A GENERALIZED BIRTHDAY ATTACK

Marc Girault[1] Robert Cohen[2] Mireille Campana[2]

[1] SEPT
42 rue des Coutures
BP 6243, 14066 Caen-Cedex, France

[2] CNET Paris-A
TIM
38-40 rue du Général Leclerc
92131 Issy-Les-Moulineaux, Paris, France

ABSTRACT

We generalize the birthday attack presented by Coppersmith at Crypto'85 which defrauded a Davies-Price message authentication scheme. We first study the birthday paradox and a variant for which some convergence results and related bounds are provided. Secondly, we generalize the Davies-Price scheme and show how the Coppersmith attack can be extended to this case. As a consequence, the case p=4 with DES (important when RSA with a 512-bit modulus is used for signature) appears not to be secure enough.

C.G. Guenther (Ed.): Advances in Cryptology - EUROCRYPT '88, LNCS 330, pp. 129-156, 1988.

INTRODUCTION

The public-key algorithms, which appeared in 1976 [1], permit among other things the attachment of digital signatures to messages. These signatures are generally produced in two steps. Firstly, the message is condensed (or hashed) into a short value: the imprint. Secondly, the secret function of a public-key digital signature scheme (for example RSA [2] or its variants) is applied to the imprint. This method of producing signatures is particularly convenient when the messages are long, because it would take too much time to apply the secret function to the entire message.

The main problem is to design hash-functions which are both efficient to compute and cryptographically secure. The first point can be achieved by using (properly) a secret-key block-cipher algorithm for which fast chips already exist (for example DES [3]). The second point requires the hash-function to be collision-free, i.e. it must be computationally infeasible to find distinct messages which hash to the same value. For if such messages were found, then a fraudor could, in an undetected manner, replace a properly signed message with another bogus one which has the same imprint (and hence the same signature).

Some general attacks on hash-functions have been described in the cryptanalytic literature [4]. Some of them (Yuval's attack [5], meet-in-the-middle attack [6]) are closely related to the famous "birthday paradox" and its variants. This paradox can be stated as follows: let r be the number of the pupils in a classroom and let q(r) be the probability that at least two pupils of this classroom have the same birthday; what is the minimal value of r such that $q(r) \geq \frac{1}{2}$? The answer is 23, much smaller than the value usually suggested by intuition (at least ours).

A variant of the birthday paradox is as follows: let r be the number of the pupils in two different classrooms and let p(r) be the probability that at least two pupils belonging to

different classrooms have the same birthday; what is the minimal value of r such that $p(r) \geq \frac{1}{2}$? The answer is now 17, but is somewhat more complicated to calculate, due to the fact that each classroom may itself contain some "twins".

In [7], Rabin introduced an efficient hash-function based on DES. However it was later shown that this scheme was subject to a meet-in-the-middle attack. In order to thwart such an attack, Davies & Price have proposed an improvement to the Rabin scheme, which consists of repeating the message twice [8] -or, by extension, using two initializing values and passing the message twice- but the new schemes were broken by Coppersmith [6], using a "triple birthday attack".

This paper aims at extending the Coppersmith attack to a general scheme using p initializing values and passing the message p times. It is organized in two main and almost independent parts: we first present a rigorous approach of the birthday paradox and its variant. We show in particular that, in both cases and under particular assumptions, the probability distribution of the number of "coincidences" converges towards a Poisson distribution, and we provide bounds for the error committed when using this limit to approximate a probability or a frequency distribution.

Secondly, we use these approximations to prove by induction that the Coppersmith attack can be extended to break the general scheme and we provide the number of "constrained" message blocks and the running time as a function of the number of initializing values.

As a consequence, the 4-pass Davies-Price scheme with DES appears not to be secure enough (Coppersmith already claimed it for the 3-pass scheme but without details). This result is particularly important when the imprint is obtained by concatenating the initializing values and the end-values. For, in that case, p=4 is the maximum number of possible passes if the modulus length of the signer is equal to 512 bits (a very usual length).

PART I: THE BIRTHDAY PARADOX

This part provides a rigorous analysis of the birthday paradox and its variant, as stated in the introduction. After having defined some symbols and recalled some classical results (section 1), we calculate (section 2) the exact probability to find i "coincidences" in:

a) a sample of size r drawn from a set of n elements with replacements (initial birthday problem);

b) in two samples of sizes r and s drawn from a set of n elements without replacements; and finally,

c) in two samples of sizes r and s drawn from a set of n elements with replacements (variant of birthday problem).
(The calculation of the last probability is a combination of the two previous ones.)

The asymptotical behaviour of these probabilities is then examined (section 3) in a particular but important case: $\frac{r^2}{2n}$, $\frac{s^2}{2n}$ and $\frac{rs}{n}$ have finite limits when r,s and $n \longrightarrow +\infty$; for each problem, the limit-distribution is shown to be a Poisson distribution, and this convergence is illustrated by some numerical results (section 4). Moreover, we provide very small bounds for the difference between a probability (or a frequency distribution) and its limit. This permits us to give some precise results (section 5) which will be used in the cryptanalysis of part II.

I.1 SYMBOLS AND DEFINITIONS

Let us define some symbols :

- E_r is the symbol for a sample of size r (drawn with or without replacements)
- $|E|$ denotes the number of elements of the set E

- $\binom{n}{k}$ is the notation for the binomial coefficient: $\frac{n!}{(n-k)!\ k!}$
- let $Q(x,y)$ be a quantity depending on x and y. Let $\mathcal{L}$ be a set of limit conditions on x and y. We denote by $\mathcal{L}\text{-lim}\ Q(x,y)$ the limit of $Q(x,y)$ when the conditions of $\mathcal{L}$ are satisfied
- the probability of the occurrence of the natural integer k in a Poisson distribution with parameter λ is equal to:

$$\mathcal{P}_\lambda(k) = e^{-\lambda}\ \frac{\lambda^k}{k!}$$

- the frequency distribution at α of a Poisson distribution with parameter λ is equal to:

$$\mathcal{F}_\lambda(\alpha) = \sum_{k=0}^{\alpha} e^{-\lambda}\ \frac{\lambda^k}{k!}$$

Let us recall that in the discrete case, and when all the possible events are equally probable, the probability $\mathbb{P}(E)$ of an event E is given by the ratio of the number of favorable events $N(E)$ to the number of possible events N :

$$\mathbb{P}(E) = \frac{N(E)}{N}$$

When drawings are made with replacements from a population of size n, we define the number of coincidences as the difference between the number of drawings and the number of distinct elements that have been drawn.

I.2 CALCULATION OF PROBABILITY

The meet-in-the-middle attack is related to the following problem, a variant of the birthday problem:

The drawing with replacements of r elements from a population of size n yields a first sample E_r. The drawing with replacements of s elements from the same population of size n yields a second sample E_s. What is the probability that exactly i elements belong to the two samples?

The probability $\mathbb{P}(|E_r \cap E_s| = i)$ that there are i distinct

elements in the intersection of the two samples is denoted by P(n,r,s,i) and is equal to:

$$P(n,r,s,i) = \mathbb{P}\left(\bigcup_{k=0}^{r-i} \bigcup_{l=0}^{s-i} \{|E_r|=r-k,\ |E_s|=s-1,\ |E_r \cap E_s|=i\}\right)$$

$$= \sum_{k=0}^{r-i} \sum_{l=0}^{s-i} \mathbb{P}(|E_r \cap E_s|=i / |E_r|=r-k, |E_s|=s-1)\ \mathbb{P}(|E_r|=r-k, |E_s|=s-1)$$

$$= \sum_{k=0}^{r-i} \sum_{l=0}^{s-i} \mathbb{P}(|E_r \cap E_s|=i / |E_r|=r-k, |E_s|=s-1)\ \mathbb{P}(|E_r|=r-k)\ \mathbb{P}(|E_s|=s-1)$$

(the last equality stands since the drawings are independent). Hence,

$$P(n,r,s,i) = \sum_{k=0}^{r-i} \sum_{l=0}^{s-i} Q(n,r,k)\ H(n,r-k,s-1,i)\ Q(n,s,1)$$

where:

- $Q(n,r,k) = \mathbb{P}(|E_r|=r-k)$ denotes the probability that k coincidences occur in the sample with replacements of r drawings from a population of size n,
- $H(n,r-k,s-1,i) = \mathbb{P}(|E_r \cap E_s|=i\ /|E_r|=r-k \cap |E_s|=s-1)$ is the probability that exactly i distinct elements have been drawn in the two (independent) samples (drawn with replacements, of respective sizes r and s) with respectively r-k and s-1 distinct elements: in other words, H(n,r-k,s-1,i) is the probability that the intersection of two independent samples drawn without replacement of respective sizes r-k and s-1 is made up of exactly i distinct elements.

I.2.1 EVALUATION OF PROBABILITY H

We first evaluate H(n,r,s,i). The problem can be stated as follows:

The drawing without replacement of r elements from a population of size n yields a first sample E_r . The drawing without replacement of s elements from the same population of

size n yields a second sample E_s. What is the probability that the intersection of the two samples is made up by exactly i elements?

The first sample yields r distinct elements drawn from n elements. Thus, i elements are drawn from among the r elements of the first sample and s-i among the n-r elements that have not been drawn. The probability distribution is the hypergeometric distribution:

$$H(n,r,s,i) = \frac{\binom{r}{i}\binom{n-r}{s-i}}{\binom{n}{s}}$$

I.2.2 EVALUATION OF PROBABILITY Q

We now evaluate Q(n,r,c), related to the birthday problem.

The drawing with replacements of r elements from a population of size n yields a sample E_r. What is the probability Q(n,r,c) that c coincidences occur in the sample?

The probability Q(n,r,c) is equal to the ratio of the number of favorable events to the number of possible events. If $r \geq n$ and $c < r-n$ then $Q(n,r,c) = 0$. If $r \leq n$, or if $r \geq n$ and $c \geq r-n$, then:

- the number of samples with replacements of size r drawn from a set of size n is equal to n^r,
- the r-c distinct elements drawn from among the n elements can be chosen in $\binom{n}{r-c}$ ways,
- the c coincidences are drawn from among the r-c elements. We choose from among the r drawings of the sample α_1 ones which correspond to the element n°1, then α_2 ones from among the remaining $r-\alpha_1$ which correspond to the element n°2, etc. up to the r-c distinct elements of the sample. There are

$\binom{r}{\alpha_1}\binom{r-\alpha_1}{\alpha_2}\cdots\binom{r-\alpha_1-\ldots-\alpha_{r-c-1}}{\alpha_{r-c}}$ possible orders for each (r-c)-vector of the set $\mathfrak{R}=\{(\alpha_1,\ldots,\alpha_{r-c}),$ with $c+1 \geq \alpha_j \geq 1$ for all j, having a sum equal to r$\}$. The product of these binomial coefficients can be simplified as: $\frac{r!}{\alpha_1!\ldots\alpha_{r-c}!}$.

The number of favorable events is obtained by taking the sum over the set $\mathfrak{R}$. Therefore the probability is:

$$Q(n,r,c) = \frac{\binom{n}{r-c}}{n^r} \sum_{(\alpha_1,\ldots,\alpha_{r-c})\in\mathfrak{R}} \frac{r!}{\alpha_1!\ldots\alpha_{r-c}!}$$

Remarks:

a) By direct computation, the probability that r distinct elements are drawn is also equal to the ratio of the $n(n-1)\ldots(n-r+1)$ favorable events to the n^r possible events. Hence: $Q(n,r,0) = \frac{n!}{(n-r)!\, n^r}$. For the "birthday paradox", this formula yields the number r: for n=365, r=23 is the lowest integer such that: $Q(365,r,0) < 0.5$.

b) Using, as in [9], the Poincaré formula, one obtains a formula which is easier to program. Let A_k denote the event "the element k is not drawn". Then the event "r-c elements in the sample E_r" can be written as:

$$\{|E_r| = r-c\} = \bigcup_{\{i_1,\ldots,i_n\}\in\mathcal{P}_{r-c}} \left(\bigcap_{j=1}^{r-c} A_{i_j}^c \bigcap \bigcap_{j=r-c+1}^{n} A_{i_j} \right)$$

where $\mathcal{P}_{r-c}$ is the set, having $\binom{n}{r-c}$ elements, of partitions of $\{1,\ldots,n\}$ in sets of r-c, and n-r+c elements. Using the relation $\mathbb{P}(A\cap B) = \mathbb{P}(A/B)\,\mathbb{P}(B)$, it follows:

$$\mathbb{P}\left(\bigcap_{j=1}^{r-c} A_{i_j}^c \bigcap \bigcap_{j=r-c+1}^{n} A_{i_j}\right) = \mathbb{P}\left(\bigcap_{j=1}^{r-c} A_{i_j}^c \,/\, \bigcap_{j=r-c+1}^{n} A_{i_j}\right) \mathbb{P}\left(\bigcap_{j=r-c+1}^{n} A_{i_j}\right)$$

The second term is easy to compute; for the first one we can use the Poincaré formula, since: $\mathbb{P}(A^c \cap B^c) = 1 - \mathbb{P}(A \cup B)$.

Since the probability does not depend on the partition of $\{1,\ldots,n\}$, it follows that:

$$Q(n,r,c) = \frac{\binom{n}{r-c}}{n^r} \sum_{\alpha=0}^{r-c} (-1)^\alpha \binom{r-c}{\alpha} \alpha^r$$

This formula differs from the one of [9] because the definitions of the coincidences are not the same.

I.3 ASYMPTOTICAL BEHAVIOUR

We now study the asymptotical behaviour of $P(n,r,s,i)$ when $\frac{r^2}{2n} \longrightarrow \lambda$, $\frac{s^2}{2n} \longrightarrow \mu$, $\frac{rs}{n} \longrightarrow \nu$, $r,s,n \longrightarrow +\infty$. We show that $Q(n,r,c)$ converges towards a Poisson distribution with parameter λ. Combining this result with the well-known convergence of the hypergeometric distribution of parameters n,r,s towards a Poisson distribution with parameter λ, we finally prove that $P(n,r,s,i)$ converges also towards this distribution. In other words, the number of elements belonging to both E_r and E_s is only slightly dependent on the fact that the samples have been drawn with or without replacements. This is due to the fact that we expect a very small number (about λ) of coincidences inside each sample.

Before starting, we recall that for any natural integer I and when $N,K \longrightarrow +\infty$:

$$\text{If } \frac{K^3}{N^2} \longrightarrow 0 \text{ then } \frac{N!}{(N-K)!} \sim N^K e^{-\frac{K^2}{2N}} \text{ and } \frac{N!}{(N-K+I)!} \sim N^{K-I} e^{-\frac{K^2}{2N}}$$

More precisely, one can prove that, for $\frac{K}{N} < \frac{1}{2}$:

$$e^{-\frac{K^2}{2N} + \frac{K}{2N} - \frac{K^3}{3N^2}} \leq \frac{N!}{N^K\ (N-K)!} \leq e^{-\frac{K^2}{2N} + \frac{K}{2N}} \qquad (1)$$

I.3.1 THE CONVERGENCE OF H

If $\{\frac{rs}{n} \to \nu,\ r,s,n \to +\infty\}$, it is well known [9] that the limit distribution of H(n,r,s,.) is a Poisson distribution:

$$\forall i \text{ fixed, if } \frac{rs}{n} \to \nu \text{ for } r,s,n \to +\infty, \text{ then } H(n,r,s,i) \to \mathcal{P}_\nu(i)$$

In particular, $H(n,r,s,0) \to e^{-\nu}$.

Remark:

In order to obtain bounds on the error for the probability P(n,r,s,i) with respect to the Poisson distribution with parameter $\nu = \frac{rs}{n}$, we first need to compute bounds relatively to H(n,r,s,i). Using the inequality (1), we obtain:

$$\mathcal{P}_\nu(i)\ e^{-i^2\frac{(r+s)}{rs} - 2\frac{r^2s+s^2r}{n^2}} \leq H(n,r,s,i) \leq \mathcal{P}_\nu(i)\ e^{2i\frac{(r+s)}{n}}$$

Therefore the error on the frequency distribution function $\mathbb{F}$, related to H, with respect to the frequency distribution function $\mathcal{F}_\nu$ related to the Poisson distribution with parameter $\nu = \frac{rs}{n}$ is:

$$|\mathbb{F}(\alpha) - \mathcal{F}_\nu(\alpha)| \leq \frac{(r+s)}{rs}\alpha^2 + \frac{3(r+s)}{n}\alpha + 2\frac{sr^2+rs^2}{n^2}$$

Example: If $n = 2^{64}$, $r=s= 2^{36}$, then $|\mathbb{F}(256) - \mathcal{F}_{256}(256)| \leq 2^{-16}$

I.3.2 THE CONVERGENCE OF Q

We study here the asymptotical behaviour of $Q(n,r,c)$ if $r^2/2n \to \lambda$, when $r,n \to +\infty$.

The most important part of $Q(n,r,c)$ comes from event "there are only pairs of coincidences". We wish to evaluate the contribution of every configuration of coincidences. Remember that:

$$Q(n,r,c) = \frac{\binom{n}{r-c}}{n^r} \sum_{(\alpha_1,\ldots,\alpha_{r-c})\in\mathcal{R}} \frac{r!}{\alpha_1!\ldots\alpha_{r-c}!}$$

We are going to divide $\mathcal{R}$ into some interesting subsets. In an event α of $\mathcal{R}$, only at most c components are not equal to 1 (if there are exactly c such components, then $\alpha_j = 2$ for every index and the others are equal to 1).

Let α be an $(r-c)$-vector of $\mathcal{R}$ with k components which are not equal to 1. As the product $\alpha_1!\ldots\alpha_{r-c}!$ is invariant by permutation, then the ratio $r!/\alpha_1!\ldots\alpha_{r-c}!$ will appear $\binom{r-c}{k}$ times in the sum. So

$$Q(n,r,c) = \frac{\binom{n}{r-c}}{n^r} \sum_{k=1}^{c} \frac{(r-c)!}{k!\ (r-c-k)!} \left(\sum_{(\alpha_1,\ldots,\alpha_k)\in\mathcal{R}_k} \frac{r!}{\alpha_1!\ldots\alpha_k!} \right)$$

where $\mathcal{R}_k = \{(\alpha_1,\ldots,\alpha_k)\in\{2,\ldots,c+1\}^k ; \sum_{j=1}^{k} \alpha_j = c+k, \text{ and } \alpha_1 \le \ldots \le \alpha_k\}$.

For c fixed, and $k \le c$, $\frac{r!}{(r-c-k)!} \sim r^{c+k}$, when $r \to +\infty$. Hence:

$$Q(n,r,c) \sim \frac{\binom{n}{r-c}}{n^r} (r-c)! \sum_{k=1}^{c} \frac{r^{c+k}}{k!} \gamma_k$$

$$= \frac{n!}{n^r\ (n-r-c)!} \frac{r^{2c}}{2^c c!} \left(1 + \frac{2^c c}{r} \gamma_{c-1} + \ldots + \frac{2^c c!}{r^{c-1}} \gamma_1 \right)$$

with

$$\gamma_k = \sum_{(\alpha_1,\ldots,\alpha_k)\in\mathcal{R}_k} \frac{1}{\alpha_1!\ldots\alpha_k!}$$

($\gamma_c = 2^{-c}$, for the c-vector defined by $\alpha_j = 2$, $j=1,\ldots,c$ is the only element of $\mathcal{R}_c$).

Finally, using obvious notation:

$$Q(n,r,c) \sim \frac{n!}{n^r\ (n-r+c)!}\ \frac{r^{2c}}{2^c\ c!}\ \left(1 + \frac{\gamma}{r}\right)$$

$$\sim \frac{e^{-\frac{r^2}{2n}}}{n^c}\ \frac{r^{2c}}{2^c\ c!}\ \left(1 + \frac{\gamma}{r}\right) \sim e^{-\frac{r^2}{2n}}\ \frac{\left(\frac{r^2}{2n}\right)^c}{c!}$$

Hence the convergence:

$$\forall c \text{ fixed, if } \frac{r^2}{2n} \to \lambda \text{ for } r,\ n \to +\infty, \text{ then } Q(n,r,c) \to \mathcal{P}_\lambda(c)$$

The limit is a Poisson distribution with parameter $\lambda = \lim_{r,n\to+\infty} \frac{r^2}{2n}$.

Remarks:

a) The probability of event "at least a coincidence is not a pair" can be dominated by the probability of event "an element is drawn at least three times", that is $\binom{r}{3}\ n\ \frac{n^{r-3}}{n^r}$. So:

$$\sum_{c=1}^{r} \frac{n!}{n^r(n-r-c)!}\ \frac{r!}{(r-2c)!\ 2^c c!}\ \frac{\gamma}{r} \le \frac{r^3}{6n^2}$$

b) Using the inequality (1), we obtain the inequality on $Q(n,r,c)$ related to the Poisson distribution $\mathcal{P}_\lambda$ with parameter $\lambda = \frac{r^2}{2n}$:

$$\mathcal{P}_\lambda(c)\, e^{-\frac{c^2}{n}-\frac{5c^2}{r}-\frac{r^3}{3n^2}} \le Q(n,r,c) \le \mathcal{P}_\lambda(c)\, e^{\frac{rc}{n}+\frac{r}{2n}+\frac{c}{r}-\frac{2c^2}{r}+\frac{r^3}{6n^2}}$$

We can evaluate the precision of approximation of frequency distribution F of the Q distribution by the frequency distribution $\mathcal{F}_\lambda$ of the Poisson distribution with parameter $\lambda = \frac{r^2}{2n}$:

$$|F(\alpha) - \mathcal{F}_\lambda(\alpha)| \le \frac{5}{r}\alpha^2 + \frac{3r}{n}\alpha + \frac{r^3}{3n^2}$$

Example: If $n = 2^{64}$, $r = 2^{36}$, then $|F(256) - \mathcal{F}_{128}(256)| \le 2^{-17}$

I.3.3 THE CONVERGENCE OF P(n,r,s,i)

Let $\mathcal{L}$ be the set of conditions $\{\frac{r^2}{2n} \to \lambda,\ \frac{s^2}{2n} \to \mu,\ r \to +\infty,\ s \to +\infty,\ n \to +\infty\}$. We study the $\mathcal{L}$-limit of:

$$P(n,r,s,i) = \sum_{k=0}^{r-i} \sum_{l=0}^{s-i} Q(n,r,k)\, H(n,r-k,s-l,i)\, Q(n,s,l)$$

1) Using (1) we obtain the following bounds for H(n,r-k,s-l,i):

$$H(n,r,s,i)\, \varphi_i(n,r,s,i,k,l) \le H(n,r-k,s-l,i),$$

with $\varphi_i(n,r,s,i,k,l) = \Psi(r,i,k;s,i,l)\, \Psi(n,r,k;n,s,l)\, e^{-\frac{k+l}{n-r-s}}$

where $\Psi(r,i,k;s,j,l) = e^{-\frac{k}{r}-\frac{k^2}{r-i}} \left(1-\frac{i}{r}\right)^k e^{-\frac{l}{s}-\frac{l^2}{s-j}} \left(1-\frac{j}{s}\right)^l$,

and:

$$H(n,r-k,s-l,i) \le H(n,r,s,i)\, \varphi_s(n,r,s,i,k,l),$$

with $\varphi_s(n,r,s,i,k,l) = \bar{\Psi}(n,r,i,k)\, \bar{\Psi}(n,s,i,l)\, e^{\frac{(k+l)^2}{n-r-s}+2(k+l)\frac{r+s}{n}}$

where $\bar{\Psi}(n,r,i,k) = e^{\frac{k^2}{r-i}+\frac{k}{r-i}+\frac{k}{n-r}}$.

For k and l fixed, we have:

$$\mathcal{L}\text{-lim } \varphi_i(n,r,s,i,k,l) = \mathcal{L}\text{-lim } \varphi_s(n,r,s,i,k,l) = 1.$$

2) Since the terms of the sum are positive, for α and β fixed:

$$P(n,r,s,i) \geq \sum_{k=0}^{\alpha} \sum_{l=0}^{\beta} Q(n,r,k)\ H(n,r-k,s-1,i)\ Q(n,s,l)$$

$$\geq H(n,r,s,i)\ \varphi_i(n,r,s,i,\alpha,\beta) \sum_{k=0}^{\alpha} Q(n,r,k) \sum_{l=0}^{\beta} Q(n,s,l)$$

Taking the $\mathcal{L}$-limit:

$$\mathcal{L}\text{-lim } P(n,r,s,i) \geq \mathcal{L}\text{-lim } H(n,r,s,i)\ \mathcal{F}_\lambda(\alpha)\ \mathcal{F}_\mu(\beta)$$

3) The double sum is broken into four parts, and we over estimate $H(n,r-k,s-1,i)$ by 1 (it is a probability) for $k \geq \alpha$ or $l \geq \beta$, and by a function of $H(n,r,s,i)$ for the last double sum. Therefore, $P(n,r,s,i)$ is bounded by:

$$H(n,r,s,i)\ \varphi_s(n,r,s,i,\alpha,\beta) \sum_{k=0}^{\alpha} \sum_{l=0}^{\beta} Q(n,r,k)\ Q(n,s,l)$$

$$+ \sum_{k=\alpha+1}^{r-i} Q(n,r,k) \sum_{l=0}^{\beta} Q(n,s,l) + \sum_{k=0}^{\alpha} Q(n,r,k) \sum_{l=\beta+1}^{s-i} Q(n,s,l)$$

$$+ \sum_{k=\alpha+1}^{r-i} Q(n,r,k) \sum_{l=\beta+1}^{s-i} Q(n,s,l)$$

By taking the $\mathcal{L}$-limit, we get:

$$\mathcal{L}\text{-lim } P(n,r,s,i) \leq \mathcal{L}\text{-lim } H(n,r,s,i)\ \mathcal{F}_\lambda(\alpha)\ \mathcal{F}_\mu(\beta)$$

$$+ (1-\mathcal{F}_\lambda(\alpha))\ \mathcal{F}_\mu(\beta) + \mathcal{F}_\lambda(\alpha)\ (1-\mathcal{F}_\mu(\beta)) + (1-\mathcal{F}_\lambda(\alpha))\ (1-\mathcal{F}_\mu(\beta))$$

4) If α and β tend to $+\infty$, the frequency distributions tend to 1 and the probabilities of drawings with or without replacement are identical:

$$\boxed{\mathcal{L}\text{-}\lim P(n,r,s,i) = \mathcal{L}\text{-}\lim H(n,r,s,i)}$$

If we add to $\mathcal{L}$ the condition $\frac{rs}{n} \to \nu$ of § I.3.1, we get:

$$\boxed{\begin{array}{l} \forall i \text{ fixed, if } \frac{r^2}{2n} \to \lambda, \quad \frac{s^2}{2n} \to \mu, \quad \frac{rs}{n} \to \nu \text{ for } r,s,n \to +\infty \\ \text{then:} \qquad P(n,r,s,i) \to \mathcal{P}_\nu(i) \end{array}}$$

The limit is a Poisson distribution of parameter $\nu = \lim_{r,s,n\to+\infty} \frac{rs}{n}$. In particular for $r=s=k\sqrt{n}$, we get a Poisson distribution with parameter k^2.

Remark:

Using the bounds on H, together with the previous inequalities, we obtain that the lower bound for P(n,r,s,i) is:

$$\mathcal{P}_\nu(i)\, e^{-i^2 \frac{(r+s)}{rs} - 2\frac{r^2s+s^2r}{n^2}}\, \varphi_i(n,r,s,i,\alpha,\beta)\, F_r(\alpha)\, F_s(\beta)$$

and the upper bound is:

$$\mathcal{P}_\nu(i)\, e^{2i\frac{(r+s)}{n}}\, \varphi_s(n,r,s,i,\alpha,\beta)\, F_r(\alpha)\, F_s(\beta)$$

$$+ (1-F_r(\alpha))\, F_s(\beta) + F_r(\alpha)\, (1-F_s(\beta)) + (1-F_r(\alpha))\, (1-F_s(\beta))$$

where here F_r is the frequency distribution of the $Q(n,r,.)$ distribution, and for arbitrary α and β.

I.4. NUMERICAL RESULTS

Some values of Q(n,r,c) and P(n,r,s,i) have been computed using the formulas of §I.2 (the formula used for Q was taken from remark b of §I.2.2). The numerical results illustrate the convergences when $r = s = \sqrt{n}$. The corresponding values of the Poisson distribution with parameter 0.5 and 1 are given for comparison.

c	Q(100,10,c)	Q(256,16,c)	Q(625,25,c)	$\mathcal{P}_{0.5}(c)$
c = 0	0.628	0.619	0.611	0.607
c = 1	0.310	0.308	0.307	0.303
c = 2	0.056	0.064	0.068	0.076
c = 3	0.004	0.007	0.009	0.013
c = 4	0.000	0.000	0.000	0.002
c = 5	0.000	0.000	0.000	0.000

i	P(100,10,10,i)	P(256,16,16,i)	P(625,25,25,i)	$\mathcal{P}_1(i)$
i = 0	0.366	0.367	0.365	0.368
i = 1	0.405	0.391	0.379	0.368
i = 2	0.179	0.182	0.182	0.184
i = 3	0.041	0.049	0.053	0.061
i = 4	0.005	0.008	0.010	0.015
i = 5	0.000	0.001	0.001	0.003
i = 6	0.000	0.000	0.000	0.001
i = 7	0.000	0.000	0.000	0.000

I.5 SOME USEFUL RESULTS FOR PART II

In the next part, some cryptanalytic attacks are exposed, based on the paradoxes we just have studied in previous sections. The probability of success of these attacks is calculated according to the numerical results we provide in this section.

We define the number n_ζ of twins between the samples $E_r=(x_1,\ldots,x_r)$ and $E_s=(y_1,\ldots,y_s)$ as the number of pairs (i,j) such that $x_i = y_j$. Since $n_\zeta \geq |E_r \cap E_s|$, we have:

$$\mathbb{P}(n_\zeta \geq i) \geq \mathbb{P}(|E_r \cap E_s| \geq i)$$

In the particular case i=1, the two probabilities are equal.

So, the meet-in-the-middle attack exposed in section II.1 has a probability of success S equal to $\mathbb{P}(|E_r \cap E_s| \geq 1)$ with $r=s=2^{32}$ and $n=2^{64}$ (hence $\nu = \frac{rs}{n} = 1$) and :

$$S = 1 - P(n,r,s,0) = 1 - \mathcal{P}_1(0) + \varepsilon = 1 - e^{-1} + \varepsilon \geq 0.632$$

(because the bounds provided in sections I.2 and I.3 allow us to show that $|\varepsilon| \leq 10^{-5}$).

If we now want the probability of success S to be $\geq 1-10^{-4}$, by changing only r and s (but preserving r=s both powers of 2), we can choose $r=s=2^{34}$ because $\nu=16$ and:

$$S = 1 - \mathcal{P}_{16}(0) + \varepsilon' = 1 - e^{-16} + \varepsilon' \geq 1-10^{-4}$$

(because $|\varepsilon'| \leq 10^{-5}$).

The attack provided in section II.3 also needs an integer x and two other integers r and s, equal, powers of two, as small as possible and such that $x^4 \geq r$ and $\mathbb{P}(n_\zeta \geq x) \geq 1 - 10^{-4}$. The minimal choice for r (and s) is 2^{37} and we can take x=609 (the smallest integer whose 4-th power is greater than 2^{37}) since:

$$\mathbb{P}(n_\zeta \geq 609) \geq \mathbb{P}(|E_r \cap E_s| \geq 609) = 1-\mathcal{F}_{1024}(608)+\varepsilon".$$

Now, an easy lemma shows that $\ln \mathcal{F}_\nu(i) \leq [i-\nu+i(\ln\nu-\ln i)]$, so that $\mathcal{F}_{1024}(608) \leq 10^{-43}$, and $|\varepsilon"|$ can be shown to be smaller than 10^{-5}. Hence, we can conclude that: $\mathbb{P}(n_\zeta \geq 609) \geq 1 - 10^{-4}$.

PART II: THE BIRTHDAY ATTACK

This part provides a generalization of Coppersmith's attack to a general scheme using p initializing values and passing the message p times. We first present the Rabin scheme and its evolutions (section 1), then present our main result (section 2) and its proof (section 3).

II.1 THE RABIN SCHEME AND ITS EVOLUTIONS

For continuity, we use (almost) the same notations (and sometimes the same expressions!) as Coppersmith did in [6]. In particular, $E_K(X)$ denotes throughout the paper the DES encipherment of the cleartext X under the key K and $D_K(Y)$ denotes the decipherment of the ciphertext Y under the key K.

In the Rabin scheme, the message M is divided into n 56-bit blocks M_j, used as keys for the iterated encipherment of some initial value H_0. The final encipherment, along with the initial value, forms the hash value:

$$\begin{cases} H_0 = \text{random} \\ H_j = E_{M_j}(H_{j-1}) \qquad 1 \le j \le n \\ \text{RSA-Sign}(H_0, H_n) \end{cases}$$

This scheme is subject to a so-called "meet-in-the-middle attack", whose invention is attributed to Merkle by Winternitz and which works as shown below. For convenience, if M is a message made up of message blocks $M_1, \ldots, M_n$, we will use the following notation:

$$\forall\ X,\ E_M(X) = E_{M_n}[E_{M_{n-1}}[\ldots.[E_{M_1}(X)]\ldots.]]$$
$$D_M(X) = D_{M_1}[D_{M_2}[\ldots\ldots[D_{M_n}(X)]\ldots.]]$$

The meet-in-the-middle attack allows the opponent, given a message M and its hash value (H_0, H_n), to construct a bogus message M' without affecting the hash value. The opponent can then replace M with M' without being detected, since the signatures of both messages are identical.

In order to achieve this, the opponent generates 2^{32} messages M_l and M_r of arbitrary length (the shorter they are, the faster the attack is). He may for example create a few (32) variations of a unique message and combine these variations together. For each message M_l (respectively M_r), he computes: $H_l = E_{M_l}(H_0)$ (respectively $H_r = D_{M_r}(H_n)$), sorts and stores these values.

If E is supposed to have good "random" properties, then the set of all the H_l and the set of all the H_r can be considered as two "random" and "independent" samples of 2^{32} drawings with replacements from a population of size 2^{64}. Therefore, as shown in Part I, the probability is greater than $\frac{1}{2}$ (about $1-e^{-1}$) that a coincidence exists (i.e.: $\exists l,r$ such that $H_l = H_r$). This coincidence will appear while sorting the values.

Let now M be the concatenation of M_l and M_r for these particular values of l and r. Then:

$$E_M(H_0) = E_{M_r}(H_l) = E_{M_r}(H_r) = H_n$$

We say that H_0 and H_n have been "linked up" or "joined up" by M. In this way, the opponent succeeds in constructing a bogus message M'.

This attack is plausible because the total number of operations is not too large, considering today's technology: for example, if the attacker chooses single-block messages M_l and M_r (in order to speed up the computation), he will have to perform $2.2^{32} = 2^{33} \simeq 10^{10}$ encipherments. To that must be added the time taken to sort values H_l and H_r, which can be evaluated to about $2^{38} \simeq 3.10^{11}$ operations. No doubt the high-speed and large-memory computers available today can achieve this (and

even more).

In order to avoid this attack, Davies and Price proposed in [8] to pass the messages twice:

$$\begin{cases} H_0 = \text{random} \\ H_j = E_{M_j}(H_{j-1}) & 1 \le j \le n \\ H_{n+j} = E_{M_j}(H_{n+j-1}) & 1 \le j \le n \\ \text{RSA-Sign}(H_0, H_{2n}) \end{cases}$$

A variant of this scheme consists of choosing two initializing values and also passing the message twice:

$$\begin{cases} H_0, H_0' = \text{random} \\ H_j = E_{M_j}(H_{j-1}) & 1 \le j \le n \\ H_j' = E_{M_j}(H_{j-1}') & 1 \le j \le n \\ \text{RSA-Sign}(H_0, H_n, H_0', H_n') \end{cases}$$

Of course, the Davies-Price scheme is easier to break than the last one (it suffices for the enemy to choose $H_0' = H_n$). At Crypto'85 [6], Coppersmith showed that a "triple birthday attack" permits the attacker to construct bogus messages in both above schemes, with not much larger computational requirements than for the Rabin scheme. He also claimed that the Davies-Price scheme remained insecure with three passes instead of two, but without providing details.

In the next section, by generalizing Coppersmith's attack, we show rigorously that the Davies-Price scheme and its extension are insecure even if the message is passed four times, provided the enemy can accept a number of encipherments in the magnitude range of 2^{46} and messages of length 14 Kbytes.

II.2 THE GENERALIZED SCHEME

We now consider the following general scheme, with p initializing values:

$$\begin{cases} H_0^1, H_0^2, \ldots, H_0^p \text{ random} \\ H_j^i = E_{M_j}(H_{j-1}^i) \qquad 1 \le j \le n \text{ and } 1 \le i \le p \\ \text{RSA-Sign}(H_0^1, H_n^1, \ldots, H_0^p, H_n^p) \end{cases}$$

For p=1, it becomes the Rabin scheme; for p=2, it becomes the Davies-Price scheme (or, rather, its strong variant). The question is: does Coppersmith's attack extend to p greater than 2? The answer is yes. More precisely, we claim the following result:

A message of 2.10^{p-1} blocks joining the H_0^i and the H_n^i for each i in [1,p] can be found using less than $2^{33}.10^p$ encipherments with probability very close to 1.

Before providing the proof in the following section, we first give a few comments about this result:

a) The above values result from a trade-off between four different parameters: the degree of significance placed on the message obtained, the length of this message, the number of encipherments and the probability of success. Of course, it is possible to improve some of them but at the detriment of the others. For example, the enemy can get a "more meaningful" message, which will necessarily becomes longer. Or he can get a shorter message but the number of encipherments will increase etc.

b) The number of blocks indicated is only, other things being equal, a minimum: these are "constrained blocks" generated by the attack, on which the attacker has no (or very little) control. But he can design his attack in such a way

that the final message will also contain an arbitrary number of other blocks completely selected by him. The proportion of bogus blocks can, in that way, be made as small as wanted (hence less visible!).

c) Though it is highly unlikely, it could theoretically occur that the attack as described below might not succeed. In practice, it suffices to (slightly) increase the number of trials at the step where the attack fails in order to render it effective.

d) Of course, the time of sorting must be added to the time of enciphering in order to get the total computation time. But a close look at the proof shows that the time of sorting grows much slower than the number of encipherments (the ratio of the geometric progression is only 3).

e) if E is replaced with a block-cipher algorithm whose block-length is L, the number of encipherments becomes $2^{\frac{L}{2}+1}.10^p$.

II.3 THE CRYPTANALYSIS

We come now to the proof of our result. In fact, we will prove the more precise following theorem:

Theorem: Let p be an integer ≥ 1, let $(A_1,\ldots,A_p)$ be distinct 64-bit values and let $(B_1,\ldots,B_p)$ be distinct 64-bit values.

1) A message M of u_p blocks can be found using t_p encipherments (or less) with probability Q_p, which is such that :

$$E_M(A_i) = B_i \qquad 1 \leq i \leq p$$

where :

$$u_p = 2.10^{p-1}$$

$$t_p = \begin{cases} 2^{35} & \text{for } p = 1 \\ 2^{36}\left(3^{p-2} + 4.10^{p-2}\left(1+\frac{10}{7}\left(1-\left(\frac{3}{10}\right)^{p-1}\right)\right)\right) & \text{for } p \geq 2 \end{cases}$$

$$Q_p \geq 1 - \frac{3^p}{2.10^4}$$

2) 609 distinct messages M of u_p blocks can be found using t'_p encipherments (or less) with probability Q'_p such that :

$$E_M(A_i) = B_i \qquad 1 \leq i \leq p$$

where :

$$t'_p = \begin{cases} 2^{38} & \text{for } p = 1 \\ 2^{36}\left(3^{p-2} + 4.10^{p-2}\left(8+\frac{10}{7}\left(1-\left(\frac{3}{10}\right)^{p-1}\right)\right)\right) & \text{for } p \geq 2 \end{cases}$$

$$Q'_p \geq 1 - \frac{3^p}{2.10^4}$$

Comments:

a) The result claimed in the previous section is clearly a consequence of the part 1 of this theorem (that t_p is less than $2^{33}.10^p$ is very easy and figures in the proof).

b) The apparition of the integer 609 (somewhat mysterious!) has been explained in section I.5.

c) The proof below implicitly assumes (as always in birthday attack literature) that good encipherment algorithms have good random properties. In particular, for any given distinct inputs X and Y, the values taken by $E_K(X)$ and $E_K(Y)$, when K runs through the key space, should be independent events.

d) if E is replaced with a block-cipher algorithm whose block-length is L, the proof remains almost unchanged and the part 1 of the theorem is still valid after having replaced 2^{35} with $2^{\frac{L}{2}+3}$, and 2^{36} with $2^{\frac{L}{2}+4}$ in t_p.

Proof: by induction on p.

• p=1

The meet-in-the-middle-attack, exposed in section II.1, permits the enemy to find (as already shown in section I.5):

1) at least one two-block junction between A_1 and B_1 (i.e. a message M such that $E_M(A_1) = B_1$) using 2.2^{34} encipherments with probability $Q_1 \geq 1-10^{-4}$.

2) at least 609 two-block junctions between A_1 and B_1 using 2.2^{37} encipherments with probability $Q_1' \geq 1-10^{-4}$.

So:

$u_1 = 2$

$t_1 = 2^{35}$ $\qquad$ $t_1' = 2^{38}$

$Q_1 \geq 1-10^{-4}$ $\qquad$ $Q_1' \geq 1-10^{-4}$

• assumed to be true at rank p

Let $(A_1,\ldots,A_{p+1})$ be p+1 distinct values.
Let $(B_1,\ldots,B_{p+1})$ be p+1 distinct values.

We now have to make A_i and B_i meet, for each i in [1,p+1] with the same message M_{p+1}. This can be done in three steps:

Step 1: Choose arbitrarily $Z_1,\ldots,Z_p$ p distinct values. Then find a set $\mathcal{E}$ of 609 u_p-block messages M_j which link up the Z_i to themselves for each i:

$E_{M_j}(Z_i) = Z_i$ for all i and all j.

From the induction hypothesis, the set $\mathcal{E}$ can be found using t_p' encipherments with probability Q_p' (note that this step, called "precomputation" by Coppersmith, needs only to be done once and can be used for any A_i and B_i).

Step 2: Find a u_p-block message M_0 such that A_i and Z_i meet for each i and let $C_0 = E_{M_0}(A_{p+1})$. This message can be found using t_p encipherments with probability Q_p.

Find also a u_p-block message M_f such that Z_i and B_i meet for each i and let $C_f = D_{M_f}(B_{p+1})$.

Step 3.1: (It remains now to link up C and D while "preserving" each Z_i)

Perform a meet-in-the-middle attack between C and D using only elements of $\mathcal{E}$. More precisely:
let $M_l = (M_1, M_2, M_3, M_4) \in \mathcal{E}^4$ and $H_l = E_{M_l}(C_0)$
let $M_r = (M_5, M_6, M_7, M_8) \in \mathcal{E}^4$ and $H_r = D_{M_r}(C_f)$.

As there are $(609)^4 \geq 2^{34}$ elements in $\mathcal{E}^4$, we can obtain two random and independent samples of 2^{34} H_l and 2^{34} H_r. We will therefore find a coincidence between the two samples with a probability of Q_1.

In other words, we can find one junction M between C_0 and C_f preserving each Z_i, constituted of $8u_p$ blocks and using $4.2.2^{34}u_p$ encipherments.

Thus, the message M_{p+1} which is equal to the concatenation of M_0, M and M_f links up A_i to B_i for each i in [1,p+1].

The total number of blocks of M_{p+1} is:

$$u_{p+1} = u_p + 8u_p + u_p = 10\,u_p$$

The number of encipherments is:

$$t_{p+1} = t_p' + 2t_p + 2^{37}u_p$$

The probability of success is :

$$Q_{p+1} = Q'_p \; Q_p^2 \; Q_1$$

Step 3.2: In step 3.1, we do not need all the elements of $\mathcal{E}^4$ to find a coincidence, since 2^{34} (at each side) will probably suffice. If we now use all the $(609)^4 \geq 2^{37}$ elements of $\mathcal{E}^4$, we will find (at least) 609 junctions with probability Q'_1.

The number of encipherments is:

$$t'_{p+1} = t'_p + 2t_p + 2^{40}u_p$$

The probability of success is:

$$Q'_{p+1} = Q'_p \; Q_p^2 \; Q'_1$$

• It remains now to solve the recurrence relations in u_p, t_p, t'_p, Q_p and Q'_p.

The sequence (u_p) is geometric and we have immediately :

$$u_p = u_1 . 10^{p-1} = 2.10^{p-1} \quad \text{for any } p \geq 1$$

Let (α_p) be the sequence equal to $t'_p + 2t_p$. We have:

$$\alpha_{p+1} = t'_{p+1} + 2t_{p+1} = 3\alpha_p + 2^{40}u_p + 2^{38}u_p = 3\alpha_p + 2^{38}10^p$$

For p = 0 this equation becomes:

$$\alpha_1 = 3\alpha_0 + 2^{38}, \text{ so we put: } \alpha_0 = \frac{2^{36}}{3}$$

We have for any $p \geq 1$:

$$\alpha_p = 3^p\alpha_0 + 2^{38}(10^{p-1} + 3.10^{p-2} + \ldots + 3^{p-2}.10 + 3^{p-1}) =$$

$$= 3^p\alpha_0 + \frac{10^p}{7} 2^{38}\left(1 - \left(\frac{3}{10}\right)^p\right)$$

So for $p \geq 2$:

$$t_p = \alpha_{p-1} + 2^{37}u_{p-1} = 2^{36}\left(3^{p-2} + 4.10^{p-2}\left(1 + \frac{10}{7}\left(1 - \left(\frac{3}{10}\right)^{p-1}\right)\right)\right)$$

$$t'_p = \alpha_{p-1} + 2^{40}u_{p-1} = 2^{36}\left(3^{p-2} + 4.10^{p-2}\left(8 + \frac{10}{7}\left(1 - \left(\frac{3}{10}\right)^{p-1}\right)\right)\right)$$

Remark that :

$$t_p \leq 2^{36}[3^{p-2} + \frac{68}{7} 10^{p-2}] \leq 2^{36}.11.10^{p-2} \leq 2^{33}.10^p$$

Now let $q = 1 - 10^{-4}$. We have:

$$\begin{cases} Q_1 \geq q \Rightarrow Q_2 \geq q^4 \Rightarrow Q_3 \geq q^{13} \ldots \\ Q_1' \geq q \Rightarrow Q_2' \geq q^4 \Rightarrow Q_3' \geq q^{13} \ldots \end{cases}$$

More generally : $Q_p \geq q^{\frac{3^p-1}{2}} \geq 1 - \frac{3^p-1}{2} 10^{-4} \geq 1 - \frac{3^p}{2.10^4}$.

Note that $Q_p \geq 0.995$ for $p = 4$.

CONCLUSION

This paper generalizes the birthday attack presented by Coppersmith at Crypto'85.

In the first part, we analyse the mathematical aspects of the birthday problem, for which exact and asymptotical results (with bounds) are provided. In particular, under some natural hypothesis, the underlying distributions are proved to converge towards Poisson distributions.

In the second part, the Coppersmith attack is generalized to schemes which cycle through the message blocks p times (instead of twice). A lower bound for the probability of success of the attack is given. For example, if DES is used and if p=4, a bogus message of 14 Kbytes can be forged with (almost surely) less than 2^{47} encipherments. As a consequence, the 4-pass Davies-Price scheme appears not to be secure enough.

This last result is of importance when the signature is obtained by signing the initializing values and the end-values.

For, in that case, p=4 is the maximum number of possible passes if the modulus length of the signer is equal to 512 bits (a very usual length).

REFERENCES

[1] W. Diffie and M. Hellman, "New directions in cryptography", IEEE Transactions on Information Theory, Vol. IT-22, Nov. 1976, pp. 644-654.

[2] R.L. Rivest, A. Shamir and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems", CACM, Vol. 21, n°2, Feb. 1978, pp. 120-126.

[3] Data Encryption Standard, FIPS Pub 46, N.B.S., U.S. Dep. of Comm., Jan. 1977.

[4] M. Campana and M. Girault, "Comment utiliser les fonctions de condensation dans la protection des données", SECURICOM 1988, pp. 91-110.

[5] G. Yuval, "How to swindle Rabin", Cryptologia, Vol. 3, N°3, Jul.1979, pp. 187-189.

[6] D. Coppersmith, "Another birthday attack", Advances in Cryptology, Proc. of Crypto'85, LNCS, Vol. 218, Springer-Verlag, 1986, pp. 14-17.

[7] M. Rabin, "Digital signatures", Foundations of Secure Computation, Academic Press, New York, 1978.

[8] D.W. Davies and W.L. Price, "The application of digital signatures based on public key cryptosystems", Proc. of the 5th Int. Conf. on Computer Communications, Atlanta, Georgia, Oct. 1980, pp. 525-530.

[9] W. Feller, "An Introduction to Probability theory and its Applications", Volume 1, Wiley, 1968.