PROF. DR. THOMAS BETH
UNIVERSITY OF KARLSRUHE
FACULTY FOR INFORMATICS
GERMANY

SECURITY SYSTEMS BASED ON EXPONENTIATION PRIMITIVES, TESS *B3*

Security Systems based on Exponentiation Primitives

TESS – The Exponential Security System

Thomas Beth

Universität Karlsruhe
Europäisches Institut für
Systemsicherheit
Am Fasanengarten 5
76128 Karlsruhe
Germany

Dieter Gollmann

Royal Holloway and Bedford New
College (RHBNC)

Egham, Egham Hill
Surrey TW 20 OEX
UK

Abstract

After the announcement of a U.S. digital signature standard by NIST, the role of the Exponential One Way Function - which had been used in the initial illustration of public key cryptography - has again received proper recognition as being another security primitive in addition to the RSA-scheme.

In this paper we present the exponential security system TESS developed at the European Institute for System Security (E.I.S.S.) embedded in a package of freeware. The system has meanwhile been applied to some TCP/IP based services such as `telnet`, `rsh` and `rcp` supplementing these services with additional security features. TESS is based on the use of the one way function *exp* that had originally been described by Pohlig and Hellman and is the central feature in the well-known Diffie-Hellman key exchange protocol. The subsequent contributions by El-Gamal have indicated the multifeature capabilities of this proper one way function. Based on these results, the invention of the Beth-Schnorr-Zero-Knowledge Protocols in extension of the Chaum-Evertse-van de Graaf-Zero Knowledge Scheme has made authentication and signature procedures available, which support the view that the exponential one way function is a security primitive suited for supporting practically all mechanisms needed for the design of secure systems.

The implementation of the authenticated key exchange protocol KATHY within the Network Security System SELANE developed at E.I.S.S., Karlsruhe, based on the Günther-Bauspieß-Knobloch scheme forms an integral part of TESS, providing a universal security toolbox for access control, authentication, key exchange, confidentiality protection, digital signatures and verifiable distributed network security management. Its suitability for the incorporation in the X.509 Directory Authentication Framework as well as its free availability make it an interesting system to extend the features of KERBEROS or DSSA towards a proposed Open System Security Architecture.

A further mechanisms composed from TESS primitives is the Electronic Exponential Signature (EES) scheme. It had been developed for EDI purposes and banking applications already in 1989, when after an in-depth study of up-to-date signature procedures, prior to the new U.S. standard, the superiority of the exponential scheme became apparent.

1. The Exponentiation Primitive

Exponentiation is the basis of the Diffie-Hellman key exchange scheme [DiHe76], the first example of a public key cryptosystem. In the original presentation, exponentiation was performed modulo a prime number p, i.e.

$$x \to g^x \bmod p$$

was the main security primitive. It takes a nonzero element $g \in \mathbb{Z}_p$ to the power $x \in \{1, \ldots, p-1\}$, where $\mathbb{Z}_p$ denotes the field of integers modulo a prime p. This mapping had been suggested as a one way function by Pohlig and Hellman [PoHe78]. The cryptographic property that a one way function serves as a 'logical' diode for information flow will be indicated by the notation

$$x \rightarrow\!\!\!\!\vdash g^x.$$

Exponentiation modulo p is, however, only an instance of a more general primitive $x \to g^x$, which maps a bit string x, interpreted as a binary number x, to the x^{th} power of an element $g \in G$, where G is a finite multiplicative group.

Above, we have used the multiplicative group $\mathbb{Z}_p^*$ of the finite field $GF(p) = \mathbb{Z}_p$. Alternatives are the multiplicative group $GF(q)^*$ of a finite field $GF(q) = GF(p^n)$, and also many other finite groups such as $GEC(q)$, the group of rational points on an elliptic curve over $GF(q)$ (see Beth and Schaefer [BeSc91]). It is desirable to find groups where exponentiation can be implemented efficiently while achieving a high degree of security at the same time. A comparison of these options has been given by Beth, Agnew and Vanstone [BeAV90].

1.1 Security

The security of the exponentiation function over Z_p lies in the hardness of the discrete logarithm problem

$$\mathrm{Dlog}_{GF(p)} \equiv \{x : y = g^x \bmod p \mid p, g, y\},$$

i.e. of computing x when $y = g^x \bmod p$, g, and p are given. To the best of today's knowledge, the complexity κ of this problem seems to be of the size

$$\kappa(\mathrm{Dlog}_{GF(p)}) = e^{c\sqrt[3]{\log p (\log\log p)^2}}$$

making it at least as hard as factoring an RSA-number of the same size. The current estimate of the security the discrete logarithm problem in $GF(p^n)$ is governed by a similar result [Odly84]. Resent results have shown that there exist subexponential algorithms for computing the discrete logarithm in an arbitrary finite field $GF(p^n)$. Due to Adleman and DeMarrais the complexity of these algorithms is bounded by

$$\kappa(\mathrm{Dlog}_{GF(p^n)}) = e^{c\sqrt{\log(p^n)\log\log(p^n)}}$$

for some suitable constant $c > 0$ [AdMa93].

Exponentiation over $GEC(q)$ is expected to provide even better security. For some types of elliptic curves the fastest known approach to figure out discrete logarithms is the well known giant step – baby step algorithm that leads to a complexity

$$\kappa(\mathrm{Dlog}_{DEC}) = \sqrt{|GEC(q)|}$$

so $|GEC(q)|$ should be in the order of magnitude of 2^{160}, an order of magnitude that fits to smart card applications when suitable hardware, that supports the arithmetic needed, is available. Details and algorithms for exponentiation on elliptic curves – including hardware layout – can be found in [Scha93].

1.2 Implementation

The computation $x \rightarrow g^x \bmod p$ can be decomposed according to the law

$$g^{x+1} = g^x \cdot g \quad \text{in } G$$

and can be performed in $O(\log p)$ multiplication steps by the well-known Square-and-Multiply-Algorithm. The implementation of this algorithm for sufficiently large p is possible with high efficiency on the CPU of any modern workstation. Implementations for high-speed throughput are discussed by Beth and Gollmann [BeGo89]. The homomorphism property

$$g^{\lambda x+\mu y} = (g^x)^\lambda \cdot (g^y)^\mu$$

and the commutativity

$$(g^x)^y = (g^y)^x$$

are the basic properties for the proof of the correctness of the protocols of Section 2. The essential feature of the exponential scheme is that its cryptographic security combined with the algebraic homomorphism properties allows for the verification of features hidden by the one way function. It should be noted that by this the trapdoor feature $N = pq$ of the RSA function

$$x \rightarrow x^e \bmod N$$

is circumvented giving an essential security gain in many applications.

1.3 Alternative Exponential Primitives

The exponential primitive has the advantage of being applicable in groups, in which the Dlog-problem is hard. By employing seemingly complicated groups it is possible to design schemes which

- require very little memory in identification tokens such as smart cards, and
- allow for high-speed implementation of the exp-function.

Furthermore the choice of the General-Exp function (see below) gives even more possibilities for one way functions with special features such as the Trace-Exp function which has been designed to overcome the well known homomorphism attacks e.g. against RSA signatures. A short list of options is given by the following table.

Oneway function	System
$x \rightarrowtail\!\!\!\!\!\!\vdash\; x^e \bmod N$	RSA with trapdoor
$x \rightarrowtail\!\!\!\!\!\!\vdash\; g^x \bmod p$	proper EXP
$x \rightarrowtail\!\!\!\!\!\!\vdash\; x^x \bmod p$	Trace EXP
$x \rightarrowtail\!\!\!\!\!\!\vdash\; G(x)^{E(x)}$	General EXP

2. Examples for EXP-based Protocols

The fundamental primitive 'exponentiation' has been used ever since the invention of the public key concept [DiHe76]. In the following, we discuss two-party protocols where the secret of participant A is denoted by $SK(A)$ whereas the corresponding public value generated by the one way function is denoted by $PK(A)$. We now focus on four examples for the use of exponentiation in cryptographic protocol design. The examples cover a wide range of needs in achieving system security: Key exchange, encryption, signatures, and zero knowledge proof techniques.

2.1 Commutative Key Exchange Protocol of Diffie and Hellman

Figure 1 shows the well known Diffie-Hellman key exchange mechanism using the discrete exponentiation as its particular commutative one way function [DiHe76].

	Alice	Channel	Bob
	choose $SK(A) \in \mathbb{Z}_{p-1}$ $SK(A) \multimap PK(A)$ $PK(A)$	$\Longrightarrow$	Parameter g, p and $PK(A)$
	Parameter $PK(B)$	$\Longleftarrow$	choose $SK(B) \in \mathbb{Z}_{p-1}$ $SK(B) \multimap PK(B)$ $PK(B)$
	$KEY := PK(B)^{SK(A)} \bmod p$		$KEY := PK(A)^{SK(B)} \bmod p$

Figure 1: Diffie-Hellman Key Exchange

2.2 Signature and Encryption Protocol of ElGamal

In 1985 ElGamal presented a cryptosystem which – like RSA – allows both message signing and encryption [ElGa85]. In contrary to RSA, it is not based on the difficulty of factoring large integers but on the discrete logarithm assumption. Figures 2 and 3 show the basic protocols for message signing and encryption via exponentiation. It should be noted that the security of these schemes also depends on the mode of generating the random values r.

	Alice	Channel	Bob
K	choose $SK(A) \in \mathbb{Z}_{p-1}$ $SK(A) \multimap PK(A)$ $PK(A)$	$\Longrightarrow$	Parameter g, p and $PK(A)$
S	Message $m \in \mathbb{Z}_{p-1}$ choose $r \in \mathbb{Z}_{p-1}^{*} \setminus \{1\}$ $r \multimap z$ Solve $m = hr + SK(A) \cdot z \bmod p-1$ for h (m, z, h)	$\Longrightarrow$	Verification of $g^m = z^h \cdot PK(A)^z \bmod p$

Figure 2: ElGamal Signature with key generation (K) and signature (S)

	Alice	Channel	Bob
			$b \dashv\triangleright\!\!\!\vdash B$
	B	$\Longleftarrow$	B
	Message $m \in \mathbb{Z}_{p-1}$ choose $r \in \mathbb{Z}^*_{p-1} r$ $r \dashv\triangleright\!\!\!\vdash R$ Encryption: $C := m + B^r \bmod p$ (C, R)	$\Longrightarrow$	Decryption: $m := C - R^b \bmod p$

Figure 3: Symmetric Encryption protocol of ElGamal

2.3 Zero-Knowledge Authentication and Identification

The authentication protocols of Beth [Beth88] and Schnorr [Schn89] are based on the fact that it is possible to prove the knowledge of a special discrete logarithm without revealing its concrete value. A special passport authority (SKIA) sends to the prover one or more ID related secrets while signatures of the passport authority are known to the verifier. The main idea is to prove knowledge of the ID related secrets without revealing it. The following protocol of Chaum, Evertse and van de Graaf [ChEG87] in figure 4 allows proving possession of a secret logarithm a for some number z with $a \dashv\triangleright\!\!\!\vdash z$. The value z is known to the verifier before the protocol starts. Repeating steps 1 and 2 for m times, the prover can have successfully cheated with probability 2^{-m}. The verifier gains no knowledge about a.

	Prover	Channel	Verifier
	Choose random numbers $r_1, \ldots, r_n$ $s_j := g^{r_j} \bmod p$	$\Longrightarrow$	receives $\{s_1, \ldots, s_n\}$
1	receive challenge (k, ϵ)	$\Longleftarrow$	choose $k \in \{1, \ldots, n\}, \epsilon \in \{0, 1\}$
2	$t_k := \epsilon a + r_k \bmod p$	$\Longrightarrow$	receives t_k and checks $g^{t_k} = z^{\epsilon} \cdot s_k \bmod p$

Figure 4: Zero Knowledge Proof of Chaum, Evertse, van de Graaf

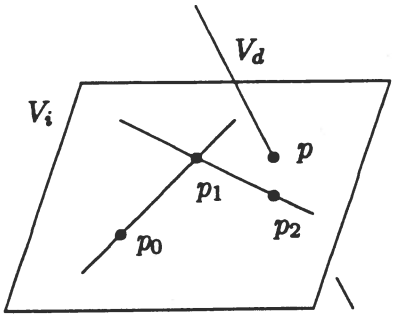

Figure 5: Realization of a monotone access structure in a geometry based secret sharing scheme: Giving Participant A the point p_0, participant B the point p_1 and giving p_2 to both participants C and D, we have found a solution for the access structure $ABC \vee ABD$.

2.4 Verifiable Secret Sharing in Geometry based Schemes

Recent results have shown how efficiently the homomorphic properties of discrete exponentiation for suitable finite fields can be exploited. Here we give a short description of a protocol for verifiable secret sharing dealing with general monotone access structures [Otte92, BeKO93]. The protocol is the first scheme for verifiable secret sharing that can be used with more complicated access structures than the commonly known threshold access structures. It is based on secret sharing with geometrical schemes such as the Simmons–Jackson–Martin scheme [SiJM91]. The scheme consists of a secret variety V_i of some n dimensional affine geometry $AG(n, q)$ over some finite field $GF(q)$, and a public known variety V_d. The secret to be distributed is the intersection of these two varieties

$$\{p\} = V_i \cap V_d$$

(see figure 5 for an illustration). Each shareholder possesses one or more points p_i in V_i in such a manner, that every designated subset of shareholders is able to construct V_i and therefore to derive the secret point p.

The main idea how to prove the claim, that a secret p was distributed according to a monotone access structure is to check the vector valued equations

$$p = p_0 + \sum_{i=i}^{m} \lambda_i (p_i - p_0) = y_0 + \sum_{j=1}^{r} \rho_j (y_j - y_0)$$

for $V_d = \langle y_0, \ldots, y_r \rangle$ and $V_i = \langle p_0, \ldots, p_m \rangle$ with coefficients λ_i and $\rho_j \in GF(q)$ under a suitable one way function. Using discrete exponentiation the last equations change to the form

$$g^p = \prod_{i=i}^{m} \left(\frac{g^{p_i}}{g^{p_0}} \right)^{\lambda_i} = \prod_{j=1}^{r} (g^{\rho_j})^{y_j - y_0} \tag{1}$$

By broadcasting the values g^p, λ_i, g^{p_i}, y_j and g^{p_j} each participant can check whether he has received on the one hand a valid share, and on the other hand if equation (1) holds (this implies that p lies in the intersection of V_i and V_d). A few other protocol steps ensure each participant, that $V_i \cap V_d$ has dimension 0 (that means p is the only point belonging to both varieties). Details of the solution can be found in the papers cited above; [Otte92] contains also a generalization of the shown approach dealing with a wider class of geometry based secret sharing schemes.

3. The KATHY Protocol

With the basic primitives mentioned above, a provably secure Key-Exchange-cum-Authentication protocol has been developed by Günther [Günt89] and by Bauspieß and Knobloch [BaKn89], incorporating an authenticated Diffie-Hellman-Scheme, whose correctness can be based on the Dlog-security assumption. The acronym KATHY expresses the central feature of this protocol, which embeds authentication within the key exchange. KATHY provides real-time authenticated log-in for a trusted session between any two participants, based on the following assumptions:

1. It is assumed that the system environment has (access to) a trusted authority SKIA (Secure Key Issuing Authority) in the role of a passport-office (not necessarily being online).
2. Every participant will be installed by the SKIA (once in a life-time).

The basic protocol steps are

1. **Setup of SKIA**
   SKIA chooses a prime p together with a primitive element g of $GF(p)$. It publishes $y_S \dashv\!\!\!\vdash x_S$ for some secret value x_S.
2. **Registration of a Participant A by SKIA**
   The name m_A of the participant is combined with the SKIA's secret. The participant receives values r_A and s_A together with m_A. It keeps s_A as its secret.
3. **Exchange of authentic keys between A and B**
   The participants generate a key depending on the secret key s_A of A, the name m_B of B, and the public key y_S of the SKIA, as well as a second key from s_B, m_A, and y_S.
4. **Interlock Procedure**
   To ensure A about B's authenticity, B has to prove that he was able to compute the two keys, and vice versa. Each participant can compute one of the keys only if he was registered by the SKIA and knows his secret key which corresponds to his name. Encryption and decryption of nonces (random challenges) R_A and R_B is used to verify the knowledge of the keys.

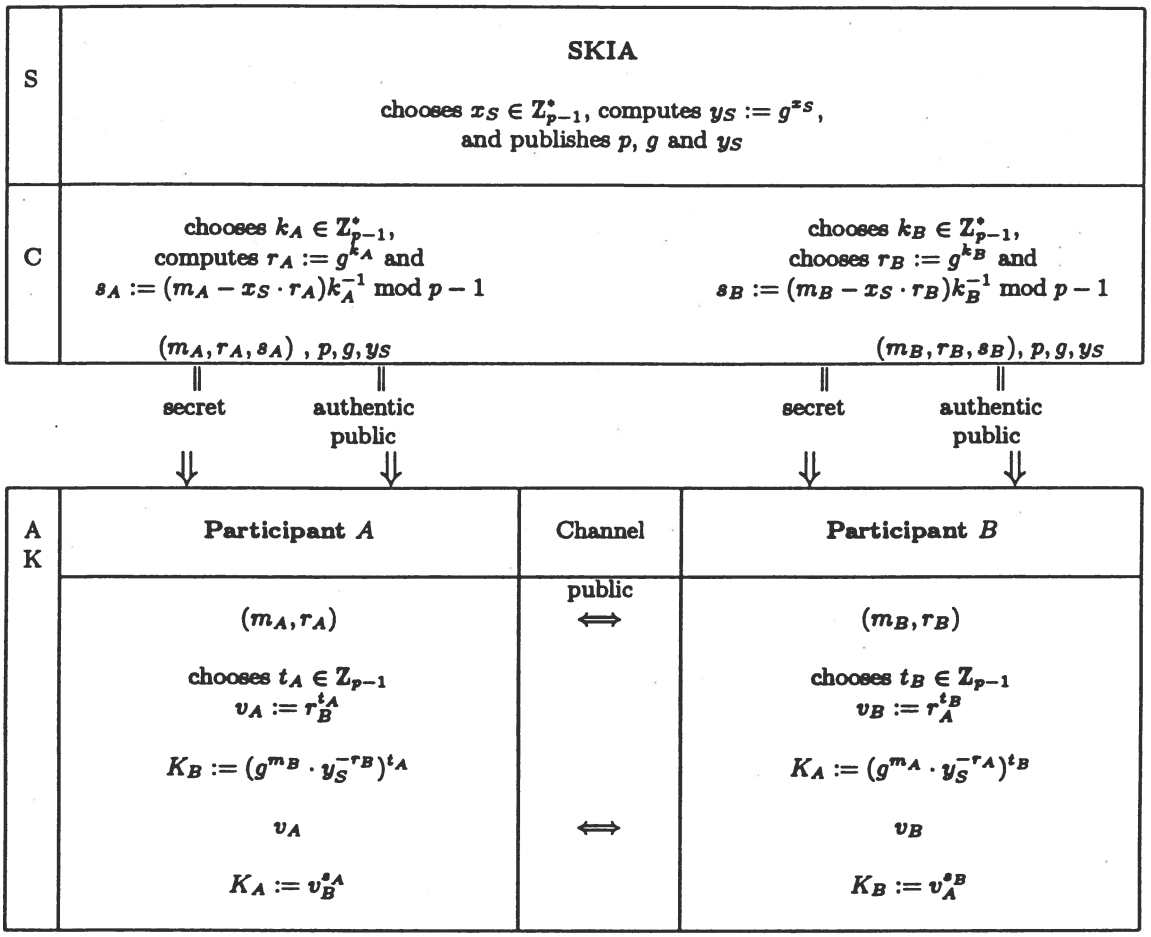

Figure 6: KATHY protocol with setup (S), certification (C) and authentication / key exchange (A, K) phase

Figure 6 shows a realization of the first three steps. Further details of the solution can be found in [BaKn89] and [Günt89]. KATHY will be used as a building block of the SELANE protocol which is described in the next section.

4. SELANE

SELANE was initially conceived as a LANSEC environment (see Bauspieß [Baus88]). Based on the KATHY Protocol, which guarantees a trusted path from participant to participant in a local network where the SKIA acts as an authentication server, the SELANE System consists of

- Authenticated Access based on the Protocol KATHY
- Confidential Session Communication according to independent Encipherment Algorithms
- Synchronization, Escape and End-of-Session management
- Automatic Reauthentication and Key Progression after the guaranteed security bounds of the Session-Encryption has been reached.

4.1 Implementations

SELANE has been implemented on common processors such as MC680xx, Intel 80x86 and SPARC processors, under UNIX, MS/DOS and the MacIntosh Operating System. Using the CPUs of SUN SPARCstation 10/30 authentication requires less than 250 milliseconds and is therefore practically invisible in the login procedure. Using SELANE some TCP/IP based services such as `telnet`, `rsh` or `rcp` have be supplemented with additional security features.

The encipherment algorithm is designed to run with additional hardware at network transmission speed. Reauthentication is carried out in the background, practically invisible. Special hardware modules have been developed at the E.I.S.S. to meet the higher performance requirements of central host CPUs serving a large number of clients at bulk traffic rate [Otto90]. This high-speed hardware modules are available as PCBs with suitable bus adapters and system interfaces for IBM PCs and SCSI.

4.2 Essential features

It should be noted that owing to the features of the KATHY protocol the SKIA

- does not need to keep any secret database after users have been issued their certificates
- can be operated off-line
- rather plays the role of a reference witness than that of a system monitor with need-to-know-everything.

These latter properties arose out of the original requirements of a large open distributed university computing environment regulated by national data privacy legislation. They provide features which make SELANE an interesting option for an truly Open Distributed System Security Environment.

5. SELANE as Open Distributed System Security Environment

Although SELANE primarily has been designed as a LANSEC System with the essential goal of authenticated access control and end-to-end user confidentiality at high performance rates, its architecture is well suited to provide system security throughout open distributed systems, (see Horster and Knobloch [HoKn91]).

5.1 Naming, Key Management and Authentication

The protocol has effectively been implemented using the format of Internet packets thus fully using the world-wide accepted naming tree. The role of a local network SKIA is fully compatible with that of the X.509 Directory Authentication Framework.

5.2 Transitivity and Delegation through a Network

The special structure of the authentication protocol not only allows a direct implementation of the X.500 recommendations. It is especially suited to authenticate participants in such a way that the validity of an authentication chain can be recomputed without exposing the private secret of each authenticator node. This fact not only provides an additional security feature, but also an unprecedented compressibility of authentication data to make feasible the use of smart cards as identification and authentication tokens. With this special construction SELANE supports the X.509 feature allowing an authentication through already 'known' sub-nodes of another branch of the network.

A token can hold the necessary authenticator information for each participant's 'acquaintances'. Also, the compressibility of authentication data allows a rather decentralized network management as a high degree of transitivity will be reached through delegation. The arithmetic structure of the SELANE protocol in particular supports the establishment of two independent directed authentication chains. This so called Bipolar Authentication allows participants to authenticate their partner through a reference point ('acquaintance') of their own choice, rather than trusting a single authority.

6. Advantages over Established Protocols

6.1 Network Authentication Management

As described above, the use of the exponential one way function provides transitivity throughout the network without large amounts of directory and authentication path information. SELANE fully incorporates the idea of a passport-token oriented network security system requiring the availability of authentication servers only at the time of installation, but not for real time operation, while KERBEROS [Kerb89] or CHIMAERA [Chim90] do require this latter property.

The security defects of X.509 as for instance described by I'Anson and Mitchell [AnMi90] are overcome in SELANE by the use of the proper one way exponential function. Problems arising in KERBEROS [Kerb89] due to the centralized role of the authentication servers do not exist in SELANE as it has been designed for open systems without central servers. This was recently carried out by Klein [Klei93].

6.2 Encryption

Authentication and key exchange have been uncoupled from the session-communication confidentiality through the use of independent enciphering algorithms. KATHY can provide an authenticated session key private to both participants only. The twin role of the KERBEROS head node as authentication server and system monitor, with the ability to act as a Big Brother as it knows the session keys, is not present in SELANE.

6.3 Security

Basing TESS on the Dlog-problem, which is considered as being even harder than factoring, gives this toolbox the highest security amongst all public key systems known today. The non-existence of an a-priori trapdoor for this system provides some superior features with respect to undeniable signatures or non-repudiable proofs of identity.

6.4 Provable Correctness and Completeness

The clear algebraic structure of proper one way functions (rather than trapdoor functions) facilitate a proper evaluation of the SELANE protocol. A correctness proof is essentially reduced to the proof of correct implementation of arithmetics. Completeness proofs also pose well defined problems, as the protocol is based on algebraic equations over conventional algebraic structures. An additional correctness proof using an extension of the logic of authentication of Burrows, Abadi, and Needham [BuAN89], which includes rules dealing with the algebraic structure of SELANE, is actually under consideration. An analysis of the SELANE protocol considering the different trust aspects of authentication protocols can be found in [YaKB93].

6.5 Portability and Migration to SELANE

With the option of a switch-on/off confidentiality module to be chosen for each application, the SELANE-System is freely available. It could therefore be adopted for any Open Information System or Open System Environment Standard without restriction. The portability is guaranteed, as the authentication part only comprises integer arithmetics (C-source code is available from E.I.S.S., cf. [Stem90]) while the optional encryption could be agreed upon in each single application.

Conventional security protocols such as KERBEROS and DSSA resting on both public key algorithms (such as Diffie-Hellman or RSA) and symmetric encryption via DES can easily be extended to implement SELANE. Note that RSA is based on taking powers modulo the RSA-integer N

$$x \rightarrow x^e \bmod N$$

while TESS uses exponentiation modulo a prime p

$$x \rightarrow g^x \bmod p$$

so the same basic algorithm is the core of either protocol. As the SELANE-session confidentiality is provided by a fast symmetric cipher, DES could serve in this role as well. A migration to SELANE therefore is only an evolutionary step at system level.

7. Conclusion

TESS is being developed by the E.I.S.S. as a toolbox of security kernel primitives for confidentiality, authenticity, and integrity. The SELANE-System is the package most advanced at present. Further applications are the Electronic Exponential Signature (EES) developed for EDI purposes and banking applications.

The exponential security system can also be a building block in establishing a mechanism called *Democratic REference MONitor* (DREMON), providing a system engineering tool for the purposes of confidentiality, integrity, authenticity as well as audit and control for Verifiable Open Distributed System Security Environments.

The structure of SELANE is based on the modular separation of key management and authentication from confidentiality algorithms. For the implementation of the former task, commutative one way functions are needed, while for the latter conventional symmetric ciphers suffice. In basing the authentication procedure on the concept of the ElGamal signature scheme, SELANE is well suited to provide one of the first implementations of the new U.S. digital signature standard independently of the decision on the encryption algorithm to be chosen. The strong algebraic theory of the underlying data types makes this system to be amongst the few Computer Security Systems that will be able to comply with the European IT-Security Evaluation Criteria [ITSE91].

References

[AdMa93] L. M. Adleman, J. DeMarrais: *A Subexponential Algorithm for Discrete Logarithms over all Finite Fields*, Santa Barbara, Crypto '93, Preprints

[AnMi90] C. I'Anson, C. J. Mitchell: *Security Defects in CCITT Recommendation X.509*, Technical Memo, HP Labs, Bristol, Jan. 1990

[Baus88] F. Bauspieß: *SELANE*, Studienarbeit, Fakultät für Informatik, Universität Karlsruhe, 1988

[BaKn89] F. Bauspieß, H.-J. Knobloch: *How to keep Authenticity Alive in a Computer Network*, Eurocrypt '89, Advances in Cryptology, LNCS 434, Springer-Verlag, Berlin, 1989, pp. 38–46

[Beth88] Th. Beth: *Efficient Zero-Knowledge Identification Scheme for Smart Cards*, Eurocrypt '88, Advances in Cryptology, LNCS 330, Springer-Verlag, Berlin, 1988, pp. 77–84

[BeAV90] Th. Beth, G. Agnew, S. A. Vanstone: *What one should know about Public Key Algorithms – Today!*, Proceedings SECURICOM '90.

[BeGo89] Th. Beth, D. Gollmann: *Algorithm Engineering for Public Key Algorithms*, IEEE JSAC, Vol. 7, No. 4, pp. 458–466, 1989

[BeKO93] Th. Beth, H.-J. Knobloch, M. Otten: *Verifiable Secret Sharing for Monotone Access Structures*, Proceedings of the 1st ACM Conference on Computer and Communications Security, Fairfax, USA, November 1993, to be published

[BeSc91] Th. Beth, F. Schaefer: *Non-Supersingular Elliptic Curves for Public Key Cryptosystems*, Eurocrypt '91, Advances in Cryptology, LNCS 547, Springer-Verlag, Berlin, 1991 pp. 316–327

[BuAN89] M. Burrows, M. Abadi, R. Needham: *A Logic of Authentication*, DEC-SRC, Research Report Series No. 39, 1989

[ChEG87] D. Chaum, J.-H. Evertse, J. van de Graaf: *An Improved Protocol for Demonstrating Possession of a Discrete Logarithm and Some Generalizations*, Eurocrypt '87, Advances in Cryptology, LNCS 304, Springer-Verlag, Berlin, 1988, pp. 127–141

[Chim90] A. Tarah, C. Huitema: *CHIMAERA: A Network Security Model*, Proc. ESORICS '90, afcet, 1990, pp. 127–145

[DiHe76] W. Diffie, M. E. Hellman: *New Directions in Cryptography*, IEEE Trans. Inf. Theory, IT-22, 1976, pp. 664–654

[ElGa85] T. ElGamal: *A public key crypto-system and signature scheme based on discrete logarithms*, IEEE Trans. Inf. Theory, IT-31, 1985, 469–472,

[Günt89] C. Günther: *Diffie-Hellman and El-Gamal Protocols With One Single Authentication Key*, Eurocrypt '89, Advances in Cryptology, LNCS 434, Springer-Verlag, Berlin, 1989, pp. 29–37

[HoKn91] P. Horster, H.-J. Knobloch: *Discrete Logarithm Based Protocols*, Eurocrypt '91, Advances in Cryptology, LNCS 547, Springer-Verlag, Berlin, 1991, pp. 399–408

[ITSE91] ITSEC: *Harmonised Criteria of France, Germany, the Netherlands, the United Kingdom*, Brussels, 1991

[Kerb89] Network Working Group J. Kohl, B. C. Neumann, J. Steiner: *MIT Project Athena: The Kerberos Network Authentication Service*, Draft 2, MIT, November 1989

[Klei93] B. Klein: *Authentifikationsdienste für sichere Informationssysteme*, Dissertation, Universität Karlsruhe, 1993, to be published

[Odly84] A. M. Odlyzko: *Discrete logarithms in finite fields and their cryptographic significance*, Eurocrypt '84, Advances in Cryptology, LNCS 209, Springer-Verlag, Berlin, 1985, pp. 224–314

[Otte92] M. Otten: *Mehrparteienprotokolle und Korrektes Verteilen von Geheimnissen*, Diplomarbeit, Fakultät für Informatik, Universität Karlsruhe, 1992

[Otto90] C. Otto: *SELANE-Hardwareentwicklung*, Diplomarbeit, Fakultät für Informatik, Universität Karlsruhe, 1990

[PoHe78] S. C. Pohlig, M. E. Hellman: *An improved algorithm for computing logarithms in GF(p) and its cryptographic significance*, IEEE Trans. Inf. Theory, IT-24, 1978, pp. 106–111

[Scha93] F. Schaefer-Lorinser: *Arithmetik auf elliptischen Kurven zur Konstruktion kryptographischer Einwegfunktionen*, Dissertation, Universität Karlsruhe, 1993

[Schn89] C. P. Schnorr: *Efficient Identification and Signatures for Smart Cards*, Crypto '89, Advances in Cryptology, LNCS 435, Springer-Verlag, Berlin, 1989, pp. 239–252

[SiJM91] G. J. Simmons, W.-A. Jackson, K. Martin: *The Geometry of Shared Secret Schemes*, Bulletin of the Institute of Combinatorics, Winnipeg Canada, January 1991

[Stem90] S. Stempel: *SELANE Pilot-Implementierung*, Diplomarbeit, Fakultät für Informatik, Universität Karlsruhe, 1990

[YaKB93] R. Yahalom, B. Klein, Th. Beth: *Trust Relationships in Secure Systems – A Distributed Authentication Perspective*, Proceedings of the IEEE Conference on Research in Security and Privacy, 1993.