# Why you should not even think to use Ore algebras in Cryptography

Michela Ceria
joint work with T. Moriarty and A. Visconti

De Cifris, Augustae Taurinorum, 21/05/2020

# Generalized Stickel's Diffie-Hellman protocols

# Stickel

## 2005

Non-abelian finite group $G$; $P, Q \in G, PQ \neq QP$, all such data being **public**.

## Alice

Alice picks secretly a pair of integers $(P_A, Q_A)$.
Then sends Bob $A = P^{P_A} Q^{Q_A}$

## Bob

Bob chooses another pair of the same fashion $(P_B, Q_B)$.
Then sends Alice $B = P^{P_B} Q^{Q_B}$.

## Secret

$$P^{P_A} B Q^{Q_A} = P^{P_A + P_B} Q^{Q_A + Q_B} = P^{P_B} A Q^{Q_B}.$$

# What is $G$?

Stickel proposed to use the group of the invertibles matrices of order $n$ over a finite field $G := GL_n(\mathbb{F})$, but some weaknesses of this choice was discussed by Shpilrain who considered more secure working on the set $M_n(R)$ of all matrices of order $n$ over a finite ring $R$.

# Shpilrain

## Data

Finite ring $R$; $P, Q \in M_n(R), PQ \neq QP$; all these data are **public**.

## Alice

Alice picks secretly a pair of commutative polynomials
$(P_A, Q_A) \in R[X] \times R[X]$.
Then she sends Bob $A = P_A(P)Q_A(Q)$

## Bob

Bob chooses another pair of the same fashion
$(P_B, Q_B) \in R[X] \times R[X]$. Then he sends Alice $B = P_B(P)Q_B(Q)$.

## Secret

$$\begin{aligned} P_A(P)BQ_A(Q) = & P_A(P)P_B(P)Q_B(Q)Q_A(Q) = \\ & P_B(P)P_A(P)Q_A(P)Q_B(P) = P_B(P)AQ_B(Q). \end{aligned}$$

Mullan successfully mounted a linear algebra attack on it.

# Maza - Monico - Rosenthal

## Data

Finite semiring $R$ with nonempty center $C$, not embeddable into a field; $L, P, Q \in M_n(R)$; all these data are public.

## Alice

Alice picks secretly a pair of commutative polynomials $(P_A, Q_A) \in C[X] \times C[X]$; then sends Bob $A = P_A(P)LQ_A(Q)$

## Bob

Bob chooses another pair of the same fashion $(P_B, Q_B) \in C[X] \times C[X]$; then sends Alice $B = P_B(P)LQ_B(Q)$.

## Secret

$$\begin{aligned} P_A(P)BQ_A(Q) = & P_A(P)P_B(P)LQ_B(Q)Q_A(Q) = \\ & P_B(P)P_A(P)LQ_A(P)Q_B(P) = P_B(P)AQ_B(Q). \end{aligned}$$

# Cao - Dong -Wang

Diffie-Hellman-like protocol, which evaluates univariate polynomials over elements in an agreed non-commutative ring $R$.

## Alice

Alice picks $a, b \in R, m, n \in \mathbb{N}, f \in \mathbb{Z}[X]$ and sends to Bob $m, n, a, b$ and $A := f(a)^m b f(a)^n$.

## Bob

Bob chooses $h \in \mathbb{Z}[X]$ and sends Alice $A := h(a)^m b h(a)^n$.

## Secret

$$f(a)^m B f(a)^n = f(a)^m h(a)^m b h(a)^n f(a)^n = h(a)^m A h(a)^n.$$

# Now on Ore extensions

# Ore extension

$\mathbf{k} = \mathbb{F}_q$, $\theta \in Aut(\mathbf{k})$:

$$\mathbf{k}[x,\theta] := \{a_0 + a_1 x + ... + a_n x^n : \ n \in \mathbb{N}, a_i \in \mathbf{k}, \forall i \in \{0,...,n\}\}$$

**Non commutative**: $xa = \theta(a)x, \forall a \in \mathbf{k}$. *Factorization not unique.*

There are **non-central elements**, commuting together.

## Example

$\mathbf{k}[x,\theta] = \mathbb{F}_4[x,\theta] = \mathbb{F}_2[\alpha][x,\theta]$, $\theta$ the Frobenius automorphism. For $q_1 = x + \alpha$ and $q_2 = x^2 + x + \alpha$: $q_1 q_2 = q_2 q_1 = x^3 + \alpha^2 x^2 + 1$.

# First idea

Alice and Bob want to share a secret on an insecure channel via a Diffie-Hellman-like cryptosystem.

## Public data

Construct $S \subset \mathbf{k}[x, \theta]$ of **non-central** but **mutually commutative** polynomials. Take a security parameter $d$ and $Q \in \mathbf{k}[x, \theta]$ of degree $d$.

# First idea

## Alice

Takes $L_A, R_A \in S$ (degree $d$) and compute $P_A = L_A Q R_A$. Send it to Bob.

## Bob

Takes $L_B, R_B \in S$ (degree $d$) and compute $P_B = L_B Q R_B$. Send it to Alice.

## Alice

Computes $P = L_A P_B R_A$

## Bob

Computes $P = L_B P_A R_B$

## Elements in S commute!

$$P = L_A P_B R_A = L_A L_B Q R_B R_A = L_B L_A Q R_A R_B = L_B P_A R_B$$

# Cryptanalysis

Ore polynomials form a *left and right Euclidean domain*. So left and right Euclidean division is possible.
Moreover it is possible to compute **left/right GCDs**.

GCD computation allows to attack the Diffie-Hellman-like polynomial.

# Burger-Heinle: Multivariate Ore Polynomials

The context of their Diffie-Hellman-like protocol is that of multivariate Ore extensions.

For multivariate Ore extensions there is **no left or right GCD** so the attack above is not feasible.

# The protocol

Alice and Bob publicly choose a multivariate Ore extension $S$ with constant subring $R$, $L \in S$ non-central and two subsets of $C_l, C_r \subset S$ whose elements do not commute with $L$, with

$$C_l = \{f(P) : \; f = \sum_{i=0}^{m} f_i x^i \in R[x], m \in \mathbb{N}, f_0 \neq 0\}$$

$$C_r = \{f(Q) : \; f = \sum_{i=0}^{m} f_i x^i \in R[x], m \in \mathbb{N}, f_0 \neq 0\}$$

and $P, Q \in S$ non commuting with $L$.

# The protocol

**Alice**
Chooses $(P_A, Q_A) \in C_l \times C_r$

**Bob**
Chooses $(P_B, Q_B) \in C_l \times C_r$

**Alice**
Sends Bob $A = P_A L Q_A$

**Bob**
Sends Alice $B = P_B L Q_B$

# The protocol

### Alice

Computes $P_A B Q_A$

### Bob

Computes $P_B A Q_B$

### The shared secret

$$P_A B Q_A = P_A P_B L Q_B Q_A = P_B P_A L Q_A Q_B = P_B A Q_B$$

# Iterated Ore extensions with power substitutions

# Effectively given rings

Let $R$ be a (not necessarily commutative) ring with identity $\mathbf{1}_R$ and $\mathcal{A}$ another (not necessarily commutative) ring with identity $\mathbf{1}_\mathcal{A}$ which is a left module on $R$.

We can consider $\mathcal{A}$ to be **effectively given** when we are given

- sets $\overline{\mathbf{v}} := \{x_1, \dots, x_j, \dots\}$, $\overline{\mathbf{V}} := \{X_1, \dots, X_i, \dots\}$, which are *countable* and
- $\overline{\mathbf{Z}} := \overline{\mathbf{v}} \sqcup \overline{\mathbf{V}} = \{x_1, \dots, x_j, \dots, X_1, \dots, X_i, \dots\}$;
- rings $\mathcal{R} \subset \mathcal{Q}$;
- surjective maps $\pi : \mathcal{R} \twoheadrightarrow R$ and $\Pi : \mathcal{Q} \twoheadrightarrow \mathcal{A}$, with

$$\Pi(x_j) = \pi(x_j)\mathbf{1}_\mathcal{A}, \text{ for each } x_j \in \overline{\mathbf{v}},$$

so that $\Pi(\mathcal{R}) = \{r\mathbf{1}_\mathcal{A} : r \in R\} \subset \mathcal{A}$.

Thus, denoting $\mathcal{I} := \ker(\Pi) \subset \mathcal{Q}$ and $I := \mathcal{I} \cap \mathcal{R} = \ker(\pi) \subset \mathcal{R}$, we have $\mathcal{A} = \mathcal{Q}/\mathcal{I}$ and $R = \mathcal{R}/I$; moreover we can assume, without loss of generality, that $R \subset \mathcal{A}$. Further, when considering $\mathcal{A}$ as effectively given in this way, we explicitly require the Ore-like requirement that $\forall X_i \in \overline{\mathbf{V}}, x_j \in \overline{\mathbf{v}}$,

$$X_i x_j \equiv \sum_{l=1}^{i} \pi(a_{lij}) X_l + \pi(a_{0ij}) \bmod \mathcal{I}, a_{lij} \in \mathbb{Z}\langle \overline{\mathbf{v}} \rangle,$$

If not, $\mathbb{Z}\langle x, y\rangle$ **as left $\mathbb{Z}[x]$-module** requires

$$X_i := x^i y \quad \mathbb{Z}\langle x, y\rangle \cong \mathbb{Z}[x]\langle X_0, X_1, \ldots, X_i, \ldots\rangle / \mathbb{I}\,(X_i x - X_{i+1})$$

$$X_0 > X_1 > X_2 > \cdots X_i > X_{i+1} \cdots$$

If we fix

- a term-ordering $<$ on $\langle\overline{\mathbf{Z}}\rangle$

we can assume $\mathcal{I}$ to be given via

- its bilateral Gröbner basis $G$ w.r.t. $<$

and, if $<$ satisfies $X_i > t$ for each $t \in \langle\overline{\mathbf{v}}\rangle$ and $X_i \in \overline{\mathbf{V}}$, also $I$ is given via

- its bilateral Gröbner basis $G_0 := G \cap \mathcal{R}$ w.r.t. $<$.

For each $X_i \in \overline{\mathbf{V}}, x_j \in \overline{\mathbf{v}}$, $f_{ij} := X_i x_j - \sum_{l=1}^{i} a_{lij} X_l - a_{0ij} \in \mathcal{I} \subset \mathcal{Q}$.
If we further require that $<$ satisfies

$$X_i x_j = \mathbf{T}(f_{ij}) \text{ for each } X_i \in \overline{\mathbf{V}}, x_j \in \overline{\mathbf{v}},$$

and denote $C := \{f_{ij} : X_i \in \overline{\mathbf{V}}, x_j \in \overline{\mathbf{v}}\}$ we have

- $G_0 \sqcup C \subset G$,
- $\mathcal{A}$ is generated as $R$-module by $\Pi(\langle\overline{\mathbf{V}}\rangle)$ and,
- as $\mathbb{Z}$-module, by a subset of $\left\{\upsilon\omega : \upsilon \in \langle\overline{\mathbf{v}}\rangle, \omega \in \langle\overline{\mathbf{V}}\rangle\right\}$.

# Szekeres notation

We further denote

- for $m \in \mathbb{N}$, $\langle \overline{\mathbf{Z}} \rangle^{(m)} := \{t\mathbf{e}_i : t \in \langle \overline{\mathbf{Z}} \rangle, 1 \leq i \leq m\}$.
- for each $\omega \in \langle \overline{\mathbf{V}} \rangle$,

$$\mathcal{I}_\omega := \{r \in \mathcal{R} : \textbf{ exists } h \in \mathcal{Q}, \mathbf{T}(h) < \omega, r\omega + h \in \mathcal{I}\} \supset I = \mathcal{I} \cap \mathcal{R}$$

- $R_\omega = \mathcal{R}/\mathcal{I}_\omega$;
- $\mathbf{L}(\mathcal{I}) := \{\omega \in \langle \overline{\mathbf{V}} \rangle : \mathcal{I}_\omega = R\}$,
- $\mathcal{B} = \langle \overline{\mathbf{V}} \rangle \setminus \mathbf{L}(\mathcal{I}) \subset \langle \overline{\mathbf{V}} \rangle$,

W.r.t. a term-ordering $<$ on $\mathcal{B}$ satisfiying the conditions above and a well-ordering on $\mathcal{B}^m$ (which we will still denote $<$), satisfying

$$\omega_1 < \omega_2 \implies \omega_1 t < \omega_2 t, t\omega_1 < t\omega_2 \forall t \in \mathcal{B}^{(m)}, \omega_1, \omega_2 \in \mathcal{B}.$$

each non-zero element $f \in \mathcal{A}^m$ has its canonical representation

$$f := \sum_{j=1}^{s} c(f, t_j \mathbf{e}_{\iota_j}) t_j \mathbf{e}_{\iota_j},$$

$t_j \in \mathcal{B}, c(f, t_j \mathbf{e}_{\iota_j}) \in R_{t_j} \setminus \{0\}, 1 \leq \iota_j \leq m$, with
$t_1 \mathbf{e}_{\iota_1} > t_2 \mathbf{e}_{\iota_2} > \cdots > t_s \mathbf{e}_{\iota_s}$ and we denote,
$\mathrm{Supp}(f) := \{t_j \mathbf{e}_{\iota_j} : 1 \leq j \leq m\}$ the *support* of $f$, $\mathbf{T}_<(f) := t_1 \mathbf{e}_{\iota_1}$ its *maximal term*, $\mathrm{lc}_<(f) := c(f, t_1 \mathbf{e}_{\iota_1})$ its *leading coefficient* and $\mathbf{M}_<(f) := c(f, t_1 \mathbf{e}_{\iota_1}) t_1 \mathbf{e}_{\iota_1}$ its *maximal monomial*.

If we denote $\mathsf{M}(\mathcal{A}^m) := \{ct\mathbf{e}_i \mid t \in \mathcal{B}, c \in R_t \setminus \{0\}, 1 \leq i \leq m\}$, the unique finite representation can be reformulated

$$f = \sum_{\tau \in \mathrm{Supp}(f)} m_\tau,\ m_\tau = c(f,\tau)\tau$$

as a sum of elements of the *monomial set* $\mathsf{M}(\mathcal{A}^m)$.

# Specializing

- $\overline{\mathbf{X}} := \{X_1, \ldots, X_n\}$, $\overline{\mathbf{Y}} := \{Y_1, \ldots, Y_m\}$, $\overline{\mathbf{V}} := \overline{\mathbf{X}} \sqcup \overline{\mathbf{Y}}$,$\langle\overline{\mathbf{V}}\rangle$ the set of all words on the alphabet $\overline{\mathbf{V}}$,
- $\mathcal{Q} := R\langle\overline{\mathbf{V}}\rangle$;
- $\Gamma := \{X_1^{d_1} \cdots X_n^{d_n} Y_1^{e_1} \cdots Y_m^{e_m} \mid (d_1, \ldots, d_n, e_1, \ldots, e_m) \in \mathbb{N}^{n+m}\}$,
- $\mathcal{T} := \{X_1^{d_1} \cdots X_n^{d_n} \mid (d_1, \ldots, d_n) \in \mathbb{N}^n\}$,
- $\mathcal{T}_j := \{X_1^{d_1} \cdots X_j^{d_j} \mid (d_1, \ldots, d_j) \in \mathbb{N}^j\} \subset \mathcal{T}$ for each $j : 1 \le j \le n$,
- $\mathcal{V} := \{Y_1^{e_1} \cdots Y_m^{e_m} \mid (e_1, \ldots, e_m) \in \mathbb{N}^m\}$,
- the lexicographical (*id est* alphabetical) ordering $<$ on $\langle\overline{\mathbf{V}}\rangle$, induced by $X_1 < \ldots < X_n < Y_1 < \ldots < Y_m$, and its restriction, still denoted $<$, on the (commutative) terms $\mathcal{T}$;

# Specializing

- for each $i, j : 1 \leq i < j \leq n$, $f_{ij} := X_j X_i - c_{ij} X_i X_j - d_{ij}$, $c_{ij}$ an invertible element in $R$, $d_{ij} \in R[\mathcal{T}_{j-1}]$,
- for each $j, l : 1 \leq j \leq n, 1 \leq l \leq m$, $f_{jl} := Y_l X_j - c_{jl} \upsilon_{jl} X_j Y_l - d_{jl}$, $c_{jl}$ an invertible element in $R$, $\upsilon_{jl} \in \mathcal{T}_j$, $d_{ij} \in R[\mathcal{T}][\mathcal{V}_{l-1}]$,
- for each $l, k : 1 \leq l < k \leq m$, $f_{lk} := Y_k Y_l - c_{lk} Y_l Y_k - d_{lk}$, $c_{lk}$ an invertible element in $R$, $d_{lk} \in R[\mathcal{V}_{k-1}]$;
- the binary operation $\circ$ on $\Gamma$ defined by

$$\begin{cases} X_j \circ X_i & = & X_i X_j & \text{for each } i, j : 1 \leq i < j \leq n, \\ Y_l \circ X_j & = & \upsilon_{jl} X_j Y_l & \text{for each } j : 1 \leq j \leq n, l : 1 \leq l \leq m, \\ Y_k \circ Y_l & = & Y_l Y_k & \text{for each } l, k : 1 \leq l < k \leq m; \end{cases}$$

- $C^L := \{f_{ij}, 1 \leq i < j \leq n\}, C^R := \{f_{lk}, 1 \leq l < k \leq m\}$,
- $C := C^L \cup \{f_{jl}, 1 \leq j \leq n, 1 \leq l \leq m\} \cup C^R$;
- $\mathcal{A} := R\langle \overline{\mathbf{V}} \rangle / \mathbb{I}_2(C)$: **iterated Ore extensions with power substitutions.**

Denote, for the semigroup $(\Gamma, \circ)$, $\Gamma^{(u)}$ the sets

$$\Gamma^{(u)} := \{\gamma e_i, \gamma \in \Gamma, 1 \le i \le u\}, u \in \mathbb{N},$$

endowed with no operation except the natural action of $\Gamma$

$$\Gamma \times \Gamma^{(u)} \times \Gamma \to \Gamma^{(u)} : (\delta_l, \gamma, \delta_r) \mapsto \delta_l \circ \gamma \circ \delta_r, \forall \delta_l, \delta_r \in \Gamma, \gamma \in \Gamma^{(u)}.$$

Given a $\Gamma$-pseudovaluation

$$\mathbf{T}(\cdot) : \mathcal{A} \setminus \{0\} \mapsto \mathcal{B} \subset \Gamma : f \to \mathbf{T}(f),$$

a module $M \subset \mathcal{A}^u$ and the $\Gamma^{(u)}$-pseudovaluation

$$\mathbf{T}(\cdot) : M \setminus \{0\} \mapsto \mathcal{B}^{(u)} \subset \Gamma^{(u)} : f \to \mathbf{T}(f),$$

and we define

- $F_\gamma(M) := \{f \in M : \mathbf{T}(f) \le \gamma\} \cup \{0\} \subset M$, for each $\gamma \in \Gamma^{(u)}$;
- $V_\gamma(M) := \{f \in M : \mathbf{T}(f) < \gamma\} \cup \{0\} \subset M$, for each $\gamma \in \Gamma^{(u)}$;
- $G_\gamma(M) := F_\gamma(M)/V_\gamma(M)$, for each $\gamma \in \Gamma^{(u)}$;
- $G(M) := \bigoplus_{\gamma \in \Gamma^{(u)}} G_\gamma(M)$.
- $\mathcal{L} : M \mapsto G(M)$ map s.t. $\mathcal{L}(0) = 0$ and, for each $f \in M, f \neq 0, t := \mathbf{T}(f), \mathcal{L}(f)$ class of $f$ mod $V_t(M)$.

# Associated graded rings and modules

We call

- *associated graded ring* of $\mathcal{A}$ the left $R$-module $G(\mathcal{A})$ which is a $\Gamma$-graded ring, and
- *associated graded module* of $M$ the left $R$-module $G(M)$, which is a $\Gamma^{(u)}$-graded $G(\mathcal{A})$-module. $\square$

# Spear's Theorem

$\mathcal{B} := \{\omega \in \langle \overline{\mathbf{V}} \rangle : \mathcal{I}_\omega \neq R\} \subset \left\{ \upsilon\omega : \upsilon \in \langle \overline{\mathbf{v}} \rangle, \omega \in \langle \overline{\mathbf{V}} \rangle \right\}$
Spear's intuition that a Buchberger Theory defined in a ring can be exported to its quotients allow us to impose on $\mathcal{A}$ the "natural" $\Gamma$-valuation/filtration

$$\mathbf{T}(\cdot) : \mathcal{A}^m \mapsto \mathcal{B}^{(m)} : f \to \mathbf{T}(f)$$

where $(\Gamma, \circ)$, $\mathcal{B} \subset \Gamma \subset \langle \overline{\mathbf{V}} \rangle$, is a suitable semigroup.

# Spear's Theorem

$$\mathcal{B} := \{\omega \in \langle \overline{\mathbf{V}} \rangle : \mathcal{I}_\omega \neq R\} \subset \left\{ \upsilon\omega : \upsilon \in \langle \overline{\mathbf{v}} \rangle, \omega \in \langle \overline{\mathbf{V}} \rangle \right\}$$

$$\mathbf{T}(\cdot) : \mathcal{A}^m \mapsto \mathcal{B}^{(m)} : f \to \mathbf{T}(f)$$

$$(\Gamma, \circ), \mathcal{B} \subset \Gamma \subset \langle \overline{\mathbf{V}} \rangle,$$

# Spear's Theorem

$$\mathcal{B} := \{\omega \in \langle\overline{\mathbf{V}}\rangle : \mathcal{I}_\omega \neq R\} \subset \left\{ \upsilon\omega : \upsilon \in \langle\overline{\mathbf{v}}\rangle, \omega \in \langle\overline{\mathbf{V}}\rangle \right\}$$

$$\mathbf{T}(\cdot) : \mathcal{A}^m \mapsto \mathcal{B}^{(m)} : f \to \mathbf{T}(f)$$

$$(\Gamma, \circ), \mathcal{B} \subset \Gamma \subset \langle\overline{\mathbf{V}}\rangle,$$

The associated $\Gamma$-graded ring $\mathcal{G} = G(\mathcal{A})$ coincides as a **set** with $\mathcal{A}$ and this is sufficient to smoothly export Buchberger test/completion but they don't coincide as **rings**:
the multiplication $\star$ of $\mathcal{A}$ does not coincide with the one, $*$, of $\mathcal{G}$

# Spear's Theorem

$$\mathcal{B} := \{\omega \in \langle \overline{\mathbf{V}} \rangle : \mathcal{I}_\omega \neq R\} \subset \left\{ \upsilon\omega : \upsilon \in \langle \overline{\mathbf{v}} \rangle, \omega \in \langle \overline{\mathbf{V}} \rangle \right\}$$

$$\mathbf{T}(\cdot) : \mathcal{A}^m \mapsto \mathcal{B}^{(m)} : f \to \mathbf{T}(f)$$

$$(\Gamma, \circ), \mathcal{B} \subset \Gamma \subset \langle \overline{\mathbf{V}} \rangle,$$

The associated $\Gamma$-graded ring $\mathcal{G} = G(\mathcal{A})$ coincides as a **set** with $\mathcal{A}$ and this is sufficient to smoothly export Buchberger test/completion but they don't coincide as **rings**:
the multiplication $\star$ of $\mathcal{A}$ does not coincide with the one, $*$, of $\mathcal{G}$
For instance, if we consider the Weyl algebra,

$$\mathcal{A} = \mathbb{Q}\langle D, X \rangle / \mathbb{I}(DX - XD - 1)$$

where

$$\mathcal{G} = \mathbb{Q}[D, X], D \star X = XD - 1, D * X = XD.$$

# Spear's Theorem

$$\mathcal{B} := \{\omega \in \langle\overline{\mathbf{V}}\rangle : \mathcal{I}_\omega \neq R\} \subset \left\{\upsilon\omega : \upsilon \in \langle\overline{\mathbf{v}}\rangle, \omega \in \langle\overline{\mathbf{V}}\rangle\right\}$$

$$\mathbf{T}(\cdot) : \mathcal{A}^m \mapsto \mathcal{B}^{(m)} : f \to \mathbf{T}(f)$$

$$(\Gamma, \circ), \mathcal{B} \subset \Gamma \subset \langle\overline{\mathbf{V}}\rangle,$$

The associated $\Gamma$-graded ring $\mathcal{G} = G(\mathcal{A})$ coincides as a **set** with $\mathcal{A}$ and this is sufficient to smoothly export Buchberger test/completion but they don't coincide as **rings**:
the multiplication $\star$ of $\mathcal{A}$ does not coincide with the one, $*$, of $\mathcal{G}$
However an old slogan stated that in order to provide a Buchberger Algorithm on $\mathcal{A}$, one just needs to modify, in the algorithm for $\mathcal{G}$, the multiplication procedure!

$\mathcal{A} = \mathcal{Q}/\mathcal{I}$ is an effectively given left $R$-module, endowed with its natural $\Gamma$-pseudovaluation $\mathbf{T}(\cdot)$ where the semigroup $(\Gamma, \circ)$ satisfies

- $\mathcal{B} \subset \Gamma \subset \langle \overline{\mathbf{V}} \rangle$ and
- the restriction of $<$ on $\Gamma$ is a semigroup ordering.

We denote $\mathcal{G} = G(\mathcal{A})$, $\star$ the multiplication of $\mathcal{A}$, $*$ the one of $\mathcal{G}$.

# Arithmetics of $\mathcal{A}$ and $G(\mathcal{A})$

Denote $\mathcal{G} = G(\mathcal{A})$, $\star$ the multiplication of $\mathcal{A}$, $*$ the one of $\mathcal{G}$.

1. For each term $\tau \in \mathcal{B} \subset \Gamma$ there are an automorphism $\alpha_\tau : R \to R$ and an $\alpha_\tau$-derivation $\theta_\tau : R \to R$ so that for each $r \in R$, $t \star r = \alpha_t(r)t + \theta_t(r)$ and $t * r = \alpha_t(r)t$.
2. For two terms $\tau_1, \tau_2 \in \mathcal{B} \subset \Gamma$, there are elements $\varpi(\tau_2, \tau_1) \in R$ and $\Delta(\tau_2, \tau_1) \in \mathcal{A}, \mathbf{T}(\Delta(\tau_2, \tau_1)) < \tau_2 \circ \tau_1$ such that $\tau_2 \star \tau_1 = \varpi(\tau_2, \tau_1)\tau_2 \circ \tau_1 + \Delta(\tau_2, \tau_1)$ and $\tau_2 * \tau_1 = \mathcal{L}(\tau_2 \star \tau_1) = \varpi(\tau_2, \tau_1)\tau_2 \circ \tau_1$.
3. $c_u\tau_u * c_v\tau_v = c_u\alpha_{\tau_u}(c_v)\varpi(\tau_u, \tau_v)\tau_u \circ \tau_v$.

# Arithmetics of $\mathcal{A}$ and $G(\mathcal{A})$

## Pesch, Nguefack–Pola

$$\mathcal{A} = \mathcal{R}\langle X_1, \ldots, X_n, Y_1, \ldots, Y_m\rangle/\mathcal{I}$$

$$X_j * X_i = a_{ij} X_i X_j, \quad Y_l * X_j = b_{jl} X_j^{e_i - 1} X_j Y_l, Y_k * Y_l = c_{lk} Y_l Y_k$$

where $a_{ij}, b_{jl}, c_{lk}$ are invertible elements in $\mathcal{R}$, $e_i \in \mathbb{N}^*$.

3. $c_u\tau_u * c_v\tau_v = c_u\alpha_{\tau_u}(c_v)\varpi(\tau_u, \tau_v)\tau_u \circ \tau_v$.
4. $\alpha_{\tau_u} = \mathrm{Id}$
5. $\tau_u \circ \tau_v = \Upsilon(\tau_u, \tau_v)\tau_u\tau_v, \Upsilon(\tau_u, \tau_v) \in \{X_1^{d_1} \cdots X_n^{d_n} \mid (d_1, \ldots, d_n) \in \mathbb{N}^n\}$;
6. $c_u\tau_u * c_v\tau_v = c_u\alpha_{\tau_u}(c_v)\varpi(\tau_u, \tau_v)\Upsilon(\tau_u, \tau_v)\tau_u\tau_v = \varpi(\tau_u, \tau_v)\Upsilon(\tau_u, \tau_v) \cdot c_u\tau_u \cdot c_v\tau_v$.

# Reduction

For our attack we do not need Buchberger Theory at all, except for the notion of **normal form** and **Buchberger reduction** within a principal ideal $\mathbb{I}(p) \subset \mathcal{A}$, $p \in \mathcal{A} \setminus \{0\}$, $\mathcal{A}$ being an iterated Ore extensions with power substitutions.

For $f \in \mathcal{A}^m \setminus \{0\}, \mathbb{I}(p) \subset \mathcal{A}^m$, an element $g := \mathrm{Nf}(f, F) \in \mathcal{A}^m$ is called a *twosided normal form* of $f$ w.r.t. $\mathbb{I}(p)$, if

- $g \neq 0 \implies \mathbf{M}(p) \nmid \mathbf{M}(g)$,
- there is a representation $f - g = \sum_{i=1}^{\mu} a_i \lambda_i \star p \star b_i \rho_i$, with $\lambda_i, \rho_i \in \mathcal{B}, a_i \in R_{\lambda_i} \setminus \{0\}, b_i \in R_{\rho_i} \setminus \{0\}$ and $\mathbf{T}(f) = \lambda_1 \circ \mathbf{T}(p) \circ \rho_1 > \ldots > \lambda_i \circ \mathbf{T}(p) \circ \rho_i > \lambda_{i+1} \circ \mathbf{T}(p) \circ \rho_{i+1} > \ldots > \mathbf{T}(g)$.

# Attacking

# The attack

We attack the Diffie-Hellman-like protocol by means of ...

## Ingredients

- Buchberger **reduction**
- left/right **divisibility**

# Recalling the setting

Alice and Bob publicly choose a multivariate Ore extension $S$ with constant subring $R$, $L \in S$ non-central and two subsets of $C_l, C_r \subset S$ whose elements do not commute with $L$, with

$$C_l = \{f(P): \ f = \sum_{i=0}^{m} f_i x^i \in R[x], m \in \mathbb{N}, f_0 \neq 0\}$$

$$C_r = \{f(Q): \ f = \sum_{i=0}^{m} f_i x^i \in R[x], m \in \mathbb{N}, f_0 \neq 0\}$$

and $P, Q \in S$ non commuting with $L$.

# The attack

## Known

The polynomials $P, Q, L \in S$ ($P, Q$ non commuting with $L$) are **publicly known**.

## Unknown

The polynomials $f, g \in R[t]$ are **kept secret**.

Alice sends $f(P)Lg(Q)$.

## The attack

Let $g(t) = \sum_{i=a}^{d} c_i t^i$, $a \leq d$, $c_a \neq 0$, so $g(Q) = \sum_{i=a}^{d} c_i Q^i$.

### Reduction

$$\mathsf{T}(Q) \to \mathbf{tail}(Q) + R$$

where $R$ is a new variable.

# The attack

## After reduction you get

$$f(P)L\sum_{i=a}^{d} c_i Q^i \rightarrow f(P)L\sum_{i=a+1}^{d} c_i Q^{i-a-1} R \cdot R^a + f(P)Lc_a R^a =$$

$$= XR \cdot R^a + YR^a$$

When $Y := f(P)Lc_a$ and $X := f(P)L\sum_{i=a+1}^{d} c_i Q^{i-a-1}$

- dividing $Y$ by $L$ from the right it is possible to find $f(P)$ and $f$ can be retrieved by reducing w.r.t. $P$;
- dividing $X$ by $Y$ from the left we get $\sum_{i=a+1}^{d} c_i Q^{i-a-1}$

# The attack

From $L\sum_{i=a+1}^{d} c_i Q^{i-a-1}$ we can find $g$ by reduction

$$\sum_{i=a+1}^{d} c_i Q^{i-a-1} \to \sum_{i=a+1}^{d} c_i R^{i-a-1}$$

## One problem left...

How can I be sure that I am in the case $Y := f(P)Lc_a$ and $X := f(P)L\sum_{i=a+1}^{d} c_i Q^{i-a-1}$?

## The attack

How can I be sure that I am in the case $Y := f(P)Lc_a$ and $X := f(P)L\sum_{i=a+1}^{d} c_i Q^{i-a-1}$?

Everything depends on the **test**: *is it true that*

$$Y \mid_L X?$$

### If not

I keep on reducing.

### But if the answer is positive

it means that we have reached the case $Y := f(P)Lc_a$ and $X := f(P)L\sum_{i=a+1}^{d} c_i Q^{i-a-1}$.

# Three-pass exchange protocol

Alice and Bob choose a public multivariate Ore extension $S$ and they choose $P, Q \in S$ (non commuting).

Alice chooses a secret $L \in S$ (non commuting with $P$ and $Q$) to share with Bob and also $f_A, g_A \in R[x]$. $P_A = f_A(P)$ and $Q_A = g_A(Q)$ are private and non-commuting with $L$. Bob does the same getting $P_B, Q_B$.

- A computes and sends Bob $P_A L Q_A$
- B computes and sends Alice $P_B P_A L Q_A Q_B = P_A P_B L Q_B Q_A$
- A divides by left for $P_A$ and by right for $Q_A$ and sends $P_B L Q_B$ to Bob
- B divides by left for $P_B$ and by right for $Q_B$ and gets $L$.

# What is the main difference?

- A computes and sends Bob $P_A L Q_A$
- B computes and sends Alice $P_B P_A L Q_A Q_B = P_A P_B L Q_B Q_A$
- A divides by left for $P_A$ and by right for $Q_A$ and sends $P_B L Q_B$ to Bob
- B divides by left for $P_B$ and by right for $Q_B$ and gets $L$.

An attacker **cannot know** $L$ and he actually has to break the protocol to get back $L$.

# The attack

It is more or less the same but we have lost one condition: we cannot make the division by $L$.

We can verify $Y \mid_L X$ but we cannot verify if $L \mid Y$ from right.

# The attack

Using reduction from right as before we get $f(P)L$ **and** $g(Q)$.
Reducing then from left we get $f(P)$ **and** $Lg(Q)$.

*What if I reduce too much or too less?*

# Too less

Suppose I have reduced by $Q$ from the right and I have found $f(P)Lh(Q)$ and $k(Q)$ instead of $f(P)L$ and $g(Q)$ with $g(Q) = h(Q)k(Q)$.
This may happen from right and from left contemporarily so I may get $a(P)b(P)Lc(Q), d(Q)$, $a(P), b(P)Lc(Q)d(Q)$ where $f(P) = a(P)b(P)$ $g(Q) = c(Q)d(Q)$.
Therefore I would believe that $b(P)Lc(Q)$ is my $L$ but it is wrong.

Anyway reducing again by $P$ on the left and $Q$ on the right we will get a remainder. The part containing only remainders is $L$ up to constants.

$$b(P)Lc(Q) = Pb'(P)Lc(Q) + b(0)Lc(Q) =$$

$$Pb'(P)Lc'(Q)Q + Pb'(P)Lc(0) + b(0)Lc'(Q)Q + \mathbf{b(0)Lc(0)}$$

# Too much

## Let us see the $P$ part

Suppose $L = P^i C$. Once performing our attack we are forced to reduce by $P$ on the left until it is not possible to reduce anymore. Therefore we would recover $C$ instead of $L$.

Anyway three public data are available and from them we would find the pairs:

- $(P^{a+i}, C)$ (coming from $P_A L$ after left reduction)
- $(P^{a+b+i}, C)$ (coming from $P_B P_A L$ after left reduction)
- $(P^{b+i}, C)$ (coming from $P_B L$ after left reduction)

Knowing $a+i$ $b+i$ and $a+b+i$ we can recover $i$.

**Thank you**
**for your attention!**