Cryptographic Key Reliable Lifetimes

Bounding the Risk of Key Exposure in the Presence of Faults

Alfonso De Gregorio

Andxor S.r.l.
Milano
Italy

Fault Diagnosis and Tolerance in Cryptography, 2005
Edinburgh

ANDXOR

Outline

1. Introduction
   - Dependability Metrics and Cryptographic Modules
   - How to bound the risk of key exposure?
   - Contribution
2. Key Lifetimes in the Presence of Faults
   - Key Points
   - Threat Model
   - Security Parameters
3. Cryptographic Key Reliable Lifetimes
   - Selecting Key Lifetimes
   - Reliability Modeling
4. Using the framework
   - Cryptographic Key Reliable Lifetimes
   - Dependable Crypto Infrastructures
   - Hazard Rates and Minimal CKFT Values

ANDXOR

Outline

1. Introduction
   - Dependability Metrics and Cryptographic Modules
   - How to bound the risk of key exposure?
   - Contribution
2. Key Lifetimes in the Presence of Faults
   - Key Points
   - Threat Model
   - Security Parameters
3. Cryptographic Key Reliable Lifetimes
   - Selecting Key Lifetimes
   - Reliability Modeling
4. Using the framework
   - Cryptographic Key Reliable Lifetimes
   - Dependable Crypto Infrastructures
   - Hazard Rates and Minimal CKFT Values

Dependability Metrics and Cryptographic Modules

Facts

- Faulty outputs may expose the secret key material;
- The nature of computation is physical;
- No dependability, no trust;
- Physical attacks are not ruled out by the remote (black-box) scenario.

Motivation

Questions

- Are fault attacks ”viable” also at standard environmental conditions (i.e., without producing excursions outside the normal operating ranges of environmental conditions)?
- What it is the risk of key exposure at standard environmental conditions? Is it negligible? – In a cryptographic sense
- How much time is necessary to expose the key material with a probability greater than ϵ at standard environmental conditions?
- How to keep the risk of key exposure below a desired security margin ϵ?

Fault Attacks: Model

The Model

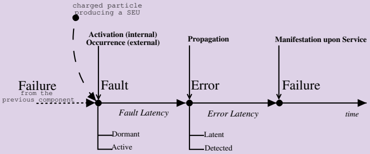
A cryptographic module contain some crypto secret.

The interaction with the outside world follows a cryptographic protocol.

On some rare occasions, the module is assumed to be affected by faults causing it to output incorrect values [Boneh *et al.* 01].

Fault Attacks: Dependability Imapairments

Dependability Impairments



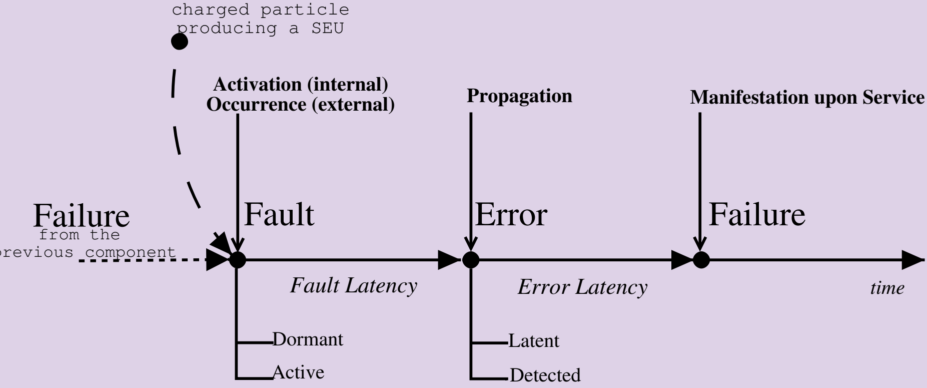
Observation

Due to the unavoidable occurrence of *transient faults* or the presence of *dormant faults*, there will be always a non-zero probability that the system will fail, sooner or later.

⏩ Next

ANDXOR

Fault Attacks: Dependability Imapairments



Motivation

Questions

- Are fault attacks ”viable” also at standard environmental conditions (i.e., without producing excursions outside the operating ranges of environmental conditions)?
- What it is the risk of key exposure at standard environmental conditions? Is it negligible? – In a cryptographic sense
- How much time is necessary to expose the key material with a probability greater than ϵ at standard environmental conditions?
- How to keep the risk of key exposure below a desired security margin ϵ?

Motivation

Questions

- Are fault attacks ”viable” also at standard environmental conditions (i.e., without producing excursions outside the operating ranges of environmental conditions)?
- What it is the risk of key exposure at standard environmental conditions? Is it negligible? – In a cryptographic sense
- How much time is necessary to expose the key material with a probability greater than ϵ at standard environmental conditions?
- How to keep the risk of key exposure below a desired security margin ϵ?

A Non-Negligible Risk of Key Exposure

A first answer

Are fault attacks viable at standard environmental conditions?

- For standard error-bounds,
- using systems with good levels of coverage,
- with typical failure rates,
- the probability of key exposure may exceed the desired bound within very short mission times,
- depending on the number of faulty outputs necessary to perform a fault attack against the given scheme.

A Non-Negligible Risk of Key Exposure

Example

- Cryptographic keys that does not tolerate any faulty outputs (e.g., RSA keys with CRT implementations)
- are exposed with a probability greater than 2^{-40}
- after operational times shorter than 1 *year*,
- if the failure rate of the crypto module is greater than 1.04×10^{-16} *failures/hours*.

ANDXOR

Motivation

Questions

- Are fault attacks viable at standard environmental conditions?
- What it is the risk of key exposure at standard environmental conditions? Is it negligible? – In a cryptographic sense
- How much time is necessary to expose the key material with a probability greater than ϵ at standard environmental conditions?
- How to keep the risk of key exposure below a desired security margin ϵ?

Outline

1. Introduction
   - Dependability Metrics and Cryptographic Modules
   - How to bound the risk of key exposure?
   - Contribution
2. Key Lifetimes in the Presence of Faults
   - Key Points
   - Threat Model
   - Security Parameters
3. Cryptographic Key Reliable Lifetimes
   - Selecting Key Lifetimes
   - Reliability Modeling
4. Using the framework
   - Cryptographic Key Reliable Lifetimes
   - Dependable Crypto Infrastructures
   - Hazard Rates and Minimal CKFT Values

How to bound the risk of key exposure?

A first approach: Increase further the coverage of fault tolerant system

Possible, in principle. However. . .

- Building (statistically) justifiable confidence in extremely low failure-rates may raise the costs of cryptographic modules, by requiring a much larger number of hours during the design and assessment phases.
- Modules in software may need to be executed on different hardware and platforms.
- SDLC models have an impact, as well.

How to bound the risk of key exposure?

A pragmatic approach

Being the reliability a function of time, it’s possible to select Key Lifetimes so that the key material will no longer be used, after the effective reliability of the system has fallen below the level required to guarantee the accepted (negligible) risk of key exposure.

How to bound the risk of key exposure?

A pragmatic approach

Being the reliability a function of time, it's possible to select Key Lifetimes so that the key material will no longer be used, after the effective reliability of the system has fallen below the level required to guarantee the accepted (negligible) risk of key exposure.

How?

Outline

1. Introduction
   - Dependability Metrics and Cryptographic Modules
   - How to bound the risk of key exposure?
   - Contribution
2. Key Lifetimes in the Presence of Faults
   - Key Points
   - Threat Model
   - Security Parameters
3. Cryptographic Key Reliable Lifetimes
   - Selecting Key Lifetimes
   - Reliability Modeling
4. Using the framework
   - Cryptographic Key Reliable Lifetimes
   - Dependable Crypto Infrastructures
   - Hazard Rates and Minimal CKFT Values

Contribution

Adapting reliability modeling techniques to crypto systems

- Introduce two security metrics: *Cryptographic Key Failure Tolerance* and *Cryptographic Key Reliable Lifetime*
- Offer a first framework that enables to bound the the risk of key exposure in the presence of faults by:
  - Modeling the reliability of cryptographic *infrastructures* and
  - Relating their failure rates,
  - the failure tolerance of *cryptographic keys*,
  - and an accepted (negligible) error-bound,
  - to the *lifetimes* of keys.

ANDXOR

Related Work

Complementarity

1. Existing guidelines to selection of keys and lifetimes;
2. Fault diagnosis and tolerance techniques aimed at increasing the dependability of cryptographic systems.

ANDXOR

Related Work

Complementarity

1. Existing guidelines to selection of keys and lifetimes;
2. Fault diagnosis and tolerance techniques aimed at increasing the dependability of cryptographic systems.

ANDXOR

Outline

1. Introduction
   - Dependability Metrics and Cryptographic Modules
   - How to bound the risk of key exposure?
   - Contribution
2. Key Lifetimes in the Presence of Faults
   - Key Points
   - Threat Model
   - Security Parameters
3. Cryptographic Key Reliable Lifetimes
   - Selecting Key Lifetimes
   - Reliability Modeling
4. Using the framework
   - Cryptographic Key Reliable Lifetimes
   - Dependable Crypto Infrastructures
   - Hazard Rates and Minimal CKFT Values

ANDXOR

Selecting Key Lifetimes in the Presence of Faults

Key Points

Key Points

1. Environmental conditions;
2. The failure tolerance of cryptographic keys - 1st security parameter;
3. Accepted (negligible) risk of key exposure: or the desired security margin - 2nd security parameter;
4. Failure rate: the rate of occurrence for incorrect values at the cryptographic module user interface - 3rd security parameter.

Selecting Key Lifetimes in the Presence of Faults

Key Points

Key Points

1. Environmental conditions;
2. The failure tolerance of cryptographic keys - 1st security parameter;
3. Accepted (negligible) risk of key exposure: or the desired security margin - 2nd security parameter;
4. Failure rate: the rate of occurrence for incorrect values at the cryptographic module user interface - 3rd security parameter.

ANDXOR

Selecting Key Lifetimes in the Presence of Faults

Key Points

Key Points

1. Environmental conditions;
2. The failure tolerance of cryptographic keys - 1st security parameter;
3. Accepted (negligible) risk of key exposure: or the desired security margin - 2nd security parameter;
4. Failure rate: the rate of occurrence for incorrect values at the cryptographic module user interface - 3rd security parameter.

ANDXOR

Selecting Key Lifetimes in the Presence of Faults

Key Points

Key Points

1. Environmental conditions;
2. The failure tolerance of cryptographic keys - 1st security parameter;
3. Accepted (negligible) risk of key exposure: or the desired security margin - 2nd security parameter;
4. Failure rate: the rate of occurrence for incorrect values at the cryptographic module user interface - 3rd security parameter.

ANDXOR

Outline

1. Introduction
   - Dependability Metrics and Cryptographic Modules
   - How to bound the risk of key exposure?
   - Contribution
2. Key Lifetimes in the Presence of Faults
   - Key Points
   - Threat Model
   - Security Parameters
3. Cryptographic Key Reliable Lifetimes
   - Selecting Key Lifetimes
   - Reliability Modeling
4. Using the framework
   - Cryptographic Key Reliable Lifetimes
   - Dependable Crypto Infrastructures
   - Hazard Rates and Minimal CKFT Values

Environmental Conditions

Context

A black-box scenario characterized by the occurrence or activation of faults at *standard environmental conditions*

Assumption 1

The security of cryptographic modules will not be compromised by any deliberate or accidental excursions outside their normal operating ranges of environmental conditions.

Example

The module has been designed according to today's security standards (e.g, [FIPS 140-2]) to operate, or to respond, in a safe way also with widely varying environmental conditions;

The computing devices can be simply kept in a controlled environment (e.g., a network-attached HSM working in a controlled data center).

Threat Model

An Opportunistic Model

Passive Fault Attacks

- The attacker does only observes failures as they are occurring,
- tries to exploit them in an opportunistic way, and
- does not deliberately induce faults.

Example

A remote attacker may observe erroneous digitally-signed objects stored in X.500 Directory Services.

Outline

1. Introduction
   - Dependability Metrics and Cryptographic Modules
   - How to bound the risk of key exposure?
   - Contribution
2. Key Lifetimes in the Presence of Faults
   - Key Points
   - Threat Model
   - Security Parameters
3. Cryptographic Key Reliable Lifetimes
   - Selecting Key Lifetimes
   - Reliability Modeling
4. Using the framework
   - Cryptographic Key Reliable Lifetimes
   - Dependable Crypto Infrastructures
   - Hazard Rates and Minimal CKFT Values

ANDXOR

Cryptographic Key Failure Tolerance: a Security Metric

1st Security Parameter

Definition

Let B be a black-box implementing a cryptographic scheme S and containing a secret key K that is inaccessible to the outside world, and with the set of security parameter(s) P.
The Cryptographic Key Failure Tolerance, $CKFT^{m}_{K_{(S,P)}} \in \mathbb{Z}^{0}_{+}$, is defined to be the maximum number of faulty values, occurring according to the fault model identified by the label 'm', that B can output through its cryptographic protocol before K gets exposed by a fault-attack

Cryptographic Key Failure Tolerance

1st Security Parameter - ctd

Remark

In the presence of fault-attacks, the CKFT is a security parameter. As the value assumed by this metric increases, the probability of succeeding in a fault-attack within time T decreases.

Note

If the *CKFT* of a a given key is equal to 0, then K do not tolerate *any* failure. Hence it is sufficient to *output* a single faulty value in order to expose the key material.

Cryptographic Key Failure Tolerance Values for some Cryptographic Schemes

Crypto Scheme + Sec. Parameter(s)	Fault Model	*CKFT*	Author(s)	Year
Fiat-Shamir Id. Scheme ($t = n$)	∼1bit	$O(n)$	*Boneh, et al.*	1996
RSA (1024 bit)	1bit	$O(n)$	*Boneh, et al.*	1996
Schnorr's Id. Protocol ($p = a, q = n$)	1bit	$n \cdot \log 4n$	*Boneh, et al.*	1996
RSA+CRT	1bit	0	*Lenstra*	1997
AES	1byte	1	*Piret, et al.*	2003
AES (n=128)	1bit	49	*Giraud*	2003
AES (n=128)	1byte	249	*Giraud*	2003
KHAZAD	1byte	2	*Piret, et al.*	2003

Table: Some CKFT values

Cryptographic Key Failure Tolerance Values for some Cryptographic Schemes

Crypto Scheme + Sec. Parameter(s)	Fault Model	*CKFT*	Author(s)	Year
Fiat-Shamir Id. Scheme ($t = n$)	$\sim$1bit	$O(n)$	*Boneh, et al.*	1996
RSA (1024 bit)	1bit	$O(n)$	*Boneh, et al.*	1996
Schnorr's Id. Protocol ($p = a, q = n$)	1bit	$n \cdot \log 4n$	*Boneh, et al.*	1996
RSA+CRT	1bit	0	*Lenstra*	1997
AES	1byte	1	*Piret, et al.*	2003
AES (n=128)	1bit	49	*Giraud*	2003
AES (n=128)	1byte	249	*Giraud*	2003
KHAZAD	1byte	2	*Piret, et al.*	2003

Table: Some CKFT values

Cryptographic Key Failure Tolerance Values for some Cryptographic Schemes

ctd

Note

Denote the set of all cryptographic keys with failure tolerance f under the fault model m, C_f^m.

Obviously, new fault attacks or improvements to the key-extraction steps of already existing attacks can determine new failure tolerance values for a given set of keys.

Example

RSA keys - used by CRT-based implementations - passed from C_1^{1bit} to C_0^{1bit}; due to the beautiful refinement by Lenstra to the Boneh *et al.* attack.

ANDXOR

Cryptographic Key Failure Tolerance Values for some Cryptographic Schemes

ctd

Note

Denote the set of all cryptographic keys with failure tolerance f under the fault model m, C_f^m.
Obviously, new fault attacks or improvements to the key-extraction steps of already existing attacks can determine new failure tolerance values for a given set of keys.

Example

RSA keys - used by CRT-based implementations - passed from C_1^{1bit} to C_0^{1bit}; due to the beautiful refinement by Lenstra to the Boneh *et al.* attack.

ANDXOR

Accepted Error-Bound

2nd Security Parameter

Desired Security Margin

It can assume every desired value in the interval $(0, 1)$. Typical values are 2^{-40} or *lower*.

ANDXOR

Failure Rates

3rd Security Parameter

μ^m

The failure rate, μ^m, is the rate of occurrence of incorrect values at the user interface of a given cryptographic module – considering the fault model *m*.

- A quantity affected negatively by the *topology* of crypto modules;
- Building statistically justifiable confidence in extremely low failure-rates may be onerous.

We should expect low failure rates from crypto modules. . . Therefore: How realistic is a Passive Fault Attack?

How realistic is a Passive Fault Attack?

An example dated 9th July 2003: Bignum code and RSA signatures with Cryptlib

- On Sat 12th July the author, following an bug report dated 9th July, announce that due to a problem deep down in the bignum code used by the RSA implementation, in some rare occasions the toolkit was computing erroneous RSA signatures;
- The MTTF was less than 400 seconds (10^{-5} *failures/hours*);
- Though the high failure rate, this dormant fault has remained unnoticed for long time in many systems based on Cryptlib (and OpenSSL as well). . . And someone that had noticed that issue, was tolerating it!
- It was tricky to find the problem - In order to activate it, an exact combination of data values in the public/private key and data to sign was needed.

How realistic is a Passive Fault Attack?

An example dated 9th July 2003: Bignum code and RSA signatures with Cryptlib - ctd

Incorrect

```
int rsaDecrypt( CRYPT_INFO *cryptInfo,
                BYTE *buffer, int noBytes )
{ /* ... snip ... */

  /* computing:
   * p2 = ((C mod p) **exponent1) mod p;
   * q2 = ((C mod q) **exponent1) mod p;
   * ... */

  /* p2 = p2 - q2;
   * if p2 < 0 then p2 = p2 + p */
  CK( BN_sub( p2, p2, q2 ) );

  if( p2->neg )
    CK( BN_add( p2, p2, p ));
  /* ... */

}
%
```

Correct

```
int rsaDecrypt( CRYPT_INFO *cryptInfo,
                BYTE *buffer, int noBytes )
{ /* ... snip ... */

  /* p2 = p2 - q2;
   * if p2 < 0 then p2 = p2 + p.In some
   * extremely rare cases
   * (q2 large, p2 small) we have to
   * add p twice to get p2 positive
   */

  CK( BN_sub( p2, p2, q2 ) );

  while( p2->neg ) {
    CK( BN_add( p2, p2, p ) );

    if( bnStatusError( bnStatus ))
      return(getBnStatus(bnStatus));
  }

  /* ... */
}
```

Outline

1. Introduction
   - Dependability Metrics and Cryptographic Modules
   - How to bound the risk of key exposure?
   - Contribution
2. Key Lifetimes in the Presence of Faults
   - Key Points
   - Threat Model
   - Security Parameters
3. Cryptographic Key Reliable Lifetimes
   - Selecting Key Lifetimes
   - Reliability Modeling
4. Using the framework
   - Cryptographic Key Reliable Lifetimes
   - Dependable Crypto Infrastructures
   - Hazard Rates and Minimal CKFT Values

ANDXOR

Bounding the Risk of Key Exposure

In order to limit the risk of key exposure, it is necessary to limit the lifetime of keys so that the key material will no longer be used when the reliability of the computing system falls below the required level.

CKRL: a Security Metric

Definition

Let B be a black-box implementing a cryptographic scheme S and containing a secret key $K \in C_f^m$.
The *Cryptographic Key Reliable Lifetime*, $CKRL_K^{\epsilon,m}$, is defined to be the longest period of time, elapsed from the activation of the key-material t_R, after which the reliability of B, $R(t_R)$, has fallen below the level required to enforce the security margin ϵ - considering the fault model identified by m.

ANDXOR

CKRL

Estimation Methodology

1. Given **M**, the accepted error-bound ϵ, and the failure tolerance for a given key $CKFT^{m}_{K(S,P)}$
2. determine the reliability level $R(t_R)$ necessary to enforce the security margin.
3. Model the reliability of specific *infrastructures* and determine the failure-rate μ^{m}_{Infr} for each fault model $m \in \mathbf{M}$.
4. The resulting values are used to compute the respective *reliabile lifes* for the given infrastructure, t^{m}_{R}
5. The smallest mission duration is the upper bound to the lifetime of the key $K_{S,P}$: $CKRL^{\epsilon,\mathbf{M}}_{K}$.

ANDXOR

CKRL

Estimation Methodology

1. Given **M**, the accepted error-bound ϵ, and the failure tolerance for a given key $CKFT^{m}_{K(S,P)}$
2. determine the reliability level $R(t_R)$ necessary to enforce the security margin.
3. Model the reliability of specific *infrastructures* and determine the failure-rate μ^{m}_{Infr} for each fault model $m \in \mathbf{M}$.
4. The resulting values are used to compute the respective *reliabile lifes* for the given infrastructure, t^{m}_{R}
5. The smallest mission duration is the upper bound to the lifetime of the key $K_{S,P}$: $CKRL^{\epsilon,\mathbf{M}}_{K}$.

ANDXOR

CKRL

Estimation Methodology

1. Given **M**, the accepted error-bound ϵ, and the failure tolerance for a given key $CKFT^{m}_{K(S,P)}$
2. determine the reliability level $R(t_R)$ necessary to enforce the security margin.
3. Model the reliability of specific *infrastructures* and determine the failure-rate μ^{m}_{Infr} for each fault model $m \in \mathbf{M}$.
4. The resulting values are used to compute the respective *reliabile lifes* for the given infrastructure, t^{m}_{R}
5. The smallest mission duration is the upper bound to the lifetime of the key $K_{S,P}$: $CKRL^{\epsilon,\mathbf{M}}_{K}$.

CKRL

Estimation Methodology

1. Given **M**, the accepted error-bound ϵ, and the failure tolerance for a given key $CKFT^{m}_{K(S,P)}$
2. determine the reliability level $R(t_R)$ necessary to enforce the security margin.
3. Model the reliability of specific *infrastructures* and determine the failure-rate μ^{m}_{Infr} for each fault model $m \in \mathbf{M}$.
4. The resulting values are used to compute the respective *reliabile lifes* for the given infrastructure, t^{m}_{R}
5. The smallest mission duration is the upper bound to the lifetime of the key $K_{S,P}$: $CKRL^{\epsilon,\mathbf{M}}_{K}$.

CKRL

Estimation Methodology

1. Given **M**, the accepted error-bound ϵ, and the failure tolerance for a given key $CKFT^{m}_{K(S,P)}$
2. determine the reliability level $R(t_R)$ necessary to enforce the security margin.
3. Model the reliability of specific *infrastructures* and determine the failure-rate μ^{m}_{Infr} for each fault model $m \in \mathbf{M}$.
4. The resulting values are used to compute the respective *reliabile lifes* for the given infrastructure, t^{m}_{R}
5. The smallest mission duration is the upper bound to the lifetime of the key $K_{S,P}$: $CKRL^{\epsilon,\mathbf{M}}_{K}$.

Outline

1. Introduction
   - Dependability Metrics and Cryptographic Modules
   - How to bound the risk of key exposure?
   - Contribution
2. Key Lifetimes in the Presence of Faults
   - Key Points
   - Threat Model
   - Security Parameters
3. Cryptographic Key Reliable Lifetimes
   - Selecting Key Lifetimes
   - Reliability Modeling
4. Using the framework
   - Cryptographic Key Reliable Lifetimes
   - Dependable Crypto Infrastructures
   - Hazard Rates and Minimal CKFT Values

ANDXOR

Reliability

- Let T be a random variable - time of occurrence of faulty values;
- Let $F(T)$ be the distribution of T;
- Assume the system fails according the the exponential distribution;
- Let the (pdf) be
  $F(T) = \mu e^{-\mu(T-\gamma)}, \quad f(T) \geq 0, \quad \mu \geq 0, \quad T \geq 0 \text{ or } \gamma$
- The (cdf): $Q(T) = 1 - e^{-\mu(T-\gamma)}$
- The reliability function:
  $R(T) = 1 - Q(T) = e^{-\mu(T-\gamma)}, \quad 0 \leq R(T) \leq 1$

ANDXOR

Single Cryptographic Modules Implementing a Generic Cryptographic Scheme

Failure Condition

The system is considered to be functioning as long as the key material has not been exposed (i.e., as long as the number of failures is less than or equal to f) with a probability greater than ϵ.

ANDXOR

Single Crypto Module

The Cryptographic Key can be viewed as. . .

- A pool of $f + 1$ of identical,
- non-repairable sub-systems,
- characterized by a failure rate μ,
- under the fault model *m*.

Single Crypto Module

pool

0	1	· · ·	· · ·	· · ·	· · ·	f	f+1

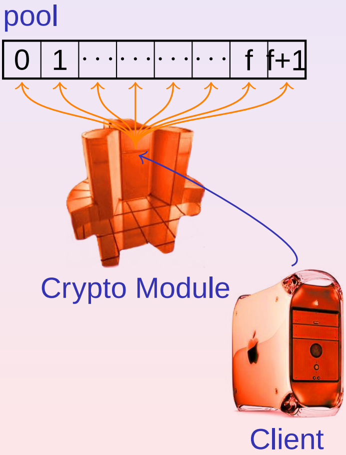
Crypto Module

Client

The Cryptographic Key can be viewed as. . .

- A pool of $f + 1$ of identical,
- non-repairable sub-systems,
- characterized by a failure rate μ,
- under the fault model m.

Single Crypto Module

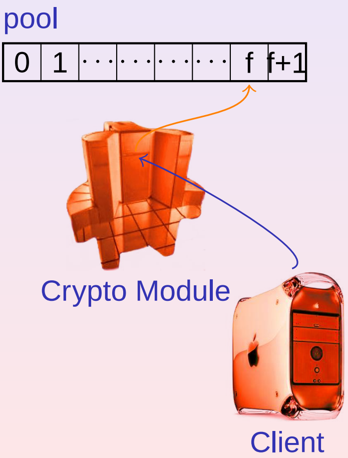


The Cryptographic Key can be viewed as. . .

- A pool of $f + 1$ of identical,
- non-repairable sub-systems,
- characterized by a failure rate μ,
- under the fault model m.

The System provides service ”in parallel”

Single Crypto Module



pool

0 | 1 | · · · | · · · | · · · | · · · | f | f+1

Crypto Module

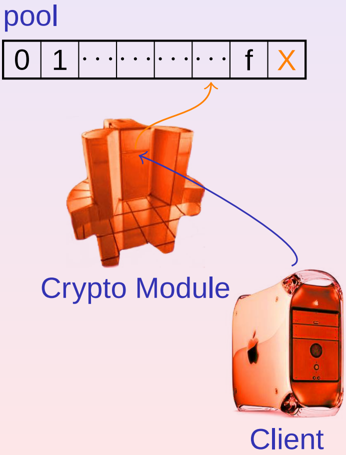
Client

The Cryptographic Key can be viewed as. . .

- A pool of $f + 1$ of identical,
- non-repairable sub-systems,
- characterized by a failure rate μ,
- under the fault model m.

As soon as a failure occurs the number of sub-systems decreases by one unit

Single Crypto Module



pool

0	1	···	···	···	···	f	X

Crypto Module

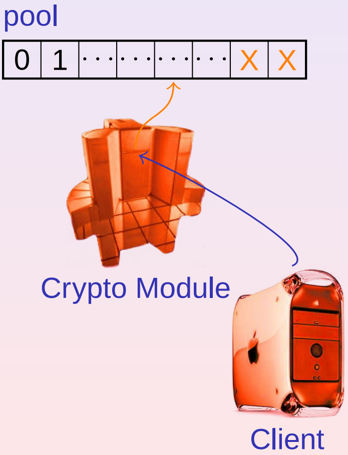
Client

The Cryptographic Key can be viewed as. . .

- A pool of $f + 1$ of identical,
- non-repairable sub-systems,
- characterized by a failure rate μ,
- under the fault model *m*.

As soon as a failure occurs the number of sub-systems decreases by one unit

Single Crypto Module

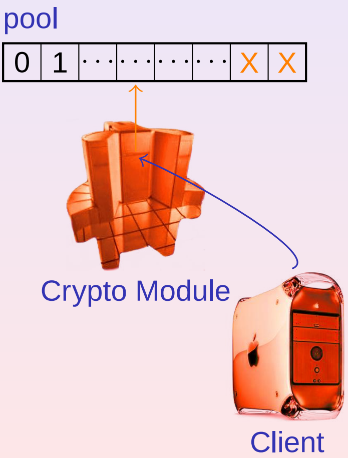


The Cryptographic Key can be viewed as. . .

- A pool of $f + 1$ of identical,
- non-repairable sub-systems,
- characterized by a failure rate μ,
- under the fault model *m*.

As soon as a failure occurs the number of sub-systems decreases by one unit

Single Crypto Module



pool

0	1	· · ·	· · ·	· · ·	· · ·	X	X

Crypto Module

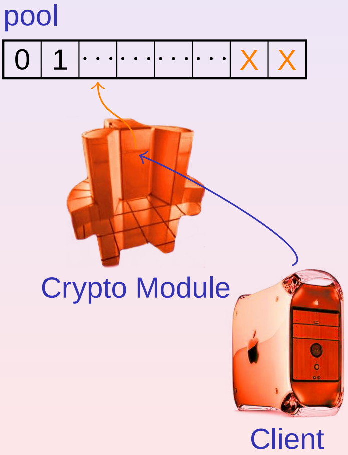
Client

The Cryptographic Key can be viewed as. . .

- A pool of $f+1$ of identical,
- non-repairable sub-systems,
- characterized by a failure rate μ,
- under the fault model *m*.

As soon as a failure occurs the number of sub-systems decreases by one unit

Single Crypto Module



pool

0	1	· · ·	· · ·	· · ·	· · ·	X	X

Crypto Module

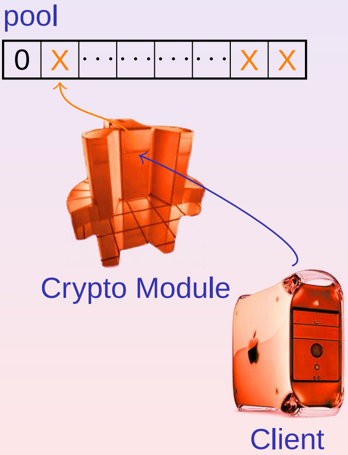
Client

The Cryptographic Key can be viewed as...

- A pool of $f + 1$ of identical,
- non-repairable sub-systems,
- characterized by a failure rate μ,
- under the fault model *m*.

As soon as a failure occurs the number of sub-systems decreases by one unit

Single Crypto Module



pool

0	X	· · ·	· · ·	· · ·	· · ·	X	X

Crypto Module

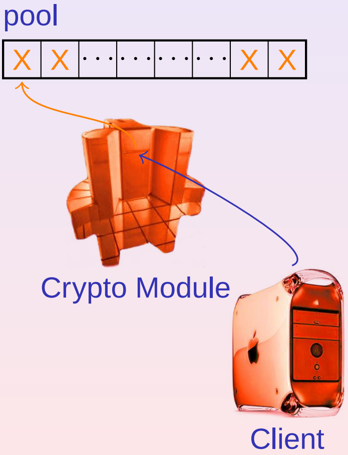
Client

The Cryptographic Key can be viewed as. . .

- A pool of $f + 1$ of identical,
- non-repairable sub-systems,
- characterized by a failure rate μ,
- under the fault model *m*.

As soon as a failure occurs the number of sub-systems decreases by one unit

Single Crypto Module



Alert

After f+1 faulty outputs
the key material is exposed

ANDXOR

Single Crypto Module

ctd

Given ϵ:

$$R(T) = 1 - \prod_{i=1}^{f+1} Q_i(T) \geq 1 - \epsilon \tag{1}$$

The subsystems are identical, thence:

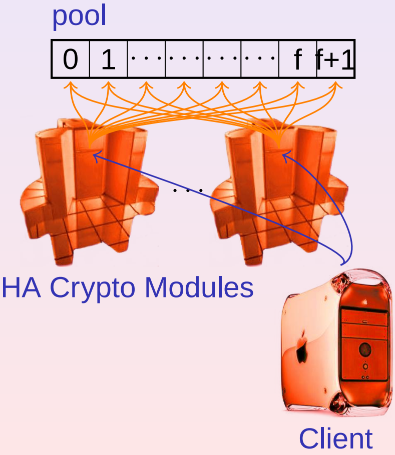
$$R(T) = e^{-\mu(T-\gamma)} \geq 1 - \sqrt[f+1]{\epsilon} \tag{2}$$

Therefore, the key lifetime for $K_{S,P}$, $L(K_{S,P})$, must be:

$$L(K_{S,P}) \leq CKRL_K^{\epsilon,m} = t_R = \gamma - \frac{\ln(1 - \sqrt[f+1]{\epsilon})}{\mu^m} \tag{3}$$

ANDXOR

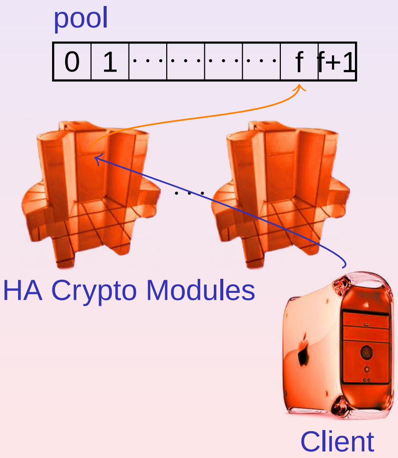
HA Crypto Infrastructures



Infrastructure

- l-Different Nodes (i.e, heterogeneous failure rates, μ_l^m);
- Independent;
- l-Active activation-model;
- Sharing the key-material with failure tolerance f.
- All the nodes start to provide service simultaneously.

HA Crypto Infrastructures

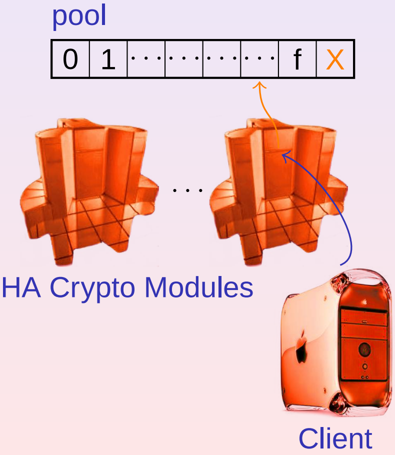


Infrastructure

- l-Different Nodes (i.e, heterogeneous failure rates, μ_l^m);
- Independent;
- l-Active activation-model;
- Sharing the key-material with failure tolerance f.
- All the nodes start to provide service simultaneously.

In this set-up the failures of all l-nodes are *cumulative*

HA Crypto Infrastructures



pool

0	1	· · ·	· · ·	· · ·	· · ·	f	X

· · ·

HA Crypto Modules

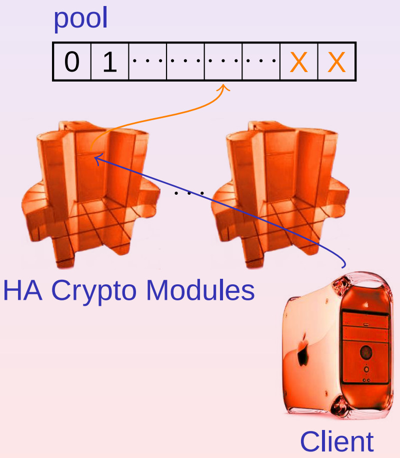
Client

Infrastructure

- l-Different Nodes (i.e, heterogeneous failure rates, μ_l^m);
- Independent;
- l-Active activation-model;
- Sharing the key-material with failure tolerance f.
- All the nodes start to provide service simultaneously.

In this set-up the failures of all l-nodes are *cumulative*

HA Crypto Infrastructures



pool

0	1	···	···	···	···	X	X

···

HA Crypto Modules

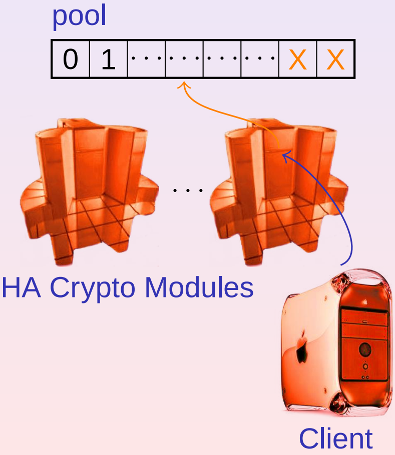
Client

Infrastructure

- l-Different Nodes (i.e, heterogeneous failure rates, μ_l^m);
- Independent;
- l-Active activation-model;
- Sharing the key-material with failure tolerance f.
- All the nodes start to provide service simultaneously.

In this set-up the failures of all l-nodes are *cumulative*

HA Crypto Infrastructures

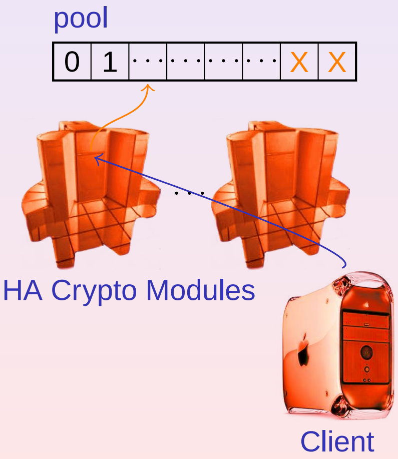


Infrastructure

- *l*-Different Nodes (i.e, heterogeneous failure rates, μ_l^m);
- Independent;
- *l*-Active activation-model;
- Sharing the key-material with failure tolerance *f*.
- All the nodes start to provide service simultaneously.

In this set-up the failures of all *l*-nodes are *cumulative*

HA Crypto Infrastructures

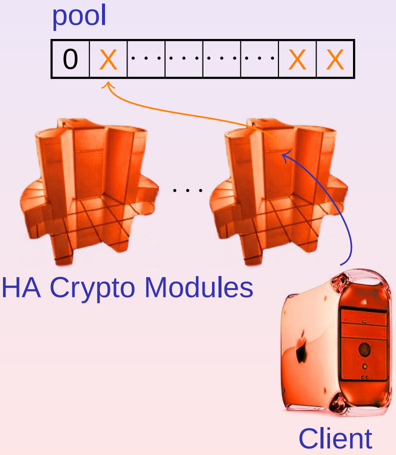


Infrastructure

- l-Different Nodes (i.e, heterogeneous failure rates, μ_l^m);
- Independent;
- l-Active activation-model;
- Sharing the key-material with failure tolerance f.
- All the nodes start to provide service simultaneously.

In this set-up the failures of all l-nodes are *cumulative*

HA Crypto Infrastructures

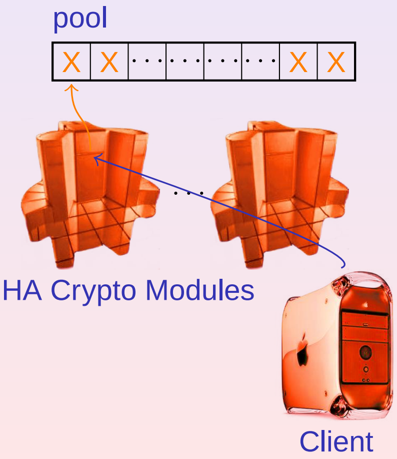


Infrastructure

- l-Different Nodes (i.e, heterogeneous failure rates, μ_l^m);
- Independent;
- l-Active activation-model;
- Sharing the key-material with failure tolerance f.
- All the nodes start to provide service simultaneously.

In this set-up the failures of all l-nodes are *cumulative*

HA Crypto Infrastructures



Infrastructure

- l-Different Nodes (i.e, heterogeneous failure rates, μ_l^m);
- Independent;
- l-Active activation-model;
- Sharing the key-material with failure tolerance f.
- All the nodes start to provide service simultaneously.

In this set-up the failures of all l-nodes are *cumulative*

HA Crypto Infrastructures
ctd

Hence, the HA (parallel) system should be modeled as a *series of nodes* w.r.t. PFA:

$$R_{\mathrm{HA}}(T) = \prod_{i=1}^{l} R_i(T) = e^{-\sum_{i=1}^{l} \mu_i^m (T-\gamma)} \tag{4}$$

This is equivalent to the reliability of a system with failure rate $\mu_{\mathrm{HA}} = \sum_{i=1}^{l} \mu_i^m$.
Using (3) is possible to compute the reliable life of the key $K_{(S,P)}$:

$$L(K_{S,P}) \leq CKRL_K^{\epsilon,m} = t_R = \gamma - \frac{\ln(1 - \sqrt[f+1]{\epsilon})}{\sum_{i=1}^{l} \mu_i^m} \tag{5}$$

Scaling-Out may be an Hazard

Topology matters

- The number of nodes present in the active-active model affects one of the security parameters;
- The use of cryptographic modules with very low failure rates becomes especially critical when its necessary to share the key-material among the nodes of an highly available infrastructure.

Scaling-Out may be an Hazard. . . and the Kent's Law

Kent's Law

"The useful lifetime of a public key certificate is inversely proportional to the number of things it's good for"

. . . and the reliable lifetime of a secret key is inversely proportional also to the number of computing systems that are using it

Using this framework

- Compute the reliable lifetime of keys for any cryptographic scheme implemented in generic cryptographic modules;
- Select cryptographic infrastructures that can provide the required level of reliability, if specific lifetimes and shemes are desired;
- Compute the cryptographic key failure tolerance required to guarantee the desired security margin – if a given cryptographic module is in use;
- Scaling-out cryptographic infrastructures;
- Estimate the risk of key exposure in presence of passive fault attacks.

A web application is available at:
`http://www.diaeresis.com/crypto/ckrl.html`

Using this framework

- Compute the reliable lifetime of keys for any cryptographic scheme implemented in generic cryptographic modules;
- Select cryptographic infrastructures that can provide the required level of reliability, if specific lifetimes and shemes are desired;
- Compute the cryptographic key failure tolerance required to guarantee the desired security margin – if a given cryptographic module is in use;
- Scaling-out cryptographic infrastructures;
- Estimate the risk of key exposure in presence of passive fault attacks.

A web application is available at:
`http://www.diaeresis.com/crypto/ckrl.html`

Using this framework

- Compute the reliable lifetime of keys for any cryptographic scheme implemented in generic cryptographic modules;
- Select cryptographic infrastructures that can provide the required level of reliability, if specific lifetimes and shemes are desired;
- Compute the cryptographic key failure tolerance required to guarantee the desired security margin – if a given cryptographic module is in use;
- Scaling-out cryptographic infrastructures;
- Estimate the risk of key exposure in presence of passive fault attacks.

A web application is available at:
`http://www.diaeresis.com/crypto/ckrl.html`

ANDXOR

Using this framework

- Compute the reliable lifetime of keys for any cryptographic scheme implemented in generic cryptographic modules;
- Select cryptographic infrastructures that can provide the required level of reliability, if specific lifetimes and shemes are desired;
- Compute the cryptographic key failure tolerance required to guarantee the desired security margin – if a given cryptographic module is in use;
- Scaling-out cryptographic infrastructures;
- Estimate the risk of key exposure in presence of passive fault attacks.

A web application is available at:
`http://www.diaeresis.com/crypto/ckrl.html`

ANDXOR

Using this framework

- Compute the reliable lifetime of keys for any cryptographic scheme implemented in generic cryptographic modules;
- Select cryptographic infrastructures that can provide the required level of reliability, if specific lifetimes and shemes are desired;
- Compute the cryptographic key failure tolerance required to guarantee the desired security margin – if a given cryptographic module is in use;
- Scaling-out cryptographic infrastructures;
- Estimate the risk of key exposure in presence of passive fault attacks.

A web application is available at:
`http://www.diaeresis.com/crypto/ckrl.html`

Outline

1. Introduction
   - Dependability Metrics and Cryptographic Modules
   - How to bound the risk of key exposure?
   - Contribution
2. Key Lifetimes in the Presence of Faults
   - Key Points
   - Threat Model
   - Security Parameters
3. Cryptographic Key Reliable Lifetimes
   - Selecting Key Lifetimes
   - Reliability Modeling
4. Using the framework
   - Cryptographic Key Reliable Lifetimes
   - Dependable Crypto Infrastructures
   - Hazard Rates and Minimal CKFT Values

ANDXOR

Upper Bounds to Key Lifetimes for Typical Failure Rates

Table: Upper Bounds to Key Lifetimes for typical failure rates, with an accepted error-bound $\epsilon = 2^{-40}$ and $\gamma = 0$. Failure rates are expressed in *failures/hours*; upper bounds to key lifetimes are expressed in *hours*.

C_f^m	μ_0^m	μ_1^m	μ_2^m	μ_3^m	μ_4^m	μ_5^m	μ_6^m
↓	1×10^{-15}	1×10^{-14}	1×10^{-13}	1×10^{-12}	1×10^{-11}	1×10^{-10}	1×10^{-9}
f=0	9.09×10^{2}	9.09×10^{1}	9.09×10^{0}	9.09×10^{-1}	9.09×10^{-2}	9.09×10^{-3}	9.09×10^{-4}
f=1	9.54×10^{8}	9.54×10^{7}	9.54×10^{6}	9.54×10^{5}	9.54×10^{4}	9.54×10^{3}	9.54×10^{2}
f=2	9.69×10^{10}	9.69×10^{9}	9.69×10^{8}	9.69×10^{7}	9.69×10^{6}	9.69×10^{5}	9.69×10^{4}
f=3	9.77×10^{11}	9.77×10^{10}	9.77×10^{9}	9.77×10^{8}	9.77×10^{7}	9.77×10^{6}	9.77×10^{5}
f=4	3.91×10^{12}	3.91×10^{11}	3.91×10^{10}	3.91×10^{9}	3.91×10^{8}	3.91×10^{7}	3.91×10^{6}
f=5	9.89×10^{12}	9.89×10^{11}	9.89×10^{10}	9.89×10^{9}	9.89×10^{8}	9.89×10^{7}	9.89×10^{6}
f=6	1.92×10^{13}	1.92×10^{12}	1.92×10^{11}	1.92×10^{10}	1.92×10^{9}	1.92×10^{8}	1.92×10^{7}
f=7	3.17×10^{13}	3.17×10^{12}	3.17×10^{11}	3.17×10^{10}	3.17×10^{9}	3.17×10^{8}	3.17×10^{7}
f=8	4.70×10^{13}	4.70×10^{12}	4.70×10^{11}	4.70×10^{10}	4.70×10^{9}	4.70×10^{8}	4.70×10^{7}
f=9	6.45×10^{13}	6.45×10^{12}	6.45×10^{11}	6.45×10^{10}	6.45×10^{9}	6.45×10^{8}	6.45×10^{7}
f=10	8.38×10^{13}	8.38×10^{12}	8.38×10^{11}	8.38×10^{10}	8.38×10^{9}	8.38×10^{8}	8.38×10^{7}
f=11	1.04×10^{14}	1.04×10^{13}	1.04×10^{12}	1.04×10^{11}	1.04×10^{10}	1.04×10^{9}	1.04×10^{8}

Upper Bounds to Key Lifetimes for Typical Failure Rates

Table: Upper Bounds to Key Lifetimes for typical failure rates, with an accepted error-bound $\epsilon = 2^{-40}$ and $\gamma = 0$. Failure rates are expressed in *failures/hours*; upper bounds to key lifetimes are expressed in *hours*.

C_f^m	μ_0^m	μ_1^m	μ_2^m	μ_3^m	μ_4^m	μ_5^m	μ_6^m
↓	1×10^{-15}	1×10^{-14}	1×10^{-13}	1×10^{-12}	1×10^{-11}	1×10^{-10}	1×10^{-9}
f=0	9.09×10^{2}	9.09×10^{1}	9.09×10^{0}	9.09×10^{-1}	9.09×10^{-2}	9.09×10^{-3}	9.09×10^{-4}
f=1	9.54×10^{8}	9.54×10^{7}	9.54×10^{6}	9.54×10^{5}	9.54×10^{4}	9.54×10^{3}	9.54×10^{2}
f=2	9.69×10^{10}	9.69×10^{9}	9.69×10^{8}	9.69×10^{7}	9.69×10^{6}	9.69×10^{5}	9.69×10^{4}
f=3	9.77×10^{11}	9.77×10^{10}	9.77×10^{9}	9.77×10^{8}	9.77×10^{7}	9.77×10^{6}	9.77×10^{5}
f=4	3.91×10^{12}	3.91×10^{11}	3.91×10^{10}	3.91×10^{9}	3.91×10^{8}	3.91×10^{7}	3.91×10^{6}
f=5	9.89×10^{12}	9.89×10^{11}	9.89×10^{10}	9.89×10^{9}	9.89×10^{8}	9.89×10^{7}	9.89×10^{6}
f=6	1.92×10^{13}	1.92×10^{12}	1.92×10^{11}	1.92×10^{10}	1.92×10^{9}	1.92×10^{8}	1.92×10^{7}
f=7	3.17×10^{13}	3.17×10^{12}	3.17×10^{11}	3.17×10^{10}	3.17×10^{9}	3.17×10^{8}	3.17×10^{7}
f=8	4.70×10^{13}	4.70×10^{12}	4.70×10^{11}	4.70×10^{10}	4.70×10^{9}	4.70×10^{8}	4.70×10^{7}
f=9	6.45×10^{13}	6.45×10^{12}	6.45×10^{11}	6.45×10^{10}	6.45×10^{9}	6.45×10^{8}	6.45×10^{7}
f=10	8.38×10^{13}	8.38×10^{12}	8.38×10^{11}	8.38×10^{10}	8.38×10^{9}	8.38×10^{8}	8.38×10^{7}
f=11	1.04×10^{14}	1.04×10^{13}	1.04×10^{12}	1.04×10^{11}	1.04×10^{10}	1.04×10^{9}	1.04×10^{8}

Outline

1. Introduction
   - Dependability Metrics and Cryptographic Modules
   - How to bound the risk of key exposure?
   - Contribution
2. Key Lifetimes in the Presence of Faults
   - Key Points
   - Threat Model
   - Security Parameters
3. Cryptographic Key Reliable Lifetimes
   - Selecting Key Lifetimes
   - Reliability Modeling
4. Using the framework
   - Cryptographic Key Reliable Lifetimes
   - Dependable Crypto Infrastructures
   - Hazard Rates and Minimal CKFT Values

ANDXOR

Using this framework

Selecting Dependable Cryptographic Infrastructures

Example

- Suppose one needs to choose a cryptographic infrastructure among a number of alternatives, each characterized by *different costs*
- The system must be able to use a key that tolerates 9 failures;
- The required lifetime is equal to 4 $\quad$ *years*.
- The desired security margin is 2^{-128}.
- Hence, the required failure rate of the infrastrcture must be not greater than $4 \times 10^{-9} \quad failures/hours$.

DXOR

Outline

1. Introduction
   - Dependability Metrics and Cryptographic Modules
   - How to bound the risk of key exposure?
   - Contribution
2. Key Lifetimes in the Presence of Faults
   - Key Points
   - Threat Model
   - Security Parameters
3. Cryptographic Key Reliable Lifetimes
   - Selecting Key Lifetimes
   - Reliability Modeling
4. Using the framework
   - Cryptographic Key Reliable Lifetimes
   - Dependable Crypto Infrastructures
   - Hazard Rates and Minimal CKFT Values

ANDXOR

Consequences. . .

If the desired error-bound is (just) $\epsilon = 2^{-40}$, in order to achieve a reliable life long at least one year:

- $\mu^m < 1.04 \times 10^{-16}$ *failures/hours* is required, if a key in C_0^m (e.g., RSA with CRT [*Boneh, et al.* 97]);
- $\mu^m < 1.09 \times 10^{-10}$ *failures/hours* is required, if a key in C_1^m (e.g., AES [*Piret et al.* 03]);

The required rates decreases further when lower error-bounds are desired.

The number of scenarios where keys in C_0^m and C_1^m find application in the presence of faults results to be remarkably limited.

. . . What is the risk of key exposure for typical lifetimes?

What is the risk of key exposure for typical lifetimes?

Credentials in C_0^m

Table: Effective risk of key exposure for credentials in C_0^m. The estimates are computed for a number of typical lifetimes (in years) and failure rates (*failures/hours*). The exponents are rounded up to the nearest integer.

T	μ_0^m	μ_1^m	μ_2^m	μ_3^m	μ_4^m	μ_5^m	μ_6^m
$\downarrow$	1×10^{-15}	1×10^{-14}	1×10^{-13}	1×10^{-12}	1×10^{-11}	1×10^{-10}	1×10^{-9}
1	2^{-36}	2^{-33}	2^{-30}	2^{-26}	2^{-23}	2^{-20}	2^{-16}
2	2^{-35}	2^{-32}	2^{-29}	2^{-25}	2^{-22}	2^{-19}	2^{-15}
3	2^{-35}	2^{-31}	2^{-28}	2^{-25}	2^{-21}	2^{-18}	2^{-15}
4	2^{-34}	2^{-31}	2^{-28}	2^{-24}	2^{-21}	2^{-18}	2^{-14}
5	2^{-34}	2^{-31}	2^{-27}	2^{-24}	2^{-21}	2^{-17}	2^{-14}
10	2^{-33}	2^{-30}	2^{-26}	2^{-23}	2^{-20}	2^{-16}	2^{-13}
20	2^{-32}	2^{-29}	2^{-25}	2^{-22}	2^{-19}	2^{-15}	2^{-12}

Many hazard rates are likely beyond those that usual security policies would consider acceptable.

What is the risk of key exposure for typical lifetimes?

Credentials in C_0^m

T	μ_0^m	μ_1^m	μ_2^m	μ_3^m	μ_4^m	μ_5^m	μ_6^m
↓	1×10^{-15}	1×10^{-14}	1×10^{-13}	1×10^{-12}	1×10^{-11}	1×10^{-10}	1×10^{-9}
1	2^{-36}	2^{-33}	2^{-30}	2^{-26}	2^{-23}	2^{-20}	2^{-16}
2	2^{-35}	2^{-32}	2^{-29}	2^{-25}	2^{-22}	2^{-19}	2^{-15}
3	2^{-35}	2^{-31}	2^{-28}	2^{-25}	2^{-21}	2^{-18}	2^{-15}
4	2^{-34}	2^{-31}	2^{-28}	2^{-24}	2^{-21}	2^{-18}	2^{-14}
5	2^{-34}	2^{-31}	2^{-27}	2^{-24}	2^{-21}	2^{-17}	2^{-14}
10	2^{-33}	2^{-30}	2^{-26}	2^{-23}	2^{-20}	2^{-16}	2^{-13}
20	2^{-32}	2^{-29}	2^{-25}	2^{-22}	2^{-19}	2^{-15}	2^{-12}

Many hazard rates are likely beyond those that usual security policies would consider acceptable.

Minimal CKFT values required to be immune to PFA

Let T_{max} the maximum lifetime of a key for any conceivable real application scenario.
The minimal CKFT is easily computable using:

$$CKFT^{m}_{min} = \lceil \log_{Q(T_{max}-\gamma)} \epsilon - 1 \rceil \tag{6}$$

Table: Minimal CKFT required to enable the selection of CKRL long up to $T_{max} = 200\ years$, for a number of ϵ and μ. $\gamma = 0$.

ϵ	μ^m_0	μ^m_1	μ^m_2	μ^m_3	μ^m_4	μ^m_5	μ^m_6
$\downarrow$	1×10^{-15}	1×10^{-14}	1×10^{-13}	1×10^{-12}	1×10^{-11}	1×10^{-10}	1×10^{-9}
2^{-40}	1	1	1	2	2	3	4
2^{-64}	2	2	2	3	4	5	6
2^{-80}	2	3	3	4	5	6	8
2^{-128}	4	4	5	6	8	10	13
2^{-256}	8	9	11	13	16	20	27

Minimal CKFT values required to be immune to PFA

ϵ	μ_0^m	μ_1^m	μ_2^m	μ_3^m	μ_4^m	μ_5^m	μ_6^m
$\downarrow$	1×10^{-15}	1×10^{-14}	1×10^{-13}	1×10^{-12}	1×10^{-11}	1×10^{-10}	1×10^{-9}
2^{-40}	1	1	1	2	2	3	4
2^{-64}	2	2	2	3	4	5	6
2^{-80}	2	3	3	4	5	6	8
2^{-128}	4	4	5	6	8	10	13
2^{-256}	8	9	11	13	16	20	27

Summary

- As long as the mathematical models of cryptography are not extended to the physical setting, reliability and security will remain stricly related.
- Security policies will have to be developed by carefully taking into account also the peculiarities inherent the execution of algorithms.
- The notions of CKFT and CKRL has been introduced.
- A first framework to bound the risk of key exposure against passive fault attacks has been proposed.

ANDXOR

Thanks!

Any Questions?

`adg (at) andxor (dot) com`

ANDXOR