An Updated Security Analysis of PFLASH

Ryann Cartor[1] & **Daniel Smith-Tone**[1,2]

[1]University of Louisville
[2]National Institute of Standards and Technology

27 June, 2017

Multivariate Digital Signatures

Public Key

A system of (generally structured) nonlinear equations. Typically a quadratic trapdoor function.

Multivariate Digital Signatures

Public Key

A system of (generally structured) nonlinear equations. Typically a quadratic trapdoor function.

Signature

A signature is generated by using secret information to invert the public nonlinear system. The preimage is the signature.

Multivariate Digital Signatures

Public Key

A system of (generally structured) nonlinear equations. Typically a quadratic trapdoor function.

Signature

A signature is generated by using secret information to invert the public nonlinear system. The preimage is the signature.

Verification

One verifies by evaluating the public key at the signature value.

Hiding Structure

Polynomial Morphisms

Let $f, g : \mathbb{F}^n \to \mathbb{F}^m$ be polynomial functions. A *polynomial morphism* between f and g is a pair of affine transformations $T \in M_m(\mathbb{F})$ and $U \in M_n(\mathbb{F})$ such that

$$g = T \circ f \circ U.$$

Hiding Structure

Polynomial Morphisms

Let $f, g : \mathbb{F}^n \rightarrow \mathbb{F}^m$ be polynomial functions. A *polynomial morphism* between f and g is a pair of affine transformations $T \in M_m(\mathbb{F})$ and $U \in M_n(\mathbb{F})$ such that

$$g = T \circ f \circ U.$$

Isomorphism of Polynomials

If T and U are nonsingular, then the pair (T, U) is an *isomorphism of polynomials*. Further, if T is the identity, then U is called a one-sided isomorphism between f and g.

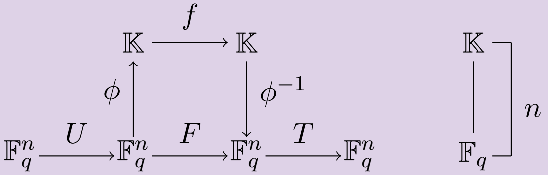
Big Field Schemes

Construct an extension field $\mathbb{K}$ of $\mathbb{F}$. One may think of the extension as a commutative $\mathbb{F}$-algebra that happens to be a field. One utilizes the multiplication in $\mathbb{K}$ to construct an invertible map.

Big Field Schemes

Construct an extension field $\mathbb{K}$ of $\mathbb{F}$. One may think of the extension as a commutative $\mathbb{F}$-algebra that happens to be a field. One utilizes the multiplication in $\mathbb{K}$ to construct an invertible map.

Butterfly Construction



C^* Scheme

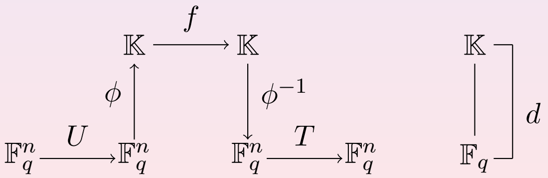
- Presented by Matsumoto and Imai at Eurocrypt '88

C* Scheme

- Presented by Matsumoto and Imai at Eurocrypt '88
- Big field scheme where the vector-valued representation of a quadratic monomial map $f(x) = x^{q^\theta+1}$ is hidden by an isomorphism.

C^* Scheme

- Presented by Matsumoto and Imai at Eurocrypt '88
- Big field scheme where the vector-valued representation of a quadratic monomial map $f(x) = x^{q^\theta+1}$ is hidden by an isomorphism.
- Thus the public key is given by $P = T \circ \phi^{-1} \circ f \circ \phi \circ U$.



Minus and projection modifiers

Minus modifier: delete r of the n public key equations.

Projection modifier: fix the value of d input variables.

PFLASH

The PFLASH scheme is a particular parametrization of pC^{*-}, i.e. a C^* scheme with the projection and minus modifiers.

PFLASH

The PFLASH scheme is a particular parametrization of pC^{*-}, i.e. a C^* scheme with the projection and minus modifiers.

The public key is given by:

$$P = \pi_r \circ T \circ \phi^{-1} \circ f \circ \phi \circ U \circ \pi_d,$$

where π_r and π_d are codimension r and d affine projections, respectively.

Discrete Differential

Given a function f, the **discrete differential** of f is defined by
$Df(a,x) = f(a+x) - f(a) - f(x) + f(0)$.

Discrete Differential

Given a function f, the **discrete differential** of f is defined by
$Df(a,x) = f(a+x) - f(a) - f(x) + f(0)$.

C^* Differential

$$Df(a,x) = (a+x)^{q^\theta+1} - a^{q^\theta+1} - x^{q^\theta+1} = ax^{q^\theta} + a^{q^\theta}x.$$

Discrete Differential

Given a function f, the **discrete differential** of f is defined by
$Df(a,x) = f(a+x) - f(a) - f(x) + f(0)$.

C^* Differential

$$Df(a,x) = (a+x)^{q^\theta+1} - a^{q^\theta+1} - x^{q^\theta+1} = ax^{q^\theta} + a^{q^\theta}x.$$

For any quadratic function f, Df is bilinear.

Differential Symmetry

A function $f : \mathbb{K} \to \mathbb{K}$ has a **differential symmetry** if there exists a pair of $\mathbb{F}_q$-linear maps $M, \Lambda_M : \mathbb{K} \to \mathbb{K}$ such that

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

Differential Symmetry

A function $f : \mathbb{K} \to \mathbb{K}$ has a **differential symmetry** if there exists a pair of $\mathbb{F}_q$-linear maps $M, \Lambda_M : \mathbb{K} \to \mathbb{K}$ such that

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

In the case of C^* the differential symmetry of f is inherited by the scheme with the minus modifier, C^{*-}, and is the basis of the attack on SFLASH of [Dubois et al.,2007].

Differential Symmetry

A function $f : \mathbb{K} \to \mathbb{K}$ has a **differential symmetry** if there exists a pair of $\mathbb{F}_q$-linear maps $M, \Lambda_M : \mathbb{K} \to \mathbb{K}$ such that

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

In the case of C^* the differential symmetry of f is inherited by the scheme with the minus modifier, C^{*-}, and is the basis of the attack on SFLASH of [Dubois et al.,2007].

Thus, differential symmetry can be exploited to remove the minus modifier when there is a space of nontrivial (i.e. non-scalar) linear maps inducing a differential symmetry on the central map.

Differential analysis of pC^*

$$\text{Fix } \Pi x = \sum_{i=0}^{d} \beta_i x^{q^i}.$$

Differential analysis of pC^*

$$\text{Fix } \Pi x = \sum_{i=0}^{d} \beta_i x^{q^i}.$$

- As shown in [Chen et al.,2015], we may assume the projection mapping is tied to f and consider differential symmetries of $f \circ \pi$.

Differential analysis of pC^*

$$\text{Fix } \Pi x = \sum_{i=0}^{d} \beta_i x^{q^i}.$$

- As shown in [Chen et al.,2015], we may assume the projection mapping is tied to f and consider differential symmetries of $f \circ \pi$.
- If $f \circ \pi$ has a differential symmetry, then the relation

$$Df(Ma, \pi x) + Df(\pi a, Mx) = \Lambda_M Df(\pi a, \pi x) \qquad (1)$$

holds for some M, where

$$Mx = \sum_{i=0}^{n-1} m_i x^{q^i} \text{ and } \Lambda_M x = \sum_{i=0}^{n-1} \lambda_i x^{q^i}.$$

Representation of $\mathbb{K}$

We use the following representation of $\mathbb{K}$:

$$\rho : \mathbb{K} \to \mathbb{A},$$

where $\mathbb{A} = \left\{ \begin{pmatrix} a & a^q & \dots & a^{q^{n-1}} \end{pmatrix}^\top : a \in \mathbb{K} \right\}$, defined by:

$$a \overset{\rho}{\mapsto} \begin{pmatrix} a & a^q & \dots & a^{q^{n-1}} \end{pmatrix}^\top =: \mathbf{a}.$$

Main Equation

Equation (1) can be expressed over $\mathbb{A}$ as follows:

$$\mathbf{a}^T(\mathbf{\Pi}^T\mathbf{DfM})\mathbf{x} + \mathbf{a}^T(\mathbf{M}^T\mathbf{Df\Pi})\mathbf{x} = \Lambda_M[\mathbf{a}^T(\mathbf{\Pi}^T\mathbf{Df\Pi})\mathbf{x}], \qquad (2)$$

Main Equation

Equation (1) can be expressed over $\mathbb{A}$ as follows:

$$\mathbf{a}^T(\mathbf{\Pi}^T\mathbf{Df}\mathbf{M})\mathbf{x} + \mathbf{a}^T(\mathbf{M}^T\mathbf{Df}\mathbf{\Pi})\mathbf{x} = \Lambda_M[\mathbf{a}^T(\mathbf{\Pi}^T\mathbf{Df}\mathbf{\Pi})\mathbf{x}], \quad (2)$$

where:

- $\mathbf{Df}$ is the matrix representing Df as a bilinear form on $\mathbb{A}$ over $\mathbb{K}$,
- $\mathbf{M}$ is the matrix representation on $\mathbb{A}$ of the map $x \mapsto Mx$ and
- $\mathbf{\Pi}$ is the matix representation on $\mathbb{A}$ of the map $x \mapsto \Pi x$.

Df Matrix

$$f(x) = x^{q^\theta+1}$$

$$Df(a,x) = f(a+x) - f(a) - f(x) + f(0) = a^{q^\theta}x + ax^{q^\theta}$$

$$\mathbf{Df} = \begin{pmatrix} 0 & 0 & \cdots & 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \cdots & \vdots & \vdots & \vdots & \cdots & \vdots \\ 1 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \cdots & \vdots & \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \end{pmatrix}$$

M Matrix

$$Mx = \sum_{i=0}^{n-1} m_i x^{q^i}$$

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

Π Matrix

$$\Pi x = \sum_{i=0}^{d} \beta_i x^{q^i}$$

$$\mathbf{\Pi} = \begin{pmatrix} \beta_0 & \beta_1 & \cdots & \beta_{d-1} & \beta_d & 0 & 0 & \cdots & 0 \\ 0 & \beta_0^q & \cdots & \beta_{d-2}^q & \beta_{d-1}^q & \beta_d^q & 0 & \cdots & 0 \\ \vdots & \vdots & \cdots & \vdots & \vdots & \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & 0 & \beta_0^{q^d} & \beta_1^{q^d} & \beta_2^{q^d} & \cdots & 0 \\ \vdots & \vdots & \cdots & \vdots & \vdots & \vdots & \vdots & \cdots & \vdots \\ \beta_1^{q^{n-1}} & \beta_2^{q^{n-1}} & \cdots & \beta_d^{q^{n-1}} & 0 & 0 & 0 & \cdots & \beta_0^{q^{n-1}} \end{pmatrix}$$

Idea of Analysis

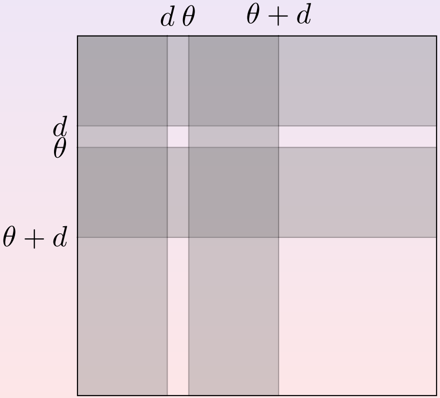
The following images assume $d < \theta + 1$. The argument in the paper is general.

$\Pi^\top D f M + M^\top D f \Pi$

If we shade the nonzero coordinates of the left hand side of (2), our matrix will look like the following:

$\Pi^\top D f M + M^\top D f \Pi$

If we shade the nonzero coordinates of the left hand side of (2), our matrix will look like the following:

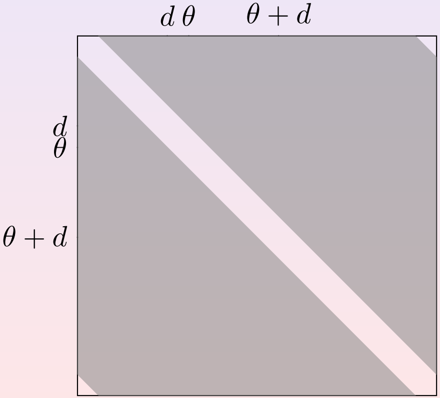


$\Lambda_M(\Pi^\top Df\Pi)$

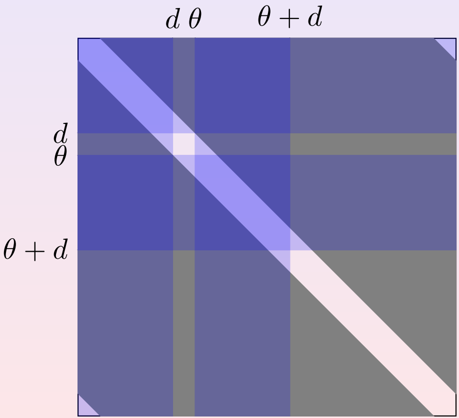
If we shade the nonzero coordinates of the right hand side of (2), our matrix will look like the following:

$\Lambda_M(\Pi^\top D f \Pi)$

If we shade the nonzero coordinates of the right hand side of (2), our matrix will look like the following:



LHS=RHS, Equation (2)



Strategy

Equation (2) is nonlinear in the coefficients of $\mathbf{\Pi}$, but linear in the coefficients of $\mathbf{M}$ and Λ_M.

Strategy

Equation (2) is nonlinear in the coefficients of $\mathbf{\Pi}$, but linear in the coefficients of $\mathbf{M}$ and Λ_M.

For fixed $\mathbf{\Pi}$ it is easy to solve, but we want to solve it with d as a parameter.

Strategy

Equation (2) is nonlinear in the coefficients of $\mathbf{\Pi}$, but linear in the coefficients of $\mathbf{M}$ and Λ_M.

For fixed $\mathbf{\Pi}$ it is easy to solve, but we want to solve it with d as a parameter.

Thus, we solve Equation (2) generically.

Strategy

Equation (2) is nonlinear in the coefficients of $\mathbf{\Pi}$, but linear in the coefficients of $\mathbf{M}$ and Λ_M.
For fixed $\mathbf{\Pi}$ it is easy to solve, but we want to solve it with d as a parameter.
Thus, we solve Equation (2) generically.

- Focus on coordinates for which (LHS=0) to determine for what r values is $m_r = 0$.

Strategy

Equation (2) is nonlinear in the coefficients of $\mathbf{\Pi}$, but linear in the coefficients of $\mathbf{M}$ and Λ_M.

For fixed $\mathbf{\Pi}$ it is easy to solve, but we want to solve it with d as a parameter.

Thus, we solve Equation (2) generically.

- Focus on coordinates for which (LHS=0) to determine for what r values is $m_r = 0$.
- Use this information to find for what values of r it is true that $\lambda_r = 0$ (RHS=0).

Strategy

Equation (2) is nonlinear in the coefficients of $\mathbf{\Pi}$, but linear in the coefficients of $\mathbf{M}$ and Λ_M.

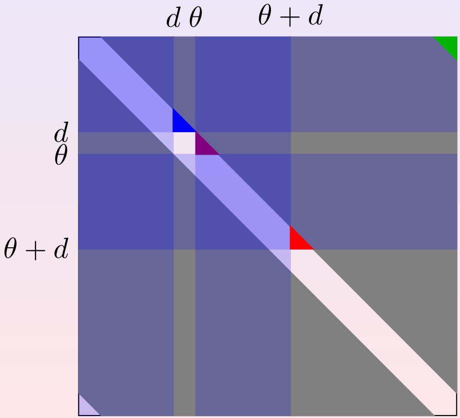
For fixed $\mathbf{\Pi}$ it is easy to solve, but we want to solve it with d as a parameter.

Thus, we solve Equation (2) generically.

- Focus on coordinates for which (LHS=0) to determine for what r values is $m_r = 0$.
- Use this information to find for what values of r it is true that $\lambda_r = 0$ (RHS=0).
- Repeat until no new generic information is produced.

Single term LHS=0 (top half only, rest by symmetry)

Critical Regions

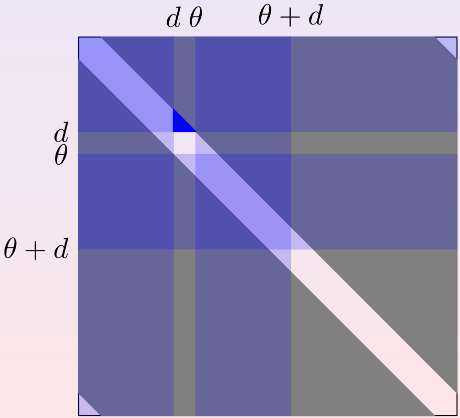


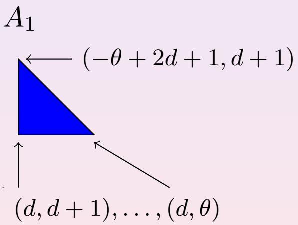
Let:

- Green= region A_2
- Blue= region A_1
- Purple= region B
- Red= region C

Coordinates of Regions

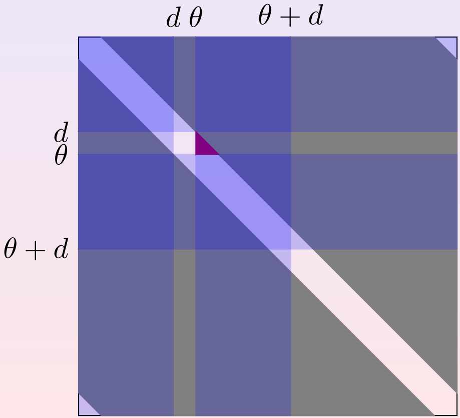
Region A_1

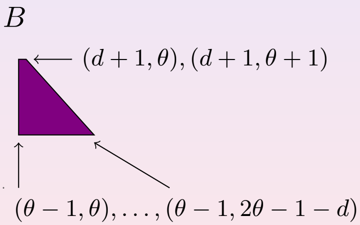




Coordinates of Regions

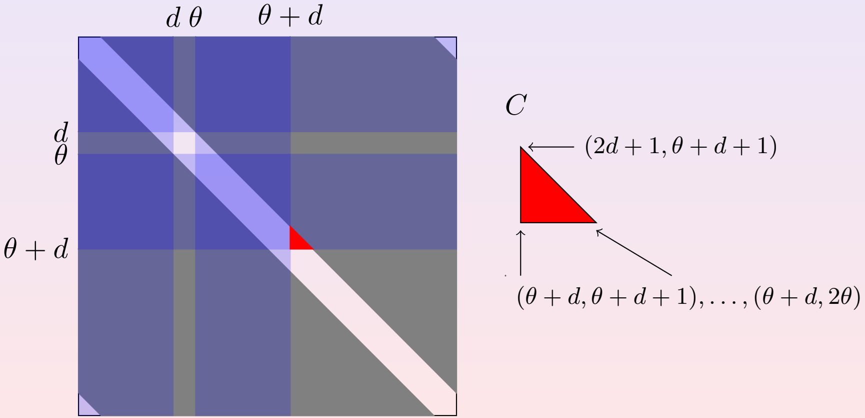
Region B





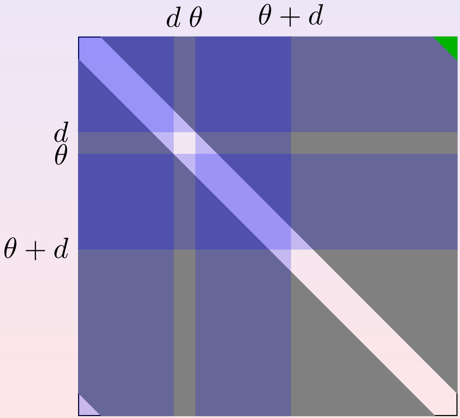
Coordinates of Regions

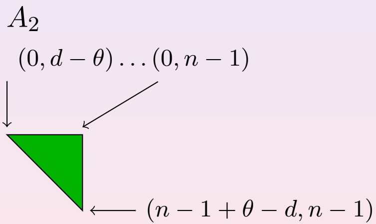
Region C



Coordinates of Regions

Region A_2





Bootstrap

[S.-T., 2011] provides a proof for any projection Π with $\beta_i \neq 0$ for $0 \leq i \leq d$ (and specific and restrictive conditions on d) that there is no non-trivial symmetry.

Bootstrap

[S.-T., 2011] provides a proof for any projection Π with $\beta_i \neq 0$ for $0 \leq i \leq d$ (and specific and restrictive conditions on d) that there is no non-trivial symmetry.

Lemma

$f(x^{q^k}) = f(x)^{q^k}$, *where* $f(x) = x^{q^\theta+1}$.

Bootstrap

[S.-T., 2011] provides a proof for any projection Π with $\beta_i \neq 0$ for $0 \leq i \leq d$ (and specific and restrictive conditions on d) that there is no non-trivial symmetry.

Lemma

$f(x^{q^k}) = f(x)^{q^k}$, *where* $f(x) = x^{q^\theta+1}$.

Theorem

If Equation (2) *holds with the condition above and either* $d < \min\{\frac{n}{2} - \theta, |n - 3\theta|, \theta - 1\}$ *or* $d < \{\theta - \frac{n}{2}, |2n - 3\theta|, n - \theta - 1\}$, *then* $M = M_\sigma \circ \Pi$.

Conclusion on Symmetry

- Notice that the existence of a differential symmetry for $f \circ \Pi$ implies that M_σ and Π commute.

Conclusion on Symmetry

- Notice that the existence of a differential symmetry for $f \circ \Pi$ implies that M_σ and Π commute.
- Thus differential symmetry implies there is a subfield $\mathbb{L}$, where $\mathbb{F}_q \subseteq \mathbb{L} \subseteq \mathbb{K}$ such that $\sigma \in \mathbb{L}$ and Π is $\mathbb{L}$-linear.

Conclusion on Symmetry

- Notice that the existence of a differential symmetry for $f \circ \Pi$ implies that M_σ and Π commute.
- Thus differential symmetry implies there is a subfield $\mathbb{L}$, where $\mathbb{F}_q \subseteq \mathbb{L} \subseteq \mathbb{K}$ such that $\sigma \in \mathbb{L}$ and Π is $\mathbb{L}$-linear.
- Since $[\mathbb{L} : \mathbb{F}_q]$ divides (n, d), choosing $d = 1$ is the most efficient way to provably eliminate symmetry.

Conclusion on Symmetry

- Notice that the existence of a differential symmetry for $f \circ \Pi$ implies that M_σ and Π commute.
- Thus differential symmetry implies there is a subfield $\mathbb{L}$, where $\mathbb{F}_q \subseteq \mathbb{L} \subseteq \mathbb{K}$ such that $\sigma \in \mathbb{L}$ and Π is $\mathbb{L}$-linear.
- Since $[\mathbb{L} : \mathbb{F}_q]$ divides (n, d), choosing $d = 1$ is the most efficient way to provably eliminate symmetry.

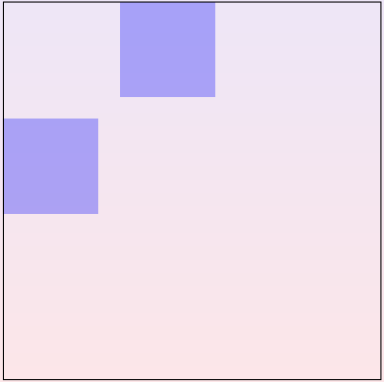
Key Choice for $d = 1$

$$\theta \in \left(2, \frac{n-1}{3}\right) \cup \left(\frac{n+1}{3}, \frac{n}{2} - 1\right) \cup \left(\frac{n}{2} + 1, \frac{2n-1}{3}\right) \cup \left(\frac{2n+1}{3}, n-2\right).$$

Q-Rank

We may consider PFLASH to have a central map of high degree but low Q-rank:

$$\mathbf{D}(f \circ \Pi) = \mathbf{\Pi}^\top \mathbf{Df}\mathbf{\Pi} =$$



Complexity of Rank Attack for PFLASH

A new version of a Q-rank attack for schemes with the minus modifier is presented in [Vates and S.T., 2017].

Complexity of Rank Attack for PFLASH

A new version of a Q-rank attack for schemes with the minus modifier is presented in [Vates and S.T., 2017].

Complexity for PFLASH(q, n, r, d)

$$\mathcal{O}\left(\binom{n+d+2}{d+r+2}^{\omega}\right),$$

where $2 \leq \omega \leq 3$ is the linear algebra constant.

Complexity of Rank Attack for PFLASH

A new version of a Q-rank attack for schemes with the minus modifier is presented in [Vates and S.T., 2017].

Complexity for PFLASH(q, n, r, d)

$$\mathcal{O}\left(\binom{n+d+2}{d+r+2}^{\omega}\right),$$

where $2 \leq \omega \leq 3$ is the linear algebra constant.

For large r, as in all proposed parameters of PFLASH, this attack is no threat.

Parameters from [Chen et al., 2015]

Our analysis supports the security claims for the following parameters from [Chen et al.,2015]:

Scheme	Public Key (Bytes)	Security (bits)
PFLASH$(16, 62, 22, 1)$	39,040	80
PFLASH$(16, 74, 22, 1)$	72,124	104
PFLASH$(16, 94, 30, 1)$	142,848	128

Table: Security levels for standard parameters of PFLASH

Conclusion

- Selecting parameters provably resistant to differential attacks does not significantly reduce the key space.

Conclusion

- Selecting parameters provably resistant to differential attacks does not significantly reduce the key space.
- Algebraically, PFLASH is a high degree HFE-.

Conclusion

- Selecting parameters provably resistant to differential attacks does not significantly reduce the key space.
- Algebraically, PFLASH is a high degree HFE-.
- For realistic parameters, the Q-rank is sufficiently high to resist all variants of the KS-attack.

And as always, thanks for watching.

Thank you for your attention.
Questions?

References:

- Chen, M.-S., Yang, B.-Y., Smith-Tone, D.: PFLASH - Secure Asymmetric Signatures on Smart Cards. Lightweight Cryptography Workshop 2015 (2015).
- Dubois, V., Fouque, P.A., Shamir, A., Stern, J.: Practical Cryptanalysis of SFLASH. CRYPTO, Vol. 4622, LNCS, Springer, (2007), 1-12.
- Smith-Tone, D.: On the Differential Security of Multivariate Public Key Cryptosystems. PQCRYPTO, Vol. 7071, LNCS, Springer, (2011), 130-142.
- Vates, J., Smith-Tone, D.: Key Recovery Attack for all Parameters of HFE-. PQCRYPTO, Vol. 10346, LNCS, Springer, (2017), xxx-yyy.