T-79.515 Cryptography: Special Topics / Pairing-based Crypthography: Comments on "ID-based signatures"

Sven Laur

March 10, 2003

# 1 Introduction

This note contains comments and suggestions about Alexey Vyskubov's survey *ID-based signatures*. The idea of ID-based cryptography was proposed already in 1984 by Shamir but recent discoveries by D. Boneh and M. Franklin have given a new means to achieve the goal. Normally public-key signing schemes require complex infrastructure for implementing authentic storage and delivery of public keys. Also the key revocation is problematic. ID-based signature schemes solve the first problem. Everybody is able to calculate public keys from ID-s using public hash function. The most important drawbacks are existence of trusted third party and more complex security requirements.

The survey examines two different types of ID-based signature schemes. First one is based on bilinear pairings and the second is based on gap groups. As all groups with bilinear pairings are gap groups the second scheme is more general. A security proof is sketched only for the second scheme because the current security proof of the first scheme was too short and hectic for survey.

The survey is well structured and gives reasonably detailed overview of signature schemes. There are some minor slips and some aspects that I would described slightly differently but generally the survey is good.

# 2 Comments and suggestions

We point out only significant errors, misleading wording and suggest some additional amendments which should make it more clear and easier to read.

**Equations** The overall use of mathematical notations is good but splitting equations is incorrect. The split equation mustn't contain duplicate binary operators(equation, plus, etc.). If the the equation in broken in text, the formula should be broken after binary operator. Alternatively if the formula is on the separate line, the formula should be broken before binary operator and second line should be tabulated.

**Comparing signature schemes** The similar structuring of the second and the third section makes it easy to compare signing schemes but implementation issues are treated only in the second section. A missing efficiency analysis of the second scheme makes it a bit inconsistent. As the group with bilinear pairing is a gap group one could really compare efficiency of both schemes.

**Obscure security proof** I agree with the Alexey that the security proof in the article [Pat] was too short and hectic to be presented in the survey. But still the connection between generalized ElGamal and the first ID-based scheme is worth mentioning and explaining shortly.

**Attack models** In a sense ID-based signing schemes are very similar to normal signing schemes therefore simple explanation why we need stronger notion of security would have been enlightening. Also a short analysis, how an adversary could obtain answers to the queries in the real world and qualitative likelihood estimate, is missing.

The attack model is well described but these extra commentaries would place the abstract model in the actual context.

**Reduction to given ID attack** The overall idea of the reduction is quite clear but informal description of the $\mathcal{A}_1$ is hard to digest in the first time. Better solution is to illustrate this by pseudo-algorithm of $\mathcal{A}_1$.

I agree with Alexey that the second observation requires more reasoning. It is not evident that adversary cannot effectively forge signature without querying public key $H_2(ID)$.

In case of doubt you should always find a more sound proof or alternatively counterexample or state in footnote that you are not convinced by original proof.

It is possible to prove that success must be less than $1-2/q$ under the assumption $q$ is prime[1]. The modified inequality has only minor impact to the following results.

For the proof we must know only the following details. A verifier knows public parameter $sP$, $s \neq 0$ which is fixed in the setup phase. The adversary must output a signature $(M, U, V)$ and $ID$ at the end or otherwise she has failed. Now the verifier has $U$, $V$ and $ID$ and he must check whether $(P, sP, U + H_1(M, U)H_2(ID), V)$ is Diffie-Hellman tuple. For a shake of contradiction let as assume that the adversary did not submit any queries about public key $H_2(ID)$ and thus the value $H_2(ID)$ is undetermined before verification. We discard possibility $H_1(M, U) = 0$ and treat other variants. The quadruple is a Diffie-Hellman tuple iff

$$s(\log U + \log H_1(M,U) \log H_2(ID)) \equiv \log V \mod q$$
$$(\log H_1(M,U))^{-1}(s^{-1}\log V - \log U) \equiv \log H_2(ID) \mod q$$

where logaritm is taken with respect to generator $P$ As the left hand side is constant and the right hand side varies uniformly over $\mathbb{Z}_q$ the success probability is $1/q$. Simple probability calculation formula gives success probability is less $2/q$.$\square$

**Reduction to CDHP** The interpretation of lemma 2 requires more detailed explanation. Because if an adversary $\mathcal{A}_1$ that has an advantage $10(q_S + 1)(q_S + q_H)/q$ then the working time $t_2 = 23q_{H_1}t_1q/((q_S + 1)(q_S + q_H))$ that is clearly exponential in $\log q$. Thus lemma 2 gives a lower bound of success rate which allows to mount the sophisticated attack. Of course if the adversary has non-negligible advantage over family of gap groups eventually the success will become larger than the lower bound and CDHP can be solved in polynomial time.

[1] For practical reasons it is sufficient because Wail and Tate pairings are defined on groups of prime order anyway.

# References

[Pat] K. Paterson. Id-based signatures from pairings on elliptic curves.