ADVANCES IN CRYPTOLOGY CRYPTO 2004 pdf

1: Cryptography Research - IBM

Crypto , the 24th Annual Crypto Conference, was sponsored by the Int- national Association for Cryptologic Research (IACR) in cooperation with the IEEE Computer Society Technical Committee on Secu.

Moreover, the length of the data block is constant. The situation discussed in this paper arises in SSL V. After that, the client and server may send their public keys and certificates. The client then generates a random secret bit 10 Daniel Bleichenbacher string called pre master secret, encrypts that secret bit string with RSA if that mode was chosen earlier , and sends the resulting ciphertext to the server. The server decrypts the ciphertext. If the plaintext is not PKCS conforming, the server sends an alert message to the client and closes the connection; otherwise, the server continues the handshake protocol. Finally, the client has to send a finished message, which contains strong authentication. In particular, the client has to know the pre master secret to compute that message. Because an attacker must generate a finished message that depends on the pre master secret, she cannot complete the handshake protocol successfully. However, she does not have to complete it; she gets the necessary information â€" namely, whether her chosen message is PKCS conforming â€" before the protocol is finished. There are details of SSL V. Figure 2 shows the format of the message containing the pre master secret before the latter is encrypted with RSA. It contains the version number of the protocol, the purpose of which is to detect versionrollback attacks, in which an attacker tries to modify the hello messages such that both client and server use the compatibility mode and hence use the Version 2. One implementation that we analyzed [12] checks the version number only if the server is running in the compatibility mode, because otherwise obviously no rollback attack has occurred. A much more secure implementation would check the version number in all modes, and, if it identified a mismatch, would send back to the client the same error alert as it sends in the case of a decryption error. The SSL documentation does not specify clearly the error conditions and corresponding alerts. As a result, different implementations of SSL do not react consistently with one another in error situations. We tested the algorithm with different bit and bit keys. The algorithm needed between thousand and 2 million chosen ciphertexts to find the message. We implemented our own version of the oracle, rather than using an existing software product. Finney checked three different SSL servers [6] to find out how carefully the servers analyze the message format and what error alerts are returned. One of the servers verified only the PKCS format. The second server checked the PKCS format, message length, and version number, but returned different message Chosen Ciphertext Attacks Against Protocols 11 alerts, thus still allowing our attack. Only the third server checked all aspects correctly and did not leak information by sending different alerts. We conclude not only that it is important to include a strong integrity check into an RSA encryption, but also that this integrity check must be performed in the correct step of the protocol â€" preferably immediately after decryption. The phase between decryption and integrity check is critical, because even sending out error messages can present a security risk. We also believe that we have provided a strong argument to use plaintext-aware encryption schemes, such as the one described by Bellare and Rogaway [3]. Note that plaintext awareness implies security against chosenciphertext attacks [2,3]. In particular, Version 2 of PKCS 1, which makes use of [3], is not susceptible to the attack described in this paper. It is a good idea to have a receiver check the integrity of a message immediately after decrypting that message. Even better is to check integrity before decrypting a message, as Cramer and Shoup show is possible [4]. I am grateful for the cooperation of the people at RSA Laboratories. Bit security of RSA and Rabin functions. SIAM Journal of computing, 17 2: Relations among notions of security for public-key encryptions schemes. A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack. Netscape, Mountain View, CA, Why and how to establish a private code on a public network. Science, pages â€", Chicago, The security of individual RSA bits. Redwood City, CA, Nov. A new public key cryptosystem is proposed and analyzed. The scheme is quite practical, and is provably secure against adaptive chosen ciphertext attack under standard intractability assumptions. There appears to be no previous cryptosystem in the literature that enjoys both of these properties simultaneously. The scheme is quite practical, requiring just a few exponentiations over a group. Moreover, the proof of security relies only on a standard intractability assumption, namely, the hardness of the Diffie-Hellman decision problem in the underlying group. The hardness of the Diffie-Hellman decision problem is essentially equivalent to the semantic security of the basic El Gamal encryption scheme [12]. Thus, with just a bit more computation, we get security against adaptive chosen ciphertext attack, whereas the basic El Gamal scheme is completely insecure against adaptive chosen ciphertext attack. Actually, the basic scheme we describe also requires a universal one-way hash function. In a typical implementation, this can be efficiently constructed without extra assumptions; however, we also present a hash-free variant as well. While there are several provably secure encryption schemes in the literature, they are all quite impractical. Also, there have been several practical cryptosystems that have been proposed, but none of them have been proven secure under standard intractability assumptions. The significance of our contribution is that it provides a scheme that is provably secure and practical at the same time. There appears to be no other encryption scheme in the literature that enjoys both of these properties simultaneously. However, this guarantee of secrecy is only valid when the adversary is completely passive, i. Indeed, semantic security offers no guarantee of secrecy at all if an adversary can mount an active attack, i. To deal with active attacks, Rackoff and Simon [20] defined the notion of security against an adaptive chosen ciphertext attack. If an adversary can inject messages into a network, these messages may be encryptions, and the adversary may be able to extract partial information about the corresponding cleartexts through its interactions with the parties in the network. The restriction proposed by Rackoff and Simon is the weakest possible: A different notion of security against active attacks, called non-malleability, was proposed by Dolev, Dwork, and Naor [9]. Here, the adversary also has access to a decryption oracle, but his goal is not to obtain partial information about the target ciphertext, but rather, to create another encryption of a different message that is related in some interesting way to the original, encrypted message. It turns out that non-malleability and security against adaptive chosen ciphertext attack are equivalent [10]. A cryptosystem secure against adaptive chosen ciphertext attack is a very powerful cryptographic primitive. It is essential in designing protocols that are secure against active adversaries. For example, this primitive is used in protocols for authentication and key exchange [11,10,2] and in protocols for escrow, certified e-mail, and more general fair exchange [1,22]. There are also intermediate notions of security, between semantic security and adaptive chosen ciphertext security. Naor and Yung [19] propose an attack model where the adversary has access to the decryption oracle only prior to obtaining the target ciphertext, and the goal of the adversary is to obtain partial information about the encrypted message. Previous Work Provably Secure Schemes. Naor and Yung [19] presented the first scheme provably secure against lunch-time attacks. Subsequently, Dolev, Dwork, and Naor [9] presented a scheme that is provably secure against adaptive chosen ciphertext attack. All of the previously known schemes provably secure under standard intractability assumptions are completely impractical albeit polynomial time , as they rely on general and expensive constructions for non-interactive zeroknowledge proofs. Damgard [8] proposed a practical scheme that he conjectured to be secure against lunch-time attacks; however, this scheme is not known to be provably secure, and is in fact demonstrably insecure against adaptive chosen ciphertext attack. Zheng and Seberry [24] proposed practical schemes that are conjectured to be secure against chosen ciphertext attack, but again, no proof based on standard intractability assumptions is known. Lim and Lee [16] also proposed practical schemes that were later broken by Frankel and Yung [13]. Bellare and Rogaway [3,4] have presented practical schemes for which they give heuristic proofs of adaptive chosen ciphertext security; namely, they prove security in an idealized model of computation, the so-called random oracle model, wherein a hash function is represented by a random oracle. Shoup and Gennaro [22] also give El Gamal-like schemes that are secure against adaptive chosen ciphertext attack in the random oracle model, and that are also amenable to efficient threshold decryption. We stress that although a security proof in the random oracle model is of some value, it is still only a heuristic proof. In particular, these types of proofs do not rule out the possibility of breaking the scheme without breaking the underlying intractability assumption. Nor do they even rule out the possibility of breaking the scheme without finding some kind of weakness in the hash function, as recently shown by Canetti, Goldreich, and Halevi [7]. Security is defined via the following game played by the adversary. After receiving the ciphertext from the encryption oracle, the adversary continues to query the decryption oracle, subject only to the restriction that the query must be different than the output of the encryption oracle. The cryptosystem is said to be secure against adaptive chosen ciphertext attack if the advantage of any polynomial-time adversary is negligible as a function of the security parameter. The one that we shall use is the following. Let G be a group of large prime order q, and consider the following two distributions: An algorithm that solves the Diffie-Hellman decision problem is a statistical test that can effectively distinguish these two distributions. That is, given a quadruple coming from one of the two distributions, it should output 0 or 1, and there should be a non-negligible difference between a the probability that it outputs a 1 given an input from R, and b the probability that it outputs a 1 given an input from D. The Diffie-Hellman decision problem is hard if there is no such polynomial-time statistical test. This formulation of the Diffie-Hellman decision problem is equivalent to several others. Note that by a trivial random self-reducibility property, it does not matter if the base g is random or fixed. Second, although we have described it as a problem of distinguishing two distributions, the Diffie-Hellman decision problem is equivalent to the worst-case decision problem: This equivalence follows immediately from a random selfreducibility property first observed by Stadler [23] and later by Naor and Reingold [17]. Related to the Diffie-Hellman decision problem is the Diffie-Hellman problem given g, g x and g y , compute g xy , and the discrete logarithm problem given g and g x , compute x. There are obvious polynomial-time reductions from the Diffie-Hellman decision problem to the Diffie-Hellman problem, and from the Diffie-Hellman problem to the discrete logarithm problem, but reductions in the reverse direction are not known. Moreover, these reductions are essentially the only known methods of solving the Diffie-Hellman or Diffie-Hellman decision problems. All three problems are widely conjectured to be hard, and have been used as assumptions in proving the security of a variety of cryptographic protocols. Some heuristic evidence for the hardness of all of these problems is provided in [21], where it is shown that they are hard in a certain natural, structured model of computation. See [23,17,6] for further applications and discussion of the Diffie-Hellman decision problem. Note that the hardness of the Diffie-Hellman decision problem is equivalent to the semantic security of the basic El Gamal encryption scheme. On the one hand, if the Diffie-Hellman decision problem is hard, then the group element hr could be replaced by a random group element without changing significantly the behavior of the attacker; however, if we perform this substitution, the message m is perfectly hidden, which implies security.

2: Advances in Cryptology â€” CRYPTO - Wikidata

Advances in Cryptology - CRYPTO 24th Annual International Cryptology Conference, Santa Barbara, California, USA, August , , Proceedings (Lecture Notes in Computer Science) Paperback - September 20,

We review and draw a unifying picture of the several approaches to expressive encryption systems that have recently appeared from lattices, and explore the innovative techniques that underpin them. To appear We introduce a broad lattice manipulation technique for expressive cryptography, and use it to realize functional encryption for access structures from post-quantum hardness assumptions. Specifically, we build an efficient key-policy attribute-based encryption scheme, and prove its security in the selective sense from learning-with-errors intractability in the standard model. Our construction is made possible by observing how to realize, in the peculiar world of lattices, certain special properties that secret sharing schemes need to satisfy in order to discriminate close but imperfect matches between key and ciphertext. Armed with this new tool, we construct an entirely new kind of hierarchical identity-based encryption system in the standard model. Its distinguishing feature is that the ciphertext dimension does not increase as one walks down the hierarchy. We extend the recent Agrawal-Boneh-Boyen identity-based mechanism from selective to adaptive security, in the standard model. Our approach is a distant relative of that of Waters in bilinear groups. However it avoids a number of earlier difficulties by exploiting some elegant mathematical features specific to lattices. As a direct application, we offer the most efficient to date fully secure signature scheme based on a classic assumption in the standard model, and make connections to IBE. From it we build a selectively secure IBE scheme that is almost as compact as the best known random-oracle scheme, but in the standard model. We further make the case that our basic IBE construction is open to many extensions: We construct the first though not only provably secure identity-based encryption system from lattices in the standard model. It is based on a very straightforward though quite inefficient bit-by-bit parsing of the recipient identity. At least two similar constructions have appeared independently and concurrently to ours. Zheng, Practical Signcryption, Springer, This book chapter defines the identity-based signcryption primitive, discusses its advantages and disadvantages over the regular public-key notion, and presents a formal security model that captures the multiple and sometimes contradictory security objectives that one could seek from it. A construction that meets a maximal set of security properties will provide a concrete example, and a brief survey of the literature will conclude the chapter. It demonstrates how any basic IBE scheme in this family can be extended generically into powerful extensions such as Hierarchical and Attribute-based IBE, akin to the similar extensions that already exist in the Commutative-Blinding IBE framework. This chapter starts by giving a comparison between the three main approaches to IBE from pairings as we currently know them, and then gives a brief overview of how the properties of this framework have been exploited to generalize the BB1 template into a broad variety of Super-IBE schemes. Practical Frameworks Compared , invited article, in Int. Applied Cryptography, inaugural issue, This updated review of identity-based encryption algorithms first provides a classification and characterization of the various approaches, and goes on to describe in further details an optimized instantiation of each of the main paradigms, with reducibility to practice as the principal optimization parameter. The survey concludes with an evaluation of the relative strengths and weaknesses of each construction, according to a number of theoretical and practical criteria, spanning the range from abstract security reduction issues to concrete algebraic implementation concerns. In this short piece, we take an informal walk through the Why, the What, and the How of bilinear pairings in cryptography. We briefly review the nature of these mathematical objects, as well as some of their recent uses in cryptographic constructions. This is an augmented full version of the following original paper: The present version has been significantly updated, and the two main schemes now called BB1 and BB2, following usage have been generalized in several ways. We show among other things that the native schemes can be used in full adaptive-security mode, with a simple parameter tweak, while remaining practical. We present a classification of existing identity-based encryption schemes, and remark that the most efficient schemes to date, such as BB2 and SK, belong to a class that is not known to support any the many extensions afforded by the BB1 scheme in particular. We define the Exponent Inversion class of IBE schemes, and give an abstraction from which it is easy to build many ad hoc extensions, such as Hierarchical and Fuzzy IBE, provided that a few general conditions are met. As a bonus, this gives us a very efficient Anonymous IBE that is the first such scheme with a proof of security in the standard model. The security of both schemes is based solely on the Decision Linear assumption in symmetric or asymmetric bilinear groups. Security proofs are given under a new complexity assumption, called Bilinear Diffie-Hellman Exponent, which generalizes the Bilinear Diffie-Hellman Inversion assumption. We describe numerous applications of the new construction; these include a very efficient broadcast cryptosystem, a time capsule, and the most efficient forward secure public key and HIBE systems to date. We present a fully secure Identity Based Encryption scheme whose proof of security does not hinge upon the random oracle heuristic. Security is based on the decisional version of the now classic Bilinear Diffie-Hellman assumption. We view our construction as an existence proof that resolves an open problem posed by Boneh and Franklin in We provide tight proofs of security of both systems in the slightly weaker sense of security against selective identity attacks, in which the adversary must commit ahead of time to the identity that it intends to attack. We also turn both constructions into practical and secure IBE systems in the stronger sense of security against adaptive identity attacks, in the standard model, under some security penalty. The construction is based on the Bilinear Diffie-Hellman assumption, and proved secure in the random oracle model. We present a very compact public-key cryptosystem secure against adaptive chosen-ciphertext attacks, with no explicit redundancy, and with a tight random-oracle reduction to a static Diffie-Hellman hardness assumption. We flesh out the many details of the construction and its security proof. We describe a very simple technique that leverages the properties of certain identity-based encryption schemes to obtain chosen ciphertext security in the standard model, without resorting to external primitives such as signatures or authentication codes. Our technique works with the Boneh-Boyen and Waters IBE systems, and relies on a property of the Boneh-Boyen simulation proof shared by these systems that makes it possible for an IBE ciphertext to authenticate itself. We define and construct a collective signature that blends the revocable anonymity of group signatures with the expressiveness of mesh signatures. These new signatures retain the user enrollment and revocable anonymity properties of group signatures, but allow any subgroup of users collectively to issue signatures, while hiding or revealing precisely how they derive the capacity to do so on behalf of the group. We define mesh signature as a modular and expressive generalization of ring signatures, which are non-repudiable anonymous signatures on behalf of a crowd. Unlike ring signatures, mesh signatures are constructed modularly from atomic signatures without requiring the private keys, and express complex access structures beyond mere disjunctions. In particular, certificate chains may be substituted for public keys that are kept off the record. Our mesh signatures are compact and unconditionally anonymous, and subsume the most efficient ring signatures with everlasting anonymity without random oracles or trusted setup authority. We construct the first practical and efficient group signature scheme that is provably secure in the standard model. Our scheme is simple and easy to implement using bilinear pairings. We prove its security without random oracles based on two mild assumptions in bilinear groups: We construct a short and practical group signature scheme whose signatures have approximately the size of standard RSA signatures with the same security. We prove security in the random oracle model using a variant of the security definition for group signatures recently given by Bellare, Micciancio, and Warinschi. Security is based on two complexity assumptions in bilinear groups: Among many improvements, we introduce a slightly weaker and more general version of the Strong Diffie-Hellman assumption, and give a proof of the BB short signature scheme based on this weaker assumption. We introduce and implement forward secure signatures with untrusted update. In forward secure signatures, signing keys are frequently updated in an non-reversible manner to ensure that signatures emitted prior to a breach remain trustworthy. Unfortunately, this typically conflicts with the customary practice of encrypting signing keys with a passphrase, used to lessen the chance of exposure in the first place. To reconcile these requirements, we introduce the notion of untrusted update on the encrypted signing key itself, without decryption. We give an example implementation to demonstrate the real-world practicality of our scheme. We describe a short signature scheme which is existentially unforgeable under a chosen message attack without using random oracles. The security of our scheme depends on a new complexity assumption we call the Strong Diffie-Hellman assumption. This assumption has similar properties to the Strong RSA assumption, which was previously used to construct signature schemes without random oracles; however the signatures generated by our scheme are much shorter and simpler. We propose a compression technique that significantly reduces the size of the public key in the Peikert-Waters lossy trapdoor construction. Our technique applies to the discrete-log realization of the lossy trapdoor, which we must instantiate in a bilinear group in order to carry out the compression. The final key size is reduced from cubic to quadratic in the security parameter, giving us the most compact lossy trapdoor of the discrete-log type though factoring-based ones are even more compact. Network coding is a method for achieving channel capacity in networks. The key idea is to allow network routers to linearly mix packets as they traverse the network so that recipients receive linear combinations of packets. Network coded systems are vulnerable to pollution attacks where a single malicious node floods the network with bad packets and prevents the receiver from decoding correctly. Cryptographic defenses to these problems are based on homomorphic signatures and MACs. These proposals, however, cannot handle mixing of packets from multiple sources, which is needed to achieve the full benefits of network coding. In this paper we address integrity of multi-source mixing. We propose a security model for this setting and provide a generic construction. Departing from the password protocols and practices in use since the early nineties, we advocate a new approach to password security that maximizes the protection offered to a human user against any attacker, whether rogue or trusted. We show how to reach the toughest attainable security from the meekest memorable secrets, online and offline, using cryptographically sound yet eminently practical techniques. In this paper we revisit the previously introduced notion of distributed public-key cryptography from weak secrets such as independent short passwords held by a small group of friends. Whereas the earlier result was mostly definitional with a proof of concept that relied on certain generic and very inefficient simulation-sound zero-knowledge proof systems, here we show how to construct such systems very efficiently from pairings, and based only on the linear assumption in the standard model. Our solution applies to a large class of ElGamal-type cryptosystems in bilinear groups. Human-memorable passwords and public-key cryptography generally do not mix: What if, instead, the private key were created from not one but many passwords held by different users? In this paper, we show how to do this in a secure manner, using distributed protocols that in particular never require the users to share their passwords with anyone else, even the other participants. We start by defining general functionalities for key-pair generation and private-key-based computations in the UC model, and then show how to realize them by giving distributed password-based protocols for the ElGamal cryptosystem. Our protocols run over adversarially controlled channels, are reasonably efficient given the nature of the problem, and generalize easily to other and more complex tasks, such as distributed signature and identity-based encryption most notably. How should we authenticate ourselves on the Internet? We propose an asymmetric password-based remote mutual authentication protocol for use between a human client and a machine server. On the client side, it requires no storage other than a small password, and it is robust to the reuse of the same password with multiple and potentially malicious servers. After analyzing the various shortcomings of several naive solutions, we propose a formal security model that captures the peculiar threats faced by the user in this endeavor. Based on this model, we show how some very ancient protocols such as unique blind signatures provide an elegant and practical solution for our task, and quantify how much of a challenge outsider and insider adversaries will be faced when trying to crack the secret. To the best of our knowledge, this paper offers the first formal study of minimally trusted credential repositories for roaming users, and has immediate applications for ad-hoc single-sign-on internet authentication. Perhaps paradoxically, we argue that the venerable concept of salted iterated hashing, utilized almost universally for deriving cryptographic keys from human-memorable passwords, does not provide the best possible security against brute-force offline dictionary attacks. We introduce the stronger notion of Halting Key Derivation Function, and show how it can improve the security of any real-world password-based encryption system. The principle is to let people attach to their password a secret and forgettable cryptographic delay, and condition the key derivation to halt after the hidden delay only when unlocked by the correct password. This design not only increases by a couple of bits the effective strength of any password that we feed to it, but also presents operational advantages that further enhance its long-term security. We demonstrate an actual implementation that interfaces nicely with existing encryption software, and quantify the exact security attained. Generally, a master password is used to encrypt a multitude of user credentials. With Kamouflage, we attempt to make even incorrect decryptions look like plausible credentials.

3: Advances in Cryptology: CRYPTO â€” NYU Scholars

Advances in Cryptology - CRYPTO 24th Annual International Cryptology Conference, Santa Barbara, California, USA, August , Proceedings.

4: dblp: CRYPTO Santa Barbara, California, USA

Advances in Cryptology - CRYPTO 24th Annual International Cryptology Conference, Santa Barbara, California, USA, August , , Proceedings.

5: Advances In Cryptology Crypto | Download eBook PDF/EPUB

Crypto , the 24th Annual Crypto Conference, was sponsored by the Int- national Association for Cryptologic Research (IACR) in cooperation with the IEEE Computer Society Technical Committee on.

6: C. Pandu Rangan - Wikipedia

Proceedings of CRYPTO Advances in Cryptology - CRYPTO , 24th Annual International CryptologyConference, Santa Barbara, California, USA, August , , Proceedings, Springer.

7: Advances in Cryptology - CRYPTO 28th Annual International Cryptology - Google Books

a| Annotation b| This book constitutes the refereed proceedings of the 24th Annual International Cryptology Conference, CRYPTO , held in Santa Barbara, California, USA in August The 33 revised full papers presented together with one invited paper were carefully reviewed and selected from submissions.

8: dblp: CRYPTO Santa Barbara, California, USA

Download advances in cryptology crypto or read online here in PDF or EPUB. Please click button to get advances in cryptology crypto book now. All books are in clear copy here, and all files are secure so don't worry about it.

9: IDB Crypto - VoCaoSan

This book constitutes the refereed proceedings of the 24th Annual International Cryptology Conference, CRYPTO , held in Santa Barbara, California, USA in August

ADVANCES IN CRYPTOLOGY CRYPTO 2004 pdf

40 baptismal meditations Sheet metal die design book The Freak Brothers Bus Line and Other Tales (Freak Brothers #11) Healthcare provider organizational structuring Jap Sahib, Swayas and Ardas Sex and the nature of things Learning without burden Celeste goes dancing, and other stories Software Process Improvement 1001 calculus problems for dummies Revelation (New Testament Readings) Feeding the healthy vegetarian family Depression and personality Shirley Yen, Meghan E. McDevitt-Murphy, and M. Tracie Shea Fedora 25 networking guide Brief chronology of the war Unemployment, Poverty and Social Policy in Europe Comprehensive management of Parkinsons disease Design by accident From parasites to public servants: the rehabilitation of the rich Symbolism of Light and Color Athenas divine birth priestesshood Biographical and Historical Memoirs of Mississippi (Vol. 2 Part 1) The Lean Six Sigma Value Proposition The Oxford guide to the English language. Workers experiences God reconciles ALL in Heavens and on Earth (Col. 1:18-23) Cry mercy, cry love Modulation of Cftr Enac Channel Function by Interacting Proteins Trafficking Good Business Pamphlet Energy, ecology, economy. Strategic management and business policy 15th ed The influence of culture on visual perception Key titles for integrating celebrations and holidays into the social studies curriculum Conservation of medicinal plants Probing our prejudices Pirandello six characters in search of an author Impact of short interspersed elements (SINEs on the host genome Autonomous flying robots Berlin stories robert walser Plantation Play-Song