Parametrization of algebraic tori

Clément DUNAND
joint work with Reynald LERCIER

Outline

Outline

Why use algebraic tori ?

T_n : subgroup of $\mathbb{F}_{q^n}^\times$ of *"optimal"* order.

$$\#\mathbb{F}_{q^n}^\times = \prod_{d|n} \Phi_d(q)$$

Why use algebraic tori ?

T_n : subgroup of $\mathbb{F}_{q^n}^\times$ of *"optimal"* order.

$$\begin{aligned} \#\mathbb{F}_{q^n}^\times &= \prod_{d|n} \Phi_d(q) \\ &= \Phi_1(q) \dots \underbrace{\Phi_n(q)}_{\#T_n}. \end{aligned}$$

Why use algebraic tori ?

T_n : subgroup of $\mathbb{F}_{q^n}^\times$ of *"optimal"* order.

$$\begin{aligned} \#\mathbb{F}_{q^n}^\times &= \prod_{d|n} \Phi_d(q) \\ &= \Phi_1(q) \dots \underbrace{\Phi_n(q)}_{\#T_n}. \end{aligned}$$

Example

$$\mathbb{F}_{q^6}^\times = \underbrace{(q-1)}_{T_1=\mathbb{F}_q^\times} \underbrace{(q+1)}_{T_2 \subset \mathbb{F}_{q^2}^\times} \underbrace{(q^2+q+1)}_{T_3 \subset \mathbb{F}_{q^3}^\times} \underbrace{(q^2-q+1)}_{T_6}.$$

Also an algebraic variety

Definition

We define the *algebraic torus* by the following relation :

$$T_n(\mathbb{F}_q) = \left\{ \alpha \in \mathbb{F}_{q^n}^{\times} : \alpha^{\Phi_n(q)} = 1 \right\}.$$

It is equivalent to write that the algebraic torus $T_n(\mathbb{F}_q)$ is the intersection of the kernels of the norms $N_{\mathbb{F}_{q^n}/F}$, over all $F \subsetneq \mathbb{F}_{q^n}$.

$$T_n(\mathbb{F}_q) = \left\{ \alpha \in \mathbb{F}_{q^n}^{\times} : \forall \mathbb{F}_q \subset F \subsetneq \mathbb{F}_{q^n} \quad N_{\mathbb{F}_{q^n}/F}(\alpha) = 1 \right\}.$$

Remark. The dimension of $T_n(\mathbb{F}_q)$ is $\varphi(n) = \deg(\Phi_n)$.

In brief

Two ways of considering the algebraic torus T_n.

$$T_n \subset \mathbb{F}_{q^n}^\times, \quad \#T_n = \Phi_n(q). \qquad \Big| \qquad T_n(\mathbb{F}_q) = \left\{\alpha \in \mathbb{F}_{q^n}^\times : \alpha^{\Phi_n(q)} = 1\right\}, \quad \dim T_n = \varphi(n).$$

Remark.

$$\#\mathbb{F}_{q^n}^\times = \prod_{d|n} \Phi_d(q),$$

$$\Rightarrow \quad \boxed{\mathbb{F}_{q^n}^\times = \prod_{d|n} T_d(\mathbb{F}_q)}$$

Outline

Compact representation

We want to send an element of the torus.
Naive representation : $T_n \subset \mathbb{F}_{q^n} \longrightarrow n$ coordinates.
Clever representation : $dim(T_n) = \varphi(n) \longrightarrow \varphi(n)$ coordinates.

Compact representation

We want to send an element of the torus.
Naive representation : $T_6 \subset \mathbb{F}_{q^6} \longrightarrow$ 6 coordinates.
Clever representation : $dim(T_6) = \varphi(6) \longrightarrow$ 2 coordinates.

Example

Parametrization of T_6 with $\varphi(6) = 2$ coordinates.

- XTR (Lenstra, Verheul)
- CEILIDH (Silverberg, Rubin)

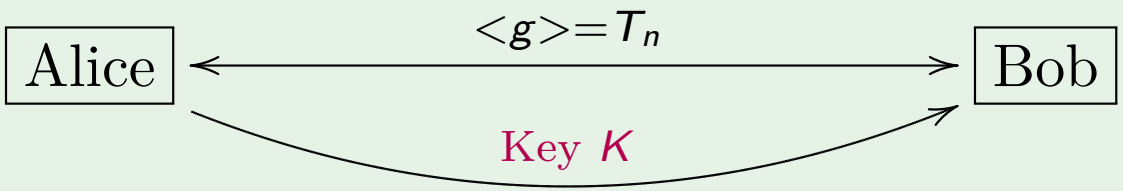
Compression and cryptography

Idea of the bijection $\Theta : T_n \times \Pi \longrightarrow \tilde{\Pi}$.

Compression and cryptography

Idea of the bijection $\Theta : T_n \times \Pi \longrightarrow \tilde{\Pi}$.

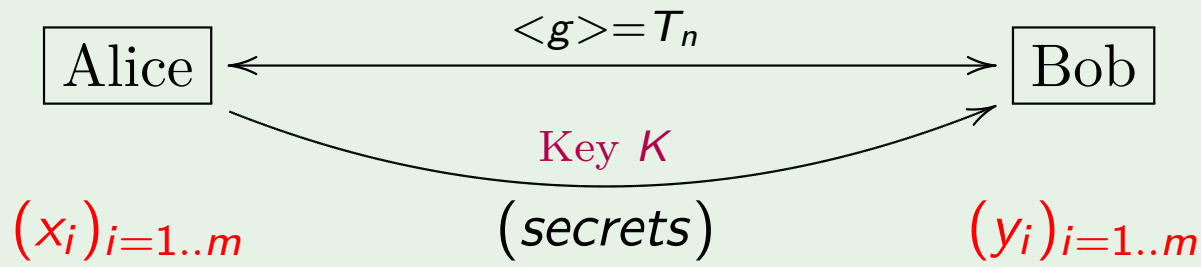
Diffie-Hellman multiple key agreement



Compression and cryptography

Idea of the bijection $\Theta : T_n \times \Pi \longrightarrow \tilde{\Pi}$.

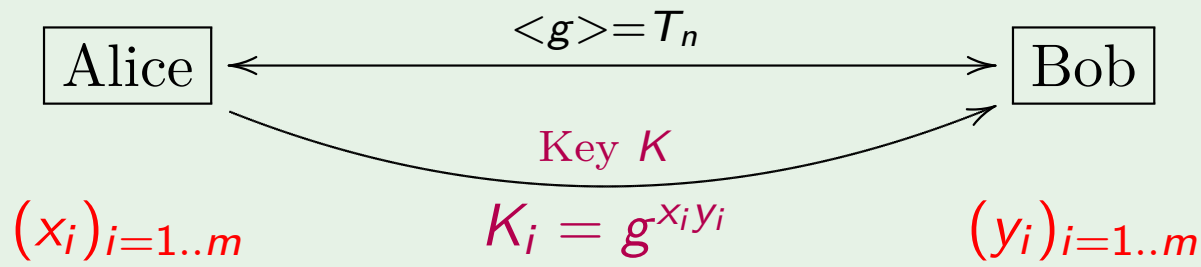
Diffie-Hellman multiple key agreement



Compression and cryptography

Idea of the bijection $\Theta : T_n \times \Pi \longrightarrow \tilde{\Pi}$.

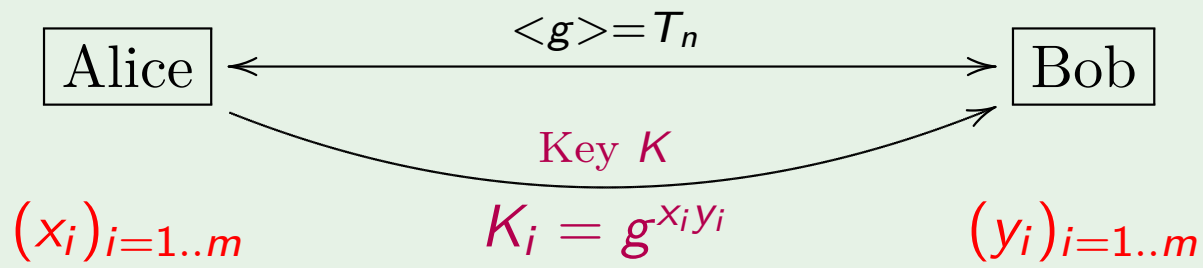
Diffie-Hellman multiple key agreement



Compression and cryptography

Idea of the bijection $\Theta : T_n \times \Pi \longrightarrow \tilde{\Pi}$.

Diffie-Hellman multiple key agreement



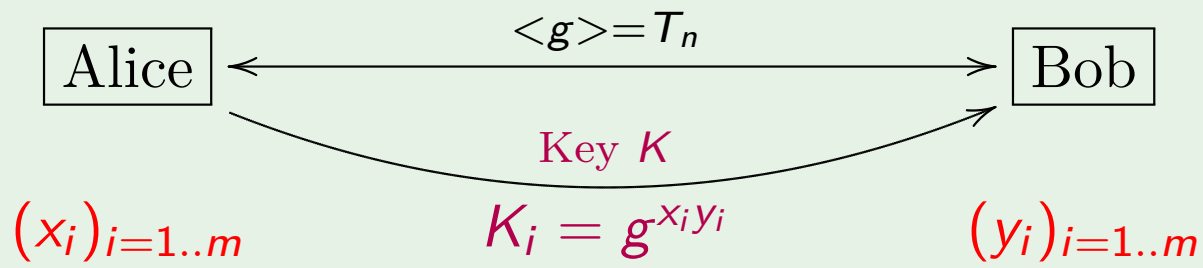
$A_i = g^{x_i}$, $S_0 \in \Pi$

$\Theta(A_i, S_{i-1}) = (a_i, S_i)$ $\xrightarrow{(a_i), S_m}$

Compression and cryptography

Idea of the bijection $\Theta : T_n \times \Pi \longrightarrow \tilde{\Pi}$.

Diffie-Hellman multiple key agreement



$A_i = g^{x_i}$, $S_0 \in \Pi$

$\Theta(A_i, S_{i-1}) = (a_i, S_i)$ $\xrightarrow{(a_i), S_m}$

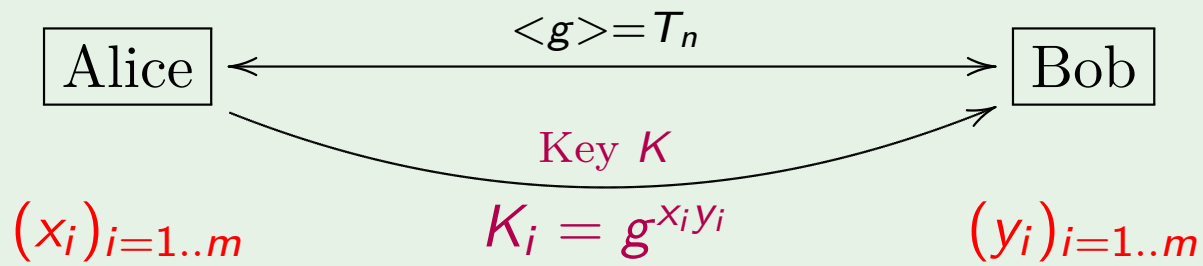
$\Theta^{-1}(a_m, S_m) = (A_m, S_{m-1})$

$\Theta^{-1}(a_{m-1}, S_{m-1}) = (A_{m-1}, S_{m-2})$

Compression and cryptography

Idea of the bijection $\Theta : T_n \times \Pi \longrightarrow \tilde{\Pi}$.

Diffie-Hellman multiple key agreement



$A_i = g^{x_i}$, $S_0 \in \Pi$

$\Theta(A_i, S_{i-1}) = (a_i, S_i)$ $\xrightarrow{(a_i), S_m}$

$\Theta^{-1}(a_m, S_m) = (A_m, S_{m-1})$

$\Theta^{-1}(a_{m-1}, S_{m-1}) = (A_{m-1}, S_{m-2})$

$K_i = A_i^{y_i}$

Idea for a bijection (van Dijk, Woodruff)

Recall that $\mathbb{F}_{q^n}^\times = \prod_{d|n} T_d$. Example in the case $n = 15$.

$$T_{15} \longrightarrow \mathbb{F}_{q^{15}}^\times$$

Idea for a bijection (van Dijk, Woodruff)

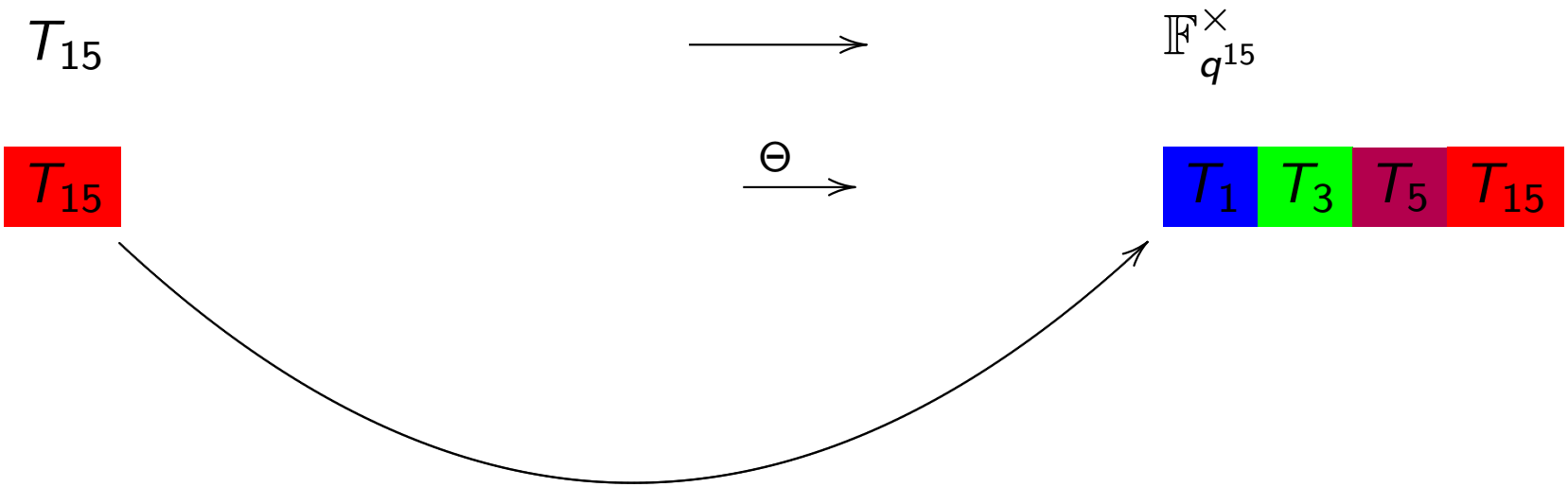
Recall that $\mathbb{F}_{q^n}^\times = \prod_{d|n} T_d$. Example in the case $n = 15$.

$$T_{15} \longrightarrow \mathbb{F}_{q^{15}}^\times$$

$$T_{15} \xrightarrow{\Theta}$$

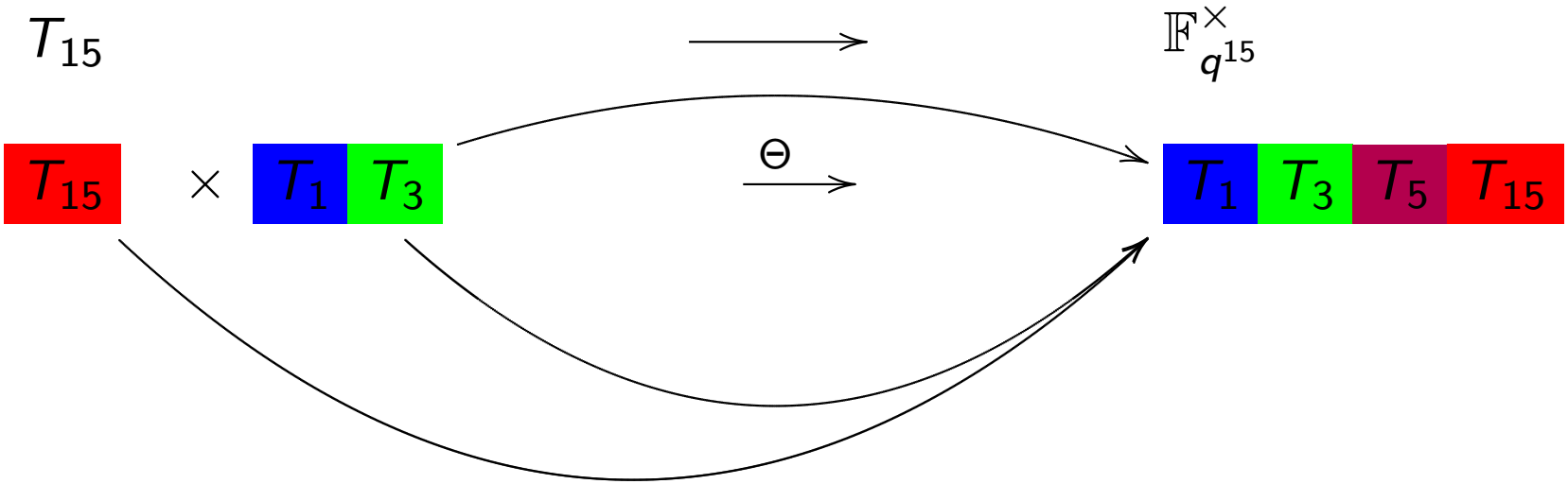
Idea for a bijection (van Dijk, Woodruff)

Recall that $\mathbb{F}_{q^n}^\times = \prod_{d|n} T_d$. Example in the case $n = 15$.



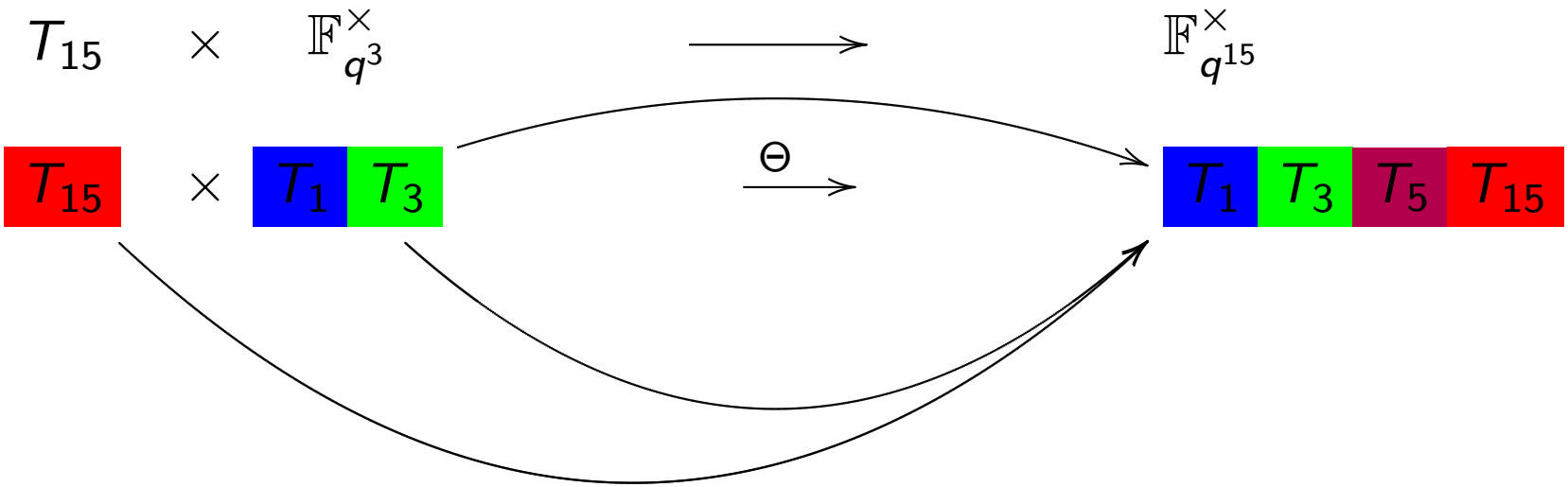
Idea for a bijection (van Dijk, Woodruff)

Recall that $\mathbb{F}_{q^n}^\times = \prod_{d|n} T_d$. Example in the case $n = 15$.



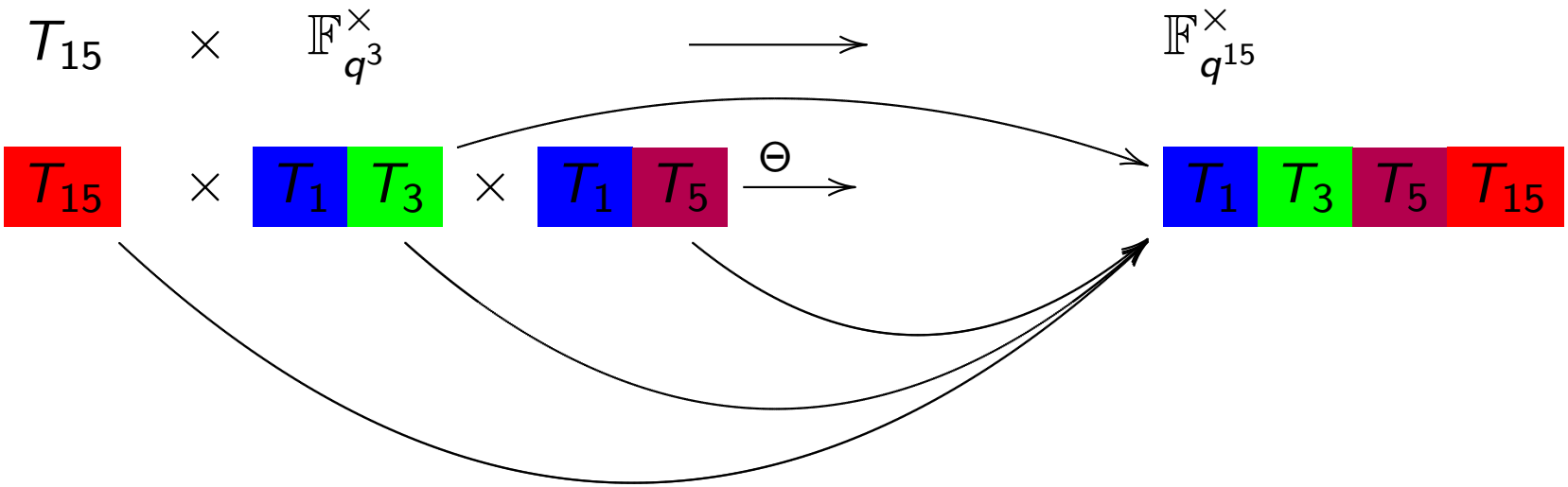
Idea for a bijection (van Dijk, Woodruff)

Recall that $\mathbb{F}_{q^n}^\times = \prod_{d|n} T_d$. Example in the case $n = 15$.



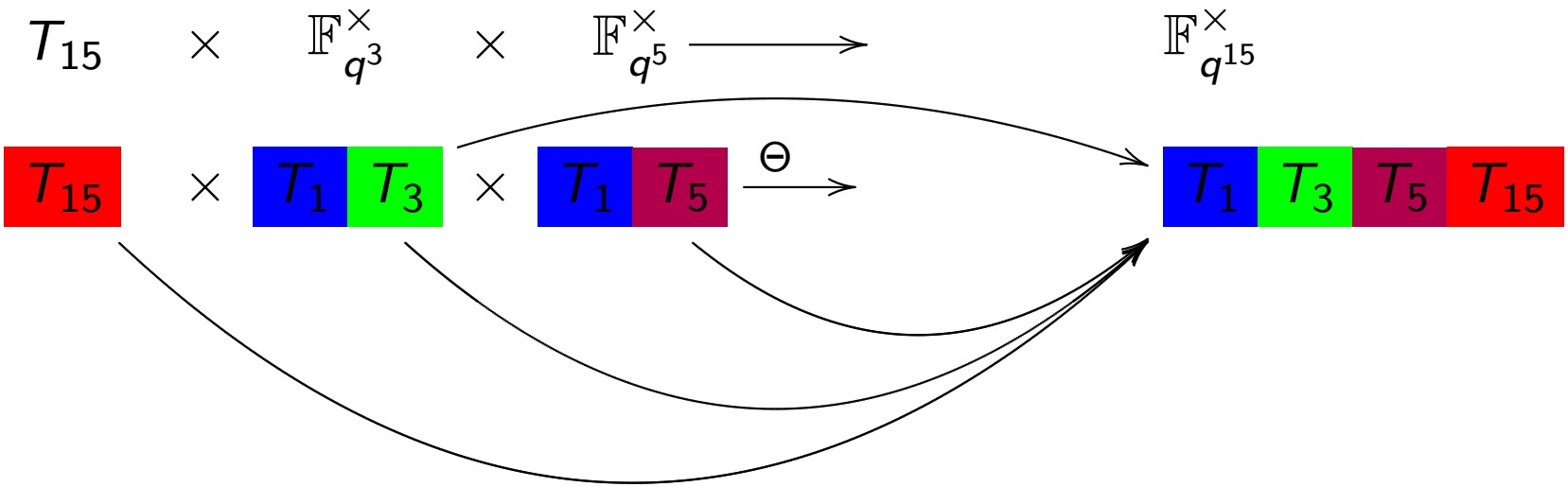
Idea for a bijection (van Dijk, Woodruff)

Recall that $\mathbb{F}_{q^n}^\times = \prod_{d|n} T_d$. Example in the case $n = 15$.



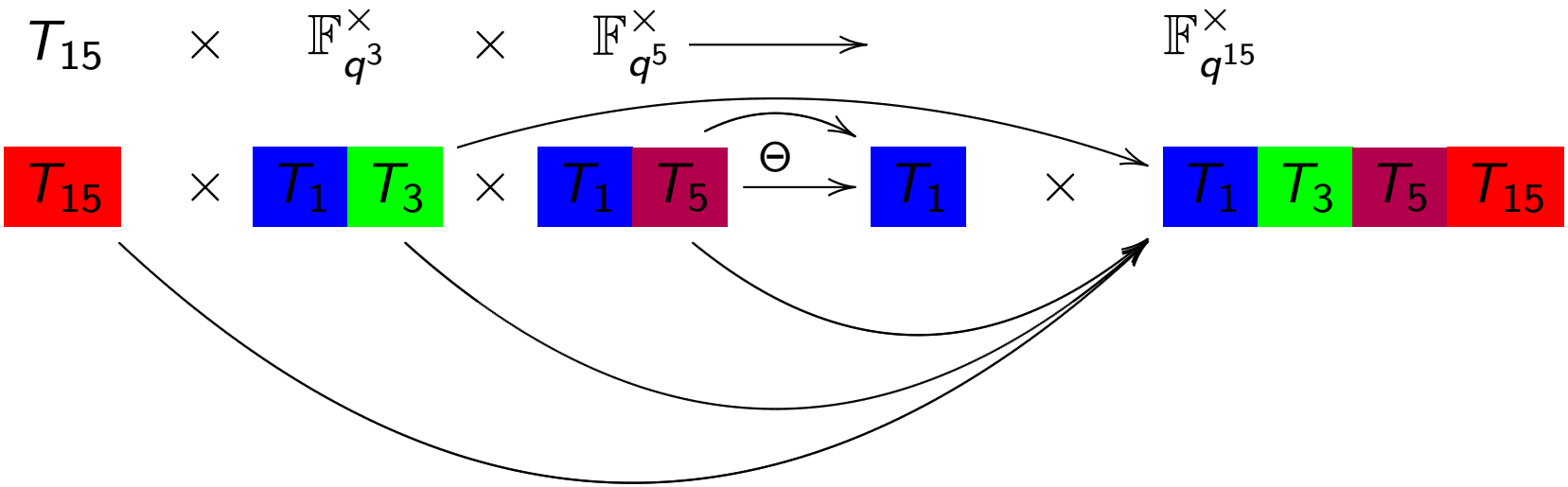
Idea for a bijection (van Dijk, Woodruff)

Recall that $\mathbb{F}_{q^n}^\times = \prod_{d|n} T_d$. Example in the case $n = 15$.



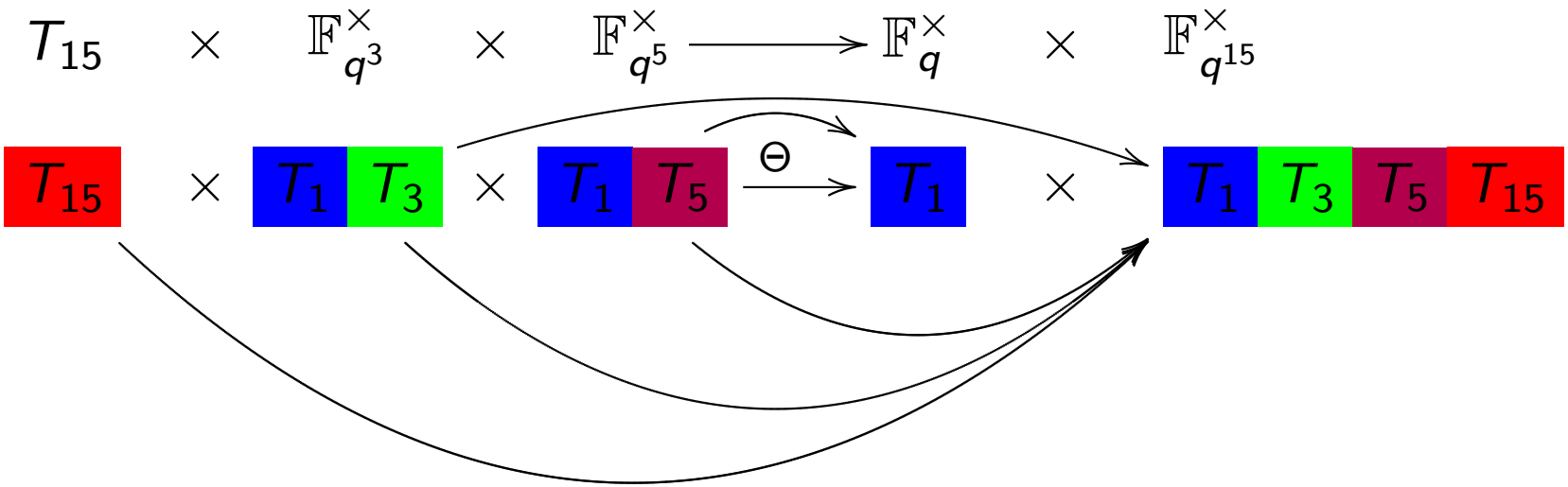
Idea for a bijection (van Dijk, Woodruff)

Recall that $\mathbb{F}_{q^n}^\times = \prod_{d|n} T_d$. Example in the case $n = 15$.



Idea for a bijection (van Dijk, Woodruff)

Recall that $\mathbb{F}_{q^n}^\times = \prod_{d|n} T_d$. Example in the case $n = 15$.

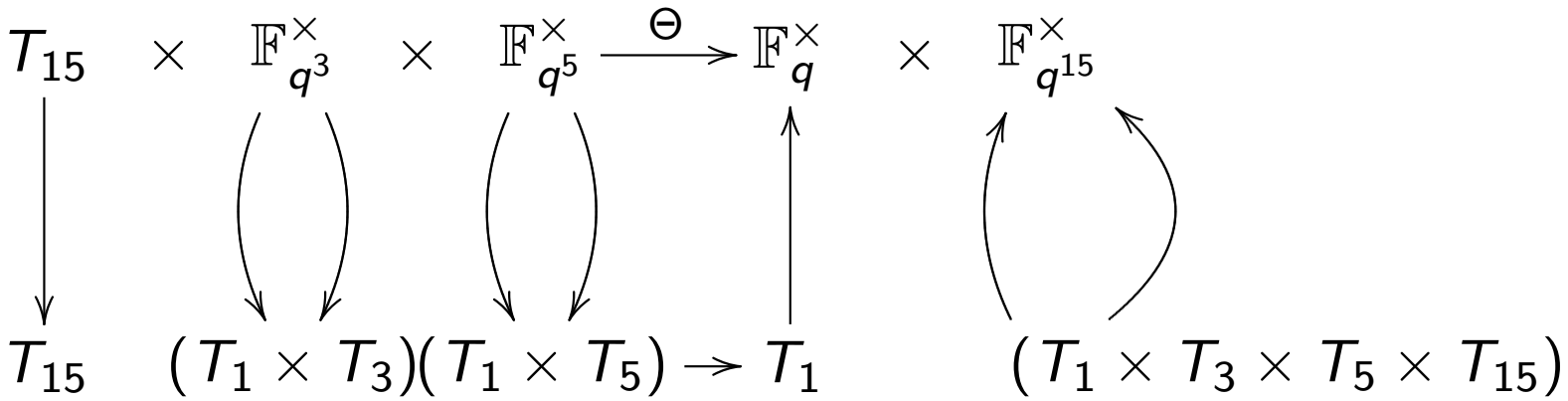


General formula

μ denotes the Möbius function.

$$\Theta : T_n(\mathbb{F}_q) \times \prod_{\substack{d|n \\ \mu(n/d)=-1}} \mathbb{F}_{q^d}^{\times} \to \prod_{\substack{d|n \\ \mu(n/d)=+1}} \mathbb{F}_{q^d}^{\times}$$

The bijection step by step



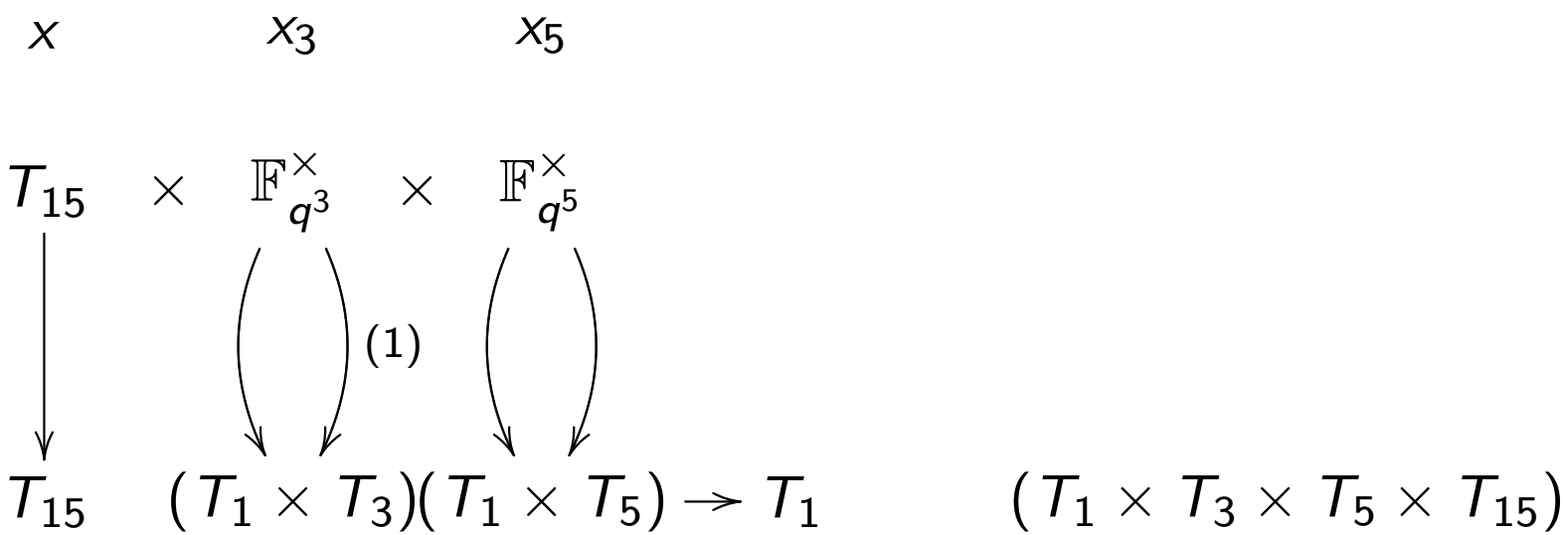
The bijection step by step

$$\begin{array}{ccccc} x & & x_3 & & x_5 \\ T_{15} & \times & \mathbb{F}_{q^3}^{\times} & \times & \mathbb{F}_{q^5}^{\times} \end{array}$$

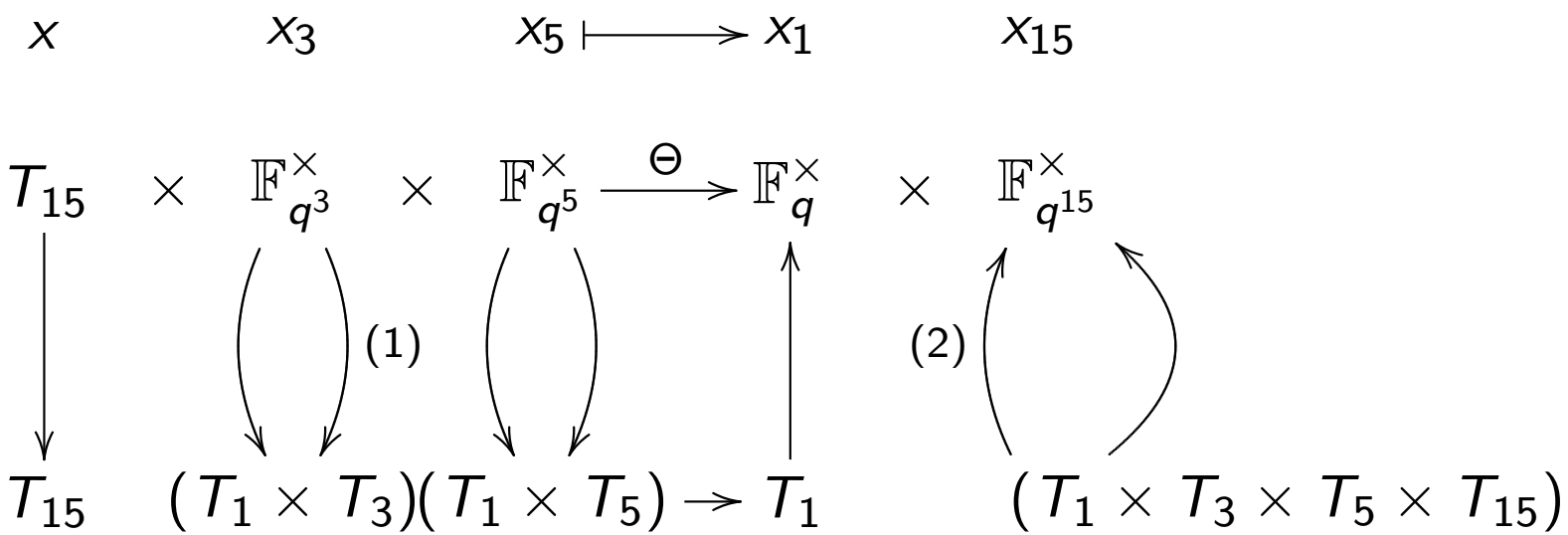
The bijection step by step

$$
\begin{array}{ccccc}
x & & x_3 & & x_5 \\
T_{15} & \times & \mathbb{F}_{q^3}^{\times} & \times & \mathbb{F}_{q^5}^{\times} \\
\downarrow & & \swarrow\ \searrow\ (1) & & \swarrow\ \searrow \\
T_{15} & & (T_1 \times T_3) & & (T_1 \times T_5)
\end{array}
$$

The bijection step by step



The bijection step by step



Outline

First operation

It is the decomposition of a point of $\mathbb{F}_{q^d}^{\times}$ into components in the tori T_1 and T_d.
We perform this operation in the most natural way :

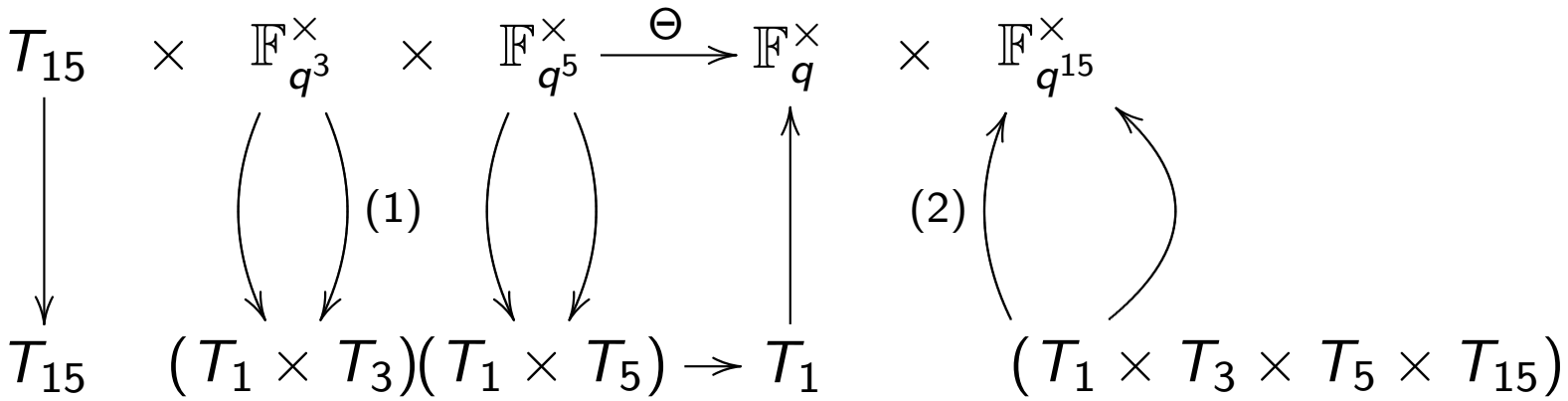
$$\begin{array}{ccccc} \mathbb{F}_{q^d}^{\times} & \xrightarrow{(1)} & T_1 & \times & T_d \\ x_d & \longmapsto & \left(x_d^{\Phi_d(q)}\right. & , & \left. x_d^{\Phi_1(q)}\right) \end{array}$$

Cost

$\Phi_d(q)$ has degree $\varphi(d)$ in q.
So performing exponentiations to the power $\Phi_d(q)$ requires

$$O(\varphi(d)\log q) \text{ multiplications in } \mathbb{F}_q.$$

The bijection step by step



Second operation

Let's see on the example $n = 15$: It is a recombination of coordinates in the tori T_1, T_3, T_5, T_{15}.

$$\begin{array}{ccc} T_1 \times T_3 \times T_5 \times T_{15} & \longrightarrow & \mathbb{F}_{q^{15}}^{\times} \\ (x_1, x_3, x_5, x_{15}) & \xrightarrow{(2)} & x \end{array}$$

$$x = x_1^{w_1} x_3^{w_3} x_5^{w_5} x_{15}^{w_{15}} \quad \text{where} \sum_{d|15} \frac{q^{15}-1}{\Phi_d(q)} w_d = 1.$$

Cost

For each divisor d of 15, we have $w_d \leqslant q^{15} - 1$. So exponentiation requires

$$O(15 \log q) \text{ multiplications.}$$

Outline

Elliptic normal bases (Couveignes, Lercier)

Theorem

For any extension $\mathbb{F}_{q^n}$ of $\mathbb{F}_q$, there exists a normal basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ such that both

- the product of two elements
- exponentiation of an element to a power of q

can be performed in linear time.

The construction of such bases uses elliptic curves, hence the name of *elliptic bases*.

First operation

Recall the first decomposition :

$$\begin{array}{ccccc} \mathbb{F}_{q^d}^{\times} & \xrightarrow{(1)} & T_1 & \times & T_d \\ x_d & \longmapsto & \left(x_d^{\Phi_d(q)}\right. & , & \left. x_d^{\Phi_1(q)}\right) \end{array}$$

Cost

$\Phi_1(q) = q - 1$, $\Phi_3(q) = q^2 + q + 1$ and $\Phi_5(q) = q^4 + q^3 + q^2 + q + 1$.
So performing exponentiations to these powers requires

$$O(\varphi(d)) \text{ multiplications in } \mathbb{F}_q.$$

Second operation

Recall the recombination on the right hand side :

$$\begin{array}{ccc} T_1 \times T_3 \times T_5 \times T_{15} & \longrightarrow & \mathbb{F}_{q^{15}}^{\times} \\ (x_1, x_3, x_5, x_{15}) & \xrightarrow{(2)} & x \end{array}$$

$$x = x_1^{w_1} x_3^{w_3} x_5^{w_5} x_{15}^{w_{15}} \quad \text{where} \sum_{d|15} \frac{q^{15}-1}{\Phi_d(q)} w_d = 1.$$

Cost

w_d are actually polynomials in q. So once again we have exponentiations to a power of q and a certain number of multiplications, depending on the coefficients. In practice, the polynomials w_d have very convenient coefficients.

Results

Global cost of the communication :

- Before improvement : $O(n^3 \log^2 q)$ operations.
- After improvement : $O(n^3 \log q)$ operations.

Usual cost of a classical D.H. cryptosystem : $O(n^2 \log^2 q)$.

Outline

Things to do (among others)

- Make clear the phenomenon with the cyclotomic polynomials.
- Question of a *birational* parametrization.

Merci de votre attention

et

bon appétit !