Agence nationale de la sécurité
des systèmes d'information

Match Box Meet-in-the-Middle Attack against KATAN

Thomas Fuhr and *Brice Minaud*

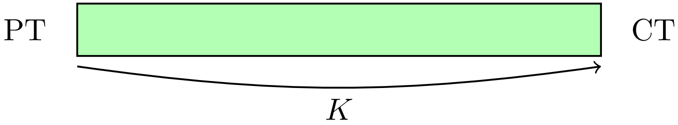
ANSSI, France

FSE, March 3-5 2014

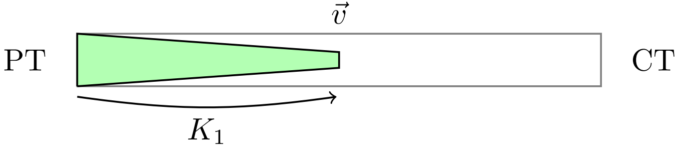
Plan

Match Box

Meet-in-the-Middle Attack

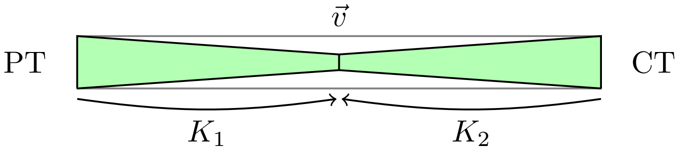


Meet-in-the-Middle Attack



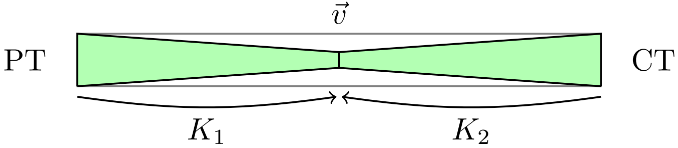
Knowledge of a portion K_1 of the key allows to compute a part $\vec{v}$ of the internal state at some intermediate round.

Meet-in-the-Middle Attack



Assume this same $\vec{v}$ can be computed from the ciphertext using K_2. Then a meet-in-the-middle attack is possible.

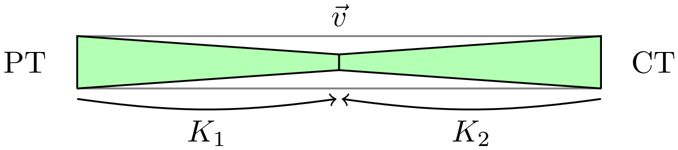
Meet-in-the-Middle Attack



Assume this same $\vec{v}$ can be computed from the ciphertext using K_2. Then a meet-in-the-middle attack is possible.

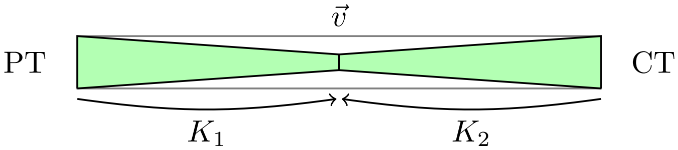
This generally assumes a simple key schedule. Lightweight ciphers are prime targets.

Meet-in-the-Middle Attack



1. Guess $K_\cap = K_1 \cap K_2$.
   - For each $K_1' = K_1 - K_\cap$, compute $\vec{v}$.
     Store $\vec{v} \to \{K_1'\}$ in a table T.
   - For each $K_2' = K_2 - K_\cap$, compute $\vec{v}$.
     Retrieve K_1''s that lead to the same $\vec{v}$ from T. Each of these K_1''s, merged with K_2', yields a candidate master key.
2. Test candidate master keys against a few plaintext/ciphertext pairs.

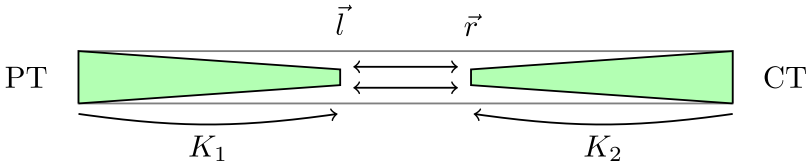
Meet-in-the-Middle Attack



1. Guess $K_\cap = K_1 \cap K_2$.
   - For each $K_1' = K_1 - K_\cap$, compute $\vec{v}$.
     Store $\vec{v} \to \{K_1'\}$ in a table T.
   - For each $K_2' = K_2 - K_\cap$, compute $\vec{v}$.
     Retrieve K_1''s that lead to the same $\vec{v}$ from T. Each of these K_1''s, merged with K_2', yields a candidate master key.
2. Test candidate master keys against a few plaintext/ciphertext pairs.

Benefit : complexity is $|K_\cap| \times (|K_1'| + |K_2'|)$ instead of $|K_\cap| \times (|K_1'| \times |K_2'|)$.

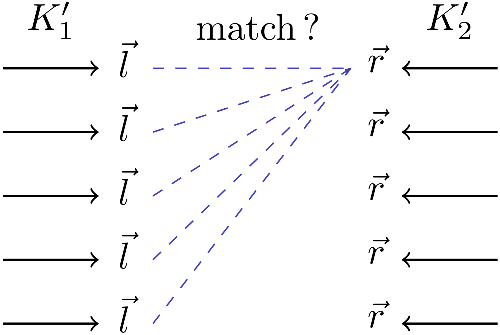
Sieve-in-the-Middle Framework



Now we compute a distinct $\vec{l}$ from the left and $\vec{r}$ from the right. Compatibility is expressed by some relation $\mathcal{R}(\vec{l}, \vec{r})$.

Introduced by Canteaut, Naya-Plasencia and Vayssière at CRYPTO 2013.

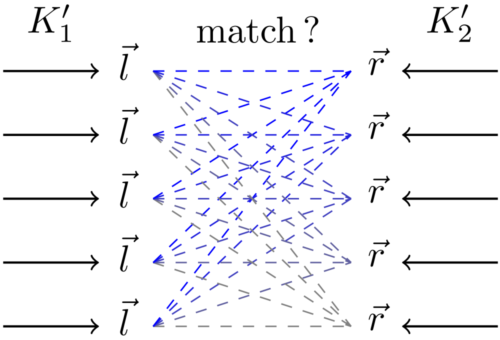
Matching problem



Problem : testing the relation $\mathcal{R}$.

$$K_1 = K_\cap \oplus K_1'$$
$$K_2 = K_\cap \oplus K_2'$$
$$K = K_\cap \oplus K_1' \oplus K_2'$$

Matching problem

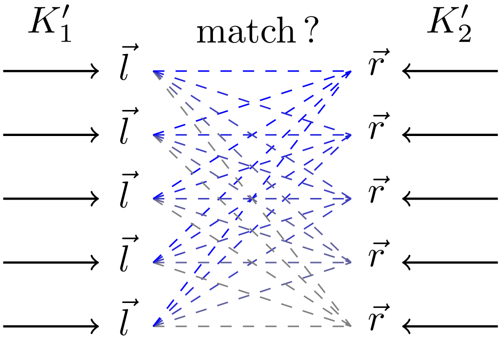


Problem : testing the relation $\mathcal{R}$.

$K_\cap \times K'_1 \times K'_2 =$ entire key $=$ brute force.

$$K_1 = K_\cap \oplus K'_1$$
$$K_2 = K_\cap \oplus K'_2$$
$$K = K_\cap \oplus K'_1 \oplus K'_2$$

Matching problem

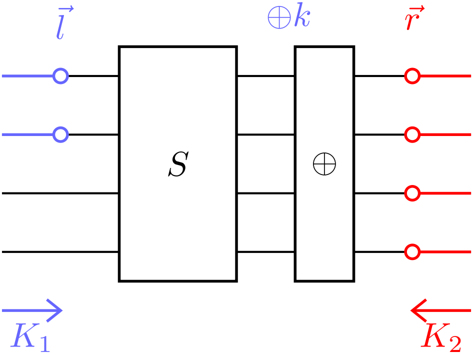


Problem : testing the relation $\mathcal{R}$.
$K_\cap \times K_1' \times K_2' =$ entire key $=$ brute force.

Solution : Precomputation of compatibilities outside the loop on $K_\cap$.

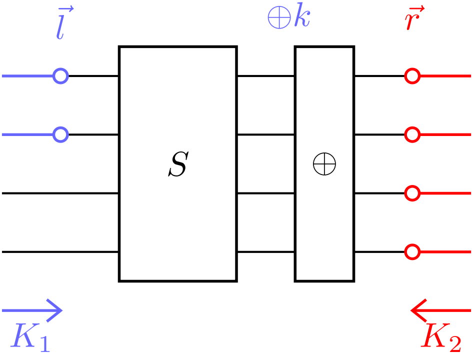
$$K_1 = K_\cap \oplus K_1'$$
$$K_2 = K_\cap \oplus K_2'$$
$$K = K_\cap \oplus K_1' \oplus K_2'$$

Example



$$K_1 = K_\cap \oplus K_1'$$
$$K_2 = K_\cap \oplus K_2'$$
$$K = K_\cap \oplus K_1' \oplus K_2'$$

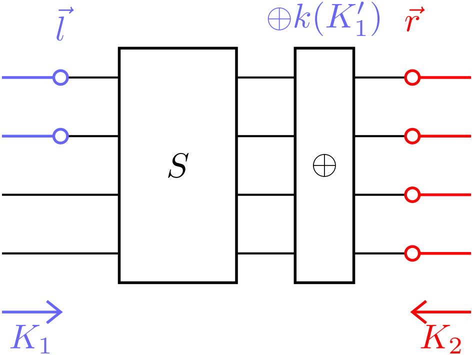
Example



Assuming the key schedule is linear, $K = K_2 \oplus K_1'$. Without loss of generality, we can assume k depends only on K_1'.

$$K_1 = K_\cap \oplus K_1'$$
$$K_2 = K_\cap \oplus K_2'$$
$$K = K_\cap \oplus K_1' \oplus K_2'$$

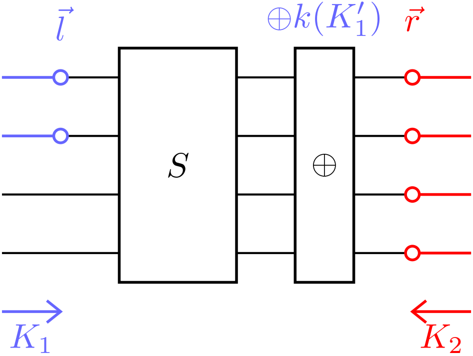
Example



Assuming the key schedule is linear, $K = K_2 \oplus K_1'$. Without loss of generality, we can assume k depends only on K_1'.

Compatibility : $\mathcal{R}(\vec{l}, \vec{r}, K_1')$ iff $S^{-1}\left(\vec{r} \oplus k(K_1')\right)_{\restriction\{0,1\}} = \vec{l}$

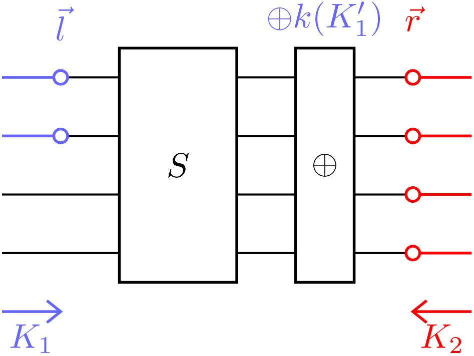
Match box



Match box : $(K'_1 \mapsto \vec{l}) \mapsto (\vec{r} \mapsto \{K'_1 : \mathcal{R}(\vec{l}, \vec{r}, K'_1)\})$

$$K_1 = K_\cap \oplus K'_1$$
$$K_2 = K_\cap \oplus K'_2$$
$$K = K_\cap \oplus K'_1 \oplus K'_2$$

Match box



Match box : $(K_1' \mapsto \vec{l}) \mapsto (\vec{r} \mapsto \{K_1' : \mathcal{R}(\vec{l}, \vec{r}, K_1')\})$

Limited by the size of the table : $2^{|\vec{l}|^{|K_1'|}+|\vec{r}|+|K_1'|}$

$$K_1 = K_\cap \oplus K_1'$$
$$K_2 = K_\cap \oplus K_2'$$
$$K = K_\cap \oplus K_1' \oplus K_2'$$

Cryptanalysis of KATAN

KATAN

Block cipher by De Cannière, Dunkelman, Knežević, CHES 2009.

Ultralightweight. Barely more surface area than what is required to store the state and key.

Based on Non-Linear Shift Feedback Registers. 254 rounds.

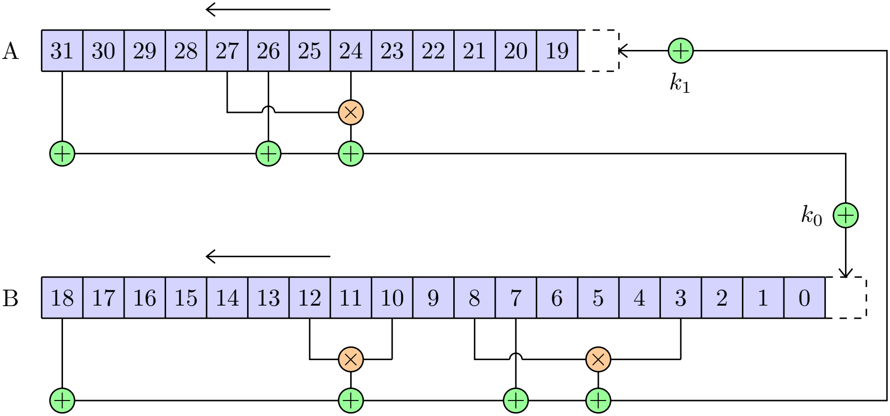
Accomodates three block sizes : 32, 48 or 64 bits.
80-bit key.

Previous work on KATAN

KATAN32

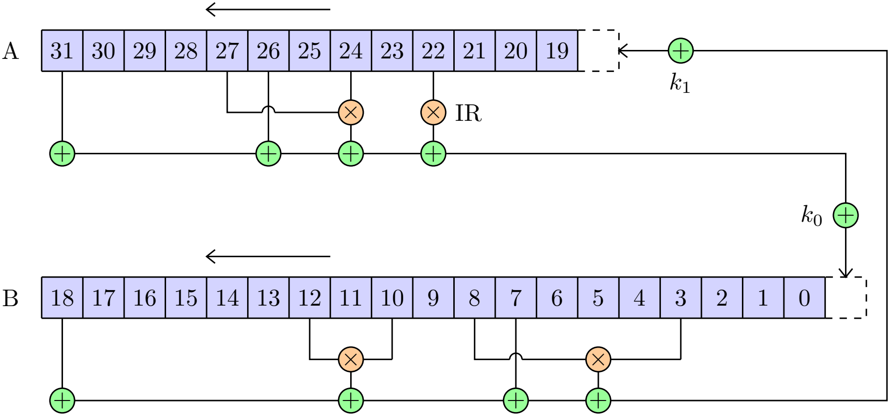
- **Conditional differential :** 78 rounds
  by Knellwolf, Meier, Naya-Plasencia, ASIACRYPT 2010.
- **Exhaustive differential :** 115 rounds
  by Albrecht and Leander, SAC 2012.
- **Meet-in-middle :** 110 rounds
  by Isobe and Shibutani, SAC 2013.

KATAN32



80-bit key loaded into an LFSR $\rightarrow k_0, k_1$ every round.

KATAN32



80-bit key loaded into an LFSR $\rightarrow$ k_0, k_1 every round.
Irregular rounds scheduled by another LFSR.

Formal description of KATAN32

Definition

Bit a_i enters register A at round i.
Bit b_i enters register B at round i.

$\Longrightarrow$ At round n :
A contains $(a_{n-12}, \ldots, a_n)$, B contains $(b_{n-18}, \ldots, b_n)$.

Formal description of KATAN32

Definition

Bit a_i enters register A at round i.
Bit b_i enters register B at round i.

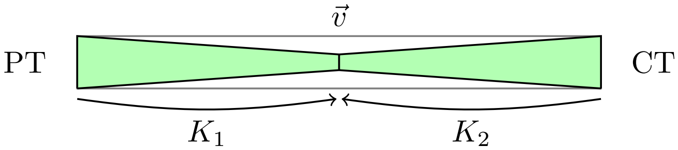
$\implies$ At round n :
A contains $(a_{n-12}, \dots, a_n)$, B contains $(b_{n-18}, \dots, b_n)$.

Plaintext = $(a_{-13}, \dots, a_{-1}, b_{-19}, \dots, b_{-1})$.

$$\text{Encryption} \begin{cases} a_n = b_{n-19} \oplus b_{n-8} \oplus b_{n-11} \cdot b_{n-13} \oplus b_{n-4} \cdot b_{n-9} \oplus rk_{2n+1} \\ b_n = a_{n-13} \oplus a_{n-8} \oplus c_n \cdot a_{n-4} \oplus a_{n-6} \cdot a_{n-9} \oplus rk_{2n} \end{cases}$$

Ciphertext = $(a_{241}, \dots, a_{253}, b_{235}, \dots, b_{253})$.

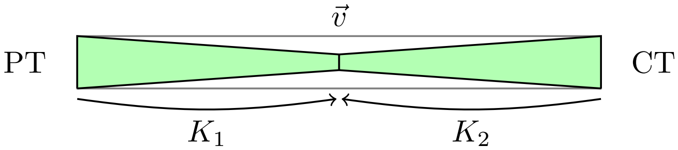
Meet-in-the-Middle Attack on KATAN



Small extras :

- **Simultaneous matching :** on several plaintext/ciphertext pairs.
- **Indirect matching** : removes key bits whose contribution is linear.

Meet-in-the-Middle Attack on KATAN



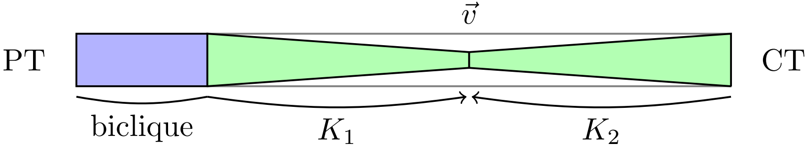
Small extras :

- **Simultaneous matching :** on several plaintext/ciphertext pairs.
- **Indirect matching** : removes key bits whose contribution is linear.

Result : attack on 121 rounds of KATAN32.

K_1 : 75 bits, K_2 : 75 bits, $K_\cap$: 70 bits
forward : 69 rounds, backward : 52 rounds
4 known plaintexts, complexity $2^{77.5}$.

Meet-in-the-Middle Attack on KATAN

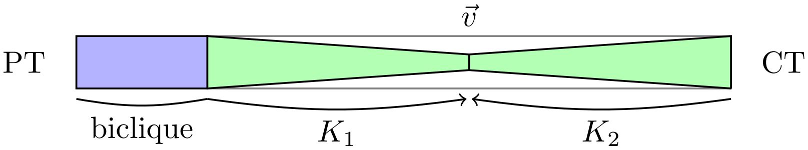


Addition of a biclique.

Originally introduced to attack SKEIN and AES [BKR11].

Makes it possible to extend a meet-in-the-middle attack. Either an accelerated key search, or a classical attack (we use the latter).

Meet-in-the-Middle Attack on KATAN



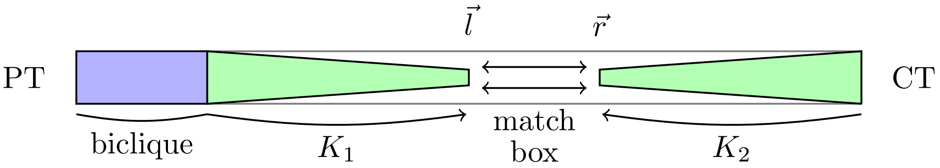
Addition of a biclique.

Originally introduced to attack SKEIN and AES [BKR11].

Makes it possible to extend a meet-in-the-middle attack. Either an accelerated key search, or a classical attack (we use the latter).

Result : attack on 131 rounds of KATAN32.
Chosen plaintexts, low data requirements.

Meet-in-the-middle attack on KATAN



Addition of a « match box ».

Match Box on KATAN

Meeting in the middle at b_{62} :

$$b_{62} = x_0 \oplus b_{68} \cdot b_{70}, \qquad x_0 = a_{81} \oplus b_{73} \oplus b_{72} \cdot b_{77} \oplus rk_{163}$$

$$b_{68} = x_1 \oplus rk_{175}, \qquad x_1 = a_{87} \oplus b_{89} \oplus b_{76} \cdot b_{74} \oplus b_{83} \cdot b_{78}$$

$$b_{70} = x_2 \oplus rk_{179}, \qquad x_2 = a_{89} \oplus b_{91} \oplus b_{78} \cdot b_{76} \oplus b_{85} \cdot b_{80}$$

Match Box on KATAN

Meeting in the middle at b_{62} :

$$b_{62} = x_0 \oplus b_{68} \cdot b_{70}, \qquad x_0 = a_{81} \oplus b_{73} \oplus b_{72} \cdot b_{77} \oplus rk_{163}$$

$$b_{68} = x_1 \oplus rk_{175}, \qquad x_1 = a_{87} \oplus b_{89} \oplus b_{76} \cdot b_{74} \oplus b_{83} \cdot b_{78}$$

$$b_{70} = x_2 \oplus rk_{179}, \qquad x_2 = a_{89} \oplus b_{91} \oplus b_{78} \cdot b_{76} \oplus b_{85} \cdot b_{80}$$

Let us decompose $rk_n = rk_n^2 \oplus rk_n^{1'}$ along $K_2 \oplus K_1'$.

$$\vec{l} \left\{ l_0 = b_{62} \right. \qquad \vec{r} \begin{cases} r_0 = x_0 \\ r_1 = x_1 \oplus rk_{175}^2 \\ r_2 = x_2 \oplus rk_{179}^2 \end{cases}$$

Compatibility $\mathcal{R}(\vec{l}, \vec{r}, K_1')$:

$$l_0 = r_0 \oplus (r_1 \oplus rk_{175}^{1'}) \cdot (r_2 \oplus rk_{179}^{1'})$$

Match Box on KATAN

$$\vec{l}\left\{ l_0 = b_{62} \right. \qquad\qquad \vec{r}\begin{cases} r_0 = x_0 \\ r_1 = x_1 \oplus rk^2_{175} \\ r_2 = x_2 \oplus rk^2_{179} \end{cases}$$

Compatibility $\mathcal{R}(\vec{l}, \vec{r}, K'_1)$:

$$l_0 = r_0 \oplus (r_1 \oplus rk^{1'}_{175}) \cdot (r_2 \oplus rk^{1'}_{179})$$

Benefit :
We no longer need to know $k^{1'}_{175}$ and $rk^{1'}_{179}$ from the right.
$\Rightarrow$ K_2 shrinks by 2.
$\Rightarrow$ We can add two brand new round keys to K_2 to add one more round to the attack.

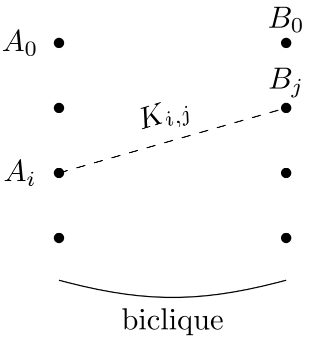
Summary of results

	Rounds	Model	Data	Memory	Time	Reference
K32	**78**	CP	2^{22}	–	2^{22}	[KMN10]
	115	CP	2^{32}	–	2^{79}	[AL12]
	110	KP	2^{7}	2^{75}	2^{77}	[IS13]
	121	KP	2^{2}	–	$2^{77.5}$	Base
	131	CP	2^{7}	–	$2^{77.5}$	Biclique
	153	CP	2^{5}	2^{76}	$2^{78.5}$	M. box
K48	**70**	CP	2^{34}	–	2^{34}	[KMN10]
	100	KP	2^{7}	2^{78}	2^{78}	[IS13]
	110	KP	2^{2}	–	$2^{77.5}$	Base
	114	CP	2^{6}	–	$2^{77.5}$	Biclique
	129	CP	2^{5}	2^{76}	$2^{78.5}$	M. box
K64	**68**	CP	2^{35}	–	2^{35}	[KMN10]
	94	KP	2^{7}	$2^{77.5}$	$2^{77.5}$	[IS13]
	102	KP	2^{2}	–	$2^{77.5}$	Base
	107	CP	2^{7}	–	$2^{77.5}$	Biclique
	119	CP	2^{5}	2^{74}	$2^{78.5}$	M. box

Thank you for your attention.

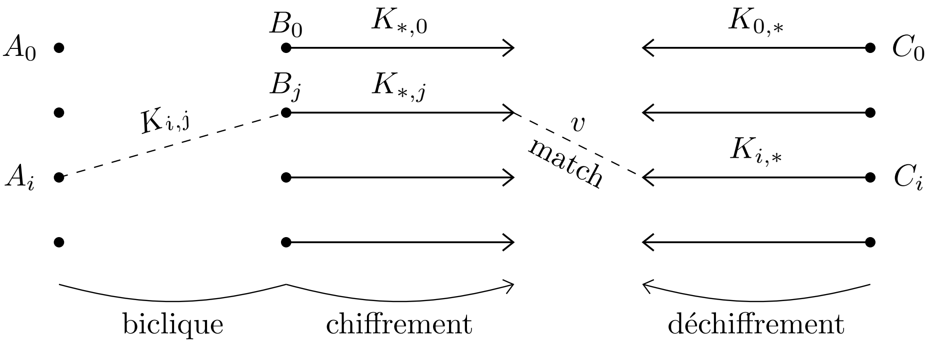
Questions ?

Biclique



Biclique : $\forall i, j, \quad \mathrm{Enc}^{0\to b}_{\mathrm{K_{i,j}}}(A_i) = B_j$.

Biclique



Biclique : $\forall i, j, \quad \mathrm{Enc}^{0\to b}_{K_{i,j}}(A_i) = B_j$.

$K_{i,*}$ = information on the key common to $K_{i,j}$ $\forall j$.
$K_{*,j}$ = information on the key common to $K_{i,j}$ $\forall i$.
Compatibility : v can be computed from $(B_j, K_{*,j})$, and also $(C_i, K_{i,*})$.