T-79.512 Cryptology: Special Topics / Pairing-based Cryptography: Comments on "ID-based cryptography from bilinear pairings"

Alexey Vyskubov

February 13, 2003

1 Introduction

In this note I give comments on Tatiana Issaeva survey. The survey contains introduction to the problem, definitions of bilinear Diffie-Hellman assumption and identity-based security notions, descriptions of basic and full IBE schemes along with security proof for basic scheme.

The overall structure of the survey is quite good, it was easy to read and understand material. Unfortunately, there are some minor errors (or unclear points); nevertheless they are not very important.

2 Errors and unclear points in the survey

2.1 Section 2: the bilinear Diffie-Hellman assumption

There is small inconsistency in definitions: definition 1 uses q as groups order but definition 2 uses p.

2.2 Section 3: Identity-based encryption security definitions

It would be nice to have a picture showing how different parts of IBE scheme interoperate.

It is non clear until the middle of subsection 3.1 where system parameters params are used (they are used by $\mathsf{Encrypt}$ algorithm). This could be mentioned before or shown on picture.

Subsection 3.1 starts with definition of "scheme [...] semantically secure against an adaptive chosen ciphertext attack"; then "semantically secure" disappears and subsection 3.2 starts with the words "Semantic security is similar to chosen ciphertext security...".

The survey says nothing about Setup algorithm: is it randomised or deterministic? Probably it is not important but maybe it is better to mention it explicitly.

In the start of subsection 3.2 we read about "encryption queries" which are not encryption but extraction queries.

2.3 Section 4: Identity-based encryption based on pairings

In step 1 of Setup algorithm description suggested after running algorithm $\mathcal{G}$ chose generator $P \in G_1$. From the other side, in section 2 it was stated that $\mathcal{G}$ returns generator as a part of group description.

In step 3 of Setup algorithm hash function H_1 defined as having G_1 as a domain but in $\mathsf{Encrypt}$ algorithm description we see that the domain is G_1^*.

In the end of Setup algorithm description param used for system parameters but in the beginning of section 3 params was used.

In the theorem 1 number e is used but e is used as a name for pairing as well. Maybe the theorem needs small notice what e is.

In proof of lemma 1, in step 4 in "H_1-queries" the notation $Q_i = H_1(\mathsf{ID}_i)$ is used but H_1 does not exist at all: $\mathcal{B}$ only emulates it for $\mathcal{A}$.

In proof of lemma 1 step 1 in "Challenge": "Then $\mathcal{B}$ guesses $b' \in \{0, 1\}$ for b". This is not true; the value of b will be chosen during H_1-query algorithm run.

In the last paragraph before "Phase 2": the first entry of "C' using d_{ch}" probably should be "C using d_{ID}".

In the "Guess" section the survey says: "then $\mathcal{A}$'s view is identical to its view of real attack, since all responses to H_1 are uniformly distributed in and are valid". It would be nice to add where they are distributed. Moreover, I think that it is more correct to speak not about "identical view" but about "identical distribution of views".

In the next sentence "probability that $\mathcal{B}$ does not abort" should be "probability that $\mathcal{B}$ guessed right" or "returns the right answer on this step".

In the beginning of proof of lemma 2 some number c is defined but during the proof c denotes completely different object.

In the proof of lemma 2 in "Challenge" step: "defines C to be the ciphertext $C = \langle P_3, R \rangle$". It is wrong; only the first part (P_3) is the part of ciphertext, the second part is defined in the next sentence (and it is only the second part, not all the ciphertext as stated).

In probabilities calculations equal signs should be inequalities.

In the first sentence after probabilities calculations the first sign in inequality should be $\leq$ not $\geq$.

3 Conclusion

Despite of minor errors, the survey gives clear understanding of IBE scheme construction and shows in a quite detail security proof. Some non-important for understanding of main idea technical details are omitted (for example, the proof that in simulation the probability of some event is the same as in real attack); this allows catch the main idea quickly without drowning in complex calculations.