Gröbner Basis Cryptosystems

§ 1 Gröbner Bases in Free Associative Algebras

K (commutative) field

$\Sigma = \{x_1, \ldots, x_n\}$ finite alphabet

Σ^* set of terms (or words) over Σ

A term w is of the form $w = x_{i_1} x_{i_2} \cdots x_{i_s}$

$K[\Sigma^*]$ free associative K-algebra

$f \in K[\Sigma^*]$ is of the form $f = a_1 w_1 + \cdots + a_r w_r$ with $a_i \in K$ and $w_i \in \Sigma^*$

Definition. A **term ordering** on Σ^* is a well-ordering σ such that

1) $w_1 \geq_\sigma w_2 \quad \Rightarrow \quad w_3 w_1 w_4 \geq_\sigma w_3 w_2 w_4$

2) $w_1 w_2 w_3 \geq_\sigma w_2$

Examples. a) $\sigma =$ `llex` length-lexicographic ordering

b) $\sigma =$ `tlex` total lexicographic ordering

Definition. a) For $f = a_1 w_1 + \cdots + a_r w_r \in K[\Sigma^*] \setminus \{0\}$, the **leading term** of f is $\mathrm{LT}_\sigma(f) = \max_\sigma \{w_i\}$.

b) For a right-ideal $I \subseteq K[\Sigma^*]$, the **leading term ideal** of I is

$$\mathrm{LT}_\sigma(I) = \langle \mathrm{LT}_\sigma(f) \mid f \in I \setminus \{0\} \rangle$$

and the **right leading term ideal** of I is

$$\mathrm{LT}_\sigma^r(I) = \langle \mathrm{LT}_\sigma(f) \mid f \in I \setminus \{0\} \rangle_r$$

c) A subset $G \subseteq I$ is called a **σ-Gröbner basis** of I if $\mathrm{LT}_\sigma(I) = \langle \mathrm{LT}_\sigma(g) \mid g \in G \rangle$. It is called a **right σ-Gröbner basis** of I if $\mathrm{LT}_\sigma^r(I) = \langle \mathrm{LT}_\sigma(g) \mid g \in G \rangle_r$.

Questions: 1) Do Gröbner bases exist?

2) Can they be computed?

3) What are they good for?

Definition. Let $I \subseteq K[\Sigma^*]$ be a right ideal and $G \subseteq I$.

a) The **rewrite rule** $\xrightarrow{G}$ defined by G is the reflexive, transitive closure of all $\xrightarrow{g}$ with $g \in G$, where $f \xrightarrow{g} h$ means that there is a term $w \in \mathrm{Supp}\,(f)$ such that $w = \mathrm{LT}_\sigma(g)w'$ and $h = f - cgw'$ with $c \in K$ such that $w \notin \mathrm{Supp}\,(h)$.

b) The rewrite rule $\xrightarrow{G}$ is called **Noetherian** if every chain $f_1 \xrightarrow{g_1} f_2 \xrightarrow{g_2} \cdots$ with $g_1, g_2, \ldots, \in G$ becomes eventually stationary.

c) The rewrite rule $\xrightarrow{G}$ is called **confluent** if $f_1 \xrightarrow{G} f_2$ and $f_1 \xrightarrow{G} f_3$ implies that there exists f_4 such that $f_2 \xrightarrow{G} f_4$ and $f_3 \xrightarrow{G} f_4$.

Proposition 1.1. Let $I \subseteq K[\Sigma^*]$ be a right ideal and $G \subseteq I$.
a) The rewrite rule $\xrightarrow{G}$ is Noetherian.
b) G is a right σ-Gröbner basis of I iff $\xrightarrow{G}$ is confluent.
c) If $\xrightarrow{G}$ is confluent, every element $f \in K[\Sigma^*]$ has a unique **normal form** $\mathrm{NF}_{\sigma,I}(f)$ such that $f \xrightarrow{G} \mathrm{NF}_{\sigma,I}(f)$ and such that $\mathrm{NF}_{\sigma,I}(f)$ cannot be reduced further.

Definition. Given $f_1, f_2 \in K[\Sigma^*]$ and $w_1, w_2 \in \Sigma^*$ such that
1) $\mathrm{LT}_\sigma(f_1)w_1 = w_2\,\mathrm{LT}_\sigma(f_2)$,
2) w_1 is not a multiple of $\mathrm{LT}_\sigma(f_2)$ and w_2 is not a multiple of $\mathrm{LT}_\sigma(f_1)$,
we call $S(f_1, f_2, w_1, w_2) = \frac{1}{\mathrm{LC}_\sigma(f_1)}\, f_1 w_1 - \frac{1}{\mathrm{LC}_\sigma(f_2)}\, w_2 f_2$ the **S-polynomial** of f_1 and f_2.

Theorem 1.2. (Buchberger Criterion)
Let $I \subseteq K[\Sigma^*]$ be a two-sided ideal and $G \subseteq I$ an LT-reduced subset. Then G is a σ-Gröbner basis of I if and only if $S(g_1, g_2, w_1, w_2) \xrightarrow{G} 0$ for all S-polynomials of elements $g_1, g_2 \in G$.

Theorem 1.3. (Buchberger's Algorithm)
Let $I = \langle f_1, \dots, f_s \rangle$ be a two-sided ideal in $K[\Sigma^*]$. Consider the following instructions.

1) Start with $G = \{g_1, \dots, g_s\}$, where $g_i = f_i$, and let B be the set of all S-polynomials involving elements of G.
2) If $B = \emptyset$, return G and stop. Otherwise, choose $S = S(g_i, g_j, w_i, w_j) \in B$ and remove it from B.
3) Compute $S' = \mathrm{NR}_{\sigma,G}(S)$. If $S' = 0$, continue with step 2).
4) Append S' to G and all S-polynomials involving S' and previous elements of G to B. Continue with step 2).

This is a procedure such that $G = \{g_1, g_2, \dots\}$ is a σ-Gröbner basis of I. If the procedure stops, the resulting set G is a finite σ-Gröbner basis of I.

Remarks. a) A finite σ-Gröbner basis of I need not exist.
b) If I has a finite Gröbner basis, we can effectively compute in the residue class ring $K[\Sigma]/I$.
c) If I is a finitely generated right ideal, it has a finite right σ-Gröbner basis which can be computed in finitely many steps.

§ 2. Gröbner Bases for Monoid Rings

M finitely presented monoid, i.e. $M = \Sigma^*/\sim_R$, where

Σ^* is the monoid of all terms in the alphabet Σ

$\sim_R$ is the congruence relation on Σ^* generated by finitely many relations $w_1 \sim w_1', \ldots, w_r \sim w_r'$.

$I_M = \langle w_1 - w_1', \ldots, w_r - w_r' \rangle \subseteq K[\Sigma^*]$

$K[M] = K[\Sigma^*]/I_M$ monoid ring

We assume that I_M has a finite Gröbner basis, i.e. that we can effectively compute in $K[M]$.

Many computational problems for monoids and groups can be treated using Gröbner bases.

Proposition 2.1. (The Word Problem for Monoids)

For $w_1, w_2 \in \Sigma^*$, the following conditions are equivalent:

1) $\bar{w}_1 = \bar{w}_2$ in M

2) $w_1 - w_2 \in I_M$ ("ideal membership")

Proposition 2.2. (The Generalized Word Problem for Monoids)

Let $S \subseteq M$, and let $\langle S \rangle$ be the submonoid of M generated by S. For $w \in \Sigma^*$, the following conditions are equivalent:

1) $\bar{w} \in \langle S \rangle$

2) $\bar{w}-1 \in K[s-1 \mid s \in S] \subseteq K[M]$ ("subalgebra membership")

Prop. 2.3. (Generalized Word Problem for Groups)

Let M be a group, $S \subseteq M$ a finite subset, and $U = \langle S \rangle$ the subgroup of M generated by S. For $\bar{w} \in K[M]$, the following conditions are equivalent:

1) $\bar{w} \in U$

2) $\bar{w} - 1 \in \langle s - 1 \mid s \in S \rangle_r \subseteq K[M]$ ("right ideal membership")

Definition. Let $\bar{f}_1, \ldots, \bar{f}_s \in K[M]$.

a) The right $K[M]$-submodule $\mathrm{Syz}^r_{K[M]}(\bar{f}_1, \ldots, \bar{f}_s) = \{(\bar{g}_1, \ldots, \bar{g}_s) \in K[M]^s \mid \bar{f}_1\bar{g}_1 + \cdots + \bar{f}_s\bar{g}_s = 0\}$ of $K[M]^s$ is called the **right syzygy module** of $(\bar{f}_1, \ldots, \bar{f}_s)$.

b) The right $K[M]$-module $\mathrm{Syz}_{K[M]}(\bar{f}_1, \ldots, \bar{f}_s) = \{(\bar{g}_1, \ldots, \bar{g}_s, \bar{h}_1, \ldots, \bar{h}_s) \in (K[M]^{\mathrm{op}})^s \oplus K[M]^s \mid \bar{g}_1\bar{f}_1\bar{h}_1 + \cdots + \bar{g}_s\bar{f}_s\bar{h}_s = 0\}$ is called the **(two-sided) syzygy module** of $(\bar{f}_1, \ldots, \bar{f}_s)$.

Prop. 2.4. (The Conjugation and the Conjugator Search Problem for Groups)

Let M be a group. For $\bar{w}_1, \bar{w}_2 \in M$, the following conditions are equivalent:

1) $\bar{w}_1 = \bar{w}_3\, \bar{w}_2\, \bar{w}_3^{-1}$ for some $\bar{w}_3 \in M$

2) $\mathrm{Syz}_{K[M]}(\bar{w}_1, \bar{w}_2) \cap \{(e, -\bar{w}, \bar{w}, e) \mid \bar{w} \in M\} \neq \emptyset$

Proof: $\bar{w}_1 = \bar{w}_3\, \bar{w}_2\, \bar{w}_3^{-1} \iff e \cdot \bar{w}_1 \cdot \bar{w}_3 - \bar{w}_3 \cdot \bar{w}_2 \cdot e = 0$ $\square$

§ 3. Gröbner Bases for Right Modules

$F = \bigoplus_{\lambda\in\Lambda} K[\Sigma^*]$ free $K[\Sigma^*]$-module

$\{e_\lambda \mid \lambda \in \Lambda\}$ canonical basis of F

$U \subseteq F$ right submodule

Definition. a) A **term** in F is an element of the form $e_\lambda w$ with $\lambda \in \Lambda$ and $w \in \Sigma^*$.

b) A **module term ordering** τ is a well-ordering on the set of terms in F such that

1) $e_\lambda w_1 \leq_\tau e_\mu w_2 \quad \Rightarrow \quad e_\lambda w_3 w_1 w_4 \leq_\tau e_\mu w_3 w_2 w_4$

2) $e_\lambda \leq_\tau e_\lambda w$ for all $w \in \Sigma^*$

c) For $v = \sum_{\lambda\in\Lambda} e_\lambda w_\lambda \neq$, the **leading term** of v is $\mathrm{LT}_\tau(v) = \max_\tau\{v_\lambda \mid v_\lambda \neq 0\}$

d) The **leading term module** of U is the right submodule $\mathrm{LT}_\tau(U) = \langle \mathrm{LT}_\tau(v) \mid v \in U \setminus \{0\}\rangle_r$ of F.

e) $G \subseteq U$ is called a **right τ-Gröbner basis** of U if $\mathrm{LT}_\tau(U) = \langle \mathrm{LT}_\tau(g) \mid g \in G\rangle_r$.

Remarks. a) One can extend Buchberger's Algorithm to right modules. Instead of S-polynomials one has to consider **S-vectors** $S(v_1, v_2, w_1, w_2) = \frac{1}{\mathrm{LC}_\tau(v_1)}\, v_1 - \frac{1}{\mathrm{LC}_\tau(v_2)}\, v_2 w$.

b) U has a finite right τ-Gröbner basis G. One can decide submodule membership and compute effectively in F/U.

c) Every $v \in F$ has a unique normal form $v' = \mathrm{NF}_{\tau,U}(v)$ which can be computed using G.

Proposition 3.1. (Macaulay Basis Theorem)
The residue classes of the terms in

$$\mathcal{O}_\tau(U) = \{e_\lambda w \mid \lambda \in \Lambda,\, w \in \Sigma^*\} \setminus \mathrm{LT}_\tau(U)$$

form a K-basis of F/U.

§ 4. Gröbner Basis Cryptosystems

$M = \Sigma^* / \sim_R$ finitely presented monoid

$F = \bigoplus_{\lambda \in \Lambda} K[\Sigma^*]$ free $K[\Sigma^*]$-module

τ module term ordering

$\bar{F} = F / I_M\, F$ free $K[M]$-module

$U \subseteq F$ right submodule which represents a right submodule $\bar{U} \subseteq \bar{F}$, i.e. such that $I_M\, F \subseteq U$

Public: F, τ, $\mathcal{O}_\tau(U)$, vectors $u_1, \ldots, u_s \in U$

Secret: G right τ-Gröbner basis of U

Encoding: A plaintext unit is a vector $v \in \langle \mathcal{O}_\tau(U) \rangle_K$, i.e. a linear combination $v = c_1 e_{\lambda_1} w_1 + \cdots + c_r e_{\lambda_r} w_r$ such that $c_i \in K$, $\lambda_i \in \Lambda$, and $w_i \in \Sigma^*$.

The corresponding ciphertext unit is $w = v + u_1 f_1 + \cdots + u_s f_s$ with "randomly" chosen $f_1, \ldots, f_s \in K[\Sigma^*]$.

[Variant: $w = (f_0, v f_0 + u_1 f_1 + \cdots + u_s f_s)$]

Decoding: Using $\xrightarrow{G}$, compute $v = \mathrm{NF}_{\sigma,G}(w)$.

[Variant: $\mathrm{NF}_{\sigma,G}(w) = v f_0$ and $v = (v f_0)/f_0$.]

Remarks. a) If the attacker can compute G, he can break the cryptosystem.

b) The attacker knows $u_1, \ldots, u_s$ and $\mathcal{O}_\tau(U)$, but not a system of generators of U. We can make his task difficult by choosing $u_1, \ldots, u_s$ such that a Gröbner basis of $\langle u_1, \ldots, u_s \rangle_r$ is hard to compute.

c) The computation of Gröbner bases is EXTSPACE-hard. (I.e. the amount of memory it requires increases exponentially with the size of the input.)

d) The advantage of using modules (rather than ideals in $K[\Sigma^*]$) is that one can encode hard combinatorial or number theoretic problems in the action of the terms on the canoncial basis vectors (see examples below).

e) The free module F is not required to be finitely generated. Any concrete calculation will involve only finitely many components.

Example 1. $K = \mathbb{F}_q$ finite field

$M = \mathbb{N}^n = \Sigma^* / \sim_R$ where $R = \{x_i x_j \sim x_j x_i\}$

$F = K[\Sigma^*]$ non-commutative polynomial ring

$\tau = \texttt{llex}$

$K[M] = K[x_1, \ldots, x_n]$ commutative polynomial ring

Public: F, τ, $\mathcal{O}_\tau(U) = \{1\}$, $\bar{u}_1, \ldots, \bar{u}_s \in K[M]$ commutative polynomials such that $\bar{u}_i(a_1, \ldots, a_n) = 0$

Secret: $(a_1, \ldots, a_n) \in \mathbb{F}_q^n$, corresponding to the Gröbner basis $\{x_1 - a_1, \ldots, x_n - a_n\}$ of the ideal $\bar{U} = (x_1 - a_1, \ldots, x_n - a_n)$

Encoding: A plaintext unit $c \in \mathbb{F}_q$ is encrypted as $w = c + u_1 f_1 + \cdots + u_s f_s$ with "randomly chosen" polynomials $f_1, \ldots, f_s \in K[M]$.

Decoding: $c = w(a_1, \ldots, a_n) = \mathrm{NF}_{\tau,G}(w)$

This is Neil Koblitz' **polly cracker** cryptosystem. Its disadvantage is that the attacker knows that there is an element in $w + u_1 \cdot K[M] + \cdots + u_s \cdot K[M]$ which has support $\{1\}$. Hence many coefficients have to vanish. This allows a linear algebra attack.

Example 2. $K = \mathbb{F}_2$, $\Sigma = \{x\}$, $M = \Sigma^* = \mathbb{N}$

$K[M] = K[x]$ polynomial ring in one indeterminate

$p \gg 0$ prime number

$F = \bigoplus_{i=1}^{p-1} K[x]\epsilon_i \oplus \bigoplus_{j=1}^{p-1} K[x]e_j$

g generator of $\mathbb{F}_q^*$

$\tau = \texttt{PosDeg}$ such that $\epsilon_{g^{p-1}} >_\tau \cdots >_\tau \epsilon_g >_\tau \epsilon_1 >_\tau$

$>_\tau e_1 >_\tau e_g >_\tau \cdots >_\tau e_{g^{p-1}}$

Public: F, τ, $\mathcal{O}_\tau(U) = \{e_1, e_2, \ldots, e_{p-1}\}$, $b = g^a (\text{mod } p)$, $\{u_1, \ldots, u_s\} = \{\epsilon_1 - e_1, x\epsilon_i - \epsilon_{gi}, xe_j - e_{bj} \mid i, j = 1, \ldots, p-1\}$ where all indices are computed modulo p.

Secret: $a \in \{1, \ldots, p-1\}$, $G = \{u_1, \ldots, u_s\} \cup \{\epsilon_i - e_{i^a} \mid i = 1, \ldots, p-1\}$ τ-Gröbner basis of $U = \langle G \rangle$

Encryption: A plaintext unit is of the form $e_1 + e_c$ with $c \in \{0, \ldots, p-1\}$. Using the variant, we randomly choose $k \in \{0, \ldots, p-1\}$ and form $x^k(e_1 + e_c)$. By adding suitable elements u_i we compute $x^k(e_1 + e_c) = x^k \epsilon_1 + x^k e_c = \epsilon_{g^k} + e_{cb^k}$ in $F/\langle u_1, \ldots, u_s \rangle$. The ciphertext unit is $w = \epsilon_{g^k} + e_{cb^k}$.

Decryption: $\mathrm{NF}_{\tau,U}(w) = \mathrm{NF}(e_{b^k} + e_{cb^k}) = \mathrm{NF}(x^k(e_1 + e_c))$. In order to divide this vector by x^k, it suffices to compute $c = (cb^k)/(b^k)$ in $\mathbb{F}_p$ and to form $e_1 + e_c$.

This is the Gröbner basis version of the **ElGamal** cryptosystem. It can be broken if the attacker is able to compute the discrete logarithm a of $b = g^a$ or k of g^k.

In the Gröbner basis version, the attacker has to reduce using $\epsilon_{g^k} \xrightarrow{u_i} \cdots \xrightarrow{u_j} x^k \epsilon_1 \xrightarrow{u_1} x^k e_1$ which takes $k \gg 0$ reduction steps. If one knows a, one can get rid of the ϵ_i by using just one reduction step $\epsilon_{g^k} \longrightarrow \epsilon_{g^{ka}}$.

Example 3. Let $K = \mathbb{F}_2$, $\Sigma = \{x, y\}$, $M = \mathbb{N}^2$

$K[M] = K[\Sigma^*]/\langle xy - yx \rangle = K[x, y]$ polynomial ring

$p, q \gg 0$ prime numbers, $n = pq$

$\bar{F} = \bigoplus_{i \in (\mathbb{Z}/n\mathbb{Z})^*} K[x, y]\epsilon_i, \quad \tau = \texttt{DegLexPos}$

Public: F (and thus n), τ, $\mathcal{O}_\tau(U) = \{\epsilon_i \mid i \in (\mathbb{Z}/n\mathbb{Z})^*\}$, $e \in (\mathbb{Z}/(p-1)(q-1)\mathbb{Z})^*$, $\{u_1, \dots, u_s\} = \{x\epsilon_i - \epsilon_{i^e}, xy\epsilon_j - \epsilon_j \mid i, j \in (\mathbb{Z}/n\mathbb{Z})^*\}$

Secret: p, q, a number $d \in \{1, \dots, n-1\}$ which satisfies $de = 1(\mathrm{mod}\ p-1)$ and $de = 1(\mathrm{mod}\ q-1)$, and the τ-Gröbner basis $G = \{u_1, \dots, u_s\} \cup \{y\epsilon_i - \epsilon_{i^d} \mid i \in (\mathbb{Z}/n\mathbb{Z})^*\}$ of $U = \langle G \rangle$.

Encryption: A plaintext unit is a vector $\epsilon_c \in \mathcal{O}_\tau(U)$. To encrypt it, we form $xy\epsilon_c$ and add elements of $\{u_1, \dots, u_s\}$ to obtain the cyphertext unit $w = y\epsilon_{c^e}$.

Decryption: Compute $\mathrm{NF}_{\tau,U}(y\epsilon_{c^e}) = \mathrm{NF}_{\tau,U}(\epsilon_{c^{ed}}) = \epsilon_c$.

This is the Gröbner basis version of the **RSA** cryptosystem. If the attacker is able to factor n, he can break the code. It is easy to see that this is equivalent to being able to find d. In the Gröbner basis version, the problem the attacker faces is that he doesn't know the Gröbner basis elements $y\epsilon_i - \epsilon_{i^d}$ which are not even elements of the submodule $\langle u_1, \ldots, u_s \rangle$ that he knows.

Example 4: Let K be a field and $M = \Sigma^*/\sim_R$ a finitely presented group.

$K[M] = K[\Sigma^*]/I_M$

$\bar{F} = \bigoplus_{\bar{w} \in M} \epsilon_{\bar{w}}\, K[M] \oplus \bigoplus_{\bar{w} \in M} e_{\bar{w}}\, K[M]$ free right $K[M]$-module

$\tau = \texttt{llex}$ such that $\epsilon_{\bar{w}} >_\tau e_{\bar{u}}$ for all $w, u \in \Sigma^*$

Public: F, τ, $g, g' \in M$ such that $g' = a^{-1}ga$, $\mathcal{O}_\tau(U) = \{e_{\bar{w}} \mid \bar{w} \in M\}$, and $\{u_\lambda \mid \lambda \in \Lambda\} = \{\epsilon_i h - \epsilon_{h^{-1}ih},\ \epsilon_g - e_{g'},\ e_j k - e_{k^{-1}jk} \mid i, j, h, k \in M\}$

Secret: $a \in M$, or equivalently, the τ-Gröbner basis $G = \{u_\lambda \mid \lambda \in \Lambda\} \cup \{\epsilon_i - e_{a^{-1}ia} \mid i \in M\}$ of $U = \langle G \rangle_r \subseteq F$

Encryption: A plaintext unit $m \in M$ is written in the form $\epsilon_g + e_{g'\tilde{m}}$, where $\tilde{m} = bmb^{-1}$. Then we multiply by the "randomly" chosen element $b \in \{c \in M \mid ca = ac\}$ and use the elements u_λ to compute $w = \epsilon_{b^{-1}gb} + e_{b^{-1}g'\tilde{m}b}$.

Decryption: Compute $\mathrm{NF}_{\tau,G}(w) = \mathrm{NF}_{\tau,G}(e_{a^{-1}g''a} + e_{b^{-1}g'bm})$ $= \mathrm{NF}_{\tau,G}(e_{b^{-1}g'b} + e_{b^{-1}g'b\,m})$, where $g'' = b^{-1}gb$. Then determine m from the relation $m = (b^{-1}g'bm)/(b^{-1}g'b)$.

This is Gröbner basis version of an ElGamal like cryptosystem based on a group with a “hard” conjugator search problem (e.g. braid groups). The attacker can break the code if he can determine a from g and $g' = a^{-1}ga$. The advantage of knowing the Gröbner basis of that one can pass from $\epsilon_{g''}$ to the corresponding e_i without going through $\epsilon_g = e_{g'}$. The computation of that Gröbner basis is equivalent to finding a.

§ 5. A Possible Generalization

- If one wants to have a theory of Gröbner bases for a ring (like $K[\Sigma^*]$ or $K[M]$), it has to be a residue class ring of a path algebra.
- The ring $K[\Sigma^*]$ is the path algebra of the graph

- By using path algebras of more general graphs Γ, it is possible to build “hard” computational problems from graph theory into the computation of Gröbner bases for ideals or modules over the ring $K[\Gamma]$.

Conclusions

• For two-sided ideals in $K[\Sigma^*]$, Gröbner bases exist, but they may not be finite.

• For finitely generated right ideals and right submodules of free modules over $K[\Sigma^*]$, finite right Gröbner bases exist and are computable.

• If the appropriate Gröbner basis exists, one can solve

— the word problem for monoids

— the generalized word problem for monoids and groups

— the conjugation problem for groups

— the conjugator search problem for groups

• Gröbner basis cryptosystems rely on the inherent difficulty of computing certain Gröbner bases.

• Many classical cryptosystems can be viewed as Gröbner basis cryptosystems:

— Koblitz' polly cracker (and its generalizations)

— ElGamal (based on discrete log)

— RSA (based on integer factorization)

— Conjugator search cryptosystems (e.g. in braid groups)

• The difficulty of computing the Gröbner basis in question can be based on a number of factors:

— computing Gröbner bases is EXTSPACE-hard

— the attacker does not know the submodule U whose Gröbner basis he needs

— the free module has a large (or infinite) rank

— the operation of $K[\Sigma^*]$ on the basis vectors of F encodes difficult computational problems (e.g. discrete log or integer factorization)

— the structure of the base ring $K[\Gamma]$ encodes difficult computational tasks (e.g. from graph theory or combinatorics)

• For certain Gröbner basis computations, there are guaranteed lower complexity bounds.