

On Keysizes for Electronic Voting Schemes

S. Srinivasan

September 2, 2010

Keysize Estimation

Keysize Estimation for Voting

Designs Considered

Keysize Estimation

- ▶ Academic papers define security in terms of security parameters.
- ▶ In the real world, security parameters need concrete values.
- ▶ Choosing concrete security parameters is an intricate and complex art.

Keysize Estimation: Factors Considered

- ▶ The lifetime and value of the asset.
- ▶ The inevitability of brute force attacks and existing better-than-brute-force attacks.
- ▶ The attack model.
 - ▶ Who is the attacker?
 - ▶ What are the resources at their disposal?
 - ▶ How will the resources develop during the lifetime of the asset? (for example Moore's Law)
- ▶ The possible cryptanalytic progress that may occur during the lifetime of the protected data.

Keysize Estimation: General Strategy

- ▶ Consider present state of the art regarding brute force and better-than-brute-force attacks if they exist.
- ▶ Make appropriate assumptions about the attack model and progress in hardware and techniques.
- ▶ Extrapolate keysize to match the security level based on the value of the asset.

Keysize Estimation: Factors Ignored

- ▶ Implementation issues
- ▶ Biased keys
- ▶ Timing/power/cache analysis
- ▶ Fault analysis
- ▶ Power consumption analysis

Minimum Key Lengths

Attacker	Budget	Hardware	Min Keysize	Recovery (d)
Hacker	\$0	PC	45	222
	\$400	FPGA	50	213
Small Org	\$10K	FPGA	55	278
Medium Org	\$300K	FPGA/ASIC	60	256
Large Org	\$10M	FPGA/ASIC	70	68
Intel Agency	\$300M	ASIC	75	73

Based on Blaze *et. al.* "Minimum Key Lengths for Symmetric Ciphers to Provide Adequate Commercial Security", 1996

Judge him by his leaps and bounces!

- ▶ Hackers have carried out attacks considered way beyond their capabilities.
- ▶ Recovery of 48-bits of DES key in 3 weeks with a small number of PC's.
- ▶ Key search distributed as part of a screen saver application.
- ▶ <http://answers.codebook.org/>

Keysize Estimation: Summary

- ▶ Keysize estimation is very complex.
- ▶ Determining equivalence between symmetric and asymmetric keysizes is particularly nuanced.
- ▶ Many studies, updated regularly (ECRYPT/ETSI/Lenstra-Verhaul/NESSIE/NIST/RSA)
- ▶ Broadly in alignment.
- ▶ Interpretations vary slightly due to different techniques used and different styles of presenting results.

Keysize Estimation for Voting

- ▶ End-to-End verifiable schemes like the ones we consider rely strongly on a bulletin board that displays encrypted ballot information.

Q and A

- ▶ How long should the bulletin board be secure against cryptanalysis?

Q and A

- ▶ How long should the bulletin board be secure against cryptanalysis?
 - ▶ At the very least, lifetime of the voter!!

Q and A

- ▶ How long should the bulletin board be secure against cryptanalysis?
 - ▶ **At the very least, lifetime of the voter!!**
 - ▶ “Everlasting Privacy” is desired, but we do not discuss that in this talk.

- ▶ Some voting papers discuss implementation issues wrt
 - ▶ Size of ciphertexts
 - ▶ Size of ZK proofs
 - ▶ Time taken to encrypt/decrypt and create/verify proofs.
- ▶ Estimates are often given based on a 1024-bit modulus in the factorization setting or 1024-bit prime field in the DL setting.

Q and A

- ▶ What security level does a 1024-bit modulus provide?

Q and A

- ▶ What security level does a 1024-bit modulus provide?
- ▶ What do ECRYPTII/NIST say about the 80-bit security level?

Q and A

- ▶ What security level does a 1024-bit modulus provide?
 - ▶ Equivalent to an 80-bit symmetric cipher!
- ▶ What do ECRYPTII/NIST say about the 80-bit security level?

Q and A

- ▶ What security level does a 1024-bit modulus provide?
 - ▶ Equivalent to an 80-bit symmetric cipher!
- ▶ What do ECRYPTII/NIST say about the 80-bit security level?
 - ▶ Use until 2010-2012!!

ECRYPTII Key Length Recommendations

Level	Protection	Symmetric	Asymmetric	Discrete Logarithm Key	Logarithm Group	Elliptic Curve	Hash
1	Attacks in "real-time" by individuals <i>Only acceptable for authentication tag size</i>	32	-	-	-	-	-
2	Very short-term protection against small organizations <i>Should not be used for confidentiality in new systems</i>	64	816	128	816	128	128
3	Short-term protection against medium organizations, medium-term protection against small organizations	72	1008	144	1008	144	144
4	Very short-term protection against agencies, long-term protection against small organizations <i>Smallest general-purpose level, 2-key 3DES restricted to 2⁴⁰ plaintext/ciphertexts, protection from 2009 to 2012</i>	80	1248	160	1248	160	160
5	Legacy standard level <i>2-key 3DES restricted to 10⁶ plaintext/ciphertexts, protection from 2009 to 2020</i>	96	1776	192	1776	192	192
6	Medium-term protection <i>3-key 3DES, protection from 2009 to 2030</i>	112	2432	224	2432	224	224
7	Long-term protection <i>Generic application-independent recommendation, protection from 2009 to 2040</i>	128	3248	256	3248	256	256
8	"Foreseeable future" <i>Good protection against quantum computers</i>	256	15424	512	15424	512	512

Figure: Screen shot from <http://www.keylength.com>

NIST Key Length Recommendations

Date	Minimum of Strength	Symmetric Algorithms	Asymmetric	Discrete Logarithm Key	Discrete Logarithm Group	Elliptique Curve	Hash (A)	Hash (B)
2007 - 2010	80	2TDEA*	1024	160	1024	160	SHA-1** SHA-224 SHA-256 SHA-384 SHA-512	SHA-1 SHA-224 SHA-256 SHA-384 SHA-512
2011 - 2030	112	3TDEA	2048	224	2048	224	SHA-224 SHA-256 SHA-384 SHA-512	SHA-1 SHA-224 SHA-256 SHA-384 SHA-512
> 2030	128	AES-128	3072	256	3072	256	SHA-256 SHA-384 SHA-512	SHA-1 SHA-224 SHA-256 SHA-384 SHA-512
>> 2030	192	AES-192	7680	384	7680	384	SHA-384 SHA-512	SHA-224 SHA-256 SHA-384 SHA-512
>>> 2030	256	AES-256	15360	512	15360	512	SHA-512	SHA-256 SHA-384 SHA-512

Figure: Screen shot from <http://www.keylength.com>

The Tragedy of Asymmetric Keysizes!

- ▶ Increasingly effective attacks against factorization and (non EC) DL, all better than brute force, have been found and are getting better each year!
- ▶ This leads to dramatically larger key sizes for higher security levels.
- ▶ This now become a real issues for applications like voting that require very high security levels.
- ▶ The ECRYPTII report specifically refers to this conundrum!

Homomorphic tallying

- ▶ Back end based on homomorphic tallying.
- ▶ Very attractive from the tallying point of view.
 - ▶ Individual votes are never decrypted, resistance to “Italian attacks”
 - ▶ Only final tally is revealed.

Homomorphic tallying

- ▶ Lots of intricate details.
- ▶ ZK proofs for every ciphertext, Additional ZK proof for ballot correctness.
- ▶ For a race with 5 candidates - 26 proofs.
- ▶ 83Kb of proof data per ballot with 1024-bit modulus (S&V, Adida and Rivest), 3 sec to compute each proof.
- ▶ Jointly generating an RSA modulus is **very** complicated.

Homomorphic tallying

- ▶ A single faked ballot that passes ballot checks can compromise the entire election. (?)

Our Implementations of Homomorphic Encryption Schemes

- ▶ Paillier Scheme.
- ▶ Damgaard-Jurik or Generalized Paillier.
- ▶ The Threshold Damgaard-Jurik Scheme, with trusted dealer (provided by Mads Jurik).

Aside: Patent Issues

- ▶ Paillier is patented! Patent owned by Gemalto.
 - ▶ US Patent: 7,054,444, filed Nov 25, 1999 awarded May 30, 2006
 - ▶ French: 99/00341, filed Jan 14, 1999
 - ▶ International: PCT/FR99/02918, filed Nov 25, 1999
- ▶ Patent may extend to cover Generalized Paillier, when the parameter $s = 1$.

Implications of Practical Keysizes

- ▶ For “long term protection” i.e. 256-bit security level, Paillier requires a 15,424-bit modulus!
- ▶ Ciphertexts are then 30,848-bits long!
- ▶ For Generalized Paillier, modulus is n^{s+1} and ciphertext is $(s + 1) \cdot n$ -bits long!
- ▶ Just about acceptable(?) for the 128-bit security level.

Timings

Let us consider some timings for the 128-bit security level.

	RSA	ElGamal	Paillier	(T)Paillier
Encryption	0.01 s	0.25 s	12 s	12 s
Re-encryption		0.2 s	6 s	6 s
Decryption	0.3 s	0.1 s	6 s	40 s
Mod size	4096-bit	4096-bit	8192-bit	8192 bit
Exponent size	17-bit, 4096-bit	256-bit	4096-bit	4096-bit

Java implementation, no optimizations.

Some Comments

- ▶ Schemes based on factorization (like RSA) become less and less attractive at higher security levels.
- ▶ This is true also for the (non EC) DL setting.
- ▶ There have been calls to withdraw RSA from government and commercial deployments.
- ▶ Unfortunately the same arguments hold for Paillier.
- ▶ Calls to move to cryptography over Elliptic Curves.

ECRYPT II Key Length Recommendations

Level	Protection	Symmetric	Asymmetric	Discrete Key	Logarithm Group	Elliptic Curve	Hash
1	Attacks in "real-time" by individuals <i>Only acceptable for authentication tag size</i>	32	-	-	-	-	-
2	Very short-term protection against small organizations <i>Should not be used for confidentiality in new systems</i>	64	816	128	816	128	128
3	Short-term protection against medium organizations, medium-term protection against small organizations	72	1008	144	1008	144	144
4	Very short-term protection against agencies, long-term protection against small organizations <i>Smallest general-purpose level, 2-key 3DES restricted to 2⁴⁰ plaintext/ciphertexts, protection from 2009 to 2012</i>	80	1248	160	1248	160	160
5	Legacy standard level <i>2-key 3DES restricted to 10⁶ plaintext/ciphertexts, protection from 2009 to 2020</i>	96	1776	192	1776	192	192
6	Medium-term protection <i>3-key 3DES, protection from 2009 to 2030</i>	112	2432	224	2432	224	224
7	Long-term protection <i>Generic application-independent recommendation, protection from 2009 to 2040</i>	128	3248	256	3248	256	256
8	"Foreseeable future" <i>Good protection against quantum computers</i>	256	15424	512	15424	512	512

Our Approach

- ▶ We have developed a cryptographic library of homomorphic cryptosystems.
- ▶ However, due to some of the reasons just mentioned, we have decided to look at other designs.

Mixnet Based schemes

- ▶ Mixnet based schemes can be implemented with the basic El-Gamal cryptosystem.
- ▶ El-Gamal can be instantiated in a number of groups.
 - ▶ Groups based on Safe/Schnorr primes.
 - ▶ Elliptic Curve Groups.

Elliptic Curve Groups

- ▶ Elliptic curve groups provide both size and speed advantages.
- ▶ It can be argued that ECC is currently the only “viable” asymmetric cryptography at the 256-bit security level.

ECRYPT II Key Length Recommendations

Level	Protection	Symmetric	Asymmetric	Discrete Key	Logarithm Group	Elliptic Curve	Hash
1	Attacks in "real-time" by individuals <i>Only acceptable for authentication tag size</i>	32	-	-	-	-	-
2	Very short-term protection against small organizations <i>Should not be used for confidentiality in new systems</i>	64	816	128	816	128	128
3	Short-term protection against medium organizations, medium-term protection against small organizations	72	1008	144	1008	144	144
4	Very short-term protection against agencies, long-term protection against small organizations <i>Smallest general-purpose level, 2-key 3DES restricted to 2⁴⁰ plaintext/ciphertexts, protection from 2009 to 2012</i>	80	1248	160	1248	160	160
5	Legacy standard level <i>2-key 3DES restricted to 10⁶ plaintext/ciphertexts, protection from 2009 to 2020</i>	96	1776	192	1776	192	192
6	Medium-term protection <i>3-key 3DES, protection from 2009 to 2030</i>	112	2432	224	2432	224	224
7	Long-term protection <i>Generic application-independent recommendation, protection from 2009 to 2040</i>	128	3248	256	3248	256	256
8	"Foreseeable future" <i>Good protection against quantum computers</i>	256	15424	512	15424	512	512

Elliptic Curve Groups

- ▶ Rather intricate setup leading many to question their security guarantees.
- ▶ Many researchers dislike ECC due to the many obscure patents.
- ▶ Thankfully, curves have been standardized and open source implementations are available.
- ▶ We have used the Bouncy Castle library to implement El-Gamal and a Distributed version over EC.

Acknowledgments

- ▶ Primary reference: ECRYPTII Yearly Report on Algorithms and Keysizes, 2009-2010.
- ▶ Screen shots from <http://www.keylength.com>, a fantastic resource for comparing various recommendations.

► Questions?

► Thank You!