P が素数であることを Mathematica Ver.4 の PrimeQ コマンドによって確認した. 点 G が位数 R = 730750818665451459161278109657831935625339375669 をもつことを付録の Mathematica プログラム elliptic.m の JPower コマンドによって確認した. よって, 上記パラメータで指定された楕円曲線の位数は R の整数倍に等しいが, Hasse-Weil bound を考慮すると, R に等しいことがわかり, 楕円曲線の trace は確かに(P+1)-R=3 である.

・ ベースポイント G の位数 R は 160 ビットであり, 素数であることを Mathematica Ver.4 の PrimeQ コマンドによって確認した. よって, G は 160 ビット素数位数の巡回群を生成するので, Pohlig-Hellman アルゴリズム, baby-step giant-step アルゴリズム, Pollard's rho アルゴリズムによる攻撃は不可能である.

・ ベースポイント G の位数 R は P と異なる素数なので，SSSA 攻撃は不可能である．

・ FR 条件をチェックする．trace が 3 に等しいので，

$$P = 2 \mod R.$$

よって，

$$P^k = 2^k \mod R$$

である． 右辺が 1 に等しくなる可能性は k=log(2,R)=160 のときのみだが，

$$2^{160} = 730750818665451459042406723058451084030593167307 \mod R$$

となり，1 とはならない． よって，1 以上 160 以下の k に対して， P^k を R でわった余りとして 1 は現れていない．したがって，MOV 攻撃もしくは FR 帰着法による攻撃は不可能である．

・ 有限体として素体 GF(p)を用いているので，Weil descent 攻撃は不可能である．

[TestVector10.txt]

P = 730750818665451459152053136261172448611426896821
A = 730750818665451459152053136261172448611426896818
B = 280006411788366030235018113338044339921767225460
R = 730750818665451459152053136261172448611426896819
X = 0
Y = 681065648261044863819755347466475153133776744153

P が素数であることを Mathematica Ver.4 の PrimeQ コマンドによって確認した．点 G が位数 R = 730750818665451459152053136261172448611426896819 をもつことを付録の Mathematica プログラム elliptic.m の JPower コマンドによって確認した．よって，上記パラメータで指定された楕円曲線の位数は R の整数倍に等しいが，Hasse-Weil bound を考慮すると，R に等しいことがわかり，楕円曲線の trace は確かに(P+1)-R=3 である．

・ ベースポイント G の位数 R は 160 ビットであり，素数であることを Mathematica Ver.4 の PrimeQ コマンドによって確認した．よって，G は 160 ビット素数位数の巡回群を生成するので，Pohlig-Hellman アルゴリズム，baby-step giant-step アルゴリズム，Pollard's rho アルゴリズムによる攻撃は不可能である．

・ ベースポイント G の位数 R は P と異なる素数なので，SSSA 攻撃は不可能である．

・ FR 条件をチェックする．trace が 3 に等しいので，

$$P = 2 \mod R.$$

よって，

$$P^k = 2^k \mod R$$

である． 右辺が 1 に等しくなる可能性は k=log(2,R)=160 のときのみだが，

$$2^{160} = 730750818665451459051631696455110571044505646157 \mod R$$

となり，1 とはならない． よって，1 以上 160 以下の k に対して， P^k を R でわった余りとして 1 は現れていない．したがって，MOV 攻撃もしくは FR 帰着法による攻撃は不可能である．

・ 有限体として素体 GF(p)を用いているので，Weil descent 攻撃は不可能である．

4. スキームの安全性

応募者は，暗号技術仕様書 1 節「技術の背景」において，「近年の特定の楕円曲線に対する攻撃は，全ユーザが同じ曲線を利用する危険性に対する警告ともいえる．つまり，安全性の観点からは，ユーザ毎に異なる楕円曲線を用いることが望ましい」と述べている．評価者はこの主張に反対である．逆に，ユーザごとに異なる楕円曲線を用いることは危険であると考える．ユーザごとに異なる楕円曲線が用いられている環境で，新たに弱い楕円曲線のクラスが発見されたとき，ユーザごとに異なる楕円曲線の安全性を検証するのは大変な作業である．危険な楕円曲線を，本人のみならず周囲のユーザもそれと気づかず，そのまま使用してしまうという事態が生じる可能性があり，セキュリティホールを生む危険性がある．

実際，危険な楕円曲線をそれと知らず使用するユーザ B が存在すれば，以下のようなアタックのシナリオが存在する．危険な楕円曲線をそれと知らず使用するユーザ B と一般のユーザ A が HDEF により交換する秘密情報は，HDEF による鍵配送プログラムの開発者 C の悪意を仮定すると，開発者 C にのみ筒抜けになる可能性がある．

以下では，ユーザ B の用いる楕円曲線の離散対数問題の解読アルゴリズム W を開発者 C が所有していると仮定する．

ユーザ A は HDEF を正しく実装したプログラムを用いて HDEF 鍵配送を行う. すなわち,

[ユーザ A]
1. ユーザ A は，乱数 r_A $(0 < r_A < p_A\text{-}2)$を生成する.
2. ユーザ A は，$R_A = r_A \cdot G_B$ を計算する.
3. 計算結果 R_A をユーザ B に送る.

ユーザ B は開発者 C によって偽造されたプログラムを（それとは知らず）用いて，以下のような処理を行う.

[ユーザ B]
1. ユーザ B のプログラムは，解読アルゴリズム W を用いて，R_A より乱数 r_A を得る：
$$r_A = W(R_A, E_B/F_{pB}, G_B).$$
2. ユーザ B のプログラムは， 対称鍵暗号 E を用いて，乱数 r_A を暗号化し r_B を得る：
$$r_B = E(k, r_A).$$
ここで，対称鍵暗号 E および使用している鍵 k を開発者 C は知っているものとする.
3. ユーザ B のプログラムは，$R_B = r_B \cdot G_A$ を計算する.
4. R_B をユーザ A に送る.

開発者 C は以下のようにして，ユーザ A とユーザ B の間で共有される秘密情報 K_A，K_B を知ることができる.

[開発者 C]
1. 解読アルゴリズム W を用いて，R_A より乱数 r_A を得る：
$$r_A = W(R_A, E_B/F_{pB}, G_B).$$
2. ユーザ B のプログラムが用いた対称鍵暗号 E および鍵 k を用いて
$$r_B = E(k, r_A)$$
を得る.
3. $K_A = r_B \cdot Y_A$，$K_B = r_A \cdot Y_B$ を計算し，秘密情報 K_A，K_B を得る.

上で，ユーザ B の利用する偽造プログラムは，解読アルゴリズム W が充分に効率的であると仮定し，対称鍵暗号 E(k，・) がランダム関数と区別できないと仮定すると，外部から観察しても正しく HDEF を実行しているように見えることに注意する.

5. 結論

HDEF は使用する楕円曲線の trace を３に固定し，またその虚数乗法の判別式が小さい値になるように範囲を限定している．使用する楕円曲線の範囲を限定することは，相応のメリットがない限り，受け入れることのできないことである

HDEF の利点は，ユーザごとに異なる楕円曲線を使用できることと主張しているが，これが利点であるとは認め難く，逆に前節でみたように， セキュリティホールを生みだす温床となりかねない.

以上から，HDEF には楕円曲線の範囲を限定することから生じる危険性に見合う利点が存在せず，逆にセキュリティホールを生じさせやすくなっていると考えられるので，電子政府において使用する鍵配送法として適切でない，と結論する.

参考文献

[Arita 00] S. Arita, “Weil descent of elliptic curves over finite fields of characteristic three”, ASIACRYPT 2000, LNCS 1976, pp.248--258, Kyoto, 2000.

[DH 76] W. Diffie and M.Hellman, “New directions in cryptography”, IEEE Trans. Inf. Theory, IT-22 (1976), 644-654.

[FR 94] G. Frey and H.-G. Ruck, “A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves”, Mathematics of Computation, 62 (1994), 865-874.

[GHS 00] P. Gaudry, F. Hess and N. Smart, “Constructive and destructive facets of Weil descent on elliptic curves,” HP Labs Tech. Report, HPL-2000-10.

[Knuth 73] D. E. Knuth, “The Art of Computer Programming --- Sorting and Searching”, volume 3, Addison-Wesley, Reading, Massachusetts, 1973.

[MOV 91] A. Menezes, T. Okamoto, and S. Vanstone, “Reducing elliptic curve logarithms to logarithms in a finite field”, Proceedings of the 23rd Annual ACM Symposium on Theory of Computing, 80-89, 1991.

[Miyaji 99] A. Miyaji and H. Shizuya, “ Integration of DLP-based cryptosystems”, IEICE Japan Tech. Rep., ISEC99-48 (1999-9), 73-80.

[Morain 91] F. Morain, “Building cyclic elliptic curves modulo large primes,” D. W. Davies, editor, *Advances in Cryptology - EUROCRYPT ‘91*, *Lecture Notes in Computer Science* **547** (1991), Springer-Verlag, 328-336.

[PH 78] S. C. Pohlig and M. E. Hellmann, “An improved algorithm for computing logarithms over GF(p) and its cryptographic significance”, IEEE Trans. Inf. Theory, IT-24 (1978), 106-110.

[Pollard 78] J. Pollard, “Monte Carlo methods for index computation mod p”, Mathematics of Computation, 32 (1978), 918-924.

[SU 98] T. Saitoh and S. Uchiyama, “A Note on the Discrete Logarithm Problem on Elliptic Curves of Trace Two”, Technical Report of IEICE, ISEC 98-27 (1998), 51-57.

[SA 98] T. Satoh, and K.Araki, “Fermat Quotients and the Polynomial Time Discrete Log Algorithm for Anomalous Elliptic Curves", COMMENTARII MATHEMATICI UNIVERSITATIS SANCTI PAULI, vol. 47, No. 1, 81-92, 1998.

[Semaev 98] I. A. Semaev, “Evaluation of discrete logarithms in a group of p-torsion points of an elliptic curves in characteristic p," Math. Comp. 67, 353-356 (1998).

[Smart 99] P. N. Smart, “The discrete logarithm problem on elliptic curves of trace one”, J. Cryptology 12, 193-196 (1999).