

OCS ./ HIT: Geometry Patent Stops Shareware Project

<http://swpat.ffii.org/pikta/xrani/ocshit/index.en.html>

Workgroup

swpatag@ffii.org

english version 2004/08/16 by Hartmut PILCH*

2005-01-06

Oberthur Card System applied in 1999 for a patent on a method of geometry (point-halving in elliptic curves). In Oct 2001, the Oberthur's legal department sent a cease-and-desist letter to Marcel Martin, French informatics student and author of the shareware library HIT, in which it asked him to "immediately stop marketing your product". Which he did, although the legal status of Oberthur's patent claims particularly in Europe is very unclear. We have published a few lines of code which, according to Oberthur's letter, seem to be infringing on the patent. Martin commented "I had to stop this project, because I cannot afford to pay an army of lawyers every time someone wants to impose conditions on my work. Software developpers react very sensitively to this kind of terrorism. If European politicians legalise software patents in Europe, that will work as a disincentive to software production in Europe".

Contents

| | |
|--------------------------|----------|
| 1 Patent Number | 2 |
| 2 Infringing Code | 2 |
| 3 History | 3 |

*<http://www.ffii.org/~phm>

1 Patent Number

WO0104742

<http://www.delphion.com/details?&pn=W000104742A1>

2 Infringing Code

Possibly FFII is also infringing on the patent by publishing this code:

```
//=====
// Compute H1 and H2 such that P = 2*H1 = 2*H2 (if such halves exist)
// Return TRUE iff the halves exist.
//=====
function TGF2NECurve.Halves(H1, H2, P: TGF2NEPoint): Boolean;
begin
  //--- Check
  if fStatus <> csHasCoefs then ErrorNoCoefs('Halves');

  //--- P = Identity ?
  if P.Is0 then
  begin
    GetOrder2Point(H1);
    H2.Set0;
    Result := true;
    Exit;
  end;

  with fField do
  begin
    //--- Compute T = X + Y/X (X and Y are unknow)
    //   Solve f(T) = T + T + A + Px
    GF2Set(H2.fY,fA);
    Add(H2.fY,P.fX);
    Result := SolveQuad(H1.fX,H2.fY); //H1.fX is used for "T"
    if not Result then
    begin
      H1.Set0;
      H2.Set0;
      Exit;
    end;
    //--- The 2 roots T and T+1 lead to the 2 halves H1 and H2
```

```

GF2Set(H2.fY,H1.fX);
GF2Set(H1.fY,H1.fX);
Add1(H1.fY); //!And not GF2Add1 because of possible Normal Basis
GF2Set(H2.fX,H1.fY);
//--- Compute H1.X
//    X := (T Px + Py)^(1/2)
Mul(H1.fX,P.fX);
Add(H1.fX,P.fY);
SqrRoot(H1.fX);
//--- Compute H1.Y
//    Y := X (X + T + 1)
Add(H1.fY,H1.fX);
Mul(H1.fY,H1.fX);
//--- Compute H2.X
//    X := ((T + 1) Px + Py)^(1/2)
Mul(H2.fX,P.fX);
Add(H2.fX,P.fY);
SqrRoot(H2.fX);
//--- Compute H2.Y
//    Y := X (X + T)
Add(H2.fY,H2.fX);
Mul(H2.fY,H2.fX);
end;
end;

```

3 History

Marcel Martin wrote to OCS, asking them to withdraw their ultimatum and explaining to them that his code uses a different method from the one described in the patent. OCS did not answer but merely asked Martin for his address and the names of his customers . When Marcel had taken HIT off the Net, they said “That’s not what we had wanted, we could have found an agreement”, but did not explain what the terms of this agreement could have been. Marcel felt that whatever these terms might be, they would not give him longterm security needed for continuing to invest his efforts in the project. He therefore decided to abandon it.