Noisy Diffie-Hellman protocols or code-based key exchanged and encryption without masking

Carlos Aguilar[1], **Philippe Gaborit**[1], Patrick Lacharme[1], Julien Schrek[1] and Gilles Zémor[2]

1 University of Limoges, France,

2 University of Bordeaux, France.

Classical Diffie-Hellman and Noisy DH

• **Classical DH protocol :** $g^a, g^b \longrightarrow g^{ab}$
Alice and Bob share the same secret.

• **Noisy Diffie-Hellman protocols**
1. Alice and Bob obtained a noisy shared secret (a correlated sequence of bits)

2. Alice and Bob communicate to obtain a common secret from the noisy shared sequence

Noisy DH protocol

Suppose $A = F_2[x]/(x^n - 1)$ a commutative ring embedded with Hamming distance.

h : a random element of A

Alice chooses a and α elements of A with small norm : $O(\sqrt{n})$

Bob chooses b and β elements of A with small norm $O(\sqrt{n})$

Alice sends $\longrightarrow$ **Bob :** $\sigma(a, \alpha) = ah + \alpha$

Bob sends $\longrightarrow$ **Alice :** $\sigma(b, \beta) = bh + \beta$

From $\sigma(b, \beta)$ Alice computes $a\sigma(b, \beta) = abh + a\beta$

From $\sigma(a, \alpha)$ Bob computes $b\sigma(a, \alpha) = abh + b\alpha$

$\longrightarrow$ these two quantities differ by $a\beta - b\alpha$ of small norm.

Practical example : Coding theory

Alice and Bob agree on a **publicly known code C** with matrix G,

Alice sends to Bob a noisy message $mG + abh + a\beta$ that Bob can decode in m.

$\longrightarrow$ New code-based system based on random circulant matrices

$\longrightarrow$ Moderate key size : 6000b

$\longrightarrow$ Very fast 2^{17} operations

$\longrightarrow$ NO MASKING and Security reduction to DH-like problem for decoding of random DC codes