Research Report

KSTS/RR-87/006
16 Aug. 1987

Probability to meet in the middle

by

Kazuo Nishimura
Masaaki Sibuya

Kazuo Nishimura
Masaaki Sibuya

Department of Mathematics
Faculty of Science and Technology
Keio University

Hiyoshi 3-14-1, Kohoku-ku
Yokohama, 223 Japan

Department of Mathematics
Faculty of Science and Technology
Keio University

Hiyoshi 3-14-1, Kohoku-ku, Yokohama, 223 Japan

KSTS/RR-87/006
August 16, 1987

PROBABILITY TO MEET IN THE MIDDLE

Kazuo Nishimura and Masaaki Sibuya

Address: Department of Mathematics, Keio University, Hiyoshi 3-14-1, Kohoku-ku, Yokohama, 223 Japan; Nishimura%koscvax.keio.junet%japan.csnet@relay.cs.net or ...seismo!kddlab!koscvax.keio.junet!Nishimura

Abstract: The classical birthday problem should be modified to model adequately the meet-in-the-middle attack to break digital signatures. This note proposes a model "matching in two samples" including "birthday problem in two groups," and clarifies probabilistic implications of the statement that "insecure digital signature schemes can be broken by efforts of the square root order in comparison with secure ones."

Keywords: authentication, digests, forgery, one-way hash functions, Data Encryption Standard, birthday problem, matching, occupancy, urn models.

1 INTRODUCTION

One merit of the public-key cryptosystem is its use in digital signature to verify a message and identify its sender [6]. With only this purpose in mind an economical way is to use the short digest rather than the whole message for the digital signature. To compress messages of arbitrary length to a short code of fixed length a hashing function using Data Encryption Standard (DES) was proposed by Rabin [13]. This first proposal turned out to be vulnerable to the meet-in-the-middle attack [3,15]. New schemes have been proposed, and some of them have also been found to be insecure to a more complicated attack [1,2,11,14].

Let an encryption and a decryption function of conventional type be denoted by

$$C = E(K, M) \quad \text{and} \quad M = D(K, C)$$

respectively, where M, a message, and C, a cipher, are l-bit codes, and K, a key, is a k-bit code. Particularly in DES l=64 and k=56. Take, for example, Rabin's simple scheme: A message M is divided into a sequence of k-bit fragments $M_1,\cdots,M_r$. Starting from some initial value H_0 generate

$$H_i = E(M_i, H_{i-1}), \quad i = 1, 2, \cdots, r,$$

and the pair (H_0, H_r) is a digest of M. The digest is signed by the public-key

authentication method, and the authenticator is sent with the message M. The receiver can verify M and identify the sender by regenerating the authenticator.

A forger, knowing (H_0, H_r), wants to tamper with the message, keeping the digest and the authenticator unchanged. (At least the sender and the receiver of the message know the digest and can become the forger.) He generates other sequences $(\tilde{M}_i)_{i=1}^{r}$ with the intention that it reaches the same H_r. An example of forging $\tilde{M}$'s by random rephrasing is illustrated by Davies and Price [3].

In the meet-in-the-middle attack, the forger fixes a middle step j, $1<j<r$, and starting from both ends, H_0 and H_r, he randomly generates forward sequences

$$H_i = E(\tilde{M}_i, H_{i-1}), \quad i = 1, 2, \cdots, j, \tag{1.1}$$

and backward sequences

$$H_{i-1} = D(\tilde{M}_i, H_i), \quad i = r, r-1, \cdots, j+1. \tag{1.2}$$

If a forward result H_j and a backward result H_j coincide then the attack is accomplished.

It is argued in the literature that straightforward attacks need efforts of the order of $m=2^l$, while the meet-in-the-middle attack needs about $m^{1/2}$, where m is the cardinality of H_j. And the reduction is said to be similar to that of the birthday problem. The arguments are correct in principle. However, they should be probabilistic, and the classical birthday problem [7] is not an adequate model to calculate the probability to meet in the middle, i.e. the probability that the meet-in-the-middle attack succeeds. (Really the probability to fail is easier to handle.)

In this note a model "matching in two samples" is proposed for the meet-in-the-middle attack. There are two cases of the model: two samples are taken from 2^l possible codes "without replacement" or "with replacement" corresponding to two forgery situations. The latter case may be better understood by the name "occupancy with two types of balls" or "birthday problem in two groups." It is shown that the meet-in-the-middle attack will succeed with probability p by $[(-m/3)\log(1-p)]^{1/2}$ or $[-m\log(1-p)]^{1/2}$ trials in these cases, respectively, while the corresponding straightforward attacks need $m(1-p)$ or $-m\log(1-p)$ trials.

The mathematical details and related probability distributions are reported in an accompanying paper [12].

2 MODELS AND PROBABILITIES

Analyses and measurements has been published on the statistics of encryption and decryption functions, especially those of DES [9,11]. From these reports it seems reasonable to assume uniformity and independence in the probabilistic model mentioned below.

2.1 MATCHING IN TWO SAMPLES WITHOUT REPLACEMENT

There are two situations. First, the forger wants to tamper with a fragment, say M_j, of the message, to change a small part like a number, a name, or a date. He will then generate randomly modified fragments $\tilde{M}_j$ and $\tilde{M}_{j+1}$, and obtain

$$H_j = E(\tilde{M}_j, H_{j-1}) \quad \text{and} \quad H_j = D(\tilde{M}_{j+1}, H_{j+1}) ,$$

expecting to obtain two types of coinciding H_j's. (To tamper with M_j, the forger can generate $\tilde{M}_{j+1}$ and $\tilde{M}_j$. The following discussion is the same for this procedure.) Here, a trial means random generation of $\tilde{M}_j$ (or $\tilde{M}_{j+1}$) and evaluation of the function E (or D).

So far as the authors know, the sets

$$L_E(H) = \{E(K,H),\ K\in\{0,1\}^k\} ,$$
$$L_D(H) = \{D(K,H),\ K\in\{0,1\}^k\} ,$$

have not been determined for a given H. For a given pair H and H', the cardinal number of $L_E(H) \cap L_D(H')$ might be large or small. Since we are not discussing a specific message, and since H_{j-1} and H_{j+1} are the results of hashing the message, let us just assume that the result of n_1 (or n_2) trials of $E(\tilde{M}_j, H_{j-1})$ (or $D(\tilde{M}_{j+1}, H_{j+1})$) is a random sample of size n_1 (or n_2) "without replacement" from $\{0,1\}^l$, and assume that the samples of the forward trials and the backward trials are independent. The number S of codes H_j's generated by both the forward and the backward samples is the number of "matchings" hypergeometrically distributed under the assumptions. Thus the model is called "matching in two samples."

The probability distribution of S is given by

$$\Pr[S=s] = \binom{n_1}{s}\binom{m-n_1}{n_2-s} \Big/ \binom{m}{n_2} = \binom{n_2}{s}\binom{m-n_2}{n_1-s} \Big/ \binom{m}{n_1} . \tag{2.1}$$

So the probability of failure by the meet-in-the-middle attack is

$$q_1 := \Pr[S=0] = \frac{(m-n_1)!\ (m-n_2)!}{m!\ (m-n_1-n_2)!} . \tag{2.2}$$

If n_1/m, $n_2/m \to 0$ as $m\to\infty$, Stirling's formula leads to

$$q_1 = \exp\left\{ -\frac{3n_1n_2}{m}\left[1 - \frac{5(n_1+n_2)-1}{6}m + O\left(\frac{1}{m^2}\right)\right]\right\} .$$

That is, approximately n_1+n_2 trials with $n_1n_2=3m\log(1/(1-p))$ give the success probability p. When n_1n_2 is fixed, n_1+n_2 is minimized if $n_1=n_2$.

In the case where only $E(\tilde{M}_j, H_{j-1})$ or $D(\tilde{M}_{j+1}, H_{j+1})$ is generated n times, the probability to obtain a specific H_j is simply n/m under the above assumption. The results are

summarized in the following proposition.

Proposition 1. In the "matching in two samples without replacement" model for the meet-in-the-middle attack, the forger's failure probability is given by q_1 of (2.2). In other words, approximately

$$n_1 = n_2 = \left(3m\log\frac{1}{1-p}\right)^{1/2} \tag{2.3}$$

trials give the success probability p. In the corresponding straightforward attack, the forger's failure probability is

$$q_2 = 1 - \frac{n}{m},$$

and

$$n = m(1-p)$$

trials give the success probability p.

Really the forger will try sequentially to meet in the middle, that is he generates $E(\tilde{M}_j, H_{j-1})$ and $D(\tilde{M}_{j+1}, H_{j+1})$ alternately, and stores them in a hash table, for example, checking coincidence. Let $N=N_1=N_2$ be the number of trials both forward and backward when the first coincidence occurs. N_1 and N_2 are waiting times for the success. Since

$$\begin{aligned}\Pr[N>n] &= \Pr[S=0 \,|\, n_1=n_2=n] \\ &= \exp\left\{-\frac{3n^2}{m}\left[1+O\left(\frac{1}{m}\right)\right]\right\},\end{aligned}$$

the variate $3N^2/m$ follows asymptotically the standard exponential distribution.

On the other hand, in the straightforward attack using $E(\tilde{M}_j, H_{j-1})$ or $D(\tilde{M}_{j+1}, H_{j+1})$,

$$\Pr[N_i>n] = 1 - \frac{n}{m},$$

which means N_i is uniformly distributed on $[1, m]$.

Proposition 2. In the model of Proposition 1, let $N=N_1=N_2$ be the waiting time for success of the sequential meet-in-the-middle attack. Then, the asymptotic distribution of $3N^2/m$ is the standard exponential distribution. While the waiting time for success of the straightforward attack is uniformly distributed on $[1, m]$.

2.2 MATCHING IN TWO SAMPLES WITH REPLACEMENT, OR BIRTHDAY PROBLEM IN TWO GROUPS

Let us move to the second situation, where the forger wants to tamper with many fragments of the message, for example, the whole message. A trial now means one generation of H_j by (1.1) or by (1.2). Since H_j is obtained by repeated encryption or decryption randomly changing the keys, each forward and backward H_j can be regarded as a random variable that is uniformly distributed on $\{0,1\}^l$ and independent trial by trial. Thus the model is matching in two random samples that are taken from $\{0,1\}^l$ independently with replacement.

In terms of urn models [8], a simple probabilistic model of the classical birthday problem is described as follows. Balls, namely birthdays, are thrown at random into one of some urns, namely 365 days, and the event of concern is a collision: more than one ball falls in a single urn. In the meet-in-the-middle attack, urns are all the possible l-bit codes H_j at the j-th stage (where j, $1<j<n$, is a fixed integer) and there are $m=2^l$ urns. Unlike birthdays, there are two types of balls: one corresponds to the results of the forward sequences (1.1) and the other the backward sequences (1.2). Regard these types as balls of different colors, say, white and red. The event of concern is a collision between the two colors. Now, modify the classical birthday problem as follows. There are two groups, say, boys and girls groups. What is the probability that a boy's birthday coincides with a girl's birthday? This is just a collision between two colors and can be called "birthday problem in two groups."

Under uniformity and independence assumptions, the probability of no collision between n_1 white and n_2 red balls is shown to be

$$q_3 := m^{-n_1} \sum_t \left\{ {n_1 \atop t} \right\} m^{(t)} \left(1-\frac{t}{m}\right)^{n_2} = m^{-n_2} \sum_t \left\{ {n_2 \atop t} \right\} m^{(t)} \left(1-\frac{t}{m}\right)^{n_1}$$

$$= m^{-n_1-n_2} \sum_v m^{(v)} \left\{ {n_1 \atop t_1} \right\} \left\{ {n_2 \atop t_2} \right\} \tag{2.4}$$

where $m^{(t)} = m(m-1)\cdots(m-t+1)$ and $\left\{ {n \atop t} \right\}$ is the Stirling number of the second kind [10], defined by

$$x^n = \sum_{t=1}^{n} \left\{ {n \atop t} \right\} x^{(t)} . \tag{2.5}$$

Because when n_1 white balls are thrown at random into one of m urns, the number T of the urns occupied by the white balls follows the classical occupancy distribution:

$$\Pr[T=t] = m^{-n_1} \left\{ {n_1 \atop t} \right\} m^{(t)}, \qquad 1 \le t \le n_1 .$$

Under the condition that $T=t$, n_2 red balls are thrown at random into the urns. Then,

the number S of the red balls falling into the urns that are occupied by white balls is a binomial random variable:

$$\Pr[S{=}s \mid T{=}t] = \binom{n_2}{s} \cdot \left(\frac{t}{m}\right)^s \left(1 - \frac{t}{m}\right)^{n_2 - s} .$$

So, unconditionally

$$q_3 = \Pr[S{=}0] = \sum \Pr[S{=}0 \mid T{=}t] \Pr[T{=}t] ,$$

and this is the first expression of (2.4). Because the above random event is symmetric with respect to the white and red balls the second expression is equivalent to the first, and the definition (2.5) leads to the third expression. It is shown that for fixed $n_1{+}n_2$ the probability q_3 is minimized if $n_1{=}n_2$.

The expression of q_3 is evaluated as follows when $n_1{=}n_2{=}n$:

$$\left(1 - \frac{1}{m}\right)^{n^2} < q_3 < \exp\left[- \frac{n^2}{m} + \lambda \cdot \exp\left(\frac{n}{m} - 1\right)\right]$$

where $\lambda{=}n^2/2(m{-}n)$. If $n/m \to 0$ as $m \to \infty$, the above inequalities lead to

$$q_3 = \exp\left\{ - \frac{n^2}{m}\left[1 + O\left(\frac{n}{m}\right)\right]\right\}. \tag{2.6}$$

The corresponding probability by the one-way straightforward attacks of n trials is the probability of missing n times to hit a specific H_j :

$$q_4 := \left(1 - \frac{1}{m}\right)^n \exp\left\{ - \frac{n}{m}\left[1 + O\left(\frac{1}{m}\right)\right]\right\}. \tag{2.7}$$

In summary,

Proposition 3. In the "matching in two samples with replacement" model, i.e. "birthday problem in two groups", for the meet-in-the-middle attack, the forger's failure probability is given by q_3 in (2.4). In other words approximately

$$n_1 = n_2 = \left(m \log\frac{1}{1-p}\right)^{1/2}$$

trials give the success probability p. In the corresponding one-way attack, the forger's failure probability is given by q_4 in (2.7). In other words approximately

$$n = m \log\frac{1}{1-p}$$

trials give the success probability p.

When the attack is tried sequentially, the argument for Proposition 2 is applied. From (2.6) and (2.7) we obtain the following result.

Proposition 4. In the model of Proposition 3, let $N=N_1=N_2$ be the waiting time for success of the sequential meet-in-the-middle attack. Then, the asymptotic distribution of N^2/m is the standard exponential distribution.
Let N^* be the waiting time for success of the straightforward attack. Then, the asymptotic distribution of N^*/m is the standard exponential distribution.

Thus, a lucky forger can succeed without enormous efforts if Rabin's original scheme for making a digest is adopted.

3 OTHER SCHEMES FOR MAKING A DIGEST

There are other insecure and secure schemes for making a digest [1,2,14]. In this section a couple of schemes are reexamined.

To prevent backward trials in the meet-in-the-middle attack a scheme was proposed by Davies and Price [4] (attributed to Bitzer). Let $\oplus$ denote exclusive-or operation. Starting from an initial value H_0, compute

$$H_i = E(M_i \oplus H_{i-1},\ H_{i-1}), \quad 1 \le i \le r,$$

to get a digest $(H_0,\ H_r)$. It is still vulnerable. Note that

$$H_{r-1} = D(M_r \oplus H_{r-1},\ H_r),$$

and take $j=r-1$ as the "middle." Generate Y at random and compute $D(Y,\ H_r)$. If this matches one of H_{r-1}'s generated forward, then $\tilde{M}_r=D(Y,\ H_r)\oplus M_r$ is the forgery fragment. A disadvantage for the forger is that $\tilde{M}_r$ is meaningless and easily detected if the message is examined by people.

Following the argument in Section 2, the values of $D(Y,\ H_r)$ will be a sample without replacement. While the values of $E(M_{r-1}\oplus H_{n-2},\ H_{r-2})$ will be a sample with replacement. The probability to meet in the middle in n_1 forward and n_2 backward trials is

$$\left(1-\frac{n_1}{m}\right)^{n_2} = \exp\left\{-\frac{n_1 n_2}{m}\left[1+O\left(\frac{n_2}{m}\right)\right]\right\},$$

and Propositions 3 and 4 hold in this case.

Another proposal by Denning [5], attributed to Davies and Price, is to go through Rabin's schemes twice: Start from an initial value H_0 and generate

$$H_i = E(M_i, H_{i-1}), \qquad 1 \leq i \leq r,$$
$$H_{r+i} = E(M_i, H_{r+i-1}), \qquad 1 \leq i \leq r.$$

The pair (H_0, H_{2r}) is a digest. Coppersmith [2] showed an ingenious method to attack the scheme. His method consists of the following steps.

(a) A preparatory step is to construct a set of pairs of k-bit codes,

$$A = \{(X_i, Y_i),\ i=1,2,\cdots,\nu\},$$

such that, for each i and for a fixed l-bit code Z,

$$E(X_i, Z) = D(Y_i, Z).$$

The size ν of A is 2^8 in [2]. If $H_{2\alpha}=Z$ then for any sequence of pairs $(\tilde{M}_{2\alpha}, \tilde{M}_{2\alpha+1})$, $(\tilde{M}_{2\alpha+2}, \tilde{M}_{2\alpha+3})$, $\cdots$, of A,

$$H_{2\alpha+1} = E(\tilde{M}_{2\alpha}, H_{2\alpha}) = D(\tilde{M}_{2\alpha+1}, Z),$$

or

$$H_{2\alpha+2} = E(\tilde{M}_{2\alpha+1}, H_{2\alpha+1}) = Z = H_{2\alpha}.$$

Thus, $H_{2\alpha}=H_{2\alpha+2}=H_{2\alpha+4}=\cdots=Z$. The set A is used to forge any message.

(b) Given a digest (H_0, H_{2n}), generate first $\tilde{M}_0$ and $\tilde{M}_1$ such that

$$E(\tilde{M}_0, H_0) = D(\tilde{M}_1, Z)$$

by the meet-in-the-middle attack.

Next, $(\tilde{M}_2, \tilde{M}_3),\cdots,(\tilde{M}_{2\beta}, \tilde{M}_{2\beta+1})$ is a sequence of pairs chosen from A as determined later. Anyhow, $H_{2\beta+2}=Z$ as explained in (a).

(c) $(\tilde{M}_{2\beta+2},\cdots,\tilde{M}_r)$ is any forgery of any length. Now hashed codes are determined forwards starting from H_0, up to H_{r+2}, the third code of the second cycle. And, backwards starting from H_{2r} up to $H_{r+2\beta+2}$ corresponding to the top of the forgery of the second cycle.

(d) The final and essential step is to form a sequence $(\tilde{M}_2, \tilde{M}_3)$, $\cdots$, $(\tilde{M}_{2\beta}, \tilde{M}_{2\beta+1})$ of pairs chosen randomly from A. If the forward codes $(H_{r+2}, H_{r+4}, \cdots)$ and the backward codes $(H_{r+2\beta+2}, H_{r+2\beta+1}, \cdots)$ meet in the middle $H_{r+\beta+2}$, then the attack is accomplished.

To prepare the set A, X_i and Y_i are randomly generated for a fixed Z. For n_1 X_i's and n_2 Y_i's the number S of matched pairs follow the hypergeometric distribution (2.1). Its mean is n_1n_2/m and variance is $n_1n_2(m-n_1)(m-n_2)/m^2(m-1)$.

Generation of $(\tilde{M}_0, \tilde{M}_1)$ of Step (b) is identical with the situation of Proposition 1 and 2. Generation of $(\tilde{M}_2,\cdots,\tilde{M}_{\beta+1})$ of Step (d) is similar to the situation of Proposition 3 and 4. The length 2β is determined so that the number $\nu^{\beta/2}$ of possible sequences $(\tilde{M}_{\beta+2},\cdots,\tilde{M}_{2\beta+2})$ will be big enough to accomplish the attack, and Coppersmith suggested β=8 to have $\nu^{\beta/2}=2^{32}$. Remark that, β can be increased when necessary. Larger size ν of A makes just the length 2β shorter.

Total amount of the forger's works is much larger. The sequence $(\tilde{M}_0,\cdots,\tilde{M}_{2\beta+1})$ is selected at random, and makes no sense even if the pairs in A are meaningful.

In conclusion, the meet-in-the-middle attack still works in more complicated schemes and the analysis of Section 2 is applied. However, if the message is a sentence, the forgery is easily detected when it is carefully examined.

REFERENCES

1. Akl, Selim G., "On the security of compressed encodings," in *Advances in Cryptology — Proceedings of Crypto 83*, ed. D. Chaum, pp. 209-230, Plenum Press, New York, 1984.

2. Coppersmith, Don, "Another birthday attack," IBM Research Report, RC 11264, 15 July 1985.

3. Davies, Donald W. and Wyn L. Price, "The application of digital signatures based on public key cryptosystems," *5th Int. Conf. on Comput. Commun.*, pp. 525-530, IEEE, at Atlanta, Georgia, held 27-30 Oct. 1980.

4. Davies, Donald W. and Wyn L. Price, "Digital signatures — An update," *7th Int. Conf. on Comput. Commun.*, pp. 845-849, IEEE, at Sydney, Australia, held 31 Oct. - 2 Nov. 1984.

5. Denning, Dorothy E., "Protecting public keys and signature keys," *Computer*, vol. 16, no. 2, pp. 27-35, Feb. 1983.

6. Diffie, Whitfield and Martin E. Hellman, "New directions in cryptography," *IEEE Trans. Inf. Theory*, vol. IT-22, no. 6, pp. 644-654, Nov. 1976.

7. Feller, William, *An Introduction to Probability Theory and Its Applications*, vol. 1, 3rd ed., John Wiley, New York, 1968.

8. Johnson, N. L. and S. Kotz, *Urn Models and Their Applications*, John Wiley, New York, 1977.

9. Kaliski, Burt S., Ronald L. Rivest, and Alan T. Sherman, "Is the Data Encryption Standard a group? (Preliminary abstract)," in *Advances in Cryptology — Eurocrypt*

'85 , ed. D. Chaum, Lecture Notes in Computer Science, pp. 81-95, Springer-Verlag, at Linz, Austria, held Apr. 1985.

10. Knuth, Donald E., *The Art of Computer Programming,* vol. 1-3, Addison-Wesley, Massachusetts, 1967-1981.

11. Mueller-Schloer, Christian, "DES-generated checksums for electronic signatures," *Cryptologia,* vol. 7, no. 3, pp. 257-273, July 1983.

12. Nishimura, Kazuo and Masaaki Sibuya, "Occupancy with two types of balls," KSTS/RR-87/002, Dept. of Math., Keio Univ., 31 March 1987.

13. Rabin, Michael O., "Digitalized signatures," in *Foundations of Secure Computation,* ed. R. A. DeMillo, et al., pp. 155-166, Academic Press, New York, 1978.

14. Winternitz, Robert S., "A secure one-way hash function built from DES," *Security and Privacy,* pp. 88-90, IEEE, at Oakland, California, held 29 Apr. - 2 May 1984.

15. Yuval, Gideon, "How to swindle Rabin," *Cryptologia,* vol. 3, no. 3, pp. 187-189, July 1979.