UNIVERSITÉ de Picardie Jules Verne

mis modelisation, information & systèmes

Cryptanalyse logique du problème du logarithme discret

Monika Trimoska

Encadrants de thèse:
Gilles Dequen
Sorina Ionica

Le problème du logarithme discret

Le problème du logarithme discret

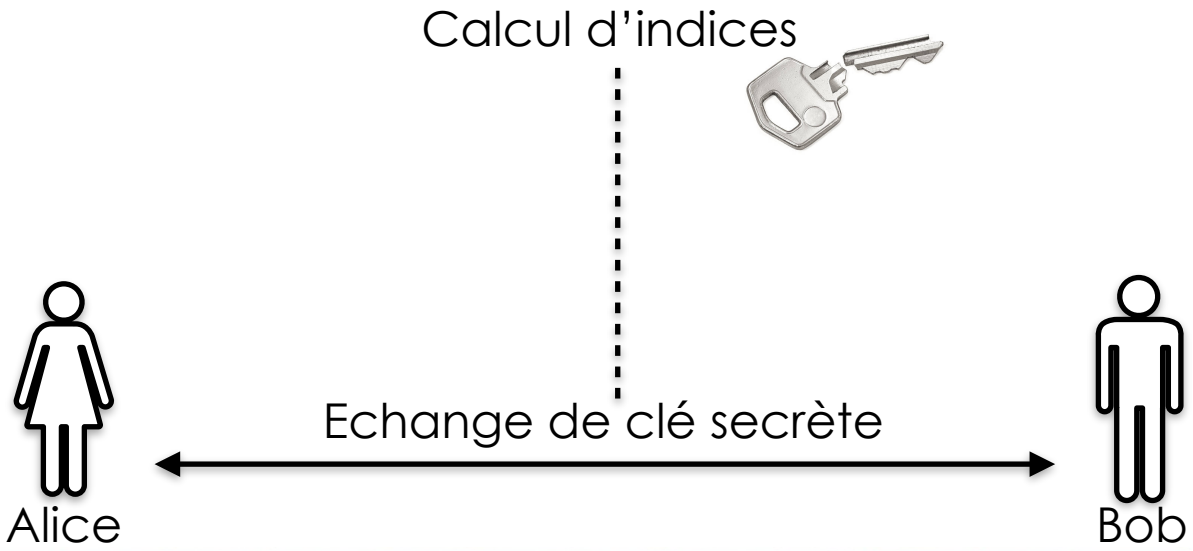
Trouver X tel que

$$h = g^x \pmod p$$

ou

ECC: $Q = xP \pmod p$

Le problème du logarithme discret



Trouver X tel que

$$h = g^x \pmod p$$

ou

ECC: $Q = xP \pmod p$

Calcul d'indices

- $\log(a \cdot b \cdot c) = \log(a) + \log(b) + \log(c)$
- Décomposition en nombres premiers

Calcul d'indices

- $\log(a \cdot b \cdot c) = \log(a) + \log(b) + \log(c)$
- Décomposition en nombres premiers

Calcul d'indices

$28 = 2^x \pmod{47}, \quad x = ?$

Soit la base de factorisation {2, 3, 5, 7}

Soit (p = 47)

Phase recherche de relations

$2^1 \equiv 2 \pmod{47}$

$2^7 \equiv 34 = 2 \cdot 17 \pmod{47}$

$2^8 \equiv 21 = 3 \cdot 7 \pmod{47}$

$2^{12} \equiv 7 \pmod{47}$

$2^{18} \equiv 25 = 5^2 \pmod{47}$

Calcul d'indices

$28 = 2^x \pmod{47}, \quad x = ?$

Soit la base de factorisation {2, 3, 5, 7}

Soit (p = 47)

Phase recherche de relations

$$2^1 \equiv 2 \pmod{47}$$

$$2^7 \equiv 34 = 2 \cdot 17 \pmod{47}$$

$$2^8 \equiv 21 = 3 \cdot 7 \pmod{47}$$

$$2^{12} \equiv 7 \pmod{47}$$

$$2^{18} \equiv 25 = 5^2 \pmod{47}$$

Calcul d'indices

$28 = 2^x \pmod{47}, \quad x = ?$

Soit la base de factorisation {2, 3, 5, 7}

Soit (p = 47)

Phase recherche de relations

$2^1 \equiv 2 \pmod{47}$

~~$2^7 \equiv 34 = 2 \cdot 17 \pmod{47}$~~

$2^8 \equiv 21 = 3 \cdot 7 \pmod{47}$

$2^{12} \equiv 7 \pmod{47}$

$2^{18} \equiv 25 = 5^2 \pmod{47}$

Calcul d'indices

$28 = 2^x \pmod{47}, \quad x = ?$

Soit la base de factorisation {2, 3, 5, 7}

Soit (p = 47)

Phase recherche de relations

$2^1 \equiv 2 \pmod{47}$

~~$2^7 \equiv 34 = 2 \cdot 17 \pmod{47}$~~

$2^8 \equiv 21 = 3 \cdot 7 \pmod{47}$

$2^{12} \equiv 7 \pmod{47}$

$2^{18} \equiv 25 = 5^2 \pmod{47}$

Calcul d'indices

$28 = 2^x \pmod{47}, \quad x = ?$

Soit la base de factorisation {2, 3, 5, 7}

Soit (p = 47)

Phase recherche de relations

$2^1 \equiv 2 \pmod{47}$

~~$2^7 \equiv 34 = 2 \cdot 17 \pmod{47}$~~

$2^8 \equiv 21 = 3 \cdot 7 \pmod{47}$

$2^{12} \equiv 7 \pmod{47}$

$2^{18} \equiv 25 = 5^2 \pmod{47}$

2	3	5	7	
1	0	0	0	1
0	1	0	1	8
0	0	0	1	12
0	0	2	0	18

Calcul d'indices

$28 = 2^x \pmod{47}, \quad x = ?$

Soit la base de factorisation {2, 3, 5, 7}

Soit (p = 47)

Phase recherche de relations

$2^1 \equiv 2 \pmod{47}$

~~$2^7 \equiv 34 = 2 \cdot 17 \pmod{47}$~~

$2^8 \equiv 21 = 3 \cdot 7 \pmod{47}$

$2^{12} \equiv 7 \pmod{47}$

$2^{18} \equiv 25 = 5^2 \pmod{47}$

2	3	5	7	
1	0	0	0	1
0	1	0	1	8
0	0	0	1	12
0	0	2	0	18

Calcul d'indices

$28 = 2^x \pmod{47}, \quad x = ?$

Soit la base de factorisation {2, 3, 5, 7}

Soit (p = 47)

Phase recherche de relations

$2^1 \equiv 2 \pmod{47}$

~~$2^7 \equiv 34 = 2 \cdot 17 \pmod{47}$~~

$2^8 \equiv 21 = 3 \cdot 7 \pmod{47}$

$2^{12} \equiv 7 \pmod{47}$

$2^{18} \equiv 25 = 5^2 \pmod{47}$

2	3	5	7	
1	0	0	0	1
0	1	0	1	8
0	0	0	1	12
0	0	2	0	18

Calcul d'indices

$28 = 2^x \pmod{47}, \quad x = ?$

Soit la base de factorisation {2, 3, 5, 7}

Soit (p = 47)

Phase recherche de relations

$2^1 \equiv 2 \pmod{47}$

~~$2^7 \equiv 34 = 2 \cdot 17 \pmod{47}$~~

$2^8 \equiv 21 = 3 \cdot 7 \pmod{47}$

$2^{12} \equiv 7 \pmod{47}$

$2^{18} \equiv 25 = 5^2 \pmod{47}$

2	3	5	7	
1	0	0	0	1
0	1	0	1	8
0	0	0	1	12
0	0	2	0	18

Calcul d'indices

$28 = 2^x \pmod{47}, \quad x = ?$

Soit la base de factorisation {2, 3, 5, 7}

Soit (p = 47)

Phase recherche de relations

$2^1 \equiv 2 \pmod{47}$

~~$2^7 \equiv 34 = 2 \cdot 17 \pmod{47}$~~

$2^8 \equiv 21 = 3 \cdot 7 \pmod{47}$

$2^{12} \equiv 7 \pmod{47}$

$2^{18} \equiv 25 = 5^2 \pmod{47}$

2	3	5	7	
1	0	0	0	1
0	1	0	1	8
0	0	0	1	12
0	0	2	0	18

Calcul d'indices

$28 = 2^x \pmod{47}, \quad x = ?$

Soit la base de factorisation {2, 3, 5, 7}

Soit (p = 47)

Phase algèbre linéaire

2	3	5	7	
1	0	0	0	1
0	1	0	1	8
0	0	0	1	12
0	0	2	0	18

Calcul d'indices

$28 = 2^x \pmod{47}, \quad x = ?$

Soit la base de factorisation {2, 3, 5, 7}

Soit (p = 47)

Phase algèbre linéaire

2	3	5	7	
1	0	0	0	1	
0	1	0	1	8	$L_2 = L_2 - L_3$
0	0	0	1	12	
0	0	2	0	18	$L_4 = L_4 / 2$

Calcul d'indices

$28 = 2^x \pmod{47}, \quad x = ?$

Soit la base de factorisation {2, 3, 5, 7}

Soit (p = 47)

Phase algèbre linéaire

2	3	5	7	
1	0	0	0	1
0	1	0	1	8
0	0	0	1	12
0	0	2	0	18

$L_2 = L_2 - L_3$

$L_4 = L_4 / 2$

2	3	5	7	
1	0	0	0	1
0	1	0	0	-4=42
0	0	0	1	12
0	0	1	0	9

Calcul d'indices

$28 = 2^x \pmod{47}, \quad x = ?$

Soit la base de factorisation {2, 3, 5, 7}

Soit (p = 47)

Phase algèbre linéaire

2	3	5	7	
1	0	0	0	1
0	1	0	1	8
0	0	0	1	12
0	0	2	0	18

2	3	5	7	
1	0	0	0	1
0	1	0	0	-4=42
0	0	0	1	12
0	0	1	0	9

$\log_2(2) = 1; \quad \log_2(3) = 42; \quad \log_2(5) = 9; \quad \log_2(7) = 12;$

Calcul d'indices

$28 = 2^x \pmod{47}, \quad x = ?$

Soit la base de factorisation {2, 3, 5, 7}

Soit (p = 47)

$\log_2(2) = 1; \quad \log_2(3) = 42; \quad \log_2(5) = 9; \quad \log_2(7) = 12;$

Calcul d'indices

$28 = 2^x \pmod{47}, \quad x = ?$

Soit la base de factorisation {2, 3, 5, 7}

Soit (p = 47)

$\log_2(2) = 1; \quad \log_2(3) = 42; \quad \log_2(5) = 9; \quad \log_2(7) = 12;$

$\log_2(28) = \log_2(2 \cdot 2 \cdot 7)$

Calcul d'indices

$28 = 2^x \pmod{47}, \quad x = ?$

Soit la base de factorisation {2, 3, 5, 7}

Soit (p = 47)

$\log_2(2) = 1; \quad \log_2(3) = 42; \quad \log_2(5) = 9; \quad \log_2(7) = 12;$

$\log_2(28) = \log_2(2 \cdot 2 \cdot 7) = 2 \cdot \log_2(2) + \log_2(7) = 14$

Calcul d'indices $28 = 2^x \pmod{47}, \quad x = ?$

Soit la base de factorisation {2, 3, 5, 7}

Soit (p = 47)

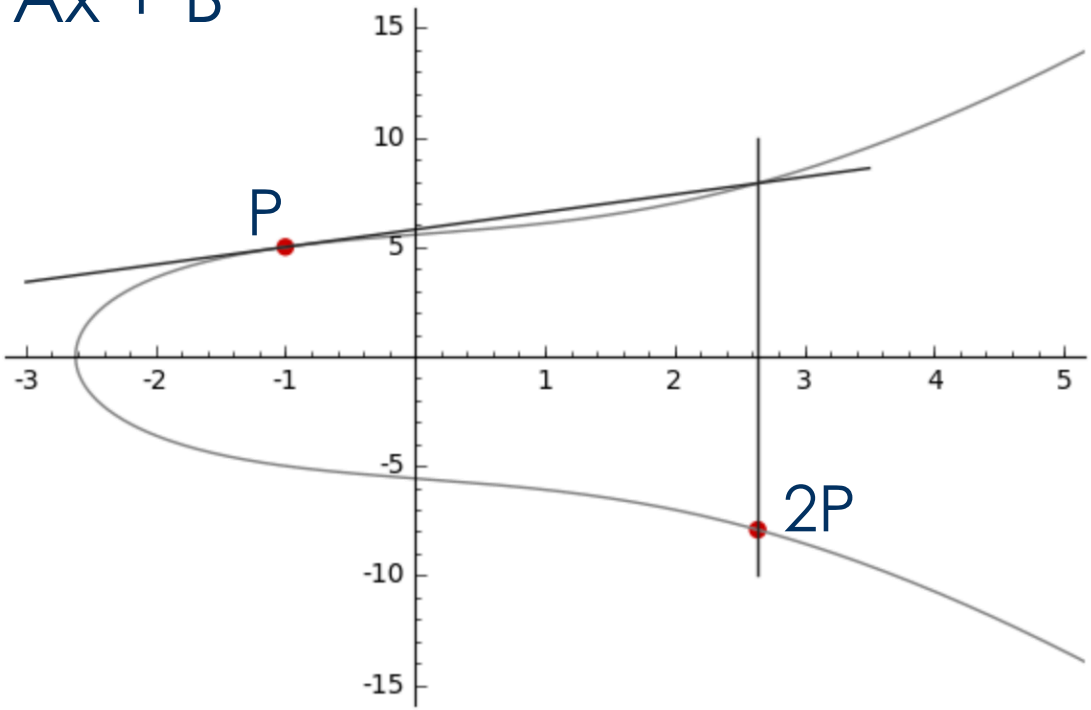
$\log_2(2) = 1; \quad \log_2(3) = 42; \quad \log_2(5) = 9; \quad \log_2(7) = 12;$

$\log_2(28) = \log_2(2 \cdot 2 \cdot 7) = 2 \cdot \log_2(2) + \log_2(7) = 14$

Calcul d'indices Q = xP, x = ?

pour les systèmes à base de courbes elliptiques ?

$E : y^2 = x^3 + Ax + B$



Calcul d'indices

pour les systèmes à base de courbes elliptiques ?

Calcul d'indices

pour les systèmes à base de courbes elliptiques ?

- $\log(P_1 + P_2 + P_3) = \log(P_1) + \log(P_2) + \log(P_3)$ 
- Points "premiers" ?
- Décomposition de points ?

Calcul d'indices

pour les systèmes à base de courbes elliptiques ?

- $\log(P_1 + P_2 + P_3) = \log(P_1) + \log(P_2) + \log(P_3)$ 
- Points "premiers" ?
- Décomposition de points ?

Calcul d'indices

Semaev (2004)

Si

$$(X_1X_2 + X_1X_3 + X_2X_3)^2 + X_1X_2X_3 + 1 = 0$$

Alors

$$P_3 = P_2 + P_1$$

où $P_1 = (X_1, Y_1)$, $P_2 = (X_2, Y_2)$ et $P_3 = (X_3, Y_3)$

Gaudry et Diem (2008 - 2009)

Courbes $E(F_{2^n})$

Exemple pour n = 5

P(X,Y) où

$X = x^4 + x^3 + x^2 + 1$

$Y = x^3 + 1$

Addition sur F_2^n

$$X = x^4 + x^3 + x^2 + 1$$
$$Y = x^3 + 1$$

Addition sur F_2^n

$$X = x^4 + x^3 + x^2 + 1$$

$$Y = x^3 + 1$$

Addition sur F_2^n

$X = x^4 + x^3 + x^2 + 1$

$Y = x^3 + 1$

$$\begin{array}{r} 1\,1\,1\,0\,1 \\ +\,0\,1\,0\,0\,1 \\ \hline 1\,0\,1\,0\,0 \end{array}$$

Addition sur F_2^n

$$X = x^4 + x^3 + x^2 + 1$$
$$Y = x^3 + 1$$

$$\begin{array}{r} 1\,1\,1\,0\,1 \\ +\,0\,1\,0\,0\,1 \\ \hline 1\,0\,1\,0\,0 \end{array}$$

XOR

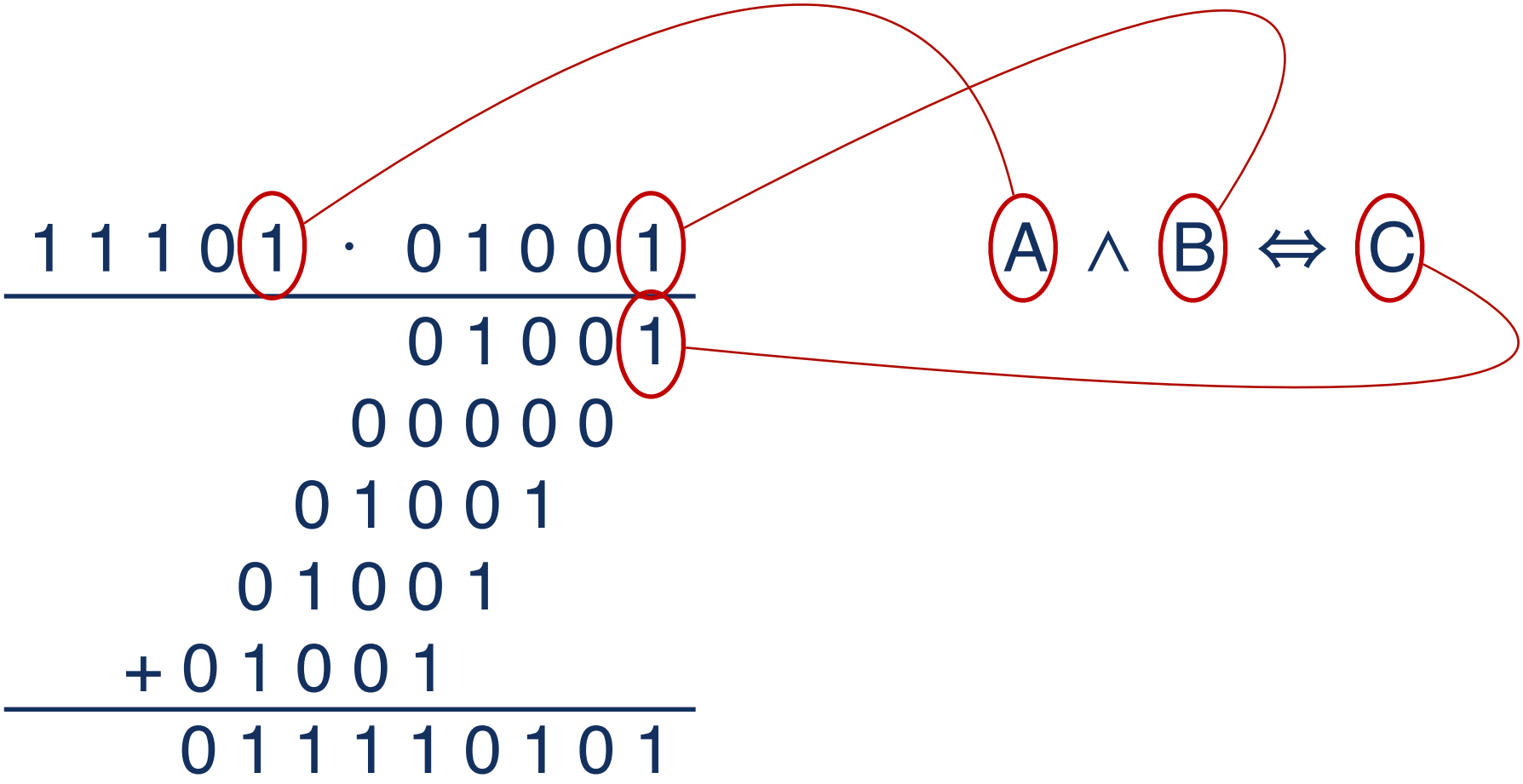
Multiplication sur F_{2^n}

$$
\begin{array}{rcl}
1\,1\,1\,0\,1 & \cdot & 0\,1\,0\,0\,1 \\
\hline
 & & 0\,1\,0\,0\,1 \\
 & & 0\,0\,0\,0\,0 \\
 & & 0\,1\,0\,0\,1 \\
 & & 0\,1\,0\,0\,1 \\
 & & 0\,1\,0\,0\,1 \\
\hline
 & & 0\,1\,1\,1\,1\,0\,1\,0\,1
\end{array}
$$

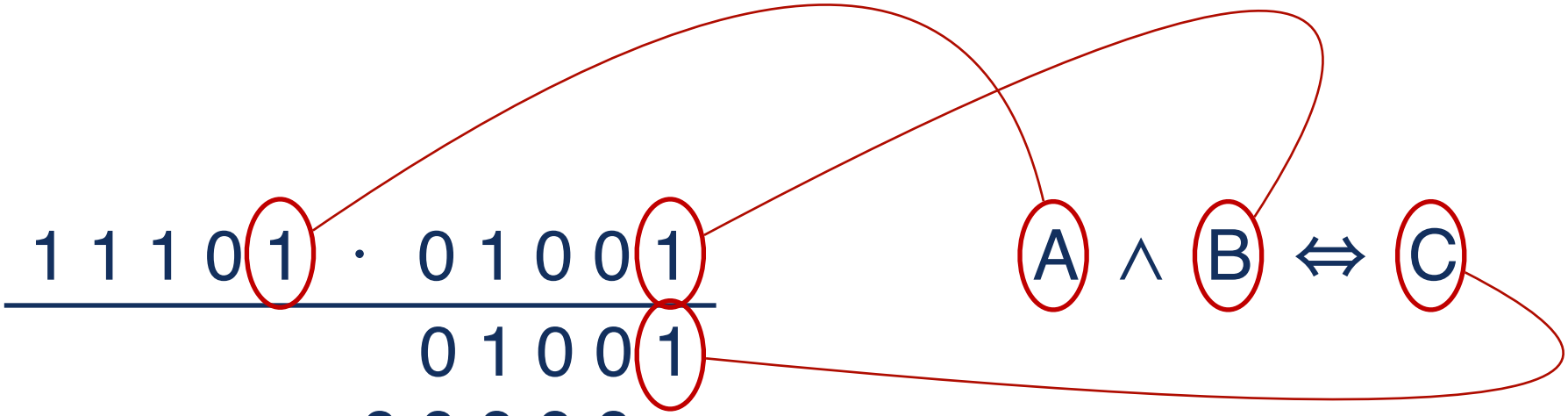
Multiplication sur F_{2^n}

$$
\begin{array}{rcl}
1\,1\,1\,0\,1 & \cdot & 0\,1\,0\,0\,1 \\
\hline
 & & 0\,1\,0\,0\,1 \\
 & & 0\,0\,0\,0\,0 \\
 & & 0\,1\,0\,0\,1 \\
 & & 0\,1\,0\,0\,1 \\
 & & +\,0\,1\,0\,0\,1 \\
\hline
 & & 0\,1\,1\,1\,1\,0\,1\,0\,1
\end{array}
$$

Multiplication sur F_{2^n}



Multiplication sur F_{2^n}



$$
\begin{array}{rcl}
1\,1\,1\,0\,1 & \cdot & 0\,1\,0\,0\,1 \\
\hline
 & & 0\,1\,0\,0\,1 \\
 & & 0\,0\,0\,0\,0 \\
 & & 0\,1\,0\,0\,1 \\
 & & 0\,1\,0\,0\,1 \\
 & + & 0\,1\,0\,0\,1 \\
\hline
 & & 0\,1\,1\,1\,1\,0\,1\,0\,1
\end{array}
$$

$A \wedge B \Leftrightarrow C$

...

$\neg C \vee A$

$\neg C \vee B$

$\neg A \vee \neg B \vee C$

Modèle SAT

$$(X_1X_2 + X_1X_3 + X_2X_3)^2 + X_1X_2X_3 + 1 = 0$$

Entrée
X_3 (11101)

Sortie
X_1 (01000)
X_2 (10110)

Modèle SAT

$\neg 1 \vee 2$
$\neg 1 \vee 3$
$\neg 2 \vee \neg 3 \vee 1$
$\neg 4 \vee 5$
$\neg 4 \vee 6$
$\neg 5 \vee \neg 6 \vee 4$
$\neg 7 \vee 8$
$\neg 7 \vee 9$
$\neg 8 \vee \neg 9 \vee 7$

CNF

$2 \oplus \neg 5$
$1 \oplus 3 \oplus \neg 6$
$1 \oplus 4 \oplus 2 \oplus \neg 7$
$1 \oplus 2 \oplus 3 \oplus \neg 4$
$1 \oplus 2 \oplus \neg 8$
$5 \oplus \neg 9$

XOR - SAT

Modèle SAT

$\neg 1 \vee 2$
$\neg 1 \vee 3$
$\neg 2 \vee \neg 3 \vee 1$
$\neg 4 \vee 5$
$\neg 4 \vee 6$
$\neg 5 \vee \neg 6 \vee 4$
$\neg 7 \vee 8$
$\neg 7 \vee 9$
$\neg 8 \vee \neg 9 \vee 7$

HORN - SAT

$2 \oplus \neg 5$
$1 \oplus 3 \oplus \neg 6$
$1 \oplus 4 \oplus 2 \oplus \neg 7$
$1 \oplus 2 \oplus 3 \oplus \neg 4$
$1 \oplus 2 \oplus \neg 8$
$5 \oplus \neg 9$

XOR - SAT

Modèle SAT

$$(X_1X_2 + X_1X_3 + X_2X_3)^2 + X_1X_2X_3 + 1 = 0$$

Entrée
X_3 (11101)

Sortie
X_1 (01000)
X_2 (10110)

Calcul d'indices

$28 = 2^x \pmod{47}, \quad x = ?$

Soit la base de factorisation {2, 3, 5, 7}

Soit (p = 47)

Phase recherche de relations

$2^1 \equiv 2 \pmod{47}$

~~$2^7 \equiv 34 = 2 \cdot 17 \pmod{47}$~~

$2^8 \equiv 21 = 3 \cdot 7 \pmod{47}$

$2^{12} \equiv 7 \pmod{47}$

$2^{18} \equiv 25 = 5^2 \pmod{47}$

2	3	5	7	
1	0	0	0	1
0	1	0	1	8
0	0	0	1	12
0	0	2	0	18

Calcul d'indices

$28 = 2^x \pmod{47}, \quad x = ?$

Soit la base de factorisation {2, 3, 5, 7}

Soit (p = 47)

$\log_2(2) = 1; \quad \log_2(3) = 42; \quad \log_2(5) = 9; \quad \log_2(7) = 12;$

Calcul d'indices $28 = 2^x \pmod{47}, \quad x = ?$

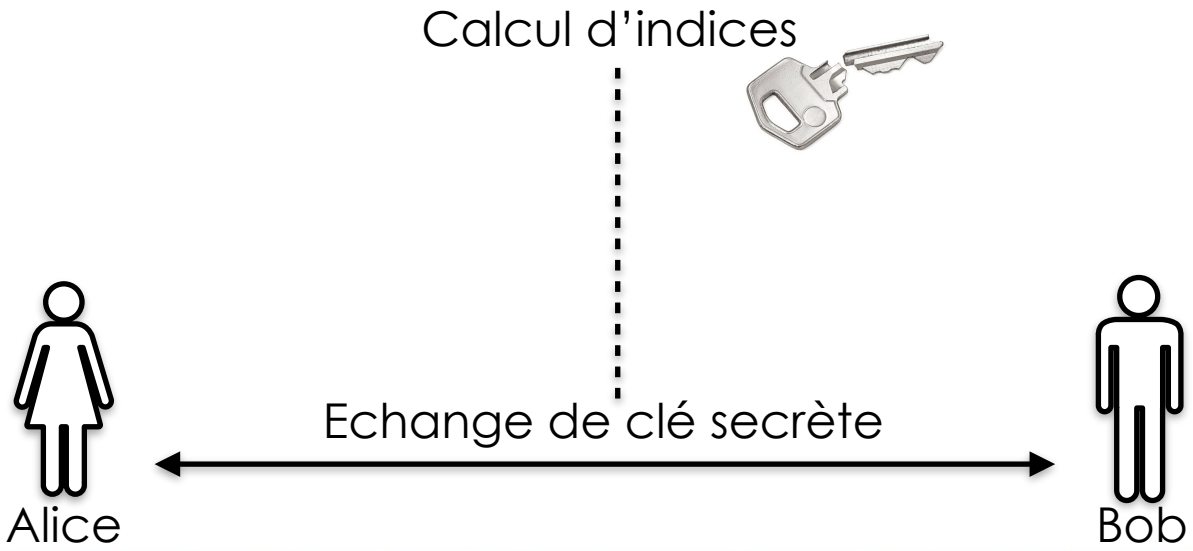
Soit la base de factorisation {2, 3, 5, 7}

Soit (p = 47)

$\log_2(2) = 1; \quad \log_2(3) = 42; \quad \log_2(5) = 9; \quad \log_2(7) = 12;$

$\log_2(28) = \log_2(2 \cdot 2 \cdot 7) = 2 \cdot \log_2(2) + \log_2(7) = 14$

Le problème du logarithme discret



Trouver X tel que

$$h = g^x \pmod p$$

ou

ECC: $Q = xP \pmod p$