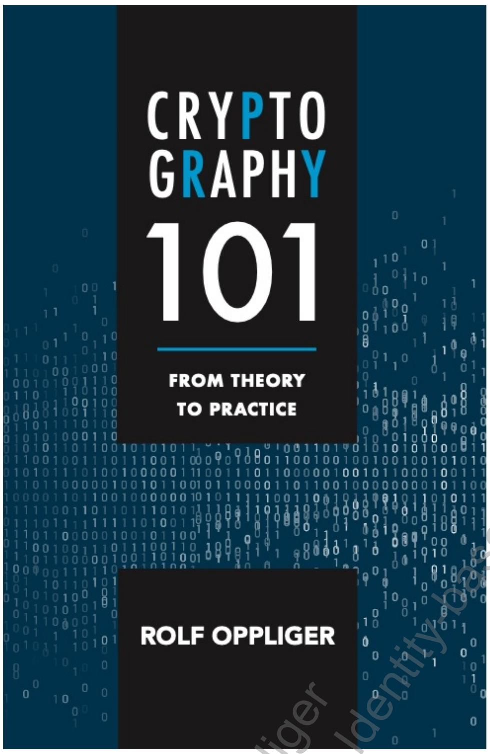

This text comprises a revised version of Section 11.5 about Identity-based Encryption from "Cryptography 101: From Theory and Practice" written by Rolf Oppliger (Artech House, 978-1-63081-846-3)

13.4 IDENTITY-BASED ENCRYPTION

In an asymmetric encryption system, every user has a public key pair, and the keys look somewhat arbitrary and random. Consequently, one faces the problem that one cannot easily attribute a given public key to a particular entity (e.g., user) and that one has to work with public key certificates. A public key certificate, in turn, is a data structure that is issued by a trusted (or trustworthy) certification authority (CA). It is digitally signed by the issuing CA, and it states that a public key really belongs to a particular entity. If there are multiple CAs in place, then one usually talks about public key infrastructures (PKIs). In general, public key certificates, CAs, and PKIs are complex topics, and their implementation has turned out to be more difficult than originally anticipated [28].

In the early 1980s, Shamir came up with an alternative idea [29]. If one chooses a public key to uniquely identify its holder, then one no longer has to care about public key certification in the first place. Instead, a public key is then self-evident in the sense that it automatically becomes clear to whom it belongs (or at least to whom it was issued in the first place). Shamir coined the term *identity-based cryptography* to refer to this cryptographic technique. Like any other technique, identity-based cryptography has advantages and disadvantages:

- The advantages are obvious and related to the avoidance of public key certificates and respective key directory services.
- The disadvantages are less obvious. The most important ones are related to the necessity of having a unique naming scheme and the fact that a trusted authority is needed to generate public key pairs and distribute them. Hence, all entities must trust this authority not to hold illegitimate copies and misuse their private keys.

Note that in a conventional asymmetric encryption system, all entities can generate their own public key pairs. In identity-based cryptography, this cannot be the case, because the public keys must have specific values and it must not be possible for anybody (except the trusted authority) to determine the private key that belongs to a specific public key (otherwise, this person could determine all private keys in use). Consequently, in identity-based cryptography, all entities must provide their identities to the trusted authority, and the trusted authority must equip them with their respective public key pairs, using, for example, smart cards or USB tokens. Another disadvantage that may occur in practice is related to key revocation. What happens, for example, if a key pair needs to be revoked? Since the public key represents the key pair holder's identity, it is not obvious how this key pair can be replaced in some meaningful way.

In [29], Shamir introduced the notion of identity-based cryptography and proposed an identity-based digital signature system (Section 14.3). Shamir also pointed out that the development of an identity-based encryption system is more involved. Note, for example, that the RSA asymmetric encryption system cannot be easily turned into an identity-based encryption system. On the one hand, if n is universal and the same for all users, then anyone who knows an encryption exponent e and a respective decryption exponent d can compute the factorization of n and compute all private keys. On the other hand, if n depends on the user's identity, then the trusted authority cannot factorize n and compute the decryption exponent d that belongs to an encryption exponent e.

It was not until 2001 that Dan Boneh and Matthew K. Franklin proposed an *identity-based encryption* (IBE) system based on bilinear maps called *pairings* on elliptic curves [30, 31]. They suggested using the IBE system as an alternative to commonly used secure messaging technologies and solutions that are based on public key certificates. In the same year, Cocks[20] proposed an IBE system based on the QRP [32]. The Cocks IBE system has a high degree of ciphertext expansion and is fairly inefficient. It is impractical for sending all but the shortest messages, such as a session key for use with a symmetric encryption system, and it is therefore not used in the field.

To explain the Boneh-Franklin IBE system, we have to briefly introduce the notion of *pairing-based cryptography* first.[21] The central idea is the construction of a special mapping between two groups that allows for new cryptographic systems based on the reduction of one problem in one group to a different—usually simpler-to-solve—problem in the other group. In most proposals, the first group is a GDH group introduced in Section 5.2.1, in which the DDHP (Definition 5.7) is simpler to solve than the (computational) DHP (Definition 5.6). While the known implementations of such pairings, such as the *Weil* and *Tate pairings*, require some heavy mathematics, they can be dealt with abstractly, using only the properties of the groups and the respective mappings. In fact, many interesting schemes have been proposed only on abstract mappings, known as *bilinear maps*.

To simplify matters, consider two prime-order groups G_1 and G_2, where G_1 is an additively written group and G_2 is multiplicatively written (even though the group operations may be very different from the usual addition and multiplication operations). The group order is q in either case. G_1 is a GDH group, whereas G_2 is not. If P and Q are two generators of G_1, then aP for $a \in \mathbb{Z}_q^*$ is defined as

$$aP = \overbrace{P + P + \ldots + P}^{a \text{ times}}$$

A mapping $e : G_1 \times G_1 \to G_2$ is called *bilinear,* if for all $P, Q \in G_1$ and $a, b \in \mathbb{Z}_q^*$

$$e(aP, bQ) = e(P, Q)^{ab}$$

holds. Furthermore, we only consider bilinear maps that are efficiently computable and non-degenerated (meaning that not everything is mapped to the identity, i.e., $P \neq 0 \Rightarrow e(P, P) \neq 1$).

If such a bilinear map $e : G_1 \times G_1 \to G_2$ exists, then one can show that DLP(G_1) $\leq_P$ DLP(G_2), meaning that the DLP in G_1, i.e., DLP(G_1), is not harder to solve than the DLP in G_2, i.e., DLP(G_2): For a given P and a random Q with $Q = aP$, DLP(G_1) is to determine a with $a = \log_P(Q)$ in G_1. In G_2, this translates to $P' = e(P, P)$, $Q' = e(P, Q)$, and hence $a = \log_{P'}(Q')$.

[20] Clifford Cocks was already mentioned in the Introduction. He was one of the GCHQ employees who discovered public key cryptography under the name NSE in the early 1970s.

[21] https://eprint.iacr.org/2004/064.

Similarly, it can be shown that the DDHP can be solved easily in G_1 (as suggested by the fact that G_1 is a GDH group). Solving the DDHP here means being able to distinguish $\langle P, aP, bP, cP\rangle$ with $a, b, c \in_R \mathbb{Z}_q^*$ and $\langle P, aP, bP, abP\rangle$. This can be achieved by determining $e(aP, bP)$ and comparing the result with $e(P, abP)$. If they are the same, then the correct tuple is $\langle P, aP, bP, abP\rangle$, because $e = (aP, bP) = e(P, P)^{ab} = e(P, abP)$.

More interestingly, bilinear maps can be used to extend the Diffie-Hellman key exchange to three parties (as announced in Section 12.5) [33]. The resulting protocol is known as *tripartite Diffie-Hellman key exchange*. If A, B, and C are three parties with secret keys $a, b, c \in \mathbb{Z}_q^*$ and respective public keys aP, bP, and cP (in the usual setting as specified above), then the protocol consists of having all parties share their public key with each other, meaning that A provides B and C with aP, B provides A and C with bP, and C provides A and B with cP. These exchange messages can be sent in parallel. In the end, A computes $e(bP, cP)^a = e(P, P)^{abc}$, B computes $e(aP, cP)^b = e(P, P)^{abc}$, and A computes $e(aP, bP)^c = e(P, P)^{abc}$, meaning that they all agree on a shared key. It goes without saying that the security of this protocol is based on the *bilinear Diffie-Hellman assumption* that basically says that computing $e(P, P)^{abc}$ given P, aP, bP, and cP is hard.

Table 13.6
The Boneh-Franklin IBE system

System parameters: G_1, G_2, P, S

Generate	Encrypt	Decrypt
(Id_A, s)	(m, A)	$(u, v, a),$
$A = h_1(Id_A)$ $a = sA$	$r \xleftarrow{r} \mathbb{Z}_q^*$ $u = rP$ $g_A = e(A, S)$ $v = m \oplus h_2(g_A^r)$	$m = v \oplus h_2(e(a, u))$
(a, A)	(u, v)	(m)

More relevant to the topic of this section, bilinear maps can also be used to implement an IBE system that relies on the bilinear Diffie-Hellman assumption and the random oracle model. The respective Boneh-Franklin system assumes a bilinear map $e : G_1 \times G_1 \rightarrow G_2$ with generator P (as above), and a system-wide public key pair (s, S), where $s \in_R \mathbb{Z}_q^*$ represents a private key and $S = sP$ represents the respective public key. Furthermore, two hash functions $h_1 : \{0, 1\}^* \rightarrow G_1$ and

$h_2 : G_2 \rightarrow \{0,1\}^*$ are required that represent random oracles (or an XOF in the case of h_2).

The Boneh-Franklin IBE system is summarized in Table 13.6. In the $\mathsf{Generate}$ algorithm, the keying material for A is generated (where A refers to the recipient of the encrypted message). It takes as input an identifier for A, i.e., Id_A, and s, and it generates as output the public key pair (a, A) for A. If somebody wants to encrypt a message m for A, he or she grabs A's public key A from a directory service and subjects m to the $\mathsf{Encrypt}$ algorithm. As usual, the algorithm takes as input m and A, and it generates as output a two-part ciphertext that consists of u and v. The algorithm randomly selects r and computes u as rP. To compute the second component, the algorithm computes $g_A = e(A, S)$, subjects g_A^r to h_2, and adds the resulting bitstring modulo 2 to the message m. Hence, v is equally long as m. The pair (u, v) is then transmitted to A, and A uses its private key a to decrypt the ciphertext. The respective $\mathsf{Decrypt}$ algorithm takes (u, v) and a as input, and generates as output m. To do so, it simply computes $m = v \oplus h_2(e(a, u))$. This yields the correct result, because

$$\begin{aligned}
\mathsf{Decrypt}(u, v, a) &= v \oplus h_2(e(a, u)) \\
&= v \oplus h_2(e(sA, rP)) \\
&= v \oplus h_2(e(A, P)^{rs}) \\
&= v \oplus h_2(e(A, sP)^r) \\
&= v \oplus h_2(e(A, S)^r) \\
&= v \oplus h_2(g_A^r) \\
&= m \oplus h_2(g_A^r) \oplus h_2(g_A^r) \\
&= m
\end{aligned}$$

As suggested in [34], the Boneh-Franklin IBE system can be made CCA2-secure. A more comprehensive overview of IBE systems is provided in [35]. Researchers have also tried to combine conventional asymmetric encryption and IBE to overcome some disadvantages of IBE. Examples include *certificateless encryption* [36] and *certificate-based encryption* [37]. The definitions and security notions of certificateless encryption and certificate-based encryption are further addressed in [38]. In particular, there is an equivalence theorem, saying that—from a security perspective—IBE, certificateless encryption, and certificate-based encryption are equivalent, meaning that a secure certificateless or certificate-based encryption system exists if and only if a secure IBE system exists. The bottom line is that IBE (together with certificateless encryption and certificate-based encryption) is a nice idea and research area, but it has not been able to move from theory to practice so far. This is unlikely to change anytime soon.

References

[28] Lopez, J., R. Oppliger, and G. Pernul, “Why have Public Key Infrastructures Failed so Far?” Internet Research, Vol. 15, No. 5, 2005, pp. 544–556.

[29] Shamir, A., “Identity-Based Cryptosystems and Signatures,” Proceedings of CRYPTO ’84, Springer-Verlag, 1984, pp. 47–53.

[30] Boneh, D., and M. Franklin, “Identity-Based Encryption from the Weil Pairing,” Proceedings of CRYPTO 2001, Springer-Verlag, 2001, pp. 213–229.

[31] Boneh, D., and M. Franklin, “Identity Based Encryption from the Weil Pairing,” SIAM Journal of Computing, Vol. 32, No. 3, 2003, pp. 586–615.

[32] C. Cocks, “An Identity Based Encryption Scheme Based on Quadratic Residues,” Proceedings of the 8th IMA International Conference on Cryptography and Coding, 2001, pp. 360–363.

[33] Joux, A, “A One Round Protocol for Tripartite DiffieHellman,” Proceedings of the 4th Interna-tional Symposium on Algorithmic Number Theory (ANTS 2000), LNCS 1838, Springer-Verlag, 2000, pp. 385–394.

[34] Fujisaki, E, and T. Okamoto, “Secure Integration of Asymmetric and Symmetric Encryption Schemes,” Journal of Cryptology, Vol. 26, 2013, pp. 80-101.

[35] Luther, M., Identity-Based Encryption, Artech House Publishers, Norwood, MA, 2008.

[36] Al-Riyami, S.S., and K.G. Paterson, “Certificateless Public Key Cryptography,” Proceedings of ASIACRYPT 2003, Springer-Verlag, 2003, pp. 452–473.

[37] Gentry, C., “Certificate-Based Encryption and the Certificate Revocation Problem,” Proceedings of EUROCRYPT 2003, Springer-Verlag, 2003, pp. 272–293.

[38] Yum, D.H., and P.J. Lee, “Identity-Based Cryptography in Public Key Management,” Proceedings of EuroPKI 2004, Springer-Verlag, 2004, pp. 71–84.