

How to guarantee files encrypted and transmitted today stay confidential for years to come.

BY CHI-SUNG LAIH, SHANG-MING JEN, AND CHIA-YU LU

Long-Term Confidentiality of PKI

The ubiquitous cryptographic Public Key Infrastructure (PKI) faces a multitude of privacy-protection risks. A notable issue is long-term security, which can be deconstructed into long-term authenticity and long-term confidentiality. Authenticity has been widely discussed over the past decade, while confidentiality

has generally been neglected. As the factorization of RSA advances, there is increased urgency to refresh the confidentiality of existing instances of PKI with longer-duration validity. Unfortunately, cryptographers have not come up with a realistic solution to the question of how to guarantee long-term confidentiality, the most challenging unaddressed open problem from previous works. In this article, we formalize the problem by defining

the concept of a Privacy-Free Window (PFW) where the previously protected file is now at risk. By taking advantage of a PKI property called “asymmetric secrecy,” we give a specific solution addressing PFW. This method can be further developed to extend the originally defined security duration of some PKIs and other cryptographic tools. We also furnish an algorithm to verify existing protocols and recommend actions for maintaining security as a PFW occurs.

PKI applications are everywhere in modern information technology, including e-commerce, Secure Sockets Layer/Transport Layer Security, and citizen-to-government and government-to-government applications (such as those involving tax reporting, medical insurance, and passports). However, maintaining PKI security is increasingly complicated since cryptographic attacks are more sophisticated than ever.


» key insights

- **Upgrading all PKI instances is systemically and logistically costly since PKI structures and scope are so variable.**
- **We define PFW and quantify long-term confidentiality to highlight the insecure period encountered by encrypted files.**
- **The asymmetric secrecy property is a practical, software-based low-cost solution requiring negligible changes to existing system hardware.**


Long-term security is an important cryptographic issue, as discussed by Lenstra and Verheul⁷ and can be divided into long-term authenticity and long-term confidentiality. Long-term authenticity focuses on the validation of digital signatures that ensures integrity, non-repudiation, and authentication over a period of time. Long-term confidentiality emphasizes privacy protection and securing a secret over a period of time and was viewed by Buchmann and Vollmer² as the most challenging open issue in PKI security. Most previous work emphasized authenticity in long-term security, as discussed in RFC 3126: Electronic Signature Format for Long-term Electronic Signatures.¹¹ Signatures are usually used to sign plaintext, so privacy is not the main concern and can be repackaged to extend validity. Other research (such as Buchmann and Vollmer²) focused on mitigating risk due to advanced computer performance (such as quantum computing) and modern cryptanalysis technology. Using quantum cryptographic methods (such as Okamoto et al.¹⁰) or applying multiple cryptosystems² is usually recommended against this kind of weakness.

To the best of our knowledge, most of the work we have just outlined focused on long-term authenticity rather than on long-term confidentiality, especially in the realm of PKI. A key point is that plaintext is disclosed with the signature, so authenticity may be addressed after signing. On the other hand, confidentiality is protected through a form of ciphertext; once encrypted data is sent, the original participants no longer have control and should assume that attackers are able to eavesdrop and archive the encrypted data. Once ciphertext is communicated, it cannot be recalled for re-encryption. Its security depends on adequate measures determined (or guessed) before sending. These are some of the reasons achieving long-term confidentiality is more difficult than achieving long-term authenticity.

Here, we use the RSA public-key algorithm¹² to illustrate the risk of unintended exposure, since most PKIs implement RSA to provide security. PKI faces two main threats: quantum



PFW is the insecure period starting when the protected file may be compromised (due to advancing cryptanalysis) and ending with its planned expiration.



computation and advancing factorization. If and when quantum computation is achieved, integer factorization in sub-exponential time will render RSA obsolete. However, a more pressing risk is the factorization progress of RSA. In August 1999, Cavallar et al.⁴ factored a 512b (155 decimal digits) RSA modulus, and in December 2009, Kleinjung et al.⁶ factored a 768b (232 decimal digits) RSA modulus. Though factoring a 1,024b RSA modulus is thousands of times more difficult than factoring a 768b modulus, it is expected the 1,024b RSA modulus will be factored by 2020.^{1,8} The estimated data and recommendations concerning the most effective ways to ensure security of various algorithms can be found in Lenstra and Verheul,⁷ NIST FIPS SP800-57,¹ and other works.

For this article, we set aside the risk from yet unrealized theoretical quantum methods to focus on solving factorization challenges facing PKIs in the near future. An important concept is that the RSA algorithm (based on factorization) is considered secure today. The deeper issue is the length of the keys used in the RSA algorithm. Most current PKI users utilize RSA keys less than or equal to 1,024b, with factoring of this key length expected by 2020. Using longer public keys may be a sound solution, but intrinsic to PKI is infrastructure, and upgrading an existing infrastructure is more difficult than creating a software-only solution. Here, we develop a low-cost framework for addressing long-term confidentiality within PKI.

Privacy-Free Window

Legal and business documents have their own retention requirements and must be kept secret for a specified period. If a file is encrypted by a PKI exchange session (or secret) key, the file's security depends not only on the session key but also on other keys, including those used to protect the session key during the exchange.

Long-term confidentiality of a file is contingent on ensured secrecy within the specified retention period so it remains uncompromised by unauthorized third parties. The scenario we explore here involves two participants who want to transmit a secret file without a shared key. Each pos-

sesses a public-key pair stored on an integrated circuit (IC) card issued by a certificate authority (CA). The participant and the CA do not require a pre-shared key. Since the security of the file relies on the encrypting session key that in turn relies on the security of the related encrypting public keys and session keys (used to protect against disclosure to third parties), the security of the file and all related keys are interdependent.

We define PFW as the insecure period starting when the protected file may be compromised (due to advancing cryptanalysis) and ending with its planned expiration (see Figure 1). PFW can serve as an indicator for quantifying long-term confidentiality. Based on retention period and key strength, not all files will exhibit a PFW. If a PFW exists, then long-term confidentiality has been compromised; the table here lists several parameters to illustrate the risks associated with the PFW.

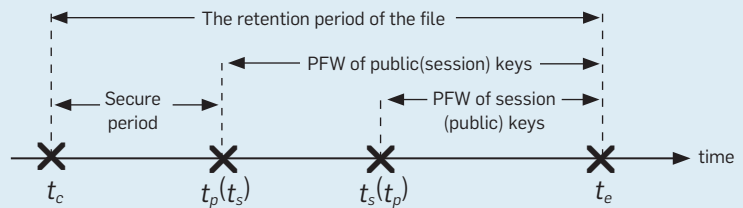
In Figure 1, the file is encrypted at the current time t_c and must be kept secret until expiration time t_e at the end of retention period. At time t_p , the public keys generated at t_c are factored, and the protected file is no longer safe, since the session keys protected by the public keys can be obtained. Even when public keys are not factored, session keys may be independently compromised at time t_s through advanced cryptanalysis. If either event happens before t_e , the protected file is considered compromised. The PFW for a file under an associated protocol can formally be expressed as

$$\min(t_p, t_s) > t_c \text{ (broken keys are not used for encryption)}$$

$$PFW = [\min(t_p, t_s), t_e]$$

If the signature is in jeopardy, the responsible entities can easily extend the validity of the signature through encapsulation. Standards (such as RFC3126¹¹) are available for encapsulation, but long-term confidentiality is not well researched. Previously proposed approaches would usually apply safer cryptographic methods, using longer encryption keys or shorter retention periods. These measures are

Figure 1. Privacy-free window.



viable in software but often fail to account for hardware limitations.

The concept of session keys in our scenario is a software issue. A sound recommendation for long-term secure communications is proactive selection of algorithms and keys with adequate security levels suitable for the entire retention period. For example, the Advanced Encryption Standard (AES) with a 128b key and 10-round encryption is adequate for achieving confidentiality for at least the next 20 years.¹ Even stronger AES can provide more robust protection. This implies it is trivial to make $t_s > t_p$ and is also a prerequisite for the following discussion. However, algorithms and keys can be limited by non-software circumstances. For example, a PKI may contain millions of IC cards, as in the case of citizen identification. In this instance, card renewal involves not only cost but also logistical concerns arising from updating or renewing cards within a reasonable amount of time. To surmount this problem we must contend with the bottleneck of infrastructure, as well as update existing PKI systems with minimal change. In the following sections, we propose a cost-efficient concept to mitigate the current PFW problem within PKI and maintain security for longer periods than originally envisioned.

Asymmetric Secrecy Property in PKI

PKI users commonly use RSA with 1,024b keys, while CAs commonly use 2,048b to 4,096b keys for safety reasons. For example, the Ministry of the Interior's Certification Authority of Taiwan (MOICA) uses a CA with 2,048b public/private keypair and administers more than 2.48 million users holding National Identification

Parameters of events and their times.

Time	Description
t_c	The time a file is encrypted.
t_p	The public keys used in the PKI at time t_c are factored or compromised.
t_s	The session keys used in the PKI at time t_c are compromised.
t_e	The expiration time of a file.

IC cards with 1,024b public/private keypair.⁹ The asymmetric secrecy property manifests in PKI because the CA usually uses cryptographic parameters with higher bit keys than normal users. This means the user-to-CA link is much safer than the CA-to-user link, since the former is protected by the CA's public key, whereas the latter is protected by the user's public key. By exploiting this property to employ a new protocol on the existing infrastructure, security issues may be mitigated without having to renew the entire infrastructure.

Consider the following example of the PFW utilizing a modified instance of an existing protocol. Kerberos,⁸ which Burrows et al.³ proved was logically secure for authentication, assumes pre-shared session keys between participants (users) and the server (CA). Our Kerberos analogue (see Figure 2) presupposes no shared keys between participants and server, using instead public keys to provide equivalent security (proved by Burrows's method³) at the time of encryption. In this scenario, A and B are principals, and S is the server. In message 1, key exchange is initiated by A , who expresses to S the desire to communicate with B . In message 2, S responds with a message encrypted by A 's public

key PU_A containing a ticket encrypted by B 's public key PU_B , the session key K_{AB} , and other temporary parameters. Principal A then sends the received ticket to share K_{AB} with B . Finally, B replies to A using a message encrypted by K_{AB} to complete the key exchange.

Since all participants are able to generate suitable session keys, as the software solution assumes in our scenario, all session keys and symmetric encryption algorithms are adequately robust and able to achieve long-term confidentiality required during the retention period. We also assume encrypting time $t_c = 2012$ and a retention period for the encrypted file of 15 years, or $t_e = 2027$.

In this example, the steps pertaining to long-term confidentiality consist of message 2 in which S responds to A and message 3 in which A connects to the requested resource, B . In

message 2, K_{AB} is encrypted through 1,024b PU_A . According to Kleinjung et al.,⁶ RSA-1024 may be factored around 2019. If factored as predicted, a PFW will exist from 2019 to 2027. PU_B in Step 3 suffers from the same problem. When it occurs, the scheme will not provide long-term confidentiality.

Figure 3 is our modified protocol taking advantage of the asymmetric secrecy property inherited from Kerberos. To ensure the feasibility of authentication, see the online appendix, where we prove the necessary authenticating behaviors—results (1) to (4) in the appendix—are maintained. They are analogous to the original Kerberos functions, as outlined by Burrows et al.³ Compared to Kerberos, our modified protocol involves two major changes: First, an unnecessary ticket in message 2 is removed, since it was redundant in Burrows³; and sec-

ond, we used the asymmetric secrecy property to exchange new safer session keys for server-to-principal links, originally protected by the principals' public keys. In our protocol, we define two new session keys, K_{AS} and K_{BS} , with exchanges protected by the safe principal-to-server links in messages 1 and 3-2. It then uses K_{AS} and K_{BS} to protect the server-to-principal links in messages 2 and 3-3.

Since authentication functionalities are proved, we now examine confidentiality in our protocol. In message 1 and message 3-2, the public key PU_{KS} is at 2,048b to 4,096b, adequate for keeping the session keys secure until the retention period ends in 2027, according to Barker et al.¹ and Lenstra and Verheul.⁷ Aside from these steps, session keys K_{AS} , K_{BS} , and K_{AB} are assumed secure since they can be regenerated as needed by principals to satisfy their security requirements.

The server in Kerberos can be viewed as a particular kind of CA. Our protocol demonstrates how the asymmetric secrecy property we have described here helps some PKIs extend their lifetimes through a low-cost method. Ours is primarily software-based for handling inherent hardware constraints, allowing use of the stronger cryptographic capabilities of servers to compensate for unplanned lapses in security assurance. If the target PKI is in a hierarchical structure, the inference is that the root CA may hold the longest public/private keypair. The asymmetric secrecy property may be extended upward to include higher-level CAs providing a longer period of security by virtue of longer keys.

Discussion

Our algorithm (in the appendix) provides criteria for determining the existence of the PFW. No matter which cryptographic method is employed (such as Elliptic Curve Cryptography and RSA), the algorithm is always suitable for evaluating the long-term confidentiality of a protocol. As long as the asymmetric secrecy property holds, the protocol can achieve long-term confidentiality. With the proposed algorithm, if the PFW does not exist, the original protocol is used since the modified protocol is slightly more complex and there is no

Figure 2. Kerberos analogue (key exchange and authentication example).

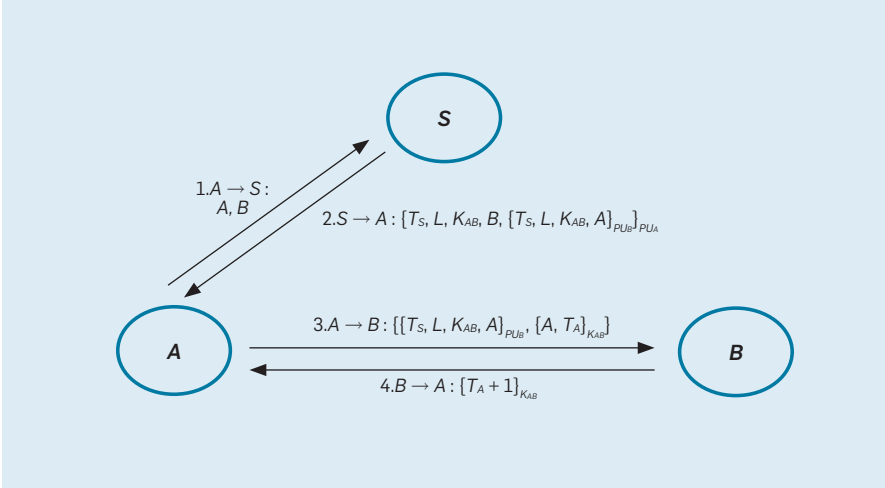
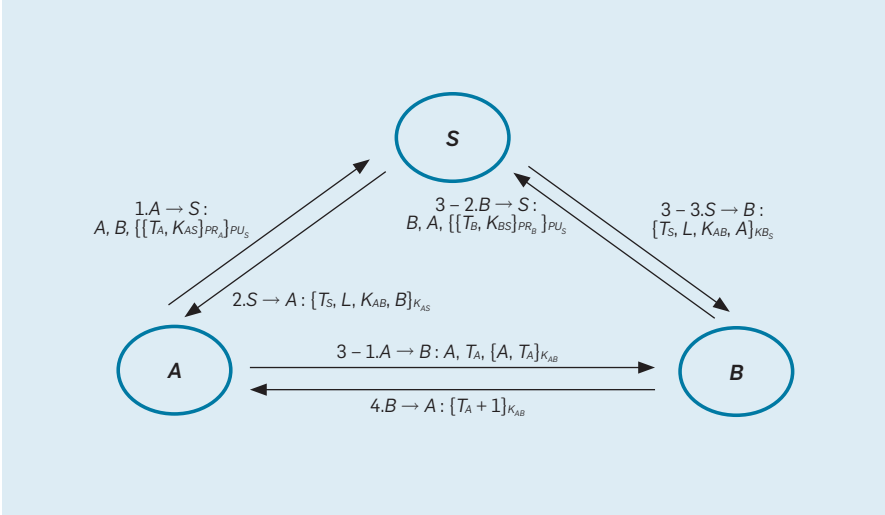


Figure 3. Modified protocol with asymmetric secrecy property.



benefit from using the asymmetric secrecy property.

Messages protected by participants' public keys in Figure 2 that were once secure are rendered insecure by a PFW. The vulnerability of these encrypting public keys is compensated in Figure 3 by supplemental messages to reinstate acceptable security using the asymmetric secrecy property. These messages consist of communications between participants and the server to exchange secure session keys through the secure channels provided by the server's public key.

Along with existing communication between participant and server, some of these supplemental messages are concatenated with existing messages. For example, the first two messages in Figure 2 and Figure 3 perform equivalent actions, though the communication in Figure 3 derives added benefit from the server's longer keys. When inter-participant communications require additional security (such as message 3 in Figure 2, originally protected by PU_B), another two messages (such as 3-2 and 3-3 in Figure 3) must be introduced to achieve the security requirement. Note the functionality of message 3 in Figure 2 is replaced by messages 3-1 to 3-3 in Figure 3.

In our key-exchange protocol, though two extra messages are required to maintain long-term confidentiality, this added load is required only when the participants are constructing new secure communications channels when a PFW exists. The key exchanges are performed only once per session. This additional overhead is marginal and should be within the CA's capacity. Even if that capacity is exhausted, additional servers can scale the service and solve the capacity problem in a centralized manner.

Conclusion

Security of cryptographic algorithms is the most important element in network applications concerning confidentiality and authenticity. All these network activities are based on trust due to cryptography. Modern cryptographic methods provide robust tools for short-term security, but how can they guarantee files encrypted today are also secure until their planned expiration date? Many

measures have been proposed in the literature, but most focus on the signature rather than privacy and lack realistic considerations. In this article, we have defined PFW to highlight the insecure period encountered by an encrypted file and quantify its long-term confidentiality.

PKI is the most common application of cryptography but suffers from a lack of long-term confidentiality. The article's most important contribution is to show how to utilize a very significant property in PKI we call the asymmetric secrecy property. By exploiting it, we provide a practical software-based, low-cost solution requiring little change to existing system hardware. Our secure modified protocol gives credence to the proposed method. An algorithm for evaluating protocols for key and data exchange is described in the appendix, along with two examples requiring different retention periods and related reactions.

Upgrading all instances of PKI is a systemic issue, since various PKIs involve different structures and purposes. However, the concept we have discussed—how to ensure long-term confidentiality—may help mitigate PKI shortcomings. Furthermore, the asymmetric secrecy concept can also be extended to upgrade existing cryptographic tools (such as Kerberos) and other protocols. Addressing PFW through uncomplicated, low-cost solutions is especially appealing today, ahead of the arrival of quantum computing. In this way, long-term security, especially involving privacy, can be ensured for the near future.

Acknowledgment

We wish to express our gratitude to Michael Chang (macst34@gmail.com) for discussions and his review of the English in this article. □

References

1. Barker, E., Barker, W., Burr, W., Polk, W., and Smid, M. *NIST Special Publication 800-57: Recommendation for Key Management*. National Institute of Standards and Technology, Gaithersburg, MD, May 2007; <http://csrc.nist.gov/publications/PubsSPs.html>
2. Buchmann J., May, A. and Vollmer, U. Perspective for cryptographic long-term security. *Commun. ACM* 49, 9 (Sept. 2006), 50–55.
3. Burrows, M., Abadi, M., and Needham, R. A logic of authentication. *ACM Transactions on Computer Systems* 8, 1 (Feb. 1990), 18–36.
4. Cavallar, S., Dodson, B., Lenstra, A.K., Lioen, W., Montgomery, P.L., Murphy, B., Riele, H., Aardal, K., Gilchrist, J., Guillerm, J., Leyland, P., Marchand, J., Morain, F., Muffett, A., Putnam, C., and Zimmermann,

- P. Factorization of a 512-bit RSA modulus. In *Proceedings of the 19th International Conference on Theory and Application of Cryptographic Techniques*, B. Preneel, Ed. Springer-Verlag, Berlin, Heidelberg, 2000, 1–18.
5. ElGamal, T. A public-key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions on Information Theory* 3, 4 (July 1985), 469–472.
6. Kleinjung, T., Aoki, K., Franke, J., Lenstra, A.K., Thomé, E., Bos, J.W., Gaudry, P., Kruppa, A., Montgomery, P.L., Osvik, D.A., Riele, H., Timofeev, A., and Zimmermann, P. Factorization of a 768-bit RSA modulus. In *Proceedings of the 30th Annual Conference on Advances in Cryptology*, T. Rabin, Ed. Springer-Verlag, Berlin, Heidelberg, 2010, 333–350.
7. Lenstra, A.K. and Verheul, E.R. Selecting cryptographic key sizes. In *Proceedings of the Third International Workshop on Practice and Theory in Public Key Cryptography*, H. Imai and Y. Zheng, Eds. Springer-Verlag, London, 2000, 446–465.
8. Miller, S.P., Neuman, B.C., Schiller, J.I., and Saltzer, J.H. Kerberos authentication and authorization system. In *Project Athena Technical Plan*, Section E.2.1. MIT, Cambridge, MA, Oct. 1988; <http://web.mit.edu/Saltzer/www/publications/athena/plan/e.2.1.pdf>
9. MOICA (Certificate Authority of the Ministry of the Interior of Taiwan). Dec. 2010; <http://moica.nat.gov.tw/html/en/index.htm>
10. Okamoto, T., Tanaka, K., and Uchiyama, S. Quantum public-key cryptosystems. In *Proceedings of the 20th Annual International Cryptology Conference on Advances in Cryptology*, M. Bellare, Ed. Springer-Verlag, London, 2000, 147–165.
11. Pinkas, D., Ross, J., and Pope, N. *Electronic Signature Formats for Long-Term Electronic Signatures*. IETF RFC 3126, Sept. 2001; <http://www.rfc-editor.org/rfc/rfc3126.txt>
12. Rivest, R., Shamir, A., and Adleman, L. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM* 21, 2 (Feb. 1978), 120–126.

Chi-Sung Laih (1956–2010) was a much-loved and respected distinguished professor in the Department of Electrical Engineering of National Cheng Kung University, Tainan City, Taiwan.

Shang-Ming Jen (smjen.tw@gmail.com) is a Ph.D. student in the Department of Electrical Engineering of National Cheng Kung University, Tainan City, Taiwan.

Chia-Yu Lu (joylu.tw@gmail.com) is a Ph.D. student in the Department of Electrical Engineering of National Cheng Kung University, Tainan City, Taiwan.