Parity (XOR) Reasoning for the Index Calculus Attack

Monika Trimoska

Sorina Ionica

Gilles Dequen

MIS Laboratory, University of Picardie Jules Verne

CP 2020

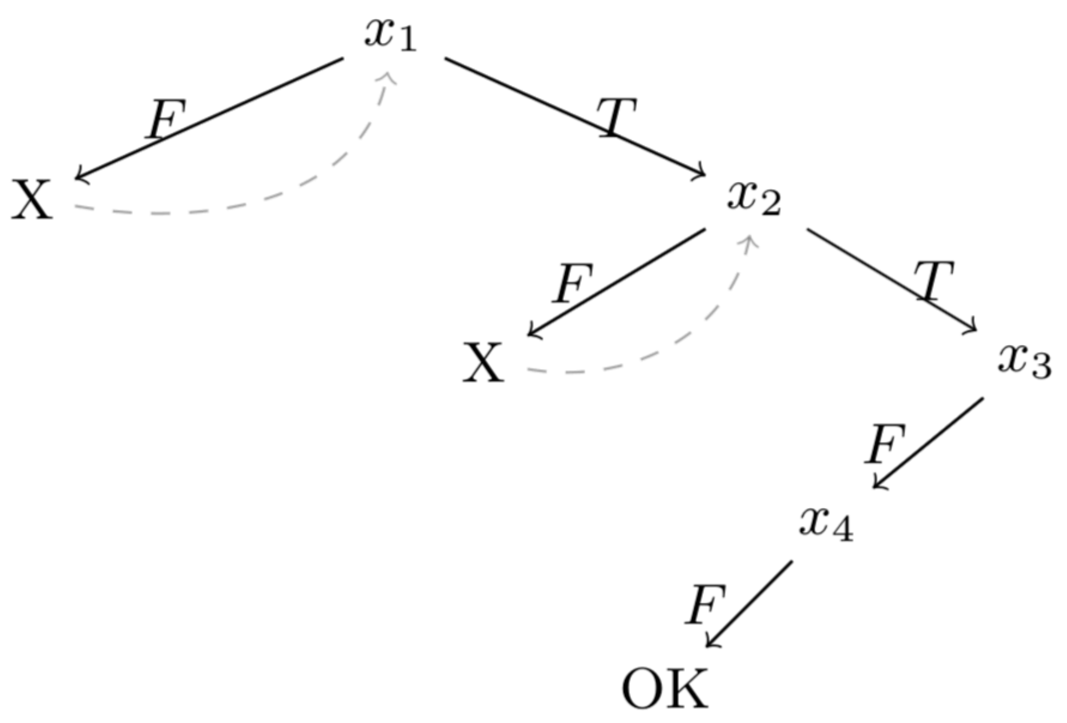
Parity (XOR) Reasoning for the IC Attack

XOR reasoning in SAT solvers

→ Gaussian Elimination

WDSat solver

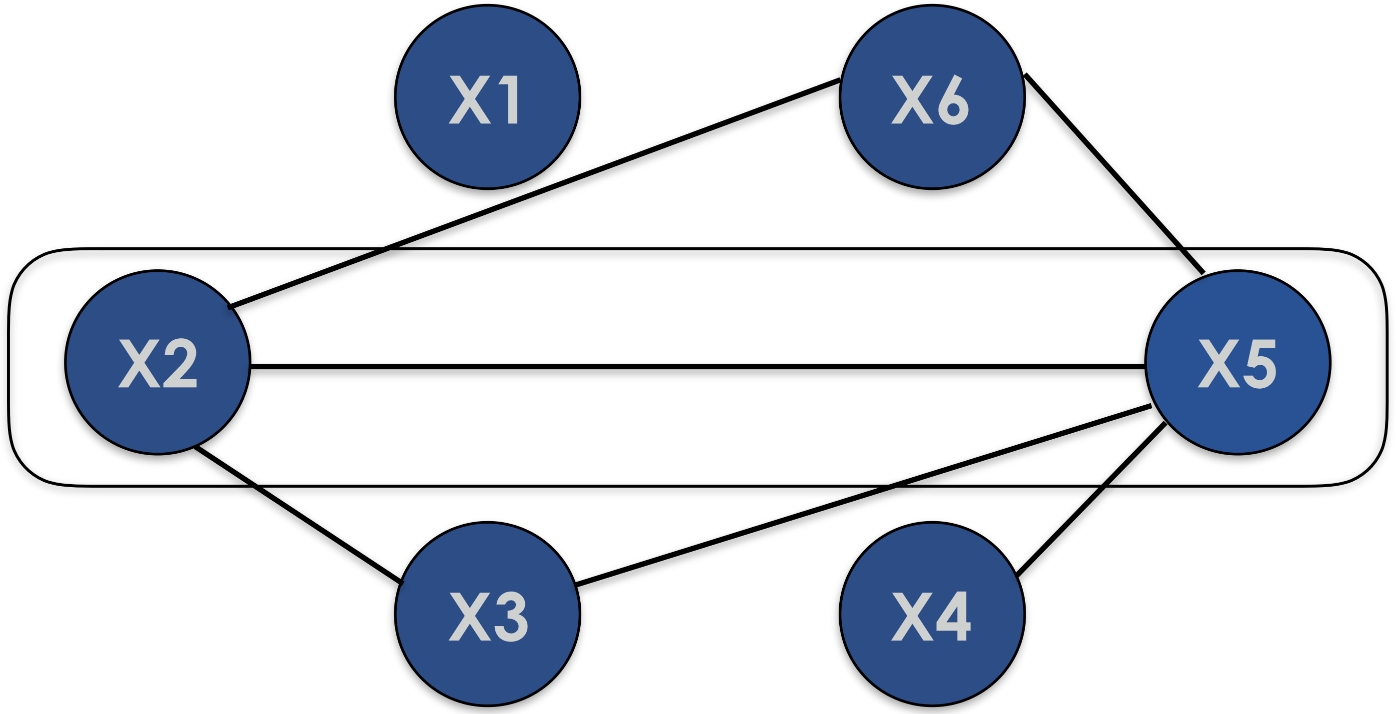
DPLL-based



- CNF module
- XORSET module
- XORGAUSS module

Parity (XOR) Reasoning for the IC Attack

Preprocessing technique based on the Minimal Vertex Cover problem



Parity (XOR) Reasoning for the IC Attack

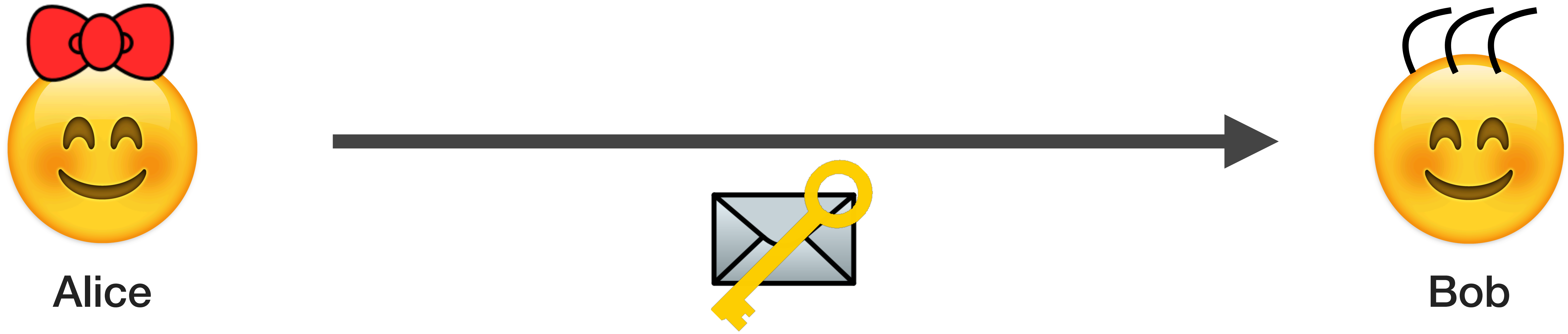
Index calculus attack on binary elliptic curves

51 variables, 52 equations

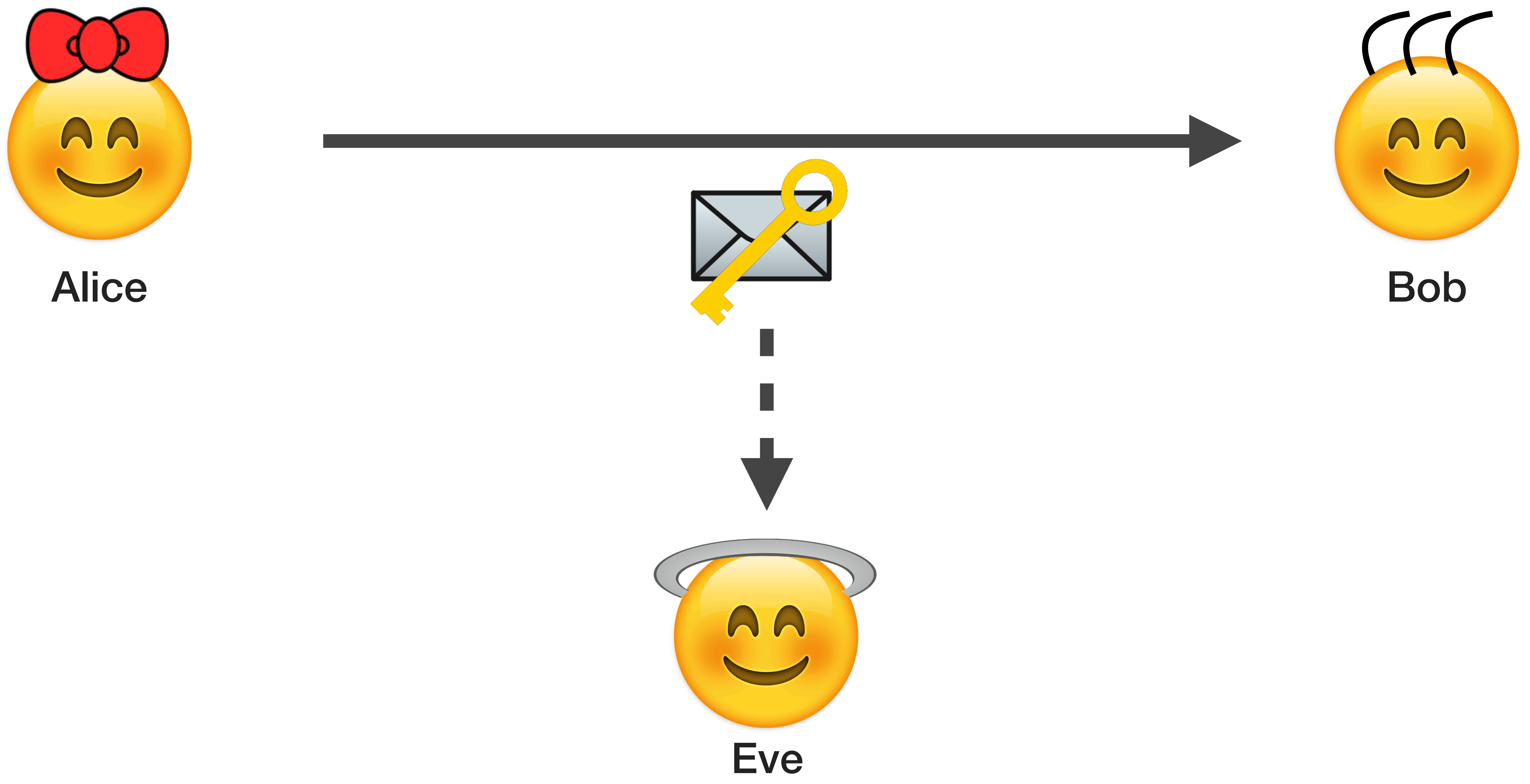
Solving approach	SAT		UNSAT	
	Runtime (s)	#Conflicts	Runtime (s)	#Conflicts
Gröbner bases	229.3	*N/A*	229.4	*N/A*
MiniSat	239.7	1840190	517.0	3433304
Glucose	189.2	1527158	274.8	2056575
MapleLCMDistChronoBT	655.1	4035131	918.7	5378945
CaDiCaL	43.6	254194	141.3	629869
CryptoMiniSat	331.8	1791188	707.9	3416526
WDSat	**0.6**	**48438**	**3.8**	**255698**

Technical presentation

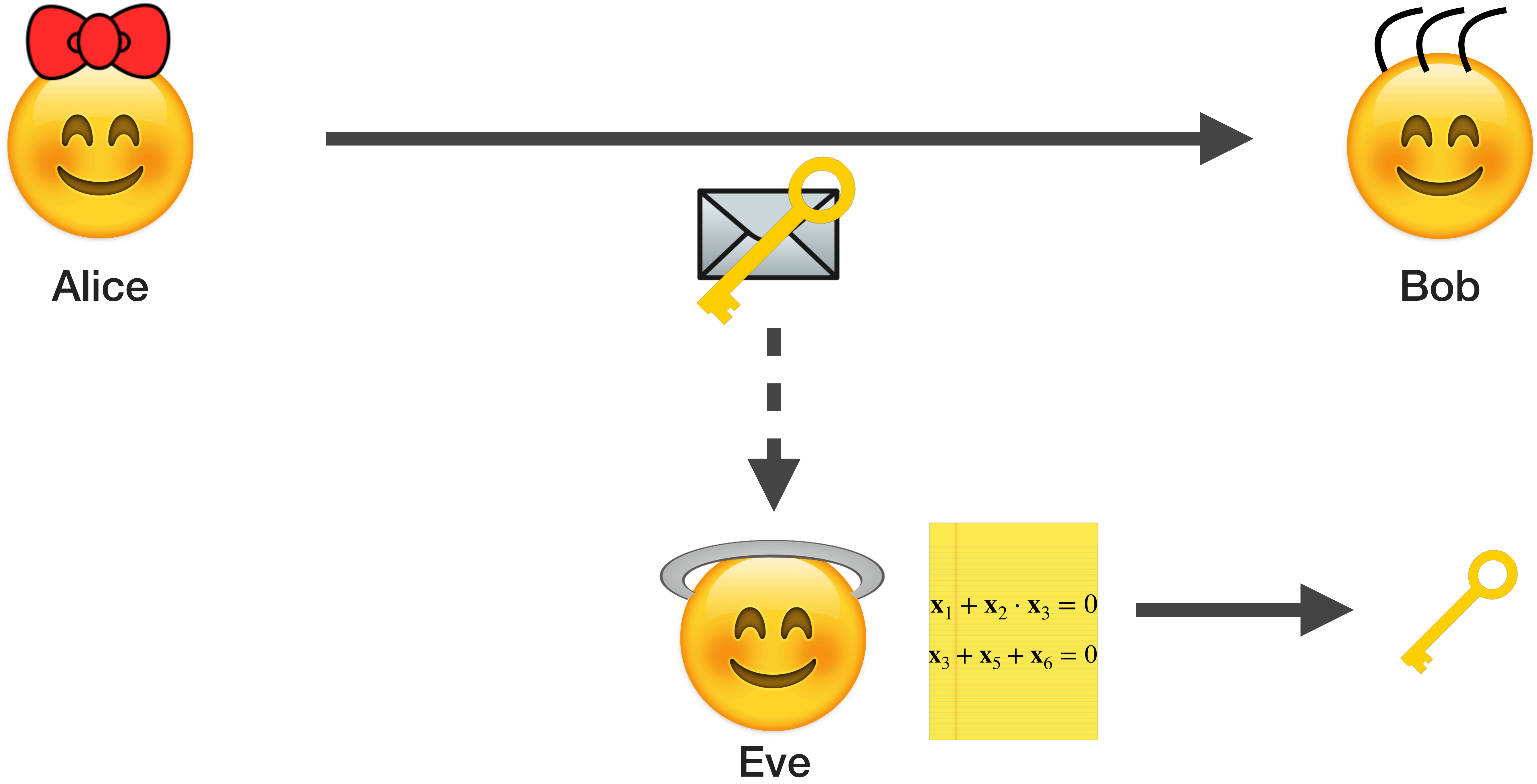
Cryptanalysis



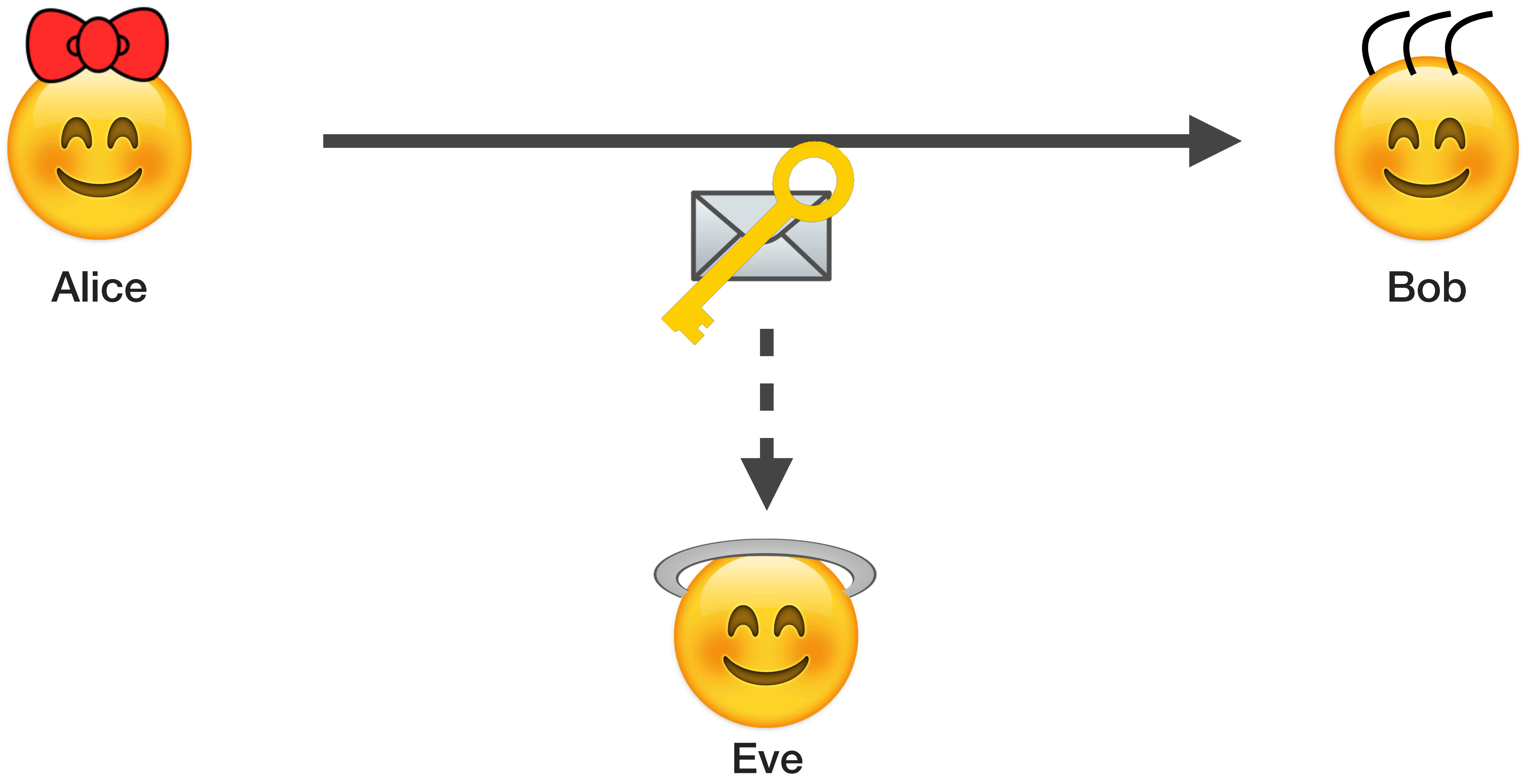
Cryptanalysis



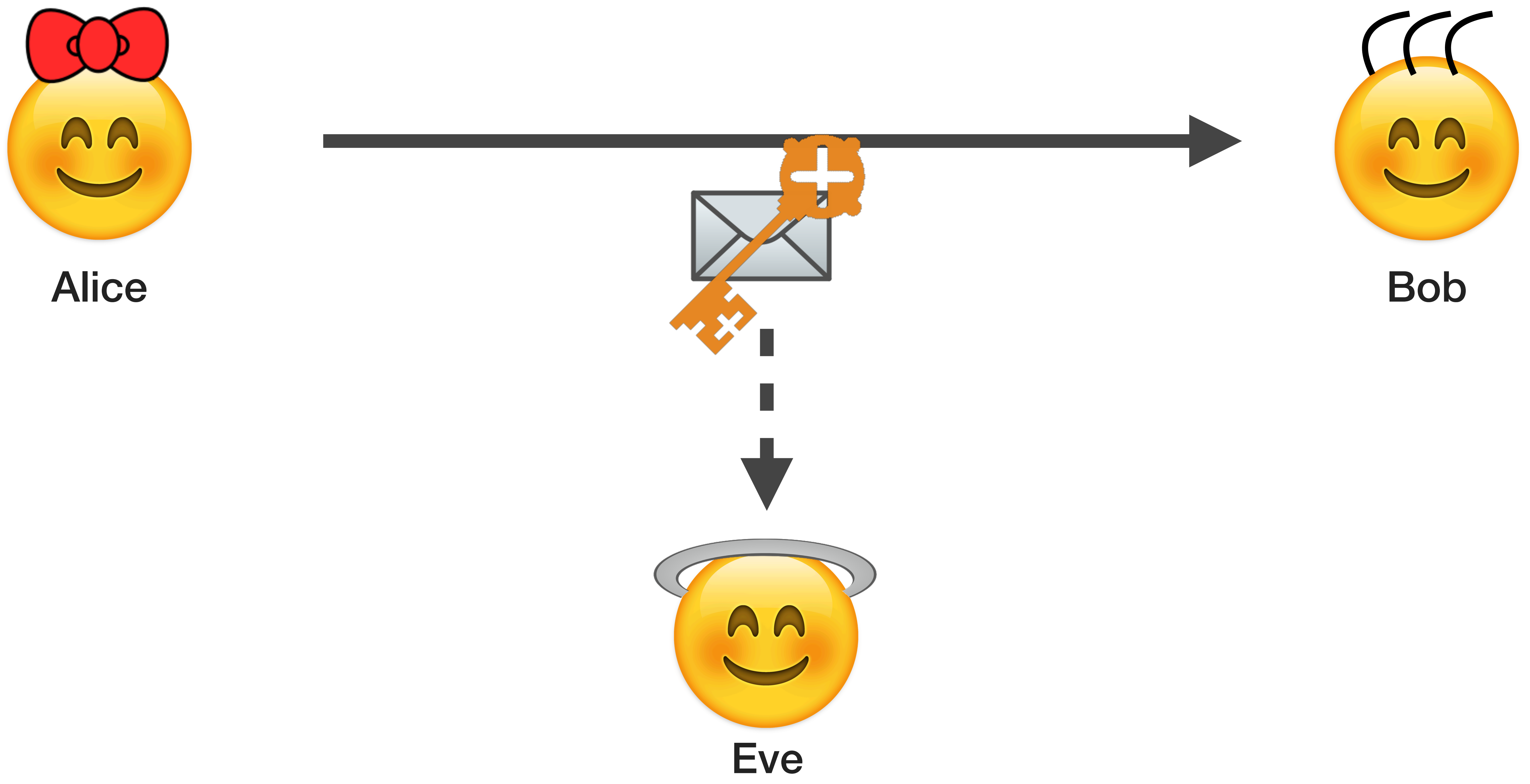
Cryptanalysis



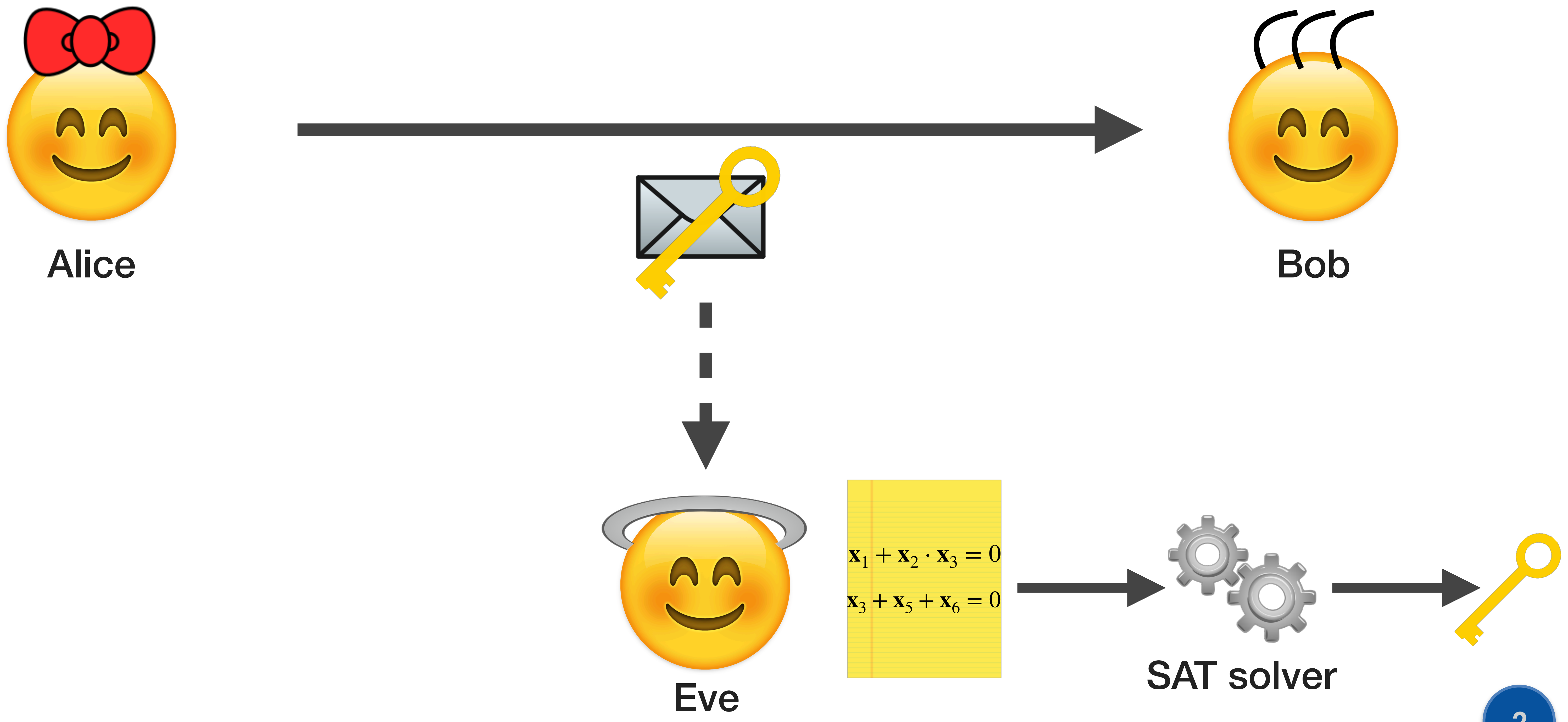
Cryptanalysis



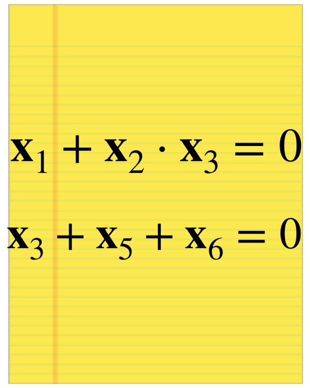
Cryptanalysis



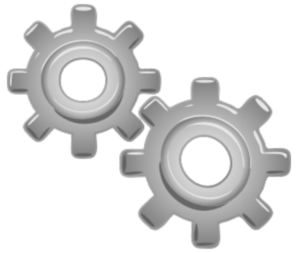
Logical cryptanalysis



Deriving a SAT model



Transforming a Boolean polynomial system to a propositional formula



SAT solver

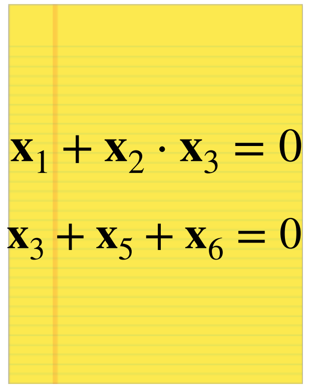
Boolean polynomial system

$$\mathbf{x}_1 + \mathbf{x}_2 \cdot \mathbf{x}_3 + \mathbf{x}_5 + \mathbf{x}_6 + 1 = 0$$
$$\mathbf{x}_3 + \mathbf{x}_5 + \mathbf{x}_6 = 0$$

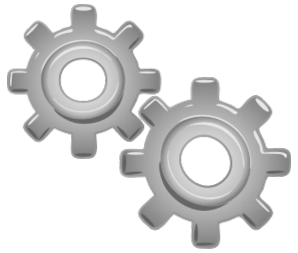
ANF formula

$$x_1 \oplus (x_2 \wedge x_3) \oplus x_5 \oplus x_6$$
$$x_3 \oplus x_5 \oplus x_6 \oplus \top$$

Deriving a SAT model



Transforming a Boolean polynomial system to a propositional formula



SAT solver

Boolean polynomial system

$$\mathbf{x}_1 + \mathbf{x}_2 \cdot \mathbf{x}_3 + \mathbf{x}_5 + \mathbf{x}_6 + 1 = 0$$
$$\mathbf{x}_3 + \mathbf{x}_5 + \mathbf{x}_6 = 0$$

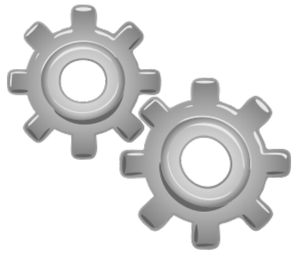
ANF formula

$$x_1 \oplus \overbrace{\boxed{(x_2 \wedge x_3)}}^{x'} \oplus x_5 \oplus x_6$$
$$x_3 \oplus x_5 \oplus x_6 \oplus \top$$

Deriving a SAT model

$$\mathbf{x}_1 + \mathbf{x}_2 \cdot \mathbf{x}_3 = 0$$
$$\mathbf{x}_3 + \mathbf{x}_5 + \mathbf{x}_6 = 0$$

Transforming a Boolean polynomial system to a propositional formula



SAT solver

$$x' \Leftrightarrow x_2 \wedge x_3$$

$$x' \Rightarrow x_2 \wedge x_3 \qquad\qquad x_2 \wedge x_3 \Rightarrow x'$$

$$\neg x' \vee (x_2 \wedge x_3) \qquad\qquad \neg(x_2 \wedge x_3) \vee x'$$

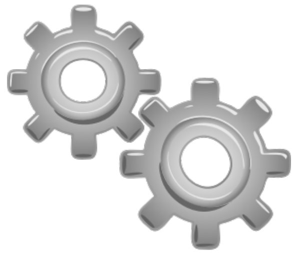
$$\neg x' \vee x_2 \qquad \neg x' \vee x_3 \qquad\qquad \neg x_2 \vee \neg x_3 \vee x'$$

Deriving a SAT model

$\mathbf{x}_1 + \mathbf{x}_2 \cdot \mathbf{x}_3 = 0$

$\mathbf{x}_3 + \mathbf{x}_5 + \mathbf{x}_6 = 0$

Transforming a Boolean polynomial system to a propositional formula



SAT solver

ANF formula

$$x_1 \oplus (x_2 \wedge x_3) \oplus x_5 \oplus x_6$$

$$x_3 \oplus x_5 \oplus x_6 \oplus \top$$

CNF-XOR formula

$$\neg x' \vee x_2$$

$$\neg x' \vee x_3$$

$$\neg x_2 \vee \neg x_3 \vee x'$$

$$x_1 \oplus x' \oplus x_5 \oplus x_6$$

$$x_3 \oplus x_5 \oplus x_6 \oplus \top$$

Gaussian Elimination

Example of a case where a possible cancellation of terms is overseen due to the CNF-XOR form

Boolean polynomial system

$$\mathbf{x}_1 + \mathbf{x}_2 \cdot \mathbf{x}_3 + \mathbf{x}_5 + \mathbf{x}_6 + 1 = 0$$

$$\mathbf{x}_3 + \mathbf{x}_5 + \mathbf{x}_6 = 0$$

CNF-XOR formula

$$\neg x' \vee x_2$$

$$\neg x' \vee x_3$$

$$\neg x_2 \vee \neg x_3 \vee x'$$

$$x_1 \oplus x' \oplus x_5 \oplus x_6$$

$$x_3 \oplus x_5 \oplus x_6 \oplus \top$$

Gaussian Elimination

Example of a case where a possible cancellation of terms is overseen due to the CNF-XOR form

$\boxed{\text{Set } \mathbf{x}_2 \text{ to } 1 \text{ / Set } x_2 \text{ to } \top}$

Boolean polynomial system

$$\mathbf{x}_1 + \mathbf{x}_2 \cdot \mathbf{x}_3 + \mathbf{x}_5 + \mathbf{x}_6 + 1 = 0$$

$$\mathbf{x}_3 + \mathbf{x}_5 + \mathbf{x}_6 = 0$$

CNF-XOR formula

$$\neg x' \vee x_2$$

$$\neg x' \vee x_3$$

$$\neg x_2 \vee \neg x_3 \vee x'$$

$$x_1 \oplus x' \oplus x_5 \oplus x_6$$

$$x_3 \oplus x_5 \oplus x_6 \oplus \top$$

Gaussian Elimination

Example of a case where a possible cancellation of terms is overseen due to the CNF-XOR form

$\boxed{\text{Set } \mathbf{x}_2 \text{ to } 1 \text{ / Set } x_2 \text{ to } \top}$

Boolean polynomial system

$$\mathbf{x}_1 + \cancel{\mathbf{x}_2} \cdot \mathbf{x}_3 + \mathbf{x}_5 + \mathbf{x}_6 + 1 = 0$$
$$\mathbf{x}_3 + \mathbf{x}_5 + \mathbf{x}_6 = 0$$

CNF-XOR formula

$$\sout{\neg x' \vee x_2}$$
$$\neg x' \vee x_3$$
$$\neg \cancel{x_2} \vee \neg x_3 \vee x'$$
$$x_1 \oplus x' \oplus x_5 \oplus x_6$$
$$x_3 \oplus x_5 \oplus x_6 \oplus \top$$

Gaussian Elimination

Example of a case where a possible cancellation of terms is overseen due to the CNF-XOR form

Boolean polynomial system

$$\mathbf{x}_1 + \underline{\mathbf{x}_3 + \mathbf{x}_5 + \mathbf{x}_6} + 1 = 0$$

$$\underline{\mathbf{x}_3 + \mathbf{x}_5 + \mathbf{x}_6} = 0$$

$$\Downarrow$$

$$\mathbf{x}_1 = 1$$

CNF-XOR formula

$$\neg x' \vee x_3$$

$$\neg x_3 \vee x'$$

$$x_1 \oplus x' \oplus x_5 \oplus x_6$$

$$x_3 \oplus x_5 \oplus x_6 \oplus \top$$

Gaussian Elimination

Define the following rule:

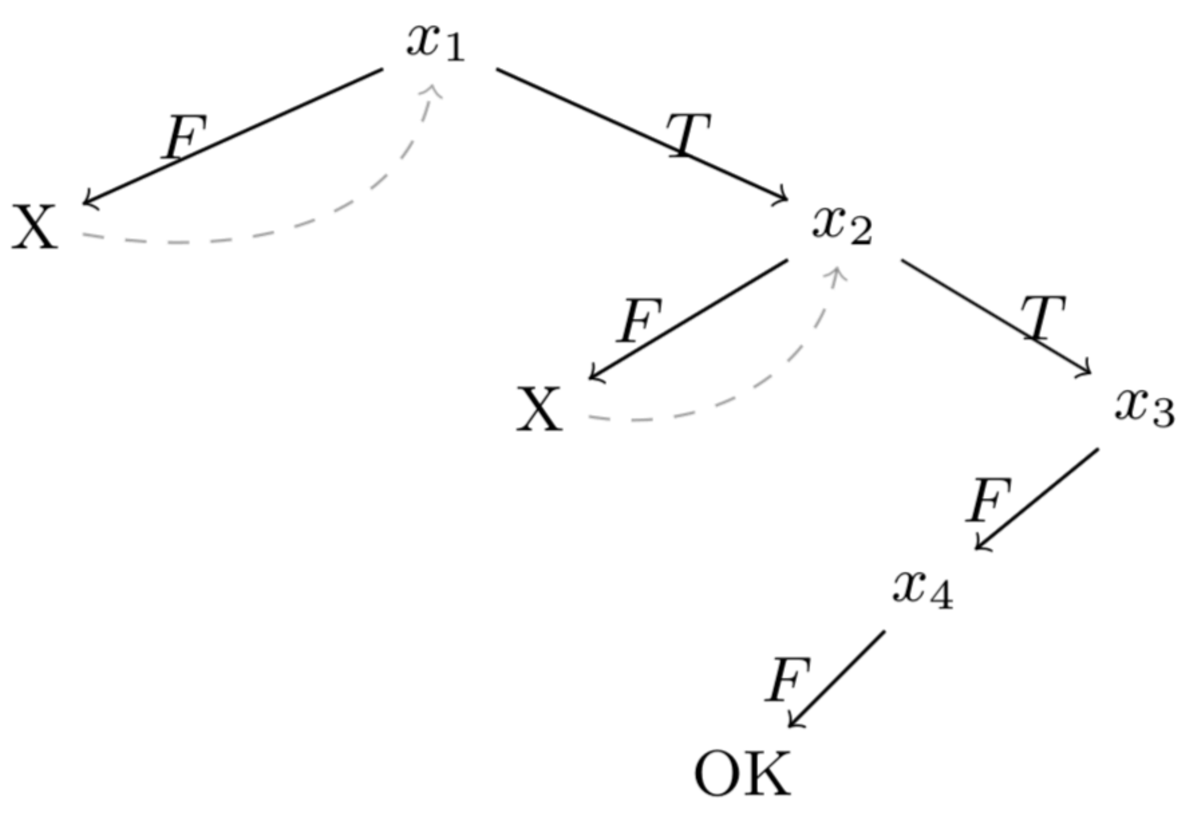
$$\frac{x_2 \qquad\qquad x' \Leftrightarrow x_2 \wedge x_3}{x' \Leftrightarrow x_3}$$

Replace all occurrences of x' by x_3.

WDSat

DPLL-based

- Recursively building a binary search tree.



Three reasoning modules:

- CNF module
- XORSET module
- XORGAUSS module

XORGAUSS module

Our example in ANF

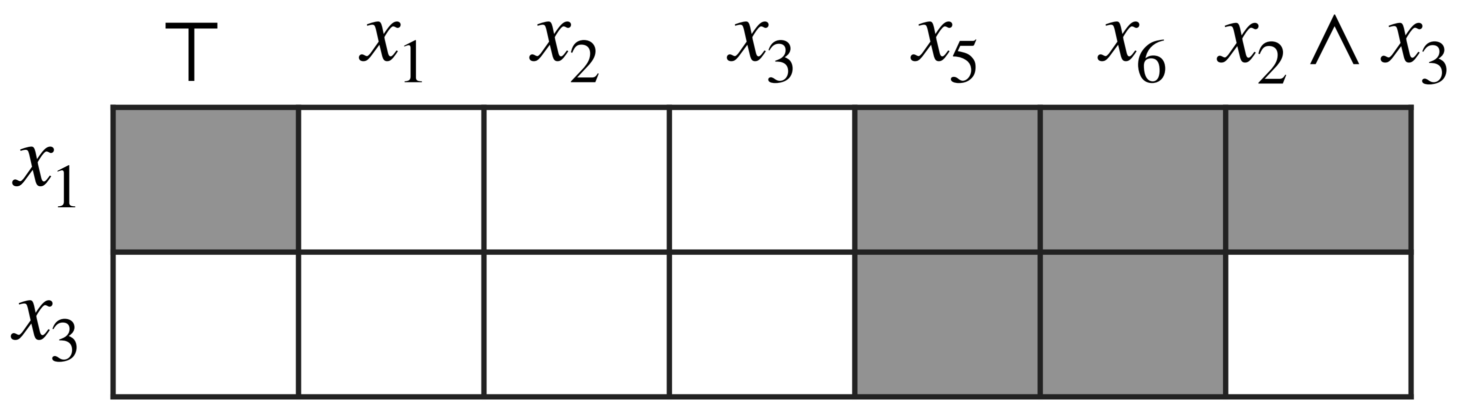
$$x_1 \oplus (x_2 \land x_3) \oplus x_5 \oplus x_6$$

$$x_3 \oplus x_5 \oplus x_6 \oplus \top$$

In the XORGAUSS module:

$$x_1 \Leftrightarrow (x_2 \land x_3) \oplus x_5 \oplus x_6 \oplus \top$$

$$x_3 \Leftrightarrow x_5 \oplus x_6$$



Preprocessing technique

$$\mathbf{x}_1 + \mathbf{x}_2 \cdot \mathbf{x}_3 + \mathbf{x}_4 + \mathbf{x}_4 \cdot \mathbf{x}_5 = 0$$

$$\mathbf{x}_1 + \mathbf{x}_2 \cdot \mathbf{x}_3 = 0$$

$$\mathbf{x}_1 + \mathbf{x}_3 \cdot \mathbf{x}_5 + \mathbf{x}_6 = 0$$

$$\mathbf{x}_1 + \mathbf{x}_2 \cdot \mathbf{x}_5 \cdot \mathbf{x}_6 + \mathbf{x}_6 = 0$$

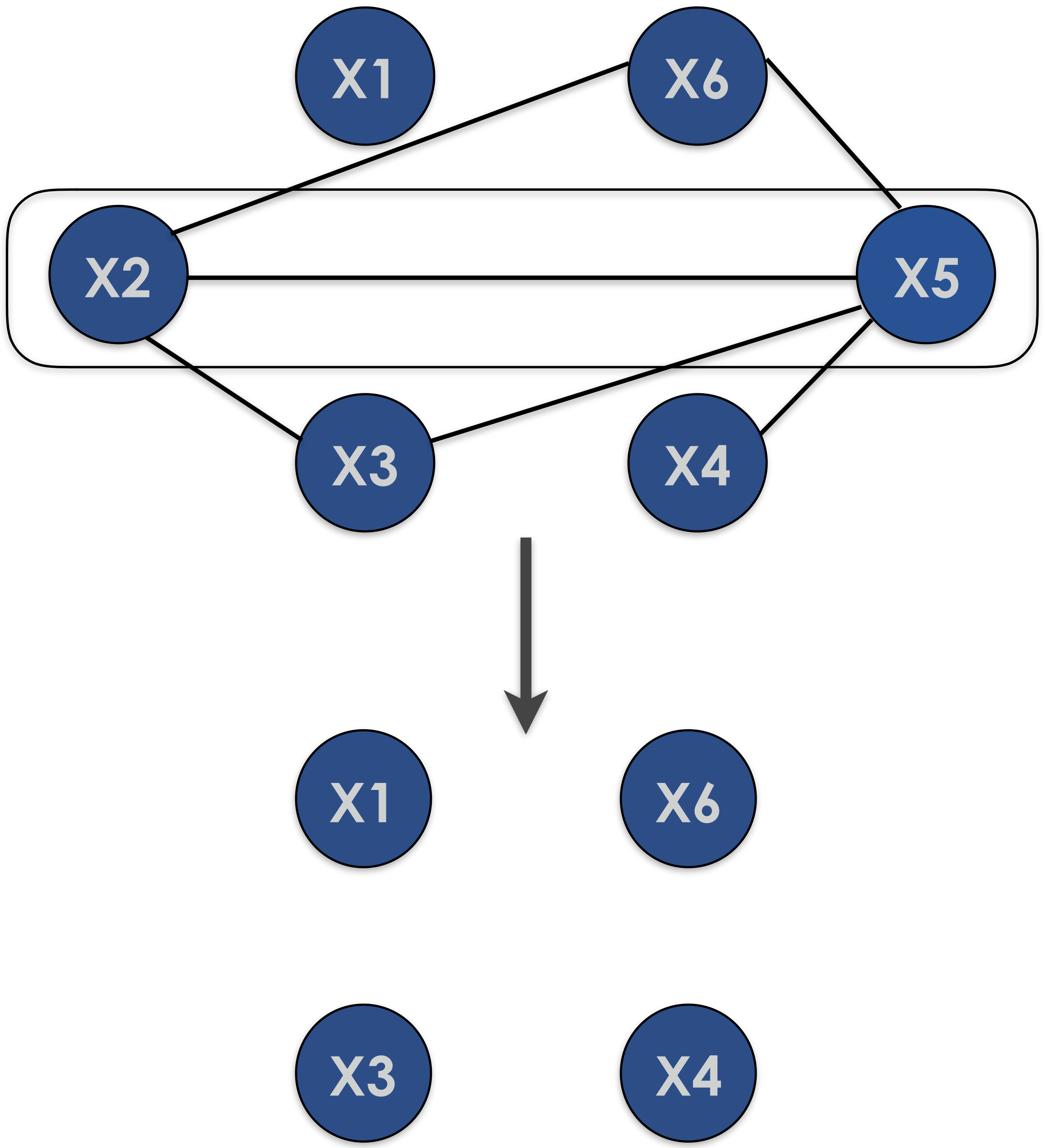
$$\downarrow$$

$$\mathbf{x}_1 + \mathbf{x}_3 = 0$$

$$\mathbf{x}_1 + \mathbf{x}_3 = 0$$

$$\mathbf{x}_1 + \mathbf{x}_3 + \mathbf{x}_6 = 0$$

$$\mathbf{x}_1 = 0$$

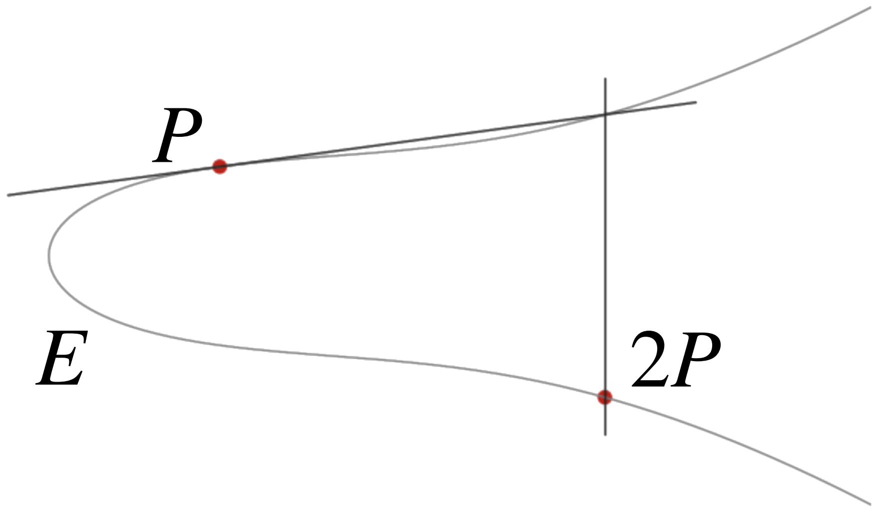


Elliptic curve discrete log problem

Let E be an elliptic curve defined by

$E : y^2 + xy = x^3 + ax^2 + b$, with $\boxed{a, b \in \mathbb{F}_{2^n} \text{ and } n \text{ prime}}$

our case



Addition law on E

For $P, Q \in E(\mathbb{F}_{2^n})$, find x such that $xP = Q$.

Elliptic curve discrete log problem

→ Generic methods (Pollard's Rho, Parallel Collision Search, Baby-Step Giant-Step, Pohlig–Hellman)

→ Index calculus attack

1. Choosing an appropriate factor base
2. Point decomposition → $R = P_1 + \cdots + P_m$
3. Linear algebra

Experimental results

$R = P_1 + P_2$

40 variables, 41 equations

Solving approach	SAT		UNSAT	
	Runtime (s)	#Conflicts	Runtime (s)	#Conflicts
Gröbner bases	16.8	*N/A*	18.7	*N/A*
MiniSat	> 600		> 600	
Glucose	> 600		> 600	
MapleLCMDistChronoBT	> 600		> 600	
CaDiCaL	> 600		> 600	
CryptoMiniSat	29.0	226668	84.3	627539
WDSat + XG-ext + MVC	**4.2**	**27684**	**13.5**	**86152**

Experimental results

$$R = P_1 + P_2 + P_3$$

51 variables, 52 equations

Solving approach	SAT		UNSAT	
	Runtime (s)	#Conflicts	Runtime (s)	#Conflicts
Gröbner bases	229.3	*N/A*	229.4	*N/A*
MiniSat	239.7	1840190	517.0	3433304
Glucose	189.2	1527158	274.8	2056575
MapleLCMDistChronoBT	655.1	4035131	918.7	5378945
CaDiCaL	43.6	254194	141.3	629869
CryptoMiniSat	331.8	1791188	707.9	3416526
WDSat	**0.6**	**48438**	**3.8**	**255698**

Conclusion

→ The oversight in XOR-enabled SAT solvers can be fixed.

→ Gröbner bases can be replaced by a SAT solver in the index calculus attack on binary elliptic curves.

→ WDSat outperforms all existing resolution approaches for this specific problem.