A Key Distribution "Paradox"

Yacov Yacobi
Bellcore
445 South St.
Morristown, NJ 07960

Abstract

The so called, Rabin "paradox" is a proof that a given signature system, which is secure under ciphertext only attack is insecure under chosen message attack. The construction that is used to prove the first clause is also used to prove the second. For several years it was believed to be inherent to public key signature systems. A similar problem existed for public key cryptosystems (under chosen ciphertext attack). Trap-door functions were inherent in the construction of the "paradox."

In 1984 Goldwasser, Micali and Rivest constructively showed that one can overcome the "paradox." Naor and Yung (1989) resolved the similar problem for public key cryptosystems. Both solution actually solve two problems. They resolve the "paradox," with the strictest definition of security (for a cryptosystem it amounts to the demand that for a given cryptogram c and two messages m_0, m_1 it should be infeasible to decide whether c resulted from m_0 or m_1 with probability significantly greater than half). Both solutions are very complicated.

We show that a similar "paradox" exists for many key distribution systems, even if non-trapdoor one way functions are used (like in the Diffie-Hellman variations). Using the simple basic definition of security (given the messages exchanged during the protocol it should be impossible to find the resulting session key in probabilistic polynomial time) we show a simple and practical key distribution system which is provably free of the paradox.

1 Introduction

Consider 2-party Key Distribution Systems (KDS) with one transmission in each direction (party i transmits r_i); these transmissions are independent of the private secret keys (and therefore, these systems are zero-knowledge as far as the private secret keys are concerned). The transmissions may be the results of computations $r_i = F_i(e_i)$, where the functions F_i may be one-way, and e_i is randomly chosen. S_i, P_i are party i's secret and public keys respectively.

A.J. Menezes and S.A. Vanstone (Eds.): Advances in Cryptology - CRYPTO '90, LNCS 537, pp. 268-273, 1991.

Let A be a "reference point" (believed to be a) hard problem, like factorization, or equivalently, Composite Diffie-Hellman (CDH) ([S],[M],
A: **Input:** I; **Output:** $O = A(I)$.

Let B_{cop} denote the cracking problem of a given KDS, under Ciphertext-Only attack, by a Passive adversary, i.e.
B_{cop}: **Input:** X, r_1, r_2 (X is the public data); **Output:** $k = g(X, r_1, r_2)$.

Let B_{kkp} denote the cracking problem (of the same system), under Know (old session) Key Attack, by a Passive adversary, i.e.
B_{kkp}: **Input:** $X, r_1, r_2, r_1', r_2', k' = g(X, r_1', r_2')$; **Output:** $k = g(X, r_1, r_2)$.

Throughout *efficient computation* means "computable in probabilistic polynomial time." If a cracking problem is efficiently solvable then a system is *insecure* for that attack. We show that if B_{kkp} is reducible to A in probabilistic polynomial time, and A is reducible to B_{cop} in probabilistic polynomial time, s.t. the second reduction holds for every [1] r_1, r_2, and such that the reductions maintain certain parameters, and the functions F_i^{-1} are efficiently computable, then B_{kkp} has efficient solution. The crux of the proof is combining the two reductions into one reduction from B_{kkp} to B_{cop}, and then using k', taken from B_{kkp}'s input to replace oracle B_{cop}. The above dichotomy (hard B_{cop}, and easy B_{kkp}) does not hold for systems s.t. triples (r_1', r_2', k') are efficiently computable given only the public data X. Using this we present a simple, secure, non "paradoxical" KDS. This system, and several of our "paradoxical" systems appeared in [MTI]. However, they do not mention the "paradox," and no formal definition of security is given.

2 The main results

Let problems A, B_{cop}, B_{kkp} be as defined above.

Theorem 1: If B_{kkp} is reducible in probabilistic polynomial time to A, and A is reducible in probabilistic polynomial time to B_{cop}, s.t.

(i) The second reduction holds for every r_1, r_2, in the targets of F_1, and F_2, respectively, and

(ii) The public data, X, of B_{kkp} is identical to that of A ($I = X$) and B_{cop}, and

(iii) F_1, F_2 are not one-way functions (i.e. F_i^{-1} are efficiently computable),

then B_{kkp} is efficiently solvable.

Proof: The reduction from B_{kkp} to A together with $I = X$ imply the existence of efficiently computable function G_1, s.t. $k = G_1(X, r_1, r_2, r_1', r_2', k', A(X))$. The reduction from A to B_{cop} together with (i) imply the existence of efficiently computable

[1] The demand that the reduction holds for every r_1, r_2 is used to substantiate uniform hardness claims.

function G_2, s.t. $A(X) = G_2(X, e'_1, e'_2, k')$. Hence B_{kkp} is efficiently solvable using $k = G_1(X, r_1, r_2, r'_1, r'_2, k', G_2(X, F_1^{-1}(r'_1), F_2^{-1}(r'_2), k'))$.
Q.E.D.

if given X, arbitrary triples (r'_1, r'_2, k') are polynomially computable, then B_{kkp} and B_{cop} are of the same complexity. A system with the above property does not have the "paradox." We later show such a KDS.

3 Example of a "paradoxical" system

The system is a slight modification of a system shown in [YS]. It belongs to the Diffie-Hellman family of KDS, which relies on the difficulty of the discrete-log problem. Let p and q be two large primes, and let $m = pq$. Let α be an element of high order in Z_m^*. Each participant i has a pair of public and secret keys (p_i, s_i), where $p_i \equiv \alpha^{-s_i} \ mod \ m$. The protocol is completely symmetric, and therefore we describe just one side, i. The other side j mirrors i's actions.

begin

1. Party i chooses a random $r_i \in_R (1, m)$ with uniform distribution, and the parties exchange these values.
2. Party i computes $k_{ij} \equiv (\alpha^{r_j} p_j)^{r_i - s_i} \ mod \ m$.

end

Clearly, $k_{ij} \equiv k_{ji} \equiv \alpha^{(r_i - s_i)(r_j - s_j)} \ mod \ m$
The initial cracking problem (before any communication) is not solvable, since there isn't enough information to determine even one bit of the key. The communication is completely independent of the secrets, so it does not provide any additional information on the secret keys (s_i and s_j). This proves Lemma 1.

Lemma 1: In the above KDS no information on the identification secrets leaks, under ciphertext only attack.

Shmuely [S] (and later McCurley [M]) analyzed a composite DH scheme, in which the public and secret keys are as in this scheme, and the session key is $k_{ij} \equiv \alpha^{s_i s_j} \ mod \ m$. We henceforth refer to this system as CDH (Composite Diffie-Hellman). Shmuely and McCurley gave evidence that for suitably chosen α and m the cracking problem of CDH is hard on the average. We summarize the CDH cracking problem (A), and the cracking problem of the new system (B_{cop}).

A: Input: $\alpha^x, \alpha^y, \alpha, m$; **Output:** $\alpha^{xy} \ mod \ m$.
B_{cop}**: Input:** $r_i, r_j, \alpha^{-s_i}, \alpha^{-s_j}, \alpha, m$; **Output:** $\alpha^{(r_i - s_i)(r_j - s_j)} \ mod \ m$.

Lemma 2: $\forall r_i, r_j$ A is reducible in polynomial time to B_{cop}.
Proof: For any $r_i, r_j \in [0, m)$, set $\alpha^{-s_i} = \alpha^x$, $\alpha^{-s_j} = \alpha^y$. The oracle outputs $\alpha^{(r_i - s_i)(r_j - s_j)} = \alpha^{r_i r_j} \cdot (\alpha^{-s_i})^{r_j} \cdot (\alpha^{-s_j})^{r_i} \cdot \alpha^{s_i s_j}$. The first three multiplicands are known, hence from the oracle's answer one can compute the fourth multiplicand, which equals the desired answer to problem A.
Q.E.D.

Remark: In [YS] a similar reduction is presented, for malicious adversary (impersonator), under ciphertext only attack.

Lemma 3: For this KDS B_{kkp} has efficient solution.
Proof: The proof is almost identical to that of Lemma 2 only now a given old key, k', plays the role of the oracle's answer (and the corresponding r'_i, r'_j are known). Once $\alpha^{s_i s_j} \ mod \ m$ is computed from the old key, one can easily compute the new key $\alpha^{(r_i - s_i)(r_j - s_j)} \ mod \ m$.
Q.E.D.

4 Example of a non "paradoxical" system

Transmissions: $r_i \equiv \alpha^{e_i} \ mod \ m$,
Session key (as computed by 1): $k \equiv (\alpha^{s_2})^{e_1} \cdot (\alpha^{e_2})^{s_1} \equiv \alpha^{s_1 e_2 + s_2 e_1} \ mod \ m$
Secrecy: A is reducible in polynomial time to B_{cop}, by the assignments $\alpha^{s_1} = \alpha^x, \alpha^{e_2} = \alpha^y$, with arbitrarily chosen s_2, e_1. Also, a reduction in reverse direction exists (with two oracle calls), hence B_{cop} is as hard as A.
Triples $(r'_1, r'_2, k' \equiv (\alpha^{s_2})^{e_1} \cdot (\alpha^{s_1})^{e_2} \ mod \ m)$, can be easily computed, hence they don't contribute any new knowledge, and B_{kkp} is as hard to solve as B_{cop}, for this system.
Resilience:
In general a protocol is assumed resilient if a disruptive adversary cannot bring the honest participants to assume a wrong outcome after executing the protocol. To end up with a practical protocol we have to impose some reasonable restrictions on this definition. Therefore, we address the following disruptive adversary: The adversary is an impersonator, playing in the middle, between i and j, pretending to be j when talking to i, and vice-versa. He tries to establish a session-key with each of the legitimate parties (not necessarily the same key). In doing so he may deviate from the original protocol by sending messages, computed entirely different from the intended computations (as long as his computations are done in probabilistic polynomial time). However, he must conform with the basic structure of the protocol, i.e. send messages of the right structure and size, when expected.
We can reduce the basic Diffie-Hellman problem to the cracking problem under impersonation attack, with known old session's information. Since old information can be reproduced by anybody easily, we can remove this obstacle and concentrate on a reduction to the cracking problem without that history. Again, the DH problem

is **Input:** $\alpha, \alpha^x, \alpha^y, N$; **Output:** $\alpha^{xy} \bmod N$.
The cracking problem for impersonator who plays in the middle, trying to impersonate j when talking to i (for example) should be defined in general terms, that is, we cannot assume that all he does is choosing some $\tilde{R}_j$ instead of R_j, but otherwise participates in the protocol as originally designed. We assume that the impersonator picks some $\tilde{R}_j$, and sends $h(\alpha, \tilde{R}_j)$ to i, where $h(.,.)$ is any probabilistic polynomial time function. This function may have more inputs; Any public information can be part of its input. So the cracking problem of the impersonator is defined as follows:
Input: $\alpha, N, \alpha^{R_i}, P_i \equiv \alpha^{S_i} \bmod N, P_j \equiv \alpha^{S_j}, h(\alpha, \tilde{R}_j)$;
Output: $h(\alpha, \tilde{R}_j)^{S_i} \cdot (\alpha^{S_j})^{R_i} \bmod N$.

The randomized reduction from the DH problem to this one goes as follows: Set $\alpha^{R_i} \leftarrow \alpha^y; P_j \leftarrow \alpha^x; N \leftarrow N$, and pick S_i and $h(\alpha, \tilde{R}_j)$ from the appropriate domains with homogeneous distribution. Compute $P_i \equiv \alpha^{S_i} \bmod N$. Given the oracles answer $h(\alpha, \tilde{R}_j)^{S_i} \cdot (\alpha^{S_j})^{R_i} \bmod N$ one can easily compute now $\alpha^{xy} \bmod N$.

Acknowledgment:
I wish to thank Shimon Even for many insightful discussions.

5 References

BCGL Ben-David, S., Chor, B., Goldreich, O., Luby, M.: "On the Theory of Average Case Complexity," *STOC*, 1989, pp. 204-216.

BM Bellare, M., and Micali, S.: "How to Sign Given Any Trap-Door Function", *STOC, 1988*, pp. 32-34.

DEK Dolev, D., Even, S., Karp, R.: "On the Security of Ping-Pong Protocols," *Advances in Cryptology: Proc. of Crypto'82*, Plenum Press, pp. 177-186, 1983.

DH Diffie, W.,, Hellman, M.: "New Directions In Cryptography," *IEEE Trans. on Inf. Theory*, 1976, IT-22, pp. 644-654.

GMR Goldwasser, S., Micali, S., Rivest, R.L.: "A Digital Signature Scheme Secure Against Chosen Message Attacks," *SIAM J. On Comput.*, Vol. 17, No. 2, 1988, pp. 281-308.

M McCurley, K.S.: "A Key Distribution System Equivalent to Factoring," *J. of Cryptology*, Vol. 1, No. 2, 1988, pp. 95-106.

MTI Matsumoto, T., Takashima, Y., Imai, H.: "On Seeking Smart Public-Key-Distribution Systems," *The Transactions of the IECE of Japan*, Vol. E69, No. 2, February 1986, pp. 99-106.

NY89 Naor, M., Yung, M.: "Universal One-Way Hash Functions and their Cryptographic Applications," *STOC*, 1989, pp. 33-43, 1989.

NY90 Naor, M., Yung, M.: "Public-Key cryptosystems provably secure against chosen ciphertext attacks," to appear.

R Rabin, M.O.: "Digital Signature and Public Key Functions as Intractable as Factoring," Technical Memo TM-212, Lab for Computer Science, MIT, 1979.

RSA Rivest, R.L., Shamir, A., and Adelman, L.: "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," *Commun. ACM* 1978, 21, pp. 120-126.

S Shmuely, Z.: "Composite Diffie-Hellman Public-Key Generating Systems Are Hard to Break," TR. No. 356, *Computer Science Dept. Technion, IIT* , Feb. 1985.

YS Yacobi, Y., Shmuely, Z.: "On Key Distribution Systems," Proc. *Crypto'89.*