Privancy Enhanced Fast Mutual Authentication in 5G Network Using Identity Based Encryption

Mohsin Khan* and Valtteri Niemi

Department of Computer Science
P.O. Box 68 (Gustaf Hllstrmin katu 2b)
FI-00014 UNIVERSITY OF HELSINKI, FINLAND
E-mail: {mohsin.khan, valtteri.niemi}@helsinki.fi
*Corresponding Author

Abstract

Subscription privacy of a user has been a historical concern with all the previous generation mobile networks, namely, GSM, UMTS, and LTE. While a little improvement have been achieved in securing the privacy of the long-term identity of a subscriber, the so called IMSI catchers are still in existence even in the LTE and advanced LTE networks. Proposals have been published to tackle this problem in 5G based on pseudonyms, and different public-key technologies. This paper looks into the problem of concealing long-term identity of a subscriber and presents a technique based on identity based encryption (IBE) to tackle it. The proposed solution can be extended to a mutual authentication and key agreement protocol between a serving network (SN) and a user equipment (UE). This mutual authentication and key agreement protocol does not need to connect with the home network (HN) on every run. A qualitative comparison of the advantages and disadvantages of different techniques show that our solution is competitive for securing the long-term identity privacy of a user in the 5G network.

1 Introduction

The NGMN Alliance has pointed out the privacy of a user as a requirement of the 5G network [**?**]. When a user equipment (UE) tries to connect to a network, the UE has to identify itself using an identifier. Once the UE is identified, an authentication protocol is run between the UE and the network. There are two types of attackers against the user privacy. A passive attacker just listens to the radio communication and tries to figure out identity of the user. An active attacker may transmit some radio messages itself. It is easier to protect against a passive attacker than an active attacker. Since 2G (GSM) the network has used temporary identities to protect against passive attackers. However, even in the LTE network the permanent identity is not protected against active attackers.

We discuss solutions to conceal the long-term identifier known as international mobile subscriber identity (IMSI) during the identification phase. These solutions are based on pseudonyms and public-key encryption. The pseudonym based approaches require to maintain a synchronization of pseudonyms between the UE and the HN. We discuss solutions based on certificates and root-key for the category of public key. Public-key based solutions do not require any synchronization. However, the public-key based solutions have higher cost both in terms of communication and computation.

We propose a novel solution based on identity based encryption (IBE). One additional advantage of our solution is that, it also works as a mutual authentication protocol between SN and UE without the involvement of the HN every time the authentication is needed. This advantage can not be achieved using root-key based approach. This advantage can be achieved using certificate based approach, but it is the heaviest in terms of communication and computation. We evaluate our solutions based on the following criteria: (1) Immunity to attackers, (2) Parts of the IMSI concealed, (3) Signalling overhead, (4) Latency, (5) PKI complexity, (6) Public-key revocation, etc. The choice of the solution depends on how much we want to achieve. Our solution based on IBE becomes a competitive one by meeting most of the important requirements.

2 3GPP-defined Aspects of Mobile Networks

A subscription describes the commercial relationship between the subscriber and the service provider, cf. 3GPP TR 21.905 [**?**]. A subscription identifier uniquely identifies a subscription in the 3GPP system and is used to access

networks based on 3GPP specifications. Subscription privacy refers to the right to protect any information that can be used to identify a subscription to whom such information relates. This definition of privacy suggests to protect any personally identifiable information (PII) from an attacker. While it may be difficult to draw a clear boundary between PII and non-PII, the long-term identifier is surely a PII.

2.1 System Overview

In the case of GSM, 3G (UMTS) and 4G (LTE) networks, IMSI is a long-term identity of a subscriber. An IMSI is usually presented as a 15 digit number but can be shorter. The first 3 digits are the mobile country code (MCC), followed by the mobile network code (MNC), either 2 digits or 3 digits. The length of the MNC depends on the value of the MCC. The remaining digits are the mobile subscription identification number (MSIN) within the network [**?**].

In order to present an easily comprehensible discussion, we need to know what are the entities and communication interfaces are involved in this identification process. We also need to know which entities can be entrusted with the IMSI of a subscriber. As the architecture of 5G is yet to be finalized, we present an abstraction of the involved entities and assume that whatever the architecture of 5G will eventually be, it will contain something for each of these entities and something for each of these interfaces. Figure 1 shows the abstraction. The abstraction involves the UE, SN and HN. Note that in a non-roaming situation, the SN and HN are the same network. There are two more entities which are not part of the network but relevant in our discussion, because they attack the network. They are passive IMSI catcher (PIC) and active IMSI cather (AIC).

The logical interface between UE and SN is initially unprotected. The logical interface between SN and HN is protected. The PICs eavesdrop on the UE-RAN interface when it is unprotected to extract an IMSI. The AICs impersonate a legitimate SN and run a legitimate looking protocol with the UE in order to find out the IMSI.

HN and UE both know the IMSI and they are trusted. Both of PIC and AIC are untrusted. It is in principle possible not to trust SN. However, by other specifications in 3GPP TS 33.106 [**?**] and TS 33.107 [**?**], it is required to reveal IMSI to the SN to enable lawful interception (LI) without involving HN.
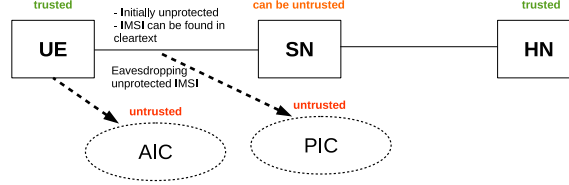
Figure 1 High-level security architecture

2.2 Current Solution Approach and its Weakness

One approach of protecting IMSI privacy is to use a temporary identifier instead of the actual IMSI and keep changing the temporary identifier frequently. Note that the temporary identifier has to be assigned confidentially. Different entities of the network may assign different temporary identifiers to the UE.

In the LTE network, the temporary identifier assigned by an SN is called globally unique temporary identity (GUTI) and the HN does not assign any temporary identifier to the UE. However, during the initial attachment of a UE to the SN, the UE has neither a GUTI nor a security context with the SN that can assign it with a GUTI. Besides, GUTI can be lost by either one or both of the UE and the SN. This would force the UE to reveal its IMSI to the SN to keep itself from permanently locked out of the network.

This problem gives an opportunity to an AIC who impersonates a legitimate SN and forces the UE to run the initial attachment protocol. This also gives an opportunity to a PIC to eavesdrop the IMSI sent in cleartext. Solutions [**?**, **?**, **?**, **?**] have been proposed by using temporary IMSI known as pseudonym. While these solutions solve the cases of lost and unsynchronised GUTI, they still have the problem of lost or unsynchronised pseudonyms. Public-key technologies have also been considered as potential approach to solve this problem.

3 Discussion on Different Proposed Solutions

Before delving into different proposed those solutions, let us introduce some notation.

1. $hnid, snid = MCC||MNC$ identifies the HN and SN respectively
2. e_A, d_A is the public and private key of entity A respectively

3. $\mathcal{X}_{A,B}(e_A, e_B)$ is the certificate of the public key e_A of A. The certificate can be verified by anyone who considers B as a root CA using the public key e_B. The certificate is a guarantee from B that the public key e_A is owned by A .

4. E, D are encryption and decryption functions so that $D(E(M, K), K) = M$.

5. $S(M, K)$ is the signature of message M signed by the key K

3.1 Solution Based on Pseudonyms:

Pseudonym based solutions have been proposed in [**?, ?, ?, ?**]. In this kind of solutions, temporary identifiers called pseudonyms are assigned to a UE. Next time when the UE tries to identify itself to an SN, it uses a pseudonym instead of IMSI. Periodically, whenever there is an opportunity, the HN sends a new pseudonym to the UE with confidentiality and integrity protection. One such opportunity could be when the HN sends the authentication vector to an SN.

3.2 Solution Based on Certificate Based Public-key Cryptography

Use of certificate based public-key encryption to conceal long-term identity has been suggested in 3GPP TR 33.821 [**?**]. To use certificate based public-key cryptography, we need to figure out who are the root CAs and who else can be a CA, who own a public key, how a certificate can be revoked, and how the UE can be re-provisioned with a new root certificate if needed. Different solutions can be devised based on the choice of root CAs and other CAs. We provide a high-level description for few variants of certificate based solution.

3.2.1 Variant 1:

It uses a global root of trust. There is a global entity trusted by everyone. Using this trusted global entity, a chain of trust can be established. The SN presents the certificate to a UE trying to attach. The UE verifies the certificate. If the verification result is positive, the UE encrypts its IMSI using the public key of the SN and sends to the SN.

3.2.2 Variant 2:

In this variant the HN of a subscriber is the root CA. The HN generates a public-private key pair and generates a certificate of the public key signed by the HN itself. A UE is provisioned with this self signed certificate. An

SN interested to serve a UE obtains a certificate $\mathcal{X}_{snid,hnid}(e_{snid}, e_{hnid})$. The UE sends $hnid, e_{hnid}$ to the SN. The SN looks up for the certificate $\mathcal{X}_{snid,hnid}(e_{snid}, e_{hnid})$. In case it exists at the disposal of the SN, the SN sends it to the UE. The UE verifies the certificate. If the certificate is verified as valid, then the UE sends the IMSI to the SN encrypted by the public key e_{snid} of the SN.

3.2.3 Variant 3:

In this variant, there is no other CA than the root CA. Hence the chain of certificates is very short. Only an HN can be a CA. The certificates of all the SNs a UE might visit are pre-provisioned to the UE by the HN. When a UE attempts to attach to an SN, the UE encrypts the IMSI with the public key of the SN which is already provisioned to the UE. If the public key of an SN is revoked, the HN has to provision the revocation to the UE.

3.3 Solution Based on Root-key based Encryption

We use only one pair of public-private key pair in this approach. Such a technique has been proposed in 3GPP TR 33.899 in solution #7.3. This key pair is owned by the HN and we call it to be the root-key. The HN provisions the public key to all its UEs. Instead of sending the IMSI, the UE encrypts the IMSI with the public root key and sends the result to the SN along with the $hnid$. The SN sends the encrypted IMSI to the HN. The HN decrypts the IMSI and sends the IMSI back to the SN along with an authentication vector (AV).

3.4 Solution Based on IBE

In the next section we discuss the basic principles of IBE and present a solution of the identity privacy using IBE.

4 Details of the IBE Based Solution

4.1 How IBE works

The idea of IBE was proposed by Adi Shamir in 1984 [?]. In IBE, the public and private keys of a receiver are computed from the identity of the receiver in conjunction with the public and private key of a trusted third party respectively. A sender does not need to authenticate the public key of a receiver each

time the sender and the receiver agree on a security context. The authenticity
of the public key in IBE is guaranteed by the trusted third party.

Usually in IBE, the trusted third party is known as the private key gen-
erator (PKG). The private key of the receiver has to be provisioned to the
receiver by the PKG. It is impossible to revoke the public key in IBE unless
the identity itself is revoked. Please note that a PKG knows the private keys
of all the receivers. As a result a PKG can decrypt any message sent by any
sender to any receiver. This implies that there must be a very high level of
trust in the PKG.

Dan Boneh and Matthew Franklin published a fully functional IBE
scheme in 2003 [**?**]. The security of this scheme was based on a natural
analogue of the computational Diffie-Hellman assumption. Based on this
assumption they showed that the new system has chosen ciphertext security
in the random oracle model. To make the revocation of public keys easier,
this scheme also suggests to use an expiry time as part of the identity of a
receiver. We use this suggestion in our solution. Clifford Cocks present an
implementation in 2001 [**?**] and show that the security of the implementation
is related to the difficulty of solving the quadratic residuosity problem.

4.2 Existing proposals of Using IBE in 5G Network

RFC 6508 [**?**] presents an algorithm SAKKE for establishment of a secret
shared value. Applications of SAKKE may include a date-time component
in their identity to ensure that identities and hence the corresponding private-
keys are only valid for a fixed period of time. Solution #7.11 in 3GPP TR
33.899 [**?**] uses IBE to protect the long-term identity according to RFC 6508.
However, the solution does not address the issue of revocation of the identity
based public-keys. RFC 6507 [**?**] describes a certificate-less signature scheme
based on IBE. In this scheme a string called public validation token (PVT)
randomly chosen by the PKG is assigned to an identity. Both the public
and private key of a receiver are computed using the PVT along with the
receiver's identity. So, the public key associated with an identity can be re-
voked by revoking the PVT. Solution #2.14 in 3GPP TR 33.899 presents an
authentication framework based on the signature scheme of RFC 6507 and
the authentication protocol EAP-TLS. This solution uses the PVT to revoke
the public key associated with an identity. However, in this solution it is not
clear how a UE can check if the public key of an SN has been revoked or not.

$$e_A \quad = \quad \text{Public key of A}, d_A = \text{Private key of A}$$

Private Key Generator
e_{PKG}, d_{PKG}

$$
\begin{aligned}
d_{Alice} &= f(d_{PKG}, Alice) \\
d_{Bob} &= f(d_{PKG}, Bob)
\end{aligned}
$$

d_{Alice}

d_{Bob}

Alice and Bob request for private key

Alice
$e_{Bob} = g(e_{PKG}, Bob)$
$M_c = E\left(M_p, e_{Bob}\right)$

Bob
$e_{Alice} = g(e_{PKG}, Alice)$
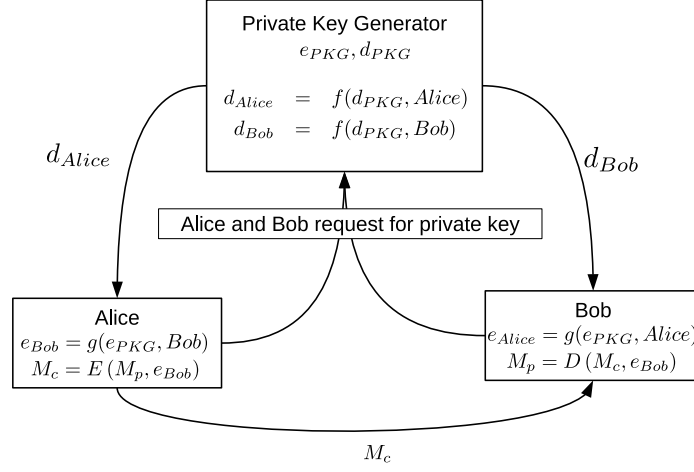$M_p = D\left(M_c, e_{Bob}\right)$

M_c

Figure 2 How IBE Works

4.3 The Proposed Solution

Next we present a protocol that serves the purposes of both privacy protected identification of UE and mutual authentication between UE and SN. This mutual authentication does not require a contact with the HN each time the protocol is run between a UE and an SN. In our solution we do not use PVT but instead use an expiry time with pre-agreed format. This expiry time can act as the PVT. If the public key of an identity needs to be revoked, the expiry time along with the identity is added to the revocation list. If the identity requires a new public key, the PKG uses another expiry time to compute the private key of the identity. The newly computed private key is then provisioned to the identity along with the the new expiry time. When the expiry time comes, all the public keys computed using the expiry time are automatically revoked. So, the revocation list does not need to include revocations whose expiry time is in the past.

4.3.1 Description of the proposed solution
The UE's HN acts as the PKG. The solution is pictorially presented in Figure ??. It has two different phases. In the first phase, the key generations and pro-
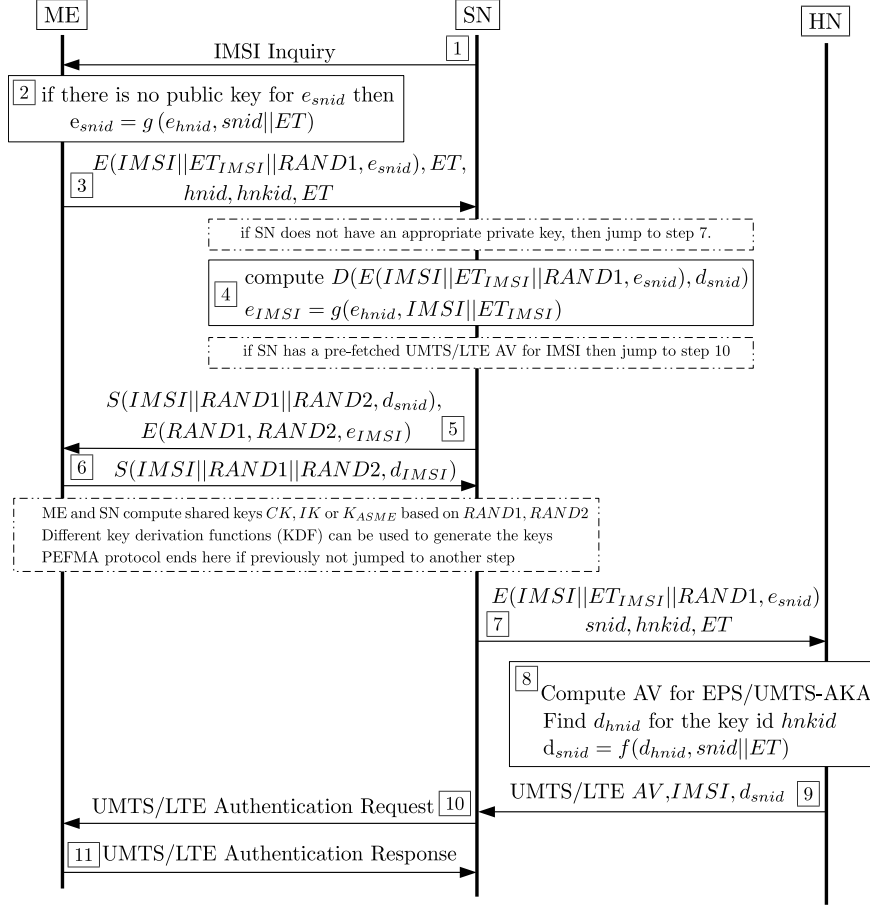
Figure 3 PEFMA

visioning take place. In the second phase the identification and authentication happens. The description follows:

- In step 1.1 the HN generates a public-private key pair e_{hnid}, d_{hnid}.
- In 1.2, the HN provisions the UE with e_{hnid} and d_{ue}. d_{ue} is generated using the private key d_{hnid}, $IMSI$, and a chosen expiry time ET_{eu}.
- In 1.3, the SN sends the *snid* to the HN. In 1.4 the HN chooses an expiry time ET and d_{snid} is computed considering $snid\|ET$ as the SN's identity.

- In 1.5, the HN sends d_{snid}, ET, e_{hnid} to the SN. The SN stores these information in its key-table.
- In 2.1, the SN broadcasts the $snid$.
- In 2.2, the UE sends $hnid, E(IMSI||ET_{ue}||RAND1, e_{snid}), ET$ to the SN.
- In 2.3, the SN looks for a suitable d_{snid} and if found, it jumps to step 2.8, Otherwise continues from step 2.4 and stops at 2.7
- In 2.4, SN sends $snid, E(IMSI||ET_{ue}||RAND1), ET$ to HN.
- In 2.5, HN computes the key d_{snid} using $d_{hnid}, snid$ and ET. Then HN decrypts the IMSI using d_{snid} and prepares an AV.
- In 2.6, HN sends $AV, IMSI, d_{snid}$ to SN. The SN stores d_{snid}, ET and in 2.7 uses the AV to run the EPS-AKA.
- In 2.8, SN decrypts the received message and compute e_{ue} using.
- In 2.9 HN sends the signature $S(IMSI||RAND1||RAND2, d_{snid})$ along with $E(RAND2, e_{ue})$ to the UE. The signature is verifiable by e_{snid} in the UE.
- In 2.10, the UE sends the signature $S(IMSI||RAND1||RAND2, d_{ue})$ to the SN which is verifiable by e_{ue}. If both UE and SN can verify the signatures as valid, the mutual authentication is completed successfully.

Note that the UE and the SN have successfully exchanged two randomly chosen values RAND1 and RAND2 with confidentiality protection. A symmetric key can be computed at both UE and SN using these random values and e_{hnid} using a function like key derivation function used in LTE security. There is also an alternative option of using Diffie-Hellman key exchange protocol.

4.3.2 Revocation of Public Keys

The ET used to generate the public key d_{snid} is quite near in the future, e.g., the day end. So, if the public key needs to be revoked, it would automatically be revoked when the expiration time comes. In this way, a compromised SN would be able mount an attack only for a short period of time. However, the SN would need to get new d_{snid} from the HN before the old d_{snid} expires.

When the public key of a UE is revoked, the IMSI and relevant ET is stored in a revocation list in the HN. An SN serving UEs of an HN has a copy of the list. The SN also periodically checks with the HN if there is any new revocations. Before computing the public key of the UE in step 2.8, the SN checks the revocation list. If it is revoked, the SN discards the message received from the UE and the authentication fails.

All the entries with expiry time older than current date-time can be removed from the revocation list, hence the revocation list will not grow to a very large size. This frequent private key exchange and refreshing the revocation list would create a bit increased traffic between an SN and HN. On the other hand, this increased traffic is not in the air interface but in the back haul network, which apparently is not very critical.

5 Comparison of Solutions

In this paper we have discussed two different categories of solutions: pseudonym based and public-key based. Different solutions [**?, ?, ?, ?**] have been and more could be devised based on pseudonyms. All these solutions would require the UE and the HN to synchronize their pseudonym states between a UE and the HN.

We have categorized the different public-key technologies into three categories: certificate based, root-key based and identity based. None of them require to maintain synchronization of states between a UE and the HN. But these solutions have some downsides. They need comparatively heavier computational resources, and the ciphertexts are longer which affect the latency. All these Solutions require a mechanism of key revocation.

In certificate based solutions there is a need of a global PKI. However, in some variants of certificate based solutions, the effort to manage a PKI can be reduced significantly. Certificate based solutions require an extra round trip between the UE and SN to exchange and verify the certificate. In a variant of a certificate based solution, this extra round trip could be removed at the expense of provisioning the certificate of an SN to a UE before the UE goes roaming to the SN. All the certificate based solutions have the requirement of exchanging certificates and verifying them. This creates signalling and computational overhead which consequently affect the latency.

The root-key based solution does not require any extra round trips or certificates, hence it has better signalling and computational overhead compared to certificate based. However, it still suffers from the increased latency in a roaming situation because every authentication needs to travel all the way to the HN. This is because no one else except the HN can decrypt the message sent by the UE. The solution creates also computational pressure in the HN.

We have proposed a novel solution based on IBE that can both accomplish the identification and mutual authentication. The solution does not need to maintain synchronized states between a UE and the HN. The solution does not require a global PKI and does not need certificates. Unlike the root-key

based approach, our solution does not need to involve HN each time authentication is needed. The aforementioned argument makes the IBE based solution a potential candidate to solve the problem in question. In Table **??**, we present a comparison among the different solutions based on different criteria.

Apparently pseudonym based solution is very good in most of the criteria. One downside of pseudonym based approach is, if the pseudonym is unsynchronized between UE and HN, the user has to visit the HN physically and get back to synchronized state by giving the IMSI in a trusted environment. The need of visiting the HN physically might make the pseudonym based solution a little clumsy. Variant 1 of certificate based approach is good in preventing AIC and also conceals $hnid$. But this is bad in many other important criteria because of exchanging and verifying certificates. Considering the concealment of $hnid$ with a bit less priority, the CertV1 is outperformed by both root-key based and IBE based solution. CertV2 and CertV3 can not even conceal $hnid$. So, the extra overhead of using Certv2 and CertV3 is not worth comparing to root-key and IBE. When comparing IBE and root-key, both of them are almost similar except that IBE based solution is extendible to a mutual authentication protocol between UE and HN. However, Cert1V can also be extended to a mutual authentication protocol.

If concealing $hnid$ is essential, then the only applicable solution is Certv1, the certificate based solution with global root of trust. If concealment of $hnid$ can be compromised, then the choice of the solution depends on the requirement of mutual authentication. If mutual authentication of UE and SN without involving HN is considered important and useful then IBE based solution is the winner. Otherwise, root-key based solution is just enough.

6 Conclusion

In this paper we have discussed different known approaches to conceal the IMSI. The solutions are based on pseudonyms and public-key encryption. We have proposed a novel solution based on identity based encryption that serves the purposes of both identification and mutual authentication. We have used expiry time as part of the identity of the entities in the system. We have presented a qualitative comparison between different solutions. We argue that identity based encryption is a competitive solution when concealing the home network identity is not necessary and mutual authentication in between a user equipment and a serving network is useful without connecting with the home network. The comparison is based on qualitative analysis based on known facts of public-key cryptography.

6.0.3 Acknowledgement.

The ends of words and sentences are marked by spaces. It doesn't matter how many spaces you type; one is as good as 100. The end of a line counts as a space.

One or more blank lines denote the end of a paragraph.

Since any number of consecutive spaces are treated like a single one, the formatting of the input file makes no difference to TEX, but it makes a difference to you. When you use LATEX, making your input file as easy to read as possible will be a great help as you write your document and when you change it. This sample file shows how you can add comments to your own input file.

Because printing is different from typewriting, there are a number of things that you have to do differently when preparing an input file than if you were just typing the document directly. Quotation marks like "this" have to be handled specially, as do quotes within quotes: " 'this' is what I just wrote, not 'that' ".

Dashes come in three sizes: an intra-word dash, a medium dash for number ranges like 1–2, and a punctuation dash—like this.

A sentence-ending space should be larger than the space between words within a sentence. You sometimes have to type special commands in conjunction with punctuation characters to get this right, as in the following sentence. Gnats, gnus, etc. all begin with G. You should check the spaces after periods when reading your output to make sure you haven't forgotten any special cases. Generating an ellipsis ... with the right spacing around the periods requires a special command.

TEX interprets some common characters as commands, so you must type special commands to generate them. These characters include the following: $ & % # { and }.

In printing, text is emphasized by using an *italic* type style.

A long segment of text can also be emphasized in this way. Text within such a segment given additional emphasis with Roman *type. Italic type loses its ability to emphasize and become simply distracting when used excessively.*

It is sometimes necessary to prevent TEX from breaking a line where it might otherwise do so. This may be at a space, as between the "Mr." and "Jones" in "Mr. Jones", or within a word—especially when the word is a symbol like *itemnum* that makes little sense when hyphenated across lines.

TEX is good at typesetting mathematical formulas like $x - 3y = 7$ or $a_1 > x^{2n}/y^{2n} > x'$. Remember that a letter like x is a formula when it denotes a mathematical symbol, and should be treated as one.

7 Notes

Footnotes[1] pose no problem.[2]

8 Displayed Text

The following is an example of an *itemized* list.

- This is the first item of an itemized list. Each item in the list is marked with a "tick". The document style determines what kind of tick mark is used.
- This is the second item of the list. It contains another list nested inside it. The inner list is an *enumerated* list.

  1. This is the first item of an enumerated list that is nested within the itemized list.
  2. This is the second item of the inner list. LATEX allows you to nest lists deeper than you really should.

  This is the rest of the second item of the outer list. It is no more interesting than any other part of the item.
- This is the third item of the list.

The following is an example of an *enumerated* list, two levels deep.

1. This is the first item of an enumerated list. Each item in the list is marked with a letter or number. The document style determines what kind of mark is used.
2. This is the second item of the list. It contains another enumerated list nested inside it.

   (a) This is the first item of an enumerated list that is nested within the enumerated list.
   (b) This is the second item of the inner list. LATEX allows you to nest lists deeper than you really should.

---

[1] This is an example of a footnote.
[2] And another one.

This is the rest of the second item of the outer list. It is no more interesting than any other part of the item.
3. This is the third item of the list.

The following is an example of a *description* list.

Cow Highly intelligent animal that can produce milk out of grass.

Horse Less intelligent animal renowned for its legs.

Human being Not so intelligent animal that thinks that it can think.

Quotations are implemented as lists. Here comes a sample quotation, repeated once to test paragraph indentation of additional paragraphs.

> Quotations are implemented as lists. Here comes a sample quotation, repeated once to test paragraph indentation of additional paragraphs.
> Quotations are implemented as lists. Here comes a sample quotation, repeated once to test paragraph indentation of additional paragraphs.

Mathematical formulas may also be displayed. A displayed formula is one-line long; multiline formulas require special formatting instructions.

$$x' + y^2 = z_i^2$$

Don't start a paragraph with a displayed equation, nor make one a paragraph by itself.

Example of a theorem:

Conjecture 1 *All conjectures are interesting, but some conjectures are more interesting than others.*

9 Tables and Figures

Cross reference should be labelled, e.g., as you can see in Table 2 and also in Table 1.

A major point of difference lies in the value of the specific production rate π for large values of the specific growth rate μ. Already in the early publications [**?**] it appeared that high glucose concentrations in the production phase are well correlated with a low penicillin yield (the 'glucose effect'). It

Table 1 Parameter set used in the model of Bunt [**?**].

$Q_{s,\mathrm{max}}$	[g/g DM h]	0.18
K_s	[g/L]	1.0
$Y_{x/s}$	[g DM/g]	0.5
$Y_{p/s}$	[g/g]	0.854
$Q_{p,\mathrm{max}}$	[g/g DM h]	0.0045
μ_{crit}	[h^{-1}]	0.01
k_h	[h^{-1}]	0.002
m_s	[g/g DM h]	0.025

Table 2 The spherical case ($I_1 = 0$, $I_2 = 0$).

Equil. Points	x	y	z	C	S
L_1	-2.485252241	0.000000000	0.017100631	8.230711648	U
L_2	0.000000000	0.000000000	3.068883732	0.000000000	S
L_3	0.009869059	0.000000000	4.756386544	-0.000057922	U
L_4	0.210589855	0.000000000	-0.007021459	9.440510897	U
L_5	0.455926604	0.000000000	-0.212446624	7.586126667	U
L_6	0.667031314	0.000000000	0.529879957	3.497660052	U
L_7	2.164386674	0.000000000	-0.169308438	6.866562449	U
L_8	0.560414471	0.421735658	-0.093667445	9.241525367	U
L_9	0.560414471	-0.421735658	-0.093667445	9.241525367	U
L_{10}	1.472523232	1.393484549	-0.083801333	6.733436505	U
L_{11}	1.472523232	-1.393484549	-0.083801333	6.733436505	U

has been confirmed recently [**?,?,?,?**] that high glucose concentrations inhibit the synthesis of the enzymes of the penicillin pathway, but not the actual penicillin biosynthesis. In other words, glucose represses (and not inhibits) the penicillin biosynthesis.

These findings do not contradict the results of [**?**] (on which Bunt [**?**] based their production kinetics) and of [**?**] which were obtained for continuous culture fermentations. Because for high values of the specific growth rate μ it is most likely (as shall be discussed below) that maintenance metabolism occurs, it can be shown that in steady state continuous culture conditions, and with μ described by a Monod kinetics

$$C_s = K_M \frac{\mu/\mu_x}{1 - \mu/\mu_x} \tag{1}$$

Pirt and Rhigelato determined π for μ between 0.023 and 0.086 h^{-1}. They also reported a value $\mu_x \approx 0.095$ h^{-1}, so that for their experiments μ/μ_x is in the range of 0.24 to 0.9. Substituting K_M in Eq. (1) by the value $K_M = 1$

Table 3 Parameter sets used by Bajpai and Reuß.

parameter		Set 1	Set 2
μ_x	$[\mathrm{h}^{-1}]$	0.092	0.11
K_x	[g/g DM]	0.15	0.006
μ_p	[g/g DM h]	0.005	0.004
K_p	[g/L]	0.0002	0.0001
K_i	[g/L]	0.1	0.1
$Y_{x/s}$	[g DM/g]	0.45	0.47
$Y_{p/s}$	[g/g]	0.9	1.2
k_h	$[\mathrm{h}^{-1}]$	0.04	0.01
m_s	[g/g DM h]	0.014	0.029

g/L as used by Bunt [**?**], one finds with the above equation $0.3 < C_s < 9$ g/L. This agrees well with the work of Bunt [**?**], who reported that penicillin biosynthesis repression only occurs at glucose concentrations from $C_s = 10$ g/L on. The conclusion is that the glucose concentrations in the experiments of Pirt and Rhigelato probably were too low for glucose repression to be detected. The experimental data published by Ryu and Hospodka are not detailed sufficiently to permit a similar analysis.

Bajpai and Reuß decided to disregard the differences between time constants for the two regulation mechanisms (glucose repression or inhibition) because of the relatively very long fermentation times, and therefore proposed a Haldane expression for π.

It is interesting that simulations with the [**?**] model for the initial conditions given by these authors indicate that, when the remaining substrate is fed at a constant rate, a considerable and unrealistic amount of penicillin is produced when the glucose concentration is still very high [**?**] Simulations with the Bajpai and Reuß model correctly predict almost no penicillin production in similar conditions.

The maintenance coefficient used by Bunt [**?**] ($m_s = 0.025$ g/g DM h) corresponds well to the value $m_s = 0.029$ g/g DM h (Set 2 of [**?**]), to the value $m_s = 0.024$ g/g DM h reported in [**?**], and to the value used in [**?**] ($m_s = 0.022$ g/g DM h) (1983). However, these values differ from the value in Set 1 of [**?**] ($m_s = 0.014$ g/g DM h). It is not clear where this difference originated from. Simulations indicated that the dynamic behaviour of the model is rather sensitive with respect to the value of m_s.

In the model of Bunt [**?**], at severe substrate limitation conditions, and thus most probably corresponding to endogenous metabolic behaviour, the biomass consumption due to maintenance and production requirements may exceed the conversion of substrate into biomass and μ eventually may become

Figure 4 Lange ijzeren brug, Dordrecht, The Netherlands.

negative. This situation may occur at the end of the growth phase during a fed-batch fermentation. For these conditions π is not defined. A straightforward extension of the $\pi(\mu)$ kinetics (10) could be $\pi(\mu \leq 0) = 0$, but there are some biochemical indications that the penicillin biosynthesis actually does not stop in that case.

Sample of cross-reference to a figure: Figure 4 shows a color image.

10 Headings

10.1 Subsection

[?, ?] based their model on balancing methods and biochemical knowledge. The original model (1980) contained an equation for the oxygen dynamics which has been omitted in a second paper (1981). This simplified model shall be discussed here.

10.1.1 Subsubsection

Carr and Goldstein [?] based their model on balancing methods and biochemical knowledge. The original model (1980) contained an equation for the oxygen dynamics which has been omitted in a second paper (1981). This simplified model shall be discussed here.

10.1.1.1 Paragraph. Carr and Goldstein [?] based their model on balancing methods and biochemical knowledge. The original model (1980) contained an equation for the oxygen dynamics which has been omitted in a second paper (1981). This simplified model shall be discussed here.

11 Equations and the Like

Two equations:

$$C_s = K_M \frac{\mu/\mu_x}{1 - \mu/\mu_x} \tag{2}$$

and

$$G = \frac{P_{\mathrm{opt}} - P_{\mathrm{ref}}}{P_{\mathrm{ref}}} \, 100 \, (\%) \tag{3}$$

Two equation arrays:

$$\frac{dS}{dt} = -\sigma X + s_F F \tag{4}$$

$$\frac{dX}{dt} = \mu X \tag{5}$$

$$\frac{dP}{dt} = \pi X - k_h P \tag{6}$$

$$\frac{dV}{dt} = F \tag{7}$$

and

$$\mu_{\text{substr}} = \mu_x \frac{C_s}{K_x C_x + C_s} \tag{8}$$

$$\mu = \mu_{\text{substr}} - Y_{x/s}(1 - H(C_s))(m_s + \pi/Y_{p/s}) \tag{9}$$

$$\sigma = \mu_{\text{substr}}/Y_{x/s} + H(C_s)(m_s + \pi/Y_{p/s}) \tag{10}$$

Let us also recall the very first equation 1.

Appendix

And this is my Appendix.

Appendix Subsection

Some text.

References

Biography

Here is space for a photograph of the author.

Author's name. A short vitae can be included here.