The security of

**Hidden Field Equations**

(HFE)

Nicolas T. Courtois
INRIA, Paris 6 and Toulon University
courtois@minrank.org

Permanent HFE web page:
hfe.minrank.org
Security of **Hidden Field Equations (HFE)**

**Road Map**

1. What is a secure public key cryptosystem?
2. RSA, EC, McEliece, HFE
3. OWF with Multivariate Quadratic equations (**MQ**)
4. Trapdoors - Hidden Field Equations (**HFE**)
5. 80-bit trapdoor HFE Challenge 1:
   - HFE $\leadsto$ MinRank $\leadsto$ MQ $\leadsto$ Solve [Shamir-Kipnis 99], $2^{152}$
   - HFE $\leadsto$ MinRank $\leadsto$ Solve [Shamir-Kipnis-Courtois 99], $2^{97}$
   - HFE $\leadsto$ Solve [Courtois 99], $2^{62}$
6. Short signatures (128 bits and less!)
What is a secure public key cryptosystem?

At least "Chosen-Ciphertext Security":

- Semantic security IND-CCA2 $\equiv$ non-malleability NM-CCA2
- Weak is enough!

Recent conversions from one-way trapdoor functions:

- OAEP+ [Bellare-Rogaway+Shoup]: for OW permutations
- Fujisaki-Okamoto and Pointcheval conversions [1999]
- REACT [Pointcheval-Okamoto 2001]: maximum efficiency. REACT also achieves strong Plaintext Awareness (PA2).

All we need:

Investigate the one-wayness of HFE trapdoor function: The HFE problem.
The RSA public key cryptosystem is based on a single modular equation in one variable. A natural generalization (...) is to consider several modular equations in several variables (...)

HFE is believed to be one of the strongest schemes of this type.

(…)

Adi Shamir

The algebraical structure of $\mathbb{Z}_N$ is too rich: RSA problem is subexponential and broken up to 512 bits.
Cryptosystems achieving exponential security

1978 McEliece cryptosystem (and Niederreiter variant)
   New signature scheme: [www.minrank.org/mceliece/](http://www.minrank.org/mceliece/)

1985 Elliptic curve systems [Koblitz, Miller]

For both, and due to existing group homomorphisms,

Problem: Attacks in $\sqrt{\text{exhaustive search}}$.

Tighter security?

The only candidate without $\sqrt{\text{exhaustive attacks}}$:
Multivariate Polynomials over finite fields:
1996 HFE family [Patarin]  

**But**...is it exponential?
Security foundations

RSA - an algebraical problem: factoring
- the RSA problem (one-wayness of RSA).

McEl. - a Goppa code looks as a random code
- Syndrome Decoding problem.

EC - obscurity of representation of a group. Nechaev group?

HFE - Several layers of security:
(a) - Algebraical problem HFE
- related problems MinRank, MQ, IP.
(b) - Operations that destroy the algebraical structure:
HFE $\leadsto$ HFEv $\leadsto$ HFEv- $\leadsto$ HFEv+ $\leadsto$ ...
Practical security

McEl. Original (1024, 524, 101) : about $2^{60}$ [Canteaut 1998].

RSA **512 bits** - broken in 1999, about $2^{58}$ CPU clocks.

EC **97 bits** - Certicom 1999, about $2^{59}$ CPU clocks.

HFE (a) The HFE problem **80 bits** - the HFE Challenge 1
       Best known attack is in $2^{62}$ [present paper].

(b) Modified versions of HFE **80 bits**, like HFE−, HFEv, HFEv- etc. No method is known to distinguish a trapdoor HFE function from random quadratic function. Only attacks very close to the exhaustive search.
Multivariate Quadratic one-way functions

The MQ problem over a ring $K$: Find (one) solution to a system of $m$ quadratic equations with $n$ variables in $K$.

$$f : \begin{cases} b_k = \sum_{i=0}^{n} \sum_{j=i}^{n} \lambda_{ijk} a_i a_j \\ \text{with } k = 1..m, \quad a_0 = 1 \end{cases}$$

Case $n = m = 1$.

$K = \mathbb{Z}_N$ is hard, factoring $N$ [Rabin].

$K = GF(q)$ solved, also for any fixed degree [Berlekamp 1967].
MQ is NP-complete for any field $K$

[Garey,Johnson], [Patarin, Goubin].

Proof for $K = GF(2)$ :

We encode 3-SAT $\sim$ cubic equations :

\[
\begin{align*}
0 &= x \lor y \lor z \\
1 &= \neg t \\
\vdots
\end{align*}
\]

\[
\begin{align*}
0 &= xyz + xy + yz + xz + x + y + z \\
1 &= 1 + t \\
\vdots
\end{align*}
\]

Transform cubic $\sim$ quadratic. We put :

- new variables $y_{ij} = x_i x_j$
- new trivial equations $0 = y_{ij} - x_i x_j$. 
Solving MQ

**Case** $m > \frac{n^2}{2}$ : MQ is solved by linearization (folklore):
- New variables $y_{ij} = x_i x_j$.
- At least $m$ linear equations with $m$ variables.

**Case** $m = \varepsilon \frac{n^2}{2}$ : MQ is expected to be polynomial in $n^{O(1/\sqrt{\varepsilon})}$.

First claimed by Shamir and Kipnis at Crypto’99.

The paper by Courtois, Patarin, Shamir and Klimov (Eurocrypt 2000) consolidated this claim. XL algorithm.

**Case** $m \approx n$ : MQ might (or not) be subexponential (unclear).
Conclusions on MQ from Eurocrypt 2000

The best known algorithms for solving $n$ multivariate equations with $n$ variables over a very small finite field are better than the exhaustive search only for about $n > 100$.

Trapdoors in MQ

General principles of design:

◦ A hidden function - invertible due to some algebraic properties.
◦ A basic (algebraic) version of a trapdoor - conceals algebraic structure with invertible affine variable changes (e.g. basic HFE).
◦ An extended (combinatorial) version of a trapdoor - destroys the algebraic structure by non-invertible operations (e.g. HFEv-).
$K$ - finite field $K = GF(q)$, $q$ prime or $q = p^\alpha$

$\exists$ a (unique) finite field $GF(q^n) = K[X]/P(X)$

with $P$ being a degree $n$ irreducible polynomial over $K$.

$GF(q^n) \equiv K^n$, vector space, dimension $n$ over $K$:

$x \in GF(q^n)$ is encoded as $(x_1, \ldots, x_n)$, $n$-tuple of coeff. of a polynomial from $K[X]$ modulo $P$.

Multivariate and univariate representations.

Every function $f : K^n \rightarrow K^n$ can be written as:

◊ a univariate polynomial.

◊ $n$ multivariate polynomials with $n$ variables over $K$. 

Multivariate and univariate degree.

If $b = f(a) = a^{q^s}$ then all the $b_i = f_i(a_1, \ldots, a_n)$ are $K$-linear.
If $f(a) = \sum a^{q^s+q^t}$ then the $f_i$ are quadratic.

Example over $GF(2)$.

$$b = f(a) = a + a^3 + a^5 =$$
$$(a_2X^2 + a_1X + a_0) + (a_2X^2 + a_1X + a_0)^3 + (a_2X^2 + a_1X + a_0)^5 \mod X^3 + X^2 + 1 =$$
$$(a_2 + a_2a_1 + a_2a_0 + a_1)X^2 + (a_2a_1 + a_1a_0 + a_2)X + (a_0 + a_2 + a_1a_0 + a_2a_0)$$

$$\begin{aligned}
  b_2 & = a_2 + a_2a_1 + a_2a_0 + a_1 \\
  b_1 & = a_2a_1 + a_1a_0 + a_2 \\
  b_0 & = a_0 + a_2 + a_1a_0 + a_2a_0
\end{aligned}$$
Hidden Field Equation (HFE).

\[ f(a) = \sum_{q^s + q^t \leq d} \gamma_{st} a^{q^s + q^t} \]

- Re-write as \( n \) multivariate quadratic equations:
  \[ f : \{ b_i = f_i(a_1, \ldots, a_n) \}_{i=1..n} \]
- Hide the univariate representation of \( f \):
  Apply two affine invertible variable changes \( S \) and \( T \).
  \[ g = T \circ f \circ S \]

\[ g : x \mapsto a \mapsto b \mapsto y \]
Security of Hidden Field Equations (HFE)

Using HFE

public key: \( n \) quadratic polynomials

\[
g : \left\{ y_i = g_i(x_1, \ldots, x_n) \right\}_{i=1..n}
\]

private key: Knowledge of \( T, S \) and \( f \).

Since \( f \) is bounded degree and univariate, we can invert it:

Several methods for factoring univariate polynomials over a finite field are known since [Berlekamp 1967]. Shoup’s NTL library.

Quite slow, example \( n=128, d=25, 0.17s \) on PIII-500.

Computing \( g^{-1} \) using the private information

\[
x \leftarrow a \leftarrow b \leftarrow y
\]
The HFE problem

A restriction of MQ to the trapdoor function \( g \) defined above.

- **Given** the multivariate representation of \( g \) and a random \( y \).
- **Find** a solution \( x \) such that \( g(x) = y \).

It is **not** about recovering the secret key.

**Claim**

Necessary and sufficient to achieve secure encryption and secure signature schemes with basic HFE.

\[
\text{HFE problem} \neq \text{HFE cryptosystem}
\]

- **basic HFE** - algebraical, \( \exists \) algebraical attacks on the trapdoor.
- **HFE-, HFEv, ..** combinatorial versions - no structural attacks.
How to recover $S$ and $T$.

If $f$ were known, $\exists$ algo in $q^{n/2} = \sqrt{\text{exhaustive search}}$.

the IP problem [Courtois, Goubin, Patarin, Eurocrypt’98].

Remark [Shamir] : $f$ is ‘known in 99%’ because $d << q^n - 1$

The weakness of HFE identified [Shamir-Kipnis, Crypto’99].

The homogenous quadratic parts of $g$ (and $f$) can be written in the univariate representation and represented by a using a symmetric matrix $G$ (resp. $F$) :

$$g(x) = \sum_{i=0}^{n-1} \sum_{j=i}^{n-1} G_{ij} x^{q^i+q^j}$$

$\text{rank}(G) = \text{supposedly } n$, and $\text{rank}(F) = r$ avec $r = \log d$. 
\[ T^{-1} \circ g \ ? \ f \circ S \]

**Lemma 1** [Shamir-Kipnis] : The matrix representation of \( f \circ S \) is of the form \( G' = WGW^t \). Same rank \( r \).

**Lemma 2** [Shamir-Kipnis] : \( T^{-1} \circ g = \sum_{k=0}^{n-1} t_k G^*k \) with \( G^*k \) being the public matrix representations of \( g^p\).

The attack focuses on finding a transformation \( T \) such that the matrix representation of \( T^{-1} \circ g \) is of small rank. Find such \( t_k \in K^n \) that

\[
\text{Rank}
\left( \sum_{k=0}^{n-1} t_k G^*k \right) = r
\]

Thus recovering the secret key of HFE is reduced to MinRank.
The problem MinRank

\[ \text{MinRank}(n \times n, m, r, K) \]

**Given**: \( m \) matrices \( n \times n \) over a ring \( K : M_1, \ldots, M_m \).

**Find** a linear combination \( \alpha \) of \( M_i \) of rank \( \leq r \).

\[ \text{Rank}(\sum_{i} \alpha_i M_i) \leq r. \]

**Fact**: MinRank is NP-complete [Shallit, Frandsen, Buss 1996].

MinRank can encode any set of multivariate equations.

MinRank contains syndrome decoding, probably exponential.

Also rank-distance syndrome decoding.
MinRank attacks on HFE in practice

Reference point: 80-bit trapdoor HFE Challenge 1.

Solving MinRank expressed as:

◊ [Shamir-Kipnis] MQ with \( n(n - r) \) quadratic equations with \( r(n - r) \) variables over \( K^n \), solve by relinearization/XL.

\[ 2^{152} \]

◊ Present paper: [cf. Coppersmith, Stern, Vaudenay]
  All the sub-matrices \((r+1) \times (r+1)\) are singular. Linearization.

\[ 2^{97} \]

◊ Exhaustive search on the underlying HFE

\[ 2^{80} \]
Do we need to recover the secret key?

Some cryptanalyses of multivariate schemes:

1. For **some** the secret key is computed:
   - $D^*$ [Courtois 97].
   - ‘Balanced Oil and Vinegar’ [Kipnis, Shamir Crypto’98]
   - HFE [Kipnis, Shamir Crypto’99].

2. In **many** cases the attack does not compute the secret key:
   - Matsumoto and Imai $C^*$ and $[C]$ schemes [Patarin]
   - Shamir birational signat. [Coppersmith, Stern, Vaudenay]
   - $D^*$, L. Dragon, S-boxes, $C^*$– [Patarin, Goubin, Courtois]
   - Equational attacks on HFE [present paper]
What characterizes functions $g$ that can(not) be inverted?

◊ Symmetric cryptography - there should be no simple way to relate $x$ and $g(x)$ with some equations [Shannon’s thoughts]
Idea of unpredictability, pseudorandomness.

◊ Asymmetric cryptography - usually explicit equations $g(x)$.
The pseudorandomness paradigm can hardly be applied.

Every deterministic attack can be seen as a series of transformations that start with some complex and implicit equations $G(x_i) = 0$.
It gives at the end some equations that are explicit and simple, e.g. $x_i = 0$ ou 1.

**Definition** [very informal] : One-way function in PKC
All ‘basic’ combinations of given equations do not give equations that are explicit or ‘simpler’.
We denote by $G_j$ the expressions in the $x_i$ of public equations of $g$ s.t. the equations to solve are $G_j = 0$.

We can generate other (multivariate) equations (true for $x$) by low degree combination of the $G_j$ and the $x_i$.

We require that such ‘trivial’ combinations of public equations remain ‘trivial’

**Definition [informal]**: A trivial equation is small degree combination of the $G_j$ and the $x_i$, with terms containing at least one $G_j$ and such that it’s complexity (e.g. multivariate degree) does not collapse.

**Soundness of the definition**: One such equation, substituted with the values of $G_j = 0$ gives a new low degree equation in the $x_i$. 
Implicit equations attacks [Patarin, Courtois].

Several attacks that use several types of equations.

Common properties:

- We can only predict the results in very simple cases.
- Experimental equations can be found with no apparent theoretical background.
- The equations are detected only beyond some threshold (e.g. 840 Mo).

**HFE Challenge 1**

We found equations of type $1 + x + y + x^2 y + x y^2 + x^3 y + x^2 y^2$.

Gives an attack in $2^{62}$.

An optimised requires ”only” 390 Gb of disk space [present paper].
### Asymptotic security of HFE

<table>
<thead>
<tr>
<th>Attack</th>
<th>Cxty</th>
<th>$d = n^\mathcal{O}(1)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shamir-Kipnis Crypto’99</td>
<td>$n \log^2 d$</td>
<td>$e \log^3 n$</td>
</tr>
<tr>
<td>HFE $\leadsto$ skHFE $\leadsto$ MinRank $\leadsto$ MQ</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Shamir-Kipnis-Courtois</td>
<td>$n \cdot 3 \log d$</td>
<td>$e \log^2 n$</td>
</tr>
<tr>
<td>HFE $\leadsto$ skHFE $\leadsto$ MinRank</td>
<td></td>
<td></td>
</tr>
<tr>
<td>My best attack</td>
<td>$n \cdot \frac{3}{2} \log d$</td>
<td>$e \log^2 n$</td>
</tr>
<tr>
<td>HFE $\leadsto$ Implicit Equations</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

HFE is **polynomial** if $d$ fixed.

The degree $d$ can be quite big in practice.

It is **subexponential**, in general: $d = n^\mathcal{O}(1)$.

The HFE problem is probably **not** polynomial in general (because MinRank is probably exponential).
State of Art on HFE security

⋄ The asymptotic complexity of breaking the algebraical HFE (HFE problem) is currently $e^{\log^2 n}$.

⋄ In practice basic HFE with $d > 128$ is still very secure.

⋄ Modified, combinatorial versions of HFE have no weaknesses known, e.g. -HFE$^-$ [Asiacrypt’98], -HFEv [Eurocrypt’99], -Quartz and even Flash and Sflash [RSA 2001].

⋄ Combinatorial versions of HFE can be either:
  - hundreds of times faster than RSA and be implemented on smart cards (Flash, Sflash), or
  - give very short signatures for memory cards (Quartz).
Digital signatures.

\( f \) - a trapdoor function, \( n \) bits.

Usual method: \[ \sigma = f^{-1}( H(m) ) \] \( H \) - cryptographic hash.

Existential Forgery: Birthday paradox attack:

1. Generate \( 2^{n/2} \) versions of the message to be signed \( m_1, \ldots, m_{2^{n/2}} \), adding spaces, commas, addenda etc..
2. Generate a list of \( 2^{n/2} \) values \( f(\sigma_j) \), for random \( \sigma_j \).
3. Sort the two lists, we expect to find \( (i, j) \) such that:
   \[ f(\sigma_j) = H(m_i) \]
Thus breaking signatures of 80 bits requires is done in about $2^{40}$.

**Feistel-Patarin signatures**

Uses two hash functions $H_1, H_2$:

$$\sigma = f^{-1} \left( H_1(m) + f^{-1} \left[ H_2(m) + f^{-1}(H_1(m)) \right] \right)$$

Comparison of typical signatures (security $\approx 2^{80}$):

<table>
<thead>
<tr>
<th>Signature</th>
<th>Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSA</td>
<td>$\sim$ 700 bits</td>
</tr>
<tr>
<td>DSA</td>
<td>$\sim$ 320 bits</td>
</tr>
<tr>
<td>EC</td>
<td>$\sim$ 321 bits</td>
</tr>
<tr>
<td>HFEv-, Quartz</td>
<td>$\sim$ 128 bits</td>
</tr>
<tr>
<td>HFEf+</td>
<td>$\sim$ 92 bits</td>
</tr>
<tr>
<td>McEliece</td>
<td>$\sim$ 87 bits</td>
</tr>
</tbody>
</table>

[www.minrank.org/quartz/](http://www.minrank.org/quartz/)

What signatures are the best? **Bad question**

Use several algorithms and issue several certificates.

Programs, terminals and devices will have at least one common algorithm for few years.

**Pro-active scenario:** Invalidate some algorithms and introduce new ones.

Example, when 768-bit RSA is broken, the 1024-bit RSA expires.

Un example of combined certificate:

\[ \text{RSA} + \text{EC} + \text{HFE} = 1024 + 321 + 128 \text{ bits}. \]

RSA is slow and signatures are so long that all the rest is for free!