Differential Security of the $HFEv^-$ Signiture Primitive

Ryann Cartor [1] Ryan Gipson [1] Daniel Smith-Tone [1,2]
Jeremy Vates [1]

[1] University of Louisville

[2] National Institute of Standards and Technology

25th February, 2016

Introduction

1. Motivation for the Differential
   1. Patarin's attack on C^*
   2. SFLASH
   3. Oil-Vinegar attack by Kipnis and Shamir
2. Previous Work
   1. Perlner, Smith-Tone on C^* and pC^*
   2. Daniels, Smith-Tone on HFE and $HFE-$

Outline

1. System Structure and Basic Definitions
2. Differential Symmetry
3. Differential Invariant
4. Future Work and Conclusion

Structure of $HFEv$

Field

Let $\mathbb{K}$ be degree n extension of a given finite field $\mathbb{F}_q$.

Definition of the Core Map

$$f(\mathbf{x}) = \sum_{\substack{i \leq j \\ q^i + q^j \leq D}} \alpha_{i,j} x^{q^i + q^j} + \sum_{\substack{i \\ q^i \leq D}} \beta_i(\tilde{x}_1, \ldots, \tilde{x}_v) x^{q^i} + \gamma(\tilde{x}_1, \ldots, \tilde{x}_v)$$

Butterfly Construction

Usually, the core map is composed with two affine transformations, $T, U : \mathbb{F}_q^n \to \mathbb{F}_q^n$. The resulting composition $P = T \circ \phi^{-1} \circ f \circ \phi \circ U$ is the public key.

The Discrete Differential

Definition

The discrete differential of a field map $f : \mathbb{K} \to \mathbb{K}$ is given by:

$$Df(a, x) = f(a + x) - f(a) - f(x) + f(0)$$

Essentially, the differential is a normalized difference operator.

Differential Adversary

We define a differential adversary as an "opponent" who attempts to gain structural information about an unknown field map by discovering properties of the map's discrete differential.

Differential Adversary cont.

Discrete Differential Properties

A differential adversary will try to compute the following:

1. A linear map M such that

$$DP(Mx, a) + DP(x, Ma) = \Lambda_M DP(a, x)$$

2. Subspaces V, W with $dim(V) + dim(W) \geq n$ where n is the number of variables, so that $DP(y, x) = 0 \, \forall x \in V, y \in W$.

Differential of $HFEv$

Core Map

$$f(x,y) = \sum_{\substack{0 \le i \le j < n \\ q^i + q^j \le D}} \alpha_{ij} x^{q^i + q^j} + \sum_{\substack{0 \le i,j < n \\ q^i \le D}} \beta_{ij} x^{q^i} y^{q^j} + \sum_{0 \le i \le j < n} \gamma_{ij} y^{q^i + q^j}.$$

$Df(a,b,x,y)$

$$\begin{aligned} Df(a,b,x,y) = & \sum \alpha_{i,j} (x^{q^i} a^{q^j} + x^{q^j} a^{q^i}) \\ & + \sum \beta_{i,j} (x^{q^i} b^{q^j} + a^{q^i} y^{q^j}) \\ & + \sum \gamma_{i,j} (y^{q^i} b^{q^j} + y^{q^j} b^{q^i}) \end{aligned}$$

Avoiding Differential Symmetry

Our Goal

Attempt to prevent an $M : \mathbb{K} \to \mathbb{K}$ linear map such that

$$DP(Mx, a) + DP(x, Ma) = \Lambda_M DP(a, x)$$

Representation

Similar to the representation used by Daniels and Smith-Tone for HFE, we use a vector representation for $\mathbb{K}$ with,

$$[x \quad y] \mapsto [x \quad x^q \quad x^{q^2} \quad \dots \quad x^{q^{n-1}} \quad y \quad y^q \quad y^{q^2} \quad \dots \quad y^{q^{n-1}}]^T,$$

Representation cont.

Note, any $\mathbb{F}_q$-linear map $M : \mathbb{K} \to \mathbb{K}$ is represented by $Mx = \sum_{i=0}^{n-1} m_i x^{q^i}$.

$$M = \begin{pmatrix} m_0 & m_1 & \cdots & m_{n-1} \\ m_{n-1}^q & m_0^q & \cdots & m_{n-2}^q \\ \vdots & \vdots & \ddots & \vdots \\ m_1^{q^{n-1}} & m_2^{q^{n-1}} & \cdots & m_0^{q^{n-1}} \end{pmatrix}$$

However, when viewing an $\mathbb{F}_q$-linear map over our vector $[\hat{x} \;\; \hat{y}]^T$, we get:

$$\overline{M} = \left[\begin{array}{c|c} M_{00} & M_{01} \\ \hline M_{10} & M_{11} \end{array}\right]$$

Working with Matrices

Matrix Representation

$$DP(Ma, x) + DP(a, Mx) = a(M^T DP + DPM)x$$

Matrix Equation

Rewriting $DP(Ma, x) + DP(a, Mx) = \Lambda_M DP(a, x)$ in matrix form gives:

$$a(M^T DP + DPM)x = a(\Lambda_M DP)x$$

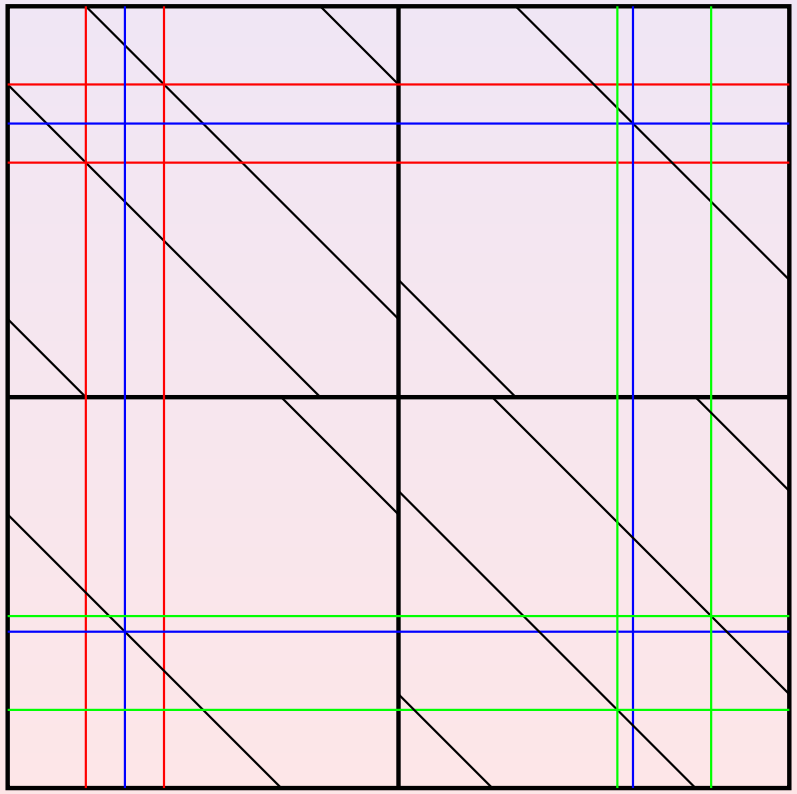
Thus, we get

$$M^T DP + DPM = \Lambda_M DP$$

and attempt to prevent non-trivial solutions.

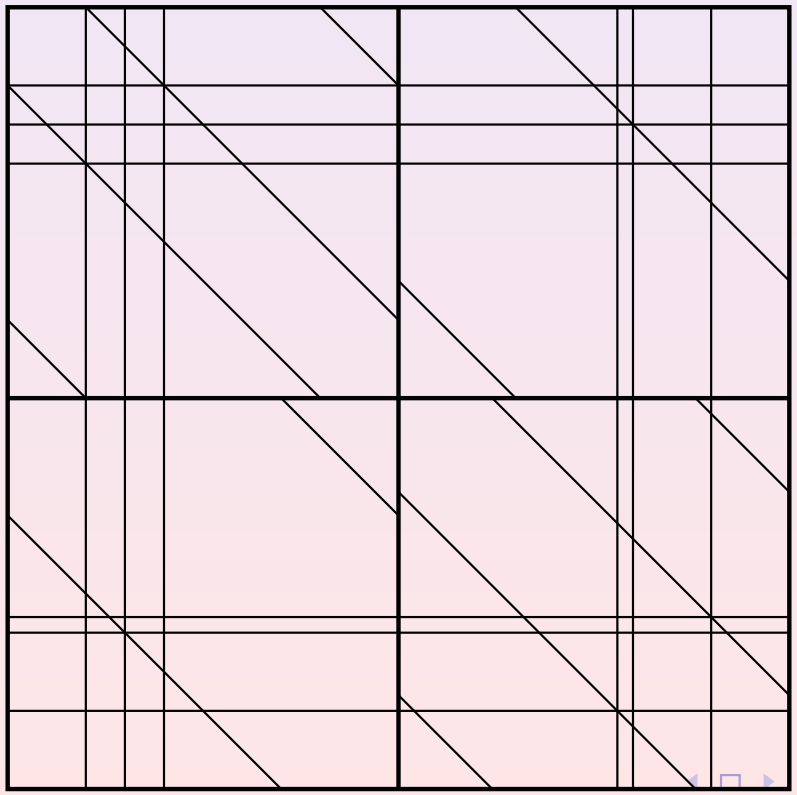
Graphical Representation

1. $f(x,y) = \alpha_{i,j} x^{q^i+q^j} + \beta_{r,s} x^{q^r} y^{q^s} + \gamma_{u,v} y^{q^u+q^v}$
2. $M^T DP + DPM = \Lambda_M DP$



Algorithm

1. Generates each set of all possible non-zero indicies of M
2. Cross reference all such sets
3. Returns all entries of M that are possibly non-zero



Restrictions

Restrictions on $HFEv$

Let $f(x, y)$ be an $HFEv$ polynomial.

1. Let no power of q be repeated among the exponents of f.
2. Make the difference of powers of q unique
3. Restrict choice of exponents to triangle numbers in suggested values provided by Ding, J.

M must be a trivial differential symmetry

After applying the algorithm to a core map with the previously described conditions, the algorithm results with the only non-zero term of M is m_0. This results in the following structure:

$$\overline{M} = \left[\begin{array}{c|c} cI & dI \\ \hline dI & cI \end{array}\right]$$

with $c, d \in \mathbb{F}_q$. Note that this is a trivial differential symmetry:

$$\begin{aligned} Dg(\overline{M}[a\ b]^T, [x\ y]^T) &= Dg([ca + db\ da + cb]^T, [x\ y]^T) \\ &= Dg([ca + db\ cb + da]^T, [x\ y]^T) \\ &= Dg(c[a\ b]^T, [x\ y]^T) + Dg(d[b\ a]^T, [x\ y]^T) \\ &= cDg(a, b, x, y) + dDg(b, a, x, y) \\ &= (c + d)Dg(a, b, x, y). \end{aligned}$$

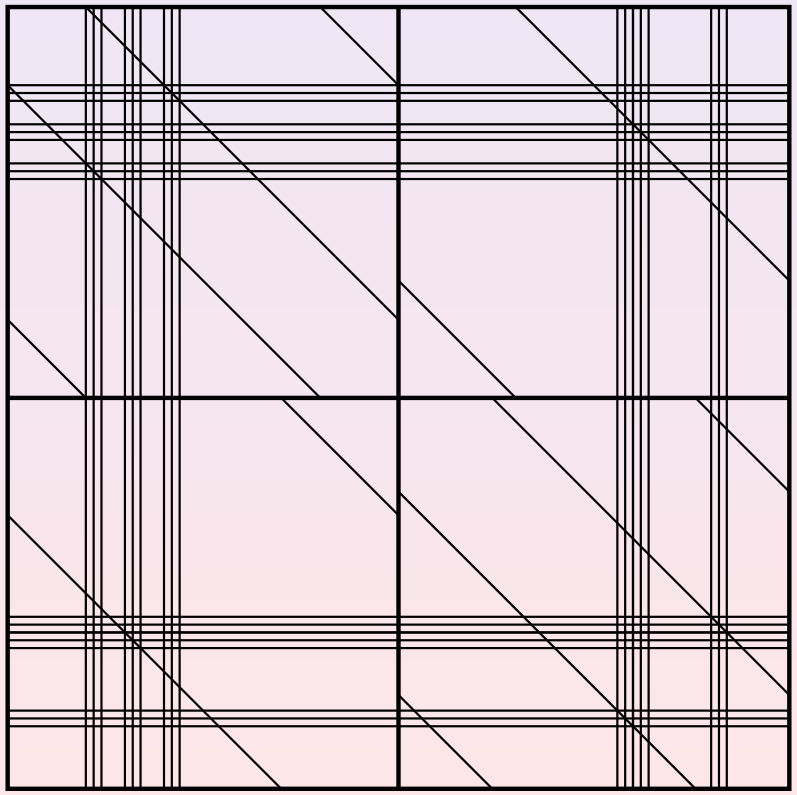
Adaptation to Key Generation

Security Against Differential Symmetry

The algorithm described would be placed within a random key generation algorithm. In doing so, you will have provable security against an Adversary attempting to find underling structure through differential symmetry.

Graphical Representation

The method used to analyze $HFEv$ extends very naturally to $HFEv^{-}$. This requires an adaptation to our figure:



Adaptations and Results

Adaptation to Algorithm

1. Call $HFEv$ subroutine
2. Append extra sets of possible non zero entries in M
3. Intersect all such sets

Results in $HFEv-$

With the previously described restrictions, the algorithm will result with m_0 being the only possible non-zero entry of M. Thus, being secure against a symmetrical attack from a Differential Adversary.

Differential Invariants

Definition

Let $f : \mathbb{F}_q^n \to \mathbb{F}_q^m$ be a function. A **differential invariant** of f is a subspace $V \subseteq \mathbb{K}$ with the property that there is a subspace $W \subseteq \mathbb{K}$ such that $dim(W) \leq dim(V)$ and $\forall A \in Span_{\mathbb{F}_q}(Df_i), AV \subseteq W$.

Definition

Assume there exists a differential invariant V, we can define a corresponding subspace
$V^{\perp} = \{x \in \mathbb{K} : \langle x, Av \rangle = 0 \, \forall v \in V, \forall A \in Span(Df_i)\}$.

Propositions

$Df(M^{\perp}y, Mx)$

Suppose that V is a subspace of $\mathbb{K}$. If $M : \mathbb{K} \to V$ and $M^{\perp} : \mathbb{K} \to V^{\perp}$, then $\forall y, x \in \mathbb{F}_q^n, Df(M^{\perp}y, Mx) = 0$, or equivalently $Df(M^{\perp}\mathbb{F}_q^n, M\mathbb{F}_q^n) = 0$.

$A = CBD$

If A, B are two $m \times n$ matrices, then $rank(A) = rank(B)$ if and only if there exists nonsingular matrices C, D, such that $A = CBD$.

Therefore

Given the two previous propositions, we can write $M^{\perp} = SMT$, with S possibly singular and T nonsingular.

$HFEv$

Theorem 1

Let $\mathbb{K}$ be a degree n extension of the finite field $\mathbb{F}_q$. Let f be an $HFEv$ core map. With high probability, f has no nontrivial differential invariant structure.

Proof Outline

1. Calculate the Differential of the core map using $SMT[a\,b]^T$ and $MT[a\,b]^T$.
2. In contrast with HFE, monomials are not necessarily independent
3. Represent the differential using generators of $I(V)$.
4. Evaluate the previously mentioned differential modulo $I(V)$.
5. Resulting monomials are linearly independent.

$HFEv$ Theorem proof cont.

Proof Cont.

1. Due to the independence of the resulting monomials, we get the following equality:

$$LS[\hat{a}_0 \cdots \hat{a}_{n-1}\, \hat{b}_0 \cdots \hat{b}_{n-1}]^T = 0$$

   where L is a $n \times 2n$ matrix with entries in $\mathbb{F}_q$.
2. We expect L to have high rank with probability more than $1 - q^{-n}$.
3. Thus, the dimension of the intersections of the null spaces of each L is zero with probability at least $1 - 2q^{-n}$.

$HFEv$ Theorem proof cont.

Proof Cont.

1. The condition for the above equation to be satisfied is that S sends V to the intersection of the null spaces of each such L. Thus, S is with high probability the zero map on V, and so $V^{\perp} = \{0\}$.
2. This implies $2n \leq dim(V) + dim(V^{\perp}) < 2n$. A contradiction.
3. Thus, with probability greater than $1 - 2q^{-n}$, f has no nontrivial differential invariant.

$HFEv-$ Theorem

Theorem 2

Let f be an $HFEv$ core map and let π be a linear projection. With high probability, $\pi \circ f$ has no nontrivial differential invariant structure.

Proof Outline

1. Proof is very similar to $HFEv$.
2. Difference in probabilities
3. One must note that since the condition of being a differential invariant is a condition on the span of the public differential forms, under projection this condition is weaker, thus easier to satisfy.

Final Thoughts

1. Above restrictions on core map does dimish the key space, however there is still plenty of entropy and you are guarenteed security against the differential symmetric attack.
2. Along with the careful analysis of Q-rank and degree of regularity present in the literature, we have shown $HFEv-$ is very secure against all attack methods known.
3. Any future successful attack on $HFEv-$ would have to be by way of a fundamentally new technique.

Thank you for your attention.