Use Cases of Implicit Authentication and Key Establishment with Sender and Receiver ID Binding

Dan Forsberg
<*dan.forsberg@nokia.com*>
Nokia Research Center

***Abstract*— In this paper we explore identity based Authentication and Key Establishment (AKE) protocols. We explain in high level the public key ID-Based AKE protocols and take a new protocol approach to the ID-Based shared secret world with key hierarchies along with some new and interesting use cases.**

Index Terms— Identity Based Cryptography (IBC), Authentication and Key Establishment (AKE), key hierarchies, key derivation, identity binding

I. INTRODUCTION

Often protocol engineers need to utilize existing security mechanisms and avoid designing new ones that are not widely reviewed and/or proved in order to lower the risks of security vulnerabilities or mismatches in their designs and especially implementations. However, in general this approach may mean that a protocol engineer and/or system/service architect Sofie does not utilize the best suited security mechanisms for her problem and use case. This may be because the architect does not know the available building blocks in her abstraction level or then just can not understand the existing mechanisms because of her background not being in cryptography or applied security. On the other hand in the deep cryptology world, cryptographers like Cecilia are many times interested in different difficult mathematical problems and how they can be used to create hard to break authentication and key establishment protocols for example. There is a middle ground between Sofie and Cecilia, which is the abstraction layer of the different security protocols. An applied security engineer Anna is most interested to find out the different building blocks in conceptual level that she can use, understand, and utilize when designing new service and protocol architectures. In this paper we provide a glimpse into Anna's world by exploring the interesting IBC AKE protocols, but we also take Anna's level of abstraction into the symmetric key cryptography with identity binding and see how it compares with the ID-based public key counterparts.

The rest of the paper is organized as follows. In chapter II we provide background to IBC in general and especially IBC AKE. We explain in high level the basic theorems behind and provide references to sources with proper proofs and deeper overviews. We also give some examples of the existing applications with IBC AKE protocols and identity binding schemes in symmetric key cryptography. Chapter III is dedicated for the introduction of the new simple symmetric key based identity binding AKE along with some new use cases presented in chapter IV. Finally we conclude our paper in chapter V.

II. ID-BASED AUTHENTICATION AND KEY ESTABLISHMENT

Identity (ID) based cryptography (IBC) [1] has become an active research topic in the recent years because of practical ID-Based encryption, signature, and key exchange applications [2, 3, 4]. The IBC system builds on the basic idea that the public key of the user is based on some unique information about the user's identity, like for example an email address (string). In addition to using the identity as the public key the IBC system public parameters are needed (see Figure 1).

IBC is controversial compared to the traditional certificate based systems, where a designated Certificate Authority (CA) signs (and creates) a user specific certificate, containing the user's identity and her public key. In a simple setup all the certificates are signed by a trusted CA. Every involved party has the CA's certificate for verifying the CA's signatures. When Bob wants to authenticate Alice or send encrypted information for her, he must first get her certificate and verify its validity (signed by the right CA and not been revoked). Then Bob can use Alice's public key from the certificate to encrypt information for the target. In an IBC system users do not have to get or store the public keys of the corresponding communicating parties, because they can be created based on the target's identity and the common parameters of the IBC system. However, the communicating parties must ensure that they are using the same public parameters, which can be considered as a weakness in the IBC scheme.

Self-certified keys and signature scheme is an alternative for traditional certificate based systems, because the sender's public key is extracted from the trusted third party's (e.g. a CA) signature for the senders identity. B. Brumley [2] presents an application of self-certified and identity based certificates with efficient three-term simultaneous elliptic scalar

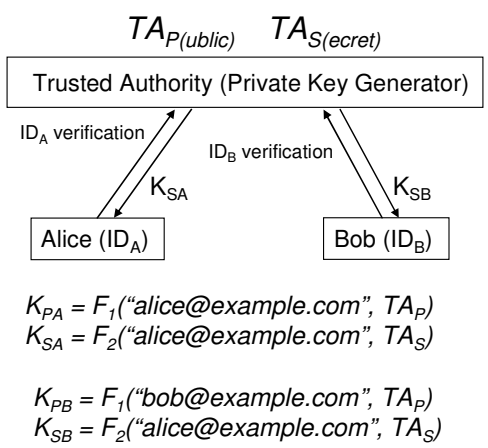

Figure 1 Private Key Generator as Trusted Authority in IBC

multiplication, where the signature scheme is based on Nyberg-Rueppel signatures by a trusted third party [3].

A. Authentication and Key Establishment

For secure communication between users, authentication and key establishment is required. Successful authentication verifies user's claimed identity for the other party. Usually the authentication must happen in both directions (mutual authentication). After authentication the entities need to agree on a shared key that is used to protect the communication further on. Diffie-Hellman protocol [7] can be seen as the first key establishment protocol based on public key cryptography. However, the protocol does not provide authentication of the communicating parties, meaning that a man-in-the-middle attack is possible (an adversary between the communicating parties modifying the messages can establish separate keys with each end point). Thus, it is essential to bind authentication and key establishment together. Protocols achieving this are called authenticated key establishment (AK) [8].

In general Dutta et al. [8] provide a nice overview of different key establishment protocols. In their paper they divide key establishment protocols into two categories, namely certificate based and ID based. Further on they divide the protocols in two-party, three-party, group, and tree based group key establishment protocols. Two-party key establishment protocols include ID based key establishment protocols based on pairings. Chen et al. [9] provide a very comprehensive comparison and overview of ID-Based key establishment protocols based on pairings. They also evaluate the efficiency of the different protocols. Pairing based IBC protocols are utilizing supersingular elliptic curve cryptography with the assumption that Bilinear Diffie-Hellman (BDH) problem is considered hard (e.g. given P, aP, bP, cP computing $\hat{e}(P,P)^{abc}$ is hard). Dutta et al. have also a survey paper on pairing based cryptographic protocols [10]. For more information about IBC systems, readers should refer to "A survey on ID-Based Cryptographic Primitives" from Gorantla et al. [11].

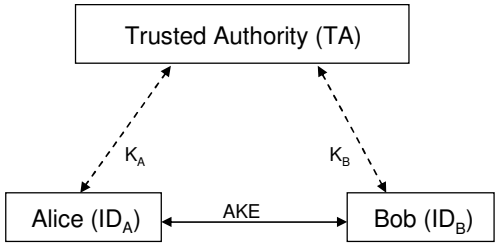

Figure 2: Trusted Authority

B. IBC Public Key Generator as Trusted Authority

In IBC with public key cryptography a private key generator (PKG) or sometimes called key generation center (KGC) is trusted by all users and is responsible for the generation of the user's corresponding private keys (e.g. a Trusted Authority). Each user then gets its private key from the PKG, but also the common parameters used to create the public keys based on the receiver's identity.

In the first ID-Based authentication and key establishment protocols key escrow is possible by the PKG, meaning that the PKG can deduce the key used to secure the communication by simply wiretapping the conversation (PKG knows how to create the corresponding secret keys based on the used identities). However, Chen and Kudla [12] developed a protocol in which the key escrow feature can be turned off. They also provided an extension to their protocol, which allows users under different PKGs to agree a key together. Later more efficient schemes were proposed [13], but with some security considerations [14].

Gentry and Silverberg introduced a Hierarchical ID-Based Encryption (HIBE) scheme [15], which is a generalization of ID-Based encryption that reflects organizational hierarchies. This lessens the burden from a single PKG to multiple PKGs. An identity at level k of the hierarchy tree can issue private keys to its descendant identities, but cannot decrypt messages intended for other identities. Boneh et al. [16] describe an improved HIBE scheme, which consumes fewer bits than the Gentry and Silverberg one. Boneh et al. also describe a mechanism on how to provide forward security for the ID-Based cryptosystem.

Balfanz et al. describe secret handshakes from Pairing-Based Key establishments [17]. Their aim is to provide an analogical secret society (for example CIA) identification handshake with the AKE protocol. They describe how IBC with pairing can be used to establish secure sessions between two entities based on the IBC TA parameters and the peer's pseudonym or even the peer's claimed role. Instead of publicly meaningful identities, they use pseudonyms for the users as well. By using pseudonyms instead of public identities they loose the best feature within IBC, namely the binding of the real identity with the public key. To overcome this they take the example of a driving license document, where the pseudonym is printed along with user's identity. Let's consider the secret society member identification scheme they propose.

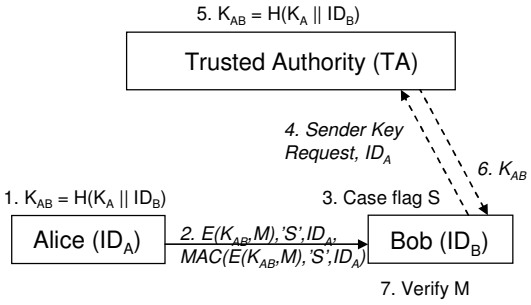

Figure 3: Receiver ID-Based AKE

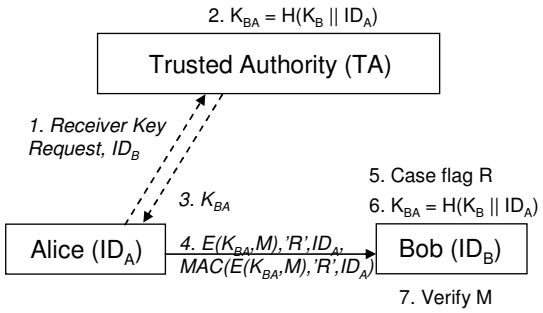

Figure 4: Sender ID-Based AKE

If an attacker in their setup compromises one member, let's say a CIA agent, who has a pseudonym with corresponding secret key and IBC TA parameters, she is able to test if other peers are part of the secret society or not. The only problem the attacker has is that scheme may also utilize roles in the AKE protocol. Thus, the attacker may not know all the possible roles. However, there are not so many roles in the system in general, that they could be considered secret. Also, if the handshake fails because the peers used different roles for each other, some information may be leaked.

Burnett et al. describe in their paper how biometric identity information can be used with ID-Based signature scheme [18]. They address the problems of fuzziness with biometric identity measurement as well. HP Laboratories have done research in the area of IBC based applications, for example within the area of role based secure message service, privacy, and identity management for the health care systems etc. [19, 20].

C. *Implicit AKE with Key Derivation*

IBC is using asymmetric key cryptography based on elliptic curves and pairings. However, identities can be bound to the symmetric keys within the key establishment protocol with key derivation functions (KDFs). In simple key derivation, a root key and an identity are used as input parameters for a one-way hash function, which then produces the new key, one level lower in the key hierarchy. Binding the identity into the key is also called *channel binding* [21]. KDF is usually a one-way hash function, which ensures that by holding a key lower in the hierarchy, an attacker can not deduce a higher level key in the hierarchy.

Usually both communicating end points derive keys similarly based on some input parameters, like used algorithm, identity, nonce, etc., but it is also possible to provide keying material to different parties from different key hierarchy levels. In effect, similar usage models can be designed compared to the public key cryptography with these kinds of constructs. Additionally, as the identity is bound to the key derivation, the mechanism provides a nice way to authenticate the identity.

Shih-I-Huang [22] presents a simple key derivation based on node identities to reduce the number of keys needed for a keying scheme for sensor networks [23]. The basic idea there is that a one-way hash function dependency between two keys of two sensors. The other sensor knows how to create a key for the other based on the target nodes number in the PIKE scheme.

Kerberos [24] is not using key derivation, but is in effect closely related to channel binding mechanisms with symmetric keys. Kerberos uses tickets, which include an encrypted session key for the authenticator. The user gets the ticket along with a session key. She provides the ticket to a server, which is able to decrypt the ticket and to get the same session key as what the user has. This way Kerberos can be seen as a key distribution protocol without explicit key derivation. However, nothing prevents improving Kerberos system in such a way that the session key is based on some KFD function that binds the keys to the right context (like users' identity).

III. ID Binding with Symmetric Keys as an Implicit AKE

Here we present this idea and generalize it into an AKE protocol with possibilities to use either sender's or receiver's symmetric key as basis for the key establishment. Although, the scheme is very simple from a cryptographic function point of view and is a special case of channel binding, we want to show that key derivations can be used to achieve similar constructs as with IBC and Kerberos with less complexity.

The model requires a common trusted authority (TA, see Figure 2) and that each node in the system must have a unique identity. Each communicating party must be able to mutually authenticate with the TA and agree a long enough symmetric key. Further on, the aim is that two nodes with a common TA can mutually authenticate and send integrity protected and/or ciphered packets to each other. To achieve this, we utilize key derivation with identity binding based on sender's key and receiver's key, a special case of channel binding.

A. *Receiver ID based AKE*

In a Receiver ID (RID) based AKE scheme, Alice takes her own shared key K_A with the TA and derives a new key K_{AB} for Bob. Using a one-way hash function *H* and the key and Bob's identity ID_B as input parameters (|| denotes concatenation and *H* produces the same number of bits as the key length for simplicity) Alice gets a proper key for Bob, K_{AB}.

$$K_{AB} = H(K_A \| ID_B) \qquad (1)$$

Using the resulting key Alice sends an integrity protected and encrypted message over an insecure channel for Bob along

with her own identity and a flag (R) in the message that indicates the usage of RID based AKE. Once Bob gets a message from Alice, he sends *Sender Key Request* along with Alice's ID for the TA through a secure authenticated channel between Bob and the TA. After TA has authenticated the request, it checks if Alice has registered and finds out that she is. Since TA knows the shared secret with Alice it can derive the same key K_{AB} for Bob. TA sends the key through the secure channel for Bob. Bob authenticates the received message and gets the key, which it uses to authenticate the message from Alice, provided that Alice's shared key with the TA has not been compromised (see Figure 2).

B. Sender ID based AKE

In the Sender ID (SID) based AKE scheme, Alice asks the TA to derive herself a session key between herself and Bob. Alice sends a *Receiver Key Request* message through a secure channel for TA along with Bob's ID. TA authenticates the request and finds out if Bob has registered. If Bob has registered to the system, TA derives receiver key K_{BA} for Alice and sends it to her via the secure authenticated channel.

$$K_{BA} = H(K_B \,||\, ID_A) \qquad (2)$$

Alice then sends integrity protected and encrypted message for Bob over an insecure channel along with her own ID and a flag (S) in the message noting that the RID based AKE is used. When Bob gets the message he takes Alice's ID and his own share key with TA KB and derives K_{BA} as in *(2)*.

C. Combined Sender and Receiver ID-Based AKE

To make the key derivation more secure we can use both sender and RIDs in the key derivation function (see Figure 5).

$$K_C = K_{BA} \; xor \; K_{AB} \qquad (3)$$

However, with this kind of scheme both Bob and Alice need to contact the TA to derive the combined key because they are not able to derive the other key based on their own keys.

D. One time PIN

In case the service provider wants to utilize one-time-passwords, and thus force the user to get a new PIN code for every new session, the TA can issue KBA for the user based on the following formula.

$$K_{BAi} = H(H(K_B \,||\, i) \,||\, ID_A) \qquad (4)$$

where i is long enough serial number starting from pre-defined value k. Both the service provider and the TA agree on the value k, at the same time they agree on the shared key. However, service provider needs then to keep counter values for each authenticated user in their profiles, which makes this scheme less interesting.

IV. Use Cases

A. User Authentication for Internet based Services with Operator Short Message Service

Let's assume that a telecom operator Opera has a TA server reachable through or integrated into the SMS (Short Message Service) gateway. Alice and Bob are both registered users of the Opera and thus have valid and unique telephone numbers. A service provider, Simon, wants to create a service into the Internet, which requires real user identity authentication from the clients. Simon's server is a simple PC connected to the Internet with a fixed line connection and with no cellular interface. However, Simon has no resources or possibilities to start creating user accounts by authenticating the client's identities face-to-face. Thus, Simon's only possibility is to leverage some existing user database and authentication service. Virtual operator Opera contacts Simon and offers a simple win-win deal as follows. Opera provides a secret key K_S for Simon and asks Simon to install it into his PC, but also to keep it secret. Then Opera explains Simon that he can start his service and accept users with their phone number as their user name and a PIN code based on the RID based AKE. Operator Opera also explains that if the key K_S is compromised, Simon can always ask a new key from the operator, and that in fact the lifetime of the key K_S is one month, after which a new key must be installed for the service.

Alice finds out about Simon's service on the Internet and decides to try it out. She browses to the URL of Simon's service and finds out that it requires user authentication based on their mobile subscription phone number. Alice then sends an SMS to the Opera's TA along with Simon's service ID (ID_S). The TA then interprets this as a *Receiver Key Request* message, checks the incoming phone number, finds out Simon's service key K_S and derives PIN code for Alice and sends it to Alice as an SMS message. Alice then types her phone number as the user name and the received PIN code as the password on the Simon's service login web page over secure connection (e.g. TLS with server certificate).

Simon's server receives a login request with Alice's phone number. Using the service key K_S, the server then derives a new key K_{SA} based on (2) and compares the result with the PIN code (using as many digits from the K_{SA} as necessary) and

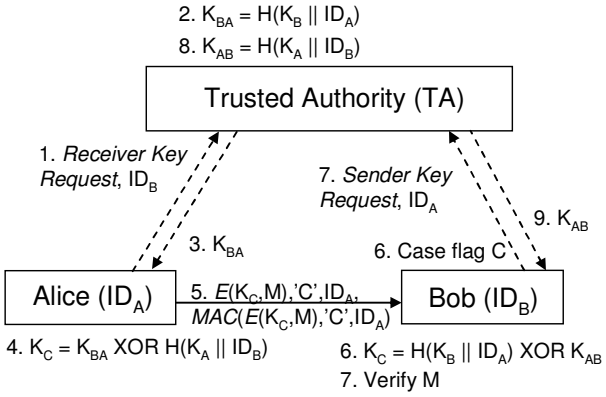

Figure 5 Combined Sender and Receiver ID Based AKE

finds out that they match. The server also checks from the user database if the user with this phone number has logged into the service before in case some user specific customization parameters would have been configured. Not at this time. Thus, Alice's login is an authenticated registration to the service. The server then stores the phone number into the user database along with any service customization parameters Alice has selected.

After a couple of days Alice tries to log in again, but notices that she has forgotten the PIN code for the service. She then sends a new SMS message with the service provider's ID to the TA. After a month has passed, Alice logs in again as usual with the same phone number and PIN code she has in her SMS messages inbox. However, the service informs Alice to get a new PIN code with the SMS message because the previous PIN code has become too old.

For another Internet service, Simon's wants to use the same authentication method, but wants to restrict the users to a certain country only in the beginning. Thus, he makes a deal with the operator Opera that only users living in the specific country area are allowed to get PIN codes for the service. Opera then filters out PIN code requests from users that are not registered into the specific country.

Alice notices that there are a huge number of services utilizing the SMS based authentication service. Thus, Alice is able to get a PIN code for the services with an SMS message indicating all the service IDs of the services Alice wants to use.

B. Authenticated push messages

Push style service providers advertise their personalized secure services, register to the SMS gateway and get their own shared secrets. Users willing to receive secure and personalized offers from the service providers, register to the SMS gateway and get their shard secrets. Users also register their preferences to the push services directory. SMS gateway provides a list of identities/phone numbers that the service provider is allowed to use along with the derived shared secrets. Service provider creates a user tailored special offer push message secured with corresponding target user's shared secret. The user gets the push message from the service provider and is able to authenticate the message by using her own shared secret and the service provider's identity and thus verify that the offer is valid (e.g. user can verify the source of the offer as well be sure that it was targeted to her only). User can use the session key further on when authenticating to the service and buying the product that the personalized push advertisement was offering for the user.

C. PSK-TLS with Sender and Receiver ID-Based AKE

Pre-shared key TLS [24] describes shared key cipher suites for TLS protocol [26]. TLS is an AKE protocol used in many applications and services, like for example in secure HTTP. However, PSK TLS does not support either Sender or Receiver ID based key derivation schemes. Adding support for this in PSK TLS would allow setups in which for example a centralized Operations & Management (O&M) server would contain a master secret and all clients for the O&M system would be using Sender ID based AKE, with pre-configured K_{BA} (e.g. steps 1, 2, and 3 skipped in Figure 4). This would allow the administrators to add clients to the O&M system, without the need to add/change configurations in the O&M server.

D. Adaptation for Internet Packet Level Authentication with Domain Name System

Candolin, Lundberg, and Kari present [27] present a packet level authentication scheme for military networks based on public keys. However, public key cryptography is considered to be computationally heavier than symmetric key cryptography. Thus, hardware support is probably required for Internet core routers. Here we sketch some ideas based on symmetric key packet level authentication with DNS as the TA.

Internet Domain Name System (DNS) security enhancement work [28] has been ongoing for some years already. If the DNS can be considered secure enough to act as a TA in the Internet, it could be used as a TA for the Sender and Receiver ID based AKE as well. Here we assume that the servers in the DNS system communicate securely with each other utilizing either symmetric key or public key mechanisms. We also assume that the link between the client and its serving DNS server is secured (e.g. based on network access authentication like WPA for WLANs or physically secure enough links like xDSL).

Consider a firewall in the Internet in a domain *example.com* with a shared key K_B with the DNS master server for that domain. Now, we can construct a system where the firewall wants to authenticate IP packets for hosts inside example.com (behind the firewall) domain, we can apply Sender ID based AKE with DNS as the TA for all incoming IP packets.

If the master DNS configures the Time To Live (TTL) value for all hosts below example.com domain as 0, it means that all DNS queries end up for the example.com master DNS server, which can then provide K_{BA} for each client A. Here, the master DNS server must know what the SID is. As is, the DNS system does not carry this information. Thus, an extension is needed for doing this.

Each client supporting packet level authentication in the form of RID based AKE, must include their SID (IP address) into the DNS queries in a backwards compatible way. One way to achieve this is to include the SID as an additional prefix for the DNS name being queried. For example:

IPaddr-X-Y-Z-V.www.example.com

Where the sender's IP address is X.Y.Z.V. Now, the master DNS server for domain example.com may or may not support this extension. If it supports it returns the IP address of www.example.com along with the K_{BA} key for the sender. To transfer the key, the DNS response must contain some records that can hold the key for the sender. Note that the response does not have to contain the SID if the request and response messages can be mapped together. Mapping the key to the SID

is not possible without also knowing the corresponding DNS request message.

Using symmetric key crypto in the firewall is fast enough for doing per packet authentication based on an IPSec authentication header on the per packet basis. When the firewall gets an incoming packet with an authentication header, it takes the source address, its own key and derives the shared secret K_{BA} with (2) and uses it to verify the packet. If needed, the key can be stored into the firewall's memory structure, which processes the packet stream associated with the sender and receiver addresses. This makes it unnecessary to derive the again and again for each incoming packet. However, the key derivation procedure can be considered fast (one-way hash function) and thus storing the key into memory may not be the best way to utilize the computing and memory resources.

The KDF can be extended to include also the receiver's ID explicitly in case the receiver has multiple IDs. In out example the domain example.com could include *www.example.com*, *blogs.example.com*, and *lists.example.com*, all with different IP addresses. The DNS response would then contain a key K_{BA} that is already bound to the IP address in question, and the client would use it as, but only with the same destination IP address. Thus, the client functionality would not change compared to the earlier case. However, the firewall functionality has to be changed. The firewall must first compute the destination IP address bounded key before it can compute the shared key used with the packet. Thus, the firewall computes the key:

$$K_{BA} = H(H(K_B \,||\, ID_D) \,||\, ID_A) \qquad (5)$$

ID_D is the destination IP address of the corresponding server in the *example.com* domain.

To make the system more efficient it is not necessary to provide integrity checksum for the whole packet as is the case with IPSec authentication header, but only certain number of bytes from the beginning of the packet need to be protected to cover for example the IP header only or any additional headers and data if needed.

We leave the security analysis of this system for further study. However, we believe that this kind of system could potentially be good enough for preventing IP source address spoofing and naturally suit with the secure DNS system. The scheme should be studied further and details clarified, though.

V. Conclusion

Sender and receiver ID based AKE with symmetric keys has many overlapping applications with public key ID-Based AKE. Both of them are useful, with slightly different setups as is also the case when comparing symmetric key and public key cryptography together. We believe that the term ID-Based Cryptography AKE used only with public key cryptography may be a slightly confusing term as identity based AKE can also be done with symmetric keys. However, binding identities to AKE with symmetric keys is more suitable to client-server type of approaches, where the master secret or root key can be stored in a secure place and derived keys can be given to clients.

We created a simple AKE protocol model that binds sender and/or receiver identities to the key establishment and thus provides implicit authentication of the identities based on the trusted third party. We provided several new and interesting use cases, especially for telecom operators, who can utilize the SMS as a good enough confidential channel for communications with the trusted third party (operator).

We also sketched a scheme for end-to-end or end-to-middle IP packet level authentication with the sender and receiver ID based AKE where the DNS system acts as the trusted third party.

Acknowledgment

We would like to thank prof. Nadarajah Asokan, prof. Kaisa Nyberg, Maarit Hietalahti, and Vesa Vaskelainen for valuable comments on this paper.

References

[1] [SHAMIR-76] Ad Shamir, "Identity-based Cryptosystems and Signature Schemes", In proceedings of Crypto 1984, LNCS 196, pp. 47-53, Springer-Verlag, 1984

[2] [BB] B. Brumley, "Efficient Three-Term Simultaneous Elliptic Scalar Multiplication with Applications ", Proceedings of Norsec 2006

[3] [NR] Giuseppe Ateniese and Breno de Medeiros, "A provably secure Nyberg-Rueppel signature variant with applications", Technical Report 93, Cryptology ePrintArchive, 2004.

[4] [BF-4] D. Boneh, M. Franklin, "Identity-based encryption from the Weil pairing", SIAM Journal of Computing, 32(3):568-615, 2003

[5] [BLS-5] D. Boneh, B. Lynn, H. Shacham, "Shor signatures from the Weil pairing", In Advances in Cryptology – Asiacrypt'2001, volume 2248 of Lecture notes in Computer Science, pages 514-532, Springer-Verlag, 2002

[6] [DH-12] A.Joux, "A one-round protocol for tripartite Diffie-Hellman", In Algorithm Number Theory Symposium –ANTS IV, volume 1838 of Lecture Notes in Computer Science, pages 385-394. Springer-Verlag, 2000.

[7] [DIFFIE] W. Diffie, M. Hellman, "New Directions in Cryptography", In IEEE Transactions on Information Theory, IT-22 (6), pp. 644-654, 1976

[8] [DUTTA] Ratna Dutta, Rana Barua, "Overview of Key establishment Protocols", 2005, Cryptology ePrint Archive: Report 2005/289, URL: http://eprint.iacr.org/2005/289.ps (referenced 2006-10-15)

[9] [CHEN] L.Chen, Z.Cheng, N.P. Smart, "Identity-based Key Agreement Protocols from Pairings", Cryptology ePrint Archive: Report 2006/199, URL: http://eprint.iacr.org/2006/199 (referenced 2006-10-15)

[10] [DUTTA2] Ratna Dutta and Rana Barua and Palash Sarkar, "Pairing-Based Cryptographic Protocols: A Survey", Cryptology ePrint Archive: Report 2004/064, URL: http://eprint.iacr.org/2004/064 (referenced 2006-10-15)

[11] [GORANTLA] M. Choudary Gorantla and Raju Gangishetti and Ashutosh Saxena, "A Survey on ID-Based Cryptographic Primitives", Cryptology ePrint Archive: Report 2005/094, URL: http://eprint.iacr.org/2005/094 (referenced 2006-10-15)

[12] [CHENKUDLA-32] L. Chen, C. Kudla, "Identity Based Authentication Key Agreement Protocols from Pairings", Cryptology ePrint Archive: Report 2002/184, URL: http://eprint.iacr.org/2002/184 (referenced 2006-10-15)

[13] [CULLAGH-63] N. McCullagh, P.S.L.M. Barreto, "A New Two-Party identity-Based Authenticated Key Agreement", In proceedings of CT-RSA 2005, LNCS 3376, pp. 262-274, Springer-Verlag, 2005.

[14] [CHOO-34] Kim-Kwang Raymond Choo, "Revisit Of McCullagh--Barreto Two-Party ID-Based Authenticated Key Agreement Protocols",

Cryptology ePrint Archive: Report 2004/343, URL: http://eprint.iacr.org/2004/343 (referenced: 2006-10-15)

[15] [HIBE] Craig Gentry and Alice Silverberg, "Hierarchical ID-Based Cryptography", Cryptology ePrint Archive: Report 2002/056, URL: http://eprint.iacr.org/2002/056 (referenced 2006-10-15)

[16] [HIBE2] D. Boneh, E.-J. Goh, and X. Boyen, "Hierarchical Identity Based Encryption with Constant Size Ciphertext", Cryptology ePrint Archive: Report 2002/015, URL: http://eprint.iacr.org/2005/015.pdf (referenced 2006-10-15)

[17] [BDS] Balfanz, D., Durfee, G., Shankar, N., Smetters, D., Staddon, J., and Wong, H. 2003. Secret Handshakes from Pairing-Based Key Agreements. In Proceedings of the 2003 IEEE Symposium on Security and Privacy (May 11 - 14, 2003). SP. IEEE Computer Society, Washington, DC, 180.

[18] [BDD] A. Burnett, A. Duffy, T. Dowling, “A Biometric Identity Based Signature Scheme”, Cryptology ePrint Archive: Report 2004/176, URL: http://eprint.iacr.org/2004/176 (referenced 2006-10-15)

[19] [CB] M. Casassa Mont, P. Bramhall, "IBE Applied to Privacy and Identity Management," Hewlett-Packard Laboratories, technical report HPL-2003-101, 2003

[20] [CBDH] M. Casassa Mont, P. Bramhall, C. R. Dalton, K. Harrison, "A Flexible Role-based Secure Messaging Service: Exploiting IBE Technology in a Health Care Trial," Hewlett-Packard Laboratories, technical report HPL-2003-21, 2003.

[21] [CHANNEL-BINDING] B. Aboba, D. Simon, J. Arkko, P. Eronen, and H. Levkowetz, "Extensible Authentication Protocol (EAP) Key Management Framework", draft-ietf-eap-keying-14.txt, Internet draft (work in progress), 2006-06-27.

[22] [SIHUANG] S.I. Huang. “Adaptive random key distribution schemes for wireless sensor networks”, In Proceedings of the International Workshop on Advanced Developments in Software and Systems Security, 2003.

[23] [PIKE] A Haowen, Chan Perrig. “Pike: Peer intermediaries for key establishment in sensor networks”, In INFOCOM 2005. 24th Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings IEEE , vol.1, no.pp. 524- 535 vol. 1, 13-17 March, 2005.

[24] [KERBEROS] J. Steiner, C. Neuman, and J.I Schiller, "Kerberos: An Authentication Service for Open Network Systems, " in Proc. Winter USENIX Conference, Dallas (1988).

[25] [PSK-TLS] P. Eronen, H. Tschofenig, “Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)”, IETF RFC4279, December 2005.

[26] [TLS] Dierks, T. and C. Allen, "The TLS Protocol Version 1.0", IETF RFC2246, January 1999.

[27] C Candolin, J Lundberg, and H Kari. “Packet level authentication in military networks”. In Proceedings of the 6th Australian Information Warfare & IT Security Conference, Geelong, Australia, November 2005.

[28] [IETF-DNS-SEC] IETF DNS Extensions (dnsext) Working Group, URL: http://www.ietf.org/html.charters/dnsext-charter.html (referenced 2006-10-15)