Breaking Symmetric Cryptosystems using Quantum Period Finding

Marc Kaplan
Paris Center for Quantum Computing & University of Edinburgh

Joint work with G. Leurent, A. Leverrier, M. Naya-Plasencia (Inria EPI Secret)

Post-quantum cryptography

Public key cryptography:

Shor's algorithm breaks RSA, DH, ECC in polynomial time

Large effort to develop quantum-resistant scheme - Lattice, code, multivariate, etc…

- D-Wave's people claim that they can solve problems fast using their quantum computer *(or can they?)*
- NSA thinks we need quantum-secure crypto *(or do they?)*

Post-quantum cryptography

Symmetric cryptography:

Grover's algorithm searches exhaustively for a key of length k in time $2^{k/2}$

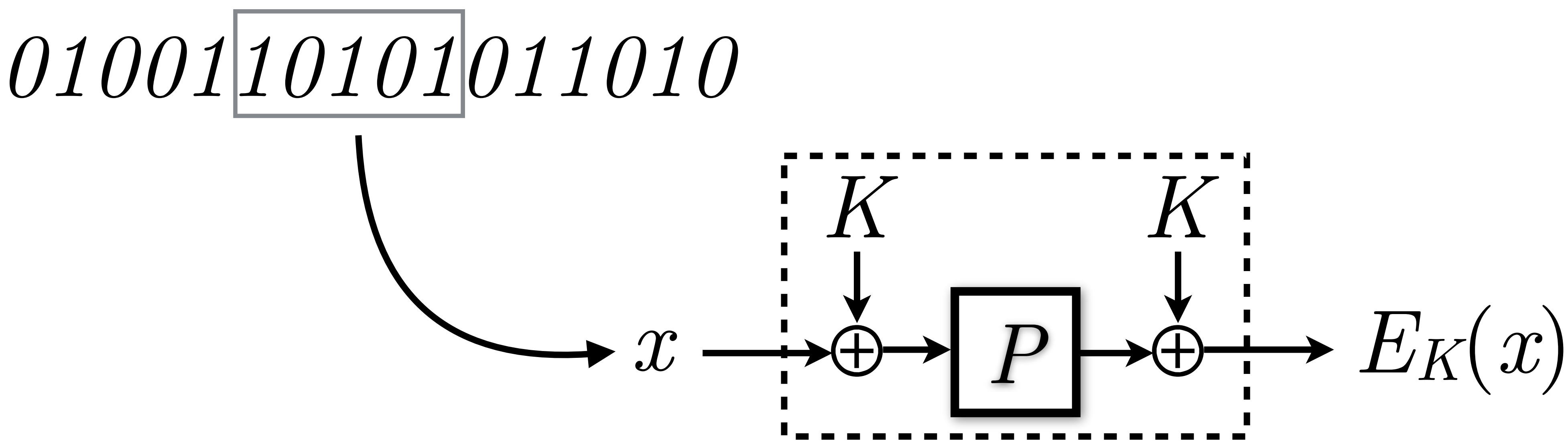
Recommendation: double the key length

Goal of this talk: go beyond this claim

But…

1. We don't break AES, but modes of operations
2. In most situations, building a quantum computer is insufficient for our attacks to work

Quantum attack on Even-Mansour

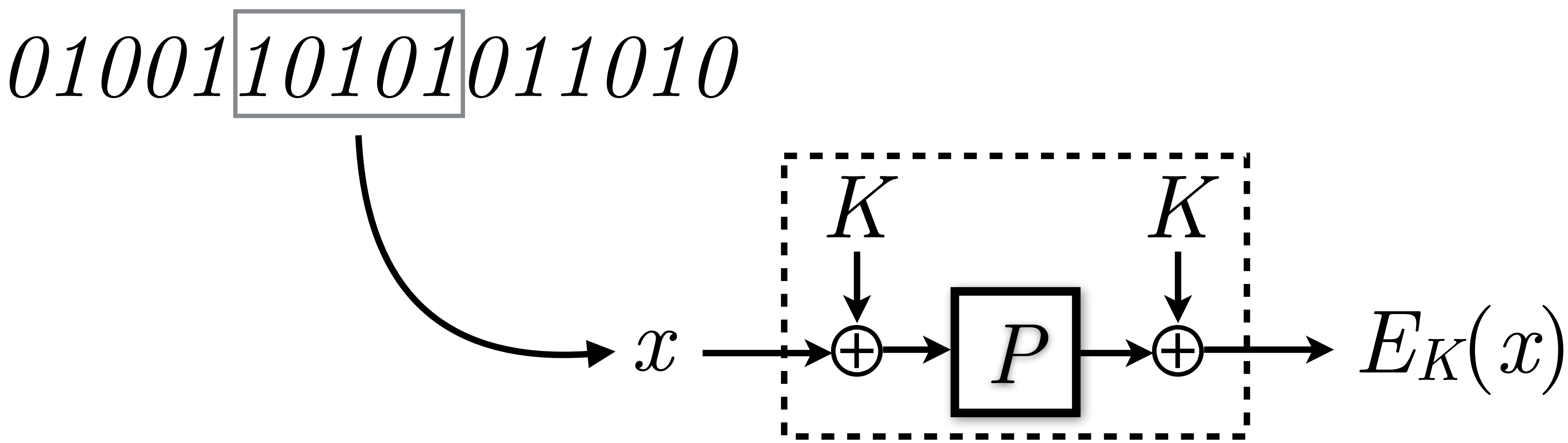


$$E_K(x) = K \oplus P(x \oplus K)$$

[Even, Mansour, 97]

For a random P, a successful attack against E_K requires $\underbrace{\mathrm{D}}_{\text{\#Queries to } E_K}\underbrace{\mathrm{T}}_{\text{\#Queries to } P} > 2^{\underbrace{n}_{\text{block size}}}$

Quantum attack on Even-Mansour



$$E_K(x) = K \oplus P(x \oplus K)$$

[Kuwakado, Mori '12]

For a random $P,$ there is a key recovery attack using $\mathrm{O}(n)$ quantum queries to E_K and P

Simon's problem

<u>Input</u> : $f\colon\{0,1\}^n \to \{0,1\}^m$

<u>promise</u> : $f(x)=f(y) \Leftrightarrow x=y$ or $x=y\oplus s$ for some s

<u>Output</u> : s

<u>Simon's algorithm</u>: $\mathrm{O}(n)$ quantum queries to f

Quantum attack on Even-Mansour

<u>Oracle</u> : $E_K(x) = K \oplus P(x \oplus K)$

<u>Function</u> : $f(x) = E_K(x) \oplus P(x)$

<u>Period</u> : $f(x \oplus K) = E_K(x \oplus K) \oplus P(x \oplus K)$

$$= K \oplus P(x) \oplus P(x \oplus K) = f(x)$$

Simon's algorithm returns K with $\mathrm{O}(n)$ quantum queries to E_K and P

Quantum attack on Even-Mansour

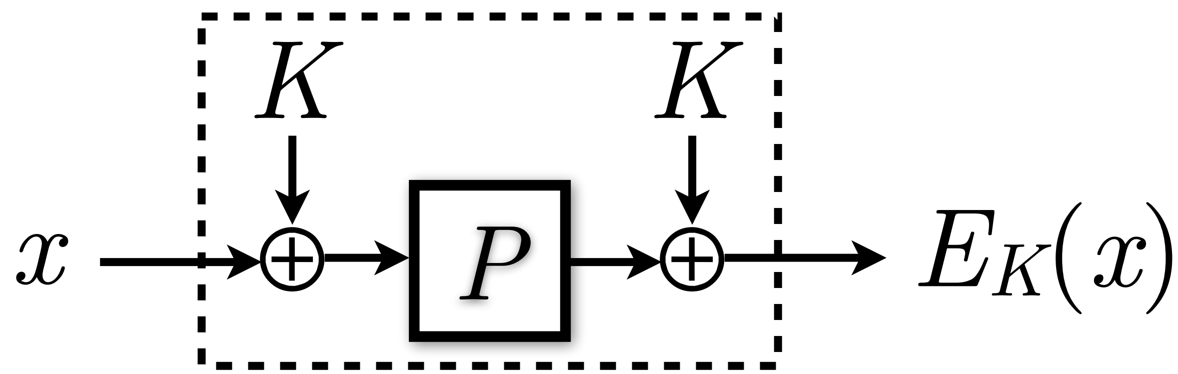
Remark 1

No reduction to Simon: $f(x) = f(x \oplus K)$ for any x, but $f(x) = f(y)$ for other values too.

Promise : $f(x) = f(y) \Leftarrow x = y$ or $x = y \oplus K$

Simon's algorithm works as long as the « bad » collisions in f looks random

Quantum attack on Even-Mansour



$$E_K(x) = K \oplus P(x \oplus K)$$

[Kuwakado, Mori '12]

For a random P, there is a key recovery attack using $\mathrm{O}(n)$ quantum queries to E_K and P

Quantum attack on Even-Mansour

Remark II

Simon's algorithm requires to make quantum queries (in superposition) to f

The adversary needs a quantum access to the cryptographic oracle

Model introduced by

- Boneh, Zhandry,'13

  Quantum chosen plaintext attacks

- Damgård, Funder, Buus Nielsen, Salvail,'13

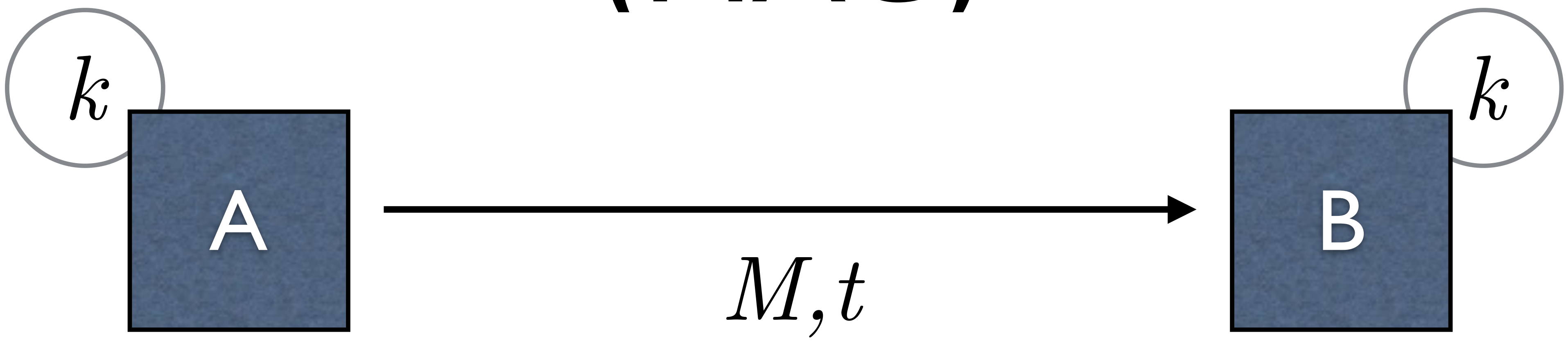
  Superposition attacks

Quantum chosen plaintext attacks

Quantum chosen plaintext attacks

- Strongest non-trivial model of quantum attacks
- Well defined
- Possible attacks
    - Hidden quantum effects
    - Obfuscation
    - Quantum internet

Message authentication code (MAC)



- Alice uses the secret key k to compute a tag :

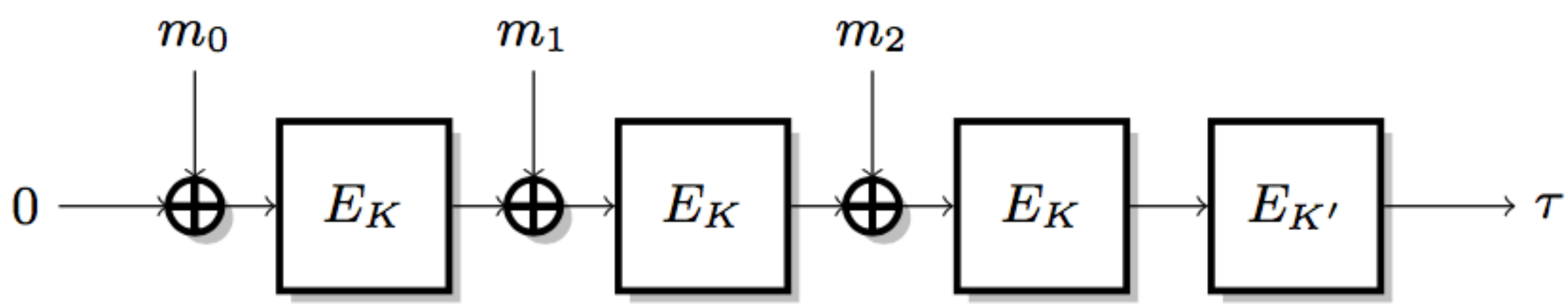
$$t = \mathrm{Mac}_k(M)$$

- Bob can detect adversarial modifications of M

- The security only depends on the security of some block cipher

Cipher Block Chaining (CBC)

$$m = m_0 \| m_1 \| m_2$$



Security proof (Bellare, Killian, Rogaway)
If E_K is a secure, then CBC-MAC is secure.

Boneh-Zhandry:
Is CBC-MAC quantum-secure?

Cipher Block Chaining (CBC)

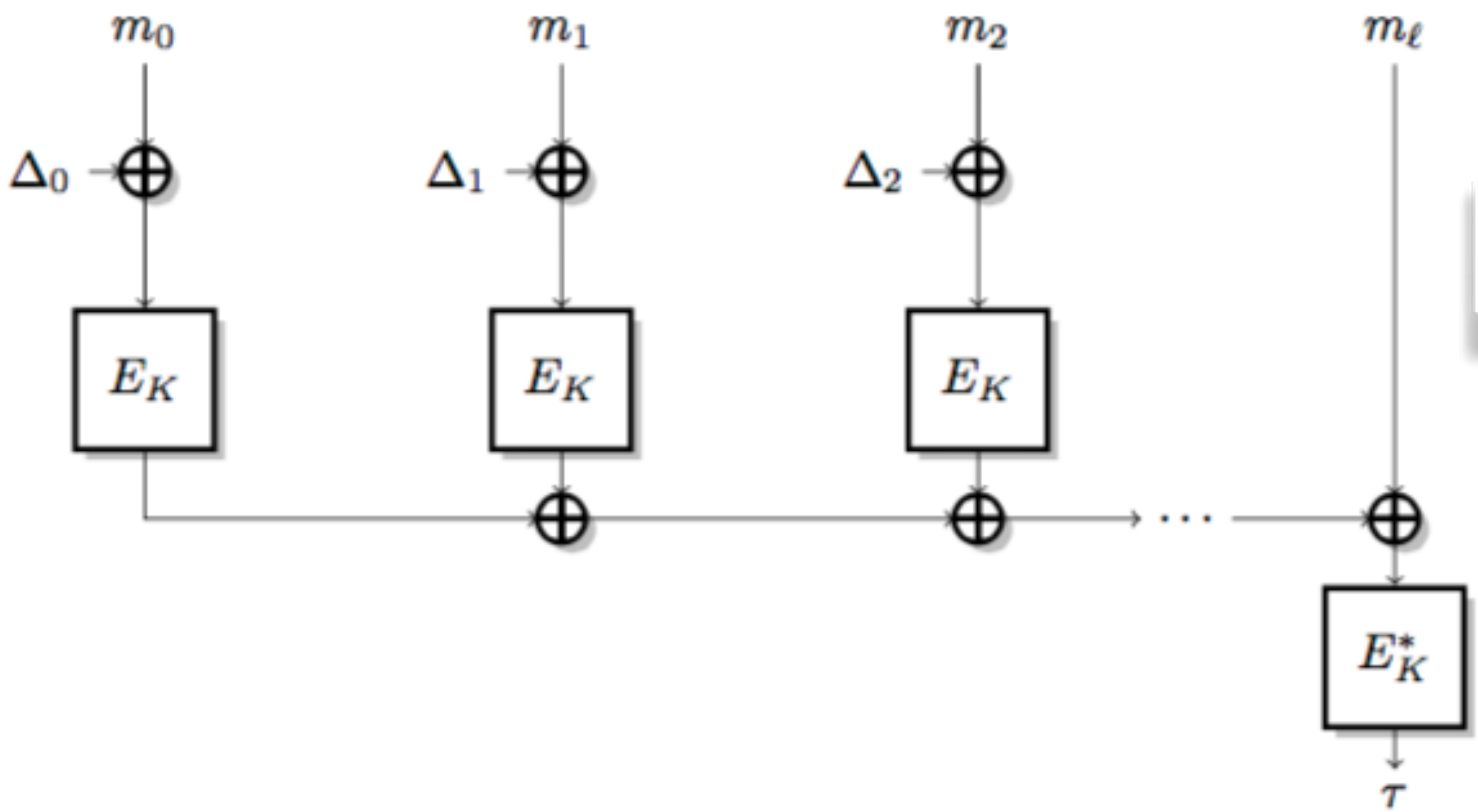
Function : $f(b,x) = \begin{cases} \text{CBC}-\text{MAC}(\alpha_0 \| x) \text{if } b = 0 \\ \text{CBC}-\text{MAC}(\alpha_1 \| x) \text{if } b = 1 \end{cases}$

Period : $f(0,x) = f(1, x \oplus E_K(\alpha_0) \oplus E_K(\alpha_1))$

Forgery : $\alpha_0 || m_1 || m_2 \longrightarrow$ Same Tag

$\alpha_1 || m_1 \oplus E_K(\alpha_0) \oplus E_K(\alpha_1) || m_2 \nearrow$

PMAC

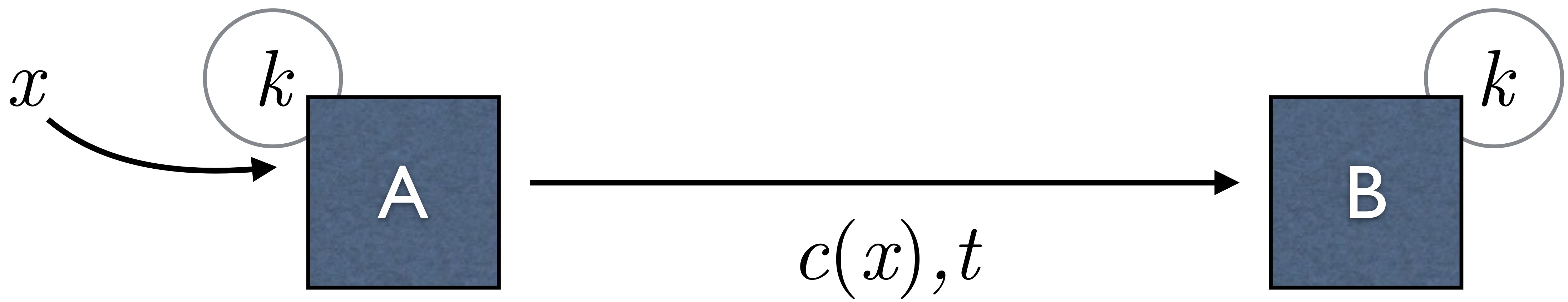


$$\Delta_i = \gamma(i) \cdot E_k(0)$$

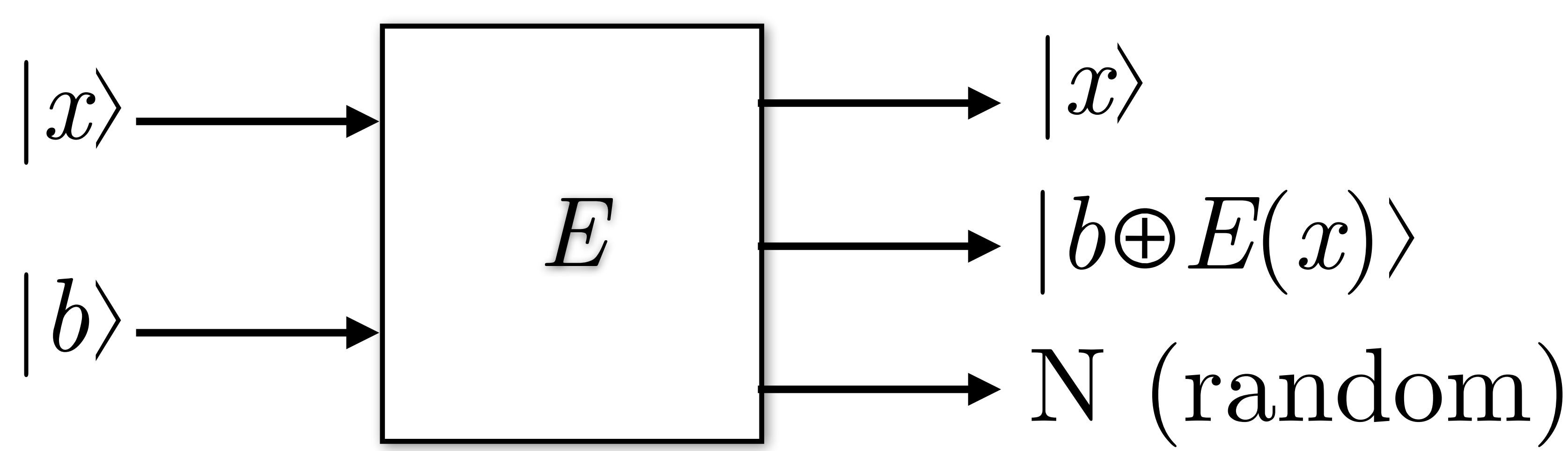
Security proof (Black, Rogaway):
If E_K is secure cipher, then PMAC is secure.

Broken by Simon's algorithm

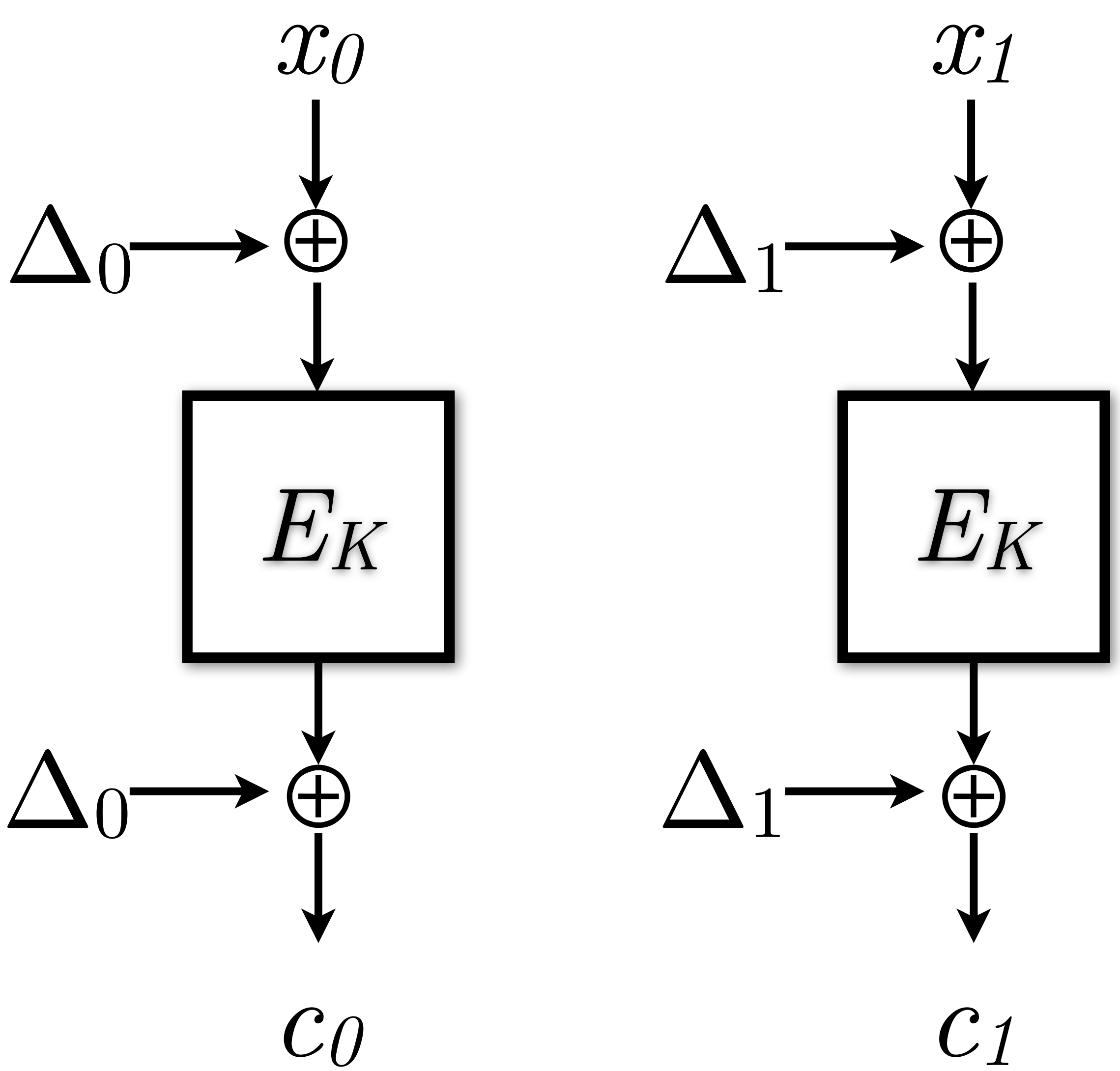
Authenticated encryption



- Confidentiality and integrity
- CAESAR competition
- Nonce based construction



Offset codebook mode (OCB)



$$\Delta_i = \Phi_K(N) \oplus \gamma(i) \cdot E_K(0)$$

N: Nonce

Goal: extract the offsets Δ_i

Offset codebook mode (OCB)

<u>Oracle</u> : $\mathrm{OCB}_k(N, m_0, m_1)$ Can not chose N

<u>Function</u> : $f(m) = c_0 \oplus c_1$
where $(c_0, c_1, \tau) = \mathrm{OCB}_k(N, m \| m, \varepsilon)$

<u>Period</u> : $\Delta_0 \oplus \Delta_1 = (\gamma(0) \oplus \gamma(1)) \cdot E_k(0)$

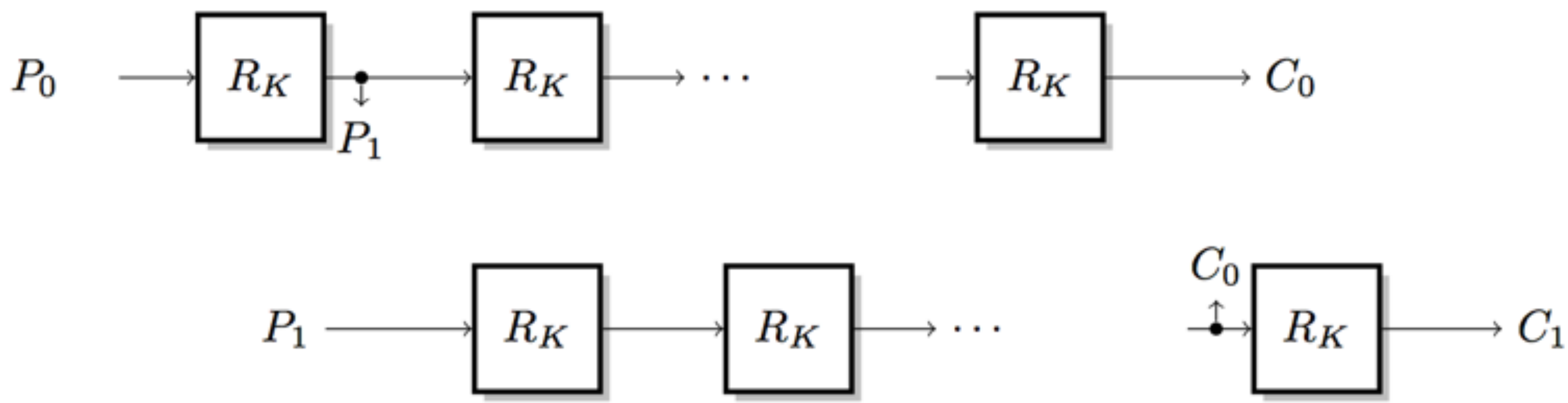
Does not depend on N

Summary: modes of operations

	3-round Feistel	Distinguisher (corrected)
	Even-Mansour	Key recovery
	LRW	Distinguisher
MAC	CBC-MAC	Forgery
	PMAC	Forgery
	GMAC	Forgery / Nonce
AE	GCM	Forgery / Nonce
	OCB	Forgery / Nonce
CAESAR	CLOC	Forgery
	AEZ	Forgery / associated data
	COPA	Forgery / associated data
	OTR	Forgery / associated data
	POET	Forgery / associated data
	OMD	Forgery / associated data
	Minalpher	Forgery / associated data

Slide attacks

[Biryukov & Wagner, FSE '99]



Slid Pair: $(P_0, C_0), (P_1, C_1)$ s.t. $P_1 = R_K(P_0)$

Simon's algorithm: Exponential speedup to find slid-pairs

Conclusion

« Simon's algorithm : […] actually maybe *not* that useless »*

« so many systems that are vulnerable to Simon attack exist and are used »*

Quantum computers threaten symmetric crypto too

But quantum-safe modes of operations also exist

www.sco

Thank you!

Simon's algorithm